A C*-Algebraic Approach to Quantum Coding Theory

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

Dissertation

von
Dipl.-Math. Lisa Steiner
aus Filderstadt

Referent:	Prof. Dr. B. Kümmerer
Korreferent:	Dr. H. Maassen
Tag der Einreichung:	12. Juli 2007
Tag der mündlichen Prüfung:	3. September 2007

Darmstadt 2008
D 17

Acknowledgments

I would like to express my thanks to Burkhard Kümmerer for supervising my thesis and for giving me the opportunity to work in his research group. His way of doing mathematics has influenced me deeply.

Let me also thank Claus Köstler and in particular Jürgen Hellmich for many stimulating conversations as well as for their support at all stages of my work.

Many thanks to all my collegues in our group, especially Nils Gebhardt, Florian Haag, Heike Müller, Kay Schwieger, Nadiem Sissouno, Walter Reusswig and Julia Wiskandt. I always enjoyed the friendly and supportive working atmosphere.

My special thanks go to my parents and sisters, as well as to Fatma, without whom I might not have finished this work. Last but not least, I am very grateful to my husband Feriz, who bravely manages to live with a mathematician.

Contents

Introduction

Placement

This work is embedded in the mathematical field of quantum information. Quantum information is one of the key technologies of the 21st century and is based on quantum mechanics.

The theory of quantum mechanics was developed approximately 100 years ago. But it wasn't until 1982 when Feynman [Fey82] first stated that it might be useful to use quantum mechanics to construct computers powerful enough to simulate quantum systems efficiently.

In 1985, Deutsch [Deu85] gave the first ideas for a quantum Turing machine, resulting from a quantum mechanical description of calculation processes. This is regarded as the first model of a quantum computer. His work is seen as the foundation of a more concrete definition of Bernstein and Vazirani [BV92], what lead to a subfield of quantum information theory named quantum complexity.

Schumacher [Sch95] eventually defined a qubit, the quantum version of a classical bit in information theory. He defined them as pure quantum states of two-level systems, described by unit vectors of the system Hilbert space. Soon there were first ideas for physical realizations of qubits as described by Berthiaume [HS97] and first results in quantum computation. The first major steps were Shors [Sho97] algorithms for factorization and discrete logarithm. Both are based on the problem of order finding and solving these problems efficiently on a quantum computer. The next step was the quantum search algorithm by Grover ([Gro96] and [Gro97]).

Quantum coding theory currently consists of two main subfields, quantum cryptography and quantum codes. In 1997, Gottesman [Got97] introduced error correcting codes. These codes work with finite tensor products of pure states, but allow a good error correcting procedure after transmission. Error correction becomes necessary as quantum states evolve with time and this evolution is usually disturbed.

However, an important question of quantum information has remained unanswered. It is to find a quantum analogue of classical coding theory. This is the objective of this thesis, together with the question, to what extent existing quantum codes and algorithms make use of quantum mechanics. We try to answer these questions by using a systematical view of quantum probability theory that was introduced by Kümmerer [Küm85b] and studied by both Kümmerer and Maassen, for example in [KM98] or [Maa06]. We follow this way of algebraization and develop analogously a quantum coding theory. A recent approach of Gohm, Kümmerer and Lang [GKL06] also leads to codes in an operator algebraic setting, but is different to ours.

Main Results

This work has reached several results. The first is, that it was possible to find an algebraic frame in which we can formulate stabilizer codes as developed by Gottesman. This formulation is independent from bases of the related Hilbert spaces which usually hide what is happening. After this result, we were able to show that the independence of generators of the stabilizer group corresponds to trace-independence. This is a notion of independence that generalizes the classical notion of independence of random variables into a quantum mechanical setting. This leads to a new characterization of stabilizer embeddings. It also leads to the insight, that the choice of generators of a stabilizer algebra corresponds to choosing a representation of finitely many Rademacher functions in a matrix algebra.

The second part of this work was to develop a quantum coding theory based on a systematical way of algebraization of classical concepts that was described in section . Our result differs in some points from what has been developed so far, mainly because we are working not only with pure but also arbitrary states. This is a natural change as there is no reason why a general quantum coding theory should be restricted to pure states and thus exclude an essential part of quantum mechanics. This approach is supported by [**AKN98**] and [**Maa06**] and also followed in quantum complexity theory. As allowing mixed states changes the usual model of quantum computers, the parallel to quantum complexity theory is important, as our choice is legitimized there. Another difference to the quantum coding theory to date is, that we focus on infinitely many coupled qubits. This has the same reasons as in classical coding theory and is further motivated in chapter 3, section 11. Last but not least, we were able to integrate the common example of stabilizer codes as developed by Gottesman into our theory and to derive examples for our definitions from it. We could also include the examples of Ollivier and Tillich ([**OT03**] and [**OT04**]). Furthermore, the examples derived from stabilizer codes as developed by Gottesman have a very important property. This property allows us to interpret these stabilizer codes as mappings which hide a given state space in a larger one.

The third main result is that we were able to show that the most important quantum algorithms, including stabilizer codes and the Shor algorithm, are in some sense commutative and thus classical. This can be done as quantum algorithms fit into the notion of quantum measurements, and our calculations imply that they can be represented as a coupling to a classical Bernoulli shift.

Survey of Chapters

The first two chapters are introductory. In **chapter 1** we give an overview of classical coding theory. We introduce the notions of alphabets, code spaces over such alphabets and coders, which are mappings between code spaces. Linear coders as well as convolutional coders will play an important role in the later chapters. The operator algebraic frame of this work and some notation are set in **chapter 2**.

The purpose of **chapter 3** is to present a well known feature in quantum coding theory, namely stabilizer embeddings. We give an easier, base independent definition in the sections 1 to 5

and give an example in section 6. We also construct special stabilizer embeddings as m-blocks and stabilizer embeddings as introduced by Ollivier and Tillich and give examples for these embeddings in the sections 7 to 10. Finally, we discuss the preliminaries of quantum code spaces in section 11.

We start the next chapter, **chapter 4**, by examining the definitions in literature. Then we define quantum alphabets and elements of quantum code spaces via algebraization of classical alphabets and codes in the sections 4 and 5. This algebraization is inspired by a certain scheme that we explain in section 2. We also define quantum coders in section 6 and give first examples, namely q-higher power coders and q-1-block coders.

In **chapter 5** we construct a q-1-block coder out of stabilizer embeddings in section 1 and give a nontrivial example of quantum convolutional coders constructed from the special stabilizer embeddings developed by Ollivier and Tillich in section 2. We finish the chapter with a discussion in section 3, in which we reflect to what extent and how in a certain way these coders might be classical.

The last chapter, **chapter 6**, contains a discussion of the preceding results as well as considerations to what extent quantum coders and quantum algorithms make use of quantum mechanics. It starts with the definition of a measurement operator as well as the notion of essential commutativity in section 1. The second section describes quantum gates, special transformations that are used to implement quantum algorithms. In section 3 we prove that important classes of quantum algorithms are essentially commutative, i.e. that their measurement operator can be obtained from a coupling to a classical Bernoulli shift. The last section describes the measurement operator of the well known Grover quantum search algorithm.

Zusammenfassung

Einordnung der Arbeit

Diese Arbeit ist im mathematischen Gebiet der Quanteninformation angesiedelt, einer Schlüsseltechnologie des 21. Jahrhunderts, die auf der Quantenmechanik aufbaut.

Die Theorie der Quantenmechanik wurde bereits vor etwa 100 Jahren entwickelt. Doch erst im Jahre 1982 schlug Feynman [**Fey82**] vor, die Quantenmechanik dazu zu benutzen, Computer zu bauen, die in der Lage wären, quantenmechanische Systeme effizient zu simulieren.

Deutsch [**Deu85**] entwickelte 1985 die ersten Ideen für eine Quantenturingmaschine, ein quantenmechanisches Modell für Berechenungsprozesse. Dieses Modell wird als das erste Modell eines Quantencomputers angesehen. Seine Arbeit bildet die Grundlage für eine konkretere Definition von Bernstein und Vazirani [**BV92**], die ein neues Untergebiet namens Quantenkomplexitätstheorie begründete.

Schumacher [**Sch95**] definierte schliesslich ein Qubit, die quantenmechanische Version eines klassischen Bits, als reine Zustände von Zwei-Niveau-Systemen, die durch Einheitsvektoren eines Hilbertraumes beschrieben werden. Bald gab es erste physikalische Realisierungen von Qubits, wie sie beispielsweise von [**HS97**] beschrieben werden, und erste Resultate im Gebiet der Quantenberechnungen. Erste wesentliche Schritte waren die Algorithmen für das Faktorisierungsproblem und den diskreten Logarithmus von Shor [**Sho97**], die auf der Aufgabenstellung des sogenannten “order-finding” beruhen, und diese Probleme effizient auf einem Quantencomputer lösen. Der nächste Schritt war der Quantensuchalgorithmus von Grover ([**Gro96**] and [**Gro97**]).

Die Quantenkodierungstheorie besteht bis heute aus zwei Hauptgebieten, der Quantenkryptographie und Quantenkodes. Im Jahr 1997 führte Gottesman [**Got97**] fehlerkorrigierende Kodes ein. Diese Kodes arbeiten mit endlichen Tensorprodukten von reinen Zuständen, erlauben aber eine gute Fehlerkorrektur nach der Übermittlung der Zustände. Dies ist notwendig, da sich quantenmechanische Zustände im Laufe der Zeit verändern und gest"ort werden.

Dennoch war eine wichtige Frage der Quanteninformationstheorie noch unbeantwortet geblieben, nämlich eine quantenmechanische Entsprechung der klassischen Kodierungstheorie zu finden. Dies zu entwickeln ist das Ziel dieser Arbeit, zusammen mit der Frage, in wie weit existierende Quantenkodes und -algorithmen die Quantenmechanik nutzen. Wir gehen diese Fragen an, indem wir einen systematischen Zugang zur Quantenwahrscheinlichkeitstheorie von Kümmerer [**Küm85b**] verwenden, der dann von Kümmerer and Maassen zum Beispiel in [**KM98**] oder [**Maa06**] weiter studiert wurde. Wir folgen diesem Ansatz und entwickeln

analog eine Quantenkodierungstheorie durch Algebraisierung. Ein neuerer Ansatz von Gohm, Kümmerer and Lang [GKL06] führt zwar auch zu Kodes in einem operatoralgebraischen Rahmen, unterscheidet sich aber von unserem.

Hauptergebnisse

Die vorliegende Arbeit hat mehrere Ergebnisse. Zunächst waren wir in der Lage, einen algebraischen Rahmen zu finden, in dem wir die Ideen von Gottesman zu den sogenannten Stabilisatorkodes formulieren konnten. Diese neue Formulierung ist basisunabhängig und verschleiert im Gegensatz zur bisherigen wegen der prägnanteren Formulierung nicht was geschieht. Weiter konnten wir zeigen, dass die Unabhängigkeit von Erzeugern der Stabilisatorgruppe der Spurunabhängigkeit entspricht, einem Unabhängigkeitsbegriff, der die klassische Unabhängigkeit von Zufallsvariablen in einen quantenmechanischen Kontext verallgemeinert. Dies führt zu einer neuen Charakterisierung von Stabilisatorkodes und der Einsicht, dass die Wahl von Erzeugern einer Stabilisatoralgebra der Wahl einer Darstellung von endlich vielen Rademacherfunktionen in einer Matrixalgebra entspricht.

Der zweite Teil dieser Arbeit entwickelt eine Quantenkodierungstheorie. Sie basiert auf einem systematischen Zugang der Algebraisieung klassischer Konzepte, der in Unterkapitel erwähnt wurde. Unser Resultat unterscheidet sich in einigen Punkten von den bisherigen Ansätzen der Literatur. Hauptsächlich unterscheidet es sich darin, dass wir nicht nur reine, sondern beliebige Zustände zulassen. Dies ist ein natürlicher Ansatz, da es keinen Grund dafür gibt, sich in der Quantenkodierungstheorie auf reine Zustände zu beschränken, und man durch die Beschränkung einen wesentlichen Teil der Quantenmechanik ausschliesst. Unser Ansatz wird von [AKN98] und [Maa06] unterstützt und auch in der Quantenkomplexitätstheorie verfolgt. Da das Zulassen von beliebigen Zuständen das übliche Modell eines Quantencomputers verändert, ist die Parallele zur Quantenkomplexitätstheorie bedeutend, da unser Vorgehen dort legitimiert wird. Ein weiterer Unterschied zur bisherigen Quantenkodierungstheorie ist, dass wir unendlich viele gekoppelte Qubits zulassen. Die Begründung dafür ist die gleiche wie in der klassischen Kodierungstheorie und wird in Kapitel 3, Unterkapitel 11 weiter beschrieben. Des weiteren waren wir in der Lage, die üblichen Beispiele der Stabilisatorkodes, wie sie von Gottesman entwickelt wurden, in unsere Theorie zu integrieren, und Beispiele für unsere Definitionen daraus zu entwickeln. Auch konnten die Beispiele von Ollivier and Tillich ([OT03] und [OT04]) beschrieben werden. Ausserdem war es uns möglich, bei den Beispielen der Stabilisatorkodes nach Gottesman eine wichtige Eigenschaft nachzuweisen. Diese Eigenschaft erlaubt es, die Stabilisatorkodes nach Gottesman als Abbildungen zu interpretieren, die einen gegebenen Zustandsraum in einem grösseren verstecken.

Das dritte Ergebnis ist, dass die meisten Quantenalgorithmen, einschliesslich der Stabilisatorkodes und des Shoralgorithmus, in einem gewissen Sinne kommutativ und somit klassisch sind. Dies war möglich, da Quantenalgorithmen unter die Definition von Quantenmessprozessen fallen und wir so zeigen konnten, dass sie als Kopplung an einen klassischen Bernoulliprozesses dargestellt werden können.

Kapitelübersicht

Die ersten beiden Kapitel sind einführender Natur. **Kapitel 1** gibt eine Übersicht über die klassische Kodierungstheorie. Wir stellen Begriffe wie Alphabete, Koderäume über solchen Alphabeten und Kodierer, die Abbildungen zwischen Koderäumen sind, vor. Lineare Kodierer und Faltungskodierer werden in späteren Kapiteln eine wichtige Rolle spielen. Der operatoralgebraische Rahmen dieser Arbeit sowie Notationen werden in **Kapitel 2** eingeführt.

Das Ziel von **Kapitel 3** ist, einen bekannten Begriff der Quantenkodierungstheorie, die Stabilisatoreinbettungen, vorzustellen. Wir geben eine einfachere, basisunabhängige Definition in den Unterkapiteln 1 bis 5 und stellen in Unterkapitel 6 ein Beispiel vor. In den Unterkapiteln 7 bis 10 konstruieren wir weitere Stabilisatoreinbettungen wie m-Blöcke und die von Ollivier and Tillich eingeführten Stabilisatoreinbettungen und liefern auch hierfür Beispiele. Schliesslich diskutieren wir in Unterkapitel 11 Voraussetzungen an Quantenkoderäume.

Wir beginnen das nächste Kapitel, **Kapitel 4** mit den bisherigen Definitionen aus der Literatur. Wir definieren daraufhin in den Unterkapiteln 4 und 5 Quantenalphabete und Elemente von Quantenkoderäumen, indem wir die klassischen Defintionen algebraisieren. Diese Algebraisierung folgt einem Schema, das in Unterkapitel 2 erklärt wird. In Unterkapitel 6 führen wir Quantenkodierer ein und geben erste Beispiele, Quanten-higher-power-Kodierer und Quanten-1-Block-Kodierer, an.

In **Kapitel 5** konstruieren wir nun in Unterkapitel 1 Quanten-1-Block-Kodierer aus den obigen Stabilisatoreinbettungen und zeigen in Unterkapitel 2 ein nichttriviales Beispiel eines Quantenfaltungskodierers, das aus den speziellen Stabilisatoreinbettungen von Ollivier and Tillich entsteht. Das Kapitel schliesst mit einer Diskussion in Unterkapitel 3, worin reflektiert wird, in wie fern diese Kodierer klassisch sind.

Das letzte Kapitel, **Kapitel 6**, enthält nun eine Diskussion der vorangegangenen Ergebnisse und auch Überlegungen, in wie weit Quantenkodierer und Quantenalgorithmen die Quantenmechanik nutzen. Es beginnt mit der Definition des Quantenmessprozesses und des Begriffs der wesentlichen Kommutativität in Unterkapitel 1. Das zweite Unterkapitel beschreibt Quantengatter, spezielle Transformationen, die benutzt werden, um Quantenalgorithmen zu implementieren. Wir zeigen in Unterkapitel 3, dass eine wichtige Klasse von Quantenalgorithmen wesentlich kommutativ ist, d.h. dass die zugehörigen Messprozesse als eine Kopplung an einen klassischen Bernoulliprozess geschrieben werden können. Das letzte Unterkapitel beschreibt den Messprozess des bekannten Quantensuchalgorithmus von Grover.

CHAPTER 1

Classical Coding Theory

As a starting point of this work we would like to briefly introduce the classical coding theory.

The word "code" is used for two different notions in mathematics and therefore we will first set the use of this term in this work.

Symbolic dynamics as well as coding theory work with alphabets like the set $\{0, 1\}$. In both fields we deal with elements of such alphabets, so called letters, and sequences of these letters. We all know that our computer works with such sequences whenever it performs an algorithm or saves data.

In symbolic dynamics, a "code" means a stationary mapping of one shift space into another, whereby a shift space stands for a shift invariant set of allowed sequences, whereas a "code" in coding theory stands for a shift space itself. Here, allowed sequences are usually finite and differ in as many places from one another as possible, which leads to error correcting codes.

In the following we speak of coders as mappings between shift spaces and consider a code to be the image shift space of a coder.

In the next section we make this more precise and give proper definitions of alphabets, letters, shift spaces and coders. The following sections describe special examples. Section 2 and section 3 present first examples of shift spaces and coders, namely higher block shifts respectively coders and higher power shifts respectively coders. Sliding block coders, linear coders and convolutional coders are presented in the sections 4 to 6.

1. Basic Definitions

This section offers basic definitions as mentioned above. A more detailed introduction can be found in [**LM99**].

A finite set A of m *symbols* is called a *(finite) alphabet*. The principal objects of study in coding theory are bi-infinite sequences $x = (x_i)_i = \ldots x_{-2}x_{-1} \,.\, x_0x_1x_2 \ldots \in A^{\mathbb{Z}}$. The symbol $x_i \in A$ is also refered to as the ith *coordinate* and the dot at the lefthand side of x_0 marks the zeroth coordinate.

1.1. Definition. We define a *full shift* to be the collection of all bi-infinite sequences of symbols of an alphabet A. A *full m-shift* simply is the full shift over an alphabet $\{0, \ldots, m-1\}$.

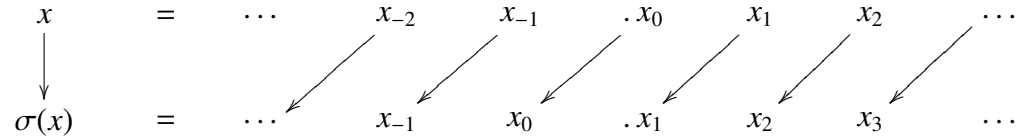
Blocks of symbols play an important role in the following theory and its generalization. A *block* or *word* u is a finite sequence of symbols in A. The *length* of a word u is denoted by

$|u|$. For $k \in \mathbb{N}$ a *k-word* is simply a word of length k. The *empty word* is denoted by ϵ and is the word of length 0. If $u = u_1 \dots u_k$, we call $u_i \dots u_j$ with $1 \leq i \leq j \leq k$ a *subword*. For $x = (x_l)_l \in \mathsf{A}^{\mathbb{Z}}$ and $u = x_i \dots x_j \subseteq x$ we also write $u = x_{[i,j]} = x_{[i,j+1)}$. u *occurs* in x, if there are $i, j \in \mathbb{Z}$, such that $u = x_{[i,j]}$. Words u, v can be *concatenated* by putting u and v together (which means that we form a new word by first writing u and then v) to uv with $|uv| = |u| + |v|$. u^n denotes concatenation of n copies of u, and $u^m u^n = u^{m+n}$ holds for all $n, m \in \mathbb{N}$. The sequence $\dots uu.uuu \dots \in \mathsf{A}^{\mathbb{Z}}$ has the shorthand notation u^∞. Recall that the dot in u^∞ is at the lefthand side of the zeroth coordinate to mark it.

The index i of a sequence $(x_i)_i$ can be interpreted as an indicator of time. The lapse of time then is a shift to the left, which gives rise to the following definition.

1.2. DEFINITION. The *shift map* $\sigma : \mathsf{A}^{\mathbb{Z}} \to \mathsf{A}^{\mathbb{Z}}$ on the full shift $\mathsf{A}^{\mathbb{Z}}$ maps an element $x \in \mathsf{A}^{\mathbb{Z}}$ to $\sigma(x)$ whose ith coordinate is given by $(\sigma(x))_i = x_{i+1}$.

The mapping σ is pictured below. We see that σ is both one-to-one and onto, so that an inverse mapping σ^{-1} also exists denoting a shift to the right.



A mapping $\phi : \mathsf{A}^{\mathbb{Z}} \to \mathsf{A}^{\mathbb{Z}}$ is called *stationary*, if $\sigma \circ \phi = \phi \circ \sigma$. In simple cases, it acts the same at each coordinate, e.g. $\phi((x_j)_j)_i = x_i + x_{i+1}$ for $(x_j)_j \in \mathsf{A}^{\mathbb{Z}}$, and thus gives us a coding operation for each coordinate of a sequence.

We now introduce a crucial notion of shift spaces, which is a subset of points of a full shift, satisfying a fixed set of constraints. This is useful, as there are many situations in coding theory where we do not make use of the full shift but contrarily consider sequences containing special words as forbidden. In fact, this gives rise to an interpretation of coders, which hide a given shift space in a larger one.

Let F be a set af words of symbols in A, which we refer to as *forbidden words*, where F may be finite or infinite. For such an F we define X_F to be the subset of sequences in $\mathsf{A}^{\mathbb{Z}}$ which do not contain any of the words in F.

1.3. DEFINITION. A *shift space* (or simply *shift*) X is a subset of the full shift $\mathsf{A}^{\mathbb{Z}}$, for which exists a set of forbidden words F such that $\mathsf{X} = \mathsf{X}_\mathsf{F}$.

1.4. EXAMPLE.

(*i*) Trivial examples are $\mathsf{A}^{\mathbb{Z}} = \mathsf{X}_\emptyset$ and $\emptyset = \mathsf{X}_{\mathsf{A}^{\mathbb{Z}}}$.
(*ii*) If X is the set of all binary sequences with no two 1's next to another, then $\mathsf{X} = \mathsf{X}_\mathsf{F}$ with $\mathsf{F} = \{11\}$. We call this shift the *golden mean shift*.

If a shift Y is contained in another shift space X we speak of Y as a *subshift of* X. There are infinitely many different shift spaces which come up with infinitely many different sets of

forbidden words. All these shifts share a common feature, the *shift invariance*: If $x \in X$ then also $\sigma(x) \in X$ as a word is forbidden wherever it starts.

If σ is the shift map of the full shift, its restriction to a shift space X is denoted by σ_X or simply σ.

If X is a shift space and $\mathcal{B}_n(X)$ the set of n-words, that occur in an $x \in X$, then we define the *language of* X respectively *the set of allowed words in* X as $\mathcal{B}(X) = \bigcup_{\mathbb{N}} \mathcal{B}_n(X)$. It follows $X = X_{\mathcal{B}(X)^c}$.

1.5. Example. The language of the full shift is

$$\mathcal{B}(A^{\mathbb{Z}}) = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, 110, 111, \ldots\},$$

whereas the language of the so called golden mean shift is

$$\mathcal{B}(X_{\{11\}}) = \{\epsilon, 0, 1, 00, 01, 10, 000, 001, 010, 100, 101, 0000, 0001, \ldots\}.$$

1.6. Definition. We call a shift space X *irreducible*, if for all $u, v \in \mathcal{B}(X)$ there is a $w \in \mathcal{B}(X)$, such that $uwv \in \mathcal{B}(X)$.

1.7. Example. The golden mean shift in example 1.4 is irreducible.

The shift $X = X_F$ with $F = \{01, 10\}$ is not irreducible, as $X = \{0^\infty, 1^\infty\}$ and hence allowed words like 0 and 1 cannot be concatenated.

At this stage we give the proper definition of a coder.

1.8. Definition. Let X, Y be shift spaces. A *coder* is a stationary map $\phi : X \to Y$ so that its image is again a shift space.

In the following sections we introduce some classical coders and shift spaces.

2. Higher Block Shifts

The first coder we study just denotes a given code in another alphabet.

2.1. Definition. Let X be a shift space over A and $A_X^{[N]} := \mathcal{B}_N(X)$ the set of all allowed N-blocks. Now we regard $(A_X^{[N]})^{\mathbb{Z}}$ as a full shift over the new alphabet $A_X^{[N]}$. We define the *Nth higher block coder* to be the map

$$\beta_N : X \to (A_X^{[N]})^{\mathbb{Z}} \text{ with } (\beta_N(x))_i = x_{[i,i+N)} \text{ for } x = (x_i)_i \in X.$$

The *Nth higher block shift* $X^{[N]}$ of X is the image of X under β_N in the full shift $(A_X^{[N]})^{\mathbb{Z}}$.

As the name suggests, a higher block shift is also a shift space ([**LM99**], Prop. 1.4.3).

2.2. Example.

$$\beta_4((x_i)_i) = \ldots \begin{pmatrix} x_0 \\ x_{-1} \\ x_{-2} \\ x_{-3} \end{pmatrix} \begin{pmatrix} x_1 \\ x_0 \\ x_{-1} \\ x_{-2} \end{pmatrix} \begin{pmatrix} x_2 \\ x_1 \\ x_0 \\ x_{-1} \end{pmatrix} . \begin{pmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \end{pmatrix} \begin{pmatrix} x_4 \\ x_3 \\ x_2 \\ x_1 \end{pmatrix} \ldots$$

3. Higher Power Shifts

Instead of using consecutively overlapping blocks, we can also define a coder with no overlaps.

3.1. DEFINITION. Let X be a shift space over A and $(A_X^{[N]})^{\mathbb{Z}}$ the full shift over the allowed N-blocks $A_X^{[N]}$. We define the *Nth higher power coder* to be the map

$$\gamma_N : X \to (A_X^{[N]})^{\mathbb{Z}} \text{ with } (\gamma_N(x))_i = x_{[iN,iN+N)} \text{ for } x = (x_i)_i \in X.$$

The *Nth higher power shift* $X^{[N]}$ of X is the image of X under γ_N in the full shift $(A_X^{[N]})^{\mathbb{Z}}$.

Again, as the name suggests, a higher power shift is a shift space ([**LM99**], Prop. 1.4.6).

4. Sliding Block Coders

Now we introduce other coders that are given by functions for each coordinate. These coders play a very important role in coding theory and give examples we will use later on. The following gives a definition of such coders.

Let X be a shift space over an alphabet A and let $\tilde{A}$ be a second alphabet. In order to construct a map $\phi : X \to \tilde{A}^{\mathbb{Z}}$ with $y = \phi(x)$, we define a *block map* Φ to be a mapping

$$\Phi : \mathcal{B}_{m+n+1}(X) \to \tilde{A}.$$

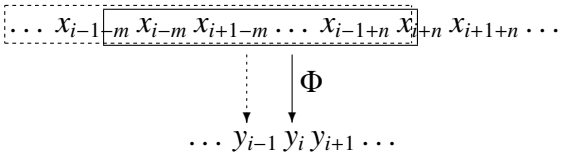
4.1. EXAMPLE. The code map of a block coder β_N is the trivial block map, if X is a shift space over A, $\tilde{A} = A_X^{[N]}, m = 0, n = N-1, Y = X^{[N]}$ and if we introduce the function describing the formation of each coordinate,

$$\Phi(x_i \dots x_{i+N}) := \beta_N((x_j)_j)_i \in A_X^{[N]}.$$

Now we do what we had in mind before, we lift block maps to coders.

4.2. DEFINITION. Let X be a shift space over A and $\Phi : \mathcal{B}_{m+n+1}(X) \to \tilde{A}$ be a block map. Then the map $\phi : X \to \tilde{A}^{\mathbb{Z}}$ with $\phi(x)_i := \Phi(x_{[i-m,i+n]})$ is called the *sliding block coder with memory m and anticipation n*. We give reverence to this construction by denoting $\phi = \Phi_\infty^{[-m,n]}$ or simply by Φ_∞. If $Y \subseteq \tilde{A}^{\mathbb{Z}}$ is a shift space with $\phi(X) = Y$, we write $\phi : X \to Y$. If $m = n = 0$, we speak of a *1-block coder*.

The action of a sliding block coder ϕ with $\phi(x)_i = \Phi(x_{[i-m,i+n]})$ as in definition 4.2 is illustrated below.



4.3. Example. Let Φ be as in example 4.1 the block map of a Nth higher block coder from 2.1. Then naturally $\phi = \Phi_\infty$ is the Nth higher block coder.

We call a sliding block coder $\phi : X \to Y$ *conjugation*, if ϕ has an inverse. In this case X and Y are *conjugate*.

4.4. Proposition. *Let X, Y be shift spaces. $\phi : X \to Y$ is a sliding block coder, if and only if $\phi \circ \sigma_X = \sigma_Y \circ \phi$ and there exists $N \geq 0$ such that $(\phi(x))_0$ is a function of $x_{[-N,N]}$.*

Proof. Let X, Y be shift spaces, $\phi : X \to Y$. If ϕ is a sliding block coder, then the block map Φ is given by definition. For the converse, let w be a $(2N+1)$-word and set $\Phi(w) := (\phi(x))_0$ for an arbitrary $x \in X$ with $x_{[-N,N]} = w$. One immediately recognizes that $(\phi(x))_i = \Phi(x_{[i-N,i+N]})$, which means that ϕ is a sliding block coder induced by Φ. □

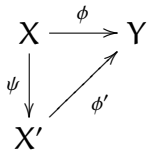
As above, also the image of a sliding block coder is a shift space.

4.5. Theorem. *Let X, Y be shift spaces and $\phi : X \to Y$ a sliding block coder. Then $\phi(X)$ is a shift space.*

Instead of proving this result we refer to [LM99], proof of theorem 1.5.13.

The next proposition will clear the connetion between higher block coders and sliding block coders.

4.6. Proposition. *Let X, Y be shift spaces and $\phi : X \to Y$ a sliding block coder. Then there exists a higher block shift X' of X, a conjugation $\psi : X \to X'$ and a 1-block coder $\phi' : X' \to Y$ such that the following diagram commutes, i.e. $\phi' \circ \psi = \phi$.*



Proof. Suppose ϕ is induced by a block map Φ with memory m and anticipation n. Let $A' = \mathcal{B}_{m+n+1}(X)$, $\psi : X \to A'^{\mathbb{Z}} : \psi(x)_i = x_{[i-m,i+n]}$. Hence $\psi = \sigma^{-m} \circ \beta_{m+n+1}$ and $X' = \psi(X) = X^{[m+n+1]}$ is a shift space. As σ and β_{m+n+1} are conjugations, so is ψ. Thus $\phi' := \phi \circ \psi^{-1}$ is a 1-block coder. □

Hence we can assume without any loss of generality that a sliding block coder is a 1-block coder on a suitable shift space.

5. Linear Coders

In this section we study special sliding block coders, namely linear block maps. We may introduce linearity of block maps, if the used alphabets are fields. The following definitions are taken from [NC00].

Let X be a shift space over a (finite) field or vector space, $\tilde{\mathsf{A}}$ another (finite) field or vectorspace and $\Phi : \mathcal{B}_{m+n+1}(\mathsf{X}) \to \tilde{\mathsf{A}}$ a block map. A coder $\phi = \Phi_\infty$ is linear, if its block map Φ is linear. This is the context of our next definition.

5.1. DEFINITION. Let $\mathbb{F}$ be a (finite) field. A *linear* $[k, n]$*-coder* is given by a linear block map $\Phi_G : \mathbb{F}^k \to \mathbb{F}^n$ defined by an $n \times k$-matrix G through $\Phi_G(x) = Gx \in \mathbb{F}^n$ for all $x \in \mathbb{F}^k$.

Note that for this definition neither the image nor the pre-image of a linear coder need to be linear subspaces of the full shift over $\mathbb{F}^k$ respectively $\mathbb{F}^n$. Instead we consider a linear coder as a sliding block coder, and thus its image is a shift space again.

The advantage of this definition is a transparent connection between the letter we want to code and its code letter, as the image of Φ_G is the linear span of the columns in G.

Transmission through noisy channels make clear that there is a need for error correction. It is hard to extract information necessary for error correction out of G. In order to do this, we need an instrument to check whether a received sequence is corrupted or not. Hence our instrument should distinguish between allowed letters and those letters which are not allowed. We solve this problem by defining a linear block map Φ_H whos kernel is given by the image of Φ_G.

5.2. DEFINITION. Let Φ be an injective linear block map. Any $(n-k) \times n$-matrix H with rank $(n-k)$ and kernel $\Phi(\mathbb{F}^k)$ is called a *parity check matrix of* Φ.

Such parity check matrices H obviously exist, as the connection of both G and H is simply a change of image and kernel of G and H: Given Φ_G repectively G, choose $(n-k)$ linearly independent vectors $x_1, \ldots, x_{n-k}$ orthogonal to all columns of G. Now set $H = (x_1 \ldots x_{n-k})^T$. As Φ_G is injective, the rank of G is k and so is the dimension of the kernel of H by definition. Hence H has rank $(n-k)$.

If conversely Φ_H respectively H are given, there are several linear block maps Φ_G with the property that H is their parity check matrix: Given H, choose k linearly independent vectors $y_1, \ldots, y_k$ spanning the kernel of H, then each choice of vectors $y_1, \ldots, y_k$ defines a coder for H via $G = (y_1 \ldots y_k)$.

We further note that by definition, $HG = 0$. Hence if G is given in the form $G = (\mathbb{1}_k \; B)^T$, we can choose $H = (-B \; \mathbb{1}_{n-k})$.

This notion gives us the desired instrument for the problem of error correction for injective linear coders, as it detects errors: Let x be a letter in $\mathbb{F}^k$ and let $y = Gx \in \mathbb{F}^n$ be the code letter of x. Assume a noisy channel disturbs the code letter y so that the channels output is $y' = y + n$. As all code words satisfy $Hy = 0$, we would get $Hy' = Hn$ and call this an *error syndrome*.

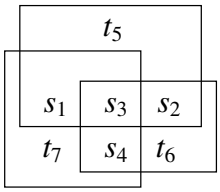
The next issue now would be to recalculate y out of the error syndrome. But instead of going deeper into the recalculation of code letters, we illustrate this with an example of a linear coder.

