TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik

A Geometric Approach to the Projective Tensor Norm

Ein Geometrischer Zugang zur projektiven Tensornorm

Vom Fachbereich Mathematik
der Technischen Universität Darmstadt
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)
genehmigte Dissertation

von

Sandra Lang, M.Sc.

aus Groß-Gerau

Referent: Prof. Dr. Burkhard Kümmerer
Korreferent: Prof. Dr. Hans Maassen

Tag der Einreichung: 10. Dezember 2021
Tag der mündlichen Prüfung: 3. Mai 2022

Darmstadt - D 17
2022

A Geometric Approach to the Projective Tensor Norm

Doctoral thesis by Sandra Lang, M.Sc.

Referee: Prof. Dr. Burkhard Kümmerer
Co-Referee: Prof. Dr. Hans Maassen

URN: urn:nbn:de:tuda-tuprints-203316
https://tuprints.ulb.tu-darmstadt.de/20331/

Veröffentlicht von tuprints im Jahr 2022

Published by tuprints in 2022

CONTENTS

PREFACE

Danksagung

Als erstes möchte ich dem Fachbereich Mathematik der TU Darmstadt danken. Meinem Betreuer Prof. Dr. Burkhard Kümmerer danke ich dafür, dass ich Teil seiner wunderbaren Arbeitsgruppe, der C*-AG, bin. Vielen Dank, Burkhard, für den wertvollen mathematischen Austausch: für die hilfreichen Ideen, für deine Unterstützung und für die zahlreichen Möglichkeiten, die Mathematik zu leben. Auch vielen Dank an dich für die zahlreichen Gespräche und Erlebnisse, wo wir Gelegenheit fanden, Begeisterung über viele spannende Themen zu teilen. Danke auch für die Aufmunterung und die Motivation. Großen Dank an Malte Brandy, Andreas Gärtner, Albrun Knof, Florian Sokoli und Felix Voigt aus der C*-AG. Ich verbinde mit euch eine wunderschöne gemeinsame Zeit. Danke für den mathematischen Austausch und die Hilfe rund um diese Arbeit. Einen ganz besonderen Dank möchte ich an Felix und Albrun für das Korrekturlesen aussprechen. Dies war mir nicht nur eine große Hilfe, sondern auch ein wichtiger Ansporn. Meinen Dank an dich, Jonathan Schürr, auch für die Ideen und die Hilfe zur Homologie, drücke ich mathematisch aus: Die Telefonvorwahlen wichtiger Orte unserer Kindheit und Ausbildung bilden eine „2×2-Minore“, wie sie für diese Arbeit so wichtig ist:

Erfelden	Gründau
Darmstadt	Gelnhausen

0	6	1	5	8	0	6	0	5	8
0	6	1	5	1	0	6	0	5	1

Einen ganz großen Dank auch an meine Mama, meinen Papa, meine Schwester und meine Freunde für den tollen Ansporn. Einen Dank auch für die Ideen zu spezielleren Themen, so beispielsweise an Anke Pohl zur Homologie oder an die Forumsteilnehmer bei „Stackexchange“ zur Berechnung der Größe der „Parity Parts“.

Allen sei an dieser Stelle herzlich Dankeschön gesagt.

Sandra Lang

Zusammenfassung

Der Schwerpunkt dieser Arbeit liegt auf der projektiven Norm auf endlichdimensionalen reellen oder komplexen Tensorprodukten. Es gibt verschiedene mathematische Themengebiete mit Bezügen zur projektiven Norm, so zum Beispiel im Kontext der Operatoralgebren oder der Quantenphysik.

Die projektive Norm auf multipartiten Tensorprodukten gilt als weniger leicht zugänglich. Daher verwenden wir eine Methode aus der konvexen algebraischen Geometrie zur Approximation der projektiven Einheitskugel durch konvexe Obermengen, sogenannte Thetakörper. Für reelle multipartite Tensorprodukte erhalten wir Thetakörper, die der projektiven Einheitskugel nahe kommen. Dies führt beispielsweise zu einer Verallgemeinerung der Schmidt-Zerlegung. In einem zweiten Schritt wird die Methode auch für komplexe Tensorprodukte angewendet, in einem dritten Schritt auf separable Zustände.

In einem allgemeineren Kontext kann die projektive Norm mit Binomidealen in Verbindung gebracht werden, insbesondere mit Hibi-Relationen. In diesem Sinne beschäftigen wir uns auch mit einer Verallgemeinerung der projektiven Einheitskugel, hier Hibi-Körper genannt, und ihren Thetakörpern. Es hat sich gezeigt, dass viele Aussagen auch in diesem allgemeinen Zusammenhang gelten.

Quantenverschränkung

Verschränkung ist ein fundamentales Konzept in der Quanteninformationstheorie. Viele überraschende Effekte, die die klassische Mechanik von der Quantenphysik unterscheiden, stehen mit verschränkten Zuständen im Zusammenhang. In der klassischen Mechanik ist der Zustand eines aus mehreren voneinander unabhängigen Teilsystemen zusammengesetzten Systems vollständig durch die Zustände seiner Teilsysteme bestimmt. Dies ist bei verschränkten Zuständen nicht der Fall.

Viele Fragestellungen zur Verschränkung sind noch offen. Man könnte sich beispielsweise fragen, wie man herausfinden kann, ob ein Zustand verschränkt ist oder nicht. Dieses sogenannte Separabilitätsproblem zu lösen ist im Allgemeinen nicht einfach. Es gibt jedoch einige notwendige oder hinreichende Bedingungen an Verschränkung. So liefert eine affine Hyperebene, welche die Eigenschaft hat, dass alle separablen (d. h. nicht verschränkten) Zustände auf einer Seite liegen, eine hinreichende Bedingung. Sie ist dann ein sogenannter Verschränkungszeuge. Weiterhin gibt es sogenannte Verschränkungsmaße, welche den Grad der Verschränkung angeben. Neben gebräuchlichen Verschränkungsmaßen wie der von-Neumann-Entropie gibt es auch solche, welche auf der projektiven Tensornorm basieren, siehe [Arv] und [Rud]. Insbesondere ist die projektive Norm ein Verschränkungsmaß für reine Zustände.

Zur Verschränkung siehe auch die Übersichten in [HHHH], [Sok] oder [Aud].

Die projektive Tensornorm

Zusätzlich zur Verschränkung gibt es weitere Anwendungen der projektiven Norm, so zum Beispiel im Umfeld der Informationstheorie, Signalanalyse und komprimierten Erfassung. Hier ist sie wichtig bei der sogenannten Rekonstruktion von Tensoren von niedrigem Rang, siehe [RS2]. Andere gebräuchliche Namen für die projektive Norm sind „nukleare Norm" oder „größte Kreuznorm".

In dieser Arbeit betrachten wir die projektive Norm auf endlichdimensionalen reellen oder komplexen Tensorprodukten. Da es im Allgemeinen nicht einfach ist, die projektive Norm global zu bestimmen, konzentrieren wir uns auf einzelne Klassen von Vektoren wie beispielsweise die maximalen Vektoren, siehe [Arv]. Dies sind Einheitsvektoren, die die projektive Norm maximieren. Sie bestimmen auch eine wichtige Kenngröße der projektiven Einheitskugel, den innere Radius. Dies ist der Radius der größten in ihr enthaltenen euklidischen Einheitskugel.

Summen von Quadraten und Thetakörper

Zur Beschreibung von kompakten konvexen Mengen, wie beispielsweise Einheitskugeln von Normen oder der Menge der separablen Zustände, nutzen wir in dieser Arbeit eine spezielle Methode aus der konvexen algebraischen Geometrie, sogenannte Thetakörper. Thetakörper können immer dann betrachtet werden, wenn die Menge als die konvexe Hülle einer reellen affinen Varietät geschrieben werden kann, vergleiche [BPT]. In diesem Fall bilden deren Thetakörper eine Kette konvexer Obermengen, welche gegen die Ursprungsmenge konvergiert.

Ein Thetakörper wird durch affine Halbräume definiert. Die zugehörigen linearen Funktionale haben bestimmte reelle algebraische Eigenschaften im Zusammenhang mit Summen von Quadraten (Sos). Grundsätzlich sei die Sos-Methode "breit anwendbar, effektiv, überraschend mächtig und einfach", siehe [PS2].

Tatsächlich kann für unseren Zweck die projektive Einheitskugel in einem reellen, bipartiten, endlichdimensionalen Tensorprodukt vollständig durch einen Thetakörper beschrieben werden. Dies wurde unabhängig voneinander sowohl in [Sto] als auch in der Masterarbeit [Lang] gezeigt und ist eine wichtige Motivation dafür, sich nun auch auf die projektive Tensornorm auf multipartiten

Tensorprodukten zu konzentrieren. In dieser Hinsicht kann diese Arbeit als eine Fortsetzung der Masterarbeit angesehen werden.

Die projektive Norm und Thetakörper — Die Einheitskugel der projektiven Norm ist gleich der konvexen Hülle der Einheitsproduktvektoren. Die letztere Menge kann als reelle algebraische Varietät ausgedrückt werden, und zwar sowohl für reelle als auch für komplexe endlichdimensionale Tensorprodukte. Für den komplexen Fall nutzen wir den Ansatz in [Voi] und führen sogenannte *komplexe Thetakörper* ein. Damit kann die projektive Einheitskugel sowohl im Reellen als auch im Komplexen durch Thetakörper approximiert werden.

Dieser Ansatz bringt Tensorprodukte mit konvexer Optimierung, reeller algebraischer Geometrie und Summen von Quadraten in Verbindung.

Im Hinblick auf die Quantenverschränkung können Thetakörper also zu einem besseren Verständnis der projektiven Norm als Verschränkungsmaß beitragen. Ein anderer interessanter Gesichtspunkt ist, Thetakörper als neue und eigenständige Verschränkungsmaße in Ergänzung zur projektiven Norm anzusehen.

In dieser Arbeit untersuchen wir verschiedene Gesichtspunkte der projektiven Einheitskugel, reell und komplex, und ihrer Thetakörper, so neben den inneren Radien beispielsweise auch deren Geometrie oder das zugrundeliegende Ideal.

Da die Thetakörper-Methode zunächst für reelle Vektorräume gedacht ist, liegt es nahe, bei der Untersuchung mit dem reellen Fall zu beginnen und den komplexen Fall auf dieser Grundlage zu entwickeln. Dafür spricht auch, dass sich das Ideal für den komplexen Fall aus dem Ideal für den reellen ableiten lässt. An vielen Stellen war es möglich, Gemeinsamkeiten und Unterschiede der beiden Fälle herauszuarbeiten und auf ihre Besonderheiten einzugehen.

Es folgen nun die Hauptresultate dieser Arbeit bezüglich der Anwendung der Thetakörper-Methode auf die projektive Norm.

Reelle Tensorprodukte — Wir konzentrieren uns auf das multipartite Tensorprodukt $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, wobei $n \geqslant 2$. Die Anzahl der Tensorfaktoren ist beliebig.

Im Fall $n \in \{2, 4, 8\}$ gelingt es uns, eine Klasse maximaler Vektoren zu finden und damit den inneren Radius des projektiven Einheitsballs zu bestimmen. Die maximalen Vektoren definieren wir mittels sogenannter *Design-Hyperebenen*. Soweit wir wissen, waren maximale Vektoren in dieser Allgemeinheit bisher noch nicht bekannt. Die zugrunde liegende kombinatorische Methode setzt Tensorprodukte mit lateinischen Quadraten und orthogonalen Designs in Beziehung.

Im allgemeineren Fall $n \geqslant 2$ gelingt es uns, eine Klasse von Vektoren mit projektiver Norm 1 und damit eine obere Schranke an den inneren Radius des projektiven

Einheitsballs zu finden. Dazu stellen wir eine weitere Klasse affiner Hyperebenen vor, die sogenannten *Paritätshyperebenen*. Auch diese werden auf kombinatorische Weise definiert. Soweit wir wissen, war die Klasse von Vektoren mit projektiver Norm 1 im Allgemeinen noch nicht bekannt.

Die Resultate können als eine Verallgemeinerung der Schmidt-Zerlegung für bestimmte Klassen von Vektoren und als eine Ergänzung der Schranken in [Arv] für reelle Tensorprodukte angesehen werden.

Komplexe Tensorprodukte — Wir werden sehen, dass sich der reelle Fall in vielerlei Hinsicht als recht geradlinig erweist. Der komplexe Fall scheint dagegen komplizierter zu sein, sodass bereits Ergebnisse für kleine Dimensionen oder bipartite Tensorprodukte interessant sind.

Im Fall $\mathbb{C}^2 \otimes \mathbb{C}^2$ können wir zeigen, dass der erste komplexe Thetakörper gleich der projektiven Einheitskugel ist.

In allen anderen Fällen $\mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_r}$, wobei $r \geqslant 2$ und $n_1, \ldots, n_r \geqslant 2$, erhalten wir maximale Vektoren für den ersten komplexen Thetakörper. Insbesondere beträgt sein innerer Radius konstant $1/\sqrt{2}$, womit er relativ weit von der projektiven Einheitskugel entfernt ist. In diesem Sinne führen der reelle und der komplexe Fall zu qualitativ unterschiedlichen Ergebnissen für den ersten Thetakörper.

Separable Zustände — In einem dritten Schritt zeigen wir, dass die Thetakörper-Methode auf die Menge der separablen Zustände angewendet werden kann. Dies ermöglicht es, Sos-Polynome als Verschränkungmaß zu verwenden.

Das Ideal, welches wir dabei verwenden, wird aus dem Ideal für die projektive Norm auf komplexen Tensorprodukten generiert. Der Ansatz baut also in einem gewissem Sinn auf dem Tensorproduktfall auf.

Das Join-Meet-Ideal — Ein weiterer Schwerpunkt dieser Arbeit ist die Anwendung der Thetakörper-Methode auf eine Verallgemeinerung der projektiven Einheitskugel.

Die Motivation hierfür ist, dass die Menge der Produktvektoren im reellen Fall eine sogenannte Hibi-Varietät ist, die durch das sogenannte Join-Meet-Ideal induziert wird. Dieses Ideal wird von Hibi-Relationen erzeugt. Dies sind Polynome, deren Variablen über distributiven Verbänden indiziert sind, vergleiche hierzu [Hibi] und [HHO].

Nun bilden die Einheitsvektoren in der Hibi-Varietät wiederum eine Varietät, die durch das *Norm-Join-Meet-Ideal* induziert wird. Um auch den komplexen Fall zu verallgemeinern, führen wir das Konzept der *komplexen Hibi-Relationen* ein, um eine entsprechende reelle Varietät zu beschreiben. Die konvexe Hülle dieser

Varietäten, der *(komplexe) Hibi-Körper*, kann somit als eine Verallgemeinerung der projektiven Einheitskugel, reell und komplex, angesehen werden.

Wir werden sehen, dass viele Aussagen über die projektive Einheitskugel und ihre Thetakörper auch in diesem allgemeinen Kontext gelten. Während die ursprüngliche Motivation darin bestand, die projektive Norm zu verstehen, können die Einführung des Hibi-Körpers und die Ergebnisse nun auch als eigenständiger Beitrag zur Untersuchung des (Norm-)Join-Meet-Ideals angesehen werden.

Insbesondere unsere elementare Methode zur Charakterisierung des ersten Thetakörpers durch einen Spektraeder, vergleiche ergänzend auch [BCR], wird sich als sehr nützlich erweisen, insbesondere für die Anwendung auf Tensorprodukte. Für diesen Fall stellen wir auch ein Computerprogramm in der Sprache Python zur Verfügung.

Darüber hinaus entwickeln wir für das Verständnis der Struktur des Join-Meet-Ideals einen aus unserer Sicht neuen Ansatz über eine *Medianbasis*. Damit lassen sich auch bereits bekannte Aussagen wie beispielsweise über Gröbnerbasen in [HHO] auf vereinfachte Weise zeigen.

Übersicht

Kapitel 1 dient der Einführung von Gröbnerbasen und homogenen Polynomen als Vorbereitung auf die Untersuchung des Join-Meet-Ideals.

In Kapitel 2 führen wir Grundbegriffe zur konvexen Geometrie, zur reellen algebraischen Geometrie und zu Thetakörpern ein.

In Kapitel 3 beschäftigen wir uns mit der projektiven Norm, insbesondere mit der Geometrie der projektiven Einheitskugel, mit der Charakterisierung der Einheitsproduktvektoren als reelle affine Varietät, reell und komplex, und mit der Geschichte der Anwendung von Thetakörpern auf die projektive Norm. Insbesondere bereitet dieses Kapitel die Anwendung der Thetakörper-Methode auf die projektive Einheitskugel vor.

Im kurzen Kapitel 4 behandeln wir endliche distributive Verbände zur Vorbereitung auf Kapitel 5.

In Kapitel 5 führen wir den Hibi-Körper als eine Verallgemeinerung der projektiven Einheitskugel ein. Zudem widmen wir uns auch dem Join-Meet-Ideal. Wir bestimmen zunächst eine Vektorraumbasis für dieses Ideal, die Median-Basis. Weitere Themen sind Gröbnerbasen, vergleiche [Hibi] und [RS2], und die Verschwindeideale des (Norm-)Join-Meet-Ideals und deren „Komplexifizierung“.

Dies ist hilfreich für Erwägungen zur Symmetrie von Thetakörpern. Schließlich führen wir noch einige nützliche Begriffe für den Tensorprodukt-Fall ein.

In Kapitel 6 charakterisieren wir den ersten Thetakörper für den Hibi-Körper durch einen Spektraeder. Dies vereinfacht die Suche nach konkreten Polynomen mit Sos-Eigenschaft, welche ihn bestimmen. Auf dieser Grundlage stellen wir im reellen Fall eine hinreichende Bedingung an Sos-Polynome vor, welche für die späteren Kapitel zentral ist. Dazu entwickeln wir das Konzept einer *Aufspaltungs-Join-Meet-Partition*. Im komplexen Fall können wir mit der genannten Charakterisierung maximale Vektoren für den ersten Thetakörper bestimmen.

In Kapitel 7 führen wir die Design-Hyperebenen und eine weitere Klasse affiner Hyperebenen ein, die *Skip-Hyperebenen*. Wir beginnen mit einer kurzen Einführung zu lateinischen Quadraten und zu orthogonalen Designs. Das Hauptresultat ist die Identifikation maximaler Vektoren für die projektive Norm auf $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, wobei $n \in \{2, 4, 8\}$.

In Kapitel 8 stellen wir die Paritätshyperebenen vor. Wir beginnen mit einigen hierfür dienlichen Aussagen mit Bezug zur Sortierung und zur homologischen Algebra. Das Hauptresultat ist die obere Schranke an den inneren Radius der projektiven Einheitskugel in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, wobei $n \geqslant 2$.

In Kapitel 9 beschäftigen wir uns mit der Anwendung der Thetakörper-Methode auf die Menge der separablen Zustände.

In Kapitel 10 fassen wir die Ergebnisse bezüglich der projektiven Einheitskugel und separabler Zustände zusammen und diskutieren diese. Außerdem definieren wir eine Verallgemeinerung der Schmidt-Zerlegung im reellen Fall.

Grafische Übersichten

Die Landkarte auf Seite xxiii dient als grafische Übersicht.

Die Anordnung der Blasen in der Landkarte folgt im Uhrzeigersinn der Struktur dieser Arbeit. Die Farben zeigen an, ob ein Thema hauptsächlich neue Aspekte enthält oder ob es sich hauptsächlich um Hintergrundwissen handelt. Es wird auch auf die wichtigsten Ergebnisse und auf einige Forschungsgebiete verwiesen. Eine Legende für die Landkarte findet sich in Abbildung 1 auf Seite xxii.

Wann immer es im Hinblick auf eine klare Struktur der Landkarte möglich ist, sind die Beziehungen zwischen den einzelnen Blasen sichtbar. So basiert beispielsweise Abschnitt 7.3 auf Abschnitt 6.3. Dies wird durch einen Querverweis in einer zusätzlichen Blase am unteren Rand dargestellt. Andere Beziehungen wie die zwischen Abschnitt 1.2 und Abschnitt 5.3 ergeben sich aus dem Kontext.

Eine weitere grafische Übersicht ist Abbildung 2 auf Seite xxv. Sie zeigt die wichtigsten Ergebnisse bezüglich der Approximation des Hibi-Körpers durch Thetakörper. Im Folgenden wird die Bedeutung der einzelnen Abbildungen und der zugehörigen Sätze erläutert.

Abbildung 2 (a) zeigt, dass der Hibi-Körper H der konvexen Hülle der Schnittmenge der Hibi-Varietät V mit der euklidischen Einheitssphäre S^1 entspricht. Die (komplexen) Thetakörper, hier bezeichnet mit $\mathcal{T}_k$, $k \in \mathbb{N}$, sind konvexe Obermengen von H.

Satz 6.1.1 zeigt, dass der Hibi-Körper die Einheitskugel einer Norm ist. Außerdem ist jeder Thetakörper in der euklidischen Einheitskugel S enthalten, und in einigen Fällen kann gezeigt werden, dass er auch die Einheitskugel einer Norm ist. Satz 6.2.2 charakterisiert $\mathcal{T}_1$ durch einen Spektraeder. In einigen Fällen werden wir zeigen, dass Thetakörper die Symmetrien des Hibi-Körpers respektieren.

Eine wichtige Folgerung für den reellen Fall liefert Satz 6.3.6. Es gibt zwei verschiedene Anwendungen dieses Satzes auf die projektive Einheitskugel H in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$. Abbildung 2 (b) veranschaulicht den Fall $n \in \{2, 4, 8\}$, in dem die Design-Hyperebenen den Rand von $\mathcal{T}_1$ berühren und wir maximale Vektoren für die projektive Einheitskugel und ihren inneren Radius erhalten, vergleiche hierzu Satz 7.3.4. Abbildung 2 (c) zeigt den allgemeineren Fall $n \geqslant 2$, in dem die Paritätshyperebenen zu oberen Schranken für den inneren Radius von H führen, siehe Satz 8.3.5 (die Klasse von Vektoren mit projektiver Norm 1 ist hier im Bild nicht dargestellt).

Der komplexe Fall $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n$ ist auf Abbildung 2 (d) dargestellt. Der innere Radius des ersten komplexen Thetakörpers $\mathcal{T}_1^{\mathbb{C}}$ lässt sich mit Satz 6.4.2 genau bestimmen. Da er nicht von der Dimension des affinen Raumes abhängt, ist er eine eher schwache Abschätzung des inneren Radius von H.

Hintergrundinformationen

Diese Arbeit kann als eine Fortsetzung der Masterarbeit [Lang] angesehen werden. Insbesondere liefert die Masterarbeit einige zusätzliche Hintergrundinformationen. Sie ist jedoch nicht notwendig für das Verständnis dieser Arbeit, welche unabhängig davon gelesen werden kann.

Weiterhin gibt es Bezüge zu einigen speziellen mathematischen Themengebieten. Die benötigten Grundlagen werden an passender Stelle jeweils kurz angeführt.

Der Quellcode der zu dieser Arbeit gehörenden Programme findet sich unter: `https://git.rwth-aachen.de/lang.sand/geometryprojectivetensornorm`

Schlüsselwörter

Projektive Norm, nukleare Norm, Thetakörper, Summen von Quadraten, konvexe algebraische Geometrie, reelle algebraische Geometrie, konvexe Optimierung, konvexe Relaxationen, Quantenverschränkung, Verschränkungszeugen, Binomideale, Hibirelationen, orthogonale Designs.

Verzeichnisse

Diese Arbeit enthält neben dem Literaturverzeichnis auch ein Notations- und ein Stichwortverzeichnis.

Englische Einleitung

Diese Zusammenfassung ist im Wesentlichen eine Übersetzung der nun folgenden englischen Einleitung, welche durch mehrere Abbildungen ergänzt wird, siehe hierzu die Landkarte auf Seite xxiii und Abbildung 2 auf Seite xxv.

Introduction

The main focus of this thesis is on the projective norm on finite-dimensional real or complex tensor products. There are various mathematical subjects with relations to the projective norm. For instance, it appears in the context of operator algebras or in quantum physics.

The projective norm on multipartite tensor products is considered to be less accessible. So we use a method from convex algebraic geometry to approximate the projective unit ball by convex supersets, so-called theta bodies. For real multipartite tensor products we obtain theta bodies which are close to the projective unit ball, leading to a generalisation of the Schmidt decomposition. In a second step the method is applied to complex tensor products, in a third step to separable states.

In a more general context, the projective norm can be related to binomial ideals, especially to so-called Hibi relations. In this respect, we also focus on a generalisation of the projective unit ball, here called Hibi body, and its theta bodies. It turns out that many statements also hold in this general context.

Quantum entanglement

Entanglement is a fundamental concept in quantum information theory, given that many surprising effects which distinguish classical mechanics from quantum physics are related to entangled states. In classical mechanics the state of a system which is a compound of several independent subsystems is completely determined by the states of its subsystems. This is not the case for entangled states.

Many questions about entanglement are still open. For example, one could ask how to prove whether a state is entangled or not. In general, solving this so-called separability problem is not easy. However, there exist some necessary or sufficient conditions for entanglement. For example, an affine hyperplane with the property that all separable (i.e. non-entangled) states lie on one side provides a sufficient condition. This hyperplane is then a so-called entanglement witness. In addition, there are so-called entanglement measures which indicate the degree of entanglement. Aside from common entanglement measures such as the von Neumann entropy, there are also those based on the projective tensor norm, see [Arv] and [Rud]. In particular, the projective norm is an entanglement measure for pure states.

Overviews concerning entanglement can be found in [HHHH], [Sok] or [Aud].

The projective tensor norm

In addition to entanglement, there are other applications of the projective norm, for example in the context of information theory, signal analysis and compressive sensing. Here it is important for low rank tensor recovery, see [RS2]. Other common names for the projective norm are "nuclear norm" or "greatest cross norm".

The main subject of this thesis is the projective norm on finite-dimensional real or complex tensor products. Since it is in general not easy to determine the projective norm globally, we focus on specific classes of vectors such as the maximal vectors, see [Arv]. These are unit vectors which maximise the projective norm. They also determine an important characteristic of the projective unit ball, the inner radius. This is the radius of the largest Euclidean unit ball that is contained within it.

Sums of squares and theta bodies

In this thesis we use a special method from convex algebraic geometry, so-called theta bodies, to describe compact convex sets such as unit balls of norms or the set of separable states. Theta bodies can be considered whenever the set is the convex hull of a real affine variety, see [BPT]. In this case, its theta bodies form a chain of convex supersets converging to the original set.

A theta body is defined by affine half-spaces. The associated linear functionals have certain real algebraic properties related to sums of squares (sos). It is said that the sos method is "broadly applicable, effective, surprisingly powerful and simple", see [PS2].

Indeed, for our purpose, the projective unit ball in a real bipartite finite-dimensional tensor product can be described as a theta body. This has been shown independently in [Sto] and in the Master's thesis [Lang] and motivates to focus on the projective tensor norm in real multipartite tensor products now. In this respect, this thesis can be regarded as a continuation of the Master's thesis.

The projective norm and theta bodies — The unit ball of the projective norm is equal to the convex hull of the unit product vectors. The latter can be expressed as a real algebraic variety, for both real and complex tensor products. For the complex case we use the approach in [Voi] and introduce so-called *complex theta bodies*. The projective unit ball can thus be approximated by theta bodies in the real case as well as in the complex case.

This approach relates tensor products to convex optimisation, real algebraic geometry and sums of squares.

With respect to quantum entanglement, theta bodies can therefore contribute to a better understanding of the projective norm as an entanglement measure. On the other hand, it can be also interesting to consider theta bodies as new entanglement measures in addition to the projective norm.

In this thesis we investigate several aspects of the projective unit ball and its theta bodies, real and complex, for example, besides the inner radii, also their geometry or the underlying ideal.

Since the theta body method is initially intended for real vector spaces, it is reasonable to begin the investigation with the real case and to develop the complex case on this basis. This is also indicated by the fact that the ideal for the complex case can be derived from the ideal for the real case. Often it was possible to work out similarities and differences between the two cases and to address their specific characteristics.

Now, we summarise the main results of this thesis concerning the application of the theta body method to the projective norm.

Real tensor products — We focus on the multipartite tensor product $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, where $n \geqslant 2$. The number of tensor factors is arbitrary.

In the case where $n \in \{2, 4, 8\}$ we are able to find a class of maximal vectors and thus to determine the inner radius of the projective unit ball. We define them by using so-called *design hyperplanes*. As far as we know, maximal vectors in this general context were not known before. The underlying combinatorial method relates tensor products to latin squares and orthogonal designs.

In the more general case $n \geqslant 2$ we are able to find a class of vectors with projective norm 1 and thus an upper bound on the inner radius of the projective unit ball. For this purpose, we introduce another class of affine hyperplanes, the so-called *parity hyperplanes*. They are defined by combinatorial means as well. As far as we know, this class of boundary vectors was in general not known before.

The results can be seen as a generalisation of the Schmidt decomposition for specific classes of vectors and as an enhancement to the bounds in [Arv] for real tensor products.

Complex tensor products — We will see that the real case is straightforward in many respects. However, the complex case seems to be more complicated, so that results even for small dimensions or bipartite tensor products become interesting.

In the case $\mathbb{C}^2 \otimes \mathbb{C}^2$ we show that the first complex theta body is equal to the projective unit ball.

In all other cases $\mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_r}$, where $r \geqslant 2$ and $n_1, \ldots, n_r \geqslant 2$, we obtain maximal vectors for the first complex theta body. In particular, its inner radius is constant and equals $1/\sqrt{2}$, which proves that it is relatively far away from the projective unit ball. In this respect, the real and the complex case lead to qualitatively different results for the first theta body.

Separable states — In a third step, we show that the theta body method can be applied to the set of separable states. This offers the possibility of using sos polynomials as entanglement measures.

The ideal we use in our approach is generated from the ideal used for the projective norm on complex tensor products. Therefore, it seems useful for future investigations to continue with the complex case for the projective norm and to proceed with the separable states on this basis.

The join-meet ideal — Another focus of this thesis is on the application of the theta body method to a generalisation of the projective unit ball.

The motivation for this is that the set of product vectors in the real case is a so-called Hibi variety which is induced by the so-called join-meet ideal. This ideal is generated by polynomials called Hibi relations whose variables are indexed by distributive lattices, see [Hibi] and [HHO].

Now, the unit vectors in the Hibi variety form again a variety induced by the *norm-join-meet ideal*. In order to generalise the complex case as well, we introduce the concept of *complex Hibi relations* in order to describe a corresponding real variety. The convex hull of these varieties, the *(complex) Hibi body*, can thus be considered as a generalisation of the projective unit ball, real and complex.

We will see that many statements about the projective unit ball and its theta bodies also hold in this general context. Even though the basic idea was to understand the projective norm, the concept of Hibi bodies and the results can be considered as an independent contribution to the study of the (norm-)join-meet ideal.

In particular, our elementary method to characterise the first theta body by a spectrahedron, see additionally also [BCR], will prove to be very useful. We support this with a computer program written in Python.

In addition, we develop an approach for the understanding of the structure of the join-meet ideal using a *median basis*. From our point of view, this approach is new. Moreover, it allows to show well-known statements about Gröbner bases such as those in [HHO] in a simpler way than before.

Overview

In Chapter 1 we provide a short introduction to Gröbner bases and to homogeneous polynomials in preparation for the investigation of the join-meet ideal.

In Chapter 2 we introduce basic notions of convex geometry, real algebraic geometry, and theta bodies.

In Chapter 3 we deal with the projective norm, in particular with the geometry of the projective unit ball, with the characterisation of the unit product vectors as a real affine variety, real and complex, and with the history of the application of theta bodies to the projective norm. In particular, this chapter prepares the application of the theta body method to the projective unit ball.

In Chapter 4 we briefly introduce finite distributive lattices for Chapter 5.

In Chapter 5 we introduce the Hibi body as a generalisation of the projective unit ball. In addition, we pay attention to the join-meet ideal. We first determine a vector space basis for it, the median basis. Further topics are Gröbner bases, compare [Hibi] and [RS2], and the vanishing ideals of the (norm-)join-meet ideal and their "complexification". This is helpful for discussions on the symmetry of theta bodies. Finally, we introduce some notions for the tensor product case.

In Chapter 6 we characterise the first theta body for the Hibi body by a spectrahedron. This simplifies the search for concrete sos polynomials that determine it. In the real case, we introduce a sufficient condition for sos polynomials which is essential for the following chapters. For this purpose, we develop the concept of a *splitting join-meet partition*. In the complex case, we can determine maximal vectors for the first theta body by using the characterisation mentioned above.

In Chapter 7 we introduce design hyperplanes and another class of affine hyperplanes, the *skip hyperplanes*. We begin with a brief introduction to latin squares and to orthogonal designs. The main result is the identification of maximal vectors for the projective norm in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, where $n \in \{2, 4, 8\}$.

In Chapter 8 we introduce parity hyperplanes, starting with some statements that are useful for this purpose with respect to sorting and to homological algebra. The main result is the upper bound on the inner radius of the projective unit ball in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, where $n \geqslant 2$.

In Chapter 9 we deal with the application of the theta body method to the set of separable states.

In Chapter 10 we summarise and discuss the results with respect to the projective unit ball. In addition, we define a generalisation of the Schmidt decomposition in the real case and we suggest how to proceed further.

Graphical Overviews

The mind map on page xxiii serves as a graphical overview.

The alignment of the bubbles in the mind map follows the structure of this thesis in clockwise direction. The colours indicate whether a topic mainly contains new aspects or whether it is mainly background. The mind map also shows main results and some references to research areas. A legend for the mind map is given in Figure 1 on page xxii.

Whenever possible with respect to a clear structure of the mind map, relations between individual bubbles are visible. For example, Section 7.3 bases on Section 6.3. This relation is shown by a cross reference in an extra bubble at the lower margin. Other relations such as the relation between Section 1.2 and Section 5.3 follow from the context.

Another graphical overview is given in Figure 2 on page xxv. It shows the main results concerning the approximation of the Hibi body by theta bodies. In the following, we explain the meaning of each subfigure and of the underlying theorems.

Figure 2 (a) illustrates that the Hibi body H corresponds to the convex hull of the intersection of the Hibi variety V with the Euclidean unit sphere S^1. The (complex) theta bodies, here denoted by $\mathcal{T}_k$, $k \in \mathbb{N}$, are convex supersets of H.

Theorem 6.1.1 shows that the Hibi body is the unit ball of a norm. Moreover, each theta body is contained in the Euclidean unit ball S, and in some cases it can be shown that it is also the unit ball of a norm. Theorem 6.2.2 characterises $\mathcal{T}_1$ by a spectrahedron. In some cases, we will show that a theta body respects the symmetries of the Hibi body.

An important corollary in the real case is provided by Theorem 6.3.6. There are two different applications of this theorem to the projective unit ball H in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$. Figure 2 (b) illustrates the case $n \in \{2, 4, 8\}$ where the design hyperplanes meet the boundary of $\mathcal{T}_1$, see Theorem 7.3.4, that is to say we obtain maximal vectors for the projective unit ball and its inner radius. Figure 2 (c) illustrates the more general case $n \geqslant 2$ where the parity hyperplanes lead to upper bounds on the inner radius of H, see Theorem 8.3.5 (the class of vectors with projective norm 1 is not visualised here).

The complex case $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n$ is illustrated in Figure 2 (d). The inner radius of the first complex theta body $\mathcal{T}_1^{\mathbb{C}}$ can be determined exactly with Theorem 6.4.2. Since it does not depend on the dimension of the affine space, it is a rather weak estimation of the inner radius of H.

Background Information

This thesis can be regarded as a continuation of the Master's thesis [Lang]. In particular, the Master's thesis provides some additional background information. However, it is not necessary for the understanding of this thesis which can be read independently.

Moreover, there are relations to some special mathematical subjects. The required background information is presented briefly throughout the thesis.

The source code of the programs which belong to this thesis is located at:
`https://git.rwth-aachen.de/lang.sand/geometryprojectivetensornorm`

Keywords

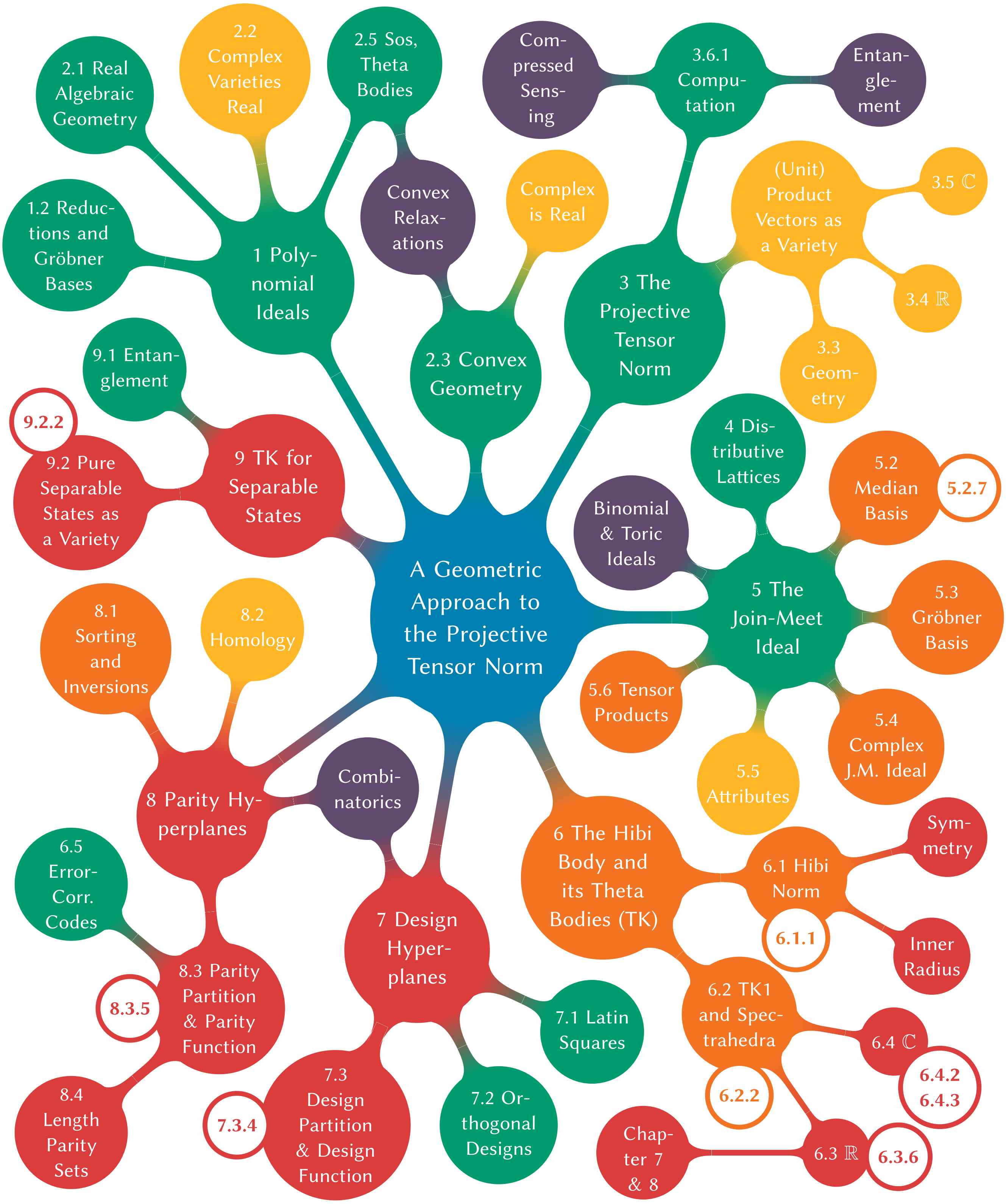
Projective norm, nuclear norm, theta bodies, sums of squares, convex algebraic geometry, real algebraic geometry, convex optimisation, convex relaxations, quantum entanglement, entanglement witnesses, binomial ideals, Hibi relations, orthogonal designs.

Notation and Index

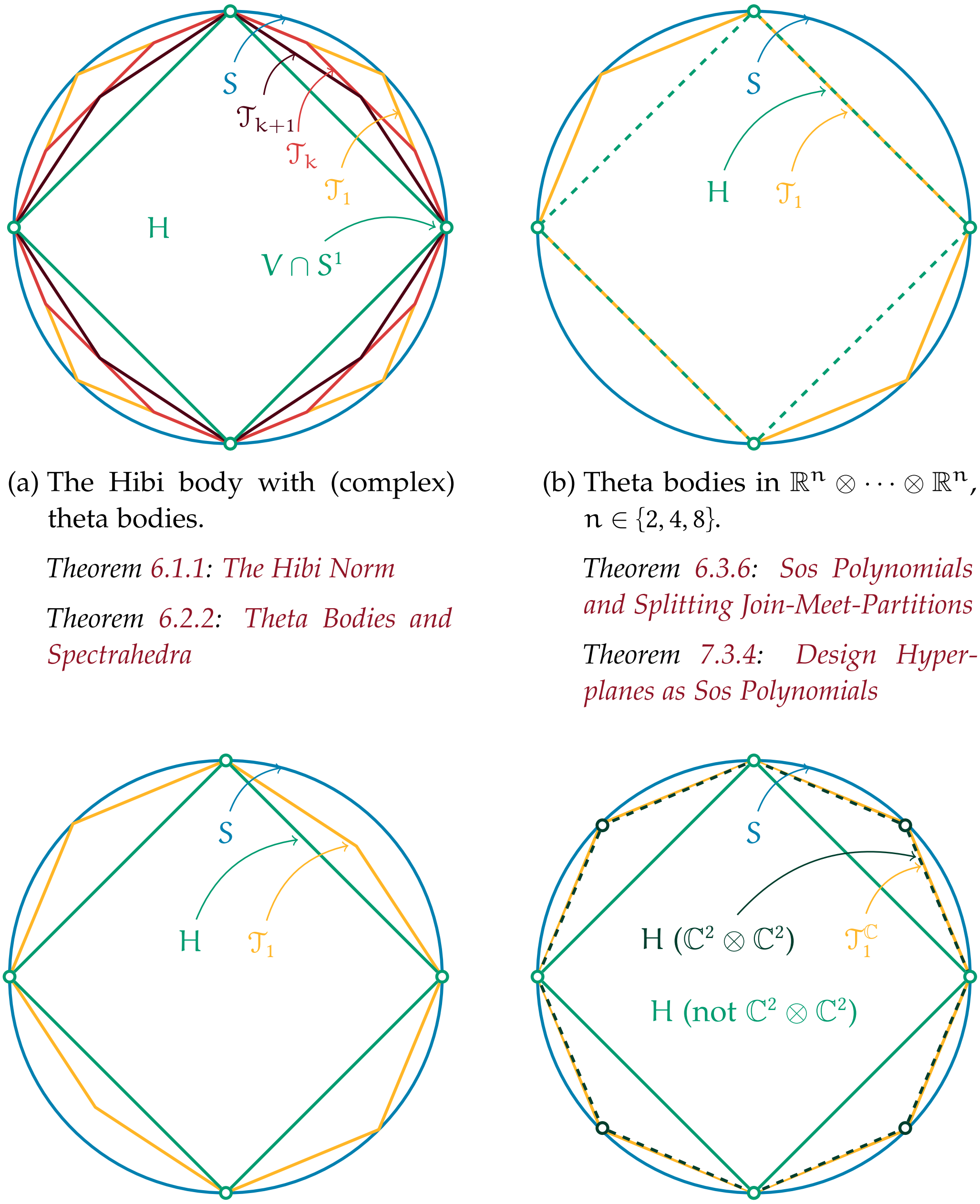
This thesis contains an index of notation and an index.

References to research areas	🟣
Background (sometimes adapted)	🟢
Background with new aspects	🟡
New concepts (with references to other works)	🟠
Mainly new and independent results	🔴
Main results	○ ○

Figure 1: Legend for the mind map on page xxiii.


A Geometric Approach to the Projective Tensor Norm
1 Polynomial Ideals
1.2 Reductions and Gröbner Bases
2.1 Real Algebraic Geometry
2.2 Complex Varieties Real
2.5 Sos, Theta Bodies
Convex Relaxations
2.3 Convex Geometry
Complex is Real
3 The Projective Tensor Norm
Compressed Sensing
3.6.1 Computation
Entanglement
(Unit) Product Vectors as a Variety
3.5 ℂ
3.4 ℝ
3.3 Geometry
4 Distributive Lattices
Binomial & Toric Ideals
5 The Join-Meet Ideal
5.2 Median Basis
5.2.7
5.3 Gröbner Basis
5.4 Complex J.M. Ideal
5.5 Attributes
5.6 Tensor Products
6 The Hibi Body and its Theta Bodies (TK)
6.1 Hibi Norm
6.1.1
Symmetry
Inner Radius
6.2 TK1 and Spectrahedra
6.2.2
6.4 ℂ
6.4.2
6.4.3
6.3 ℝ
6.3.6
Chapter 7 & 8
7 Design Hyperplanes
7.1 Latin Squares
7.2 Orthogonal Designs
7.3 Design Partition & Design Function
7.3.4
Combinatorics
8 Parity Hyperplanes
8.1 Sorting and Inversions
8.2 Homology
6.5 Error-Corr. Codes
8.3 Parity Partition & Parity Function
8.3.5
8.4 Length Parity Sets
9 TK for Separable States
9.1 Entanglement
9.2 Pure Separable States as a Variety
9.2.2

- empty page -


S
$\mathcal{T}_{k+1}$
$\mathcal{T}_k$
$\mathcal{T}_1$
H
$V \cap S^1$
S
H
$\mathcal{T}_1$
S
H
$\mathcal{T}_1$
S
H $(\mathbb{C}^2 \otimes \mathbb{C}^2)$
$\mathcal{T}_1^{\mathbb{C}}$
H (not $\mathbb{C}^2 \otimes \mathbb{C}^2$)

(a) The Hibi body with (complex) theta bodies.

Theorem 6.1.1: The Hibi Norm

Theorem 6.2.2: Theta Bodies and Spectrahedra

(b) Theta bodies in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, $n \in \{2, 4, 8\}$.

Theorem 6.3.6: Sos Polynomials and Splitting Join-Meet-Partitions

Theorem 7.3.4: Design Hyperplanes as Sos Polynomials

(c) Theta bodies in $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, $n \geqslant 2$.

Theorem 6.3.6: Sos Polynomials and Splitting Join-Meet-Partitions

Theorem 8.3.5: Parity Hyperplanes as Sos Polynomials

(d) The first complex theta body in $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n$, contrasting $\mathbb{C}^2 \otimes \mathbb{C}^2$ with the other cases.

Theorem 6.4.2: The Inner Radius of the First Complex Theta Body

Theorem 6.4.3: The First Complex Theta Body in a Special Case

Figure 2: The Hibi body with (complex) theta bodies.

Chapter 1

POLYNOMIAL IDEALS

Let $K[\vec{x}] := K[x_1, \ldots, x_n]$ be the multivariate polynomial ring in n variables over a field K. Given a set $P \subseteq K[\vec{x}]$ of polynomials we want to decide whether a polynomial $f \in K[\vec{x}]$ can be expressed in terms of P as a finite sum $f = \sum_{p \in P} a_p \cdot p$, where $a_p \in K[\vec{x}]$. In other words, we ask whether f lies in the ideal generated by P. According to the *Hilbert Basis Theorem*, every ideal in $K[\vec{x}]$ has a finite generating set (see [CLS], Chapter 1, §5), so we can assume that P is finite. This problem is often called the *ideal membership problem*. At the same time, we could ask whether two ideals are equal, which is called the *ideal equality problem*.

The aim of this chapter is to give a concise overview of these problems. For each polynomial ideal there are finite generating sets, so-called *Gröbner bases*, which guarantee that the ideal membership problem can be solved with an algorithm in a finite number of steps. For details we refer to textbooks on computational algebraic geometry and Gröbner bases such as [BW], [CLS] or [Stu].

The last section deals with homogeneous polynomials and homogeneous ideals. Details can be found in textbooks on algebraic geometry such as [GW] or [Har].

1.1 Term Orders

This section deals with *term orders* according to [CLS].

1.1.1 Terms and Monomials

A *term* in the variables $x_1, \dots, x_n$ is a product of the form $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \in K[\vec{x}]$, where $\alpha_k \in \mathbb{N}_0$ for all $k \in \{1, \dots, n\}$ and $1 = x_1^0 \cdot \ldots \cdot x_n^0$. The set of all terms in n variables is an abelian monoid under multiplication. In what follows, terms are identified with elements in $\mathbb{N}_0^n$, that is,

$$x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} \quad \leftrightarrow \quad \alpha = (\alpha_1, \dots, \alpha_n).$$

This identification transforms term multiplication into addition on $\mathbb{N}_0^n$. A *monomial* is a polynomial of the form $a \cdot x^\alpha$, where $a \in K$, $a \neq 0$ and $\alpha \in \mathbb{N}_0^n$. The notion follows [BW].

The terms are a standard basis of $K[\vec{x}]$, regarded as a vector space over the field K, that is, each polynomial $f \in K[\vec{x}]$ can be written uniquely as $f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha$ with $a_\alpha \in K$, where $a_\alpha = 0$ for almost all $\alpha \in \mathbb{N}_0^n$. Elements of the set $\{x^\alpha \colon \alpha \in \mathbb{N}_0^n, a_\alpha \neq 0\}$ are called *terms of* f.

1.1.2 Monomial Ideals

Let $f, g \in K[\vec{x}]$ with $g \neq 0$, then g *divides* f, written $g \mid f$, if there exists $h \in K[\vec{x}]$ with $g \cdot h = f$. In this case, we write $h = \frac{f}{g}$. Therefore, $x^\alpha \mid x^\beta$, where $\alpha = (\alpha_1 \dots, \alpha_n), \beta = (\beta_1 \dots, \beta_n) \in \mathbb{N}_0^n$, if and only if $\alpha_k \leqslant \beta_k$ for all $k \in \{1, \dots, n\}$. Two non-zero polynomials $f, g \in K[\vec{x}]$ are said to be *coprime* if $h \mid f$ and $h \mid g$ for $h \in K[\vec{x}]$ implies $h \in K$. A term x^α with $\alpha = (\alpha_1 \dots, \alpha_n) \in \mathbb{N}_0^n$ is called *square-free*, if $\alpha_k \in \{0, 1\}$ (which means that x^α is not divisible by x_k^2) for all $k \in \{1, \dots, n\}$.

An ideal I is called a *monomial ideal*, if there exists a subset $A \subseteq \mathbb{N}_0^n$ such that $I = \mathrm{Id}(x^\alpha \colon \alpha \in A)$. That is, a monomial ideal is generated by terms. According to [CLS, Chapter 2, §4], it has the following property:

Proposition. Let $A \subseteq \mathbb{N}_0^n$ and $I := \mathrm{Id}(x^\alpha \colon \alpha \in A)$. For all $x^\beta \in I$, we have $\beta \in \mathbb{N}_0^n$, if and only if $x^\alpha \mid x^\beta$ for some $\alpha \in A$.

Proof. A polynomial $f \in I$ has the form $f = \sum_{\alpha \in A} g_\alpha x^\alpha$, where $g_\alpha \in K[\vec{x}]$ (almost all zero). Hence, each term of f is divisible by a term in $\{x^\alpha \colon \alpha \in A\}$. $\diamond$

Based on this statement, one can conclude that every monomial ideal is finitely generated by terms (see [CLS, §4, *Dickson's Lemma*]).

1.1.3 The Degree of a Polynomial

Definition. Let $|\alpha| := \sum_{k=1}^{n} \alpha_k$ denote the *degree* of $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ and of the term x^α. The *degree* $\deg(f)$ of a polynomial $f \in K[\vec{x}]$ is defined as the maximum of the degrees of its terms, whereupon we agree with $\deg(0) := -\infty$.

If $\deg(f) \leqslant 1$ (that is, f has the form $f = a_0 + \sum_{k=1}^{n} a_k x_k$ with $a_k \in K$ for all $k \in \{1, \dots, n\}$), then f is called an *affine functional*.

For each $k \in \mathbb{N}_0$, let $K[\vec{x}]_k$ denote the polynomials of degree less or equal than k.

1.1.4 Term Orders

Definition. A *term order* $\leqslant$ on $\mathbb{N}_0^n$ is a total order on $\mathbb{N}_0^n$ (that is, it is antisymmetric, transitive, and, in addition, any two elements are comparable), satisfying

(i) If $\alpha \leqslant \beta$ and $\gamma \in \mathbb{N}_0^n$, then $\alpha + \gamma \leqslant \beta + \gamma$.
(ii) Every non-empty subset of $\mathbb{N}_0^n$ has a smallest element under $\leqslant$, that is, $\leqslant$ is a well-ordering.

As usual, we also write $\alpha < \beta$ if $\alpha \leqslant \beta$ and $\alpha \neq \beta$.

The latter condition is equivalent to the statement that every strictly decreasing sequence in $\mathbb{N}_0^n$ eventually terminates.

According to the identification of terms with elements in $\mathbb{N}_0^n$, any term order on $\mathbb{N}_0^n$ induces a total order on the terms of $K[\vec{x}]$, which is called a *term order* on $K[\vec{x}]$. Furthermore, any term order $\leqslant$ on $K[\vec{x}]$ defines a total order on the variables $x_1, \dots, x_n$. We say that $\leqslant$ *is based on* this total order.

Definition. Let $\alpha, \beta \in \mathbb{N}_0^n$. The following relations are term orders:

(i) (*Lexicographical Order*) We say $\alpha >_{\text{lex}} \beta$ if the leftmost non-zero entry in $\alpha - \beta \in \mathbb{Z}^n$ is positive.

(ii) (*Graded Lexicographical Order*) We say $\alpha >_{\text{grlex}} \beta$ if $|\alpha| > |\beta|$ or, if $|\alpha| = |\beta|$, we have $\alpha >_{\text{lex}} \beta$.

(iii) (*Graded Reverse Lexicographical Order*) We say $\alpha >_{\text{grevlex}} \beta$ if $|\alpha| > |\beta|$ or, if $|\alpha| = |\beta|$, the rightmost non-zero entry in $\alpha - \beta \in \mathbb{Z}^n$ is negative.

The term x_k is identified with $(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{N}_0^n$ (the k^{th} entry equals 1). In this respect, each of the three term orders base on the order $x_1 > x_2 > \dots > x_n$.

The following example and the following proposition justify the term "reverse lexicographical". It will be useful in Section 5.3 and in Section 5.4.

Example. We give some examples to outline the difference between the proposed term orders. The brackets and the commas in the notation for elements in $\mathbb{N}_0^n$ are omitted:

$$\begin{aligned}
&1\,0\,0\,0 >_{\text{lex}} 0\,1\,1\,1, && 1\,0\,0\,1 >_{\text{lex}} 0\,1\,1\,0,\\
&1\,0\,0\,0 <_{\text{grlex}} 0\,1\,1\,1, && 1\,0\,0\,1 >_{\text{grlex}} 0\,1\,1\,0,\\
&1\,0\,0\,0 <_{\text{grevlex}} 0\,1\,1\,1, && 1\,0\,0\,1 <_{\text{grevlex}} 0\,1\,1\,0.
\end{aligned}$$

The following diagram shows grlex (upper case) and grevlex (lower case):

$$1\,1\,0\,0 > 1\,0\,1\,0 > \begin{matrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{matrix} > \begin{matrix} 0\,1\,1\,0 \\ 1\,0\,0\,1 \end{matrix} > 0\,1\,0\,1 > 0\,0\,1\,1\,.$$

In this respect, the main difference is that $x_1x_4 >_{\text{grlex}} x_2x_3$, but $x_1x_4 <_{\text{grevlex}} x_3x_4$.

For any $\alpha \in \mathbb{N}_0^n$, let $\operatorname{supp}(\alpha) := \{k \in \{1, \dots, n\} \colon \alpha_k \neq 0\} \subseteq \{1, \dots, n\}$ be the *support* of α and of the term x^α.

The following simple observation will be helpful in Chapter 5:

Proposition. Let $\alpha, \beta \in \mathbb{N}_0^n$ with $|\alpha| = |\beta|$ and with $\alpha_k, \beta_k \in \{0, 1\}$ for all $k \in \{1, \dots, n\}$. Let $A := \operatorname{supp}(\alpha) \setminus \operatorname{supp}(\beta)$ and let $B := \operatorname{supp}(\beta) \setminus \operatorname{supp}(\alpha)$. Then we have:

(i) $\alpha >_{\text{grlex}} \beta$, if and only if

$$\min(A) < \min(B)\,.$$

(ii) $\alpha >_{\text{grevlex}} \beta$, if and only if

$$\max(A) < \max(B)\,.$$

(Where max and min refer to the "standard order" $1 < 2 < \ldots$ on $\mathbb{N}$)

Proof. Let $\alpha, \beta \in \mathbb{N}_0^n$ with $|\alpha| = |\beta|$. Now, we have $\alpha >_{\text{grlex}} \beta$, if and only if the entries of α exceed those of β in the leftmost position, where they differ, and we have $\alpha >_{\text{grevlex}} \beta$, if and only if the entries of β exceed those of α in the rightmost position, where they differ. ◇

1.1.5 The Multidegree of a Polynomial

Definition. Let $\leqslant$ be a term order on $\mathbb{N}_0^n$ and let $f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha \in K[\vec{x}]$ be a non-zero polynomial.

(i) The *multidegree* of f is

$$\text{mdeg}(f) := \max(\alpha \in \mathbb{N}_0^n \colon a_\alpha \neq 0)\,,$$

where max refers to $\leqslant$.

(ii) The *leading term* of f is $\text{LT}(f) := x^{\text{mdeg}(f)}$.

(iii) The *leading coefficient* of f is $\text{LC}(f) := a_{\text{mdeg}(f)}$.

For convenience, we agree with $\text{mdeg}(0) := -\infty$. For any subset $M \subseteq K[\vec{x}]$, we write $\text{LT}(M) := \{\text{LT}(f) \colon f \in M \setminus \{0\}\}$.

The leading term has the following properties, see [CLS, Chapter 2, §2, Lemma 8]:

Proposition. For all non-zero polynomials $f, g \in K[\vec{x}]$, we have

(i) $\text{LT}(f + g) \leqslant \max(\text{LT}(f), \text{LT}(g))$,

(ii) $\text{LT}(f \cdot g) = \text{LT}(f) \cdot \text{LT}(g)$.

Proof. Statement (i) can be obtained immediately. Let $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{N}_0^n$. Let us assume that $\alpha_1 \leqslant \beta_1$ and $\alpha_2 \leqslant \beta_2$. Since $\leqslant$ is a term order, it follows that $\alpha_1 + \alpha_2 \leqslant \beta_1 + \beta_2$. This shows (ii). ◇

Example. If we consider $K[x_{22}, x_{21}, x_{12}, x_{11}]$ with the graded reverse lexicographical order based on $x_{22} > x_{21} > x_{12} > x_{11}$, then the leading term of the polynomial $x_{22}x_{11} - x_{21}x_{12}$ is $x_{21}x_{12}$. It is coprime with the leading term x_{22}^2 of the polynomial $x_{22}^2 + x_{21}^2 + x_{12}^2 + x_{11}^2 - 1$.

1.2 Polynomial Reduction and Gröbner Bases

In this section, we introducte *reduction relations*, the *multivariate polynomial division* and Gröbner bases according to [BW].

1.2.1 Reduction Relations

Definition. A binary relation $\longrightarrow$ on a set G is called a *reduction relation*, if it is strictly antisymmetric (that is, $g \longrightarrow h$ and $h \longrightarrow g$ is not possible). A reduction relation is said to be *noetherian*, if every strictly decreasing sequence $g_1 \longrightarrow g_2 \longrightarrow g_3 \longrightarrow \dots$ eventually terminates. The reflexive-transitive closure of a reduction relation $\longrightarrow$ is denoted by $\xrightarrow{\star}$ and the reflexive-transitive-symmetric closure of $\longrightarrow$ (that is, the smallest equivalence relation on G extending $\longrightarrow$) is denoted by $\xleftrightarrow{\star}$. For $g, h \in G$, we say g *reduces to* h, if $g \xrightarrow{\star} h$. An element $h \in G$ is said to be a *normal form* of $g \in G$ (with respect to $\longrightarrow$), if $g \xrightarrow{\star} h$ and if h is maximal (that is, it cannot be properly reduced).

Details can be found in [BW], where reduction relations are used as an approach to Gröbner bases.

Reduction relations will also appear in Section 5.2.

1.2.2 Multivariate Polynomial Division

Throughout this section, we fix a term order $\leqslant$ on $\mathbb{N}_0^n$. We note that the definitions below depend on the term order.

Definition. Let P be a non-empty and finite subset of $K[\vec{x}]$ with $0 \notin P$. A non-zero polynomial $f \in K[\vec{x}]$ *reduces to* g *modulo* P, written $f \longrightarrow_P g$, if there exists $p \in P$, a term t of f and a term s such that $s \cdot \mathrm{LT}(p) = t$ and

$$f = \frac{a}{\mathrm{LC}(p)} \cdot s \cdot p + g,$$

where a is the coefficient of t in f.

In this case, g evolves from f by replacing the monomial $a \cdot t$ in f by the polynomial $h := a \cdot (t - \frac{1}{\mathrm{LC}(p)} \cdot s \cdot p)$, where $\mathrm{mdeg}(h) < \mathrm{mdeg}(t)$. Hence, we obtain

$$\mathrm{mdeg}(f) \geqslant \max\left(\mathrm{mdeg}(f - g), \mathrm{mdeg}(g)\right).$$

Reducing modulo P is a binary relation on $K[\vec{x}]$. In [BW, Theorem 5.21] it is stated that $\longrightarrow_P$ is a noetherian reduction relation on $K[\vec{x}]$, that is, normal forms always exist. This statement relies on the requirement that term orders are well-orderings. The reduction relation $\longrightarrow_P$ is also called the *multivariate polynomial division*. In the more general case $f \xrightarrow{\star}_P g$ we also say that f *reduces to* g *modulo* P. A normal form of f with respect to $\longrightarrow_P$ is also called a *normal form of* f *modulo* P.

It is convenient to define that f is the single normal form of f modulo $\emptyset$ and that 0 is the single normal form of 0 modulo P.

For practical purposes, the determination of a normal form of a given polynomial can be realised by means of a *division algorithm* on $K[\vec{x}]$.

Normal forms with respect to $\longrightarrow_P$ have the following form:

Proposition. Let P be a non-empty and finite subset of $K[\vec{x}]$ with $0 \notin P$. Let $f \in K[\vec{x}]$ be a non-zero polynomial and let $r \in K[\vec{x}]$ be a normal form of f with respect to $\longrightarrow_P$. Then there exist $q_p, r \in K[\vec{x}]$, $p \in P$, such that

$$f = \sum_{p \in P} q_p \cdot p + r$$

and such that the following conditions are fulfilled:

(i) For all $p \in P$ with $q_p \neq 0$, we have $\mathrm{mdeg}(f) \geqslant \mathrm{mdeg}(q_p \cdot p)$.

(ii) For all $p \in P$, none of the terms of r is divisible by the leading term of p.

Proof. See [BW, Proposition 5.22]. A sketch of the proof can be found here: If r is a normal form of f and $r \neq f$, then there exist polynomials $r_1, \ldots, r_l$ such that $r_0 := f \longrightarrow_P r_1 \longrightarrow_P \ldots \longrightarrow_P r_l = r$. Hence, there exist polynomials $s_1, \ldots, s_l \in \mathrm{Id}(P)$, each having the form $s_k = q_k \cdot p_k$, where $q_k \in K[\vec{x}]$ and $p_k \in P$, such that for all $k \in \{1, \ldots, l\}$, we have

$$r_{k-1} = s_k + r_k$$

and

$$\mathrm{mdeg}(r_{k-1}) \geqslant \max(\mathrm{mdeg}(s_k), \mathrm{mdeg}(r_k)).$$

It follows that $f = \sum_{k=1}^{l} s_k + r$, where $\mathrm{mdeg}(f) \geqslant \mathrm{mdeg}(s_k)$ for all $k \in \{1, \dots, l\}$. Condition (ii) holds since r is a normal form. ◇

Example. Let $P := \{x, x+1\} \subseteq K[x]$.

(i) Normal forms modulo P are *not* unique, since $x \xrightarrow{\star}_P 0$ and $x \xrightarrow{\star}_P -1$.

(ii) From $f \in \mathrm{Id}(P)$ does *not* automatically follow $f \xrightarrow{\star}_P 0$, since $1 \in \mathrm{Id}(P)$, which is a normal form modulo P.

(iii) The multivariate polynomial division has *no* additive property in general. If $f_1, f_2, g_1, g_2 \in K[\vec{x}]$ with $f_1 \longrightarrow_P g_1$ and $f_2 \longrightarrow_P g_2$, then we do not have $f_1 + f_2 \longrightarrow_P g_1 + g_2$ in general: In contrast to $-x$ and $x+1$, the polynomial $1 = (-x) + (x+1)$ does not reduce to zero modulo P.

(iv) If a non-zero polynomial f has the form

$$f = \sum_{p \in P} q_p \cdot p + r$$

and conditions (i) and (ii) from Proposition 1.2.2 are fulfilled, then r does *not* have to be a normal form of f modulo P in general. Indeed, we have $x + 2 = (2(x+1) - x) + 0 \in \mathrm{Id}(P)$, but $x + 2$ does not reduce to zero modulo P.

1.2.3 Gröbner Bases and the Ideal Membership Problem

If $f \xrightarrow{\star}_P 0$, then $f \in \mathrm{Id}(P)$. However, Example 1.2.2 has shown that the converse statement is not true in general. The following theorem which is adapted from [BW, Theorems 5.35 and 5.62] and [CLS, Chapter 2, §6] deals with subsets P for which the converse is always true. In this case, normal forms are unique:

Theorem. Let G be a finite subset of $K[\vec{x}]$ with $0 \notin G$ and $I := \mathrm{Id}(G)$. The following are equivalent:

(a) The reduction relation $\longrightarrow_G$ has unique normal forms.

(b) For all $f \in I$, we have $f \xrightarrow{\star}_G 0$.

(c) For all $f \in K[\vec{x}]$, we have $f \in I$ if and only if each normal form of f modulo G vanishes.

(d) For all $f \in K[\vec{x}]$, there exists a unique representation $f = g + r$ with $g \in I$ and $r \in K[\vec{x}]$ such that none of the terms of r are divisible by any $\mathrm{LT}(g)$, $g \in G$.

(e) The normal forms modulo G form a system of unique representatives for the partition $\{f + I \colon f \in K[\vec{x}]\}$ of $K[\vec{x}]$.

(f) We have $\mathrm{Id}(\mathrm{LT}(G)) = \mathrm{Id}(\mathrm{LT}(I))$.

(g) For all $0 \neq f \in I$, there exists $g \in G$ such that $\mathrm{LT}(g) \mid \mathrm{LT}(f)$.

(h) For all $0 \neq f \in I$, there exists $q_p \in K[\vec{x}]$ for all $p \in P$ with $\mathrm{mdeg}(f) \geqslant \mathrm{mdeg}(q_p \cdot p)$ such that $f = \sum_{p \in P} q_p \cdot p$.

Definition. A finite subset $G \subseteq K[\vec{x}]$ with $0 \notin G$ is called a *Gröbner basis*, if it satisfies the equivalent conditions of Theorem 1.2.3. If $I \subseteq K[\vec{x}]$ is an ideal, then a *Gröbner basis* of I is a Gröbner basis $G \subseteq K[\vec{x}]$ with $\mathrm{Id}(G) = I$.

We note that the definition of a Gröbner basis requires a term order. A Gröbner basis is called *universal*, if it is a Gröbner basis with respect to any term order on $\mathbb{N}_0^n$. We note that Gröbner bases are not uniquely determined in general, even if the term order remains unchanged. In the literature it is common to define a Gröbner basis according to (f) or (g). The representation in (h) does not have to be unique.

Given an ideal and a finite generating set (which always exists according to the Hilbert Basis Theorem), the *Buchberger algorithm* guarantees that a Gröbner basis can be found within a finite number of steps, see [CLS, Chapter 2, §7]. Thus, the ideal membership problem can be solved with the aid of Gröbner bases.

1.2.4 The Buchberger Criterion

Let $\alpha, \beta \in \mathbb{N}_0^n$. Let $\gamma \in \mathbb{N}_0^n$ be defined by $\gamma_k := \max(\alpha_k, \beta_k)$ for all $k \in \{1, \ldots, n\}$. The term x^γ is called the *least common multiple* of α and β. Two non-zero polynomials $f, g \in K[\vec{x}]$ are called *relatively prime* if $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$ are coprime.

Definition. The *S-polynomial* of two non-zero polynomials $g, h \in K[\vec{x}]$ is

$$S(g,h) := \mathrm{LC}(h) \cdot \frac{X^\gamma}{\mathrm{LT}(g)} \cdot g - \mathrm{LC}(g) \cdot \frac{X^\gamma}{\mathrm{LT}(h)} \cdot h,$$

where $\gamma \in \mathbb{N}_0^n$ is the least common multiple of $\mathrm{mdeg}(g)$ and $\mathrm{mdeg}(h)$.

Proposition. Let G be a finite subset of $K[\vec{x}]$ with $0 \notin G$. Let $g, h \in G$ be relatively prime. Then $S(g,h) \xrightarrow{\star}_G 0$.

Proof. See [CLS, Chapter 2, §9, Proposition 4]. ◇

The following theorem gives a necessary and sufficient condition that a set of polynomials is a Gröbner basis. It will be useful in Section 5.3.

Theorem. *(Buchberger Criterion)*
Let G be a finite subset of $K[\vec{x}]$ with $0 \notin G$. The following are equivalent:

(a) G is a Gröbner basis.
(b) For all $g, h \in G$, $g \neq h$, we have $S(g,h) \xrightarrow{\star}_G 0$.

Proof. See [CLS, Chapter 2, §6, Theorem 6]. ◇

1.2.5 The Ideal Equality Problem

Definition. A Gröbner basis G is called *reduced* if for all $g \in G$ the following holds:

(i) $\mathrm{LC}(g) = 1$,
(ii) No term of g lies in $\mathrm{Id}(\mathrm{LT}(G) \setminus \{g\})$.

Every ideal in $K[\vec{x}]$ has a uniquely defined reduced Gröbner basis, see [CLS, Chapter 2, §7, Theorem 5]. Thus, the ideal equality problem can be solved by comparing the reduced Gröbner bases.

1.2.6 A Basis of the Coordinate Ring

Let $I \subseteq K[\vec{x}]$ be an ideal. The set $K[\vec{x}]/I$ is a vector space over K and is referred to as the *coordinate ring* with respect to I. Let $G \subseteq K[\vec{x}]$ be a Gröbner basis of I and let

$$\begin{aligned} \mathcal{B}_0 &:= \{x^\beta : \beta \in \mathbb{N}_0^n, x^\beta \notin \mathrm{Id}(\mathrm{LT}(G))\}, \quad \text{and} \\ \mathcal{B} &:= \mathcal{B}_0 + I. \end{aligned}$$

The following statement can be found in [BPT, Example A.37].

Proposition. A vector space basis of the coordinate ring $K[\vec{x}]/I$ is given by $\mathcal{B}$.

Proof. According to Theorem 1.2.3 (e) and Proposition 1.1.2, each element in $K[\vec{x}]/I$ has a representative which lies in the linear hull of $\mathcal{B}_0$, that is, $\mathcal{B}$ generates $K[\vec{x}]/I$. Furthermore, $\mathcal{B}$ consists of linearly independent elements. To see this, let f be in the linear hull of $\mathcal{B}_0$ and let $f \in I$. Assuming that $f \neq 0$, we obtain $\mathrm{LT}(f) \in \mathrm{Id}(\mathrm{LT}(G))$ according to Theorem 1.2.3 (f). But this is impossible. Hence, $f = 0$◇

Hence, a basis of the coordinate ring can easily be deduced from a Gröbner basis by deciding for each term whether it is divisible by one of the leading terms of the Gröbner basis.

1.3 Homogeneous Polynomials

Details on homogeneous polynomials can be found in textbooks on algebraic geometry such as [Hat, Chapter 1].

Definition. A non-zero polynomial $f \in K[\vec{x}]$ is called *homogeneous* of degree $d \in \mathbb{N}_0$ if each of its terms has the same degree d. The zero polynomial is called *homogeneous* of all degrees $d \in \mathbb{N}_0$. An ideal I in $K[\vec{x}]$ is called *homogeneous* if it is generated by homogeneous polynomials.

Each polynomial $f \in K[\vec{x}]$ has a unique decomposition $f = \sum_{d \geqslant 0} f_d$, where f_d is a homogeneous polynomial of degree d. The elements of an ideal I in $K[\vec{x}]$ which are homogeneous of degree $d \in \mathbb{N}_0$ form a vector space I_d over K, the *homogeneous part* of degree d of I.

The following statement about homogeneous polynomials, on which projective algebraic geometry is based on, will be useful:

Proposition. An ideal I in $K[\vec{x}]$ is homogeneous if and only if it equals the direct sum of its homogeneous parts.

Proof. Let I be homogeneous, that is, there exist homogeneous polynomials f_i, $i \in I$, which generate I. Let $f \in I$, that is, there exist polynomials g_i, $i \in I$, almost all equal to zero, such that $f = \sum_{i \in I} g_i \, f_i$. Each polynomial g_i has a decomposition $g_i = \sum_{d \geqslant 0} g_{i,d}$, where $g_{i,d}$ is homogeneous of degree d. The polynomial $g_{i,d} \, f_i$ is homogeneous and lies in I. Hence,

$$f = \sum_{d \geqslant 0} \sum_{i \in I} g_{i,d}\, f_i$$

is a linear combination of homogeneous polynomials in I_d, $d \geqslant 0$. On the other hand, if I equals the direct sum of the vector spaces I_d, $d \in \mathbb{N}_0$, it is homogeneous by definition. ◇

Corollary. Let I be an ideal in $K[\vec{x}]$ which is generated by homogeneous polynomials $f_1, \ldots, f_m$ of the same degree $d \geqslant 0$. Let $d' \in \mathbb{N}_0$. Then the homogeneous part $I_{d+d'}$ is generated by the polynomials $g\, f_i$, where g is a term of degree d' and $i \in \{1, \ldots, m\}$. In particular, if $d' = 0$, then each polynomial in I_d is a linear combination of the polynomials $f_1, \ldots, f_m$.

Proof. For all $f \in I$, there exist homogeneous polynomials $g_{i,e} \in K[\vec{x}]$ of degree $e \geqslant 0$, $i \in \{1, \ldots, m\}$, such that

$$f = \sum_{e \geqslant 0} \sum_{i=1}^{m} g_{i,e}\, f_i.$$

The polynomial $g_{i,e}\, f_i$ has degree $d + e$. Now, let $f \in I_{d+d'}$. For all $e \neq d'$, it follows that $\sum_{i=1}^{m} g_{i,e}\, f_i = 0$. ◇

Chapter 2

CONVEX ALGEBRAIC GEOMETRY AND THETA BODIES

The computation of the projective norm or a test on separability can be difficult in general. An approach is to investigate the unit ball of the projective norm or the set of all separable states as a convex set.

In order to obtain information about a convex set, it can also be helpful to investigate a convex superset with specific properties, a so-called *convex relaxation*.

In this respect, we recall that a closed convex set in $\mathbb{R}^n$ is characterised by the set of all those affine half-spaces in which it is contained. This set can be large, so it could be helpful to look more closely at subsets which are easier to handle. This may describe the convex set completely, but even if not, it describes a convex relaxation.

Figure 2.1 shows a convex set (grey) and a convex relaxation (white and gray) which is defined by the intersection of four affine half-spaces whose complements are indicated by colours.

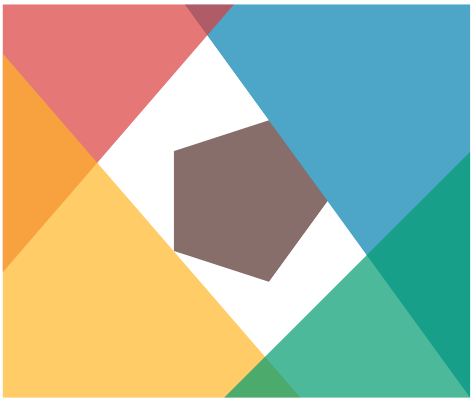


Figure 2.1: A relaxation of a convex set.

In this chapter, we introduce *theta bodies* according to [BPT]. Theta bodies are convex relaxations defined by affine half-spaces related to sums of polynomial squares.

In this respect, this chapter deals with convex algebraic geometry, which is the interplay between convex geometry and real algebraic geometry. The focus lies on sums of squares and theta bodies.

Section 2.1 deals with the notions of (real) algebraic geometry based on the standard literature.

Section 2.2 describes how a complex variety can be regarded as a real variety. This allows us to define *complex theta bodies* in Section 2.5.

Section 2.3 deals with the basic notions of convex geometry in complex and in real vector spaces. We pay special attention to the fact that convexity is a real notion.

Section 2.4 deals with some notions which can be helpful to understand a norm with the aid of its unit ball, which is, in particular, a convex set.

Section 2.5 deals with theta bodies.

2.1 Real Algebraic Geometry

Basics about algebraic geometry can be found in textbooks such as [GW], [Har], [Hat] or [Hul]. Basics about real algebraic geometry can be found in the standard textbook [BCR].

2.1.1 Basic Concepts of Algebraic Geometry

The polynomial ring in n variables over $\mathbb{K}$ is denoted by $\mathbb{K}[x_1, \dots, x_n]$ or by $\mathbb{K}[\vec{x}]$.

A polynomial in $\mathbb{K}[\vec{x}]$ can be regarded as a functional on $\mathbb{K}^n$. In this respect, $\mathbb{K}^n$ is called the *real* or the *complex affine space*.

The set of zeros of a polynomial $f \in \mathbb{K}[\vec{x}]$ or a subset $M \subseteq \mathbb{K}[\vec{x}]$ is denoted by

$$\begin{aligned} \mathcal{Z}_{\mathbb{K}}(f) &:= \{v \in \mathbb{K}^n \colon f(v) = 0\} \text{ and} \\ \mathcal{Z}_{\mathbb{K}}(M) &:= \{v \in \mathbb{K}^n \colon g(v) = 0 \text{ for all } g \in M\}, \end{aligned}$$

respectively. Such sets are called *real* or *complex affine algebraic varieties*, briefly *varieties*. We immediately obtain $\mathcal{Z}_{\mathbb{K}}(M) = \mathcal{Z}_{\mathbb{K}}(\mathrm{Id}(M))$. According to the Hilbert Basis Theorem, each affine variety is defined by a finite set of polynomials.

For any $V \subseteq \mathbb{K}^n$, let

$$\mathcal{I}_{\mathbb{K}}(V) := \{f \in \mathbb{K}[\vec{x}] \colon f(v) = 0 \text{ for all } v \in V\}.$$

This set is called the *real* and the *complex vanishing ideal* of V, respectively.

The following useful properties of varieties can be found in [Hat, Proposition 1.1 and Proposition 1.2]:

Proposition. Let $M, N \in \mathbb{K}[\vec{x}]$ with $M \subseteq N$, let S be an arbitrary index set and let $(M_s)_{s \in S}$ be a family of subsets of $\mathbb{K}[\vec{x}]$. Then we have

(i) $\mathcal{Z}_{\mathbb{K}}(N) \subseteq \mathcal{Z}_{\mathbb{K}}(M)$,

(ii) $\mathcal{Z}_{\mathbb{R}}(\mathbb{K}[\vec{x}]) = \emptyset$ and $\mathcal{Z}_{\mathbb{R}}(0) = \mathbb{K}^n$,

(iii) $\bigcap_{s \in S} \mathcal{Z}_{\mathbb{K}}(M_s) = \mathcal{Z}_{\mathbb{K}}\left(\bigcup_{s \in S} M_s\right)$, that is, arbitrary intersections of varieties are also varieties, and

(iv) $\mathcal{Z}_{\mathbb{K}}(M) \cup \mathcal{Z}_{\mathbb{K}}(N) = \mathcal{Z}_{\mathbb{K}}(\mathrm{Id}(M) \cap \mathrm{Id}(N))$, that is, finitely many unions of varieties are also varieties.

Proof. The statements (i)-(iii) can be easily verified. To show (iv), we first note that $\mathcal{Z}_{\mathbb{K}}(M) \cup \mathcal{Z}_{\mathbb{K}}(N) \subseteq \mathcal{Z}_{\mathbb{K}}(\mathrm{Id}(M) \cap \mathrm{Id}(N))$ can be obtained immediately. The remaining implication can be shown by contraposition. Assuming that $v \notin \mathcal{Z}_{\mathbb{K}}(M) \cup \mathcal{Z}_{\mathbb{K}}(N)$, there exist $f \in M$ and $g \in N$ with $f(v) \neq 0$ and $g(v) \neq 0$. Since $fg(v) \neq 0$ and $fg \in \mathrm{Id}(M) \cap \mathrm{Id}(N)$, we obtain $v \notin \mathcal{Z}_{\mathbb{K}}(\mathrm{Id}(M) \cap \mathrm{Id}(N))$. ◇

Remark. The complements of the algebraic varieties form the basis of a topology on the affine space $\mathbb{K}^n$, the *Zariski topology*. The Zariski topology is both an essential concept of algebraic geometry and an example for a topology which is (usually) not Hausdorff.

2.1.2 Hilbert's Nullstellensatz

Definition. An ideal $I \subseteq \mathbb{C}[\vec{x}]$ is said to be a *radical ideal*, if for all $f \in \mathbb{C}[\vec{x}]$ and for all $m \in \mathbb{N}$, the statement $f^m \in I$ implies $f \in I$.

The following well-known theorem can be regarded as a characterisation of vanishing ideals in the complex case.

Theorem. *(Hilbert's Nullstellensatz)*
Let $I \subseteq \mathbb{C}[\vec{x}]$ be an ideal. Then $I = \mathcal{I}_{\mathbb{C}}(\mathcal{Z}_{\mathbb{C}}(I))$ if and only if it is a radical ideal.

Proof. See [Har, Theorem 5.1]. ◇

Remark. The *radical* $\sqrt{I}$ of an ideal $I \subseteq \mathbb{C}[\vec{x}]$ is defined as the smallest radical ideal of $\mathbb{C}[\vec{x}]$ containing I. It is given by all $f \in \mathbb{C}[\vec{x}]$ such that $f^m \in I$ for some $m \in \mathbb{N}$, cf. [Har, Lecture 5].

2.1.3 The Real Nullstellensatz

Also for the real case, there exists a characterisation of vanishing ideals. The corresponding theorem will be useful below when we deal with symmetries of theta bodies.

Definition. An ideal $I \subseteq \mathbb{R}[\vec{x}]$ is said to be *real*, if for all $s \in \mathbb{N}$ and for all $g_1, \dots, g_s \in \mathbb{R}[\vec{x}]$ the statement $\sum_{t=1}^{s} g_t^2 \in I$ implies $g_1, \dots, g_s \in I$.

Theorem. *(Real Nullstellensatz)*
Let $I \subseteq \mathbb{R}[\vec{x}]$ be an ideal. Then $I = \mathcal{I}_{\mathbb{R}}(\mathcal{Z}_{\mathbb{R}}(I))$ if and only if I is real.

Proof. See [BCR, Proposition 4.4.6]. $\diamond$

Remark. The *real radical* $\sqrt[\mathbb{R}]{I}$ of an ideal $I \subseteq \mathbb{R}[\vec{x}]$ is defined as the smallest real ideal of $\mathbb{R}[\vec{x}]$ containing I. It is given by all $f \in \mathbb{R}[\vec{x}]$ with the property that there exists $m \in \mathbb{N}$ and $g_1, \dots, g_s \in \mathbb{R}[\vec{x}]$ such that $f^{2m} + \sum_{t=1}^{s} g_t^2 \in I$, see [BCR, Proposition 4.1.7].

Example. Since the real numbers are not algebraically closed, the real case and the complex case are different. To illustrate this, let $I := \mathrm{Id}(x^2 + 1) \subseteq \mathbb{K}[x]$. In the case where $\mathbb{K} = \mathbb{R}$, it can be easily verified that $1 \in \sqrt[\mathbb{R}]{I}$, in other words, $\mathbb{R}[x] = \sqrt[\mathbb{R}]{I}$. Indeed, we obtain $\mathbb{R}[x] = \mathcal{I}_{\mathbb{R}}(\mathcal{Z}_{\mathbb{R}}(I))$ since the polynomial $x^2 + 1$ has no real zero. On the other hand, we have $1 \notin \mathcal{I}_{\mathbb{C}}(\mathcal{Z}_{\mathbb{C}}(I))$, that is, $\mathbb{C}[x] \neq \mathcal{I}_{\mathbb{C}}(\mathcal{Z}_{\mathbb{C}}(I))$.

2.1.4 Projective Varieties

One could ask how varieties behave under intersections. As an example, there exists exactly one point of intersection between two distinct lines in the plane, if they are not parallel. However, the one-point perspective suggests parallel lines to meet "at infinity". This viewpoint has the advantage that there is always exactly one "point of intersection".

Those ideas can be realised by projective spaces. In Subsection 2.1.1 we considered the vector space $\mathbb{K}^n$ as a (real or complex) affine space, that is, as a set of "points", at which polynomials in $\mathbb{K}[x_0, \dots, x_n]$ can be evaluated.

The *real* or *complex projective space* $\mathbb{P}^n$ is defined as the set of all one-dimensional subspaces in $\mathbb{K}^{n+1}$, that is, the set of all lines in $\mathbb{K}^{n+1}$ which pass the origin. A line in $\mathbb{K}^{n+1}$, passing through $v := (v_0, v_1, \dots, v_n) \in \mathbb{K}^{n+1}$, $v \neq 0$, represents a *point* in $\mathbb{P}^n$. This point is denoted by $[v]$ or by $v_0 : v_1 : \dots : v_n$. It is equal to $\lambda v_0 : \lambda v_1 : \dots : \lambda v_n$ for each factor $\lambda \neq 0$.

With respect to the affine space $\mathbb{K}^{n+1}$, a polynomial $f \in \mathbb{K}[x_0, \dots, x_n]$ can be evaluated at each point $v \in \mathbb{K}^{n+1}$. In general, the result for another representative of $[v]$ is different. Assuming that f is homogeneous leads to the result $f(\lambda v) = \lambda^{\deg(f)} f(v)$ for each $\lambda \in \mathbb{K}$. Thus, in the case that f vanishes on v, it vanishes also at each representative of $[v]$. Hence, according to the definitions in Subsection 2.1.1, the set of zeros of a homogeneous polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ or a subset M of homogeneous polynomials in $\mathbb{K}[x_0, \ldots, x_n]$ can be defined by

$$\begin{aligned} \mathcal{Z}_{\mathbb{K}}(f) &:= \{[v] \in \mathbb{P}^n \colon f(v) = 0\} \text{ and} \\ \mathcal{Z}_{\mathbb{K}}(M) &:= \{[v] \in \mathbb{P}^n \colon g(v) = 0 \text{ for all } g \in M\}, \end{aligned}$$

respectively. Such sets are called *real* or *complex projective algebraic varieties*, briefly *(projective) varieties*. The generated ideal $\text{Id}(M)$ is homogeneous and we immediately obtain $\mathcal{Z}_{\mathbb{K}}(M) = \mathcal{Z}_{\mathbb{K}}(\text{Id}(M))$. Thus, a projective variety is the set of zeros of a homogeneous ideal.

According to Proposition 2.1.1, one can show that arbitrary intersections and finitely many unions of projective varieties are also projective varieties.

In this respect, it is appropriate to define *points*, *lines*, *planes* and so on as follows: Since the coordinate functions are homogeneous, any injective linear map from $\mathbb{K}^{k+1}$ to $\mathbb{K}^{n+1}$, where $k \in \{0, \ldots, n\}$, can also be considered as a function from $\mathbb{P}^k$ to $\mathbb{P}^n$. The image is called a k-*plane* of $\mathbb{P}^n$. The 0-planes are called *points*, the 1-planes *lines* and the 2-planes *planes*. Now, it can be easily verified that two distinct lines always have exactly one point in common.

Indeed, k-planes are projective varieties, since they can always be expressed as the set of zeros of appropriate linear forms.

2.1.5 Affine Varieties as Projective Varieties

There are several possibilities to identify the affine space $\mathbb{K}^n$ with a subset of $\mathbb{P}^n$. For example, a point $(v_1, \ldots, v_n) \in \mathbb{K}^n$ can be identified with the point $1 : v_1 : \cdots : v_n$ by "fixing" the first entry (this function is denoted by α). Another possibility is to identify $\mathbb{K}^n$ with the "half sphere" $\{w = (w_0, \ldots, w_n) \in \mathbb{K}^{n+1} \colon \|w\| = 1, w_0 > 0\}$.

An affine variety in $\mathbb{K}^{n+1}$, defined by homogeneous polynomials, can also be regarded as a projective variety in $\mathbb{P}^n$.

An affine variety in $\mathbb{K}^n$, which is defined by an arbitrary ideal, can also be regarded as a projective variety in the following sense: Each polynomial $f \in \mathbb{K}[x_0, \ldots, x_n]$ can be assigned uniquely to a homogeneous polynomial $f_h \in \mathbb{K}[x_0, \ldots, x_{n+1}]$: Let $k := \deg(f)$ be the degree of f. Each term t of f is assigned to the term $x_0^{k-\deg(t)} \cdot t$, which has degree k. If $v = (v_1, \ldots, v_n) \in \mathbb{K}^n$ vanishes at f, then $1 : v_1 : \cdots : v_n$ vanishes at f_h, that is, the set of zeros of f_h in $\alpha(\mathbb{K}^n)$ equals $\alpha(\mathcal{Z}_{\mathbb{K}}(f))$.

2.1.6 Dimension and Degree of a Projective Variety

Now, let $\mathbb{K} = \mathbb{C}$.

In the following, we outline some notions and properties of projective varieties which can be helpful at a later stage to understand the theta bodies which are interesting for us.

A projective variety $V \subseteq \mathbb{P}^n$ is called *irreducible*, if it is not possible to write it as the union of two projective varieties, both different from V. It can be shown (see [Har] for details) that any projective variety can be expressed uniquely as a finite union of irreducible components.

Definition. The *dimension* of an irreducible projective variety $V \subseteq \mathbb{P}^n$, written $\dim(V)$, is the length k of a maximal chain of irreducible subvarieties

$$V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_k = V,$$

where V_0 is a point. The dimension of an arbitrary projective variety is defined as the maximum of the dimensions of its irreducible components.

This definition of "dimension" goes along with the concept of "dimension" of manifolds, see [Har] for details.

For example, a *hypersurface* is the set of zeros of a homogeneous polynomial. It can be shown that the hypersurfaces are exactly those varieties in $\mathbb{P}^n$ with dimension $n-1$.

The *degree* of the set of zeros of an irreducible homogeneous polynomial is defined as its degree.

An alternative viewpoint could be motivated as follows: Let $f \in \mathbb{R}[x, y]$ be a polynomial of the form $y = f_0(x)$, where $f_0 \in \mathbb{R}[x]$ has degree 2. The degree of f is equal to the maximal number of points of intersections of $\mathcal{Z}_{\mathbb{R}}(f)$ in the x-y-plane with a horizontal line.

The *degree* of a projective variety is defined in [Har]. The definition involves so-called "general planes", which means that a statement should be true for "almost all" planes. We give a rough sketch:

Let $V \subseteq \mathbb{P}^n$ be an irreducible k-dimensional projective variety. Let P be a "general $(n-k)$-plane" in $\mathbb{P}^n$. Then the "degree" of V, written $\deg(V)$, is the number of points of intersection of P with V.

2.1.7 The Hilbert Function

Projective varieties can be regarded as intersections of hypersurfaces: A variety $V \subseteq \mathbb{P}^n$ is determined by a homogeneous ideal $I \subseteq \mathbb{C}[x_0, \ldots, x_n]$, generated by a set of homogeneous polynomials, each defining a hypersurface which contains V. Moreover, for each degree $m \in \mathbb{N}_0$, each polynomial which lies in the homogeneous part I_m defines a hypersurface which contains V.

The function

$$\begin{aligned} \mathcal{H} : \ & \mathbb{N}_0 \to \mathbb{N}_0 \\ & m \mapsto \dim\left(\mathbb{C}[x_0, \ldots, x_n]_m / I_m\right) \end{aligned}$$

is called the *Hilbert function*. It "collects" the codimensions of the homogeneous part I_m with respect to the space of homogeneous polynomials of degree m.

The Hilbert function gives rise to a polynomial whose leading term gives the dimension and the degree of V:

Theorem. There exists a univariate polynomial $p \colon \mathbb{C} \to \mathbb{C}$, called *Hilbert polynomial*, and $m_0 \in \mathbb{N}$ such that $\mathcal{H}(m) = p(m)$ for all $m \geqslant m_0$. We have

(i) $\dim(V) = \deg(p)$,
(ii) $\deg(V) = \mathrm{LC}(p) \cdot \deg(p)!$.

Proof. See [Har, Proposition 13.2 and page 166]. ◇

2.1.8 Transformations of Varieties

We conclude this section with our simple, but useful observation that linear transformations of varieties go along with transformations of the associated vanishing ideal. It will be essential for the proofs which are related to symmetries of theta bodies.

Proposition. Let $V \subseteq \mathbb{K}^n$ be a real or a complex affine algebraic variety and let $I := \mathcal{I}_{\mathbb{K}}(V)$ be the real or complex vanishing ideal of V. Let $A \in \mathcal{M}_n(\mathbb{K})$ be an invertible matrix. Then we have

$$\mathcal{I}_{\mathbb{K}}(A(V)) = I \circ A^{-1}.$$

If $A(V) = V$, then we have $I = I \circ A^{-1}$.

Proof. The following equivalence holds:

$$\begin{aligned} f \in \mathcal{I}_{\mathbb{K}}(A(V)) &\Leftrightarrow f(v) = 0 \text{ for all } v \in A(V) \\ &\Leftrightarrow f \circ A \in \mathcal{I}_{\mathbb{K}}(V) = I \\ &\Leftrightarrow f \in I \circ A^{-1}. \end{aligned}$$

If $A(V) = V$, then we have $I = \mathcal{I}_{\mathbb{K}}(V) = \mathcal{I}_{\mathbb{K}}(A(V)) = I \circ A^{-1}$. ◇

2.2 Complex Varieties as Real Varieties

We will see in Section 2.5 that the concept of theta bodies requires special properties of the real numbers which the complex numbers miss, for example, that squares are always positive numbers. Indeed, a key feature which distinguishes real algebraic geometry from complex algebraic geometry is that polynomials which are sums of squares are always positive.

However, a vector space over the complex numbers can also be considered as a vector space over the reals with double dimension. This simple observation helps to apply concepts which work in the real setting also to a complex setting.

The main theorem of this section shows that a complex variety can always be identified uniquely with a real variety, see Theorem 2.2.5. The idea is to decompose a complex polynomial into its *real part* and its *imaginary part* according to [Voi]. This allows us to define complex theta bodies in Section 2.5.

2.2.1 The Decomplexification of Complex Affine Spaces

The complex vector space $\mathbb{C}^n$ can be identified (real-linear) with the real vector space $\mathbb{R}^{2n}$. This can be done by separating the real and the imaginary part from the complex coordinates, by way of example with the following real linear isometry:

$$\begin{array}{rccl} \imath\colon & \mathbb{C}^n & \to & \mathbb{R}^{2n} \\ & (\nu_k)_{k=1}^n & \mapsto & (\operatorname{Re}(\nu_k), \operatorname{Im}(\nu_k))_{k=1}^n \,. \end{array}$$

The basis vectors of $\mathbb{R}^{2n}$ are indexed by the set $\{1, \dots, n\} \times \{1, 2\}$, so that for all $k \in \{1, \dots, n\}$, the images of e_k and of $i\, e_k$ are denoted by $e_{k,1}$ and $e_{k,2}$, respectively. For all $\nu \in \mathbb{C}^n$, the image $\imath(\nu)$ is also called the *decomplexification* of ν, see [KM, §12, page 75].

2.2.2 The Real and the Imaginary Part of the Coefficients

Using the notation from Section 1.1, a term in $\mathbb{C}[x_1, \dots, x_n]$ has the form $x^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$.

We first consider the following real linear maps:

$$\begin{array}{rrcl} \operatorname{Re}_0\colon & \mathbb{C}[x_1, \dots, x_n] & \to & \mathbb{R}[x_1, \dots, x_n] \\ & c \cdot x^\alpha & \mapsto & \operatorname{Re}(c) \cdot x^\alpha, \\ \operatorname{Im}_0\colon & \mathbb{C}[x_1, \dots, x_n] & \to & \mathbb{R}[x_1, \dots, x_n] \\ & c \cdot x^\alpha & \mapsto & \operatorname{Im}(c) \cdot x^\alpha. \end{array}$$

Proposition. Let $f, g \in \mathbb{C}[x_1, \dots, x_n]$. Then

$$\begin{aligned} \operatorname{Re}_0(f \cdot g) &= \operatorname{Re}_0(f) \cdot \operatorname{Re}_0(g) - \operatorname{Im}_0(f) \cdot \operatorname{Im}_0(g), \\ \operatorname{Im}_0(f \cdot g) &= \operatorname{Re}_0(f) \cdot \operatorname{Im}_0(g) + \operatorname{Im}_0(f) \cdot \operatorname{Re}_0(g). \end{aligned}$$

Proof. Let $c, d \in \mathbb{C}$ and let $x^\alpha, x^\beta \in \mathbb{C}[x_1, \dots, x_n]$. It suffices to show the statement for $f := cx^\alpha$ and $g := dx^\beta$:

$$\begin{aligned} \operatorname{Re}_0(f \cdot g) &= \operatorname{Re}_0(cd \cdot x^{\alpha+\beta}) = \operatorname{Re}(cd) \cdot x^{\alpha+\beta} \\ &= \operatorname{Re}(c) \operatorname{Re}(d) x^{\alpha+\beta} - \operatorname{Im}(c) \operatorname{Im}(d) x^{\alpha+\beta} \\ &= \operatorname{Re}_0(f) \operatorname{Re}_0(g) - \operatorname{Im}_0(f) \operatorname{Im}_0(g), \\ \operatorname{Im}_0(f \cdot g) &= \operatorname{Im}(cd) \cdot x^{\alpha+\beta} \\ &= \operatorname{Re}_0(f) \operatorname{Im}_0(g) + \operatorname{Im}_0(f) \operatorname{Re}_0(g). \end{aligned}$$

◇

Lemma. Let $g \in \mathbb{C}[x_1, \dots, x_n]$. We have

$$g = \operatorname{Re}_0(g) + i \operatorname{Im}_0(g).$$

Hence, for all $v \in \mathbb{R}^n \subseteq \mathbb{C}^n$, it follows that

$$\begin{aligned} \operatorname{Re}(g(v)) &= \operatorname{Re}_0(g)(v), \\ \operatorname{Im}(g(v)) &= \operatorname{Im}_0(g)(v), \end{aligned}$$

and

$$\mathcal{Z}_{\mathbb{C}}(g) \cap \mathbb{R}^n = \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}_0(g), \operatorname{Im}_0(g)).$$

Proof. The equation $g = \operatorname{Re}_0(g) + i \operatorname{Im}_0(g)$ can be easily verified. For any $v \in \mathbb{C}^n$ with real coordinates (that is, $v \in \mathbb{R}^n$), we obtain $\operatorname{Re}(g(v)) = \operatorname{Re}_0(g)(v)$ and $\operatorname{Im}(g(v)) = \operatorname{Im}_0(g)(v)$. Furthermore, we obtain

$$\begin{aligned} v \in \mathcal{Z}_{\mathbb{C}}(g) &\Leftrightarrow g(v) = 0 \\ &\Leftrightarrow \operatorname{Re}(g(v)) = 0 \text{ and } \operatorname{Im}(g(v)) = 0 \\ &\Leftrightarrow v \in \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}_0(g)) \text{ and } v \in \mathcal{Z}_{\mathbb{R}}(\operatorname{Im}_0(g)). \end{aligned}$$

Now, $v \in \mathcal{Z}_{\mathbb{C}}(g)$ if and only if $v \in \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}_0(g), \operatorname{Im}_0(g))$. ◇

We note that the last lemma requires that $v \in \mathbb{R}^n$. In particular, it states that for any finite subset $M \subseteq \mathbb{C}[x_1, \ldots, x_n]$, we obtain

$$\mathcal{Z}_{\mathbb{C}}(M) \cap \mathbb{R}^n = \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}_0(M) \cup \operatorname{Im}_0(M)).$$

Hence, the real coordinates of a complex variety can be expressed as a real variety. In what follows, we want to express the whole complex variety as a real variety. To do so, it seems to be helpful to consider real coordinates for both the real and the imaginary part of each complex coordinate, using the decomplexification $\imath$ from Subsection 2.2.1. But this requires to work in a polynomial ring with more variables, since for both the real and the imaginary part there has to be a corresponding functional.

