Mutually Unbiased Bases and Their Symmetries

Gernot Alber *[ORCID] and Christopher Charnes

Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt, Germany; ccharnes@gmail.com

*   Correspondence: gernot.alber@physik.tu-darmstadt.de; Tel.: +49-6151-16-20400

check for updates

Abstract: We present and generalize the basic ideas underlying recent work aimed at the construction of mutually unbiased bases in finite dimensional Hilbert spaces with the help of group and graph theoretical concepts. In this approach finite groups are used to construct maximal sets of mutually unbiased bases. Thus the prime number restrictions of previous approaches are circumvented and this construction principle sheds new light onto the intricate relation between mutually unbiased bases and characteristic geometrical structures of Hilbert spaces.

Keywords: mutually unbiased bases; group representations; graphs; quantum information

1. Introduction

Mutually unbiased bases of Hilbert spaces, as originally pioneered by Schwinger [1], are not only of mathematical interest by exhibiting characteristic geometric properties of Hilbert spaces, but they have also interesting practical applications in quantum technology. Current applications range from quantum state discrimination [2] and quantum state reconstruction [3,4], to quantum error correction [5,6] and quantum key distribution [7]. They also have been used as signature schemes for CDMA systems in various radio communication technologies [8].

Since the early work of Schwinger [1] the influential work of Wootters and Fields [3] has exhibited intriguing relations between mutually unbiased bases and discrete mathematics. A major result of these authors established that in a Hilbert space of d dimensions the maximum possible number of mutually unbiased bases is $(d+1)$ provided such bases exist. Mutually unbiased bases that saturate this bound are called complete. Previously many investigations have constructed complete sets of mutually unbiased bases (see e.g., [9–16]). Typically, these investigations exploit variants of the two constructions proposed by Wootters and Fields [3] and rely on the properties of Galois fields in odd and even characteristics. Within this framework it is possible to construct systematically maximal sets of mutually unbiased bases in Hilbert spaces whose dimensions are prime powers. Although these developments have exhibited numerous interesting structural properties of complete sets of mutually unbiased bases in prime-power dimensional Hilbert spaces, many questions remain open. Especially interesting is the question of the construction of complete sets of mutually unbiased bases in Hilbert spaces whose dimensions are not prime powers. The lowest dimensional example is dimension $d = 6$ for which it is still unknown whether there are mutually unbiased bases saturating the upper bound of $d + 1 = 7$ originally established by Wootters and Fields.

Here we discuss and generalize a recently developed group and graph theoretical method aimed at the systematic construction of large sets of mutually unbiased bases. This approach stems from the early ideas of Charnes and Beth [17] which were recently developed in [18,19]. The underlying idea in this approach is the systematic use of groups as the setting for constructing large sets of mutually unbiased bases. An important new feature of this framework is the formulation of the construction of systems of mutually unbiased bases as a clique finding problem in Cayley graphs of groups which are

naturally associated with sets of mutually unbiased bases. Besides the possible practical advantages, this method is independent of prime power restrictions of previous techniques and thus may offer interesting novel conceptual advantages and links to other areas of mathematics.

The purpose of this manuscript is to present the central ideas of this group and graph theoretical method in a self contained way, and to exhibit new connections between mutually unbiased bases and the symmetries encoded in the related basis groups and basis graphs. Thus, we will explore the theme for which Hilbert space dimensions the Cayley graphs of basis groups are the 1-skeletons of polyhedra in Euclidean 3-space cf. polytopal graphs [20]. The examples of polytopal graphs presented are restricted to low dimensional Hilbert spaces, i.e., $d = 2, 3, 4$, and thus do not address the still open questions concerning dimension $d = 6$. However, these examples demonstrate interesting new links between mutually unbiased bases and the symmetries of graphs which are not apparent with the more orthodox constructions based on Galois fields in prime power dimensions.

2. Mutually Unbiased Bases and Their Construction by Finite Groups

Based on the early work of Charnes and Beth [17] we summarize in this section the basic definitions encompassing the relations between mutually unbiases bases, their basis groups and associated Cayley graphs which are capable of encoding characteristic features of mutually unbiased bases of Hilbert spaces [18,19]. In particular, based on a recent theorem of Charnes [19], which establishes a structural link between complete multipartite Cayley graphs of finite groups and complete sets of mutually unbiased bases, all polytopal basis graphs in Euclidean 3-space are determined. The cliques of these graphs yield complete sets of mutually unbiased bases.