5.3. EXAMPLE. $[7, 4]$*-Hamming coder*

Let $\mathbb{F} = \mathbb{F}_2$. A $[7, 4]$-Hamming coder is a $[7, 4]$-linear code

$$\phi : \mathbb{F}^4 \ni (s_1 s_2 s_3 s_4)^t \mapsto (s_1 s_2 s_3 s_4 t_5 t_6 t_7)^t \in \mathbb{F}^7$$

such that in the following diagram the parity of each box is even, i.e. the sum modulo 2 equals 0.



We get

s_1	s_2	s_3	s_4	t_5	t_6	t_7
0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	1
0	0	1	1	1	0	0
0	1	0	0	1	1	0
		⋮		⋮		

and thus

$$G = \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right).$$

Note that all code words differ in at least three places from each other and that only 16 of all 128 words in $\mathbb{F}^7$ are code words.
We choose a parity check matrix H according to the discussion after 5.2 and get

$$H = \left(\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right).$$

We see that in each row of H we have four 1's. The multiplication $Hy' \stackrel{!}{=} 0$ corresponds to the rule of choosing the symbols t_5, t_6 and t_7 such that the sum of the symbols in one field equals 0 modulo 2. If, for example, the original code word was $(1000101)^T$ and the channel changed the second coordinate from 0 to 1, we count two "unhappy" boxes, the upper one and the one on the right hand side. This is represented in $H(1100101)^T = (110)^T$ - the first 1 stands for the upper box and the second for the right box. Those boxes share the second and the third coordinate. As the left box doesn't signalize an error, the most probable error is a change of the second coordinate.

6. Convolutional Coders

Engineers have quite a different understanding from codes and coders than we have presented until now. The purpose of this section is to have a look at this second approach, as these "convolutional codes" have wide applications. We are also going to use this notion in the quantum case later on.

Let $\mathbb{F}$ be a finite field, $\mathbb{F} = \mathbb{F}_2$ may serve as an example, and consider formal Laurent series $f(t) = \sum_{i=-\infty}^{\infty} f_i t^i$, $f_i \in \mathbb{F}$. Now a given convolutional coder is a black box ϕ in which we insert our Laurent series and of which we know that it operates linearly on sums of polynomes. We may feed it with an impulse δ_0 with $\delta_0(t) = \sum_{i=-\infty}^{\infty} \delta_{0i} t^i$, δ_{ij} standing for the Kronecker symbol, and register a finite Laurent polynomial as the output $\phi(\delta_0)$. Then ϕ maps Laurent series f to $\phi(f) = \phi(\delta_0) \cdot f$. In order to see this, we set $\phi(\delta_0)(t) = \sum_{k=-m}^{n} d_k t^k$. We further remark that $\delta_0(t) = t$ and hence $\sigma^i(\delta_0)(t) = t^i$ and that the multiplication of a Laurent polynomial with a Laurent series is just the convolution of their coefficients. We obtain

$$\begin{aligned}\phi(f) &= \phi\Big(\sum_{i\in\mathbb{Z}} f_i \sigma^i(\delta_0)\Big) = \sum_{i\in\mathbb{Z}} f_i \sigma^i(\phi(\delta_0)) \\ &= \sum_{i\in\mathbb{Z}} \sum_{k=-n}^{m} d_k f_i \sigma^{k+i}(\delta_0) = \sum_{i\in\mathbb{Z}} \underbrace{\Big(\sum_{k=-m}^{n} d_{-k} f_{i+k}\Big)}_{=(d_j)_j * (f_j)_j} \sigma^i(\delta_0) \\ &= \sum_{k=-n}^{m} d_k \sigma^k(\delta_0) \cdot \sum_{i\in\mathbb{Z}} f_i \sigma^i(\delta_0) = \phi(\delta_0) \cdot f.\end{aligned}$$

This fact is the reason why we speak of ϕ as a *convolutional coder*. Let us follow this idea with an example.

6.1. EXAMPLE. Let $\mathbb{F} = \mathbb{F}_2$ and let $\phi(\delta_0) = 1 + t$ be the impulse answer, $I(t) = \sum_{i=-\infty}^{\infty} I_i t^i$ our input Laurent series. Then the output series is given by

$$O(t) = \phi(\delta_0)(t) \cdot I(t) = \sum_{i=-\infty}^{\infty} (1+t) I_i t^i = \sum_{i=-\infty}^{\infty} (I_{i-1} + I_i) t^i.$$

If we go back to the shift space notation of the previous sections and set $I_{[i,i+1]} = (I_{i-1}\, I_i)$, the map ϕ in the example obviously defines a block map

$$\Phi : \mathbb{F}_2^2 \to \mathbb{F}_2 : I_{[i,i+1]} \mapsto I_{i-1} + I_i = (1\ 1) I_{[i,i+1]}.$$

Φ is related to the matrix $G = (1\ 1)$ which corresponds to the coefficients of the impulse answer $\phi(\delta_0)$.

In the following, we define convolutional coders more generally than in the above example and discuss the resulting block maps and parity check matrices.

Let $\mathcal{L}(\mathbb{F})$ denote the set auf *Laurent series* $f(t) = \sum_{i=-\infty}^{\infty} f_i t^i$, $f_i \in \mathbb{F}$. As above, we understand this notation as purely formal, so that we do not worry about convergence. A bi-finite Laurent series $\sum_{i=-m}^{n} f_i t^i$ is called a *Laurent polynomial*. In order to keep the linear block idea in mind,

note that $\mathcal{L}(\mathbb{F})$ is isomorphic to the full shift $\mathbb{F}^{\mathbb{Z}}$ via the identification of $\sum_{i=-\infty}^{\infty} f_i t^i$ and $(f_i)_{i\in\mathbb{Z}}$. We analogously identify $\mathcal{L}(\mathbb{F}^k)$, the Laurent series with vector coefficients, with $(\mathbb{F}^k)^{\mathbb{Z}}$ and obtain

$$\mathcal{L}(\mathbb{F}^k) \simeq \mathcal{L}(\mathbb{F})^k \simeq (\mathbb{F}^k)^{\mathbb{Z}} \simeq (\mathbb{F}^{\mathbb{Z}})^k.$$

6.2. Definition. Let $G(t) = [G_{ij}(t)]_{n\times k}$ a matrix of Laurent polynomials.
A (k, n)-*convolutional coder* is a map

$$F : \mathcal{L}(\mathbb{F})^k \to \mathcal{L}(\mathbb{F})^n : I(t) \mapsto O(t) = G(t) \cdot I(t)$$

for vectors of Laurent series $I(t) = [I_1(t), \ldots, I_k(t)]^T$ and $O(t) = [O_1(t), \ldots, O_n(t)]^T$.

We illustrate this definition with the following example.

6.3. Example. $\mathbb{F} = \mathbb{F}_2, G(t) = \begin{pmatrix} 1 & 0 \\ 0 & t \\ 1+t & t \end{pmatrix}$.

Then

$$O(t) = G(t) \cdot I(t) = [I_1(t),\ t \cdot I_2(t),\ (1+t) \cdot I_1(t) + t \cdot I_2(t)]^T$$

and with

$$I_1(t) = \sum_{i=-\infty}^{\infty} I_1^i t^i,\ I_2(t) = \sum_{i=-\infty}^{\infty} I_2^i t^i \text{ respectively } I(t) = \sum_{i=-\infty}^{\infty} (I_1^i, I_2^i)^T t^i$$

we have

$$O(t) = \sum_{i=-\infty}^{\infty} (I_1^i, I_2^{i-1}, I_1^i + I_1^{i-1} + I_2^{i-1})^T t^i.$$

Hence the image of the given convolutional coder in shift space notation is

$$F((\mathbb{F}_2^2)^{\mathbb{Z}}) = \{...(I_1^i, I_2^{i-1}, I_1^i + I_1^{i-1} + I_2^{i-1})^T ... \in (\mathbb{F}_2^3)^{\mathbb{Z}}; I_1^k, I_2^k \in \mathbb{F}_2\}.$$

6.4. Remark. As the shift map σ here is realized by multiplication with t, images of convolutional coders are shift invariant,

$$F(\sigma(I(t)) = G(t) \cdot t \cdot I(t) = t \cdot O(t) = \sigma(F(I(t))).$$

Now we have a look at the connection of convolutional coders and sliding block coders we already saw in the discussion of example 6.1. Analogously to the fact that an operator on $L^2(\mathbb{R})$ is linear and invariant under translations if and only if it is a convolution operator, we get the following theorem.

6.5. Theorem. *Let $F : (\mathbb{F}^k)^{\mathbb{Z}} \to (\mathbb{F}^n)^{\mathbb{Z}}$, $X \subseteq (\mathbb{F}^n)^{\mathbb{Z}}$. Then*

(*i*) *F is a convolutional coder, if and only if F is a linear sliding block coder of the full shift over the alphabet $\mathbb{F}$,*
(*ii*) *X is the image of a convolutional coder, if and only if X is a linear irreducible shift space over the alphabet $\mathbb{F}$.*

The proof of the theorem follows the intuition we obtained in the discussion of example 6.1. To get an idea of how things work out in the higher dimensional setting, we present one direction of the proof. For the rest of the proof we refer to [**LM99**], proof of theorem 1.6.3.

PROOF. "⇒": Let $F : \mathcal{L}(\mathbb{F})^k \to \mathcal{L}(\mathbb{F})^n$ be a convolutional coder with the $G(t) = [G_{ij}]_{ij}$ as its matrix of Laurent polynomials. If we admit some coefficients g_{ij}^l to be zero, we may assume that all Laurent polynomials in $G(t)$ are of the form

$$G_{ij}(t) = \sum_{l=-N}^{M} g_{ij}^l \cdot t^l \text{ and } I_i(t) = \sum_{l=-\infty}^{\infty} I_i^l \cdot t^l.$$

We easily see that $F : I(t) \mapsto F(I(t))$ is induced by a map $\Phi : (\mathbb{F}_2^k)^{[M+N+1]} \to \mathbb{F}_2^n$ with

$$\Phi\left((I_1^{0-M} \dots I_1^{0+N}) \dots (I_k^{0-M} \dots I_k^{0+N})\right)^T = \left(\sum_{l=-M}^{N}\sum_{j=1}^{k} g_{1j}^{-l} I_j^{0+l}, \dots, \sum_{l=-M}^{N}\sum_{j=1}^{k} g_{nj}^{-l} I_j^{0+l}\right)^T,$$

describing the formation of the zeroth coordinate of $O(t)$. Hence F is shift invariant and so F is a sliding block coder of the full shift over $\mathbb{F}$ by proposition 4.4. As Φ is linear, so is F. Thus the image of the vector space $\mathcal{L}(\mathbb{F})^k$ under the linear transformation F also is a vector space. It is easy to see that $F(\mathcal{L}(\mathbb{F})^k)$ is irreducible, so $F(\mathcal{L}(\mathbb{F})^k)$ is a linear irreducible shift space. □

As convolutional coders are linear sliding block codes, we may calculate the matrix G of the block map and a paritiy check matrix H. This will lead us to syndrome equations for error correction of convolutional codes.

6.1. Convolutional Coders and Syndrome Equations. In this subsection we exploit the structure of convolutional coders as linear sliding block coders by obtaining equations describing coded words out of block maps.

First we investigate the matrix form of block maps of sliding block coders. At the end of section 6 we saw that $(O(t))_i$ only depends on $\left((I_1^{-M} \dots I_1^N) \dots (I_k^{-M} \dots I_k^N)\right)^t$ if M denotes the maximal power of the Laurent polynomials and $-N$ the minimal,

$$\Phi\left((I_1^{-M} \dots I_1^N) \dots (I_k^{-M} \dots I_k^N)\right)^T = \left(\sum_{l=-M}^{N}\sum_{j=1}^{k} g_{1j}^{-l} I_j^l, \dots, \sum_{l=-M}^{N}\sum_{j=1}^{k} g_{nj}^{-l} I_j^l\right)^T.$$

Thus G_Φ is given through

$$O_i = \begin{pmatrix} O_1^i \\ \vdots \\ O_n^i \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} g_{11}^{-M} & \cdots & g_{11}^{N} \\ g_{12}^{-M} & \cdots & g_{12}^{N} \end{pmatrix} & \cdots & \begin{pmatrix} g_{k1}^{-M} & \cdots & g_{k1}^{N} \\ g_{k2}^{-M} & \cdots & g_{k2}^{N} \end{pmatrix} \\ & \vdots & \\ \begin{pmatrix} g_{1n}^{-M} & \cdots & g_{1n}^{N} \end{pmatrix} & \cdots & \begin{pmatrix} g_{kn}^{-M} & \cdots & g_{kn}^{N} \end{pmatrix} \end{pmatrix} \cdot \begin{pmatrix} \begin{pmatrix} I_1^{i-M} \\ \vdots \\ I_1^{i+N} \end{pmatrix} \\ \vdots \\ \begin{pmatrix} I_k^{i-M} \\ \vdots \\ I_k^{i+N} \end{pmatrix} \end{pmatrix}.$$

If we set $L_C = M + N + 1$ (the reason for the name L_C can be found in subsection 6.2), we get $G_\Phi \in \mathbb{F}^{n \times L_C \cdot k}$.

Now we would like to discuss about parity check matrices H_Φ as defined in 5.2. We see that in general cases, one output letter is insuffiecient to recalculate the input, as one input letter influences several output letters. This is why convolutional coders are so interesting. Let ϕ be a convolutional coder such that $\phi(x)_i = \Phi(x_{[i-M,i+N]})$ and $\Phi(x_{[i-M,i+N]}) = G_\Phi x_{[i-M,i+N]}$, $G_\Phi \in \mathbb{F}^{n \times L_C \cdot k}$. If G_Φ has rank n, then any linear map mapping the image of G_Φ to zero is the null map and hence so is any parity check matix H_Φ of ϕ.

Therefore instead of using parity check matrices exploiting the orthogonal complement of an image subspace we rather use another feature of convolutional coders in order to describe output sequences. This feature is the multiple influence of input letters on output letters, as one input letter (I_i), $i \in \mathbb{Z}$, influences L_C output letters $O_{i-N}, \ldots, O_{i+M}$. In other words, we have $n \cdot L_C$ linear equations with k variables. If we are able to eliminate these k variables, we obtain equations for the output letters.

This is best explained if we have a look at example 6.3, where we had

$$\begin{array}{rcl} O_1[k] &=& a_k \\ O_2[k] &=& b_{k-1} \\ O_3[k] &=& a_k + a_{k-1} + b_{k-1} \end{array} \quad \text{and} \quad \begin{array}{rcl} O_1[k+1] &=& a_{k+1} \\ O_2[k+1] &=& b_k \\ O_3[k+1] &=& a_{k+1} + a_k + b_k. \end{array}$$

These equations lead to two equations that any kth output letter must satisfy,

$$O_3[k] + O_1[k] + O_1[k-1] + O_2[k] = 0$$

and

$$O_3[k+1] + O_1[k+1] + O_1[k] + O_2[k+1] = 0.$$

6.6. Remark. The definition of quantum stabilizer block maps in [NC00] and hence quantum convolutional block maps by Ollivier and Tillich in [OT03] and [OT04] is based on the idea of syndrome equations.

6.2. Visualisation of Convolutional Coders. Here we give an illustration of convolutional coders. It is based on a picture of convolutional coders one often finds in engineering books.

We use example 6.3, where we had

$$G(t) = \begin{pmatrix} 1 & 0 \\ 0 & t \\ 1+t & t \end{pmatrix}$$

respectively

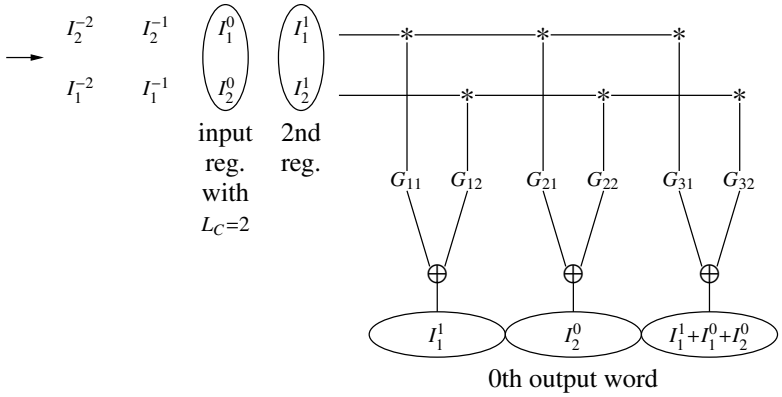
$$O(t) = \phi(I(t)) = \sum_{i=-\infty}^{\infty} (I_1^i, I_2^{i-1}, I_1^i + I_1^{i-1} + I_2^{i-1})^T t^i$$

for $I(t) = \sum_{i=-\infty}^{\infty} (I_1^i, I_2^i) t^i$. We focus on the spaces $(\mathbb{F}^2)^{\mathbb{Z}}$ respectively $(\mathbb{F}^{\mathbb{Z}})^2$ instead of $\mathcal{L}(\mathbb{F}^2)$ and the corresponding spaces for the output. We define the *constraint length* to be the number of

influencing coordinates, here $L_C = 2$. We further introduce vectors describing the coefficients in G to be able to mark the convolution,

$$\begin{aligned} G_{11} &= (1,0) \simeq 1 \\ G_{12} &= (0,0) \simeq 0 \\ G_{21} &= (0,0) \simeq 0 \\ G_{22} &= (0,1) \simeq t \\ G_{31} &= (1,1) \simeq 1+t \\ G_{32} &= (0,1) \simeq t. \end{aligned}$$

Thus we get the following visualization.



This uses the fact that for $G(t) = [G_{ij}(t)]_{k\times n}$ with $G_{ij}(t) = \sum_{l=-n}^{m} g_{ij}^l t^l$ we have

$$O(t) = I(t)\cdot G(t) = \begin{pmatrix} I_1(t)G_{11}(t) + ... + I_k(t)G_{k1}(t) \\ I_1(t)G_{12}(t) + ... + I_k(t)G_{k2}(t) \\ \vdots \\ I_1(t)G_{1n}(t) + ... + I_k(t)G_{kn}(t) \end{pmatrix}.$$

If M stands for the highest power in G_{11} and $-N$ the smallest, we get

$$\begin{aligned} I_1(t)G_{11}(t) &= (\textstyle\sum_{i=-\infty}^{\infty} I_1^i t^i)(\sum_{l=-N}^{M} g_{11}^l t^l) \\ &= \textstyle\sum_{i=-\infty}^{\infty} (\underbrace{\sum_{l=-N}^{M} I_1^{i-l} g_{11}^l}_{(I_1^i)_i \star (g_{11}^i)_i}) \cdot t^i. \end{aligned}$$

We get $L_C = M + N + 1$, as I_j^{i-M} is the oldest coordinate in the register at step i and I_j^{i+N} the youngest.

CHAPTER 2

Notation and Basics of Operator Algebras

In this chapter we fix some notations and then give a brief overview over the necessary definitions concerning groups and algebras, inductive limits, AF-algebras and states. For further details, we refer to [Sak98], [Tak79], [Tak03], [Ped79] and [BR87].

1. Notation

By $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{C}$ we denote the natural numbers, whole numbers and complex numbers and set $\mathbb{N}_n = \{1, \ldots, n\} \subseteq \mathbb{N}$. i denotes the imaginary symbol and the dimension of a vector space is denoted by dim.

We consider only separable Hilbert spaces over the field of complex numbers, usually denoted by $\mathcal{H}$. Its scalar product $\langle \cdot\,, \cdot \rangle$ is linear in the second component and anti-linear in the first. $\mathcal{K}^\perp$ stands for the orthogonal complement of a linear subspace $\mathcal{K} \subseteq \mathcal{H}$ and $\mathcal{B}(\mathcal{H})$ stands for the bounded linear operators on $\mathcal{H}$ equipped with the operator norm $\|\cdot\|$.

x^* denotes the adjoint operator of $x \in \mathcal{B}(\mathcal{H})$. For an isometry $c : \mathcal{H}_1 \to \mathcal{H}_2$ between Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, we define $\mathrm{Ad}(c) : \mathcal{B}(\mathcal{H}_1) \to \mathcal{B}(\mathcal{H}_2)$ by setting $\mathrm{Ad}(c)x := c^* x c$ for all $x \in \mathcal{B}(\mathcal{H}_1)$. If $\mathcal{H}$ has finite dimension n, we identify it with $\mathbb{C}^n$. In this case, we write $\mathbb{M}_n$ instead of $\mathcal{B}(\mathcal{H})$ and mean the complex $n \times n$-matrices. For $\xi \in \mathbb{C}^n$ let $t_{\xi,\eta} \in \mathbb{M}_n$ be the rank-1-operator defined by $t_{\xi,\eta} : \varphi \mapsto \xi \cdot \langle \eta\,, \varphi \rangle$.

An important subject will be $\mathbb{M}_2$ and tensor products of $\mathbb{M}_2$. For natural numbers n, k set $N = 2^n$ and $K = 2^k$ and, for example, $\mathbb{M}_N = \mathbb{M}_{2^n}$.

Let tr_2 denote the normalized trace on $\mathbb{M}_2$ and tr_N the normalized trace on $\mathbb{M}_N$ given by the product state $\bigotimes^n \mathrm{tr}_2$ via the identification $\mathbb{M}_N = \bigotimes^n \mathbb{M}_2$. If the size of the matix algebra is clear, we forget the indices.

When dealing with diagonal matrices, we use the notation $\mathrm{diag}(a_1, \ldots, a_n)$ for a diagonal matrix with entries $a_1, \ldots, a_n$.

2. Groups and Algebras

A **-algebra* is an algebra closed under the involution $*$. Let $G(\cdot)$ be the group and $\mathcal{A}(\cdot)$ the *-algebra generated by the elements standing between the brackets. Let further denote $\mathrm{lin}(\cdot)$ the linear span of the elements between the brackets.

For groups $(G, *)$ and $(H, *)$, a *group homomorphism* is a map $\Phi : G \to H$ such that $\Phi(g * h) = \Phi(g) * \Phi(h)$ for all $g, h \in G$. Φ is a *group isomorphism*, if it is one-to-one. If G is a commutative group, the set of all group homomorphisms from G into the group of complex numbers is called the *spectrum* of G and we denote it by $\hat{G}$.

A *C*-algebra* $\mathcal{A}$ is a Banach *-algebra such that $\|xy\| \leq \|x\|\|y\|$ and $\|xx^*\| = \|x\|^2$ for all $x, y \in \mathcal{A}$. If $\mathcal{A}$ is a C*-algebra with identity $\mathbb{1}$, we call $\mathcal{A}$ *unital*. In this case, the *spectrum* $\sigma(x)$ of $x \in \mathcal{A}$ stands for the set of all complex numbers λ such that $(x - \lambda\mathbb{1})$ is not invertible in $\mathcal{A}$. If $\mathcal{A}$ has no identity, the spectrum $\sigma(x)$ of $x \in \mathcal{A}$ is the spectrum of x as an element of the C*-algebra generated by $\mathcal{A}$ and the identity $\mathbb{1}$.

For C*-algebras $\mathcal{A}$ and $\mathcal{B}$, a linear map $\Phi : \mathcal{A} \to \mathcal{B}$ is called a *homomorphism*, if $\Phi(xy) = \Phi(x)\Phi(y)$ for $x, y \in \mathcal{A}$. Φ is a **-homomorphism*, if further $\Phi(x^*) = \Phi(x)^*$. We say Φ is an *isomorphism* respectively a **-isomorphism*, if Φ is a one-to-one homomorphism respectively a one-to-one *-homomorphism. We say that C*-algebras $\mathcal{A}, \mathcal{B}$ are *isomorphic*, if there exists a *-isomorphism of $\mathcal{A}$ onto $\mathcal{B}$.

A *representation* $(\pi, \mathcal{H})$ is a *-homomorphism π of a C*-algebra $\mathcal{A}$ into the C*-algebra $\mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$. Two representations $(\pi_1, \mathcal{H}_1)$ and $(\pi_2, \mathcal{H}_2)$ are said to be *unitarily equivalent*, if there exists a unitary map U from $\mathcal{H}_1$ onto $\mathcal{H}_2$ such that $U\pi_1(x)U^* = \pi_2(x)$ for all $x \in \mathcal{A}$. If $\pi(x) \neq 0$ for any $0 \neq x \in \mathcal{A}$, then π is called *faithful*.

If $\mathcal{A}$ is a commutative C*-algebra, we call the set of all nontrivial *-homomorphisms from $\mathcal{A}$ into the algebra of complex numbers the *spectrum* of $\mathcal{A}$ and denote it by $\hat{\mathcal{A}}$.

Let $\mathcal{A}, \mathcal{B}$ be C*-algebras. A self-adjoint element $a \in \mathcal{A}$ is said to be *positive*, if $a = y^*y$ for some $y \in \mathcal{A}$. Note that this is equivalent to the fact that a has a positive spectrum, $\sigma(a) \subseteq [0, \infty)$. A linear mapping $T : \mathcal{A} \to \mathcal{B}$ is called *positive*, if T maps positive elements of $\mathcal{A}$ to positive elements of $\mathcal{B}$, in other words, if $T(x^*x)$ is positive for all $x \in \mathcal{A}$. Let $\mathbb{M}_n(\mathcal{A})$ denote the set of all $n \times n$-matrices $a = (a_{ij})_{i,j}$ with entries $a_{ij} \in \mathcal{A}$. Then we may identify $\mathbb{M}_n(\mathcal{A})$ with $\mathbb{M}_n \otimes \mathcal{A}$ by a identification mapping $\gamma : \mathbb{M}_n(\mathcal{A}) \to \mathbb{M}_n \otimes \mathcal{A}$ such that $(a_{ij})_{i,j}$ is mapped to $\sum_{i,j=1}^n t_{e_j,e_i} \otimes a_{ij}$ for an orthonormal basis $(e_i)_{i=1}^n$ of $\mathbb{C}^n$. Let $T : \mathcal{A} \to \mathcal{B}$ be linear. Then we may define

$$T_n : \mathbb{M}_n(\mathcal{A}) \to \mathbb{M}_n(\mathcal{B}) : (a_{ij})_{i,j} \mapsto (T(a_{ij}))_{i,j}.$$

T is *completely positive*, if T_n is positive for all $n \in \mathbb{N}$.

If we combine these definitions, we obtain the following two corollaries.

2.1. COROLLARY. *Let $\mathcal{A}, \mathcal{B}$ be C*-algebras and $T : \mathcal{A} \to \mathcal{B}$ a linear map. Then T is completely positive if and only if*

$$\sum_{i,j=1}^{n} y_i^* T(x_i^* x_j) y_j \geq 0$$

for all $n \in \mathbb{N}$, $x_1, \ldots, x_n \in \mathcal{A}$ and $y_1, \ldots, y_n \in \mathcal{B}$.

2.2. COROLLARY. *Let $\mathcal{A}, \mathcal{B}$ be C*-algebras. If $T : \mathcal{A} \to \mathcal{B}$ is a *-homomorphism, then T is completely positive and $T(\mathbb{1}) = \mathbb{1}$.*

Furthermore there is another important theorem about completely positive maps due to Choi [Cho75].

2.3. Theorem. *Let $T : \mathbb{M}_k \to \mathbb{M}_n$ be a linear map. Then T is completely positive if and only if there exist $n \in \mathbb{N}$ and operators $a_1, \dots, a_n : \mathbb{C}^n \to \mathbb{C}^k$ such that for all $x \in \mathbb{M}_k$*

$$Tx = \sum_{i=1}^{n} a_i^* x a_i.$$

We call $(a_i)_{i=1}^n$ an *unravelling* of T. Unravelings are not uniquely determined. But if the matrices $a_1, \dots, a_n$ are linearly independent and $(b_l)_{l=1}^m$ is an other unravelling of T, the matrices are determined up to a transformation of the form

$$b_l = \sum_{j=1}^{n} v_{ij} a_j$$

for an isometric $m \times n$-matrix $v = (v_{ij})_{ij}$. If further the matrices $b_1, \dots, b_m$ are also independent, we get $m = n$ and $v \in \mathbb{M}_n$ is unitary. In this case, $(a_i)_i$ and $(b_l)_l$ are called *unitary equivalent unravellings* of T.

We can easily calculate the operator norm of a completely positive map due to the following lemma by Paulsen [Pau86].

2.4. Lemma. *Let $\mathcal{A}, \mathcal{B}$ be C*-algebras, $\mathbb{1} \in \mathcal{A}$ and $T : \mathcal{A} \to \mathcal{B}$ a completely positive map. Then $\|T\| = \|T(\mathbb{1})\|$.*

3. Inductive Limits and AF-Algebras

As an important construction, we study inductive limits of C*-algebras in this section. This introduction is mainly based on [Tak03].

An *inductive sequence $(\mathcal{A}_n, \pi_n)_{n\in\mathbb{N}}$ of C*-algebras* is given by a sequence $(\mathcal{A}_n)_{n\in\mathbb{N}}$ of C*-algebras together with a sequence $(\pi_n)_{n\in\mathbb{N}}$ of injective *-homomorphisms $\pi_n : \mathcal{A}_n \to \mathcal{A}_{n+1}$ for each $n \in \mathbb{N}$,

$$\mathcal{A}_1 \xrightarrow{\pi_1} \mathcal{A}_2 \xrightarrow{\pi_2} \mathcal{A}_3 \longrightarrow \cdots \longrightarrow \mathcal{A}_n \xrightarrow{\pi_n} \mathcal{A}_{n+1} \cdots$$

If each $\mathcal{A}_n$ is unital and each π_n preserves the identity, $(\mathcal{A}_n, \pi_n)_n$ is called *unital*. Two sequences $(\mathcal{A}_n^1, \pi_n^1)_n$ and $(\mathcal{A}_n^2, \pi_n^2)_n$ are *conjugate* if there exist isomorphisms $\theta_n : \mathcal{A}_n^1 \to \mathcal{A}_n^2$ such that $\pi_n^2 \circ \theta_n = \theta_{n+1} \circ \pi_n^1$, i.e. the following diagram commutes.

$$\begin{array}{ccc} \mathcal{A}_n^1 & \xrightarrow{\pi_n^1} & \mathcal{A}_{n+1}^1 \\ {\scriptstyle\theta_n}\downarrow & & \downarrow{\scriptstyle\theta_{n+1}} \\ \mathcal{A}_n^2 & \xrightarrow[\pi_n^2]{} & \mathcal{A}_{n+1}^2 \end{array}$$

If the θ_n are only homomorphisms, we call $(\theta_n)_n$ a homomorphism of $(\mathcal{A}_n^1, \pi_n^1)_n$ and $(\mathcal{A}_n^2, \pi_n^2)_n$ instead.

Now let $(\mathcal{A}_n, \pi_n)_n$ be an inductive sequence of C*-algebras. For $k \in \mathbb{N}$ we set

$$\pi_{n+k,n} := \pi_{n+k-1} \circ \pi_{n+k-2} \circ \cdots \circ \pi_{n+1} \circ \pi_n$$

and $\pi_{n,n} = \mathrm{id}$. It follows that

$$\pi_{k,j} \circ \pi_{j,i} = \pi_{k,i} \text{ for } i \leq j \leq k.$$

By viewing $(A_n)_n$ as a sequence of disjoint sets, we set

$$X := \bigcup_{n\in\mathbb{N}} \mathcal{A}_n \text{ with } \mathcal{A}_n \cap \mathcal{A}_m = \emptyset \text{ for } n \neq m$$

and introduce an equivalence relation by writing $a \sim b$ for $a \in \mathcal{A}_n$ and $b \in \mathcal{A}_m$, if $\pi_{l,n}(a) = \pi_{l,m}(b)$ for an $l \in \mathbb{N}$. Hence two elements of X are considered to be the same, if they eventually get mapped onto the same element. We obtain a new set $\mathcal{A}_\infty := X/\sim$, the set of all equivalence classes in X, where we denote the equivalence class of $a \in X$ by $[a]$ or $\pi_{\infty,n}(a)$, if $a \in \mathcal{A}_n$. We define a *-algebra structure on $\mathcal{A}_\infty$ as follows. Let $\lambda \in \mathbb{C}$, $a \in \mathcal{A}_n$ and $b \in \mathcal{A}_m$ and choose $l > n, m$. Then set

$$\begin{aligned}
\lambda[a] &= [\lambda a], \\
[a] + [b] &= [\pi_{l,n}(a) + \pi_{l,m}(b)], \\
[a] \cdot [b] &= [\pi_{l,n}(a) \cdot \pi_{l,m}(b)], \\
[a]^* &= [a^*].
\end{aligned}$$

These operations do not depend on the choice of the representative and make $\mathcal{A}_\infty$ to a *-algebra. Each $\pi_{\infty,n}$ is a *-isomorphism from $\mathcal{A}_n$ onto $\pi_{\infty,n}(\mathcal{A}_n) \subset \mathcal{A}_\infty$ and

$$\begin{aligned}
&\pi_{\infty,1}(\mathcal{A}_1) \subset \pi_{\infty,2}(\mathcal{A}_2) \subset \cdots \subset \pi_{\infty,n}(\mathcal{A}_n) \subset \cdots \\
&\mathcal{A}_\infty = \bigcup_{n\in\mathbb{N}} \pi_{\infty,n}(\mathcal{A}_n).
\end{aligned}$$

As each $\mathcal{A}_n$ is a C*-algebra, so is its *-isomorphic image $\pi_{\infty,n}(\mathcal{A}_n)$ and the norms on $\pi_{\infty,n}(\mathcal{A}_n)$ for $n \in \mathbb{N}$ induce a norm on $\mathcal{A}_\infty$. This norm makes $\mathcal{A}_\infty$ to a *-algebra, and the completion $\mathcal{A}$ of $\mathcal{A}_\infty$ becomes a C*-algebra.

In the following we identify $\mathcal{A}_n$ with $\pi_{\infty,n}(\mathcal{A}_n)$ for simplicity.

3.1. DEFINITION. The C*-algebra $\mathcal{A}$ as obtained above is called the *inductive limit* of $(\mathcal{A}_n, \pi_n)_n$ and we write $\mathcal{A} = \varinjlim_n (\mathcal{A}_n, \pi_n)$.
$\mathcal{A}$ is called an *AF-algebra* or *approximately finite-dimensional*, if it is the inductive limit of a sequence of finite-dimensional C*-algebras.

We finish this section with an important example.

3.2. EXAMPLE. Let $(\mathcal{B}_n)_{n\in\mathbb{N}}$ be a sequence of unital C*-algebras and put

$$\mathcal{A}_n := \mathcal{B}_1 \otimes \mathcal{B}_2 \otimes \cdots \otimes \mathcal{B}_n \text{ for } n \in \mathbb{N},$$

where $\otimes$ stands for the minimal tensor product. If

$$\pi_n : \mathcal{A}_n \ni x \mapsto x \otimes \mathbb{1} \in \mathcal{A}_{n+1},$$

$(\mathcal{A}_n, \pi_n)_{n\in\mathbb{N}}$ is an inductive sequence of C*-algebras. We set

$$\mathcal{A} := \varinjlim_{n\in\mathbb{N}}(\mathcal{A}_n, \pi_n)_n = \varinjlim_{n\in\mathbb{N}}(\otimes_{i=1}^n \mathcal{B}_i, \pi_n)_n,$$

and call $\mathcal{A}$ the *infinite tensor product* of $(\mathcal{B}_n)_n$. In this case we often write

$$\mathcal{A} = \bigotimes_{n\in\mathbb{N}} \mathcal{B}_n.$$

4. States

In this section we give the definitions concerning states that are the most relevant ones for this work.