2.2.3 The Real and the Imaginary Part of a Polynomial

We consider the ring homomorphism

$$\begin{array}{rccc} \jmath\colon & \mathbb{C}[x_1, \ldots, x_n] & \to & \mathbb{C}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}] \\ & x_k & \mapsto & x_{k,1} + i \cdot x_{k,2}, \end{array}$$

that is, for all terms $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} = x^\alpha$, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, we have

$$\jmath(x^\alpha) = (x_{1,1} + i \cdot x_{1,2})^{\alpha_1} \cdot \ldots \cdot (x_{n,1} + i \cdot x_{n,2})^{\alpha_n}$$

and the function is complex linear.

For the purpose of a clear subscription, the basis vectors in the corresponding affine space $\mathbb{C}^{2n}$ are indexed by the set $\{1,\dots,n\}\times\{1,2\}$, so that the terms $x_{k,s}$, where $k \in \{1,\dots,n\}$ and $s \in \{1,2\}$, are (regarded as a function) determined by

$$x_{k,s}(e_{l,t}) := \begin{cases} 1, & k = l \text{ and } s = t, \\ 0, & \text{otherwise} \end{cases}$$

for all $l \in \{1,\dots,n\}$ and for all $t \in \{1,2\}$.

Definition. For all $f \in \mathbb{C}[x_1,\dots,x_n]$, let

$$\begin{aligned} \operatorname{Re}(f) &:= \operatorname{Re}_0(\jmath(f)), \\ \operatorname{Im}(f) &:= \operatorname{Im}_0(\jmath(f)). \end{aligned}$$

be the *real* and the *imaginary part* of f, respectively.

Proposition. Let $f, g \in \mathbb{C}[x_1,\dots,x_n]$. Then

$$\begin{aligned} \operatorname{Re}(f \cdot g) &= \operatorname{Re}(f) \cdot \operatorname{Re}(g) - \operatorname{Im}(f) \cdot \operatorname{Im}(g), \\ \operatorname{Im}(f \cdot g) &= \operatorname{Re}(f) \cdot \operatorname{Im}(g) + \operatorname{Im}(f) \cdot \operatorname{Re}(g). \end{aligned}$$

Proof. The statement follows from Proposition 2.2.2, since $\jmath$ is a ring homomorphism. ◇

The real and the imaginary part of the term x^α (see above) can be derived explicitly as follows: For all $\beta = (\beta_1,\dots,\beta_n) \in \mathbb{N}_0^n$ and $\gamma = (\gamma_1,\dots,\gamma_n) \in \mathbb{N}_0^n$, let $x_1^\beta := x_{1,1}^{\beta_1} \cdot \ldots \cdot x_{n,1}^{\beta_n}$ and $x_2^\beta := x_{1,2}^{\beta_1} \cdot \ldots \cdot x_{n,2}^{\beta_n}$. Now, let

$$\begin{aligned} A_\alpha &:= \{(\beta,\gamma) \in (\mathbb{N}_0^n)^2 \colon \beta + \gamma = \alpha\}, \\ A_{\alpha,1} &:= \{(\beta,\gamma) \in A_\alpha \colon |\gamma| \bmod 2 = 0\}, \text{ and} \\ A_{\alpha,2} &:= \{(\beta,\gamma) \in A_\alpha \colon |\gamma| \bmod 2 = 1\}. \end{aligned}$$

Then

$$\begin{aligned} \operatorname{Re}(x^\alpha) &= \sum_{(\beta,\gamma)\in A_{\alpha,1}} i^{|\gamma|}\, x_1^\beta \cdot x_2^\gamma, \\ \operatorname{Im}(x^\alpha) &= \sum_{(\beta,\gamma)\in A_{\alpha,2}} -i^{|\gamma|+1}\, x_1^\beta \cdot x_2^\gamma. \end{aligned}$$

Furthermore, we have $\operatorname{Re}(i\,x^\alpha) = -\operatorname{Im}(x^\alpha)$ and $\operatorname{Im}(i\,x^\alpha) = \operatorname{Re}(x^\alpha)$.

2.2.4 The Decomplexification of a Complex Ideal

Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal.

Definition. The ideal $\imath(I)$ in the polynomial ring $\mathbb{R}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}]$ which is generated by $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$, where $f \in I$, is called the *decomplexification* of the *complex ideal* I. An ideal in $\mathbb{R}^{2n}$ is called *decomplexified*, if it is the decomplexification of a complex ideal.

The decomplexification of I is generated by the real and imaginary parts of the polynomials in I, but it suffices to consider a generating set of I:

Proposition. Let $F \subseteq I$ be a generating set of I. Then the decomplexification $\imath(I)$ is generated by $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$, where $f \in F$.

Proof. Let I^F be the ideal in $\mathbb{R}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}]$ which is generated by $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$, where $f \in F$. We show that $\imath(I) = I^F$.

By definition, we have $I^F \subseteq \imath(I)$. On the other hand, each $h \in I$ is a sum of polynomials $g \cdot f$, where $g \in \mathbb{C}[x_1, \ldots, x_n]$ and $f \in F$. Proposition 2.2.3 says that both $\mathrm{Re}(gf)$ and $\mathrm{Im}(gf)$ are in I^F. Hence, $\mathrm{Re}(h) \in I^F$ and $\mathrm{Im}(h) \in I^F$, so that $\imath(I) \subseteq I^F$. ◇

Remark. We note that it is not clear until now whether the decomplexification (that is, the function $\imath$ on the ideals of $\mathbb{C}[x_1, \ldots, x_n]$) is injective.

2.2.5 The Decomplexification of a Complex Variety

The following theorem is an adaption of Theorem 3.1.4 in [Voi]:

Theorem. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal. For all $v \in \mathbb{C}^n$, we have

$$\mathrm{Re}(f(v)) = \mathrm{Re}(f)(\imath(v)),$$
$$\mathrm{Im}(f(v)) = \mathrm{Im}(f)(\imath(v)),$$

that is,

(i) $f = \mathrm{Re}(f) \circ \imath + i \cdot \mathrm{Im}(f) \circ \imath$,
(ii) $\imath(\mathcal{Z}_{\mathbb{C}}(f)) = \mathcal{Z}_{\mathbb{R}}(\mathrm{Re}(f), \mathrm{Im}(f))$, and

(iii) $\imath(\mathcal{Z}_{\mathbb{C}}(I)) = \mathcal{Z}_{\mathbb{R}}(\imath(I))$.

In particular, there exists an injection from the varieties in $\mathbb{C}^n$ to the varieties in $\mathbb{R}^{2n}$.

Proof. We first state that

$$f(\nu) = \operatorname{Re}\left(\jmath(f)(\imath(\nu))\right) + i \cdot \operatorname{Im}\left(\jmath(f)(\imath(\nu))\right), \tag{2.1}$$

which implies the equation

$$\operatorname{Re}\left(f(\nu)\right) = \operatorname{Re}\left(\jmath(f)(\imath(\nu))\right). \tag{2.2}$$

Since $\imath(\nu) \in \mathbb{R}^{2n}$, Lemma 2.2.2 can be applied with $g := \jmath(f) \in \mathbb{C}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}]$, which leads to the equation

$$\operatorname{Re}\left(\jmath(f)(\imath(\nu))\right) = \left(\operatorname{Re}_0(\jmath(f))\right)(\imath(\nu)), \tag{2.3}$$

which equals $\operatorname{Re}(f)(\imath(\nu))$ by definition of the real part of f. Hence, equations (2.2) and (2.3) yield $\operatorname{Re}(f(\nu)) = \operatorname{Re}(f)(\imath(\nu))$. Similar arguments lead to $\operatorname{Im}(f(\nu)) = \operatorname{Im}(f)(\imath(\nu))$, so that (i) follows from equation (2.1). Now, we obtain

$$\begin{aligned} \nu \in \mathcal{Z}_{\mathbb{C}}(f) &\Leftrightarrow f(\nu) = 0 \\ &\Leftrightarrow \operatorname{Re}(f(\nu)) = 0 \text{ and } \operatorname{Im}(f(\nu)) = 0 \\ &\Leftrightarrow \operatorname{Re}(f)(\imath(\nu)) = 0 \text{ and } \operatorname{Im}(f)(\imath(\nu)) = 0 \\ &\Leftrightarrow \imath(\nu) \in \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}(f)) \cap \mathcal{Z}_{\mathbb{R}}(\operatorname{Im}(f)), \end{aligned}$$

which shows (ii). Finally, let $M \subseteq \mathbb{C}[x_1, \ldots, x_n]$. Proposition 2.1.1 (iii) yields $\imath(\mathcal{Z}_{\mathbb{C}}(M)) = \mathcal{Z}_{\mathbb{R}}(\operatorname{Re}(M) \cup \operatorname{Im}(M))$. ◇

Definition. Let $V \subseteq \mathbb{C}^n$ be a complex affine variety. Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ such that $V = \mathcal{Z}_{\mathbb{C}}(I)$. The real affine variety $\imath(V) = \mathcal{Z}_{\mathbb{R}}(\imath(I))$ is called the *decomplexification* of the variety V. A variety in $\mathbb{R}^{2n}$ is called *decomplexified*, if it is the decomplexification of a complex variety.

We note that up to now, the symbol "$\imath$" stands for the decomplexification of a complex set, of a complex ideal, and of a complex variety, see the index of notation on page 305. In Subsection 2.2.10 this symbol will also stand for the decomplexification of a complex operator.

There is a one-to-one correspondence between complex varieties in $\mathbb{C}^n$ and decomplexified real varieties in $\mathbb{R}^n$.

2.2.6 Comparison of the Zariski Topologies

Each complex variety can be identified with a real variety. This allows to compare the corresponding Zariski topologies. For this purpose, we consider the Euclidean unit sphere $(\mathbb{K}^n)_1$ in $\mathbb{K}^n$. The Euclidean norm of $v = (v_1, \dots, v_n) \in \mathbb{C}^n$ is given by

$$\|v\|^2 = \sum_{k=1}^{n} v_k \cdot \bar{v}_k = \sum_{k=1}^{n} v_{k,1}^2 + v_{k,2}^2.$$

The unit sphere $(\mathbb{R}^n)_1$ is a real manifold in $\mathbb{R}^n$ with dimension $n-1$. It is also a real variety, induced by the polynomial $\sum_{k=1}^n x_k^2 - 1 \in \mathbb{R}[x_1, \dots, x_n]$. Hence, also $(\mathbb{R}^{2n})_1$ is a real manifold in $\mathbb{R}^{2n}$ with dimension $2n-1$, which is an odd number. This set is the decomplexification of the unit sphere $(\mathbb{C}^n)_1$, that is, $(\mathbb{R}^{2n})_1 = \imath((\mathbb{C}^n)_1)$. As a real variety, it is induced by $\sum_{k=1}^n (x_{k,1}^2 + x_{k,2}^2) - 1 \in \mathbb{R}[x_{1,1}, x_{1,2}, \dots, x_{n,1}, x_{n,2}]$.

Proposition. The unit sphere $(\mathbb{C}^n)_1$ is not a complex variety, that is, the unit sphere $(\mathbb{R}^{2n})_1$ is not decomplexified. In particular, the Zariski topology in the complex affine space $\mathbb{C}^n$ is strictly coarser than the Zariski topology in the corresponding real affine space $\mathbb{R}^{2n}$.

Proof. Let $V \subseteq \mathbb{C}^n$ be a variety. Due to [Hul, Section 3], the set of smooth points of V is open and dense in V. For each smooth point $v \in V$, there exists a neighbourhood U of v in V such that U is a manifold. The dimension r of U equals the dimension of the tangential space at v, which is a vector space over $\mathbb{C}$. Hence, we may conclude that, regarded as a real manifold, U has dimension $2r$, which is even. The dimension of $\imath((\mathbb{C}^n)_1)$ as a real manifold is odd, and hence, $(\mathbb{C}^n)_1$ is not a complex variety. ◇

Example. The Zariski closed sets in $\mathbb{C}$ are given by finitely many points, the empty set and $\mathbb{C}$. But in $\mathbb{R}^2$, also the coordinate axes are Zariski closed sets, since they are the sets of zeros of the ideals $\mathrm{Id}(x_1)$ and $\mathrm{Id}(x_2)$ in $\mathbb{R}[x_1, x_2]$. Hence, each of them cannot be decomplexified.

2.2.7 Decomplexified Ideals as Vector Spaces

Any ideal $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ can also be considered as a vector space over $\mathbb{C}$.

Proposition. Let $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ be an ideal with $I \neq \mathbb{C}[x_1, \ldots, x_n]$ and let $B \subseteq I$. Let $B' := \mathrm{Re}(B) \cup \mathrm{Im}(B)$. If B is linearly independent in I as a vector space over $\mathbb{C}$, then B' is linearly independent in $\imath(I)$ as a vector space over $\mathbb{R}$. In particular, B' is a basis of $\mathrm{LH}(B')$.

Proof. Each polynomial in B is non-constant, since $I \neq \mathbb{C}[x_1, \ldots, x_n]$ (which means that $1 \notin I$). Let $f_1, \ldots, f_k$ be non-constant linearly independent polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. We show that the polynomials $\mathrm{Re}(f_1), \ldots, \mathrm{Re}(f_k), \mathrm{Im}(f_1), \ldots, \mathrm{Im}(f_k)$ are linearly independent.

To do this, we assume that $\mathrm{Re}(f_1), \ldots, \mathrm{Re}(f_k), \mathrm{Im}(f_1), \ldots, \mathrm{Im}(f_k)$ are linearly dependent, that is, there exists

$$\lambda_{1,1}, \ldots, \lambda_{1,k}, \lambda_{2,1}, \ldots, \lambda_{2,k} \in \mathbb{R},$$

which are not all zero, such that

$$g := \sum_{l=1}^{k} (\lambda_{l,1}\,\mathrm{Re}(f_l) - \lambda_{l,2}\,\mathrm{Im}(f_l)) = 0.$$

This yields $g = \mathrm{Re}(f_\lambda)$ for

$$f_\lambda := \sum_{l=1}^{k} \lambda_l f_l,$$

where $\lambda_l := \lambda_{l,1} + i\lambda_{l,2}$ and $0 \neq \lambda := (\lambda_1, \ldots, \lambda_k) \in \mathbb{C}^n$. Hence, for all $v \in \mathbb{C}^n$, we obtain

$$0 = g(\imath(v)) = (\mathrm{Re}(f_\lambda))(\imath(v)) = \mathrm{Re}(f_\lambda(v)).$$

Hence, f_λ is a multivariate polynomial whose real part is zero. A holomorphic function on $\mathbb{C}$ which is non-constant maps open sets on open sets. Thus, each section of f_λ is a constant function, so that f_λ is a constant function. It follows that $1, f_1, \ldots, f_k$ are linearly dependent. By assumption, $f_1, \ldots, f_k$ are linearly independent, which implies that also $1, f_1, \ldots, f_k$ are linearly independent, since $1 \notin I$. This is a contradiction. ◇

The last statement requires $I \neq \mathbb{C}[x_1, \ldots, x_n]$ since $\mathrm{Im}(1) = 0$.

Example. The following example illustrates that even if $B \subseteq I$ is a basis of I, the decomplexification $\imath(I)$ can be larger than $\mathrm{LH}(B')$. Let $I := \mathrm{Id}(x) \subseteq$

$\mathbb{C}[x]$. Then $B := \{x^k : k \in \mathbb{N}\}$ is a basis of I as a vector space over $\mathbb{C}$. We obtain

$$\begin{aligned} \operatorname{Re}(B) &= \{x_1,\ x_1^2 - x_2^2,\ x_1^3 - 3x_1x_2^2,\ \dots\}, \\ \operatorname{Im}(B) &= \{x_2,\ 2x_1x_2,\ 3x_1^2x_2 - x_2^3,\ \dots\}. \end{aligned}$$

Now, we can see that $x_1^2 \notin \mathrm{LH}(B')$ but $x_1^2 \in \imath(I) = \mathrm{Id}(x_1, x_2)$. Nevertheless, it could be interesting to find a basis of $\imath(I)$.

2.2.8 Decomplexified Ideals and Sums of Squares

Let $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal. Below, we investigate theta bodies of the decomplexification $\imath(I)$ in specific settings. The question arises whether the property of being an affine functional and a sum of squares modulo I can be expressed in real terms to obtain affine functionals which are sums of squares modulo $\imath(I)$. Let $l \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an affine functional such that $l = s + h$ for $h \in I$ and a sum of squares $s \in \mathbb{C}[x_1, \dots, x_n]$. Now, $\operatorname{Re}(l)$ and $\operatorname{Im}(l)$ are also affine functionals, and both $\operatorname{Re}(h)$ and $\operatorname{Im}(h)$ are in $\imath(I)$ by definition. Hence, both properties, to be an affine functional and to be in I, are "compatible" with the real setting.

However, the property of being a sum of squares is not "compatible" with the real setting: Let $f \in \mathbb{C}[x_1, \dots, x_n]$, then $\operatorname{Re}(f^2) = \operatorname{Re}(f)^2 - \operatorname{Im}(f)^2$, which is no sums of squares in general. Also $\operatorname{Im}(f^2) = 2\operatorname{Re}(f) \cdot \operatorname{Im}(f)$ is no sums of squares in general. Indeed, from Proposition 2.2.7, it follows that there exists no non-constant polynomial f such that $\operatorname{Re}(f)$ and $\operatorname{Im}(f)$ are scalar multiples of each other.

2.2.9 Gröbner Bases of Decomplexified Ideals

Let $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal. We assume that a Gröbner basis G of I is given, with respect to a term order on $\mathbb{C}[x_1, \dots, x_n]$. Now, one could ask for a Gröbner basis of the decomplexification $\imath(I)$. For instance, it suggests itself to ask whether the set $G' := \{\operatorname{Re}(g), \operatorname{Im}(g) : g \in G\}$ is a Gröbner basis of $\imath(I)$ with respect to an appropriate term order on $\mathbb{R}[x_{1,1}, x_{1,2}, \dots, x_{n,1}, x_{n,2}]$. In Section 5.4 we investigate this question in a special case. As we will see, a positive answer depends strongly on the underlying term order and does not seem to be canonically guaranteed.

2.2.10 The Decomplexification of Complex Operators

Interpreting the complex number field as a real vector space, the multiplication with a complex number $z \in \mathbb{C}$ can be represented by a 2×2 matrix $\imath(z)$:

$$\begin{aligned} &\mathbb{R}^2 \to \mathbb{R}^2, \\ &v \mapsto \begin{pmatrix} \mathrm{Re}(z) & -\mathrm{Im}(z) \\ \mathrm{Im}(z) & \mathrm{Re}(z) \end{pmatrix} \cdot v. \end{aligned}$$

A linear map $f\colon \mathbb{C}^n \to \mathbb{C}^m$ can be identified with a real linear map $\imath(f) \in \mathbb{R}^{2n} \to \mathbb{R}^{2m}$, which is called the *decomplexification* of f, see [KM, §12, page 75]. A corresponding $m \times n$ matrix $A = (a_{i,j})_{i,j=1}^{n}$ (with complex entries) can be assigned to a $2m \times 2n$ matrix $\imath(A)$ with real entries, representing the decomplexification of f: For instance, depending on the order on the basis, $\imath(A) = (\imath(a_{k,l}))_{k=1,\dots,m;l=1,\dots,n}$ or

$$\imath(A) = \begin{pmatrix} \mathrm{Re}(A) & -\mathrm{Im}(A) \\ \mathrm{Im}(A) & \mathrm{Re}(A) \end{pmatrix},$$

see also [KM, Theorem 12.3] and [BN, Theorem 1.4.2].

The Euclidean scalar products fulfils the equality $\mathrm{Re}(\langle\cdot,\cdot\rangle_{\mathbb{C}^n}) = \langle\cdot,\cdot\rangle_{\mathbb{R}^{2n}}$.

Proposition. Let $A \in \mathcal{M}_{m,n}(\mathbb{C})$ and $B \in \mathcal{M}_{n,m'}(\mathbb{C})$.

(i) $\imath(A \cdot B) = \imath(A) \cdot \imath(B)$.

(ii) If A is invertible, then $\imath(A)$ is invertible and $\imath(A^{-1}) = \imath(A)^{-1}$.

(iii) $\imath(A^\star) = \imath(A)^t$.

Proof. The product of two matrices or the transpose of a matrix can be determined block by block. ◇

Corollary. If A is quadratic and normal/self-adjoint/unitary/positive, then $\imath(A)$ is normal/symmetric/orthogonal/positive (respectively).

Proof. This statement follows from the last proposition. ◇

An affine functional in $\mathbb{C}[x_1, \dots, x_n]$ has the form

$$l = c_0 + c_1x_1 + \cdots + c_nx_n,$$

where $c_k \in \mathbb{C}$. The real and the imaginary part are given by

$$\begin{aligned}\operatorname{Re}(l) &= \operatorname{Re}(c_0) + \sum_{k=1}^{n} (\operatorname{Re}(c_k)\operatorname{Re}(x_k) - \operatorname{Im}(c_k)\operatorname{Im}(x_k)) \text{ and}\\ \operatorname{Im}(l) &= \operatorname{Im}(c_0) + \sum_{k=1}^{n} (\operatorname{Im}(c_k)\operatorname{Re}(x_k) + \operatorname{Re}(c_k)\operatorname{Im}(x_k)).\end{aligned}$$

Remark. There is also another approach to consider a complex affine-linear map as a real affine-linear map, using the component functions together with Theorem 2.2.5. Let $A\colon \mathbb{C}^n \to \mathbb{C}^m$ be an affine-linear map, that is, there exist polynomials $f_k = \sum_{l=1}^{n} c_{k,l}x_l + c_{k,0} \in \mathbb{C}[x_1,\dots,x_n]_1$, where $c_{k,l}, c_{k,0} \in \mathbb{C}$, such that $A(v) = (f_1(v),\dots,f_m(v))^t$ for all $v \in \mathbb{C}^n$. Now, the linear part of A can be represented by the $m \times n$ matrix $B := (c_{k,l})_{k=1,\dots,m;l=1,\dots,n}$. The translation is represented by $C := (c_{1,0},\dots,c_{m,0})^t \in \mathbb{C}^m$. From Theorem 2.2.5, it follows that

$$A = \operatorname{Re}(A) \circ \imath + i \cdot \operatorname{Im}(A) \circ \imath.$$

In terms of matrices, arranging $\imath(v) = (\operatorname{Re}(v), \operatorname{Im}(v))^t$, we obtain

$$\begin{aligned}\imath(A(v)) &= \imath \begin{pmatrix} (\operatorname{Re}(f_1) + i \cdot \operatorname{Im}(f_1))\,(\imath(v)) \\ \vdots \\ (\operatorname{Re}(f_m) + i \cdot \operatorname{Im}(f_m))\,(\imath(v)) \end{pmatrix}\\ &= \begin{pmatrix} \operatorname{Re}(B) & -\operatorname{Im}(B) \\ \operatorname{Im}(B) & \operatorname{Re}(B) \end{pmatrix} \cdot \begin{pmatrix} \operatorname{Re}(v) \\ \operatorname{Im}(v) \end{pmatrix} + \begin{pmatrix} \operatorname{Re}(c) \\ \operatorname{Im}(c) \end{pmatrix}\\ &= \imath(B) \cdot \imath(v) + \imath(c).\end{aligned}$$

2.3 Convex Geometry

This section deals with basic notions from convex geometry according to the textbooks [Gru], [Roc] and [SW].

As above, we can consider a complex vector space as a real vector space with double dimension. For both spaces, the definition of convexity uses only real numbers. Therefore, convex sets in the former are convex sets in the latter and vice versa. In this respect, we compare some notions that are related to convexity over the real and complex numbers such as *affine half-space*, *face*, or *extreme point*.

The next section deals with those convex sets which are the unit ball of a norm.

Details for both sections can also be found in books or in articles on functional analysis such as [Con], [BN], or [Arv]. With a focus on theta bodies, see [BPT], [Voi], or [Lang].

2.3.1 Convex Sets

Definition. A point $z \in \mathbb{K}^n$ is called a *convex combination* of points $v_1, \dots, v_m \in \mathbb{K}^n$, if it can be written as $z = \lambda_1 \cdot v_1 + \cdots + \lambda_m \cdot v_m$, where $0 \leqslant \lambda_k \leqslant 1$ for all $k \in \{1, \dots, m\}$ and $\lambda_1 + \cdots + \lambda_m = 1$. In this case, it is called *proper*, if $z \notin \{v_1, \dots, v_m\}$. A subset $C \subseteq \mathbb{K}^n$ is called *convex*, if all convex combinations of points in C are contained in C. The *convex hull* $\operatorname{co}(S)$ of a subset $S \subseteq \mathbb{K}^n$ is defined as the intersection of all convex sets $C \in \mathbb{K}^n$ with $S \subseteq C$. A compact convex set is called a *convex body*, which is called *proper*, if it has an interior point. A proper convex body C is called *strictly convex*, if all proper convex combinations of points in C are contained in the interior of C.

The convex hull $\operatorname{co}(S)$ of a set $S \subseteq \mathbb{K}^n$ is the set of all convex combinations of points of S, see [Gru, Lemma 3.1]. Due to Carathéodory's Theorem, each point in $\operatorname{co}(S)$ can be written as a convex combination of $n+1$ points of S, see [Gru, Theorem 3.1]. The convex hull of a compact set is a convex body, see [Gru, Corollary 3.1]. The closure of a convex set is convex, see [Gru, Proposition 3.1]. The convex hull of a closed set does not have to be closed in general. As an example may serve the convex hull of the union of a line and a point which is not on the line.

We note that decomplexification from Subsection 2.2.1 preserves convexity, that is, the notions for $\mathbb{C}^n$ trace back to the notions for $\mathbb{R}^{2n}$ which may be more geometrically intuitive.

2.3.2 Affine Hyperplanes and Affine Half-Spaces

We have seen above that convexity is defined using real numbers, so it would be sufficient to introduce the following notions only for the real case. Nevertheless, we decided explicitly to include both cases to avoid confusion.

As usual, the set of zeros of a non-constant affine functional is called an *affine hyperplane* in $\mathbb{K}^n$. It is a translate of a linear subspace of dimension $n-1$. The decomplexification of an affine hyperplane in $\mathbb{C}^n$ has real dimension $2n-2$, which implies that it does not trace back to an affine hyperplane in $\mathbb{R}^{2n}$, which has dimension $2n-1$. However, the complex case can be traced back to the real case by using the real part of an affine functional (in the literature, it is common to consider "real" affine functionals on $\mathbb{C}^n$, see [BN, Section 1.5]).

Definition. A translate of a real linear subspace of $\mathbb{K}^n$ is called a *real affine subspace*. The *real affine hull* of a set $M \subseteq \mathbb{K}^n$ is the smallest real affine subspace which contains M. A subset $H \subseteq \mathbb{K}^n$ is called an *affine half-space* if there exists an affine functional l of degree 1 such that

$$H = H_l = \{y \in \mathbb{K}^n \colon \operatorname{Re}(l(y)) \geqslant 0\}.$$

The set

$$P_l := \{y \in \mathbb{K}^n \colon \operatorname{Re}(l(y)) = 0\}$$

is called a *real affine hyperplane*.

The notions are adapted from [BN]. The real affine hull of $M \subseteq \mathbb{K}^n$ is given by all points $\lambda_1 \cdot v_1 + \cdots + \lambda_m \cdot v_m$, where $v_k \in M$ and $\lambda_k \in \mathbb{R}$ for all $k \in \{1, \ldots, m\}$ and where $\lambda_1 + \cdots + \lambda_m = 1$, see [Roc]. For any non-constant affine functional l, we have $\mathbb{K}^n = H_l \cup H_{-l}$, and the boundary of both H_l and H_l is given by P_l, which is a real affine subspace of $\mathbb{K}^n$. According to Theorem 2.2.5, for all $y \in \mathbb{K}^n$, we obtain $\operatorname{Re}(l(y)) = \operatorname{Re}(l)(\imath(y))$. Thus, $\imath(H_l) = H_{\operatorname{Re}(l)}$ and $\imath(P_l) = P_{\operatorname{Re}(l)}$.

Proposition. There is a one-to-one correspondence between affine half-spaces in $\mathbb{C}^n$ and in $\mathbb{R}^{2n}$ (and real affine hyperplanes, respectively).

Proof. As we have seen, the decomplexification of an affine half-space (a real affine hyperplane) in $\mathbb{C}^n$ equals an affine half-space (/ hyperplane, respectively) in $\mathbb{R}^{2n}$.

On the other hand, each affine half-space (/ hyperplane) in $\mathbb{R}^{2n}$ is induced by a non-constant polynomial of the following form:

$$l_0 = c_{0,1} + \sum_{k=1}^{n} (c_{k,1} \cdot x_{k,1} + c_{k,2} \cdot x_{k,2}),$$

where $c_{k,1}, c_{k,2} \in \mathbb{R}$. Now, with $c_k := c_{k,1} + ic_{k,2} \in \mathbb{C}$, the polynomial l_0 is the real part of the non-constant polynomial $\overline{c_0} + \overline{c_1} \cdot x_1 + \cdots + \overline{c_n} \cdot x_n$ in $\mathbb{C}[x_1, \ldots, x_n]$. ◇

Theorem. (*Separation Theorem for Convex Bodies*)
A convex body in $\mathbb{K}^n$ equals the intersection of all those affine half-spaces in which it is contained.

Proof. See [Gru, Theorem 4.4]. ◇

The following term is adapted from convex optimisation.

Definition. Let $M \subseteq \mathbb{K}^n$. Each convex superset of a M is called a *convex relaxation* of M.

Usually, the term "relaxation" refers to a modelling strategy which replaces a difficult optimisation problem by a related optimisation problem which is, at the best, easier to solve. See, for example, [CT].

Let C be a convex set which is the intersection of affine half-spaces $\mathcal{H}$. Now, for any $\mathcal{H}' \subseteq \mathcal{H}$, the intersection of all affine half-spaces in $\mathcal{H}'$ is a convex relaxation of C. This special case will be important.

2.3.3 Support Functionals

The real parts of two non-constant affine functionals define the same real affine hyperplane if and only if they are equal up to a non-zero real multiple.

A real affine hyperplane defines two affine half-spaces. At least one of them contains 0. The real part of a corresponding affine functional is non-negative on 0. It is uniquely determined up to a non-negative constant. Now, for all $y = (y_1, \ldots, y_n)^t \in \mathbb{K}^n$, we consider the affine functional

$$l^y := 1 - \langle \cdot\,, y \rangle = 1 - (\overline{y_1} \cdot x_1 + \cdots + \overline{y_n} \cdot x_n).$$

Proposition. The affine half-spaces with interior point 0 are represented by the real parts of the affine functionals l^y for $y \neq 0$.

Proof. Let $y_k = y_{k,1} + iy_{k,2}$. We first note that

$$\mathrm{Re}(l^y) = 1 - \sum_{k=1}^{n} (y_{k,1}x_{k,1} + y_{k,2}x_{k,2}) = l^{\imath(y)},$$

that is, $\imath(H_{l^y}) = H_{l^{\imath(y)}}$ and $\imath(P_{l^y}) = P_{l^{\imath(y)}}$. Hence, it suffices to consider the real case. Let l be a non-constant affine functional with the required properties. Its real part is positive on 0, that is, there exists $\lambda > 0$ and $y' \in \mathbb{K}^n$ with $l = \lambda \cdot l^{y'}$. ◇

Let P be a real affine hyperplane. Amongst all points in P, there exists a unique point which is closest to zero. In this respect, we consider the following affine functionals:

Definition. For all $y \in \mathbb{K}^n$, $y \neq 0$, let

$$l_y := 1 - \left\langle \cdot\, , \frac{y}{\|y\|^2} \right\rangle = 1 - \frac{1}{\|y\|^2} \cdot (\overline{y_1} \cdot x_1 + \cdots + \overline{y_n} \cdot x_n)$$

be the *support functional* to y.

We immediately obtain $l_y(0) = 1$ and $l_y(y) = 0$. The distance of P_{l_y} to zero is minimal at y and the linear subspaces $\mathrm{LH}(y)$ and $P_{l_y} - y$, regarded as linear subspaces in $\mathbb{R}^{2n}$, are orthogonal. In this respect, the vector y is called the *support vector* of P_{l_y}.

For all $v, w \in \mathbb{K}^n$, $v, w \neq 0$, the statements $v = {}^{w}/_{\|w\|^2}$ and $w = {}^{v}/_{\|v\|^2}$ are equivalent. It follows that $l_y = l^{y/\|y\|^2}$ and $l^y = l_{y/\|y\|^2}$. Consequently, also the support functionals are suitable as representatives for the affine half-spaces with interior point 0.

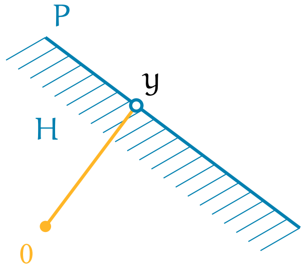


Figure 2.2: The support functional to y.

Figure 2.2 illustrates the real affine hyperplane $P := P_{l_y}$, which is perpendicular to y, and the corresponding affine half-space $H := H_{l_y}$, which is indicated by hashed lines.

Example. Figure 2.3 illustrates a convex set C. The Euclidean unit sphere is denoted by S. The support functional l_y to the boundary vector y induces an affine half-space in which C is contained. In contrast, C is not contained in the affine half-space which is induced by the support functional $l_{y'}$ to the boundary vector y'. Theorem 2.4.7 will make this precise.

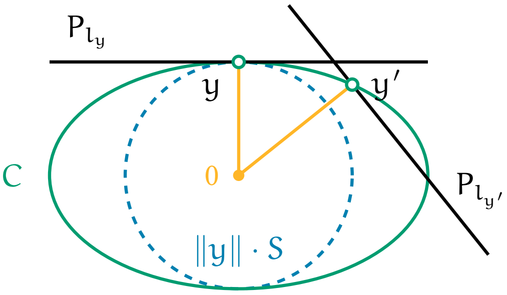


Figure 2.3: Support functionals to boundary vectors.

2.3.4 Witness Half-Spaces, Hyperplanes, and Functionals

Let $y \in \mathbb{K}^n$, $y \neq 0$. The real part of the support functional l_y provides a test whether a given vector $z \in \mathbb{R}^n$ lies in the corresponding affine half-space H_l or not.

Definition. Let C be a convex body with interior point 0. Let H be an affine half-space such that $C \subseteq H$. Then H is called a *witness half-space* for C, the corresponding real affine hyperplane is called a *witness hyperplane* for C, and the corresponding support functional is called a *witness functional* for C. If it is clear from the context, we often just write *witness*.

By Theorem 2.3.2, C can be characterised by its witness half-spaces. They provide a test whether a given vector $z \in \mathbb{K}^n$ is contained in C:

Membership Test

- If there exists a witness functional l for C with $\mathrm{Re}(l(z)) < 0$, then z is not contained in C.
- If $\mathrm{Re}(l(z)) \geqslant 0$ for all witness functionals l of C, then $z \in C$.

Figure 2.4 illustrates the membership test: Let l be a witness functional of C. The real affine hyperplane $P := P_l$ is represented by a blue line segment. Now, the witness functional outlines whether a given point z on the coloured line segment from the origin lies on the "left side" of P ("yes"). If this is not the case, then $z \notin C$ ("no").

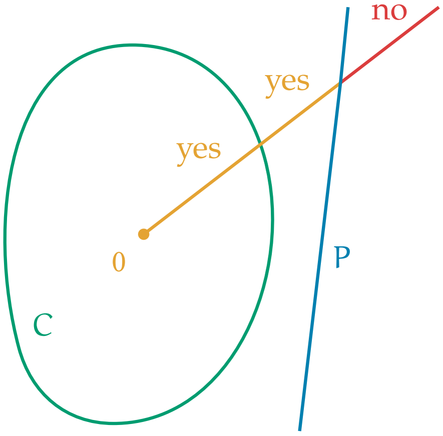


Figure 2.4: Membership test with a witness functional.

In a figurative language, z is a "defendant" which can be "absolved" of "guilt" (that is, being in C) based on the "testimony" of a "witness".

2.3.5 Faces and Extreme Points

Definition. A point z of a convex set $C \subseteq \mathbb{K}^n$ is called an *extreme point* of C, if z is no proper convex combination of points of C. The set of all extreme points of C is denoted by $\operatorname{ext}(C)$.

Let C be a convex body. Due to a finite-dimensional version of the Krein-Milman Theorem, the set $\operatorname{ext}(C)$ equals the smallest subset $S \subseteq C$ with respect to the set inclusion such that $C = \operatorname{co}(S)$, see [Gru, Theorem 5.5]. In particular, $C = \operatorname{co}(\operatorname{ext}(C))$, that is, C is characterised by its extreme points.

Even if C is compact, $\operatorname{ext}(C)$ is not compact in general. An example is the set $E := \{(y_1, y_2, 0) \colon y_1^2 + y_2^2 = 1, y_1 \neq 1\} \cup \{(1, 0, 1), (1, 0, -1)\} \subseteq \mathbb{R}^3$ (since $E = \operatorname{ext}(\operatorname{co}(E))$).

Definition. Let $C \subseteq \mathbb{K}^n$ be a convex set. A non-empty subset $F \subseteq C$ is called a *face* of C, if for all $z \in C$, the following holds: If z is a non-trivial convex combination of $v, w \in C$, then $v, w \in F$. Let F be a face of C. If $F \neq C$, then it is called *proper*. It is called *maximal*, if it is proper and there are no proper faces F' of C with $F \subseteq F'$ and $F \neq F'$. It is called *exposed*, if there exists a non-constant affine functional l such that $F = C \cap P_l$. The *dimension* $\dim(F)$ of F is the dimension of its affine hull.

Extreme points are the faces with dimension zero. A proper face of a convex set C is a closed subset of the boundary of C, see [Roc, Theorems 18.1 and 18.2]. If F, G are faces of C with $F \subsetneq G$ and $F \neq G$, then $\dim(F) < \dim(G)$ due to [Roc, Theorem 18.1]. If C is contained in an affine half-space H_l, and if $C \cap P_l \neq \emptyset$, then $C \cap P_l$ is an exposed face of C. Figure 2.5 shows an extreme point e of a convex set C which is contained in a maximal face M. The face $\{e\}$ is not exposed. Nevertheless, due to [BN, Theorem 4.4], each proper face of C is contained in an exposed face. The previous statements imply that each face is contained in a maximal face of C which is exposed (see also Figure 2.5).

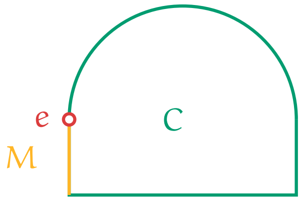


Figure 2.5: Exposed and not exposed faces.

Proposition. Let C be a convex set and let F be a face of C. Then $\mathrm{ext}(F) = \mathrm{ext}(C) \cap F$. If, in addition, F is an exposed face, that is, there exists a real affine hyperplane P such that $F = C \cap P$, then $\mathrm{ext}(F) = \mathrm{ext}(C) \cap P$.

Proof. Both assertions can be easily verified. ◇

The following statement can be found in [Lang, Proposition 6.2.3].

Proposition. If an arbitrary intersection of exposed faces of C is not empty, it is an exposed face.

Proof. Let F_1 and F_2 be induced by support functionals l_1 and l_2. Either $F_1 \cap F_2$ is empty or it is induced by the support functional $1/2(l_1 + l_2)$. In the latter case, $\dim(F_1 \cap F_2) < \min(\dim(F_1), \dim(F_2))$. To show the infinite case, let $\mathcal{F}$ be a system of exposed faces of C such that the intersection of all faces is not empty. The partially ordered set X of all finite intersections of faces in $\mathcal{F}$ (ordered by inverted set inclusion) has the property that every total ordered subset, which is not empty, has a largest element, since the dimensions are decreasing. Following Zorn's Lemma, X contains at least one largest element, that is, the intersection of all faces in $\mathcal{F}$ terminates after finitely many steps. $\diamond$

2.3.6 The Real Polar and the Absolute Polar

Definition. Let $C \subseteq \mathbb{K}^n$. The *real polar* of C is defined by

$$\begin{aligned} C^\circ &:= \{y \in \mathbb{K}^n\colon\ \forall z \in C\colon\ \mathrm{Re}(\langle z, y\rangle) \leqslant 1\} \\ &= \{y \in \mathbb{K}^n\colon\ \forall z \in C\colon\ \mathrm{Re}(l^y(z)) \geqslant 0\} \\ &= \{y \in \mathbb{K}^n \backslash \{0\}\colon C \subseteq H_{l^y}\} \cup \{0\}. \end{aligned}$$

A set $D \subseteq \mathbb{K}^n$ with $C = D^\circ$ is called a *real prepolar* of C.

Some examples can be found in [Lang]. The following common statements can be deduced immediately:

Proposition. Let $C \subseteq \mathbb{K}^n$. Then we have

(i) If $D \subseteq \mathbb{K}^n$ with $C \subseteq D$, then $C^\circ \subseteq D^\circ$.
(ii) The real polar C° is convex and closed.
(iii) If C is a convex body with interior point 0, then C° is also a convex body with interior point 0.
(iv) In the case where $\mathbb{K} = \mathbb{C}$, we have $\imath(C^\circ) = (\imath(C))^\circ$.

Proof. The proofs of (i) and (ii) are straightforward.

To show (iii) we note that besides of 0 the set C° consists of all $y \in \mathbb{K}^n \backslash \{0\}$ such that C lies in the affine half-space H_{l^y}. Now, H_{l^y} equals $H_{l_{\tilde{y}}}$, where $\tilde{y} := \frac{1}{\|y\|^2} \cdot y$. In particular, we have $\|y\| = \frac{1}{\|\tilde{y}\|}$. On the one hand, if there exists $\lambda_1 > 0$ such that $\lambda_1 \cdot \mathcal{B}_{1,\|\cdot\|} \subseteq C$, then $C^\circ \subseteq \frac{1}{\lambda_1} \cdot \mathcal{B}_{1,\|\cdot\|}$. On the other hand, if there exists $\lambda_2 > 0$ such that $C \subseteq \lambda_2 \cdot \mathcal{B}_{1,\|\cdot\|}$, then $\frac{1}{\lambda_2} \cdot \mathcal{B}_{1,\|\cdot\|} \subseteq C^\circ$.

Finally, we show (iv) with Theorem 2.2.5:

$$\imath(C^\circ) = \{y \in \mathbb{R}^{2n}\colon\ \forall z \in \imath(C)\colon l^y(z) \geqslant 0\} = (\imath(C))^\circ.$$

$\diamond$

Hence, the complex case can be traced back to the real case.

Theorem. (*Bipolar Theorem*)
Let $C \subseteq \mathbb{K}^n$, then $(C^\circ)^\circ = \mathrm{cl}(\mathrm{co}(C \cup \{0\}))$.

Proof. See [Wer, Satz VIII.3.9]. ◇

The Bipolar Theorem realises a dual relationship between convex bodies with interior point 0. It is closely related to the Separating Theorem for Convex Bodies Theorem 2.3.2, that is, a closed convex set in $\mathbb{K}^n$ can be described by the intersection of all those affine half-spaces in which it is contained.

Corollary. Let C be a closed convex set with $0 \in C$. A set $D \subseteq \mathbb{K}^n$ is a real prepolar of C if and only if the affine half-spaces H_{l_y}, where $y \in D \backslash \{0\}$, define C. In this case, we have $C^\circ = \mathrm{cl}(\mathrm{co}(D \cup \{0\}))$.

Proof. We have

$$\begin{aligned} D^\circ &= \{y \in \mathbb{K}^n \colon \ \forall z \in D \colon \ \mathrm{Re}(\langle z, y \rangle) \leqslant 1\} \\ &= \{y \in \mathbb{K}^n \colon y \in H_{l_z},\ z \in D \backslash \{0\}. \end{aligned}$$

The last statement is a consequence of the Bipolar Theorem. ◇

Hence, if $C \subseteq \mathbb{K}^n$ has a real prepolar D and H is an affine half-space with $C \subseteq H$, then there exists $y \in \mathrm{cl}(\mathrm{co}(D \cup \{0\}))$ such that $H = H_{l_y}$.

Definition. Let $C \subseteq \mathbb{K}^n$ be a convex set with $0 \in C$. The *absolute polar* of C is defined by

$$C^\bullet := \{y \in \mathbb{K}^n \colon \ \forall z \in C \colon |\langle z, y \rangle| \leqslant 1\}.$$

A subset M of $\mathbb{K}^n$ is called *balanced* in $\mathbb{K}$, if for any $\lambda \in \mathbb{K}$, $|\lambda| = 1$, and $z \in M$, we have $\lambda \cdot z \in M$.

In the real case the real polar and the absolute polar are equal. The notion of the real polar in $\mathbb{C}^n$ can be identified with the notion of the absolute polar in $\mathbb{R}^{2n}$. Also for balanced sets, the real polar and the absolute polar are equal, see [BN, Remark 8.3.2]. In those cases, the term *polar* refers to both the real and the absolute polar.

2.4 Convex Sets and Norms

A subset M of $\mathbb{K}^n$ is called *absorbing*, if $0 \in M$ and if the *Minkowski functional*

$$y \mapsto \inf \left\{ r \in (0, \infty] : y \in r \cdot M \right\}$$

is finite for every $y \in \mathbb{K}^n$.

If $C \subseteq \mathbb{K}^n$ is convex, bounded, balanced and absorbing, then the Minkowski functional is a norm, denoted by $\| \cdot \|^C$, whose unit ball equals the closure of C, see [Con, Proposition 1.14]. Hence, there is a one-to-one correspondence between norms on $\mathbb{K}^n$ and balanced convex bodies C with interior point 0.

Let $\| \cdot \|^C$ be a norm on $\mathbb{K}^n$ with corresponding unit ball C. In this section, we deal with some notions which can be helpful to understand the norm $\| \cdot \|^C$ with the aid of the convex set C or its polar.

2.4.1 Geometric Approach

The following simple observation can help to understand $\| \cdot \|^C$ if the extreme points or the faces of C are known.

Let $\mathcal{C} := \{\mathrm{co}(E) \colon E \subseteq \mathrm{ext}(C)\}$ and let $y \in \mathbb{K}^n$. Then

$$\|y\|^C = \inf \left\{ r \in (0, \infty] : y \in r \cdot B, \text{ where } B \in \mathcal{C} \right\},$$

see also Figure 2.6 (the coloured line segments refer to elements of $\mathcal{C}$).

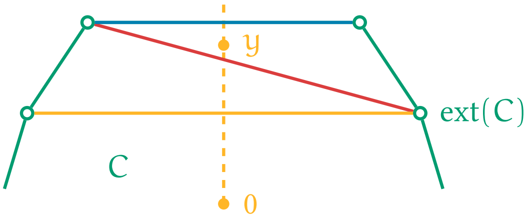


Figure 2.6: Geometric approach to $\| \cdot \|^C$.

2.4.2 The Norm Maximisation Problem

Another approach to $\| \cdot \|^C$ is its maximum on the unit sphere.

Definition. The convex optimisation problem of finding the value

$$\max\{\|z\|^{C} \colon \|z\| = 1\}$$

is called the *norm maximisation problem* for $\| \cdot \|^{C}$.

This optimisation problem will play an important role in the following chapters. It will be also discussed at the end of this section.

2.4.3 Dual Norms and the Polar

Now, we show that the polar of C provides information about $\|\cdot\|^{C}$.

Definition. The *dual norm* $\| \cdot \|^{C,\star}$ of $\| \cdot \|^{C}$ on $\mathbb{K}^n$ is given by

$$\|z\|^{C,\star} = \sup\{|\langle z, y\rangle| \colon y \in C\}.$$

The following statement shows that the dual norm equals the norm corresponding to the polar, see also [BN, Example 8.3.3]:

Proposition. We have $\| \cdot \|^{C,\star} = \| \cdot \|^{C^{\bullet}} = \| \cdot \|^{C^{\circ}} = \sup\{\mathrm{Re}(\langle \,\cdot\, , y\rangle) \colon y \in C\}$.

Proof. Since C is balanced, we obtain $C^{\bullet} = C^{\circ}$, and for all $z \in \mathbb{K}^n$, we have

$$z \in C^{\bullet} \;\Leftrightarrow\; \|z\|^{C,\star} \leqslant 1.$$

◇

Example. The dual norm of the 1-norm is the max norm and the dual norm of the 2-norm is the 2-norm.

2.4.4 Exposed Faces and the Polar

The following statement is a part of Satz 6.2.11 in [Lang].

Lemma. The proper exposed faces of C have the form $C \cap P_{l^{v}}$, where $v \in C^{\circ}$, $\|v\|^{C^{\circ}} = 1$.

Proof. Let F be a proper exposed face of C, then there exists $v \in \mathbb{K}^n$, $v \neq 0$, such that $F = C \cap P_{l^{v}}$. The definition of the real polar yields $v \in C^{\circ}$. Then $1 \geqslant \|v\|^{C^{\circ}} = \sup\{\mathrm{Re}(\langle v, y\rangle) \colon y \in C\}$. Since F is proper, there exists $y_0 \in C$ with $y \in P_{\iota^v}$, that is, $1 = \operatorname{Re}(\langle v, y_0 \rangle)$. Consequently, we obtain $\|v\|^{C^\circ} = 1$.

On the other hand, let $v \in C^\circ$ with $\|v\|^{C^\circ} = 1$. We show that $F := C \cap P_{\iota^v}$ is a proper exposed face of C. By definition of $\|\cdot\|^{C^\circ}$, there exists $y_0 \in C$ with $1 = \|v\|^{C^\circ} = \operatorname{Re}(\langle v, y_0 \rangle)$, that is, $y_0 \in P_{\iota^v}$. Hence, F is not empty. Now, let $z \in F$ be arbitrary. From $z \in P_{\iota^v}$ we obtain $1 = \operatorname{Re}(\langle v, z \rangle)$. Assuming that $\lambda \cdot z \in C$ for $\lambda > 1$, then $\|v\|^{C^\circ} = \sup\{\operatorname{Re}(\langle v, y \rangle) \colon y \in C\} \geqslant \lambda > 1$, which is a contradiction. Hence, z is a boundary point of C. ◇

2.4.5 Dual Faces

Definition. Let F be a face of C. The *dual face* $F^{\vartriangle}$ of F is defined by

$$\begin{aligned} F^{\vartriangle} &:= \{y \in C^\circ \colon\ \forall z \in F \colon\ \operatorname{Re}(\langle z, y \rangle) = 1\} \\ &= \{y \in C^\circ \setminus \{0\} \colon\ \forall z \in F \colon\ \operatorname{Re}(\iota^y(z)) = 0\} \\ &= \{y \in C^\circ \setminus \{0\} \colon F \subseteq P_{\iota^y}\} \\ &= \bigcap_{z \in F} (C^\circ \cap P_{\iota^z}). \end{aligned}$$

In the case where $F = \emptyset$, the dual face is defined by $F^{\vartriangle} := C^\circ$.

As an intersection of exposed faces, the dual face of F is either empty or an exposed face of C° (this follows from Proposition 2.3.5.II and Lemma 2.3.5). We note that also this notion can be traced back to the real case. In [Lang], some properties of dual faces are outlined. At this point, we remind on Propositions 6.2.17 and 6.2.18:

Proposition. Let F and F' be faces of C with $F \subseteq F'$. Then we have

(i) $(F')^{\vartriangle} \subseteq F^{\vartriangle}$.

(ii) F is exposed, if and only if $(F^{\vartriangle})^{\vartriangle} = F$.

(iii) F is proper, if and only if $F^{\vartriangle}$ is a proper face of C°.

(iv) In the case where F contains an exposed extreme point $e \in C$, we have $F = \{e\}$ if and only if $F^{\vartriangle}$ is a maximal face of C°.

Proof. Statement (i) follows immediately from the definition.

To show (ii) we first note that $(F^{\vartriangle})^{\vartriangle}$ is an exposed face and $F \subseteq (F^{\vartriangle})^{\vartriangle}$. If F is exposed, then there exists $v \in C^\circ$ such that $F = C \cap P_{\iota^v}$, that is, for all $y \in C$, we have $1 = \operatorname{Re}(\langle v, y \rangle)$ if and only if $y \in F$. Let

$v' \in (F^{\vartriangle})^{\vartriangle} \subseteq C$. From $v \in F^{\vartriangle}$ we obtain $1 = \mathrm{Re}(\langle v, v' \rangle)$, that is, $v' \in F$.

Now, we show (iii). If F is not proper (that is, $F = C$), then $F^{\vartriangle} = \emptyset$. On the other hand, if F is proper, then F is contained in a maximal face M of C. Statement (ii) yields $M = (M^{\vartriangle})^{\vartriangle}$. This implies $\emptyset \neq M^{\vartriangle} \subseteq F^{\vartriangle}$. Since F contains an extreme point e (which is also an extreme point of C using Proposition 2.3.5.I), we have $F^{\vartriangle} \subseteq \{e\}^{\vartriangle} \neq C^{\circ}$.

Finally, we show (iv). Let $e \in F$ be an exposed extreme point of C. If $F = \{e\}$, then $\{e\}^{\vartriangle}$ is a proper face of C° using (iii). Now, we assume that there exists a maximal face M of C° with $\{e\}^{\vartriangle} \subseteq M$ and $\{e\}^{\vartriangle} \neq M$. In this case, we obtain $\emptyset \neq M^{\vartriangle} \subseteq (\{e\}^{\vartriangle})^{\vartriangle} = \{e\}$ using (ii) and (iii), which implies $M^{\vartriangle} = \{e\}$. Thus, we obtain $M = (M^{\vartriangle})^{\vartriangle} = \{e\}^{\vartriangle}$, which is a contradiction. To show the second implication, we first note that $F^{\vartriangle} \subseteq \{e\}^{\vartriangle}$. If $F^{\vartriangle}$ is maximal, then $F^{\vartriangle} = \{e\}^{\vartriangle}$. Since $\{e\}$ is exposed, there exists $w \in \{e\}^{\vartriangle}$ such that the equation $1 = \mathrm{Re}(\langle v, w \rangle)$ for $v \in C$ has the unique solution $v = e$. But since $w \in F^{\vartriangle}$, any $v \in F$ solves the equation. Hence, $v = e$. ◇

Example. Figure 2.7 shows different relationships between faces and their dual faces, see [Lang, Beispiel 6.2.20]. The Euclidean unit sphere is denoted by S. The proper faces of the convex set C are represented by the maximal faces $\{a\}$, $\{c\}$, $\mathrm{co}(b, c)$, and by the face $\{b\}$, which is not even exposed. The proper faces of C° are represented by the maximal faces $\{d\}$, $\mathrm{co}(e, f)$, and by the face $\{e\}$. Relationships between those faces are summarised in the table which follows below.

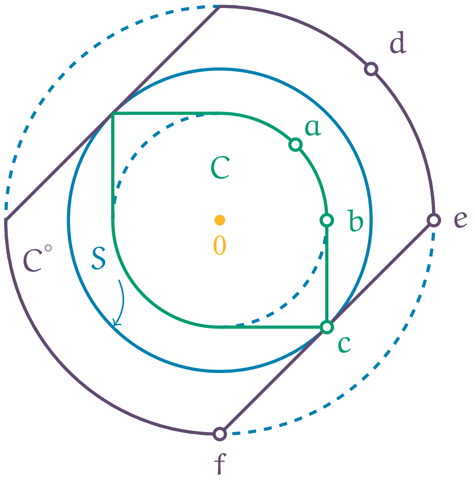


Figure 2.7: A convex set and its real polar.

Face F	$F^{\triangle}$	$(F^{\triangle})^{\triangle}$
$\{a\}$	$\{d\}$	$\{a\}$
$\{b\}$	$\{e\}$	$\operatorname{co}(b,c)$
$\{c\}$	$\operatorname{co}(e,f)$	$\{c\}$
$\operatorname{co}(b,c)$	$\{e\}$	$\operatorname{co}(b,c)$

2.4.6 The Inner and the Outer Radius

The following notions from [Arv] are among the most important in this thesis.

Definition. (i) The *inner radius* $r(C)$ of C is given by the radius of the greatest Euclidean ball with center 0 which is contained in C:

$$r(C) := \sup\{r \geqslant 0 \colon r \cdot \mathcal{B}_{1,\|\cdot\|} \subseteq C\}$$

(ii) The *outer radius* $o(C)$ of C is given by the radius of the smallest Euclidean ball with center 0 in which C is contained:

$$o(C) := \inf\{r \geqslant 0 \colon C \subseteq r \cdot \mathcal{B}_{1,\|\cdot\|}\}$$

From now on, we assume that C has a subset V which satisfies the following conditions:

V0: *(V is normed)*
For all $v \in V$, we have $\|v\| = 1$.

V1: *(V is balanced)*
For all $\lambda \in (\mathbb{K})_1$, we have $\lambda \cdot V \subseteq V$.

V2: *(V separates points)*
For all $z \in \mathbb{K}^n$ with $\langle z, v\rangle = 0$ for all $v \in V$, we have $z = 0$.

V3: *(V generates C)*
$C = \operatorname{cl}(\operatorname{co}(V))$.

In this case, C is contained in the Euclidean unit ball $\mathcal{B}_{1,\|\cdot\|}$.

Theorem. If V is a subset of C which satisfies V0 - V3, then the inner radius of C can be characterised by the following equations:

$$r(C) = \inf\{\|z\| \colon \|z\|^{C} = 1\} = \inf\{\|z\|^{C^{\circ}} \colon \|z\| = 1\},$$

$$o(C^\circ) = \frac{1}{r(C)} = \sup\{\|z\| \colon \|z\|^{C^\circ} = 1\} = \sup\{\|z\|^C \colon \|z\| = 1\},$$
$$\sqrt{2(1 - r(C))} = \sup\{d(z, V) \colon \|z\| = 1\}.$$

Proof. See [Arv, Theorem 3.2]. ◇

The last theorem motivates different ways to determine the inner radius of C, for example, with the polar. In particular, it shows the following:

- The solution of the norm maximisation problem for $\|\cdot\|^C$ is given by $1/r(C)$.
- The maximum of $\|\cdot\|^{C^\circ}$ on $(\mathbb{K}^n)_1$ is given by $r(C)$.
- We have $C \subseteq \mathcal{B}_{1,\|\cdot\|} \subseteq C^\bullet = C^\circ$.
- With Proposition 2.4.3, for any $z \in \mathbb{K}^n$, we have

$$\|z\|^{C^\circ} = \|z\|^{C,\star} \leqslant \|z\| \leqslant \|z\|^C = \|z\|^{C^\circ,\star}.$$

Remark. The theorem requires that C has a subset V with the properties V0 - V3. Otherwise, even $C \subseteq C^\circ$ is not true, see [Lang, Beispiel 6.2.7].

2.4.7 Maximal Vectors

Also here, we assume that C has a subset V which satisfies V0 - V3. The following notion goes back to [Arv].

Definition. A unit vector $y \in \mathbb{K}^n$ is called *maximal* for C or for the norm $\|\cdot\|^C$, if it maximises the distance to V, that is, if

$$d(y, V) = \sup\{d(z, V) \colon \|z\| = 1\}.$$

The following theorem is an adaption of [Sok, Theorem 3.4.6] and [Lang, Satz 6.2.14].

Theorem. Let $y \in (\mathbb{K}^n)_1$. Let $v := r(C) \cdot y$ and $w := 1/r(C) \cdot y$. The following are equivalent:

(a) y is maximal for C.
(b) $d(y, V) = \sqrt{2(1 - r(C))}$.
(c) $d(y, C) = \sup\{d(z, C) \colon \|z\| = 1\} = 1 - r(C)$.
(d) $\|y\|^C = \frac{1}{r(C)}$.
(e) y solves the norm maximisation problem.

(f) v is contained in a maximal face M of C.

(g) w is an exposed extreme point of C°.

In this case, $M = C \cap P_{l_v}$ and $\{w\} = C^{\circ} \cap P_{l_w}$ are dual faces of each other.

Proof. The equivalence of (a) and (b) follows directly from Theorem 2.4.6.

Now, we show (a) $\Leftrightarrow$ (d) $\Leftrightarrow$ (e): According to [Sok, Theorem 3.4.6], y is a maximal vector for C if and only if $\|y\|^C = \frac{1}{r(C)}$. In this case, the last value equals $\sup\{\|z\|^C \colon \|z\| = 1\}$ according to Theorem 2.4.6, that is, y solves the norm maximisation problem.

To show (f) $\Rightarrow$ (a), we first note that the distance of M to zero takes its minimum exactly at v since $\|v\| = r(C)$. By assumption, $d(0, M) = r(C)$. It follows that v lies in M, that is, in the boundary of C. Hence, y is maximal.

To show (a) $\Rightarrow$ (g), we look at the support functional l_w of w. The distance of l_w to zero takes its minimum exactly at w. From $C^{\circ} \subseteq \|w\| \cdot \mathcal{B}_{1,\|\cdot\|}$, it follows that $C^{\circ} \cap P_{l_w} = \{w\}$, that is, w is an exposed extreme point of C°. The equation $\{w\} = M^{\vartriangle}$ follows from Proposition 2.4.5.

Now, we show (g) $\Rightarrow$ (f). Using Proposition 2.4.5, $\{w\}^{\vartriangle}$ is a maximal face of C. Since $\|w\| = o(C^{\circ})$, we obtain $v = {}^{1}\!/\!{}_{\|w\|^2} \cdot w$, and $\{w\}^{\vartriangle} = \{z \in C \colon \operatorname{Re}(\langle z, w \rangle) = 1\} = C \cap P_{l_v}$. From $v \in \{w\}^{\vartriangle} =: M$ and $\|v\| = r(C)$ we obtain $d(0, M) = r(C)$.

Now, also the equivalence of (b) and (c) is clear. ◇

Hence, the norm maximisation problem can be solved by maximal vectors and their maximal faces. In addition, it can be solved by extreme points of C° with maximal length.

In the case of the last theorem, M comes closest to zero amongst all faces of C and w has the largest distance to zero amongst all extreme points of C°. The following table serves as an overview:

	$\|\cdot\|^C$	$\|\cdot\|$	$\|\cdot\|^{C^{\circ}}$
v	1	$r(C)$	$r(C)^2$
y	$1/r(C)$	1	$r(C)$
w	$1/r(C)^2$	$1/r(C)$	1

Example. Figure 2.8 shows a maximal vector y for a convex set C, its corresponding maximal face M and its corresponding extreme point w of the polar C°. Let S denote the Euclidean unit sphere.

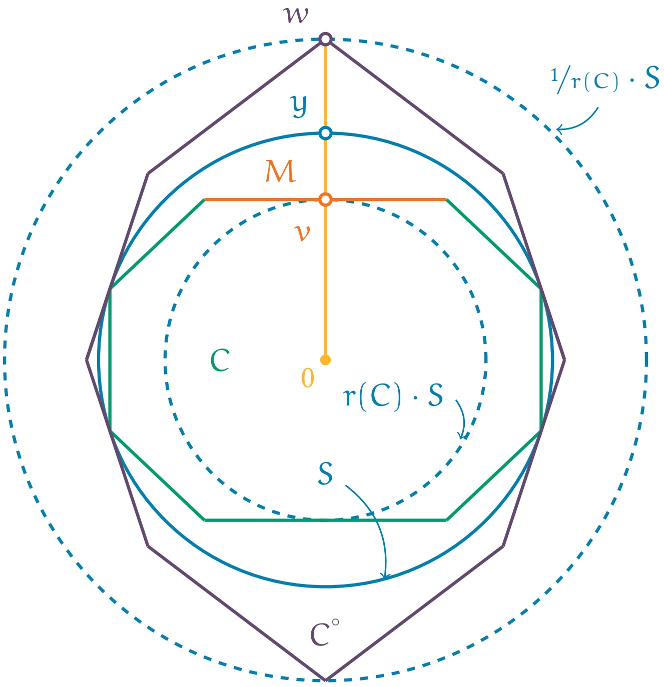


Figure 2.8: A maximal vector.

Remark. Let $r(C) := r$, let y be a maximal vector for C and let $z \in V$ with $d(y, V) = d(y, z)$. Figure 2.9 illustrates the equation $d(y, V) = \sqrt{2(1-r)}$.

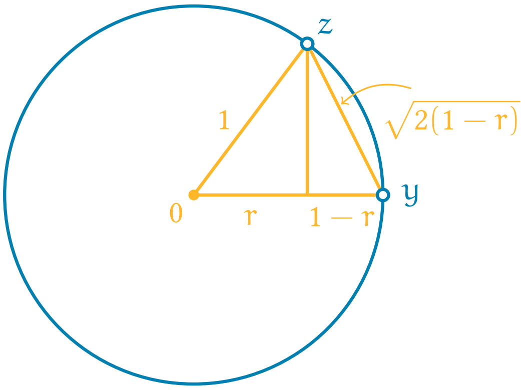


Figure 2.9: Maximal vectors and their distance to V.

2.5 Sums of Squares and Theta Bodies

In this section, we introduce the concept of theta bodies according to [BPT]. Given a convex set with the property that the extreme points or a larger subset is a real affine variety, the theta bodies are a chain of convex relaxations.

The main idea is that the affine functionals which define a theta body can be handled from an algebraic perspective. In particular, they have to be written as a sum of squares in the coordinate ring corresponding to the underlying variety. Indeed, in the case of real affine spaces, the variety lies on one side of the affine half space, since a sum of squares is a polynomial with non-negative values. According to this observation, the concept of theta bodies seems to work only in real affine spaces. However, we present a way to use it also in complex settings by introducing complex theta bodies.

Basics and notion can be found in [BCR] and in [BPT].

2.5.1 Sums of Squares and Cones

Let $I \subseteq \mathbb{R}[x_1, \ldots, x_n] =: \mathbb{R}[\vec{x}]$ be an ideal.

Definition. Let $k \in \mathbb{N}_0$.

(i) A polynomial $s \in \mathbb{R}[\vec{x}]$ is called a k-*sum of squares* (k-sos), if there exist $h_1, \ldots, h_s \in \mathbb{R}[\vec{x}]$, where the degrees of $h_1, \ldots, h_s$ each do not exceed k, such that s has the form

$$s = h_1^2 + \cdots + h_s^2.$$

It is called a *proper* k-*sum of squares*, if it is 0-sos or k-sos, but not $(k-1)$-sos.

(ii) A polynomial $f \in \mathbb{R}[\vec{x}]$ is called a k-*sum of squares modulo* I (k-sos-mod I), if there exists a k-sum of squares $s \in \mathbb{R}[\vec{x}]$ and $h \in I$, such that f has the form

$$f = s + h.$$

A polynomial which is a k-sum of squares (modulo I) is also called a *sum of squares* (*modulo* I, respectively).

According to Subsection 1.1.3, let $\mathbb{R}[\vec{x}]_k$ denote the polynomials whose degrees do not exceed k. Let Σ denote the set of all sum of squares, and let Σ_{2k} denote the set of all k-sum of squares in $\mathbb{R}[\vec{x}]$. If we consider the leading term of a sum of squares, then it is obvious that $\Sigma_{2k} = \Sigma \cap \mathbb{R}[\vec{x}]_{2k}$.

Definition. Let R be a commutative ring with 1. A subset $P \subseteq R$ is called a *cone*, if P satisfies the following conditions:

(i) For all $r, s \in P$, we have $r + s \in P$ and $r \cdot s \in P$.

(ii) For all $r \in R$, we have $r^2 \in P$.

A cone P is called *proper*, if $-1 \notin P$.

Hence, Σ is a proper cone in $\mathbb{R}[\vec{x}]$, and $\Sigma/I = \{f + I \colon f \in \Sigma\}$ is a cone in $\mathbb{R}[\vec{x}]/I$.

In general, an affine functional is not a sum of squares, but it can be a sum of squares modulo an ideal. This special case will be interesting for us below.

2.5.2 Positivstellenmengen

Definition. The *Positivstellenmenge* of a polynomial $f \in \mathbb{R}[\vec{x}]$ or a subset $M \subseteq \mathbb{R}[\vec{x}]$ is denoted by

$$\begin{aligned} \mathcal{W}(f) &:= \{x \in \mathbb{R}^n \colon f(x) \geqslant 0\} \text{ and} \\ \mathcal{W}(M) &:= \{x \in \mathbb{R}^n \colon g(x) \geqslant 0 \text{ for all } g \in M\}, \text{ respectively.} \end{aligned}$$

Moreover, f is called *non-negative* on a subset $S \subseteq \mathbb{R}^n$, if $f(x) \geqslant 0$ for all $x \in S$, that is, if $S \subseteq \mathcal{W}(f)$.

The real numbers are a special case of an ordered field. This property guarantees that $\mathcal{W}(M) \cup \mathcal{W}(-M) = \mathbb{R}^n$. Hence, for example, the Positivstellenmenge of an affine functional is an affine half-space. Even more important for our applications is the property that squares, that is, polynomials of the form f^2, are non-negative on $\mathbb{R}^n$. Consequently, sums of squares are non-negative on $\mathbb{R}^n$.

Let $I \subseteq \mathbb{R}[\vec{x}]$ be an ideal. Then $\mathcal{Z}_{\mathbb{R}}(I) \subseteq \mathcal{W}(I)$. This observation will be useful below.

Remark. Given a set $A \subseteq \mathbb{R}^n$, we may ask for the cone of all polynomials which are non-negative on A. In particular, we may ask whether this cone contains polynomials which are not equal to a sum of squares. An answer is given by the *Positivstellensatz*, see [BCR, Corollary 4.4.3]. For $M = \mathbb{R}^n$, this question is known as *Hilbert's* 17th *problem*, see [BCR, Theorem 6.1.1]. In particular, Hilbert showed the existence of a real polynomial in two variables which is non-negative on $\mathbb{R}^2$ without being a sum of squares, see [Hil]. The Real Nullstellensatz Theorem 2.1.3 is a corollary of the Positivstellensatz. Both theorems, their proofs and other versions of the Positivstellensatz are also presented in the Master's thesis [Lang].

2.5.3 Theta Bodies

From now on, let $I \subseteq \mathbb{R}[\vec{x}]$ be an ideal.

A theta body of I is defined as the intersection of the Positivstellenmengen which come from polynomials which are both an affine functional and a sum of squares modulo I, see [BPT].

More details on the basic idea and intuition of theta bodies can be found in [Sto, Appendix B]. Some other viewpoints on theta bodies are outlined and summarised in [BPT]: Theta bodies as so-called semialgebraic sets, as so-called projected dual cones, as so-called projected spectrahedra, theta bodies and moment matrices, and more. Some of these viewpoints are presented in detail in the Master's thesis [Lang]. Here, we only deal with the aspects that are required specifically for this thesis.

Let $\mathcal{C}_k := \mathcal{C}_k(I)$ be the set of all affine functionals in $\mathbb{R}[\vec{x}]$ which are k-sos-mod I. The k^{th} theta body $\mathcal{T}_k$ is defined by the intersection of $\mathbb{R}^n$ with all affine half-spaces which come from non-constant polynomials in $\mathcal{C}_k$:

Definition. Let $k \in \mathbb{N}$. The k^{th} *theta body* of I is the set

$$\mathcal{T}_k := \mathcal{T}_k(I) := \{x \in \mathbb{R}^n : l(x) \geqslant 0 \text{ for all } l \in \mathcal{C}_k\}.$$

The number k denotes the *degree* of $\mathcal{T}_k$.

A theta body is a closed and convex superset of the real algebraic variety $V := \mathcal{Z}_{\mathbb{R}}(I)$. If a polynomial is k-sos-mod I, so it is also

$(k+1)$ -sos-mod I. Thus, the theta bodies are a descending chain of relaxations of the closed convex set $C := \mathrm{cl}(\mathrm{co}(V))$:

$$\mathcal{T}_1 \supseteq \mathcal{T}_2 \supseteq \cdots \supseteq \mathcal{T}_k \supseteq \mathcal{T}_{k+1} \supseteq \cdots \supseteq C \supseteq V.$$

In this respect, we say that the theta bodies *approximate* C. However, we will deal with the question of how "close" the theta bodies come to C. The chain is illustrated in Figure 2.10.

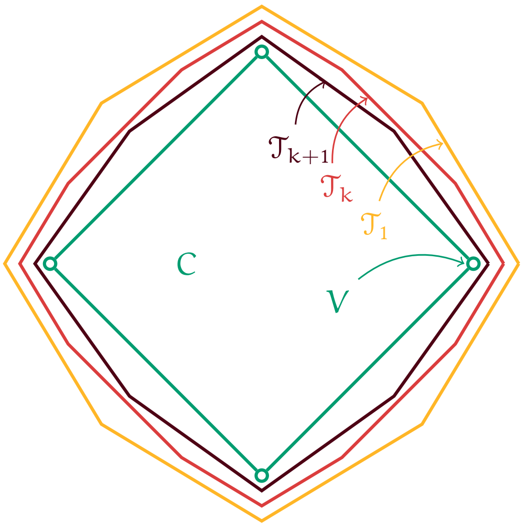


Figure 2.10: Approximation by theta bodies.

Remark. We recall that the Real Nullstellensatz Theorem 2.1.3 says that vanishing ideals correspond to real ideals. It also says that the real radical $\sqrt[\mathbb{R}]{I}$ is the largest ideal amongst all ideals defining $\mathcal{Z}_{\mathbb{R}}(I)$, so we have $\mathcal{T}_k(\sqrt[\mathbb{R}]{I}) \subseteq \mathcal{T}_k(I)$. In an applied context, it may therefore be tempting to replace I with its real radical to yield a "better" approximation. In this respect, if I is real, then $\mathcal{T}_k(I)$ can also be referred to as the k^{th} *theta body* of V. In practice, however, the real radical can be quite "large", which makes it difficult to deal with. Therefore, if the underlying ideal is specified, then the notion k^{th} *theta body* of V is also possible.

Example. By definition, a k-sum of squares modulo I is also a $k+1$-sum of squares modulo I. The inverse statement does not hold in general. However, to get a sense for the theta body chain, we make the following observation. Let $f \in \mathbb{R}[\vec{x}]$ be a k-sum of squares modulo I, that is, there exists a k-sum of squares $s = s_1^2 + \cdots + s_t^2$ and a polynomial $h \in I$ such that $l = s + h$. In this example, we show how to write f as a proper (!) $k+1$-sum of squares $\widetilde{s}$ modulo I. To do this, we assume that there exits $h_0 \in I$ with $\deg(h_0) \leqslant k+1$. Now, let $h_1, \dots, h_t \in I$ such that the maximum of the degrees of $h_1, \dots, h_t$ equals $k+1$ (this is possible due to the assumption). Then f can be written as $f = \widetilde{s} + \widetilde{h}$ with

$$\begin{aligned} \widetilde{s} &:= (s_1 + h_1)^2 + \dots + (s_t + h_t)^2 \text{ and} \\ \widetilde{h} &:= h - 2(s_1 h_1 + \dots + s_t h_t) - (h_1^2 + \dots + h_t^2). \end{aligned}$$

One can easily see that $\widetilde{s}$ is a proper $k+1$-sum of squares and $\widetilde{h} \in I$. For instance, using a polynomial $u \in I$ with $\deg(u) = k+1$, one obtains $f = (s + u^2) + (h - u^2)$. Nevertheless, the more complicated question is how to find a polynomial which is a $k+1$-sum of squares modulo I but no k-sum of squares modulo I.

2.5.4 A Real Prepolar of a Theta Body

For any $y \in \mathbb{R}^n$, we recall that $l^y = 1 - \langle \cdot, y \rangle$, see Subsection 2.3.3. Now, let $k \in \mathbb{N}$. We consider the set

$$\mathcal{D}_k := \mathcal{D}_k(I) := \{y \in \mathbb{R}^n : l^y \text{ is } k\text{-sos-mod}\, I\},$$

which is convex and contains 0. In the case where $0 \in \mathcal{T}_k$, each affine half-space, which contains $\mathcal{T}_k$, can be represented by an affine functional l^y, where $y \in \mathbb{R}^n$ with $y \neq 0$, see Proposition 2.3.3, and we have

$$\mathcal{C}_k = \{\lambda \cdot l^y : y \in \mathcal{D}_k, \lambda \geqslant 0\}.$$

In this case, we immediately see that $\mathcal{D}_k$ is a real prepolar of $\mathcal{T}_k$:

Proposition. If $0 \in \mathcal{T}_k$, then $\mathcal{T}_k = (\mathcal{D}_k)^\circ$ and $(\mathcal{T}_k)^\circ = \mathrm{cl}(\mathcal{D}_k)$.

Proof. The first assertion follows directly from Corollary 2.3.6. The second assertion holds with the Bipolar Theorem Theorem 2.3.6. ◇

This observation will be useful in Chapter 6.

2.5.5 Convergence of Theta Bodies

Definition. The *theta bodies of* I *converge*, if

$$\bigcap_{k=1}^{\infty} \mathcal{T}_k = \mathrm{cl}(\mathrm{co}(\mathcal{Z}_{\mathbb{R}}(I))).$$

The k^{th} theta body is called *exact*, if $\mathcal{T}_k = \mathrm{cl}(\mathrm{co}(\mathcal{Z}_{\mathbb{R}}(I)))$.

The following important theorem is a corollary of the Theorem of Schmüdgen, see [Sch].

Theorem. If $\mathcal{Z}_{\mathbb{R}}(I)$ is compact, then we have

$$\bigcap_{k=1}^{\infty} \mathcal{T}_k = \mathrm{co}(\mathcal{Z}_{\mathbb{R}}(I)).$$

Proof. See [BPT, Theorem 7.32]. ◇

Remark. In [Lang], this theorem, the Theorem of Schmüdgen and their proofs are presented in detail. In particular, the idea was that this might give some clues to understand the theta bodies and their convergence.

2.5.6 Theta Bodies provide Witnesses

Let $I \subseteq \mathbb{R}[\vec{x}]$ be an ideal such that $\mathcal{Z}_{\mathbb{R}}(I)$ is compact and such that 0 is an interior point of $C := \mathrm{cl}(\mathrm{co}(\mathcal{Z}_{\mathbb{R}}(I)))$. For each $k \in \mathbb{N}$, every polynomial in $\mathcal{D}_k$ is a witness for C according to Subsection 2.3.4. Now, since the theta bodies of I converge, we can test whether a given vector $z \in \mathbb{R}^n$ lies in C (see also Figure 2.4):

Membership test

- If there exists $k \in \mathbb{N}$ and $l \in \mathcal{D}_k$ with $l(z) < 0$, then z is not contained in C.
- If $l(z) \geqslant 0$ for all $k \in \mathbb{N}$ and for all $l \in \mathcal{D}_k$, then $z \in C$.

Of course, in general, we may expect to know only finitely many witnesses, which is not sufficient to show $z \in C$. However, the witnesses which are known could serve as a measure for the "closeness" of z to C.

2.5.7 The Symmetry Group of a Theta Body

Now, we deal with the symmetry group of a theta body. Our observations will be useful in Section 6.1.

Proposition. Let $V \subseteq \mathbb{R}^n$ be a real affine variety. Let $I := \mathcal{I}_{\mathbb{R}}(V) \subseteq \mathbb{R}[\vec{x}]$ be the vanishing ideal of V. Then we have

$$\mathrm{Sym}_{\mathbb{R}^n}(V) \subseteq \mathrm{Sym}_{\mathbb{R}^n}(\mathcal{T}_k(I))$$

for all $k \in \mathbb{N}$.

Proof. Let $A \in \mathcal{M}_n(\mathbb{R})$ be an invertible matrix with $A(V) = V$ (that is, $A \in \mathrm{Sym}_{\mathbb{R}^n}(V)$).

Preliminary Statement: For all $f \in \mathbb{R}[\vec{x}]$, we have $\deg(f) = \deg(f \circ A)$.
Proof: The assertion holds for terms. This can be seen as follows: Let $p := x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}_0$. For each variable x_t, $t \in \{1, \ldots, n\}$, let y_t denote a term in $(A(x_1, \ldots, x_n))_t$ whose degree is maximal. The part of $y_1^{\alpha_1} \cdot \ldots \cdot y_n^{\alpha_n}$ does not vanish in $p \circ A$. Since the assertion holds for terms, it also holds for arbitrary polynomials.

Statement 1: Let $l \in \mathbb{R}[\vec{x}]$. We show that the following are equivalent:

(a) l is an affine functional and k-sos-mod I.
(b) $l \circ A$ is an affine functional and k-sos-mod I.

Proof: Let l be an affine functional which is k-sos-mod I. There exist polynomials $h_1, \ldots, h_s \in \mathbb{R}[\vec{x}]_k$ and there exists $h \in I$ with $l = \sum_{t=1}^{s} h_t^2 + h$. We obtain

$$l \circ A = \sum_{t=1}^{s} (h_t \circ A)^2 + h \circ A.$$

According to the preliminary statement, the degree of $h_t \circ A$ equals the degree of h_t for all $t \in \{1, \ldots, s\}$. According to Proposition 2.1.8, we obtain $h \circ A \in I$. Thus, $l \circ A$ is also an affine functional and k-sos-mod I. The equivalence holds since V is also invariant under A^{-1}.

Statement 2: We have $\mathcal{T}_k(I) = A(\mathcal{T}_k(I))$.
Proof: From $x \in \mathcal{T}_k(I)$ we obtain $l(A(x)) = (l \circ A)(x) \geqslant 0$ for each polynomial l which is an affine functional and k-sos-mod I, that is, $A(x) \in \mathcal{T}_k(I)$. ◇

Proposition. Let $V_0 \subseteq \mathbb{R}^n$ be a real affine variety, let $V := V_0 \cap (\mathbb{R}^n)_1 = \{v \in V_0 \colon \|v\| = 1\}$, and let $C := \mathrm{co}(V)$. Let $I := \mathcal{I}_{\mathbb{R}}(V_0) \subseteq \mathbb{R}[\vec{x}]$ be the vanishing ideal of V_0. With $u := x_1^2 + \cdots + x_n^2 - 1 \in \mathbb{R}[\vec{x}]$, we first have $V = \mathcal{Z}_{\mathbb{R}}(J) = \mathrm{ext}(C)$, where $J := \mathrm{Id}(I, u)$. Moreover, if I is a homogeneous ideal, then we have

$$\mathrm{Sym}_{\mathbb{R}^n}(V) \cap \mathcal{U}_n(\mathbb{R}) = \mathrm{Sym}_{\mathbb{R}^n}(C) \cap \mathcal{U}_n(\mathbb{R}) \subseteq \mathrm{Sym}_{\mathbb{R}^n}(\mathcal{T}_k(J))$$

for all $k \in \mathbb{N}$.

Proof. Let $A \in \mathcal{M}_n(\mathbb{R})$ be an orthogonal matrix with $A(V_0) = V_0$ (that is, $A \in \mathrm{Sym}_{\mathbb{R}^n}(V_0) \cap \mathcal{U}_n(\mathbb{R})$).

Statement 1: For all $l \in \mathbb{R}[\vec{x}]$, the following are equivalent:

(a) l is an affine functional and k-sos-mod J.

(b) $l \circ A$ is an affine functional and k-sos-mod J.

Proof: Let l be an affine functional which is k-sos-mod J. There exist polynomials $h_1, \ldots, h_s \in \mathbb{R}[\vec{x}]_k$ and there exist $h \in I$ and $g \in \mathbb{R}[\vec{x}]$ with $l = \sum_{t=1}^{s} h_t^2 + h + g \cdot u$. We obtain

$$l \circ A = \sum_{t=1}^{s} (h_t \circ A)^2 + h \circ A + (g \circ A) \cdot (u \circ A).$$

Using the preliminary statement of the proof of the last proposition, the degree of $h_t \circ A$ equals the degree of h_t for all $t \in \{1, \ldots, s\}$. According to Proposition 2.1.8, we have $h \circ A \in I$. Since A is an orthogonal matrix, we have $u \circ A = u$, which implies $h \circ A + (g \circ A) \cdot (u \circ A) \in J$. Thus, $l \circ A$ is also an affine functional and k-sos-mod J.

Statement 2: We have $\mathcal{T}_k(J) = A(\mathcal{T}_k(J))$.

Proof: If $x \in \mathcal{T}_k(J)$, then we have $l(A(x)) = (l \circ A)(x) \geqslant 0$ for each polynomial l which is an affine functional and k-sos-mod J, that is, $A(x) \in \mathcal{T}_k(J)$.

Statement 3: We have $\mathrm{ext}(C) = V$.

Proof: Since C is the convex hull of V, we have $\mathrm{ext}(C) \subseteq V$. On the other hand, since the Euclidean unit ball is strictly convex, each point in V is an extreme point of C.

Statement 4: If I is homogeneous, then we have $\mathrm{Sym}_{\mathbb{R}^n}(C) \cap \mathcal{U}_n(\mathbb{R}) \subseteq \mathrm{Sym}_{\mathbb{R}^n}(\mathcal{T}_k(J))$.

Proof: For all $v \in \mathbb{R}^n$, $v \neq 0$, we have $v \in V_0$, if and only if $1/\|v\| \cdot v \in V_0$. Hence, we have $\mathrm{Sym}_{\mathbb{R}^n}(V_0 \cap (\mathbb{R}^n)_1) \cap \mathcal{U}_n(\mathbb{R}) = \mathrm{Sym}_{\mathbb{R}^n}(V_0) \cap \mathcal{U}_n(\mathbb{R})$. With statement 3, we have $\mathrm{Sym}_{\mathbb{R}^n}(V) \cap \mathcal{U}_n(\mathbb{R}) = \mathrm{Sym}_{\mathbb{R}^n}(C) \cap \mathcal{U}_n(\mathbb{R})$. With statement 2, we have $\mathrm{Sym}_{\mathbb{R}^n}(V_0) \cap \mathcal{U}_n(\mathbb{R}) \subseteq \mathrm{Sym}_{\mathbb{R}^n}(\mathcal{T}_k(J))$. ◇

2.5.8 Complex Theta Bodies

Basically, the concept of theta bodies relies on some special properties of the real numbers, mainly, that each square is a positive number. In Section 2.3, however, we outlined that convex sets are invariant under decomplexification and in Section 2.2 we have shown that a convex affine variety can be expressed as a real affine variety. These observations can be used to apply the concept of theta bodies also to complex affine spaces. Here, we propose one notion. However, at this point, we have not excluded that there exist alternative notions.

Definition. Let $I \subseteq \mathbb{R}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}]$ be an ideal. The k^{th} *complex theta body* of I is the set

$$\begin{aligned} \mathcal{T}_k^{\mathbb{C}}(I) &:= \imath^{-1}\left(\mathcal{T}_k(I)\right) \\ &= \{x \in \mathbb{C}^n \colon l(\imath(x)) \geqslant 0 \text{ for all } l \in \mathcal{C}_k(I)\} \subseteq \mathbb{C}^n. \end{aligned}$$

The number k denotes the *degree* of $\mathcal{T}_k^{\mathbb{C}}(I)$.

Chapter 3

THE PROJECTIVE TENSOR NORM

The aim of this chapter is to show that the concept of theta bodies can be applied to the unit ball of the projective tensor norm in finite-dimensional tensor products. In the following chapters, we investigate the theta bodies and the underlying ideal.

In Section 3.1 we briefly introduce the basic terminology on tensor products and the projective norm.

Section 3.3 deals with the geometry of the unit ball of the projective norm.

In Section 3.4 and in Section 3.5 we show that the extreme points of the projective unit ball, the unit product vectors, can be expressed as a real algebraic variety.

In Section 3.6 we outline two applications of the projective norm in quantum entanglement and in signal processing. In this context, we discuss the advantages of an application of the theta body method to the unit ball of the projective norm.

3.1 Tensor Products and Cross Norms

In this section we briefly introduce tensor products and some cross norms on tensor products. Details can be found in [Ryan] or [Ta1].

3.1.1 Properties of the Tensor Product

Let X and Y be vector spaces over $\mathbb{K}$. Let $B(X, Y)$ denote the vector space of all bilinear maps from $X \times Y$ to $\mathbb{K}$.

Definition. For each $x \in X$ and $y \in Y$, let

$$\begin{aligned} x \otimes y : \ B(X, Y) &\to \mathbb{K}, \\ b &\mapsto b(x, y), \end{aligned}$$

which lies in $B(X, Y)^\star$. It is called a *product vector* or an *elementary tensor*. The linear hull $X \otimes Y$ of all elementary tensors in $B(X, Y)^\star$ is called the *tensor product* of X and Y. Elements of $X \otimes Y$ are called *tensors*. The vector spaces X and Y are called *tensor factors* of $X \otimes Y$.

The tensor product has the following properties, see [Ryan]:

Proposition. Let $x, x_1, x_2 \in X$ and $y, y_1, y_2 \in Y$ with $x_1 \neq 0 \neq x_2$, $y_1 \neq 0 \neq y_2$.

(i) We have $x \otimes y = 0$, if and only if $x = 0$ or $y = 0$.

(ii) Let $\mu \in \mathbb{K}$. We have

$$\begin{aligned} (x_1 + x_2) \otimes y &= x_1 \otimes y + x_2 \otimes y, \\ x \otimes (y_1 + y_2) &= x \otimes y_1 + x \otimes y_2, \\ \mu(x \otimes y) &= (\mu x) \otimes y = x \otimes (\mu y). \end{aligned}$$

(iii) We have $x_1 \otimes y_1 = x_2 \otimes y_2$, if and only if there exists $\lambda \neq 0$ such that $x_2 = \lambda x_1$ and $y_1 = \lambda y_2$.

(iv) If $\{e_k : k \in K\}$ is a basis of X and $\{f_l : l \in L\}$ is a basis of Y, then

$$\{e_k \otimes f_l : k \in K, l \in L\}$$

is a basis of $X \otimes Y$.

(v) Let W be a vector space over $\mathbb{K}$ with the following property: There exists a bilinear function $f : X \times Y \to W$ and for each vector space Z over $\mathbb{K}$ and for each bilinear function $h : X \times Y \to Z$, there exists a uniquely defined linear map $g : W \to Z$ with $h = g \circ f$. Then W is isomorphic to $X \otimes Y$.

The last property is called the *universal property of the tensor product*. It is illustrated in Figure 3.1.

$$\begin{tikzcd}
X \times Y \arrow[d, "f"'] \arrow[dr, "h"] & \\
W \arrow[r, "g"'] & Z
\end{tikzcd}$$

Figure 3.1: The universal property of the tensor product.

Proof. See [Ryan, Propositions 1.1, 1.2 and 1.4]. ◇

The tensor product of two vector spaces is called a *bipartite tensor product*. In an analogous manner, the tensor product of r vector spaces, $r \geqslant 2$, can be defined. It is called a *multipartite tensor product*, see [Sok, Definition 1.1.2]. The properties of the last proposition hold in an analogous manner. In addition, the tensor product is associative: Let Z be a vector space over $\mathbb{K}$, then $(X \otimes Y) \otimes Z$ is isomorphic to $X \otimes (Y \otimes Z)$, see [Sok, Proposition 1.1.12].

If $X = \mathbb{K}^m$ and $Y = \mathbb{K}^n$, then Proposition 3.1.1 (iv) shows that a basis of the tensor product $X \otimes Y$ is given by the maps

$$\begin{aligned} e_k \otimes e_l \,:\, & B(X,Y) \to \mathbb{K}, \\ & b \mapsto b(e_k, e_l) =: b_{k,l}, \end{aligned}$$

where $k \in \{1, \dots, m\}$, $l \in \{1, \dots, n\}$. From (ii), it follows that $X \otimes Y$ and $\mathcal{M}_{m,n}(\mathbb{K})$ are isomorphic, by identifying the product vector $x \otimes y$ with $x \cdot y^t$, for all $x \in X$ and $y \in Y$. Thus, non-zero product vectors relate to matrices of rank 1. We note that the definition of a tensor product is not unique in the literature. For instance, if X and Y are finite-dimensional, then $X \otimes Y$ can also be defined as $B(X,Y)$. This is common in differential geometry (see [Lee]).

3.1.2 Product Vectors

From now on, we consider finite-dimensional tensor products of Euclidean vector spaces. In this respect, let $V := \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ for $r, n_1, \dots, n_r \geqslant 2$.

The set of all product vectors is denoted by

$$\mathcal{P}_V := \{v_1 \otimes \cdots \otimes v_r \colon v_t \in \mathbb{K}^{n_t}, t \in \{1, \ldots, r\}\}.$$

Elements of the set

$$\mathcal{E}_V := \{v_1 \otimes \cdots \otimes v_r \colon v_t \in (\mathbb{K}^{n_t})_1, t \in \{1, \ldots, r\}\}$$

are referred to as *unit product vectors* (we recall that the Euclidean unit sphere in $\mathbb{K}^n$ is denoted by $(\mathbb{K}^n)_1$, see the index of notation).

Each tensor $v \in V$ can be written as a linear combination of product vectors. The *rank* of v is the smallest number $k \in \mathbb{N}_0$ such that v is a linear combination of k product vectors (which is zero, if and only if $v = 0$). In particular, $\mathcal{P}_V$ equals the set of all tensors with rank zero or rank one.

3.1.3 Cross Norms

Definition. A norm $\|\cdot\| : V \to \mathbb{R}_0^+$ is called a *cross norm* on V, if the norm of each unit product vector equals 1.

If $\|\cdot\|$ is a cross norm on V, then we have $\|v_1 \otimes \cdots \otimes v_r\| = \|v_1\| \cdot \ldots \cdot \|v_r\|$ for all $v_t \in \mathbb{K}^{n_t}$, $1 \leqslant t \leqslant r$. In particular, the norm of a product vector is 1 if and only if it is a unit product vector. Thus, one may immediately obtain that for all $v \in \mathbb{K}^{n_2} \otimes \cdots \otimes \mathbb{K}^{n_r}$, the function $\mathbb{K}^{n_1} \to V$, $x \mapsto x \otimes v$ is continuous. This is an indication that cross norms can be considered as "natural" norms on tensor products.

3.1.4 The Projective Norm

The *projective (tensor) norm* $\|\cdot\|_\pi$ on V is defined by

$$\|z\|_\pi = \inf \left\{ \sum_{k=1}^{s} \|v_1^k\| \cdot \ldots \cdot \|v_r^k\| \, : z = \sum_{k=1}^{s} v_1^k \otimes \cdots \otimes v_r^k \right\}$$

for $z \in V$. It is called *pi-norm* or *nuclear norm*. The pair $(V, \|\cdot\|_\pi)$ is called the *projective tensor product*.

The projective norm is a norm, see [Ryan, Proposition 2.1]. Indeed, it is the largest cross norm on V, since for any cross norm $\|\cdot\|$ on V, we obtain immediately the inequality

$$\left\| \sum_{k=1}^{s} v_1^k \otimes \cdots \otimes v_r^k \right\| \leqslant \sum_{k=1}^{s} \|v_1^k\| \cdot \ldots \cdot \|v_r^k\|,$$

where $v_t^k \in \mathbb{K}^{n_t}$, $t \in \{1, \dots, r\}$. Its unit ball $\mathcal{B}_{1,\pi}$, the *projective unit ball*, is given by the convex hull of the unit product vectors, which are its extreme points, that is, $\mathcal{B}_{1,\pi} = \mathrm{co}(\mathcal{E}_V)$. This follows from [Ryan, Proposition 2.2]. In this respect, the projective norm can be expressed geometrically, see Example 2.4: Let $z \in V$. Then

$$\begin{aligned} \|z\|_\pi &= \inf \left\{ \sum_{k=1}^{s} |\lambda_k| : z = \sum_{k=1}^{s} \lambda_k \cdot z_k, \text{ where } z_k \in \mathcal{E}_V \right\} \\ &= \inf \Bigg\{ \lambda : z = \lambda \cdot \sum_{k=1}^{s} \lambda_k \cdot z_k, \text{ where} \\ &\qquad \lambda, \lambda_k \geqslant 0, \sum_{k=1}^{s} \lambda_k = 1, \text{ and } z_k \in \mathcal{E}_V \Bigg\} \\ &= \inf \left\{ \lambda : z \in \lambda \cdot \mathrm{co}(C), \text{ where } \lambda \geqslant 0, C \subseteq \mathcal{E}_V \right\}. \end{aligned}$$

The projective norm satisfies an associative rule: Let $m, n, k \in \mathbb{N}$, then $\big((\mathbb{K}^m \otimes \mathbb{K}^n, \|\cdot\|_\pi) \otimes \mathbb{K}^k, \|\cdot\|_\pi\big)$ and $\big(\mathbb{K}^m \otimes \mathbb{K}^n \otimes \mathbb{K}^k, \|\cdot\|_\pi\big)$ coincide, see [Sok, Proposition 1.2.27].

The norm maximisation problem for the projective norm is an important subject in this thesis. We refer to it as the *projective norm maximisation*. In the literature, this problem is also known as the *nuclear norm minimization*, see Subsection 3.6.3. We recall that maximal vectors for the projective unit ball solve the projective norm maximisation, see Subsection 2.4.2.

Remark. Due to [Ryan], the projective tensor product derives its name from its behaviour with respect to quotient space constructions. It is shown there that the projective norm on bipartite tensor products is equal to the so-called nuclear norm for nuclear operators, which justifies the synonym "nuclear norm".

3.1.5 The Hilbert-Schmidt Norm

The *Hilbert-Schmidt scalar product* $\langle \cdot, \cdot \rangle_{\mathrm{HS}}$ is defined as the scalar product on $V \otimes V$ which is uniquely determined by

$$\langle v, w \rangle_{\mathrm{HS}} := \langle v_1, w_1 \rangle \cdot \ldots \cdot \langle v_r, w_r \rangle,$$

where $v, w \in \mathcal{P}_V$ with $v = v_1 \otimes \cdots \otimes v_r$ and $w = w_1 \otimes \cdots \otimes w_r$.

The norm $\|\cdot\|_{\mathrm{HS}}$ on V which is induced by the Hilbert-Schmidt scalar product is referred to as the *Hilbert-Schmidt norm*. Its unit ball is called the *Hilbert-Schmidt unit ball*.