2.1. Mutually Unbiased Bases - Basic Concepts

Two orthonormal bases, say $B := \{|B_i\rangle; i = 1, \cdots, d\}$ and $C := \{|C_i\rangle; i = 1, \cdots, d\}$, of a d-dimensional Hilbert space $\mathcal{H}^d$ with scalar product $\langle .|.\rangle$ are called mutually unbiased if and only if the relation

$$| \langle B_i | C_j \rangle |^2 = \frac{1}{d} \tag{1}$$

is independent of the chosen pair (B_i, C_j). Simple well known examples are the eigenstates of any pair of Pauli spin operators in the case of $d = 2$ or the eigenstates of the quantum mechanical position and momentuma operators for $d = \infty$. In the following, however, we shall restrict our considerations to finite dimensional Hilbert spaces.

Subsequent non-selective quantum measurements of two observables associated with mutually unbiased states completely erase any quantum information contained in an arbitrarily prepared quantum state. This becomes apparent if for example we consider two such observables, namely

$$\hat{O}_B = \sum_{i=1}^{d} b_i |B_i\rangle\langle B_i|, \ \ b_i \in \mathbb{R},$$

$$\hat{O}_C = \sum_{j=1}^{d} c_j |C_j\rangle\langle C_j|, \ \ c_j \in \mathbb{R}, \tag{2}$$

and an arbitrary quantum state with density operator $\hat{\rho}$. The subsequent non-selective measurement [21] of observables $\hat{O}_B$ and $\hat{O}_C$ yields the chaotic quantum state $\hat{I}/d$, i.e.,

$$\hat{\rho}' = \sum_{j=1}^{d} |C_j\rangle\langle C_j| \left(\sum_{i=1}^{d} |B_i\rangle\langle B_i|\hat{\rho}|B_i\rangle\langle B_i| \right) |C_j\rangle\langle C_j| = \frac{\text{Tr}(\hat{\rho})}{d} \sum_{j=1}^{d} |C_j\rangle\langle C_j| = \frac{\hat{I}}{d}, \tag{3}$$

thus erasing all previous quantum information contained in the quantum state $\hat{\rho}$. In Equation (3) we have used the completeness relation $\hat{I} = \sum_{j=1}^{d} |C_j\rangle\langle C_j|$ in the Hilbert space $\mathcal{H}^d$.

2.2. Mutually Unbiased Bases and Their Encoding by Unitary Matrices

It should be noted that within quantum theory the ordering of an orthonormal basis is physically relevant. This is apparent from Equation (2), for example, because each basis vector $|B_i\rangle$ can be associated with a different physically measurable eigenvalue b_i of the associated observable $\hat{O}_B$. Therefore, the different elements of an orthonormal basis B are distinguishable physically.

Hence in our subsequent discussion we select an arbitrarily chosen orthonormal ordered basis $(|\alpha\rangle; \alpha = 1, \cdots, d)$ of a finite dimensional Hilbert space $\mathcal{H}^d$. Based on this choice any other ordered orthonormal basis, say $B := (|B_i\rangle; i = 1, \cdots, d)$, can be mapped onto a unitary matrix $M_B \in U(d)$ by

$$(M_B)_{i\alpha} := \langle B_i | \alpha \rangle^* \tag{4}$$

with $*$ denoting complex conjugation. In this mapping row i of the matrix M_B contains the components of the basis vector $|B_i\rangle$ in the canonical basis $(|\alpha\rangle; \alpha = 1, \cdots, d)$. The group of d-dimensional unitary matrices $U(d)$ acts transitively on all ordered orthonormal bases of the Hilbert space $\mathcal{H}^d$ by right multiplication. So to each pair of ordered orthonormal bases, say B and C, there corresponds a unique unitary matrix U satisfying the relation

$$M_B U = M_C. \tag{5}$$

Consequently the defining property (1) of mutually unbiases bases can be reformulated in terms of the matrices associated with different ordered orthonormal bases. Thus, two ordered orthonormal bases B and C are mutually unbiased if and only if for all $i, j \in \{1, \cdots, d\}$

$$| \langle B_i | C_j \rangle |^2 = | \left(M_C M_B^\dagger \right)_{ji} |^2 = \frac{1}{d}. \tag{6}$$

Note that the map $\hat{O}_B \longrightarrow B \longrightarrow M_B$ takes into account the distinguishability of the orthonormal basis vectors associated with different eigenvalues of the observable $\hat{O}_B$, contrary to previous approaches [12].