For a Banach space V, let V^* denote its *dual space*, the space of all continuous linear functionals over V.

A continuous linear functional φ over a C*-algebra $\mathcal{A}$ is said to be *positive*, if $\varphi(x^*x) \geq 0$ for all $x \in \mathcal{A}$. If further $\|\varphi\| = 1$ or equivalently $\varphi(\mathbb{1}) = 1$, we call φ a *state* on $\mathcal{A}$. We denote the set of all states on $\mathcal{A}$ by $\mathcal{S}(\mathcal{A}) \subseteq \mathcal{A}^*$ and call it the *state space* of $\mathcal{A}$.

A state $\varphi \in \mathcal{S}(\mathcal{A})$ on a C*-algebra $\mathcal{A}$ is called *pure*, if it is an extremal point of $\mathcal{S}(\mathcal{A})$. If $\mathcal{A} = \mathcal{B}(\mathcal{H})$, a pure state has the form $x \mapsto \langle \xi\,, x\xi\rangle$ for a unit vector $\xi \in \mathcal{H}$.

Let φ be a bounded positive linear functional over a C*-algebra $\mathcal{A}$. We introduce a bilinear functional $(x, y) = \varphi(y^*x)$ in $\mathcal{A}$ and set $J = \{x \in \mathcal{A} : \varphi(x^*x) = 0\}$. Then J is a closed left ideal of $\mathcal{A}$. Hence we can define a bilinear functional on the quotient space $\mathcal{A}/J$ such that for $x_\varphi, y_\varphi \in \mathcal{A}/J$ we have $(x_\varphi, y_\varphi) = \varphi(y^*x)$ for elements x in the class x_φ respectively $y \in y_\varphi$. (x_φ, y_φ) does not depend on the choice of the representatives x, y and thus (x_φ, y_φ) defines a scalar product on $\mathcal{A}/J$ making it to a pre-Hilbert space. Let $\mathcal{H}_\varphi$ be the completition of $\mathcal{A}/J$ with respect to this scalar product. Then $\mathcal{H}_\varphi$ is a Hilbert space. In order to define a representation of $\mathcal{A}$ on $\mathcal{H}_\varphi$, we define $\pi_\varphi(a)$ as a linear operator on $\mathcal{A}/J$ via $\pi_\varphi(a)x_\varphi = (ax)_\varphi$. Due to

$$\|\pi_\varphi(a)x_\varphi\|^2 = \varphi(x^*a^*ax) \leq \|a^*a\|\varphi(x^*x) = \|a\|^2\|x_\varphi\|^2$$

$\pi_\varphi(a)$ is bounded on $\mathcal{A}/J$ and can be extended to a bounded linear operator on $\mathcal{H}_\varphi$, which we denote by the same symbol. Obviously $a \mapsto \pi_\varphi(a)$ is a *-homomorphism of $\mathcal{A}$ into $\mathcal{B}(\mathcal{H}_\varphi)$. As

$$(\pi_\varphi(a)b_\varphi, c_\varphi) = \varphi(c^*ab) = \varphi((a^*c)^*b) = (b_\varphi, \pi_\varphi(a^*)c_\varphi)$$

for $a, b, c \in \mathcal{A}$, $\pi_\varphi(a^*) = \pi_\varphi(a)^*$. Thus $(\pi_\varphi, \mathcal{H}_\varphi)$ is a representation of $\mathcal{A}$, *the representation associated with* φ.

For the following lemma and definition we refer to [**BR87**], 4.1.19 and 4.1.20.

4.1. Lemma. *Let φ_1, φ_2 be positive linear functionals over a C*-algebra $\mathcal{A}$, $\varphi = \varphi_1 + \varphi_2$. Then are equivalent:*

(*i*) *If φ' is a positive linear functional over $\mathcal{A}$ satisfying $\varphi' \leq \varphi_1$ and $\varphi' \leq \varphi_2$, then $\varphi' = 0$.*

(*ii*) *The representation associated with φ is a direct sum of the representations associated with φ_1 and φ_2,*

$$\mathcal{H}_\varphi = \mathcal{H}_{\varphi_1} \oplus \mathcal{H}_{\varphi_2} \text{ and } \pi_\varphi = \pi_{\varphi_1} \oplus \pi_{\varphi_2}.$$

If one of the above conditions is satisfyied, then φ_1 and φ_2 are said to be *orthogonal*.

When we consider states on infinite tensor products, we may define product states. Let $(\mathcal{A}_n, \pi, n)_n = (\otimes_{i=1}^n \mathcal{B}_i, \pi_n)_n$ be an inductive sequence of C*-algebras with inductive limit $\mathcal{A}$. Let further ϕ_i be a state on B_i for all $i \in \mathbb{N}$. Then

$$\phi_1 \otimes \cdots \otimes \phi_n : \mathcal{B}_1 \otimes \cdots \otimes \mathcal{B}_n : x_1 \otimes \cdots \otimes x_n \mapsto \phi(x_1) \cdots \phi(x_n)$$

can be linearly extended from the elementary tensors to their linear hull. As this extension is bounded, we can identify it with its continuous extension onto the full tensor product $\otimes_{i=1}^n \mathcal{B}_i$ and hence $\phi_1 \otimes \cdots \otimes \phi_n$ defines a state on $\mathcal{A}_n = \otimes_{i=1}^n \mathcal{B}_i$.

Now we move to $\mathcal{A}_\infty = \bigcup_{n\in\mathbb{N}} \otimes_{i=1}^n \mathcal{B}_n$ and define here

$$\bigotimes_{n\in\mathbb{N}} \phi_n : \mathcal{A}_\infty \to \mathbb{C} : \mathcal{A}_n \ni x \mapsto \left(\otimes_{i=1}^n \phi_i\right)(x).$$

As

$$\left(\phi_1 \otimes \cdots \otimes \phi_n \otimes \phi_{n+1}\right)(x \otimes \mathbb{1}) = \left(\phi_1 \otimes \cdots \otimes \phi_n\right)(x),$$

$\otimes_{n\in\mathbb{N}} \phi_n$ is well defined and as it is bounded, it has a continuous extension onto $\mathcal{A}$, which we denote by the same symbol. Of course, $\otimes_{n\in\mathbb{N}} \phi_n$ is a state.

We call $\otimes_{n\in\mathbb{N}} \phi_n$ the *product state* of the sequence $(\phi_n)_n$ on $\otimes_{n\in\mathbb{N}} \mathcal{B}_n$.

CHAPTER 3

Stabilizer Embeddings

In this chapter we present examples of quantum coders as presented in literature. These mappings are usually called "stabilizer codes", but to avoid confusion with the word code, we call them "stabilizer embeddings".

First, we give a definition of these stabilizer embeddings, independent of orthonormal bases of Hilbert spaces. This is a new description of stabilizer embeddings that allows us to formulate things in an easier, more algebraic way. We will see that this formulation can be generalized to a notion that can be viewed as a generalization of classical codes. We develop the definition in several steps, beginning with the Pauli group in section 1. We define stabilizer groups in section 2, stabilizer algebras in section 3 and we characterize stabilizer algebras in section 4. It is only at this point that we are able to give the definition of stabilizer embeddings in section 5. We illustrate this notion in section 6 in a concrete case. The sections 7 and 9 describe more abstract examples, m-blocks of stabilizer embeddings and embeddings that were introduced by Ollivier and Tillich ([**OT03**] and [**OT04**]) using this new description. These m-blocks and Ollivier-Tillich-embeddings are illustrated in sections 8 and 10. We use m-blocks as well as Ollivier-Tillich-embeddings to construct quantum coders in chapter 5. The last section of this chapter reflects to what extent we can use the Hilbert space approach to define quantum alphabets.

1. The Pauli Group

Let the *Pauli group* G_1 be the group generated by the Pauli spin matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \text{ and } \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Now we list some obvious properties of G_1.

1.1. Theorem.

(*i*) *The Pauli spin matrices are unitary and hermitian.*
(*ii*) *We have*

$$\sigma_x\sigma_y = -\sigma_y\sigma_x = \mathrm{i}\sigma_z, \quad \sigma_y\sigma_z = -\sigma_z\sigma_y = \mathrm{i}\sigma_x, \quad \sigma_z\sigma_x = -\sigma_x\sigma_z = \mathrm{i}\sigma_y$$

and

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}.$$

(*iii*) *The Pauli spin matrices have spectrum* $\sigma(\sigma_x) = \sigma(\sigma_y) = \sigma(\sigma_z) = \{1, -1\}$.

(*iv*) *The matrices* $\mathbb{1}, \sigma_x, \sigma_y, \sigma_z$ *form a orthogonal basis of the vector space* $\mathbb{C}^{2\times 2}$ *with the scalar product* $tr(A^*B)$ *for* $A, B \in \mathbb{C}^{2\times 2}$.

(*v*) *The Pauli group is given by*

$$G_1 = \{\pm\mathbb{1}, \pm i\mathbb{1}, \pm\sigma_x, \pm i\sigma_x, \pm\sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\} \subseteq \mathbb{M}_2.$$

(*vi*) *The Pauli group has order 16 and center* $\mathcal{Z}(G_1) = \{\pm\mathbb{1}, \pm i\mathbb{1}\} \leq \mathcal{U}_2$. $\mathcal{Z}(G_1)$ *is cyclic and of order 4.*

(*vii*) *The factor group* $\overline{G}_1 = G_1/\mathcal{Z}(G_1)$ *is isomorphic to* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(*viii*) *Each element* $g \in G_1$ *has a unique representation* $g = i^a\sigma_x^b\sigma_z^c$ *with* $a \in \{0, 1, 2, 3\}$ *and* $b, c \in \{0, 1\}$.

(*ix*) *All elements* g *of* G_1 *either commute or anticommute.*

(*x*) *Each element of* $g \in G_1 \backslash \mathcal{Z}(G_1)$ *is unitary and has* $tr(g) = 0$.

Now define the *n-fold Pauli group* G_n to be the n-fold tensor product of G_1.

1.2. DEFINITION. Let G_n be the group generated by all elementary tensors of elements in G_1, $G_n := G(\otimes_{j=1}^n f_j, f_j \in G_1) \subseteq \mathbb{M}_{2^n} = \mathbb{M}_N$.

Obviously the elements of G_n are given by the elementary tensor products of elements in G_1. Now we introduce the notion of independent generators of a group in order to be able to talk about generators of the Paul group respectively its subgroups.

1.3. DEFINITION. We say a group G is generated by *generators* $(g_i)_{i\in I}$, if G is the smallest subgroup of G containing all generators g_i, $i \in I$.

We call such generators *independent*, if taking one generator away makes the generated group really smaller.

1.4. REMARK. Generators $g_1, \ldots, g_l$ of a group G are independent, if and only if no generator g_i is a product of other generators or their inverses, as groups are closed under multiplication of elements and their inverses. If G is finite, we only need to check the products of generators, as the inverse g^{-1} of any element $g \in G$ is a power of g itself: If $\mathbb{1} \neq g \in G(g_1, \ldots, g_l) \subseteq G$ is finite, there must be a $k_g \in \mathbb{N}$ such that all g^k are pairwise different for $1 \leq k \leq k_g$. Hence there must be a $k \leq k_g$ such that $g^k = g^{k_g+1}$, so $g^{k_g-k+1} = \mathbb{1}$ and $g^{-1} = g^{k_g-k}, k_g - k \geq 0$.

The following lemma gives an estimation for the maximal number of independent generators of a group.

1.5. LEMMA. *Any group* G *with* $|G|$ *elements has at most* $\log_2(|G|)$ *independent generators.*

PROOF. Let G be a group with $|G|$ elements. Suppose $g_1, \ldots, g_l \in G$ are independent generators of a subgroup $G(g_1, \ldots, g_l)$ of G. If $g \notin G(g_1, \ldots, g_l)$, then $fg \notin G(g_1, \ldots, g_l)$ for all $f \in G(g_1, \ldots, g_l)$, since otherwise $g = f^{-1}fg \in G(g_1, \ldots, g_l)$. We see that adding an independent generator g to $g_1, \ldots, g_l$ at least adds the elements $G(g_1, \ldots, g_l)g$ to $G(g_1, \ldots, g_l)$ in the resulting subgroup $G(g, g_1, \ldots, g_l)$, hence it at least doubles the number of elements. Therefore, if $G = G(g_1, \ldots, g_l)$, we must have $l \leq \log_2(|G|)$. □

In the following we consider sets of generators to be independent.

The next theorem shows that G_n inherits most of the structure of G_1. Some of the properties are taken from [Gra01].

1.6. Theorem.

(*i*) $\mathcal{Z}(G_n) = \{\pm\mathbb{1}, \pm\mathrm{i}\mathbb{1}\}$ *and all elements* g *of* G_n *either commute or anticommute.*
(*ii*) *Each element* $g \in G_n \backslash \mathcal{Z}(G_n)$ *is unitary and has* $tr(g) = 0$.
(*iii*) *Each element* $g \in G_n$ *has a unique representation*

$$g = \mathrm{i}^a \sigma_x^{b_1} \sigma_z^{c_1} \otimes \cdots \otimes \sigma_x^{b_n} \sigma_z^{c_n}$$

with $a \in \{0, 1, 2, 3\}$ *and* $b_i, c_i \in \{0, 1\}$ *for* $i \in \mathbb{N}_n$.
(*iv*) G_n *is of order* 4^{n+1} *and has at most* 2^{n+1} *generators.*
(*v*) *Let* g *be an element of* $G_n \backslash \mathcal{Z}(G_n)$. *Then* g *has spectrum*

$$\sigma(g) = \{1, -1\} \text{ or } \{\mathrm{i}, -\mathrm{i}\}.$$

(*vi*) *If* $g \in G_n \backslash \mathcal{Z}(G_n)$, *the eigenspaces of* g *have both dimension* $\frac{N}{2}$.

Proof. (*i*) to (*iv*) are clear.
Through the proof of (*v*) and (*vi*), we use 1.6 (*iii*): An element $g \in G_n$ has the form $g = i^a \sigma_x^{b_1} \sigma_z^{c_1} \otimes \cdots \otimes \sigma_x^{b_n} \sigma_z^{c_n}$ with $a \in \{0, 1, 2, 3\}$ and $b_i, c_i \in \{0, 1\}$ for $i \in \mathbb{N}_n$.

ad (*v*): The eigenvalues of g are given by the products of eigenvalues of the matrix factors of g multiplied by i^a. Hence if at least one matrix factor is not equal to $\mathbb{1}$, the elementary tensor has spectrum $\{1, -1\}$. Multiplication with i^a leads to either spectrum $\{1, -1\}$ or spectrum $\{\mathrm{i}, -\mathrm{i}\}$.

ad (*vi*): We perform an induction over n: Obviously any element of G_1 that isn't a scalar multiple of $\mathbb{1}$ has two onedimensional eigenspaces. Now $g = \mathrm{i}^a \bigotimes_{j=1}^{n+1} \sigma_x^{b_j} \sigma_z^{c_j}$. Let $ES_j(g)$ denote the eigenspace of g to the eigenvalue j, here due to the proof of (*v*) $j \in \{\mathrm{i}^a, -\mathrm{i}^a\}$. Then

$$ES_j(g) = \mathrm{lin}(ES_j(\mathrm{i}^a \otimes_{j=1}^n \sigma_x^{b_j} \sigma_z^{c_j}) \otimes ES_1(\sigma_x^{b_{n+1}} \sigma_z^{c_{n+1}}),$$
$$ES_{-j}(\mathrm{i}^a \otimes_{j=1}^n \sigma_x^{b_j} \sigma_z^{c_j}) \otimes ES_{-1}(\sigma_x^{b_{n+1}} \sigma_z^{c_{n+1}})),$$

even if $\sigma_x^{b_{n+1}} \sigma_z^{c_{n+1}} = \mathbb{1}_2$. □

For convenience, let us set

$$g(b, c) := \mathrm{i}^{\langle b, c \rangle} \bigotimes_{j=1}^{n} \sigma_x^{b_j} \sigma_z^{c_j} = \mathrm{i}^{\langle b, c \rangle} \sigma_x^b \sigma_z^c$$

with

$$\sigma_x^b := \otimes_{j=1}^n \sigma_x^{b_j} \quad \text{and} \quad \sigma_z^c := \otimes_{j=1}^n \sigma_z^{c_j}$$

and $\langle \cdot, \cdot \rangle$ denoting the inner product in $\mathbb{F}_2^n$.

Looking at subgroups of G_n we make the following observations.

1.7. Theorem. *Let* S *be a subgroup of* G_n *generated by the generators* $g_1, \ldots, g_l \in G_n$.

(*i*) *If* $-\mathbb{1} \notin S$, *then* $\pm\mathrm{i}\mathbb{1} \notin S$ *and* g *is an involution for all* $g \in S$.

(*ii*) $g \in S$ *is an involution if and only if* g *is of the form*

$$g = g(b,c) \quad \text{or} \quad g = -g(b,c)$$

with $b, c \in \mathbb{F}_2^n$.
$-\mathbb{1} \notin S$ *if and only if for fixed* $b, c \in \mathbb{F}_2^n$ *either* $g(b,c) \in S$ *or* $-g(b,c) \in S$ *or none of them.*

(*iii*) *If* $-\mathbb{1} \notin S$, *then all elements of* S *are hermitian and hence* S *is commutative.*

(*iv*) $-\mathbb{1} \notin S$ *if and only if no* g_i *is the negative product of generators.*

PROOF. ad (*i*): $\pm \mathrm{i}\mathbb{1} \in S$ implies $(\pm \mathrm{i}\mathbb{1})^2 = -\mathbb{1}$, a contradicition if $-\mathbb{1} \notin S$.

Due to 1.6 we have

$$g^2 = \mathrm{i}^{2a} \otimes_{j=1}^n (-1)^{b_j c_j} \sigma_x^{b_j + b_j} \sigma_z^{c_j + c_j} = (-1)^{a + \langle b\,, c \rangle} \otimes_{j=1}^n \sigma_x^{2b_j} \sigma_z^{2c_j}$$

for $a \in \{0,1,2,3\}$ and $b, c \in \mathbb{F}_2^n$. Thus $g^2 = \pm\mathbb{1}$ and since $-\mathbb{1} \notin S$ we have $g^2 = \mathbb{1}$.

ad (*ii*): As in (*i*) we have $g^2 = (-1)^{a + \langle b\,, c \rangle} \otimes_{j=1}^n \sigma_x^{2b_j} \sigma_z^{2c_j}$ for $a \in \{0,1,2,3\}$ and $b, c \in \mathbb{F}_2^n$. But $g^2 = \mathbb{1}$ if and only if $a = \langle b\,, c \rangle$ modulo 2 respecticely if and only if $a = \langle b\,, c \rangle + 2k$, $k \in \{0,1\}$.

Let $b, c \in \mathbb{F}_2^n$. If $-\mathbb{1} \in S$ and $(-)g(b,c) \in S$ then obviously $-(-)g(b,c) \in S$. For the converse, let $-\mathbb{1} \notin S$. If both $g(b,c)$ and $-g(b,c)$ are elements of S, then $-g(b,c)g(b,c) = -g(b,c)^2 = -\mathbb{1} \in S$, a contradiction.

ad (*iii*): If $-\mathbb{1} \notin S$, then due to (*i*) all elements of S are involutions. Hence for any $\mathbb{1} \neq g \in S$, $g^{-1} = g$. But as g is unitary due to (*i*) and theorem 1.6 (*ii*), $g = g^{-1} = g^*$.

If all elements of S are hermitian, then for all $g, h \in S$ we have $gh \in S$ and $gh = (gh)^* = h^* g^* = hg$.

ad (*iv*): "$\Rightarrow$": Let $i_0, i_{i_1}, \ldots, i_m \in \mathbb{N}_l$ be such that $g_{i_0} = -g_{i_1} \cdots g_{i_m}$ and let us assume that $-\mathbb{1} \notin S$. Then $g_i^2 = \mathbb{1}$ for all generators g_i by (*i*). But then we get $-\mathbb{1} = g_{i_0} g_{i_1} \cdots g_{i_m} \in S$, a contradiction.

"$\Leftarrow$": Let $-\mathbb{1}$ be an element of S and suppose that no generator is the negative product of others. But if $-\mathbb{1} \in S$, then there must be $i_1, \ldots, i_m \in \mathbb{N}_l$ such that $-\mathbb{1} = g_{i_1} \cdots g_{i_m}$ as S is finite. Thus $g_1 = -g_1 g_{i_1} \cdots g_{i_m}$, a contradiction. □

1.8. REMARK. Note that we can show analogously to the second part of (*ii*) that $-\mathbb{1} \notin S$ if and only if for any $g \in S$ we have $-g \notin S$.
Nielsen and Chuang state another version of (*iv*) in [NC00], page 454. They claim that $-\mathbb{1} \notin S$ if and only if $g_i^2 = \mathbb{1}$ and $g_i \neq -\mathbb{1}$. However, this is not true: Let $g_1 = \sigma_z$ and $g_2 = -\sigma_z$ generate S, then $-\mathbb{1} = g_1 g_2 \in S$.

We also obtain the following lemma.

1.9. LEMMA. *If* $g_1, \ldots, g_l \in G_n$ *are independent generators such that* $-\mathbb{1} \notin G(g_1, \ldots, g_l)$, *then* $-g_1, g_2, \ldots, g_l$ *are also independent generators and* $-\mathbb{1} \notin G(-g_1, g_2, \ldots, g_l)$

Proof. As $-\mathbb{1} \notin G(g_1, \ldots, g_l)$, $-g_1 \notin G(g_1, \ldots, g_l)$ due to 1.7. Hence $-g_1 \notin G(g_2, \ldots, g_l)$ and $-g_1, g_2, \ldots, g_l$ are independent.

Let us assume that $-\mathbb{1} \in G(-g_1, g_2, \ldots, g_l)$. As $G(-g_1, g_2, \ldots, g_l)$ is finite, $-\mathbb{1}$ must be a product of different generators out of $\{-g_1, g_2, \ldots, g_l\}$. But then $\mathbb{1}$ is a product of different generators out of $\{g_1, g_2, \ldots, g_l\}$, a contradiction, as $g_1, \ldots, g_l$ are independent. □

1.10. Remark. The lemma above implies that we may assume from now on without any loss of generality that subgroups not containing $-\mathbb{1}$ consist only of elements of the form $g(b, c)$. This simplifies theorem 1.7 (*ii*) and will be used later.

We can also code commutativity and independence in terms of the representations we mentioned in theorem 1.7. This leads to the following.

1.11. Theorem.

(*i*) *Let $g, \tilde{g} \in G_n$ and hence*

$$g = \mathrm{i}^a \sigma_x^b \sigma_z^c \text{ and } \tilde{g} = \mathrm{i}^{\tilde{a}} \sigma_x^{\tilde{b}} \sigma_z^{\tilde{c}}$$

for $a, \tilde{a} \in \{0, 1, 2, 3\}$ and $b, \tilde{b}, c, \tilde{c} \in \mathbb{F}_2^n$ where $\langle \cdot\,, \cdot \rangle$ stands for the inner product in $\mathbb{F}_2^n$. Then $g\tilde{g} = \tilde{g}g$ if and only if $\langle \tilde{b}\,, c \rangle = \langle \tilde{c}\,, b \rangle$.

(*ii*) *Let $\mathbb{S}$ be a linear subspace of $\mathbb{F}_2^{2n}$ such that $\langle \tilde{b}\,, c \rangle = \langle \tilde{c}\,, b \rangle$ for $(b, c), (\tilde{b}, \tilde{c}) \in \mathbb{S}$. Then*

$$g : \mathbb{F}_2^{2n} \to G_n : (b, c) \mapsto g(b, c)$$

is injective, $-\mathbb{1} \notin g(\mathbb{F}_2^{2n})$ and the restriction of g to $\mathbb{S}$ is a group isomorphism.

(*iii*) *Let $\mathbb{S}$ be a linear subspace of $\mathbb{F}_2^{2n}$ such that $\langle \tilde{b}\,, c \rangle = \langle \tilde{c}\,, b \rangle$ for $(b, c), (\tilde{b}, \tilde{c}) \in \mathbb{S}$. Then every set of linearly independent vectors $(b_i, c_i) \in \mathbb{S}$, $i \in \mathbb{N}_l$, corresponds to a set of independent elements $g(b_i, c_i)$, $i \in \mathbb{N}_l$.*

Proof. ad (*i*):

$$g\tilde{g} = \mathrm{i}^{a+\tilde{a}} (-1)^{\langle \tilde{b}, c \rangle} \sigma_x^{b+\tilde{b}} \sigma_z^{c+\tilde{c}} \stackrel{!}{=} \tilde{g}g = \mathrm{i}^{\tilde{a}+a} (-1)^{\langle \tilde{b}, c \rangle} \sigma_x^{\tilde{b}+b} \sigma_z^{\tilde{c}+c}$$

Now $g\tilde{g} = \tilde{g}g$ if and only if $\langle \tilde{b}\,, c \rangle = \langle b\,, \tilde{c} \rangle$.

ad (*ii*): The first two assertions are given by definition. Let $b, \tilde{b}, c, \tilde{c} \in \mathbb{F}_2^n$ such that $\langle \tilde{b}\,, c \rangle = \langle \tilde{c}\,, b \rangle$. Then

$$\begin{aligned} g(b, c)g(\tilde{b}, \tilde{c}) &= \mathrm{i}^{\langle b, c \rangle + \langle \tilde{b}, \tilde{c} \rangle} \sigma_x^b \sigma_z^c \sigma_x^{\tilde{b}} \sigma_z^{\tilde{c}} = \mathrm{i}^{\langle b, c \rangle + \langle \tilde{b}, \tilde{c} \rangle} (-1)^{\langle \tilde{b}, c \rangle} \sigma_x^{b+\tilde{b}} \sigma_z^{c+\tilde{c}} \\ &= \mathrm{i}^{\langle b, c \rangle + \langle \tilde{b}, \tilde{c} \rangle} \mathrm{i}^{2\langle \tilde{b}, c \rangle} \sigma_x^{b+\tilde{b}} \sigma_z^{c+\tilde{c}} = \mathrm{i}^{\langle b, c \rangle + \langle \tilde{b}, \tilde{c} \rangle} \mathrm{i}^{\langle \tilde{b}, c \rangle + \langle b, \tilde{c} \rangle} \sigma_x^{b+\tilde{b}} \sigma_z^{c+\tilde{c}} \\ &= \mathrm{i}^{\langle b+\tilde{b}, c+\tilde{c} \rangle} \sigma_x^{b+\tilde{b}} \sigma_z^{c+\tilde{c}} = g(b + \tilde{b}, c + \tilde{c}) = g((b, c) + (\tilde{b}, \tilde{c})). \end{aligned}$$

ad (*iii*): Let us first assume that $(b_i, c_i) \in \mathbb{S}$, $i \in \mathbb{N}_l$ are linearly independent. In order to show that all $g(b_i, c_i)$ are independent, we assume further that $g(b_1, c_1) \in G(g(b_2, c_2), \ldots, g(b_l, c_l))$.

As $G(g(b_2,c_2),\dots,g(b_l,c_l))$ is finite, we thus can write $g(b_1,c_1)$ as a product, $g(b_1,c_1) = \prod_{r=1}^{m} g(b_{i_r},c_{i_r})$ with $i_r \geq 2$. As $g(b_1,c_1)^2 = \mathbb{1}$, we get

$$g(0,0) = \mathbb{1} = g(b_1,c_1)\prod_{r=1}^{m} g(b_{i_r},c_{i_r}) = g((b_1,c_1) + \sum_{r=1}^{m}(b_{i_r},c_{i_r})).$$

As g is injective, $(0,0) = (b_1,c_1)+\sum_{r=1}^{m}(b_{i_r},c_{i_r})$, a contradiction if the vectors (b_i,c_i) are linearly independent.

For the converse direction, let $g(b_i,c_i) \in \mathbb{S}$, $i \in \mathbb{N}_l$ be independent. Let us further assume that $(b_1,c_1) = \sum_{r=1}^{m}(b_{i_r},c_{i_r})$, $i_r \geq 2$. Thus $g(b_1,c_1) = g(\sum_{r=1}^{m}(b_{i_r},c_{i_r})) = \prod_{r=1}^{m} g(b_{i_r},c_{i_r})$ and hence $g(b_1,c_1) \in G(g(b_{i_1},c_{i_1}),\dots,g(b_{i_m},c_{i_m}))$, a contradiction if all elements $g(b_i,c_i) \in \mathbb{S}$, $i \in \mathbb{N}_l$, are independent. □

1.12. REMARK. Let $\mathbb{S}$ be a linear subspace of $\mathbb{F}_2^{2n}$ such that $\langle \tilde{b}\,, c\rangle = \langle \tilde{c}\,, b\rangle$ for all $(b,c),(\tilde{b},\tilde{c}) \in \mathbb{S}$. Note that by theorem 1.11 (*iii*), a linearly independent set of vectors $(b_i,c_i) \in \mathbb{S}$, $i \in \mathbb{N}_l$, corresponds to a set of independent elements $g_i := g(b_i,c_i)$. Further $-\mathbb{1} \notin G(g_1,\dots,g_l)$ by theorem 1.11 (*ii*). Thus by lemma 1.9 and remark 1.10, we may replace any g_i by $-g_i$ and we still obtain a set of independent elements that do not generate $-\mathbb{1}$. Therefore we may assume without any loss of generality that the map g from theorem 1.11 (*ii*) defines a bijection between $\mathbb{S}$ and $G(g_1,\dots,g_l)$.

All these observations about representations of S now let us make a statement about abelian subgroups of G_n not containing $-\mathbb{1}$.

1.13. THEOREM. *Any set of $m < n$ independent elements of G_n not generating $-\mathbb{1}$ can be filled up to a set of n independent elements of G_n not generating $-\mathbb{1}$ and the generated group is isomorphic to* $\underbrace{\mathbb{F}_2 \times \cdots \times \mathbb{F}_2}_{n}$.

The proof is based on theorem 1.7 and remark 1.12, but also uses the idea of Gaussian elimination, which can be found in [**NC00**].

PROOF. Note that elements of subgroups of G_n not containing $-\mathbb{1}$ are involutions and commute due to 1.7. Let $g_1,\dots,g_m \in G_n$, $m < n$ be a set of commuting independent generators, with $-\mathbb{1} \notin G(g_1,\dots,g_m)$. By remark 1.12 we may assume that $g_1,\dots,g_m$ are of the form $g_i = g(b_i,c_i)$ with linearly independent vectors $(b_i,c_i) \in \mathbb{F}_2^{2n}$, $i \in \mathbb{N}_m$ and $\langle b_j\,, c_i\rangle = \langle c_j\,, b_i\rangle$ for all $i \neq j = 1,\dots,m$.

Set $l := \dim \operatorname{lin}\{c_1,\dots,c_m\} \leq m$ and assume that for $0 < l \leq m$, $c_1,\dots,c_l$ are linearly independent. But then for each $k \in [l+1,m]$ there is a set $I_k \subseteq \mathbb{N}_l$ such that $c_k = \sum_{i\in I_k} c_i$ and thus $\sigma_z^{c_k} = \prod_{i\in I_k} \sigma_z^{c_i}$. This implies that

$$G(g(b_1,c_1),\dots,g(b_l,c_l),g(b_k,c_k)) = G(g(b_1,c_1),\dots,g(b_l,c_l),g(b_k + \sum_{i\in I_k} b_i,0)).$$

Hence we may replace g_k by $g(b_k + \sum_{i\in I_k} b_i,0)$ without changing the generated subgroup and reverse this replacement, if desired, after choosing $g_{m+1},\dots,g_n$. Note that $l = 0$ is possible, but then all $c_i = 0$ anyway.

Thus we may assume that $c_{l+1}, \ldots, c_m = 0$. But if $c_{l+1}, \ldots, c_m = 0$, then $b_{l+1}, \ldots, b_m$ must be linearly independent.

If c_i, $i \in \mathbb{N}_l$, has a 1 at position j, then for any c_k, $i \neq k \in \mathbb{N}_l$, with a 1 at position j we know that $c_k + c_i$ has a 0 at position j. But replacing (b_k, c_k) by $(b_k + b_i, c_k + c_i)$ corresponds to replacing g_k by $g_k \cdot g_i$. This replacement doesn't change the generated groups,

$$G(g_1, \ldots, g_m) = G(g_1, \ldots, g_{k-1}, g_k \cdot g_i, g_{k+1}, \ldots, g_m),$$

and hence it doesn't change the generators to add. If we now admit a renummeration of the generators and a permutation of the tensor product factors, we may perform a Gaussian elemination procedure on the vectors belonging to $g_1, \ldots, g_m$. Hence we may assume that these vectors are of the form

$$\left(\begin{array}{c|c} b_1 & c_1 \\ \vdots & \vdots \\ b_m & c_m \end{array}\right) = \left(\begin{array}{c|ccc} * & \mathbb{1}_l & B & A \\ * & 0 & 0 & 0 \end{array}\right)$$

for the identity $\mathbb{1}_l \in \mathbb{M}_l$, a $l \times (m-l)$-matrix B and a $l \times (n-m)$-matrix A. As $b_{m+1}, \ldots, b_m$ are linearly independent, we can repeat the above argumentation and further assume that

$$\left(\begin{array}{c|c} b_1 & c_1 \\ \vdots & \vdots \\ b_m & c_m \end{array}\right) = \left(\begin{array}{ccc|ccc} * & * & * & \mathbb{1}_l & B & A \\ C & \mathbb{1}_{m-l} & D & 0 & 0 & 0 \end{array}\right)$$

for the identity $\mathbb{1}_{m-l} \in \mathbb{M}_{m-l}$, a $(m-l) \times l$-matrix C and a $(m-l) \times (n-m)$-matrix D. Let us now choose

$$\left(\begin{array}{c|c} b_{m+1} & c_{m+1} \\ \vdots & \vdots \\ b_n & c_n \end{array}\right) = \left(\begin{array}{ccc|ccc} A^T & 0 & \mathbb{1}_{n-m} & 0 & 0 & 0 \end{array}\right).$$

As $c_{m+1}, \ldots, c_n = 0$, $(b_{m+1}, c_{m+1}), \ldots, (b_n, c_n)$ are linearly independent due to the $\mathbb{1}_{n-m}$-matrix and linearly independent from $(b_{l+1}, c_{l+1}), , \ldots, (b_m, c_m)$ as the null matrix meets the $\mathbb{1}_{m-l}$-matrix. They are obviously linearly independent from $(b_1, c_1), \ldots, (b_l, c_l)$. Checking the commutativity relations, we notice that $g(b_{m+1}, c_{m+1}), \ldots, g(b_n, c_n)$ commute as obviously $\langle b_i \, , c_j \rangle = 0 = \langle b_j \, , c_i \rangle$ for $m+1 \leq i \leq n$ and $m+1 \leq j \leq n$. Let $m+1 \leq i \leq n$, $1 \leq j \leq l$. Then

$$\begin{array}{rcccccccccccccccc} b_i & = & (& a_{1i} & \cdots & a_{ji} & \cdots & a_{li} & | & 0 & \cdots & 0 & | & 0 & \cdots & 1 & \cdots & 0 &), \\ c_j & = & (& 0 & \cdots & 1 & \cdots & 0 & | & b_{j1} & \cdots & b_{j(m-l)} & | & a_{j1} & \cdots & a_{ji} & \cdots & a_{j(n-m)} &), \end{array}$$

and thus $\langle b_i \, , c_j \rangle = a_{ji} + 0 + a_{ji} = 0 = \langle b_j \, , c_i \rangle$ in $\mathbb{F}_2$.