By identifying V with $\mathbb{K}^N$ as a vector space over $\mathbb{K}$ using the orthonormal basis $e_{a_1} \otimes \cdots \otimes e_{a_r}$, for all $a = (a_1, \ldots, a_r) \in \{1, \ldots, n_1\} \times \cdots \times \{1, \ldots, n_r\}$, the Hilbert-Schmidt scalar product equals the Euclidean scalar product and the Hilbert-Schmidt norm equals the Euclidean norm.

Since $\operatorname{ext}(\mathcal{B}_{1,\pi}) = \mathcal{E}_V$, the Hilbert-Schmidt norm coincides with the projective norm exactly at $\mathcal{P}_V$, and the symmetry group $\operatorname{Sym}_V(\mathcal{E}_V)$ equals the symmetry group $\operatorname{Sym}_V(\mathcal{B}_{1,\pi})$, which will be determined in Subsection 3.3.5.

For all $k \in \{1, \ldots, r\}$, let $U_k \in \mathcal{U}_{n_k}(\mathbb{K})$. The linear operator $V \to V$, $v_1 \otimes \cdots \otimes v_r \mapsto U_1(v_1) \otimes \cdots \otimes U_r(v_r)$, denoted by $U_1 \otimes \cdots \otimes U_r$, is called a *local unitary operator* ($\mathbb{K} = \mathbb{C}$) or *local orthogonal operator* ($\mathbb{K} = \mathbb{R}$). It is unitary (or orthogonal) with respect to the Hilbert-Schmidt norm. Let $\mathcal{U}_{\mathrm{loc}}$ be the group of all local unitary (or orthogonal) operators. It can be easily seen that $\mathcal{U}_{\mathrm{loc}}$ is contained in $\operatorname{Sym}_V(\mathcal{B}_{1,\pi})$.

3.1.6 The Injective Norm

The dual norm of the projective norm on V is called the *injective norm* $\|\cdot\|_\epsilon$. It is also defined by

$$\|z\|_\epsilon = \sup\{|\langle z, w\rangle_{\mathrm{HS}}| \colon w \in \mathcal{E}_V\} = \sup\{|\langle z, w\rangle_{\mathrm{HS}}| \colon \|w\|_\pi \leqslant 1\}$$

for $z \in V$. Its unit ball $\mathcal{B}_{1,\varepsilon}$ is called the *injective unit ball*.

With Proposition 2.4.3 and the Bipolar Theorem 2.3.6, the dual norm of the injective norm equals the projective norm. In particular, the real and the absolute polar of the projective unit ball equals the injective unit ball, and vice versa.

Theorem 2.4.6 can be applied to $\mathcal{B}_{1,\pi}$ since $\mathcal{E}_V$ is a subset of $\mathcal{B}_{1,\pi}$ which satisfies the conditions V0 - V3 in Subsection 2.4.6, so that the norm maximisation problem for the projective norm is strongly related to the injective norm. Hence, the injective norm may help to determine bounds on the inner radius of $\mathcal{B}_{1,\pi}$. See also Subsection 2.4.2 and see [Sok] for examples.

The injective norm is the smallest cross norm on V such that the dual norm is also a cross norm:

Proposition. Let $\|\cdot\|_c$ be an arbitrary cross norm on V. Then the following are equivalent:

(a) $\|\cdot\|_c^\star$ is a cross norm.
(b) $\|\cdot\|_\epsilon \leqslant \|\cdot\|_c \leqslant \|\cdot\|_\pi$.
(c) $\|\cdot\|_\epsilon \leqslant \|\cdot\|_c^\star \leqslant \|\cdot\|_\pi$.

Proof. The assertion holds according to the preceding remarks and since the projective norm is the largest cross norm on V. ◇

3.2 Group Actions

At this point, we recall some basic notions related to group actions which can be found in standard textbooks such as [Bos] or [Cam].

3.2.1 Right and Left Group Actions

Throughout this section, let G be a group with neutral element $1 \in G$ and let X be a set.

Definition. A function $G \times X \to X$, $(g,x) \mapsto g.x$ (respectively, $(g,x) \mapsto x.g$) is called a *left group action* (respectively, a *right group action*), if for all $x \in X$ and for all $g, h \in G$, we have

(i) $1.x = x$.
(ii) $(gh).x = g.(h.x)$ (respectively, $x.(gh) = (x.g).h$).

We note that each right group action can be transformed in a left group action via $g.x := x.g^{-1}$. In this respect, the term "group action" refers usually to left group actions.

Each $g \in G$ gives rise to a bijection $\pi_g \colon X \to X$, $x \mapsto g.x$. It can be easily verified that $g \mapsto \pi_g$ is a group homomorphism from G into the symmetric group S_X of X.

Example. (i) The group G acts on itself through multiplication. In this case, π_g equals the left translation.
(ii) The symmetric group S_X defines a group action on X via $(\sigma, x) \mapsto \sigma.x = \sigma(x)$, that is, $\pi_\sigma = \sigma$.

3.2.2 The Orbit-Stabiliser Theorem

For every $x \in X$, the *orbit* of x under G is the subset

$$[x] := \{g.x \colon g \in G\}$$

of X. Sometimes, we write $G.x$ instead of $[x]$ to outline the corresponding group. The set of all orbits is denoted by

$$X/G := \{[x] \colon x \in X\}$$

and is a partition of X. The group action is called *transitive*, if there is exactly one orbit, that is, for all $x, y \in X$, there exists $g \in G$ with $y = g.x$.

For every $x \in X$, the *stabiliser* of x under G is the subgroup

$$G_x := \{g \in G \colon g.x = x\}$$

of G. If $G_x = G$, then x is called a *fixpoint* of X under the action of G.

The intersection K_G of all stabilisers, the *stabiliser* of X in G, is equal to the kernel of the homomorphism $G \to S_G$, $g \mapsto (x \mapsto g.x)$. If K_G is trivial, G is said to act *faithful* on X. If G is abelian, it can be easily verified that the action of G/K_G on X defined by $(g\,K_G).x := g.x$ is well-defined and faithful.

By the Orbit-stabiliser Theorem, see [Cam, Theorem 7.2], the set of all left cosets $G/G_x = \{g\,G_x \colon g \in G\}$ and the orbit $[x]$ have the same cardinality. A natural bijection is given by $g\,G_x \mapsto g.x$. If G is abelian, G_x is a normal subgroup of G and hence, G/G_x carries also a group structure.

Let G and H be two groups acting on X. We call G and H *commuting*, if for all $x \in X$, we have $g.(h.x) = h.(g.x)$. In this case, G is also a well-defined action on the orbits of H. (Also, H is a well-defined action on the orbits of G.)

3.2.3 A Group Action for Symmetrisations

Many settings involve the observation of "ground transformations" on the domain of a space of functions. To express this, let G be a group acting on a set X. Let A be a subset of the set $\mathcal{A}(X, Y)$ of all functions from X to a set Y.

Proposition. A group action of G on A is given by

$$g.a := a \circ \pi_{g^{-1}} = (x \mapsto a(g^{-1}.x))$$

for all $g \in G$ and $a \in A$.

Proof. Let $a \in A$. It can be easily verified that $1.a = a$. For all $g, h \in G$, we obtain

$$\begin{aligned}(gh).a = a \circ \pi_{(gh)^{-1}} &= a \circ \pi_{h^{-1}g^{-1}} \\ &= a \circ (\pi_{h^{-1}} \circ \pi_{g^{-1}}) = (a \circ \pi_{h^{-1}}) \circ \pi_{g^{-1}} \\ &= (h.a) \circ \pi_{g^{-1}} = g.(h.a).\end{aligned}$$

◇

Example. Let $n \in \mathbb{N}$. With Example 3.2 (ii) and the last proposition, the symmetric group $S_n = S_{\{1,\ldots,n\}}$ acts on X^n, regarded as the set of all functions from $\{1, \ldots, n\}$ to X, from the left: For all $\pi \in S_n$ and all $x = (x_1, \ldots, x_n) \in X^n$, we obtain

$$\pi.x = (x_{\pi^{-1}(1)}, \ldots, x_{\pi^{-1}(r)}) = x \circ \pi^{-1}.$$

The quotient set X^n/S_n can be regarded as a "symmetrisation" of X^n by S_n. Likewise, we may define a right group action of S_n on X^n by $x.\pi := x \circ \pi$ for $\pi \in S_n$ and $x \in X^n$.

We conclude with the warning that a permutation $\pi \in S_n$ can also be written as $(\pi_1, \ldots, \pi_n) \in \{1, \ldots, n\}^n$. Hence, in the special case where $X = \{1, \ldots, n\}$ and x has exactly the entries 1, …, n, we could read x as a permutation $k \mapsto x_k$. But in this context, the group action of S_n on X^2 does *not* equal the left multiplication $\circ$ of permutations, since $\pi.x = x \circ \pi^{-1}$ and $\pi \circ x$ are different in general.

3.3 Geometry of the Projective Unit Ball

To discuss some approaches to the computation of the projective norm we focus on selected tensors as well as on general methods such as the *Schmidt decomposition*, the *generalised Schmidt decomposition*, or the bounds on the projective norm due to Arveson.

Afterwards, we investigate the geometry of the projective unit ball. In this respect, we compute its symmetry group and we focus on exposed faces and their stabilisers. In the bipartite case, the maximal faces can be completely determined.

As above, let $V := \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ for $r, n_1, \ldots, n_r \geqslant 2$.

3.3.1 The Schmidt Decomposition

Here, we investigate the bipartite case.

As above, a tensor $z \in \mathbb{K}^m \otimes \mathbb{K}^n$ can be identified with an $m \times n$ matrix Z. The *singular value decomposition* states that there exists a unitary (or orthogonal) matrix $U \in \mathcal{U}_m(\mathbb{K})$, a diagonal $m \times n$ matrix S with non-negative real entries $\sigma_1, \dots, \sigma_{\min(m,n)}$ on the diagonal and a unitary (or orthogonal) matrix $W \in \mathcal{U}_n(\mathbb{K})$ such that $Z = USW^\star$. Now, let $u_1, \dots, u_m$ be the columns of U and $w_1, \dots, w_n$ be the rows of $W^\star$. It follows that $z = \sum_{k=1}^{\min(m,n)} \sigma_k \cdot u_k \otimes w_k$, which is called the *Schmidt decomposition* of z, see [Aud, Section 8.2]. Using the equation $Z = USW^\star$, we obtain immediately that the *singular values* (or *Schmidt coefficients*) $\sigma_1, \dots, \sigma_{\min(m,n)}$ of Z are the eigenvalues of the positive semidefinite matrix $\sqrt{Z^\star Z}$.

The *trace norm* $\|\cdot\|_{\mathrm{tr}}$ on a matrix space $\mathcal{M}_n(\mathbb{K})$ is defined by

$$\|A\|_{\mathrm{tr}} =: \mathrm{tr}\, \sqrt{A^\star A}$$

for all $A \in \mathcal{M}_n(\mathbb{K})$. We conclude:

(i) The projective norm of z equals equals the 1-norm of the singular values of Z, that is, $\|z\|_\pi = \sum_{k=1}^{\min(m,n)} \sigma_k = \|Z\|_{\mathrm{tr}} = \mathrm{tr}\, \sqrt{Z^\star Z}$.

(ii) The Hilbert-Schmidt norm of z is given by the 2-norm of the singular values of Z, that is, $\|z\|_{\mathrm{HS}} = (\sum_{k=1}^{\min(m,n)} \sigma_k^2)^{1/2} = \sqrt{\mathrm{tr}\, Z^\star Z}$.

(iii) The injective norm of z is given by the max norm of the singular values of Z, which is equal to the operator norm of Z, that is, $\|z\|_\epsilon = \|Z\|_{\mathrm{op}}$.

A summary can be found in the following table, where the definitions are extended to $r = 1$.

r	1	2
$\|\cdot\|_\pi$	1-norm	trace norm
$\|\cdot\|_{\mathrm{HS}}$	2-norm	2-norm
$\|\cdot\|_\epsilon$	max norm	operator norm

3.3.2 The Generalised Schmidt Decomposition

So far, the projective norm of a bipartite tensor is given by the singular values of the corresponding operator. The question arises whether there are generalisations to multipartite tensor products which allow to compute the projective norm. We first have to overcome the difficulty that an identification with operators cannot be generalised in a canonical way. Nevertheless, there are some approaches, for example, by generalising the Schmidt decomposition due to [AS] (there is another notion due to [Der]):

Definition. Let $r = 3$ and let $z \in V$. A representation of z of the form

$$z = \sum_{k=1}^{s} \sigma_k \cdot v_k^1 \otimes v_k^2 \otimes w_k,$$

where $(v_k^1)_{k=1}^s$ and $(v_k^2)_{k=1}^s$ are orthonormal systems of $\mathbb{K}^{n_1}$ and $\mathbb{K}^{n_2}$, respectively; and where $w_1, \ldots, w_s \in (\mathbb{K}^{n_3})_1$ and $\sigma_1, \ldots, \sigma_s \geqslant 0$ is called a *generalised Schmidt decomposition* (*gsd-decomposition*) of z. If z possesses a decomposition of this form, then it is called *generalised Schmidt decomposable* or a *gsd-vector*.

If $z \in V$ has a gsd-decomposition as above, then $\|z\|_\pi = \sum_{k=1}^s \sigma_k$, see [AS, Theorem 3].

Example. Let $z := e_1 \otimes e_1 \otimes (ae_1 + be_2) + e_2 \otimes e_2 \otimes (ce_1 + de_2) \in \mathbb{K}^2 \otimes \mathbb{K}^2 \otimes \mathbb{K}^2$ with $a, b, c, d \in \mathbb{K}$, where $1 = |a|^2 + |b|^2 + |c|^2 + |d|^2$, that is, z is a unit vector. A short calculation shows that the projective norm of z equals $\sqrt{|a|^2 + |b|^2} + \sqrt{1 - |a|^2 - |b|^2}$, see [AS, Example 3]. Hence, if $v \in V$ is a unit gsd-vector, then $\|v\|_\pi \leqslant \sqrt{2}$.

In what follows, we discuss whether (or not) gsd-vectors could be candidates for maximal vectors for the projective unit ball.

3.3.3 The GHZ-Vector and the W-Vector

The unit vectors in $V = \mathbb{K}^2 \otimes \mathbb{K}^2 \otimes \mathbb{K}^2$ defining the so-called GHZ-state and the so-called W-state are given by

$$\xi_{\mathrm{GHZ}} := \frac{1}{\sqrt{2}}(e_1 \otimes e_1 \otimes e_1 + e_2 \otimes e_2 \otimes e_2) \quad \text{and}$$

$$\xi_W := \frac{1}{\sqrt{3}}(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1),$$

respectively. We refer to them as the *GHZ-vector* and the *W-vector*. With Example 3.3.2, we obtain $\|\xi_{GHZ}\|_\pi = \sqrt{2}$. For $\mathbb{K} = \mathbb{C}$, we have $\|\xi_W\|_\pi = \frac{3}{2}$, which implies $r(V) \leqslant {}^2\!/\!_3$, see [FL, Lemma 6.2] (cf. [AS]). For $\mathbb{K} = \mathbb{R}$, we will show below that $\|\xi_W\|_\pi = \sqrt{3}$, see Example 7.3.5.IV, which is larger than $\sqrt{2}$. Hence, for both $\mathbb{K} = \mathbb{R}$ and $\mathbb{K} = \mathbb{C}$, the W-vector is not generalised Schmidt decomposable, and gsd-vectors such as the GHZ-vector cannot be maximal vectors for the projective unit ball in V.

Now, we consider the vector

$$\xi_4 := \frac{1}{2}(e_1 \otimes e_1 \otimes e_2 + e_1 \otimes e_2 \otimes e_1 + e_2 \otimes e_1 \otimes e_1 - e_2 \otimes e_2 \otimes e_2).$$

In the case where $\mathbb{K} = \mathbb{R}$, this vector is maximal due to [Wie, Abschnitt 5.3], see also [FL, Lemma 6.1]. Hence, the inner radius of $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$ is equal to ${}^1\!/\!_2$. In particular, the W-vector is not maximal in the real case. These statements appear as special cases of our results below, see Section 10.1. In general, a summary of the cases where the inner radius can be determined in connection with this thesis is given in Section 10.1.

The real case motivates to consider ξ_4 as a candidate for maximality also in the complex case. However, it is interesting that this case is completely different. A reason is that there are strictly more local unitary operators on $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ than local orthogonal operators on $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$. This leads to situations like the following:

Proposition. There exists a local unitary operator $U = U_1 \otimes U_2 \otimes U_3$, where U_1, U_2, U_3 are unitary matrices on $\mathbb{C}^2$, such that $U(\xi_{GHZ}) = \xi_4$.

Proof. Let $U := T \otimes D \otimes D$ with the unitary matrices $T := \frac{1}{\sqrt{2}}\begin{pmatrix} -i & -i \\ 1 & -1 \end{pmatrix}$ and $D := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$. A simple computation shows that $U(\xi_{GHZ}) = \xi_4$. ◇

The last statement shows that $\|\xi_4\|_\pi = \|\xi_{GHZ}\|_\pi = \sqrt{2}$ in the case where $\mathbb{K} = \mathbb{C}$, see also [FL, Lemma 6.1]. Hence, ξ_4 is a gsd-vector, but not maximal for $\mathcal{B}_{1,\pi}$ in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Instead, we are motivated due to [DVC] that the W-vector could be a candidate for maximality. Some details on this "base field dependence" can also be found in [FL, Section 6].

3.3.4 The Arveson Bound

Approaches to the inner radius of the projective unit ball for general multipartite tensor products can be found in [Arv]. The following theorem, which is adopted from [Arv, Theorems 10.1 and 11.1], gives a lower bound on the inner radius. It states also that in the case where $\mathbb{K} = \mathbb{C}$, the lower bound will be attained if and only if the dimension of the last tensor factor is large enough. Let $N_{r-1} := \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_{r-1}\}$.

Theorem. The inner radius of the projective unit ball in V satisfies the inequality

$$r(\mathcal{B}_{1,\pi}) \geqslant \operatorname{Arv}(V) := \frac{1}{\sqrt{n_1 \cdot \ldots \cdot n_{r-1}}},$$

where $\operatorname{Arv}(V)$ is called the *Arveson bound*. For $\mathbb{K} = \mathbb{C}$, the following are equivalent:

(a) $r(\mathcal{B}_{1,\pi}) = \operatorname{Arv}(V)$.
(b) $n_r \geqslant n_1 \cdot \ldots \cdot n_{r-1}$.

In this case, maximal vectors are given by

$$\frac{1}{\sqrt{n_1 \cdot \ldots \cdot n_{r-1}}} \cdot \sum_{a=(a_1,\dots,a_{r-1}) \in N_{r-1}} v^1_{a_1} \otimes \cdots \otimes v^{r-1}_{a_{r-1}} \otimes w_a,$$

where $(v^k_t)_{t=1}^{n_k}$ is an orthonormal basis of $\mathbb{C}^{n_k}$ for each $k \in \{1, \dots r-1\}$ and $(w_a)_{a \in N_{r-1}}$ is an orthonormal system in $\mathbb{C}^{n_r}$.

Corollary. For $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, we have $1/2\sqrt{2} < r(\mathcal{B}_{1,\pi}) \leqslant 2/3$.

Proof. This statement follows from $\|\xi_W\|_\pi = \frac{3}{2}$ and the Arveson bound. ◇

Corollary. Let $s := \min(m, n)$. The maximal vectors in $\mathbb{K}^m \otimes \mathbb{K}^n$ are given by the unit vectors with s Schmidt coefficients $1/\sqrt{s}$, that is, by vectors of the form

$$\frac{1}{\sqrt{s}} \cdot (v_1 \otimes w_1 + \cdots + v_s \otimes w_s),$$

where $(v_k)_{k=1}^s$ and $(w_k)_{k=1}^s$ are orthonormal systems in $\mathbb{K}^m \otimes \mathbb{K}^n$, respectively. In this case, the inner radius of $\mathcal{B}_{1,\pi}$ equals $1/\sqrt{s}$.

Proof. This statement follows immediately from Theorem 3.3.4. ◇

For $\mathbb{K} = \mathbb{C}$ and $n_r \geqslant n_1 \cdot \ldots \cdot n_{r-1}$, the inner radius of the projective unit ball in V equals the inner radius of the projective unit ball for the bipartite tensor product $(\mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_{r-1}}) \otimes \mathbb{C}^{n_r}$. From the Schmidt decomposition, it follows that the projective norms are equal, that is, V can be considered as a bipartite tensor product in terms of the projective norm. Hence, the tensor products whose dimensions are balanced such as $\mathbb{C}^n \otimes \cdots \otimes \mathbb{C}^n$ are an interesting counterpart.

For real tensor products, the Arveson bound can be attained even if $n_r \geqslant n_1 \cdot \ldots \cdot n_{r-1}$ is not true. This can be verified with the values for the inner radius which can be determined in connection with this thesis, see Section 10.1. For further information, see [Sok].

Let $\mathcal{U}^0_{\text{loc}}$ be the subgroup of all local unitary (or orthogonal) operators which have the form $\mathbb{1}_{n_1} \otimes \cdots \otimes \mathbb{1}_{n_{r-1}} \otimes O$, where $O \in \mathcal{U}_{n_r}(\mathbb{K})$. This group induces a faithful group action on the maximal vectors (in the case where $r = 2$, this can be easily verified with the Schmidt decomposition, and all other cases can be traced back to the bipartite case from above by considering the $\{1, \ldots, r-1\}$-$\{r\}$-unfolding of V). In the case where $n_r \geqslant n_1 \cdot \ldots \cdot n_{r-1}$, the group action is not only faithful, but also transitive, see [Arv, Theorem 12.1].

3.3.5 The Symmetry Group of the Projective Unit Ball

Here, we determine the symmetry group $\operatorname{Sym}_V(\mathcal{B}_{1,\pi})$. We have seen above that it contains the group $\mathcal{U}_{\text{loc}}$ of all local unitary (or orthogonal) operators. Moreover, let F be the subgroup of the permutation group S_r of r elements which consists of all $\sigma \in S_r$ such that each cycle κ of σ has the property that $n_s = n_t$ for all $s, t \in \operatorname{supp}(\kappa)$. Each $\sigma \in F$ induces a *flip operator*

$$F_\sigma \colon V \to V,\ v_1 \otimes \cdots \otimes v_r \mapsto v_{\sigma^{-1}(1)} \otimes \cdots \otimes v_{\sigma^{-1}(r)}.$$

The set F_V of all flip operators is contained in $\operatorname{Sym}_V(\mathcal{B}_{1,\pi})$.

Details on the symmetry group of $\mathcal{B}_{1,\pi}$ can be found in [Maa], which deals with the case where the tensor factors are equal.

Proposition. $\operatorname{Sym}_V(\mathcal{B}_{1,\pi}) = \mathcal{U}_{\text{loc}} \rtimes F_V$.

Proof. Let $U \in S := \operatorname{Sym}_V(\mathcal{B}_{1,\pi})$. For each $k \in \{1, \ldots, r\}$, let $V_k := \bigotimes_{\substack{l=1\\ l \neq k}}^{r} \mathbb{K}^{n_l}$.

For each non-zero product vector $v \in V_k$, let

$$U_{k,v}\colon \mathbb{K}^{n_k} \to V,\ w \mapsto U(v \otimes w)$$

(as an abbreviation, "$v \otimes w$" means that w is "inserted" in v in position k, that is, $v \otimes w := v_1 \otimes \cdots \otimes v_{k-1} \otimes w \otimes v_{k+1} \otimes \cdots \otimes v_r$ for $v = v_1 \otimes \cdots \otimes v_{k-1} \otimes v_{k+1} \otimes \cdots \otimes v_r$). We recall that each factor of a non-zero product vector is determined up to multiplication with a number in $\mathbb{K}$. We also recall that for all non-zero product vectors $v_1, v_2 \in V$, the sum $v_1 + v_2$ is a product vector, if and only if in each position up to at most one position, the factors of v_1 and v_2 are linearly dependent.

Statement 1: There exists $\tilde{k} = \tilde{k}(v) \in \{1, \dots, r\}$ and an isometry on its image $U^2_{k,v}\colon \mathbb{K}^{n_k} \to \mathbb{K}^{n_{\tilde{k}}}$ such that the $\tilde{k}^{\text{th}}$ factor of $U_{k,v}(w)$ equals $U^2_{k,v}(w)$ for all $w \in \mathbb{K}^{n_k}$ (up to multiplication with a number in $\mathbb{K}$, which depends on v).

Proof: The image of $U_{k,v}$ consists of product vectors. In particular, for all $w_1, w_2 \in \mathbb{K}^{n_k}$, the sum $U_{k,v}(w_1) + U_{k,v}(w_2)$ is a product vector. If w_1 and w_2 are non-zero, then the factors of $U_{k,v}(w_1)$ and $U_{k,v}(w_2)$ in each position, except at most one, have to be linearly dependent. Let us assume that there exist non-zero $w_0, w_1, w_2 \in \mathbb{K}^{n_k}$ such that $U_{k,v}(w_0)$ and $U_{k,v}(w_l)$ are linearly independent in positions $\tilde{k}_l$ with $\tilde{k}_1 \neq \tilde{k}_2$. It follows that there are two positions in which $U_{k,v}(w_1)$ and $U_{k,v}(w_2)$ are linearly independent. But this is impossible according to the previous statement.
Hence, there exist $\tilde{k} = \tilde{k}(v) \in \{1, \dots, r\}$, $\tilde{v} \in V_{\tilde{k}}$ with $\|\tilde{v}\| = \|v\|$ and a linear map $U^2_{k,v}\colon \mathbb{K}^{n_k} \to \mathbb{K}^{n_{\tilde{k}}}$ with

$$U_{k,v}(w) = \tilde{v} \otimes \underbrace{U^2_{k,v}(w)}_{\uparrow\ \text{position } \tilde{k}}$$

for all $w \in \mathbb{K}^{n_k}$. Since U preserves the length of product vectors, $\|w\| = \|U^2_{k,v}(w)\|$ for all $w \in \mathbb{K}^{n_k}$. Hence, $U^2_{k,v}$ is injective and an isometry on its image. In particular, it follows that $n_{\tilde{k}} \geqslant n_k$. We note that $\tilde{v}$ does not depend on w. Hence, for all $l \in \{1, \dots, r\}$, $l \neq k$, the linear hull of "the" factor of $U(v \otimes w)$ in position l does not depend on w.

Statement 2: $\tilde{k}$ does not depend on v.

Proof: Let $v_1, v_2 \in V_k$ be non-zero product vectors such that also $v_1 + v_2$ is a product vector. In this case, $U_{k,v_1}(w) + U_{k,v_2}(w)$ is also a product vector for all $w \in \mathbb{K}^{n_k}$. Let us assume that $\tilde{k}(v_1) \neq \tilde{k}(v_2)$. It follows that $(\tilde{v}_1)_{\tilde{k}(v_2)}$ and $U^2_{k,v_2}(w)$ are linearly dependent or $(\tilde{v}_2)_{\tilde{k}(v_1)}$ and $U^2_{k,v_1}(w)$ are linearly dependent. But this is impossible since w was arbitrary and $n_l \geqslant 2$ for all $l \in \{1, \dots, r\}$. Thus, $\tilde{k}(v_1) = \tilde{k}(v_2)$. The statement follows by induction, since the product vectors emerge from each other by interchanging the factors one after another.

Statement 3: The function $\sigma\colon \{1, \dots, r\} \to \{1, \dots, r\}$, $k \mapsto \tilde{k}$ is a permutation.

Proof: We also have $U^{-1}(\mathcal{E}_V) = \mathcal{E}_V$. For all $l \in \{1, \dots, r\}$ and for all $v \in V_k$, there exist $l' \in \{1, \dots, r\}$ and $v' \in V_{n_{l'}}$ such that for all $w \in \mathbb{K}^{n_k}$, we have

$$U^{-1}(v \otimes w) = (U^{-1})_{l,v}(w) = v' \otimes \underbrace{(U^{-1})^2_{l,v}(w)}_{\uparrow \text{ position } l'} \,.$$

Hence,

$$v \otimes w = U(v' \otimes (U^{-1})^2_{l,v}(w)) = U_{l',v'}\big((U^{-1})^2_{l,v}(w)\big).$$

We have seen above that the function $(U^{-1})^2_{l,v} =: V_{l,v}\colon \mathbb{K}^{n_l} \to \mathbb{K}^{n_{l'}}$ is injective. Now, for any $w' \in V_{l,v}(\mathbb{K}^{n_l}) \subseteq \mathbb{K}^{n_{l'}}$, we obtain

$$\begin{aligned} U_{l',v'}(w') &= (\tilde{v'}) \otimes U^2_{l',v'}(w') \\ &= v \otimes ((V_{l,v})^{-1})(w'). \end{aligned}$$

Now, we show $\sigma(l') = l$ with an argument similar to the first in statement 1: Let $w_1, w_2 \in V_{l,v}(\mathbb{K}^{n_l})$ be linearly independent (this is possible since $n_l \geqslant 2$). Then $U_{l',v'}(w_1)$ and $U_{l',v'}(w_2)$ are linearly independent, and the factors in each position up to exactly one, $\sigma(l')$, are linearly dependent. The last equation shows that this position also equals l, that is, $\sigma(l') = l$. Hence, σ is surjective.

Statement 4: The linear map $U^2_{k,v}$ is unitary (here, we use the notion "unitary" also in the case $\mathbb{K} = \mathbb{R}$).

Proof: As we have seen, σ is a permutation, and $n_k \leqslant n_{\sigma(k)}$ for all $k \in \{1, \dots, r\}$. It follows that $n_k = n_{\sigma(k)}$ for all $k \in \{1, \dots, r\}$, that is, $U^2_{k,v}$ is unitary.

Statement 5: For all $k \in \{1, \dots, r\}$, there exists a unitary map $U^2_k\colon \mathbb{K}^{n_k} \to \mathbb{K}^{n_{\sigma(k)}}$ and there exists a phase $\xi \in \mathbb{K}$ such that $U = \xi \cdot U'$ with $U' := F_\sigma(U^2_1 \otimes \cdots \otimes U^2_r)$.

Proof: For any product vector $v = v_1 \otimes \cdots \otimes v_r \in V$, we have

$$U'(v) = U^2_{\sigma^{-1}(1)}(v_{\sigma^{-1}(1)}) \otimes \cdots \otimes U^2_{\sigma^{-1}(r)}(v_{\sigma^{-1}(r)}).$$

Let v be non-zero. For all $l \in \{1, \dots, r\}$, let $v^l := v_1 \otimes \dots \otimes v_{l-1} \otimes v_{l+1} \otimes \dots \otimes v_r$. As we have seen, there exists a phase $\varphi \colon V \to (\mathbb{K})_1$ with

$$U(v) = \varphi(v) \cdot U^2_{\sigma^{-1}(1), v^{\sigma^{-1}(1)}}(v_{\sigma^{-1}(1)}) \otimes \dots \otimes U^2_{\sigma^{-1}(r), v^{\sigma^{-1}(r)}}(v_{\sigma^{-1}(r)}).$$

From statement 1, we know that for all $k \neq l$, the linear hull of a factor of $U(v)$ in position $\sigma(l)$ does not depend on v_k. Hence, it depends only on v_l. Thus, there exists a phase $\xi_l \colon V_k \to (\mathbb{K})_1$ such that the expression $U^2_l(v_l) := \xi_l(v^l) \cdot U^2_{l,v^l}(v_l)$ depends only on v_l. Now, the function $U^2_l \colon \mathbb{K}^{n_l} \to \mathbb{K}^{n_{\sigma(l)}}$, $w \mapsto \xi_l(v^l) \cdot U^2_{l,v^l}(w)$ is linear, bijective and preserves the length, hence, it is unitary. We consider the function $\xi \colon V \to (\mathbb{K})_1$, $\xi(v) := \varphi(v) \cdot \xi_1(v^1)^{-1} \cdot \ldots \cdot \xi_r(v^r)^{-1}$, so that $U(v)$ has the form

$$U(v) = \xi(v) \cdot U^2_{\sigma^{-1}(1)}(v_{\sigma^{-1}(1)}) \otimes \dots \otimes U^2_{\sigma^{-1}(r)}(v_{\sigma^{-1}(r)}).$$

Since U is linear, it follows that ξ is independent from v.

Statement 6: $S = \mathcal{U}_{\text{loc}} \rtimes F_V$.

Proof: Up to now, we have seen that $S = \mathcal{U}_{\text{loc}} \cdot F_V$. In particular, S is the semidirect product of $\mathcal{U}_{\text{loc}}$ and F_V, since $\mathcal{U}_{\text{loc}}$ is a normal subgroup of S and $\mathcal{U}_{\text{loc}} \cap F_V = \{\text{id}\}$. $\diamond$

3.3.6 Faces of the Projective Unit Ball

An exposed face F of $\mathcal{B}_{1,\pi}$ has the form $F = \mathcal{B}_{1,\pi} \cap P$, where P is a real affine hyperplane. With Proposition 2.3.5.I, the extreme points of F are given by $\mathcal{E}_V \cap P$.

Obviously, the projective norm of each vector which lies in an exposed face is equal to 1.

Proposition. Let $V = \mathbb{K}^2 \otimes \mathbb{K}^2 \otimes \mathbb{K}^2$ and let $v_0 := \frac{1}{2}(e_1 \otimes e_1 \otimes e_1 + e_2 \otimes e_2 \otimes e_2)$. The exposed face $F := \mathcal{B}_{1,\pi} \cap P_{l_{v_0}}$ which is induced by v_0 equals $F = \text{co}(\{e_1 \otimes e_1 \otimes e_1, e_2 \otimes e_2 \otimes e_2\})$.

Proof. Let $x = (x_1, x_2)^t, y = (y_1, y_2)^t, z = (z_1, z_2)^t \in (\mathbb{K}^2)_1$ be unit vectors. Now, we consider the unit product vector $v' := x \otimes y \otimes z \in \mathcal{E}_V$. We have $v' \in P_{l_{v_0}}$, if and only if $1 = \text{Re}(x_1 y_1 z_1 + x_2 y_2 z_2) = \text{Re}(\langle w, \bar{z} \rangle)$, where $w := (x_1 y_1, x_2 y_2)^t$. The norm of w equals $\|w\| = |x_1 y_1|^2 + |x_2 y_2|^2 = |x_1|^2 |y_1|^2 + |x_2|^2 |y_2|^2 \leqslant 1$. It is equal to 1, if and only if either $x_1 = y_1 = 1$ or $x_2 = y_2 = 1$. In this case, $1 = \text{Re}(\langle w, \bar{z} \rangle)$, if and only if $z = \overline{w}$. On the other hand, if $\|w\| < 1$, then $\mathrm{Re}(\langle w, \overline{z}\rangle) < 1$. In summary, $\mathrm{Re}(\langle w, \overline{z}\rangle) = 1$, if and only if $x \otimes y \otimes z$ is equal to $e_1 \otimes e_1 \otimes e_1$ or to $e_2 \otimes e_2 \otimes e_2$. ◇

3.3.7 Maximal Vectors and Maximal Faces

It can be easily verified that the unit product vectors, as a subset of the projective unit ball $\mathcal{B}_{1,\pi}$, satisfy the conditions V0 - V3 from Subsection 2.4.6. According to Theorem 2.4.7, there is a one-to-one correspondence between maximal vectors and maximal faces which are induced by maximal vectors. In particular, each maximal vector y induces a maximal face $M_v := \mathcal{B}_{1,\pi} \cap P_{l_v}$ of $\mathcal{B}_{1,\pi}$, where $v := r(\,\mathcal{B}_{1,\pi}\,) \cdot y$ and where $l_v = 1 - r(\mathcal{B}_{1,\pi})^{-1} \cdot \langle\,\cdot\,, y\rangle$ is the support functional to y.

The set of all maximal vectors is invariant under the symmetry group $\mathrm{Sym}_V(\mathcal{B}_{1,\pi})$, which equals $\mathcal{U}_{\mathrm{loc}} \rtimes F_V$ according to Proposition 3.3.5.

Definition. Two maximal faces F_1, F_2 of $\mathcal{B}_{1,\pi}$ are called *equivalent*, if there exists $U \in \mathrm{Sym}_V(\mathcal{B}_{1,\pi})$ with $U(F_1) = F_2$. The *distance* of an equivalence class to zero is defined as the distance to zero of any representative.

The question arises whether all maximal faces are induced by maximal vectors. Alternatively, one could ask about the distances of the equivalence classes of maximal faces to zero (however, it is not clear whether the distance characterises the equivalence classes).

3.3.8 Maximal Faces in the Bipartite Case

For any subset $B \subseteq V$, let

$$\mathrm{Sym}_V^{\pi}(B) := \{U \in \mathrm{Sym}_V(\mathcal{B}_{1,\pi}) \colon U(B) = B\}$$

denote the stabiliser of B under $\mathrm{Sym}_V(\mathcal{B}_{1,\pi})$.

In what follows, we investigate the maximal faces and their stabilisers under $\mathrm{Sym}_V(\mathcal{B}_{1,\pi})$ in the bipartite case $V = \mathbb{K}^n \otimes \mathbb{K}^n$. The special case $\mathbb{R}^2 \otimes \mathbb{R}^2$ is outlined in [Lang, Satz 6.3.4].

Let $\mathcal{U}^1_{\mathrm{loc}} := \{O \otimes \overline{O} \colon O \in \mathcal{U}_n(\mathbb{K})\}$. We have $F_V = \{F_{(1\,2)}, \mathrm{id}\}$, so that we may consider the group $S_0 := \mathcal{U}^1_{\mathrm{loc}} \rtimes F_V$.

Now, we consider the maximal vector

$$y := \frac{1}{\sqrt{n}} \cdot (e_1 \otimes e_1 + \cdots + e_n \otimes e_n).$$

Let $v := \frac{1}{\sqrt{n}} \cdot y = \frac{1}{n}(e_1 \otimes e_1 + \cdots + e_n \otimes e_n)$. The support functional of v equals $l_v = 1 - \langle \cdot, e_1 \otimes e_1 + \cdots + e_n \otimes e_n \rangle$.

For the proof of the following theorem we use arguments from [Eis] about mean ergodic projections. One can imagine that this theorem is common knowledge, but we have not yet encountered it in the literature.

Theorem. (*Maximal Faces of the Projective Unit Ball*)
The maximal face $M := M_v$ has the form

$$M = \left\{ U\Big(\sum_{l=1}^{n} \lambda_l \cdot e_l \otimes e_l \Big) \ : \ \lambda_l \in [0,1],\ \sum_{l=1}^{n} \lambda_l = 1,\ U \in S_0 \right\}.$$

In particular, we have

(i) $\text{ext}(M) = \{u \otimes \overline{u} \colon \|u\| = 1\} = S_0(e_1 \otimes e_1)$,
(ii) $\text{Sym}_V^{\pi}(v) = \text{Sym}_V^{\pi}(\text{ext}(M)) = \text{Sym}_V^{\pi}(M) = S_0$,
(iii) S_0 has exactly one fixpoint in M, which equals v.

Proof. We first show (i). Let $P := P_{l_v}$. Let $w \in V$, then $w \in \text{ext}(M) = \mathcal{E}_V \cap P$ if and only if there exist $u_1, u_2 \in \mathbb{K}^n$, $\|u_1\| = \|u_2\| = 1$, such that $w = u_1 \otimes u_2$ and $1 = \text{Re}(\langle u_1, \overline{u_2} \rangle)$, which implies $u_2 = \overline{u_1}$.

Now, we show (ii). Let $\text{Sym}_V(\mathcal{B}_{1,\pi}) =: G$. We use the notation from Subsection 3.2.2, that is, $\text{Sym}_V^{\pi}(B) = G_B$ for all $B \subseteq V$. A symmetry argument implies $G_{\text{ext}(M)} = S_0$ and it can be easily verified that $G_M = G_{\text{ext}(M)}$. Finally, we show $G_v = S_0$.

Step 1: $G_v \subseteq S_0$.
Let $U \in G$ with $Uv = v$. We obtain $U(P) = P$. Hence, $U(\text{ext}(M)) = U(\mathcal{E}_V \cap P) = U(\mathcal{E}_V) \cap U(P) = \mathcal{E}_V \cap P = \text{ext}(M)$, that is, $G_v \subseteq G_{\text{ext}(M)} = S_0$.

Step 2: $S_0 \subseteq G_v$.
We assume that there exists $U_0 \in S_0$ with $U_0 v \neq v$. Let $w := {}^1\!/\!_2(U_0 v + v)$. Since the Hilbert-Schmidt unit sphere in V is strictly convex, we may conclude that $\|w\| < \|v\| = \|U_0 v\|$, which is a contradiction, since $w \in M$. Hence, $U_0 v = v$, that is, v is a fixpoint of S_0.

Now, we show that M has the form which is stated at the beginning. Let $w \in M$. On the one hand, w corresponds to a positive semidefinite matrix, since $\operatorname{ext}(M)$ corresponds to the projections of rank 1. On the other hand, $\|w\|_\pi = 1$, since M is a proper face of $\mathcal{B}_{1,\pi}$. Hence, the Schmidt decomposition of w has the form $w = \sum_{l=1}^n \lambda_l \cdot u_l \otimes \overline{u_l}$, where $\lambda_l \geqslant 0$ with $\lambda_1 + \cdots + \lambda_n = 1$ and where $(u_l)_{l=1}^n$ is an orthonormal basis of $\mathbb{K}^n$. Thus, there exists $U \in S_0$ with $w = U(\sum_{l=1}^n \lambda_l \cdot e_l \otimes e_l)$. In addition, we obtain

$$\begin{aligned} w = v \;&\Leftrightarrow\; w \text{ has minimal Hilbert-Schmidt norm} \\ &\Leftrightarrow\; \lambda_1 = \cdots = \lambda_n = \frac{1}{n} \\ &\Leftrightarrow\; w \text{ is a fixpoint of } S_0, \end{aligned}$$

which proves (iii). ◇

With the Schmidt decomposition, each boundary vector of $\mathcal{B}_{1,\pi}$ is contained in a maximal face, which is induced by a maximal vector. Hence, there is a one-to-one correspondence between maximal faces and operators in $\mathcal{U}^0_{\text{loc}}$: For each pair M_1, M_2 of maximal faces, there exists $U \in \mathcal{U}^0_{\text{loc}}$ such that $M_2 = U(M_1)$. In summary, the projective unit ball in $\mathbb{K}^n \otimes \mathbb{K}^n$ has exactly one equivalence class of maximal faces.

Given a multipartite tensor product it is not clear whether $\mathcal{U}^0_{\text{loc}}$ is transitive on the maximal vectors. Also, it is not clear whether all maximal faces of $\mathcal{B}_{1,\pi}$ are given by maximal vectors.

Remark. Let y, v, M be as defined in Theorem 3.3.8. With [Eis, Theorem 8.32], the orthogonal projection onto the maximal vector y is the so-called mean ergodic projection corresponding to the so-called mean ergodic group S_0. In this respect, the vector v could also be regarded as a "barycenter" of M. However, a definition of "barycenter" in the sense of Choquet Theory, see, for example [Ta1, Lemma 6.3, Chapter IV], needs an appropriate probability measure on the maximal face, on which we do not concentrate here.

3.4 (Unit) Product Vectors as a Variety

In this section, we show that the product vectors in a real or complex finite-dimensional tensor product are an affine variety, see the Determinant Criterion Theorem 3.4.6. In the real case we show that also the unit product vectors are an affine variety, see the Criterion for

Unit Product Vectors Theorem 3.4.7. Both statements can be found in [Sto] (or in [RS2]) and in [Lang]. Compare also with [GKM].

Just as defined in the previous section, let $V := \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$, where $r, n_1, \dots, n_r \geqslant 2$.

3.4.1 Tensor Products as Affine Spaces

From now on, let $N := \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$. As a finite-dimensional vector space, V can be identified with $\mathbb{K}^N$ via the following identification, depending on the choice of an orthonormal basis for each tensor factor:

$$\begin{array}{ccc} \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r} & \to & \mathbb{K}^N \\ e_{a_1} \otimes \cdots \otimes e_{a_r} & \mapsto & e_{(a_1,\dots,a_r)}. \end{array}$$

This identification is real linear for $\mathbb{K} = \mathbb{R}$ and complex linear for $\mathbb{K} = \mathbb{C}$. Hence, in the sense of algebraic geometry, a finite-dimensional tensor product can be treated as a real or complex affine space. Doing so, polynomials in $\mathbb{K}[x_a \colon a \in N]$ are functionals on $\mathbb{K}^N$ as follows: For all $a, b \in N$, we obtain

$$x_a(e_b) := \begin{cases} 1, & a = b, \\ 0, & a \neq b. \end{cases}$$

3.4.2 The Indexing Tuples

Definition. The set N is called the *indexing tuples* for V. For any $a := (a_1, \dots, a_r) \in N$, we write also $a = a_1 \cdots a_r$. For all $k \in \{1, \dots, r\}$, the number a_k is called the *entry* of a in *position* k.

In what follows, we collect some viewpoints on the indexing tuples which could be helpful for the understanding of the product vectors and of the projective norm.

Let $n := \max(n_1, \dots, n_r)$. In general, the indexing tuples N can be identified with a subset of the set $\mathcal{A}(\{1, \dots, r\}, \{1, \dots, n\})$ of all functions from $\{1, \dots, r\}$ to $\{1, \dots, n\}$. In this respect, $a \in N$ is given by the evaluations $a_k = a(k)$, for all $k \in \{1, \dots, r\}$.

Moreover, the indexing tuples can be considered as a finite distributive lattice. This viewpoint will be very useful in the chapters below.

In the case where $n_1 = \cdots = n_r =: n$, the indexing tuples can be identified with the words of length r with the letters $1, \ldots, n$. This viewpoint "justifies" the notation $a_1 \cdots a_r$ for any $(a_1, \ldots, a_r) \in N$.

The indexing tuples can be considered as the vertices of a graph, where $a, b \in N$ are adjacent vertices, if and only if the entries of a and b are equal in all positions up to exactly one position, where they are adjacent numbers. This graph can be identified with a hypercube (in the case where $n = 2$) or a grid. For example, the graph yields a three-dimensional cube for $n = 2$, $r = 3$ or a tesseract for $n = 2$, $r = 4$.

Finally, the indexing tuples can be considered as a code space.

The different viewpoints are summarised in table 3.1.

Viewpoint	Reference
Basis of a tensor product	3.4.1
Function space	3.4.2
Lattice	4.2.3
Set of words	8.4
Grid, hypercube	4.2.3, 6.3.4
Code space	6.5, 6.3.1

Table 3.1: Viewpoints on the indexing tuples.

3.4.3 Product Vectors as a Variety (Bipartite Case)

Proposition. For finite-dimensional bipartite tensor products, the rank of a tensor equals the rank of the corresponding matrix.

Proof. The *rank factorisation* from linear algebra states that a real or complex $m \times n$ matrix A of rank $k \in \mathbb{N}$ can be expressed as a product of an $m \times k$ matrix B and a $k \times n$ matrix C. Hence, if B has the columns $b_1, \ldots, b_k$ and C has the rows $c_1, \ldots, c_k$, then $A = \sum_{t=1}^{k} b_k \cdot c_k$, which corresponds to the tensor $\sum_{t=1}^{k} b_k \otimes c_k$. ◇

Alternatively, this statement follows from the Schmidt decomposition or the from the singular value decomposition. The number of singular values equals the rank. In particular, product vectors correspond to matrices of rank one or of rank zero.

Example. If we consider $N = \{1,2\} \times \{1,2\}$, corresponding to $\mathbb{K}^2 \otimes \mathbb{K}^2$, a product vector $v = \left(\begin{smallmatrix} x_1 \\ x_2 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} y_1 \\ y_2 \end{smallmatrix}\right)$, where $x_1, x_2, y_1, y_2 \in \mathbb{K}$, can be identified with

$$\begin{pmatrix} x_1y_1 \\ x_1y_2 \\ x_2y_1 \\ x_2y_2 \end{pmatrix} \in \mathbb{K}^4 \quad \text{as well as with} \quad \begin{pmatrix} x_1y_1 & x_1y_2 \\ x_2y_1 & x_2y_2 \end{pmatrix} \in \mathcal{M}_2(\mathbb{K}).$$

The polynomial $d := x_{11}x_{22} - x_{12}x_{21} \in \mathbb{K}[x_{22}, x_{21}, x_{12}, x_{11}]$ equals the determinant on $\mathcal{M}_2(\mathbb{K})$. We observe that d vanishes on v, since $d(v) = x_1y_1 \cdot x_2y_2 - x_1y_2 \cdot x_2y_1 = 0$. Hence, $v \in \mathcal{Z}_{\mathbb{K}}(d)$. On the other hand, any matrix vanishing on d has rank zero or rank one, which corresponds to a product vector.

Generalising the last example, the following lemma shows that the set of all product vectors in an arbitrary finite-dimensional bipartite tensor product is a variety, which is known as the *Segré variety*. This variety is a specific *determinantal variety*. For details, see [Har, Example 9.1] or [Hat, Exercise 2.14].

Lemma. A tensor $v \in \mathbb{K}^m \otimes \mathbb{K}^n$ is a product vector if and only if the determinant of each 2×2 submatrix vanishes, that is, v vanishes on each polynomial

$$x_{a\,b}\, x_{c\,d} - x_{a\,d}\, x_{c\,b} \ \in \mathbb{K}[\,x_a \colon a \in \{1, \dots, m\} \times \{1, \dots, n\}],$$

where $1 \leqslant a < c \leqslant m$ and $1 \leqslant b < d \leqslant m$.

Proof. This statement is an immediate consequence of a statement from linear algebra, saying that the rank of a real or complex matrix equals the side length of the largest quadratic submatrix with non-vanishing determinant. ◇

3.4.4 Unfoldings

We have seen above that finite-dimensional bipartite tensor products can be identified with matrix spaces. In the finite-dimensional multipartite case, the image of a tensor $v \in V$ in $\mathbb{K}^N$ can be interpreted as a *multi matrix*. In particular, for all $a \in N$, let v_a be the coordinate of v with respect to the basis vector e_a. Then v is identified with the multi matrix $(v_a)_{a \in N} \in \mathbb{K}^N$. Now, let v be a product vector, that is, $v = v^1 \otimes \cdots \otimes v^r$. Let v^t_k be the coordinate of v^t with respect to the basis vector e_k of $\mathbb{K}^{n_t}$, where $t \in \{1, \ldots, r\}$ and $k \in \{1, \ldots, n_t\}$. Consequently, v can be expanded to

$$v = \sum_{a_1 \cdots a_r \in N} v^1_{a_1} \cdot \ldots \cdot v^r_{a_r} \cdot e_{a_1} \otimes \cdots \otimes e_{a_r},$$

that is, v can be identified with the multi matrix $(v^1_{a_1} \cdot \ldots \cdot v^r_{a_r})_{a_1 \cdots a_r \in N}$.

There are various ways to interpret a finite-dimensional multipartite tensor product also as a finite-dimensional bipartite tensor product by interpreting successively two factors as one. This observation which we adopt from [RS2] (or [Sto]) will help to generalise the last lemma, leading to a characterisation of product vectors by polynomials.

For all $a \in N$ and for all $S = \{s_1, \ldots, s_n\} \subseteq \{1, \ldots, r\}$, where $s_1 < s_2 < \cdots < s_n$, let $a_S := (a_{s_1}, \ldots, a_{s_n})$. This is an indexing tuple in $N_S := \prod_{s \in S} \{1, \ldots, n_s\}$. Let $n_S := \prod_{s \in S} n_s = \#N_S$.

Definition. Let R and C be a complementary partition of the set $\{1, \ldots, r\}$. The map

$$\begin{aligned} \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r} &\to \Big(\bigotimes_{s \in R} \mathbb{K}^{n_s}\Big) \otimes \Big(\bigotimes_{t \in C} \mathbb{K}^{n_t}\Big) \\ &\to \mathbb{K}^{N_R} \otimes \mathbb{K}^{N_C} \quad (\to \mathcal{M}_{n_R, n_C}(\mathbb{K})) \\ e_{a_1} \otimes \cdots \otimes e_{a_r} &\mapsto e_{a_R} \otimes e_{a_C} \end{aligned}$$

is called a R-C-*unfolding* of $\mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$. The image of a tensor under an unfolding is called an *unfolding* of the tensor.

In what follows, we indicate unfoldings either by assigning R and C explicitly or just by merging the corresponding factors by brackets. Of course, the interpretation of R and C as "row indices" and "column indices", respectively, can be interchanged.

A similar version of the following statement can be found in [Lang, Lemma 5.1.5].

Theorem. A tensor $v \in V$ is a product vector if and only if it is a product vector under all R-C-unfoldings, where R and C are a complementary partition of the set $\{1, \ldots, r\}$, with $s < t$ for all $s \in R$, $t \in C$.

Proof. The proof has two parts. We first consider the case $r = 3$. Afterwards, we use induction on r.

Part 1: Let $v \in \mathbb{K}^{n_1} \otimes \mathbb{K}^{n_2} \otimes \mathbb{K}^{n_3}$ with $v \neq 0$ be a product vector for all unfoldings, that is, v is a product vector in $(\mathbb{K}^{n_1} \otimes \mathbb{K}^{n_2}) \otimes \mathbb{K}^{n_3}$ and also in $\mathbb{K}^{n_1} \otimes (\mathbb{K}^{n_2} \otimes \mathbb{K}^{n_3})$. Then there exist two representations

$$\begin{aligned} v &= \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sum_{k=1}^{n_3} \lambda_{i,j}\eta_k \cdot (e_i \otimes e_j) \otimes e_k \\ &= \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sum_{k=1}^{n_3} \tilde{\eta}_i\tilde{\lambda}_{j,k} \cdot e_i \otimes (e_j \otimes e_k) \end{aligned}$$

with coefficients in $\mathbb{K}$. Since $v \neq 0$, there exists $i \in \{1, \dots, n_1\}$ such that $\tilde{\eta}_i \neq 0$. Hence, we obtain

$$\lambda_{i,j}\eta_k = \tilde{\eta}_i\tilde{\lambda}_{j,k} \;\Leftrightarrow\; \tilde{\lambda}_{j,k} \;=\; \frac{\lambda_{i,j}}{\tilde{\eta}_i}\eta_k = \mu_j \cdot \eta_k,$$

since ${}^{\lambda_{i,j}}/_{\tilde{\eta}_i} =: \mu_j$ does not depend on i. This leads to the representation

$$\begin{aligned} v &= \sum_{i=1}^{n_1} \sum_{j=1}^{n_2} \sum_{k=1}^{n_3} \tilde{\eta}_i\mu_j\eta_k \cdot e_i \otimes e_j \otimes e_k \\ &= \left(\sum_{i=1}^{n_1} \tilde{\eta}_i e_i\right) \otimes \left(\sum_{j=1}^{n_2} \mu_j e_j\right) \otimes \left(\sum_{k=1}^{n_3} \eta_k e_k\right). \end{aligned}$$

Hence, v is a product vector.

Part 2: It can be easily verified that the assertion is true for $r = 2$. Now, let us assume that it is true for $r \geqslant 2$ and let $v \in \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r} \otimes \mathbb{K}^{n_{r+1}}$, where $n_{r+1} \in \mathbb{N}$, fulfil the premise. Since v is a product vector under the R-C-unfolding with $R := \{1, \dots, r\}$ and $C := \{r+1\}$, there exists a representation

$$v = x_{1,r} \otimes x_{r+1}$$

where $x_{1,r} \in \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ and $x_{r+1} \in \mathbb{K}^{n_{r+1}}$. Furthermore, it can be easily verified that v is a product vector under all required unfoldings of the tensor product $\mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_{r-1}} \otimes (\mathbb{K}^{n_r} \otimes \mathbb{K}^{n_{r+1}})$. By assumption, the assertion is true for r tensor factors. Thus, this leads to another representation

$$v = x_1 \otimes \cdots \otimes x_{r-1} \otimes x_{r,r+1},$$

where $x_t \in \mathbb{K}^{n_t}$ for all $t \in \{1, \dots, r-1\}$ and $x_{r,r+1} \in \mathbb{K}^{n_r} \otimes \mathbb{K}^{n_{r+1}}$. From the first step, it follows that v is a product vector in $(\mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_{r-1}}) \otimes \mathbb{K}^{n_r} \otimes \mathbb{K}^{n_{r+1}}$. In particular, there exists $x_r \in \mathbb{K}^{n_r}$ such that

$$v = (x_1 \otimes \cdots \otimes x_{r-1}) \otimes x_r \otimes x_{r+1}.$$

It follows that v is a product vector. ◇

3.4.5 PV-Determinants and Determinantal Hibi Relations

According to Theorem 3.4.4, a tensor in V is a product vector if and only if, under all unfoldings, the determinants of all 2×2 submatrices vanish. To make this more explicit, let R, C be a complementary partition of $\{1, \dots, r\}$. We may consider the R-C-unfolding of V as a matrix space, where the rows are indexed by N_R and the columns are indexed by N_C. Now, a 2×2 submatrix M of the image of v under the R-C-unfolding is determined by two row indices $r_1, r_2 \in N_R$ and two column indices $c_1, c_2 \in N_C$, where $r_1 \neq r_2$ and $c_1 \neq c_2$. The row and column indices of M are outlined by the following visualisation:

$$\begin{array}{c|c} (r_1, c_1) & (r_1, c_2) \\ \hline (r_2, c_1) & (r_2, c_2) \end{array}$$

Now, let $a, b, c, d \in N$ such that

$$\begin{aligned} r_1 &= a_R = c_R, & r_2 &= d_R = b_R, \\ c_1 &= a_C = d_C, & c_2 &= c_C = b_C. \end{aligned}$$

That is, on R, the entries of both a and c, and d and b are equal; on C, the entries of both a and d, and c and b are equal. Now, the rows and columns, which determine the submatrix M, can be indexed by a, b, c, and d:

$$\begin{array}{c|c} (r_1, c_1) & (r_1, c_2) \\ \hline (r_2, c_1) & (r_2, c_2) \end{array} = \begin{array}{c|c} a = (a_R, a_C) & c = (a_R, b_C) \\ \hline d = (b_R, a_C) & b = (b_R, b_C) \end{array},$$

where "$a = (a_R, a_C)$" (and so on) means that a equals (a_R, a_C) up to a permutation on the entries which depends on the unfolding.

Now, for any $v \in V$, the determinant of M is given by the value (or its negative) at v of the homogeneous polynomial

$$x_a \cdot x_b - x_c \cdot x_d$$

in $\mathbb{K}[x_a \colon a \in N]$. In this context, we consider the map

$$\begin{aligned} \det : N^4 &\to \mathbb{K}[x_a \colon a \in N] \\ (a, b, c, d) &\mapsto \det_{a,b,c,d} := x_a \cdot x_b - x_c \cdot x_d. \end{aligned}$$

Those polynomials in the range of det, which correspond to the indices of a (possible trivial) submatrix of an unfolding, are covered by the following definition:

Definition. Let $a, b, c, d \in N$. The polynomial $\det_{a,b,c,d}$ is called a *product vector determinant* or *PV-determinant*, if there exists a complementary partition R, C of the set $\{1, \ldots, r\}$ such that

$$\begin{aligned} a_R &= c_R, \quad d_R = b_R && (\textit{row indices}), \\ a_C &= d_C, \quad c_C = b_C && (\textit{column indices}). \end{aligned}$$

The set of all non-zero PV-determinants is denoted by $\mathcal{D}_N$. The ideal in $\mathbb{K}[x_a \colon a \in N]$ which is generated by $\mathcal{D}_N$ is denoted by $\mathcal{I}_N$.

It can be easily verified that a PV-determinant $\det_{a,b,c,d}$ is not equal to the zero polynomial if and only if $a_R \neq b_R$ and $a_C \neq b_C$. In this case, it is homogeneous and has degree two. However, it can be convenient to consider also the cases where it equals zero.

Now, we outline a smaller generating set for the ideal $\mathcal{I}_N$ which will play a major role in Chapter 5.

For all $a, b \in N$, let $a \vee b \in N$ and $a \wedge b \in N$ be defined by

$$\begin{aligned} a \vee b &:= (\max(a_t, b_t))_{t=1,\ldots,r}, \\ a \wedge b &:= (\min(a_t, b_t))_{t=1,\ldots,r}. \end{aligned}$$

Definition. For all $a, b \in N$, we call

$$h_{a,b} := \det_{a,b,a \vee b, a \wedge b}$$

a *determinantal Hibi relation*. Let $\mathcal{H}_N$ be the set of all non-zero determinantal Hibi relations.

Proposition. We have $\mathcal{I}_N = \mathrm{Id}(\mathcal{D}_N) = \mathrm{Id}(\mathcal{H}_N)$. In particular, $\mathcal{H}_N \subseteq \mathcal{D}_N$, and for all $a, b, c, d \in N$ such that $f := \det_{a,b,c,d}$ is a PV-determinant, we have $f = h_{a,b} - h_{c,d}$.

Proof. We first show $\mathcal{H}_N \subseteq \mathcal{D}_N$. Let $a, b \in N$. Let R be the set of all $t \in \{1, \ldots, r\}$ such that $a_t < b_t$ and let C be the set of all $t \in \{1, \ldots, r\}$ such that $a_t \geqslant b_t$. Then R, C is a complementary partition of $\{1, \ldots, r\}$ with the required properies, that is, $h_{a,b}$ is a PV-determinant.

On the other hand, if $f = \det_{a,b,c,d}$ is a PV-determinant, then $a \vee b = c \vee d$ and $a \wedge b = c \wedge d$ by definition. Now, we obtain

$$\begin{aligned} f &= x_a\, x_b - x_c\, x_d \\ &= (x_a\, x_b - x_{a\vee b}\, x_{a\wedge b}) - (x_c\, x_d - x_{a\vee b}\, x_{a\wedge b}) \\ &= (x_a\, x_b - x_{a\vee b}\, x_{a\wedge b}) - (x_c\, x_l - x_{c\vee d}\, x_{c\wedge d}) \\ &= \det_{a,b,a\vee b,a\wedge b} - \det_{c,d,c\vee d,c\wedge d} \\ &= h_{a,b} - h_{c,d}, \end{aligned}$$

that is, $\mathcal{D}_N \subseteq \mathrm{Id}(\mathcal{H}_N)$. ◇

3.4.6 Product Vectors as a Variety (Multipartite Case)

Theorem. *(Determinant Criterion)*
The product vectors equal the set of zeros of the determinantal Hibi relations, that is,

$$\mathcal{P}_V = \mathcal{Z}_{\mathbb{K}}(\mathcal{D}_N) = \mathcal{Z}_{\mathbb{K}}(\mathcal{H}_N) = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_N).$$

Proof. According to Theorem 3.4.4, a tensor $v \in V$ is a product vector if and only if, under all unfoldings, the determinants of all 2×2 submatrices vanish (that is, they have rank zero or rank one). As stated above, this is equivalent to the property that v vanishes on the corresponding non-zero PV-determinants. Hence, v is a product vector if and only if it is contained in the set of zeros of all non-zero PV-determinants. ◇

Remark. On the one hand, it can be helpful if a generating set of an ideal describing the product vectors such as $\mathcal{H}_N$ is as small as possible. On the other hand, it can also be helpful to consider the vanishing ideal of the product vectors, which is the largest set. Hence, depending on the situation, there are many candidates amongst all sets (or ideals) G with $\mathcal{Z}_{\mathbb{K}}(G) = \mathcal{P}_V$ to choose from, such as $\mathcal{H}_N$, $\mathcal{D}_N$, $\mathcal{I}_N$. Further candidates are the set of all PV-determinants which come from a complementary partition R, C with $s < t$ for all $s \in R$, $t \in C$, (see Theorem 3.4.4) and, another candidate, the set which is proposed in

[Lang, Satz 5.3.5]. Concerning the vanishing ideal of $\mathcal{P}_V$ we refer to Corollary 5.5.3.I.

3.4.7 Unit Product Vectors as a Variety

The Hilbert-Schmidt norm on V equals the Euclidean norm. In the case where $\mathbb{K} = \mathbb{R}$, the Euclidean unit sphere is a real affine variety, see Subsection 2.2.6. This variety is induced by the *norming polynomial* which describes the squared norm of a tensor:

$$u_N := \sum_{a \in N} x_a^2 - 1,$$

that is, $\mathcal{Z}_{\mathbb{R}}(u_N) = (\mathbb{R}^N)_1$. Let $\mathcal{N}_N := \{u_N\}$ and let $\mathcal{J}_N$ be the ideal generated by $\mathcal{D}_N$ (or $\mathcal{H}_N$) and $\mathcal{N}_N$.

Theorem. *(Criterion for Unit Product Vectors)*
If $\mathbb{K} = \mathbb{R}$, then the unit product vectors equal the set of zeros of the determinantal Hibi relations and the norming polynomial, that is,

$$\mathcal{E}_V = \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_N \cup \mathcal{N}_N) = \mathcal{Z}_{\mathbb{R}}(\mathcal{J}_N).$$

Consequently, we have $\mathcal{B}_{1,\pi} = \mathrm{co}(\mathcal{Z}_{\mathbb{R}}(\mathcal{J}_N))$.

Proof. The set $\mathcal{E}_V$ of all unit product vectors equals the intersection of the product vectors with the Hilbert-Schmidt unit sphere. From Proposition 2.1.1 (iii) and the Determinant Criterion Theorem 3.4.6, we obtain $\mathcal{E}_V = \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_N) \cap \mathcal{Z}_{\mathbb{R}}(\mathcal{N}_N) = \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_N \cup \mathcal{N}_N) = \mathcal{Z}_{\mathbb{R}}(\mathcal{J}_N)$. ◇

3.5 Complex Unit Product Vectors as a Variety

The aim of this section is to show that the unit product vectors of a finite-dimensional complex tensor product can be considered as a real variety, see Theorem 3.5.3.

Just as defined in the previous sections, let $r, n_1, \dots, n_r \geqslant 2$ and let $N = \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$.

Let $V_{\mathbb{K}} := \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ and $N_{\mathbb{C}} := N \times \{1, 2\}$.

3.5.1 Complex Tensor Products as Affine Spaces

As outlined in Subsection 3.4.1, $V_{\mathbb{C}}$ can be identified with the complex affine space $\mathbb{C}^N$. According to Subsection 2.2.1, $\mathbb{C}^N$ can be identified with the real affine space $\mathbb{R}^{N_{\mathbb{C}}}$:

$$\begin{aligned} \imath\colon \quad \mathbb{C}^N &\to \mathbb{R}^{N_{\mathbb{C}}} \\ e_a &\mapsto e_{a,1}, \\ \mathrm{i}\, e_a &\mapsto e_{a,2}. \end{aligned}$$

For each $f \in \mathbb{C}[x_a \colon a \in N]$, the real and the imaginary part, $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$, are elements of $\mathbb{R}[x_a \colon a \in N_{\mathbb{C}}]$.

3.5.2 Product Vectors as a Real Variety

In the last section, we have shown that the set of all product vectors can be expressed as a real or a complex affine variety, induced by $\mathcal{H}_N$. In this respect, let $N_{\mathbb{C}} := N \times \{1,2\}$ and $\mathcal{H}_{N_{\mathbb{C}}} := \mathrm{Re}(\mathcal{H}_N) \cup \mathrm{Im}(\mathcal{H}_N)$, which are polynomials in $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in N]$. The following theorem is adapted from [Voi, Satz 3.1.4]. We will encounter it again in Theorem 5.1.3.

Theorem. *(Determinant Criterion)*
In the case where $\mathbb{K} = \mathbb{C}$, the product vectors can be considered as a real variety which is induced by the real and imaginary parts of the determinantal Hibi relations:

$$\imath(\mathcal{P}_{V_{\mathbb{C}}}) = \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{N_{\mathbb{C}}}) = \mathcal{Z}_{\mathbb{R}}(\imath(\mathcal{I}_N)).$$

Proof. The Determinant Criterion Theorem 3.4.6 says that $\mathcal{P}_{V_{\mathbb{C}}} = \mathcal{Z}_{\mathbb{C}}(\mathcal{H}_N)$. Theorem 2.2.5 implies that the decomplexification $\imath(\mathcal{P}_{V_{\mathbb{C}}})$ is a real variety which is induced by $\imath(\mathcal{I}_N)$. Using Proposition 2.2.4, the ideal $\imath(\mathcal{I}_N)$ is generated by $\mathcal{H}_{N_{\mathbb{C}}}$. ◇

How do the real and the imaginary parts look like? Let $a, b, c, d \in N$ and $f := \det_{a,b,c,d} = x_a\, x_b - x_c\, x_d$, then a short calculation shows that the real and the imaginary part of f are given by

$$\begin{aligned} \mathrm{Re}(f) &= (x_{a,1}\, x_{b,1} - x_{c,1}\, x_{d,1}) - (x_{a,2}\, x_{b,2} - x_{c,2}\, x_{d,2}), \\ \mathrm{Im}(f) &= (x_{a,1}\, x_{b,2} - x_{c,1}\, x_{d,2}) + (x_{a,2}\, x_{b,1} - x_{c,2}\, x_{d,1}). \end{aligned}$$

3.5.3 Unit Product Vectors as a Real Variety

We have seen in Subsection 2.2.6 that the decomplexification of the complex Euclidean unit sphere is a real variety. This variety is induced by the *complex norming polynomial* $u_{N_\mathbb{C}} := \sum_{a \in N_\mathbb{C}} x_a^2 - 1$. Let $\mathcal{N}_{N_\mathbb{C}} := \{u_{N_\mathbb{C}}\}$ and let $\mathcal{J}_{N,\mathbb{C}}$ be the ideal which is generated by $\mathcal{H}_{N_\mathbb{C}} \cup \mathcal{N}_{N_\mathbb{C}}$. The following theorem is adapted from [Voi, Proposition 3.1.a]. We will encounter it again in Theorem 5.1.4.

Theorem. *(Criterion for Unit Product Vectors)*
If $\mathbb{K} = \mathbb{C}$, then the unit product vectors can be considered as a real variety which is induced by the real and imaginary parts of the determinantal Hibi relations and the complex norming polynomial:

$$\imath(\mathcal{E}_{V_\mathbb{C}}) = \mathcal{Z}_\mathbb{R}(\mathcal{H}_{N_\mathbb{C}} \cup \mathcal{N}_{N_\mathbb{C}}) = \mathcal{Z}_\mathbb{R}(\mathcal{J}_{N,\mathbb{C}}).$$

Consequently, we have $\imath(\mathcal{B}_{1,\pi}) = \mathrm{co}(\mathcal{Z}_\mathbb{R}(\mathcal{J}_{N,\mathbb{C}}))$.

Proof. Proposition 2.1.1 (iii) and the Determinant Criterion Theorem 3.5.2 yield

$$\begin{aligned} \imath(\mathcal{E}_{V_\mathbb{C}}) &= \imath(\mathcal{P}_{V_\mathbb{C}} \cap (V_\mathbb{C})_1) = \imath(\mathcal{P}_{V_\mathbb{C}}) \cap \imath((V_\mathbb{C})_1) \\ &= \mathcal{Z}_\mathbb{R}(\mathcal{H}_{N_\mathbb{C}}) \cap \mathcal{Z}_\mathbb{R}(u_{N_\mathbb{C}}) = \mathcal{Z}_\mathbb{R}(\mathcal{H}_{N_\mathbb{C}} \cup \mathcal{N}_{N_\mathbb{C}}) \\ &= \mathcal{Z}_\mathbb{R}(\mathcal{J}_{N,\mathbb{C}}). \end{aligned}$$

Since $\imath$ preserves convexity, we obtain $\imath(\mathcal{B}_{1,\pi}) = \mathrm{co}(\mathcal{Z}_\mathbb{R}(\mathcal{J}_{N,\mathbb{C}}))$. ◇

3.5.4 Comparison Real and Complex

Here, we show with the aid of theta bodies that the inner radius of the projective unit ball in a complex tensor product can be compared with the inner radius of the projective unit ball in a real tensor product.

Let $V_{\mathbb{R},2} := \mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r} \otimes \mathbb{R}^2$. According to Subsection 3.5.1, there exists a real-linear embedding $V_\mathbb{R} \to V_\mathbb{C}$ which maps e_a, $a \in N$, to e_a and a real-linear isomorphism $\imath \colon V_\mathbb{C} \to V_{\mathbb{R},2}$:

$$\begin{tikzcd} V_\mathbb{R} & V_\mathbb{C} & V_{\mathbb{R},2} \\ \mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r} \arrow[r, hook] & \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_r} \arrow[r, leftrightarrow] & \mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r} \otimes \mathbb{R}^2 \\ e_a \arrow[r, mapsto] & e_a \arrow[r, leftrightarrow] & e_{a,1} \\ & ie_a \arrow[r, leftrightarrow] & e_{a,2}. \end{tikzcd}$$

The projective unit balls in $V_{\mathbb{C}}$ and $V_{\mathbb{R},2}$ are denoted by $\mathcal{B}_{1,\pi}(V_{\mathbb{C}})$ and $\mathcal{B}_{1,\pi}(V_{\mathbb{R},2})$, respectively. We obtain the following inequality for the inner radii of those sets:

Proposition. We have $r(\mathcal{B}_{1,\pi}(V_{\mathbb{R},2})) \leqslant r(\mathcal{B}_{1,\pi}(V_{\mathbb{C}}))$.

Proof. It can be easily verified that $\mathcal{J}_{N,\mathbb{C}} \subseteq \mathcal{J}_{N\times\{1,2\}}$. Hence, for all $k \in \mathbb{N}$, it follows that the k^{th} theta body of $\mathcal{J}_{N\times\{1,2\}}$ is contained in the k^{th} theta body of $\mathcal{J}_{N,\mathbb{C}}$. Now, the statement follows since the theta bodies converge against the unit ball of the corresponding projective norm, see Theorem 2.5.5. ◇

The question arises whether it is possible to compare the projective unit balls of $V_{\mathbb{R}}$ and $V_{\mathbb{C}}$, but this seems to be more difficult at this stage (however, we recall the discussions in Section 3.3).

3.5.5 Discussion

In summary, the approach of [Voi] is based on a real-linear identification of the complex tensor product, regarded as a complex affine space, with a real affine space. Theorem 2.2.5 says that a complex variety (such as the product vectors according to the Determinant Criterion Theorem 3.5.2) can always be identified uniquely with a real variety. Also the decomplexification of the complex Euclidean unit sphere is a real variety. Putting both together, the unit product vectors are a real variety.

It is worth to mention that also other approaches could be conceivable. For instance, one could think about transferring the algebraic concept of theta bodies to complex settings (which is rather difficult, since it is based on the fact that sums of squares are positive) or not to consider the Euclidean unit vectors, which are no variety in a complex setting (which is also difficult, since it is essential to reproduce the projective unit ball). Main advantages of our approach are that the decomplexification preserves convexity, that is, the terminology based on convex geometry can be preserved one-to-one, and that the Euclidean unit sphere is a real variety. See also the discussions in [Voi]. The question whether there are alternative approaches arose since the treatment of the decomplexified ideal seems to be rather difficult; indeed, many properties of the determinantal Hibi relations cannot be transferred. We will encounter some indications in Chapter 5 (in connection with Gröbner bases and with vector space bases) and in Chapter 6 (in connection with the first theta body). Nevertheless, we have seen above that complex tensor products behave different in comparison with real tensor products, see, for example, Proposition 3.3.3. No matter which approach is used, it has to encounter this difference. With our approach, the difference is "condensed" in the structure of the decomplexified ideal.

By the way, to use the concept of theta bodies, it is an advantage (or just "luck") that the algebraic description of the Euclidean unit sphere is even easier in a real space than in a complex space.

3.6 Applications of the Projective Norm

In this section we first discuss some reasons why the computation of the projective norm in multipartite tensor products is rather difficult.

Moreover, we outline the role of the projective norm in quantum entanglement (which is our motivation) and in signal processing. We also discuss the advantages that an approximation by theta bodies could have. It is interesting to note that there are two applications of the approximation in both areas of research: The starting point of all applications is that the computation of the projective norm is rather difficult. Thus, in the first place, theta bodies can help to improve the understanding of the projective norm. Secondly, theta bodies can also be used to replace the projective norm in the particular setting. In the context of these applications, we formulate several questions in relation to theta bodies. Most of these questions can be adressed in this thesis.

3.6.1 The Computation of the Projective Norm

So far, we have seen that the Hilbert-Schmidt norm of a tensor can be easily obtained and the projective norm on a bipartite tensor product corresponds to the Schmidt decomposition.

In Section 3.3, we have encountered some approaches to compute the projective norm in multipartite tensor products. We have seen that it can be possible to compute the projective norm of a given tensor or of a family of tensors. It is also possible to obtain some information about the geometry of the unit ball of the projective norm. However, in the multipartite case, a general approach seems to be difficult.

There are several hints in the literature sketching the problem. For example, one could have the idea to obtain the projective norm of a tensor from the projective norms of its unfoldings, but this does not work in general. This shows an illustrative example from [RS2]. Indeed, the algorithmic computation of the tensor rank is in general NP-hard, and thus, the same is true for a decomposition which gives the projective norm, see [HL], [FL] or [Sto].

Further approaches to obtain the projective norm in special cases or to provide bounds on it can be found amongst others in [AS], [Arv], [Sok] (approximations in the complex case), [Der, Theorems 1.10 - 1.14] (complex case) or in [FL] (symmetric tensors).

In this thesis, we focus on the projective norm maximisation.

Remark. In general, the rank of a tensor cannot be led back uniquely to the rank of its unfoldings. In this respect, there are other notions for a "tensor rank" which base on the ranks of the unfoldings. For example, the *Tucker rank* t of a tensor $v \in \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ is given by $t = (t_1, \dots, t_r)$, where t_k is the rank of v under the unfolding for $R = \{k\}$ and $C = \{1, \dots, r\} \backslash \{k\}$, for all $k \in \{1, \dots, r\}$. In contrast, the *tensor train rank*, or *TT rank*, is given by $s = (s_1, \dots, s_{r-1})$, where s_k is the rank of v under the unfolding for $R = \{1, \dots, k\}$ and $C = \{k+1, \dots, r\}$.

3.6.2 The Projective Norm in Quantum Entanglement

Let V be a finite-dimensional complex tensor product.

We will see below in Chapter 9 that a pure state (as a linear operator on V) corresponds to a unit vector in V. It is also outlined there that a pure state (that is, a unit vector) $v \in V$ is separable, if and only if it is a unit product vector.

The projective norm identifies (pure) separable states, that is, given a unit vector $v \in V$, then v is separable if and only if v has projective norm 1. This is due to the fact that the extreme points of the projective unit ball are the unit product vectors. Moreover, those unit vectors which maximise the projective norm maximise also the Euclidean distance to the unit product vectors, see [Arv, Theorem 3.2].

In summary, the projective norm fulfils the following two properties, which suggests to consider it as an entanglement measure on pure states, see [Arv]:

(i) The projective norm solves the separability problem for pure states.
(ii) The projective norm maximisation helps to identify maximally entangled pure states.

In this respect, any cross norm on V between the projective norm and the Hilbert-Schmidt norm could be considered as a candidate for an entanglement measure, provided it satisfies the two properties.

At this stage, we first note that the separability problem can be solved easily for pure states with the Determinant Criterion Theorem 3.4.6. We also note that there are also other entanglement measures based on the projective norm, see, for instance, [Rud].

In this thesis, we want to use the theta body method mainly as a tool to determine the projective norm. Here, of course, it is important that a theta body is close to the projective unit ball.

Another interesting point of view is to consider theta bodies as new and independent entanglement measures in addition to the projective norm and other measures. However, a theta body should induce a cross norm which is able to solve the separability problem for pure states.

Therefore, a discussion whether theta bodies are suitable for both applications could include the following aspects:

(1) How close are the theta bodies to the projective unit ball?
(2) How accessible are the theta bodies?
(3) Does a theta body induce a cross norm?
(4) Does a theta body lie in the Hilbert-Schmidt unit ball?
(5) Does a theta body respect the symmetries of the unit product vectors?
(6) Can a theta body identify pure separable states?

The following chapters address questions (1) and (2). We will also discuss questions (3), (4) and (5). Question (6) still remains open.

3.6.3 The Projective Norm in Signal Processing

Compressive sensing is a technique in signal processing for the recovery of sparse signals from few measurements in a comparatively large signal space. The signal space is assumed to be a finite-dimensional real vector space and the measurements are affine-linear equations. The idea is that the signal is assumed to be sparse, so only a few measurements are necessary for a recovery.

Sparsity can appear in different contexts. For example, a large "sparsity" could mean that the weight of the vector, that is, the number of non-zero entries, is as small as possible. In this respect, the *affine sparse minimization problem* or the *sparse vector recovery* minimises the weight over the solutions of a system of linear equations. Alternatively, the 1-norm could be minimised. In some applications such as machine learning, video compression, or seismology, the signal space equals a finite-dimensional tensor product, and the term "sparsity" refers to a small rank of the tensor, leading to the subjects *low rank matrix recovery* and *low rank tensor recovery* or *tensor completion* to recover tensors of low rank from incomplete linear information, see [RSS]. An illustrative example for low rank matrix recovery is the *Netflix problem* for the prediction of user ratings for movies from a small number of user-provided ratings, see [PS] and [PS1]. Assuming that the user ratings are linearly correlated in some sense, it suggests to concentrate on solutions with low rank, for example, with rank 1:

		Movie		
		A	B	C
User	1	1	?	2
	2	?	9	6
	3	?	?	8

$\rightsquigarrow$

		Movie		
		A	B	C
User	1	1	3	2
	2	3	9	6
	3	4	12	8

The search for more tractable problems lead to the minimisation of the nuclear norm, as a a generalisation of the 1-norm minimisation of vectors and as an alternative to the rank minimisation. It is referred to as the *nuclear norm minimization for low-rank tensor recovery*.

Since the rank and the nuclear norm of a tensor is not easy to compute, the approach in [Sto] replaces the nuclear norm with a so-called tensor theta norm which corresponds to a theta body. See also [RS2] and [RS1].

Convex relaxations with sums of squares are used widely in compressive sensing, see [BS] or [PS]. Some authors such as [BM] or [NW] use *Lasserre's relaxation* which is very close to the theta body method. It is interesting that there are also relations to quantum entanglement, see [BK].

Chapter 4

DISTRIBUTIVE LATTICES

This chapter begins with a brief introduction to the terminology of lattice theory in Section 4.1 and to distributive lattices in Section 4.2 based on standard textbooks like [Bir] or [BD]. The notions are used in Chapter 5 and in Chapter 6 to generalise the projective unit ball.

In Section 4.2 we introduce examples of distributive lattices which are useful for the discussions in the following chapters. For instance, we will see that product lattices can be regarded as a generalisation of indexing sets, the lattice D_{18} helps to illustrate the notions in Section 5.2 and boolean lattices can be used in Section 6.1 to show that theta bodies induce norms. We also introduce the notion *pentagonal lattice* for the discussion in Section 5.4. The section ends with a notion related to boolean sublattices of distributive lattices which will be important for one of the main results Theorem 6.3.6.

4.1 Lattices

In this section, we introduce some aspects of lattice theory.

4.1.1 Posets

Definition. Let $(P, \leqslant)$ be a partially ordered set, briefly *poset*, that is, it is reflexive, antisymmetric and transitive. Let $a, b \in P$. If $a \leqslant b$ or $b \leqslant a$, then a and b are called *comparable*. If $a < b$ and if $a < c \leqslant b$ implies $b = c$ for all $c \in P$, then a is *covered* by b. A poset which is also a total order, that is, all elements are comparable, is called a *chain*. The *length* of a finite chain with n elements is $n - 1$. The *length* of P is defined as the least upper bound of the lengths of the chains in P (which is possibly infinite).

If P is finite, one can obtain a graphical representation, called *Hasse diagram*, by drawing a representative for each element of P under the following condition: Whenever a is covered by b for $a, b \in P$, ensure that b is placed higher than a, and draw a straight line segment from a to b. A Hasse diagram can be realised by a finite directed graph.

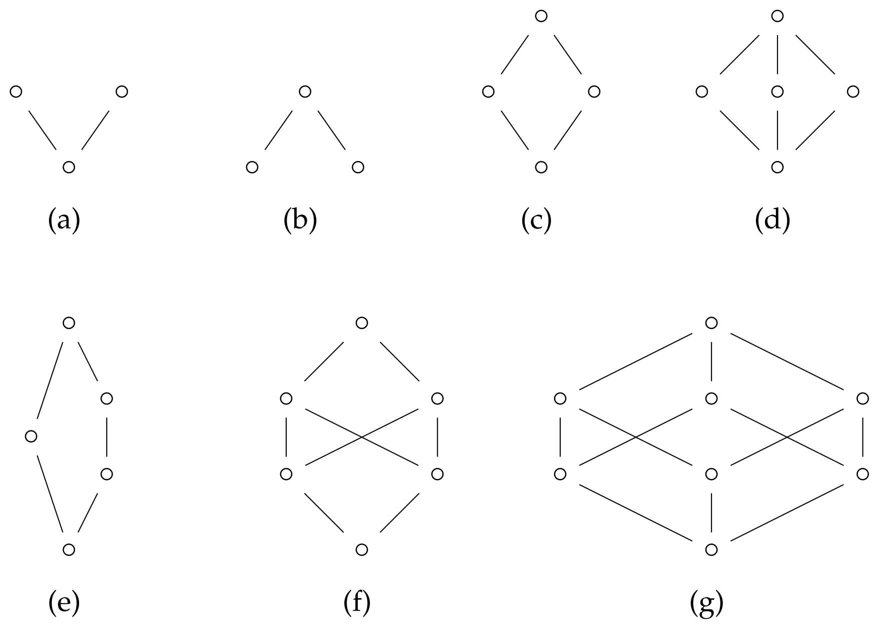


Figure 4.1: Some examples for posets.

Example. Figure 4.1 shows Hasse diagrams of some finite posets. Poset (d) is called a *diamond* and poset (e) is called a *pentagon*, see [Gra]. We say that poset (c) is a *rhomb*.

4.1.2 Lattices

Let $(P, \leqslant)$ be a partially ordered set and let $A \subseteq P$.

An element $l \in P$ is called a *lower bound* for A if $l \leqslant a$ for all $a \in A$. A lower bound $l \in P$ is called the *greatest lower bound* for A if $l' \leqslant l$ for all lower bounds $l' \in P$ for A.

An element $u \in P$ is called an *upper bound* for A if $a \leqslant u$ for all $a \in A$. An upper bound $u \in P$ is called the *least upper bound* for A if $u \leqslant u'$ for all upper bounds $u' \in P$ for A.

Definition. A partially ordered set L is called a *meet-semilattice* if for any two elements $a, b \in L$, there exists a greatest lower bound $a \wedge b$, called *meet*. It is called a *join-semilattice* if for any two elements $a, b \in L$, there exists a least upper bound $a \vee b$, called *join*. It is called a *lattice* if it is both a meet-semilattice and a join-semilattice.

The meet is also called *infimum* and the join is also called *supremum*. A subset S of a lattice L is called a *sublattice* of L if for each two elements in S their meet and join are also contained in S.

The greatest lower bound $\perp$ of a lattice, if existent, is called *bottom*. The least upper bound $\top$, if existent, is called *top*.

A lattice is called *complete* if each subset possesses a greatest lower bound and a least upper bound. In this case, it possesses a bottom and a top. Any finite lattice is complete.

Example.

(i) The posets (a) and (b) in Figure 4.1 are no lattices, since there exists no upper bound (or no lower bound) of the two elements which are on the same "level". Poset (f) is no lattice as well, since each two elements which are on the same "level" either have no meet or no join. The rhomb (poset (c)) is a lattice. Posets (d), (e) and (g) are lattices.

(ii) Let S be a set. The power set $\mathfrak{P}(S)$ is a lattice with the set inclusion. The meet operation is $\cap$ and the join operation is $\cup$.

(iii) Let R be a ring. The set of all ideals of R, together with the set inclusion, is a lattice with meet $I \cap J$ and join $I + J$, for all ideals I, J of R.

(iv) The partitions of a set, ordered by refinement, are a lattice.

Each sublattice of a lattice L of the form (c) from Figure 4.1 is called a *rhomb* of L. Rhombs are the "smallest" sublattices which cannot be ordered totally.

4.1.3 Algebraic Definition of a Lattice

Definition. A set L equipped with two binary operations $\wedge$ and $\vee$ is called a *general lattice*, written $(L, \wedge, \vee)$, if for all $a, b, c \in L$, the following identities hold:

L1: $a \wedge a = a, \quad a \vee a = a,$ *(Idempotence)*

L2: $a \wedge b = b \wedge a, \quad a \vee b = b \vee a,$ *(Commutativity)*

L3: $a \wedge (b \wedge c) = (a \wedge b) \wedge c, \quad a \vee (b \vee c) = (a \vee b) \vee c$ *(Associativity)*

L4: $a \wedge (a \vee b) = a \vee (a \wedge b) = a.$ *(Law of Absorption)*

Lattices can be characterised by their algebraic properties, namely, by the identities L1 - L4, see [Bir, Theorem 8, Chapter I]:

Proposition. A lattice L with meet $\wedge$ and join $\vee$ is a general lattice. On the other hand, a general lattice $(L, \wedge, \vee)$ with the relation $a \leqslant b$, if and only if $a = a \wedge b$ (or, equivalently, $b = a \vee b$), is a lattice.

Proof. The first statement can be easily verified. The proof of the second statement requires to show that the meet and join operations coming from $\leqslant$ equal $\wedge$ and $\vee$, respectively. ◇

4.1.4 Morphisms between Lattices

Definition. Let L and M be two lattices. A function $L \to M$ is called *isotone* if it preserves the order. If it respects meet and join, it is called a *morphism*.

It can be easily verified that a morphism is isotone. The converse is not true in general. For example, there exists an isotone function from the lattice (c) in Figure 4.1 to a chain with length 3.

4.2 Distributive Lattices

In this section we concentrate on distributive lattices. They can be regarded as a generalisation of the indexing tuples. Finally, we introduce pentagonal lattices and we investigate boolean sublattices of distributive lattices.

4.2.1 Distributive Lattices

Definition. A lattice L is called *distributive* if for all $a, b, c \in L$, it satisfies

$$\text{L6:}\quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c), \qquad \textit{(Distributivity)}$$
$$\text{L7:}\quad a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c).$$

It can be shown that if L6 is true (for all $a, b, c \in L$), then also L7, and vice versa, see [Bir, Theorem 9, Chapter I].

Proposition. In a distributive lattice L, for all $a, b, c \in L$ with $a \leqslant c$, we have

$$\text{M:}\quad a \vee (b \wedge c) = (a \vee b) \wedge c. \qquad \textit{(Modularity)}$$

Proof. This statement follows immediately from L7. ◇

Theorem. A lattice L is distributive if and only if it satisfies one of the following conditions:

(a) It fulfils the *self-dual median law*:

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$$

for all $a, b, c \in L$.

(b) Neither the diamond nor the pentagon is a sublattice of L.

(c) For all $a, b, c \in L$, the equations $a \wedge c = b \wedge c$ and $a \vee c = b \vee c$ imply $a = b$.

Proof. See [Bir]: For (a) Theorem 8 in Chapter II, for (b) Theorem 12 in Chapter I and Theorem 13 in Chapter II, and for (c) Theorem 13 in Chapter II. ◇

Example. The lattices (c) and (g) in Figure 4.1 are distributive and the lattices (d) and (e) are not distributive.

4.2.2 Boolean Lattices

Let L be a lattice with bottom $\bot$ and with top $\top$. An element $a \in L$ has a *complement* if there exists $b \in L$ with $a \wedge b = \bot$ and $a \vee b = \top$. In this case, a is called *complemented*. Depending on the context we write $b =: a'$. If all elements have complements, then L is called *complemented*.

Definition. A complemented distributive lattice is called a *boolean lattice*.

Theorem 4.2.1 implies that complements are unique in a boolean lattice.

Example.
(i) Let S be an arbitrary set. The power set $\mathfrak{P}(S)$ is a boolean lattice with the set inclusion.
(ii) The lattices (c) and (g) in Figure 4.1 are boolean.
(iii) The open and closed subsets of a topological space (with the set inclusion) are a boolean lattice.

One can show that there are no more boolean lattices of finite length than those presented in the last example:

Theorem. Each Boolean lattice of finite length n is isomorphic to the lattice $(\mathfrak{P}(\{1, \ldots, n\}), \cap, \cup)$. In particular, there is just one Boolean lattice of length n.

Proof. See [Bir, Theorem 4, Chapter III]. ◇

Definition. A *ring of sets* is a family R of subsets of a set such that with any two sets in R, also their intersection and their union is contained in R.

Theorem. Any finite distributive lattice is isomorphic to a ring of sets.

Proof. See [Bir, Theorem 3, Chapter III]. ◇

Hence, any finite distributive lattice is a sublattice of a boolean lattice.

4.2.3 Product Lattices

On the cartesian product $L \times M$ of two lattices $(L, \leqslant_L)$ and $(M, \leqslant_M)$, a partial order $\leqslant$ is defined by $(l, m) \leqslant (l', m')$ if and only if $l \leqslant_L l'$ and $m \leqslant_M m'$, for all $l, l' \in L$ and for all $m, m' \in M$. The poset $(L \times M, \leqslant)$ is a lattice and is called the *direct product* of $(L, \leqslant_L)$ and $(M, \leqslant_M)$.

For example, for any $r \in \mathbb{N}$, the r-fold direct product of $(\mathbb{N}, \leqslant)$ is a lattice. Also, the r-fold direct product of $(\mathbb{R}, \leqslant)$ is a lattice, which is called a *(real) vector lattice*, see [EFHN].

Let $n_1, \dots, n_r \in \mathbb{N}$. Through our focus on finite-dimensional tensor products, we consider the set

$$N := \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$$

which is equal to a set of indexing tuples, see Subsection 3.4.2. This set can be regarded as the direct product of r finite chains, that is, as a sublattice of $\mathbb{N}^r$. The meet and join of $a, b \in N$ are given by

$$\begin{aligned} a \wedge b &:= (\min(a_k, b_k))_{k=1}^r, \\ a \vee b &:= (\max(a_k, b_k))_{k=1}^r. \end{aligned}$$

It can be easily verified that N is distributive. In the case where $r = 2$, it is called a *uniquely relatively complemented* lattice (or *URC-lattice*), see [Qur, Proposition 1.7]. A URC-lattice is an example for a *planar* distributive lattice.

Any boolean lattice of length r is isomorphic to $\{1, 2\}^r$.

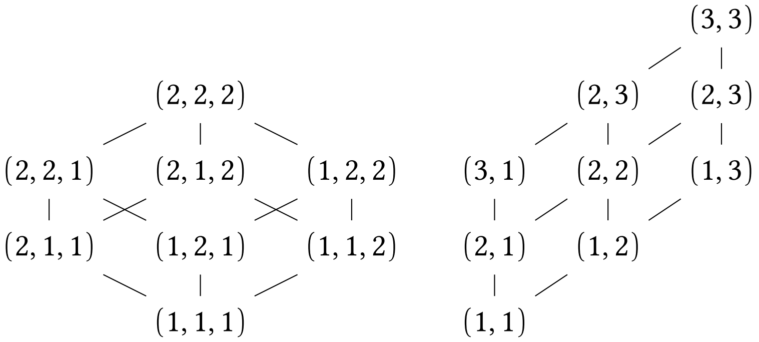


Figure 4.2: Two product lattices.

Example. Figure 4.2 shows the Hasse diagrams for the boolean lattice $\{1, 2\}^3$ and for the planar lattice $\{1, 2, 3\}^2$.

4.2.4 Distributive Lattices Generated by Three Elements

Figure 4.3 shows the lattice D_{18}. The top is given by $l := a \vee b \vee c$ and the bottom is given by $s := a \wedge b \wedge c$. The element

$$m := (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$$

is called the *median* of a, b and c. Each of the three elements l, s, m has the property that it is comparable with all elements of D_{18}.

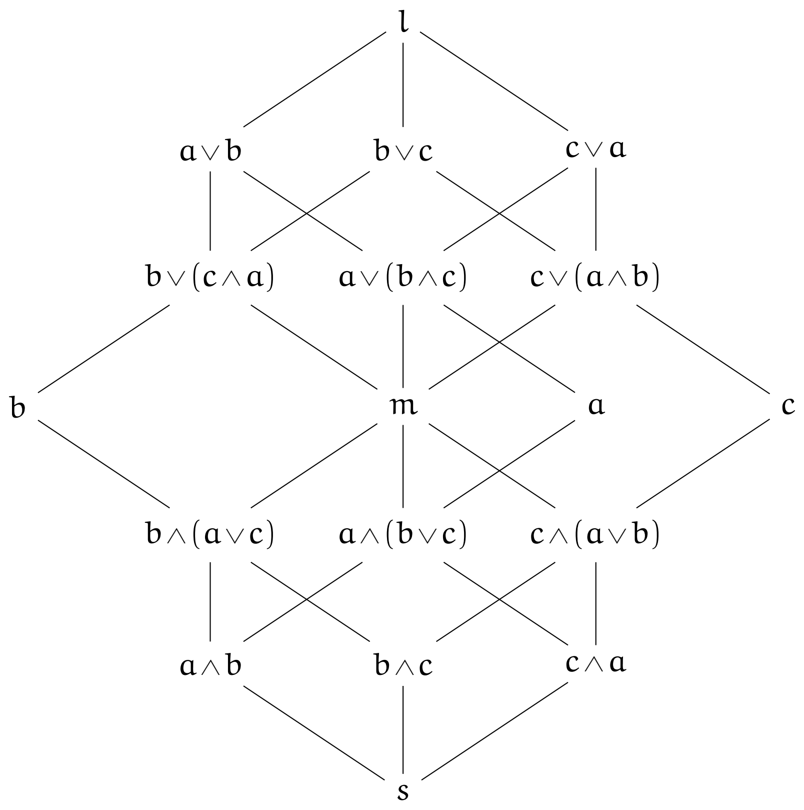


Figure 4.3: The lattice D_{18}.

Now, let L be a distributive lattice and let $a_0, b_0, c_0 \in L$. One can show that there exists a morphism $f\colon D_{18} \to L$ such that $f(a) = a_0$, $f(b) = b_0$ and $f(c) = c_0$, see [Bir, Chapter II, Theorem 9]. In this respect, D_{18} can be regarded as the "largest" distributive lattice which can be "generated" by three elements.

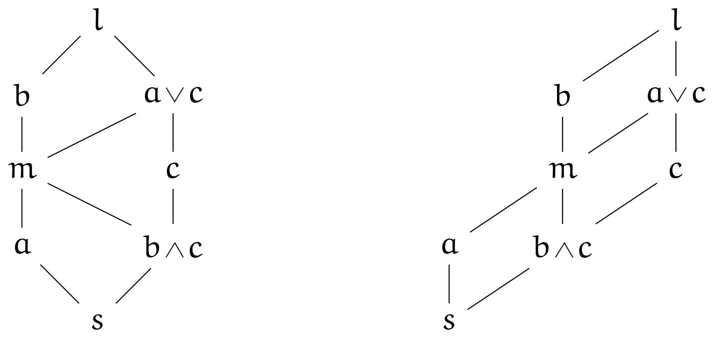
4.2.5 Pentagonal Lattices

For some purposes D_{18} does not seem to be "simple" enough to serve as an example, so we developed the following notion as a source for examples which will be used mainly in Proposition 5.4.3.

Definition. A lattice L is called *pentagonal*, if there exist three distinct elements $a_0, b_0, c_0 \in L$ such that $a_0 < b_0$, a_0 and c_0 are not comparable, and b_0 and c_0 are not comparable.