2.3. Mutually Unbiased Bases and Their Basis Groups

With a set of $n + 1$ pairwise mutually unbiased ordered orthonormal bases $\{B^{(0)}, B^{(1)}, \cdots, B^{(n)}\}$ of a Hilbert space $\mathcal{H}^d$ one can associate a basis group G, which is generated by the corresponding unitary matrices, i.e.,

$$G = \langle M_{B^{(0)}}, M_{B^{(1)}}, \cdots, M_{B^{(n)}} \rangle \subset U(d). \tag{7}$$

This subgroup of the unitary group in d dimensions $U(d)$ has the following properties:

- One of the matrices, e.g., $M_{B^{(0)}}$, is the unit matrix E_d. So it can be removed from the generating set, i.e.,

$$G = \langle M_{B^{(1)}}, \cdots, M_{B^{(n)}} \rangle. \tag{8}$$

- G is a subgroup of $U(d)$ which has finite or infinite order.
- Not all pairs of elements of G correspond to mutually unbiased bases.
- The structure of the mutually unbiased bases contained in G can be captured by an associated Cayley graph.

2.4. Basis Groups of Mutually Unbiased Bases and Their Cayley Graphs

To each (finite) basis group G there is an associated Cayley graph $\Gamma(G, S)$ defined by the following properties:

- The vertices of $\Gamma(G, S)$ are the group elements of G.
- A generating set $S \subset G$ is defined as all the elements of G which are mutually unbiased to the canonical basis, i.e., mutually unbiased to E_d in the case of a d dimensional Hilbert space. (S does not contain the identity matrix E_d.) Therefore, $z \in S$ implies $z^{-1} \in S$, i.e., $S = S^{-1}$.
- The edge set of $\Gamma(G, S)$ is defined as follows. Two vertices, say x and y, of the graph $\Gamma(G, S)$ are connected by an edge, if and only if $yx^{-1} \in S$, or equivalently if and only if there is an $s \in S$ with $y = sx$. The totality of edges obtained in this way comprises the edge set of $\Gamma(G, S)$.

These Cayley graphs $\Gamma(G, S)$ have the following basic properties:

- As $S^{-1} = S$, the graphs $\Gamma(G, S)$ are simple undirected graphs, i.e., they do not have multiple edges or vertex loops.
- The graphs are represented by symmetric $N \times N$ adjacency matrices with $N = |G|$. Their rows and columns are indexed by the group elements. These adjacency matrices have 0 on the diagonal positions and 0 or 1 elsewhere. Their entries are calculated using Equation (6).
- If two elements of the set S, say $M_{B^{(i)}}, M_{B^{(j)}} \in S$, are mutually unbiased not only with respect to the canonical basis but also among themselves, the set S also contains the matrix $M_{B^{(i)}} M_{B^{(j)}}^{\dagger} \in S$.
- Right multiplication by group elements preserves the adjacency relation of $\Gamma(G, S)$, so G is a subgroup of the automorphism group of $\Gamma(G, S)$.
- Since Cayley graphs are connected, there is an edge connected path between every pair of vertices of $\Gamma(G, S)$.
- As Cayley graphs are regular, each vertex of $\Gamma(G, S)$ is connected to the same number of neighbouring vertices, i.e., it has constant valency. The valency k of a graph is the number of non-zero entries in any row or column of its adjacency matrix.

It should now be apparent that the cliques of a Cayley graph $\Gamma(G, S)$, i.e., the complete subgraphs in which any two vertices are joined by an edge, correspond to mutually unbiased bases. In view of this correspondence, the clique number $\omega(\Gamma(G, S))$ of the Cayley graph $\Gamma(G, S)$, i.e., the size of its largest clique, is not only a mathematically interesting characteristic property of $\Gamma(G, S)$ but it also determines the maximal number of mutually unbiased bases characterized by this graph.

2.5. Maximal Sets of Mutually Unbiased Bases and the Structure of Their Associated Cayley Graphs

The physical relevance of the clique number $\omega(\Gamma(G, S))$ raises the interesting question whether there is a relationship between the maximal possible number of mutually unbiased bases in a d-dimensional Hilbert space, i.e., $d + 1$, and the structure of the corresponding Cayley graphs $\Gamma(G, S)$. The following recent theorem [19] demonstrates that for finite basis groups G there is such a relationship.