If $l = 0$, then $b_1, \ldots, b_m$ are linearly independent and we may assume that all $c_i = 0$. But then we choose $b_{m+1}, \ldots, b_n \in \mathbb{F}_2^n$ such that $b_1, \ldots, b_n$ are linearly independent and set $c_{m+1}, \ldots, c_n = 0$. Then $(b_1, c_1), \ldots, (b_n, c_n)$ are linearly independent and the inner product relation obviously is satisfied. □

Abelian subgroups of G_n containing $-\mathbb{1}$ can be filled up to $n+1$ independent generators, n generating a commutative subgroup not containing $-\mathbb{1}$ and the last generator being either $-\mathbb{1}$ (or a negative product of the first n generators) or $\mathrm{i}\mathbb{1}$ respectively $-\mathrm{i}\mathbb{1}$ (or a product of the first n generators multiplied by $\pm\mathrm{i}$).

We can also give a condition for maximality of subgroups of G_n not containing $-\mathbb{1}$. In fact, the following theorem contains theorem 1.13 and gives an alternative proof.

1.14. THEOREM. *Let $S \subseteq G_n$ be a subgroup such that $-\mathbb{1} \notin S$. Let $\mathbb{S} \subseteq \mathbb{F}_2^{2n}$ be the corresponding linear subspace. If*

$$U = \begin{pmatrix} 0 & \mathbb{1} \\ \mathbb{1} & 0 \end{pmatrix} \text{ and } M^\perp = \{v \in \mathbb{F}_2^{2n} : \langle v, m\rangle = 0 \text{ for all } m \in M\} \text{ for } M \subseteq \mathbb{F}_2^{2n},$$

then S is maximal if and only if $\mathbb{S} = (U\mathbb{S})^\perp$. In this case, $\dim \mathbb{S} = n$.

PROOF. By remark 1.12 we consider only subgroups consisting of elements of the form $g(b,c)$. Note that $\langle \tilde{b}, c\rangle = \langle \tilde{c}, b\rangle$ respectively

$$\langle (b,c), U(\tilde{b},\tilde{c})\rangle = 0$$

for all $(b,c), (\tilde{b},\tilde{c}) \in \mathbb{S}$ as we work over $\mathbb{F}_2$ by means of $-\mathbb{1} \notin S$. But then $\mathbb{S} \subseteq (U\mathbb{S})^\perp = U(\mathbb{S}^\perp)$ (respectively $U\mathbb{S} \subseteq \mathbb{S}^\perp$ as $M_1 \subseteq M_2 \subseteq \mathbb{F}_2^{2n}$ implies $M_2^\perp \subseteq M_1^\perp$).

Let us denote $\{s\}^\perp$ for $s \in \mathbb{F}_2^{2n}$ by $s^\perp$ for simplicity and better reading.

Let us further assume that there is an element $s \in \mathbb{F}_2^{2n}$ such that $s \notin \mathbb{S}$ but $s \in (U\mathbb{S})^\perp$. Then $U\mathbb{S} \subseteq s^\perp$ and hence $\mathbb{S} \subseteq (Us)^\perp$. But this implies

$$\Big(U(\mathrm{lin}(\mathbb{S}, s))\Big)^\perp = \mathrm{lin}(U\mathbb{S}, Us)^\perp = (U\mathbb{S})^\perp \cap (Us)^\perp \supseteq (U\mathbb{S})^\perp \cap \mathbb{S} = \mathbb{S}.$$

Since $\langle s, Us\rangle = 0$, we have $s \in (Us)^\perp$ and thus we obtain by the choice of s that $s \in (U\mathbb{S})^\perp \cap (Us)^\perp$. Hence

$$\mathrm{lin}(\mathbb{S}, s) \subseteq (U\mathbb{S})^\perp \cap (Us)^\perp = \Big(U(\mathrm{lin}(\mathbb{S}, s))\Big)^\perp.$$

All together we get $\mathrm{lin}(\mathbb{S}, s) \subseteq \Big(U(\mathrm{lin}(\mathbb{S}, s))\Big)^\perp$. But then $S \neq G(S, g(s)) \subseteq G_n$ and $-\mathbb{1} \notin G(S, g(s))$.

Therefore, maximality of S is equivalent to the fact that there is no element $s \in \mathbb{F}_2^{2n}$ such that $s \notin \mathbb{S}$ and $s \in (U\mathbb{S})^\perp$. But then S is maximal if and only if $\mathbb{S} = (U\mathbb{S})^\perp$.

Now let $\mathbb{S}$ have dimension k. Then obviously $U\mathbb{S}$ has also dimension k. Let $s_1, \ldots, s_k$ be a basis of $U\mathbb{S}$. Put

$$A = \begin{pmatrix} s_1^T \\ \vdots \\ s_k^T \end{pmatrix},$$

then $(U\mathbb{S})^\perp$ is given by the kernel of A. Hence $(U\mathbb{S})^\perp$ has dimension $2n-k$ due to the dimension formula. Thus if $\dim \mathbb{S} = \dim U\mathbb{S} = \dim(U\mathbb{S})^\perp$, we obtain $k = 2n - k$ and therefore $k = n$. □

2. The Stabilizer Group

Let us now fix a subgroup S of G_n generated by $l = n - k < n$ independent and commuting generators $g_1, \ldots, g_{n-k}$ such that $-\mathbb{1} \notin S$. We call subgroups of this type $[k,n]$-*stabilizer groups*.

We give some properties of stabilizer groups additional to those mentioned in the previous section. They are inspired by [NC00].

2.1. Theorem. *Let S be a stabilizer group.*

(*i*) *The choice of generators $g_1, \dots, g_{n-k}$ for S defines a bijective representation*

$$\pi : \{0,1\}^{n-k} \to S \subseteq \mathbb{M}_N : (x_i)_{i=1}^{n-k} \mapsto \prod_{i=1}^{n-k} g_i^{x_i}.$$

(*ii*) *The dual group of S is given by*

$$\hat{S} = \{1,-1\}^{n-k} = \widehat{\{0,1\}^{n-k}}$$

where a character $\chi_{(y_j)_{j=1}^{n-k}} \in \hat{S}$ is fixed by its action on the generators.

(*iii*) *If $g \in S$ and $g \neq \mathbb{1}$, then g has spectrum $\sigma(g) = \{1,-1\}$.*

Proof. (*i*) is trivial, ad (*ii*): The characters of S are multiplicative forms, hence the only choice is to choose what the generators are mapped on. As $g^2 = \mathbb{1}$, the generators can only be mapped on 1 or -1. Thus $\hat{S} = \{1,-1\}^{n-k}$.

ad (*iii*): We use theorem 1.6 (*iii*) and theorem 1.7 (*ii*), hence $g = \mathrm{i}^a \sigma_x^{b_1} \sigma_z^{c_1} \otimes \cdot \otimes \sigma_x^{b_{n-k}} \sigma_z^{c_{n-k}}$ with $a \in \{0,2\}$ and $b_i, c_i \in \{0,1\}$ for $i \in \mathbb{N}_{n-k}$. Elementary tensors of Pauli matrices have spectrum $\{1,-1\}$ if they aren't all equal to $\mathbb{1}$. Multiplication with $\mathrm{i}^2 = -1$ doesn't change this. □

We finally make the following observation.

2.2. Remark. Every subgroup S of G_n such that $-\mathbb{1} \notin S$ and $S \simeq \{0,1\}^{n-k}$ is a $[k,n]$-stabilizer group.

3. The Stabilizer Algebra

We define

$$\mathcal{A}_S := \mathcal{A}(S) = \mathrm{lin}(S) \subseteq \mathbb{M}_N.$$

Obviously, $\mathcal{A}_S$ is a commutative subalgebra of $\mathbb{M}_N$, has dimension 2^{n-k} as a vector space and satisfies $\hat{\mathcal{A}}_S = \hat{S}$.

Hence we can decompose $\mathbb{C}^N$ such that the diagonalizable operators with respect to this decomposition are given by $\mathcal{A}_S$.

3.1. Theorem. *Let $S \subseteq \mathbb{M}_N$ be a stabilizer group. Then there exists a decomposition of $\mathbb{C}^N$ such that*

$$\mathbb{C}^N = \bigoplus_{(y_i)_i \in \hat{\mathcal{A}}_S} \mathcal{H}_{(y_i)_i}, \quad \mathcal{H}_{(y_i)_i} \simeq \mathbb{C}^K, \ K = 2^k,$$

and the diagonalizable operators are given by $\mathcal{A}_S$.

In order to prove the theorem, we introduce some orthogonal projections and the notion of trace-independence and study both. The proof of 3.1 can be found at the end of this section.

For the generators $g_1, \ldots, g_{n-k}$ of S define the following orthogonal projections

$$E_1^i := \tfrac{1}{2}(\mathbb{1} + g_i), \;\; E_{-1}^i := \tfrac{1}{2}(\mathbb{1} - g_i).$$

3.2. REMARK. $E_{y_i}^i$ is an orthogonal projection and projects $\mathbb{C}^N$ onto the eigenspace $ES_{y_i}(g_i)$ of the eigenvalue y_i of the generator g_i for all $i \in \mathbb{N}_{n-k}$ and $y_i \in \{1, -1\}$. We have $E_1^i E_{-1}^i = 0$ and $E_1^i + E_{-1}^i = \mathbb{1}$ and the projections $E_{y_i}^i$ with $y_i \in \{1, -1\}$ for $i \in \mathbb{N}_{n-k}$ generate $\mathcal{A}_S$. As we know due to 1.6 (*vii*), the dimension of the image $ES_{y_i}(g_i)$ of $E_{y_i}^i$ is $\frac{N}{2}$. Hence we get $\mathrm{tr}(E_{y_i}^i) = \frac{1}{2}$.

We combine these projections to other orthogonal projections

$$E_{(y_j)_j} := \prod_{i=1}^{n-k} E_{y_i}^i,$$

for any $(y_j)_j \in \{1, -1\}^{n-k}$, which turn out to be the common spectral projections of the commutative algebra generated by the generators $g_1, \ldots, g_{n-k}$.

3.3. REMARK. For all $(y_j)_j \in \{1, -1\}^{n-k}$, $E_{(y_j)_j}$ is an orthogonal projection and $E_{1^{n-k}}$ is the projection onto the fixed space of all generators g_i. The projections $E_{(y_i)_i}$ with $(y_i)_i \in \{1, -1\}^{n-k}$ generate $\mathcal{A}_S$.

Due to [NC00], the projections $E_{(y_j)_j}$ have the following useful properties.

3.4. LEMMA.

(*i*) *For* $(y_j)_j \neq (z_j)_j \in \{1, -1\}^{n-k}$ *we have* $E_{(y_j)_j} E_{(z_j)_j} = 0$.
(*ii*) $\sum_{(y_j)_j \in \{1,-1\}^{n-k}} E_{(y_j)_j} = \mathbb{1}$

PROOF. ad (*i*): If $(y_j)_j \neq (z_j)_j \in \{1, -1\}^{n-k}$ then there is at least one $i \in \mathbb{N}_{n-k}$ such that $y_i \neq z_i$. Hence $E_{y_i}^i E_{z_i}^i = 0$. As the eigenspace projections commute due to 3.2 (*iv*), $E_{(y_j)_j} E_{(z_j)_j} = 0$ by definition.

ad (*ii*):

$$\begin{aligned} \mathbb{1} &= E_1^1 + E_{-1}^1 = E_1^1(E_1^2 + E_{-1}^2) + E_{-1}^1(E_1^2 + E_{-1}^2) = \ldots \\ &= \sum_{(y_i)_i \in \{1,-1\}^{n-k}} \prod_{i=1}^{n-k} E_{y_i}^i = \sum_{(y_i)_i \in \{1,-1\}^{n-k}} E_{(y_i)_i} \end{aligned}$$

□

In order to show that the images of the projections $E_{(y_i)_i}$ have all the same dimension K, the common way is to use the correspondence used in the proof of 1.13. Instead of doing this, we give a new proof using the notion of tr-independence and we start by giving the definition.

3.5. DEFINITION. Let $\mathcal{A}$ be an operator algebra with normalized trace tr. Two subalgebras $\mathcal{B}, C \subseteq \mathcal{A}$ are called tr-*independent*, if $\mathrm{tr}(BC) = \mathrm{tr}(B) \cdot \mathrm{tr}(C)$ for all elements $B \in \mathcal{B}$ and $C \in C$.

3.6. Remark. We have

$$\operatorname{tr}(f)\cdot\operatorname{tr}(g)=\operatorname{tr}(fg) \text{ for } f,g\in G_n \text{ with } f,g,fg\neq\pm\mathbb{1},\pm i\mathbb{1}, \tag{1}$$

as $\operatorname{tr}(f)=\operatorname{tr}(g)=\operatorname{tr}(fg)=0$ for all $f,g\in G_n$ and f,g,fg beeing elementary tensors in G_n containing at least one Pauli spin matrix. If $f,g\in S$, as then $-\mathbb{1},\pm i\mathbb{1}\notin S$ due to 1.7 (i) and if f,g are also independent, we get $f,g\neq\mathbb{1}$ and $g\neq f,f^{-1}$. Hence we have (1) for independent elements of S.

We use the idea of remark 3.6 for the following lemma.

3.7. Lemma.

- (i) *Independent elements of S have tr-independent generated *-algebras. Especially*
  - (α) *$\mathcal{A}(g_i)$ and $\mathcal{A}(g_j)$ are tr- independent for $i\neq j\in\mathbb{N}_{n-k}$.*
  - (α') *$\mathcal{A}(E_1^i,E_{-1}^i)$ and $\mathcal{A}(E_1^j,E_{-1}^j)$ with $i\neq j\in\mathbb{N}_{n-k}$ are tr-independent.*
  - (β) *For fixed $l,l+1\in\mathbb{N}_{n-k}$, $\mathcal{A}(g_1,\dots,g_l)$ and $\mathcal{A}(g_{l+1})$ are tr-independent.*
  - (β') *For fixed $l,l+1\in\mathbb{N}_{n-k}$, $\mathcal{A}(E_1^i,E_{-1}^i:i\in\mathbb{N}_l)$ is tr-independent from $\mathcal{A}(E_1^{l+1},E_{-1}^{l+1})$.*
- (ii) *It is $tr(E_{y_i}^i)=\frac{1}{2}$ for all $i\in\mathbb{N}_{n-k}$ and $y_i\in\{1,-1\}$.*
- (iii) *We have $tr(E_{(y_i)_i})=\frac{1}{2^{n-k}}$ for all $(y_i)_i\in\{1,-1\}^{n-k}$ and hence the dimension of the image of $E_{(y_i)_i}$ is $\frac{N}{2^{n-k}}=K$.*

Proof. ad (i): Let $f,g\in S$ be independent. Then $\mathcal{A}(f)=\{\lambda_1\mathbb{1}+\lambda_2 f:\lambda_i\in\mathbb{C}\}$, $\mathcal{A}(g)=\{\lambda_1\mathbb{1}+\lambda_2 g:\lambda_i\in\mathbb{C}\}$. Let $\lambda_1\mathbb{1}+\lambda_2 f\in\mathcal{A}(f),\mu_1\mathbb{1}+\mu_2 g\in\mathcal{A}(g)$. Then

$$\begin{aligned}\operatorname{tr}((\lambda_1\mathbb{1}+\lambda_2 f)(\mu_1\mathbb{1}+\mu_2 g))&=\operatorname{tr}(\lambda_1\mu_1\mathbb{1}+\lambda_1\mu_2 g+\lambda_2\mu_1 f+\lambda_2\mu_2 fg)\\&\overset{3.6}{=}\lambda_1\mu_1=\operatorname{tr}(\lambda_1\mathbb{1}+\lambda_2 f)\cdot\operatorname{tr}(\mu_1\mathbb{1}+\mu_2 g).\end{aligned}$$

ad (ii): Obviously $\operatorname{tr}(E_{y_i}^i)=\operatorname{tr}(\frac{1}{2}(\mathbb{1}+y_i g_i))=\frac{1}{2}$.

(iii) follows from (ii) and (i) (β'): $\operatorname{tr}(E_{(y_i)_i})=\prod_{i=1}^{n-k}\operatorname{tr}(E_{y_i}^i)=(\frac{1}{2})^{n-k}$. □

Now we can prove the theorem just by using the previous results.

Proof of 3.1. $\mathbb{C}^N=\oplus_{(y_i)_i\in\{1,-1\}^{n-k}}E_{(y_i)_i}\mathbb{C}^N$ by 3.3 (ii) and $\hat{\mathcal{A}}_S=\{1,-1\}^{n-k}$. $E_{(y_i)_i}\mathbb{C}^N\simeq\mathbb{C}^K$ by 3.7. As $\mathcal{A}_S$ is generated by the pairwise orthogonal projections $E_{(y_i)_i}$, any element $A\in\mathcal{A}_S$ is a linear combination of these projections, $A=\sum_{(y_i)_i\in\hat{\mathcal{A}}_S}\lambda_{(y_i)_i}E_{(y_i)_i}$. As $E_{(y_i)_i}$ is the identity on $H_{(y_i)_i}$, A is a diagonalizable operator with respect to this decomposition. □

4. Characterization of $\mathcal{A}_S$

The aim of this section is to give a characterization of the stabilizer algebra $\mathcal{A}_S$. We start by recalling some facts about Rademacher functions. Further details in this matter can be found in [Wal00].

We set $X := [0,1)$ and equip it with its Borel σ-algebra $\mathcal{B}$ as well as with the Lebesgue measure λ. Obviously, $(X, \mathcal{B}, \lambda)$ forms a probability space. We define a transformation on X,

$$R\colon X \to X; x \mapsto \begin{cases} 2x & x \in [0, \frac{1}{2}) \\ 2x-1 & x \in [\frac{1}{2}, 1) \end{cases}.$$

Note that R is not measure preserving, as $R(\left[0, \frac{1}{4}\right)) = \left[0, \frac{1}{2}\right)$. Let χ_A denote the characteristic function of a Borel set A. Then we can define the *Rademacher functions*

$$r_i : (X, \mathcal{B}, \lambda) \to (\{1,-1\}, \mathcal{P}(\{1,-1\}), (\frac{1}{2}, \frac{1}{2}))$$

for $i \in \mathbb{N}$ by setting

$$\begin{aligned} r_1 &= \chi_{[0,\frac{1}{2})} - \chi_{[\frac{1}{2},1)}, \\ r_{i+1} &= r_i \circ R \text{ for } i \geq 1. \end{aligned}$$

As an example, r_2 is given by

$$r_2 = \chi_{[0,\frac{1}{4})} - \chi_{[\frac{1}{4},\frac{1}{2})} + \chi_{[\frac{1}{2},\frac{3}{4})} - \chi_{[\frac{3}{4},1)},$$

as

$$\begin{array}{lllll} \left[0, \frac{1}{4}\right) & \overset{R}{\longmapsto} & \left[0, \frac{1}{2}\right) & \overset{r_1}{\longmapsto} & 1, \\ \left[\frac{1}{4}, \frac{1}{2}\right) & \overset{R}{\longmapsto} & \left[\frac{1}{2}, 1\right) & \overset{r_1}{\longmapsto} & -1, \\ \left[\frac{1}{2}, \frac{3}{4}\right) & \overset{R}{\longmapsto} & \left[0, \frac{1}{2}\right) & \overset{r_1}{\longmapsto} & 1 \quad \text{and} \\ \left[\frac{3}{4}, 1\right) & \overset{R}{\longmapsto} & \left[\frac{1}{2}, 1\right) & \overset{r_1}{\longmapsto} & -1. \end{array}$$

4.1. REMARK. Let $(r_i)_{i\in\mathbb{N}}$ be the Rademacher functions and let $\mathbb{E}$ stand for the expectation value. Then

(*i*) each r_i is a centered random variable, as $\mathbb{E}(r_i) := \int_X r_i \mathrm{d}\lambda = 0$ for all $i \in \mathbb{N}$,
(*ii*) the random variables r_i for $i \in \mathbb{N}$ generate the σ-algebra $\mathcal{B}$ and
(*iii*) r_i and r_j are independent random variables for $i \neq j$, as

$$\begin{aligned} P(r_i \leq -1) &= \int_{\{x\in X : r_i(x) = -1\}} \mathrm{d}\lambda = \frac{1}{2} \text{ and} \\ P(r_i \leq \ \ 1) &= \int_{\{x\in X : r_i(x) = \ 1\}} \mathrm{d}\lambda = \int_X \mathrm{d}\lambda = 1, \end{aligned}$$

and hence we have for $i \neq j$ that

$$\begin{aligned} \mathbb{P}(r_i \leq a, r_j \leq b) &= \int_{\{x\in X : r_i(x) \leq a, r_j(x) \leq b\}} \mathrm{d}\lambda = \begin{cases} \frac{1}{4} & \text{if } a = b = -1 \\ 1 & \text{if } a = b = 1 \\ \frac{1}{2} & \text{if } a \neq b \end{cases} \\ &= \mathbb{P}(r_i \leq a) \cdot \mathbb{P}(r_j \leq b). \end{aligned}$$

Note that we obtain by independence

$$\mathbb{E}(r_i \cdot r_j) = \mathbb{E}(r_i) \cdot \mathbb{E}(r_j) \text{ for } i \neq j.$$

We define characteristic functions $e_y^i := \chi_{\{r_i=y\}} = \frac{1}{2}(\mathbb{1} + yr_i)$ for $y \in \{1,-1\}$ and $i \in \mathbb{N}$ and obtain $\mathbb{E}(e_y^i) = \frac{1}{2}$ for all $y \in \{1,-1\}$, $i \in \mathbb{N}$. Also $\{E_1^i, E_{-1}^i$ with $i \in \mathbb{N}\}$ generate $\mathcal{B}$ and clearly e_y^i and $E_{y'}^j$ are independent for $i \neq j$.

In chapter 4, we are going to define a quantum probability space, the non-commutative analogue of a classical measure space $L^\infty(\Omega, \Sigma, \mu)$. We may regard $(\mathcal{A}_S, \mathrm{tr})$ as such a quantum probability space. But we have even more, as we see in the following that we are able to find a purely classical description of $(\mathcal{A}_S, \mathrm{tr})$.

By doing this we will notice that there is only one stabilizer algebra $\mathcal{A}_S$ up to isomorphisms.

4.2. Theorem. *Let $\mathcal{A}_S$ be a stabilizer algebra and let $r_1, \dots, r_{n-k}$ be the first $(n-k)$ Rademacher functions on $([0,1), \mathcal{B}, \lambda)$. Let $\mathcal{B}_{n-k}$ be the σ-algebra generated by $(r_i)_{i=1}^{n-k}$. Then there exists an isomorphism*

$$\alpha : L^\infty([0,1), \mathcal{B}_{n-k}, \lambda) \to (\mathcal{A}_S, tr)$$

such that $\int_{[0,1)} f \mathrm{d}\lambda = tr(\alpha(f))$ for all $f \in L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$.

Proof. Let $\mathcal{A}_S$ be generated by independent and commuting elements $g_1, \dots, g_{n-k}$ of the Pauli group G_n such that $-\mathbb{1} \notin G(g_1, \dots, g_{n-k})$.

Let $\mathcal{W}_{n-k}$ denote the algebra generated by the products of $r_1, \dots, r_{n-k}$. Then each such product is called a *Walsh function* and we may assume in this case that these products are finite. Then the algebra of bounded measurable functions on $([0,1), \mathcal{B}_{n-k}, \lambda)$, $L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$, is given by $\mathcal{W}_{n-k}$.

Now the choice of generators $g_1, \dots, g_{n-k}$ for S defines a bijective representation α of $\mathcal{W}_{n-k}$ in $\mathbb{M}_N$ with $\alpha(\mathbb{1}) = \mathrm{id}$ and

$$\alpha : \mathcal{W}_{n-k} \to S \subseteq \mathbb{M}_N : \prod_{i=1}^{n-k} r_i^{x_i} \mapsto \prod_{i=1}^{n-k} g_i^{x_i}$$

for $x_1, \dots, x_{n-k} \in \{0,1\}$. In fact, common diagonalization of all elements of S yields the values of the corresponding Walsh functions on the diagonal.

We now have to prove that α is state-preserving. Let $f = r_{l_1} \cdots r_{l_m}$ be a finite product of different Rademacher functions out of the set $\{r_1, \dots, r_{n-k}\}$. Then

$$\int_{[0,1)} f \mathrm{d}\lambda = \int_{[0,1)} r_{l_1} \cdots r_{l_m} \mathrm{d}\lambda \overset{4.1}{=} \mathbb{E}(r_{l_1}) \cdots \mathbb{E}(r_{l_{n-k}}) = 0 \overset{3.7}{=} \mathrm{tr}(\alpha(f)).$$

By linearity, this extends to all functions $f \in \mathcal{W}_{n-k}$. □

5. Stabilizer Embeddings

Let $S \subseteq \mathbb{M}_N$ be a stabilizer group generated by $(g_i)_{i=1}^{n-k}$. Then there exists a decomposition of $\mathbb{C}^N$ such that

$$\mathbb{C}^N = \bigoplus_{(y_i)_i \in \hat{\mathcal{A}}_S} \mathcal{H}_{(y_i)_i}, \quad \mathcal{H}_{(y_i)_i} \simeq \mathbb{C}^K,$$

due to theorem 3.1, that means there exist partial isometries $c : \mathbb{C}^K \to \mathbb{C}^N$ such that $c(\mathbb{C}^K) = \mathcal{H}_{1^{n-k}}$. In other words, there are partial isometries c such that $E_{1^{n-k}} = cc^*$.

With these isometries, we have finally reached our target, as we are now able to define stabilizer embeddings.

5.1. DEFINITION. Let c be such a partial isometry with

$$c : \mathbb{C}^K \to \mathcal{H}_{1^{n-k}} \oplus 0 \oplus \cdots \oplus 0 \subseteq \mathbb{C}^N = \bigoplus_{(y_i)_i \in \hat{\mathcal{A}}_S} \mathcal{H}_{(y_i)_i}.$$

Then c is called a $[k, n]$-*stabilizer Hilbert space embedding generated by* $(g_i)_{i=1}^{n-k}$.

5.2. REMARK. Note that now it makes sense that we speak about "stabilizer embeddings" instead of "stabilizer codes". Of course, there are many partial isometries c satisfying the above condition.
The space $\mathcal{H}_{1^{n-k}}$ is important in the context of stabilizer embeddings, as $\mathcal{B}(\mathcal{H}_{1^{n-k}})$ will later serve as an example of an algebra of a quantum alphabet. Consequences of the choice of S respectively $\mathcal{H}_{1^{n-k}}$ will be mentioned in chapter 5, section 3. In fact, this choice is the art of coding.

Now we lift the above definition to the state spaces.

5.3. DEFINITION. Let $c : \mathbb{C}^K \to \mathbb{C}^N$ be a $[k, n]$-stabilizer Hilbert space embedding and set

$$C : \mathcal{S}(\mathbb{M}_K) \to \mathcal{S}(\mathbb{M}_N) : \varphi \mapsto \varphi(c^* \cdot c) = \varphi \circ \mathrm{Ad}(c).$$

We call such maps C $[k, n]$-*stabilizer embeddings generated by* $(g_i)_{i=1}^{n-k}$.

If C is a stabilizer embedding generated by $(g_i)_i$ and $x \mapsto \mathrm{tr}(t_{\xi,\eta}x)$ the state induced by a rank-1-operator $t_{\xi,\eta} \in \mathbb{M}_K$ respectively $\mathbb{M}_N$, then

$$C(\mathrm{tr}(t_{\xi,\eta}\cdot)) = \mathrm{tr}(t_{\xi,\eta}c^* \cdot c) = \mathrm{tr}(ct_{\xi,\eta}c^*\cdot) = \mathrm{tr}(t_{c\xi,c\eta}\cdot).$$

It follows that C maps pure states to pure states. As C is isometric, it is injective.

If $\mathrm{Ad}(c) : \mathbb{M}_N \to \mathbb{M}_K : x \mapsto c^*xc$, C is the adjoint operator of $\mathrm{Ad}(c)$ restricted to the unit sphere with respect to the operator norm.

Now we characterize the image of a stabilizer embedding.

5.4. THEOREM. *Let $C : \mathcal{S}(\mathbb{M}_K) \to \mathcal{S}(\mathbb{M}_N)$ be a stabilizer embedding and $E_{(y_i)_i} \in \mathcal{A}_S$ as defined in section 3. For $(y_i)_i \in \hat{\mathcal{A}}_S$ set*

$$\mathcal{S}^{(y_i)_i} := \{\varphi \in \mathcal{S}(\mathbb{M}_N) : \varphi = \varphi \circ Ad(E_{(y_i)_i})\}.$$

Then all orthogonal states with respect to the decomposition in 3.1 are given by the disjoint union

$$\bigcup_{(y_i)_i \in \hat{\mathcal{A}}_S} \mathcal{S}^{(y_i)_i}$$

and the image of C is given by

$$C(\mathcal{S}(\mathbb{M}_K)) = \{\varphi \in \mathcal{S}(\mathbb{M}_N) : \varphi = \varphi \circ Ad(E_{1^{n-k}})\} = \mathcal{S}^{1^{(n-k)}}$$

$$= \{\varphi \in \mathcal{S}(\mathbb{M}_N) : \varphi = \varphi \circ Ad(E_1^i) \text{ for all } i \in \mathbb{N}_{n-k}\},$$

hence the image states have support only on the first component of the decomposable operators of the decomposition in theorem 3.1.

Proof. The orthogonal states are given by $\bigcup_{(y_i)_i \in \hat{\mathcal{A}}_S} \mathcal{S}^{(y_i)_i}$, as the decomposition itself is given by $(E_{(y_i)_i})_{(y_i)_I \in \hat{\mathcal{A}}_S}$ with $\sum_{(y_i)_i \in \hat{\mathcal{A}}_S} E_{(y_i)_i} = \mathbb{1}$ and $E_{(y_i)_i} E_{(z_i)_i} = 0$ for $(y_i)_i \neq (z_i)_i$.

We now prove the first equation for the image of C.

"$\subseteq$": If $\psi \in \mathcal{S}(\mathbb{M}_K)$, then $C(\psi) = \psi \circ \mathrm{Ad}(c) = \psi \circ \mathrm{Ad}(\underbrace{E_{1^{n-k}} c}_{=c})$.

"$\supseteq$": Let $\psi \in \mathcal{S}(\mathbb{M}_N)$ with $\psi = \psi \circ \mathrm{Ad}(E_{1^{n-k}})$. Then $\psi \circ \mathrm{Ad}(c^*) \in \mathcal{S}(\mathbb{M}_K)$ and

$$C(\psi \circ \mathrm{Ad}(c^*)) = \psi \circ \mathrm{Ad}(cc^*) = \psi \circ \mathrm{Ad}(E_{1^{n-k}}) = \psi.$$

For the second equation, we show the following.

"$\subseteq$": As $E_{1^{n-k}} E_1^i = E_1^i E_{1^{n-k}} = E_{1^{n-k}}$ we get

$$\varphi = \varphi(E_{1^{n-k}} \cdot E_{1^{n-k}}) = \varphi(E_{1^{n-k}} E_1^i \cdot E_1^i E_{1^{n-k}}) = \varphi(E_1^i \cdot E_1^i).$$

"$\supseteq$": $E_{1^{n-k}} = \prod_{i=1}^{n-k} E_1^i$ leads to the assertion. □

6. Example of a Stabilizer Embedding

In this section we make an example of the preceding definitions and theory.

Set $k = 1$, $n = 2$ and let $g_1 = \sigma_x \otimes \mathbb{1} \in G_2 \subset \mathbb{M}_K = \mathbb{M}_4$ be the only generator.

Then S and $\mathcal{A}_S$ are given by

$$S = \{\mathbb{1} \otimes \mathbb{1}, \sigma_x \otimes \mathbb{1}\} \text{ and } \mathcal{A}_S = \mathrm{lin}(S) = \{\lambda(\mathbb{1} \otimes \mathbb{1}) + \mu(\sigma_x \otimes \mathbb{1}) : \lambda, \mu \in \mathbb{C}\}.$$

The eigenspaces of $g_1 = \sigma_x \otimes \mathbb{1}$ are

$$ES_1(g_1) = \{\lambda \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} : \lambda, \mu \in \mathbb{C}\}$$

and

$$ES_{-1}(g_1) = \{\lambda \cdot \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + \mu \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ -1 \end{pmatrix} : \lambda, \mu \in \mathbb{C}\}$$

and we obtain for the spectral projections

$$E_1 = E_1^1 = \frac{1}{2}(\mathbb{1} + g_1) = \frac{1}{2} \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}$$

as well as

$$E_{-1} = E^1_{-1} = \frac{1}{2}(\mathbb{1} - g_1) = \frac{1}{2} \cdot \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \mathbb{1}.$$

Hence

$$\mathbb{C}^4 = E_1\mathbb{C}^4 \oplus E_{-1}\mathbb{C}^4 = \mathcal{H}_1 \oplus \mathcal{H}_{-1}$$

and we choose for example the stabilizer Hilbert space embedding

$$c : \quad \mathbb{C}^2 \quad \to \quad \mathcal{H}_1 \oplus 0 \subset \mathbb{C}^4 :$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \quad \mapsto \quad \tfrac{1}{\sqrt{2}} \begin{pmatrix} a \\ b \\ a \\ b \end{pmatrix} = a \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + b \cdot \tfrac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}.$$

If we describe c as a linear map $c : \mathbb{C}^2 \to \mathbb{C}^4$, then c is given by

$$c = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus

$$\mathrm{Ad}(c) : \mathbb{M}_4 \to \mathbb{M}_2 : (x_{ij})_{ij} \mapsto \frac{1}{2} \cdot \begin{pmatrix} x_{11} + x_{13} + x_{31} + x_{33} & x_{12} + x_{14} + x_{32} + x_{34} \\ x_{21} + x_{23} + x_{41} + x_{43} & x_{22} + x_{24} + x_{42} + x_{44} \end{pmatrix}.$$

Let us assume $\varphi = \mathrm{tr}(\varrho\,\cdot) \in \mathcal{S}(\mathbb{M}_2)$ and $\varphi' = \mathrm{tr}(\varrho'\,\cdot) \in \mathcal{S}(\mathbb{M}_4)$. Then the stabilizer embedding

$$C : \mathcal{S}(\mathbb{M}_2) \to \mathcal{S}(\mathbb{M}_4) : \varphi \mapsto \varphi \circ \mathrm{Ad}(c)$$

maps φ to φ' if and only if

$$\varrho' = \mathrm{Ad}(c^*)(\varrho) = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varrho.$$

Of course we have as a consequence

$$\varphi' = \varphi' \circ \mathrm{Ad}(E_1)$$

as in theorem 5.4.