The pentagon is a pentagonal lattice. Hoewever, a pentagonal distributive lattice cannot contain the pentagon as a sublattice according to Theorem 4.2.1. The rhomb $\{1, 2\}^2$ is not pentagonal.

Example. In this example we consider the pentagonal distributive lattice in Figure 4.4 (a) which we denote by D_1. The labels of the elements in the Hasse diagram of D_1 are obtained by choosing an appropriate morphism $D_{18} \to D_1$. From [Gra, page 23], it follows that D_1 is the "largest" distributive lattice which can be generated by three elements a, b and c with $a < b$. It can be identified with a sublattice of $\{1, 2, 3\}^2$. This can be seen in Figure 4.4 (b).

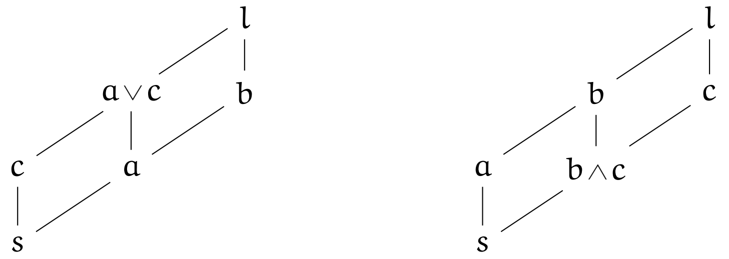


(a) (b)

Figure 4.4: The lattice D_1.

Further examples are the pentagonal lattices D_2 and D_3 in Figure 4.5 which are each the image of a morphism from D_1.

Now, let $L = \{1, \ldots, n\}^r$ for $n, r \geqslant 2$. The last examples show that L is pentagonal, if and only if $n \geqslant 3$ or $r \geqslant 3$.



(a) The lattice D_2.

(b) The lattice D_3.

Figure 4.5: The lattices D_2 and D_3.

4.2.6 Boolean Sublattices of Distributive Lattices

We now introduce a notion which seems to be useful for dealing with the Hibi relations in Chapter 5.

Let L be a distributive lattice. For any $a, b \in L$, let

$$\begin{aligned} L(a,b) := \{c \in L\colon\ & \text{there exists } d \in L \text{ with} \\ & a \wedge b = c \wedge d \ \text{ and } \ a \vee b = c \vee d\}. \end{aligned}$$

Proposition. $L(a, b)$ is the largest boolean sublattice of L such that:

(i) $a \wedge b$ equals the bottom and $a \vee b$ equals the top.

(ii) b is the complement of a.

Proof. *Statement 1:* $L(a, b)$ is a sublattice of L.
Proof: Let $g \in L$. By definition, $g \in L(a, b)$ if and only if there exists $g' \in L(a, b)$ such that $g \wedge g' = a \wedge b$ and $g \vee g' = a \vee b$. Theorem 4.2.1 implies that g' is uniquely defined. Let $c, d \in L(a, b)$. In the following, we show that $e := c \wedge d \in L(a, b)$ and $f := c \vee d \in L(a, b)$.

Statement 1.1: $e' = c' \vee d'$, and, hence, $e \in L(a, b)$.
Proof: We obtain

$$\begin{aligned} e \wedge (c' \vee d') &= (c \wedge d) \wedge (c' \vee d') \\ &= (c \wedge d \wedge c') \vee (c \wedge d \wedge d') \\ &= (a \wedge b) \vee (a \wedge b) = a \wedge b, \\ e \vee (c' \vee d') &= (c \wedge d) \vee (c' \vee d') \\ &= (c \vee c' \vee d') \wedge (d \vee c' \vee d') \\ &= (a \vee b) \wedge (a \vee b) = a \vee b. \end{aligned}$$

Statement 1.2: $f' = c' \wedge d'$, and, hence, $f \in L(a, b)$.
Proof: This follows from statement 1.

Statement 2: $L(a, b)$ is the largest boolean sublattice of L such that (i) is fulfilled.
Proof: By definition, $L(a, b)$ is boolean with bottom $a \wedge b$ and with top $a \vee b$. The definition guarantees that any boolean sublattice of L with this property is contained in $L(a, b)$.

Statement 3: The parts (i) and (ii) are equivalent.
Proof: This can be easily verified. ◇

As a boolean lattice, the number of elements in $L(a, b)$, if finite, is a power of two. Namely, if $L(a, b)$ is a finite chain, then $\#L(a, b) \in \{0, 2\}$; else, $\#L(a, b)$ is divisible by four. This observation will be helpful for Lemma 6.3.5.

Remark. We note that $L(a, b)$ is a sublattice of the lattice $[a \wedge b, a \vee b] := \{c \in L \colon a \wedge b \leqslant c \leqslant a \vee b\}$. Equality does not hold in general, since in D_{18}, we obtain $\#L(a, b) = 4 < 9 = \#[a \wedge b, a \vee b]$, see Figure 4.3.

Chapter 5

THE JOIN-MEET IDEAL

Throughout the chapter, let $(L, \leqslant)$ be a non-empty finite distributive lattice. The so-called Hibi relations, which go back to [Hibi], are polynomials in $\mathbb{K}[x_a : a \in L]$. The corresponding variety is called the Hibi variety. In Section 5.1 we define the *Hibi body* as the convex hull of the elements in the Hibi variety with length 1. In a finite-dimensional tensor product, the Hibi body is equal to the projective unit ball. We will see that many statements that hold for the projective unit ball also hold for the Hibi body.

Basically, a Hibi relation has the form $xy - vw$, where x, y, v, w are variables. Vividly spoken, an algebraic division of the polynomial ring by $xy - vw$ can be interpreted as an identification of the term xy with the term vw. In this respect, the polynomial $xy - vw$ serves as a "relation" between the terms xy and vw, which justifies the notion "Hibi relation". In Section 5.2 we express this "relation" by a reduction relation on the terms. This approach is rather combinatorial than algebraic.

The homogeneous binomial ideal which is generated by the Hibi relations is called the join-meet ideal. In Section 5.2 we determine a vector space basis of this ideal, which we call the *median basis*. Basically, this basis can be found in [Stu, Lemma 4.1], but the independent approach here focuses on normal forms of the reduction relation, the *medians*. With the median basis, the ideal membership problem for the join-meet ideal can be solved in a simple and convenient way.

It is well known that the Hibi relations are a Gröbner basis of the join-meet ideal, see [HHO, Theorem 6.17]. In Section 5.3 we give an alternative approach by using the reduction relation. Based on [Sto], we also determine a Gröbner basis of this ideal together with the *norming polynomial*. Gröbner bases will be important for determining vanishing ideals in Section 5.5. This is useful for discussions on symmetries of theta bodies.

Moreover, in this section, the dimension and the degree of the Hibi variety are determined (at least for the special case which will be essential in the following chapters).

In Section 5.1 we introduce *complex Hibi relations*, which are the real and the imaginary parts of the Hibi relations. We call the generated ideal the *complex-join-meet ideal*. In Section 5.4 we discuss the difficulty of finding a Gröbner basis of the complex-join-meet ideal.

Let $V_{\mathbb{K}} := \mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$ denote a real or complex finite-dimensional tensor product, where $r \geqslant 2$ and $n_1, \dots, n_r \geqslant 2$. The indexing tuples for $V_{\mathbb{K}}$ are given by the lattice $L = N = \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$ (as a product of finite chains). Let $L_{\mathbb{C}} := L \times \{1, 2\}$. Section 5.6 deals with the application to tensor products.

5.1 Real and Complex Hibi Relations

In this section we introduce the Hibi body as a generalisation of the projective unit ball.

In order to do so, we recall that the projective unit ball is the convex hull of a real variety, see the Determinant Criterions Theorem 3.4.6 and Theorem 3.5.2 as well as the Criterions for Unit Product Vectors Theorem 3.4.7 and Theorem 3.5.3. Here, we have a closer look on the polynomials which define this variety such that the theorems can be generalised.

The terms and the symbols which will be introduced here are summarised at the end of this section in Table 5.1 and Table 5.2.

5.1.1 Hibi Relations, the Join-Meet Ideal and the Hibi Body

Definition. A polynomial in $\mathbb{K}[x_a \colon a \in L]$ of the form

$$x_a x_b - x_{a \wedge b} x_{a \vee b}$$

for $a, b \in L$ is called a *Hibi relation*. It equals zero if and only if a and b are comparable. Let $\mathcal{H}_L$ be the set of all non-zero Hibi relations in $\mathbb{K}[x_a \colon a \in L]$. The ideal $\mathcal{I}_L = \mathrm{Id}(\mathcal{H}_L)$ which is generated by the Hibi relations is called the *join-meet ideal*. The real affine variety $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_L)$ is called the *Hibi variety*.

Remark. The term "Hibi relation" goes back to [Hibi], see [EHM]. Since the term "Hibi ideal" is reserved for a special monomial ideal, see [EHM], we use the term "join-meet ideal" from [HHO]. The term "Hibi variety" is used in [LM].

The join-meet ideal provides information about the lattice L: If L is a chain, then there exists no Hibi relation, which is non-zero. On the other hand, for each rhomb in L (that is, a sublattice of the form (c) in Figure 4.1), there exists a unique non-zero Hibi relation. Thus, the join-meet ideal "encodes" the appearance of rhombs in L. Alternatively, it could be regarded as a "measure" for the "closeness" of a lattice to a boolean lattice.

In the case where $L = N$, the Hibi relations equal the determinantal Hibi relations and the Hibi variety equals the product vectors in $V_{\mathbb{K}}$, see the Determinant Criterion Theorem 3.4.6.

Definition. The convex hull of the set $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_L) \cap (\mathbb{K}^L)_1$ is called the *Hibi body*.

The Hibi body is a convex body. In the case where $L = N$, it equals the projective unit ball, see the Criterion for Unit Product Vectors Theorem 3.4.7.

Definition. A polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$ is called a *binomial*, if there exist $\alpha, \beta \in \mathbb{N}_0^n$ such that $f = x^\alpha - x^\beta$. An ideal $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ is called a *prime ideal*, if $x \cdot y \in I$ implies $x \in I$ or $y \in I$. It is called a *toric ideal*, if it is a prime ideal which is generated by binomials. The corresponding variety is called a *toric variety*.

It can be easily verified that an ideal is prime, if and only if the coordinate ring is an integral domain (that is, the coordinate ring is free from zero divisors). See [CLSc], [Pla] or [Stu] for detailed information about toric ideals.

Proposition. For $\mathbb{K} = \mathbb{C}$, the join-meet ideal $\mathcal{I}_L$ is a prime toric ideal.

Proof. See [Hibi, page 100]. ◇

Now, the main idea is to understand the projective unit ball by investigating the join-meet ideal and the corresponding variety.

5.1.2 The Normed Hibi Variety

Definition. The polynomial

$$u_L := \sum_{a \in L} x_a^2 - 1$$

is referred to as the *norming polynomial*. The Hibi relations, together with u_L, generate the ideal $\mathcal{J}_L = \mathrm{Id}(\mathcal{H}_L, u_L)$, which we refer to as the *norm-join-meet ideal*. We refer to the variety which is induced by the norm-join-meet ideal as the *normed Hibi variety*.

In the case where $\mathbb{K} = \mathbb{R}$, the normed Hibi variety is given by $\mathcal{Z}_{\mathbb{R}}(\mathcal{J}_L) = \mathcal{Z}_{\mathbb{R}}(\mathcal{I}_L) \cap (\mathbb{R}^L)_1$, that is, the Hibi body equals the convex hull of a real affine variety.

5.1.3 Complex Hibi Relations

Now, we concentrate on the case where $\mathbb{K} = \mathbb{C}$. We note that the unit sphere $(\mathbb{C}^L)_1$ is no variety in general, see Subsection 2.2.6. However, its decomplexification is a variety.

Definition. The real and imaginary parts of the Hibi relations are called the *complex Hibi relations*. The ideal which is generated by the complex Hibi relations is referred to as the *complex-join-meet ideal*. Its variety is referred to as the *complex Hibi variety*.

The set of all non-zero complex Hibi relations is denoted by $\mathcal{H}_{L_\mathbb{C}} := \mathrm{Re}(\mathcal{H}_L) \cup \mathrm{Im}(\mathcal{H}_L)$. The complex-join-meet ideal equals the decomplexification $\imath(\mathcal{J}_L)$ of the join-meet ideal $\mathcal{J}_L$, see Proposition 2.2.4.

Theorem. The complex Hibi variety equals $\mathcal{Z}_\mathbb{R}(\imath(\mathcal{J}_L)) = \mathcal{Z}_\mathbb{R}(\mathcal{H}_{L_\mathbb{C}}) = \imath(\mathcal{Z}_\mathbb{C}(\mathcal{J}_L))$. In the case where $L = N$, it equals $\imath(\mathcal{P}_{V_\mathbb{C}})$.

Proof. With Theorem 2.2.5, the complex Hibi variety equals $\imath(\mathcal{Z}_\mathbb{C}(\mathcal{J}_L))$. In the special case where $L = N$, the Determinant Criterion Theorem 3.4.6 states that $\mathcal{P}_{V_\mathbb{C}} = \mathcal{Z}_\mathbb{C}(\mathcal{J}_L)$. ◇

Let $h := x_a x_b - x_{a \wedge b} x_{a \vee b}$, where $a, b \in L$, be a Hibi relation in $\mathbb{C}[x_c : c \in L]$. Its real and imaginary parts are polynomials in $\mathbb{R}[x_{c,1}, x_{c,2} : c \in L]$. A short calculation shows that they are given by

$$\begin{aligned} \mathrm{Re}(h) &= x_{a,1} x_{b,1} - x_{a,2} x_{b,2} - x_{a \wedge b,1} x_{a \vee b,1} + x_{a \wedge b,2} x_{a \vee b,2}, \\ \mathrm{Im}(h) &= x_{a,1} x_{b,2} + x_{a,2} x_{b,1} - x_{a \wedge b,1} x_{a \vee b,2} - x_{a \wedge b,2} x_{a \vee b,1}. \end{aligned}$$

Both $\mathrm{Re}(h)$ and $\mathrm{Im}(h)$ are non-zero, if and only if h is non-zero.

5.1.4 The Complex Normed Hibi Variety

Definition. The polynomial

$$u_{L_\mathbb{C}} := \sum_{a \in L_\mathbb{C}} x_a^2 - 1 = \sum_{a \in L} (x_{a,1}^2 + x_{a,2}^2) - 1$$

in $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ is referred to as the *complex norming polynomial*. The complex Hibi relations, together with $u_{L_\mathbb{C}}$, generate the ideal $\mathcal{J}_{L,\mathbb{C}}$, which we refer to as the *complex-norm-join-meet ideal*. We refer to the variety $\mathcal{Z}_\mathbb{R}(\mathcal{J}_{L,\mathbb{C}})$ as the *complex normed Hibi variety*. The convex hull of the complex normed Hibi variety is called the *(complex) Hibi body*.

Theorem. The complex normed Hibi variety equals $\mathcal{Z}_\mathbb{R}(\mathcal{J}_{L,\mathbb{C}}) = \imath(\mathcal{Z}_\mathbb{C}(\mathcal{I}_L) \cap (\mathbb{C}^L)_1)$. In the case where $L = N$, the complex normed Hibi variety equals $\imath(\mathcal{E}_{V_\mathbb{C}})$, and the complex Hibi body equals $\imath(\mathcal{B}_{1,\pi}) = \mathrm{co}(\mathcal{Z}_\mathbb{R}(\imath(\mathcal{J}_N)))$.

Proof. According to Subsection 2.2.6, we have $\|v\| = 1$ if and only if $u_{L_\mathbb{C}}(\imath(v)) = 0$. Hence,

$$\begin{aligned}\imath(\mathcal{Z}_\mathbb{C}(\mathcal{I}_L)_1) &= \imath(\mathcal{Z}_\mathbb{C}(\mathcal{I}_L) \cap (V_\mathbb{C})_1) = \imath(\mathcal{Z}_\mathbb{C}(\mathcal{I}_L)) \cap \imath((V_\mathbb{C})_1) \\ &= \mathcal{Z}_\mathbb{R}(\mathcal{H}_{L_\mathbb{C}}) \cap \mathcal{Z}_\mathbb{R}(u_{L_\mathbb{C}}) = \mathcal{Z}_\mathbb{R}(\mathcal{H}_{L_\mathbb{C}} \cup \{u_{L_\mathbb{C}}\}) = \mathcal{Z}_\mathbb{R}(\mathcal{J}_{L,\mathbb{C}}).\end{aligned}$$

In the special case where $L = N$, we obtain $\imath(\mathcal{E}_{V_\mathbb{C}}) = \mathcal{Z}_\mathbb{R}(\mathcal{J}_{N,\mathbb{C}})$ according to the Criterion for Unit Product Vectors Theorem 3.5.3. ◇

Hence, the complex Hibi body equals the decomplexification of the Hibi body.

5.1.5 Summary

The terms and the symbols which are introduced in this section are summarised in Table 5.1 and in Table 5.2.

Table 5.1 summarises the notions related to Hibi relations. In the case where $L = N$, the Hibi relations describe the product vectors in $V_\mathbb{K}$ as a real or complex affine variety. The last column of this table refers to the complex Hibi relations.

Table 5.2 is based on the fact that the Euclidean unit sphere is a real affine variety. In particular, in the case where $L = N$, the unit product vectors in $V_\mathbb{K}$ can be written as a real affine variety. We note that in general, it is not possible to write the unit product vectors in $V_\mathbb{C}$ as a complex variety (in Table 5.2, the symbol $\lightning$ refers to this situation).

Field	$\mathbb{K}$	$\mathbb{R}$
Lattice	L	$L_{\mathbb{C}}$
Polynomial ring	$\mathbb{K}[x_a \colon a \in L]$	$\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$
Polynomials	$x_a x_b - x_{a \wedge b} x_{a \vee b}$ $\mathcal{H}_L$ Hibi relations	$x_{a,1} x_{b,1} - x_{a,2} x_{b,2} \ldots$ $-x_{a \wedge b,1} x_{a \vee b,1} + x_{a \wedge b,2} x_{a \vee b,2}$ (Re) $x_{a,1} x_{b,2} + x_{a,2} x_{b,1} \ldots$ $-x_{a \wedge b,1} x_{a \vee b,2} - x_{a \wedge b,2} x_{a \vee b,1}$ (Im) $\mathcal{H}_{L_{\mathbb{C}}}$ Complex Hibi relations
Gröbner basis?	yes	no (in general)
Ideal	$\mathcal{J}_L$ Join-meet ideal	$\imath(\mathcal{J}_L)$ Complex-join-meet ideal
Variety	$\mathcal{Z}_{\mathbb{K}}(\mathcal{J}_L)$ Hibi variety	$\mathcal{Z}_{\mathbb{R}}(\imath(\mathcal{J}_L)) = \imath(\mathcal{Z}_{\mathbb{C}}(\mathcal{J}_L))$ Complex Hibi variety
for $L = N$	$\mathcal{P}_{V_{\mathbb{K}}}$ Product vectors	$\imath(\mathcal{P}_{V_{\mathbb{C}}})$ Decomplexification of $\mathcal{P}_{V_{\mathbb{C}}}$

Table 5.1: Hibi Relations

Field	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{R}$
Lattice	L		$L_{\mathbb{C}}$
Polynomial ring	$\mathbb{K}[x_a \colon a \in L]$		$\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$
Polynomials	$\mathcal{H}_L$ and $u_L = \sum_{a \in L} x_a^2 - 1$ Norming polynomial	↯	$\mathcal{H}_{L_{\mathbb{C}}}$ and $u_{L_{\mathbb{C}}} = \sum_{a \in L}(x_{a,1}^2 + x_{a,2}^2) - 1$ Complex norming polynomial
Gröbner basis?	yes	–	no (in general)
Ideal	$\mathfrak{J}_L$ Norm-join-meet ideal	–	$\mathfrak{J}_{L,\mathbb{C}}$ Complex-norm-join-meet ideal
Variety	$\mathcal{Z}_{\mathbb{R}}(\mathfrak{J}_L)$ Normed Hibi variety	–	$\mathcal{Z}_{\mathbb{R}}(\mathfrak{J}_{L,\mathbb{C}})$ Complex normed Hibi variety
for $L = N$	$\mathcal{E}_{V_{\mathbb{R}}}$ Unit product vectors		$\imath(\mathcal{E}_{V_{\mathbb{C}}})$ Decomplexification of $\mathcal{E}_{V_{\mathbb{C}}}$
Convex body	$\mathrm{co}(\mathcal{Z}_{\mathbb{K}}(\mathcal{J}_L) \cap (\mathbb{K}^L)_1)$ Hibi body		$\mathrm{co}(\mathcal{Z}_{\mathbb{R}}(\imath(\mathcal{J}_L)) \cap (\mathbb{R}^{L_{\mathbb{C}}})_1)$ Complex Hibi body
for $L = N$	$\mathcal{B}_{1,\pi}$ Projective unit ball		$\imath(\mathcal{B}_{1,\pi})$ Decomplexification of $\mathcal{B}_{1,\pi}$

Table 5.2: Hibi Relations and Norming

5.2 The Median Basis of the Join-Meet Ideal

In this section we introduce the median basis as a vector space basis of the join-meet ideal. With the help of this basis it is very easy to solve the ideal membership problem. Indeed, it seems to be a "natural" basis for this ideal: The Hibi relations are homogeneous polynomials of degree 2. What is the meaning of the number "2"? Even though determinantal Hibi relations are related to determinants of 2×2 matrices (which is a rather obvious "relation" to the number "2"), their set of zeros equals the product vectors of a finite-dimensional tensor product, see Section 3.4. It seems to be quite difficult to relate product vectors to the number "2". This discrepancy vanishes with the median basis, since the number 2 will have no more meaning than the degree of the first non-trivial homogeneous part of the join-meet ideal.

The median basis is based on a reduction relation on the term monoid. In particular, it is not necessary to include the rich structure of the polynomial ring. However, if one wants to find a basis for an ideal with generators that have more than two terms, for example a generator like $x^2 + y^2 - 1 \in \mathbb{K}[x, y]$, then the proposed approach might not work anymore.

5.2.1 The Join-Meet Ideal is Homogeneous

The join-meet ideal is homogeneous, so it can be regarded as a vector space over $\mathbb{K}$ (actually, in general, the underlying field is arbitrary). According to Proposition 1.3, it equals the direct sum of its homogeneous parts $(\mathcal{J}_L)_m$ for the degrees $m \in \mathbb{N}_0$. According to Corollary 1.3, for $m \geqslant 2$, the homogeneous part $(\mathcal{J}_L)_m$ is generated by the polynomials $g \cdot h$, where g is a term of degree $m - 2$ and h is a Hibi relation.

5.2.2 The Terms

In what follows, a term $x_{a_1} \cdot \ldots \cdot x_{a_m} \in (\mathbb{K}[x_a \colon a \in L])_m$ is identified with the tuple $(a_1, \ldots, a_m) \in L^m$. Since the polynomial ring is commutative, there is a one-to-one correspondence between terms in $(\mathbb{K}[x_a \colon a \in L])_m$ and elements in L^m/S_m, where the symmetric group S_m acts via permutations of the entries on L^m. In what follows, we use the notation $\overline{a} \in L^m/S_m$ and we write $\overline{x}_{\overline{a}}$ for $x_{a_1} \cdot \ldots \cdot x_{a_m}$. Let $L^0/S_0 := \{\emptyset\}$ and $\overline{x}_{\emptyset} := 1$.

Hence, the elements of the sets L^m/S_m, $m \in \mathbb{N}_0$, serve as a basis of the polynomial ring.

We say that $\overline{a} \in L^m/S_m$ is a *chain*, if there exist $a_1, \ldots, a_m \in L$ such that $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_m$ and $\overline{a} = (a_1, \ldots, a_m)$. We note that in contrast to a chain of length $m-1$ in L, defined in Subsection 4.1.1, which requires m different elements in L, an entry of a chain in L^m/S_m can appear several times.

5.2.3 A Reduction Relation

On L^m/S_m, we define the following reduction relation $\longrightarrow$: For all $a_1, \ldots, a_m \in L$ and for all $p, q \in \{1, \ldots, m\}$ such that a_p and a_q are not comparable in L we have

$$\begin{aligned} & (a_1, \ldots, a_{p-1}, \boxed{a_p}, a_{p+1}, \ldots, a_{q-1}, \boxed{a_q}, a_{q+1}, \ldots, a_m) \\ \longrightarrow\ & (a_1, \ldots, a_{p-1}, \boxed{a_p \wedge a_q}, a_{p+1}, \ldots, a_{q-1}, \boxed{a_p \vee a_q}, a_{q+1}, \ldots, a_m). \end{aligned}$$

In what follows, the notation "$\longrightarrow$" relates to this specific relation.

Proposition. The relation $\longrightarrow$ is a noetherian reduction relation.

Proof. Let $\kappa_{\overline{a}}$ be the number of comparable pairs in $\overline{a} = (a_1 \ldots, a_m) \in L^m/S_m$, that is,

$$\kappa_{\overline{a}} := \{(r, s) \colon 1 \leqslant r < s \leqslant m,\ a_r \leqslant a_s \ \text{ or } \ a_r \geqslant a_s\}.$$

Now, let $\overline{b} \longrightarrow \overline{c}$. In the following, we show $\kappa_{\overline{b}} < \kappa_{\overline{c}}$. Let $\overline{b} = (b_1 \ldots, b_m)$ and $\overline{c} = (c_1, \ldots, c_m)$. Without loss of generality, let $c_1 = b_1 \wedge b_2$, $c_2 = b_1 \vee b_2$, and $c_s = b_s$ for $s \in \{3, \ldots, m\}$. We obtain $c_1 < c_2$. For all $s \in \{3, \ldots, m\}$, we have

1. $b_1 \leqslant b_s$ or $b_2 \leqslant b_s \Rightarrow c_1 \leqslant c_s$,
   $b_1 \leqslant b_s$ and $b_2 \leqslant b_s \Rightarrow c_2 \leqslant c_s$.
2. $b_1 \geqslant b_s$ or $b_2 \geqslant b_s \Rightarrow c_2 \geqslant c_s$,
   $b_1 \geqslant b_s$ and $b_2 \geqslant b_s \Rightarrow c_1 \geqslant c_s$.

It follows that $\kappa_{\overline{b}} < \kappa_{\overline{c}}$. Hence, the relation is strictly antisymmetric. Since $\kappa_{\overline{a}} \leqslant 1/2 \cdot m(m-1)$ for all $\overline{a} \in L^m/S_m$, it is also noetherian. ◇

Let $\mathcal{R}_m$ denote the set of all equivalence classes with respect to $\xleftrightarrow{\star}$. The equivalence class of $\overline{a} \in L^m/S_m$ is denoted by $[\overline{a}]$. It consists of all elements which share its normal form with $\overline{a}$.

Proposition. Let $\overline{a} \in L^m/S_m$. Then the following are equivalent:

(a) $\overline{a}$ is a normal form.

(b) $\overline{a}$ is a chain.

Proof. This statement follows by definition of the reduction relation. ◇

Hence, there is exactly one chain in $[\overline{a}]$, and this chain equals the normal form of $\overline{a}$.

Proposition. Let $\overline{a}, \overline{b} \in L^m/S_m$.

(i) If $\overline{a} \longrightarrow \overline{b}$, then $m \geqslant 2$ and there exists $\overline{c} \in L^{m-2}/S_{m-2}$ and a non-zero Hibi relation $h \in \mathcal{H}_L$ such that

$$x_{\overline{a}} - x_{\overline{b}} = x_{\overline{c}} \cdot h.$$

(ii) If $\overline{a} \xrightarrow{\star} \overline{b}$, then

$$x_{\overline{a}} - x_{\overline{b}} \in (\mathcal{J}_L)_m.$$

In particular, $(\mathcal{J}_L)_m$ is generated by those polynomials as a vector space over $\mathbb{K}$.

Proof. Let $m \geqslant 2$ (for all other cases, $\longrightarrow$ is empty). Let $\overline{a} = (a_1, \ldots, a_m)$. We first consider the special case where $\overline{a} \longrightarrow \overline{b}$. In this case, $\overline{b}$ has the form

$$\overline{b} = (a_1, \ldots, a_{p-1}, a_p \wedge a_q, a_{p+1}, \ldots, a_{q-1}, a_p \vee a_q, a_{q+1}, \ldots, a_m)$$

for suitable $p, q \in \{1, \ldots, m\}$, such that a_p and a_q are not comparable in L. Hence,

$$x_{\overline{a}} - x_{\overline{b}} = \left(\prod_{\substack{k=1 \\ k \notin \{p,q\}}}^{m} x_{a_k} \right) \cdot \underbrace{\left(x_{a_p} x_{a_q} - x_{a_p \wedge a_q} x_{a_p \vee a_q} \right)}_{=:\, h}.$$

This expression is a product of a term of degree $m-2$ and a non-zero Hibi relation h, so that it belongs to $(\mathcal{J}_L)_m$.

Now, we consider the more general case where $\overline{a} \xrightarrow{\star} \overline{b}$. With the preceding result, $\overline{x}_{\overline{a}} - \overline{x}_{\overline{b}}$ can be written as a "telescoping sum" of expressions which belong to $(\mathcal{J}_L)_m$.

Now, the statement follows with Subsection 5.2.1. ◇

5.2.4 Visualisation of the Reduction Relation

Let $a, b, c \in L$. As mentioned in Subsection 4.2.4, a, b and c generate a sublattice of L. In this sublattice, $l := l(a, b, c) := a \vee b \vee c$ is the "largest" (top) element, $s := s(a, b, c) := a \wedge b \wedge c$ is the "smallest" (bottom) element, and

$$\begin{aligned} m &:= m(a, b, c) \\ &:= (a \wedge b) \vee (b \wedge c) \vee (c \wedge a) = (a \vee b) \wedge (b \vee c) \wedge (c \vee a) \end{aligned}$$

is the "median"; see also Figure 4.3 on page 104. We note that (s, m, l) is a chain. Also, they do not depend on the order of a, b and c. Vividly spoken, in Figure 4.3, they lie on a "vertical axis", where a, b and c lie on a "horizontal axis".

Example. If we consider the special case where $L = N$, the entry l_t, m_t, s_t (where l_t denotes the t^{th} entry of l, and so on) equals the largest, middlemost and the smallest (respectively) of the numbers a_t, b_t, c_t, for all $t \in \{1, \dots, r\}$.

Proposition. In L^3/S_3, the normal form of (a, b, c) is given by (s, m, l).

Proof. The following reduction is possible:

$$\begin{aligned} (a, b, c) &\xrightarrow{\star} (a \wedge b, a \vee b, c) \\ &\xrightarrow{\star} (a \wedge b, (a \vee b) \wedge c, \underbrace{a \vee b \vee c}_{=l}) \\ &\xrightarrow{\star} (\underbrace{a \wedge b \wedge ((a \vee b) \wedge c)}_{=s}, \underbrace{(a \wedge b) \vee ((a \vee b) \wedge c)}_{=m}, l)\,. \end{aligned}$$

Since $s \leqslant m \leqslant l$ in L, the last element is the normal form. ◇

5.2.5 Normal Forms are Unique

Proposition. Normal forms with respect to $\longrightarrow$ are unique.

Proof. Due to Newman's Lemma, see [BW, Theorem 4.75], a noetherian reduction relation $\longrightarrow'$ on a set G has unique normal forms if and only if it is *locally confluent*, that is, if $g \longrightarrow' h_1$ and $g \longrightarrow' h_2$, then there exists $g_0 \in G$ with $h_1 \overset{\star}{\longrightarrow}{}' g_0$ and $h_2 \overset{\star}{\longrightarrow}{}' g_0$.

Now, let $\overline{a} = (a_1, \dots, a_m), \overline{b_1}, \overline{b_2} \in L^3/S_3$ such that $\overline{a} \longrightarrow \overline{b_1}$ and $\overline{a} \longrightarrow \overline{b_2}$. Without loss of generality, let $\overline{b_1} = (a_1 \wedge a_2, a_1 \vee a_2, a_3, \dots, a_m)$.

Case 1: There exist $p, q \in \{3, \dots, m\}$, $p < q$, such that

$$\overline{b_2} = (a_1, \dots, a_{p-1}, a_p \wedge a_q, a_{p+1}, \dots, a_{q-1}, a_p \vee a_q, a_{q+1}, \dots, a_m)\,.$$

Let

$$\overline{c} := (a_1 \wedge a_2, a_1 \vee a_2, \dots, a_p \wedge a_q, \dots, a_p \vee a_q, \dots, a_m)\,.$$

Then $\overline{b_1} \overset{\star}{\longrightarrow} \overline{c}$ and $\overline{b_2} \overset{\star}{\longrightarrow} \overline{c}$.

Case 2: There exists $p \in \{3, \dots, m\}$ such that

$$\overline{b_2} = (a_1 \wedge a_p, a_2, \dots, a_{p-1}, a_1 \vee a_p, a_{p+1}, \dots, a_m)\,.$$

In this case, according to Proposition 5.2.4, both $\overline{b_1}$ and $\overline{b_2}$ reduce to

$$\begin{aligned}\overline{c} := (&s(a_1, a_2, a_p), m(a_1, a_2, a_p), l(a_1, a_2, a_p),\\ &a_3, \dots, a_{p-1}, \dots, a_{p+1}, \dots, a_m)\,.\end{aligned}$$

◇

5.2.6 The Median

Given $\overline{a} \in L^m/S_m$, the following definition helps us to determine the normal form of $\overline{a}$ without applying an algorithm based on the reduction relation.

Definition. Let $a_1, \dots, a_m \in L$ and $k \in \{1, \dots, m\}$. The k-*median* of $a_1, \dots, a_m$ is defined by

$$M_k(a_1, \dots, a_m) := \bigvee_{\substack{A \subseteq \{1,\dots,m\} \\ \#A = k}} \bigwedge_{l \in A} a_l\,.$$

Since this definition is independent of the order of $a_1, \dots, a_m$, it is also well-defined on L^m/S_m.

Example. We have

$$\begin{aligned} M_1(a_1,\dots,a_m) &= a_1 \vee \cdots \vee a_m, \\ M_m(a_1,\dots,a_m) &= a_1 \wedge \cdots \wedge a_m, \\ M_2(a_1,a_2,a_3) &= m(a_1,a_2,a_3). \end{aligned}$$

Proposition. Let $\overline{a} \in L^m/S_m$. For all $k \in \{1,\dots,m-1\}$, we have $M_k(\overline{a}) \geqslant M_{k+1}(\overline{a})$.

Proof. We have

$$\begin{aligned} M_k(\overline{a}) \vee M_{k+1}(\overline{a}) &= \left(\bigvee_{\substack{A \subseteq \{1,\dots,m\} \\ \#A=k}} \bigwedge_{l \in A} a_l \right) \vee \left(\bigvee_{\substack{B \subseteq \{1,\dots,m\} \\ \#B=k+1}} \bigwedge_{l \in B} a_l \right) \\ &= M_k(\overline{a}), \end{aligned}$$

since for each $B \subseteq \{1,\dots,m\}$ with $\#B = k+1$, there exists $A \subseteq \{1,\dots,m\}$ with $\#A = k$ such that $\bigwedge_{l \in B} a_l \leqslant \bigwedge_{l \in A} a_l$. ◇

Proposition. The normal form of $\overline{a} \in L^m/S_m$ is given by

$$\mathcal{M}(\overline{a}) := (M_1(\overline{a}), M_2(\overline{a}), \dots, M_m(\overline{a})),$$

which we call the *median* of $\overline{a}$.

Proof. We use induction on m. For $m = 0$ or $m = 1$ the assertion is true. Now let the assertion be true for $m \in \mathbb{N}$. Let $\overline{a} = (a_1,\dots,a_m) \in L^m/S_m$ and let $a_{m+1} \in L$. We write $\mu_l := M_l(\overline{a})$ for all $l \in \{1,\dots,m\}$. The assumptions yield

$$\begin{aligned} &(a_1,\dots,a_m,a_{m+1}) \\ &\xrightarrow{\star} (\mu_m,\dots,\mu_1,a_{m+1}) \\ &\xrightarrow{\star} (\mu_m,\dots,\mu_2,\mu_1 \wedge a_{m+1}, \underbrace{\mu_1 \vee a_{m+1}}_{=M_1(a_1,\dots,a_{m+1})}) \\ &\xrightarrow{\star} ((M_k(\mu_m,\dots,\mu_2,\mu_1 \wedge a_{m+1}))_{k=1}^{m}, M_1(a_1,\dots,a_{m+1})). \end{aligned}$$

Now we show that for all $k \in \{1,\dots,m\}$, we have

$$M_k(\mu_m,\dots,\mu_2,\mu_1 \wedge a_{m+1}) = M_{k+1}(a_1,\dots,a_{m+1}),$$

which finishes the proof. For all $k \in \{1,\dots,m-1\}$, this equality holds since

$$M_k(\mu_m,\dots,\mu_2,\mu_1 \wedge a_{m+1})$$

$$
\begin{aligned}
&= \Big(\bigvee_{\substack{A\subseteq\{2,\dots,m\}\\ \#A=k}} \bigwedge_{l\in A} \mu_l \Big) \vee \Big(\bigvee_{\substack{A\subseteq\{2,\dots,m\}\\ \#A=k-1}} \Big(\bigwedge_{l\in A} \mu_l \Big) \wedge \mu_1 \wedge a_{m+1} \Big) \\
&= \mu_{k+1} \vee \Big(\Big(\bigvee_{\substack{A\subseteq\{1,\dots,m\}\\ \#A=k}} \bigwedge_{l\in A} \underbrace{\mu_l \wedge \mu_1}_{=\mu_l} \Big) \wedge a_{m+1} \Big) \\
&= \mu_{k+1} \vee (\mu_k \wedge a_{m+1}),
\end{aligned}
$$

and also

$$
\begin{aligned}
&M_{k+1}(a_1,\dots,a_{m+1}) \\
&= \Big(\bigvee_{\substack{A\subseteq\{1,\dots,m\}\\ \#A=k+1}} \bigwedge_{l\in A} a_l \Big) \vee \Big(\bigvee_{\substack{A\subseteq\{1,\dots,m\}\\ \#A=k}} \Big(\bigwedge_{l\in A} a_l \Big) \wedge a_{m+1} \Big) \\
&= \mu_{k+1} \vee \Big(\Big(\bigvee_{\substack{A\subseteq\{1,\dots,m\}\\ \#A=k}} \bigwedge_{l\in A} a_l \Big) \wedge a_{m+1} \Big) \\
&= \mu_{k+1} \vee (\mu_k \wedge a_{m+1}).
\end{aligned}
$$

For $k = m$ we obtain

$$M_m(\mu_m,\dots,\mu_2,\mu_1 \wedge a_{m+1}) = \mu_m \wedge a_{m+1} = M_{m+1}(a_1,\dots,a_{m+1}). \quad \diamond$$

Example. If we consider determinantal Hibi relations, that is, if we consider $L = N$, we may identify $\overline{a} = (a_1,\dots,a_m) \in N^m/S_m$ by an $m \times r$ matrix

$$
\begin{pmatrix}
a_{1,1} & a_{1,2} & \dots & a_{1,r} \\
a_{2,1} & a_{2,2} & \dots & a_{2,r} \\
\vdots & \vdots & & \vdots \\
a_{m,1} & a_{m,2} & \dots & a_{m,r}
\end{pmatrix},
$$

where $a_l = (a_{l,1},\dots,a_{l,r}) \in N$ for all $l \in \{1,\dots,m\}$. The k-median of $\overline{a}$ is determined by applying the median to each column, which gives the k-largest element in that column. Hence, if we sort the entries of each column in descending order, we obtain a new matrix, whose k^{th} row gives $M_k(\overline{a})$ for all $k \in \{1,\dots,m\}$. Hence, this matrix represents $\mathcal{M}(\overline{a})$.

In the case where $n_1 = n_2 = \dots = n_r =: n$, the quotient N^m/S_m can be identified with $\mathcal{M}_{m,r}(\{1,\dots,n\})$ modulo permutations of the rows.

Example. Let $(a,b),(c,d) \in L^2/S_2$. Then the following are equivalent:

(a) $(a, b) \overset{\star}{\longleftrightarrow} (c, d)$.
(b) The polynomial $x_a\, x_b - x_c\, x_d$ lies in $\mathcal{J}_L$.
(c) The medians of (a, b) and (c, d) coincide.
(d) $a \wedge b = c \wedge d$ and $a \vee b = c \vee d$.
(e) $L(a, b) = L(c, d)$.

We recall that $L(a, b)$ is the largest boolean sublattice of L such that a and b are complements, see Proposition 4.2.6.

5.2.7 The Median Basis

For all $m \in \mathbb{N}_0$ and for all $\overline{a} \in L^m/S_m$, let

$$h_{\overline{a}} := \overline{x}_{\overline{a}} - \overline{x}_{\mathcal{M}(\overline{a})}.$$

Let $\mathcal{B}_L$ denote the set of all polynomials $h_{\overline{a}}$ such that $\overline{a}$ is not a chain. Let $V_{[\overline{a}]}$ denote the linear hull of all polynomials $h_{\overline{b}}$, where $\overline{a} \overset{\star}{\longleftrightarrow} \overline{b}$.

Theorem. A vector space basis of the join-meet-ideal $\mathcal{J}_L$ is given by $\mathcal{B}_L$. In particular, for all $m \in \mathbb{N}_0$, $(\mathcal{J}_L)_m$ equals the direct sum of the vector spaces $V_{[\overline{c}]}$, for all chains $\overline{c} \in L^m/S_m$ with $\#[\overline{c}] \geqslant 2$.

Proof. With Proposition 5.2.6.II, the normal form of $\overline{a}$ is given by $\overline{c} := \mathcal{M}(\overline{a})$. From Proposition 5.2.3.III, it follows that $V_{[\overline{c}]} \subseteq (\mathcal{J}_L)_m$. On the other hand, $(\mathcal{J}_L)_m$ is generated by polynomials of the form $f := g\, h$, where g is a term of degree $m - 2$ and h is a non-zero Hibi relation, which is the difference of two terms $\overline{a}, \overline{b} \in L^2/S_2$ with $\overline{a} \longrightarrow \overline{b}$. Hence, $\overline{a}$ and $\overline{b}$ have the same normal form $\overline{c}$ and

$$\overline{x}_{\overline{a}} - \overline{x}_{\overline{b}} = (\overline{x}_{\overline{a}} - \overline{x}_{\overline{c}}) - (\overline{x}_{\overline{b}} - \overline{x}_{\overline{c}}),$$

which lies in $V_{[\overline{c}]}$.

It can be easily seen that the polynomials in $\mathcal{B}_L$ are linearly independent. ◇

Definition. We refer to the basis $\mathcal{B}_L$ of the join-meet ideal $\mathcal{J}_L$ as the *median basis*.

5.2.8 The Median of a Polynomial

Corollary. The ideal membership problem for the join-meet ideal $\mathcal{J}_L$ the can be solved as follows: Let

$$\begin{aligned} \mathcal{M} : \ \mathbb{K}[x_a \colon a \in L] &\to \mathbb{K}[x_a \colon a \in L], \\ \overline{x}_{\overline{a}} &\mapsto \overline{x}_{\mathcal{M}(\overline{a})}. \end{aligned}$$

Given $f \in \mathbb{K}[x_a \colon a \in L]$, then $f - \mathcal{M}(f) \in \mathcal{J}_L$ and the following are equivalent:

(a) $f \in \mathcal{J}_L$.

(b) $\mathcal{M}(f) = 0$.

Proof. See Theorem 5.2.7. ◇

We call $\mathcal{M}(f)$ the *median of* f or the *normal form of* f *with respect to* $\mathcal{J}_L$. The second notion refers to the statement that if f is a term, then $\mathcal{M}(f)$ is its normal form. Furthermore, for arbitrary f, we will see that $\mathcal{M}(f)$ equals a normal form of f modulo $\mathcal{J}_L$ in a setting according to Subsection 1.2.2.

We call $f - \mathcal{M}(f)$ the *projection of* f *onto* $\mathcal{J}_L$, although we note that for each homogeneous part f_m of f, $m \geqslant 0$, the polynomial $f_m - \mathcal{M}(f_m)$ does *not* equal the orthogonal projection of f onto $(\mathcal{J}_L)_m$.

5.3 A Gröbner Basis of the (Norm-)Join-Meet Ideal

We have seen in Chapter 1 that a Gröbner basis of a given ideal helps to solve the ideal membership problem. Also, it helps to determine a basis of the coordinate ring. With respect to the join-meet ideal, both problems are already solved with the median basis, see Section 5.2 and Section 5.5. However, to solve them for the norm-join-meet ideal, it may have advantages to know a Gröbner basis.

The non-zero Hibi relations are a Gröbner basis of the join-meet ideal. This result is formulated in [HHO, Theorem 6.17]. Other related works are [Hibi] or [Qur]. Moreover, the non-zero Hibi relations, together with the norming polynomial, are a Gröbner basis of the norm-join-meet ideal. This result is formulated in [Sto, Theorem 4.8] for the special case where $\mathbb{K} = \mathbb{R}$ and $L = N$. Even though this case is the most relevant for our applications, it turns out that the statement can be formulated in a more general context. Both statements have the advantage that for all practical purposes, it is not necessary to compute a Gröbner basis with the aid of a computer algebra system.

Although we are mainly interested in the case where $\mathbb{K} = \mathbb{R}$ (such that the normed Hibi variety corresponds to the unit product vectors), the computation of the Gröbner bases does not depend on the choice of the field $\mathbb{K}$.

In this section we formulate both statements in our general context. The approach in this thesis uses the reduction relation $\longrightarrow$ from Section 5.2 which seems to be rather new. It allows a geometric viewpoint of the Gröbner basis according to Subsection 5.2.4 and it respects the lattice structure. Concerning the second result, we also do not require case distinctions (in comparison to [Sto]).

5.3.1 Linear Extensions

To specify a term order on $\mathbb{K}[x_a \colon a \in L]$ it is convenient to begin with a total order on the variables x_a, $a \in L$, which can also be regarded as an order on L (by identifying x_a with a). In what follows, it turns out that this order should be compatible with the partial order on L corresponding to the lattice structure; formally (see [HHO, Example 6.16]):

Definition. A total order (chain) $\leqslant'$ on the set L is called a *linear extension* of the lattice L if the map

$$\begin{aligned}(L, \leqslant) &\to (L, \leqslant'),\\ a &\mapsto a\end{aligned}$$

is isotone (that is: whenever $a \leqslant b$ for $a, b \in L$, then $a \leqslant' b$).

Example. In this example we consider the case where $L = N$. The set N can be regarded as a subset of $\mathbb{N}_0^n$. On the lattice N, a linear extension $\leqslant'$ is given by the lexicographical order, that is, $a >' b$ if and only if $a \neq b$ and the leftmost non-zero entry in $a - b$ is positive. We refer to Definition 1.1.4 (for the purpose to define an order on the variables, not on the terms in $\mathbb{K}[x_a \colon a \in L]$).

By way of example, for $N = \{1,2\}^2$, on $\mathbb{K}[x_{22}, x_{21}, x_{12}, x_{11}]$, we have

$$x_{22} >' x_{21} >' x_{12} >' x_{11},$$

and for $N = \{1,2\}^3$, we have

$$x_{222} >' x_{221} >' x_{212} >' x_{211} >' x_{122} >' x_{121} >' x_{112} >' x_{111}.$$

Proposition. On any finite distributive lattice, there exists a linear extension.

Proof. According to the Theorem 4.2.2.II, any finite distributive lattice L can be considered as a ring of sets, that is, as a family of subsets of a finite set X. Hence, there exists an injective function $L \to (\mathfrak{P}(X), \subseteq)$, $a \mapsto a$, which is isotone. Since $(\mathfrak{P}(X), \subseteq)$ is a boolean lattice, there exists $r \in \mathbb{N}$ such that it can be identified with $\{1,2\}^r$ (as a r-fold direct product of the chain $\{1,2\}$). With the last example, in this special case, there exists a total order which is a linear extension of $(\mathfrak{P}(X), \subseteq)$; hence, also of the subset L. ◇

Proposition. Let $\leqslant'$ be a linear extension of L. For all $a, b, c \in L$ with $a <' b$, we have

$$a \wedge c \leqslant' a <' b \leqslant' b \vee c.$$

Proof. This statement follows from $a \wedge c \leqslant a$ and from $b \leqslant b \vee c$. ◇

5.3.2 The Graded Reverse Lexicographical Order

We recall that a Gröbner basis depends on the underlying term order. So far, specifying a term order on the polynomial ring $\mathbb{K}[x_a \colon a \in L]$ was not necessary. Thus, we are free to choose a term order which has a "good" reduced Gröbner basis.

Based on a linear extension of L, it appears that the graded reverse lexicographical order on $\mathbb{K}[x_a \colon a \in L]$ due to [Sto] is suitable in the sense that the non-zero Hibi relations (and the norming polynomial, respectively) are a reduced Gröbner basis.

The non-zero Hibi relations are not a universal Gröbner basis, see [Lang, Lemma 5.3.8].

Let $\leqslant'$ be a linear extension of L (which induces a total order on the variables in $\mathbb{K}[x_a \colon a \in L]$).

The set $\mathbb{N}_0^L$ represents the terms in $\mathbb{K}[x_a : a \in L]$ by assuming that the variables are aligned from left to right in descending order with respect to $\leqslant'$. (To be precise: For all $t \in \{1, \dots, \#L\}$, let c be the t^{th} largest element in L with respect to $\leqslant'$. The variable x_c is identified with $(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{N}_0^L$, where the entry 1 appears in position t. For example, the top $\top$ is identified with $(1, 0, \dots, 0)$.)

In what follows, we consider the graded reverse lexicographical order $\leqslant_{\text{grevlex}}$ on $\mathbb{N}_0^L$: For $\alpha, \beta \in \mathbb{N}_0^L$, we have $\alpha >_{\text{grevlex}} \beta$ if and only if $|\alpha| > |\beta|$ or, if $|\alpha| = |\beta|$, the rightmost non-zero entry in $\alpha - \beta$ is negative (see also Definition 1.1.4 and Proposition 1.1.4).

Proposition. The leading term of a non-zero Hibi relation

$$x_a\, x_b - x_{a \wedge b}\, x_{a \vee b}$$

for $a, b \in L$ is given by $x_a\, x_b$. The leading term of the norming polynomial $\sum_{a \in L} x_a^2 - 1$ is given by $(x_\top)^2$, where $\top$ denotes the top in L.

Proof. Since the Hibi relation does not vanish, $a \neq b$ in L. Assuming $a <' b$ (without loss of generality), we obtain $a \wedge b <' a <' b <' a \vee b$. Let $L_0 := \{a, b, a \wedge b, a \vee b\}$ be the smallest sublattice of L which contains a and b. The terms $x_a\, x_b$ and $x_{a \wedge b}\, x_{a \vee b}$ are identified with elements in $\mathbb{N}_0^L$ as outlined above. If we consider only those positions which belong to an element in L_0 (since the entries on all other positions vanish), then the first term is identified with $\alpha := (0,\ 1,\ 1,\ 0)$ and the second term is identified with $\beta := (1,\ 0,\ 0,\ 1)$. Since $\alpha - \beta = (-1,\ 1,\ 1,\ -1)$ (or from Proposition 1.1.4), it follows that $\alpha >_{\text{grevlex}} \beta$, and thus, $x_a\, x_b >_{\text{grevlex}} x_{a \wedge b}\, x_{a \vee b}$.

With respect to the graded reverse lexicographical order, the term $x_\top^2$ is the largest amongst the terms x_c^2, $c \in L$. ◇

Indeed, this term order is an example for a so-called compatible term order, see [HHO, Chapter 6].

Example. In the special case where $L := \{1, 2\}^2$ and with the linear extension from Example 5.3.1, the leading term of the determinantal Hibi relation $x_{21} x_{12} - x_{22} x_{11}$ is $x_{21} x_{12}$.

5.3.3 Two Reduction Relations

The multivariate polynomial division by the non-zero Hibi relations $\mathcal{H}_L$ with respect to the graded reverse lexicographical order defines a reduction relation $\longrightarrow_{\mathcal{H}_L}$ on the polynomial ring $\mathbb{K}[x_a \colon a \in L]$, see Subsection 1.2.2. It is closely related to the reduction relation $\longrightarrow$ on the terms in $\mathbb{K}[x_a \colon a \in L]$ (the terms of degree $m \in \mathbb{N}_0$ can be identified with L^m/S_m), which is introduced in Section 5.2:

Proposition. Let $m \in \mathbb{N}_0$ and $\overline{a}, \overline{b} \in L^m/S_m$. The restriction of $\longrightarrow_{\mathcal{H}_L}$ to L^m/S_m is equal to $\longrightarrow$, that is, the following are equivalent:

(a) $\overline{a} \xrightarrow{\star} \overline{b}$.

(b) $\overline{x}_{\overline{a}} \xrightarrow{\star}_{\mathcal{H}_L} \overline{x}_{\overline{b}}$.

In particular, in this case, we have

$$\overline{x}_{\overline{a}} \geqslant_{\text{grevlex}} \overline{x}_{\overline{b}}.$$

Proof. Let $m \geqslant 2$. According to Proposition 5.3.2, the leading term of a non-zero Hibi relation $x_c\, x_d - x_{c \wedge d}\, x_{c \vee d}$, where $c, d \in L$, with respect to the graded reverse lexicographical order is given by $x_c\, x_d$. Now, with a similar argument, for all terms s, we obtain

$$s \cdot x_a \cdot x_b \geqslant_{\text{grevlex}} s \cdot x_{c \wedge d} \cdot x_{c \vee d}.$$

If $\overline{a} \longrightarrow \overline{b}$, then from Proposition 5.2.3.III (i), it follows that there exists $\overline{c} \in L^{m-2}/S_{m-2}$ and a non-zero Hibi relation $h \in \mathcal{H}_L$ such that

$$\overline{x}_{\overline{a}} = \overline{x}_{\overline{c}} \cdot h + \overline{x}_{\overline{b}},$$

where $\overline{x}_{\overline{a}} = s \cdot \mathrm{LT}(h)$ for the term $s := \overline{x}_{\overline{c}}$. By definition of $\longrightarrow_{\mathcal{H}_L}$, it follows that $\overline{x}_{\overline{a}} \longrightarrow_{\mathcal{H}_L} \overline{x}_{\overline{b}}$.

On the other hand, if $\overline{x}_{\overline{a}}$ reduces to $\overline{x}_{\overline{b}}$ modulo $\{h\}$, where $h \in \mathcal{H}_L$, then $\overline{x}_{\overline{a}} = s \cdot h + \overline{x}_{\overline{b}}$, where s is a term such that $s \cdot \mathrm{LT}(h) = \overline{x}_{\overline{a}}$. By definition of $\longrightarrow$, it follows that $\overline{a} \longrightarrow \overline{b}$.

The general statements for $\overline{a} \xrightarrow{\star} \overline{b}$ and $\overline{x}_{\overline{a}} \xrightarrow{\star}_{\mathcal{H}_L} \overline{x}_{\overline{b}}$ follow by induction. ◇

Lemma. Let $f \in \mathbb{K}[x_a \colon a \in L]$. The normal form of f modulo $\mathcal{H}_L$ is given by $\mathcal{M}(f)$.

Proof. In general, the multivariate polynomial division has no additive property according to Example 1.2.2 (iii). However, the last proposition states that the reduction relations $\longrightarrow_{\mathcal{H}_L}$ and $\longrightarrow$ are closely related, which will be essential for the proof.

Step 1: On the one hand, by any single reduction step modulo $\longrightarrow_{\mathcal{H}_L}$, a term $x_{\overline{a}}$ is replaced by a term $x_{\overline{b}}$, where $\overline{a} \longrightarrow \overline{b}$. Hence, the median $\mathcal{M}(f)$ is a normal form modulo $\longrightarrow_{\mathcal{H}_L}$.

Step 2: On the other hand, any term $x_{\overline{a}}$ with $\overline{a} \neq \mathcal{M}(\overline{a})$ can be reduced modulo $\longrightarrow_{\mathcal{H}_L}$ to a term $x_{\overline{b}}$ with $\overline{a} \longrightarrow \overline{b}$ by a single reduction step. Hence, if r is a normal form modulo $\longrightarrow_{\mathcal{H}_L}$, then all terms of r are normal forms with respect to $\longrightarrow$. Thus, combined with step 1, the normal forms modulo $\longrightarrow_{\mathcal{H}_L}$ are exactly the medians.

Step 3: We have seen above that a single reduction step does not affect more than a single term. Also, $\overline{a} \xrightarrow{\star} \overline{b}$ and $\overline{a} \xrightarrow{\star} \overline{c}$ implies that $\overline{a}$,$\overline{b}$ and $\overline{c}$ have a common normal form with respect to $\longrightarrow$. It follows that amongst all polynomials g with $f \xrightarrow{\star}_{\mathcal{H}_L} g$, there exists only one normal form, which equals the median $\mathcal{M}(f)$ of f. ◇

5.3.4 A Gröbner Basis of the (Norm-)Join-Meet Ideal

The first part of the following theorem is an adaption of [HHO, Theorem 6.17]. For the proof, we use the reduction relation $\longrightarrow$ of Section 5.2, which seems to be a new approach. The second part generalises [Sto, Theorem 4.8] by replacing determinantal Hibi relations with arbitrary distributive lattices. Also here, the reduction relation is used for the proof.

Theorem. With respect to the graded reverse lexicographical order $\leqslant_{\text{grevlex}}$ based on a lattice-preserving order on L, the non-zero Hibi relations $\mathcal{H}_L$ are a reduced Gröbner basis of the join-meet ideal $\mathcal{I}_L$.

Moreover, the non-zero Hibi relations $\mathcal{H}_L$ together with the norming polynomial u_L are a reduced Gröbner basis of the norm-join-meet ideal $\mathcal{J}_L$.

Proof. Let $\mathcal{N}_L := \{u_L\}$.

Statement 1: $\mathcal{H}_L$ is a Gröbner basis of $\mathcal{I}_L$.

By definition, $\mathcal{H}_L$ generates $\mathcal{I}_L$. The statement follows from Theorem 1.2.3 (a) and Lemma 5.3.3.

Statement 2: $\mathcal{H}_L$ is reduced.

Condition (i) from Definition 1.2.5 is fulfilled since the leading coefficients are always equal to 1. Let g be a non-zero Hibi relation. To show condition (ii), we show with Lemma 1.1.2 that no term of g lies in the monomial ideal generated by the leading terms of the other non-zero Hibi relations. A non-zero Hibi relation h is uniquely defined by the term $x_a\, x_b$, where $a, b \in L$ are not comparable, and $h = x_a\, x_b - x_{a\wedge b}\, x_{a\vee b}$. According to Proposition 5.3.2, the first term is the leading term of h. The second term is a chain. Hence, none of the two terms can be the leading term of any other Hibi relation.

Statement 3: $\mathcal{H}_L \cup \mathcal{N}_L$ is a Gröbner basis of $\mathcal{J}_L$.
By definition, $\mathcal{H}_L \cup \mathcal{N}_L$ generates $\mathcal{J}_L$. Using the Buchberger Criterion Theorem 1.2.4 and the previous results, it suffices to show that $S(h, u_L)$ reduces to zero for all $h \in \mathcal{H}_L$. According to Proposition 5.3.2, there exist $a, b \in L$ such that the leading term of h is given by $x_a\, x_b$, where a and b are not comparable, and the leading term of u_L is given by $x_\top^2$, where $\top$ is the top element in L. Since $x_\top$ is comparable with any element in L, it follows that $x_a \neq x_\top \neq x_b$. Hence, $x_\top^2$ is coprime with $x_a\, x_b$, that is, h and u_L are relatively prime. According to Proposition 1.2.4, $S(h, u_L)$ reduces to zero.

Statement 4: $\mathcal{H}_L \cup \mathcal{N}_L$ is reduced.
The Gröbner basis is reduced since the leading coefficient of u_L is equal to 1 and no term of u_L is equal to any term of any Hibi relation. ◇

Remark. Theorem 1.2.3 and the Buchberger Criterion Theorem 1.2.4 allow different viewpoints on Gröbner bases. From each viewpoint, it could be possible to show that $\mathcal{H}_L$ is a Gröbner basis of $\mathcal{I}_L$. Here, we give a sketch of an alternative proof using the Buchberger Criterion, since it is common in the literature (see [HHO] and [RS2]).

Statement: $\mathcal{H}_L$ is a Gröbner basis of $\mathcal{I}_L$ with respect to the graded reverse lexicographical order.

Proof: Using the Buchberger Criterion, it is sufficient to verify that the S-polynomial of two non-zero Hibi relations f, h with $f \neq h$ reduces to zero modulo $\mathcal{H}_L$. The leading terms of f and h are given by $LT(f) = x_a\, x_b$ and $LT(h) = x_c\, x_d$, where $a, b, c, d \in L$. They are relatively prime, if and only if $x_a\, x_b$ and $x_c\, x_d$ are coprime, that is, if and only if a, b, c, d are pairwise distinct. In this case, the S-polynomial $S(f, h)$ reduces to zero modulo $\mathcal{I}_L$ according to Proposition 1.2.4. It remains to consider the case that f and h are not relatively prime. We may assume that $a = d$. The least common multiple of the leading terms is given by $x_a\, x_b\, x_c$. Hence, the S-polynomial of f and h is given by

$$\begin{aligned} S(f,h) &= x_c \cdot f - x_b \cdot h \\ &= x_c \cdot (x_a\, x_b - x_{a\wedge b}\, x_{a\vee b}) - x_b \cdot (x_a\, x_c - x_{a\wedge c}\, x_{a\vee c}) \\ &= x_b\, x_{a\wedge c}\, x_{a\vee c} - x_c\, x_{a\wedge b}\, x_{a\vee b}. \end{aligned}$$

By Lemma 5.3.3, the normal form of $S(f,h)$ modulo $\mathcal{H}_L$ is given by

$$\mathcal{M}(S(f,h)) = \overline{x}_{\mathcal{M}(b,a\wedge c,a\vee c)} - \overline{x}_{\mathcal{M}(c,a\wedge b,a\vee b)} = 0,$$

since $(a,b,c) \xrightarrow{\star} (b, a\wedge c, a\vee c)$ and $(a,b,c) \xrightarrow{\star} (c, a\wedge b, a\vee b)$, that is, both terms have the same median (which equals $\mathcal{M}(a,b,c) = (s,m,l)$ from Subsection 5.2.4).

Hence, the S-polynomial of f and h reduces to zero.

5.4 Complex Hibi Relations and Gröbner Bases

In this section, we investigate the following question:

Does there exist a term order such that the non-zero complex Hibi relations, also together with the complex norming polynomial, are a Gröbner basis?

We will see that the answer is positive in the special case where $L = \{1,2\}^2$, which corresponds to the tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2$. In the general case, we focus on term orders which, in appropriate senses, could be regarded as promising candidates for a positive answer. But it seems not to be easy to obtain a positive answer. So an answer to the question remains open, even though computations with a computer algebra system suggest that it is negative.

Nevertheless, the complex Hibi relations provide a basis of the second homogeneous part of the complex-join-meet ideal.

We use the notation from Table 5.1 on page 115 and from Table 5.2. Elements in $L_{\mathbb{C}}$ are written in the form $a{,}1$ and $a{,}2$, where $a \in L$. If it seems to be convenient, the letter "x" in the notation for variables in $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ is omitted.

5.4.1 A Gröbner Basis in a Special Case

The following example outlines that the answer is positive in a special case.

Example. Let $L = \{1, 2\}^2$. The complex-norm-join-meet ideal is generated by

$$\begin{aligned} f_1 &:= 2\,1{,}2 \cdot 1\,2{,}2 - 2\,2{,}2 \cdot 1\,1{,}2 - 2\,1{,}1 \cdot 1\,2{,}1 + 2\,2{,}1 \cdot 1\,1{,}1, \\ f_2 &:= 1\,1{,}2 \cdot 2\,2{,}1 - 1\,2{,}2 \cdot 2\,1{,}1 - 2\,1{,}2 \cdot 1\,2{,}1 + 2\,2{,}2 \cdot 1\,1{,}1, \\ u &= 2\,2{,}2^2 + 2\,1{,}2^2 + 1\,2{,}2^2 + 1\,1{,}2^2 \\ &\quad + 2\,2{,}1^2 + 2\,1{,}1^2 + 1\,2{,}1^2 + 1\,1{,}1^2 - 1\,. \end{aligned}$$

Based on the total order on $L_{\mathbb{C}}$ which is given by

$$1\,1{,}1 < 1\,2{,}1 < 2\,1{,}1 < 2\,2{,}1 < 1\,1{,}2 < 1\,2{,}2 < 2\,1{,}2 < 2\,2{,}2$$

and with respect to the graded reverse lexicographical term order, the leading terms of the three polynomials are

$$\mathrm{LT}(f_1) = 2\,1{,}2 \cdot 1\,2{,}2,\ \mathrm{LT}(f_2) = 1\,1{,}2 \cdot 2\,2{,}1,\ \mathrm{LT}(u) = 2\,2{,}2^2.$$

Since each two of the three leading terms are relatively prime, the three S-polynomials $S(f_1, f_2)$, $S(f_1, u)$, $S(f_2, u)$ reduce to zero modulo f_1, f_2 and u. Hence, with respect to this term order, $\{f_1, f_2, u\}$ is a Gröbner basis.

5.4.2 Criteria on the Total Order

Example 5.4.1 shows that the answer of the introductory question is positive in a special case. Now, we investigate whether it is positive also for arbitrary lattices L.

To do so, we focus on different term orders which could be regarded as promising candidates.

The non-zero Hibi relations $\mathcal{H}_L$, together with the norming polynomial u_L, are a Gröbner basis according to Theorem 5.3.4. An appropriate term order on $\mathbb{K}[x_a \colon a \in L]$ is the graded reverse lexicographical order which is based on a linear extension of L. Such a term order is closely related to the reduction relation $\longrightarrow$ from Section 5.2, see Proposition 5.3.3 and Lemma 5.3.3.

We should therefore have in mind that a term order on the polynomial ring $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ induces a reduction relation which is induced by the multivariate polynomial division by the non-zero complex Hibi relations $\mathcal{H}_{L_{\mathbb{C}}}$ (and the complex norming polynomial $u_{L_{\mathbb{C}}}$). It could be promising to consider term orders which are (in an appropriate sense) related to the reduction relation $\longrightarrow$ or to the graded reverse lexicographical order.

A term order on $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ induces a total order $\leqslant$ on the variables, that is, on the elements in $L_{\mathbb{C}}$. The orders which are involved are shown in the following diagram:

$$\begin{tikzcd}
(L, \leqslant') \arrow[r] \arrow[d] & (L_{\mathbb{C}}, \leqslant) \arrow[d] \\
(\mathbb{N}_0^L, \leqslant_{\text{grevlex}}) \arrow[r] & (\mathbb{N}_0^{L_{\mathbb{C}}}, \leqslant) \\
\mathbb{K}[x_a \colon a \in L] & \mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]
\end{tikzcd}$$

Now, we collect some possible criteria on $\leqslant$. The term orders which we suggest in the following fulfil some of the criteria (not all together, since they can be contradictory):

C1: If $a < b$ in L, then $a{,}1 < b{,}1$ and $a{,}2 < b{,}2$.
C2: For all $a, b \in L$, we have $a{,}1 < b{,}2$.
C3: For all $a \in L$, we have $a{,}1 < a{,}2$.

With respect to a linear extension $<'$ of L, the following criteria are also possible:

C4: If $a <' b$ in L, then $a{,}1 < b{,}1$ and $a{,}2 < b{,}2$.
C5: If $a <' b$ in L, then for all $t_1, t_2 \in \{1, 2\}$, we have $a{,}t_1 < b{,}t_2$.

Criterion C5 is stronger than criterion C4, which is stronger than criterion C1. Criterion C2 is stronger than criterion C3.

5.4.3 Stacking Orders

We begin with a notion which could be regarded as a generalisation of the term order from the last example. We note that C2 and C4 together define $\leqslant$ completely (and imply C1): For all $a <' b$ in L, we have

$$\cdots < a{,}1 < \cdots < b{,}1 < \cdots < a{,}2 < \cdots < b{,}2 < \ldots$$

Definition. Let $\leqslant'$ be a linear extension of L. Based on the total order $\leqslant$ on $L_{\mathbb{C}}$ with C2 and C4, the graded reverse lexicographical order on $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ is called the *stacking order* with respect to $\leqslant'$.

Indeed, Example 5.4.1 shows that a stacking order can give a positive answer for $\{1, 2\}^2$. However, in general, a stacking order does not seem to give a positive answer. To see this, we consider the lattice D_2 from Example 4.2.5.

Proposition. If $L = D_2$, then the non-zero complex Hibi relations are no Gröbner basis with respect to a stacking term order on $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$.

Proof. Let L be an arbitrary finite distributive lattice and let $e, f \in L$ such that e and f are not comparable. Let $d := d(e, f) := e \cdot f - e{\wedge}f \cdot e{\vee}f$ be a non-zero Hibi relation. Let $\leqslant$ be the stacking term order with respect to a linear extension $\leqslant'$ of L. Since we have

$$\begin{aligned} \operatorname{Re} d &= e{,}1 \cdot f{,}1 \;-\; e{,}2 \cdot f{,}2 \;-\; e{\wedge}f{,}1 \cdot e{\vee}f{,}1 \;+\; e{\wedge}f{,}2 \cdot e{\vee}f{,}2, \\ \operatorname{Im} d &= e{,}1 \cdot f{,}2 \;+\; e{,}2 \cdot f{,}1 \;-\; e{\wedge}f{,}1 \cdot e{\vee}f{,}2 \;-\; e{\wedge}f{,}2 \cdot e{\vee}f{,}1, \end{aligned}$$

the leading term of $\operatorname{Re} d$ equals $e{,}2 \cdot f{,}2$ and the leading term of $\operatorname{Im} d$ equals $e{\wedge}f{,}2 \cdot e{\vee}f{,}1$.

Now, we assume that L is equal to D_2. To prove the assumption, it suffices to show that there are two complex Hibi relations whose S-polynomial does not reduce to zero. To do this, we consider the complex Hibi relations $g_1 := \operatorname{Im}(d(a, c))$ and $g_2 := \operatorname{Im}(d(b, c))$, that is,

$$\begin{aligned} g_1 &= a{,}1 \cdot c{,}2 \;+\; a{,}2 \cdot c{,}1 \;-\; s{,}1 \cdot a{\vee}c{,}2 \;-\; s{,}2 \cdot \underline{a{\vee}c{,}1}, \\ g_2 &= b{,}1 \cdot c{,}2 \;+\; b{,}2 \cdot c{,}1 \;-\; s{,}1 \cdot l{,}2 \;-\; \underline{s{,}2 \cdot l{,}1}. \end{aligned}$$

The leading terms of g_1 and g_2 are underlined, respectively. They are not relatively prime, since $s{,}2$ is a common factor. The S-polynomial of g_1 and g_2 is given by

$$\begin{aligned} S(g_1, g_2) &= l{,}1 \cdot g_1 \;-\; a{\vee}c{,}1 \cdot g_2 \\ &= \underline{a{,}1 \cdot c{,}2 \cdot l{,}1} \;+\; \underline{a{,}2 \cdot c{,}1 \cdot l{,}1} \\ &\quad - s{,}1 \cdot a{\vee}c{,}2 \cdot l{,}1 \;-\; \underline{b{,}1 \cdot c{,}2 \cdot a{\vee}c{,}1} \\ &\quad - \underline{b{,}2 \cdot c{,}1 \cdot a{\vee}c{,}1} \;+\; s{,}1 \cdot l{,}2 \cdot a{\vee}c{,}1. \end{aligned}$$

Now, using the introductory comments, we show that the leading term t of $S(g_1, g_2)$ cannot be divisible by the leading term of any complex Hibi relation. By exclusion, we can identify four terms which could be the leading term of $S(g_1, g_2)$. The terms in question are underlined.

Case 1: $t = a{,}1 \cdot c{,}2 \cdot l{,}1$.
It is clear that $a{,}1 \cdot l{,}1$ cannot be a leading term. Also $a{,}1 \cdot c{,}2$ since a and c are not comparable and $c{,}2 \cdot l{,}1$ since c and l are not top and bottom of a rhomb.

Case 2: $t = b{,}1 \cdot c{,}2 \cdot a{\vee}c{,}1$.

It is clear that $b,1 \cdot a \vee c,1$ cannot be a leading term. Also $b,1 \cdot c,2$ since b and c are not comparable and $c,2 \cdot a \vee c,1$ since c and $a \vee c,1$ are not top and bottom of a rhomb.

Case 3: $t = a,2 \cdot c,1 \cdot l,1$.
This case requires that $a,1 <' b,1 <' c,1$. As above, $c,1 \cdot l,1$ cannot be a leading term; also $a,2 \cdot c,1$ since a and c are not comparable. The term $a,2 \cdot l,1$ is the leading term of $g_3 := \mathrm{Im}(d(b, a \vee c))$, that is,

$$g_3 = b,1 \cdot a \vee c,2 \;+\; b,2 \cdot a \vee c,1 \;-\; a,1 \cdot l,2 \;-\; \underline{a,2 \cdot l,1}.$$

Reducing $S(g_1, g_2)$ modulo g_3 leads to

$$\begin{aligned} S(g_1, g_2) + c,1 \cdot g_3 = a,1 \cdot c,2 \cdot l,1 \;&-\; s,1 \cdot a \vee c,2 \cdot l,1 \\ -\; \underline{b,1 \cdot c,2 \cdot a \vee c,1} \;&+\; s,1 \cdot l,2 \cdot a \vee c,1 \\ +\; c,1 \cdot b,1 \cdot a \vee c,2 \;&-\; c,1 \cdot a,1 \cdot l,2. \end{aligned}$$

The leading term is underlined. But this term cannot be a leading term of a complex Hibi relation, see the preceding case.

Case 4: $t = b,2 \cdot c,1 \cdot a \vee c,1$.
It is clear that $c,1 \cdot a \vee c,1$ cannot be a leading term. Also $b,2 \cdot c,1$ since b and c are not comparable and $b,2 \cdot a \vee c,1$ since b and $a \vee c$ are not comparable.

It follows that $S(g_1, g_2)$ does not reduce to zero. ◇

5.4.4 Expanding Orders

Also the next notion does not provide a positive answer.

Definition. Let $\leqslant'$ be a linear extension of L. A term order $\leqslant$ on $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ is called an *expanding order* with respect to $\leqslant'$, if

(i) The term order $\leqslant$ fulfils C5 with respect to $\leqslant'$.

(ii) For all $m \in \mathbb{N}$, for all $a_1, \ldots, a_m \in L$, $b_1, \ldots, b_m \in L$, where

$$a_1 \cdot a_2 \cdot \ldots \cdot a_m < b_1 \cdot b_2 \cdot \ldots \cdot b_m,$$

and for all $t_1, \ldots, t_m \in \{1, 2\}$, we have

$$a_1,t_1 \cdot a_2,t_2 \cdot \ldots \cdot a_m,t_m < b_1,t_1 \cdot b_2,t_2 \cdot \ldots \cdot b_m,t_m.$$

Proposition. If L contains a rhomb, then the non-zero complex Hibi relations are no Gröbner basis with respect to an expanding term order on $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$.

Proof. Let $d = a \cdot b - a{\wedge}b \cdot a{\vee}b$ be a non-zero Hibi relation (where $a, b \in L$ such that a and b are not comparable). Let $\leqslant$ be an expanding term order. Since we have

$$\begin{aligned} \operatorname{Re} d &= a{,}1 \cdot b{,}1 \ - \ a{,}2 \cdot b{,}2 \ - \ a{\wedge}b{,}1 \cdot a{\vee}b{,}1 \ + \ a{\wedge}b{,}2 \cdot a{\vee}b{,}2, \\ \operatorname{Im} d &= a{,}1 \cdot b{,}2 \ + \ a{,}2 \cdot b{,}1 \ - \ a{\wedge}b{,}1 \cdot a{\vee}b{,}2 \ - \ a{\wedge}b{,}2 \cdot a{\vee}b{,}1, \end{aligned}$$

the leading term of $\operatorname{Re} d$ equals $a{,}1 \cdot b{,}1$ or $a{,}2 \cdot b{,}2$, and the leading term of $\operatorname{Im} d$ equals $a{,}1 \cdot b{,}2$ or $a{,}2 \cdot b{,}1$. Without loss of generality, we may assume that $\mathrm{LT}(\operatorname{Re} d) = a{,}1 \cdot b{,}1$ and $\mathrm{LT}(\operatorname{Im} d) = a{,}1 \cdot b{,}2$. The terms are not relatively prime, since $a, 1$ is a common factor. The S-polynomial of $\operatorname{Re} d$ and $\operatorname{Im} d$ is given by

$$\begin{aligned} S(\operatorname{Re} d, \operatorname{Im} d) &= b{,}2 \cdot \operatorname{Re} d \ - \ b{,}1 \cdot \operatorname{Im} d \\ &= - \ b{,}2 \cdot a{,}2 \cdot b{,}2 \ - \ b{,}1 \cdot a{,}2 \cdot b{,}1 \\ &\quad - \ b{,}2 \cdot a{\wedge}b{,}1 \cdot a{\vee}b{,}1 \ + \ b{,}1 \cdot a{\wedge}b{,}1 \cdot a{\vee}b{,}2 \\ &\quad + \ b{,}2 \cdot a{\wedge}b{,}2 \cdot a{\vee}b{,}2 \ + \ b{,}1 \cdot a{\wedge}b{,}2 \cdot a{\vee}b{,}1. \end{aligned}$$

With the introductory comments on the leading term of a complex Hibi relation with respect to an expanding order, we may show whether any of the six terms can be divisible by the leading term of $\operatorname{Re} h$ or $\operatorname{Im} h$ for any non-zero complex Hibi relation h. We first state that both $b{,}2^2 \cdot a{,}2$ and $b{,}1^2 \cdot a{,}2$ cannot be divisible by any leading term (we note that this also holds for $h = d$). Also the four remaining terms cannot be divisible, since $a{\wedge}b < b < a{\vee}b$ in L. It follows that $S(\operatorname{Re} d, \operatorname{Im} d)$ is reduced, but not zero. ◇

Example. Based on a lattice-preserving order $\leqslant'$ on L, conditions C3 and C5 define a total order $\leqslant$ on $L_{\mathbb{C}}$: It is given by

$$\cdots < a{,}1 < a{,}2 < \cdots < b{,}1 < b{,}2 < \ldots$$

whenever $a <' b$ in L.

The set $L_{\mathbb{C}} = L \times \{1, 2\}$ can be regarded as lattice: It is the direct product of L with the chain $\{1, 2\}$, where 2 is the top and 1 is the bottom. In this respect, $\leqslant$ is lattice-preserving for $L_{\mathbb{C}}$.

The graded reverse lexicographical order based on $\leqslant$ is expanding. The leading terms of the real and imaginary part of a non-zero Hibi relation $d := a \cdot b - a{\wedge}b \cdot a{\vee}b$, where $a, b \in L$ are not comparable, are given by

$$\mathrm{LT}(\operatorname{Re} d) = a{,}2 \cdot b{,}2,$$

$$\mathrm{LT}(\mathrm{Im}\, d) = \begin{cases} a{,}1 \cdot b{,}2, & a >' b, \\ a{,}2 \cdot b{,}1, & a <' b. \end{cases}$$

Example. Let $L = \{1, 2\}^2$. The graded reverse lexicographical order based on the total order on $L_{\mathbb{C}}$ which is given by

$$1\,1{,}1 < 1\,1{,}2 < 1\,2{,}1 < 1\,2{,}2 < 2\,1{,}1 < 2\,1{,}2 < 2\,2{,}1 < 2\,2{,}2$$

is expanding, see the last example. The leading terms of the polynomials f_1, f_2 and u from Example 5.4.1 are

$$\mathrm{LT}(f_1) = 1\,2{,}2 \cdot 2\,1{,}2,\ \mathrm{LT}(f_2) = 1\,2{,}2 \cdot 2\,1{,}1,\ \mathrm{LT}(u) = 2\,2{,}2^2.$$

In contrast to Example 5.4.1, the first two leading terms are not relatively prime. According to Proposition 5.4.4, with respect to this term order, $\{f_1, f_2, u\}$ is not a Gröbner basis.

5.4.5 Numerical Examples

With the help of the computer algebra program *SageMath*, see [Sage], we computed the reduced Gröbner basis (GB) of the ideal for the complex normed Hibi variety with respect to different term orders. There are $\#\mathcal{H}_{L_{\mathbb{C}}} = 2 \cdot \#\mathcal{H}_L$ complex Hibi relations and 1 complex norming polynomial. If the length of the reduced GB is larger than $\#\mathcal{H}_{L_{\mathbb{C}}} + 1$, then they are not a GB with respect to the underlying order. Nevertheless, a comparison of lengths could give rise to ideas for promising term orders. With the program, we only consider graded reverse lexicographical orders which base on the lexicographical order on L and which fulfil condition C3.

Example. Let $L = \{1, 2\}^3$. There are 18 complex Hibi relations. For example, we consider the following term order, which we refer to as the *mixed order*:

$$\begin{aligned} &\ 2\,2\,2{,}2 < 2\,2\,1{,}2 < 2\,1\,2{,}2\ \ldots \\ &< 2\,2\,2{,}1 < 2\,2\,1{,}1 < 2\,1\,2{,}1\ \ldots \\ &< 2\,1\,1{,}2 < 1\,2\,2{,}2 < 1\,2\,1{,}2 < 1\,1\,2{,}2 < 1\,1\,1{,}2\ \ldots \\ &< 2\,1\,1{,}1 < 1\,2\,2{,}1 < 1\,2\,1{,}1 < 1\,1\,2{,}1 < 1\,1\,1{,}1\,. \end{aligned}$$

The following table lists three different term orders together with the length of the reduced GB of the ideal for the complex normed Hibi variety.

Term order	Length GB
Stacking order	42
Expanding order with C3 and grevlex	42
Mixed order	36

Since $\min(42, 36) > 19$, an answer to the introductory question for the lattice $\{1, 2\}^3$, which corresponds to the tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$, is still open. The mixed order provides the shortest GB, which suggests that the stacking and expanding orders may not be the most promising candidates for a positive answer. Nevertheless, 36 was the smallest length which could be reached by a test with randomly generated term orders with the required properties.

5.4.6 A Basis of the Second Homogeneous Part

Using the median basis, we obtain the following statement:

Proposition. A basis of the second homogeneous part of the complex-join-meet ideal $\imath(\mathcal{J}_L)$ is given by the real and the imaginary parts of the non-zero Hibi relations in $\mathbb{R}[x_a \colon a \in L]$.

Proof. This statement follows from Corollary 1.3, Proposition 2.2.7 and Theorem 5.2.7. ◇

The second homogeneous part of $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$ equals the direct sum of the vector spaces

$$\begin{aligned} V_{\mathrm{Re,Re}} &:= \mathrm{LH}(a{,}1 \cdot b{,}1 \,:\, a, b \in L), \\ V_{\mathrm{Im,Im}} &:= \mathrm{LH}(a{,}2 \cdot b{,}2 \,:\, a, b \in L), \text{ and} \\ V_{\mathrm{Re,Im}} &:= \mathrm{LH}(a{,}1 \cdot b{,}2 \,:\, a, b \in L). \end{aligned}$$

Let $a, b \in L$ be not comparable. The real and the imaginary part of the Hibi relation $d := a \cdot b - a{\wedge}b \cdot a{\vee}b$ are given by

$$\begin{aligned} \mathrm{Re}(d) &= (a{,}1 \cdot b{,}1 - a{\wedge}b{,}1 \cdot a{\vee}b{,}1) - (a{,}2 \cdot b{,}2 - a{\wedge}b{,}2 \cdot a{\vee}b{,}2), \\ \mathrm{Im}(d) &= a{,}1 \cdot b{,}2 + a{,}2 \cdot b{,}1 - a{\wedge}b{,}1 \cdot a{\vee}b{,}2 - a{\wedge}b{,}2 \cdot a{\vee}b{,}1. \end{aligned}$$

Now, it is obvious that $\mathrm{Re}(d) \in V_{\mathrm{Re,Re}} + V_{\mathrm{Im,Im}}$ and $\mathrm{Im}(d) \in V_{\mathrm{Re,Im}}$.

5.5 Attributes of the Hibi Variety

So far, we have considered the Hibi variety as an affine variety. In this section, we consider it as a projective variety to determine its dimension and its degree according to [HHO, Theorem 6.38].

With the aid of Gröbner bases, we show that the vanishing ideal of the Hibi variety is not larger than the join-meet ideal. Hence, a polynomial which vanishes on the Hibi variety is completely determined by the Hibi relations.

5.5.1 The Coordinate Ring

For each $\overline{a} \in L^m/S_m$, let $U_{[\overline{a}]}$ be the linear subspace of $(\mathcal{J}_L)_m$ which is spanned by all terms $\overline{x}_{\overline{b}}$ with $\overline{a} \overset{\star}{\longleftrightarrow} \overline{b}$. It can be identified with the Euclidean vector space $\mathbb{K}^{\#[\overline{a}]}$ as follows: Since the median $\mathcal{M}(\overline{a})$ is a canonical representative of the equivalence class $[\overline{a}]$, it can be identified with the last coordinate. The other coordinates are identified with the other elements of $[\overline{a}]$.

Now, $V_{[\overline{a}]}$ equals the linear hull of the vectors

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ -1 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ -1 \end{pmatrix}.$$

It is a subspace of $U_{[\overline{a}]}$ of codimension 1 and equals the orthogonal complement of the vector

$$u_{[\overline{a}]} := \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}.$$

Hence, a basis of the coordinate ring is given by the vectors $u_{[\overline{a}]} + \mathcal{J}_L$ (or, alternatively, by the vectors $\overline{a} + \mathcal{J}_L$) for all chains $\overline{a} \in L^m/S_m$.

Let $\mathbb{K}[x_a \colon a \in L])_m/(\mathcal{J}_L)_m$ be the m^{th} *homogeneous part* of the coordinate ring $\mathbb{K}[x_a \colon a \in L]/\mathcal{J}_L$. It is a direct sum of the quotients

U_R/V_R of dimension 1, where $R \in \mathcal{R}_m$. The coordinate ring can be decomposed into its homogeneous parts:

$$\mathbb{K}[x_a \colon a \in L]/\mathcal{I}_L = \bigoplus_{m \in \mathbb{N}_0} \Big(\bigoplus_{R \in \mathcal{R}_m} U_R/V_R \Big).$$

Hence, for all $m \in \mathbb{N}_0$, we have

$$\dim\big((\mathbb{K}[x_a \colon a \in L])_m/(\mathcal{I}_L)_m\big) = \#\mathcal{R}_m \,,$$

which equals the number of all chains in L^m/S_m.

5.5.2 Dimension and Degree of the Product Vectors

Since the Hibi relations are homogeneous, the Hibi variety can also be regarded as a projective variety, the *projective Hibi variety*, see Subsection 2.1.5.

The projective Hibi variety equals set of zeros of the join-meet ideal $\mathcal{I}_L \subseteq \mathbb{C}[x_a \colon a \in L]$ in the projective space $\mathbb{P}^{\#L-1}$. Its Hilbert function is given by $\mathbb{N}_0 \to \mathbb{N}_0, m \mapsto \#\mathcal{R}_m$. The Hilbert polynomial gives the dimension and the degree of the projective Hibi variety, see [HHO].

Hence, the product vectors in the tensor product $\mathbb{C}^N$ can be characterised as a projective variety. Here, we determine the dimension and the degree of the projective Hibi variety in this special case.

In the special case where $r = 2$, the projective Hibi variety equals the Segré variety which is discussed widely in [Har] (see also Subsection 3.4.3). To be consistent with the notation there, we use the lattice $N_0 := \{0, \dots, n_1\} \times \cdots \times \{0, \dots, n_r\}$ instead of N, and consider the join-meet ideal $\mathcal{I}_{N_0}$ in $\mathbb{C}[x_a \colon a \in N_0]$ and the projective Hibi variety in $\mathbb{P}^{\prod_{l=1}^r (n_l+1)-1}$. The product vectors $\mathcal{Z}_\mathbb{C}(\mathcal{I}_N)$ can be identified with those points of $\mathbb{P}^{\prod_{l=1}^r (n_l+1)-1}$ in $\mathcal{Z}_\mathbb{C}(\mathcal{I}_{N_0})$ which have the form $1 : 1 : \cdots : 1 : v$, where $v \in \mathbb{C}^N$ (the other positions belong to the elements in N_0 with at least one entry which equals 0).

Lemma. The dimension of the mth homogeneous part of the coordinate ring $\mathbb{K}[x_a \colon a \in N]/\mathcal{I}_N$ is given by

$$\#\mathcal{R}_m = \prod_{l=1}^{r} \binom{n_l + m - 1}{m} \,.$$

The function $\mathbb{N}_0 \to \mathbb{N}_0, m \mapsto \#\mathcal{R}_m$ is a polynomial in m, whose leading term equals

$$\left(\prod_{l=1}^{r}(n_l-1)!\right)^{-1} \cdot m^{\sum_{l=1}^{r}(n_l-1)}.$$

Proof. According to Example 5.2.6.II, a chain in L^m/S_m can be identified with a $m \times r$ matrix $(a_{k,l})_{k\in\{1,\dots,m\},l\in\{1,\dots,r\}}$, where $1 \leqslant a_{k,l} \leqslant a_{k+1,l} \leqslant n_l$ for all $k \in \{1,\dots,m\}$, $l \in \{1,\dots,r\}$. The number of possibilities to fill the l^{th} column with respect to this requirement is given by

$$\binom{n_l+m-1}{m} = ((n_l-1)!)^{-1} \cdot (m+1) \cdot \ldots \cdot (m+n_l-1)\,,$$

which is a polynomial in m with leading coefficient $((n_l-1)!)^{-1}$ and degree n_l-1. This can be seen as follows: Each ascending sequence of m numbers in the range 1 to n_l can be uniquely identified with an ascending sequence of m different numbers in the range 1 to $n_l+(m-1)$. This can be done by adding the number $k-1$ to the number in position k, for all $k \in \{1,\dots,m\}$.
The product of those numbers equals $\#\mathcal{R}_m$. ◇

Corollary. The number of non-zero Hibi relations, $\#\mathcal{H}_N$, equals

$$\frac{n_1 \cdot \ldots \cdot n_r}{2}\big(n_1 \cdot \ldots \cdot n_r + 1 - \frac{1}{2^{r-1}}(n_1+1) \cdot \ldots \cdot (n_r+1)\big).$$

Proof. Let $d := n_1 \cdot \ldots \cdot n_r$. The number of non-zero Hibi relations equals

$$\begin{aligned}\frac{d(d+1)}{2} - \#\mathcal{R}_2 &= \frac{d(d+1)}{2} - \prod_{l=1}^{r}\frac{n_l(n_l+1)}{2}\\ &= \frac{d}{2}\left(d+1-\frac{1}{2^{r-1}}(n_1+1)\cdot\ldots\cdot(n_r+1)\right).\end{aligned}$$ ◇

A general formulation of the next statement can be found in [HHO, Theorem 6.38].

Theorem. The dimension of the projective Hibi variety equals $\sum_{l=1}^{r} n_l$. The degree equals the multinomial coefficient

$$\binom{\sum_{l=1}^{r} n_l}{n_1\ n_2\ \cdots\ n_r}.$$

Proof. According to Subsection 2.1.7, the Hilbert function is given by

$$\mathbb{N}_0 \to \mathbb{N}_0,\ m \mapsto \prod_{l=1}^{r} \binom{n_l + m}{m}.$$

The leading term of the Hilbert polynomial equals

$$\left(\prod_{l=1}^{r} n_l!\right)^{-1} \cdot m^{\sum_{l=1}^{r} n_l}.$$

◇

Remark. In the case of arbitrary finite distributive lattices L, we can use the following "trick" to identify the affine Hibi variety in the corresponding projective space: From L, we may obtain another finite distributive lattice L_0 by adding a point 0 to L, which, with respect to the partial order on L, is covered by the bottom element $\bot$ of L:

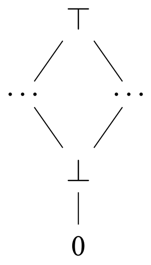


Figure 5.1: The lattice L, extended by an element 0.

Adding the point 0 has no effect on the Hibi relations (the variables involved in a non-zero Hibi relation form the "corners" of a rhomb, but 0 is not contained in a rhomb). Hence, one could consider the join-meet ideal $\mathcal{I}_{L_0}$ in the projective space $\mathbb{P}^{\#L_0-1}$. The affine Hibi variety, defined by $\mathcal{I}_L$, equals those points of $\mathbb{P}^{\#L_0-1}$ which have the form $1 : v$, where $v \in \mathbb{C}^L$ (the first position belongs to $0 \in L_0$).

5.5.3 The Vanishing Ideal

Here, we show that the vanishing ideal of the Hibi variety is not larger than the join-meet ideal. To do so, we generalise [Lang, Satz 5.3.9]. These observations are useful to determine symmetries of theta bodies in Section 6.1.

Theorem. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal with Gröbner basis G such that each leading term $\mathrm{LT}(g)$, $g \in G$, is square-free. Then the vanishing ideal of $\mathcal{Z}_{\mathbb{K}}(I)$ equals I, that is,

$$I = \mathcal{I}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I)).$$

Proof. Let $t, r \in \mathbb{K}[x_1, \ldots, x_n]$ and $m \in \mathbb{N}$. If t is a square-free term and r^m is divisible by t, then also r is divisible by t.

Case 1: $\mathbb{K} = \mathbb{R}$.

We show that I is a real ideal, so that the statement follows from the Real Nullstellensatz Theorem 2.1.3.

Step 1: To show that I is real, we show that $\sum_{t=1}^{s} g_t^2 \in I$ with $s \in \mathbb{N}$ and $g_1, \ldots, g_s \in \mathbb{R}[x_a \colon a \in L]$ implies $g_t \in I$ for all $t \in \{1, \ldots, s\}$. Let us assume that this statement is not true by assuming $g_1 \notin I$. Furthermore, we assume that there exists $l \in \{1, \ldots, s\}$ such that $g_1, \ldots, g_l \notin I$ and $g_t \in I$ for all $t \in \{1, \ldots, s\}$ with $t > l$. We have $-g_t^2 \in I$ for all $t \in \{1, \ldots, s\}$ with $t > l$, which leads to $\sum_{t=1}^{l} g_t^2 \in I$.

Step 2: For all $t \in \{1, \ldots, l\}$, let $0 \neq r_t$ denote the normal form of g_t modulo G. Since $g_t - r_t =: h_t \in I$ for all $t \in \{1, \ldots, l\}$, we obtain

$$\sum_{t=1}^{l} g_t^2 = \sum_{t=1}^{l} (h_t + r_t)^2 = \sum_{t=1}^{l} \underbrace{(h_t^2 + 2h_t r_t)}_{\in I} + \sum_{t=1}^{l} r_t^2 \ \in I.$$

Hence, $0 \neq \sum_{t=1}^{l} r_t^2 \in I$.

Step 3: From Proposition 1.1.5 (ii), it follows that $\mathrm{LT}(r_t^2) = \mathrm{LT}(r_t)^2$ for all $t \in \{1, \ldots, l\}$. Hence, we may assume that $\mathrm{LT}(\sum_{t=1}^{l} r_t^2) = \mathrm{LT}(r_1)^2$. Since G is a Gröbner basis, Theorem 1.2.3 (g) gives a polynomial $f \in G$ such that $\mathrm{LT}(\sum_{t=1}^{l} r_t^2) = \mathrm{LT}(r_1)^2$ is divisible by $\mathrm{LT}(f)$. The leading term of f is square-free. This implies that $\mathrm{LT}(r_1)$ is divisible by $\mathrm{LT}(f)$. This contradicts the premise that r_1 is reduced modulo G.

Case 2: $\mathbb{K} = \mathbb{C}$.

We show that I is a radical ideal, so that the statement follows from Hilbert's Nullstellensatz Theorem 2.1.2.

Step 1: To show that I is a radical ideal, we show that $g^m \in I$ with $g \in \mathbb{C}[x_a \colon a \in L]$ and $m \in \mathbb{N}$ implies $g \in I$. We suppose that this statement is not true by assuming $g \notin I$.

Step 2: Let $0 \neq r$ denote the normal form of g modulo G. Since $g - r =: h \in I$, we obtain

$$g^m = (h + r)^m = \sum_{s=0}^{m} \binom{m}{s} h^s r^{m-s} = \underbrace{\sum_{s=1}^{m} \binom{m}{s} h^s r^{m-s}}_{\in I} + r^m \ \in I.$$

Hence, $0 \neq r^m \in I$.

Step 3: Proposition 1.1.5 (ii) implies $\mathrm{LT}(r^m) = \mathrm{LT}(r)^m$. Since G is a Gröbner basis, Theorem 1.2.3 (g) gives a polynomial $f \in G$ such that $\mathrm{LT}(r)^m$ is divisible by $\mathrm{LT}(f)$. The leading term of f is square-free. This implies that also $\mathrm{LT}(r)$ is divisible by $\mathrm{LT}(f)$. This contradicts the premise that r is reduced modulo G. ◇

Corollary. We have $\mathcal{J}_L = \mathcal{J}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(\mathcal{J}_L))$, that is, the vanishing ideal of the Hibi variety equals the join-meet ideal.

Proof. Let $I := \mathcal{J}_L$ and let G be the set of all non-zero Hibi relations, which is a Gröbner basis of I according to Theorem 5.3.4. Let $f \in G$. There exist $a, b \in L$ with $a \neq b$ such that the leading term of f is given by $\mathrm{LT}(f) = x_a x_b$, which is a square-free term. ◇

Corollary. Let $f \in \mathbb{K}[x_a \colon a \in L]$ be a non-zero Hibi relation and let I be the principal ideal which is generated by f. Then we have $I = \mathcal{J}_{\mathbb{K}}(\mathcal{Z}_{\mathbb{K}}(I))$.

Proof. Let $I := \mathrm{Id}(f)$ and let $G := \{f\}$, which is a Gröbner basis of I. ◇

Corollary. In the case where $L = \{1, 2\}^2$, we have $\imath(\mathcal{J}_L) = \mathcal{J}_{\mathbb{R}}(\mathcal{Z}_{\mathbb{R}}(\imath(\mathcal{J}_L)))$, that is, the vanishing ideal of the complex Hibi variety equals the complex-join-meet ideal.

Proof. Let $I := \imath(\mathcal{J}_L)$ and let G be the set of all non-zero complex Hibi relations, which is a Gröbner basis of I according to Example 5.4.1. Let $f \in G$. Then there exist $a, b \in L$ with $a \neq b$ and $t_1, t_2 \in \{1, 2\}$ such that $\mathrm{LT}(f) = x_{a,t_1} x_{b,t_2}$, which is a square-free term. ◇

It is open whether the last corollary holds for arbitrary lattices L, see also Section 5.4.

5.6 Application to Tensor Products

According to Section 3.4, the product vectors in $V_{\mathbb{K}}$ are characterised by the join-meet ideal $\mathcal{J}_N$ in $\mathbb{K}[x_a \colon a \in N]$. The idea is that everything we know about $\mathcal{J}_N$ or, alternatively, about a generating set of $\mathcal{J}_N$ can help to understand the structure of the product vectors.

So far, the generating set we mostly focused on are the Hibi relations $\mathcal{H}_N$. In this section, we want to focus on the PV-determinants $\mathcal{D}_N$.

First of all, we introduce some notions which will be helpful in the following.