Theorem 1. *(Charnes Theorem 2 [19]) Let G be a finite basis group of order N with S a generating set of mutually unbiased bases in a Hilbert space $\mathcal{H}^d$. The corresponding Cayley graph $\Gamma(G, S)$ of valency k has a clique of maximum size $d + 1$ whenever the condition*

$$\frac{N}{N - k} = \omega(\Gamma(G, S)) = d + 1 \tag{9}$$

is fulfilled. In such a case $\Gamma(G, S)$ is a k-regular and complete multipartite graph.

A detailed proof of this theorem is presented in [19]. Here we just outline its basic idea. For this purpose let us consider a Cayley graph $\Gamma(G, S)$ with N vertices and with constant valency k. It is known [22,23] that the clique number $\omega(\Gamma(G, S))$ of such a Cayley graph, i.e., the largest clique size, is lower bounded by the relation

$$\frac{N}{N - k} \leq \omega(\Gamma(G, S)). \tag{10}$$

In addition, Yildirim [23] has shown that this inequality is saturated for complete multipartite graphs, i.e.,

$$\frac{N}{N-k} = \omega(\Gamma(G,S)). \tag{11}$$

Therefore, a sufficient condition that a Cayley graph $\Gamma(G,S)$ yields maximal sets of $d+1$ mutually unbiased bases in a d-dimensional Hilbert space is given by the nested inequalities

$$d+1 = \frac{N}{N-k} \leq \omega(\Gamma(G,S)) \leq d+1 \tag{12}$$

and the associated Cayley graphs $\Gamma(G,S)$ are complete multipartite, as stated in the theorem.

2.6. Maximal Sets of Mutually Unbiased Bases and Associated Polyhedra in Euclidean 3-Space

According to the previous section k-regular complete multipartite graphs satisfying Equation (9) play an important role in the group theoretical construction of maximal sets of mutually unbiased bases. We will now explore their relation to polyhedra in Euclidean 3-space [20].

Let us start our discussion with the definitions of k-regularity and complete multipartiteness of graphs. A graph is k-regular if every vertex has exactly k edges. Furthermore, a graph is complete multipartite if its vertices can be partitioned into independent sets, also called colour classes, in such a way that

- vertices within an independent set are not connected by any edge and
- there is an edge between every pair of vertices from different independent sets.

In Figure 1 the complete multipartite graph $K_{2,2,2}$ is an example of a k-regular complete multipartite graph. Its valency is $k = 4$ and the vertices belong to three independent sets each containing two vertices. However, this graph is not only complete multipartite with constant valency, it is also the 1-skeleton of a regular polyhedron in Euclidean 3-space, namely an octahedron. Therefore, the interesting question arises whether there are other polyhedra in Euclidean 3-space, whose 1-skeletons are k-regular complete multipartite graphs and are relevant in determining maximal sets of mutually unbiased bases. Interestingly, all such polyhedra can be determined by combining the condition of Equation (9) with the Steinitz criterion [24] for polytopal graphs in Euclidean 3-space and by making use of the four-color theorem [25].
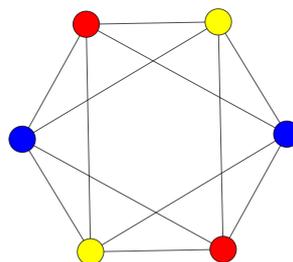

Figure 1. The graph $K_{2,2,2}$ as an example of a k-regular complete multipartite graph which is also the 1-skeleton of an octahedron in Euclidean 3-space: Each vertex has exactly $k = 4$ edges. The vertices can be partitioned into 3 independent sets (color classes) each containing 2 vertices. Vertices within the same color class are not connected by an edge and there is an edge between every pair of vertices within different color classes.

According to the Steinitz criterion a graph is polytopal in Euclidean 3-space iff the graph is planar and 3-connected [24]. A graph is planar if it can be drawn in the plane so that its edges do not intersect, and a graph is 3-connected if there is an at most 3-connected path between every two vertices of the graph.