7. m-Blocks of Stabilizer Embeddings

In this section we lift stabilizer embeddings to m-blocks of stabilizer embeddings in order to construct new stabilizer embeddings out of old ones. The blockwise structure leads to shift invariance that will be an important feature of quantum codes and coders.

The section is devided into two parts. Part one describes the algebraical part of the definition, whereas the second part describes the stabilizer embeddings and their properties.

7.1. m-Block Stabilizer Group and Algebra. We start with stabilizer groups, that are given in the form of blocks. Let $S \subseteq G_n$ be a stabilizer group generated by $(g_i)_{i=1}^{n-k}$. Then we can define the *m-block stabilizer group* $T_m := \otimes^m S \subseteq \otimes^m \mathbb{M}_N$ with the notation

$$g_{ij} := \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \otimes \underbrace{g_i}_{j} \otimes \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N$$

for $i \in \mathbb{N}_{n-k}$ and $j \in \mathbb{N}_m$. Then the *-algebras generated by g_{ij} and g_{pq} for $(i,j) \neq (p,q)$ and $i,p \in \mathbb{N}_{n-k}$, $j,q \in \mathbb{N}_m$ are tr-independent, commute and do not generate $-\mathbb{1}$. Hence the g_{ij} are generators of $T_m \subseteq G_{n\cdot m} \subseteq \otimes^m \mathbb{M}_N = \mathbb{M}_{2^{n\cdot m}}$. We further have $G_{n\cdot m} = \otimes^m G_n$ in the sense that elements of $G_{n\cdot m}$ are elementary tensor products of elements of G_n.

The stabilizer algebra of T_m is given by $\mathcal{A}_{T_m} = \otimes^m \mathcal{A}_S$.

7.2. m-Block Stabilizer Embeddings. Now we introduce the according stabilizer embeddings. Let $c : \mathbb{C}^K \to \mathbb{C}^N$ a $[k,n]$-stabilizer Hilbert space embedding of S and $C : \mathcal{S}(\mathbb{M}_K) \to \mathcal{S}(\mathbb{M}_N) : \varphi \mapsto \varphi \circ \mathrm{Ad}(c)$ the adjoint operator of $\mathrm{Ad}(c)$ restricted to the unit sphere, its $[k,n]$-stabilizer embedding. We define

$$c_m := \otimes^m c : \otimes^m \mathbb{C}^K \to \otimes^m \mathbb{C}^N$$

to be a *m-block Hilbert space embedding*. Hence $\mathrm{Ad}(c_m) = \otimes^m \mathrm{Ad}(c)$. Let C^m denote the adjoint operator of $\mathrm{Ad}(c_m)$ restricted to the unit sphere,

$$C^m : \mathcal{S}(\otimes^m \mathbb{M}_K) \to \mathcal{S}(\otimes^m \mathbb{M}_N) : \varphi \mapsto \varphi \circ (\otimes^m \mathrm{Ad}(c))$$

and call C^m the *m-block of the stabilizer embedding* C.

7.1. Remark. C^m obviously maps tensor product states $\varphi_1 \otimes \cdots \otimes \varphi_m \in \mathcal{S}(\otimes^m \mathbb{M}_K)$ with $\varphi_i \in \mathcal{S}(\mathbb{M}_K)$ onto tensor product states $C(\varphi_1) \otimes \cdots \otimes C(\varphi_m)$.

This leads us to see that m-blocks of stabilizer embeddings really are blocks of stabilizer embeddings, but on the other side, they are stabilizer embeddings themselves. This is formulated in the following lemma.

7.2. Lemma. *Let C^m be the m-block of a $[k,n]$-stabilizer embedding C. Then C^m is the $[m\cdot k, m\cdot n]$-stabilizer embedding generated by the stabilizer group T_m respectively the $(g_{ij})_{ij}$ with $i \in \mathbb{N}_{n-k}$ and $j \in \mathbb{N}_m$ as definined in subsection 7.1.*

Proof. We have $\hat{\mathcal{A}}_{T_m} \simeq \hat{\mathcal{A}}_S^m = \{1,-1\}^{m\cdot(n-k)}$. Let $(y_{ij})_{i,j} = ((y_{i1})_i, \ldots, (y_{im})_i) \in \hat{\mathcal{A}}_T$. As

$$\begin{aligned} E_{(y_{ij})_{ij}} &= \prod_{i,j} E^{ij}_{y_{ij}} \\ &= \prod_{i,j} \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \otimes \underbrace{E^i_{y_{ij}}}_{j} \otimes \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \\ &= \left(\prod_i E^i_{y_{i1}} \otimes \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \right) \cdots \left(\prod_i \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \otimes E^i_{y_{im}} \right) \end{aligned}$$

$$= \left(\prod_i E^i_{y_{i1}}\right) \otimes \cdots \otimes \left(\prod_i E^i_{y_{im}}\right) = \bigotimes_j E_{(y_{ij})_i},$$

we get

$$\begin{aligned} \otimes^m \mathbb{C}^N &= \bigoplus_{(y_{ij})_{ij} \in \hat{\mathcal{A}}_T} \mathcal{H}_{(y_{ij})_{ij}}, & \mathcal{H}_{(y_{ij})_{ij}} &\simeq \otimes^m \mathbb{C}^K \\ &= \bigotimes_{j=1}^m \left(\bigoplus_{(y_{ij})_i \in \hat{\mathcal{A}}_S} \mathcal{H}_{(y_{ij})_i}\right), & \mathcal{H}_{(y_{ij})_i} &\simeq \mathbb{C}^K, \mathcal{H}_{(y_{ij})_{ij}} = \otimes_j \mathcal{H}_{(y_{ij})_i}. \end{aligned}$$

Note $\otimes^m \mathbb{C}^K = \mathbb{C}^{K^m} = \mathbb{C}^{2^{m \cdot k}}$. Hence if $c : \mathbb{C}^K \to \mathcal{H}_{1^{n-k}} \oplus 0 \oplus \cdots \oplus 0 \subseteq \mathbb{C}^N$ is the partial isometry defining C, $\otimes^m c : \otimes^m \mathbb{C}^K \to \otimes^m \mathbb{C}^N$ is the $[m \cdot k, m \cdot n]$-stabilizer Hilbert space embedding generated by T_m, as $\otimes^m \mathcal{H}_{1^{n-k}} = \mathcal{H}_{1^{m \cdot (n-k)}}$. Its lifting to the state space is given by C^m, as

$$C^m : \mathcal{S}(\otimes^m \mathbb{M}_K) \to \mathcal{S}(\otimes^m \mathbb{M}_N) : \varphi \mapsto \varphi \circ \mathrm{Ad}(\otimes^m c) = \varphi \circ (\otimes^m \mathrm{Ad}(c)). \qquad \square$$

This lemma lets us find the properties of stabilizer embeddings.

7.3. COROLLARY. *Let C^m be the m-block of a $[k, n]$-stabilizer embedding C and*

$$S_{R,N} : \otimes_{i=1}^m \mathbb{M}_N \to \otimes_{i=1}^m \mathbb{M}_N : \otimes_{i=1}^m x_i \mapsto \mathbb{1}_N \otimes \left(\otimes_{i=1}^{m-1} x_i\right)$$

for $x_i \in \mathbb{M}_N$ the tensor right shift. If we set

$$E^j_{1^{n-k}} := \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N \otimes \underbrace{E_{1^{n-k}}}_{j} \otimes \mathbb{1}_N \otimes \cdots \otimes \mathbb{1}_N$$

for $j \in \mathbb{N}_m$, the image of C^m is given by

$$\begin{aligned} C^m(\mathcal{S}(\mathbb{M}_{K^m})) &= \{\varphi \in \mathcal{S}(\mathbb{M}_{K^m}) : \varphi = \varphi \circ Ad(E_{1^{m \cdot (n-k)}})\} \\ &= \{\varphi \in \mathcal{S}(\mathbb{M}_{K^m}) : \varphi = \varphi \circ Ad(E^j_{1^{n-k}}) \text{ for } j \in \mathbb{N}_m\} \\ &= \{\varphi \in \mathcal{S}(\mathbb{M}_{K^m}) : \varphi = \varphi \circ Ad(S^j_{R,N}(E^1_{1^{n-k}})) \text{ for } 0 \le j \le m-1\} \qquad (1) \\ &= \{\varphi \in \mathcal{S}(\mathbb{M}_{K^m}) : \varphi = \varphi \circ Ad(E^{ij}_1) \text{ for } j \in \mathbb{N}_m, i \in \mathbb{N}_{n-k}\} \\ &= \{\varphi \in \mathcal{S}(\mathbb{M}_{K^m}) : \varphi = \varphi \circ Ad(S^j_{R,N}(E^{i1}_1)) \text{ for } 0 \le j \le m-1, i \in \mathbb{N}_{n-k}\}. \qquad (2) \end{aligned}$$

We notice in corollary 7.3 (1) and (2) shift invariance by $\varphi = \varphi \circ S_{R,N}$ for any state $\varphi \in C^m(\mathcal{S}(\otimes^m \mathbb{M}_K))$. It comes from the blockwise construction and we will keep this shift invariance in mind for later.

7.4. COROLLARY. *Let C^m be the m-block of a $[k, n]$-stabilizer embedding C and set for $(y_{ij})_{ij} \in \hat{\mathcal{A}}_{T_m}$*

$$\begin{aligned} \mathcal{S}^{(y_{ij})_{ij}}_{[0,m]} &= \{\varphi \in \mathcal{S}(\otimes_0^m \mathbb{M}_N) : \varphi = \varphi \circ Ad(E_{(y_{ij})_i}) \text{ for } 0 \le j \le m\} \\ &= \{\varphi \in \mathcal{S}(\otimes_0^m \mathbb{M}_N) : \varphi = \varphi \circ Ad(E^{ij}_{y_{ij}}) \text{ for } 0 \le j \le m \text{ and } i \in \mathbb{N}_{n-k}\}. \end{aligned}$$

Then the orthogonal states with respect to this decomposition are given by

$$\bigcup_{(y_{ij})_{ij}\in\hat{\mathcal{A}}_{T_m}} \mathcal{S}_{[0,m]}^{(y_{ij})_{ij}}.$$

8. Example of an m-Block of a Stabilizer Embedding

In this section we make an example of the m-block of a given stabilizer embedding. We continue the example of section 6.

We saw there that $x \otimes \mathbb{1} \in G_2$ generates a stabilizer embedding for

$$E_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ and } c = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $m = 3$. As $C^3 = \left(\otimes^3 \mathrm{Ad}(c)\right)^* = \otimes^3 \left(\mathrm{Ad}(c)^*\right)$ and

$$\mathrm{Ad}(c)^*(\varrho) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varrho$$

for a density matrix $\varrho \in \mathbb{M}_2$, we obtain

$$C^3(\varrho_1 \otimes \varrho_2 \otimes \varrho_3) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varrho_1 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varrho_2 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varrho_3.$$

As

$$E_{111} = \otimes^3 E_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}_2 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}_2 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{1}_2,$$

we get

$$\mathcal{B}(\mathcal{H}_{111}) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{M}_2 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{M}_2 \otimes \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \mathbb{M}_2.$$

This is a $8 = 2^3$-dimensional *-algebra and its state space is the image of C^3.

9. Stabilizer Embeddings à la Ollivier and Tillich

In this section we give a definition of the special stabilizer embeddings that Ollivier and Tillich are using in [OT03] and [OT04]. We keep the base free formalism developed in this chapter.

As section 7 also this section is devided into two parts. The first subsection describes again the algebraical part of the definition, whereas the second one is dedicated to the stabilizer embeddings and their properties.

9.1. The Ollivier-Tillich-Stabilizer Group and Algebra. We start by studying the special stabilizer group used by Ollivier and Tillich. Instead of using consecutive blocks of shifted versions of one set of generators, we form one big block of overlapping blocks of stabilizer groups now.

Let $S \subseteq G_{n+m}$ be a $[k, n+m]$-stabilizer group generated by independent generators $(g_i)_{i=1}^{n+m-k}$ and consider S as such a block. Recall that hence $S \subseteq \mathbb{M}_{2^{n+m}}$. Let

$$S_{R,2} : \otimes_{-p}^{p}\mathbb{M}_2 \to \otimes_{-p}^{p}\mathbb{M}_2, \otimes_{i=-p}^{p} x_i \mapsto x_p \otimes \left(\otimes_{i=-p}^{p-1} x_i\right)$$

for $x_i \in \mathbb{M}_2$ be the cyclic tensor right shift and

$$S_{L,2} : \otimes_{-p}^{p}\mathbb{M}_2 \to \otimes_{-p}^{p}\mathbb{M}_2, \otimes_{i=-p}^{p} x_i \mapsto \left(\otimes_{i=-p+1}^{p} x_i\right) \otimes x_{-p}$$

for $x_i \in \mathbb{M}_2$ be the cyclic tensor left shift on tensor products of $\mathbb{M}_2$. Now regard a group generated by nth powers of shifts to the right and to the left of the generators of S, namely for $t \in \mathbb{N}$

$$T_t := G(S_{R,2}^{nj}(g_i) \text{ for } 0 \leq j \leq t, i \in \mathbb{N}_{n+m-k},$$
$$S_{L,2}^{nj}(g_i) \text{ for } 0 < j \leq t, i \in \mathbb{N}_{n+m-k}).$$

We require for technical reasons $m < k < n$ and choose only triples m, k, n such that $2p + 1 = m + n(2t + 1)$ for a $p \in \mathbb{N}$. Then $G_{2p+1} \subseteq \otimes_{-p}^{p}\mathbb{M}_2$ is the Pauli group in which we can describe T_t.

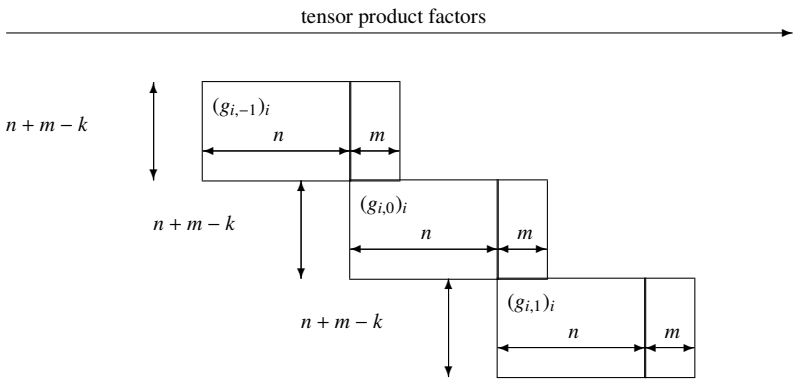
With these requirements obviously only two consecutive blocks are able to overlap. Hence, if all $g_1, \ldots, g_{n+m-k}$ commute with all $S_{R,2}(g_1), \ldots, S_{R,2}(g_{n+m-k})$, T_t is commutative. If $-\mathbb{1} \notin G(S, S_{R,2(S)})$, then one can show that $-\mathbb{1} \notin T_t$. Furthermore, we see that the elements $g_1, \ldots, g_{n+m-k}$, $S_{R,2}(g_1), \ldots, S_{R,2}(g_{n+m-k})$ of the group T_t are independent by construction. Thus under the above assumptions, T_t is a stabilizer group that we call an *OT-stabilizer group*.

Now we fix some notation for the shifted versions of the generators g_i, $i \in \mathbb{N}_{n+m-k}$,

$$g_{ij} = S_{R,2}^{nj}(g_i) \text{ for } 0 \leq j \leq t \text{ and } g_{ij} = S_{L,2}^{-nj}(g_i) \text{ for } -t \leq j < 0.$$

With these abbreviations T_t is generated by $(g_{ij})_{i \in \mathbb{N}_{n+m-k}, -t \leq j \leq t}$.

We sketch this shift generated structure in the following diagramme for $t = 1$.



The *OT-stabilizer algebra* $\mathcal{A}_{T_t} \subseteq \mathcal{M}_2$ *generated by* $(g_{ij})_{i\in\mathbb{N}_{n+m-k},-t\le j\le t}$ is given by

$$\mathcal{A}_{T_t} = \mathcal{A}(g_{ij} : i \in \mathbb{N}_{n+m-k}, -t \le j \le t) = \mathcal{A}(T_t).$$

Obviously an OT-stabilizer group is a stabilizer group and its OT-stabilizer algebra is a stabilizer algebra.

9.2. Ollivier-Tillich-Embeddings. In this section we introduce stabilizer embeddings as Ollivier and Tillich have done.

With $\mathcal{B}_n^0 = \mathbb{M}_{n+m}$, $\mathcal{B}_n^i = \mathbb{M}_n$, we get $\otimes_{-p}^p \mathbb{M}_2 \simeq \otimes_{-t}^t \mathcal{B}_n^i$. Then we have $\mathcal{A}_{T_t} \subseteq \otimes_{-t}^t \mathcal{B}_n^i \simeq \otimes_{-p}^p \mathbb{M}_2$ and $\hat{\mathcal{A}}_{T_t} = \{1,-1\}^{(2t+1)(n+m-k)}$. Note that $\mathcal{A}_{T_t}$ defines $[k_t, n_t]$-stabilizer embeddings with $(2t+1)(n+m-k)$ generators that are elements of G_{n_t} with $n_t = m + (2t+1)n$, and hence $k_t = n_t - (2t+1)(n+m-k) = m + (2t+1)(k-m)$. Thus we have embeddings

$$c_t : \mathbb{C}^{K_t} \to \mathbb{C}^{N_t} = \bigoplus_{(y_{ij})_{ij}\in\hat{\mathcal{A}}_{T_t}} \mathcal{H}_{(y_{ij})_{ij}}$$

with $c_t(\mathbb{C}^{K_t}) \simeq \mathcal{H}_{1^{(2t+1)(n+m-k)}}$ and

$$C_t : \mathcal{S}(\mathbb{M}_{K_t}) \to \mathcal{S}(\mathbb{M}_{N_t}) : \varphi \mapsto \varphi \circ \mathrm{Ad}(c_t).$$

We call C_t the $[k_t, n_t, m]$-*Ollivier-Tillich-embedding*. As in the previous section, we define projections $E_{1^{(2t+1)(n+m-k)}}$, $E^j_{1^{n+m-k}}$ and E^{ij}_1 for $i \in \mathbb{N}_{n+m-k}$ and $-t \le j \le t$. Then we may derive the following two corollaries from theorem 5.4 and the corollaries 7.4 and 7.3.

9.1. Corollary. *Let C_t be a $[k_t, n_t, m]$-Ollivier-Tillich-embedding. Then*

$$\begin{aligned}
C_t(\mathcal{S}(\mathbb{M}_{K_t})) &= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(E_{1^{(2t+1)(n+m-k)}})\} \\
&= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(E^j_{1^{n+m-k}}) \text{ for } -t \le j \le t\} \\
&= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(S^{nj}_{R,2}(E^0_{1^{n+m-k}})) \text{ for } 0 \le j \le t \\
&\qquad \text{and } \varphi = \varphi \circ Ad(S^{-nj}_{L,2}(E^0_{1^{n+m-k}})) \text{ for } -t \le j < 0\} \qquad (1) \\
&= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(E^{ij}_1) \text{ for } i \in \mathbb{N}_{n+m-k}, -t \le j \le t\} \\
&= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(S^{nj}_{R,2}(E^{i0}_1)) \text{ for } 0 \le j \le t, i \in \mathbb{N}_{n+m-k} \\
&\qquad \text{and } \varphi = \varphi \circ Ad(S^{-nj}_{L,2}(E^{i0}_1)) \text{ for } -t \le j < 0, i \in \mathbb{N}_{n+m-k}\}. \qquad (2)
\end{aligned}$$

9.2. Corollary. *Let C_t be a $[k_t, n_t, m]$-Ollivier-Tillich-embedding.*
If we set for all $(y_{ij})_{ij} \in \hat{\mathcal{A}}_{T_t}$

$$\begin{aligned}
\mathcal{S}^{(y_{ij})_{ij}}_{[-t,t]} &= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(E_{(y_{ij})_t}) \text{ for } -t \le j \le t\} \\
&= \{\varphi \in \mathcal{S}(\mathbb{M}_{N_t}) : \varphi = \varphi \circ Ad(E^{ij}_{y_{ij}}) \text{ for } i \in \mathbb{N}_{n+m-k} \text{ and } -t \le j \le t\},
\end{aligned}$$

the orthogonal states with respect to this decomposition are given by

$$\bigcup_{(y_{ij})_{ij}\in\hat{\mathcal{A}}_{T_t}} \mathcal{S}_{[-t,t]}^{(y_{ij})_{ij}}.$$

(1) and (2) give us shift invariance in this finite context as $\varphi = \varphi \circ S_N$ for states $\varphi \in C_t(\mathcal{S}(\mathbb{M}_{K_t}))$. We had the same shift invariance already in corollary 7.3, but this time it comes from the shift structure instead of the blockwise construction.

10. Example of an Ollivier-Tillich-Embedding

Of course, any m-block of a stabilizer embedding is an Ollivier-Tillich-embedding with $m = 0$. Hence a first example of an Ollivier-Tillich-embedding is the example in section 8. It has $m = 0$, $n = 2$ and $k = 1$.

But in this section we want to discuss a litte larger and less trivial example. We choose for $m = 1$, $k = 2$ and $n = 3$

$$g_1 = \sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \mathbb{1}_2,$$
$$g_2 = \mathbb{1}_2 \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z.$$

These generators are obviously commuting and tr-independent. As $\mathrm{diag}(a_1, \ldots, a_n)$ stands for the diagonal matrix with entries $a_1, \ldots, a_n$,

$$\sigma_z \otimes \sigma_z \otimes \sigma_z = \mathrm{diag}(1, -1, -1, 1, -1, 1, 1, -1) \text{ and}$$
$$\frac{1}{2}(\mathbb{1} + \sigma_z \otimes \sigma_z \otimes \sigma_z) = \mathrm{diag}(1, 0, 0, 1, 0, 1, 1, 0).$$

Thus

$$\begin{aligned}
E_{11} &= \frac{\mathbb{1} + \sigma_z \otimes \sigma_z \otimes \sigma_z \otimes \mathbb{1}}{2} \cdot \frac{\mathbb{1} + \mathbb{1} \otimes \sigma_z \otimes \sigma_z \otimes \sigma_z}{2} \\
&= \frac{\mathbb{1} + \sigma_z \otimes \sigma_z \otimes \sigma_z}{2} \otimes \mathbb{1} \cdot \mathbb{1} \otimes \frac{\mathbb{1} + \sigma_z \otimes \sigma_z \otimes \sigma_z}{2} \\
&= \mathrm{diag}(1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0) \cdot \\
&\quad \mathrm{diag}(1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 1, 1, 0) \\
&= \mathrm{diag}(1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0) \\
&= \mathrm{diag}(1, 0) \otimes \mathrm{diag}(1, 0) \otimes \mathrm{diag}(1, 0) \otimes \mathrm{diag}(1, 0) + \\
&\quad \mathrm{diag}(1, 0) \otimes \mathrm{diag}(0, 1) \otimes \mathrm{diag}(0, 1) \otimes \mathrm{diag}(1, 0) + \\
&\quad \mathrm{diag}(0, 1) \otimes \mathrm{diag}(1, 0) \otimes \mathrm{diag}(0, 1) \otimes \mathrm{diag}(0, 1) + \\
&\quad \mathrm{diag}(0, 1) \otimes \mathrm{diag}(0, 1) \otimes \mathrm{diag}(1, 0) \otimes \mathrm{diag}(0, 1).
\end{aligned}$$

This is obviously a $4 = 2^2$ dimensional projection onto H_{11}. If $f_0 \ldots, f_{15}$ denote the canonical basis in $\mathbb{C}^{2^4}$, we may choose

$$c_0 = (f_{0000}, f_{0110}, f_{1011}, f_{1101}) = (f_0, f_6, f_{11}, f_{13}).$$

Of course, $C_0 = \mathrm{Ad}(c_0)^*$ is an OT-embedding for $t = 0$.

If $t = 1$, the projection onto the code Hilbert space $\mathcal{H}_{(11)(11)(11)}$ is given by

$$\begin{aligned} E_{(11)(11)(11)} &= (\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes E_{11} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}) \cdot \\ &\quad (E_{11} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}) \cdot \\ &\quad (\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes E_{11}) \\ &= (\mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} \otimes E_{11} \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1}) \cdot (E_{11} \otimes \mathbb{1} \otimes \mathbb{1} \otimes E_{11}) \end{aligned}$$

After introducing short cuts $a = \mathrm{diag}(1, 0)$ and $b = \mathrm{diag}(0, 1)$ and skipping the tensor product symbols, we calculate

$$\begin{aligned} E_{(11)(11)(11)} &= (\mathbb{1}\mathbb{1}\mathbb{1}a(aa + bb)a\mathbb{1}\mathbb{1}\mathbb{1} + \mathbb{1}\mathbb{1}\mathbb{1}b(ab + ba)b\mathbb{1}\mathbb{1}\mathbb{1}) \cdot \\ &\quad (a(aa + bb)a\mathbb{1}\mathbb{1}a(aa + bb)a + a(aa + bb)a\mathbb{1}\mathbb{1}b(ab + ba)b + \\ &\quad b(ab + ba)b\mathbb{1}\mathbb{1}a(aa + bb)a + b(ab + ba)b\mathbb{1}\mathbb{1}b(ab + ba)b) \\ &= a(aa + bb)a(aa + bb)a(aa + bb)a + b(ab + ba)b(ab + ba)b(ab + ba)b. \end{aligned}$$

This defines a $16 = 2^4$-dimensional projection onto the Hilbert space.

11. Discussion

In this section we discuss to what extent stabilizer embeddings can be seen as coders.

In literature we notice that stabilizer embeddings are injective mappings from one finite-dimensional Hilbert space into a larger finite-dimensional Hilbert space. The choice of the image space is an important instrument, as it may lead to good error correction strategies, as can be found in [NC00].

In quantum information theory, elements of these finite-dimensional Hilbert spaces are seen as qubits, if the Hilbert space dimension is two, or qudits for d-dimensional spaces. Coupled quantum systems are described via the tensor product of the original quantum systems. Therefore quantum versions of classical words would be elements of the tensor product of the system Hilbert space, our possible quantum analogue, with itself.

However, we wish to develop a quantum coding theory with shift spaces consisting of something like infinite words as we did in classical coding theory. Let us for example consider convolutional codes and coders. Both of them only make sense if we look at infinite sequences, as we saw in chapter 1, section 6. Another argument is that considerations about data compression as well as about entropy in the classical theory are inspired by infinite sequences. Last but not least we saw that we may integrate a theory of finite sequences into the infinite setting by using block codes, as we did in chapter 1, section 5. There are also many other reasons for classical code spaces to be infinite and therefore also quantum code spaces will be infinite.

Considering Hilbert spaces as quantum versions of classical alphabets, we have to face another problem - infinite tensor products of Hilbert spaces are problematic. This problem even leads to a lack of clarity in [OT03]. Either we have to define the infinite tensor product with special embeddings along fixed unit vectors, leading to an incomplete tensor product, or we have to work with the more general complete tensor product consisting of all incomplete tensor

products. This complete tensor product is rather unwieldy to work with. Furthermore, the interpretation of elements as coupled qubits becomess difficult.

Therefore we will not choose Hilbert spaces as candidates for quantum alphabets. We will develop a more general quantum coding theory, that can be obtained by algebraisation of classical coding theory in the next chapter. But we will still use stabilizer embeddings to generate examples of our codes, as can be seen in chapter 5. This will be achieved by using stabilizer embeddings working on the state spaces instead of Hilbert space stabilizer embeddings, as we can already conjecture from chapter 3.

As the convex hull of all infinite tensor product states is only contained in the set of states of the infinite tensor product of the algebra with itself, we will instead work on state spaces of infinite tensor products of algebras.

CHAPTER 4

A Quantum Coding Theory

The aim of this chapter is to develop a quantum coding theory.

In order to do this, we first give a brief overview over existing literature and the common ideas about quantum computing. The second section presents a procedure of algebraization of classical concepts. We learn this procedure by example while developing elements of quantum probability. Section 3 presents the usual scheme of a quantum algorithm and describes to what extent our approach will change the scheme. We follow our approach by defining quantum alphabets, quantum shifts and quantum coders in the last three sections. The resulting change of the scheme of a quantum algorithm will be formally noted in section 7.

1. Literature

As already mentioned, Deutsch [**Deu85**] gave the first definition of a quantum Turing machine that was later precised by Bernstein and Vazirani [**BV92**].

In classical information theory, a bit corresponds to a letter in a classical alphabet $A = \{0, 1\}$ as defined in chapter 1. Schumacher specified Deutsch's idea to the definition of a qubit, a quantum version of the above mentioned bits, in [**Sch95**]. For a description of physical realizations of qubits we refer also to [**HS97**]. Qubits were defined to be pure quantum states of two-level systems, described by a unit vector of the system Hilbert space.

After first results in quantum computation by Shor and Grover, Gottesman [**Got97**] introduced error correcting codes in 1997. These codes still work with pure states but allow a good error correcting procedure after transmission. Error correction is necessary as quantum states evolve with time, and this time evolution is disturbed.

As mentioned in the discussion in section 11 of the previous chapter, taking Hilbert spaces as candidates for quantum alphabets causes problems.

In 1998, Aharanov, Kitaev and Nisan [**AKN98**] noted that the restriction to pure states is unnecessary, that mixed states could also be used. This approach is supported by Kribs, Laflamme, Poulin and Lesosky in [**KLPL06**] and [**Pou05**], when they give a more operator algebraic frame to error correction.

2. Some Elements of Quantum Probability

In the following, we give a brief overview over some elements of quantum probability as introduced by Kümmerer and Maassen. For a more detailed description, we refer again to

[KM98] and [Maa06]. We will see later, that these definitions, resulting from a systematical way of algebraization of classical definitions, meet the definitions which we will derive from classical coding theory by the same way of algebraization.

A classical probability space (Ω, Σ, μ) consists of a set of possible outcomes $\omega \in \Omega$, a sigma-algebra Σ consisting of the subsets of Ω that are considered as events, and a probabilty measure μ that associates to each of the events $S \in \Sigma$ a probability $\mu(S)$.

Let us now consider such a probability space (Ω, Σ, μ) and the algebra $l^\infty(\Omega, \Sigma, \mu)$ of bounded functions on Ω. Then μ induces a state φ on $l^\infty(\Omega)$ by

$$\varphi_\mu : l^\infty(\Omega, \Sigma, \mu) \to \mathbb{C} : f \mapsto \int_\Omega f \mathrm{d}\mu.$$

Events $S \in \Sigma$ correspond to characteristic functions on Ω and thus to projections in $l^\infty(\Omega, \Sigma, \mu)$. Thus all information of (Ω, Σ, μ) is also contained in $(l^\infty(\Omega, \Sigma, \mu), \varphi_\mu)$, more exactly, we have obtained an equivalent description of classical probability theory. This description has the advantage, that we can generalize it to the quantum case by swapping to non-commutative algebras and arbitrary states. We come to the following definition.

2.1. DEFINITION. A *quantum probability space* is given by a *-algebra $\mathcal{A}$ and a state φ on $\mathcal{A}$. We denote this tuple by $(\mathcal{A}, \varphi)$.

Independent events $S_1, S_2 \subseteq \Omega$ in (Ω, Σ, μ) are characterized by

$$\mu(S_1 \cap S_2) = \mu(S_1) \cdot \mu(S_2).$$

This can be generalized to independent sub-σ-algebras $\Sigma_1, \Sigma_2 \subseteq \Sigma$ such that all elements of these sub-σ-algebras have to be independent. It can be shown that this is equivalent to the following factorization propery for $f \in l^\infty(\Omega, \Sigma_1, \mu)$ and $g \in l^\infty(\Omega, \Sigma_2, \mu)$,

$$\varphi_\mu(f \cdot g) = \varphi_\mu(f) \cdot \varphi_\mu(g).$$

If we apply this to our quantum definitions, we obtain the following definition introduced by Kümmerer in [Küm85c].

2.2. DEFINITION. Let $(\mathcal{A}, \varphi)$ be a quantum probability space, $\mathcal{B}_1, \mathcal{B}_2$ subalgebras of $\mathcal{A}$ and $B_1 \in \mathcal{B}_1$ respectively $B_2 \in \mathcal{B}_2$. Then B_1 and B_2 are *φ-independent* if and only if

$$\varphi(B_1 \cdot B_2) = \varphi(B_1) \cdot \varphi(B_2).$$

$\mathcal{B}_1$ and $\mathcal{B}_2$ are *φ-independent* if and only if B_1 and B_2 are φ-independent for all $B_1 \in \mathcal{B}_1$ and $B_2 \in \mathcal{B}_2$.

Now we come to quantum operations on quantum probability spaces, i.e. mappings, that take one unital quantum probability space $(\mathcal{A}, \varphi)$ to another $(\mathcal{B}, \psi)$. But then there must be a map taking the input state φ on $\mathcal{A}$ and mapping it to ψ on $\mathcal{B}$. First we discuss the natural requirements for such operations.

Let $f : \mathcal{S}(\mathcal{A}) \to \mathcal{S}(\mathcal{B})$ be such a mapping and $\varphi, \varphi_1, \varphi_2 \in \mathcal{S}(\mathcal{A})$. The *stochastic equivalence principle* states, that a system in a state $\lambda\varphi_1 + (1 - \lambda)\varphi_2$ for $\lambda \in (0, 1)$ can not be distinguished

from a system that is with probability λ in the state φ_1 and with probability $(1-\lambda)$ in φ_2. Thus we have to require

$$f(\lambda\varphi_1 + (1-\lambda)\varphi_2) = \lambda f(\varphi_1) + (1-\lambda)f(\varphi_2),$$

in other words, f has to be *affine*. Hence f can be extended to a unique linear map $T^* : \mathcal{A}^* \to \mathcal{B}^*$, as any element of $\mathcal{A}^*$ respectivey $\mathcal{B}^*$ is given as a linear combination of four states. Hence T^* is the adjoint operator of a linear map $T : \mathcal{B} \to \mathcal{A}$. But of course, T^* still maps states onto states, and thus positive funcionals onto positive functionals - it must be positive. But the classical requirement of positivity must be extended in the quantum case, as shown by Kraus in 1983. The additional requirement is that T must be *completely positive*, i.e. $\mathrm{id}_n \otimes \mathcal{B} : \mathbb{M}_n(\mathcal{B}) \to \mathbb{M}_n(\mathcal{A})$ must be positive for all $n \in \mathbb{N}$. If we want T^* to map states onto states, we need also another requirement, we need for obvious reasons $T(\mathbb{1}) = \mathbb{1}$. We accumulate this to the following definition.