Afterwards, we show Theorem 5.6.5 which provides a formula for the total number $D(n_1, \ldots, n_r) := \#\mathcal{D}_N$ of the non-zero PV-determinants.

The idea of looking at the total number comes from an earlier phase of this thesis. Indeed, in [Lang, Satz 5.3.5] a generating set of $\mathcal{I}_N$ is proposed whose total number turned out to be closely related to the formula given in [Par] for the dimension of a so-called completely entangled subspace in $V_{\mathbb{C}}$. This relation will not be repeated here, but it is a motivation to look closer at the total number of other generating sets like the Hibi relations (see Corollary 5.5.2) or the PV-determinants. Later, the approach of this chapter to understand $\mathcal{I}_N$ using the median basis has turned out to be more fruitful. Nevertheless, the formula is provided here for further research.

5.6.1 A Notation for PV-Determinants

A PV-determinant in $\mathbb{K}[x_a \colon a \in N]$ has the form

$$d := \overline{x}_{\overline{a}} - \overline{x}_{\overline{b}} = x_{a_1} x_{a_2} - x_{b_1} x_{b_2},$$

where $\overline{a} = (a_1, a_2), \overline{b} = (b_1, b_2) \in N^2/S_2$ with $\overline{a} \xleftrightarrow{\star} \overline{b}$.

If we look at d just with respect to its set of zeros, it makes no difference whether we look at d or at $-d$. In this respect, we use the following notation for d from Subsection 3.4.5:

$$\begin{array}{c|c} a_{1,1} \cdots a_{1,r} & b_{1,1} \cdots b_{1,r} \\ \hline b_{2,1} \cdots b_{2,r} & a_{2,1} \cdots a_{2,r} \end{array}$$

where $a_k = (a_{k,1}, \ldots, a_{k,r})$ and $b_k = (b_{k,1}, \ldots, b_{k,r})$ for $k \in \{1, 2\}$. This is a 2×2 matrix in $\mathcal{M}_2(N)$. It can be easily verified that d (together with $-d$) belongs exactly to those 2×2 matrices with the entries $\{a_1, a_2, b_1, b_2\}$ where a_1 and a_2 (if different) are in different rows and in different columns. The 2×2 matrices can be obtained by interchanges of rows or columns, by transpositions of two entries on opposite sides, or by rotations clockwise or counter clockwise.

This notation points out that a PV-determinant can be interpreted as the determinant of a 2×2 submatrix of an unfolding of the tensor product $V_{\mathbb{K}}$.

Some examples for PV-determinants can be found at the end of this section.

5.6.2 A Group Action on the Quadratic Terms

In the following, we define a group action of the abelian group $Z := ((\mathbb{Z}_2)^r, +)$ on N^2/S_2.

Let $z \in Z$. We can identify z with the set $A_z := \{k \in \{1, \dots, r\} \colon z_k = 1\}$. Using the notions from Subsection 3.4.4, we write $a_z := a_{A_z}$ for all $a \in N$.

Now, for all $(a_1, a_2) \in N^2/S_2$, let

$$z.(a_1, a_2) := (b_1, b_2) \quad \in N^2/S_2$$

with

$$\begin{aligned} (b_1)_z &= (a_1)_z, & (b_2)_z &= (a_2)_z, \\ (b_1)_{1-z} &= (a_2)_{1-z}, & (b_2)_{1-z} &= (a_1)_{1-z}, \end{aligned}$$

that is, (b_1, b_2) emerges from (a_1, a_2) by interchanging the entries of a_1 and a_2 in the positions which are determined by z. Indeed, this is a group action, since it can be easily verified that $0 \in Z$ (and also $1 \in Z$) define the identity on N^2/S_2 and for all $\overline{a} \in N^2/S_2$ and for all $z_1, z_2 \in Z$, we obtain

$$z_1.(z_2.\,\overline{a}) = (z_1 + z_2).\,\overline{a}.$$

We note also that $z.\,\overline{a} = (1 - z).\,\overline{a}$.

Hence, the group Z can be identified with the power set $\mathfrak{P}(\{1, \dots, r\})$, equipped with the symmetric difference $\triangle$ (which is, as usual, defined by $A \triangle B := (A \cup B) \setminus (A \cap B)$ for subsets $A, B \subseteq \{1, \dots, r\}$). In this respect, we write $A_z.(a_1, a_2) := z.(a_1, a_2)$.

5.6.3 The Support and the Stabiliser

Let $\overline{a} = (a_1, a_2) \in N^2/S_2$, where $a_k = (a_{k,1}, \dots, a_{k,r})$ for $k \in \{1, 2\}$.

The following definition will be helpful to investigate the equivalence class $[\overline{a}]$.

Definition. The set $C_{\overline{a}} := \{l \in \{1, \dots, r\} \colon a_{1,l} = a_{2,l}\} \subseteq \{1, \dots, r\}$ of all positions in which the entries of a_1 and a_2 are equal is called the *coincidence set* of $\overline{a}$ and the set $S_{\overline{a}} := \{1, \dots, r\} \setminus C_{\overline{a}} \subseteq \{1, \dots, r\}$ is called the *support* of $\overline{a}$. The number $\#S_{\overline{a}}$ is called the *length* of the support.

The stabiliser $Z_{\overline{a}}$ of $\overline{a} \in L^2/S_2$ under Z is given by

$$Z_{\overline{a}} = \{z \in Z \colon z.\overline{a} = \overline{a}\},$$

see Subsection 3.2.2. Hence, $Z_{\overline{a}}$ is given by the subsets of the coincidence set $C_{\overline{a}}$ and its complements. If the support is empty, then $Z_{\overline{a}} = Z$. Otherwise, $Z_{\overline{a}}$ is isomorphic to $(\mathbb{Z}_2)^{\#C_{\overline{a}}+1}$.

The group action of Z on N^2/S_2 is not faithful, since 0 and 1 are contained in all stabilisers. On the other hand, since $n_1, \dots, n_r \geqslant 2$, for each $z \in Z$ with $0 \neq z \neq 1$, there exist $\overline{a} \in N^2/S_2$ such that $z.\overline{a} \neq \overline{a}$. Thus, the intersection of the stabilisers equals $K := \{0, 1\}$. The quotient group Z/K acts faithful on N^2/S_2, see Subsection 3.2.2. The stabiliser $(Z/K)_{\overline{a}}$ can be identified with the subsets of $C_{\overline{a}}$. If the support is not empty, $(Z/K)_{\overline{a}}$ is isomorphic to $(\mathbb{Z}_2)^{\#C_{\overline{a}}}$. Otherwise, it equals Z/K and is isomorphic to $(\mathbb{Z}_2)^{r-1}$.

The notions can be extended to PV-determinants:

Definition. Let $\overline{b} \in N^2/S_2$ with $\overline{a} \overset{\star}{\longleftrightarrow} \overline{b}$. Since $\overline{a}$ and $\overline{b}$ have the same coincidence set C and the same support $S := C^c$, we refer to C as the *coincidence set* of the PV-determinant $d := x_{\overline{a}} - x_{\overline{b}}$ and we refer to S as the *support* of d with *length* $\#S$.

5.6.4 The Orbits

Let $\overline{a} = (a_1, a_2) \in N^2/S_2$. The orbit $Z.\overline{a}$ of $\overline{a}$ under Z can be determined easily:

Proposition. We have $Z.\overline{a} = [\overline{a}]$, that is, for any $\overline{b} = (b_1, b_2) \in N^2/S_2$, the following are equivalent:

(a) There exists $z \in Z$ with $z.\overline{a} = \overline{b}$.
(b) $\overline{a} \overset{\star}{\longleftrightarrow} \overline{b}$.
(c) $\mathcal{M}(\overline{a}) = \mathcal{M}(\overline{b})$.
(d) $x_{\overline{a}} - x_{\overline{b}}$ is a PV-determinant.
(e) $N(a_1, a_2) = N(b_1, b_2)$ (see Proposition 4.2.6).

Proof. See Example 5.2.6.II and Example 5.2.6.III. $\diamond$

Proposition. There is a one-to-one correspondence between $Z.\overline{a}$ and complementary partitions of $S_{\overline{a}}$. Hence, with $t := \#S_{\overline{a}}$, we have

$$\#Z.\overline{a} = \#[\overline{a}] = \begin{cases} 2^{t-1}, & t \neq 0, \\ 1, & t = 0. \end{cases}$$

Proof. If the support $S_{\overline{a}}$ of $\overline{a}$ is empty, then $\#[\overline{a}] = 1$. In all other cases, let $s_0 \in S_{\overline{a}}$ be arbitrary. Each element in $Z.\overline{a}$ can be identified with a set $A \in \mathfrak{P}(\{1,\dots,r\})$ with the following property: $A \subseteq S_{\overline{a}}$ and $s_0 \notin A$. Now, let $A' \subseteq \{1,\dots,r\}$ such that A and A' are a complementary partition of the support, that is, $A \cup A' = S_{\overline{a}}$. Hence, $Z.\overline{a}$ can be identified with $(\mathbb{Z}_2)^{t-1}$, if $t \geqslant 1$, and with $(\mathbb{Z}_2)^0$, if $t = 0$. $\diamond$

5.6.5 The Total Number of the PV-Determinants

Now, we want to determine $D(n_1,\dots,n_r)$.

For all $t \in \{0,\dots,r\}$, let $\mathcal{D}_{t,p}$ denote the set of all non-zero PV-determinants whose support has length t.

Lemma. If $t = 0$, then we have $\#\mathcal{D}_{t,p} = 0$. Otherwise, we have

$$\#\mathcal{D}_{t,p} = \frac{\dim(V_{\mathbb{K}})}{2} \cdot (2^{t-1} - 1) \cdot \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \#M = t}} \prod_{k \in M} (n_k - 1) \Big).$$

Proof. *Step 1*: For all $\overline{a} \in N^2/S_2$, let $\mathcal{D}_{\overline{a},p}$ denote the set of all non-zero PV-determinants $x_{\overline{a}} - x_{\overline{b}}$, where $\overline{b} \in [\overline{a}]$.

Step 2: Now, let $\overline{a} = (a_1, a_2) \in N^2/S_2$ with support length t. If $t = 0$, then we obtain $\#[\overline{a}] = 1$ and $\#\mathcal{D}_{\overline{a},p} = 0$. If $t \geqslant 0$, then we recall that $\#[\overline{a}] = 2^{t-1}$. Hence, we have

$$\#\mathcal{D}_{\overline{a},p} = \begin{cases} 2^{t-1} - 1, & t \neq 0, \\ 0, & t = 0. \end{cases}$$

Step 3: Let $(N^2/S_2)_t$ denote the set of all elements in N^2/S_2 whose support has length t.

Step 4: According to Proposition 5.6.4.II, both $\#[\overline{a}]$ and $\#\mathcal{D}_{\overline{a},p}$ depend only on t. Thus, the preliminary statements give

$$\#\mathcal{D}_{t,p} = \#(N^2/S_2)_t \cdot \#\mathcal{D}_{\overline{a},p}.$$

Step 5: The formula is true in the case $t = 1$ so that we can assume that $t \geqslant 2$. The entries of a_1 and a_2 coincide on the coincidence set $C_{\overline{a}}$ and differ on the support $S_{\overline{a}}$. There are $\prod_{k \in C_{\overline{a}}} n_k$ possibilities to coincide on $C_{\overline{a}}$ and $\frac{1}{2} \cdot \prod_{k \in S_{\overline{a}}} n_k(n_k - 1)$ possibilities to differ on $S_{\overline{a}}$. Hence, we obtain

$$\begin{aligned} \#(N^2/S_2)_t &= \sum_{\substack{M \subseteq \{1,\dots,r\} \\ \#M = t}} \frac{1}{2} \cdot \Big(\prod_{k \in M} n_k(n_k - 1) \Big) \cdot \prod_{k \in \{1,\dots,r\} \setminus M} n_k \\ &= \frac{1}{2} \cdot \prod_{k=1}^{r} n_k \cdot \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \#M = t}} \prod_{k \in M} n_k(n_k - 1) \Big). \end{aligned}$$

Step 6: We recall that $\dim(V_{\mathbb{K}}) = \prod_{k=1}^{r} n_k$. From Proposition 5.6.4.II, it follows that

$$\begin{aligned} \#\mathcal{D}_{t,p} &= \#(N^2/S_2)_t \cdot \#\mathcal{D}_{\overline{a},p} \\ &= \frac{2^{t-1} - 1}{2} \cdot \dim(V_{\mathbb{K}}) \cdot \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \#M = t}} \prod_{k \in M} (n_k - 1) \Big). \end{aligned}$$

◇

Now, we can determine the total number of the non-zero PV-determinants:

Theorem. We have

$$D(n_1, \dots, n_r) = \frac{\dim(V_{\mathbb{K}})}{4} \cdot \Big(1 - 2\dim(V_{\mathbb{K}}) + \prod_{k=1}^{r} (2n_k - 1) \Big).$$

In the case where $n_1 = \dots = n_r =: n$, we obtain

$$D(n, \dots, n) = \frac{n^r}{4} \cdot (1 - 2n^r + (2n - 1)^r).$$

Proof. Let $D := D(n_1, \dots, n_r)$. We first note that $D = \sum_{t=2}^{r} \#\mathcal{D}_{t,p}$. Using Lemma 5.6.5, it follows that

$$D = \frac{\dim(V_{\mathbb{K}})}{2} \cdot \underbrace{\sum_{t=2}^{r} \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \#M = t}} \prod_{k \in M} (n_k - 1) \Big) \cdot (2^{t-1} - 1)}_{=:A}.$$

In the following, we show $A = B$ for

$$B := \frac{1}{2}\Big(\prod_{k=1}^{r}(2n_k - 1)\Big) - \dim(V_{\mathbb{K}}) + \frac{1}{2}$$

by comparison of coefficients. For each subset $M \subseteq \{1, \dots, r\}$, we denote the coefficient of $\prod_{k \in M} n_k$ in A and B by $n_{M,A}$ and $n_{M,B}$, respectively.

Constant term: An elementary computation $(\star)$ gives

$$n_{\emptyset,A} = \sum_{t=2}^{r} \binom{r}{t} (-1)^t (2^{t-1} - 1) \overset{(\star)}{=} \frac{1}{2}(-1)^r + \frac{1}{2} = n_{\emptyset,B}.$$

Leading term: We obtain immediately $n_{\{1,\dots,r\},A} = 2^{r-1} - 1 = n_{\{1,\dots,r\},B}$.

Variables: Let $s \in \{1, \dots, n\}$. The coefficient of $n_{\{s\},A}$ is equal to the coefficient of n_s in

$$\sum_{t=1}^{r-1} \Bigg(\sum_{\substack{M \subseteq \{1,\dots,r\} \setminus \{s\} \\ \# M = t}} \Big(\prod_{k \in M} (n_k - 1) \Big) \cdot (n_s - 1) \Bigg) \cdot (2^{(t+1)-1} - 1).$$

An elementary computation $(\star)$ gives

$$n_{\{s\},A} = \sum_{t=1}^{r-1} \binom{r-1}{t} (-1)^t (2^t - 1) \overset{(\star)}{=} (-1)^{r-1} = n_{\{s\},B}.$$

The remaining terms: Let $2 \leqslant s < r$ and $M_0 \subseteq \{1, \dots, r\}$ with $\# M_0 = s$. The coefficient $n_{M_0,A}$ is equal to the coefficient of $\prod_{k \in M_0} n_k$ in the polynomial

$$\sum_{t=s}^{r} \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \# M = t \\ M_0 \subseteq M}} \prod_{k \in M} (n_k - 1) \Big) \cdot (2^{t-1} - 1).$$

An elementary computation $(\star)$ gives

$$\begin{aligned} n_{M_0,A} &= \sum_{t=s}^{r} \Big(\sum_{\substack{M \subseteq \{1,\dots,r\} \\ \# M = t \\ M_0 \subseteq M}} (-1)^{t-s} \Big) \cdot (2^{t-1} - 1) \\ &= \sum_{t=0}^{r-s} \sum_{\substack{M \subseteq \{1,\dots,r\} \setminus M_0 \\ \# M = t}} (-1)^t (2^{t+s-1} - 1) \end{aligned}$$

$$= \sum_{t=0}^{r-s} \binom{r-s}{t} (-1)^t (2^{t+s-1} - 1)$$
$$\overset{(\star)}{=} \frac{1}{2} \cdot 2^s \cdot (-1)^{r-s} = n_{M_0,B}.$$

The coefficients of all terms coincide, so we obtain $A = B$. This finishes the proof. ◇

5.6.6 Some Examples

Example. In this example, we consider the bipartite tensor product $\mathbb{K}^m \otimes \mathbb{K}^n$. The non-zero PV-determinants are given by

$$\begin{array}{c|c} a_{1,1}\, a_{1,2} & a_{1,1}\, a_{2,2} \\ \hline a_{2,1}\, a_{1,2} & a_{2,1}\, a_{2,2} \end{array}$$

where $a_{1,1}, a_{2,1} \in \mathbb{K}^m$, $a_{1,2}, a_{2,2} \in \mathbb{K}^n$ with $a_{1,1} \neq a_{2,1}$ and $a_{1,2} \neq a_{2,2}$, and we have

$$D(m,n) = \frac{mn}{2} \cdot (m-1)(n-1).$$

Example. In this example, we determine the non-zero PV-determinants for the tensor product $\mathbb{K}^2 \otimes \mathbb{K}^2 \otimes \mathbb{K}^2$. We first determine all PV-determinants whose support has length 3. Let $\overline{a} := (1\,1\,1,\ 2\,2\,2)$. According to Proposition 5.6.4.I, we obtain

$$\begin{aligned}[\overline{a}] = \{&(1\,1\,1,\ 2\,2\,2),\ (2\,2\,1,\ 1\,1\,2),\\ &(2\,1\,2,\ 1\,2\,1),\ (1\,2\,2,\ 2\,1\,1)\}.\end{aligned}$$

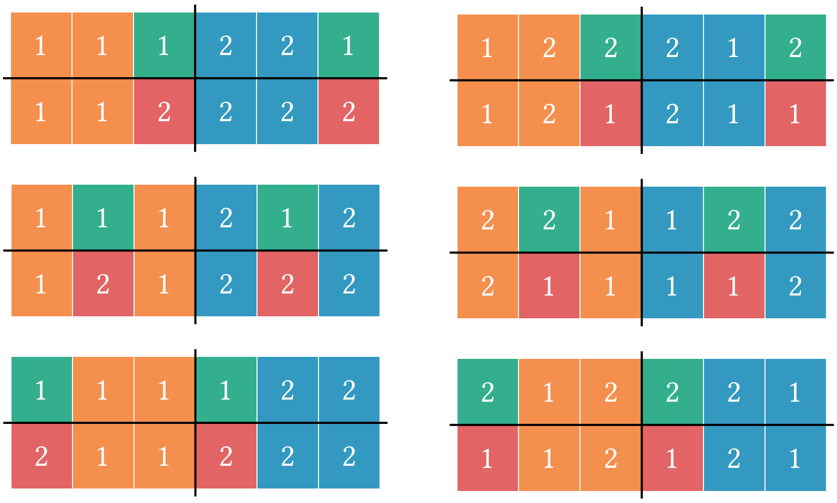
According to Lemma 5.6.5, the number of all non-zero PV-determinants whose support has length 3 is $\#\mathcal{D}_{3,p} = 12$.

Secondly, we consider the PV-determinants whose support has length 2, that is, the set $\mathcal{D}_{2,p}$. There are 3 possibilities to choose the coincidence set and 2 possibilities to choose the entry on the coincidence set. This gives $\#\mathcal{D}_{2,p} = 3 \cdot 2 \cdot 2 = 12$.

The following diagrams show the $D(2,2,2) = 24$ non-zero PV-determinants. In each diagram, the colours show the coincidence set S and the partition R, C of the support:

S	yellow,
R	green and red,
C	orange and blue.

The set $\mathcal{D}_{3,p}$ has $12 = 2 \cdot 6$ elements:



1	1	1	2	2	1
1	1	2	2	2	2

1	2	2	2	1	2
1	2	1	2	1	1

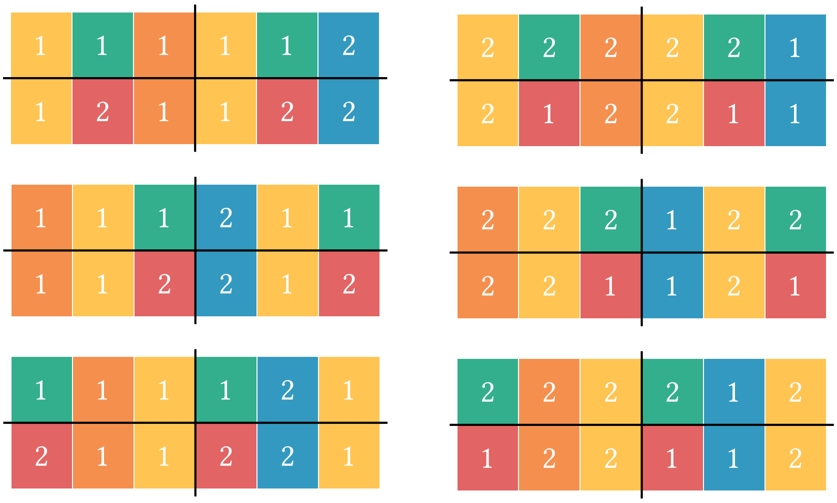
1	1	1	2	1	2
1	2	1	2	2	2

2	2	1	1	2	2
2	1	1	1	1	2

1	1	1	1	2	2
2	1	1	2	2	2

2	1	2	2	2	1
1	1	2	1	2	1

The set $\mathcal{D}_{2,p}$ has $12 = 2 \cdot 6$ elements as well:



1	1	1	1	1	2
1	2	1	1	2	2

2	2	2	2	2	1
2	1	2	2	1	1

1	1	1	2	1	1
1	1	2	2	1	2

2	2	2	1	2	2
2	2	1	1	2	1

1	1	1	1	2	1
2	1	1	2	2	1

2	2	2	2	1	2
1	2	2	1	1	2

Thus, the Hibi relations for the lattice $N = \{1,2\}^3$ are

$$x_{221}x_{112} - x_{111}x_{222},$$
$$x_{121}x_{212} - x_{111}x_{222},$$
$$x_{211}x_{122} - x_{111}x_{222}$$

and

$$x_{112}x_{121} - x_{111}x_{122},$$
$$x_{211}x_{112} - x_{111}x_{212},$$
$$x_{121}x_{211} - x_{111}x_{221},$$

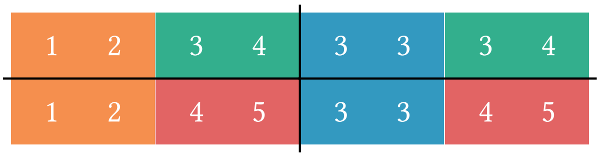
$$
\begin{aligned}
&x_{2\,2\,1}\,x_{2\,1\,2} - x_{2\,1\,1}\,x_{2\,2\,2},\\
&x_{2\,2\,1}\,x_{1\,2\,2} - x_{1\,2\,1}\,x_{2\,2\,2},\\
&x_{2\,1\,2}\,x_{1\,2\,2} - x_{1\,1\,2}\,x_{2\,2\,2}.
\end{aligned}
$$

The 9 polynomials are a reduced Gröbner basis of the join-meet ideal $\mathcal{I}_N$ with respect to the graded reverse lexicographical term order, see Theorem 5.3.4. Together with the norming polynomial $1 - x_{1\,1\,1}^2 + x_{2\,1\,1}^2 + x_{1\,2\,1}^2 + x_{2\,2\,1}^2 + x_{1\,1\,2}^2 + x_{2\,1\,2}^2 + x_{1\,2\,2}^2 + x_{2\,2\,2}^2$, they are a reduced Gröbner basis of the norm-join-meet ideal $\mathcal{J}_N$.

Example. In this example, we consider the tensor product $\mathbb{K}^5 \otimes \mathbb{K}^5 \otimes \mathbb{K}^5 \otimes \mathbb{K}^5$. Let $\overline{a} := (1\,2\,3\,4, 3\,3\,4\,5) \in \mathrm{N}^2/S_2$ and $z := (1,1,0,0) \in \mathrm{Z}$. We have $z.\overline{a} = (3\,3\,3\,4,\ 1\,2\,4\,5)$, so that

$$\overline{x}_{\overline{a}} - \overline{x}_{z.\overline{a}} \;=\; x_{1\,2\,3\,4} \cdot x_{3\,3\,4\,5} \;-\; x_{1\,2\,4\,5} \cdot x_{3\,3\,3\,4}$$

is a non-zero PV-determinant (the colours are explained above):



1	2	3	4	3	3	3	4
1	2	4	5	3	3	4	5

Chapter 6

THE HIBI BODY AND ITS THETA BODIES

This chapter deals with the approximation of the Hibi body by theta bodies. Our aim is to obtain witnesses for the first theta body in order to outline the geometry of the Hibi body. In Chapter 7 and in Chapter 8 we apply the main results of this chapter to the projective unit ball in real tensor products.

Section 6.1 deals with the geometry of the theta bodies. For instance, we show that the Hibi body induces a norm, which we call the *Hibi norm*. In the real case also the corresponding theta bodies induce norms, which we call the *Hibi theta norms*. They generalise the *tensor theta norms* from [Sto] or from [RS2]. This statement appears also independently in [Lang].

In general, each theta body is a so-called projected spectrahedron, see [BPT, Theorem 5.60]. This approach to theta bodies uses so-called moment matrices. We have investigated it before in [Lang, Satz 4.3.3]. It can also be used for a numerical approach to theta bodies using so-called semidefinite programming, see [Lang, Kapitel 7] and [Sto]. In Section 6.2, we focus on a direct approach which fits our particular purpose rather than the approach with moment matrices. In particular, we show that the 1-sums of squares modulo the (complex)-norm-join-meet ideal are a projected spectrahedron, see Theorem 6.2.2.

In Section 6.3 we obtain witnesses for the first theta body in the real case. The main results are Theorem 6.3.6 and Corollary 6.3.6, which are essential for Chapter 7 and for Chapter 8. For this purpose, we introduce the notions *join-meet partition* and *splitting function*.

In Section 6.4, we determine the inner radius of the first complex theta body. The main result is Theorem 6.4.2. It shows that in general, the first complex theta body is relatively "far" from the Hibi body.

Section 6.5 provides a brief introduction to error-correcting codes and their relation to join-meet partitions.

Now, we refer to the notions of the previous chapters, especially from Table 5.2.

Let L be a non-empty finite distributive lattice. Let $L_{\mathbb{R}} := L$ and let $L_{\mathbb{C}} := L \times \{1, 2\}$. Let $n := \# L_{\mathbb{K}}$.

Case $\mathbb{K} = \mathbb{R}$:

The join-meet ideal $\mathcal{I} := \mathcal{I}_L$ is generated by the non-zero Hibi relations $\mathcal{H}_L$. The norm-join-meet ideal $\mathcal{J} := \mathcal{J}_L$ is generated by $\mathcal{H}_L$ and the norming polynomial u_L. Let $V := \mathcal{Z}_{\mathbb{R}}(\mathcal{J}_L) = \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_L) \cap (\mathbb{R}^L)_1$. The Hibi body is given by $H := \mathrm{co}(V) \subseteq \mathbb{R}^L$.

Let $k \in \mathbb{N}$. The k^{th} theta body $\mathcal{T}_k := \mathcal{T}_k(\mathcal{J})$ of $\mathcal{J}$ is a superset of the Hibi body H.

Case $\mathbb{K} = \mathbb{C}$:

The complex-join-meet ideal $\mathcal{I} := \mathcal{I}_{L_{\mathbb{C}}}$ is generated by the non-zero complex Hibi relations $\mathcal{H}_{L_{\mathbb{C}}}$. The complex-norm-join-meet ideal $\mathcal{J} := \mathcal{J}_{L,\mathbb{C}}$ is generated by $\mathcal{H}_{L_{\mathbb{C}}}$ and the complex norming polynomial $u_{L_{\mathbb{C}}}$. Let $V := \imath^{-1}(\mathcal{Z}_{\mathbb{R}}(\mathcal{J}_{L,\mathbb{C}})) = \mathcal{Z}_{\mathbb{C}}(\mathcal{H}_L) \cap (\mathbb{C}^L)_1$. The Hibi body is given by $H := \mathrm{co}(V) \subseteq \mathbb{C}^L$.

Let $k \in \mathbb{N}$. The k^{th} complex theta body $\mathcal{T}_k := \mathcal{T}_k^{\mathbb{C}}(\mathcal{J}) = \imath^{-1}(\mathcal{T}_k(\mathcal{J}))$ of $\mathcal{J}$ is a superset of the Hibi body H.

6.1 The Hibi Norm and Hibi Theta Norms

This section deals with the geometry of the Hibi body and its theta bodies. We outline some cases where they can be regarded as the unit balls of a norm, we determine the outer radius of a theta body, and we focus on the symmetry group of both the Hibi body and its theta bodies.

6.1.1 The Hibi Norm

Theorem. The Hibi body H is the unit ball of a norm. Moreover, the set V fulfils the criteria V0 - V3 from Subsection 2.4.6 with respect to the convex body H.

Proof. To show that H induces a norm, it is sufficient to show that it is balanced and absorbing (see Section 2.4).

Statement 1: For each phase $\varphi \in \mathbb{K}_1$ and for each $z \in V$, we have $\varphi \cdot z \in V$, that is, V is balanced (and thus, H is balanced). In particular, $0 \in H$.

Proof: We first note that $V = \mathcal{Z}_{\mathbb{K}}(\mathcal{I}_L) \cap (\mathbb{K}^L)_1$. Since $(\mathbb{K}^n)_1$ is invariant under multiplication with φ, it is left to show that the Hibi variety $\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_L)$ is invariant under multiplication with φ: A Hibi relation f is homogeneous, so for each $z \in \mathbb{K}^L$, we have $f(z) = 0$, if and only if $f(\varphi \cdot z) = 0$. In particular, the Hibi variety is invariant under multiplication with -1, so $0 \in H$.

Statement 2: H is absorbing.

Proof: The proof has two parts.

Part 1: From Theorem 4.2.2.II, we know that L is isomorphic to a ring of sets, that is, a sublattice of a boolean lattice. Hence, we may assume that there exists $r \in \mathbb{N}$ such that L is a sublattice of the direct product $L' := \{1,2\}^r$. Let $L'_{\mathbb{R}} := L'$ and $L'_{\mathbb{C}} := L' \times \{1,2\}$. Let $\mathcal{J}'$ be the ideal in $\mathbb{R}[x_a \colon a \in L'_{\mathbb{K}}]$ which is generated by $\mathcal{H}_{L'_{\mathbb{K}}}$ and $u_{L'_{\mathbb{K}}}$.

Part 2: Let $B := \operatorname{co}(\mathcal{Z}_{\mathbb{R}}(\mathcal{J}))$ and let $B' := \operatorname{co}(\mathcal{Z}_{\mathbb{R}}(\mathcal{J}'))$. We already know that B' (or $\imath^{-1}(B')$ in the case where $\mathbb{K} = \mathbb{C}$) is equal to the projective unit ball in $\mathbb{K}^2 \otimes \cdots \otimes \mathbb{K}^2$ (with r tensor factors). Hence, 0 is an interior point of B'. Let P be the orthogonal projection from $\mathbb{R}^{L'_{\mathbb{K}}}$ onto $\mathbb{R}^{L_{\mathbb{K}}}$. We show that $P(B') \subseteq B$. In this case, 0 is also an interior point of B. To show this, we state at first that $B' = \operatorname{co}(A')$, where $A' :=$

$\mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{L'_{\mathbb{K}}}) \cap (\mathbb{R}^{L'_{\mathbb{K}}})_1$, and $B = \mathrm{co}(A)$, where $A := \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{L_{\mathbb{K}}}) \cap (\mathbb{R}^{L_{\mathbb{K}}})_1$. Now, it suffices to show $P(A') \subseteq B$. Let Q be the projection from $\mathbb{R}[x_a \colon a \in L'_{\mathbb{K}}]$ onto $\mathbb{R}[x_a \colon a \in L_{\mathbb{K}}]$ defined as follows: Q is linear and any term in $\mathbb{R}[x_a \colon a \in L'_{\mathbb{K}}]$ is mapped onto itself, if it is also in $\mathbb{R}[x_a \colon a \in L_{\mathbb{K}}]$, and on zero, if not. It can be easily verified that Q is multiplicative. Since L is a sublattice of L', it follows that $\mathcal{H}_{L_{\mathbb{K}}} \subseteq Q(\mathcal{H}_{L'_{\mathbb{K}}})$. Hence, if $z' \in \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{L'_{\mathbb{K}}})$, then $P(z') \in \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{L_{\mathbb{K}}})$. From statement 1 and since P is a contraction, we obtain $P(A') \subseteq B$.

Statement 3: V fulfils the criteria V0 - V3.

Proof: With the previous statements, V is normed, balanced and generates H. Also, V separates points, since each basis vector e_a, where $a \in L$, is contained in V. ◇

Definition. The norm which is induced by the Hibi body is called the *Hibi norm*. It is denoted by $\|\cdot\|_H$.

The outer radius of H equals 1, see Definition 2.4.6. Hence, the Hibi norm is stronger than the Euclidean norm. In the case where $L = N$, it equals the projective norm on the tensor product $\mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$.

The inner radius of H depends on the lattice L. The following chapters deal with the inner radius of the projective unit ball.

6.1.2 Theta Bodies for the Hibi Body

The (complex) theta bodies $\mathcal{T}_k$ converge against the Hibi body H, see Theorem 2.5.5:

$$\bigcap_{k=1}^{\infty} \mathcal{T}_k = H.$$

The following statement is an adaption of [Lang, Satz 6.1.2].

Proposition. The k^{th} (complex) theta body $\mathcal{T}_k$ is a convex body with interior point 0 and outer radius 1.

Proof. Theorem 6.1.1 implies that $\mathcal{T}_k$ is absorbing. Now, we show that the outer radius of $\mathcal{T}_k$ is 1. Let $z = (z_a)_{a \in L_{\mathbb{K}}} \in \mathbb{R}^n$ be a unit vector, that is, $\sum_{a \in L_{\mathbb{K}}} z_a^2 = 1$. We show that the polynomial $l_z = 1 - \sum_{a \in L_{\mathbb{K}}} z_a \cdot x_a$ is a 1-sum of squares modulo $u_{L_\mathbb{K}}$, and, hence, modulo $\mathcal{J}$: We consider the sum of squares $s := \frac{1}{2} \cdot \sum_{a \in L_\mathbb{K}} (x_a - z_a)^2$ and obtain

$$\begin{aligned} s - l_z &= \frac{1}{2} \cdot \sum_{a \in L_\mathbb{K}} x_a^2 + \frac{1}{2} \cdot \sum_{a \in L_\mathbb{K}} z_a^2 - \sum_{a \in L_\mathbb{K}} z_a \cdot x_a - l_z \\ &= \frac{1}{2} \cdot \sum_{a \in L_\mathbb{K}} x_a^2 - \frac{1}{2} = \frac{1}{2} \cdot \left(\sum_{a \in L_\mathbb{K}} x_a^2 - 1 \right) = \frac{1}{2} \cdot u_{L_\mathbb{K}} \in \mathcal{J}. \end{aligned}$$

Now, the statement follows from $l_z(z) = 0$. ◇

Hence, we have $V \subseteq \mathcal{T}_1 \cap (\mathbb{C}^L)_1$. For arbitrary lattices L, it is an open question whether equality holds.

6.1.3 The Symmetry Group of a Theta Body

Proposition. We have $\operatorname{ext}(H) = V$, that is, $\operatorname{Sym}_{\mathbb{K}^L}(H) = \operatorname{Sym}_{\mathbb{K}^L}(V)$.

Proof. Since H is the convex hull of V, we have $\operatorname{ext}(H) \subseteq V$. On the other hand, since the Euclidean unit ball is strictly convex, each point in V is an extreme point of H. ◇

Proposition. In the case where $\mathbb{K} = \mathbb{R}$, we have

$$\operatorname{Sym}_{\mathbb{R}^L}(H) \cap \mathcal{U}_{\#L}(\mathbb{R}) \subseteq \operatorname{Sym}_{\mathbb{R}^L}(\mathcal{T}_k)$$

for all $k \in \mathbb{N}$.

Proof. With Corollary 5.5.3.I, the homogeneous join-meet ideal $\mathcal{I}$ is a vanishing ideal. Hence, Proposition 2.5.7.II can be applied with $J := \mathcal{J}$, $V_0 := \mathcal{Z}_\mathbb{R}(\mathcal{I})$ and $C := H$, which gives $\operatorname{Sym}_{\mathbb{R}^L}(H) \cap \mathcal{U}_{\#L}(\mathbb{R}) \subseteq \operatorname{Sym}_{\mathbb{R}^L}(\mathcal{T}_k)$. ◇

The complex case will be discussed in Subsection 6.4.3.

In the tensor product case, the symmetry group of $\mathcal{B}_{1,\pi}$ can be determined explicitly, see Proposition 3.3.5.

6.1.4 Hibi Theta Norms

The following statement is an adaption of [Sto] and [Lang].

Theorem. In the case where $\mathbb{K} = \mathbb{R}$, the k^{th} theta body $\mathcal{T}_k$ induces a norm.

Proof. It is left to show that the k^{th} theta body $\mathcal{T}_k$ is balanced. From Proposition 6.1.3.II and since H is balanced, it follows that $z \in \mathcal{T}_k$ implies $-z \in \mathcal{T}_k$. ◇

This leads to the following definition:

Definition. The norm which is induced by $\mathcal{T}_k$ in the case where $\mathbb{K} = \mathbb{R}$ is called the k^{th} *Hibi theta norm*. It is denoted by $\| \cdot \|_{\mathcal{T}_k}$.

Each Hibi theta norm is stronger than the Euclidean norm and weaker than the Hibi norm. In the tensor product case, it says that the projective norm can be approximated by a chain of cross norms, reaching from the Hilbert-Schmidt unit ball up to the projective unit ball.

Up to now, we cannot guarantee that $\mathcal{T}_k$ is balanced in the case where $\mathbb{K} = \mathbb{C}$. In fact, the proof of the last theorem is based on an explicit Gröbner basis of the underlying ideal, see Theorem 5.5.3, and the difficulty of finding a Gröbner basis of the complex-join-meet ideal is outlined in Section 5.4.

6.2 The First Theta Body and Spectrahedra

We know from the last section that 0 is an interior point of the first (complex) theta body $\mathcal{T}_1$. Thus, according to Proposition 2.5.4, $\mathcal{D}_1$ is a real prepolar of $\mathcal{T}_1(\mathcal{J})$, that is, we have $\mathcal{D}_1^\circ = \mathcal{T}_1(\mathcal{J})$, with

$$\mathcal{D}_1 = \mathcal{D}_1(\mathcal{J}) = \{b \in \mathbb{R}^n : l^b \text{ is } 1\text{-sos-mod}\, \mathcal{J}\}.$$

The aim of this section is to characterise $\mathcal{D}_1$ as a projected spectrahedron.

6.2.1 A Direct Approach to the First Theta Body

Lemma. We have

$$\mathcal{D}_1 = \Big\{ (\langle w_a, w \rangle)_{a \in L_{\mathbb{K}}} : \\ \exists\, t \in \mathbb{N}, \exists\, w, w_\alpha \in (\mathbb{R}^t)_1 : \sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w_a, w_b \rangle \; x_a x_b \in \mathcal{I} \Big\}.$$

Proof. We recall that the set $\mathcal{C}_1 := \mathcal{C}_1(\mathcal{J})$ of all affine functionals in the polynomial ring $\mathbb{R}[x_a \colon a \in L_{\mathbb{K}}]$ which are 1-sos-mod $\mathcal{J}$ is given by $\mathcal{C}_1 = \{\lambda \cdot l^b \colon b \in \mathcal{D}_1, \lambda \geqslant 0\}$. Hence, for all $b \in \mathbb{R}^{L_{\mathbb{K}}}$, we have $b \in \mathcal{D}_1$ if and only if $l^b \in \mathcal{C}_1$.

The proof is divided into several parts. We first give a necessary and a sufficient condition on a 1-sum of squares to be an affine functional modulo $\mathcal{J}$. To do this, a polynomial $s \in \mathbb{R}[x_a \colon a \in L_{\mathbb{K}}]$ which is a 1-sum of squares has the form

$$s = \sum_{q=1}^{t} h_q^2$$

where $h_1, \ldots, h_t \in \mathbb{R}[x_a \colon a \in L_{\mathbb{K}}]$ are affine functionals. Let $h_q = w_q + \sum_{a \in L_{\mathbb{K}}} w_{q,a} \cdot x_a$ with $w_q, w_{q,a} \in \mathbb{R}$. Let $w := (w_q)_{q=1}^t$ and $w_a := (w_{q,a})_{q=1}^t$. Then

$$\begin{aligned} s &= \sum_{q=1}^{t} w_q^2 + 2 \sum_{q=1}^{t} \sum_{a \in L_{\mathbb{K}}} w_{q,a} w_q \cdot x_a + \sum_{q=1}^{t} \sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} w_{q,a} w_{q,b} \cdot x_a x_b \\ &\quad + \sum_{q=1}^{t} \sum_{a \in L_{\mathbb{K}}} w_{q,a}^2 \cdot x_a^2 \\ &= \underbrace{\langle w, w \rangle + 2 \sum_{a \in L_{\mathbb{K}}} \langle w_a, w \rangle \cdot x_a}_{\text{affine-linear part}} + \underbrace{\sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w_a, w_b \rangle \cdot x_a x_b}_{\text{mixed part}} \\ &\quad + \underbrace{\sum_{a \in L_{\mathbb{K}}} \langle w_a, w_a \rangle \cdot x_a^2}_{\text{quadratic part}} . \end{aligned}$$

Statement 1: s is an affine functional modulo $\mathcal{J}$, if and only if the following statements hold:

(i) There exists $c \geqslant 0$ such that $\langle w_a, w_a \rangle = c$ for all $a \in L_{\mathbb{K}}$, and

(ii) $\sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w_a, w_b \rangle \cdot x_a x_b \in \mathcal{I}$.

In this case, the affine functional is given by

$$l' := c + \langle w, w \rangle + 2 \sum_{a \in L_{\mathbb{K}}} \langle w_a, w \rangle \cdot x_a .$$

Proof: In $\mathcal{J}$ are no affine functionals except 0. On the one hand, each polynomial in the second homogeneous part of the (complex) join-meet ideal does not contain any "quadratic" term x_a^2, $a \in L$. On the other hand, each polynomial in the ideal which is generated by the (complex) norming polynomial $u_{L_{\mathbb{K}}}$ does not contain any "mixed" term $x_a x_b$ with $a, b \in L$, $a \neq b$, and each "quadratic" term has the same coefficient. Hence, s is an affine functional modulo $\mathcal{J}$ if and only if $h := \sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w_a, w_b \rangle \cdot x_a x_b$ lies in the (complex) join-meet ideal and $c := \langle w_a, w_a \rangle$ is constant for all $a \in L_{\mathbb{K}}$. In this case, we have

$$s = \big(c + \langle w, w \rangle + 2 \sum_{a \in L_{\mathbb{K}}} \langle w_a, w \rangle \cdot x_a\big) + h + c \cdot u_{L_{\mathbb{K}}}$$

and $l' = s + (-h - c \cdot u_{L_{\mathbb{K}}})$ is an affine functional and 1-sos-mod $\mathcal{J}$.

Statement 2: The set $\mathcal{C}_1 \cap \{l^b : b \in \mathbb{R}^{L_{\mathbb{K}}}\}$ is given by all affine functionals of the form

$$1 + \sum_{a \in L_{\mathbb{K}}} \langle w_a, w \rangle \cdot x_a,$$

where $t \in \mathbb{N}$, $w, w_a \in (\mathbb{R}^t)_1$ and $\sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w_a, w_b \rangle \cdot x_a x_b \in \mathcal{J}$.

Proof: A polynomial $l' \in \mathcal{C}_1$ has the form from statement 1. It is constant, if and only if $\langle w_a, w \rangle = 0$ for all $a \in L_{\mathbb{K}}$. Now, let l' be not constant, that is, $c > 0$ and $m := \langle w, w \rangle > 0$. Let $d := 1/(c+m)$ and

$$\begin{aligned} l := d \cdot l' &= 1 + \sum_{a \in L_{\mathbb{K}}} \frac{2 \langle w_a, w \rangle}{c + m} \cdot x_a \\ &= 1 + \sum_{a \in L_{\mathbb{K}}} \frac{2\sqrt{c}}{c + m} \langle w'_a, w \rangle \cdot x_a, \end{aligned}$$

where $w'_a := \sqrt{1/c} \cdot w_a$ are unit vectors. Let L denote the set of all affine functionals of this form. It follows that $\mathcal{C}_1 \cap \{l^b : b \in \mathbb{R}^{L_{\mathbb{K}}}\} = L$.

Now, we develop an easier expression. Let

$$b := -\left(\frac{2\sqrt{c}}{c + \langle w, w \rangle} \langle w'_a, w \rangle\right)_{a \in L_{\mathbb{K}}}.$$

Then $l = l^b$, and the distance of l to zero equals $1/\|b\|$. With $w' := \sqrt{1/m} \cdot w$, which is a unit vector, we obtain

$$b = -\left(\frac{2\sqrt{cm}}{c + m} \cdot \langle w'_a, w' \rangle\right)_{a \in L_{\mathbb{K}}} = \frac{2\sqrt{cm}}{c + m} \cdot b',$$

where $b' = -\left(\langle w'_a, w' \rangle\right)_{a \in L_{\mathbb{K}}}$. Fixing b', we may consider $b = b(m)$ for $m \geqslant 0$.

For different values of m, the hyperplanes with respect to $b(m)$ are parallel, and the distance to zero is given by

$$\frac{1}{\|b\|} = \frac{c+m}{2\sqrt{cm}} \cdot \frac{1}{\|b'\|}.$$

The function $f\colon \mathbb{R}^+ \to \mathbb{R}^+$, $m \mapsto \frac{c+m}{2\sqrt{cm}}$ is minimal for $m = c$, and $f(c) = 1$. It follows that the hyperplane for $b(c) = b'$ is closest to zero, which belongs to the polynomial

$$1 + \sum_{a \in L_{\mathbb{K}}} \langle w'_a, w' \rangle \cdot x_a,$$

where w'_a and w are unit vectors, and where

$$\sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle w'_a, w'_b \rangle \cdot x_a x_b \in \mathcal{J}.$$

Hence, we have shown that the polynomial $l^{b'}$ has the desired form. It is left to show that any polynomial $l^{\lambda b'}$, where $\lambda \in [0,1]$ (in particular, this includes all polynomials $l^{b(m)}$ for different values of m), has the desired form. This can be realised by choosing t sufficiently large:

$$l^{\lambda b'} = 1 + \lambda \sum_{a \in L_{\mathbb{K}}} \langle w'_a, w' \rangle \cdot x_a = 1 + \sum_{a \in L_{\mathbb{K}}} \langle \tilde{w}'_a, \tilde{w}' \rangle \cdot x_a,$$

where $\tilde{w}'_a := (w'_a, 0)^t \in (\mathbb{R}^{t+1})_1$, $\tilde{w}' := (\lambda w', (1-\lambda^2)^{\frac{1}{2}})^t \in (\mathbb{R}^{t+1})_1$, which satisfies $\sum_{\substack{a,b \in L_{\mathbb{K}} \\ a \neq b}} \langle \tilde{w}'_a, \tilde{w}'_b \rangle \cdot x_a x_b \in \mathcal{J}$.

Statement 3: With the preceding statements, for any $b \in \mathbb{R}^{L_{\mathbb{K}}}$, we have $l^b \in \mathcal{C}_1$ if and only if $l^{-b} \in \mathcal{C}_1$. Hence, using statement 2, the assertion is true. ◇

6.2.2 Theta Bodies and Spectrahedra

Definition. Let $m \in \mathbb{N}$. A subset of $\mathcal{S}_m(\mathbb{R})$ is called a *spectrahedron* if it equals the intersection of the cone of the positive semidefinite matrices with finitely many affine subspaces (that is, with finitely many affine hyperplanes). The image of a spectrahedron under an orthogonal projection is called a *projected spectrahedron*.

A (projected) spectrahedron is a convex set.

The optimisation of the values of a linear functional over a spectrahedron is called a *semidefinite program*. It is part of the field of non-linear optimisation. There exist several algorithms and implementations to solve semidefinite programs. Omitting the objective function, the problem of finding an optimal value turns into a feasibility problem, that is, the question whether the spectrahedron is empty or, alternatively, whether a given symmetric matrix lies in the spectrahedron. More information about spectrahedra and semidefinite programming can be found in [BPT].

The following theorem states that the set $\mathcal{D}_1$ is a projected spectrahedron. It implies also that it is sufficient to consider $n+1$ sum of squares to describe an affine functional which is 1-sos-mod $\mathcal{J}$ (we recall that $n = \#L_{\mathbb{K}}$).

Theorem. There exists a spectrahedron $\widetilde{S} \subseteq \mathcal{S}_{n+1}(\mathbb{R})$ such that

$$\mathcal{D}_1 = \left\{ b \in \mathbb{R}^{L_{\mathbb{K}}} \colon \exists\, \widetilde{B} \in \widetilde{S} \;\text{ with }\; \widetilde{B} = \left(\begin{array}{c|c} \star & b \\ \hline b^t & 1 \end{array} \right) \right\} .$$

Proof. *Step 1*: Let $m \in \mathbb{N}$. The linear subspace $\mathbb{R}[x_1, \dots, x_m]_2$ of all polynomials with degree two is (linearly) isomorphic to the set $\mathcal{S}_m(\mathbb{R})$ of all symmetric matrices by identifying $x_k x_l$ with $\frac{1}{2}(\Delta_{k,l} + \Delta_{l,k})$ for all $k, l \in \{1, \dots, n\}$, where $\Delta_{k,l} \in \mathcal{M}_m(\mathbb{R})$ is a matrix unit (all entries are zero except the entry in position (k, l), which equals 1).

Step 2: Let I be a homogeneous ideal in $\mathbb{R}[x_1, \dots, x_m]$. Then the homogeneous part of $\mathbb{R}[x_1, \dots, x_m]$ of degree two, $\mathbb{R}[x_1, \dots, x_m]_2$, is the direct sum of I_2, the homogeneous part of I of degree two, and its orthogonal complement. In particular, I_2 can be characterised in $\mathbb{R}[x_1, \dots, x_m]_2$ by finitely many hyperplanes. Hence, I_2 equals a linear subspace L_I of $\mathcal{S}_m(\mathbb{R})$.

Step 3: Positive semidefinite matrices are exactly the Gram matrices: For all $t \in \mathbb{N}$ and $A \in \mathcal{M}_{t,m}(\mathbb{R})$, the matrix $A^t A \in \mathcal{S}_m(\mathbb{R})$ is positive semidefinite. On the other hand, each positive semidefinite matrix in $\mathcal{S}_m(\mathbb{R})$ can be written as $A^t A$, where $A \in \mathcal{M}_m(\mathbb{R})$ is a quadratic matrix.

Step 4: Let $L_{\mathcal{J}}$ denote the affine subspace in $\mathcal{S}_n(\mathbb{R})$ of all symmetric matrices whose diagonal elements are equal to 1.

Step 5: Now, let

$$\widetilde{S} := \left\{ \widetilde{B} = \left(\begin{array}{c|c} B & b \\ \hline b^t & 1 \end{array} \right) \in \mathcal{S}_{n+1}(\mathbb{R}) \colon \widetilde{B} \geqslant 0, B \in L_{\mathcal{J}} \cap L_{\mathscr{J}} \right\}.$$

Then $\widetilde{S}$ is a spectrahedron.

Step 6: Let $b \in \mathcal{D}_1$. According to Lemma 6.2.1, there exists $t \in \mathbb{N}$ and $w, w_\alpha \in (\mathbb{R}^t)_1$ with $b = (\langle w_a, w \rangle)_{a \in L_\mathbb{K}}$ and

$$\sum_{\substack{a,b \in L_\mathbb{K} \\ a \neq b}} \langle w_a, w_b \rangle \ x_a x_b \in \mathcal{J}_2. \tag{6.1}$$

Now, we consider the matrix $A := (\cdots | w_a | \cdots)_{a \in L_\mathbb{K}} \in \mathcal{M}_{t,n}(\mathbb{R})$. Then the matrix $B := A^t A = (\langle w_a, w_b \rangle)_{a,b \in L_\mathbb{K}}$ is positive semidefinite. With $\widetilde{A} := (A \,|\, w) \in \mathcal{M}_{t,n+1}(\mathbb{R})$, also the matrix

$$\widetilde{B} := \widetilde{A}^t \widetilde{A} = \left(\begin{array}{c|c} B & b \\ \hline b^t & 1 \end{array} \right)$$

is positive semidefinite. Since w_α is an unit vector, $B \in L_{\mathcal{J}}$. Because of (6.1), $B \in L_{\mathscr{J}}$. Hence, $\widetilde{B} \in \widetilde{S}$.

On the other hand, let $\widetilde{B} = \left(\begin{smallmatrix} B & b \\ b^t & 1 \end{smallmatrix} \right) \in \widetilde{S}$. Since $\widetilde{B} \geqslant 0$, there exists $\widetilde{A} \in \mathcal{M}_{n+1}(\mathbb{R})$ with $\widetilde{A}^t \widetilde{A} = \widetilde{B}$. With $\widetilde{A} = (A \,|\, w)$ and $A = (w_a)_{a \in L_\mathbb{K}}$, where $w, w_\alpha \in (\mathbb{R}^{n+1})_1$, we have $b = (\langle w_a, w \rangle)_{a \in L_\mathbb{K}}$. From $B \in L_{\mathcal{J}} \cap L_{\mathscr{J}}$, we obtain $\langle w_a, w_a \rangle = 1$ and $\sum_{\substack{a,b \in L_\mathbb{K} \\ a \neq b}} \langle w_a, w_b \rangle \ x_a x_b \in \mathcal{J}_2$. Also, we have $\langle w, w \rangle = 1$. Hence, $b \in \mathcal{D}_1$. ◇

Corollary. There exists a projected spectrahedron $S \subseteq \mathcal{S}_n(\mathbb{R})$ such that

$$\mathcal{D}_1 = \big\{ b \in \mathbb{R}^{L_\mathbb{K}} \colon \\ b = A^t w \colon A \in \mathcal{M}_{n+1,n}(\mathbb{R}), A^t A \in S, w \in (\mathbb{R}^{n+1})_1 \big\}.$$

Proof. *Step 1*: Let S be the projection of $\widetilde{S}$ onto $\mathcal{S}_n(\mathbb{R})$, that is,

$$S := \left\{ B \colon \exists\, b \in \mathbb{R}^n \text{ with } \left(\begin{array}{c|c} B & b \\ \hline b^t & 1 \end{array} \right) \in \widetilde{S} \right\}.$$

Then S is a projected spectrahedron.

Step 2: Let $b \in \mathcal{D}_1$. Then there exists $\widetilde{B} \in \widetilde{S}$ with $\widetilde{B} = \left(\begin{smallmatrix} B & b \\ b^t & 1 \end{smallmatrix} \right)$. Let $A \in \mathcal{M}_{n+1,n}(\mathbb{R})$ and $w \in (\mathbb{R}^{n+1})_1$ such that $B = A^t A$ and $b = A^t w$. Then $B \in S$.

On the other hand, let $A \in \mathcal{M}_{n+1,n}(\mathbb{R})$ such that $B := A^t A \in S$. Then there exists $b' \in \mathbb{R}^n$ with $\left(\begin{smallmatrix} B & b' \\ b'^t & 1 \end{smallmatrix} \right) \in \widetilde{S}$. But for any $w \in (\mathbb{R}^{n+1})_1$, also $\left(\begin{smallmatrix} B & b \\ b^t & 1 \end{smallmatrix} \right) \in \widetilde{S}$, where $b := A^t w$, that is, $b \in \mathcal{D}_1$. ◇

Example. Let $L = \{1,2\}^2$. In the case where $\mathbb{K} = \mathbb{R}$, the spectrahedron $\widetilde{S}$ consists of all positive semidefinite matrices of the form

$$\begin{array}{c|cccc:c|}
 & 1\,1 & 1\,2 & 2\,1 & 2\,2 & \\ \cline{2-6}
1\,1 & 1 & 0 & 0 & \alpha & b_1 \\
1\,2 & 0 & 1 & -\alpha & 0 & b_2 \\
2\,1 & 0 & -\alpha & 1 & 0 & b_3 \\
2\,2 & \alpha & 0 & 0 & 1 & b_4 \\ \hdashline
 & b_1 & b_2 & b_3 & b_4 & 1 \\ \cline{2-6}
\end{array}$$

where $\alpha \in \mathbb{R}$ and $b_k \in \mathbb{R}$ for all $k \in \{1,2,3,4\}$. With $\alpha := 1$, the matrix

$$\begin{array}{|cccc:c|}
\hline
1 & 0 & 0 & 1 & 1 \\
0 & 1 & -1 & 0 & 0 \\
0 & -1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 \\ \hdashline
1 & 0 & 0 & 1 & 1 \\ \hline
\end{array}$$

lies in $\widetilde{S}$. It corresponds to the support functional $1 - x_{1\,1} - x_{2\,2}$ to the vector $\frac{1}{2}(e_{1\,1} + e_{2\,2})$.

In the case where $\mathbb{K} = \mathbb{C}$, the spectrahedron $\widetilde{S}$ consists of all positive semidefinite matrices of the form

$$\begin{array}{c|cccc:cccc:c|}
 & 1\,1\,1 & 1\,2\,1 & 2\,1\,1 & 2\,2\,1 & 1\,1\,2 & 1\,2\,2 & 2\,1\,2 & 2\,2\,2 & \\ \cline{2-10}
1\,1\,1 & 1 & 0 & 0 & \alpha & 0 & 0 & 0 & \beta & b_1 \\
1\,2\,1 & 0 & 1 & -\alpha & 0 & 0 & 0 & -\beta & 0 & b_2 \\
2\,1\,1 & 0 & -\alpha & 1 & 0 & 0 & -\beta & 0 & 0 & b_3 \\
2\,2\,1 & \alpha & 0 & 0 & 1 & \beta & 0 & 0 & 0 & b_4 \\ \hdashline
1\,1\,2 & 0 & 0 & 0 & \beta & 1 & 0 & 0 & -\alpha & b_5 \\
1\,2\,2 & 0 & 0 & -\beta & 0 & 0 & 1 & \alpha & 0 & b_6 \\
2\,1\,2 & 0 & -\beta & 0 & 0 & 0 & \alpha & 1 & 0 & b_7 \\
2\,2\,2 & \beta & 0 & 0 & 0 & -\alpha & 0 & 0 & 1 & b_8 \\ \hdashline
 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & b_8 & 1 \\ \cline{2-10}
\end{array},$$

where $\alpha, \beta \in \mathbb{R}$ and $b_k \in \mathbb{R}$ for all $k \in \{1, \dots, 8\}$. A concrete example follows in Section 6.4.

6.2.3 Optimising the Inner Radius

Let $\rho(B)$ denote the spectral radius of a real matrix B. The inner radius of the first theta body can be determined by optimising the spectral radius over S:

Proposition. The inner radius of $\mathcal{T}_1$ equals

$$\begin{aligned} r(\mathcal{T}_1) &= \left(\sup\{\|b\| \colon \left(\begin{smallmatrix} \star & b \\ b^t & 1 \end{smallmatrix}\right) \in \widetilde{S}\}\right)^{-1} \\ &= \left(\sup\{\rho(B) \colon B \in S\}\right)^{-\frac{1}{2}} \end{aligned}$$

Proof. The operator norm of a linear map $A \colon \mathbb{R}^n \to \mathbb{R}^m$ with respect to the Euclidean norm is given by

$$\begin{aligned} \|A\|_{\mathrm{op}} &= \sup\{\|Av\| \colon v \in (\mathbb{R}^n)_1\} \\ &= \sup\{\langle Av, w\rangle : v \in (\mathbb{R}^n)_1, w \in (\mathbb{R}^m)_1\} = \|A^t\|_{\mathrm{op}}. \end{aligned}$$

The operator norm of $B = A^tA$ equals the spectral radius $\rho(B)$ of B. In particular, we obtain $\|B\|_{\mathrm{op}} = \sup\{\langle Bv, v\rangle : v \in (\mathbb{R}^n)_1\} = \|A\|_{\mathrm{op}}^2$. Now, let $0 \neq A \in \mathcal{M}_{n+1,n}(\mathbb{R})$ and $B = A^tA$. For all $w \in (\mathbb{R}^{n+1})_1$ with $0 \neq b = A^tw$, we obtain

$$\|b\| = \|A^tw\| \leqslant \|A\|_{\mathrm{op}}.$$

The distance of l^b to zero equals $1/\|b\| \geqslant 1/\|A\|_{\mathrm{op}}$. Furthermore, we obtain $\|A^tw_0\| = \|A\|_{\mathrm{op}} = \sqrt{\rho(B)}$, where w_0 is a unit eigenvector of B with respect to the eigenvalue $\rho(B)$. Hence, we obtain

$$\|B\|_{\mathrm{op}} = \sup\left\{\|b\|^2 \colon \left(\begin{smallmatrix} B & b \\ b^t & 1 \end{smallmatrix}\right) \geqslant 0\right\}.$$

Now, let $B \in S$. From Corollary 6.2.2, it follows that the set

$$P_B := \left\{A^tw \colon A \in \mathcal{M}_{n+1,n}(\mathbb{R}), A^tA = B, w \in (\mathbb{R}^{n+1})_1\right\}$$

lies in $\mathcal{D}_1$. Now, the second equality follows from

$$\sup\{\|b\| \colon b \in P_B\} = \sqrt{\rho(B)}.$$

◇

In general, the 2-norm cannot be optimised over a given set with a linear objective function. Hence, unfortunately, it seems that the optimisation of a linear functional over S or over $\widetilde{S}$ cannot be expressed as a semidefinite program (the operator norm would be less problematic, see [Sto, Example C.3]).

The identity matrix $\mathbb{1}_n$ is always in the spectrahedron $\mathcal{S}$, so that each polynomial l^b, where $b \in (\mathbb{R}^n)_1$, is 1-sos-mod $\mathcal{J}$.

Remark. Let $B \in \mathcal{M}_n(\mathbb{R})$ be positive semidefinite. For practical purposes, it can be useful to attain $\rho(B)$ as follows: Let $A := \sqrt{D}S$, where D is a diagonal matrix and S is an orthogonal matrix such that $B = S^t DS$. Let $k \in \{1, \dots, n\}$ such that the entry (k, k) of D equals $\rho(B)$. Let $w := (0, \dots, 0, 1, 0, \dots, 0)^t$, where the entry 1 is in position k, and let $b := A^t w$. Then $\|A\|_{\text{op}} = \sqrt{\rho(B)} = \|b\|$. In particular, b equals the largest row of A with respect to the Euclidean norm.

6.2.4 A Special Case

Here, we focus on a special class of polynomials, which will be important in the next section where we deal with the case $\mathbb{K} = \mathbb{R}$.

Proposition. Let $\mathcal{P}$ be a proper partition of the set $L_\mathbb{K}$ and let $s\colon L_\mathbb{K} \to \{1, -1\}$ be an arbitrary function. If the polynomial

$$\sum_{T \in \mathcal{P}} \sum_{\substack{a,b \in T \\ a \neq b}} s(a)\, s(b) \cdot x_a x_b$$

lies in $\mathcal{I}$, then for all $T_0 \in \mathcal{P}$, the support functional $1 - \sum_{a \in T_0} s(a) \cdot x_a$ to the vector $y := \frac{1}{\# T_0} \sum_{a \in T_0} s(a) \cdot e_a$ is 1-sos-mod $\mathcal{J}$. Hence, in this case, the inner radius of $\mathcal{T}_1$ is smaller or equal than $r^{-1/2}$, where r is the relative size of $\mathcal{P}$.

Proof. Let $m \in \mathbb{N}$ be the width of $\mathcal{P}$ and let $p\colon \mathcal{P} \to \{1, \dots, m\}$ be a bijective function. Let $T_0 \in \mathcal{P}$, let

$$w_0 := (0, \dots, 0, \underset{\uparrow \text{ position } p(T_0)}{1}, 0, \dots, 0)^t \in \mathbb{R}^m$$

and for all $a \in L_\mathbb{K}$, let

$$w_a := (0, \dots, 0, \underset{\uparrow \text{ position } p(T_a)}{s(a)}, 0, \dots, 0)^t \in \mathbb{R}^m,$$

where T_a is the part of $\mathcal{P}$ with $a \in T$. Now, we consider the matrices $A := (w_a)_{a \in L}$ and $\widetilde{A} := (A|w_0)$. Since $\widetilde{A}^t \widetilde{A} \in \widetilde{\mathcal{S}}$, Theorem 6.2.2

implies that the polynomial l^b with $b := A^t w_0$ is 1-sos-mod $\mathcal{J}$. This polynomial equals the support functional of $y := \frac{1}{\#T_0} \sum_{a \in T_0} s(a) \cdot e_a$, since $l_y = 1 - \sum_{a \in T_0} s(a) \cdot x_a = l^b$. The inner radius of $\mathcal{T}_1(\mathcal{J})$ is smaller or equal than $\|y\| = (\#T_0)^{-1/2}$. $\diamond$

6.2.5 Algorithmic Approach with SageMath

We have implemented the tensor product case with the computer algebra system *SageMath*, see [Sage], which is based on the programming language Python, to describe the first theta body as a projected spectrahedron. (The location of the code can be found on page xxi. To run the code without installing Python, you can use the *SageMathCell*, which is accessible at `https://sagecell.sagemath.org/`). The title of the program is:

A Convex Relaxation of the Projective Unit Ball, Real or Complex: The First Theta Body as a Projected Spectrahedron.

The first part of the program deals with the computation of the following sets for $L = N = \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$, where $r \geqslant 2$ and $n_t \in \{2, \dots, 9\}$:

- (Complex) non-zero Hibi relations $\mathcal{H}_{N_{\mathbb{K}}}$
- (Complex) norming polynomial $u_{N_{\mathbb{K}}}$
- Gröbner basis of $\mathcal{J}$

The second part of the program is based on Theorem 6.2.2. The key features are:

1.a Given a tensor y, we can check whether the support functional l^y is 1-sos-mod $\mathcal{J}$ with the aid of semidefinite programming (see Theorem 6.2.2). If the answer is positive, then l^y is a witness functional for the projective unit ball, and $\|y\|$ is an upper bound on the inner radius of the first theta body $\mathcal{T}_1(\mathcal{J})$, and, hence, of the projective unit ball $\mathcal{B}_{1,\pi}$.

1.b In a second step, if the answer is positive, then we can check according to Proposition 6.2.3 whether the solution can be improved with respect to the length of y.

2. Alternatively, we can search for vectors y whose length is as small as possible such that l^y is 1-sos-mod $\mathcal{J}$ with the aid of random test vectors.

6.3 The First Theta Body in the Real Case

In general, it is not clear how to choose the partition $\mathcal{P}$ and the function s such that Proposition 6.2.4 gives an upper bound on the inner radius of the Hibi body. In this section, we outline a sufficient condition on $\mathcal{P}$ and s in the case where $\mathbb{K} = \mathbb{R}$. It will be essential for Chapter 7 and for Chapter 8 where we obtain explicit bounds on the inner radius of the projective unit ball.

6.3.1 Join-Meet Partitions

Definition. A proper partition $\mathcal{P}$ of L is called a *join-meet partition* of L if for all $T \in \mathcal{P}$ and for all $a, b \in T$, we have

(i) For all $(c, d) \in L^2/S_2$ with $(c, d) \overset{\star}{\longleftrightarrow} (a, b)$, there exists $T' \in \mathcal{P}$ with $c, d \in T'$.

(ii) If $a \neq b$, then $L(a, b)$ is no chain.

Examples for join-meet partitions follow soon.

Let $\mathfrak{T}$ denote the set of all join-meet partitions of L. It is partially ordered by refinement. There exists a common lower bound, the partitions whose parts are the atoms $\{a\}$ with $a \in L$. In particular, $\mathfrak{T}$ is a meet-semilattice. In general, it is not a join-semilattice (we will see this below in Example 6.3.4.IV).

Proposition. Let $\mathcal{P}$ be a join-meet partition of L. Then we have:

(i) Let $X := \cup_{T \in \mathcal{P}} T^2$. The set X/S_2 is the disjoint union of all equivalence classes $[(a, b)]$, where $T \in \mathcal{P}$ and $a, b \in T$.

(ii) If $T \in \mathcal{P}$ and $a, b \in T$ with $a \neq b$, then $\#L(a, b)$ is divisible by four and $\#[(a, b)]$ is divisible by two.

Proof. We first show (i): Let $(c, d) \in [(a, b)]$. Since $\mathcal{P}$ is a join-meet partition, there exists $T' \in \mathcal{P}$ with $c, d \in T'$, that is, $(c, d) \in X/S_2$.

Now, we show (ii): In this case, $\#L(a, b)$ is divisible by four (see Subsection 4.2.6). Hence, the cardinality of

$$[(a, b)] = \{(c, d) \colon a \wedge b = c \wedge d, a \vee b = c \vee d\}$$

is divisible by two. ◇

6.3.2 Optimisation Problems

Since the join-meet partitions do not form a join-semilattice in general, a partition which is maximal for the relative size does not have to be minimal with respect to the width, and vice versa. Now, we discuss those optimisation problems for boolean lattices:

Proposition. Let $n \in \mathbb{N}$ and $B_n := \mathfrak{P}(\{1, \ldots, n\})$.

(i) There exists a join-meet partition $\mathcal{P}_n$ of B_n with two parts of the same length. In particular, $\mathcal{P}_n$ is maximal with respect to the relative size and minimal with respect to the width. If n is even, then $\perp$ and $\top$ have the same colour; otherwise, they have different colours.

(ii) If $n \geqslant 3$ is odd, then there exists a join-meet partition $\mathcal{P}'_n$ of B_n with four parts of the same length such that $\perp$ and $\top$ have the same colour.

Proof. We first look at the lattice $N := \{1, 2, 3\}^n$. For all $a = (a_1, \ldots, a_n) \in N$ and for all $t \in \{1, 2, 3\}$, let $p(a, t)$ denote the *parity* of t in a, that is,

$$p(a, t) = \#\{s \in \{1, \ldots, n\} \colon a_s = t\} \bmod 2.$$

Now, let

$$\begin{aligned} \rho\colon\ N &\to \mathbb{F}_2^3 \\ a &\mapsto (p(a,1),\ p(a,2),\ p(a,3)). \end{aligned}$$

This function will play a major role in Chapter 8.

Statement 1: The pre-images under ρ are a join-meet partition of N. *Proof*: Let $a, b \in N$ with $\rho(a) = \rho(b)$. Let $c, d \in L(a, b)$ with $c \wedge d = a \wedge b$ and $c \vee d = a \vee b$. Since c and d emerge from a and b by an interchange of the entries of a and b in specified positions, we conclude that $\rho(c) = \rho(d)$.

Step 2: B_n can be considered as the boolean sublattice $N(a, b)$ of N with $a := (1, \ldots, 1)$ and $b := (2, \ldots, 2)$. It can be easily proved that the restriction $\mathcal{P}_n$ of the partition from statement 1 to B_n is a join-meet partition, since $B_n = N((1, \ldots, 1), (2, \ldots, 2))$. We obtain

$$\rho(1, \ldots, 1) = \begin{cases} (0, 0, 0), n \text{ even}, \\ (1, 0, 0), n \text{ odd}, \end{cases} \quad \text{and}$$

$$\rho(2,\dots,2) = \begin{cases} (0,0,0), n \text{ even}, \\ (0,1,0), n \text{ odd}, \end{cases}$$

which proves (i).

Step 3: To show (ii) in the case where $n \geqslant 3$ and n is odd, we consider the boolean sublattice $N(c,d)$ of N for $c := (2,1,1,\dots,1)$ and $d := (3,3,2,\dots,2)$. Let $\mathcal{P}'_n$ denote the restriction of the partition from statement 1 to $N(c,d)$. It can be easily verified that $\mathcal{P}'_n$ is a join-meet partition. We obtain $\rho(c) = \rho(d) = (0,1,0)$, that is, c and d have the same colour. The boolean sublattice $\{1,2\}^{n-3}$ of $N(c,d)$ (we consider the last $n-3$ coordinates) can be partitioned with the parts $G := \rho^{-1}(0,0,0)$ and $U := \rho^{-1}(1,1,0)$. For each $a \in G$ and for each $b \in U$, we obtain

$$\begin{aligned}
&(2,1,1,b),(3,3,2,b),(2,1,2,a),(3,3,1,a) \in \rho^{-1}(1,0,0),\\
&(2,1,1,a),(3,3,2,a),(2,1,2,b),(3,3,1,b) \in \rho^{-1}(0,1,0),\\
&(2,3,2,a),(3,1,1,a),(2,3,1,b),(3,1,2,b) \in \rho^{-1}(0,0,1),\\
&(2,3,2,b),(3,1,1,b),(2,3,1,a),(3,1,2,a) \in \rho^{-1}(1,1,1).
\end{aligned}$$

Hence,

$$\#\rho^{-1}(1,0,0) = \#\rho^{-1}(0,1,0) = \#\rho^{-1}(0,0,1) = \#\rho^{-1}(1,1,1) = 2^{n-2}.$$

◇

6.3.3 Splitting Functions

Let B be a finite boolean lattice. As above, the complement of $a \in B$ is denoted by a'.

Definition. A function $s \colon B \to \{-1,1\}$ is called a *splitting function* for B if there exists a bijection $\beta \colon B \to B$ such that $\beta(b)' = \beta(b')$ and $s(b)s(b') = -s(\beta(b))s(\beta(b'))$ for all $b \in B$.

Proposition. Let $s \colon B \to \{-1,1\}$ be a function. The following are equivalent:

(a) s is a splitting function for B.

(b) The parts

$$\begin{aligned} S_B^+ &:= \{b \in B \colon s(b) = s(b')\} \text{ and} \\ S_B^- &:= \{b \in B \colon s(b) \neq s(b')\} \end{aligned}$$

have the same length.

Proof. If s is non-constant, then the sets S_B^+ and S_B^- are a complementary partition of B. For all $b \in B$, the complement b' lies in the same part of this partition.

We first show (a) $\Rightarrow$ (b). If s is a splitting function for B, then $\beta(S_B^+) \subseteq S_B^-$ and $\beta(S_B^-) \subseteq S_B^+$, that is, $\#S_B^+ = \#S_B^-$.

Now, we show (b) $\Rightarrow$ (a). The bijection β can be constructed as follows: There exist complementary partitions $S_B^{+,1}$, $S_B^{+,2}$ of S_B^+ and $S_B^{-,1}$, $S_B^{-,2}$ of S_B^- in parts of the same length such that b and b' lie in different sets, for all $b \in B$. Now, we choose an arbitrary bijection $\beta_B^1 \colon S_B^{+,1} \to S_B^{-,1}$. The function $\beta_B^2 \colon S_B^{+,2} \to S_B^{-,2}$, $b \mapsto \beta_B^1(b')'$, is also a bijection. Hence, the following diagram commutes:

$$\begin{tikzcd}
S_B^{+,1} \arrow[r, "'"] \arrow[d, "\beta_B^1"] & S_B^{+,2} \arrow[d, "\beta_B^2"] \\
S_B^{-,1} \arrow[r, "'"] & S_B^{-,2}
\end{tikzcd}$$

Let β be piece-wise defined by β_B^1, β_B^2, $(\beta_B^1)^{-1}$ and $(\beta_B^2)^{-1}$. ◇

Definition. Let $\mathcal{P}$ be a join-meet partition of L. A function $s \colon L \to \{-1, 1\}$ is called a *splitting function* for $\mathcal{P}$, if for all $T \in \mathcal{P}$ and for all $a, b \in T$ with $a \neq b$, the restriction of s to $L(a, b)$ is a splitting function for $L(a, b)$. In this case, the join-meet partition $\mathcal{P}$ is called *splitting*.

6.3.4 Some Examples

A partition of L can be indicated by a "numbering" or "colouring" of the Hasse diagram of L, whereas two elements are assigned to the same number (or colour, respectively) if and only if they belong to the same part. In the case of a join-meet partition, neighbouring elements have different colours (or numbers). A splitting function could be indicated by a colouring or by an additional minus sign, whenever an element is assigned to -1.

The following three examples show different join-meet partitions which have a splitting function.

Example. Figure 6.1 on page 174 shows three different join-meet partitions of the lattice D_{18}, each with a splitting function. In each case, the parts are indicated by numbers, and a splitting function is indicated by a red colouring, whenever an element is assigned to -1, and a black colouring, whenever an element is assigned to 1.

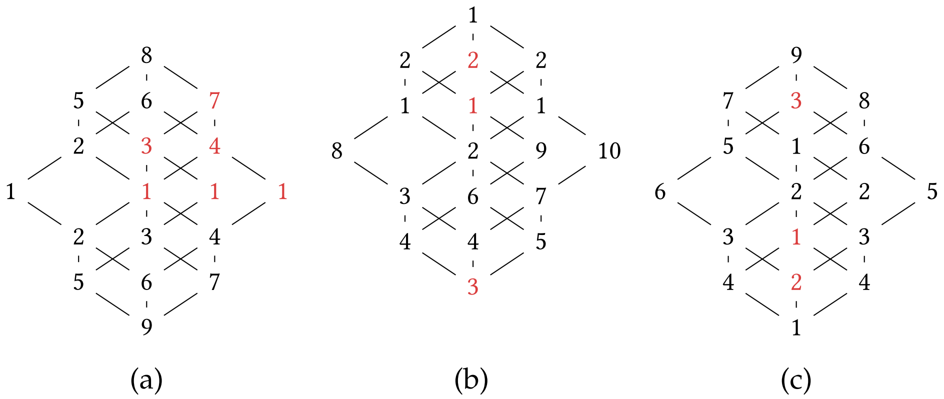


Figure 6.1: Three different join-meet partitions of D_{18}.

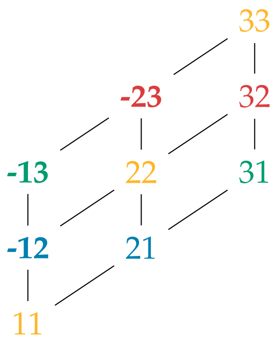


Figure 6.2: A splitting join-meet partition of $\{1, 2, 3\}^2$.

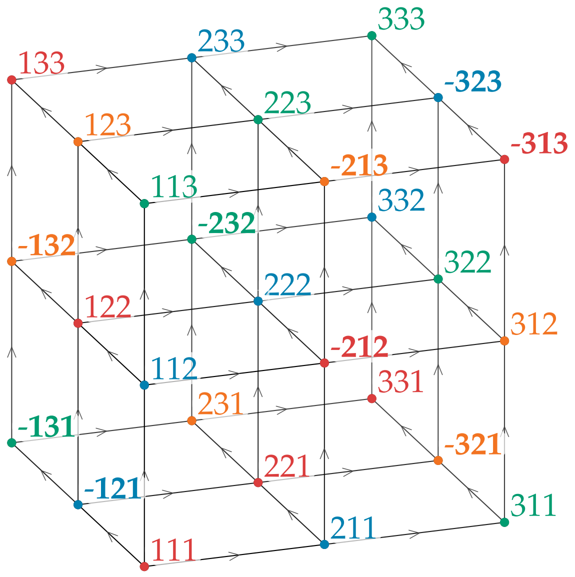


Figure 6.3: A splitting join-meet partition of $\{1, 2, 3\}^3$.

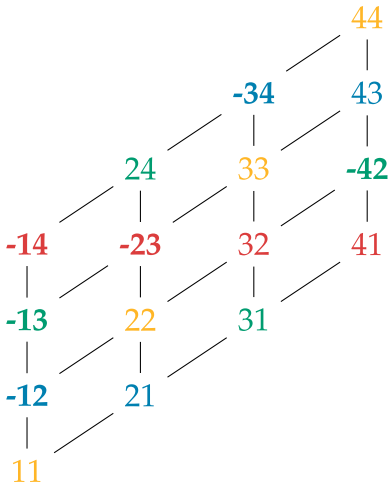


Figure 6.4: A splitting join-meet partition of $\{1,2,3,4\}^2$.

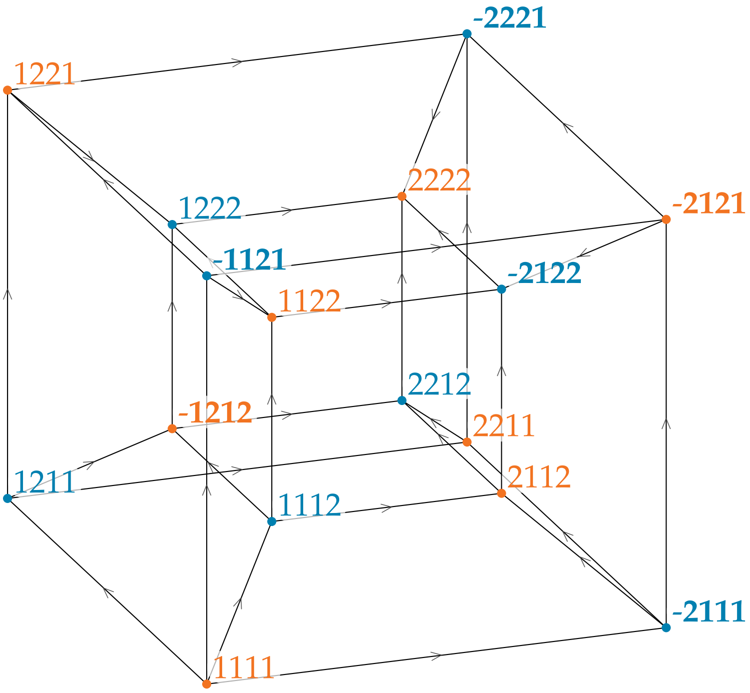


Figure 6.5: A splitting join-meet partition of the tesseract $\{1,2\}^4$.

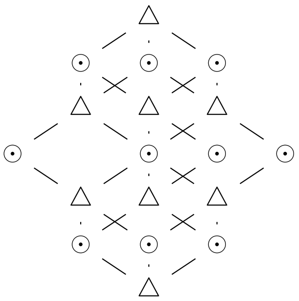


Figure 6.6: A least upper bound, but no join-meet partition.

Example. Figure 6.2 shows a Hasse diagram of the lattice $\{1, 2, 3\}^2$. Figure 6.3 shows a Hasse diagram of the lattice $\{1, 2, 3\}^3$, which looks like a three-dimensional grid. Here, the partial order is indicated by arrows. In each example, the parts of a join-meet partition are indicated by colours, and a splitting function is indicated by a minus sign and by bold text whenever an element is assigned to -1. The background for these examples can be found in Chapter 8.

Example. Figure 6.4 shows a Hasse diagram of the lattice $\{1, 2, 3, 4\}^2$. Figure 6.5 shows a diagram (not a Hasse diagram) of the lattice $\{1, 2\}^4$, reminding of a tesseract, which is a four-dimensional cube. The join-meet partitions and the splitting functions are indicated according to the last example. The motivation for these examples can be found in Chapter 7.

Example. This example shows that the join-meet partitions of a given lattice are, in general, no join-semilattice. Figure 6.6 on page 176 shows the least upper bound of the partitions (a) and (b) in Figure 6.1. The two parts of this partition are indicated by the shapes $\triangle$ and $\odot$. It is no join-meet partition and there is no coarser partition which is a join-meet partition. Hence, the join-meet partitions (a) and (b) have no least upper bound.

Up to now, it is an open question whether there is always a splitting function for a given join-meet partition.

6.3.5 Splitting Join-Meet Partitions and the Join-Meet Ideal

Lemma. Let $s\colon L \to \{-1,1\}$ be an arbitrary function. Let $\mathcal{P}$ be a join-meet partition of L. Then the following are equivalent:

(a) For all $T \in \mathcal{P}$ and for all $a, b \in \mathcal{P}$, $a \neq b$, the polynomial

$$f^s_{a,b} := \sum_{(c,d)\in[(a,b)]} s(c)\, s(d) \cdot x_c\, x_d$$

lies in the join-meet ideal $\mathcal{J}$.

(b) For all $T \in \mathcal{P}$ and for all $a, b \in \mathcal{P}$, $a \neq b$, we have

$$\sum_{(c,d)\in[(a,b)]} s(c)\, s(d) = 0.$$

(c) s is a splitting function for $\mathcal{P}$.

Proof. The equivalence of (a) and (b) follows from Subsection 5.5.1.

Now, we show the equivalence of (b) and (c). Let $T \in \mathcal{P}$ and let $a, b \in \mathcal{P}$, $a \neq b$. Let $L' := L(a,b)$ and let

$$S^+_{L'} := \{c \in L' \colon s(c) = s(c')\} \text{ and}$$
$$S^-_{L'} := \{c \in L' \colon s(c) \neq s(c')\}$$

(also here, c' denotes the complement of c in L'). In what follows, for all $c \in L'$, we write c' for the complement of c in L' (that is, c' is the uniquely defined element with $a \wedge b = c \wedge c'$ and $a \vee b = c \vee c'$). In particular, we have

$$[(a,b)] = \{(c,c') \colon c \in S^+_{L'}\} \cup \{(d,d') \colon d \in S^-_{L'}\}.$$

By definition, for all $c \in S^+_{L'}$, we have $s(c)\, s(c') = 1$, and for all $d \in S^-_{L'}$, we have $s(d)\, s(d') = -1$. Hence, it follows that

$$\begin{aligned}\sum_{(c,d)\in[(a,b)]} s(c)\, s(d) \qquad\qquad (6.2)\\ &= \frac{1}{2}\sum_{c\in S^+_{L'}} \underbrace{s(c)\, s(c')}_{=1} + \frac{1}{2}\sum_{d\in S^-_{L'}} \underbrace{s(d)\, s(d')}_{=-1}\\ &= \frac{1}{2}\Big(\sum_{c\in S^+_{L'}} 1 - \sum_{d\in S^-_{L'}} 1\Big)\\ &= \frac{1}{2}\Big(\#S^+_{L'} - \#S^-_{L'}\Big).\end{aligned}$$

Now, we see the following: If s is a splitting function for $\mathcal{P}$, then the parts $S^+_{L'}$ and $S^-_{L'}$ have the same length (see Proposition 6.3.3). Hence, expression (6.2) equals zero. This proves (c). On the other hand, if expression (6.2) equals zero for all $T \in \mathcal{P}$ and for all $a, b \in \mathcal{P}$, $a \neq b$, then s is a splitting function for $\mathcal{P}$ according to Proposition 6.3.3. This proves (b). ◇

6.3.6 Sos Polynomials and Splitting Join-Meet-Partitions

Here, we come to the most important result of this section, saying that a splitting join-meet partition leads to explicit witnesses for $\mathcal{T}_1$ in the real case.

Theorem. Let $\mathcal{P}$ be a join-meet partition and let $s \colon L \to \{-1, 1\}$ be a splitting function for $\mathcal{P}$. Let $T_0 \in \mathcal{P}$ and let

$$y := \frac{1}{\#T_0} \sum_{a \in T_0} s(a) \cdot e_a \in \mathbb{R}^L.$$

Then the support functional

$$l_y = 1 - \sum_{a \in T_0} s(a) \cdot x_a$$

is a 1-sos-mod $\mathcal{J}$-polynomial.

Proof. We show that the polynomial

$$d := \sum_{T \in \mathcal{P}} \sum_{\substack{a,b \in T \\ a \neq b}} s(a)s(b) \cdot x_a x_b$$

lies in $\mathcal{I}$. Then the statement follows from Proposition 6.2.4.

Let Q be the set of all equivalence classes $[(a, b)]$, where there exists $T \in \mathcal{P}$ with $a, b \in T$ and $a \neq b$. Since $\mathcal{P}$ is a join-meet partition and according to Proposition 6.3.1, the disjoint union of the elements of Q equals the set $P := \{(a, b) \in (\cup_{T \in \mathcal{P}} T^2)/S_2 \colon a \neq b\}$. Hence, we obtain

$$\begin{aligned} d &= 2 \sum_{(a,b) \in P} s(a)s(b) \cdot x_a x_b \\ &= 2 \sum_{[(a,b)] \in Q} \Bigg(\sum_{(c,d) \in [(a,b)]} s(c)s(d) \cdot x_c x_d \Bigg) \end{aligned}$$

$$= 2 \sum_{[(a,b)] \in Q} f^s_{a,b}.$$

According to Lemma 6.3.5, the polynomial $f^s_{a,b}$ lies in the ideal $\mathcal{I}$. Hence, also d lies in $\mathcal{I}$. ◇

The witness hyperplanes of the last theorem can be used to obtain upper bounds on the inner radius of the Hibi body:

Corollary. Let $r \in \mathbb{N}$ be the relative size of $\mathcal{P}$. Then the inner radius $r(H)$ of the Hibi body H satisfies the inequality

$$r(H) \leqslant r(\mathcal{T}_1) \leqslant 1/\sqrt{r}.$$

Proof. For any $T \in \mathcal{P}$, the distance of l_y to zero equals $\|y\| = 1/\sqrt{\#T}$ and is an upper bound on the inner radius. ◇

Remark. An explicit decomposition of l_y as a sum of squares modulo $\mathcal{J}$ is given as follows: At first, a short computation shows that there exists a polynomial $d \in \mathcal{I}$ such that

$$\begin{aligned}\sum_{T\in\mathcal{P}} \Big(\sum_{a\in T} s(a)\cdot x_a\Big)^2 &= \sum_{T\in\mathcal{P}} \Big(\sum_{a\in T} s(a)^2 \cdot x_a^2 + \sum_{\substack{a,b\in T\\ a\neq b}} s(a)s(b)\cdot x_a x_b\Big)\\ &= \sum_{a\in L} x_a^2 + d.\end{aligned}$$

Let $p_y := 1 - l_y = \sum_{a\in T_0} s(a)\cdot x_a$. A sum of squares is given by

$$\begin{aligned} q &:= l_y^2 + \sum_{\substack{T\in\mathcal{P}\\ T\neq T_0}} \Big(\sum_{a\in T} s(a)\cdot x_a\Big)^2\\ &= 1 - 2p_y + \sum_{T\in\mathcal{P}} \Big(\sum_{a\in T} s(a)\cdot x_a\Big)^2\\ &= 2 - 2p_y + \underbrace{\sum_{a\in L} x_a^2 - 1}_{=u_L} + d\\ &= 2l_y + u_L + d.\end{aligned}$$

The polynomial $h := -u_L - d$ lies in $\mathcal{J}$. Hence, $l_y = 1/2 \cdot (q + h)$ is a sum of squares modulo $\mathcal{J}$.

6.3.7 Application to the Projective Unit Ball

The following statement is essential for Chapter 7 and Chapter 8. It shows how theta bodies can be used to calculate the projective norm of a tensor.

Proposition. Let y be a tensor in a real finite-dimensional tensor product with $0 < \|y\|_\pi \leqslant 1$ and let $k \in \mathbb{N}$ such that the support functional l_y to y is k-sos-mod $\mathcal{J}$ (for instance, this is the case if y has the form from Theorem 6.3.6). Then $\|y\|_\pi = 1$.

Proof. Let us assume that $d := \|y\|_\pi < 1$. Now, on the one hand, we have $1/d \cdot y \in \mathcal{B}_{1,\pi} \subseteq \mathcal{T}_k$. On the other hand, we have

$$l_y\left(\frac{1}{d}\cdot y\right) = 1 - \left\langle \frac{1}{d}\cdot y, \frac{y}{\|y\|^2} \right\rangle = 1 - \frac{1}{d} < 0,$$

which implies $1/d \cdot y \notin \mathcal{T}_k$. This is a contradiction. ◇

The following statement can be found in [Lang] and in [RS2]:

Proposition. Let $m, n \in \mathbb{N}$ with $n \leqslant m$. The projective unit ball $\mathcal{B}_{1,\pi}$ in the tensor product $\mathbb{R}^m \otimes \mathbb{R}^n$ equals its first theta body $\mathcal{T}_1$.

Proof. We consider the tensor $y := \frac{1}{n}(e_1 \otimes e_1 + \ldots + e_n \otimes e_n)$.
Step 1: A join-meet partition $\mathcal{P}$ of the indexing tuples $L = \{1, \ldots, m\} \times \{1, \ldots, n\}$ is given by the parts

$\{1\,1,\ \ldots,\ n\,n\}$,
$\{a\,b,\ b\,a\}$ for all $a, b \in \{1, \ldots, n\}$ with $a \neq b$,
$\{a\,b\}$ for all $a \in \{n+1, \ldots, m\}$, $b \in \{1, \ldots, n\}$.

A splitting function s for $\mathcal{P}$ is given by

$$s(a\,b) = \begin{cases} 1, & a \geqslant b, \\ -1, & a < b, \end{cases}$$

where $a \in \{1, \ldots, m\}$, $b \in \{1, \ldots, n\}$. Now, with Theorem 6.3.6, the support functional $l_y = 1 - (x_{1\,1} + \ldots + x_{n\,n})$ to y is a sum of squares modulo $\mathcal{J}$. (In the case $m = n$, this partition is a special case of the parity partition which will be defined in Chapter 8.)

Step 2: Let $z \in \mathbb{R}^m \otimes \mathbb{R}^n$ with $\|z\|_\pi = 1$. With the Schmidt decomposition, see Subsection 3.3.1, there exist orthogonal maps $U \in \mathcal{U}_m(\mathbb{R})$, $V \in \mathcal{U}_n(\mathbb{R})$ and $\sigma_1, \ldots, \sigma_n \in [0,1]$ with $\sum_{k=1}^n \sigma_k = 1$ such that

$$z = (U \otimes V)\Big(\sum_{k=1}^{n} \sigma_k \cdot e_k \otimes e_k\Big).$$

The tensor $z_0 := \sum_{k=1}^n \sigma_k \cdot e_k \otimes e_k$ (whose projective norm equals 1) is a zero of l_y. Hence, z_0 lies in the boundary of $\mathcal{T}_1$. With Proposition 6.1.3.II, also z lies in the boundary of $\mathcal{T}_1$. Hence, $\mathcal{B}_{1,\pi}$ and $\mathcal{T}_1$ coincide. (In the case $m = n$, we refer also to Theorem 3.3.8.) ◇

6.4 The First Complex Theta Body

In this section, we consider the case where $\mathbb{K} = \mathbb{C}$. Using Theorem 6.2.2, it is possible to determine the inner radius of the first complex theta body.

6.4.1 An Upper Bound on the Inner Radius

Proposition. Let $a, b \in L$ such that $L(a,b)$ is no chain. Then the support functional

$$l_y = 1 - x_{a,1} - x_{b,1}$$

to $y := \frac{1}{2}(e_{a,1} + e_{b,1})$ is 1-sos-mod $\mathcal{J}$. Hence, $1/\sqrt{2}$ is an upper bound on the inner radius of the first complex theta body $\mathcal{T}_1$.

Proof. *Step 1*: The boolean lattice $L(a,b)$ is no chain. *Case 1.1*: a and b are comparable. Then there exist $c, d \in L(a,b)$ which are not comparable such that $L(a,b) = L(c,d)$. *Case 1.2*: a and b are not comparable. In this case, let $c := a \wedge b$ and $d := a \vee b$.

Step 2: Since either (a,b) or (c,d) is a chain in L^2/S_2, the polynomial

$$d := 2\left((x_{a,1}x_{b,1} - x_{c,1}x_{d,1}) - (x_{a,2}x_{b,2} - x_{c,2}x_{d,2})\right)$$

is a multiple of a complex Hibi relation, that is, it lies in $\mathcal{J}$.

Step 3: Now, we show that l_y is a sum of squares modulo $\mathcal{J}$. A simple computation shows that $l_y = 1/2 \cdot (s + h)$, where

$$s := \Big(1 - x_{a,1} - x_{b,1}\Big)^2 + \Big(x_{a,2} - x_{b,2}\Big)^2$$

$$+ (x_{c,1} - x_{d,1})^2 + (x_{c,2} + x_{d,2})^2 + \sum_{e \in L \setminus \{a,b,c,d\}} (x_{e,1}^2 + x_{e,2}^2)$$

is a sum of squares and

$$h := 1 - \sum_{e \in L} (x_{e,1}^2 + x_{e,2}^2) - d$$

lies in $\mathcal{J}$. The distance of l_y to zero equals $\|y\| = 1/\sqrt{2}$, and the inner radius of $\mathcal{T}_1$ is smaller or equal than $\|y\|$. ◇

Example. The projective norm of the GHZ-vector $\xi_{\mathrm{GHZ}} = 1/\sqrt{2} \cdot (e_{1\,1\,1} + e_{2\,2\,2})$ in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ equals $\sqrt{2}$, see Subsection 3.3.3. With $a := 1\,1\,1$ and $b := 2\,2\,2$, Proposition 6.4.1 implies that the boundary of the first complex theta body touches the projective unit sphere at $\frac{1}{2}(e_{1\,1\,1} + e_{2\,2\,2})$.

6.4.2 The Inner Radius of the First Complex Theta Body

To determine the inner radius of the first complex theta body, we deal with the spectral radius of a specific block matrix.

Lemma. Let $m \in \mathbb{N}$ and let $Q, R \in \mathcal{M}_m(\mathbb{R})$ with $R = R^t$ or $R = -R^t$. Let $r > 0$. Let $B \in \mathcal{M}_{2m}(\mathbb{R})$ such that the spectrum of B lies in $[0, \infty)$ and such that B has the form

$$B = \left(\begin{array}{c|c} Q & R \\ \hline R^t & -Q + r\mathbb{1}_m \end{array} \right).$$

Then $\rho(B) \leqslant r$.

Proof. We first note that it suffices to show the statement in the case where $r = 1$.

Statement 1: Let $r = 1$ and $\lambda \in \mathbb{R}$. Then λ is an eigenvalue of B if and only if $1 - \lambda$ is an eigenvalue of B.

Proof: If $v = \binom{v_1}{v_2}$ is an eigenvector of B with respect to the eigenvalue λ, then

$$Bv = \begin{pmatrix} Qv_1 + Rv_2 \\ R^t v_1 - Qv_2 + v_2 \end{pmatrix} = \lambda \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}.$$

If R is symmetric, then it follows that

$$B \begin{pmatrix} v_2 \\ -v_1 \end{pmatrix} = \begin{pmatrix} Qv_2 - Rv_1 \\ Rv_2 + Qv_1 - v_1 \end{pmatrix} = (1 - \lambda) \begin{pmatrix} v_2 \\ -v_1 \end{pmatrix},$$

and if R is antisymmetric, then it follows that

$$B\begin{pmatrix} v_2 \\ v_1 \end{pmatrix} = \begin{pmatrix} Qv_2 + Rv_1 \\ -Rv_2 - Qv_1 + v_1 \end{pmatrix} = (1-\lambda)\begin{pmatrix} v_2 \\ v_1 \end{pmatrix},$$

that is, $1-\lambda$ is also an eigenvalue of B.

Step 2: If $B \geqslant 0$, then statement 1 implies that $0 \leqslant \lambda \leqslant 1$ for each eigenvalue λ of B. ◇

The most important case for us occurs when B is positive semidefinite (that is, Q is symmetric).

Theorem. The inner radius of the first complex theta body $\mathcal{T}_1^{\mathbb{C}}(\mathcal{J})$ equals $1/\sqrt{2}$.