According to the four-color theorem [25] all planar graphs can be colored using at most 4 colors. Therefore, by Equation (9) and the four-color theorem a maximal set of $d + 1$ mutually unbiased bases can be constructed in a d-dimensional Hilbert space using a finite group G of order N with a generating set S and associated Cayley graph $\Gamma(G, S)$ of valency k, if the following relation

$$\frac{N}{N - k} = d + 1 \leq 4 \tag{13}$$

is statisfied. Therefore, the necessary condition for the existence of complete multipartite polytopal graphs $\Gamma(G, S)$ which saturate the bound $d + 1$ for complete sets of mutually unbiased bases is that the Hilbert space has dimension $d = 2$ or 3.

In order to determine the possible orders N of the groups and the possible valencies k a further relation is needed. The Descartes-Euler relation [26], involving the number of vertices f_0, edges f_1 and facets f_2 of a finite convex polyhedron, establishes the equation $f_0 - f_1 + f_2 = 2$. This relation gives the additional constraint. It places an upper bound on the possible values of the valencies of the form

$$k \quad \leq \quad 5, \tag{14}$$

because every 3-polytopal graph has a vertex of valency at most 5 [24]. Consequently the dimensions d of the Hilbert spaces, the orders N and valencies k of all Cayley graphs $\Gamma(G, S)$ can be determined. Such triples (N, k, d) are the feasibility parameters of polytopal graphs in Euclidean 3-space which yield maximal sets of mutually unbiased bases. They are summarized in Table 1.

Table 1. Orders of basis groups $|\ G\ | = N$, valencies k of basis Cayley graphs $\Gamma(G, S)$, dimensions of the Hilbert spaces d and polytopal Cayley graphs $\Gamma(G, S)$ in Euclidean 3-space for which maximal sets of mutually unbiased bases can be constructed.

N	$k = Nd/(d+1)$	d	Polyhedron in 3-Space
3	2	2	triangle (degenerate)
6	4	2	octahedron
4	3	3	tetrahedron

3. Examples of Maximal Sets of Mutually Unbiased Bases, Their Basis Groups and Cayley Graphs

In this section examples are presented which exemplify the theoretical developments of the previous section in Hilbert spaces of low dimensions, i.e., $d = 2, 3$ and 4. These examples include complete multipartite polytopal Cayley graphs in Euclidean 3-space as well as more general scenarios.

3.1. A Cyclic Basis Group for $d = 2$ with an Octahedral Cayley Graph

In two dimensional Hilbert spaces a one-parameter family of cyclic basis groups $G_\varphi = < M_\varphi >$ of order $N = 6$, i.e., $M_\varphi^6 = E_2$, yielding maximal sets of mutually unbiased bases is generated by the matrix

$$M_\varphi \quad = \quad \frac{1}{\sqrt{2}} \begin{pmatrix} e^{-i\pi/4} & e^{i\varphi} \\ -e^{-i\varphi} & e^{i\pi/4} \end{pmatrix} \tag{15}$$

with $\varphi \in [0, 2\pi)$. The group generators defining the Cayley graph $\Gamma(G_\varphi, S_\varphi) = K_{2,2,2}$ are

$$S_\varphi \quad = \quad \{M_\varphi, M_\varphi^2, M_\varphi^\dagger, M_\varphi^{2\dagger}\}. \tag{16}$$

This Cayley graph is the 1-skeleton of an octahedron. It is 4-regular, complete multipartite and its vertices are partitioned into $N/(N - k) = 3 = d + 1$ independent sets $I_i = \{M_\varphi^i, M_\varphi^{i+3}\}$ ($i \in \{1, 2, 3\}$) each containing $N - k = 2$ elements. It is apparent that this Cayley graph satisfies the feasibility constraints of Table 1. The number of maximal mutually unbiased bases, i.e., complete subgraphs K_3,

is $(N-k)^{d+1} = 2^3 = 8$. Since the basis group is cylic the defining representation of G_φ splits into the direct sum of 2 one dimensional representations [27].