2.3. Definition. A *quantum operation* $T : \mathcal{B} \to \mathcal{A}$ is a linear map between unital *-algebras $\mathcal{A}, \mathcal{B}$ with $T(\mathbb{1}_{\mathcal{B}}) = \mathbb{1}_{\mathcal{A}}$ such that T is completely positive.

An important example of completely positive maps are unit preserving *-homomorphisms.

2.4. Lemma. *If $\mathcal{A}, \mathcal{B}$ are unital *-algebras and $T : \mathcal{B} \to \mathcal{A}$ is a *-homomorphism with $T(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$, then T is a quantum operation.*

Proof. Let n be a natural number and $x_1, \ldots, x_n \in \mathcal{B}$ as well as $y_1, \ldots, y_n \in \mathcal{A}$. Then due to corollary 2.1

$$\begin{aligned}\sum_{i,j=1}^{n} y_i^* T(x_i^* x_j) y_j &= \sum_{i,j=1}^{n} y_i^* T(x_i)^* T(x_j) y_j \\ &= \left(\sum_{i=1}^{n} T(x_i) y_i\right)^* \left(\sum_{j=1}^{n} T(x_j) y_j\right) \geq 0.\end{aligned}$$

□

3. The Usual Scheme of a Quantum Algorithm

In Quantum information theory it is usually agreed, that quantum algorithms follow a certain scheme. This scheme using definitions from [HS97] can be found in [Gra01] or in [NC00]. It consists of the following steps.

(1) We prepare the input state, a pure quantum state φ_0 of a quantum system.
(2) We manipulate the input state φ_0 with automorphisms $\mathrm{Ad}(u)$ given by unitary transformations u on the system Hilbert space and obtain a transformed state φ_1.
(3) We perform measurements on φ_1.

Quantum versions of coders, that have been developed so far, are special quantum algorithms. Therefore the above scheme has also been applied to these quantum coders. This implies that these coders start with pure states on quantum systems and unitary transformations on these Hilbert space vectors, as we mentioned in section 1.

We will use a wider frame and allow mixed states as well as quantum operations as defined in secion 2. This approach will be derived in the next section by applying the same procedure of algebraization on the classical definitions of coding theory. Our approach will lead to a modified scheme of a quantum algorithm described in chapter 6, section 2. Then we will see that both the usual scheme as well as our modified scheme can be described in terms of a quantum mechanical measurement as defined by Kraus. In the same chapter we will describe consequences of the restriction to pure states and quantum operations given by unitary transformations.

4. Quantum Alphabets

Now we follow the procedure of algebraization of a classical definition, which was introduced in section 2. This leads to an operator algebraic frame of a quantum coding theory instead of the Hilbert space theory as in chapter 3, which is usually used.

Let x be an element of a classical finite alphabet A. Then we may identify the letter x with the characteristic function $\chi_{\{x\}} \in l^\infty(\mathrm{A})$ such that $\chi_{\{x\}}(x) = 1$ and $\chi_{\{x\}}(a) = 0$ for $x \neq a \in \mathrm{A}$. If we generalize this to noncommutative algebras, we obtain an observable algebra as a candidate for the quantum version of an alphabet. But as the definitions in quantum information theory usually are given on state spaces, we define as follows.

4.1. DEFINITION. Let $\mathcal{H} = \mathbb{C}^d$ be a finite-dimensional Hilbert space and $\mathcal{A} \subseteq \mathcal{B}(\mathcal{H})$ a C*-algebra. Then $\mathcal{S}(\mathcal{A})$ is a *q-alphabet* and its elements are *q-letters*. $\mathcal{A}$ itself is called the *algebra of the q-alphabet* $\mathcal{S}(\mathcal{A})$. States on $\mathbb{M}_2$ are also refered to as *q-bits* and states on $\mathbb{M}_d$ as *q-dits*.

Since q-alphabets are given by states on observable algebras of quantum systems, blocks of letters respectively letters of a higher alphabet should be states on observable algebras of coupled quantum systems. A coupling of two quantum systems is realized by the tensor product of their observable algebras. This meets the algebraization of classical letters $(x, y) \in \mathrm{A} \times \mathrm{A}$ to functions $\chi_{(x,y)}$ in $l^\infty(\mathrm{A} \times \mathrm{A}) = l^\infty(\mathrm{A}) \otimes l^\infty(\mathrm{A})$.

4.2. DEFINITION. Let $\mathcal{A}$ be the algebra of a q-alphabet $\mathcal{S}(\mathcal{A})$ and $N \in \mathbb{N}$. An *Nth q-higher alphabet* $\mathcal{S}(\mathcal{A}^{[N]})$ *of the q-alphabet* $\mathcal{S}(\mathcal{A})$ is the state space of the N-fold tensor product of $\mathcal{A}$ with itself. Elements of $\mathcal{S}(\mathcal{A}^{[N]})$ are called *N-q-words over the q-alphabet* $\mathcal{S}(\mathcal{A})$.

This definition also meets the definition of quantum registers in [Sch95] and [HS97], as they also used coupled systems to define blocks of their versions of quantum analogues of bits.

4.3. EXAMPLE.

(*i*) Let $\mathcal{H}$ be a finite-dimensional Hilbert space and $\xi_1, \ldots, \xi_N \in \mathcal{H}$. Then $\otimes_{i=1}^N \xi_i$ is an N-q-word over the q-alphabet $\mathcal{S}(\mathcal{B}(\mathcal{H}))$ via the identification of Hilbert space vectors with pure states.

(*ii*) Let e_1, e_2 be an orthonormal basis of $\mathbb{C}^2$. Then the EPR state

$$\phi = \frac{1}{\sqrt{2}} e_1 \otimes e_2 + \frac{1}{\sqrt{2}} e_2 \otimes e_1.$$

is a linear combinations of the two 2-q-words $e_1 \otimes e_2$ and $e_2 \otimes e_1$.

Obviously, higher q-alphabets are also q-alphabets, as the observable algebra of coupled systems is again an observable algebra.

5. Quantum Shifts

In this section we define quantum codes. As mentioned in chapter 3, section 11, we consider a quantum code space to consist of infinitely many coupled q-dits. In the context of classical coding theory, infinite code spaces are shift invariant. This is a very important property. As we hope to implement classical features in quantum coding theory, we establish this notion also in this context. As we did in the beginning of the chapter dealing with classical coding theory, we first define the quantum version of a full shift.

5.1. Definition. Let $\mathcal{A}$ be a the algebra of a q-alphabet $\mathcal{S}(\mathcal{A})$. The *q-full shift* over $\mathcal{A}$ respectively over $\mathcal{S}(\mathcal{A})$ is the state space $\mathcal{S}(\otimes_{\mathbb{Z}}\mathcal{A})$ of the infinite tensor product $\otimes_{\mathbb{Z}}\mathcal{A}$.

Note that $\otimes_{\mathbb{Z}}\mathcal{A}$ is naturally equipped with the tensor right shift and is invariant under this shift. Thus the q-full shift $\mathcal{S}(\otimes_{\mathbb{Z}}\mathcal{A})$ is invariant under the adjoint mapping of the tensor right shift.

Now we want to define the general case, a quantum version of a shift space. Looking at the definition above, we notice that $\otimes_{\mathbb{Z}}\mathcal{A}$ is obtained by an inductive limit construction as defined in chapter 2, section 3,

$$\otimes_{\mathbb{Z}}\mathcal{A} = \overline{\bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m}\mathcal{A}}^{\|\,\|},$$

which is quite similar to the definition of language in chapter 1. To see this, let X be a classical shift space over a finite alphabet A. Recall that classical shift spaces are defined by forbidden words. The language $\mathcal{B}(\mathsf{X})$ of X then is given by

$$\mathcal{B}(\mathsf{X}) = \bigcup_{m\in\mathbb{N}} \mathcal{B}_m(\mathsf{X}),$$

where $\mathcal{B}_m(\mathsf{X})$ stands for the set of all allowed m-words. There exists a mapping

$$P_m : \mathcal{B}_{m+1}(\mathsf{X}) \ni u = u_1 ... u_{m+1} \mapsto u_1 ... u_m \in \mathcal{B}_m(\mathsf{X})$$

that cuts off the last letter of an m-word. We dualize P_m to

$$I_m : l^\infty(\mathcal{B}_m(\mathsf{X})) \to l^\infty(\mathcal{B}_{m+1}(\mathsf{X})) : f \mapsto f \circ P_m.$$

As P_m is surjective, I_m is an embedding. Hence we are able to make an inductive limit construction for the inductive system $(l^\infty(\mathcal{B}_m(\mathsf{X})), I_m)_{m\in\mathbb{N}}$. Its C*-inductive limit is given by the continuous functions on X, $C(\mathsf{X}) = \varinjlim_m l^\infty(\mathcal{B}_m(\mathsf{X}))$. As a generalization of language we use it to define quantum shift spaces.

5.2. Definition. Let $\mathcal{A}$ be the algebra of a q-alphabet $\mathcal{S}(\mathcal{A})$. A subalgebra $\mathcal{A}_m \subseteq \mathcal{A}^{[m]}$ of the algebra of the mth q-higher alphabet $\mathcal{S}(\mathcal{A}^{[m]})$ is called the *algebra of the allowed m-q-words*, its state space $\mathcal{S}(\mathcal{A}_m)$ is the *set of allowed m-q-words*.

Let $(\mathcal{A}_m, \pi_m)_{m\in\mathbb{N}}$ be an inductive sequence where $\mathcal{A}_m$ corresponds to the algebra of allowed m-q-words and the C*-inductive limit $\mathcal{X} := \varinjlim_{m\in\mathbb{N}} \mathcal{A}_m$.

If there exist C*-algebras $C, \mathcal{D}$ and a *-isomorphism $\phi : \mathcal{X} \to (\otimes_{\mathbb{Z}}\mathcal{D}) \otimes C$, we define $S_R \otimes \mathrm{id}_C$ on $(\otimes_{\mathbb{Z}}\mathcal{D})\otimes C$ acting as the tensor right shift S_R on $\otimes_{\mathbb{Z}}\mathcal{D}$ and as the identity on C, and pull back this map on $\mathcal{X}$ via conjugation with ϕ.

In this case we call the conjugated mapping $\phi^{-1}\,(S_R \otimes \mathrm{id}_C)\,\phi$ an *(abstract) tensor right shift* on $\mathcal{X}$, $\mathcal{X}$ the *algebra of the q-shift space over the q-alphabet* $\mathcal{S}(\mathcal{A})$ and its state space $\mathcal{S}(\mathcal{X})$ the *q-shift space over the q-alphabet* $\mathcal{S}(\mathcal{A})$.

Note that $\mathcal{S}(\mathcal{X})$ is invariant under the adjoint mapping of the right shift mentioned in the definition above.

Obviously, q-full shifts equipped with the usual tensor right shift are q-shift spaces and the algebras of general q-shift spaces are AF-algebras. Examples that are not just q-full shift spaces and need a nontrivial abstract right shift will be given in chapter 5.

In order to speak more easily about parts $x_n \otimes \cdots \otimes x_m$ of finite or infinite elementary tensors $\otimes_i x_i$, we put $x_n \otimes \cdots \otimes x_m =: x_{[n,m]} =: x_{(n-1,m+1)} \in \otimes_{i=n}^{m}\mathcal{A}$. We introduce the same notation for restrictions $\varphi_n \otimes \cdots \otimes \varphi_m$ of product states $\otimes_i\varphi_i$ by setting $\varphi_n \otimes \cdots \otimes \varphi_m =: \varphi_{[n,m]} =: \varphi_{(n-1,m+1)}$.

6. Quantum Coders

Looking for quantum analogues of the classical theory, quantum coders should be mappings between quantum shift spaces. They should be structure preserving. This means in this context, that we ask for mappings consistent with the inductive limit constructions of the q-shift spaces, that intertwine the respective shifts. They should also be derived from quantum operations on q-alphabets as defined in section 2. This idea is made more precise in the following definition. In order to make the definition more clear, we give the according commuting diagrams.

6.1. DEFINITION. Let $\mathcal{A}, \mathcal{B}$ be the algebras of q-alphabets $\mathcal{S}(\mathcal{A})$ and $\mathcal{S}(\mathcal{B})$. Let further $\mathcal{X} = \varinjlim_{m\in\mathbb{N}}(\mathcal{A}_m, \pi_m)$ and $\mathcal{Y} = \varinjlim_{m\in\mathbb{N}}(\mathcal{B}_m, \varrho_m)$ be algebras of q-shift spaces over these q-alphabets with shifts $S_{\mathcal{X}}$ and $S_{\mathcal{Y}}$. Let $\Phi_m : \mathcal{A}_m \to \mathcal{B}_m$ for $m \in \mathbb{N}$ be quantum operations satisfying $\Phi_{m+1} \circ \pi_m = \varrho_m \circ \Phi_m$ and let $\Gamma_* : \mathcal{X} \to \mathcal{Y}$ be a quantum operation derived as a continuous extension from $(\Phi_m)_{m\in\mathbb{N}}$.

If Γ_* intertwines the shifts $S_{\mathcal{X}}$ and $S_{\mathcal{Y}}$, i.e. $\Gamma_* \circ S_{\mathcal{X}} = S_{\mathcal{Y}} \circ \Gamma_*$, then Γ_* is called *stationary*.

In this case we call the adjoint mapping $\Gamma : \mathcal{S}(\mathcal{Y}) \to \mathcal{S}(\mathcal{X})$ of Γ_* a *q-coder*.

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{\Gamma_*} & \mathcal{Y} \\ {\scriptstyle S_{\mathcal{X}}}\downarrow & & \downarrow{\scriptstyle S_{\mathcal{Y}}} \\ \mathcal{X} & \xrightarrow{\Gamma_*} & \mathcal{Y} \end{array} \qquad\qquad \begin{array}{ccc} \mathcal{A}_m & \xrightarrow{\Phi_m} & \mathcal{B}_m \\ {\scriptstyle \pi_m}\downarrow & & \downarrow{\scriptstyle \varrho_m} \\ \mathcal{A}_{m+1} & \xrightarrow{\Phi_{m+1}} & \mathcal{B}_{m+1} \end{array}$$

The following theorem helps to find examples for q-coders.

6.2. Theorem. *Let $\mathcal{A}, \mathcal{B}$ be the algebras of q-alphabets and let $\mathcal{X} = \varinjlim_{m\in\mathbb{N}}(\mathcal{A}_m, \pi_m)$ respectively $\mathcal{Y} = \varinjlim_{m\in\mathbb{N}}(\mathcal{B}_m, \varrho_m)$ be algebras of q-shift spaces. Let further $\Phi_m : \mathcal{A}_m \to \mathcal{B}_m$ for $m \in \mathbb{N}$ be linear maps such that $\Phi_{m+1} \circ \pi_m = \varrho_m \circ \Phi_m$.*

If Φ_m is a quantum operation for all $m \in \mathbb{N}$, then $(\Phi_m)_m$ has a unique continuous extension $\Gamma_* : \mathcal{X} \to \mathcal{Y}$ and Γ_* is a quantum operation.

*This holds in particular if Φ_m is a unit preserving *-homomorphism for all $m \in \mathbb{N}$.*

Proof. $\bigcup_{m\in\mathbb{N}} \Phi_m : \bigcup_{m\in\mathbb{N}} \mathcal{A}_m \to \bigcup_{m\in\mathbb{N}} \mathcal{B}_m$ is welldefined. As Φ_m is completely positive, $\|\Phi_m\| = \|\Phi_m(\mathbb{1})\| = \|\mathbb{1}\| = 1$ due to lemma 2.4 in chapter 2 and hence $\bigcup_{m\in\mathbb{N}} \Phi_m$ is bounded. Thus it has a continuous extension that we denote by $\Gamma_* : \mathcal{X} \to \mathcal{Y}$.

Since $\mathbb{1}_{\mathcal{X}} = \mathbb{1}_{\mathcal{A}_0} \in \mathcal{A}_0$ and $\mathbb{1}_{\mathcal{Y}} = \mathbb{1}_{\mathcal{B}_0} \in \mathcal{B}_0$, we obtain

$$\Gamma_*(\mathbb{1}_{\mathcal{X}}) = \bigcup_{m\in\mathbb{N}} \Phi_m(\mathbb{1}_{\mathcal{X}}) = \Phi_0(\mathbb{1}_{\mathcal{A}_0})) = \mathbb{1}_{\mathcal{B}_0} = \mathbb{1}_{\mathcal{Y}}.$$

Thus Γ_* preserves the units.

In order to see that Γ_* is completely positive, let n be a natural number and let $x_1, \dots, x_n \in \mathcal{X}$ and $y_1, \dots, y_n \in \mathcal{Y}$. Then there exist sequences $(x_i^k)_k$ an $(y_i^k)_k$ such that $\lim_k x_i^k = x_i$ and $\lim_k y_i^k = y_i$ for $i \in \mathbb{N}_n$. But then

$$\sum_{i,j=1}^{n} y_i \Gamma_*(x_i^* x_j) y_j = \lim_k \sum_{i,j=1}^{n} y_i^k \Phi_k((x_i^k)^* x_j^k) y_j^k.$$

$\left(\sum_{i,j=1}^{n} y_i^k \Phi_k((x_i^k)^* x_j^k) y_j^k\right)$ is positive as Φ_k is completely positive. As a limit of positive elements is positive, so is $\sum_{i,j=1}^{n} y_i \Gamma_*(x_i^* x_j) y_j$ and hence Γ_* is completely positive. Thus Γ_* is a quantum operation due to definition 2.3.

As *-homomorphisms are completely positive due to lemma 2.2 in chapter 2, the second assertion follows immediately. □

Note that the algebra of a q-shift space over a q-alphabet $\mathcal{A}$ usually is not a subalgeba of the algebra of a q-full shift over $\mathcal{A}$. Therefore we cannot simply require quantum coders to be defined on algebras of q-full shifts that can be restricted later onto smaller algebras of q-shift spaces if wanted.

We first consider examples of q-coders with a blockwise structure, such that their q-shift space can be written as a q-full shift for a q-alphabet $\mathcal{A}$. In the next chapter, we will give examples with more general q-shift spaces.

Now we discuss the examples we introduced in chapter 1.

6.1. There is no Quantum Analogue of a Higher Block Coder. We first try to generalize the notion of a higher block coder from chapter 1, section 2. Then we have to look for unit-preserving *-homomorphisms on algebras of q-alphabets or q-higher alphabets that implement a copying operation.

But the so called *no cloning theorem* ([WZ82], [Die82]) states that it is impossible to create identical copies of an arbitrary unknown quantum state. We present both the description of a classical copying machine as well as the no cloning theorem in the language of quantum operations according to [Maa06].

If A is a finite classial alphabet, then a classical copying operation is given by $t_{\text{copy}} : A \to A \times A : \omega \mapsto (\omega, \omega)$. t_{copy} induces an operation $T_{\text{copy}} : l^\infty(A) \otimes l^\infty(A) = l^\infty(A \times A) \to l^\infty(A) : f \mapsto f \circ t_{\text{copy}}$ such that $T_{\text{copy}}(f)(\omega) = f \circ t_{\text{copy}}(\omega) = f(\omega, \omega)$. Obviously $T_{\text{copy}}(\mathbb{1} \otimes f)(\omega) = (\mathbb{1} \otimes f)(\omega, \omega) = f(\omega)$ and also $T_{\text{copy}}(f \otimes \mathbb{1})(\omega) = (f \otimes \mathbb{1})(\omega, \omega) = f(\omega)$ for all $f \in l^\infty(A)$ and $\omega \in A$ and thus $T_{\text{copy}}(\mathbb{1} \otimes f) = T_{\text{copy}}(f \otimes \mathbb{1}) = f$.

This leads to the definition of a quantum copying operation.

6.3. DEFINITION. Let $\mathcal{A}$ be a finite-dimensional unital *-algebra. A quantum operation $T : \mathcal{A} \otimes \mathcal{A} \to \mathcal{A}$ is a *quantum copying operation*, if $T(\mathbb{1} \otimes A) = T(A \otimes \mathbb{1}) = A$ for all $A \in \mathcal{A}$.

Then the no cloning theorem states the following.

6.4. THEOREM. *Let $\mathcal{A}$ be a finite-dimensional unital *-algebra. Then $\mathcal{A}$ admits a copying operation if and only if $\mathcal{A}$ is abelian.*

The proof of this theorem can be found in [Maa06].

The above theorem states that a copying machine exists only in the classical case. Unfortunately this implies, that there is no hope for quantum versions of higher block coders.

6.2. Quantum Higher Power Coders. We can easily define a quantum version of a higher power coder from chapter 1, section 3. We do this in the following by using the notation introduced at the end of the previous chapter.

Let $N \in \mathbb{N}$. We look at the canonical identification

$$\mathrm{id}_m^N : \otimes_{-m\cdot N}^{(m-1)\cdot N} \mathcal{A} \to \otimes_{-m}^{m-1} \left(\otimes^N \mathcal{A}\right) : x_{[-m\cdot N, m\cdot N)} \mapsto \otimes_{i=-m}^{m} x_{[i\cdot N, i\cdot N+N)}.$$

As $(\mathrm{id}_m^N)_m$ are compatible with the canonical embeddings,

$$\mathrm{id}_{m+1}^N \left((\otimes^N \mathbb{1}_{\mathcal{A}}) \otimes x_{[-m\cdot N, m\cdot N)} \otimes (\otimes^N \mathbb{1}_{\mathcal{A}})\right) = \mathbb{1}_{\otimes^N \mathcal{A}} \otimes \mathrm{id}_m^N(x_{[-m\cdot N, m\cdot N)}) \otimes \mathbb{1}_{\otimes^N \mathcal{A}},$$

we are able to define

$$\mathrm{id}^N : \bigcup_{m\in\mathbb{N}} \otimes_{-m\cdot N}^{m\cdot N} \mathcal{A} \to \bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m} \left(\otimes^N \mathcal{A}\right) : x_{[-m\cdot N, m\cdot N)} \mapsto \otimes_{i=-m}^{m} x_{[i\cdot N, i\cdot N+N)}.$$

As id^N is obviously bounded, it has a continuous extension to the C*-inductive limits $\otimes_{\mathbb{Z}} \mathcal{A}$ respectively $\otimes_{\mathbb{Z}} \left(\otimes^N \mathcal{A}\right)$, that we denote by the same symbol id^N.

Now we consider the adjoint operator $\Gamma_N := (\mathrm{id}^N)^*$ of id^N,

$$\Gamma_N : \mathcal{S}(\otimes_{\mathbb{Z}} \mathcal{A}) \to \mathcal{S}(\otimes_{\mathbb{Z}} (\otimes^N \mathcal{A})).$$

Γ_N acts on tensor product states as follows,

$$\otimes_{i\in\mathbb{Z}} \varphi_i \mapsto \otimes_{i\in\mathbb{Z}} \varphi_{[N\cdot i, N\cdot i+N)}.$$

Γ_N is a quantum version of a higher power coder and obviously a q-coder. Thus we call it the *N-th q-higher power coder*.

6.3. Quantum Sliding Block Coders. The next coders we want to generalize are sliding block coders from chapter 1, section 4. But theorem 4.6 in chapter 1 states, that sliding block coders with nontrivial memory and anticipation make use of higher block coders. As the no cloning theorem 6.4 made quantum versions of higher block coders impossible, it also reduces any quantum version of sliding block coders to quantum versions of 1-block coders. We construct such quantum analogues of 1-block codes in the following.

Let $\mathcal{S}(\mathcal{A})$ and $\mathcal{S}(\mathcal{B})$ be q-alphabets with according algebras $\mathcal{A}$ and $\mathcal{B}$. A *q-1-block map* is a *-isomorphism $\Phi : \mathcal{A} \to \mathcal{B}$ such that $\Phi(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$. An example is given in chapter 5, section 1. Then we can construct a unit preserving *-isomorphism between the infinite tensor products $\otimes_{\mathbb{Z}}\mathcal{A}$ and $\otimes_{\mathbb{Z}}\mathcal{B}$ from Φ as we did for the q-higher power coders. We start by checking that

$$(\otimes_{-m-1}^{m+1}\Phi)(\mathbb{1}_{\mathcal{A}} \otimes x_{[-m,m]} \otimes \mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}} \otimes ((\otimes_{-m}^{m}\Phi)(x_{[-m,m]})) \otimes \mathbb{1}_{\mathcal{B}}.$$

Hence we can define

$$\phi : \bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m}\mathcal{A} \to \bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m}\mathcal{B} : \otimes_{-m}^{m} x_i \mapsto \otimes_{-m}^{m}\Phi(x_i).$$

ϕ is bounded and thus has a continuous extension, which we denote by the same symbol, $\phi : \otimes_{\mathbb{Z}}\mathcal{A} \to \otimes_{\mathbb{Z}}\mathcal{B}$ due to 6.2. $\otimes_{\mathbb{Z}}\mathcal{A}$ and $\otimes_{\mathbb{Z}}\mathcal{B}$ are naturally equipped with the tensor right shift and ϕ intertwines those shifts.

6.5. Lemma. *Let $\Gamma_\phi = \phi^*$ be a q-1-block coder. Let $S_{R,\otimes_{\mathbb{Z}}\mathcal{A}}$ respectively $S_{R,\otimes_{\mathbb{Z}}\mathcal{B}}$ denote the right shift on $\otimes_{\mathbb{Z}}\mathcal{A}$ respectively $\otimes_{\mathbb{Z}}\mathcal{B}$. Then ϕ intertwines the shifts,*

$$\phi \circ S_{R,\otimes_{\mathbb{Z}}\mathcal{A}} = S_{R,\otimes_{\mathbb{Z}}\mathcal{B}} \circ \phi,$$

respectively the following diagramme commutes.

$$\begin{array}{ccc} \otimes_{\mathbb{Z}}\mathcal{A} & \xrightarrow{\phi} & \otimes_{\mathbb{Z}}\mathcal{B} \\ {\scriptstyle S_{R,\otimes_{\mathbb{Z}}\mathcal{A}}}\downarrow & & \downarrow{\scriptstyle S_{R,\otimes_{\mathbb{Z}}\mathcal{B}}} \\ \otimes_{\mathbb{Z}}\mathcal{A} & \xrightarrow{\phi} & \otimes_{\mathbb{Z}}\mathcal{B} \end{array}$$

Proof. Let Γ_ϕ, $S_{R,\otimes_{\mathbb{Z}}\mathcal{A}}$, $S_{R,\otimes_{\mathbb{Z}}\mathcal{B}}$ and a fixed $m \in \mathbb{N}$ be given. Let further $\otimes_{-m}^{m} x_i$ be an element of $\otimes_{\mathbb{Z}}\mathcal{A}$. As $\phi(\otimes_{-m}^{m} x_i) = \otimes_{-m}^{m}\Phi(x_i)$, we get

$$\begin{aligned} \phi \circ S_{R,\otimes_{\mathbb{Z}}\mathcal{A}}\Big(\mathbb{1}_{\mathcal{A}} \otimes (\otimes_{-m}^{m} x_i) \otimes \mathbb{1}_{\mathcal{A}}\Big) &= \phi\Big(\mathbb{1}_{\mathcal{A}} \otimes \mathbb{1}_{\mathcal{A}} \otimes (\otimes_{-m}^{m} x_i)\Big) \\ &= \mathbb{1}_{\mathcal{B}} \otimes \mathbb{1}_{\mathcal{B}} \otimes \Big(\otimes_{-m}^{m}\Phi(x_i)\Big) \\ &= S_{R,\otimes_{\mathbb{Z}}\mathcal{B}}\Big(\mathbb{1}_{\mathcal{B}} \otimes (\otimes_{-m}^{m}\Phi(x_i)) \otimes \mathbb{1}_{\mathcal{B}}\Big) \\ &= S_{R,\otimes_{\mathbb{Z}}\mathcal{B}} \circ \phi\Big(\mathbb{1}_{\mathcal{A}} \otimes (\otimes_{-m}^{m} x_i) \otimes \mathbb{1}_{\mathcal{A}}\Big). \end{aligned}$$

As ϕ is linear and continuous, this equality for shift invariance holds on all elements. □

Thus ϕ is stationary. Hence its adjoint operator $\Gamma_\phi := \phi^*$,

$$\Gamma_\phi : \mathcal{S}(\otimes_{\mathbb{Z}}\mathcal{B}) \to \mathcal{S}(\otimes_{\mathbb{Z}}\mathcal{A}) : \varphi \mapsto \varphi \circ \phi$$

is a q-coder mapping one q-shift space of infinitely many q-bits to an other.

If we define $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{A}}$ respectively $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{B}}$ to be the shift on tensor product states on $\otimes_{\mathbb{Z}}\mathcal{A}$ respectively $\otimes_{\mathbb{Z}}\mathcal{B}$, we obtain that Γ_ϕ intertwines the shifts on the state spaces. This is made more precise in the following remark.

6.6. REMARK. Let $\Gamma_\phi = \phi^*$ be a q-1-block coder, $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{A}}$ the left shift on the set of tensor product states $\otimes_{\mathbb{Z}}\mathcal{S}(\mathcal{A}) := \{\otimes_{\mathbb{Z}}\varphi_i : \varphi_i \in \mathcal{S}(\mathcal{A})\}$ and $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{B}}$ the left shift on $\otimes_{\mathbb{Z}}\mathcal{S}(\mathcal{B}) := \{\otimes_{\mathbb{Z}}\varphi_i : \varphi_i \in \mathcal{S}(\mathcal{B})\}$. Then Γ_ϕ as well as the shifts leave the tensor product states invariant and since $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{A}} = S^*_{R,\otimes_{\mathbb{Z}}\mathcal{A}}$ and $\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{B}} = S^*_{R,\otimes_{\mathbb{Z}}\mathcal{B}}$, the shifts are intertwined by Γ_ϕ,

$$\Gamma_\phi \circ \sigma_{L,\otimes_{\mathbb{Z}}\mathcal{B}} = \sigma_{L,\otimes_{\mathbb{Z}}\mathcal{A}} \circ \Gamma_\phi.$$

Since Γ_ϕ is a quantum version of a 1-block coder, and we call it a *q-1-block coder*.

We can make q-1-block coders a little bit more interesting by looking at q-1-block coders on q-full shifts over a q-higher alphabet. As mentioned in chapter 3, section 11, examples for such q-1-block maps can be constructed using stabilizer embeddings. Their q-1-block coders are studied in chapter 5, section 1.

6.4. Quantum Analogues of Linear Coders and Convolutional Coders. Clearly, q-coders are in particular generalizations of classical linear coders as defined in chapter 1, section 5.

If we recall the definition and properties of classical convolutional coders as defined in chapter 1, section 6, the characterization which fits most into our context is to ask for continuous q-coders mapping one q-shift space onto another. But all q-coders satisfy this requirement. Thus any q-coder can be considered as a quantum version of a convolutional coder.

In order to obtain examples for q-coders that are not q-1-block coders, we will use Ollivier-Tillich-stabilizer embeddings, which we introduced in chapter 3, section 9. We will construct q-coders from these mappings in chapter 5, section 2.

7. The New Scheme of a Quantum Algorithm

In this chapter we generalized the common scheme of quantum algorithms using only pure states and automorphisms given by unitary transformations to a more general one. This more general scheme allows mixed states as well as arbitrary quantum operations and is described below.

(1) We prepare a mixed quantum state φ_0 of a quantum system as the input state.
(2) We manipulate the input state φ_0 with adjoint mappings of unit preserving quantum operations and obtain a transformed state φ_1.
(3) We perform measurements on φ_1.

Also this new scheme fits into the context of quantum measurements as defined by Kraus. We will describe these quantum mechanical measurements in chapter 6, section 1.

Obviously the usual scheme working with pure states and automorphisms $\mathrm{Ad}(u)$ for unitary transformations u on the Hilbert space is contained in the new scheme.

CHAPTER 5

Examples of Quantum Coders

Examples of q-coders should be derived from stationary quantum operations on AF-algebras. We first have a look at the examples, which we can define by using stabilizer embeddings.

Considering $[k, n]$-stabilizer embeddings as defined in chapter 3, we may simply let k and n tend to infinity, but then we lose all hope for shift invariance. If we discuss m-blocks of $[k, n]$-stabilizer embeddings instead, we may also enlarge the number of blocks m instead of k and n, and we obtain shift invariance on the m-block. Looking at Ollivier-Tillich-stabilizer embeddings, we may enlarge the number of shifted blocks specified by the parameter t instead of k and n. We will etablish shift invariance in both cases.

We also describe the image state space of an infinite block of a stabilizer embedding as a subset of states in a larger state space.

1. Infinite Blocks of Stabilizer Embeddings

In this section we regard a stabilizer embedding as the quantum analogue of a classical 1-block map of a higher alphabet. We lift this to a mapping on a q-full shift.

Let $c : \mathbb{C}^K \to \mathbb{C}^N$ be a $[k, n]$-stabilizer embedding as in chapter 3, section 5. Recall that $c^*c = \mathbb{1}_K$ and that cc^* is a projection in $\mathbb{M}_N$. Then $\mathrm{Ad}(c^*) : \mathbb{M}_K \to \mathbb{M}_N$ is injective since $cyc^* = 0$ if and only if $c^*cyc^*c = y = 0$. As $\mathrm{Ad}(c)\mathrm{Ad}(c^*)x = c^*cxc^*c = x$, we see that $\mathrm{Ad}(c)$ is injective on the image $c\mathbb{M}_Kc^* \subseteq \mathbb{M}_N$ of $\mathrm{Ad}(c^*)$. We easily check that $\mathrm{Ad}(c^*) : \mathbb{M}_K \to c\mathbb{M}_Kc^*$ is a *-isomorphism and hence $c\mathbb{M}_Kc^*$ is isomorphic to $\mathbb{M}_K$.

Thus $\mathrm{Ad}(c) : \mathbb{M}_N \supseteq c\mathbb{M}_Kc^* \to \mathbb{M}_K$ defines a q-1-block map $\mathrm{Ad}(c)^*$ between the q-alphabets $\mathcal{S}(c\mathbb{M}_Kc^*)$ and $\mathcal{S}(\mathbb{M}_K)$ as in chapter 4, section 6. Since $\mathbb{M}_N = \otimes^n\mathbb{M}_2$ and $\mathbb{M}_K = \otimes^k\mathbb{M}_2$ we may also interpret both algebras as the algebras of q-higher alphabets of the q-alphabet $\mathcal{S}(\mathbb{M}_2)$.