Proof. According to Proposition 6.4.1, the inner radius of $\mathcal{T}_1^{\mathbb{C}}(\mathcal{J})$ is smaller or equal than $1/\sqrt{2}$. We show with Proposition 6.2.3 and Corollary 6.2.2 that it cannot be smaller. To do this, we show that the spectral radius of any $B \in S$ is smaller or equal than 2.

The polynomials in $\mathbb{C}[x_a\colon a \in L]$ can be identified with symmetric $2n \times 2n$ matrices via

$$\begin{array}{c|ccc|ccc}
 & \cdots & b,1 & \cdots & \cdots & b,2 & \cdots \\
\hline
\vdots & & \vdots & & & \vdots & \\
a,1 & \cdots & x_{a,1}x_{b,1} & \cdots & \cdots & x_{a,1}x_{b,2} & \cdots \\
\vdots & & \vdots & & & \vdots & \\
\hline
\vdots & & \vdots & & & \vdots & \\
a,2 & \cdots & x_{a,2}x_{b,1} & \cdots & \cdots & x_{a,2}x_{b,2} & \cdots \\
\vdots & & \vdots & & & \vdots &
\end{array},$$

where L is ordered arbitrary and $L_{\mathbb{C}}$ is ordered by $c,1 > d,1 > c,2 > d,2$ (whenever $c > d$, where $c, d \in L$). According to Proposition 5.4.6, a basis of the second homogeneous part $(\imath(\mathcal{I}))_2$ of $\imath(\mathcal{I})$ is given by the real and the imaginary parts of the non-zero Hibi relations in $\mathbb{R}[x_a\colon a \in L]$. We recall that

$$\begin{aligned} V_{\mathrm{Re,Re}} + V_{\mathrm{Im,Im}} &= \mathrm{LH}(x_{a,1}x_{b,1},\, x_{a,2}x_{b,2} \,:\, a, b \in L) \text{ and} \\ V_{\mathrm{Re,Im}} &= \mathrm{LH}(x_{a,1}x_{b,2} \,:\, a, b \in L) \end{aligned}$$

(see Subsection 5.4.6). The projection of $(\imath(\mathcal{I}_L))_2$ onto $V_{\mathrm{Re,Re}} + V_{\mathrm{Im,Im}}$ lies in the linear hull of

$$\{x_{a,1}x_{b,1} - x_{a,2}x_{b,2}\colon a, b \in L, a \neq b\},$$

and the projection of $(\imath(\mathcal{J}_L))_2$ onto $V_{\mathrm{Re,Im}}$ lies in the linear hull of

$$\{x_{a,1}x_{b,2} + x_{a,2}x_{b,1} \colon a, b \in L, a \neq b\}.$$

Hence, an element of $(\imath(\mathcal{J}_L))_2$ has the form

$$\left(\begin{array}{c|c} Q_0 & R_0 \\ \hline R_0 & -Q_0 \end{array}\right), \tag{6.3}$$

where $Q_0, R_0 \in \mathcal{M}_n(\mathbb{R})$ are symmetric matrices and the diagonal of Q_0 is zero. Now, let $B \in S$. The main diagonal elements of B are equal to 1, and the other elements of B have the form (6.3). Hence, B has the form

$$B = \left(\begin{array}{c|c} Q_0' & R_0 \\ \hline R_0 & -Q_0' + 2\mathbb{1}_n \end{array}\right),$$

where $Q_0' := Q_0 + \mathbb{1}_n$. From the previous lemma, it follows that the spectral radius of B is not larger than 2. ◇

Example. A matrix B in the spectrahedron S which corresponds to the polynomial $1 - x_{a,1} - x_{b,1}$ from Proposition 6.4.1 is given by

$$B := \left(\begin{array}{c|c} Q & 0 \\ \hline 0 & -Q + 2\mathbb{1}_n \end{array}\right)$$

with

$$Q \;:=\; \begin{array}{c|cccc|c} & a & b & a\wedge b & a\vee b & \cdots \\ \hline a & 1 & 1 & & & \\ b & 1 & 1 & & & \\ a\wedge b & & & 1 & -1 & \\ a\vee b & & & -1 & 1 & \\ \vdots & & & & & \mathbb{1} \end{array}$$

(up to the order of the rows and columns), see also Example 6.2.2. Letting $A := {}^1\!/\!\sqrt{2}\,B$, $w := {}^1\!/\!\sqrt{2}\,(1, 1, 0, \dots, 0)^t$ and $b := A^t w$, we obtain $B = A^t A$ and $l^b = 1 - x_{a,1} - x_{b,1}$.

6.4.3 The First Complex Theta Body in a Special Case

Now, we can show that the projective unit ball in $\mathbb{C}^2 \otimes \mathbb{C}^2$ equals the first complex theta body.

Theorem. In the case where $\mathbb{K} = \mathbb{C}$ and $L = \{1, 2\}^2$, the first complex theta body is exact, that is, $\mathcal{T}_1 = H$.

Proof. *Statement 1*: We have $\imath(\mathrm{Sym}_{\mathbb{C}^L}(H)) \subseteq \mathrm{Sym}_{\mathbb{R}^{L_\mathbb{C}}}(\mathcal{T}_k(\mathcal{J}))$ for all $k \in \mathbb{N}$.
Proof: With Corollary 2.2.10, we have $\imath(\mathrm{Sym}_{\mathbb{C}^L}(H)) \subseteq \mathrm{Sym}_{\mathbb{R}^{L_\mathbb{C}}}(\imath(H))$. From Corollary 5.5.3.III, it follows that the homogeneous complex-join-meet ideal $\mathcal{I}$ is a vanishing ideal. Hence, Proposition 2.5.7.II can be applied with $J := \mathcal{J}$, $V_0 := \mathcal{Z}_\mathbb{R}(\mathcal{I})$ and $C := \imath(H)$, which gives

$$\mathrm{Sym}_{\mathbb{R}^{L_\mathbb{C}}}(\imath(H)) \cap \mathcal{U}_{\#L_\mathbb{C}}(\mathbb{R}) \subseteq \mathrm{Sym}_{\mathbb{R}^{L_\mathbb{C}}}(\mathcal{T}_k(\mathcal{J})).$$

Finally, let $V := V_0 \cap (\mathbb{C}^L)_1$ and let $A \in \mathrm{Sym}_{\mathbb{C}^L}(V)$ (according to Proposition 6.1.3.I, we have $\mathrm{Sym}_{\mathbb{C}^L}(V) = \mathrm{Sym}_{\mathbb{C}^L}(H)$). Since V contains the vectors $e_{1,1}$, $e_{1,2}$, $e_{2,1}$, $e_{2,2}$, which form an orthonormal basis of $\mathbb{C}^L$, we conclude that A is unitary, and $\imath(A)$ is orthogonal (see Corollary 2.2.10).

Statement 2: Each boundary point of H is also a boundary point of $\mathcal{T}_1$, which yields $H = \mathcal{T}_1$.
Proof: (The following arguments can also be found in the proof of Proposition 6.3.7.II.) We have $H = \mathcal{B}_{1,\pi}$. The vector $\frac{1}{2}(e_1 \otimes e_1 + e_2 \otimes e_2)$ is contained in a maximal face F_0 of $\mathcal{B}_{1,\pi}$. According to Proposition 6.4.1, F_0 is contained in a face W_0 of $\mathcal{T}_1$. Let F be a maximal face of $\mathcal{B}_{1,\pi}$, see Theorem 3.3.8. With the < (see also Theorem 3.3.4), there exists a symmetry $U \in \mathrm{Sym}_{\mathbb{C}^L}(H)$ with $U(F_0) = F \subseteq U(W_0)$. Now, statement 1 says that $U(W_0)$ is a subset of the boundary of $\mathcal{T}_1$. Hence, the maximal faces of $\mathcal{B}_{1,\pi}$ are contained in the boundary of $\mathcal{T}_1$. ◇

Up to now, it is not clear whether Theorem 6.4.3 can be generalised. Indeed, it is based on Example 5.4.1 and on the Schmidt decomposition. Previous discussions suggest that a generalisation might not be straightforward.

6.5 Join-Meet Partitions and Codes

In this section we discuss the relation of join-meet partitions to error-correcting codes. To do this, we first introduce basic notions related to (linear) codes according to the standard literature such as [Bet], [Ebe] or [MS] (non-linear codes). See also textbooks on sphere packings such as [CS]. We then show in Theorem 6.5.2 that each part of a join-meet partition of indexing tuples can be considered as a (in general non-linear) code. Secondly, we deal with linear codes to provide the basic notions for Theorem 8.4.6.

Let $\mathbb{F}$ be a finite field.

6.5.1 Codes

Definition. A *code* C of *length* $n \in \mathbb{N}$ is a non-empty subset of $\mathbb{F}^n$. In the case where $\mathbb{F} = \mathbb{F}_2$, it is called a *binary code*. If C is a linear subspace of the vector space $\mathbb{F}^n$, it is called a *linear code*. The elements of C are called *codewords*.

Let $v \in \mathbb{F}^n$. The *weight* $\mathrm{wt}(v)$ of v is the number of non-zero entries in v. For all $v, w \in \mathbb{F}^n$, the *Hamming distance* $d(v, w)$ of v and w is defined by $d(v, w) := \mathrm{wt}(v - w)$. The *minimum distance* $d(C)$ of the code C is defined as the minimum of $d(v, w)$, ranging over $v, w \in C$ with $v \neq w$ (in the case where C has just one codeword, the minimum distance is defined as 0). Thus, $d(C)$ is the largest number $d \in \mathbb{N}_0$ with the property that any two different vectors differ in at least d positions. The *minimum distance* $d(w, C)$ of $w \in \mathbb{F}^n$ to C is defined as the minimum of $d(v, w)$, ranging over $v \in C$.

A linear code in $\mathbb{F}^n$ with dimension $k \in \mathbb{N}_0$ and minimum distance $d \in \mathbb{N}_0$ is called a (n, k, d)*-code* or a (n, k)*-code*.

Since the Hamming distance is a sum of copies of the discrete metric, it follows that $\mathbb{F}^n$, equipped with the Hamming distance, is a metric space.

Given a codeword $v \in C$ and an arbitrary element $b \in \mathbb{F}^n$, which is called *noise*, then each position where b has a non-zero entry is called an *error* of $w := v + b$ with respect to v. Hence, the number of errors of w with respect to v equals $\mathrm{wt}(b)$. Now, one can ask for a codeword $\widetilde{v} \in C$, such that $d(w, C) = d(w, \widetilde{v}) =: m$. If $\widetilde{v}$ is uniquely determined and equals v, we say that w *can be corrected* by C with respect to v. If $v + b$ can be corrected for all codewords $v \in C$ and for all noises $b \in \mathbb{F}^n$ with $\mathrm{wt}(b) \leqslant m$ with respect to v, we say that C *can correct* m errors.

Now, it can be easily seen that a code C with $\#C \geqslant 2$ and minimum distance $d := d(C)$ can correct m (and at most m) errors, where m is defined by $d = 2m + 1$ for d odd and by $d = 2(m + 1)$ for d even, see [Bet, page 6].

Example. The *binary repetition code* $C := \{(0,0,0),(1,1,1)\} \subseteq \mathbb{F}_2^3$ has minimum distance $d(C) = 3$ and can correct 1 error. For instance, C can correct $(0,1,0)$ with respect to $(0,0,0)$ since $d((0,1,0),(0,0,0)) = 1$ and $d((0,1,0),(1,1,1)) = 2$. Figure 6.7 shows this code (orange) as a subset of $\mathbb{F}_2^3$ (grid). Those elements in $\mathbb{F}_2^3 \backslash C$ which can be corrected with respect to $(0,0,0)$ are coloured in blue and those which can be corrected with respect to $(1,1,1)$ are coloured in green.

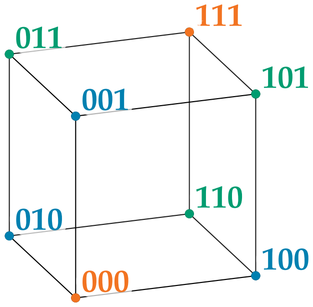


Figure 6.7: A binary repetition code.

6.5.2 Join-Meet Partitions and Codes

We now outline that join-meet partitions can be related to codes.

Let $\tilde{n}, r \geqslant 2$ and let $N := \{1,\ldots,\tilde{n}\}^r$ be the indexing tuples for the tensor product $\mathbb{R}^{\tilde{n}} \otimes \cdots \otimes \mathbb{R}^{\tilde{n}}$. We can embed the set $\{1,\ldots,\tilde{n}\}$ in a finite field. This gives the following relationship to codes:

Theorem. Each part of a join-meet partition $\mathcal{P}$ of N is a (in general non-linear) code C of length r with $d(C) \geqslant 2$.

Proof. Let $T \in \mathcal{P}$. If $a, b \in T$ with $a \neq b$, then a and b are not comparable according to the definition of a join-meet partition, so their entries differ in at least two positions. ◇

Example. Each part of the join-meet partitions in Example 6.3.4.II and Example 6.3.4.III is a code with minimum distance 2, but it cannot correct errors. A join-meet partition of $N = \mathbb{F}_2^4$ is given by the parts $\{a, a + (1,1,1,1)\}$ for all $a \in \mathbb{F}_2^4$. Each part (for instance, the part $\{(0,0,0,0),(1,1,1,1)\}$) is a code with minimum distance 4, which can correct 1 error.

6.5.3 Optimising the Dimension of a Linear Code

There is another relation of join-meet partitions to codes which is completely different from the one just mentioned.

In Subsection 8.4.6, we will be interested in binary linear codes in $\mathbb{F}^n$ whose minimum distance does not fall below 3 and whose dimension is as large as possible. These codes help us to find join-meet partitions whose relative size is as large as possible.

A related problem is the following: Given n and k, one can ask for linear (n, k)-codes whose minimum distance is as large as possible. The following tables Table 6.1, Table 6.2 and Table 6.3 on pages 189 and 190 base on the tables on pages 742 and 743 in [Bet]. For some given lengths n and dimensions k, they show the maximal possible $d \in \mathbb{N}_0$ such that there exists a (n, k, d)-code. Values which are unknown are omitted. An implementation of the underlying algorithm from Anton Betten is available under `https://github.com/abetten/orbiter`.

For instance, following the tables, there exists a $(13, 9, 3)$-code. On the other hand, they do not show whether there exists a $(13, k', d')$-code with $k' \geqslant 10$ and $d' \geqslant 3$.

In what follows, we will briefly discuss linear codes to characterise those codes that solve the optimisation problem.

$n \setminus k$	1	2	3	4	5	6	7	8	9	10
4	4									
5	5	3								
6	6	4	3							
7	7	4	4	3						
8	8	5	4	4						
9	9	6	4	4	3					
10	10	6	5	4	4	3				
11	11	7	6	5	4	4	3			
12	12	8	6	6	4	4	4	3		
13	13	8	7	6	5	4	4	4	3	
14	14	9	8	7	6	5	4	4	4	3
15	15	10	8	8	7	6	5	4	4	4
16	16	10	8	8	8	6	6	5	4	4
17	17	11	9	8	8	7	6	6	5	4
18	18	12	10	8	8	8	7	6	6	
19		12	10	9	8	8	8	7	6	5
20			11	10	9	8	8	8	7	6
21				10	10			8	8	7
22					10	9			8	8
23						10	9			8
24							10			

Table 6.1: Optimal binary linear codes.

$n \setminus k$	11	12	13	14	15	16	17	18	19
15	3								
16	4								
17	4	3							
18	4	4	3						
19		4	4	3					
20	5			4	3				
21	6	5			4	3			
22	7	6	5			4	3		
23	8	7	6	5			4	3	
24	8	8		6				4	3
25		8							4

Table 6.2: Optimal binary linear codes (cont.).

$n \setminus k$	20	21	22	23	24	25	26
25	3						
26	4	3					
27		4	3				
28			4	3			
29				4	3		
30					4	3	
31						4	3
32							4

Table 6.3: Optimal binary linear codes (cont.).

6.5.4 Generator Matrices of Linear Codes

Let C be a linear (n, k)-code. We first show that it is not necessary to compare each codeword pair to find $d(C)$.

Proposition. Let $C \neq \{0\}$. The minimum distance of C is the minimum weight:

$$d(C) = \min(\mathrm{wt}(c)\colon c \in C \setminus \{0\}).$$

Proof. See [Bet, Corollary 1.2.8]: In the case where C has only one codeword (that is, $C = \{0\}$), $d(C)$ is defined by $0 = \mathrm{wt}(0)$. Now, let $\#C \geqslant 2$ and $v, w \in C$. According to linearity, $v - v = 0 \in C$ and $w - v =: z \in C$, that is, $d(v, w) = d(v - v, w - v) = d(0, z) = \mathrm{wt}(z)$. $\diamond$

A $k \times n$ matrix $\Gamma \in \mathcal{M}_{k,n}(\mathbb{F})$ whose rows contain a basis of C is called a *generator matrix* of C. Therefore, if we consider the vectors in $\mathbb{F}^n$ and in $\mathbb{F}^k$ as row vectors, we have $C = \{v \cdot \Gamma\colon v \in \mathbb{F}^k\}$.

Example. The minimum weight of the rows of a generator matrix of C give an upper bound on $d(C)$. This example from [Bet, E.1.3.8] shows that $d(C)$ can be smaller: An elementary computation shows that

$$\Gamma := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

is a generator matrix of the binary $(10, 3)$-code

$$C := \begin{array}{cccccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}$$

(each row corresponds to a codeword). The minimum distance of C is 4. Obviously, it does not equal the minimum weight of the rows of Γ (which is 5).

6.5.5 Decomposition of Linear Codes

Definition. Two linear codes $C, C' \subseteq \mathbb{F}^n$ are called *linearly isometric*, if there exists a linear isometry of $\mathbb{F}^n$, equipped with the Hamming metric, that maps C onto C'.

Definition. Let C_1 be a (n_1, k_1)-code and let C_2 be a (n_2, k_2)-code. The *(outer) direct sum* of C_1 and C_2 is defined as the $(n_1 + n_2, k_1 + k_2)$-code given by $C_1 \oplus C_2 := \{(c_1, c_2) \colon c_1 \in C_1, c_2 \in C_2\}$. A linear code is called *indecomposable* if it cannot be decomposed into a proper outer direct sum.

A generator matrix of $C_1 \oplus C_2$ is given by $\left(\begin{smallmatrix} \Gamma_1 & 0 \\ 0 & \Gamma_2 \end{smallmatrix}\right) \in \mathcal{M}_{k_1+k_2, n_1+n_2}(\mathbb{F})$, where Γ_1 and Γ_2 are generator matrices of C_1 and C_2, respectively. Now, it can be easily seen that the minimum distance of $C_1 \oplus C_2$ is given by $d(C_1 \oplus C_2) = \min(d(C_1), d(C_2))$.

Theorem. *(Decomposition Theorem of Linear Codes)*
A linear code C is linearly isometric to an outer direct sum of indecomposable codes $C_1, \ldots, C_s$. The decomposition is unique in the following sense: If C is the direct sum of indecomposable codes $C'_1, \ldots, C'_{s'}$, then $s = s'$ and there exists a permutation σ in the symmetric group S_s such that C_t and $C'_{\sigma(t)}$ are linearly isometric, for all $t \in \{1, \ldots, s\}$.

Proof. See [Bet, Theorem 6.2.7]. ◇

Theorem. Let C be an (n, k)-code with $k < n$ and with minimum distance d. There exists an indecomposable (n, k)-code C' such that $d(C') \geqslant d$.

Proof. See [Bet, Theorem 6.2.16]. ◇

Thus, given n and k, there exists an indecomposable code amongst all (n, k)-codes which maximise the minimum distance, so that the optimisation problem from Subsection 6.5.3 reduces to its solution for indecomposable codes.

Example. Here we give an example of an indecomposable linear code. The minimum distance of the binary $(4,3)$-code

$$C := \begin{matrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{matrix}$$

is 2. With [Bet, Test on Indecomposability 6.2.13] and the generator matrix

$$\Gamma := \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

of C, one can verify that C is indecomposable.

Chapter 7

DESIGN HYPERPLANES

In this chapter, we introduce a class of affine hyperplanes in the real tensor product $V := \mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$ for $n \in \{2, 4, 8\}$ which we call *design hyperplanes*. The main result of this chapter is Theorem 7.3.4. It says that a design hyperplane is a witness for the projective unit ball which touches the projective unit sphere at a scaled maximal vector. This gives an explicit formula for the inner radius of the projective unit ball in V and solves the projective norm maximisation. It gives also a class of maximal vectors.

Each design hyperplane is a sum of squares modulo the norm-join-meet ideal. In the sense of Theorem 6.3.6, it is based on a join-meet partition, called *design partition*, with a splitting function, the *design function*.

Both the design partition and the design function can be visualised by a cube which helps to determine them easily by hand for small dimensions of V.

The main areas which are involved in this chapter are latin squares, orthogonal designs and orthogonal arrays, see Section 7.1 and Section 7.2. In Section 7.3 we define the design partition as a join-meet partition which is based on a latin square of order n. The design function is based on an orthogonal design which comes from a latin square. For instance, this orthogonal design could be a multiplication table related to the complex numbers, the quaternions or the octonions.

Finally, the design hyperplanes give rise to a new class of affine hyperplanes in the tensor product $V' := \mathbb{R}^{n'} \otimes \cdots \otimes \mathbb{R}^{n'}$ for $n' \in \{3, 5, 6, 7\}$, the *skip hyperplanes*, which are introduced in Section 7.4. The main result is Theorem 7.4.2. It says that the skip hyperplanes are witnesses for the projective unit ball. This gives an upper bound on the inner radius which we call the *skip bound*, and a class of vectors in V' with projective norm 1.

In contrast to the number of tensor factors of V or V', which is arbitrary, the dimension of a tensor factor does not exceed 8. In Chapter 8 we introduce another class of witness hyperplanes for arbitrary values of n. However, in general, they are farer from zero than the design hyperplanes.

7.1 Latin Squares

This section begins with a brief introduction to latin squares and its relation to finite quasigroups due to [KD]. It focuses also on the concepts of isotopy, parastrophy and paratopy from [KD], which define different equivalence relations on the set of all latin squares.

Afterwards, we proceed with our *Rectangle Rule* for latin squares and with a word problem.

7.1.1 Quasigroups

Definition. A non-empty set S with a binary operation $\cdot$ is called a *quasigroup*, if for all $a, b \in S$, the equations $a \cdot x = b$ and $y \cdot a = b$ each have exactly one solution $x \in S$, $y \in S$. A quasigroup has an *identity* (or *neutral*) *element*, if there exists $1 \in S$ with $1 \cdot s = s \cdot 1 = s$.

If a quasigroup has an identity element, then the left and right inverses exist. However, a quasigroup has to be neither associative nor commutative. It is elementary to show that every associative quasigroup is a group, compare [KD, Problem 1.1].

A non-empty set S with a binary operation $\cdot$ is a quasigroup if and only if for all $a \in S$, the left-multiplication $S \to S$, $x \mapsto a \cdot x$ and the right-multiplication $S \to S$, $x \mapsto x \cdot a$ by a are bijective.

A finite quasigroup can be described by a so-called multiplication table, as it is common for groups. Formally, a *multiplication table* (B_1, B_2, M) of a finite quasigroup $(S, \cdot)$ consists of two lists B_1, B_2 of length $n := \#S$, where the entries of each list cover the elements in S, called *boundaries*, and an $n \times n$ matrix M with entries in S, where for all $i, j \in \{1, \ldots, n\}$, we have $M(i, j) := B_1(i) \cdot B_2(j)$. We refer to M as a *multiplication table* of $(S, \cdot)$ *without boundaries*. The multiplication table can be written in the following form:

$$\begin{array}{c|c} \cdot & B_2 \\ \hline B_1 & M \end{array} \quad = \quad \begin{array}{c|ccc} \cdot & \cdots & B_2(j) & \cdots \\ \hline \vdots & & \vdots & \\ B_1(i) & \cdots & B_1(i) \cdot B_2(j) & \cdots \\ \vdots & & \vdots & \end{array}$$

7.1.2 Latin Squares

Definition. A *latin square of order* $n \in \mathbb{N}$ is an $n \times n$ matrix with entries in a finite set S with n elements, in which the entries of each row and each column cover all *symbols*, that is, the elements in S. A *latin subsquare* of a latin square L is a quadratic submatrix of L which is again a latin square.

The following statement is adopted from [KD, Theorem 1.1.1].

Theorem. There is a one-to-one correspondence between multiplication tables without boundaries and latin squares.

Proof. Let (B_1, B_2, M) be a multiplication table of a finite quasigroup $(S, \cdot)$, where $n := \#S$. Let $i, j \in \{1, \dots, n\}$. The entries of the i^{th} row of M cover the image of the left-multiplication by $B_1(i)$ (which is bijective). Also, the entries of the j^{th} column of M cover the image of the right-multiplication by $B_2(j)$ (which is bijective). Hence, M is a latin square.

On the other hand, a latin square can be complemented with two arbitrary boundaries to a multiplication table of a finite quasigroup, since the structure of a latin square guarantees that for all $a \in S$, the left- and the right-multiplication by a are bijective. ◇

Definition. A latin square L with the symbols $1, \dots, n$ is said to be in *standard form* if the first row and the first column of L equals $(1, \dots, n)$.

Example. Let $n \in \mathbb{N}$. The set $\mathbb{Z}_n$, equipped with a binary operation $\star$, defined by $a \star b := ha + kb + l$ for all $a, b \in \mathbb{Z}_n$, where each h and k have no common prime factor with n and where $l \in \mathbb{Z}$, is a finite quasigroup. In this example, we discuss some special cases.

(i) If $h = k = 1$ and $l = 0$, then $(\mathbb{Z}_n, \star)$ equals $(\mathbb{Z}_n, +)$.

(ii) A multiplication table for the case where $n = 3$, $h = 2$, and $k = l = 1$ is given by:

$\star$	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

(iii) A simple way to construct latin squares of order n is to write the numbers $1, \ldots, n$ in the first row and to construct the next row by shifting the entries from the preceding row one position to the right (the entry which sticks out is placed on the left). This can be reached by setting $h = n - 1$, $k = 1$, and $l = 0$. For instance, we obtain the latin square

$$\begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}$$

Shifting to the left gives the multiplication table of $(\mathbb{Z}_n, +)$ with boundaries $(1, \ldots, n)$, see also (i).

7.1.3 Isotopy

Definition. Two quasigroups $(G, \cdot)$ and $(H, \star)$ are called *isotopic*, if there exist bijective functions θ, ϕ, ψ from G onto H such that for all $x, y \in G$, we have

$$\psi(x \cdot y) = \theta(x) \star \phi(y).$$

In this case, the triple (θ, ϕ, ψ) is called an *isotopism* from $(G, \cdot)$ onto $(H, \star)$. If $G = H$ and $\psi = \mathrm{id}$, $(H, \star)$ is said to be a *principal isotope* of $(G, \cdot)$. If $\theta = \phi = \psi$, $(H, \star)$ is said to be *isomorphic* to $(G, \cdot)$.

Let $(G, \cdot)$ be a finite quasigroup with multiplication table (B_1, B_2, L) and let (θ, ϕ, ψ) be an isotopism from $(G, \cdot)$ onto $(H, \star)$. Naturally, ψ gives rise to a latin square $\psi(L)$, emerging from L by applying ψ entry-wise, with symbols H. Applying θ (and ϕ) entry-wise to the boundaries B_1 and B_2, respectively, leads to boundaries $\theta(B_1)$, $\phi(B_2)$ of a multiplication table of $(H, \star)$:

$$\begin{array}{c|c} \star & \phi(B_2) \\ \hline \theta(B_1) & \psi(L) \end{array}$$

Hence, if $G = H$, then θ and ϕ permute the boundaries B_1 and B_2, respectively, and ψ permutes the symbols of L.

Clearly, the multiplication tables without boundary of a finite quasigroup are pairwise isotopic. Hence, modulo isotopy, a quasigroup can be represented by a single latin square.

The following statement is adopted from [KD, Theorem 1.3.3].

Proposition. Among the principal isotopes of a quasigroup, there always exists a quasigroup with identity element.

Proof. Let $(S, \cdot)$ be a quasigroup and let $a, b \in S$. Let θ and ϕ be the right-multiplication by b and the left-multiplication by a, that is, $\theta(x) = x \cdot b$ and $\phi(x) = a \cdot x$ for all $x \in S$. A principal isotope $(S, \star)$ of $(S, \cdot)$ is defined by the multiplication $x \star y := \theta^{-1}(x) \cdot \phi^{-1}(y)$ for all $x, y \in S$. Letting $e := a \cdot b$, for all $y \in S$, we obtain

$$\begin{aligned} y \star e &= \theta^{-1}(y) \cdot \phi^{-1}(e) = x \cdot b = y, \\ e \star y &= \theta^{-1}(e) \cdot \phi^{-1}(y) = a \cdot x' = y, \end{aligned}$$

where $x := \theta^{-1}(y)$ and $x' := \phi^{-1}(y)$ are the unique solutions of the equations $x \cdot b = y$ and $a \cdot x' = y$. It follows that e is an identity element for $(S, \star)$. ◇

Definition. Two latin squares are called *isotopic*, if they can be obtained from the multiplication tables of two quasigroups which are isotopic. If the two quasigroups are also isomorphic, then also the latin squares are called *isomorphic*.

Hence, two latin squares are isotopic, if and only if they can be obtained from each other by permutations of the rows and of the columns and by a replacement of the symbols.

Let $\mathcal{L}$ be the set of all latin squares which are a multiplication table without boundaries of a given finite quasigroup. Let $L \in \mathcal{L}$. The set $\mathcal{L}$ consists exactly of the latin squares which can be obtained from L by permutations of the rows and of the columns. In this respect, the concept of isotopy clusters latin squares which can be regarded as "representatives" of the "same" algebraic structure.

Example. Each latin square is isotopic to a latin square in standard form.

7.1.4 Parastrophy and Paratopy

The usual representation of a latin square as a matrix disguises the symmetry of the rows, columns and the symbols. For this reason, it can be advantageous to consider another representation of a latin square L, given by

$$\mathrm{Tri}(L) := \{(i, j, L(i, j)) \colon i, j \in \{1, \ldots, n\}\}.$$

Let A be an arbitrary non-empty set. Each permutation σ in the symmetric group S_3 gives rise to a function

$$\sigma\colon\ A^3 \to A^3,\ (c_1, c_2, c_3) \mapsto (c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, c_{\sigma^{-1}(3)}).$$

If L has the symbols $1, \dots, n$ (which can also be regarded as representatives of the elements in $\mathbb{Z}_n$), then $\mathrm{Tri}(L)$ is a subset of $\{1, \dots, n\}^3$. The image of $\mathrm{Tri}(L)$ under σ gives another latin square L_σ. See also [KD, page 15].

Now, we come to a notion which will be useful in the next section.

Definition. Let L be a latin square with symbols S and let ψ be a bijective function from S to $\{1, \dots, \#S\}$. The latin square $L_{\sigma,\psi} := \psi^{-1}(\psi(L)_\sigma)$ is called the (σ, ψ) *parastrophe* of L.

Clearly, if $S = \{1, \dots, n\}$ and $\psi = \mathrm{id}$, then we obtain $L_{\sigma,\psi} = L_\sigma$.

Definition. Two latin squares are called *paratopic*, if they can be obtained from each other by isotopy and parastrophy. The equivalence classes according to paratopy are called *main classes*.

Example.

(i) The following two isotopic latin squares L

$$L := \begin{matrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{matrix} \quad \text{and} \quad L' := \begin{matrix} 3 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix}$$

are also parastrophes of each other, since

$$\begin{aligned} \mathrm{Tri}(L) = \{ &(1,1,2), (1,2,3), (1,3,1), \\ &(2,1,1), (2,2,2), (2,3,3), \\ &(3,1,3), (3,2,1), (3,3,2) \} \end{aligned}$$

and $L' = L_{(23)}$.

(ii) Let L be defined according to (i). For all $\sigma \in S_3$, the upper left entry of the (σ, id) parastrophe of L is different from 1. Hence, it is not in standard form. However, choosing $\psi\colon 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$ and $\sigma := (2\,3)$, the (σ, ψ) parastrophe L' of L, given by

$$L' = \begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{matrix},$$

is in standard form.

(iii) Representatives of the two main classes of latin squares of order 4 are given by

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{array}, \qquad \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array}.$$

There are 283657 main classes of latin squares of order 8. For details, see [KD, Section 4.2].

(iv) The smallest order such that there exist latin squares which are paratopic, but not isotopic, is 6, see [KD, page 134]. For example, no two of the parastrophes of the following latin square are isotopic:

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \\ 3 & 5 & 1 & 6 & 4 & 2 \\ 4 & 6 & 5 & 2 & 3 & 1 \\ 5 & 3 & 6 & 1 & 2 & 4 \\ 6 & 4 & 2 & 5 & 1 & 3 \end{array}$$

Definition. Two finite quasigroups are called *paratopic*, if each two of their multiplication tables without boundary are paratopic.

Example. Let $(G, \cdot)$ be a finite quasigroup and let $(G, \star)$ be defined by $a \star b := b \cdot a$ for all $a, b \in G$. Then $(G, \cdot)$ and $(G, \star)$ are paratopic.

7.1.5 A Rectangle Rule for Latin Squares

So far we have introduced some standard terms on latin squares. Until the end of the section, we follow up with some observations which we have not found yet in the literature, but which fit our particular situation.

The following theorem illustrates the structure of the multiplication tables of a direct sum of copies of $\mathbb{Z}_2$.

Theorem. Let L be a latin square with the symbols $1, \ldots, n$. The following are equivalent:

(a) There exists $t \in \mathbb{N}_0$ such that $n = 2^t$ and L is a multiplication table without boundaries for a group isomorphic to $(\mathbb{Z}_2)^t$.

(b) (*Rectangle Rule, for columns*)
For all $i, j, k \in \{1, \dots, n\}$, $i \neq j$, there exists $l \in \{1, \dots, n\}$ with

$$L(i,k) = L(j,l) \text{ and } L(j,k) = L(i,l).$$

(c) (*Rectangle Rule, for rows*)
For all $i, k, l \in \{1, \dots, n\}$, $k \neq l$, there exists $j \in \{1, \dots, n\}$ with

$$L(i,k) = L(j,l) \text{ and } L(j,k) = L(i,l).$$

(d) Each two entries of L that are in the same row (or in the same column) can be expanded to a latin subsquare of L of order 1 or 2.

(e) Let σ_k be the permutation in S_n which maps the first column of L to the k^{th} column, for all $k \in \{1, \dots, n\}$. Then $P := \{\sigma_1, \dots, \sigma_n\}$ is a permutation group and each element (except the identity) is self-inverse.

Proof. At first, we show (a) ⇒ (b): Let $G := \{1, \dots, 2^t\}$ and let $\cdot$ be a binary relation on G such that $(G, \cdot)$ is a group which is isomorphic to $(\mathbb{Z}_2)^t$. Let L be the latin square which comes from the multiplication table of G with the boundaries $(1, \dots, n)$. Let $i, j, k \in G$. Since G is commutative and each element is self-inverse, letting $l := k \cdot i \cdot j$, we obtain

$$L(i,k) = i \cdot k = j \cdot l = L(j,l) \text{ and}$$
$$L(j,k) = j \cdot k = i \cdot l = L(i,l).$$

This proves the assertion.

Now, we show (b) ⇒ (a): We first note that (d) also holds for each latin square which can be obtained from L by a permutation of the rows and by a permutation of the columns. Hence, we can rearrange the rows and the columns of L to obtain a latin square L' which is in standard form, that is, the first row and the first column equals $B := (1, \dots, n)$. Thus, the quasigroup $(G, \cdot)$ with multiplication table (B, B, L') admits the identity element 1. We note that (b) holds if and only if for all $i, j, k \in G$, there exists a unique $l \in G$ with $i \cdot k = j \cdot l$ and $j \cdot k = i \cdot l$, since the equation $i \cdot k = j \cdot l$ has exactly one solution $l \in G$. With other words, for all $i, j, k \in G$, $i \cdot k = j \cdot l$ implies $j \cdot k = i \cdot l$.

Statement 1: G is commutative and each element is self-inverse.

Let $i, j \in G$. From $1 \cdot i = i \cdot 1$, we obtain $i \cdot i = 1 \cdot 1 = 1$, that is, i is self-inverse:

$\cdot$	1	i
1	1	i
i	i	1

Moreover, $1 = i \cdot i = j \cdot j$ yields $j \cdot i = i \cdot j$, that is, G is commutative:

$\cdot$	i	j
i	1	$i \cdot j$
j	$j \cdot i$	1

Statement 2: G is associative.
There exists $l \in G$ with $i = i \cdot 1 = j \cdot l$ and $j = j \cdot 1 = i \cdot l$:

$\cdot$	1	l	j
1	1	l	j
i	i	j	$i \cdot j$
j	j	i	1

From the latter equation $1 \cdot j = i \cdot l$, it follows that $i \cdot j = 1 \cdot l = l$. This leads to $j = i \cdot (i \cdot j)$ (that is, *Sade's left "keys" law* holds. See [KD, Chapter 2] for details. *Sade's right "keys" law* also holds since G is commutative).

For all $k \in G$, we have $j = i \cdot (i \cdot j) = k \cdot (k \cdot j)$. From (b), it follows that $k \cdot (i \cdot j) = i \cdot (k \cdot j)$. Since G is commutative, we conclude that $k \cdot (j \cdot i) = (k \cdot j) \cdot i$, that is, G is associative.

Statement 3: G is a group.
This statement follows from the associativity.

Statement 4: G is isomorphic to a direct sum of copies of $\mathbb{Z}_2$.
It is well-known that a group, in which each element (except the identity) has order 2, is isomorphic to a direct sum of copies of $\mathbb{Z}_2$.

Now, we show (e) $\Rightarrow$ (a): Without loss of generality, we may assume that L belongs to a multiplication table without boundaries for a quasigroup $(G, \cdot)$ with identity element 1. Theorem 1.2.2 in [KD] states that L is group-based if and only if P is group-based. Hence, G is a group. We have $\sigma_k(i) = L(i, k) = i \cdot k$.

Statement 1: Each element in G is self-inverse.
Let $i \in G$ and let $k \in G$ such that $i \cdot k = 1$. Since σ_k is self-inverse, we obtain $1 \cdot k = i$. It follows that $k = i$ and hence, $i \cdot i = 1$. Thus, each element is self-inverse.

Statement 2: Statement (a) holds.
A group, in which each element (except the identity) has order 2, is isomorphic to a direct sum of copies of $\mathbb{Z}_2$.

Now, we show (a) $\Rightarrow$ (e): This implication follows immediately from Theorem 1.2.2 in [KD], which states that P is isomorphic to a direct sum of copies of $\mathbb{Z}_2$.

Finally, we easily see that (a) is also equivalent to (c) and (d). ◇

7.1.6 The Word Problem

Let $(S, \cdot)$ be a finite quasigroup and let $r \in \mathbb{N}$. We recall that S^r can be considered as the set of all words of length r with the alphabet S. Let

$$\begin{aligned} \mathrm{prod}_{(S,\cdot)} \;:\; & S^r \to S \\ (a_1, \dots, a_r) & \mapsto (\cdots((a_1 \cdot a_2) \cdot a_3) \cdots) \cdot a_r \,. \end{aligned}$$

We refer to $\mathrm{prod}_{(S,\cdot)}(a)$ as the *product* of $a = (a_1, \dots, a_r)$.

Let $r \geqslant 2$. For given $s \in S$, we may ask for those words of length r whose product equals s, that is, we may ask for the pre-image of s under $\mathrm{prod}_{(S,\cdot)}$. Alternatively, we may ask for the product of $a \in S^r$. We refer to the first question as the *word problem* for s, and to the second question as the *word problem* for a.

Clearly, the word problem can be solved easily in some cases: For example, if $(S, \cdot)$ is a group, then the solutions of the word problem for s have the form $(a, \mathrm{prod}_{(S,\cdot)}(a)^{-1} \cdot s)$, where $a \in S^{r-1}$.

For each $s \in S$, let

$$T_{s,r} := \{a \in S^r \colon\ \mathrm{prod}_{(S,\cdot)}(a) = s\} \ \subseteq S^r$$

denote the set of all solutions of the word problem for s.

Proposition. The sets $T_{s,r}$, $s \in S$, have the same length $\#S^{r-1}$. They are the parts of a partition $\mathcal{P}_r$ of S^r. The partition is symmetric, if S is an abelian group.

Proof. We use induction on r. Clearly, the statement holds for $r = 1$. Now, let $r \geqslant 2$. Let $a_1, \dots, a_{r-1} \in S$. For all $s \in S$, a solution $x \in S$ of the equation $a_1 \cdot \ldots \cdot a_{r-1} \cdot x = s$ exists and is uniquely defined, that is, the elements $(a_1, \dots, a_{r-1}, x)$, $x \in S$, lie in $\#S$ different sets.

Let $a \in S^r$ and let $\pi \in S_r$. If S is associative and commutative, then the products of a and $\pi.a$ coincide. This implies that $\mathcal{P}_r$ is symmetric. $\diamond$

Proposition. If $r \geqslant 2$, $s \in S$ and $a, b \in T_{s,r}$ with $a \neq b$, then the letters of the words a and b differ in at least two positions.

Proof. According to the proof of the previous proposition, this statement holds since the left- and the right-multiplication by elements of S is bijective. $\diamond$

7.1.7 Orthogonal Arrays

Let $r \geqslant 2$. The set $T_{s,r}$ can be represented by a matrix by writing its elements in rows (or in columns). This matrix has $\#S^{r-1}$ rows and r columns. Its rows cover all solutions of the word problem for s.

Example. Let $S = \mathbb{Z}_3$. The set $T_{0,3}$ (which covers all words whose letters sum up to 0) can be represented by the following matrix:

$$\begin{matrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 0 & 2 \\ 1 & 1 & 1 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \\ 2 & 1 & 0 \\ 2 & 2 & 2 \end{matrix}$$

We will see shortly that the matrix above is an example for a so-called orthogonal array. For details on orthogonal arrays, see [HSS].

Definition. Let $m, k, s, d, \lambda \in \mathbb{N}$. An $m \times k$ matrix A with entries in $\{1, \dots, s\}$ is called an *orthogonal array* with m *runs*, k *factors*, s *levels*, *strength* d and *index* λ, denoted $\mathrm{OA}(m, k, s, d)$, if for each $m \times d$ submatrix of A, the rows cover all words in $\{1, \dots, s\}^d$, and each word appears exactly λ times.

Now, we encounter an easy method to obtain examples for orthogonal arrays (which we have not found in the literature yet).

Proposition. Let $(S, \cdot)$ be a finite abelian group and let $s \in S$. Let A be a matrix which represents $T_{s,r}$ (that is, the rows of A cover the words in S^r with product s). Then A is an $\mathrm{OA}(m, r, \#S, r-1)$ with index 1.

Proof. *Step 1*: Let A_0 be the submatrix of A which comes from omitting the last column. By construction of $T_{s,r}$, the rows of A_0 cover all words in S^{r-1}, and each word appears exactly once.

Step 2: Now, let $\sigma \in S_r$ be a permutation and let B be the matrix which comes from permuting the columns of A by σ. Since $(S, \cdot)$ is associative and commutative, the image of each row is again a word in S^r which multiplies up to s. It follows that the rows of A equal the rows of B. Now, let B_0 be the submatrix of B which comes from omitting the last column. By step 1, the rows of B_0 cover all words in S^{r-1}, and each word appears exactly once. Hence, for each $r-1$ columns of A, the rows of the corresponding submatrix cover all words in S^{r-1}. ◇

Example. The last example gives an $\mathrm{OA}(9, 3, 3, 2)$.

7.1.8 Visualisation of the Word Problem

Now, we present a visualisation of the word problem for a quasigroup $(G, \cdot)$ which is isomorphic to $((\mathbb{Z}_2)^t, +)$ for $t \in \mathbb{N}$. Let $n := 2^t$. Without loss of generality, let $1, \ldots, n$ be the symbols of $(G, \cdot)$ and let 1 be the identity element. Let L be the latin square which comes from the multiplication table of $(G, \cdot)$ with the boundaries $(1, \ldots, n)$.

Proposition. For any $a, b \in G$, the product $a \cdot b$ can be obtained from L as follows:

$$L = \begin{array}{c:ccccc} 1 & 2 & \cdots & \boxed{a} & \cdots & 2^t \\ \hdashline 2 & & & & & \\ \vdots & & & \downarrow & & \\ \boxed{ab} & & \leftarrow & \boxed{b} & & \\ \vdots & & & & & \\ 2^t & & & & & \end{array}$$

Proof. We first state that the multiplication table has the following form:

$$\begin{array}{c|cccccc}
\cdot & 1 & 2 & \cdots & b & \cdots & 2^t \\
\hline
1 & 1 & 2 & \cdots & b & \cdots & 2^t \\
2 & 2 & & & & & \\
\vdots & \vdots & & & \vdots & & \\
a & a & & \cdots & a \cdot b & & \\
\vdots & \vdots & & & & & \\
2^t & 2^t & & & & &
\end{array}$$

If we look at this table, we see that the first column and the first row of L are copies of the boundaries (actually, this is because the boundary starts with the identity element). Hence, to obtain the product $a \cdot b$ for any $a, b \in G$, it suffices to look at L, since the boundaries do not provide any new information.

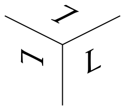
In a second step, we state that it is also possible to find the product $a \cdot b$ in the first column. To see this, let L_0 be the latin square coming from a multiplication table of $(G, \cdot)$ and let $\hat{L_0}$ be the parastrophe of L_0 which comes from rotating the third to the first position, that is, $\text{Tri}(\hat{L_0}) = \text{Tri}((L_0)_{(123)}) = \{(ab, a, b) \colon a, b \in G\}$. Since $(G, \cdot)$ is commutative and each element in G is self-inverse, we obtain $\hat{L_0} = L_0$. It follows that any multiplication table of $(G, \cdot)$ (on the left of the equality sign) equals the scheme on the right:

$$\begin{array}{c|c} \cdot & b \\ \hline a & ab \end{array} = \begin{array}{c|c} \cdot & a \\ \hline ab & b \end{array}.$$

◇

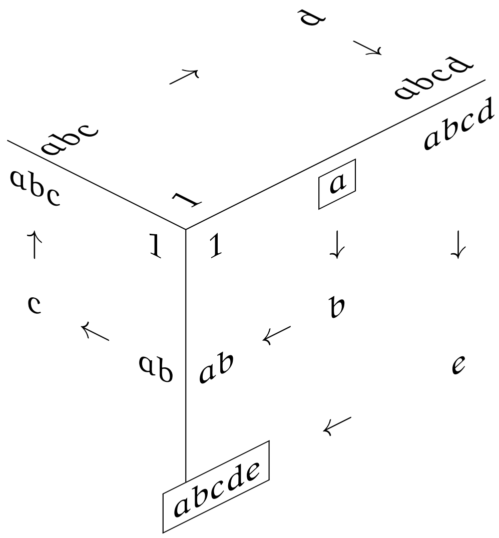
With this identification of the product of a and b, the elements in the first column of L have a "double role", since they can serve as both factor and product.

Now, we write three copies of L in the following triple scheme:



The scheme consists of $3 \cdot n^2$ *cells* with entries in $\{1, \ldots, n\}$.

Doing this, the product of, say, 5 elements $a, b, c, d, e \in G$ can be obtained in the following way:



Let $r \geqslant 2$ and let $a_1, \ldots, a_r \in G$. In general, a *spiral with* $r-1$ *turns through* $a_1, \ldots, a_r$ can be constructed with the following algorithm:

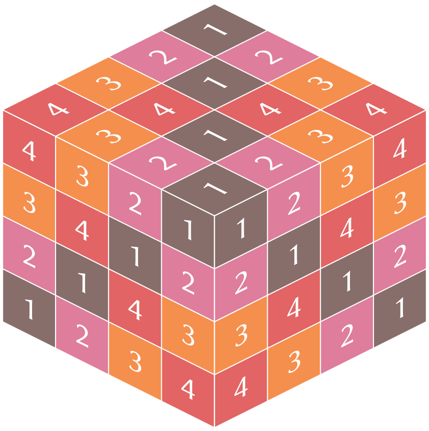
0. The spiral begins in the first row of the right cube in the cell with the entry a_1.

   Now, let $k := 2$. The current cube is the right cube.
1. Connect $a_1 \cdot \ldots \cdot a_{k-1}$ in the first row of the current cube with a_k in the same column. The cell containing a_k is called a *corner* of the spiral.
2. Connect this corner with the cell with the entry $(a_1 \cdot \ldots \cdot a_{k-1}) \cdot a_k$ in the same row. This cell can be found in the very left column.
3. If $k < r$, connect this cell with the neighbouring cell in the first row of the next cube (counter clockwise). The entries of both cells coincide. Let $k \rightsquigarrow k+1$, and continue with 1.

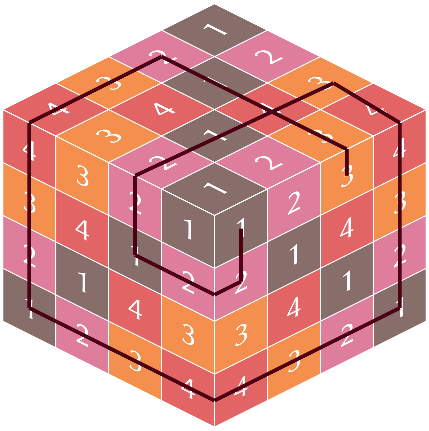
   If $k = r$, then the entry of the current cell equals the product $s := a_1 \cdot \ldots \cdot a_r$, that is, the spiral *ends in* s.

Hence, for given $s \in S$, the word problem can be visualised by those spirals which have $r-1$ turns and end in s. For given $a \in S^r$, the word problem can be visualised by the spiral with $r-1$ turns which is given by a.

Example. A triple scheme for $(\mathbb{Z}_2)^2$, the Klein four-group, looks like the following cube:



By way of example, we have $(1, 2, 1, 3, 1, 1, 2) \in T_{3,7}$, which can be visualised by the corresponding spiral with 6 turns ending in 3:



In the next section we extend this visualisation in a more general context.

7.2 Orthogonal Designs

This section begins with a brief introduction to orthogonal designs based on [Seb]. Orthogonal designs will play a major role in our definition of the design function in the next section. The main idea is to "amplify" each entry of a latin square by a positive or negative sign.

We continue with our *Rectangle Rule* for orthogonal designs and with a word problem.

7.2.1 Orthogonal Designs

Let $n, m \in \mathbb{N}$. Let $x_1, \dots, x_m$ be independent and commuting variables (that is, they generate the polynomial ring $\mathbb{Z}[x_1, \dots, x_m]$ which, more generally, lies in the field of fractions of $\mathbb{Z}[x_1, \dots, x_m]$). Let X be an $n \times n$ matrix whose entries $X_{\alpha,\beta}$, where $\alpha, \beta \in \{1, \dots, n\}$, lie in the set $\{0, \pm x_1, \dots, \pm x_m\}$.

The rows of X are called an *orthogonal system* if and only if for all $\alpha, \beta \in \{1, \dots, n\}$, $\alpha \neq \beta$, we have $\sum_{\gamma=1}^{n} X_{\alpha,\gamma} \cdot X_{\beta,\gamma} = 0$. The columns of X are called an *orthogonal system* if and only if the rows of X^t are an orthogonal system.

Proposition. The following are equivalent:

(a) There exists $s_1, \dots, s_m \in \mathbb{N}$ such that

$$X \cdot X^t = \left(\sum_{k=1}^{m} s_k \, x_k^2 \right) \mathbb{1}_n.$$

(b) There exists $s_1, \dots, s_m \in \mathbb{N}$ such that each row and each column of X has s_k entries $\pm x_k$, $k \in \{1, \dots, m\}$, and both rows and columns are an orthogonal system.

Proof. Clearly, we have

$$X \cdot X^t = \left(\sum_{\gamma=1}^{n} X_{\alpha,\gamma} \cdot X_{\beta,\gamma} \right)_{\alpha,\beta=1}^{n}.$$

We first show (a) ⇒ (b). The rows of X are an orthogonal system. If X does not equal zero, then X is an invertible matrix (with respect to the field of fractions of $\mathbb{Z}[x_1, \dots, x_m]$), and we obtain $X \cdot X^t = X^t \cdot X$, that is, also the columns of X are an orthogonal system. The second implication (b) ⇒ (a) follows immediately. ◇

Definition. In the case of the last proposition, X is called an *orthogonal design* of *order* n and *type* $(s_1, \dots, s_m)$ with the *symbols* $x_1, \dots, x_m$, denoted $\mathrm{OD}(n; s_1, \dots, s_m)$. An orthogonal design with no zero entry is called a *full* orthogonal design.

If X is an orthogonal design, then one can obtain a multiple of an orthogonal $n \times n$ matrix from X by evaluating each variable

x_k at a given point $y_k \in \mathbb{R}$, for all $k \in \{1, \dots, n\}$. If X is a full orthogonal design, then the matrix which can be obtained with $y_1 = \cdots = y_m = 1$ is called a *Hadamard matrix*.

7.2.2 The Existence of Orthogonal Designs

Let $n \in \mathbb{N}$. There exist uniquely defined numbers $a \in \mathbb{N}_0$ and $b \in \mathbb{N}$ odd such that $n = 2^a b$. Furthermore, there exist uniquely defined numbers $c \in \mathbb{N}_0$ and $0 \leqslant d < 4$ such that $a = 4c + d$. Let $\rho(n) := 8c + 2^d$.

From [Seb, Theorem 1.3], we obtain the following useful restriction to the number of variables in an orthogonal design:

Theorem. (i) Any orthogonal design of order n can involve at most $\rho(n)$ symbols.
(ii) There exists an orthogonal design of order n involving $\rho(n)$ symbols.

For our particular situation we are interested in full orthogonal designs of type $(1, \dots, 1)$, that is, each symbol appears exactly once in a row.

Corollary. A full orthogonal design of type $(1, \dots, 1)$ has order $n \in \{1, 2, 4, 8\}$.

Proof. Let X be a full orthogonal design of type $(1, \dots, 1)$ and of order $n \in \mathbb{N}$. If X is full, then $n = \rho(n)$. Moreover, we have

$$n = 2^a b = 16^c 2^d b \geqslant 8c + 2^d = \rho(n).$$

Equality holds only for $b = 1$ and $c = 0$. Thus, we obtain $n = 2^d$, where $d \in \{0, 1, 2, 3\}$. ◇

Example. Here, we give examples for full orthogonal designs of type $(1, \dots, 1)$ and of order $2, 4$ and 8. The symbols $x_1, \dots, x_8$ are replaced by the symbols $A, B, \dots, H$.

(i) From [Wal], we obtain the following orthogonal designs. They are "skew symmetric" with respect to the upper right and the lower left triangle:

$$\begin{pmatrix} A & B \\ -B & A \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F & G & H \\ -B & A & D & -C & F & -E & -H & G \\ -C & -D & A & B & G & H & -E & -F \\ -D & C & -B & A & H & -G & F & -E \\ -E & -F & -G & -H & A & B & C & D \\ -F & E & -H & G & -B & A & -D & C \\ -G & H & E & -F & -C & D & A & -B \\ -H & -G & F & E & -D & -C & B & A \end{pmatrix}.$$

(ii) Examples for full orthogonal designs of type $(1, \ldots, 1)$ can also be obtained from the multiplication tables for the basis vectors of a canonical expansion of the reals to the complex numbers, quaternions and octonions:

$$\begin{pmatrix} A & B \\ B & -A \end{pmatrix}, \quad \begin{pmatrix} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F & G & H \\ B & -A & D & -C & F & -E & H & -G \\ C & -D & -A & B & G & -H & -E & F \\ D & C & -B & -A & -H & -G & F & E \\ E & -F & -G & H & -A & B & C & -D \\ F & E & H & G & -B & -A & -D & -C \\ G & -H & E & -F & -C & D & -A & B \\ H & G & -F & -E & D & C & -B & -A \end{pmatrix}$$

The tables can be constructed by means of the *Cayley-Dickson construction*; see, for example, [Bal]. The next step of this construction leads to a multiplication table for the sedenions, which does not belong to an orthogonal design. Therefore, for higher orders, it does not lead to orthogonal designs (in fact, according to Corollary 7.2.2, this is impossible).

Remark. We will see below that it is a "disadvantage" for our applications that full orthogonal designs of type $(1, \ldots, 1)$ exist only up to order 8.

In the literature, attention was drawn to them to obtain Hadamard matrices. In this respect, a common alternative are *Baumert-Hall arrays*, which are full orthogonal designs of order $4t$, $t \in \mathbb{N}$, with four variables and type (t, t, t, t); see, for instance, [Wal]. Unfortunately, this and other related alternatives do not seem to fit our problem.

7.2.3 A Rectangle Rule for Full Orthogonal Designs

Let $A = (A_{k,l})_{k,l=1}^{n}, B = (B_{k,l})_{k,l=1}^{n} \in \mathcal{M}_{n,n}(\mathbb{K})$ be two $n \times n$ matrices. As usual, the *entry-wise product* of A and B is defined by the $n \times n$ matrix $A \star B := (A_{k,l}B_{k,l})_{k,l=1}^{n}$.

So far we have introduced some standard terms on orthogonal designs. Until the end of this section, we follow up with some observations which we have not found yet in the literature, but which fit our particular situation.

Proposition. Every full orthogonal design X of type $(1, \dots, 1)$ can be written uniquely as the entry-wise product of a latin square $|X|$ with the same symbols, the *absolute value* of X, and a Hadamard matrix.

Proof. Let X be a full orthogonal design. Let H be the Hadamard matrix which comes from evaluating the entries of X at 1. If X has type $(1, \dots, 1)$, then each symbol appears exactly once in a row and exactly once in a column according to Proposition 7.2.1. It follows that the matrix $|X| := H \star X$ is a latin square of order n with the symbols x_1, $\dots$, x_n, and we obtain $H \star |X| = X$. ◇

Given a latin square, we may ask whether it is equal to the absolute value of a full orthogonal design of type $(1, \dots, 1)$.

Lemma. Let $X = (X_{\alpha,\beta})_{\alpha,\beta=1}^{n}$ be an $n \times n$ matrix with entries in $\{\pm x_1, \dots, \pm x_n\}$ such that each variable appears exactly once in a row (up to its sign). Then the following are equivalent:

(a) X is a full orthogonal design of type $(1, \dots, 1)$.

(b) (*Rectangle Rule, for columns*)
For all $\alpha, \beta \in \{1, \dots, n\}$, $\alpha \neq \beta$, and for all $\gamma \in \{1, \dots, n\}$, there exists a uniquely defined number $\delta \in \{1, \dots, n\}$ such that

$$X_{\alpha,\gamma} \cdot X_{\beta,\gamma} + X_{\alpha,\delta} \cdot X_{\beta,\delta} = 0.$$

(c) (*Rectangle Rule, for rows*)
For all $\gamma, \delta \in \{1, \dots, n\}$, $\gamma \neq \delta$, and for all $\alpha \in \{1, \dots, n\}$, there exists a uniquely defined number $\beta \in \{1, \dots, n\}$ such that

$$X_{\alpha,\gamma} \cdot X_{\beta,\gamma} + X_{\alpha,\delta} \cdot X_{\beta,\delta} = 0.$$

Proof. We first note that X is a full orthogonal design if and only if $X \cdot X^t = \sum_{k=1}^m x_k^2 \, \mathbb{1}_n$, that is, if and only if each two different rows are orthogonal. In this case, its type equals $(1, \dots, 1)$.

Now, we prove (a) ⇒ (b):
Let $\alpha, \beta, \gamma \in \{1, \dots, n\}$ with $\alpha \neq \beta$. The entry of $X \cdot X^t$ in position (α, β) equals

$$(X \cdot X^t)_{\alpha,\beta} = \sum_{k=1}^{n} X_{\alpha,k} X_{\beta,k} = 0. \tag{7.1}$$

Hence, since the entries of each row cover all variables, there exists $\delta \in \{1, \dots, n\}$, uniquely defined, such that $X_{\alpha,\gamma}$ and $X_{\beta,\delta}$ involve the same variable. Thus, according to equation (7.1) and by comparison of coefficients, we obtain

$$X_{\alpha,\gamma} \cdot X_{\beta,\gamma} + X_{\alpha,\delta} \cdot X_{\beta,\delta} = 0.$$

Now, we prove (b) ⇒ (a):
Let $\alpha, \beta, \gamma \in \{1, \dots, n\}$ with $\alpha \neq \beta$. The requirement in (b) gives rise to a bijective function π on $\{1, \dots, n\}$ with $\pi(\gamma) = \delta$. Since also $\pi(\delta) = \gamma$, the sets $\{k, \pi(k)\}$, $k \in \{1, \dots, n\}$, are a partition of the set $\{1, \dots, n\}$ (by the way, in particular, this implies that n is even). Let R be a system of representatives of this partition. Then

$$(X \cdot X^t)_{\alpha,\beta} = \sum_{k=1}^{n} X_{\alpha,k} X_{\beta,k} = \sum_{r \in R} (X_{\alpha,r} X_{\beta,r} + X_{\alpha,\pi(r)} X_{\beta,\pi(r)}) = 0.$$

Since also $(X \cdot X^t)_{\alpha,\alpha} = \sum_{k=1}^n X_{\alpha,k}^2 = \sum_{k=1}^n x_k^2$, the statement follows.

Finally, we show (a) ⇔ (c):
According to Proposition 7.2.1, statement (a) holds if and only if X^t is a full orthogonal design of type $(1, \dots, 1)$, so the statement follows from the equivalence of (a) and (b). ◇

Corollary. Let X be a full orthogonal design of type $(1, \dots, 1)$. Then $|X|$ is isotopic to a multiplication table without boundaries for the groups $\{0\}$, $\mathbb{Z}_2$, $(\mathbb{Z}_2)^2$ or $(\mathbb{Z}_2)^3$.

Proof. With the previous lemma, each 2×2 submatrix which we obtain from two rows α, β and from two columns γ, δ is again an orthogonal design:

$$\begin{array}{c|ccccc} & \cdots & \gamma & \cdots & \delta & \cdots \\ \hline \vdots & & \vdots & & \vdots & \\ \alpha & \cdots & X_{\alpha,\gamma} & \cdots & X_{\alpha,\delta} & \cdots \\ \vdots & & \vdots & & \vdots & \\ \beta & \cdots & X_{\beta,\gamma} & \cdots & X_{\beta,\delta} & \cdots \\ \vdots & & \vdots & & \vdots & \end{array}$$

Hence, from Theorem 7.1.5, it follows that $|X|$ is a multiplication table without boundaries for a group isomorphic to $(\mathbb{Z}_2)^t$, where $t \in \mathbb{N}_0$ with $n = 2^t$. Now, the statement follows from Corollary 7.2.2. $\diamond$

7.2.4 Quasigroups Based on Full Orthogonal Designs

In what follows, let X be a full orthogonal design of type $(1, \ldots, 1)$ and order $n \in \{1, 2, 4, 8\}$. Let H be the Hadamard matrix with $X = H \star |X|$.

Now, both $|X|$ and X give rise to a quasigroup. Let $(S_0, \star)$, where $S_0 := \{x_1, \ldots, x_n\}$, be the quasigroup with the following multiplication table:

$$\begin{array}{c|ccc} \star & x_1 & \cdots & x_n \\ \hline x_1 & & & \\ \vdots & & |X| & \\ x_n & & & \end{array}$$

Let $-X := (-H) \star |X|$. Also this multiplication table

$$\begin{array}{c|ccc:ccc} \cdot & x_1 & \cdots & x_n & -x_1 & \cdots & -x_n \\ \hline x_1 & & & & & & \\ \vdots & & X & & & -X & \\ x_n & & & & & & \\ \hdashline -x_1 & & & & & & \\ \vdots & & -X & & & X & \\ -x_n & & & & & & \end{array}$$

is based on a latin square, since each symbol appears once in each row and once in each column. Hence, it corresponds to a quasigroup

$(S, \cdot)$, where $S := \{\pm x_k : k \in \{1, \ldots, n\}\}$. This quasigroup is called the *canonical quasigroup* of X. The multiplication table above is referred to as the *canonical multiplication table* for S or for X. The following example shows that in general, $(S, \cdot)$ is not associative and hence, not group-based.

Example. The canonical quasigroups of two orthogonal designs of the same order and type can have different algebraic properties (even if they have the same absolute value). For instance, using the border (A, B, C, D), the canonical quasigroup of the 4×4 orthogonal design in Example 7.2.2 (ii) is associative (since the quaternions are an associative algebra), but the canonical quasigroup of the 4×4 orthogonal design in Example 7.2.2 (i) is not associative, since $(BA)C = -(B(AC))$.

7.2.5 The Sign

Let $\mathrm{sign}\colon S \to (\{1, -1\}, \cdot)$ be the function defined by

$$\begin{aligned} \mathrm{sign}(x_k) &:= 1, \\ \mathrm{sign}(-x_k) &:= -1 \end{aligned}$$

for all $k \in \{1, \ldots, n\}$. Let $|-x_k| := |x_k| := x_k$. It can be easily seen that for all $y \in S$, we have $\mathrm{sign}(-y) = -\mathrm{sign}(y)$ and $y = \mathrm{sign}(y)|y|$.

Let $r \in \mathbb{N}$. On S^r, we consider the function

$$\begin{aligned} \mathrm{sign}\colon \quad & S^r \to (\{1, -1\}, \cdot), \\ & a \mapsto \mathrm{sign}(\mathrm{prod}_{(S,\cdot)}(a)). \end{aligned}$$

We refer to $\mathrm{sign}(a)$ as the *sign* of a.

7.2.6 Visualisation of the Word Problem

Here, we extend the visualisation from Subsection 7.1.8 to solve also the word problem for $(S, \cdot)$. In particular, we obtain an extended cube which can be used to calculate products in $(S, \cdot)$. The main idea is to divide the word problem into two problems, namely, the word problem for $(S_0, \star)$, which can be visualised by a cube with side length n, and the problem to obtain the corresponding sign.

Now, we look at the following $n \times n$ matrix $\hat{X}$ with entries in S: For all $\alpha, \beta \in \{1, \dots, n\}$, let

$$\hat{X}_{\alpha,\beta} := \pm x_\gamma$$

with $\gamma \in \{1, \dots, n\}$ such that $x_\beta \cdot (\pm x_\gamma) = x_\alpha$.

The following statement points out the analogy to the term of parastrophy of latin squares:

Proposition. Let

$$Y := \begin{pmatrix} X & -X \\ -X & X \end{pmatrix}.$$

Let $\sigma := (1\,2\,3)$. Let $\psi \colon S \to \{1, \dots, 2n\}, x_i \mapsto i, -x_i \mapsto i + r$. Let $\hat{Y} := \psi^{-1}((\psi(Y))_\sigma)$ be the (σ, ψ) parastrophe of Y. Then $\hat{X}$ equals the upper left submatrix of $\hat{Y}$.

Proof. For all $\alpha, \beta \in \{1, \dots, n\}$, we have

$$\begin{aligned}
& \hat{Y}_{\alpha,\beta} && = \pm x_\gamma \\
\Leftrightarrow\quad & (\psi(\hat{Y}))_{\alpha,\beta} && \in \{\gamma, \gamma + r\} \\
\Leftrightarrow\quad & ((\psi(Y))_\sigma)_{\alpha,\beta} && \in \{\gamma, \gamma + r\} \\
\Leftrightarrow\quad & Y_{\beta,\gamma} && = \pm x_\alpha \\
\Leftrightarrow\quad & x_\beta \cdot (\pm x_\gamma) && = x_\alpha \\
\Leftrightarrow\quad & \hat{X}_{\alpha,\beta} && = \pm x_\gamma.
\end{aligned}$$

$\diamond$

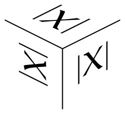
Proposition. $\hat{X}$ is a full orthogonal design of type $(1, \dots, 1)$ and $|\hat{X}| = |X|$.

Proof. Let $a, b, c \in S_0$. Since the transpose of X is again an orthogonal design, using the Rectangle Rule Lemma 7.2.3, there exists $d \in S$ with $(ab)(ac) + (db)(dc) = 0$. Since $(db)(dc) = ((-d)b)((-d)c)$, we may assume $d \in S_0$ without loss of generality. Hence, we obtain $ab = \pm dc$ and $ac = \mp db$. It follows that $\hat{X}$ has the following form:

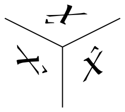
$$\begin{array}{c|ccccc}
 & \cdots & a & \cdots & d & \cdots \\ \hline
\vdots & & \vdots & & \vdots & \\
ab & \cdots & b & \cdots & \pm c & \cdots \\
\vdots & & \vdots & & \vdots & \\
ac & \cdots & c & \cdots & \mp b & \cdots \\
\vdots & & \vdots & & \vdots &
\end{array}$$

From Lemma 7.2.3, we conclude that $\hat{X}$ is a full orthogonal design of type $(1, \dots, 1)$. We have $|\hat{X}| = |X|$ since $(S_0, \star)$ is isomorphic to $(\mathbb{Z}_2)^t$ for $t \in \mathbb{N}$ appropriate, see Proposition 7.1.8. $\diamond$

In what follows, we assume that 1 is the neutral element in $(S_0, \star)$ (without loss of generality). Now, for given $b \in (S_0)^r$, the product $\mathrm{prod}_{(S_0,\star)}(b)$ can be obtained by visual means with the following cube:



Now, we write three copies of $\hat{X}$ in the following triple scheme:



This triple scheme carries the whole information about the multiplication in $(S_0, \star)$, since by ommitting the signs, we obtain the triple scheme for $|X|$. In what follows, we show that it contains also the information about the multiplication in $(S, \cdot)$.

Let $a := (a_1, \dots, a_r) \in S^r$. Let $b := (|a_1|, \dots, |a_r|) \in (S_0)^r$ and let $s := \mathrm{prod}_{(S,\cdot)}(a)$. We have already found a visualisation for $|s| = \mathrm{prod}_{(S_0,\star)}(b)$ by a spiral with $r - 1$ turns in the triple scheme for $|X|$; it is left to visualise the sign of s in the triple scheme for $\hat{X}$. Initially, we state that the sign of s can be lead back to the sign of b: From $-(xy) = (-x)y = x(-y)$ for each $x, y \in S$, it follows that

$$s = (\mathrm{sign}(a_1) \cdot \ldots \cdot \mathrm{sign}(a_r)) \cdot \mathrm{prod}_{(S,\cdot)}(b).$$

The sign of b can be visualised as follows: We first copy the spiral for b from the triple scheme for $|X|$ into the triple scheme for $\hat{X}$. Now, each negative sign in a corner of this spiral corresponds to a change in sign, since $-((xy)z) = (-xy)z = (xy)(-z)$ for all $x, y, z \in S$. Hence, the sign of b is given by $\mathrm{sign}(b) = (-1)^m$, where m is the total number of negative signs which appear in the corners of the spiral (of course, it may happen that one and the same cell has to be considered a number of times).

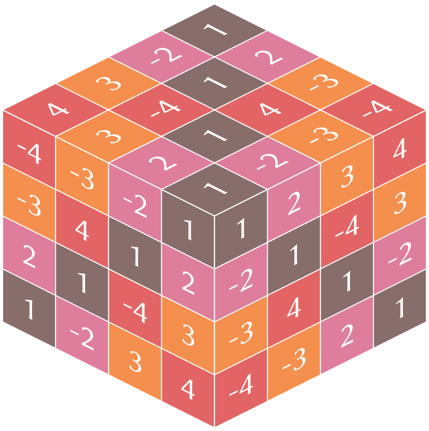
In summary, the solution of the word problem for s is given by those spirals with $r-1$ turns which end in s. Each spiral represents exactly one word $b := (b_1, \dots, b_r) \in (S_0)^r$ which multiplies up to $|s|$ in $(S_0, \star)$. Now, each word $(g_1 b_1, \dots, g_r b_r) \in S^r$, where $g_1, \dots, g_r \in \{1, -1\}$ with $g_1 \cdot \ldots \cdot g_r \cdot \text{sign}(b) = \text{sign}(s)$, multiplies up to s.

The solution of the word problem for $a = (a_1, \dots, a_r) \in S$ is given by the spiral with $r-1$ turns for the word $b := (|a_1|, \dots, |a_r|)$. The sign of $\text{prod}_{(S,\cdot)}(a)$ is given by $\text{sign}(a_1) \cdot \ldots \cdot \text{sign}(a_r) \cdot \text{sign}(b)$.

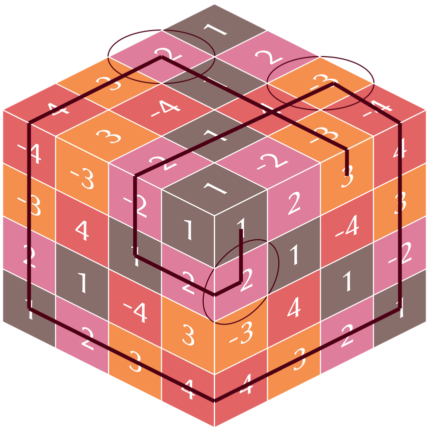
Example. In this example, we consider the canonical quasigroup based on the following orthogonal design:

$$\begin{array}{cccc}
x_1 & -x_2 & -x_3 & -x_4 \\
x_2 & x_1 & -x_4 & x_3 \\
x_3 & x_4 & x_1 & -x_2 \\
x_4 & -x_3 & x_2 & x_1
\end{array}$$

The orthogonal design coming from the $(1\ 2\ 3)$ parastrophe of this quasigroup equals the 4×4 orthogonal design in Example 7.2.2 (i). Omitting the symbol "x", the corresponding cube looks like:



By way of example, $a := (1, 2, 1, 3, 1, 1, 2) \in T_{3,7}$ and $\text{prod}_{(S,\cdot)}(a) = -3$. This can be visualised as follows:



There are three corners of the spiral which belong to a negative sign (each of them is highlighted by a circle).

7.3 Design Hyperplanes

In this section, we define the design partition, the design function and, finally, the design hyperplanes.

Let $n \in \{2,4,8\}$ and let $V = \mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$ with $r \geqslant 2$ tensor factors. The indexing tuples for V are given by $N := \{1,\dots,n\}^r = (S_0)^r$.

Let X be a full orthogonal design of type $(1,\dots,1)$ and order n (see Corollary 7.2.3). The symbols of X are denoted by $1, \dots, n$, that is, the entries of X lie in $\{\pm 1,\dots,\pm n\}$. We have described in the last section that X gives rise to the canonical quasigroup $(S,\cdot)$, and, using the boundaries $(1,\dots,n)$, $|X|$ gives rise to a group $(S_0,\star)$ which is isomorphic to $\mathbb{Z}_2$, $(\mathbb{Z}_2)^2$ or $(\mathbb{Z}_2)^3$. Without loss of generality, let 1 be the neutral element.

7.3.1 The Design Partition and the Design Function

Now, we recall the notions from Subsections 7.1.6 and Subsection 7.2.5. In particular, the partition $\mathcal{P}_{\mathrm{D}} := \mathcal{P}_r$ of $N = (S_0)^r$ is given by the parts $T_s := T_{s,r} = \{a \in (S_0)^r \colon \operatorname{prod}_{(S_0,\star)}(a) = s\}$, for all $s \in S_0$.

Definition. In this special context, we refer to $\mathcal{P}_{\mathrm{D}}$ as the *design partition*. Each part of this partition is called a *design part*. Moreover, we refer to $s_{\mathrm{D}} :=$ sign on N as the *design function*.

The multiplication $\star$ on S_0 extends to a pointwise multiplication on N so that N can be regarded as a group. In particular, for each $h \in N$, we consider the translation by h:

$$\beta \colon N \to N, \ a \mapsto h \star a.$$

This function is bijective with $\beta^2 = 1$.

Let $a = (a_1, \ldots, a_r), b = (b_1, \ldots, b_r) \in N$. We recall from Section 5.6 that $[(a, b)]$ is equal to the orbit of $(a, b) \in N^2/S_2$ under $Z = (\mathbb{Z}_2)^r$ (which can also be identified with $\mathfrak{P}(\{1, \ldots, r\})$). Now, for all subsets $A \subseteq \{1, \ldots, r\}$, let $h_A := (h_1, \ldots, h_t) \in N$ with $h_t = a_t \star b_t$ for all $t \in A$ and $h_t = 1$ for all $t \in A^c$. Then we have $A.(a, b) = (h_A \star a, h_A \star b)$.

7.3.2 The Design Partition

Lemma. The design partition is a join-meet partition.

Proof. Let $a, b \in N$ with $\mathrm{prod}_{(S_0,\star)}(a) = \mathrm{prod}_{(S_0,\star)}(b) =: s$, that is, $a, b \in T_s$. If $c, d \in N$ with $(c, d) \overset{\star}{\longleftrightarrow} (a, b)$, then there exists $h \in N$ such that $(c, d) = (h \star a, h \star b)$. Hence, $c, d \in T_t$, where $t := \mathrm{prod}_{(S_0,\star)}(h) \star s$. If $a \neq b$, then Proposition 7.1.6.II implies that the entries of a and b differ in at least two positions, that is, $N(a, b)$ is no chain. ◇

7.3.3 The Design Function

Let $T \in \mathcal{P}_D$ and let $a, b \in T$ with $a \neq b$. Let $t \in \{1, \ldots, r\}$ be the last position in which the entries of a and b are different. From Proposition 7.1.6.II, we know that $t \geqslant 2$. Let $\beta_{a,b}$ be the translation by $h := (1, \ldots, 1, a_t \star b_t, 1, \ldots, 1)$, where the entry in position t equals $a_t \star b_t$.

In particular, $\beta_{a,b}$ swaps the entries of a and b in position t. This can be seen as follows: Letting

$$a_0 := (a_1, a_2, \ldots, a_{t-1}),$$
$$b_0 := (b_1, b_2, \ldots, b_{t-1}),$$

and $c := (a_{t+1}, \ldots, a_r) = (b_{t+1}, \ldots, b_r)$ yields $\beta_{a,b}(a) = h \star a = (a_0, b_t, c) =$ and $\beta_{a,b}(b) = h \star b = (b_0, a_t, c)$.

Lemma. Let $a, b \in N$ with $a \neq b$ such that a and b are in the same design part. Then we have

$$s_D(a) \cdot s_D(b) = -s_D(\beta_{a,b}(a)) \cdot s_D(\beta_{a,b}(b)).$$

Proof. *Preliminary statement*:
We first note that for $x, y, z \in S$ with $y = x$ or $y = -x$, we have

$$s_D(x) \cdot s_D(y) = s_D(x \cdot z) \cdot s_D(y \cdot z).$$

Case $t = r$:
Let $\mathrm{prod}_{(S,\cdot)}(a_0, a_t) =: p_1$ and $\mathrm{prod}_{(S,\cdot)}(b_0, b_t) =: p_2$. Since a and b are in the same design part, we have $|p_1| = |p_2|$. From $a_t \neq b_t$, we obtain $\mathrm{prod}_{(S,\cdot)}(a_0) =: r_1 \neq r_2 := \mathrm{prod}_{(S,\cdot)}(b_0)$. Now, we have $h \star a = (a_1, \dots, a_{t-1}, b_t) = (a_0, b_t)$ and $h \star b = (b_1, \dots, b_{t-1}, a_t) = (b_0, a_t)$. Let $\mathrm{prod}_{(S,\cdot)}(h \star a) =: q_1$ and $\mathrm{prod}_{(S,\cdot)}(h \star b) =: q_2$. It follows that $|q_1| = |q_2|$. Now, the equation follows from the rectangle rule Lemma 7.2.3. This can be seen with a multiplication table of $(S, \cdot)$:

$$\begin{array}{c|ccccc}
 & \cdots & a_t & \cdots & b_t & \cdots \\
\hline
\vdots & & \vdots & & \vdots & \\
r_1 & \cdots & p_1 & \cdots & q_1 & \cdots \\
\vdots & & \vdots & & \vdots & \\
r_2 & \cdots & q_2 & \cdots & p_2 & \cdots \\
\vdots & & \vdots & & \vdots &
\end{array}$$

Case $t < r$:
From the last case, we know that the assertion holds for $a' := (a_1, \dots, a_t)$ and $b' := (a_1, \dots, a_t)$. Let $s := s_D$. Now, the preliminary statement can be applied, since $b_{t'} = a_{t'}$ for all $t' \in \{t+1, \dots, r\}$:

$$\begin{aligned}
s(a) \cdot s(b) = s(a', c) \cdot s(b', c) \\
&= s((\cdots(\mathrm{prod}_{(S,\cdot)}(a_0, a_t) \cdot a_{t+1}) \cdot \ldots) \cdot a_r) \\
&\quad \cdot s((\cdots(\mathrm{prod}_{(S,\cdot)}(b_0, b_t) \cdot a_{t+1}) \cdot \ldots) \cdot a_r) \\
&= -s((\cdots(\mathrm{prod}_{(S,\cdot)}(a_0, b_t) \cdot a_{t+1}) \cdot \ldots) \cdot a_r) \\
&\quad \cdot s((\cdots(\mathrm{prod}_{(S,\cdot)}(b_0, a_t) \cdot a_{t+1}) \cdot \ldots) \cdot a_r) \\
&= -s(\beta_{a,b}(a)) \cdot s(\beta_{a,b}(b)).
\end{aligned}$$

◇

Corollary. The design function is a splitting function for the design partition.

Proof. We consider the boolean lattice $B := N(a, b)$ and the function $\beta\colon B \to B$, $d \mapsto \beta_{a,b}(d)$. Then, using Lemma 7.3.3, for all $d \in B$, we have

$$s_{\mathrm{D}}(d) \cdot s_{\mathrm{D}}(d') = -\, s_{\mathrm{D}}(\beta(d)) \cdot s_{\mathrm{D}}(\beta(d')).$$

Hence, s_{D} is a splitting function for the join-meet partition $\mathcal{P}_{\mathrm{D}}$. ◇

In particular, the following polynomial is a Hibi relation:

$$s_{\mathrm{D}}(a)\ s_{\mathrm{D}}(b) \cdot x_a\, x_b + s_{\mathrm{D}}(h \star a)\ s_{\mathrm{D}}(h \star b) \cdot x_{h\star a}\, x_{h\star b}. \tag{7.2}$$

This shows that $\det_{a,b,h\star a,h\star b}$ is a non-zero PV-determinant (the meaning of the colours is explained in Subsection 5.6.6):

a_0	a_t	c	a_0	b_t	c
b_0	a_t	c	b_0	b_t	c

7.3.4 Design Hyperplanes as Sos Polynomials

Here, we state the main results of this chapter. They say that each design part gives rise to a witness hyperplane which touches the projective unit ball $\mathcal{B}_{1,\pi}$ in V at a scaled maximal vector.

Let $T \in \mathcal{P}_{\mathrm{D}}$ be a design part. Since the parts of the design partition have the same length, we have $\#T = n^{r-1}$. Let

$$y := \frac{1}{n^{r-1}} \cdot \sum_{a \in T} s_{\mathrm{D}}(a) \cdot e_a \in V.$$

Definition. The affine hyperplane in V which is defined by the support functional $l_y = 1 - \sum_{a\in T} s_{\mathrm{D}}(a) \cdot x_a$ to y is called a *design hyperplane*.

Theorem. The support functional l_y to y is a 1-sos-mod $\mathcal{J}_N$-polynomial.

Proof. This follows from Theorem 6.3.6, since $\mathcal{P}_{\mathrm{D}}$ is a join-meet partition and s_{D} is a splitting function for $\mathcal{P}_{\mathrm{D}}$, see Corollary 7.3.3. ◇

Corollary. We have $\|y\|_\pi = 1$. In particular, the inner radius of $\mathcal{B}_{1,\pi}$ equals $r(\mathcal{B}_{1,\pi}) = \sqrt{1/n^{r-1}}$, such that the vector $\sqrt{1/n^{r-1}} \cdot \sum_{a\in T} s_{\mathrm{D}}(a) \cdot e_a$ is maximal for $\mathcal{B}_{1,\pi}$. In addition, for any vector $z \in V$ which lies in a design hyperplane, we have $\|z\|_\pi \geqslant 1$.

Proof. The last theorem states that l_y is a witness for $\mathcal{B}_{1,\pi}$, yielding $\|z\|_\pi \geqslant 1$. It can be easily seen that $\|y\|_\pi \leqslant 1$ according to the definition of the projective norm, so that $\|y\|_\pi = 1$. With the Arveson bound Theorem 3.3.4, we obtain $\|y\| = \sqrt{1/n^{r-1}} = \mathrm{Arv}(V) \leqslant r(\mathcal{B}_{1,\pi}) \leqslant \|y\|$. ◇

On this basis we obtain a class of vectors with projective norm 1 in Chapter 10. This leads to a generalisation of the Schmidt decomposition in the real case. There is also a summary of the results.

With the computer program described in Subsection 6.2.5 one can check Theorem 7.3.4 for some small values of r.

7.3.5 Some Examples

In the following examples we consider design partitions and design functions for different values of n and r. From now on, design parts are also represented by matrices. The values of a design function are shown in front of the corresponding row (negative values are indicated by "−" and positive values are omitted).

Example. A design partition with a design function in the case $n = 4$ and $r = 2$ can be found in Example 6.3.4.III, see Figure 6.4 on page 175.

Example. With the OD$(4; 1, 1, 1, 1)$ from Example 7.2.6 and $r = 3$, we obtain:

$T_{1,3}$	$T_{2,3}$	$T_{3,3}$	$T_{4,3}$
1 1 1	− 1 1 2	− 1 1 3	− 1 1 4
2 2 1	− 2 2 2	− 2 2 3	− 2 2 4
3 3 1	− 3 3 2	− 3 3 3	− 3 3 4
4 4 1	− 4 4 2	− 4 4 3	− 4 4 4
− 1 2 2	− 1 2 1	− 1 2 4	1 2 3
2 1 2	2 1 1	2 1 4	− 2 1 3
− 3 4 2	− 3 4 1	− 3 4 4	3 4 3
4 3 2	4 3 1	4 3 4	− 4 3 3
− 1 3 3	1 3 4	− 1 3 1	− 1 3 2
2 4 3	− 2 4 4	2 4 1	2 4 2
3 1 3	− 3 1 4	3 1 1	3 1 2
− 4 2 3	4 2 4	− 4 2 1	− 4 2 2
− 1 4 4	− 1 4 3	1 4 2	− 1 4 1
− 2 3 4	− 2 3 3	2 3 2	− 2 3 1
3 2 4	3 2 3	− 3 2 2	3 2 1
4 1 4	4 1 3	− 4 1 2	4 1 1

Hence, for example, the following affine functional is 1-sos-mod $\mathcal{J}_N$:

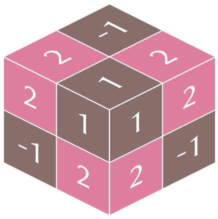
$$\begin{aligned} 1 - (x_{111} \quad &+ x_{221} + x_{331} + x_{441} \quad - x_{234} + x_{243} \\ &- x_{122} - x_{133} - x_{144} \quad + x_{324} - x_{342} \\ &+ x_{212} + x_{313} + x_{414} \quad - x_{423} + x_{432}). \end{aligned}$$

We note that each matrix (without the signs) is an orthogonal array, in particular, an $\mathrm{OA}(16,3,4,2)$.

Example. Let $n = 2$. By way of example, the following tensor in $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$ is the support vector of a design hyperplane:

$$y = \frac{1}{4} \cdot (e_{111} + e_{221} + e_{122} - e_{212}).$$

Hence, its projective norm equals 1. This can be seen by considering the orthogonal design $\left(\begin{smallmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{smallmatrix}\right)$ from Example 7.2.2. The corresponding cube looks like:



The design parts and the design function for $r \in \{1,2,3\}$ are given by

$T_{1,1}$	$T_{2,1}$	$T_{1,2}$	$T_{2,2}$	$T_{1,3}$	$T_{2,3}$
1	2	$1\,1$	$1\,2$	$1\,1\,1$	$1\,1\,2$
		$2\,2$	$-2\,1$	$2\,2\,1$	$2\,2\,2$
				$1\,2\,2$	$-1\,2\,1$
				$-2\,1\,2$	$2\,1\,1$

As an alternative to the cube, the partition and the signs can be obtained recursively by a concatenation rule in dependence of $r \geqslant 2$. In this respect, a change in sign corresponds to a minus sign in the appropriate position:

$$T_{1,r+1} = \left(\begin{array}{c:c} T_{1,r} & v_{1,r} \\ \hdashline T_{2,r} & v_{2,r} \end{array}\right), \quad T_{2,r+1} = \left(\begin{array}{c:c} T_{1,r} & v_{2,r} \\ \hdashline -T_{2,r} & v_{1,r} \end{array}\right),$$

where $v_{1,r}$ ($v_{2,r}$) is a column vector of length r whose entries equal 1 (2, respectively). With this rule, the design partitions can be easily obtained for the cases where $r = 4$ and $r = 5$:

$T_{1,4}$	$T_{2,4}$	$T_{1,5}$	$T_{2,5}$
1 1 1 1	1 1 1 2	1 1 1 1 1	1 1 1 1 2
2 2 1 1	2 2 1 2	2 2 1 1 1	2 2 1 1 2
1 2 2 1	1 2 2 2	1 2 2 1 1	1 2 2 1 2
− 2 1 2 1	− 2 1 2 2	− 2 1 2 1 1	− 2 1 2 1 2
1 1 2 2	− 1 1 2 1	1 1 2 2 1	1 1 2 2 2
2 2 2 2	− 2 2 2 1	2 2 2 2 1	2 2 2 2 2
− 1 2 1 2	1 2 1 1	− 1 2 1 2 1	− 1 2 1 2 2
2 1 1 2	− 2 1 1 1	2 1 1 2 1	2 1 1 2 2
		1 1 1 2 2	− 1 1 1 2 1
		2 2 1 2 2	− 2 2 1 2 1
		1 2 2 2 2	− 1 2 2 2 1
		− 2 1 2 2 2	2 1 2 2 1
		− 1 1 2 1 2	1 1 2 1 1
		− 2 2 2 1 2	2 2 2 1 1
		1 2 1 1 2	− 1 2 1 1 1
		− 2 1 1 1 2	2 1 1 1 1

We note that this example gives orthogonal arrays (in particular, an $\mathrm{OA}(2,2,2,1)$, two $\mathrm{OA}(4,3,2,2)$, two $\mathrm{OA}(8,4,2,3)$ and two $\mathrm{OA}(16,5,2,4)$). The case where $r = 4$ (the "tesseract") can also be found in Example 6.3.4.III, see Figure 6.5 on page 175. In addition, $T_{1,4}$ can be regarded as a binary linear $(4,3)$-code, see Example 6.5.5.

Example. The last example shows that the projective norm of the W-vector $\xi_W = \frac{1}{\sqrt{3}}(e_{112}+e_{121}+e_{211})$ in $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$ (see Subsection 3.3.3) is equal to $\sqrt{3}$. This can be seen as follows: Let $y := \frac{1}{3} \cdot (e_{112} + e_{222} + e_{211})$, then $\|y\|_\pi \leqslant 1$. Since y is a zero of the polynomial $1-(x_{112}+x_{222}-x_{121}+x_{211})$, which defines a design hyperplane, we also have $\|y\|_\pi \geqslant 1$, that is, $\|y\|_\pi = 1$. Now, we have $\|\xi_W\|_\pi = \|y\|_\pi \cdot \sqrt{3} = \sqrt{3}$.

7.3.6 Discussion

One might ask whether it is possible to obtain witness hyperplanes which are based on orthogonal designs and on Theorem 6.3.6 also for values of n other than 2, 4 and 8.

The next section deals with the case where $n \in \{3, 5, 6, 7\}$.

What about the case where $n > 8$? Let us first consider the case where $n = 2^k$ for any $k \geqslant 4$. This case seems to be promising, since each orthogonal design which was interesting for us based on a latin square whose order is a power of 2. Indeed, Lemma 7.3.2 holds for any quasigroup S_0 which is isomorphic to $(\mathbb{Z}_2)^k$ such that we are able to find a join-meet partition of $N = \{1, \ldots, 2^k\}^r$. The question arises whether there also exists a splitting function for this join-meet partition. However, this seems to be more difficult because there exists no full orthogonal design of type $(1, \ldots, 1)$ in this case.

7.3.7 Symmetric Partitions and Symmetric Functions

The symmetric group S_r acts on N from the left, see Example 3.2.3: For all $\pi \in S_r$ and for all $a = (a_1, \ldots, a_r) \in N$, we have

$$\pi.a = (a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(r)}) = a \circ \pi^{-1}.$$

Definition. A proper partition $\mathcal{P}$ of N is called *symmetric*, if for all $T \in \mathcal{P}$, for all $a \in T$ and for all permutations $\pi \in S_r$, we have $\pi.a \in T$.

Definition. A function $s\colon N \to \{1, -1\}$ is called *symmetric*, if for all $\pi \in S_r$ and for all $a \in N$, we have $s(\pi.a) = s(a)$.

Since we assume that $(S_0, \star)$ is associative and commutative, it follows that the design partition is symmetric. The design function is not symmetric in general, see Example 7.3.5.II.

Example. In this example, we consider the multiplication table for the complex numbers 1 and i,

$$\begin{array}{c|cc} \cdot & 1 & i \\ \hline 1 & 1 & i \\ i & i & -1 \end{array},$$

see Example 7.2.2. The design partition and the design function are symmetric. With $S := \{1, i\}$, the design parts are $T_{1,r} = \{a \in \{1, i\}^r \colon \operatorname{prod}_{(S,\cdot)}(a) \in \mathbb{R}\}$ and $T_{2,r} = \{a \in \{1, i\}^r \colon \operatorname{prod}_{(S,\cdot)}(a) \in i\mathbb{R}\}$, and for all $a \in \{1, i\}^r$, the sign of $\operatorname{prod}_{(S,\cdot)}(a)$ equals $s_D(a)$.

7.4 Skip Hyperplanes

Let $n' \in \{3, 5, 6, 7\}$ and let $V' = \mathbb{R}^{n'} \otimes \cdots \otimes \mathbb{R}^{n'}$ with $r > 2$ tensor factors.

In this section, we define the skip partition, the skip function and, finally, the skip hyperplanes and the skip bound on the inner radius of the projective unit ball in the tensor product V'.

7.4.1 The Skip Partition and the Skip Function

The indexing tuples of V' are given by $N' := \{1, \ldots, n'\}^r$. In the case where $n' = 3$, let $n := 4$ and in the case where $n' \in \{5, 6, 7\}$, let $n := 8$. Let $N := \{1, \ldots, n\}^r$.

Definition. Let $\mathcal{P}_{\mathrm{D}}$ be a design partition with corresponding design function s_{D} for the lattice N. The restriction $\mathcal{P}_{\mathrm{S}}$ of $\mathcal{P}_{\mathrm{D}}$ on N' is called a *skip partition*. The restriction s_{S} of s_{D} on N' is called a *skip function*.

Proposition. The skip partition is a join-meet partition of N' and the skip function is a splitting function for it.

Proof. This can be easily verified, since $\mathcal{P}_{\mathrm{D}}$ is an inf-sup-partition with splitting function s_{D}. ◇

7.4.2 Skip Hyperplanes as Sos Polynomials

Let $T \in \mathcal{P}_{\mathrm{S}}$ and let $y := \frac{1}{(n')^{r-1}} \cdot \sum_{a \in T} s_{\mathrm{S}}(a) \cdot e_a \in V'$.

Definition. The affine hyperplane in V which is defined by the support functional $l_y = 1 - \sum_{a \in T} s_{\mathrm{S}}(a) \cdot x_a$ to y is called a *skip hyperplane*.

Theorem. The support functional l_y to y is a 1-sos-mod$\,\mathcal{J}_{N'}$-polynomial.

Proof. This follows immediately from Theorem 6.3.6, since $\mathcal{P}_{\mathrm{S}}$ is a join-meet partition and s_{S} is a splitting function for $\mathcal{P}_{\mathrm{S}}$. ◇

7.4.3 The Skip Bound

Let m_{Skip} denote the relative size of the skip partition and let

$$\text{Skip}(V') := \sqrt{1/m_{\text{Skip}}}.$$

Definition. We refer to $\text{Skip}(V')$ as the *skip bound*.

Corollary. Let y be the support vector of a skip hyperplane. We have $\|y\|_\pi = 1$, and for any vector z which lies in a skip hyperplane, we have $\|z\|_\pi \geqslant 1$. The inner radius of the projective unit ball $\mathcal{B}_{1,\pi}$ in V' satisfies the inequality

$$r(\mathcal{B}_{1,\pi}) \leqslant \text{Skip}(V').$$

Proof. The last theorem states that the skip hyperplanes are witnesses for the projective unit ball in V', which yields $\|z\|_\pi \geqslant 1$. It can be easily seen that $\|y\|_\pi \leqslant 1$ according to the definition of the projective norm, so that $\|y\|_\pi = 1$. From Corollary 6.3.6, it follows that $r(\mathcal{B}_{1,\pi}) \leqslant \sqrt{1/m_{\text{Skip}}} = \text{Skip}(V')$. ◇

Example. We consider the design partition from Example 7.3.5.II. At first, we mark each row which contains the entry 4 in orange:

T'_1	T'_2	T'_3	T'_4
1 1 1	−1 1 2	−1 1 3	−1 1 4
2 2 1	−2 2 2	−2 2 3	−2 2 4
3 3 1	−3 3 2	−3 3 3	−3 3 4
4 4 1	−4 4 2	−4 4 3	−4 4 4
−1 2 2	−1 2 1	−1 2 4	1 2 3
2 1 2	2 1 1	2 1 4	−2 1 3
−3 4 2	−3 4 1	−3 4 4	3 4 3
4 3 2	4 3 1	4 3 4	−4 3 3
−1 3 3	1 3 4	−1 3 1	−1 3 2
2 4 3	−2 4 4	2 4 1	2 4 2
3 1 3	−3 1 4	3 1 1	3 1 2
−4 2 3	4 2 4	−4 2 1	−4 2 2
−1 4 4	−1 4 3	1 4 2	−1 4 1
−2 3 4	−2 3 3	2 3 2	−2 3 1
3 2 4	3 2 3	−3 2 2	3 2 1
4 1 4	4 1 3	−4 1 2	4 1 1

Now, if we omit the marked rows, we obtain a skip partition (together with a skip function) for $n' = r = 3$, whose parts are denoted by T'_s, where $s \in \{1, 2, 3, 4\}$. This example illustrates that the parts of a skip partition do not have the same length in general. The relative size equals $m_{\text{Skip}} = 7$ and an upper bound for the inner radius is given by $\operatorname{Skip}(\mathbb{R}^3 \otimes \mathbb{R}^3 \otimes \mathbb{R}^3) = \sqrt{1/7}$. However, numeric tests, see Subsection 6.2.5, suggest that even $\sqrt{7}/9$ is an upper bound, so that we expect $r(\mathcal{B}_{1,\pi}) < \sqrt{1/7}$.

In Chapter 10 we obtain a class of vectors with projective norm 1 on the basis of Corollary 7.4.3. This leads to a generalisation of the Schmidt decomposition in the real case. There one can find also a summary of the results and more examples.

On the next page, we give an example how the relative size of the skip partition can be determined with the aid of *SageMath*, see [Sage]. (The code can also be found on the internet, see page xxi. You can use `https://sagecell.sagemath.org/` to run the code without installing Python).

```
print("Design Partition and Skip Partition")

import numpy as np

# FUNCTIONS - - - - - - - - - - - - - - - -

def app(M, z):
    """
    matrix = app(matrix, integer)
    --> append a new column, each entry equals z
    """
    return np.append(M,np.tile(z,(M.shape[0],1)),axis=1)

def con(M1, M2):
    """
    matrix = con(matrix, matrix)
    --> append M2 under M1:
    M1
    M2
    """
    return np.append(M1,M2,axis=0)

def printarr(M):
    """
    print = printarr(matrix)
    --> pretty print M
    """
    for i in M:
        for j in i:
            print(j, end=" ")
        print()

def skipfrompart(M,C):
    """
    integer = skipfrompart(matrix, list)
    --> number of rows which do not contain the numbers in C
    """
    yes = 0
    for i in range(M.shape[0]):
        a = M[i,:]
        a = a.tolist()
        no = 0
        for c in C:
            if c in a:
                no = 1
        if no == 0:
            yes = yes + 1
    return yes

# INITIAL VALUES  - - - - - - - - - - - - -

n = 4
r = 3

# PRINT - - - - - - - - - - - - - - - - - -

if n == 4:
    L = np.array([[1,2,3,4],[2,1,4,3],[3,4,1,2],[4,3,2,1]]);
if n == 8:
    L = np.array([[1,2,3,4,5,6,7,8],[2,1,4,3,6,5,8,7],#
    [3,4,1,2,7,8,5,6],[4,3,2,1,8,7,6,5],[5,6,7,8,1,2,3,4],#
    [6,5,8,7,2,1,4,3],[7,8,5,6,3,4,1,2],[8,7,6,5,4,3,2,1]]);
print("n = %.0f" % n)
print("r = %.0f" % r)
print("Relative size design partition = %d" % n^(r-1))
print("Number of parts = %d" % n)
print("Latin square =")
printarr(L)

# MAIN  - - - - - - - - - - - - - - - - - - -

T = [np.matrix([L[0,i]]) for i in range(n)] # initialise T

list = [] # empty list

for i in range(r-1):
    Talt = np.array(T, copy=True)  # copy values of T
    for j in range(n): # j: row in L
        Tjneu = np.array(list) # empty array
        for k in range(n): # k: column in L
            TT = app(Talt[k],L[j,k])
            if k == 0:
                Tjneu = TT
            if k > 0:
                Tjneu = con(Tjneu,TT)
        T[j] = Tjneu

# DESIGN PARTITION  - - - - - - - - - - - - -

for i in range(n):
    print("\nDesign part T_(%d,%d)\n" % (i+1,r))
    printarr(T[i])

# SKIP PARTITION  - - - - - - - - - - - - - -

print("\nSkip partition")
print("\nNumbers which are skipped:")
skip = np.array([4])
print(skip)

print("\nLength of parts skip partition:")
without = [skipfrompart(T[i],skip) for i in range(n)]
for i in range(n):
    print(’T_%d: %d ’ % (i+1,without[i]))

mskip = np.max(np.array(without))
print(’\nRelative size skip partition: m_Skip = %d’ % mskip)
print(’Skip bound: Skip(V) = %.6f’ % (1/mskip^0.5))
```

Chapter 8

PARITY HYPERPLANES

In this chapter, we introduce a class of affine hyperplanes in the real tensor product $V := \mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$ for $n \in \mathbb{N}$, $n \geqslant 2$, which we call *parity hyperplanes*. The main results of this chapter are Theorem 8.3.5 and Theorem 8.4.5. They say that the parity hyperplanes are witnesses for the projective unit ball in V. This gives an explicit upper bound on the inner radius which we call the *parity bound*. The support vectors give a class of vectors with projective norm 1.

The parity hyperplanes are sos polynomials in the sense of Theorem 6.3.6, based on a join-meet partition, called *parity partition*, together with a splitting function, the *parity function*.

It can be easily verified that the parity partition is a join-meet partition, but it is more challenging to show that the parity function is a splitting function, see Section 8.3. Section 8.4 deals with the relative size of the parity partition.

Not only the design hyperplanes, but also the parity hyperplanes illustrate that the computation of the projective norm can be related to combinatorics. In addition, this chapter uses some aspects from homological algebra which can be found in Section 8.2.

In contrast to the design hyperplanes, the parity hyperplanes are defined for arbitrary values of n. As far as we know, for large values of n and r, it is an open question whether there exist better upper bounds on the inner radius.

Let $r \geqslant 2$ be the number of tensor factors of V and let $N := \{1, \ldots, n\}^r$ be the indexing tuples for V, which can be considered as the set of all words of length r with the alphabet $1, \ldots, n$. In this respect, for any $a = (a_1, \ldots, a_r) \in N$, we write $a = a_1 \cdots a_r$.

8.1 Sorting and Inversions

In this section we define the two notions *inversion rest* and *inversion symmetrisation* in preparation for the following sections. For this purpose, we begin with some aspects of sorting based on [Knu, Chapter 5 - Sorting] and [CLRS].

8.1.1 Inversion Tables

Definition. Let $a = a_1 \cdots a_r \in N$ and let $s_1, s_2 \in \{1, \dots, r\}$. The ordered pair (s_1, s_2) is called an *inversion* of a, if $s_1 < s_2$ and $a_{s_1} > a_{s_2}$. In this case, we call s_1 *leftgreater* to s_2 and s_2 *rightsmaller* to s_1 (with respect to a). The *left inversion table* $\mathrm{LIT}(a) := (p_1, \dots, p_r)$ of a is obtained by letting p_s, $s \in \{1, \dots, r\}$, be the number of positions which are leftgreater to s, that is, p_s is the number of inversions whose second component is s. Similarly, we define the *right inversion table* $\mathrm{RIT}(a) := (q_1, \dots, q_r)$ of a by letting q_s, $s \in \{1, \dots, r\}$, be the number of positions which are rightsmaller to s, that is, q_s is the number of inversions whose first component is s. Let $\mathrm{inv}(a)$ be the total number of inversions of a.

Obviously, elements of N with no inversions are sorted in ascending order, that is, they have the form $1 \cdots 1\, 2 \cdots 2 \cdots n \cdots n$, whereas not all of the numbers $1, \dots, n$ have to occur.

Both the left and the right inversion table consider each inversion exactly once, so that we obtain $\mathrm{inv}(a) = \sum_{s=1}^{r} p_s = \sum_{s=1}^{r} q_s$.

Example. Let $n = 3$ and $r = 5$. Here are three examples:

a	2 2 1 2 2	2 1 3 2 2	1 2 1 3 1
$\mathrm{LIT}(a)$	0 0 2 0 0	0 1 0 1 1	0 0 1 0 2
$\mathrm{RIT}(a)$	1 1 0 0 0	1 0 2 0 0	0 2 0 1 0
$\mathrm{inv}(a)$	2	3	3

Remark. In the special case where $n = r$, the symmetric group S_r can be considered as a subset of N. In [Knu], the inversion table $\mathrm{KIT}(a)$ for a permutation $a \in S_r$ is defined as follows: The s^{th} entry of $\mathrm{KIT}(a)$ equals the total number of those entries of a which are left to and greater than the *entry* (not the position) s. Our definition, however, can easily be traced back to the permutation case (for instance, if we assign $a := 1\,1\,2\,3\,2\,1$ to the "permutation" $b := 1\,2\,4\,6\,5\,3$, then we have $\mathrm{inv}(a) = \mathrm{inv}(b)$). Here we give an example which contrasts the three definitions:

a	5 9 1 8 2 6 4 7 3
$\mathrm{LIT}(a)$	0 0 2 1 3 2 4 2 6
$\mathrm{RIT}(a)$	4 7 0 5 0 2 1 1 0
$\mathrm{KIT}(a)$	2 3 6 4 0 2 2 1 0

8.1.2 Inversions and Sorting Algorithms

Let $a = a_1 \cdots a_r \in \mathbb{N}$. We have seen that $\mathrm{inv}(a)$ can be obtained with the left or the right inversion table. Now we show an alternative to obtain $\mathrm{inv}(a)$ by using sorting algorithms. To do this, we introduce the *bubble sort algorithm*. The analogy to rising bubbles in a glass of sparkling water gave the algorithm its name, see [Knu, Section 5.2.2]. See also [CLRS].

Bubble sort algorithm

```
IN: $a = a_1\, a_2 \cdots a_r$
  0. Let $b := a$, $k := 1$, $l := 2$, $s := 1$.
  1. Let $c := b$.
     If $b_k > b_l$, then we set $c_k := b_l$ and $c_l := b_k$.
     We set $b := c$.
  2. Case 1: $k < r - s$. Let $k \rightsquigarrow k + 1$ and $l \rightsquigarrow l + 1$.
     Proceed with 1.
     Case 2: $k = r - s$.
     Let $s \rightsquigarrow s + 1$. Proceed with Case 2.1 or Case 2.2.
     Case 2.1: $s < r$.
     Let $k \rightsquigarrow 1$, $l \rightsquigarrow 2$, and proceed with 1.
     Case 2.2: $s = r$.
     In this case, the entries of $b$ are sorted in ascending order.
     The algorithm stops.
OUT: $b = b_1 \cdots b_r$
```

The algorithm proceeds position by position from left to right, interchanging an entry with its neighbour if they are not sorted in ascending order. In case 2, the last s positions contain the s largest elements sorted in ascending order. At this stage, it is sufficient to sort only the entries in the first $r - s$ positions, starting with the first two positions. The following proposition shows that the number of interchanges under step 1 is equal to $\mathrm{inv}(a)$.

We recall from Example 3.2.3 that the symmetric group S_r acts on N from the left. In particular, we have $\pi.a = a_{\pi^{-1}(1)} \cdots a_{\pi^{-1}(r)}$ for all $\pi \in S_r$.

Proposition. There exists a permutation $\pi \in S_r$ with $\pi = \pi_s \cdot \ldots \cdot \pi_1$, where $\pi_1, \ldots, \pi_s \in S_r$, $s \in \mathbb{N}_0$, are adjacent transpositions, such that the entries of $\pi.a$ are sorted in ascending order and $\mathrm{inv}(a) = s$.

Proof. Let $\pi = (k\ k+1)$ be an adjacent transposition, where $k \in \{1, \ldots, r\}$. Now, if k is leftgreater to $k+1$ with respect to a, then $\mathrm{inv}(a) = \mathrm{inv}(\pi.a) + 1$. Hence, an interchange in bubble sort under step 1 corresponds to an adjacent transposition. Bubble sort shows that π exists, that is, each entry has to pass the entries of its rightsmaller positions. The statement $\mathrm{inv}(a) = s$ follows by induction. ◇

Example. Let $n = 5$ and $r = 5$. The following scheme shows the application of the bubble sort algorithm to $a := 4\,3\,5\,1\,2$, yielding $\mathrm{inv}(a) = 7$:

$$\begin{aligned} 4\ 3\ 5\ 1\ 2 &\xrightarrow{(1\,2)} 3\ 4\ 5\ 1\ 2 \xrightarrow{(3\,4)} 3\ 4\ 1\ 5\ 2 \xrightarrow{(4\,5)} 3\ 4\ 1\ 2\ 5 \quad (s=1)\\ &\xrightarrow{(2\,3)} 3\ 1\ 4\ 2\ 5 \xrightarrow{(3\,4)} 3\ 1\ 2\ 4\ 5 \quad (s=2)\\ &\xrightarrow{(1\,2)} 1\ 3\ 2\ 4\ 5 \xrightarrow{(2\,3)} 1\ 2\ 3\ 4\ 5 \quad (s=3). \end{aligned}$$

8.1.3 Geometric Views of Inversions

The next example shows nicely how inversions can be visualised. It can be found in [Knu] and [Zie].

Example. The orbit of $a := 1\,2\,3\,4 \in \{1, 2, 3, 4\}^4$ under S_4 can be identified with the vertices of a graph, see Figure 8.1 on page 237. Two vertices are connected by an edge, if the corresponding elements emerge from each other by an adjacent transposition. This graph is called the

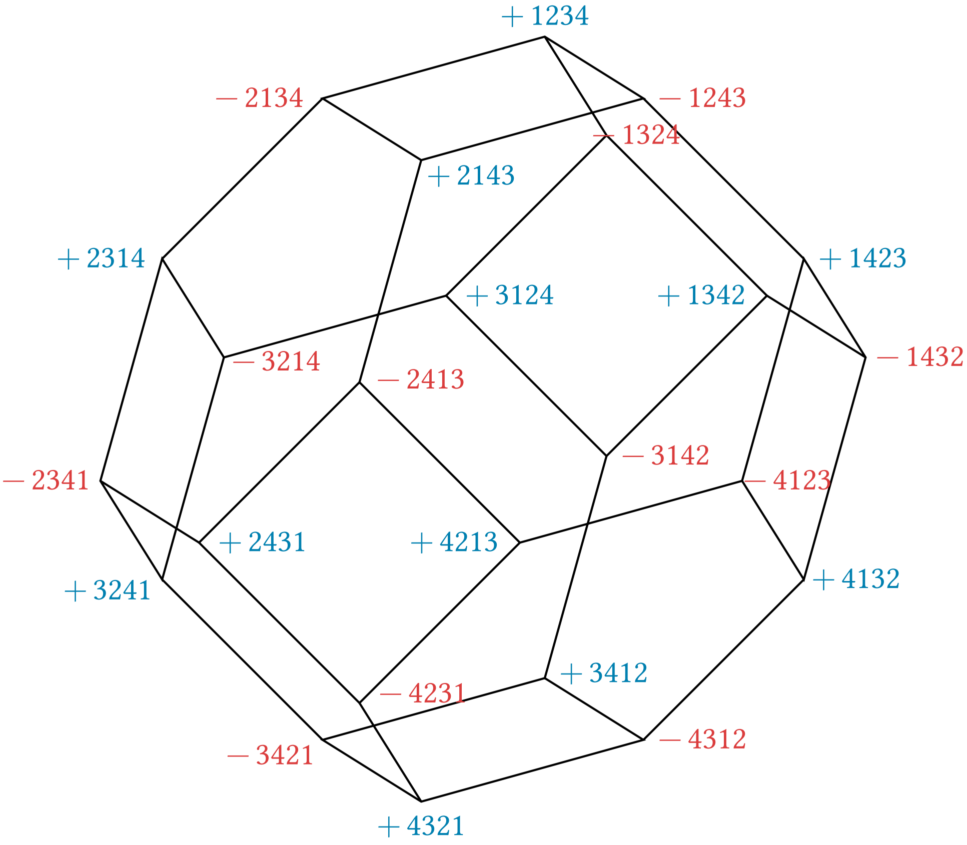


Figure 8.1: The permutahedron of order 4.

permutahedron of order 4. It is equivalent to a truncated octahedron. The signs indicate whether the corresponding permutation is even (+ and blue) or odd (− and red).

Figure 8.3 on page 239 shows only those vertices which have a positive sign. Here, two vertices are are connected by an edge, if the corresponding elements emerge from each other by two adjacent transpositions. This graph is equivalent to an icosahedron.

Figure 8.2 on page 238 shows how the icosahedron emerges from the truncated octahedron (visualised three-dimensionally).

The truncated octahedron can also be interpreted as the Hasse diagram of a lattice L corresponding to the so-called weak order of permutations. It is shown on Figure 8.4 on page 240. This lattice is not distributive, but there exists an isotone function from L to the distributive lattice $L' := \{0, 1, 2, 3\}^3$ (with top 333 and bottom 000).

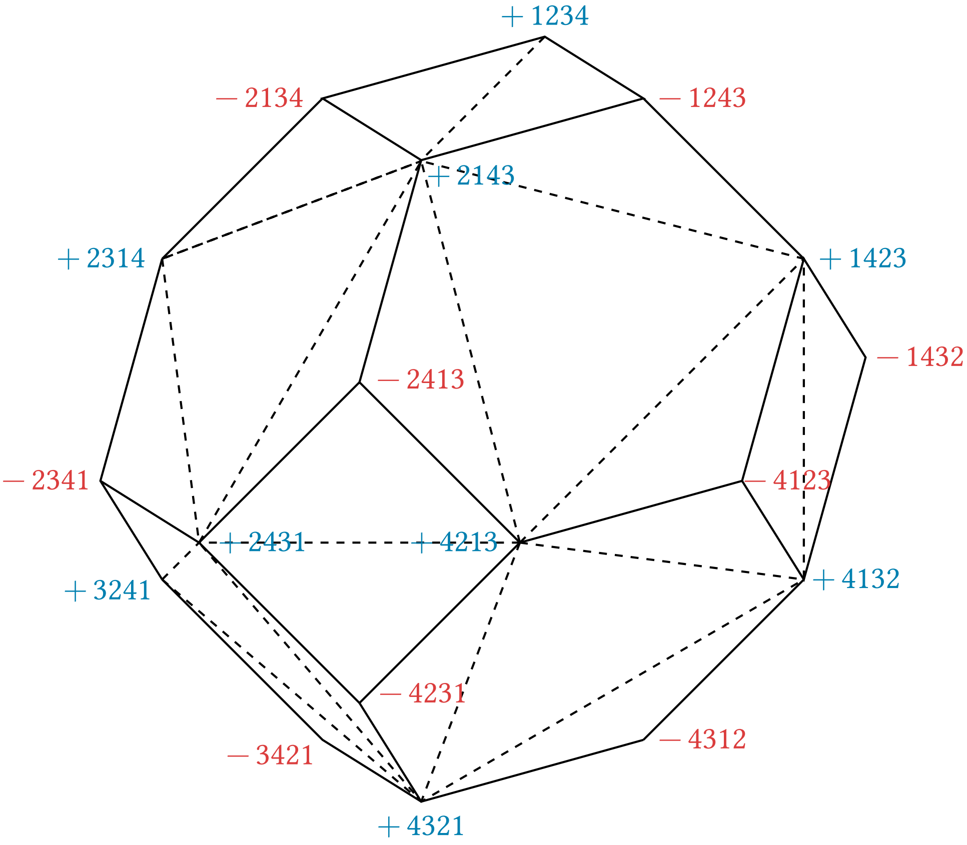


Figure 8.2: An icosahedron in the truncated octahedron.

8.1.4 The Inversion Rest

We now ask how the number of inversions behaves when a change is made in exactly one position. In this respect we come to our first definition.

Let $a = a_1 \cdots a_r \in N$. Let $s_0 \in \{1, \ldots, r\}$ and let $c \in \{1, \ldots, n\}$. Let $\widetilde{a} \in N$ emerge from a by replacing the s_0^{th} entry of a by c, that is,

$$\widetilde{a} := a(s_0, c) := a_1 \cdots a_{s_0-1} \underset{\uparrow s_0}{c} a_{s_0+1} \cdots a_r.$$

Definition. The *inversion rest* of a with respect to (s_0, c) is defined by

$$R(a, s_0, c) := (\text{inv}(\widetilde{a}) - \text{inv}(a)) \bmod 2.$$

Let $k_0 := \min(a_{s_0}, c)$ and $l_0 := \max(a_{s_0}, c)$.

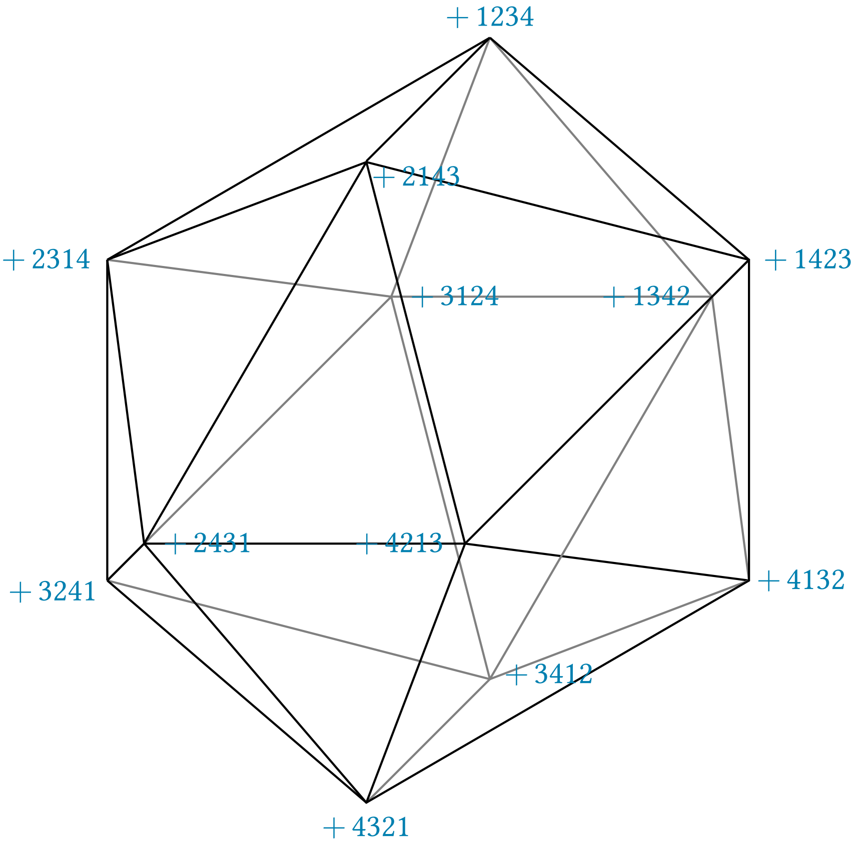


Figure 8.3: The positive permutations.

Proposition. We have

$$R(a, s_0, c) = \big(\#\{s \in \{1, \dots, s_0 - 1\} \colon k_0 < a_s \leqslant l_0\} \\ + \#\{s \in \{s_0 + 1, \dots, r\} \colon k_0 \leqslant a_s < l_0\} \big) \bmod 2.$$

Proof. Let $g = g_1 \cdots g_r \in N$. Let $\mathrm{LIT}(g) = (f_1^g, \dots, f_r^g)$ be the left inversion table, that is, f_s^g is equal to the number of positions in g which are leftgreater to s, that is, $f_s^g = \#\{t \in \{1, \dots, s-1\} \colon g_t > g_s\}$. According to Subsection 8.1.1, we have $\mathrm{inv}(g) = \sum_{s=1}^{r} f_s^g$. Obviously, the assertion holds in the case where $a_{s_0} = c$, so it is sufficient to consider the cases where $a_{s_0} < c$ and where $a_{s_0} > c$.

Case 1: $a_{s_0} < c$.

The entries of a and $\widetilde{a}$ coincide in the first $s_0 - 1$ positions. It follows that $f_s^a = f_s^{\widetilde{a}}$ for all $s \in \{1, \dots, s_0 - 1\}$. Now, we consider position s_0. A position which is leftgreater to s_0 in $\widetilde{a}$ is also leftgreater to s_0 in a, since c is larger than a_{s_0}, but the converse does not hold

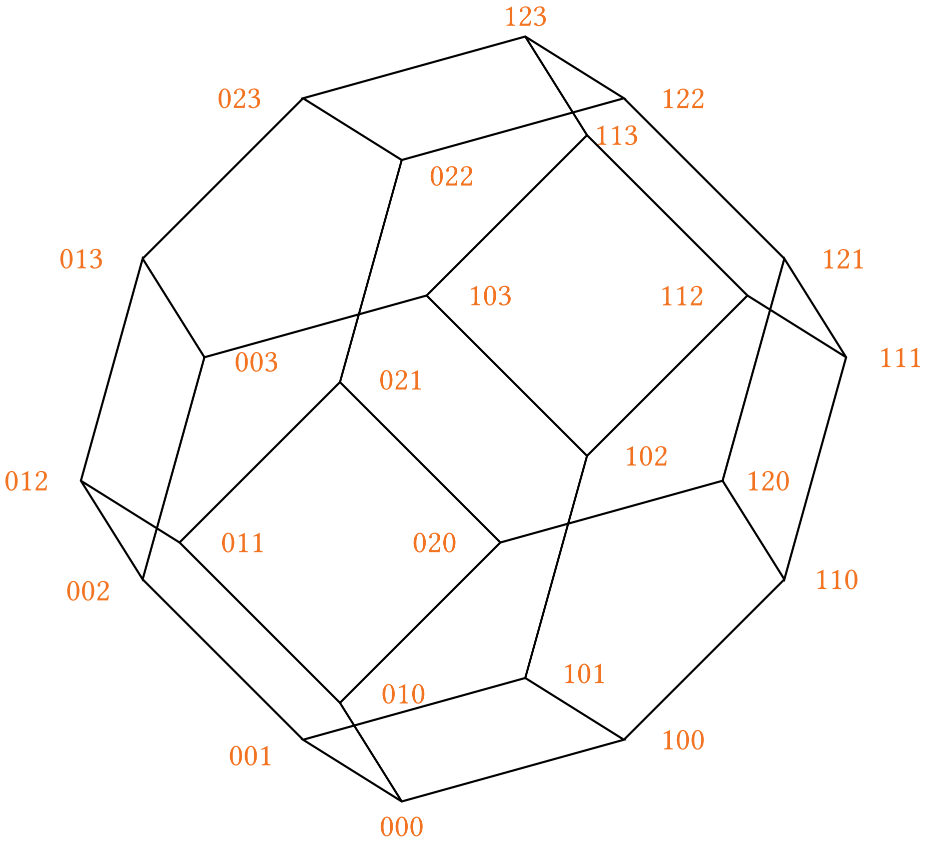


Figure 8.4: The permutahedron as a lattice.

in general. In particular, the difference results from counting all positions $s \in \{1, \ldots, s_0 - 1\}$ which are leftgreater to s_0 in a, but not in $\tilde{a}$. Hence, we obtain

$$f^{\tilde{a}}_{s_0} - f^{a}_{s_0} = -\#\{s \in \{1, \ldots, s_0 - 1\} \colon a_{s_0} < a_s \leqslant c\}.$$

Finally, let $s \in \{s_0 + 1, \ldots, r\}$. If position s_0 is leftgreater to s in a, it is also in $\tilde{a}$, since c is larger than a_{s_0}. The converse does not hold in general. In particular, a difference occurs if and only if a_s is less than c, but not less than a_{s_0}, that is,

$$f^{\tilde{a}}_{s} - f^{a}_{s} = \begin{cases} 1, & a_{s_0} \leqslant a_s < c \\ 0, & \text{otherwise.} \end{cases}$$

We conclude that

$$\operatorname{inv}(\tilde{a}) - \operatorname{inv}(a) = \sum_{s=1}^{r} (f^{\tilde{a}}_{s} - f^{a}_{s}) = \sum_{s=s_0}^{r} (f^{\tilde{a}}_{s} - f^{a}_{s})$$

$$
\begin{aligned}
&= (f^{\tilde{a}}_{s_0} - f^{a}_{s_0}) + \sum_{s=s_0+1}^{r} (f^{\tilde{a}}_{s} - f^{a}_{s}) \\
&= -\#\{s \in \{1, \dots, s_0 - 1\} \colon a_{s_0} < a_s \leqslant c\} \\
&\quad + \#\{s \in \{s_0 + 1, \dots, r\} \colon a_{s_0} \leqslant a_s < c\}.
\end{aligned}
$$

Since $a_{s_0} = k_0$ and $c = l_0$, we conclude that

$$
\begin{aligned}
R(a, s_0, c) = \big(&\#\{s \in \{1, \dots, s_0 - 1\} \colon k_0 < a_s \leqslant l_0\} \\
&+ \#\{s \in \{s_0 + 1, \dots, r\} \colon k_0 \leqslant a_s < l_0\}\big) \bmod 2.
\end{aligned}
\tag{8.1}
$$

Case 2: $a_{s_0} > c$.
It suffices to consider Case 1, since

$$
\begin{aligned}
R(a, s_0, c) &= (\operatorname{inv}(\tilde{a}) - \operatorname{inv}(a)) \bmod 2 \\
&= (\operatorname{inv}(a) - \operatorname{inv}(\tilde{a})) \bmod 2 \\
&= R(\tilde{a}, s_0, a_{s_0})
\end{aligned}
$$

and the right side of equation (8.1) is symmetric in c and in a_{s_0}. ◇

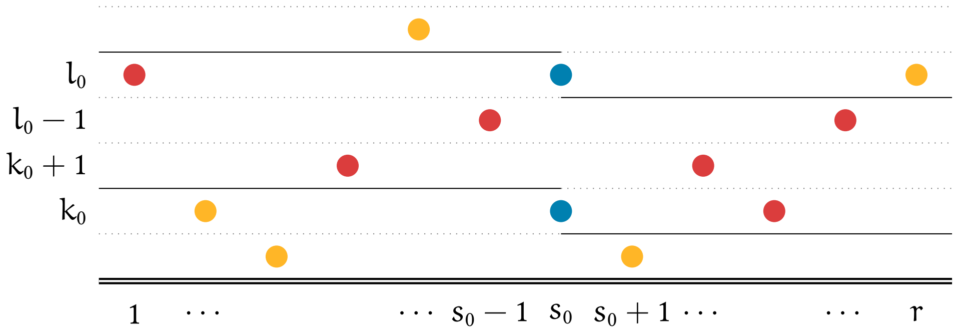


Figure 8.5: Illustration of the inversion rest.

Example. This example shows how we can obtain the inversion rest graphically. Let

$$a := 5\,2\,1\,3\,6\,4\,2\,1\,3\,2\,4\,5$$

and let $s_0 := 7$ and $c := 5$. Figure 8.5 shows a and $\tilde{a}$ by coloured dots. The positions are shown on the horizontal axis and the entries are shown on the vertical axis.

The positions which are leftgreater to position 7 with respect to a, but not with respect to $\tilde{a}$, correspond to the dots which lie within the two horizontal lines on the left, given by $k_0 := \min(2,5) = 2$ and $l_0 := \max(2,5) = 5$. The positions which have 7 as a leftgreater position with respect to $\widetilde{a}$, but not with respect to a, correspond to the dots which lie within the two right lines.

The dots that lie within (or outside) the two lines are coloured in red (or in yellow, respectively), so that $R(a, s_0, c) = R(a, 7, 5) = (3+3) \bmod 2 = 0$ is equal to the total number of red dots modulo 2.

8.1.5 The Inversion Symmetrisation

The inversion rest depends on the entries of a in positions different from s_0. In what follows, we introduce another notion which depends only on the entries in positions where a change is made.

Let $s_1, s_2 \in \{1, \ldots, r\}$ with $s_1 < s_2$ and let $c_1, c_2 \in \{1, \ldots, n\}$.

Let $a^0 := a$, $a^1 := a(s_1, c_1)$, $a^2 := a(s_2, c_2)$ and $a^3 := a^1(s_2, c_2)$:

$$\begin{aligned}
a^1 &:= (a_1, \ldots, a_{s_1-1}, \boxed{c_1}, a_{s_1+1}, \ldots, a_{s_2-1}, \ a_{s_2}\ , a_{s_2+1}, \ldots, a_r),\\
a^2 &:= (a_1, \ldots, a_{s_1-1}, \ a_{s_1}\ , a_{s_1+1}, \ldots, a_{s_2-1}, \boxed{c_2}, a_{s_2+1}, \ldots, a_r),\\
a^3 &:= (a_1, \ldots, a_{s_1-1}, \boxed{c_1}, a_{s_1+1}, \ldots, a_{s_2-1}, \boxed{c_2}, a_{s_2+1}, \ldots, a_r).
\end{aligned}$$

The boxes show the positions where changes can occur with respect to a.

Definition. The *inversion symmetrisation* of a with respect to (s_1, s_2, c_1, c_2) is defined by

$$S := S(a, s_1, s_2, c_1, c_2) := \left(\sum_{k=0}^{3} \operatorname{inv}(a^k) \right) \bmod 2.$$

Now, we show that the inversion symmetrisation depends only on c_1, c_2 and the entries of a in positions s_1 and s_2. To do this, let

$$\begin{aligned}
k_1 &:= \min(a_{s_1}, c_1),\\
l_1 &:= \max(a_{s_1}, c_1),\\
k_2 &:= \min(a_{s_2}, c_2), \text{ and}\\
l_2 &:= \max(a_{s_2}, c_2).
\end{aligned}$$

Lemma. We have $S = \operatorname{inv}(k_1, l_1, k_2, l_2) \bmod 2$.

Proof. From Proposition 8.1.4, we obtain

$$\begin{aligned} R(a^0, s_2, c_2) &= (\mathrm{inv}(a^2) - \mathrm{inv}(a^0)) \bmod 2 \\ &= (\,\#\{s \in \{1, \dots, s_2 - 1\}\colon k_2 < a_s \leqslant l_2\} \\ &\quad + \#\{s \in \{s_2 + 1, \dots, r\}\colon k_2 \leqslant a_s < l_2\}\,) \bmod 2, \text{ and} \\ R(a^1, s_2, c_2) &= (\mathrm{inv}(a^3) - \mathrm{inv}(a^1)) \bmod 2 \\ &= (\,\#\{s \in \{1, \dots, s_2 - 1\}\colon k_2 < (a^1)_s \leqslant l_2\} \\ &\quad + \#\{s \in \{s_2 + 1, \dots, r\}\colon k_2 \leqslant (a^1)_s < l_2\}\,) \bmod 2 \\ &= (\,\#\{s \in \{1, \dots, s_1 - 1\}\colon k_2 < a_s \leqslant l_2\} \\ &\quad + \#\{s \in \{s_1\}\colon k_2 < c_1 \leqslant l_2\} \\ &\quad + \#\{s \in \{s_1 + 1, \dots, s_2 - 1\}\colon k_2 < a_s \leqslant l_2\} \\ &\quad + \#\{s \in \{s_2 + 1, \dots, r\}\colon k_2 \leqslant a_s < l_2\}\,) \bmod 2. \end{aligned}$$

For any boolean expression A, let $\delta(A) := 1$ if A is true, otherwise let $\delta(A) := 0$. Now, it follows that

$$\begin{aligned} \left(\sum_{k=0}^{3} \mathrm{inv}(a^k)\right) \bmod 2 &= (R(a^0, s_2, c_2) + R(a^1, s_2, c_2)) \bmod 2 \\ &= (\,\#\{s \in \{s_1\}\colon k_2 < a_{s_1} \leqslant l_2\} \\ &\quad + \#\{s \in \{s_1\}\colon k_2 < c_1 \leqslant l_2\}\,) \bmod 2 \\ &= (\delta(k_2 < k_1 \leqslant l_2) \\ &\quad + \delta(k_2 < l_1 \leqslant l_2)) \bmod 2. \end{aligned} \tag{8.2}$$

From $k_1 \leqslant l_1$ and $k_2 \leqslant l_2$, it follows by a short calculation that

$$\begin{aligned} \delta(k_2 < k_1 \leqslant l_2) \bmod 2 &= (\delta(k_2 < k_1) + \delta(l_2 < k_1)) \bmod 2, \\ \delta(k_2 < l_1 \leqslant l_2) \bmod 2 &= (\delta(k_2 < l_1) + \delta(l_2 < l_1)) \bmod 2. \end{aligned}$$

Let $j := (k_1, l_1, k_2, l_2) \in \{1, \dots, n\}^4$. With equation (8.2), we obtain

$$\begin{aligned} \mathrm{inv}(j) \bmod 2 &= (\underbrace{\delta(l_1 < k_1)}_{=0} + \delta(k_2 < k_1) + \delta(k_2 < l_1) \\ &\quad + \delta(l_2 < k_1) + \delta(l_2 < l_1) + \underbrace{\delta(l_2 < k_2)}_{=0}) \bmod 2 \\ &= \left(\sum_{k=0}^{3} \mathrm{inv}(a^k)\right) \bmod 2. \end{aligned}$$

◇

Corollary. Let $a, b \in N$ and let $s_1, s_2 \in \{1, \dots, r\}$ with $s_1 < s_2$. Then we have

$$S(a, s_1, s_2, b_{s_1}, b_{s_2}) = S(b, s_1, s_2, a_{s_1}, a_{s_2}).$$

Proof. With Lemma 8.1.5, we obtain

$$S(a, s_1, s_2, b_{s_1}, b_{s_2}) = \mathrm{inv}(k_1, l_1, k_2, l_2) = S(b, s_1, s_2, a_{s_1}, a_{s_2})$$

with

$$\begin{aligned} k_1 &:= \min(a_{s_1}, b_{s_1}), \\ l_1 &:= \max(a_{s_1}, b_{s_1}), \\ k_2 &:= \min(a_{s_2}, b_{s_2}), \text{ and} \\ l_2 &:= \max(a_{s_2}, b_{s_2}). \end{aligned}$$

◇

8.2 Some Homological Algebra

The main result of this section is Theorem 8.2.3 which will be important for the next section. For this purpose, we introduce some standard notions related to homological algebra.

8.2.1 Cochain Complexes

Definition. A finite *cochain complex* of length 3 is a chain

$$C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2,$$

where C^0, C^1, C^2 are abelian groups and d^0 and d^1 are group homomorphisms with the property $d^1 \circ d^0 = 0$.

The image B^1 of d^0 is called the $1-$*coboundary* and the kernel Z^1 of d^1 is called the $1-$*cocycle*. The $1-$coboundary is a subgroup of the $1-$cocycle. The quotient Z^1/B^1 is called the 1^{th} *cohomology group* of this complex.

In what follows, we introduce a special cochain complex which is common in the literature. For details, see [Ser] or [Bos, page 201], who used it to formulate a cohomological version of the so-called Hilbert's Theorem 90.

8.2.2 A Special Cochain Complex

We first note that the set $\mathcal{A}(P, Q)$ of all functions from a non-empty set P in an abelian group Q is an abelian group under pointwise multiplication.

From now on, let G be a group acting on a non-empty set X and let H be an abelian group. We write $A := \mathcal{A}(X, H)$.

According to Proposition 3.2.3, a group action of G on A is given by $g.a := (x \mapsto a(g^{-1}.x))$. Moreover, for each $g \in G$, we consider the function $\pi_g \colon A \to A$, $a \mapsto g.a$. It can be easily verified that π_g is an automorphism on A. The set A can also be considered as a G-module (with the multiplication $g \cdot a =: g.a$).

To specify our setting, let $C^k := \mathcal{A}(G^k, A)$ for $k \in \{0, 1, 2\}$, that is, $C^0 = A$, $C^1 = \mathcal{A}(G, A)$ and $C^2 = \mathcal{A}(G^2, A)$.

We first define d^0 by

$$\begin{aligned} d^0 \colon\ & A \to \mathcal{A}(G, A) \\ & a \mapsto \varphi_a, \end{aligned}$$

where

$$\begin{aligned} \varphi_a \colon\ & G \to A \\ & g \mapsto \varphi_a(g) := \frac{g.a}{a}, \end{aligned}$$

that is,

$$\begin{aligned} \varphi_a(g) \colon\ & X \to H \\ & x \mapsto \frac{a(g^{-1}.x)}{a(x)}. \end{aligned}$$

From $g.a = \pi_g(a)$ and from the introductory comment that π_g is an automorphism, it can be seen that d^0 is a group homomorphism with image

$$B^1 = \left\{ \varphi \in \mathcal{A}(G, A) \colon \text{ There exists } a \in A \text{ with } \varphi = \frac{(\,\cdot\,).a}{a} \right\}.$$

Now, we define

$$\begin{aligned} d^1 \colon\ & \mathcal{A}(G, A) \to \mathcal{A}(G^2, A), \\ & \varphi \mapsto d\varphi, \end{aligned}$$

where

$$\begin{aligned} d\varphi \colon\ & G^2 \to A \\ & (g, h) \mapsto d\varphi(g, h) := \frac{g.(\varphi(h)) \cdot \varphi(g)}{\varphi(gh)}. \end{aligned}$$

With the introductory comments, it follows that d^1 is a group homomorphism with kernel

$$Z^1 = \{\varphi \in \mathcal{A}(G, A)\colon \text{ For all } g, h \in G\colon \varphi(gh) = g.(\varphi(h)) \cdot \varphi(g)\}.$$

The latter equation is also called the *cocycle property*.

We note that if G acts trivially on A, then the cocycle Z^1 consists of all group homomorphisms $G \to A$.

To check $d^1 \circ d^0 = 0$, we will make use of the following observation:

Proposition. For all $a \in A$ and for all $g, h \in G$, we have

$$\varphi_a(gh) = g.(\varphi_a(h)) \cdot \varphi_a(g).$$

Proof. Since π_g is an automorphism on A, we obtain

$$\begin{aligned}\varphi_a(gh) &= \frac{(gh).a}{a}\\ &= \frac{g.(h.a)}{g.a} \cdot \frac{g.a}{a}\\ &= g.\left(\frac{h.a}{a}\right) \cdot \frac{g.a}{a}\\ &= g.(\varphi_a(h)) \cdot \varphi_a(g).\end{aligned}$$

◇

With the last proposition, we see that $B^1 \subseteq Z^1$. Thus, we have $d^1 \circ d^0 = 0$ and our setting specifies a finite cochain complex.

8.2.3 Cocycles and Homomorphisms

The following helpful statements will be specifically important for Lemma 8.3.4.

Proposition. Let $\varphi \in Z^1$. The preimage of a sub-G-module of A under φ is a subgroup of G.

Proof. Let U be a sub-G-module of A and let W denote the preimage of U under φ. We have $\varphi(1) = \varphi(1 \cdot 1) = 1.(\varphi(1)) \cdot \varphi(1) = \varphi(1) \cdot \varphi(1)$. It follows that $\varphi(1) = 1$, which lies in U, that is, $1 \in W$. Now, let $g, h \in W$. We obtain $\varphi(gh) = g.(\varphi(h)) \cdot \varphi(g) \in U$, so that $gh \in W$. Hence, W is a subgroup of G. ◇

Theorem. Let $\mathcal{G}$ be a generating set of G. Let $\varphi \in Z^1$ such that for all $g, h \in \mathcal{G}$, we have

$$\varphi(gh) = \varphi(g) \cdot \varphi(h).$$

Then φ is a group homomorphism.

Proof. Let $g, h \in G$ with $\varphi(gh) = \varphi(g) \cdot \varphi(h)$. From the cocycle property of φ, it follows that $\varphi(gh) = \varphi(g) \cdot g.\varphi(h)$. This yields $\varphi(h) = g.\varphi(h)$, that is, $\varphi(h)$ is invariant under g. The set of all elements of A which are invariant under G is a sub-G-module $\mathrm{Fix}_G(A)$ of A. Hence, φ is a group homomorphism if and only if $\varphi(G) \subseteq \mathrm{Fix}_G(A)$.

For $V \subseteq G$, we write $\mathrm{gen}(V)$ to denote the generated subgroup of V in G. For $U \subseteq A$, we write $\mathrm{gen}(U)$ to denote the generated sub-G-module of U in A.

Statement 1: $\varphi(\mathcal{G}) \subseteq \mathrm{Fix}_G(A)$.

Proof: Let $h \in \mathcal{G}$. By assumption and according to the introductory comment, for all $g \in G$, $\varphi(h)$ is invariant under g. Hence, $\varphi(h)$ is also invariant under $\mathrm{gen}(\varphi(\mathcal{G})) = G$, so that the statement follows.

Statement 2: $\varphi(G) \subseteq \mathrm{Fix}_G(A)$.

Proof: By definition, $\mathrm{gen}(\varphi(\mathcal{G}))$ is a sub-G-module of A. This implies that its preimage V_0 under φ is a subgroup of G according to Proposition 8.2.3. From $\mathcal{G} \subseteq V_0$ we obtain $V_0 = G$. Hence, we obtain

$$\varphi(G) = \varphi(V_0) \subseteq \mathrm{gen}(\varphi(\mathcal{G})). \tag{8.3}$$

From statement 1, we obtain $\mathrm{gen}(\varphi(\mathcal{G})) \subseteq \mathrm{Fix}_G(A)$. Statement 2 follows with the inclusion (8.3). ◇

8.2.4 Application to the Special Case

The evaluation functional on A at $x \in X$ is denoted by $\delta_x \colon A \to H$, $f \mapsto f(x)$. For all $a \in A$, let $\varphi_{a,x} := \delta_x \circ \varphi_a$ denote the composition of the coboundary φ_a with δ_x. In particular:

$$\varphi_{a,x} \colon\ G \xrightarrow{\varphi_a} A \xrightarrow{\delta_x} H$$
$$g \mapsto \frac{a(g^{-1}.x)}{a(x)}.$$

Corollary. Let $\mathcal{G}$ be a generating set of G. Let $a \in A$ such that for all $g, h \in \mathcal{G}$ and for all $x \in X$, we have

$$\varphi_{a,x}(gh) = \varphi_{a,x}(g) \cdot \varphi_{a,x}(h).$$

Then $\varphi_{a,x}$ is a group homomorphism for all $x \in X$. In addition, if $\varphi_{a,x}$ is a non-trivial (i.e. non-constant), then also $\varphi_{a,g.x}$ is non-trivial for all $g \in G$.

Proof. *Step 1*: Using the cocycle property, a short calculation shows that for all $g, h \in G$, we have

$$\varphi_{a,x}(gh) = \varphi_{a,g^{-1}.x}(h) \cdot \varphi_{a,x}(g). \tag{8.4}$$

Step 2: We have $\varphi_a \in B^1 \subseteq Z^1$. The assumption yields $\varphi_a(gh) = \varphi_a(g) \cdot \varphi_a(h)$ for all $g, h \in \mathcal{G}$, so that we can apply Theorem 8.2.3. Hence, φ_a is a group homomorphism, and so is $\varphi_{a,x}$ for all $x \in X$. The second statement follows from equation (8.4).

By the way, it can be noted that step 2 could also be shown without Theorem 8.2.3 by using equation (8.4) and induction. ◇

Corollary. Let G be abelian and let $H = (\{1, -1\}, \cdot)$. Let $a \in A$ and let $x \in X$ such that $\varphi_{a,x}$ is a non-trivial group homomorphism. Then the orbit $G.x$ of x under G can be partitioned into the parts $\{y \in G.x \colon a(y) = 1\}$ and $\{y \in G.x \colon a(y) = -1\}$ which have the same length.

Proof. We show that the two parts have the same length. The stabiliser G_x of x under G is a normal subgroup of the kernel of $\varphi_{a,x}$ (since G is abelian), so we can consider the homomorphism

$$\begin{aligned} \widetilde{\varphi}_{a,x} : \ G/G_x &\to \{1, -1\} \\ g\, G_x &\mapsto \frac{a(g^{-1}.x)}{a(x)}, \end{aligned}$$

which is non-trivial. Thus, there are two cosets of the kernel $\widetilde{\varphi}_{a,x}^{-1}(1)$ (that is, the index of $\widetilde{\varphi}_{a,x}^{-1}(1)$ in G/G_x is 2). They have the same length. The statement follows since $a(x)$ is a constant factor of $\varphi_{a,x}$ and since G/G_x and the orbit $G.x$ have the same cardinality, which follows from the Orbit-Stabiliser Theorem in Subsection 3.2.2. ◇

8.3 Parity Hyperplanes

In this section, we define the parity partition, the parity function and, finally, the parity hyperplanes.

With Corollary 6.3.6, the relative size of the parity partition gives rise to an upper bound on the inner radius of the projective unit ball.

In the next section, we determine an explicit formula for this upper bound.

8.3.1 The Parity Partition

Definition. For all $a = (a_1, \dots, a_r) \in N$ and for all $t \in \{1, \dots, n\}$, the *parity* of t in a is defined by

$$\rho(a)_t := \#\{s \in \{1, \dots, r\} \colon a_s = t\} \bmod 2.$$

We say that the parity of t in a is *even*, if $\rho(a)_t = 0$, and *odd*, if $\rho(a)_t = 1$. Now, let us consider the function

$$\begin{aligned} \rho \colon N &\to \mathbb{F}_2^n \\ a &\mapsto (\rho(a)_1, \dots, \rho(a)_n). \end{aligned}$$

The image $\rho(a)$ of a is called the *parity* of a in N.

The parity $\rho(a)_t$ indicates whether the total number of the entry t in a is even or odd.

Elements in $\mathbb{F}_2^n$ can be regarded as codewords, see Section 6.5 (we will return to this reference in Subsection 8.4.6). Now, we obtain $v \in \rho(N)$ if and only if $\mathrm{wt}(v) \bmod 2 = r \bmod 2$ and $\mathrm{wt}(v) \leqslant \min(n, r)$.

Definition. For all $v \in \rho(N)$, we refer to the set $T_v := \rho^{-1}(v)$ as a *parity part*. The parity parts define a partition $\mathcal{P}_P$ of N which we call the *parity partition*.

It can be easily seen that the parity partition $\mathcal{P}_P$ is symmetric.

The length of a parity part T_v depends only on n, r and $k := \mathrm{wt}(v)$. In Section 8.4 we give an explicit formula for the length $F(n, r, k)$.

Example. Let $r = 3$ and $n \geqslant 2$. In this example, we determine the parity parts for $N := \{1, \dots, n\}^3$ and their lengths. The image $\rho(N)$ of ρ is given by all $v \in \mathbb{F}_2$ with $\mathrm{wt}(v) = 1$ or, if $n \geqslant 3$, $\mathrm{wt}(v) = 3$. If $\mathrm{wt}(v) = 1$, then we have $v = (0, \dots, 0, 1, 0, \dots, 0)$, which is zero except in position $c \in \{1, \dots, n\}$, so that

$$T_v = \{(c,c,c)\} \cup \left(\bigcup_{\substack{d=1 \\ d \neq c}}^{n} \{(c,d,d), (d,c,d), (d,d,c)\} \right),$$

whose length equals $F(n,3,1) = 1 + (n-1)\cdot 3 = 3n-2$. If $\mathrm{wt}(v) = 3$, then there exists $c, d, e \in \{1, \ldots, n\}$ with $c < d < e$ such that v is zero except in positions c, d and e, so that

$$T_v = \{(c,d,e), (c,e,d), (d,c,e), (d,e,c), (e,c,d), (e,d,c)\},$$

whose length equals $F(n,3,3) = 6$. Hence, the parity partition of N consists of n parity parts whose length equals $3n-2$ and, if $n \geqslant 3$, of $\binom{n}{3} = \frac{1}{6}(n^3 - 3n^2 + 2n)$ parity parts whose length equals 6.

8.3.2 The Parity Partition is a Join-Meet Partition

Proposition. The parity partition is a join-meet partition.

Proof. Let $T \in \mathcal{P}_P$ and let $a, b \in T$. Let $c, d \in N$ with $(a,b) \overset{\star}{\longleftrightarrow} (c,d)$, that is, there exists $z \in Z$ with $z.\overline{a} = \overline{b}$, where $\overline{a} = (a,b)$ and $\overline{b} = (c,d)$, see Subsection 5.6.2. We recall that the group $(Z,+)$ can be identified with $(\mathfrak{P}(\{1,\ldots,r\}), \triangle)$. We show that there exists $T' \in \mathcal{P}_P$ with $c, d \in T'$, that is, $\rho(c) = \rho(d)$.

Step 1: Let us first assume that there exists $s_0 \in \{1, \ldots, r\}$ such that $z = \{s_0\}$, that is, (c,d) emerges from (a,b) by interchanging the entries of a and b in position s_0. The entries are denoted by a_{s_0} and b_{s_0}, respectively. Clearly, for all $t \in \{1, \ldots, n\} \setminus \{a_{s_0}, b_{s_0}\}$, this does neither change the total number of t's in a nor in b. Thus, from $\rho(a) = \rho(b)$ we obtain $\rho(c)_t = \rho(a)_t = \rho(b)_t = \rho(d)_t$. Now, let $t \in \{a_{s_0}, b_{s_0}\}$. From $\rho(a) = \rho(b)$ we obtain

$$\rho(c)_t \pm 1 = \rho(a)_t = \rho(b)_t = \rho(d)_t \mp 1 \ \in \mathbb{F}_2,$$

that is, $\rho(c)_t = \rho(d)_t$. It follows that $\rho(c) = \rho(d)$.

Step 2: The statement follows by induction for arbitrary $z \in Z$. ◇

8.3.3 The Parity Function

The *parity function* is defined as follows:

$$\begin{aligned} s_P\colon\ N &\to \{1, -1\} \\ a &\mapsto (-1)^{\mathrm{inv}(a)}. \end{aligned}$$

For each $(a,b) \in N^2/S_2$ (see Subsection 5.2.2), let

$$\mathrm{sig}(a,b) := s_P(a) \cdot s_P(b).$$

Example. Let $n = 2$ and let $r \in \{2, 3, 4, 5\}$. We will show below in Example 8.3.6 that the parity parts and the parity functions for those values coincide with the design functions from Example 7.3.5.III.

8.3.4 The Parity Function is a Splitting Function

Here, we show that the parity function is a splitting function for the parity partition.

For all $\overline{a} \in N^2/S_2$, let

$$\begin{aligned} \varphi_{\overline{a}}: \ & Z \to (\{1, -1\}, \cdot) \\ & z \mapsto \frac{\mathrm{sig}(z^{-1}.\overline{a})}{\mathrm{sig}(\overline{a})} = \mathrm{sig}(z.\overline{a}) \cdot \mathrm{sig}(\overline{a}). \end{aligned}$$

Lemma. For all $\overline{a} \in N^2/S_2$, the function $\varphi_{\overline{a}}$ is a group homomorphism.

Proof. *Step 1*: Here, we make use of the small introduction to homological algebra, see Section 8.2. We identify G with $Z = ((\mathbb{Z}_2)^r, +)$, see Section 5.6, H with $(\{1, -1\}, \cdot)$ and X with N^2/S_2. Alternatively, X could be identified with the orbit of $\overline{a}$ under Z. The function α is chosen as sig. Now, we have $\varphi_{\overline{a}} = \varphi_{\mathrm{sig}, \overline{a}}$.

Step 2: According to Corollary 8.2.4.I, it suffices to show the "multiplicativity" of $\varphi_{\overline{a}}$ on a generating set of Z, which is given by the singletons $\{s\}$, for all $s \in \{1, \dots, r\}$. Thus, the statement follows from verifying that for all $s_1, s_2 \in \{1, \dots, r\}$, the following equation holds:

$$\begin{aligned} \varphi_{\overline{a}}(\{s_1\} \triangle \{s_2\}) = \varphi_{\overline{a}}(\{s_1\}) \cdot \varphi_{\overline{a}}(\{s_2\}), \quad & \text{that is,} \\ 1 = \varphi_{\overline{a}}(\{s_1\}) \cdot \varphi_{\overline{a}}(\{s_2\}) \cdot & \varphi_{\overline{a}}(\{s_1\} \triangle \{s_2\}). \end{aligned} \tag{8.5}$$

Step 3: In the following, we show equation (8.5). To do this, we first note that it holds in the case where $s_1 = s_2$, so it is sufficient to assume $s_1 < s_2$. With $\{s_1\} \triangle \{s_2\} = \{s_1, s_2\}$, equation (8.5) is equivalent to the equation

$$1 = \mathrm{sig}(\overline{a}) \cdot \mathrm{sig}(\{s_1\}.\overline{a}) \cdot \mathrm{sig}(\{s_2\}.\overline{a}) \cdot \mathrm{sig}(\{s_1, s_2\}.\overline{a}). \tag{8.6}$$

The elements in N^2/S_2 which appear in equation (8.6) belong to the same equivalence class. Let $a = a_1 \cdots a_r$, $b = b_1 \cdots b_r \in N$ such that $\overline{a} = (a, b)$. Now, let $\overline{a}_1 := \{s_1\}.\overline{a}$, $\overline{a}_2 := \{s_2\}.\overline{a}$, and $\overline{a}_3 := \{s_1, s_2\}.\overline{a}$, which emerge from a and b by interchanging the entries in the positions s_1, s_2, and both s_1 and s_2, respectively. Thus, it follows that $\overline{a}_1 = (a^1, b^1)$, $\overline{a}_2 = (a^2, b^2)$ and $\overline{a}_3 = (a^3, b^3)$, where

$$\begin{aligned}
a^1 &:= (a_1, \dots, a_{s_1-1}, \boxed{b_{s_1}}, a_{s_1+1}, \dots, a_{s_2-1}, a_{s_2}, a_{s_2+1}, \dots, a_r),\\
b^1 &:= (b_1, \dots, b_{s_1-1}, \boxed{a_{s_1}}, b_{s_1+1}, \dots, b_{s_2-1}, b_{s_2}, b_{s_2+1}, \dots, b_r),\\[1ex]
a^2 &:= (a_1, \dots, a_{s_1-1}, a_{s_1}, a_{s_1+1}, \dots, a_{s_2-1}, \boxed{b_{s_2}}, a_{s_2+1}, \dots, a_r),\\
b^2 &:= (b_1, \dots, b_{s_1-1}, b_{s_1}, b_{s_1+1}, \dots, b_{s_2-1}, \boxed{a_{s_2}}, b_{s_2+1}, \dots, a_r),\\[1ex]
a^3 &:= (a_1, \dots, a_{s_1-1}, \boxed{b_{s_1}}, a_{s_1+1}, \dots, a_{s_2-1}, \boxed{b_{s_2}}, a_{s_2+1}, \dots, a_r),\\
b^3 &:= (b_1, \dots, b_{s_1-1}, \boxed{a_{s_1}}, b_{s_1+1}, \dots, b_{s_2-1}, \boxed{a_{s_2}}, b_{s_2+1}, \dots, a_r).
\end{aligned}$$

The boxes show the positions where changes can occur with respect to a or b. Let $a^0 := a$ and $b^0 := b$. With the definition of the parity function, equation (8.6) simplifies to the equation

$$\begin{aligned}
1 &= \operatorname{sig}(\overline{a}) \cdot \operatorname{sig}(\overline{a}_1) \cdot \operatorname{sig}(\overline{a}_2) \cdot \operatorname{sig}(\overline{a}_3)\\
&= \prod_{k=0}^{3} s_{P}(a^k)\, s_{P}(b^k)\\
&= \prod_{k=0}^{3} (-1)^{\operatorname{inv}(a^k)} (-1)^{\operatorname{inv}(b^k)}\\
&= (-1)^{\sum_{k=0}^{3} (\operatorname{inv}(a^k) + \operatorname{inv}(b^k))}.
\end{aligned} \tag{8.7}$$

Equation (8.7) is equivalent to the equation

$$0 = \sum_{k=0}^{3} (\operatorname{inv}(a^k) + \operatorname{inv}(b^k)) \bmod 2. \tag{8.8}$$

Corollary 8.1.5 implies that $S(a, s_1, s_2, b_{s_1}, b_{s_2}) = S(b, s_1, s_2, a_{s_1}, a_{s_2})$. This is equivalent to equation (8.8). ◇

Theorem. Let $T \in \mathcal{P}_{P}$ and $a, b \in T$ with $a \neq b$. Let $\overline{a} := (a, b)$. Then $\varphi_{\overline{a}}$ is a proper group homomorphism.

Proof. *Step 1*: Let $a, b \in N$. Let $s_0 \in \{1, \dots, r\}$ be the first position from the left where the entries of a and b are different, that is, $a_{s_0} \neq b_{s_0}$ and $a_t = b_t$ for all $t \in \{1, \dots, s_0 - 1\}$. Now, we set $z_0 := \{s_0\} \in Z$, $a^1 := a(s_0, b_{s_0})$ and $b^1 := b(s_0, a_{s_0})$, that is, $z_0.\overline{a} = (a^1, b^1)$.

With Lemma 8.3.4, the statement follows from verifying that

$$\varphi_{\overline{a}}(z_0) = -1. \tag{8.9}$$

We have

$$\begin{aligned}\varphi_{\overline{a}}(z_0) &= \operatorname{sig}(z_0.\overline{a})\cdot\operatorname{sig}(\overline{a})\\ &= s_P(a^1)\,s_P(b^1)\,s_P(a)\,s_P(b)\\ &= (-1)^{(\operatorname{inv}(a^1)-\operatorname{inv}(a))+(\operatorname{inv}(b^1)-\operatorname{inv}(b))}\\ &= (-1)^{R(a,s_0,b_{s_0})+R(b,s_0,a_{s_0})},\end{aligned}$$

so with $V := (R(a,s_0,b_{s_0})+R(b,s_0,a_{s_0})) \bmod 2$, equation (8.9) is equivalent to the equation

$$V = 1 \bmod 2. \tag{8.10}$$

In what follows, we show equation (8.10).

Step 2: The definition of the parity partition $\mathcal{P}_P$ yields $\rho(a)_t = \rho(b)_t$ for all $t \in \{1,\dots,n\}$.

Step 3: According to Proposition 8.1.4, we have

$$\begin{aligned}R(a,s_0,b_{s_0}) = (\,&\#\{s\in\{1,\dots,s_0-1\}\colon k_0 < a_s \leqslant l_0\}\\ &+\#\{s\in\{s_0+1,\dots,r\}\colon k_0 \leqslant a_s < l_0\}\,) \bmod 2 \quad\text{and}\\ R(b,s_0,a_{s_0}) = (\,&\#\{s\in\{1,\dots,s_0-1\}\colon k_0 < b_s \leqslant l_0\}\\ &+\#\{s\in\{s_0+1,\dots,r\}\colon k_0 \leqslant b_s < l_0\}\,) \bmod 2,\end{aligned}$$

where $k_0 := \min(a_{s_0}, b_{s_0})$ and $l_0 := \max(a_{s_0}, b_{s_0})$. A reformulation of V using $\{a_{s_0}, b_{s_0}\} = \{k_0, l_0\}$ leads to

$$\begin{aligned}V &= (\,\#\{s\in\{1,\dots,s_0-1\}\colon k_0 < a_s \leqslant l_0\}\\ &\quad+\#\{s\in\{1,\dots,s_0-1\}\colon k_0 < b_s \leqslant l_0\}\\ &\quad+\#\{s\in\{s_0+1,\dots,r\}\colon k_0 \leqslant a_s < l_0\}\\ &\quad+\#\{s\in\{s_0+1,\dots,r\}\colon k_0 \leqslant b_s < l_0\}\,) \bmod 2\\ &= \left.\begin{aligned}&(\,\#\{s\in\{1,\dots,r\}\colon k_0 < a_s < l_0\}\\ &+\#\{s\in\{1,\dots,r\}\colon k_0 < b_s < l_0\}\end{aligned}\right\} = 0 \bmod 2 \qquad (8.11)\\ &\quad\left.\begin{aligned}&+\#\{s\in\{1,\dots,s_0-1\}\colon a_s = l_0\}\\ &+\#\{s\in\{1,\dots,s_0-1\}\colon b_s = l_0\}\end{aligned}\right\} = 0 \bmod 2 \qquad (8.12)\\ &\quad\left.\begin{aligned}&+\#\{s\in\{s_0+1,\dots,r\}\colon a_s = k_0\}\\ &+\#\{s\in\{s_0+1,\dots,r\}\colon b_s = k_0\}\,)\end{aligned}\right\} = 1 \bmod 2 \qquad (8.13)\\ &\quad\bmod 2\\ &= 1 \bmod 2,\end{aligned}$$

where equation (8.11) follows from $\rho(a)_t = \rho(b)_t$ for all $t \in \{k_0 + 1, \dots, l_0 - 1\}$, equation (8.12) follows from the fact that a and b coincide in the first $s_0 - 1$ positions, and since either $a_{s_0} = k_0$ or $b_{s_0} = k_0$, and $\rho(a)_{k_0} = \rho(b)_{k_0}$, it follows that the total number of k_0's in a in positions greater than s_0 differs from that in b in 1, so that equation (8.13) holds. ◇

Corollary. The parity function is a splitting function for the parity partition.

Proof. Let $T \in \mathcal{P}_P$ and $a, b \in T$ with $a \neq b$. Let $\overline{a} := (a, b)$. From Theorem 8.3.4, it follows that $\varphi_{\overline{a}}$ is a proper group homomorphism. Hence, from Corollary 8.2.4.II, it follows that the orbit of $\overline{a}$ under Z can be separated in two parts with equal length with respect to the values of the parity function, that is, the parts

$$\{(c, d) \in \overline{a} \colon \operatorname{sig}(c, d) = 1\},$$
$$\{(c, d) \in \overline{a} \colon \operatorname{sig}(c, d) = -1\}$$

have the same length. ◇

Example. Here we give an example for Theorem 8.3.4. Let $a = 3\,2\,1\,3$ and $b = 2\,1\,2\,2$ (we recall the notation convention from page 233). For all $z \in Z$, we have $\varphi_{\overline{a}}(z) = \varphi_{\overline{a}}(1 - z) = \operatorname{sig}(z.\overline{a}) \cdot \operatorname{sig}(\overline{a})$. From $\operatorname{sig}(\overline{a}) = s_P(a) \cdot s_P(b) = (-1) \cdot (-1) = 1$, we obtain

$$\begin{aligned}
\varphi_{\overline{a}}(\emptyset) &= 1,\\
\varphi_{\overline{a}}(\{1\}) &= s_P(2\,2\,1\,3) \cdot s_P(3\,1\,2\,2) = -1,\\
\varphi_{\overline{a}}(\{2\}) &= s_P(3\,1\,1\,3) \cdot s_P(2\,2\,2\,2) = 1,\\
\varphi_{\overline{a}}(\{3\}) &= s_P(3\,2\,2\,3) \cdot s_P(2\,1\,1\,2) = 1,\\
\varphi_{\overline{a}}(\{4\}) &= s_P(3\,2\,1\,2) \cdot s_P(2\,1\,2\,3) = -1,\\
\varphi_{\overline{a}}(\{1,2\}) &= s_P(2\,1\,1\,3) \cdot s_P(3\,2\,2\,2) = -1,\\
\varphi_{\overline{a}}(\{1,3\}) &= s_P(2\,2\,2\,3) \cdot s_P(3\,1\,1\,2) = -1,\\
\varphi_{\overline{a}}(\{1,4\}) &= s_P(2\,2\,1\,2) \cdot s_P(3\,1\,2\,3) = 1.
\end{aligned}$$

Hence, $\varphi_{\overline{a}}$ is proper and $\#(\varphi_{\overline{a}}^{-1}(1)) = \#(\varphi_{\overline{a}}^{-1}(-1))$.

Example. The proof of Theorem 8.3.4 uses that the parities in a and b are equal. The following example shows that we cannot reject this requirement. Let $a = 1\,1\,1$ and $b = 2\,3\,4$. From $\operatorname{sig}(\overline{a}) = s_P(a) \cdot s_P(b) = 1 \cdot 1 = 1$, we obtain

$$\varphi_{\overline{a}}(\emptyset) = 1,$$

$$\begin{aligned}\varphi_{\overline{a}}(\{1\}) &= s_{\mathrm{P}}(2\,1\,1)\cdot s_{\mathrm{P}}(1\,3\,4) = 1\cdot 1 = 1,\\ \varphi_{\overline{a}}(\{2\}) &= s_{\mathrm{P}}(1\,3\,1)\cdot s_{\mathrm{P}}(2\,1\,4) = (-1)\cdot(-1) = 1,\\ \varphi_{\overline{a}}(\{3\}) &= s_{\mathrm{P}}(1\,1\,4)\cdot s_{\mathrm{P}}(2\,3\,1) = 1\cdot 1 = 1,\end{aligned}$$

that is, $\varphi_{\overline{a}}$ is not proper.

Remark. Alternatively, the corollary can be shown as follows: Let $T \in \mathcal{P}_{\mathrm{P}}$ and let $a, b \in T$ with $a \neq b$. Let $\overline{a} := (a, b)$. Let s_0 be the first position from the left where the entries of a and b are different and let $z = \{s_0\} \in Z$. The function

$$\beta\colon [\overline{a}] \to [\overline{a}],\ \overline{b} \mapsto z.\overline{b}$$

is bijective with $\beta^2 = 1$. It is left to show that $\mathrm{sig}(\overline{b}) \cdot \mathrm{sig}(\beta(\overline{b})) = -1$ for all $\overline{b} \in [\overline{a}]$. This approach does not use Lemma 8.3.4. A similar approach was used in Chapter 7.

8.3.5 Parity Hyperplanes as Sos Polynomials

Let $T \in \mathcal{P}_{\mathrm{P}}$ be a parity part. Let

$$y := \frac{1}{\#T} \cdot \sum_{a \in T} s_{\mathrm{P}}(a) \cdot e_a,$$

which lies in V.

Definition. The affine hyperplane in V which is defined by the support functional $l_y = 1 - \sum_{a \in T} s_{\mathrm{P}}(a) \cdot x_a$ to y is called a *parity hyperplane*.

Each parity hyperplane is a witness hyperplane for the projective unit ball $\mathcal{B}_{1,\pi}$ in V:

Theorem. The support functional l_y to y is a 1-sos-mod $\mathcal{J}_N$-polynomial.

Proof. This follows from Theorem 6.3.6, since $\mathcal{P}_{\mathrm{P}}$ is a join-meet partition and s_{P} is a splitting function for $\mathcal{P}_{\mathrm{P}}$, see Corollary 8.3.4. ◇

Now, we obtain the projective norm of y:

Corollary. We have $\|y\|_\pi = 1$, and for any vector $z \in V$ which lies in a parity hyperplane, we have $\|z\|_\pi \geqslant 1$.

Proof. The last theorem states that l_y is a witness for $\mathcal{B}_{1,\pi}$, yielding $\|z\|_\pi \geqslant 1$. It can be easily seen that $\|y\|_\pi \leqslant 1$ according to the definition of the projective norm, so that $\|y\|_\pi = 1$. ◇

In Chapter 10 we obtain a class of vectors with projective norm 1 on the basis of Corollary 8.3.5. This leads to a generalisation of the Schmidt decomposition in the real case.

With Corollary 6.3.6, we obtain an upper bound on the inner radius of $\mathcal{B}_{1,\pi}$. In the next section, we derive an explicit formula for it, see Theorem 8.4.5. See also Chapter 10 for a summary of the results.

With the computer program described in Subsection 6.2.5, one can check Theorem 8.3.5 for some small values of n and r.

8.3.6 Comparison with the Design Hyperplanes

In the case where $n \in \{2, 4, 8\}$, the question arises how to compare the design and the parity hyperplanes. First we compare the width and the relative size of the design and the parity partition. It can also be interesting to compare the corresponding splitting functions.

Proposition. The design partition $\mathcal{P}_{\mathrm{D}}$ is coarser than the parity partition $\mathcal{P}_{\mathrm{P}}$. In the case where $n \in \{4, 8\}$, it is strictly coarser. In the case where $n = 2$, the partitions can be equal.

Proof. *Step 1*: Let T be a parity part. We show that there exists a design part T' with $T \subseteq T'$. By definition, there exists $v = (v_1, \dots, v_n) \in \mathbb{F}_2^n$ with $T = \rho^{-1}(v)$. We recall that $N = (S_0)^r$, where $S_0 = \{1, \dots, n\}$. Let p be the product in $(S_0, \star)$ of all $s \in \{1, \dots, n\}$ with $v_s = 1$. Now, we consider the design part $T' := T_{p,r} = \{a \in N \colon \operatorname{prod}_{(S_0,\star)}(a) = p\}$. Let $a \in T$. Since $(S_0, \star)$ is commutative and each element is self-inverse, we obtain $\operatorname{prod}_{(S_0,\star)}(a) = p$, that is, $a \in T'$.

Step 2: In the case where $n \geqslant 4$, Example 7.3.5.II shows that $\mathcal{P}_{\mathrm{D}}$ is strictly coarser.

Step 3: In the case where $n = 2$, we consider the orthogonal design $\left(\begin{smallmatrix} 1 & 2 \\ -2 & 1 \end{smallmatrix}\right)$ from Example 7.3.5.III. It can be easily verified that the design parts are given by

$$T_{1,r} = \{a \in N \colon \operatorname{prod}_{(S_0,\star)}(a) = 1\} = \{a \in N \colon \rho(a)_2 = 0\} \text{ and}$$
$$T_{2,r} = \{a \in N \colon \operatorname{prod}_{(S_0,\star)}(a) = 2\} = \{a \in N \colon \rho(a)_2 = 1\}.$$

This shows that this design partition and the parity partition are equal. ◇

The length of a design part is n^{r-1}. In the next section, we compute the length of a parity part.

Proposition. In the case where $n = 2$, the parity function is equal to the design function from Example 7.3.5.III. In the case where $n \in \{4, 8\}$ and $r = 2$, the parity function is not equal to a design function.

Proof. *Case* $n = 2$: Again, we consider the orthogonal design $\left(\begin{smallmatrix} 1 & 2 \\ -2 & 1 \end{smallmatrix}\right)$ from Example 7.3.5.III. We show $s_{\mathrm{P}}(a) = s_{\mathrm{D}}(a)$ for all $a \in N$ by induction on r. The example shows that the statement is true in the case where $r = 2$. Let $r \geqslant 2$. Let $b = (b_1, \dots, b_r, b_{r+1}) \in \{1, 2\}^{r+1}$ and $(b_1, \dots, b_r) =: a$. We write also $b = a, b_{r+1}$ and $s := s_{\mathrm{D}}(a)$. Let k be the number of 2's in a. In the following, we consider $s_{\mathrm{D}}(b)$ in dependence of k and b_{r+1}. If k is even, then $\mathrm{prod}_{(S_0,\star)}(a) = 1$ and

$$\begin{aligned} s_{\mathrm{D}}(a, 1) &= s \cdot s_{\mathrm{D}}(1 \cdot 1) = s, \\ s_{\mathrm{D}}(a, 2) &= s \cdot s_{\mathrm{D}}(1 \cdot 2) = s. \end{aligned}$$

If k is odd, then $\mathrm{prod}_{(S_0,\star)}(a) = 2$ and

$$\begin{aligned} s_{\mathrm{D}}(a, 1) &= s \cdot s_{\mathrm{D}}(2 \cdot 1) = -s, \\ s_{\mathrm{D}}(a, 2) &= s \cdot s_{\mathrm{D}}(2 \cdot 2) = s. \end{aligned}$$

In summary, the sign changes exactly in the case where k is odd and $b_{r+1} = 1$. On the other hand, we have $\mathrm{inv}(a) \bmod 2 \neq \mathrm{inv}(b) \bmod 2$ if and only if k is odd and and $b_{r+1} = 1$, since in this case, an odd number of 2's has to pass the additional 1 to bring the entries of b in an ascending order.

Case $n \in \{4, 8\}$: Let X be an orthogonal design of order n and let $r = 2$. We show that there exists $a \in \{1, \dots, n\}^2$ such that $s_{\mathrm{D}}(a) \neq s_{\mathrm{P}}(a)$. We first note that a $n \times n$ Hadamard matrix has at least one negative entry in the upper right triangle (diagonal included). Since X can be decomposed in a Hadamard matrix and a latin square, there exists $\gamma, \delta \in \{1, \dots, n\}$, $\gamma \leqslant \delta$, such that $X_{\gamma,\delta}$ is a negative entry of X. Now, let $a := \gamma\,\delta$. We have $\mathrm{sign}(x_\gamma \cdot x_\delta) = s_{\mathrm{D}}(a) = -1$. On the other hand, we have $s_{\mathrm{P}}(a) = 1$, since a has no inversions. ◇

8.4 The Relative Size of the Parity Partition

In this section we first obtain an explicit formula for the length of a parity part. Then we obtain the relative size of the parity partition which gives the parity bound on the inner radius of the projective unit ball in V. We conclude with a discussion whether the parity bound can be improved.

Sincere thanks to the contributors of the mathematical forum `https://math.stackexchange.com` for their helpful hint to consider the multinomial expansion as a generating function.

8.4.1 The Parity Property

We recall that N can be considered as the set of all words of length r with the alphabet $1, \ldots, n$.

Let $F(n, r, k)$ be the number of all words $a \in N$ with the following property, which we call the *parity property*: The parity of each letter 1 to k in a is odd and the parity of each letter $k+1$ to n in a is even.

The length of a parity part $T \in \mathcal{P}_P$ equals $F(n, r, \mathrm{wt}(\nu))$, where $T = T_\nu$ for an appropriate $\nu \in \rho(N)$.

Clearly, we have $F(n, r, k) > 0$ if and only if $k \bmod 2 = r \bmod 2$ and $k \leqslant r$. In all other cases, we obtain $F(n, r, k) = 0$. The case where $r \leqslant n$ and $k = r$ simplifies to $F(n, r, k) = k!$.

By the way, the number of all words $a \in N$ such that the parity of exactly k letters in a is odd is given by $\binom{n}{k} \cdot F(n, r, k)$.

We say that $p = (p_1, \ldots, p_n) \in \mathbb{N}_0^n$ *sums up to* r, if $\sum_{t=1}^{n} p_t = r$. It is well-known that in this case, the multinomial coefficient

$$\binom{r}{p} := \binom{r}{p_1,\, p_2,\, \cdots,\, p_n} = \frac{p!}{p_1! \cdot p_2! \cdot \ldots \cdot p_n!}$$

gives the number of words of length r such that the letter t appears exactly p_t number of times for all $t \in \{1, \ldots, n\}$. We note that a word with this property has the parity property if and only if

$$p \bmod 2 = (\underbrace{1, \ldots, 1}_{k \text{ times}}, 0, \ldots, 0).$$

Hence, either all words with this property have the parity property or none of them do.

8.4.2 Generating Functions

A sequence of numbers can also be regarded as the coefficients of a formal power series in one or more commuting variables. In this respect, the formal power series is also called a *generating function* for the sequence or for its coefficients.

For example, the multinomial expansion

$$(z_1 + \ldots + z_n)^r = \sum_{\substack{p=(p_1,\ldots,p_n)\in\mathbb{N}_0^n \\ p \text{ sums up to } r}} \binom{r}{p} \cdot z_1^{p_1} \cdot \ldots \cdot z_n^{p_n},$$

where $z_1, \ldots, z_n$ are independent and commuting variables over $\mathbb{Z}$, is a generating function for the multinomial coefficients. This expression can be regarded as a polynomial in $\mathbb{R}[z_1, \ldots, z_n]$, whose value (regarded as a functional) at $(1, \ldots, 1) \in \mathbb{Z}^n$ equals n^r, which is the total number of words of length r.

Now, let $f = (f_1, \ldots, f_n) \in \{0,1\}^n$. Also as a formal power series in the variables $z_1, \ldots, z_n$ we consider the generating function

$$\begin{aligned} P(f) &:= ((-1)^{f_1} z_1 + \ldots + (-1)^{f_n} z_n)^r \\ &= \sum_{\substack{p=(p_1,\ldots,p_n)\in\mathbb{N}_0^n \\ p \text{ sums up to } r}} (-1)^{f_1 p_1 + \ldots + f_n p_n} \binom{r}{p} \cdot z_1^{p_1} \cdot \ldots \cdot z_n^{p_n}. \end{aligned}$$

Example. Here is an example which illustrates the usefulness of this generating function for our purposes. The value of $P(f)$ at $(1, \ldots, 1)$ is given by

$$\begin{aligned} A(f) &:= ((-1)^{f_1} + \ldots + (-1)^{f_n})^r \\ &= \sum_{\substack{p=(p_1,\ldots,p_n)\in\mathbb{N}_0^n \\ p \text{ sums up to } r}} (-1)^{f_1 p_1 + \ldots + f_n p_n} \binom{r}{p}. \end{aligned}$$

Now, the number of all words $a \in N$ such that the parity of the letter 1 in a is even (or odd, respectively) is given by

$$\begin{aligned} \frac{1}{2}\left(A(0,\ldots,0) + A(1,0,\ldots,0)\right) &= \frac{1}{2}(n^r + (n-2)^r) \\ &= \sum_{\substack{p=(p_1,\ldots,p_n)\in\mathbb{N}_0^n \\ p \text{ sums up to } r}} \frac{1+(-1)^{p_1}}{2} \binom{r}{p} \quad \text{and} \end{aligned}$$

$$\frac{1}{2}\left(A(0,\ldots,0) - A(1,0,\ldots,0)\right) = \frac{1}{2}(n^r - (n-2)^r)$$

$$= \sum_{\substack{p=(p_1,\dots,p_n)\in\mathbb{N}_0^n \\ p \text{ sums up to } r}} \frac{1-(-1)^{p_1}}{2} \binom{r}{p}.$$

8.4.3 The Length of a Parity Part

In what follows, we consider the generating function

$$G(n,r,k) := \frac{1}{2^n} \sum_{f=(f_1,\dots,f_n)\in\{0,1\}^n} (-1)^{f_1+\dots+f_k} \cdot P(f).$$

We will see shortly that this is a generating function for the multinomial coefficients which belong to words with the parity property, leading to an explicit formula for the length of a parity part:

Proposition. The value of $G(n,r,k)$ at $(1,\dots,1) \in \mathbb{Z}^n$ equals $F(n,r,k)$. In particular, we have

$$F(n,r,k) = \frac{1}{2^n} \sum_{m=0}^{k} \sum_{l=0}^{n-k} (-1)^m \binom{k}{m} \binom{n-k}{l} \big(n-2(m+l)\big)^r.$$

Proof. Let $\tilde{F}(n,r,k)$ be the value of $G(n,r,k)$ at $(1,\dots,1)$, that is,

$$\begin{aligned} &\tilde{F}(n,r,k) \\ &= \frac{1}{2^n} \sum_{(f_1,\dots,f_n)\in\{0,1\}^n} (-1)^{f_1+\dots+f_k} \cdot \big((-1)^{f_1} + \dots + (-1)^{f_n}\big)^r. \end{aligned}$$

A short calculation leads to

$$\begin{aligned} &\tilde{F}(n,r,k) \\ &= \frac{1}{2^n} \sum_{m=0}^{k} \sum_{l=0}^{n-k} (-1)^m \binom{k}{m} \binom{n-k}{l} \big((k-m)-m \\ &\qquad\qquad + (n-k-l)-l\big)^r \\ &= \frac{1}{2^n} \sum_{m=0}^{k} \sum_{l=0}^{n-k} (-1)^m \binom{k}{m} \binom{n-k}{l} \big(n-2(m+l)\big)^r. \end{aligned}$$

In what follows, we show $\tilde{F}(n,r,k) = F(n,r,k)$, which proves the assertion. To do this, let $p = (p_1,\dots,p_n) \in \mathbb{N}_0^n$ sum up to r and let $c(p)$ be the coefficient of $z_1^{p_1} \cdot \ldots \cdot z_n^{p_n}$ in $G(n,r,k)$.

Statement 1: We have

$$c(p) = \begin{cases} \binom{r}{p}, & p \bmod 2 = (\underbrace{1, \ldots, 1}_{k \text{ times}}, 0, \ldots, 0), \\ 0, & \text{otherwise.} \end{cases}$$

Proof: We have

$$c(p) = \frac{1}{2^n} \sum_{(f_1,\ldots,f_n)\in\{0,1\}^n} (-1)^{f_1(p_1+1)+\ldots+f_k(p_k+1)+f_{k+1}p_{k+1}+\ldots+f_n p_n} \binom{r}{p}.$$

Now, for all $f = (f_1, \ldots, f_k) \in \{0,1\}^k$ and for all $g = (f_{k+1}, \ldots, f_n) \in \{0,1\}^{n-k}$, let

$$d_1(f) := f_1(p_1+1) + \ldots + f_k(p_k+1),$$
$$d_0(g) := f_{k+1}p_{k+1} + \ldots + f_n p_n.$$

We obtain

$$c(p) = \frac{1}{2^n} \sum_{f\in\{0,1\}^k} \sum_{g\in\{0,1\}^{n-k}} (-1)^{d_1(f)+d_0(g)} \binom{r}{p}.$$

In the case where $p \bmod 2 = (1, \ldots, 1, 0, \ldots, 0)$, both $d_1(f) = 2 \cdot (f_1 + \ldots + f_k)$ and $d_0(g)$ are even numbers, which yields

$$c(p) = \frac{1}{2^n} \sum_{f\in\{0,1\}^n} \binom{r}{p} = \binom{r}{p}.$$

Otherwise, we may assume that $p_1 = 0$ or $p_{k+1} = 1$. In the first case, the parts

$$C_0 := \{f \in \{0,1\}^k : d_1(f) \text{ is even}\} \text{ and}$$
$$C_1 := \{f \in \{0,1\}^k : d_1(f) \text{ is odd}\}$$

have the same length. Hence, we obtain

$$c(p) = \frac{1}{2^n}\Big(\sum_{f\in C_0} 1 + \sum_{f\in C_1}(-1)\Big) \sum_{g\in\{0,1\}^{n-k}} (-1)^{d_0(g)} \binom{r}{p} = 0.$$

In an analogous manner, the second case gives $c(p) = 0$.

Statement 2: $\tilde{F}(n,r,k) = F(n,r,k)$.

Proof: Statement 1 says that the non-zero coefficients of the generating function $G(n,r,k)$ equal the multinomial coefficients $\binom{r}{p}$, where $p \bmod 2 = (1, \ldots, 1, 0, \ldots, 0)$. Hence, it follows that the value of $G(n,r,k)$ at $(1, \ldots, 1) \in \mathbb{Z}^n$ equals the total sum of all words which have the parity property. ◇

Example. Let $n = k = 2$. With Proposition 8.4.3, a short calculation gives

$$F(2,r,2) = \frac{1}{4}\big(2^r + (-2)^r\big).$$

This value is also equal to the value of

$$\begin{aligned} G(2,r,2) &= \frac{1}{4}\big((z_1+z_2)^r - ((-z_1)+z_2)^r\big) \\ &\quad - \frac{1}{4}\big((z_1+(-z_2))^r - ((-z_1)+(-z_2))^r\big) \end{aligned}$$

at $z_1 = z_2 = 1$.

8.4.4 The Relative Size of the Parity Partition

Proposition. The formula for the length of the parity parts has the following recursive property: For all $k \in \{0,\dots,n-2\}$ with $k \bmod 2 = r \bmod 2$ and $k \leqslant r$, we have

$$F(n,r,k) = \begin{cases} F(n,r,k+2) + F(n-2,r,k), & k \leqslant r-2, \\ k!, & k = r. \end{cases}$$

Proof. The case where $k = r$ was mentioned above, so it suffices to concentrate on the case where $k \leqslant r-2$. Let

$$\begin{aligned} v_1 &:= (\underbrace{1,\dots,1}_{k \text{ times}}, 0,0,0,\dots,0) \quad \text{and} \\ v_2 &:= (\underbrace{1,\dots,1}_{k \text{ times}}, 1,1,0,\dots,0). \end{aligned}$$

Now, the length of the parity parts $T := T_{v_1}$ and $T' := T_{v_2}$ is equal to $\#T = F(n,r,k)$ and $\#T' = F(n,r,k+2)$, respectively.

Step 1: We first construct an injection $\imath$ from T' to T with an "interchanging method": Let $a = a_1 \cdots a_r \in T'$. According to the assumption, the parity of each letter $k+1$ and $k+2$ in a is odd. Hence, there exists $m \in \{1,\dots,r\}$ such that a_m is the first entry in a from the left which equals $k+1$ or $k+2$. Now, let $b = b_1 \cdots b_r \in T$ such that $b_m = \{k+1,k+2\} \backslash a_m$ and in all other positions, the entries of b coincide with the entries of a. Let $b = \imath(a)$. By construction, the function $\imath\colon T' \to \imath(T')$ is bijective.

Step 2: The elements of T which are not in $\imath(T')$ are exactly those words in which both $k+1$ and $k+2$ do not appear, that is, with the letters $1,\dots,k$ (each of them have an odd parity) and $k+3,\dots,n$ (each of them have an even parity). ◇

Now, we denote the maximal length of a parity part by

$$m(n, r) := \max(F(n, r, k) \colon k \in \{0, \ldots, n\}).$$

Lemma. The maximal length of a parity part is given by

$$m(n, r) = \begin{cases} F(n, r, 0), & r \text{ is even}, \\ F(n, r, 1), & r \text{ is odd}. \end{cases}$$

In particular, we have

$$F(n, r, 0) = \frac{1}{2^n} \sum_{m=0}^{n} \binom{n}{m} (n - 2m)^r,$$

$$F(n, r, 1) = \frac{1}{2^n} \sum_{m=0}^{n-1} \binom{n-1}{m} \left((n - 2m)^r - (n - 2(m+1))^r\right).$$

Proof. This statement follows from Proposition 8.4.3 and from Proposition 8.4.4, since $F(n, r, k) \geqslant F(n, r, k+2)$ for all $k \in \{0, \ldots, \min(n-2, r-2)\}$ and since $F(n, r, 0) \neq 0$ if and only if r is even. ◇

Example. We consider the case where $n = 3$. If r is even, we have

$$F(3, r, 0) = \frac{1}{4}(3^r + 3) \text{ and } F(3, r, 2) = \frac{1}{4}(3^r - 1).$$

If r is odd, we have

$$F(3, r, 1) = \frac{1}{4}(3^r + 1) \text{ and } F(3, r, 3) = \frac{1}{4}(3^r - 3).$$

In each case, both values differ by one. This can be seen as follows: $1 \cdots 1$ is the only word which is not in the range of the function $\imath$ which is used in the proof of Proposition 8.4.4. The special cases where $n = 3$ and $r \in \{2, 3\}$ are outlined in Example 6.3.4.II, see Figure 6.2 and Figure 6.3 on page 174:

$$F(3, 2, 0) = 3, \; F(3, 2, 2) = 2, \; F(3, 3, 1) = 7 \text{ and } F(3, 3, 3) = 6.$$

Remark. The formula has another recursive property: For all $s \in \{2, \ldots, r-1\}$, we have

$$F(n, s+1, k) = \begin{cases} k \cdot F(n, s, k-1) & \\ \quad +(n-k) \cdot F(n, s, k+1), & 1 \leqslant k \leqslant n-1, \\ n \cdot F(n, s, n-1), & k = n, \\ n \cdot F(n, s, 1), & k = 0. \end{cases}$$

This can be seen as follows: If we choose a letter and concatenate it with the end of a given word of length s, which gives a new word of length $s+1$, then its parity changes compared to the original word.

8.4.5 The Parity Bound

Here, we state the second main result of this chapter.

Definition. Let

$$\operatorname{Par}(V) := \left(\frac{1}{2^n}\sum_{m=0}^{n}\binom{n}{m}(n-2m)^r\right)^{-1/2},$$

if r is even, and

$$\operatorname{Par}(V) := \left(\frac{1}{2^n}\sum_{m=0}^{n-1}\binom{n-1}{m}\left((n-2m)^r-(n-2(m+1))^r\right)\right)^{-1/2},$$

if r is odd, which we refer to as the *parity bound*.

Theorem. The inner radius of the projective unit ball $\mathcal{B}_{1,\pi}$ in V satisfies the inequality

$$r(\mathcal{B}_{1,\pi}) \leqslant \operatorname{Par}(V).$$

Proof. The relative size of the parity partition equals $m := m(n,r)$, whose explicit formula is given in Lemma 8.4.4. From Corollary 6.3.6, it follows that $r(\mathcal{B}_{1,\pi}) \leqslant 1/\sqrt{m} = \operatorname{Par}(V)$. ◇

Hence, the parity bound is an upper bound on the inner radius. We recall that the Arveson bound $\operatorname{Arv}(V)$ is a lower bound, so that we have

$$\operatorname{Arv}(V) = \frac{1}{\sqrt{n^{r-1}}} \leqslant r(\mathcal{B}_{1,\pi}) \leqslant \operatorname{Par}(V).$$

Example. Using the parity partition, one can easily show that the projective unit ball $\mathcal{B}_{1,\pi}$ in the bipartite tensor product $\mathbb{R}^n \otimes \mathbb{R}^n$ equals its first theta body $\mathcal{T}_1$. This can be seen with Proposition 6.3.7.II, since the join-meet partition in the proof is a parity partition. In particular, $\{1\,1, \dots, n\,n\}$ is a parity part and $\operatorname{Par}(V) = 1/\sqrt{n}$.

8.4.6 Discussion

One might ask whether it is possible to find witness hyperplanes for which the parity bound can be improved.

If we want to use Theorem 6.3.6 for an improvement, we need a join-meet partition of $N = \{1, \dots, n\}^r$ together with an appropriate splitting function. In what follows, we consider join-meet partitions which are coarser than the parity partition (in terms of refinement), so that the new partition has a larger relative size. The method which we present here is based on error-correcting codes (this method has nothing to do with the idea that a parity part is a (in general non-linear) code, see Theorem 6.5.2). However, finding an appropriate splitting function remains the biggest challenge.

Theorem. Let C be a binary linear code in $\mathbb{F}_2^n$ with $d(C) \geqslant 3$. Let $\mathcal{C}$ be the set of all affine translates of C, that is, $\mathcal{C} := \{v + C \colon v \in \mathbb{F}_2^n\}$. Let

$$\mathcal{P} := \{\rho^{-1}(C') \colon C' \in \mathcal{C}, \rho^{-1}(C') \neq \emptyset\}.$$

Then $\mathcal{P}$ is a join-meet partition of N which is coarser (or equal) than the parity partition $\mathcal{P}_{\mathrm{P}}$ of N.

Proof. Since C is a linear code with $d(v + C) \geqslant 3$, each affine translate $v + C$, where $v \in \mathbb{F}_2^n$, is a (in general non-linear) code with $d(v + C) \geqslant 3$.

The set $\mathcal{C}$ is a partition of $\mathbb{F}_2^n$. This implies that $\mathcal{P}$ is a proper partition of N which is coarser than (or equal to) the parity partition $\mathcal{P}_{\mathrm{P}}$. Let $T \in \mathcal{P}$ and let $a, b \in T$ with $a \neq b$.

Case 1: $\rho(a) = \rho(b)$.
The parity partition $\mathcal{P}_{\mathrm{P}}$ is a join-meet partition, so that $N(a, b)$ is no chain and for any $(c, d) \in N^2/S_2$ with $(c, d) \in [(a, b)]$, there exists $T' \in \mathcal{P}_{\mathrm{P}}$ with $c, d \in T'$. But since $\mathcal{P}$ is coarser than (or equal to) $\mathcal{P}_{\mathrm{P}}$, there exists $T'' \in \mathcal{P}$ with $T' \subseteq T''$, and hence, $c, d \in T''$.

Case 2: $\rho(a) \neq \rho(b)$.
Step 2.1: There exists $v_0 \in \mathbb{F}_2^n$ with $\rho(a), \rho(b) \in v_0 + C$. If we assume that $N(a, b)$ is a chain (which means that a and b differ in exactly one position), then the parities of a and b are equal except of exactly two numbers, but the distance of $\rho(a)$ and $\rho(b)$ is at least 3. This is a contradiction, and hence, $N(a, b)$ is no chain.
Step 2.2: With step 2.1, there exists $(c, d) \in N^2/S_2$ with $(c, d) \in [(a, b)]$ and $(c, d) \neq (a, b)$. Here, we consider the special case where

$(c,d) = \{s_0\}.(a,b)$ for an appropriate $s_0 \in \{1,\ldots,r\}$. We may assume that $c = a(s_0, b_{s_0})$ and $d = b(s_0, a_{s_0})$. Then the parities of all $t \in \{1,\ldots,n\} \setminus \{a_{s_0}, b_{s_0}\}$ in a or in b, respectively, remain unchanged, that is, we have $\rho(c)_t = \rho(a)_t$ and $\rho(d)_t = \rho(b)_t$. Now, let $t \in \{a_{s_0}, b_{s_0}\}$. The interchange in position s_0 changes the total number of t both in a and in b. Thus, we obtain

$$\rho(c)_t = \rho(a)_t \mp 1, \text{ and } \rho(d)_t = \rho(b)_t \pm 1 \ \in \mathbb{F}_2.$$

With $\nu_1 := (0,\ldots,0,1,0,\ldots,0,1,0,\ldots,0)$ (which is zero in all positions except in the positions a_{s_0} and b_{s_0}), we have $\rho(c), \rho(d) \in (\nu_0+\nu_1)+C$. It follows that $c, d \in \rho^{-1}((\nu_0+\nu_1)+C)$.
Step 2.3: The statement follows by induction for arbitrary $z \in Z$. ◇

If $C = \{(0,\ldots,0)\}$, then $\mathcal{P}$ equals the parity partition of N. Optimising the dimension of the linear code C is strongly connected to an optimisation of the width of the join-meet partition $\mathcal{P}$. In Subsection 6.5.3, we have outlined ways to optimise the dimension of a linear code with respect to its minimum distance.

One might ask whether the parity function is still a splitting function for $\mathcal{P}$. The next example, however, shows that this does not seem to be the case in general. In this respect, the question is still open at the moment whether there exists a splitting function for $\mathcal{P}$, so that $\mathcal{P}$ could remain a candidate for further investigations.

Example. In this example, we deal with the case where $n = 4$. Let us consider the code $C := \{(0,0,0,0),(1,1,1,1)\}$ in $\mathbb{F}_2^4$. Let $\mathcal{P}$ be the partition based on C. The minimum distance of C is 4 and the elements of $\mathcal{C}$ other than C are

$$\begin{aligned}
C_1 &:= \{(1,1,0,0),(0,0,1,1)\},\\
C_2 &:= \{(1,0,1,0),(0,1,0,1)\},\\
C_3 &:= \{(1,0,0,1),(0,1,1,0)\},\\
C_4 &:= \{(1,0,0,0),(0,1,1,1)\},\\
C_5 &:= \{(0,1,0,0),(1,0,1,1)\},\\
C_6 &:= \{(0,0,1,0),(1,1,0,1)\} \text{ and}\\
C_7 &:= \{(0,0,0,1),(1,1,1,0)\}.
\end{aligned}$$

(i) We show that the parity function is no splitting function for $\mathcal{P}$ in the case $r = 2$. To see this, let $a := 1\,4$ and $b := 2\,3$, which are in the same set, $\rho^{-1}(C_3)$. The equivalence class $[(a, b)]$ equals $\{(a, b), (c, d)\}$ with $c := 1\,3$ and $d := 2\,4$. We have $\mathrm{sig}(a, b) = \mathrm{sig}(c, d) = 1$, that is, the parity function s_P is no splitting function for $\mathcal{P}$.

(ii) We show that the parity function is no splitting function for $\mathcal{P}$ in the case $r = 3$. To see this, let $a := 3\,1\,3$ and $b := 4\,3\,2$, which are in the same set, $\rho^{-1}(C_4)$. The equivalence class $[(a, b)]$ equals

$$\{(3\,1\,3,\ 4\,3\,2),\ (3\,3\,2,\ 4\,1\,3),\ (3\,3\,3,\ 4\,1\,2),\ (3\,1\,2,\ 4\,3\,3)\}.$$

The function sig is constant on $[(a, b)]$, so that s_P is no splitting function for $\mathcal{P}$. We note that there is an interesting relation to the design partition from Example 7.3.5.II, since a and b are in the same design part $T_{1,3}$.

Chapter 9

THETA BODIES FOR SEPARABLE STATES

In this chapter we show that the theta body method can be applied to the set of all separable states. This offers the possibility of using sos polynomials as an entanglement measure. To do this, we show that the set of all pure separable states is a variety, see Theorem 9.2.2. A discussion will follow in Chapter 10.

9.1 Entanglement

In this section, we briefly introduce the concept of entanglement along the mathematical description in [Aud].

9.1.1 Pure States, Mixes States and Compound Systems

A pure state in a quantum system refers to a specific preparation for the system. The mathematical description of the pure states are the unit vectors in a complex Hilbert space. In what follows, we assume that the Hilbert space is finite-dimensional. The dimension equals the maximal number of states of the quantum system which can be distinguished by a single measurement. A pure state can be identified with an operator on the corresponding Hilbert space as follows:

Formally, a quantum system is characterised by a complex Hilbert space $\mathcal{H}$ of dimension n, that is, by $\mathbb{C}^n$. A *pure state* is a unit vector in $\mathcal{H}$. The set of all linear operators $\mathcal{H} \to \mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$. A pure state $v \in (\mathcal{H})_1$ can be identified with the orthogonal projection $P_v \in \mathcal{L}(\mathcal{H})$ on the linear subspace spanned by v.

A mixed state is physically realised by the preparation of a quantum system in dependence of several preparations which appear with a fixed probability.