Now we define

$$\otimes^m_{-m}\mathrm{Ad}(c) : \bigotimes_{-m}^{m} c\mathbb{M}_Kc^* \to \bigotimes_{-m}^{m} \mathbb{M}_K.$$

Now we want to lift the mapping to $\bigcup_{m\in\mathbb{N}} \otimes^m_{-m} c\mathbb{M}_Kc^*$ and define embeddings

$$\pi_m : \otimes^m_{-m} c\mathbb{M}_Kc^* \to \otimes^{m+1}_{-m-1} c\mathbb{M}_Kc^* : x \mapsto cc^* \otimes x \otimes cc^*$$

for $x \in \otimes_{-m}^{m} c\mathbb{M}_K c^*$. In order to check whether the $(2m+1)$-blocks $\otimes_{-m}^{m}\mathrm{Ad}(c)$ of the stabilizer embedding c are compatible with the embeddings $(\pi_m)_m$, we compute as for general q-1-block-coders in chapter 4 at the end of section 6 that the following diagramme commutes.

$$\begin{array}{ccc} \otimes_{-m}^{m} c\mathbb{M}_K c^* & \xrightarrow{\otimes_{-m}^{m}\mathrm{Ad}(c)} & \otimes_{-m}^{m}\mathbb{M}_K \\ {\scriptstyle \pi_m}\downarrow & & \downarrow \\ \otimes_{-m-1}^{m+1} c\mathbb{M}_K c^* & \xrightarrow{\otimes_{-m-1}^{m+1}\mathrm{Ad}(c)} & \otimes_{-m-1}^{m+1}\mathbb{M}_K \end{array}$$

This is shown in the following equation,

$$\begin{aligned} \otimes_{-m-1}^{m+1}\mathrm{Ad}(c)(cc^* \otimes (\otimes_{-m}^{m} x_i) \otimes cc^*) &= c^*cc^*c \otimes (\otimes_{-m}^{m} cx_ic^*) \otimes c^*cc^*c \\ &= \mathbb{1}_K \otimes (\otimes_{-m}^{m} cx_ic^*) \otimes \mathbb{1}_K. \end{aligned}$$

Hence we can set

$$\begin{array}{rcccl} \otimes_{\mathbb{Z}}\mathrm{Ad}(c) & : & \bigcup_{m\in\mathbb{Z}} \bigotimes_{-m}^{m} c\mathbb{M}_K c^* & \to & \bigcup_{m\in\mathbb{Z}} \bigotimes_{-m}^{m} \mathbb{M}_K \\ & & \otimes_{-m}^{m} x_i & \mapsto & (\otimes_{-m}^{m}\mathrm{Ad}(c))\,(\otimes_{-m}^{m} x_i) \\ & & & & = \otimes_{-m}^{m} cx_ic^*. \end{array}$$

1.1. LEMMA. *$\otimes_{\mathbb{Z}}Ad(c)$ has a unique continuous extension to $\mathcal{M}_c = \varinjlim_m \bigotimes_{-m}^{m} c\mathbb{M}_K c^*$, which we denote by the same symbol, $\otimes_{\mathbb{Z}}Ad(c) : \mathcal{M}_c \to \mathcal{M}_K = \varinjlim_m \bigotimes_{-m}^{m} \mathbb{M}_K$.*

PROOF. As $\otimes_{-m}^{m}\mathrm{Ad}(c) = \mathrm{Ad}(\otimes_{-m}^{m} c)$ is completely positive on $\otimes_{-m}^{m} c\mathbb{M}_K c^*$ and as obviously $\otimes_{-m}^{m}\mathrm{Ad}(c)(cc^*) = \mathbb{1}_K$, we obtain due to lemma 2.4 in chapter 2 that $\|\otimes_{-m}^{m}\mathrm{Ad}(c)\| = 1$. Analogously we obtain $\|\otimes_{\mathbb{Z}}\mathrm{Ad}(c)\| = 1$ on $\otimes_{-m}^{m} c\mathbb{M}_K c^*$. Thus $\otimes_{\mathbb{Z}}\mathrm{Ad}(c)$ can be extended to a bounded operator on the inductive limit having the same operator norm. □

1.2. REMARK. We obtain that $\otimes_{\mathbb{Z}}\mathrm{Ad}(c) : \otimes_{\mathbb{Z}} c\mathbb{M}_K c^* \to \mathcal{M}_K$ is a *-isomorphism between AF-algebras. But it is not the inverse of an embedding of $\mathcal{M}_K$ into $\mathcal{M}_N$, as $\mathcal{M}_K$ is not a subalgebra of $\mathcal{M}_N$.

Looking again at the state spaces, we get the following.

1.3. DEFINITION. Given $\mathcal{M}_K$, $\mathcal{M}_c$ and $\otimes_{\mathbb{Z}}\mathrm{Ad}(c)$ as above, we let

$$\Gamma_{\otimes_{\mathbb{Z}}} : \mathcal{S}(\mathcal{M}_K) \to \mathcal{S}(\mathcal{M}_c) : \varphi \mapsto \varphi \circ \otimes_{\mathbb{Z}}\mathrm{Ad}(c)$$

be the *infinite block of a $[k,n]$-stabilizer embedding c*.

As $\Gamma_{\otimes_{\mathbb{Z}}}$ is the adjoint mapping of a *-isomorphism, it is bijective.
The structure of $\Gamma_{\otimes_{\mathbb{Z}}}$ as a q-1-block coder implies that $\otimes_{\mathbb{Z}}\mathrm{Ad}(c)$ intertwines the shifts $S_{R,N}$ on $\mathcal{M}_c$ and $S_{R,K}$ on $\mathcal{M}_K$ due to lemma 6.5 in chapter 4,

$$\otimes_{\mathbb{Z}}\mathrm{Ad}(c) \circ S_{R,N} = S_{R,K} \circ \otimes_{\mathbb{Z}}\mathrm{Ad}(c),$$

respectively the following diagramme commutes.

$$\begin{array}{ccc} \mathcal{M}_c & \xrightarrow{\otimes_{\mathbb{Z}}\mathrm{Ad}(c)} & \mathcal{M}_K \\ {\scriptstyle S_{R,N}}\downarrow & & \downarrow{\scriptstyle S_{R,K}} \\ \mathcal{M}_c & \xrightarrow{\otimes_{\mathbb{Z}}\mathrm{Ad}(c)} & \mathcal{M}_K \end{array}$$

As in chapter 4, remark 6.6, we thus obtain stationarity on the state spaces as well as on the tensor product states.

Classical coders usually hide a given code space in a larger one. Therefore in the image code space of a classical coder only certain sequences are images of the mapped code space. Of course, we would like to establish this property also in the quantum case. We are going to see in the following that image states of $\Gamma_{\otimes_{\mathbb{Z}}}$ can be seen as states on $\mathcal{M}_N$, that are invariant under projections of the form $\cdots \otimes \mathbb{1}_N \otimes cc^* \otimes \mathbb{1}_N \otimes \cdots$.

In order to do this, we define projections as we did for C in chapter 3, section 5 respectively section 7. By doing this we will notice why it makes sense to call $\Gamma_{\otimes_{\mathbb{Z}}}$ an infinite block of a stabilizer embedding. We set

$$g_{ij} := \cdots \otimes \mathbb{1}_N \otimes \underbrace{g_i}_{j} \otimes \mathbb{1}_N \otimes \cdots \in \mathcal{M}_N$$

for any generator g_i of S. Then the g_{ij} commute and do not generate $-\mathbb{1}$. If $\mathrm{tr} := \otimes_{\mathbb{Z}}\mathrm{tr}_N$, the *-algebras they generate are tr-independent. Hence these operators g_{ij} generate a group $T_{\mathbb{Z}} \subseteq \mathcal{M}_N$. Note that we could call $T_{\mathbb{Z}}$ a generalized stabilizer group, as it meets all requirements exept that it is not an element of a finite-dimensional Pauli group. This is the reason why we call $\Gamma_{\otimes_{\mathbb{Z}}}$ an infinite block of a stabilizer embedding. But we are not able to preserve the whole algebraic structure concerning stabilizer algebras. To see this, let $\mathcal{A}_{T_{\mathbb{Z}}} \subseteq \mathcal{M}_N$ denote the algebra generated by $T_{\mathbb{Z}}$. Then

$$\begin{aligned} \hat{\mathcal{A}}_{T_{\mathbb{Z}}} &= (\{1,-1\}^{n-k})^{\mathbb{Z}} \\ &= \{(\ldots,(y_{i0})_i,(y_{i1})_i,(y_{i2})_i,\ldots) : (y_{ij})_i \in \{1,-1\}^{n-k} \text{ for } j \in \mathbb{Z}\}. \end{aligned}$$

We further have $\sigma(g_{ij}) = \{1,-1\}$. Defining the corresponding spectral projections F_y^{ij} by

$$F_y^{ij} := \cdots \otimes \mathbb{1}_N \otimes \underbrace{E_y^i}_{j} \otimes \mathbb{1}_N \otimes \cdots \in \mathcal{A}_{T_{\mathbb{Z}}} \subseteq \mathcal{M}_N$$

for $y \in \{1,-1\}$, we obtain $g_{ij} = F_1^{ij} - F_{-1}^{ij}$. Now put

$$\begin{aligned} F_{(y_{ij})_i} &:= \cdots \otimes \mathbb{1}_N \otimes \underbrace{E_{(y_{ij})_i}}_{j} \otimes \mathbb{1}_N \otimes \cdots \\ &= \prod_{i=1}^{n-k} F_{y_{ij}}^{ij} \in \mathcal{A}_{T_{\mathbb{Z}}} \subseteq \mathcal{M}_N \end{aligned}$$

for $(y_{ij})_i \in \hat{\mathcal{A}}_S$ and $E_{(y_{ij})_i} = \prod_{i=1}^{n-k} E^i_{y_{ij}}$. An important case for the following is given for $(y_{ij})_{ij} = 1^{(n-k)\mathbb{Z}}$,

$$\begin{aligned} F_{1^{n-k},j} &= \cdots \otimes \mathbb{1}_N \otimes \underbrace{E_{1^{n-k}}}_{j} \otimes \mathbb{1}_N \otimes \cdots \\ &= \cdots \otimes \mathbb{1}_N \otimes \underbrace{cc^*}_{j} \otimes \mathbb{1}_N \otimes \cdots =: F_j. \end{aligned}$$

In order to calculate the common spectral projections of the elements of $\mathcal{A}_{T_\mathbb{Z}}$, we would have to define the infinite product over all $j \in \mathbb{Z}$ of the projections $F_{(y_{ij})_i}$ for $(y_{ij})_{i\in\mathbb{N}_{n-k},j\in\mathbb{Z}} = ((y_{ij})_{i=1}^{n-k})_{j\in\mathbb{Z}} \in \mathcal{A}_{T_\mathbb{Z}}$. But this product corresponds to the infinite tensor product over all $j \in \mathbb{Z}$ of the projections $E_{(y_{ij})_i}$ and therefore is not an element of $\mathcal{M}_N$ and hence not an element of $\mathcal{A}_{T_\mathbb{Z}}$. But we can still calculate the image of $\Gamma_{\otimes_\mathbb{Z}}$. We start by setting

$$\mathcal{S}^{(y_{ij})_{ji}}_{[K,N]} := \{\varphi \in \mathcal{S}(\mathcal{M}_N) : \varphi = \varphi \circ \mathrm{Ad}(F_{(y_{ij})_i}) \text{ for all } j \in \mathbb{Z}\}.$$

Hence we obtain for $(y_{ij})_{ij} = 1^{(n-k)\mathbb{Z}}$

$$\mathcal{S}^{1^{(n-k)\mathbb{Z}}}_{[K,N]} = \{\varphi \in \mathcal{S}(\mathcal{M}_N) : \varphi = \varphi \circ \mathrm{Ad}(F_j) \text{ for all } j \in \mathbb{Z}\}.$$

1.4. REMARK. Let $(y_{ij})_{ij} \in \hat{\mathcal{A}}_{T_\mathbb{Z}}$ and $J \subseteq \mathbb{Z}$ be finite. As $\mathcal{S}(\mathcal{M}_N)$ is a compact convex set,

$$\mathcal{S}(\mathcal{M}_N)^J := \{\varphi \in \mathcal{S}(\mathcal{M}_N) : \varphi = \varphi \circ \mathrm{Ad}(F_{(y_{ij})_i}) \text{ for all } j \in J\}$$

is nonempty and closed. But as finite intersections of sets $\mathcal{S}(\mathcal{M}_N)^J$ are again of this form, any finite intersection is not empty. Hence by compactness of $\mathcal{S}(\mathcal{M}_N)$,

$$\mathcal{S}^{(y_{ij})_{ij}}_{[K,N]} = \bigcap_{J\subseteq\mathbb{Z} \text{ finite}} \mathcal{S}(\mathcal{M}_N)^J$$

is not empty.

The following theorem states that infinite blocks of stabilizer embeddings have an analogue property as classical coders, as we mentioned above.

1.5. THEOREM. *Let $\Gamma_{\otimes_\mathbb{Z}} : \mathcal{S}(\mathcal{M}_K) \to \mathcal{S}(\mathcal{M}_c)$ be the infinite block of a $[k, n]$-stabilizer embedding c. Then the image of $\Gamma_{\otimes_\mathbb{Z}}$ is given by $\mathcal{S}^{1^{(n-k)\mathbb{Z}}}_{[K,N]}$.*

PROOF. In the following consider $Ad(c) : \mathbb{M}_N \to \mathbb{M}_K$ instead of its restriction to $c\mathbb{M}_K c^*$ and recall that cc^* is a projection in $\mathbb{M}_N$.

First we show that $\Gamma_{\otimes_\mathbb{Z}}(\mathcal{S}(\mathcal{M}_K)) = \mathcal{S}(\mathcal{M}_c) \subseteq \mathcal{S}^{1^{(n-k)\mathbb{Z}}}_{[K,N]}$.

$$\mathrm{Ad}(cc^*) = \mathrm{Ad}(c^*) \circ \mathrm{Ad}(c) : \mathbb{M}_N \to c\mathbb{M}_K c^*$$

is completely positive and $\mathrm{Ad}(cc^*)(\mathbb{1}_N) = cc^* = \mathbb{1}_{c\mathbb{M}_K c^*}$. As obviously for all $x \in \otimes^m_{-m}\mathbb{M}_N$

$$\otimes^{m+1}_{-m-1}\mathrm{Ad}(cc^*)(\mathbb{1}_N \otimes x \otimes \mathbb{1}_N) = cc^* \otimes \Big(\otimes^m_{-m} \mathrm{Ad}(cc^*)(x)\Big) \otimes cc^*,$$

we may define

$$\bigcup_{m\in\mathbb{N}} \otimes^m_{-m}\mathrm{Ad}(cc^*) : \bigcup_{m\in\mathbb{N}} \otimes^m_{-m}\mathbb{M}_N \to \bigcup_{m\in\mathbb{N}} \otimes^m_{-m} c\mathbb{M}_K c^*.$$

Also $\bigcup_{m\in\mathbb{Z}} \otimes_{-m}^{m} \mathrm{Ad}(cc^*)$ is completely positive, unit preserving and therefore bounded due to lemma 2.4 in chapter 2. Thus it has a continuous extension $A : \mathcal{M}_N \to \mathcal{M}_c$. Its adjoint mapping A^* maps states $\varphi \in \mathcal{S}(\mathcal{M}_c)$ to states $A^*(\varphi) \in \mathcal{S}(\mathcal{M}_N)$ and we have to show that $A^*(\varphi) = A^*(\varphi) \circ \mathrm{Ad}(F_j)$ for all $j \in \mathbb{Z}$. Let $x \in \otimes_{i=-m}^{m} \mathbb{M}_N$. Then

$$A^*(\varphi)(x) = \varphi \circ A(x) = \varphi \circ \Big(\otimes_{i=-m}^{m} \mathrm{Ad}(cc^*)\Big)(x).$$

But as $\otimes_{j=-m}^{m} \mathrm{Ad}(cc^*) = \prod_{j=-m}^{m} \mathrm{Ad}(F_j)$, $\otimes_{-m}^{m} \mathrm{Ad}(cc^*) = \otimes_{-m}^{m} \mathrm{Ad}(cc^*) \circ \mathrm{Ad}(F_j)$ for all $-m \le j \le m$, and we obtain $A^*(\varphi)(x) = A^*(\varphi) \circ \mathrm{Ad}(F_j)(x)$ for all $-m \le j \le m$. As this holds for all $m \in \mathbb{N}$, $A^*(\varphi) = A^*(\varphi) \circ \mathrm{Ad}(F_j)$ on $\bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m} \mathbb{M}_N$ and hence on all of $\mathcal{M}_N$ for all $j \in \mathbb{Z}$.

For the converse direction, let $\varphi \in \mathcal{S}_{[K,N]}^{1^{(n-k)\mathbb{Z}}}$. Thus $\varphi \in \mathcal{S}(\mathcal{M}_N)$ with $\varphi = \varphi \circ \mathrm{Ad}(F_j)$ for all $j \in \mathbb{Z}$. Put $\varphi_m := \varphi|_{\otimes_{-m}^{m} \mathbb{M}_N}$. Then φ_m is a state on $\otimes_{-m}^{m} \mathbb{M}_N$ and $\varphi_{m+1}(\mathbb{1}_N \otimes x \otimes_m \mathbb{1}_N) = \varphi_m(x)$ via the identification of $\otimes_{-m}^{m} \mathbb{M}_N$ with the subalgebra $\cdots \mathbb{1}_N \otimes \Big(\otimes_{-m}^{m} \mathbb{M}_N\Big) \otimes \mathbb{1}_N \cdots \subseteq \mathcal{M}_N$. Hence

$$\bigcup_{m\in\mathbb{N}} \varphi_m : \bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m} \mathbb{M}_N \to \mathbb{C} : \otimes_{-m}^{m} x_i \mapsto \varphi_m(\otimes_{-m}^{m} x_i)$$

is a state on $\bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m} \mathbb{M}_N$ and its continuous extension on $\mathcal{M}_N$ is φ. Then

$$\begin{aligned} \varphi_m &= \varphi_m \circ \mathrm{Ad}(F_j) \quad \text{for all } -m \le j \le m \\ &= \varphi_m \circ \underbrace{\prod_{j=-m}^{m} \mathrm{Ad}(F_j)}_{=\otimes_{-m}^{m} \mathrm{Ad}(cc^*)} = \varphi_m|_{\underbrace{\otimes_{-m}^{m} c\mathbb{M}_K c^*}_{\subseteq \otimes_{-m}^{m} \mathbb{M}_N}} \end{aligned}$$

and $\psi_m := \varphi_m|_{\otimes_{-m}^{m} c\mathbb{M}_K c^*}$ is a positive linear functional on $\otimes_{-m}^{m} c\mathbb{M}_K c^*$. ψ_m is a state, since

$$\begin{aligned} \psi_m(\otimes_{-m}^{m} \mathbb{1}_{c\mathbb{M}_K c^*}) &= \varphi_m(\otimes_{-m}^{m} cc^*) = \varphi_m\Big((\otimes_{-m}^{m} cc^*)(\otimes_{-m}^{m} \mathbb{1}_N)(\otimes_{-m}^{m} cc^*)\Big) \\ &= \varphi_m \circ \otimes_{-m}^{m} \mathrm{Ad}(cc^*)(\otimes_{-m}^{m} \mathbb{1}_N) = \varphi_m(\otimes_{-m}^{m} \mathbb{1}_N) = 1. \end{aligned}$$

As further for all $y \in \otimes_{-m}^{m} c\mathbb{M}_K c^*$

$$\begin{aligned} \psi_{m+1}(\mathbb{1}_{c\mathbb{M}_K c^*} \otimes y \otimes \mathbb{1}_{c\mathbb{M}_K c^*}) &= \varphi_{m+1}(cc^* \otimes \Big(\otimes_{-m}^{m} \mathrm{Ad}(cc^*)(y)\Big) \otimes cc^*) \\ &= \varphi_{m+1} \circ \Big(\otimes_{-m}^{m} \mathrm{Ad}(cc^*)\Big)(\mathbb{1}_N \otimes y \otimes \mathbb{1}_N) \\ &= \varphi_{m+1}(\mathbb{1}_N \otimes y \otimes \mathbb{1}_N) = \varphi_m(y) = \psi_m(y), \end{aligned}$$

we can define

$$\bigcup_{m\in\mathbb{N}} \psi_m : \bigcup_{m\in\mathbb{N}} \otimes_{-m}^{m} c\mathbb{M}_K c^* \to \mathbb{C} : \otimes_{-m}^{m} y_i \mapsto \psi_m(\otimes_{-m}^{m} y_i).$$

$\bigcup_{m\in\mathbb{N}} \psi_m$ is bounded and has a continuous extension $\psi \in \mathcal{S}(\mathcal{M}_c)$. Now we still have to show that $A^*(\psi) = \varphi$. But this holds, as A is continuous and therefore

$$A^*(\psi) = A^*(\lim_m \psi_m) = (\lim_m \psi_m) \circ A = \lim_m (\psi_m \circ A) = \lim_m \varphi_m,$$

since for all $x_i = cy_i c^* \in c\mathbb{M}_K c^*$ with $y_i \in \mathbb{M}_K$

$$\begin{aligned} \psi_m \circ A(\otimes_{-m}^{m} x_i) &= \psi_m(\otimes_{-m}^{m} Ad(cc^*)x_i) = \psi_m(\otimes_{-m}^{m} cc^* x_i cc^*) \\ &= \psi_m(\otimes_{-m}^{m} c(c^*c)y_i(c^*c)c^*) = \psi_m(\otimes_{-m}^{m} cy_i c^*) = \varphi_m(\otimes_{-m}^{m} x_i). \end{aligned}$$

□

Hence we can interpret infinite blocks of stabilizer embeddings as mappings that hide a given state space in a larger one. This is realized by mapping the state space $\mathcal{S}(\mathcal{M}_c)$ to states in $\mathcal{S}(\mathcal{M}_N)$, which are invariant under all projections $F_j = \cdots \otimes \mathbb{1}_N \otimes \underbrace{cc^*}_{j} \otimes \mathbb{1}_N \otimes \cdots$ for $j \in \mathbb{Z}$.

2. Infinite Ollivier-Tillich-Embeddings

When we looked for examples for quantum coders, we considered in the previous section m-blocks of stabilizer embeddings for m tending to infinity. But we also have another option coming from Ollivier-Tillich-embeddings, which we defined in chapter 3, section 9. In this section we consider such embeddings C_t and let t tend to infinity.

We recall that Ollivier-Tillich-embeddings C_t are defined by surjective mappings

$$\mathrm{Ad}(c_t) : \mathbb{M}_{N_t} \to \mathbb{M}_{K_t}$$

with $N_t = 2^{n_t}$, $n_t = m + (2t+1)n$ and $K_t = 2^{k_t}$, $k_t = m + (2t+1)(k-m)$. Looking at

$$\mathrm{Ad}(c_t^*) : \mathbb{M}_{K_t} \to \mathbb{M}_{N_t},$$

we see that $\mathrm{Ad}(c_t^*)$ is injective, as $c_t y c_t^* = 0$ if and only if $c_t^* c_t y c_t^* c_t = y = 0$. As $\mathrm{Ad}(c_t)\mathrm{Ad}(c_t^*)x = c_t^* c_t x c_t^* c_t = x$, we see that $\mathrm{Ad}(c_t)$ is injective on the image of $\mathrm{Ad}(c_t^*)$. So let us fix

$$\mathcal{A}_t := \mathrm{Ad}(c_t^*)(\mathbb{M}_{K_t}) = c_t \mathbb{M}_{K_t} c_t^* \subseteq \mathbb{M}_{N_t}.$$

Obviously $\mathcal{A}_t$ is a *-algebra, as $(c_t x_1 c_t^*)(c_t x_2 c_t^*) = c_t x_1 x_2 c_t^*$ and $\mathrm{Ad}(c_t^*)$ is a *-isomorphism. As $\mathrm{Ad}(c_t^*)$ is injective, $\mathcal{A}_t$ is isomorphic to $\mathbb{M}_{K_t}$, and $\mathrm{Ad}(c_t)$, respectively $\mathrm{Ad}(c_t^*)$, are the according bijections inverse to each other,

$$\mathrm{Ad}(c_t^*) : \mathbb{M}_{K_t} \to \mathcal{A}_t \text{ and } \mathrm{Ad}(c_t) : \mathcal{A}_t \to \mathbb{M}_{K_t}.$$

We have the inductive system $(\mathbb{M}_{K_t}, j_t)$ with embeddings

$$j_t : \mathbb{M}_{K_t} \to \mathbb{M}_{K_{t+1}} = \mathbb{M}_{2^{k-m}} \otimes \mathbb{M}_{K_t} \otimes \mathbb{M}_{2^{k-m}} : \; x \mapsto \mathbb{1}_{2^{k-m}} \otimes x \otimes \mathbb{1}_{2^{k-m}}$$

and limit

$$\varinjlim_{t \in \mathbb{N}} \mathbb{M}_{K_t} = (\otimes_{t=-\infty}^{-1} \mathbb{M}_{2^{k-m}}) \otimes \mathbb{M}_{2^m} \otimes (\otimes_{t=0}^{\infty} \mathbb{M}_{2^{k-m}})$$

isomorphic to $\mathbb{M}_{2^m} \otimes (\otimes_{\mathbb{Z}} \mathbb{M}_{2^{k-m}})$. Now we will see that $\mathcal{A}_t \subseteq \mathcal{A}_{t+1}$. To do this, we define embeddings

$$i_t : \mathcal{A}_t \to \mathcal{A}_{t+1} : \; x \mapsto \mathrm{Ad}(c_{t+1}^*)\Big(\underbrace{\mathbb{1}_{2^{k-m}} \otimes \mathrm{Ad}(c_t)(x) \otimes \mathbb{1}_{2^{k-m}}}_{j_t(\mathrm{Ad}(c_t)(x))} \Big)$$

via the following commuting diagramm.

$$\begin{array}{ccc} \mathcal{A}_t & \xrightarrow{\mathrm{Ad}(c_t)} & \mathbb{M}_{K_t} \\ {\scriptstyle i_t}\downarrow & & \downarrow{\scriptstyle j_t} \\ \mathcal{A}_{t+1} & \xrightarrow{\mathrm{Ad}(c_{t+1})} & \mathbb{M}_{K_{t+1}} \end{array}$$

Hence we can define the C*-inductive limit $\lim_{t\in\mathbb{N}} \mathcal{A}_t$ of the system $(\mathcal{A}_t, i_t)$. But as

$$\begin{aligned}\mathrm{Ad}(c_{t+1})\Big(i_t(x)\Big) &= c_{t+1}^* c_{t+1}\Big(\mathbb{1}_{2^{k-m}} \otimes \mathrm{Ad}(c_t)(x) \otimes \mathbb{1}_{2^{k-m}}\Big) c_{t+1}^* c_{t+1} \\ &= \mathbb{1}_{2^{k-m}} \otimes \mathrm{Ad}(c_t)(x) \otimes \mathbb{1}_{2^{k-m}} = j_t(\mathrm{Ad}(c_t)(x)),\end{aligned}$$

we can lift $\mathrm{Ad}(c_t)$ to

$$(\Gamma_{\mathrm{OT}})_* : \bigcup_{t\in\mathbb{N}} \mathcal{A}_t \to \bigcup_{t\in\mathbb{N}} \mathbb{M}_{K_t} : \ \mathcal{A}_t \ni x \mapsto \mathrm{Ad}(c_t)(x).$$

As $\|\mathrm{Ad}(c_t)\| = 1$ for all $t \in \mathbb{N}$, $(\Gamma_{\mathrm{OT}})_*$ has a continuous extension onto the inductive limits, that we denote by the same symbol,

$$(\Gamma_{\mathrm{OT}})_* : \varinjlim_{t\in\mathbb{N}} \mathcal{A}_t \to \varinjlim_{t\in\mathbb{N}} \mathbb{M}_{K_t}.$$

$(\Gamma_{\mathrm{OT}})_*$ is a bijective *-isomorphism between the AF-algebras $\varinjlim_t \mathcal{A}_t$ and $\varinjlim_t \mathbb{M}_{K_t}$. Note that $\varinjlim_t \mathcal{A}_t \not\subseteq \varinjlim_t \mathbb{M}_{N_t}$. If we define its adjoint operator

$$\Gamma_{\mathrm{OT}} : \mathcal{S}(\varinjlim_{t\in\mathbb{N}} \mathbb{M}_{K_t}) \to \mathcal{S}(\varinjlim_{t\in\mathbb{N}} \mathcal{A}_t) : \ \varphi \mapsto \varphi \circ (\Gamma_{\mathrm{OT}})_*,$$

also Γ_{OT} is bijective.

2.1. Definition. Let $\Gamma_{\mathrm{OT}} : \mathcal{S}(\varinjlim_t \mathbb{M}_{K_t}) \to \mathcal{S}(\varinjlim_t \mathcal{A}_t)$ be as defined above. Then we call Γ_{OT} an *infinite OT-embedding*.

As $\varinjlim_t \mathbb{M}_{K_t}$ is isomorphic to $\mathbb{M}_{2^m} \otimes (\otimes_{\mathbb{Z}} \mathbb{M}_{2^{k-m}})$, we may define a map

$$S_R := \mathrm{id}_{2^m} \otimes S_{R,2^{k-m}}$$

acting as a the tensor right shift $S_{R,2^{k-m}}$ on $\otimes_{\mathbb{Z}} \mathbb{M}_{2^{k-m}}$, leaving $\mathbb{M}_{2^m}$ invariant,

$$S_R = \begin{matrix}\mathrm{id}_{2^m} \\ \otimes \\ S_{R,2^{k-m}}\end{matrix} \quad \text{on} \quad \begin{matrix}\mathbb{M}_{2^m} \\ \otimes \\ \cdots \mathbb{M}_{2^{k-m}} \otimes \mathbb{M}_{2^{k-m}} \otimes \quad \mathbb{M}_{2^{k-m}} \quad \otimes \mathbb{M}_{2^{k-m}} \otimes \mathbb{M}_{2^{k-m}} \cdots\end{matrix}$$

We can pull back this map on $\varinjlim_t \mathcal{A}_t$ via the *-isomorphism $(\Gamma_{\mathrm{OT}})_*$,

$$\tilde{S}_R(a) := \Big((\Gamma_{\mathrm{OT}})_*\Big)^{-1} S_R\Big((\Gamma_{\mathrm{OT}})_*(a)\Big)$$

for $a \in \varinjlim_t \mathcal{A}_t$. By construction $\tilde{S}_R$ is conjugate to the shift S_R via the conjugation $(\Gamma_{\mathrm{OT}})_*$, i.e.

$$(\Gamma_{\mathrm{OT}})_* \circ \tilde{S}_R = S_R \circ (\Gamma_{\mathrm{OT}})_*.$$

Note that $\tilde{S}_R$ is an abstract shift and that neither S_R nor $\tilde{S}_R$ have a connection with the shifts mentioned in chapter 3, section 9.2.

However, $(\Gamma_{\mathrm{OT}})_*$ is a q-coder. Hence we get the same result for OT-embeddings as remark 6.6 in chapter 4 for infinite blocks of stabilizer embeddings. More precisely, we have for an infinite OT-embedding Γ_{OT} and for the adjoint maps S_R^* on $\mathcal{S}(\varinjlim_t \mathbb{M}_{K_t})$ and $\tilde{S}_R^*$ on $\mathcal{S}(\varinjlim_t \mathcal{A}_t)$

$$\Gamma_{\mathrm{OT}} \circ S_R^* = \Big(S_R \circ (\Gamma_{\mathrm{OT}})_*\Big)^* = \Big((\Gamma_{\mathrm{OT}})_* \circ \tilde{S}_R\Big)^* = \tilde{S}_R^* \circ \Gamma_{\mathrm{OT}}$$

with the above considerations.

Of course, we would like to generalize the interpretation for infinite blocks of stabilizer embeddings in section1, theorem 1.5. But there is no hope for that, as in general cases, c_t and c_{t+1} do not have to be connected. This makes it impossible to establish a connection between $\mathcal{S}(\varinjlim_t \mathcal{A}_t)$ and $\mathcal{S}(\varinjlim_t \mathbb{M}_{N_t})$.

However, we obtained an example of a q-coder, which is not just a q-1-block coder. But the price we had to pay is an abstract shift together with the loss of an important interpretation.

3. Discussion

As we saw in chapter 3, section 4, a stabilizer algebra $\mathcal{A}_S$ given by its $(n-k)$ commuting and independent generators is isorphic to $L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$, where $\mathcal{B}_{n-k}$ denotes the σ-algebra generated by the first $(n-k)$ Rademacher functions.

The projections $E_y^i \in \mathcal{A}_S$ for $y \in \{1,-1\}$ and $i \in \mathbb{N}_{n-k}$ correspond to the characteristic functions $e_y^i \in L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$. They generate $\mathcal{A}_S$ respectively $L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$, are independent for $i \neq j$ and have the same "measure": $\mathrm{tr}(E_y^i) = \frac{1}{2} = \int_{[0,1)} e_y^i \mathrm{d}\lambda$. If we define for $(y_i)_i \in \{1,-1\}^{n-k}$

$$e_{(y_i)_i} := \prod_{i=1}^{n-k} e_{y_i}^i,$$

$\{E_{(y_i)_i} : (y_i)_i \in \{1,-1\}^{n-k}\}$ as well as $\{e_{(y_i)_i} : (y_i)_i \in \{1,-1\}^{n-k}\}$ are generating sets of their algebras and pairwise independent.

By setting $A_{(y_i)_i} := \{x \in [0,1) : e_{(y_i)_i}(x) = 1\}$, we obtain classically independent events $A_{(y_i)_i} \in \mathcal{B}_{n-k}$ for $(y_i)_i \in \{1,-1\}^{n-k}$.

This notion of classical independence is the same as we have in classical Bernoulli shifts. This comes from the fact that $([0,1), \mathcal{B}, \lambda)$ equipped with the transformation R is isomorphic to the Bernoulli shift

$$\Upsilon := \prod_{\mathbb{N}} (\{0,1\}, \mathcal{P}(\{0,1\}), \mu)$$

given by $\{0,1\}$ and the measure $\mu = (\frac{1}{2}, \frac{1}{2})$, equipped with the right shift on the binary decomposition.

Hence, by regarding $(\mathcal{A}_S, \mathrm{tr})$ as a quantum probability space, we have implemented the classical probability space $L^\infty([0,1), \mathcal{B}_{n-k}, \lambda)$ into an algebraical and therefore into quantum mechanical setting. In this setting, the classically independent events $(A_{(y_i)_i})_{(y_i)_i}$ correspond to something like "independent Hilbert spaces" $E_{(y_i)_i}\mathbb{C}^{2^k}$. This is reflected in the considerations of the next chapter, where we will discuss to what extent these codes really make use of the quantum setting.

The advantage of this method of choosing q-1-block maps into such an independent Hilbert space is error correction. As quantum states change rapidly, error correction is an important

feature of data transmission. We will not go deeper into this matter but refer to the detailed description in [NC00].

This leads to the question, whether there are quantum codes, where we use more quantum features in choosing subalgebras or subspaces, but where we are still able to give a good error correction theory. We would also like to preserve the interpretation of a coder as mapping that hides a given state space in a larger one.

CHAPTER 6

On the Realization of Quantum Algorithms

In this section we study the realization of quantum algorithms.

As we may deduce from chapter 4, section 3, such realizations include measurements. Therefore, we give a brief definition of a measurement operator in the first section. The next section describes the modified scheme of a quantum algorithm we use in this work as mentioned in chapter 4, section 3. Here, we also discuss the connection between the scheme of a quantum algorithm and measurement operators and introduce special quantum gates, i.e. certain operations permitted in both schemes. The second section shows that measurement operators belonging to quantum algorithms constructed in a certain way are almost classical. We will call this notion essentially commutative. Examples for such measurement operators are the realizations of stabilizer embeddings and the important phase-estimation algorithm developed by Shor. The last section finally discusses the measurement operator of the well known Grover algorithm.