Formally, a convex combination of pure states, regarded as operators in $\mathcal{L}(\mathcal{H})$, is called a *mixed state* or a *state* on $\mathcal{H}$. In this respect, the set $\mathfrak{S}(\mathcal{H})$ of all states, the *state space*, is a convex set.

A compound system describes the composition of several particles or partial systems. Formally, it can be characterised by their tensor product. In this respect, each factor of the tensor product relates to a partial system. Hence, the understanding of compound systems is closely related to the understanding of tensor products.

Formally, the compound system of two quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$ is characterised by the tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$ with the Hilbert-Schmidt norm.

9.1.2 The State Space

Fixing an orthonormal basis $e_1, \dots, e_n$ of $\mathcal{H}$, the dual Hilbert space $\mathcal{H}^\star$ is isomorphic to $\mathcal{H}$, via $\langle \cdot, w\rangle \mapsto \overline{w} = \sum_{i=1}^n \overline{w_i} \cdot e_i$ for all $w = \sum_{i=1}^n w_i \cdot e_i \in \mathcal{H}$, where $w_i \in \mathbb{C}$. (Likewise, $\mathcal{H}^\star$ is isomorphic to the conjugated Hilbert space $\overline{\mathcal{H}}$, via $\langle \cdot, w\rangle \mapsto w$.)

Now, $\mathcal{L}(\mathcal{H})$ is isomorphic to $\mathcal{H} \otimes \mathcal{H}$ and to the matrix space $\mathcal{M}_n(\mathbb{C})$ via $\langle \cdot, w\rangle \cdot v \mapsto v \otimes \overline{w} \mapsto v \cdot \overline{w}^t$ for all $v, w \in \mathcal{H}$. The image of a state on $\mathcal{H}$ is called its *density matrix*.

As usual, the *trace* on $\mathcal{L}(\mathcal{H})$ is defined by

$$\mathrm{tr}\colon \mathcal{L}(\mathcal{H}) \to \mathbb{C}, \ \langle \cdot, w\rangle \cdot v \mapsto \langle v, w\rangle \,.$$

Let $v \in \mathcal{H}$ be a unit vector. The pure state P_v is identified with the tensor $v \otimes \overline{v}$ (and with the matrix $v \cdot \overline{v}^t$), which has Hilbert-Schmidt norm 1. With the Schmidt decomposition, the state space $\mathfrak{S}(\mathcal{H})$ equals the set of all positive operators (which correspond to the positive semidefinite matrices) in $\mathcal{L}(\mathcal{H})$ with trace 1.

Hence, $\mathfrak{S}(\mathcal{H})$ is contained in the Hilbert-Schmidt unit ball. This implies that the extreme points of $\mathfrak{S}(\mathcal{H})$ are given by the pure states, that is, $\mathrm{ext}(\mathfrak{S}(\mathcal{H})) = \{P_v \colon v \in (\mathcal{H})_1\}$.

Finally, we would like to point out that states can also be defined as linear functionals. This is often the case in the literature.

To do so, we identify the operator $A \in \mathcal{L}(\mathcal{H})$ with the linear functional $\varphi_A \colon \mathcal{L}(\mathcal{H}) \to \mathbb{C}$, $B \mapsto \mathrm{tr}(A^\star \cdot B)$. Considering $\mathcal{L}(\mathcal{H})$ as the Hilbert space $(\mathcal{H} \otimes \mathcal{H}, \langle \cdot, \cdot \rangle_{\mathrm{HS}})$, it follows from the Riesz representation theorem that $\mathcal{L}(\mathcal{H})$ can be identified with $\mathcal{L}(\mathcal{H})^\star$ via $A \mapsto \varphi_A$.

Now, we have $\mathrm{tr}(A) = 1$ if and only if $\varphi_A(\mathbb{1}_n) = 1$. A linear functional on $\mathcal{L}(\mathcal{H})$ is called *positive*, if it maps positive operators on non-negative real numbers. A short calculation shows that the functional corresponding to a pure state induced by $v \in (\mathcal{H})_1$ equals $\varphi_{P_v} \colon B \mapsto \langle B(v), v\rangle$, which is positive. Also, we have $\varphi_{P_v}(\mathbb{1}_n) = 1$. Indeed, the states correspond to the positive linear functionals which assign the identity $\mathbb{1}_n$ to 1, see [Mur, Example 5.1.1] for the converse statement. For instance, the linear functional $\varphi_{\frac{1}{n}\mathbb{1}_n}$ corresponds to a state.

9.1.3 Separable States

From now on, let $\mathcal{H} := \mathcal{H}_1 \otimes \mathcal{H}_2$, where $\mathcal{H}_1$ and $\mathcal{H}_2$ are complex Hilbert spaces of dimension m and n, respectively. In terms of tensor products, $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is isomorphic to $V := \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$, such that the pure states on $\mathcal{H}$ correspond to the vectors $v \otimes \overline{v}$, $v \in (\mathcal{H})_1$, under the R-C-unfolding of V with $R := \{1, 3\}$ and $C := \{2, 4\}$.

A state A on $\mathcal{H}$ is called a *product state*, if it is a product vector under the R-C-unfolding of V with $R := \{1, 2\}$, $C := \{3, 4\}$ and each factor is a state (that is, if $A = A_1 \otimes A_2$ where A_1 and A_2 are states on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively). In this case, A can be identified with the functional $\varphi_A =: \varphi_{A_1} \otimes \varphi_{A_2}$, where

$$\varphi_A \colon V \to \mathbb{C},\ v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \mapsto \varphi_{A_1}(v_1 \otimes \overline{v_2}) \cdot \varphi_{A_2}(w_1 \otimes \overline{w_2}).$$

A state on $\mathcal{H}$ is called *separable*, if it lies in the convex hull of the product states in the space $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$. Otherwise, it is called *entangled*. The states which are pure and separable are called the *pure separable* states. We denote the set of all separable states by $\mathcal{S}$, the set of all entangled states by $\mathcal{S}^c$ and the set of all pure separable states by $\mathcal{S}_{\text{pure}}$.

In our context, an *entanglement witness* is the real part of an affine functional on $\mathcal{L}(\mathcal{H})$ which separates an entangled state from the set $\mathcal{S}$ of all separable states. In this respect, an entanglement witness provides a sufficient criterion for entanglement.

9.1.4 Partial Traces

The maps

$$\begin{aligned}
\operatorname{tr}_1 &\colon V \to \mathcal{L}(\mathcal{H}_2),\ v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \mapsto \langle v_1, v_2 \rangle \cdot w_1 \otimes \overline{w_2}, \\
\operatorname{tr}_2 &\colon V \to \mathcal{L}(\mathcal{H}_1),\ v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \mapsto \langle w_1, w_2 \rangle \cdot v_1 \otimes \overline{v_2}
\end{aligned}$$

are called *partial traces* on V. Partial traces appear as so-called tensor contractions in the literature on tensor networks or differential geometry (see, for example, [Eis] or [Lee]). The trace on $\mathcal{L}(\mathcal{H})$ can also be obtained with the partial trace, that is, $\operatorname{tr} = \operatorname{tr}^2 \circ \operatorname{tr}_1 = \operatorname{tr}^1 \circ \operatorname{tr}_2$, where tr^1 and tr^2 denote the traces on $\mathcal{L}(\mathcal{H}_1)$ or $\mathcal{L}(\mathcal{H}_2)$, respectively, see also [Aud, 7.2.2]:

$$\operatorname{tr} \colon V \to \mathbb{C},\ v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \mapsto \langle v_1, v_2 \rangle \cdot \langle w_1, w_2 \rangle\,.$$

9.1.5 Pure Separable States

The following statement can be found in [Aud, 8.1.3]. Compare also with Theorem 3.4.4.

Proposition. The pure separable states on $\mathcal{H}$ are given by the states of the form $A_1 \otimes A_2$, where A_1 and A_2 are pure states on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. That is, $\mathcal{S}_{\text{pure}} = \{v \otimes \overline{v} \otimes w \otimes \overline{w} \colon v \in (\mathcal{H}_1)_1, w \in (\mathcal{H}_2)_1\}$.

Proof. Let A be a state on $\mathcal{H}$ which is pure and separable. On the one hand, it follows from the Schmidt decomposition and from the assumption that A is a pure state that there exist $\lambda_1, \dots, \lambda_{n_1} > 0$ with $\sum_{i=1}^{n_1} \lambda_i^2 = 1$ and orthonormal systems $(v_i)_{i=1}^{n_1}$ in $\mathcal{H}_1$, $(w_i)_{i=1}^{n_1}$ in $\mathcal{H}_2$ such that

$$A = \sum_{i=1}^{n_1} \sum_{j=1}^{n_1} \lambda_i \lambda_j \cdot v_i \otimes \overline{v_j} \otimes w_i \otimes \overline{w_j}. \tag{9.1}$$

On the other hand, since A is separable (and pure!), there exist states $A_1 \in \mathcal{L}(\mathcal{H}_1)$, $A_2 \in \mathcal{L}(\mathcal{H}_2)$ with $A = A_1 \otimes A_2$. Now, we have

$$\operatorname{tr}_1(A) = \sum_{j=1}^{n_1} \lambda_j^2 \, w_j \otimes \overline{w_j} = A_2,$$

$$\operatorname{tr}_2(A) = \sum_{i=1}^{n_1} \lambda_i^2 \, v_i \otimes \overline{v_i} = A_1.$$

Hence, A has the form

$$A = \sum_{i=1}^{n_1} \sum_{j=1}^{n_1} \lambda_i^2 \lambda_j^2 \cdot v_i \otimes \overline{v_i} \otimes w_j \otimes \overline{w_j}.$$

A comparison with equation (9.1) leads to $\overline{v_j} \otimes w_i = \lambda_i \lambda_j \, \overline{v_i} \otimes w_j$ for all $i, j \in \{1, \dots, n_1\}$, which implies $n_1 = 1$ and $\lambda_1^2 = 1$. This yields $A = v_1 \otimes \overline{v_1} \otimes w_1 \otimes \overline{w_1}$. ◇

A separable state on $\mathcal{H}_1 \otimes \mathcal{H}_2$ is a convex combination of pure separable states, since every state on $\mathcal{H}_1$ (and on $\mathcal{H}_2$) is a convex combination of pure states. Since the pure separable states have Hilbert Schmidt norm 1 and the separable states are contained in the Hilbert Schmidt unit ball, it follows that the extreme points of the separable states are given by the pure separable states.

With the previous proposition, a pure state $P_{A_0} \in V$ is separable if and only if the unit vector $A_0 \in \mathcal{H}_1 \otimes \mathcal{H}_2$ is a product vector. This observation gives rise to a definition of separability in $\mathcal{H}_1 \otimes \mathcal{H}_2$: A unit vector in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is called *separable*, if it is a product vector. Otherwise, it is called *entangled*. See also Subsection 3.6.2.

The trace on $\mathcal{L}(\mathcal{H})$ provides a simple test whether a unit product vector is separable:

Proposition. A unit product vector $v \in V$ is a pure separable state if and only if $\operatorname{tr}(v) = 1$.

Proof. Let $v = v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \in V$ be a unit product vector where $v_1, v_2 \in (\mathcal{H}_1)_1$ and $w_1, w_2 \in (\mathcal{H}_2)_1$. Then $\operatorname{tr}(v) = \langle v_1, v_2 \rangle \langle w_1, w_2 \rangle$.

At first, let $v_2 = v_1$ and $w_2 = w_1$, so that v is a pure separable state. Then we have $\operatorname{tr}(v) = 1$.

Now, let $\operatorname{tr}(v) = 1$. Since $|\langle v_1, v_2 \rangle| \leqslant 1$ and $|\langle w_1, w_2 \rangle| \leqslant 1$, we have $1 = \operatorname{tr}(v) = |\langle v_1, v_2 \rangle| = |\langle w_1, w_2 \rangle|$, that is, there exist $\lambda, \mu \in \mathbb{C}_1$ with $v_2 = \lambda v_1$ and $w_2 = \mu w_1$. Now, we have $1 = \operatorname{tr}(v) = \overline{\lambda \mu}$ so that $v = v_1 \otimes \overline{v_1} \otimes w_1 \otimes \overline{w_1}$, which is a pure separable state. ◇

9.1.6 Summary

Table 9.1 on page 275 summarises the physical concepts together with their mathematical description.

9.2 Pure Separable States as a Variety

In this section, we show that the pure separable states are a real affine variety. Hence, the separable states are the convex hull of a variety, which allows us to apply the theta body method on the separable states.

As above, let $\mathcal{H}_1$ and $\mathcal{H}_2$ be Hilbert spaces of dimension m and n, respectively, and let $V := \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$.

According to Chapter 3, the tensor product V can be identified with the real or complex affine space $\mathbb{C}^N$, where $N = \{1, \ldots, m\}^2 \times \{1, \ldots, n\}^2$ are the indexing tuples of V. In particular, for all $v_s = (v_{s,1}, \ldots, v_{s,m}) \in \mathcal{H}_1$ and for all $w_s = (w_{s,1}, \ldots, w_{s,n}) \in \mathcal{H}_2$, $s \in \{1, 2\}$,

Quantum system	Complex Hilbert space $\mathcal{H}$ (here: finite-dimensional)
Pure states	Unit vectors $v \in \mathcal{H}$ Projections $P_v \in \mathcal{L}(\mathcal{H})$ of rank 1 Tensors $v \otimes \overline{v}$ Extreme points of $\mathfrak{S}(\mathcal{H})$
State space $\mathfrak{S}(\mathcal{H})$	Convex hull of pure states Positive operators in $\mathcal{L}(\mathcal{H})$ with trace 1
Compound of two quantum systems $\mathcal{H}_1$, $\mathcal{H}_2$	Tensor product $\mathcal{H}_1 \otimes \mathcal{H}_2$
Product state	State of the form $A_1 \otimes A_2$, where A_1, A_2 are states on $\mathcal{H}_1$, $\mathcal{H}_2$
Separable states $\mathcal{S}$	Convex hull of the product states
Entangled states $\mathcal{S}^c$	States which are not separable
Pure separable states $\mathcal{S}_{\text{pure}}$	States of the form $A_1 \otimes A_2$, where A_1, A_2 are pure states Tensors $v \otimes \overline{v} \otimes w \otimes \overline{w}$, where $v \in \mathcal{H}_1$, $w \in \mathcal{H}_2$ are unit vectors Extreme points of $\mathcal{S}$ Unit product vectors with trace 1

Table 9.1: Physical concepts and mathematical analogy.

the product vector $v_1 \otimes \overline{v_2} \otimes w_1 \otimes \overline{w_2} \in V$ is identified with the multi matrix $(v_{1,i}\,\overline{v_{2,j}}\,w_{1,k}\,\overline{w_{2,l}})_{(i,j,k,l)\in N} \in \mathbb{C}^N$.

The polynomials in $\mathbb{C}[\,x_a \colon a \in N]$ can be regarded as functionals on the complex affine space $\mathbb{C}^N$. We recall that $\mathbb{C}^N$ can also be regarded as the real affine space $\mathbb{R}^{N_\mathbb{C}}$, where $N_\mathbb{C} = N \times \{1, 2\}$, see Section 3.5. We also recall that $\mathcal{H}_{N_\mathbb{C}}$ are the complex Hibi relations in $\mathbb{R}[x_a \colon a \in N_\mathbb{C}]$ and $\mathcal{N}_{N_\mathbb{C}} = \{u_{N_\mathbb{C}}\}$, where $u_{N_\mathbb{C}}$ is the complex norming polynomial.

9.2.1 The Trace Functional

Now, we consider the following polynomial in $\mathbb{C}[\,x_a \colon a \in N]$:

$$t_{N_\mathbb{C}} := 1 - \sum_{k=1}^{m} \sum_{l=1}^{n} x_{k\,k\,l\,l}.$$

We call it the *trace functional*. It defines an affine hyperplane $H_{\mathrm{tr}} := \mathcal{Z}_\mathbb{C}(t_{N_\mathbb{C}})$ in V.

Proposition. The trace functional equals $1 - \mathrm{tr}$.

Proof. Let $k, i \in \{1, \dots, m\}$ and $l, j \in \{1, \dots, n\}$, and $v := e_k \otimes e_i \otimes e_l \otimes e_j \in V$. Now, we obtain

$$\begin{aligned}\Big(\sum_{k=1}^{m} \sum_{l=1}^{n} x_{k\,k\,l\,l}\Big)(v) &= \begin{cases} 0, & k \neq i \text{ or } l \neq j, \\ 1, & k = i \text{ and } l = j \end{cases} \\ &= \langle e_k, e_i\rangle\,\langle e_l, e_j\rangle = \mathrm{tr}(v),\end{aligned}$$

that is, $v \in H_{\mathrm{tr}}$ if and only if v has trace 1. ◇

The real and the imaginary part of the trace functional are polynomials in $\mathbb{R}[x_a \colon a \in N_\mathbb{C}]$, given by

$$\mathrm{Re}(t_{N_\mathbb{C}}) = 1 - \sum_{k=1}^{m} \sum_{l=1}^{n} x_{k\,k\,l\,l,\,1}\,,$$

$$\mathrm{Im}(t_{N_\mathbb{C}}) = \sum_{k=1}^{m} \sum_{l=1}^{n} x_{k\,k\,l\,l,\,2}\,.$$

Let $\mathcal{T}_{N_\mathbb{C}} := \{\mathrm{Re}(t_{N_\mathbb{C}}), \mathrm{Im}(t_{N_\mathbb{C}})\}$. Now, in the real picture, Theorem 2.2.5 yields $\imath(H_{\mathrm{tr}}) = \mathcal{Z}_\mathbb{R}(\mathcal{T}_{N_\mathbb{C}})$.

9.2.2 Pure Separable States as a Variety

Let $\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}$ be the ideal which is generated by $\mathcal{H}_{N_{\mathbb{C}}}$, $\mathcal{N}_{N_{\mathbb{C}}}$ and $\mathcal{T}_{N_{\mathbb{C}}}$.

We may consider V as a tensor product with four factors and the projective unit ball $\mathcal{B}_{1,\pi}$ in V, whose extreme points are the unit product vectors. Together with Proposition 9.1.5, we find the following result:

Theorem. (*Pure Separable States as a Variety*)
In the real picture, the pure separable states equal the set of zeros of the Hibi relations, the norming polynomial and the real and imaginary part of the trace functional, that is,

$$\mathcal{S}_{\mathrm{pure}} = \imath^{-1}(\mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{N_{\mathbb{C}}} \cup \mathcal{N}_{N_{\mathbb{C}}} \cup \mathcal{T}_{N_{\mathbb{C}}})) = \imath^{-1}(\mathcal{Z}_{\mathbb{R}}(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}})).$$

Consequently, we have $\mathcal{S} = \mathrm{co}(\mathcal{Z}_{\mathbb{R}}(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}))$, that is, the separable states are the convex hull of a variety.

Proof. In the real picture, the unit product vectors are a variety, induced by the complex Hibi relations $\mathcal{H}_{N_{\mathbb{C}}}$ and the norming polynomial $u_{N_{\mathbb{C}}}$, see the Criterion for Unit Product Vectors Theorem 3.5.3.

Now, let $v \in V$ be a unit vector. Proposition 9.1.5 says that $v \in \mathcal{S}_{\mathrm{pure}}$ if and only if $v \in H_{\mathrm{tr}}$ and v is a product vector, which yields

$$\begin{aligned}\imath(\mathcal{S}_{\mathrm{pure}}) &= \imath(H_{\mathrm{tr}} \cap \mathcal{P}_V)_1 = \imath(H_{\mathrm{tr}}) \cap \imath(\mathcal{E}_V) \\ &= \mathcal{Z}_{\mathbb{R}}(\mathcal{T}_{N_{\mathbb{C}}}) \cap \mathcal{Z}_{\mathbb{R}}(\mathcal{H}_{N_{\mathbb{C}}} \cup \mathcal{N}_{N_{\mathbb{C}}}) \\ &= \mathcal{Z}_{\mathbb{R}}(\mathcal{T}_{N_{\mathbb{C}}} \cup \mathcal{H}_{N_{\mathbb{C}}} \cup \mathcal{N}_{N_{\mathbb{C}}}) = \mathcal{Z}_{\mathbb{R}}(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}).\end{aligned}$$

Since $\imath$ preserves convexity, we obtain $\imath(\mathcal{S}) = \mathrm{co}(\mathcal{Z}_{\mathbb{R}}(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}))$. ◇

Corollary. The complex theta bodies of $\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}$ converge against $\mathcal{S}$.

Proof. This follows directly from Theorem 2.5.5, since $\mathcal{S}_{\mathrm{pure}}$ is compact, and since $\mathcal{T}_k^{\mathbb{C}}(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}) = \imath^{-1}(\mathcal{T}_k(\mathcal{I}_{\mathrm{tr},N_{\mathbb{C}}}))$. ◇

Figure 9.1 represents the projective unit ball $\mathcal{B}_{1,\pi}$ (yellow octahedron), the separable states $\mathcal{S}$ (green triangle), the entangled states $\mathcal{S}^c$ (red triangles) in V by solids in the three-dimensional real Euclidean space with coordinates x, y and z. The extreme points of $\mathcal{B}_{1,\pi}$, of the state space and of $\mathcal{S}$ are represented by coloured spots. The

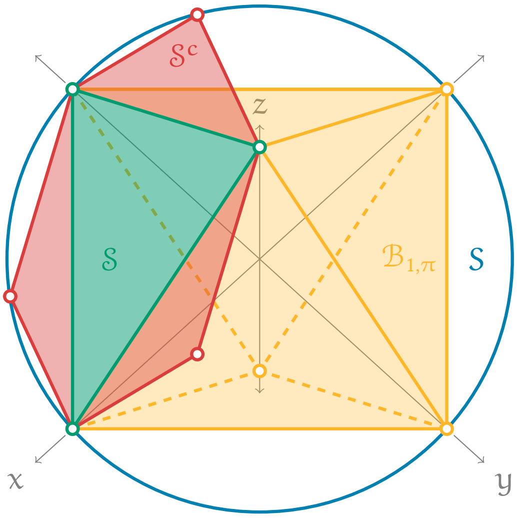


Figure 9.1: The projective unit ball and separable states.

(two-dimensional) Euclidean unit sphere S is represented by a (one-dimensional) blue circle. We see that the unit product vectors are represented by the spots which are yellow or green, the pure states by the spots which are red or green, and the pure separable states by the spots which are green.

The picture shows the following aspects:

- The state space (the red and green hexagon) lies in the affine hyperplane H_{tr}, which is induced by the trace.
- A unit product vector is a pure separable state if and only if it lies in H_{tr}.
- The separable states are the convex hull of the pure separable states.
- The projective unit sphere is absorbing.

The analogy with this picture is limited. Indeed, it is not easy to understand the geometry of the state space, so a three-dimensional picture can only consider a few aspects. For instance, the geometry of the separable states is not considered here.

A summary and a discussion follow in Section 10.3.

Chapter 10

SUMMARY AND DISCUSSION

This chapter is a summary of the results of this thesis which are related to the projective tensor norm and to the separable states. We also define some new notions and make suggestions for further research.

Section 10.1 deals with real tensor products. The design hyperplanes, skip hyperplanes and parity hyperplanes from Chapter 7 and Chapter 8 are explicit witnesses for the projective unit ball. In some special cases, the projective norm maximisation can be completely solved. We can therefore identify maximal vectors and thus obtain the inner radius of the projective unit ball. In all other cases we obtain a class of vectors with projective norm 1 and thus upper bounds on the inner radius of the projective unit ball.

To determine the projective norm for several classes of vectors we have seen some approaches to generalise the Schmidt decomposition such as the gsd-decomposition. In the end of Section 10.1, we introduce new decompositions based on the design hyperplanes, the skip hyperplanes and the parity hyperplanes, the *design decomposition*, the *skip decomposition* and the *parity decomposition*. Indeed, provided that a vector is decomposable, the projective norm can be obtained from the decomposition.

Section 10.2 deals with the results for the projective unit ball in complex tensor products which can be found in Chapter 6.

Section 10.3 deals with the results for separable states according to Chapter 9.

In this chapter we deal also with open questions and ideas for further investigations. For instance, the results are mainly based on the first theta body so that we discuss approaches to address also higher theta bodies. The discussions of the real case apply also to the complex case and to the results for separable states.

We point out that this summary deals only with the projective norm and the separable states. Further results of this thesis can also be mentioned in this context but are actually not the main subject of this summary.

Let $n \geqslant 2$ and $V_{\mathbb{K}} := \mathbb{K}^n \otimes \cdots \otimes \mathbb{K}^n$ with $r \geqslant 2$ tensor factors.

10.1 The Projective Unit Ball, Real

This section deals with the projective norm on real tensor products. In particular, we find some classes of vectors with projective norm 1 and some bounds on or values for the inner radius of the projective unit ball $\mathcal{B}_{1,\pi}$.

To do this, we summarise the results related to the design hyperplanes, skip hyperplanes and parity hyperplanes, followed by the definitions of the design decomposition, skip decomposition and parity decomposition.

Afterwards, we address some open questions and discuss ideas for further investigations.

10.1.1 Our Previous State of Knowledge

The inner radius of and maximal vectors for $\mathcal{B}_{1,\pi}$ in real tensor products were already known in the bipartite case (that is, $r = 2$) and in the tripartite case $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$ (that is, $n = 2$ and $r = 3$) due to the Schmidt decomposition, Theorem 3.3.4 and [Wie]. In all other cases, the inner radius does not seem to be known so far. However, a lower bound is given by the Arveson bound $\operatorname{Arv}(V_{\mathbb{R}}) = \sqrt{1/m_{\text{Arveson}}}$, where $m_{\text{Arveson}} := n^{r-1}$, see Theorem 3.3.4.

10.1.2 Design Hyperplanes

In the case where $n \in \{2, 4, 8\}$ the theta body method can be used to obtain explicit witnesses for the projective unit ball $\mathcal{B}_{1,\pi}$ in $V_{\mathbb{R}}$ based on latin squares and orthogonal designs, the design hyperplanes.

Let $m_{\text{Design}} := n^{r-1}$ denote the length of a design part. Since the design parts have equal length, this is also the relative size of the design partition. The support vector y with respect to a design part T_D and a corresponding design function s_D has the form

$$y = \frac{1}{n^{r-1}} \sum_{a \in T_D} s_D(a) \cdot e_a.$$

It is a scaled maximal vector for $\mathcal{B}_{1,\pi}$ and satisfies $\|y\|_\pi = 1$, see Theorem 7.3.4 and Corollary 7.3.4. The (Euclidean) length of y is given by $\|y\| = \sqrt{1/m_{\text{Design}}}$.

In summary, we obtain a class of maximal vectors and therefore the inner radius of $\mathcal{B}_{1,\pi}$, given by $r(\mathcal{B}_{1,\pi}) = \sqrt{1/m_{\text{Design}}}$. This solves the projective norm maximisation in $V_{\mathbb{R}}$, $n \in \{2, 4, 8\}$.

We have discussed in Subsection 7.3.6 whether latin squares and orthogonal designs can be used to obtain witnesses for the projective unit ball also in the case where $n > 8$.

Table 10.1 on page 283 gives some examples for design hyperplanes, given by their support vectors.

10.1.3 Skip Hyperplanes

In the case where $n \in \{3, 5, 6, 7\}$ the theta body method can be used to obtain explicit witnesses for the projective unit ball $\mathcal{B}_{1,\pi}$ in $V_{\mathbb{R}}$, the skip hyperplanes.

On the basis of the design hyperplanes we obtain a class of vectors with projective norm 1 and thus obtain an explicit upper bound on the inner radius, the skip bound $\text{Skip}(V_{\mathbb{R}}) = \sqrt{1/m_{\text{Skip}}}$, where m_{Skip} denotes the relative size of the skip partition, see Theorem 7.4.2 and Corollary 7.4.3.

10.1.4 Parity Hyperplanes

In the case where $n \geqslant 2$ the theta body method can be used to obtain explicit witnesses for the projective unit ball $\mathcal{B}_{1,\pi}$ in $V_{\mathbb{R}}$, the parity hyperplanes.

The support vector y with respect to a parity hyperplane T_P and the parity function s_P has the form

$$y = \frac{1}{\#T_P} \sum_{a \in T_P} s_P(a) \cdot e_a.$$

It satisfies $\|y\|_\pi = 1$ due to Theorem 8.3.5 and Corollary 8.3.5.

The length of y equals $\|y\| = \sqrt{1/\#T_P}$. An explicit formula for $\#T_P$ is given by Proposition 8.4.3. We note that the length of y depends on the parity part (in general, the parity parts do not all have the same length). The maximal length is given by the parity bound $\text{Par}(V_{\mathbb{R}}) = \sqrt{1/m_{\text{Parity}}}$, where m_{Parity} denotes the relative size of the parity partition, see Lemma 8.4.4.

The parity bound $\mathrm{Par}(V_{\mathbb{R}})$ is therefore an upper bound on the inner radius of $\mathcal{B}_{1,\pi}$. Theorem 8.4.5 gives an explicit formula for it.

In Subsection 8.4.6 we have discussed some ideas to improve the parity bound.

Table 10.2 on page 283 summarises some values for the parity bound and gives some examples for parity hyperplanes, given by their support vectors.

10.1.5 Values for and Bounds on the Inner Radius

Table 10.3 on page 284 compares the values of m_{Arveson}, m_{Design}, m_{Skip} and m_{Parity} for some small values of n and r.

Table 10.4 on page 285 compares the values of the Arveson bound $\mathrm{Arv}(V_{\mathbb{R}})$, the inner radius $r(\mathcal{B}_{1,\pi})$, the skip bound $\mathrm{Skip}(V_{\mathbb{R}})$ and the parity bound $\mathrm{Par}(V_{\mathbb{R}})$ for some small values of n and r. The best new values for and the new bounds on the inner radius $r(\mathcal{B}_{1,\pi})$ are marked in red. The values which are previously known are marked in grey. In particular, this refers to the values for $r = 2$ since they can be obtained using the Schmidt decomposition and also to the values for $\mathrm{Arv}(V_{\mathbb{R}})$.

We recall that $\mathrm{Arv}(V_{\mathbb{R}})$ is a lower bound on $r(\mathcal{B}_{1,\pi})$ while $\mathrm{Skip}(V_{\mathbb{R}})$ and $\mathrm{Par}(V_{\mathbb{R}})$ are upper bounds on $r(\mathcal{B}_{1,\pi})$.

The table demonstrates that for each approach (design hyperplanes, skip hyperplanes or parity hyperplanes) there are cases where this approach leads to new upper bounds or even to new values on $r(\mathcal{B}_{1,\pi})$.

Tensor product $V_{\mathbb{R}}$	Support vector y	Inner radius $r(\mathcal{B}_{1,\pi})$
$\mathbb{R}^2 \otimes \mathbb{R}^2$	$\frac{1}{2}(e_{11} + e_{22})$	$\sqrt{1/2}$
$\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$	$\frac{1}{4}(e_{111} + e_{122} - e_{212} + e_{221})$	$1/2$
$\mathbb{R}^4 \otimes \mathbb{R}^4 \otimes \mathbb{R}^4$	$\frac{1}{16}\,(e_{111} - e_{122} + e_{212} + e_{221}$ $-e_{234} - e_{133} + e_{313} + e_{331}$ $+e_{243} - e_{144} + e_{414} + e_{441}$ $+e_{324} - e_{342} - e_{423} + e_{432})$	$1/4$
$\mathbb{R}^n \otimes \mathbb{R}^n$ $_{(n \in \{2,4,8\})}$	$\frac{1}{n}\sum_{k=1}^{n} e_{kk}$	$\sqrt{1/n}$
$\bigotimes_{s=1}^{r} \mathbb{R}^2$	$\frac{1}{2^{r-1}}\sum_{a \in T_D} s_D(a) \cdot e_a$	$\sqrt{1/2^{r-1}}$
$\bigotimes_{s=1}^{r} \mathbb{R}^4$	$\frac{1}{4^{r-1}}\sum_{a \in T_D} s_D(a) \cdot e_a$	$\sqrt{1/4^{r-1}}$
$\bigotimes_{s=1}^{r} \mathbb{R}^8$	$\frac{1}{8^{r-1}}\sum_{a \in T_D} s_D(a) \cdot e_a$	$\sqrt{1/8^{r-1}}$

Table 10.1: Values for the inner radius.

Tensor product $V_{\mathbb{R}}$	Support vector y	Parity bound $\mathrm{Par}(V_{\mathbb{R}})$
$\mathbb{R}^2 \otimes \mathbb{R}^2$	$\frac{1}{2}(e_{11} + e_{22})$	$\sqrt{1/2}$
$\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$	$\frac{1}{4}(e_{111} + e_{122} - e_{212} + e_{221})$	$1/2$
$\mathbb{R}^4 \otimes \mathbb{R}^4 \otimes \mathbb{R}^4$	$\frac{1}{10}\,(e_{111} + e_{122} - e_{212} + e_{221}$ $e_{133} - e_{313} + e_{331}$ $e_{144} - e_{414} + e_{441})$	$\sqrt{1/10}$
$\mathbb{R}^n \otimes \mathbb{R}^n$	$\frac{1}{n}\sum_{k=1}^{n} e_{kk}$	$\sqrt{1/n}$
$\mathbb{R}^n \otimes \mathbb{R}^n \otimes \mathbb{R}^n$	$\frac{1}{3n-2}\Big(e_{111} +$ $\sum_{k=2}^{n}(e_{1kk} - e_{k1k} + e_{kk1})\Big)$	$\sqrt{1/(3n-2)}$
$\bigotimes_{s=1}^{r} \mathbb{R}^n$	$\frac{1}{\#T_P}\sum_{a \in T_P} s_P(a) \cdot e_a$	$\sqrt{1/m_{\mathrm{Parity}}}$

Table 10.2: The parity bound.

n	r	$\dim(V_{\mathbb{R}})$	m_{Arveson}	m_{Design}	m_{Skip}	m_{Parity}
2	2	4	2	2	—	2
2	4	16	8	8	—	8
2	6	64	32	32	—	32
3	2	9	3	—	3	3
3	4	81	27	—	21	21
3	6	729	243	—	183	183
4	2	16	4	4	—	4
4	4	256	64	64	—	40
4	6	4096	1024	1024	—	544
6	2	36	6	—	6	6
6	4	1296	216	—	168	96
6	6	46656	7776	—	5856	2256
8	2	64	8	8	—	8
8	4	4096	512	512	—	176
8	6	262144	32768	32768	—	5888
10	2	100	10	—	—	10
10	4	10000	1000	—	—	280
10	6	1000000	100000	—	—	12160

Table 10.3: Relative sizes design, parity and skip partition.

n	r	$\mathrm{Arv}(V_{\mathbb{R}})$	$r(\mathcal{B}_{1,\pi})$	$\mathrm{Skip}(V_{\mathbb{R}})$	$\mathrm{Par}(V_{\mathbb{R}})$
2	2	0.7071	0.7071		0.7071
2	4	0.3536	**0.3536**		**0.3536**
2	6	0.1768	**0.1768**		**0.1768**
3	2	0.5774	0.5774	0.5774	0.5774
3	4	0.1925		**0.2182**	**0.2182**
3	6	0.0642		**0.0739**	**0.0739**
4	2	0.5000	0.5000		0.5000
4	4	0.1250	**0.1250**		0.1581
4	6	0.0313	**0.0313**		0.0429
6	2	0.4082	0.4082	0.4082	0.4082
6	4	0.0680		**0.0772**	0.1021
6	6	0.0113		**0.0131**	0.0211
8	2	0.3536	0.3536		0.3536
8	4	0.0442	**0.0442**		0.0754
8	6	0.0055	**0.0055**		0.0130
10	2	0.3162	0.3162		0.3162
10	4	0.0316			**0.0598**
10	6	0.0032			**0.0091**

Table 10.4: Some new bounds on and values for the inner radius.

10.1.6 The Design, Skip and Parity Decompositions

Let T be a design part, skip part or parity part and let s be the design function, skip function or parity function, respectively. The support vector y of the corresponding design hyperplane (or skip hyperplane or parity hyperplane, respectively) induced by T has the form

$$y = \frac{1}{\#T} \sum_{a \in T} s(a) \cdot e_a.$$

Now, y lies in an exposed face F of $\mathcal{B}_{1,\pi}$ given by $F = \mathcal{B}_{1,\pi} \cap P_{l_y}$. If T is a design part, this face is also maximal, see Theorem 2.4.7. We consider the subset $F_0 := F_0(y) := \mathrm{co}(\{s(a) \cdot e_a \colon a \in T\})$ of F.

Definition. A vector $z \in V$ is called *design decomposable* (or *skip decomposable* or *parity decomposable*), if there exists a design hyperplane (or a skip hyperplane or a parity hyperplane, respectively) with support vector y, a symmetry $U \in \mathrm{Sym}_V(\mathcal{B}_{1,\pi})$ and $\mu \in \mathbb{R}$ such that $U(z) \in \mu \cdot F_0(y)$.

The projective norm of a vector which is design, skip or parity decomposable can now be obtained as follows:

Corollary. If z is design, skip or parity decomposable, then $\|z\|_\pi = |\mu|$.

Proof. See Corollary 7.3.4, Corollary 7.4.3 and Corollary 8.3.5. ◇

In this case, there exists $\lambda_a \in [0, 1]$ with $\sum_{a \in T} \lambda_a = 1$ such that z has the form

$$z = \sum_{a \in T} \underbrace{\big(s(a) \cdot \mu \cdot \lambda_a\big)}_{=: \delta_a} \cdot U^{-1}(e_a).$$

The numbers $|\delta_a|$, $a \in T$, are called the *design coefficients* (or *skip coefficients* or *parity coefficients*, respectively) of z.

With regard to the symmetry group $\mathrm{Sym}_V(\mathcal{B}_{1,\pi})$, we refer to Proposition 3.3.5.

Now, we discuss whether the design, skip and parity decompositions can be regarded as a generalisation of the Schmidt decomposition.

Example. In this example, we consider the bipartite case where $V = \mathbb{R}^n \otimes \mathbb{R}^n$. One can easily verify that the Schmidt coefficients are equal to the parity coefficients with respect to $y := \frac{1}{n}(e_{11} + \cdots + e_{nn})$, since $T := \{1\,1,\ \ldots,\ n\,n\}$ is a parity part (it can be easily verified analogous to Example 7.3.5.II and Example 7.3.5.III that T is also a design part in the case where $n \in \{2, 4, 8\}$).

Remark. For a dicussion on the decompositions, it can be helpful to consider the following questions. Let $z_0, z \in V_{\mathbb{R}}$. Let z_0 be design decomposable (or skip / parity decomposable, respectively).

(i) It is an open question whether the design coefficients (or skip / parity coefficients) of z_0, in ascending order, are unique.

(ii) It is an open question how the design coefficients (or skip / parity coefficients) of z_0 depend on the choice of the design hyperplane (or skip / parity hyperplane, respectively).

(iii) Of course, we have $\|z\|_\pi = |\mu|$ also in the case where there exists $U \in \mathrm{Sym}_V(\mathcal{B}_{1,\pi})$ and $\mu \in \mathbb{R}$ such that $U(z) \in \mu \cdot F$. However, it is an open question whether $F \subseteq \mathrm{Sym}_{V_{\mathbb{R}}}(\mathcal{B}_{1,\pi})(F_0)$. It might be interesting to see which aspects of Theorem 3.3.8 also hold in the multipartite case.

10.1.7 Discussion on the Geometry of the Projective Unit Ball

Here we address some open questions about the geometry of the projective unit ball $\mathcal{B}_{1,\pi}$ in $V_{\mathbb{R}}$.

The main results of this thesis concerning real or complex tensor products are based on our characterisation of the first theta body $\mathcal{T}_1$ of $\mathcal{B}_{1,\pi}$ by a spectrahedron, Theorem 6.2.2. This theorem and also the corresponding computer program (only for small dimensions) can be used to identify witness hyperplanes for $\mathcal{T}_1$ and thus for $\mathcal{B}_{1,\pi}$, in both the real and the complex case.

Indeed, we have seen that the design hyperplanes, skip hyperplanes and parity hyperplanes induce exposed faces of $\mathcal{B}_{1,\pi}$. In this respect, $\mathcal{T}_1$ can be very close to $\mathcal{B}_{1,\pi}$. In some cases we obtain even maximal faces.

For further investigations we now ask some questions about $\mathcal{T}_1$. For instance, one can ask which faces of $\mathcal{T}_1$ meet $\mathcal{B}_{1,\pi}$. In the bipartite case it has already been known that $\mathcal{T}_1$ is sufficient to describe $\mathcal{B}_{1,\pi}$.

Up to now, it is not clear whether this holds also in the multipartite case.

One can also ask whether the first theta body meets the unit vectors only at the unit product vectors. This refers to question (6) in Subsection 3.6.2 and is important to consider the first theta body as an "entanglement measure" (however, we are in the real case). The question can also be formulated as follows: We ask whether $\|z\|_{\mathcal{T}_1} = \|z\|$ if and only if z is a product vector, for all $z \in V_{\mathbb{R}}$. Another reformulation is: Given a unit vector $z \in V_{\mathbb{R}}$ such that z is no product vector, how to find a witness half-space for $\mathcal{T}_1$ which does not contain z.

If the first theta body is not equal to $\mathcal{B}_{1,\pi}$, one can move on to higher theta bodies, that is, to the k-th theta body $\mathcal{T}_k$ in the case where $k \geqslant 2$. For instance, the following scenarios are possible:

(i) Scenario 1: There exists $k \in \mathbb{N}$ such that $\mathcal{T}_k$ is exact.

(ii) Scenario 2: For each face F of $\mathcal{B}_{1,\pi}$ there exists $k \in \mathbb{N}$ such that F lies in the boundary of $\mathcal{T}_k$.

(iii) Scenario 3: There exists a boundary point $y \in \mathcal{B}_{1,\pi}$ such that y lies in the interior of $\mathcal{T}_k$ for all $k \in \mathbb{N}$.

In the following, we discuss approaches to understand the higher theta bodies.

10.1.8 Discussion on Higher Theta Bodies

Here we would like to discuss some approaches and open questions to understand also the higher theta bodies $\mathcal{T}_k$, $k \geqslant 2$.

In the case of complex tensor products we have seen in Chapter 6 that the first theta body is not sufficient to describe the projective unit ball in $V_{\mathbb{C}}$. This suggests to consider also higher theta bodies. However, the discussion here can be helpful in the real case as well, so that it can be found in this section and not in the next which deals with the complex case.

The main question is how $\mathcal{T}_2$ lies in $\mathcal{T}_1$, or, given $k \in \mathbb{N}$, how $\mathcal{T}_{k+1}$ lies in $\mathcal{T}_k$. In the following, we also ask whether the methods which were successful for the investigation of $\mathcal{T}_1$ can be modified to use it also for $\mathcal{T}_k$ or whether they have to be replaced by other methods.

In the following, we discuss both analytic and numerical approaches.

We also refer to the introduction of Subsection 2.5.3.

Let $\mathcal{I}$ be the (complex-)join-meet ideal, $\mathcal{J}$ the (complex-)norm-join-meet ideal and u the (complex) norming polynomial.

A first example — For all $k \geqslant 2$, Example 2.5.3 shows a (probably affine-linear) polynomial f which is a proper k-sum of squares modulo $\mathcal{J}$. However, this example requires that f has already been written as a $(k-1)$-sum of squares modulo $\mathcal{J}$, that is, it already defines $\mathcal{T}_{k-1}$.

The median basis — The median basis in Section 5.2 contributes to the understanding of $\mathcal{I}$ in the real case. With this basis we know the homogeneous parts of $\mathcal{I}$. Moreover, the ideal membership problem for $\mathcal{I}$ can be solved easily, see Corollary 5.2.8. The ideal membership problem for $\mathcal{I}$ can also be solved with a Gröbner basis for $\mathcal{I}$, but the median basis makes the reduction obsolete. In this respect, the median basis can be used for the investigation of higher theta bodies. The problem is the following: Given an affine-linear polynomial f, how to choose a sum of squares s and a polynomial g such that

$$f - s - gu \in \mathcal{I}. \tag{10.1}$$

Once a choice is made, one can imagine that a verification of inclusion (10.1) (that is, the ideal membership problem in this case) can be done by hand. However, there are still many degrees of freedom in the choice of f, s and g. One can also ask whether the median basis can be generalised for complex tensor products. A first approach can be found in Proposition 5.4.6.

The Hibi body — We have seen that many statements about the projective unit ball and its theta bodies also hold for the Hibi body and its theta bodies. Moreover, the general context was advantageous to clarify the notation. This could also be helpful for the study of higher theta bodies.

The Theorem of Schmüdgen — In the Master's thesis, we have investigated the derivation of the Theorem of Schmüdgen in order to understand the theta body chain. The idea was to obtain properties of an affine-linear polynomial which is a $(k+1)$-sum of squares modulo $\mathcal{J}$ in contrast to a k-sum of squares modulo $\mathcal{J}$.

Gröbner bases — With a Gröbner basis of the norm-join-meet ideal $\mathfrak{J}$, see Theorem 5.3.4 and [HHO], one can solve the ideal membership problem for $\mathfrak{J}$. The problem is the following: Given an affine-linear polynomial f, how to choose a sum of squares s such that

$$f - s \in \mathfrak{J}. \tag{10.2}$$

However, it is still not clear how to choose f and s in inclusion 10.2. While doing the research for this thesis, we have tried to understand the second theta body on occasion in order to find regularities during the reduction and in order to show how the highest terms are removed. For this purpose, we investigated the reduction algorithm. The idea was that the reduction could follow fixed steps (for example, alternating reductions by the norming polynomial and a single Hibi relation). It was also interesting to compare the real and the complex case. These observations suggest that the reduction requires many steps and is very complex, therefore tedious by hand. Computer aid can be helpful, but we recommend to understand the structure of the underlying Gröbner basis first.

An optimisation problem — Let G be a Gröbner basis of $\mathfrak{J}$. Let s be a k-sum of squares. The normal form r of s modulo G can be written uniquely as a sum $r = f - \varepsilon$, where f is an affine-linear polynomial and the degree of each term of ε lies in $\{2, 3, \dots, 2k-1, 2k\}$. In this case, there exists $h \in \mathfrak{J}$ such that $s = -h + r$, that is, we have

$$f = s + h + \varepsilon.$$

However, this is not very useful if $\varepsilon \neq 0$, so the question arises how to modify s to obtain $\varepsilon = 0$. An idea to turn this in an optimisation problem is the following: The direct sum of the homogeneous parts of degree $d \in \{0, 1, \dots, 2k\}$ of the underlying polynomial ring can be identified with a real vector space $\mathbb{R}^t$ (where t appropriate), by identifying factors with entries. Now, we ask how to find a polynomial s such that $\|\varepsilon\|$ is sufficiently small. In the course of this thesis we have tried out this approach with the help of the computer algebra program *SageMath*. However, the question arises how to find the minimum of $\|\varepsilon\|$. For example, one may ask whether ε depends continuously on s. Moreover, one may ask whether the Euclidean norm (that is, the l^2 norm on the coefficients) is appropriate or whether it can rather be formulated as an optimisation problem in discrete geometry or as an algebraic problem.

Numerical approach using moment matrices — An approach to understand higher theta bodies is given in [BCR] and uses moment matrices, going back to the original ideas of Lasserre with respect to sos polynomials. The approach is based on a Gröbner basis of the underlying ideal. The main theorem [BCR, Theorem 7.13] says that the theta body can be written as the closure of a projected spectrahedron. This can be implemented with the aid of a computer algebra system in terms of a semidefinite program. On this basis, one can check whether a given vector lies in the theta body or not.

To obtain the main results of this thesis, we used our characterisation of the first theta body Theorem 6.3.6. This can be seen as an alternative to the moment matrix method in a special case. However, a introduction to the moment matrix method, some examples and a derivation can be found in the Master's thesis [Lang]. In an earlier stage of this thesis, we have implemented the method with a computer algebra system for the real case. In this context, we would like to note the following points of view:

(i) The moment matrix method is based on Gröbner bases. One can use the Buchberger algorithm to find a Gröbner basis, but it would be advantageous to find a term order for which the Gröbner basis is as short or as simple as possible. Indeed, a deeper understanding can help to identify possible sources of errors, especially during the testing phase of an implementation of the method. Moreover, it can be helpful to take into account that the computational complexity depends on the length of the Gröbner basis and can be rather high, even for small dimensions. In the real case there is a Gröbner basis which is well understood due to Theorem 5.3.4. A discussion for the complex case can be found in Section 5.4. It is also an open question how to find a Gröbner basis in the case of separable states.

(ii) The moment matrix method can be used to check whether a vector is in the theta body or not. An open question is how to determine concrete sos polynomials and also their sos decomposition with this method.

(iii) The method can be used only in the case where the underlying ideal does not contain any affine-linear polynomial. Eventually, we want to apply the theta body method on the set $\mathcal{S}$ of all separable states. The underlying ideal $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$ contains affine-linear polynomials. The following "trick" can be an approach to avoid this problem: Given $m, n \in \mathbb{N}$ and an ideal $I \subseteq \mathbb{R}[x_1, \dots, x_n]$ generated by polynomials $f_1, \dots, f_m$, one may regard the ideal $\widetilde{I} := I \cdot \mathrm{Id}(x_1^2, \dots, x_n^2)$ instead of I. If I contains affine-linear polynomials, then $\widetilde{I}$ does not, and we have $\mathcal{Z}_{\mathbb{R}}(\widetilde{I}) = \mathcal{Z}_{\mathbb{R}}(I) \cup \{0\}$. However, this method needs a Gröbner basis for the ideal $\widetilde{I}$. Due to the definition of the ideal $\widetilde{I}$, one could assume that a Gröbner base for $\widetilde{I}$ will be longer than a Gröbner basis for I (although we have not checked this yet). Now, if we set $I = \mathcal{J}_{\mathrm{tr}, N_{\mathbb{C}}}$, we have $\mathcal{S} = \mathrm{co}(\mathcal{Z}_{\mathbb{R}}(I))$ and the theta bodies with respect to $\widetilde{I}$ refer to the convex set $C := \mathrm{co}(\mathcal{S} \cup \{0\})$. Since $0 \notin \mathcal{S}$, we have $\mathcal{S} \neq C$, compare also with Figure 9.1. It is left to discuss which witness hyperplanes for C can also be used as entanglement witnesses.

In summary, the results of this thesis can also be useful for the study of higher theta bodies, for example the discussions on Gröbner bases, the study of the join-meet ideal, the results on symmetries and on Hibi theta norms or the discussions on the differences between the real and the complex case.

The subjects of this thesis related to tensor products and separable states can be found within the range of subjects in Table 10.5. We tried mostly to start with the cases whose structure seems to be most simple so that the other cases can be developed on this basis. For example, the theta body method is originally intended for real vector spaces so that we decided to start with the first theta body in the real case.

Tensor product	real	complex	
Subject	projective norm	separable states	
Theta body	first	second	higher
Dimensions	low	high	
Tensor factors	bipartite	multipartite	
Approach	analytic	numerical	
Statements	local	global	

Table 10.5: Subjects of this thesis.

10.2 The Projective Unit Ball, Complex

Here, we summarise the main results for the complex case with respect to question (1) and to question (2) in Subsection 3.6.2: "How close are the theta bodies to the projective unit ball?" and "How accessible are the theta bodies?".

Theorem 2.5.5 guarantees that the theta bodies converge. With our characterisation of the first theta body Theorem 6.3.6, one can check whether a polynomial is 1-sos modulo the complex norm-join-meet ideal and thus determine the first theta body. To do this, one can use the corresponding computer program (the dimension of each tensor factor should not exceed 9). In the case $\mathbb{C}^2 \otimes \mathbb{C}^2$, we have shown that the first theta body is exact, see Theorem 6.4.3. In all other cases, we have obtained the inner radius of the first theta body which is constant and equals $1/\sqrt{2}$, see Theorem 6.4.2.

Therefore, if one wants to estimate the projective norm using theta bodies, it is necessary to consider higher theta bodies. Some approaches to higher theta bodies and ideas for future investigations can be found in Subsection 10.1.8.

On the other hand, the first theta body (and also each higher theta body) can be considered as a new entanglement measure in addition to the projective norm. To do this, it is important that it lies in the Hilbert-Schmidt unit ball, see question (3) in Subsection 3.6.2, and that it meets the unit vectors only at the unit product vectors, see question (6). While the first requirement is fulfilled, see Chapter 6, it is open whether this is also the case for the second.

We have not ruled out at this point that it might be possible to use the design hyperplanes, skip hyperplanes or parity hyperplanes from Chapter 7 and Chapter 8 (see also Section 10.1) also in the complex case. However, it can be difficult to overcome the differences between the real and the complex case. In particular, maximal vectors in the real tensor product $V_{\mathbb{R}}$, regarded as elements in the complex tensor product $V_{\mathbb{C}}$, lose their maximality in general, see Proposition 3.3.3. In addition, in the complex case one has to include complex Hibi relations and to consider higher theta bodies. So we may ask whether there are alternative methods to address the complex case.

We refer also to the discussions in Section 10.1 and recommend the following steps for further investigations:

(1) Consider the second theta body of $\mathcal{B}_{1,\pi}$ in the bipartite tensor product $\mathbb{C}^n \otimes \mathbb{C}^n$ for small values of n. It can be helpful to begin with the case $n = 3$. The aim is to find explicit sos polynomials whose distance to zero is significantly close to the inner radius ${}^1\!/\!\sqrt{n}$ of $\mathcal{B}_{1,\pi}$. Since the complexity of the second theta body seems to be significantly high, we recommend the use of additional computer assistance. For instance, the moment matrix method, see [BCR], can be helpful. This method needs a Gröbner basis. We have seen in Subsection 10.1.8 that it is advantageous to find a term order for which the Gröbner basis is as short and as simple as possible. This has been discussed in Section 5.4.

(2) If the first step is successful, one can move on to the multipartite case $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$. We recall that ${}^2\!/\!{}_3$ is an upper bound on the inner radius of $\mathcal{B}_{1,\pi}$, see Subsection 3.3.3, so the aim is to attain or fall below this bound.

(3) If the first step is not successful, it could be helpful to consider theta bodies of degree 3 or higher.

10.3 Separable States

In Chapter 9 we have shown that the theta body method yields a chain of convex relaxations of the set of the separable states. In particular, each polynomial which is a sum of squares modulo the ideal $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$ is a candidate for an entanglement witness. This offers the possibility of using sos polynomials to solve the separablity problem for a given state. In this section, we discuss the possibilities and the difficulties of this method.

The main question is how to find an explicit polynomial which is sos modulo $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$. Once an sos polynomial is given, it is important to check whether it is an entanglement witness.

Since the theta body method is initially intended for real vector spaces, we started our investigations in this thesis with the projective norm on real tensor products, proceeded with complex tensor products and developed the application on separable states on this basis. Hence, it could be helpful to look at the tensor product case to obtain entanglement witnesses. Since the ideal $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$ contains the complex Hibi relations, the real case seems to be further away than the complex case, see also the discussions in Section 10.2. In particular, the ideal $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$ evolves from the complex-norm-join-meet ideal $\mathcal{J}$ by adding the real and the imaginary part of the trace functional so that an affine functional l which is sos modulo $\mathcal{J}$ is also sos modulo $\mathcal{J}_{\mathrm{tr},N_{\mathbb{C}}}$. Therefore, we could try to modify l using the trace functional.

However, l is primarily a witness functional for $\mathcal{B}_{1,\pi}$, see also Figure 9.1, and we do not know the algebraic role of the trace functional in our context yet. In particular, it is not clear how to ensure that the affine half-space does not cover the entire state space.

Moreover, it can be important that the first complex theta body of $\mathcal{B}_{1,\pi}$ is not very close to $\mathcal{B}_{1,\pi}$ due to Theorem 6.4.2, so that we cannot expect a better situation for the separable states. To guarantee that a sos polynomial is also an entanglement witness it could therefore be necessary to consider higher theta bodies. Some approaches to higher theta bodies and ideas for future investigations can be found in Subsection 10.1.8.

In summary, we recommend the following steps for further investigation:

(1) First, we recommend working through the steps (1) - (3) in the last section.

(2) Now, one can move on to theta bodies of $\mathcal{B}_{1,\pi}$ in the complex tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. It can be helpful to begin with the second theta body. The aim is to find explicit sos polynomials whose distance to zero is as small as possible.

(3) Afterwards, one can use the real and the imaginary part of the trace functional to find explicit sos polynomials which are entanglement witnesses.

(4) It would be interesting to see whether the separability problem can be solved with theta bodies for certain states. Candidates for those states could be the so-called Werner states, see [Maa].

The moment matrix method (see [BCR]) can be used for step (2). We note that this approach cannot be used in the first instance for step (3), since the underlying ideal has to be free from affine functionals, and we note that this method needs a Gröbner basis (which is preferably short and simple), see the discussions in Subsection 10.1.8.

BIBLIOGRAPHY

[AS] Alber, Gernot; Sokoli, Florian: *Generalized Schmidt decomposability and its relation to projective norms in multipartite entanglement*. Journal of Physics A: Mathematical and Theoretical, Vol. 47, 18pp, Bristol 2014. Cited on pages 69, 70, and 92.

[Arv] Arveson, William: *Maximal vectors in Hilbert space and quantum entanglement*. Journal of Functional Analysis, Vol. 256, No. 5, pp. 1476–1510, 2009. Cited on pages viii, x, xv, xvi, xvii, 32, 45, 46, 71, 72, 92, and 93.

[Aud] Audretsch, Jürgen: *Verschränkte Systeme - Die Quantenphysik auf neuen Wegen*. WILEY-VCH, Weinheim 2005. Cited on pages viii, xv, 68, 270, 272, and 273.

[BD] Balbes, Raymond; Dwinger, Philip: *Distributive Lattices*. University of Missouri Press, Columbia (Missouri) 1974. Cited on page 97.

[Bal] Bales, John W.: *A Tree for Computing the Cayley-Dickson Twist*. Missouri Journal of Mathematical Sciences, Vol. 21, No. 2, pp. 83–93, 2009. Cited on page 212.

[BK] Barak, Boaz; Kothari, Pravesh; Steurer, David: *Quantum entanglement, sum of squares, and the log rank conjecture*. STOC Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, Association for Computing Machinery, pp. 975–988, New York 2017. Cited on page 95.

[BM] Barak, Boaz; Moitra, Ankur: *Noisy Tensor Completion via the Sum-of-Squares Hierarchy*. COLT Proceedings of the 29th Annual Conference on Learning Theory, Columbia University, pp. 417–445, New York 2016. Cited on page 95.

[BS] Barak, Boaz; Steurer, David: *Sum-of-squares proofs and the quest toward optimal algorithms*. ECCC Electronic Colloquium on Computational Complexity, article 59, 2014. Cited on page 95.

[BN] Beckenstein, Edward; Narici, Lawrence: *Topological Vector Spaces*. Chapman & Hall, Boca Raton 2011. Cited on pages 30, 32, 33, 38, 40, and 42.

[BW] Becker, Thomas; Weispfenning, Volker: *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer, 1993. Cited on pages 1, 2, 6, 7, 8, and 121.

[Bet] Betten, Anton; Braun, Michael; Fripertinger, Harald; Kerber, Adalbert; Kohnert, Axel; Wassermann, Alfred: *Error-Correcting Linear Codes*. Springer, Berlin Heidelberg 2006. Cited on pages 185, 186, 188, 191, 192, and 193.

[Bir] Birkhoff, Garrett: *Lattice Theory*. American Mathematical Society, Providence 1973. Cited on pages 97, 100, 101, 102, and 104.

[BPT] Blekherman, Grigoriy; Parrilo, Pablo A.; Thomas, Rekha R. (Hrsg.): *Semidefinite Optimization and Convex Algebraic Geometry*. Cambridge University Press, Cambridge 2013. Cited on pages viii, xvi, 10, 14, 32, 49, 51, 54, 155, and 164.

[BCR] Bochnak, Jacek; Coste, Michel; Roy, Marie-Françoise: *Real Algebraic Geometry*. Springer, Berlin Heidelberg 1998. Cited on pages xi, xviii, 15, 17, 49, 51, 291, 294, and 296.

[Bos] Bosch, Siegfried: *Algebra*. Springer, Berlin Heidelberg 2009. Cited on pages 65 and 244.

[CT] Candès, Emmanuel J.; Tao, Terence: *The Power of Convex Relaxation: Near-Optimal Matrix Completion*. EEE Transactions on Information Theory, 2010. Cited on page 34.

[Cam] Cameron, Peter Jephson: *Introduction to Algebra*. Oxford University Press, New York 2008. Cited on pages 65 and 66.

[Con] Conway, John B.: *A Course in Functional Analysis*. Springer, New York 1985. Cited on pages 32 and 41.

[CS] Conway, John Horton; Sloane, Neil James Alexander: *Sphere Packings, Lattices and Groups*. Springer, New York 1993. Cited on page 185.

[CLRS] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford: *Introduction to Algorithms*. The Massachusetts Institute of Technology, Cambridge (Massachusetts) 2001. Cited on pages 234 and 235.

[CLSc] Cox, David; Little, John; Schenck, Henry: *Toric Varieties*. American Mathematical Society, Providence 2009. Cited on page 112.

[CLS] Cox, David; Little, John; O'Shea, Donal: *Ideals, Varieties, and Algorithms. An Introduction to Computional Algebraic Geometry and Commutative Algebra*. Springer, New York 2008. Cited on pages 1, 2, 3, 5, 8, 9, and 10.

[Der] Derksen, Harm: *On the Nuclear Norm and the Singular Value Decomposition of Tensors*. Foundations of Computational Mathematics, Vol. 16, No. 3, pp. 779–811, 2016. Cited on pages 69 and 92.

[DVC] Dür, W.; Vidal, G.; Cirac, J. I.: *Three qubits can be entangled in two inequivalent ways*. Physical Review A, Vol. 62, article 062314, 2000. Cited on page 70.

[Ebe] Ebeling, Wolfgang: *Lattices and Codes*. Vieweg, Braunschweig/Wiesbaden 2002. Cited on page 185.

[Eis] Eisert, Jens: *Entanglement and Tensor Network States*. In: *Emergent Phenomena in Correlated Matter, Vol. 3*. Forschungszentrum Jülich, Jülich 2013. Cited on pages 77, 78, and 272.

[EFHN] Eisner, Tanja; Farkas, Bálint; Haase, Markus; Nagel, Rainer: *Operator Theoretic Aspects of Ergodic Theory*. Springer International, 2015. Cited on page 103.

[EHM] Ene, Viviana; Herzog, Jürgen; Mohammadi, Fatemeh: *Monomial ideals and toric rings of Hibi type arising from a finite poset*. European Journal of Combinatorics, Vol. 32, No. 3, pp. 404–421, 2011. Cited on page 111.

[FL] Friedland, Shmuel; Lim, Lek-Heng: *Nuclear Norm of Higher Order Tensors*. Mathematics of Computation, American Mathematical Society, Vol. 87, No. 311, pp. 1255–1281, Providence 2018. Cited on pages 70 and 92.

[GW] Görtz, Ulrich; Wedhorn, Torsten: *Algebraic Geometry I: Schemes*. Springer Spektrum, Second Edition, Wiesbaden 2020. Cited on pages 1 and 15.

[GKM] Grabowski, Janusz; Kuś, Marek; Marmo, Guiseppe: *Segre maps and entanglement for multipartite systems of indistinguishable particles*. Journal of Physics A: Mathematical and Theoretical, Vol. 45, No. 10, 2012. Cited on page 79.

[Gra] Grätzer, George: *Lattice Theory: Foundation*. Birkhäuser (Springer), Basel 2011. Cited on pages 99 and 105.

[Gru] Gruber, Peter M.: *Convex and Discrete Geometry*. Springer, Berlin Heidelberg New York 2007. Cited on pages 31, 32, 34, and 37.

[Har] Harris, Joe: *Algebraic Geometry. A First Course*. Springer International,

1992. Cited on pages 1, 15, 16, 19, 20, 81, and 141.

[Hat] HARTSHORNE, Robin: *Algebraic Geometry*. Springer, New York 1997. Cited on pages 11, 15, and 81.

[HSS] HEDAYAT, A.S.; SLOANE, Neil James Alexander; STUFKEN, John: *Orthogonal Arrays: Theory and Applications*. Springer, New York 1999. Cited on page 205.

[HHO] HERZOG, Jürgen; HIBI, Takayuki; OHSUGI, Hidefumi: *Binomial Ideals*. Springer, 2018. Cited on pages x, xi, xviii, 109, 111, 125, 126, 128, 130, 131, 140, 141, 142, and 290.

[Hibi] HIBI, Takayuki: *Distributive Lattices, Affine Semigroup Rings and Algebras with Straightening Laws*. Advanced Studies in Pure Mathematics, Vol. 11: Commutative Algebra and Combinatorics, pp. 93–107, 1987. Cited on pages x, xi, xviii, xix, 109, 111, 112, and 125.

[Hil] HILBERT, David: *Ueber die Darstellung definiter Formen als Summen von Formenquadraten*. Mathematische Annalen, Vol. 32, pp. 342–350, 1888. Cited on page 51.

[HL] HILLAR, Christopher J.; LIM, Lek-Heng: *Most Tensor Problems Are NP-Hard*. Journal of the ACM (JACM), Vol. 60, No. 6, article 45, 2013. Cited on page 92.

[HHHH] HORODECKI, Karol; HORODECKI, Michał; HORODECKI, Paweł; HORODECKI, Ryszard: *Quantum Entanglement*. Reviews of Modern Physics, Vol. 81, No. 2, pp. 865–942, 2009. Cited on pages viii and xv.

[Hul] HULEK, Klaus: *Elementare algebraische Geometrie*. Vieweg und Teubner, Wiesbaden 2012. Cited on pages 15 and 27.

[KD] KEEDWELL, Donald A.; DÉNES, Jószef: *Latin Squares and Their Applications*. Elsevier, Amsterdam 2015. Cited on pages 196, 197, 198, 200, 201, 203, and 204.

[Knu] KNUTH, Donald: *The Art of Computer Programming. Volume 3: Sorting and Searching*. Addison-Wesley, Reading (Massachusetts) 1998. Cited on pages 234, 235, and 236.

[KM] KOSTRIKIN, Alexei I.; MANIN, Yu. I.: *Linear Algebra and Geometry*. CRC Press, 1989. Cited on pages 22 and 30.

[LM] LAKHSMIBAI, Venkatramani; MUKHERJEE, Himadri: *Singular Loci of Hibi toric varieties*. Journal of Ramanujan Mathematical Society, Vol. 26, No. 1, pp. 1–29, 2011. Cited on page 111.

[Lang] Lang, Sandra: *Approximation projektiver Tensornormen mit konvexer algebraischer Geometrie*. Master's thesis, Arbeitsgruppe Burkhard Kümmerer, Technische Universität Darmstadt 2015. Cited on pages viii, xiii, xvi, xxi, 32, 38, 39, 42, 43, 44, 46, 51, 54, 76, 79, 82, 87, 127, 143, 146, 155, 158, 159, 180, and 291.

[Lee] Lee, John M.: *Introduction to Riemannian Manifolds*. Springer, New York 2018. Cited on pages 61 and 272.

[Maa] Maassen, Hans: *Entanglement of completely symmetric quantum states*. Talk, Edinburgh January 18, 2012. Cited on pages 72 and 296.

[MS] MacWilliams, F. J.; Sloane, Neil James Alexander: *The theory of error correcting codes*. Elsevier, Amsterdam 1977. Cited on page 185.

[Mur] Murphy, Gerard J.: *C*-Algebras and Operator Theory*. Academic Press, San Diego 1990. Cited on page 271.

[NW] Nie, Jiawang; Wang, Li: *Semidefinite Relaxations for Best Rank-1 Tensor Approximations*. SIAM Journal on Matrix Analysis and Applications, Vol. 35, No. 3, pp. 1155–1179, 2014. Cited on page 95.

[Par] Parthasarathy, Kalyanapuram Rangachari: *On the maximal dimension of a completely entangled subspace for finite level quantum systems*. Proceedings Mathematical Sciences, Vol. 114, No. 4, pp. 365–374, 2004. Cited on page 146.

[Pla] Plaumann, Daniel: *Vorlesung über torische Varietäten*. Vorlesungsskript, Universität Konstanz 2013. Cited on page 112.

[PS] Potechin, Aaron; Steurer, David: *Exact tensor completion with sum-of-squares*. COLT Conference on Learning Theory, 2017. Cited on pages 94 and 95.

[PS1] Potechin, Aaron; Steurer, David: *Exact Tensor Completion*. KTH Royal Institute of Technology, SOS seminar lecture notes, lecture 15, 2017. Cited on page 94.

[PS2] Potechin, Aaron; Steurer, David: *Introduction to the Sum of Squares Hierarchy*. KTH Royal Institute of Technology, SOS seminar lecture notes, lecture 1, 2017. Cited on pages viii and xvi.

[Qur] Qureshi, Ayesha Asloob: *Indispensable Hibi Relations and Gröbner Bases*. Algebra Colloquium, Vol. 22, No. 04, pp. 567–580, 2015. Cited on pages 103 and 125.

[RSS] Rauhut, Holger; Schneider, Reinhold; Stojanac, Željka: *Tensor completion in hierarchical tensor representations*. Compressed Sensing and Its

Applications, pp. 419–450. Springer, Cham 2015. Cited on page 94.

[RS1] Rauhut, Holger; Stojanac, Željka: *Recovery of Third Order Tensors via Convex Optimization*. Proc. SampTA2015, 2015. Cited on page 94.

[RS2] Rauhut, Holger; Stojanac, Željka: *Tensor theta norms and low rank recovery*. Numerical Algorithms, Vol. 88, pp. 25–66, 2021 / preprint, 2015. Cited on pages viii, xi, xvi, xix, 79, 82, 92, 94, 131, 155, and 180.

[Roc] Rockafellar, R. Tyrrell: *Convex Analysis*. Princeton University Press, Princeton 1970. Cited on pages 31, 33, and 38.

[Rud] Rudolph, Oliver: *A new class of entanglement measures*. Journal of Mathematical Physics, Vol. 42, pp. 5306–5314, 2001. Cited on pages viii, xv, and 93.

[Ryan] Ryan, Raymond A.: *Introduction to Tensor Products of Banach Spaces*. Springer, London 2002. Cited on pages 60, 61, 62, and 63.

[Sch] Schmüdgen, Konrad: *The K-moment problem for compact semi-algebraic sets*. Mathematische Annalen, Vol. 289, No. 2, pp. 203–206, 1991. Cited on page 54.

[Seb] Seberry, Jennifer: *Orthogonal Designs. Hadamard Matrices, Quadratic Forms and Algebras*. Springer, New York 2017. Cited on pages 209 and 211.

[Sage] *SageMath*. SageMath - Open-Source Mathematical Software System. Home page: `http://www.sagemath.org`, 2021. Cited on pages 138, 169, and 230.

[Ser] Serre, Jean-Pierre: *Local Fields*. Springer, New York 1979. Cited on page 244.

[Sok] Sokoli, Florian: *Topological Tensor Products and Quantum Entanglement*. Dissertation, Technische Universität Darmstadt 2017. Cited on pages viii, xv, 46, 47, 61, 63, 64, 72, and 92.

[SW] Stoer, Josef; Witzgall, Christoph: *Convexity and Optimization in Finite Dimensions I*. Springer, Berlin Heidelberg 1970. Cited on page 31.

[Sto] Stojanac, Željka: *Low-rank Tensor Recovery*. Dissertation, Technische Universität Bonn 2016. Cited on pages viii, xvi, 51, 79, 82, 92, 94, 109, 125, 126, 127, 130, 155, 159, and 168.

[Stu] Sturmfels, Bernd: *Gröbner Bases and Convex Polytopes*. American Mathematical Society, Providence 1996. Cited on pages 1, 109, and 112.

[Ta1] Takesaki, Masamichi: *Theory of Operator Algebras I*. Springer, Berlin

Heidelberg New York 1979. Cited on pages 60 and 78.

[Voi] Voigt, Felix: *Thetakörper und die konvexe Hülle komplexer Varietäten*. Bachelor's thesis, Arbeitsgruppe Burkhard Kümmerer, Technische Universität Darmstadt 2015. Cited on pages ix, xvi, 21, 25, 32, 88, 89, and 90.

[Wal] Wallis, Walter D.: *Combinatorial Designs*. Marcel Dekker, New York 1988. Cited on pages 211 and 213.

[Wer] Werner, Dirk: *Funktionalanalysis*. Springer Spektrum, Berlin 2018. Cited on page 40.

[Wie] Wiedenmann, Stefan: *Arvesons Beschreibung der Quantenverschränkung*. Bachelor's thesis, Arbeitsgruppe Burkhard Kümmerer, Technische Universität Darmstadt 2010. Cited on pages 70 and 280.

[Zie] Ziegler, Günter Matthias: *Lectures on Polytopes*. Springer, New York 1995. Cited on page 236.

INDEX OF NOTATION

Standard Notation

Numbers — The natural numbers $\mathbb{N}$ begin with 1. If nothing else is specified, n denotes a natural number.

The complex unit is denoted by i.

Sets — The power set of a set M is denoted by $\mathfrak{P}(M)$.

The set of all functions from a set M in a set N is denoted by $\mathcal{A}(M, N)$. The identity in $\mathcal{A}(M, M)$ is denoted by id.

The number of elements of a finite set M is denoted by $\#M$.

Let M be a non-empty set and let $A \subseteq M$. In this context, A^c denotes the complement of A in M, that is, $A^c = S \setminus A$.

A *partition* $\mathcal{P}$ of a non-empty set M is a set of non-empty subsets of M, which are called the *parts* of $\mathcal{P}$, such that M is their disjoint union. The *length* of a part is its cardinality. A partition $\mathcal{P}$ of M is called *proper*, if all parts are proper subsets of M. It is called *complementary*, if it has exactly two parts. Its *width* is the number of its parts. Its *relative size* is the length of its largest part.

Symmetric Groups — Let M be a set. The symmetric group, which is the set of all bijections $M \to M$, is denoted by S_M (or by S_n, if M is finite and $\#M = n$).

Let $\pi \in S_M$. The *support* of π is given by $\mathrm{supp}(\pi) := \{k \in M \colon \pi(k) \neq k\}$. Each element of M which is not in the support of π is called a *fixpoint* of π.

A permutation $\pi \in S_M$ is called a *cycle*, if $m_1 \mapsto m_2 \mapsto \cdots \mapsto m_k \mapsto m_1$ under π, where $\{m_1, \dots, m_k\}$ is the support of π.

In the case where $M = \{1, \dots, n\}$, a cycle $\pi \in S_n$ is called an *adjacent transposition*, if there exists $k \in \{1, \dots, n-1\}$ such that $\mathrm{supp}(\pi) = \{k, k+1\}$, $\pi(k) = k+1$, and $\pi(k+1) = k$. In this case, we write $\pi = (k\ k+1)$.

Groups — Let G be a group with neutral element 1, let N be a normal subgroup of G and let H be a subgroup of G, such that $N \cap H = \{1\}$ and $G = NH$. Then G is the semidirect product of N and H, denoted by $N \rtimes H$.

Rings — Let R be a commutative ring.

Let $M \subseteq R$. The ideal generated by M is denoted by $\mathrm{Id}(M)$, where $\mathrm{Id}(\emptyset) := \{0\}$.

An element $s \in R$ is called a *square*, if $s = r^2$ for some $r \in R$. It is called a *sum of squares*, in short, *sos*, if it can be written as $s = r_1^2 + \cdots + r_t^2$ for some $t \in \mathbb{N}$ and $r_1, \ldots, r_t \in R$.

Vector Spaces — Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{K} = \mathbb{C}$. Let X be a vector space over $\mathbb{K}$.

A function from X to $\mathbb{K}$ is called a *functional* on X. The linear hull of a set $M \subseteq X$ is denoted by $\mathrm{LH}(M)$. The algebraic dual of X is denoted by $X^\star$.

The *symmetry group* $\mathrm{Sym}_X(M)$ of a set $M \subseteq X$ is defined as the set of all invertible linear maps A on X with $A(M) = M$.

The *unit ball* of an arbitrary norm $\|\cdot\|$ on X is denoted by $\mathcal{B}_{1,\|\cdot\|} := \{x \in X \colon \|x\| \leqslant 1\}$. Its *unit sphere* is denoted by $X_1 := \{x \in X \colon \|x\| = 1\}$.

Euclidean Vector Spaces — A canonical (orthonormal) basis of $\mathbb{K}^n$ is denoted by $e_1, \ldots, e_n$. The closure of an arbitrary subset $M \subseteq \mathbb{K}^n$ is denoted by $\mathrm{cl}(M)$.

The Euclidean scalar product is denoted by $\langle \cdot, \cdot \rangle$ and the Euclidean norm by $\|\cdot\|$.

The set of all $m \times n$ matrices with entries in $\mathbb{K}$ is denoted by $\mathcal{M}_{m,n}(\mathbb{K})$, where $\mathcal{M}_{n,n}(\mathbb{K}) =: \mathcal{M}_n(\mathbb{K})$. The transpose and the adjoint of a matrix $A \in \mathcal{M}_{m,n}(\mathbb{K})$ are denoted by A^t and $A^\star$, respectively. The identity matrix in $\mathcal{M}_n(\mathbb{K})$ is denoted by $\mathbb{1}_n$. The set of unitary maps on $\mathbb{C}^n$ is denoted by $\mathcal{U}_n(\mathbb{C})$, the set of orthogonal maps on $\mathbb{R}^n$ is denoted by $\mathcal{U}_n(\mathbb{R})$, and the set of self-adjoint or symmetric maps on $\mathbb{K}^n$ is denoted by $\mathcal{S}_n(\mathbb{K})$. The trace of a matrix $A \in \mathcal{M}_n(\mathbb{K})$ is denoted by $\mathrm{tr}(A)$. If a matrix $A \in \mathcal{M}_n(\mathbb{K})$ is positive semidefinite, we also write $A \geqslant 0$.

The operator norm of a linear map $\mathbb{K}^n \to \mathbb{K}^m$ with respect to the Euclidean norm is denoted by $\|\cdot\|_{\mathrm{op}}$.

Let $x \in \mathbb{K}^n$ and let $M \subseteq \mathbb{K}^n$. The *distance* of x to the set M is denoted by $d(x, M) := \inf\{\|x - y\| \colon y \in M\}$.

Special Notation

The following entries are listed in order of appearance.

1 Polynomial Ideals

1.1 Term Orders

K	field	1
$K[\vec{x}]$	polynomial ring in n variables over K	1
x^α	term $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, where $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$	2
$g \mid f$	g divides f	2
$\lvert\alpha\rvert$	degree of $\alpha \in \mathbb{N}_0^n$	3
$\deg(f)$	degree of $f \in K[\vec{x}]$	3
$K[\vec{x}]_k$	polynomials of degree less or equal than $k \in \mathbb{N}$	3
$\leqslant$	term order on $\mathbb{N}_0^n$ or on $K[\vec{x}]$	3
$\leqslant_{\text{lex}}$	lexicographical order	3
$\leqslant_{\text{grlex}}$	graded lexicographical order	3
$\leqslant_{\text{grevlex}}$	graded reverse lexicographical order	3
$\text{supp}(\alpha)$	support of $\alpha \in \mathbb{N}_0^n$	3
$\text{mdeg}(f)$	multidegree of $f \in K[\vec{x}]$	5
$\deg(f)$	degree of f	5
$\text{LT}(f)$	leading term of f	5
$\text{LC}(f)$	leading coefficient of f	5

1.2 Polynomial Reduction and Gröbner Bases

$\longrightarrow$	reduction relation	6
$\overset{\star}{\longrightarrow}$	reflexive-transitive closure of $\longrightarrow$	6
$\overset{\star}{\longleftrightarrow}$	reflexive-transitive-symmetric closure of $\longrightarrow$	6
$f \longrightarrow_P g$	f reduces to g modulo P	6
G	Gröbner basis	8
$S(g, h)$	S-polynomial of f and h	9
$K[\vec{x}]/I$	coordinate ring with respect to an ideal $I \subseteq K[\vec{x}]$	10
$\mathcal{B}$	standardbasis of $K[\vec{x}]/I$	10

1.3 Homogeneous Polynomials

I_d	homogeneous part of degree $d \in \mathbb{N}_0$ of I	11

2 Convex Algebraic Geometry and Theta Bodies

2.1 Real Algebraic Geometry

$\mathbb{K}[\vec{x}]$	polynomial ring in n variables over $\mathbb{K}$	13

$\mathcal{Z}_{\mathbb{K}}(I) =: \mathcal{Z}(I)$	real or complex affine variety, $I \subseteq \mathbb{K}[\vec{x}]$	15
$\mathcal{I}_{\mathbb{K}}(V) =: \mathcal{I}(V)$	real or complex vanishing ideal of a variety $V \subseteq \mathbb{K}^n$	15
$\sqrt{I}$	radical of an ideal $I \subseteq \mathbb{C}[\vec{x}]$	16
$\sqrt[\mathbb{R}]{I}$	real radical of an ideal $I \subseteq \mathbb{R}[\vec{x}]$	16
$\mathbb{P}^n$	real or complex projective space	17
$[v]$	point $[v] = v_0 : v_1 : \cdots : v_n$ in $\mathbb{P}^n$, $v \in \mathbb{K}^{n+1}$	17
$\mathcal{Z}_{\mathbb{K}}(I)$	real or complex projective variety, $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ homogeneous ideal	17
α	identification of $\mathbb{K}^n$ in $\mathbb{P}^n$	18
$\dim(V)$	dimension of irred. projective variety $V \subseteq \mathbb{P}^n$, $\mathbb{K} = \mathbb{C}$	19
$\deg(V)$	degree of V	19
$\mathcal{H}$	Hilbert function	20
p	Hilbert polynomial	20

2.2 Complex Varieties as Real Varieties

$\imath$	decomplexification of a complex set	21
$e_{k,1}, e_{k,2}$	image under $\imath$ of e_k and of $i\, e_k$, respectively	21
$\mathrm{Re}_0, \mathrm{Im}_0$	real linear maps $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{R}[x_1, \ldots, x_n]$	22
$\jmath$	ring hom. $\mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_{1,1}, x_{1,2}, \ldots, x_{n,1}, x_{n,2}]$	23
$\mathrm{Re}(f), \mathrm{Im}(f)$	real and imaginary part of $f \in \mathbb{C}[x_1, \ldots, x_n]$	23
$\imath$	decomplexification of a complex ideal	25
$\imath$	decomplexification of a complex variety	25
$\imath$	decomplexification of a complex operator	30

2.3 Convex Geometry

$\mathrm{co}(S)$	convex hull of a subset $S \subseteq \mathbb{K}^n$	32
H_l	affine half-space, where $l \in \mathbb{K}[x_1, \ldots, x_n]_1$ non-constant	32
P_l	real affine hyperplane	32
l^y	representative of an affine half-space, $y \in \mathbb{K}^n$, $y \neq 0$	34
l_y	support functional	34
$\mathrm{ext}(C)$	extreme points of a convex set $C \subseteq \mathbb{K}^n$	37
$\dim(F)$	dimension of a face F of C	37
$C^{\bullet}$	polar of a convex set $C \subseteq \mathbb{K}^n$ with $0 \in C$	39
C°	real polar of C	39

2.4 Convex Sets and Norms

$\|\cdot\|^C$	norm with unit ball $C \subseteq \mathbb{K}^n$	41
$\|\cdot\|^{C,*}$	dual norm of $\|\cdot\|^C$	42
$F^{\triangle}$	dual face of face $F \subseteq C$	43
$r(C)$	inner radius of C	45
$o(C)$	outer radius of C	45

2.5 Sums of Squares and Theta Bodies

k-sos	k-sum of squares in $\mathbb{R}[\vec{x}]$, $k \in \mathbb{N}$	49

k-sos-mod I	k-sum of squares modulo an ideal $I \subseteq \mathbb{R}[\vec{x}]$	49
Σ	set of all sums of squares	49
Σ_{2k}	set of all k-sum of squares	49
$\mathcal{W}(M)$	Positivstellenmenge of a set $M \subseteq \mathbb{R}[\vec{x}]$	50
$\mathcal{C}_k$	affine functionals which are k-sos-mod I w.r.t. ideal I	51
$\mathcal{T}_k$	theta body of degree k w.r.t. I	51
$\mathcal{D}_k$	a real prepolar of $\mathcal{T}_k$	53
$\mathcal{T}_k^{\mathbb{C}}(I)$	complex theta body in $\mathbb{C}^n$ of degree k w.r.t. ideal $I \subseteq \mathbb{R}[x_{1,1}, x_{1,2}, \dots, x_{n,1}, x_{n,2}]$	57

3 The Projective Tensor Norm

3.1 Tensor Products and Cross Norms

$B(X, Y)$	bilinear maps from $X \times Y$ to $\mathbb{K}$; X, Y vector spaces	60
$x \otimes y$	product vector, $x \in X$, $y \in Y$	60
$X \otimes Y$	tensor product of X and Y	60
$\mathcal{P}_V$	product vectors in $V := \mathbb{K}^{n_1} \otimes \dots \otimes \mathbb{K}^{n_r}$, $r \geqslant 2$, $n_t \geqslant 2$	61
$\mathcal{E}_V$	unit product vectors in V	61
$\lVert \cdot \rVert_\pi$	projective norm on V	62
$\mathcal{B}_{1,\pi}$	projective unit ball	62
$\langle \cdot, \cdot \rangle_{\mathrm{HS}}$	Hilbert-Schmidt scalar product on V	63
$\lVert \cdot \rVert_{\mathrm{HS}}$	Hilbert-Schmidt norm on V	63
$\mathcal{U}_{\mathrm{loc}}$	local unitary (or orthogonal) operators on V	63
$\lVert \cdot \rVert_\epsilon$	injective norm on V	64

3.2 Group Actions

$g.x$	left group action of $g \in G$ on $x \in X$	65
π_g	permutation in S_X, induced by g	65
$[x], G.x$	orbit of x under G	66
X/G	set of all orbits	66
G_x	stabiliser of x under G	66
K_G	stabiliser of X	66
$g.a$	group action of $g \in G$ on $a \in \mathcal{A}(X, Y)$	66

3.3 Geometry of the Projective Unit Ball

$\lVert \cdot \rVert_{\mathrm{tr}}$	trace norm on a bipartite tensor product	68
ξ_{GHZ}	GHZ-vector	69
ξ_W	W-vector	69
$\mathrm{Arv}(V)$	Arveson bound	71
$\mathcal{U}_{\mathrm{loc}}^0$	operators of the form $\mathbb{1} \otimes \dots \otimes \mathbb{1} \otimes O$, $O \in \mathcal{U}_{n_r}(\mathbb{K})$	71
F_σ	flip operator, where $\sigma \in S_r$	72
F_V	flip operators	72
M_ν	max. face ind. by max. vector $y \in V$, $\nu := r(\mathcal{B}_{1,\pi})y$	76

4.2 Distributive Lattices

$L \times M$	product lattice of two lattices L and M	103
N	direct product $\{1,\dots,n_1\} \times \cdots \times \{1,\dots,n_r\}$	103
D_{18}	(largest) lattice generated by three elements	104
s	smallest element of D_{18}	104
l	largest element of D_{18}	104
m	median of D_{18}	104
D_1, D_2, D_3	three examples of pentagonal lattices	105
$L(a,b)$	largest boolean sublattice of L spanned by $a, b \in L$	106

5 The Join-Meet Ideal

L	non-empty finite distributive lattice	109
$V_{\mathbb{K}}$	tensor product $\mathbb{K}^{n_1} \otimes \cdots \otimes \mathbb{K}^{n_r}$	109
$L_{\mathbb{C}}$	equals $L \times \{1,2\}$	109

5.1 Real and Complex Hibi Relations

$\mathcal{H}_L$	set of all non-zero Hibi relations	111
$\mathcal{I}_L$	join-meet ideal	111
$\mathcal{Z}_{\mathbb{K}}(\mathcal{I}_L)$	Hibi variety	111
u_L	norming polynomial	112
$\mathcal{J}_L$	norm-join-meet ideal	112
$\mathcal{Z}_{\mathbb{R}}(\mathcal{J}_L)$	normed Hibi variety	112
$\mathcal{H}_{L_{\mathbb{C}}}$	set of all non-zero complex Hibi relations	113
$\imath(\mathcal{I}_L)$	complex-join-meet ideal	113
$\mathcal{Z}_{\mathbb{R}}(\imath(\mathcal{I}_L))$	complex Hibi variety	113
$u_{L_{\mathbb{C}}}$	complex norming polynomial	113
$\mathcal{J}_{L,\mathbb{C}}$	complex-norm-join-meet ideal	113
$\mathcal{Z}_{\mathbb{R}}(\mathcal{J}_{L,\mathbb{C}})$	complex normed Hibi variety	113

5.2 The Median Basis of the Join-Meet Ideal

L^m/S_m	index set for terms in $(\mathbb{K}[x_a\colon a \in L])_m$, $m \in \mathbb{N}_0$	117
$\overline{a}$	class of $a = (a_1,\dots,a_m) \in L^m$ in L^m/S_m	117
$\overline{x}_{\overline{a}}$	corresponding term $x_{a_1} \cdot \ldots \cdot x_{a_m}$	117
$\longrightarrow$	reduction relation on L^m/S_m	118
$\mathcal{R}_m$	set of all equivalence classes w.r.t. $\xleftrightarrow{\star}$	118
$[\overline{a}]$	equivalence class of $\overline{a}$	118
$M_k(a_1,\dots,a_m)$	k-median of $a_1,\dots,a_m \in L$, $k \in \{1,\dots,m\}$	121
$\mathcal{M}(\overline{a})$	median of $\overline{a}$	121
$h_{\overline{a}}$	equals $\overline{x}_{\overline{a}} - \overline{x}_{\mathcal{M}(\overline{a})}$	124
$\mathcal{B}_L$	median basis of the join-meet ideal	124
$V_{[\overline{a}]}$	linear hull of all polynomials $h_{\overline{b}}$, where $\overline{a} \xleftrightarrow{\star} \overline{b}$	124

$\mathcal{M}(f)$	median of $f \in \mathbb{K}[x_a \colon a \in L]$	124
$f - \mathcal{M}(f)$	projection of f onto $\mathcal{I}_L$	124

5.3 A Gröbner Basis of the (Norm-)Join-Meet Ideal

$\leqslant'$	linear extension of L	126

5.4 Complex Hibi Relations and Gröbner Bases

$a,1; a,2$	elements in $L_\mathbb{C}$ or variables in $\mathbb{R}[x_{a,1}, x_{a,2} \colon a \in L]$, $a \in L$	132
$V_{\mathrm{Re},\mathrm{Re}}$	$\mathrm{LH}(a,1 \cdot b,1 : a, b \in L)$	139
$V_{\mathrm{Im},\mathrm{Im}}$	$\mathrm{LH}(a,2 \cdot b,2 : a, b \in L)$	139
$V_{\mathrm{Re},\mathrm{Im}}$	$\mathrm{LH}(a,1 \cdot b,2 : a, b \in L)$	139

5.5 Attributes of the Hibi Variety

$U_{[\overline{a}]}$	linear hull of $\{\overline{x}_{\overline{b}} \colon \overline{b} \in [\overline{a}]\}$	140
N_0	indexing tuples in the projective case	141

5.6 Application to Tensor Products

$D(n_1, \dots, n_r)$	total number of non-zero PV-determinants	145
Z	group $((\mathbb{Z}_2)^r, +)$ (acts on N^2/S_2)	147
$\triangle$	symmetric difference	147
$C_{\overline{a}}$	coincidence set of $\overline{a} \in N^2/S_2$	147
$S_{\overline{a}}$	support of $\overline{a}$	147
$\mathcal{D}_{t,p}$	set of all non-zero PV-det. with support length t	149

6 The Hibi Body and its Theta Bodies

$L_\mathbb{K}$	$L_\mathbb{R} := L$, $L_\mathbb{C} := L \times \{1, 2\}$	155
n	$\#L_\mathbb{K}$	155
$\mathcal{I}$	(complex-)join-meet-ideal	155
$\mathcal{J}$	(complex-)norm-join-meet ideal	155
V	$\mathcal{Z}_\mathbb{R}(\mathcal{J})$ (or $\imath^{-1}(\mathcal{Z}_\mathbb{R}(\mathcal{J}))$)	155
H	Hibi body	155
$\mathcal{T}_k$	k^{th} (complex) theta body of $\mathcal{J}$	155

6.1 The Hibi Norm and Hibi Theta Norms

$\lVert \cdot \rVert_H$	Hibi norm	157
$\lVert \cdot \rVert_{\mathcal{T}_k}$	k^{th} theta norm (case $\mathbb{K} = \mathbb{R}$)	159

6.2 The First Theta Body and Spectrahedra

$\widetilde{S}$	a spectrahedron in $\mathcal{S}_{n+1}(\mathbb{R})$	163
S	a projected spectrahedron in $\mathcal{S}_n(\mathbb{R})$	163
$\rho(B)$	spectral radius of a positive semidefinite matrix B	167

6.3 The First Theta Body in the Real Case

$\mathcal{P}$	join-meet partition of L	170
B	finite boolean lattice	173
a'	complement of a in B	173
s	splitting function for B or for $\mathcal{P}$	173

S_B^+, S_B^-	a complementary partition of B	173
$f^s_{a,b}$	a polynomial	177

6.4 The First Complex Theta Body

6.5 Join-Meet Partitions and Codes

$\mathbb{F}$	finite field	185
C	code in $\mathbb{F}^n$	186
$\mathrm{wt}(v)$	weight of $v \in \mathbb{F}^n$	186
$d(v, w)$	Hamming distance of v and $w \in \mathbb{F}^n$	186
$d(C)$	minimum distance of C	186
$d(w, C)$	minimum distance of w to C	186
Γ	generator matrix of a linear code C	191
$C_1 \oplus C_2$	(outer) direct sum of codes C_1 and C_2	192

7 Design Hyperplanes

V	tensor product $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$, $n \in \{2, 4, 8\}$	195

7.1 Latin Squares

$(S, \cdot)$	quasigroup	196
(B_1, B_2, M)	a multiplication table of $(S, \cdot)$ with ...	196
B_1, B_2	boundaries	196
M	a multiplication table of $(S, \cdot)$ without boundaries	196
L	latin square	197
(θ, ϕ, ψ)	isotopism, where θ, ϕ, ψ bijections	198
$\psi(L)$	entry-wise application of ψ on L	198
$\mathrm{Tri}(L)$	representation of L	199
L_σ	entry-wise application of $\sigma \in S_3$ on $\mathrm{Tri}(L)$	199
$L_{\sigma,\psi}$	(σ, ψ) parastrophe of L	199
$\mathrm{prod}_{(S,\cdot)}(a)$	product of $a \in S^r$, where $r \in \mathbb{N}$	204
$\mathcal{P}_r$	a partition of S^r	204
$T_{s,r}$	part of $\mathcal{P}_r$, where $s \in S$	204
$\mathrm{OA}(m, k, s, d)$	orthogonal array: m runs, k factors, s levels, strength d	205

7.2 Orthogonal Designs

X	orthogonal design $\mathrm{OD}(n; s_1, \dots, s_m)$	210
n	order of X	210
$(s_1, \dots, s_m)$	type of X	210
$A \star B$	entry-wise product of two matrices A, B	213
$\lvert X \rvert$	absolute value of X	213
$(S_0, \star)$	quasigroup with mult. tab. $((x_1, \dots, x_n), (x_1, \dots, x_n), \lvert X \rvert)$	215
$(S, \cdot)$	canonical quasigroup of X	215
$\mathrm{sign}(a)$	sign of $a \in S^r$	216
$\hat{X}$	an orthogonal design related to X	216

7.3 Design Hyperplanes

n	number in $\{2, 4, 8\}$	220
$\mathcal{P}_D$	design partition of $N = \{1, \dots, n\}^r$	220
T_s	design part, where $s \in S_0$	220
s_D	design function on N	220
β	translation by $h \in N$: $\beta \colon N \to N$, $a \mapsto h \star a$	220

7.4 Skip Hyperplanes

V'	tensor product $\mathbb{R}^{n'} \otimes \cdots \otimes \mathbb{R}^{n'}$, $n' \in \{3, 5, 6, 7\}$	228
$\mathcal{P}_S$	skip partition of $N' = \{1, \dots, n'\}^r$	228
s_S	skip function on N'	228
m_{Skip}	relative size of the skip partition	229
$\text{Skip}(V')$	skip bound	229

8 Parity Hyperplanes

V	tensor product $\mathbb{R}^n \otimes \cdots \otimes \mathbb{R}^n$	233

8.1 Sorting and Inversions

$\text{LIT}(a)$	left inversion table for $a \in N = \{1, \dots, n\}^r$	234
$\text{RIT}(a)$	right inversion table for a	234
$\text{inv}(a)$	total number of inversions of a	234
$a(s_0, c)$	emerges from a by replacing the s_0^{th} entry by c	238
$R(a, s_0, c)$	inversion rest of a with respect to (s_0, c)	238
$S(a, s_1, s_2, c_1, c_2)$	inversion symmetrisation of a w.r.t. (s_1, s_2, c_1, c_2)	242

8.2 Some Homological Algebra

$C^0 \xrightarrow{d^0} C^1 \xrightarrow{d^1} C^2$	cochain complex	244
B^1	$1-$coboundary	244
Z^1	$1-$cocycle	244
Z^1/B^1	1^{th} cohomology group	244
G	group acting on a set X	244
H	abelian group	244
A	equal to $\mathcal{A}(X, H)$	244
φ_a	function $G \to A$ with $g \mapsto {}^{g \cdot a}/_{a}$, where $a \in A$	244
$\varphi_{a,x}$	equal to $\delta_x \circ \varphi_a$, where δ_x evaluation func. at $x \in X$	247

8.3 Parity Hyperplanes

$\rho(a)_t$	parity of t in a, where $a \in N$	249
$\rho(a)$	parity of a	249
T_ν	parity part, where $\nu \in \rho(N)$	249
$\mathcal{P}_P$	parity partition of N	249
s_P	parity function on N	250
$\text{sig}(a, b)$	equal to $s_P(a) \cdot s_P(b)$	250
$\varphi_{\overline{a}}$	equal to $\varphi_{\text{sig},\overline{a}}$ for all $\overline{a} \in N^2/S_2$	251

INDEX

CURRICULUM VITAE

2008 – 2011 **Hochschule Darmstadt (h_da)**
Bachelor of Science „Angewandte Mathematik"

Bachelorthesis:
Die Radon-Transformation und ihre Anwendungen
(*The Radon Transform and its Applications*)

2010 - 2011 **Dublin Institute of Technology (DIT)**
Auslandssemester

2011 **Max-Planck-Institut für Hirnforschung (MPI)**
Entwicklung von Bildverarbeitungsalgorithmen

2011 - 2015 **Technische Universität (TU) Darmstadt**
Master of Science „Mathematik"

Masterthesis:
Approximation projektiver Tensornormen
mit konvexer algebraischer Geometrie
(*Approximation of Projective Tensor Norms*
with Convex Algebraic Geometry)

2015 - 2021 **Technische Universität (TU) Darmstadt**
Wissenschaftliche Mitarbeiterin
Fachbereich Mathematik
AG Operatoralgebren und Quantenstochastik
Prof. Dr. Burkhard Kümmerer

Dissertation:
A Geometric Approach to the Projective Tensor Norm
(*Ein Geometrischer Zugang zur projektiven Tensornorm*)