1. Measurements

A quantum mechanical system, or shorter a *quantum system*, is given by a quantum probability space, i.e. a *-algebra $\mathcal{A}$ equipped with a state φ. If we perform a measurement on the quantum system $(\mathcal{A}, \varphi)$, the system will be changed. In the *Schrödinger picture*, this change is expressed by a change of the state whereas the algebra remains unchanged. The *Heisenberg picture* is a dual but equivalent description, where the algebra gets transformed but the state remains the same. The purpose of a measurement is to find out more information about φ. Let (C, ψ) be a second quantum system describing the measurement apparatus and $\mathcal{A}$ and C be unital. Due to Kraus [**Kra71**], a measurement in the Schrödinger picture consists of the following steps. A detailed introduction can be found in [**SF06**].

- (α) We couple the systems $(\mathcal{A}, \varphi)$ and (C, ψ) and obtain the system $(\mathcal{A} \otimes C, \varphi \otimes \psi)$.
- (β) The coupled systems evolves with time. This time evolution is given by an automorphism $\alpha : (\mathcal{A} \otimes C, \varphi \otimes \psi) \to (\mathcal{A} \otimes C, (\varphi \otimes \psi) \circ \alpha)$.
- (γ) We measure an observable $\sum_{i \in I} \lambda_i p_i \in C$ with countably many outcomes λ_i and according spectral projetions p_i, $i \in I$. Measuring λ_i leads to a new quantum system $(\mathcal{A} \otimes C, \varphi_i)$ with $\varphi_i = (\varphi \otimes \psi) \circ \alpha \circ \mathrm{Ad}(\mathbb{1}_{\mathcal{A}} \otimes p_i)$.
- (δ) We learn something about φ by restricting φ_i to $\varphi_i|_{\mathcal{A}}$.

In the dual Heisenberg picture, we obtain an equivalent description leaving the states invariant but working on the algebras.

(δ') We map $x \in \mathcal{A}$ to $x \otimes \mathbb{1}_C \in \mathcal{A} \otimes C$.
(γ') The measurement with outcome λ_i reduces $x \otimes \mathbb{1}_C$ to $x \otimes p_i$.
(β') The system evolves with time, $x \otimes p_i \mapsto \alpha(x \otimes p_i)$
(α') We separate the systems by applying a *conditional expectation*

$$P_\psi : x \otimes y \mapsto \psi(y)x$$

and obtain $P_\psi(\alpha(x \otimes p_i))$.

Considering all possible outcomes $i \in I$ in a countable set I leads to the definition of a *measurement*

$$T : \mathcal{A} \to \mathcal{A} : x \mapsto \sum_{i \in I} P_\psi(\alpha(x \otimes p_i)) =: \sum_{i \in I} T_i x.$$

The following case is called a *perfect measurement* and is presented in more details in [**SF06**]. Let $\mathcal{A} = \mathbb{M}_n$, $C = \mathbb{M}_m$, $\mathcal{A} \otimes C = \mathbb{M}_m(\mathbb{M}_n)$, $\psi = (\psi_1, \dots, \psi_m)^T \in \mathbb{C}^m$ be a pure state and p_i a one-dimensional projection onto $\mathrm{lin}(\xi_i)$ with $\xi_i = (\xi_1^i, \dots, \xi_m^i)^T \in \mathbb{C}^m$ for all $i \in I$, i.e. $p_i = (\xi_i \bar{\xi}_j)_{ij}$. As α is an automorphism, it is of the form $\alpha = \mathrm{Ad}(u)$ for a unitary $u = (u_{ij})_{ij} \in \mathbb{M}_m(\mathbb{M}_n)$. Then we can calculate the explicit form of T_i as in [**Ste01**],

$$\begin{aligned}
T_i x &= P_\psi\Big(u^*(x \otimes p_i)u\Big) = P_\psi\Big((u^*_{gh})_{hg}(\xi^i_g \bar{\xi}^i_j x)_{gj}(u_{jk})_{jk}\Big) \\
&= P_\psi\Big((\sum_{g,j=1}^m u^*_{gh}\xi^i_g x \bar{\xi}^i_j u_{jk})_{hk}\Big) = P_\psi\Big(\big((\sum_{g=1}^m \bar{\xi}^i_g u_{gh})^* x (\sum_{g=1}^m \bar{\xi}^i_g u_{gk})\big)_{hk}\Big) \\
&= \Big\langle (\psi_h)_h \,, \Big(\sum_{k=1}^m (\sum_{g=1}^m \bar{\xi}^i_g u_{gh})^* x (\sum_{g=1}^m \bar{\xi}^i_g u_{gk})\psi_k \Big)_h \Big\rangle \\
&= \sum_{h=1}^m \bar{\psi}_h \Big((\sum_{g=1}^m \bar{\xi}^i_g u_{gh})^* x (\sum_{g,k=1}^m \bar{\xi}^i_g u_{gk}\psi_k) \Big) \\
&= \Big((\sum_{g,h=1}^m \bar{\xi}^i_g u_{gh}\psi_h)^* x (\sum_{g,k=1}^m \bar{\xi}^i_g u_{gk}\psi_k) \Big) \\
&= a_i^* x a_i \text{ with } a_i = \xi_i^* u \psi.
\end{aligned}$$

T_i and T are completely positive. T additionally preserves the identity and hence is a quantum operation. We call T in the following the *measurement operator* or just the *measurement*.

Due to chapter 2, section 2, the unravelling $(a_i)_i$ of a completely positive map T is usually not unique. But we saw that if the matrices $a_1, \dots, a_m$ are linearly independent, they are determined up to isometric transformations.

A quantum operation T is called *essentially commutative*, if it has an unravelling $Tx = \sum_{i=1}^m \lambda_i v_i^* x v_i$ for unitary matrices $v_i \in \mathbb{M}_n$ and a probability measure $\lambda = (\lambda_1, \dots, \lambda_m)$. In other words, T is essentially commutative, if it is an element of the convex hull of automorphisms. In this case, the iterated quantum operation T^n, $n \in \mathbb{N}$, can be obtained from a coupling to a classical Bernoulli shift. It thus has an interpretation as a time evolution due to a external stochastic classical field, but for these details see [**KM87**].

Kümmerer proved a theorem with which makes it easy to check, whether a completely positive map $T : \mathbb{M}_2 \to \mathbb{M}_2$ is essentially commutative. It can be found in [Küm85a].

1.1. Theorem. *let $T : \mathbb{M}_2 \to \mathbb{M}_2$ be a completely positive map. Then T is essentially commutative if and only if $tr(x) = tr(T(x))$ for all $x \in \mathbb{M}_2$.*

2. Realization of Quantum Algorithms

In chapter 4 we generalized the common scheme of quantum algorithms using only pure states and automorphisms given by unitary transformations as described in chapter 4, section 3 to a more general one. This more general scheme allows mixed states as well as arbitrary quantum operations and was described in the same chapter in section 7. Note that the new scheme and the common scheme fit into the context of quantum measurements as described in the previous section, if we take the automorphism respectively the quantum operation for the time evolution.

Existing quantum algorithms including stabilizer embeddings make use only of the common scheme. In fact, they are implemented in the following way.

- All quantum systems are finite-dimensional.
- φ_0 is a tensor product state of a pure state in the system of interest as well as in the system of the measurement apparatus.
- The time evolution is given by an automorphism $\mathrm{Ad}(u)$ for a unitary operator u on the Hilbert space of the coupled system. These unitary operators u are generated by a set of so called quantum gates.
- The measurements we perform on the system of the measurement apparatus have one-dimensional spectral projections.

Note that this corresponds exactly to the definition of a perfect measurement.

Now we define the most common quantum gates. A *quantum gate* is a quantum operation $\mathrm{Ad}(u)$ for a unitary element u of a finite-dimensional *-algebra. We list the most important ones in the following. For more details we refer to [NC00].

The *Pauli quantum gates* are quantum gates on the algebra $\mathbb{M}_2$ belonging to the set of q-bits and given by the Pauli matrices,

$$\mathrm{Ad}(\sigma_i) : \mathbb{M}_2 \to \mathbb{M}_2,\ i \in \{x, y, z\}.$$

Other important gates on the algebra belonging to the set of q-bits are the *Hadamard gate* $\mathrm{Ad}(H)$, the *phase gate* $\mathrm{Ad}(S)$ and the $\pi/8$-*gate* $\mathrm{Ad}(T)$ for

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}.$$

Another important quantum gate is the *controlled NOT* gate,

$$\mathrm{Ad(CNOT)} : \mathbb{M}_2 \otimes \mathbb{M}_2 \to \mathbb{M}_2 \otimes \mathbb{M}_2 \text{ for CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

The interpretation is that Ad(CNOT) performs a σ_x-gate on the algebra of the first qubit provided that the second q-bit is given by the vector state $(0,1)^T$.

We can define in a similar way controlled operations for any unitary matrix $U \in \mathbb{M}_d$,

$$\mathrm{Ad(CU)} : \mathbb{M}_d \otimes \mathbb{M}_2 = \mathbb{M}_2(\mathbb{M}_d) \to \mathbb{M}_d \otimes \mathbb{M}_2 \text{ for U} = \begin{pmatrix} \mathbb{1} & 0 \\ 0 & U \end{pmatrix}.$$

Ad(CU) performs the quantum gate Ad(U) on the algebra belonging to the q-dit provided that the qubit is given by the vector state $(0,1)^T$.

3. Properties of Realizations of Quantum Algorithms

There is an important theorem by Gottesman and Knill.

3.1. THEOREM. *Let $\mathcal{H}$ be a finite dimensional Hilbert space equipped with an othonormal basis. Suppose we perform a quantum algorithm on $\mathcal{H}$ such that*

- *we start with a pure state given by a vector from the othonormal basis,*
- *we use only Hadamard gates, phase gates, CNOT-gates and Pauli gates,*
- *we measure only observables in the Pauli group, and*
- *we may manipulate the quantum system after the measurements depending on the outcomes of the measurements.*

Then such an algorithm can be efficiently simulated by a classical computer.

The possibility to manipulate a system depending on the outcomes of a measurement is usually refered to as *classical control conditioned on the outcome of measurements*.

The proof of the theorem can be found in [**NC00**].

This result mirrors another important property of realizations of quantum algorithms.

3.2. THEOREM. *Let $(\mathcal{A}, \varphi)$ be a quantum system consisting of a finite-dimensional *-algebra $\mathcal{A}$ and a pure state φ. Let $(\mathbb{M}_{2^m}, \psi)$ be a second quantum system with the pure state ψ given by $(1,0,\ldots,0)^T \in \mathbb{C}^{2^m}$, and let $(p_i)_{i=1}^{2^m}$ be projections onto the canonical basis of $\mathbb{C}^{2^m}$. Further identify $\mathbb{M}_{2^m}$ with $\otimes^m \mathbb{M}_2$.*

If

$$U = (\mathbb{1}_{\mathcal{A}} \otimes A) \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_{2^m} \end{pmatrix} (\mathbb{1}_{\mathcal{A}} \otimes \left(\otimes^m H \right)) \in \mathcal{A} \otimes \mathbb{M}_{2^m}$$

with unitary matrices $A \in \mathbb{M}_{2^m}, B_i \in \mathcal{A}$ and the Hadamard-matrix H, then the measurement operator T with

$$Tx = \sum_{i=1}^{2^m} P_\psi(Ad(U)(x \otimes p_i))$$

is essentially commutative.

Proof. Let $(f_i)_{i=1}^{2^m}$ denote the canonical basis of $\mathbb{C}^{2^m}$ and $U = (u_{ij})_{ij}$. We know that $Tx = \sum_{i=1}^{2^m} a_i^* x a_i$ for $a_i = f_i^T U f_1 = f_i^T (u_{11}, \ldots, u_{2^m 1})^T = u_{i1}$. Let further $*$ stand for matrix entries that are not interesting to us. Then we calculate

$$\otimes^m H = \frac{1}{\sqrt{2^m}} \begin{pmatrix} 1 & \\ \vdots & * \\ 1 & \end{pmatrix}, \text{ respectively } \mathbb{1}_{\mathcal{A}} \otimes \left(\otimes^m H \right) = \frac{1}{\sqrt{2^m}} \begin{pmatrix} \mathbb{1} & \\ \vdots & * \\ \mathbb{1} & \end{pmatrix}.$$

If we further denote $A = (a_{ij})_{ij}$, we obtain $\mathbb{1}_{\mathcal{A}} \otimes A = (a_{ij} \mathbb{1}_{\mathcal{A}})_{ij}$ and finally

$$\begin{aligned} U &= (\mathbb{1}_{\mathcal{A}} \otimes A) \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_{2^m} \end{pmatrix} (\mathbb{1}_{\mathcal{A}} \otimes \left(\otimes^m H \right)) \\ &= (a_{ij} \mathbb{1}_{\mathcal{A}})_{ij} \frac{1}{\sqrt{2^m}} \begin{pmatrix} B_1 & \\ \vdots & * \\ B_{2^m} & \end{pmatrix} = \frac{1}{\sqrt{2^m}} \begin{pmatrix} \sum_{j=1}^{2^m} a_{1j} B_j & \\ \vdots & * \\ \sum_{j=1}^{2^m} a_{2^m j} B_j & \end{pmatrix}. \end{aligned}$$

Therefore, $a_i = u_{i1} = \frac{1}{\sqrt{2^m}} \sum_{j=1}^{2^m} a_{ij} B_j$. As A is unitary,

$$Tx = \sum_{i=1}^{2^m} a_i^* x a_i = \sum_{i=1}^{2^m} \frac{1}{2^m} B_i^* x B_i.$$

by theorem 2.3 in chapter 2. Then the assertion follows due to the definition at the end of section 1, since all B_i, $i \in \mathbb{N}_{2^m}$, are unitary. □

3.3. Remark. The quantum algorithms for the phase-estimation algorithm and thus for the quantum algorithms of order-finding and factoring are exactly of this form. Hence their measurement operators are essentially commutative.

The coding scheme for a stabilizer embedding is also of this form and hence the according measurement operator is essentially commutative as well.

For details of these quantum algorithms we refer to [**NC00**] and [**Got97**].

4. Measurement Operator of the Grover Algorithm

The Grover algorithm is one of the most important quantum algorithms. It solves the problem of finding an element satisfying a certain property in a search space of size 2^n, $n \in \mathbb{N}$. For simplicity we consider the case that only one element has this property. We are not going

into the details of how the Grover algorithm works but consider just its realization in order to calculate the corresponding measurement operator.

Let $(\mathbb{M}_2, \varphi)$ be the quantum system given by the pure vector state $(1,0)^T \in \mathbb{C}^2$. Let $(\mathbb{M}_{2^n}, \psi)$ be a second quantum system with the pure vector state $\psi = (1,0,\ldots,0)^T \in \mathbb{C}^{2^n}$, and let $(p_i)_{i=1}^{2^n}$ be projections onto the canonical basis of $\mathbb{C}^{2^n}$.

Then according to [NC00] and via identification of $\mathbb{M}_{2^n}$ with $\otimes^n \mathbb{M}_2$, the Grover algorithm for m iterations, $m \in \mathbb{N}$, is given by

$$U_m = ((\mathbb{1}_{\mathbb{M}_2} \otimes A)O)^m (\mathbb{1}_{\mathbb{M}_2} \otimes (\otimes^n H)) \in \mathbb{M}_2 \otimes \mathbb{M}_{2^n}$$

for fixed unitary matrices $A \in \mathbb{M}_{2^n}$ and $O \in \mathbb{M}_2 \otimes \mathbb{M}_{2^n}$ and the Hadamard-matrix H. O is the most interesting matrix of this algorithm as it describes the socalled *oracle gate* $\mathrm{Ad}(O)$.

The oracle gate works as follows. Let $x_0 \in \mathbb{N}_{2^n}$ be the solution of the search problem. The O is given by

$$O = \sigma_x \otimes p_{x_0} + \sum_{x \in \mathbb{N}_{2^m}, x \neq x_0} \mathbb{1}_{\mathbb{M}_2} \otimes p_x.$$

Obviously, O ís of the form

$$O = \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_{2^n} \end{pmatrix}$$

with $B_{x_0} = \sigma_x$ and $B_x = \mathbb{1}$ for $x \in \mathbb{N}_{2^n}, x \neq x_0$.

For $m = 1$, the measurement is essentially commutative by lemma 3.2.

Now we calculate also the measurement operator T in the case $m = 2$ with

$$Tx = \sum_{i=1}^{2^n} P_\psi \mathrm{Ad}(U_2)(x \otimes p_i)).$$

We have shown in section 1 that in this case $Tx = \sum_{i=1}^{2^n} a_i^* x a_i$ with $a_i = f_i^T U_2 f_1 = u_{i1}^2$ for

$$U_2 = (\mathbb{1}_{\mathbb{M}_2} \otimes A)O(\mathbb{1}_{\mathbb{M}_2} \otimes A)O(\mathbb{1}_{\mathbb{M}_2} \otimes (\otimes^n H)) =: (u_{ij}^2)_{ij} \in \mathbb{M}_{2^n}(\mathbb{M}_2).$$

Setting $\mathbb{1}_{\mathbb{M}_2} \otimes A = (a_{ij}\mathbb{1}_{\mathbb{M}_2})_{ij}$, we obtain $(\mathbb{1}_{\mathbb{M}_2} \otimes A)O = (a_{ij}B_j)_{ij}$ and hence

$$\Big((\mathbb{1}_{\mathbb{M}_2} \otimes A)O\Big)^2 = (\sum_{k=1}^{2^m} a_{ik}a_{kj}B_kB_j)_{ij}.$$

If we further denote $\mathbb{1}_{\mathbb{M}_2} \otimes (\otimes^n H) = (h_{ij}\mathbb{1}_{\mathbb{M}_2})_{ij}$ and recall that $h_{i1} = 1$ for all $i \in \mathbb{N}_{2^n}$, we get

$$U_2 = \left(\sum_{k=1}^{2^n} a_{ik}a_{kj}B_kB_j\right)_{ij} (h_{ij}\mathbb{1}_{\mathbb{M}_2})_{ij} = \begin{pmatrix} \sum_{k,j=1}^{2^n} a_{1k}a_{kj}B_kB_j & & \\ \vdots & & * \\ \sum_{k,j=1}^{2^n} a_{2^nk}a_{kj}B_kB_j & & \end{pmatrix}.$$

As $B_j \in \{\mathbb{1}_{\mathbb{M}_2}, \sigma_x\}$ for $j \in \mathbb{N}_{2^n}$, we also have $B_kB_j \in \{\mathbb{1}_{\mathbb{M}_2}, \sigma_x\}$ and hence $a_i = u_{i1}^2 \in \mathrm{lin}\{\mathbb{1}_{\mathbb{M}_2}, \sigma_x\}$.

In fact,

$$\begin{aligned} a_i &= \sum_{k,j=1}^{2^n} a_{ik} a_{kj} B_k B_j \\ &= \underbrace{\Big(a_{ix_0} a_{x_0 x_0} + \sum_{k,j \neq x_0} a_{ik} a_{kj} \Big)}_{=:\alpha_i} \cdot \mathbb{1} + \underbrace{\Big(\sum_{j \neq x_0} a_{ix_0} a_{x_0 j} + a_{ij} a_{jx_0} \Big)}_{=:\beta_i} \cdot \sigma_x \end{aligned}$$

Due to theorem 1.1, completely positive maps on $\mathbb{M}_2$ are essentially commutative if and only if they preserve the trace tr on $\mathbb{M}_2$. Therefore, we consider $x = (x_{ij})_{ij} \in \mathbb{M}_2$ and calculate $\mathrm{tr}\,(\sum_{i=1}^{2^n} a_i^* x a_i)$. But as $a_i = \alpha_i \mathbb{1} + \beta_i \sigma_x$, we obtain

$$a_i^* x\, a_i = |\alpha_i|^2 x + \bar{\alpha}_i \beta_i\, x\, \sigma_x + \alpha_i \bar{\beta}_i\, \sigma_x \mathbb{1} + |\beta_i|^2\, \sigma_x x\, \sigma_x.$$

Thus

$$\mathrm{tr}\,(a_i^* x\, a_i) = \Big(|\alpha_i|^2 + |\beta_i|^2 \Big) \cdot (x_{11} + x_{22}) + \Big(\bar{\alpha}_i \beta_i + \alpha_i \bar{\beta}_i \Big) \cdot (x_{21} + x_{12})$$

and hence $\mathrm{tr}\,(x) = x_{11} + x_{22} = \mathrm{tr}\,(\sum_{i=1}^{2^n} a_i^* x\, a_i) = \sum_{i=1}^{2^n} \mathrm{tr}\,(a_i^* x\, a_i)$ if and only if

$$\sum_{i=1}^{2^n} \Big(|\alpha_i|^2 + |\beta_i|^2 \Big) = 1 \quad \text{and} \quad \sum_{i=1}^{2^n} \Big(\bar{\alpha}_i \beta_i + \alpha_i \bar{\beta}_i \Big) = 0.$$

According to [NC00], the matrix $A = (a_{ij})_{ij}$ is of the form

$$A = \frac{1}{2^{n-1}} \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - \mathbb{1}_{\mathbb{M}_{2^n}}$$

and hence we have

$$a_{ii} = \frac{1 - 2^{n-1}}{2^{n-1}} \quad \text{and} \quad a_{ij} = \frac{1}{2^{n-1}} \quad \text{for } i \neq j.$$

But then for $n = 1$, we obtain $a_{ii} = 0$ and $a_{ij} = 1$ for $i \neq j$. If we denote the element of the search space that is not x_0 by $\neg x_0$, we get

$$\begin{array}{lcll} \alpha_{x_0} & = & a_{x_0(\neg x_0)} a_{(\neg x_0)(\neg x_0)} + a_{x_0 x_0} a_{x_0 x_0} & = 0, \\ \beta_{x_0} & = & a_{x_0 x_0} a_{x_0(\neg x_0)} + a_{x_0(\neg x_0)} a_{(\neg x_0) x_0} & = 1, \\ \alpha_{\neg x_0} & = & a_{(\neg x_0)(\neg x_0)} a_{(\neg x_0)(\neg x_0)} + a_{(\neg x_0) x_0} a_{x_0 x_0} & = 0 \quad \text{and} \\ \beta_{\neg x_0} & = & a_{(\neg x_0) x_0} a_{x_0(\neg x_0)} + a_{(\neg x_0)(\neg x_0)} a_{(\neg x_0) x_0} & = 1. \end{array}$$

Then obviously

$$|\alpha_{x_0}|^2 + |\beta_{x_0}|^2 + |\alpha_{\neg x_0}|^2 + |\beta_{\neg x_0}|^2 = 2 \neq 1$$

and therefore the measurement operator of the Grover algorithm for $m = 2$ iterations in the case that the search space consists only of two elements, $\sum_{i=1}^{2} a_i^* x a_i$, is not essentially commutative.

5. Discussion

We noticed in this chapter that the Gottesman-Knill theorem finds a correspondence in the fact, that the measurement operators of common schemes of quantum algorithms are essentially commutative. Hence recapitulating this chapter together with the previous one, we note the following. In the discussion of chapter 5 we asked, whether there are new examples of quantum coders, that still have good error correcting features and maybe also the interpretation of hiding a given state space in a larger one. This challenge has become bigger - after the considerations above we ask ourselves whether these examples will have essentially commutative measurement operators.

APPENDIX

Glossary

$\mathcal{A}$	C*-algebra	14
$\mathcal{A}$	algebra of a q-alphabet	46
$\mathcal{A}^{[N]}$	algebra of an Nth higher q-alphabet	46
$\mathcal{A}_S$	stabilizer algebra	27
$\mathcal{A}_{T_m}$	stabilizer algebra of m-block	35
$\mathcal{A}_{T_t}$	stabilizer algebra of OT-embedding	39
$\otimes_{\mathbb{Z}}\mathcal{A}$	q-full shift	47
$\hat{\mathcal{A}}$	spectrum of $\mathcal{A}$	14
$\otimes_{n\in\mathbb{N}}\mathcal{A}_n$	infinite tensor product	17
$(\mathcal{A},\varphi)$	quantum probability space	44
A	alphabet	1
$\mathsf{A}^{[N]}$	allowed words of length N	3
$(\mathsf{A}^{[N]})^{\mathbb{Z}}$	higher block shift	3
$\mathsf{A}^{\mathbb{Z}}$	full shift	1
$\mathcal{B}$	Borel sigma algebra	30
$\mathcal{B}(\mathcal{H})$	bounded linear operators	13
$\mathcal{B}(\mathsf{X})$	language of a shift space X	3
$\mathcal{B}_n(\mathsf{X})$	allowed words of length n	3
$\mathcal{B}_{n-k}$	reduced sigma algebra	31
β_N	higher block coder	3
C	stabilizer embedding	32
C^m	m-block of c resp. C	35
C_t	OT-embedding	39
$\mathbb{C}$	complex numbers	13
c	stabilizer Hilbert space embedding	32
c^m	m-block of c resp. C	35
c_t	OT-Hilbert space embedding	39
$E_{(y_i)_i}$	common spectral projection	28
E_y^i	projection onto $ES_y(g_i)$	28
$\mathbb{E}$	expectation value	31
$e_{(y_i)_i}$	common spectral projections	60
e_y^i	summand of r_i	31
F	convolutional coder	9
F	forbidden words	2

G	group	14
$\hat{G}$	spectrum of G	14
G_n	Pauli group	20
$g(b,c)$	special elements of the Pauli group	21
g_i	generator of a group	26
γ_N	higher power coder	4
Γ_{OT}	infinite OT-embedding	59
Γ_ϕ	q-1-block coder	52
Γ_N	q-higher power coder	50
H	parity check matrix	6
$\mathcal{H}_{1^{n-k}}$	code Hilbert space	32
$\mathcal{H}$	separable Hilbert space	13
$\varinjlim_n (\mathcal{A}_n, \pi_n)$	inductive limit	16
$\varinjlim_m \mathcal{A}_m$	algebra of a q-shift space	48
λ	Lebesgue measure	30
$\mathcal{M}_c$	image algebra of an infinite stabilizer embedding	54
$\mathcal{M}_K$	infinite tensor product	54
$\mathbb{N}$	natural numbers	13
$\mathbb{N}_n$	$\{1,\ldots,n\} \subseteq \mathbb{N}$	13
(Ω, Σ, μ)	probability space	44
ϕ	coder	3
Φ_G	linear block map	6
$\Phi_\infty^{[-m,n]}$	sliding block coder	4
Φ	block map	4
R	transformation on $[0,1)$	30
r_i	Rademacher function	30
S	subgroup and mostly stabilizer group	26
$S_{L,2}$	tensor left shift	38
$S_{R,N}$	tensor right shift	36
S_R	right shift on OT-matrix-AF-algebra	59
$\tilde{S}_R$	right shift on abstract OT-AF-algebra	59
$\mathcal{S}(\varinjlim_m \mathcal{A}_m)$	q-shift space	48
$\mathcal{S}(\overrightarrow{\mathcal{A}^{[N]}})$	Nth higher q-alphabet	46
$\mathcal{S}(\mathcal{A})$	q-alphabet	46
σ	left shift	2
$\sigma_{L,\otimes_{\mathbb{Z}}\mathcal{A}}$	left shift on tensor product states	52
T_m	stabilizer group of m-block	35
T_t	stabilizer group of OT-embedding	38
tr_N	trace on $\mathbb{M}_N$	13
X	shift space	2
$\mathsf{X}^{[N]}$	higher power shift	4
$\mathbb{Z}$	whole numbers	13

Bibliography

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum Circuits with Mixed States. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing (STOC)*. ACM, 1998. viii, xii, 43

[BR87] O. Bratteli and D. W. Robinson. *Operator Algebras and Quantum Statistical Mechanics*, volume I. New York, 1987. 13, 17

[BV92] E. Bernstein and U. Vazirani. Quantum Complexity Theory. In *Proceedings of the 7th IEEE Conference on Structure in Complexity Theory*, pages 132–137, 1992. vii, xi, 43

[Cho75] M.-D. Choi. Completely Positive Linear Maps on Complex Matrices. *Linear Algebra and its Applications*, 10, 1975. 15

[Deu85] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proc. Roy. Soc. Lond*, A400:97–117, 1985. vii, xi, 43

[Die82] D. Dieks. Communication by EPR Devices. *Physics Letters A*, 92(6):271–272, 1982. 50

[Fey82] R. P. Feynman. Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21:467–488, 1982. vii, xi

[GKL06] R. Gohm, B. Kümmerer, and T. Lang. Noncommutative Symbolic Coding. *J. Ergodic Theory and Dynamical Systems*, 26, 2006. vii, xii

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction*. PhD thesis, California Institute of Technology, Pasadena, CA, arXiv, quant-ph 9705052, 1997. vii, xi, 43, 69

[Gra01] M. Grassl. *Fehlerkorrigierende Codes für Quantensysteme: Konstruktionen und Algorithmen*. PhD thesis, Institut für Informatik, Universität Karlsruhe, Germany, 2001. 21, 45

[Gro96] L. K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, pages 212–219. ACM, 1996. also arXive quant-ph 9605043. vii, xi

[Gro97] L. K. Grover. Quantum Mechanics helps in Searching a Needle in a Haystack. *Phys. Rev. Lett.*, 79(2):325, 1997. also arXiv, quant-ph 9706033. vii, xi

[HS97] L. A. Hemaspaandra and A. L. Selman. *Complexity Theory Retrospective*, volume II, chapter Berthiaume, A.: Quantum Computation. New York: Springer, 1997. vii, xi, 43, 45, 46

[KLPL06] D. Kribs, R. Laflamme, D. Poulin, and M. Lesosky. Operator Quantum Error Correction. *Quant. Info. and Comp.*, 6:382, 2006. Also ArXiv, cs. OH/0504189. 43

[KM87] B. Kümmerer and H. Maassen. The Essentially Commutative Dilations of Dynamical Semigroups on M_n. *Commun. Math. Phys.*, 109:1–22, 1987. 66

[KM98] B. Kümmerer and H. Maassen. Elements of Quantum Probability. In R. L. Hudson and J. M. Lindsay, editors, *Quantum Probability Communications*, pages 73–100. World Scientific Singapore, 1998. vii, xi, 44

[Kra71] K. Kraus. General State Changes in Quantum Theory. *Ann. Phys.*, 64:331–335, 1971. 65

[Küm85a] B. Kümmerer. Markov Dilations on the 2x2-Matrices. In H. Araki, C.C. Moore, S. Stratila, and D. Voiculescu, editors, *Operator Algebras and Their Connections With Topology and Ergodic Theory*, pages 312–323. Berlin: Springer Lecture Notes in Mathematics, 1985. 67

[Küm85b] B. Kümmerer. Markov Dilations on W*-Algebras. *Journal Functional Analysis*, 63:139–177, 1985. vii, xi

[Küm85c] B. Kümmerer. On the Structure of Markov Dilations on W*-Algebras. In L. Accardi and W. von Waldenfels, editors, *Quantum Probability and Applications*, pages 318–331. Berlin: Springer Lecture Notes in Mathematics, 1985. 44

[LM99] D. Lind and B. Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, 1999. 1, 3, 4, 5, 10

[Maa06] H. Maassen. Quantum Probability and Quantum Information Theory. www.math.ru.nl/maassen, 2006. Summer School Trieste, Lecture Notes. vii, viii, xi, xii, 44, 50

[NC00] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 5, 11, 22, 24, 27, 28, 41, 45, 63, 67, 68, 69, 70, 71

[OT03] H. Olliver and J.-P. Tillich. Description of a Quantum Convolutional Code. *Physical Review Letters*, 91(17):177902, 2003. Also ArXiv, quant-ph 0304189. viii, xii, 11, 19, 37, 41

[OT04] H. Olliver and J.-P. Tillich. Quantum Convolutional Codes: fundamentals. ArXiv: quant-ph 040113451, 01 2004. viii, xii, 11, 19, 37

[Pau86] V. Paulsen. *Completely Bounded Maps and Dilations*. Longman Scientific and Technical, 1986. 15

[Ped79] G.K. Pedersen. *C*-Algebras and their Automorphism Groups*. Academic Press, 1979. 13

[Pou05] D. Poulin. Stabilizer Formalism for Operator Quantum Error Correction. *Phys. Rev. Lett.*, 95:230504, 2005. 43

[Sak98] S. Sakai. *C*-Algebras and W*-Algebras*. Springer New York, 1998. 13

[Sch95] B. Schumacher. Quantum coding. *Physical Review*, 51(4):2738–2747, 1995. vii, xi, 43, 46

[SF06] M Schürmann and U. Franz, editors. *Quantum Independent Increment Processes*, volume II, chapter Kümmerer, B.: Quantum Markov Processes Applications in Physics, pages 259–330. Heidelberg: Springer, 2006. 65, 66

[Sho97] P. W. Shor. Polynomial-Time Algorithms for Prime Factorizaion and Discrete Logarithms on a Quantum Computer. *SIAM J. Comp.*, 26(5):1484–1509, 1997. Also arXive quant-ph 9508027. vii, xi

[Ste01] L. Steiner. Ein neuer Blick auf Davies-Prozesse. diploma thesis, Mathematisches Institut A, Universität Stuttgart, Germany, 2001. 66

[Tak79] M. Takesaki. *Theory of Operator Algebras I*. Springer New York, 1979. 13

[Tak03] M. Takesaki. *Theory of Operator Algebras III*. Springer New York, 2003. 13, 15

[Wal00] P. Walters. *An Introduction to Ergodic Theory*. Springer New York, Heidelberg, 2000. 29

[WZ82] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. 50

Akademischer Werdegang

Lisa Steiner
geboren am 10. Mai 1976 in Filderstadt

08/1982 - 07/1986	*Pestalozzi-Grundschule* in Stuttgart-Rohr
08/1986 - 07/1995	*Hegel-Gymnasium* in Stuttgart-Rohr
06/1995	Abitur
10/1995 - 05/2002	Mathematik- und Physikstudium an der *Universität Stuttgart*
02/1996	Vierwöchiges, freiwilliges Schulpraktikum am *Johannes-Kepler-Gymnasium* in Stuttgart-Bad-Cannstadt
03/1997	Zwischenprüfung in Mathematik
09/1997	Vordiplom in Mathematik
10/1997	Zwischenprüfung in Physik
12/2000 - 06/2001	Zulassungs- und Diplomarbeit im Fach Mathematik: *Ein neuer Blick auf Davies-Prozesse*
10/2001	Wissenschaftliche Prüfung für das Lehramt an Gymnasien und Diplomprüfung in Mathematik
05/2002	Wissenschaftliche Prüfung für das Lehramt an Gymnasien in Physik
10/2002 - 09/2007	Wissenschaftliche Mitarbeiterin und Doktorandin am Fach Mathematik an der *Technischen Universität Darmstadt*