3.2. A Non-Abelian Basis Group for d = 2 with an Octahedral Cayley Graph

In two dimensional Hilbert spaces a non-Abelian basis group $G =< M_1, M_2 >$ is generated by the following matrices

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & i \\ -i & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & -e^{i\pi/4} \\ e^{3i\pi/4} & 0 \end{pmatrix} \tag{17}$$

satisfying the defining relations $M_1^2 = M_2^2 = (M_1 M_2)^3 = E_2$. This representation of the symmetric group S_3 is irreducible. A generating set of S_3 used to define the Cayley graph $\Gamma(G, S)$ is

$$S = \{M_2 M_1 M_2, M_1, M_1 M_2, M_2 M_1\}. \tag{18}$$

Once again this Cayley graph is $K_{2,2,2}$ and it is the 1-skeleton of an octahedron thus satisfying the feasibility parameters of Table 1. It is 4-regular and complete multipartite with $N/(N-k) = 3 = d+1$ independent sets $I_1 = \{M_2, M_2^2\}$, $I_2 = \{M_1 M_2, M_2 M_1 M_2\}$ and $I_3 = \{M_1, (M_1 M_2)^2\}$ each containing $N - k = 2$ elements. Furthermore, the number of maximal mutually unbiased bases, i.e., of complete subgraphs K_3, is $(N-k)^{d+1} = 2^3 = 8$. Comparing this graph with the previous example demonstrates that isomorphic Cayley graphs can be associated with different basis groups and generating sets, i.e., $K_{2,2,2} \cong \Gamma(G_\varphi, S_\varphi) \cong \Gamma(G, S)$.

3.3. A Non-Abelian Basis Group for d = 3 with a Non Polytopal Cayley Graph

In three dimensional Hilbert spaces the following matrices R_1 and R_2, where $\omega := exp(\frac{2i\pi}{3})$, i.e.,

$$R_1 = \frac{1}{3} \begin{pmatrix} \omega - \omega^2 & -2\omega - \omega^2 & -2\omega - \omega^2 \\ \omega + 2\omega^2 & -2\omega - \omega^2 & \omega + 2\omega^2 \\ \omega + 2\omega^2 & \omega + 2\omega^2 & -2\omega - \omega^2 \end{pmatrix}, \quad R_2 = \frac{1}{3} \begin{pmatrix} \omega - \omega^2 & \omega - \omega^2 & \omega - \omega^2 \\ \omega - \omega^2 & -2\omega - \omega^2 & \omega + 2\omega^2 \\ \omega - \omega^2 & \omega + 2\omega^2 & -2\omega - \omega^2 \end{pmatrix}, \tag{19}$$

satisfy the defining relations $R_1^4 = E_3$, $R_1^2 = R_2^2$; $R_2^{-1} R_1 R_2 = R_1^{-1}$. Thus they generate the non-Abelian basis group $Q_8 =< R_1, R_2 >$, which is isomorphic to the quaternion group of order $| Q_8 |= N = 8$. The defining representation of Q_8 is reducible and splits into irreducible representations as $1 \oplus 2$. The entries of the matrices $3R_1$ and $3R_2$ are the Eisenstein integers. The associated Cayley graph is defined by the following set S of generators of Q_8

$$S = \{R_1, R_2, R_2 R_1, R_1^\dagger, R_2^\dagger, R_1^\dagger R_2^\dagger\}. \tag{20}$$

The resulting Cayley graph $\Gamma(Q_8, S)$ is $k = 6$-regular and complete multipartite. Each of its $N/(N-k) = 4 = d+1$ independent sets has size $N - k = 2$ (compare with Figure 2). In contrast to the two previous examples $\Gamma(Q_8, S)$ is not a polytopal graph in Euclidean 3-space.
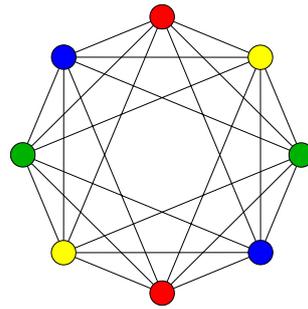
Figure 2. The Cayley graph $\Gamma(Q_8, S) = K_{2,2,2,2}$ as defined by the set S of Equation (20): This complete multipartite Cayley graph is $k = 6$-regular with 4 independent sets each containing 2 vertices. It is not a polytopal graph in Euclidean 3-space as it does not fulfill the conditions of Table 1.

The number of maximal mutually unbiased bases, i.e., complete subgraphs K_4 of $\Gamma(Q_8, S)$, is $(N - k)^{d+1} = 2^4 = 16$. A sample of four representative mutually unbiased bases, corresponding to the K_4 subgraphs of $\Gamma(Q_8, S)$, is: $\{R_1^2, R_2 R_1, R_2^3, R_1^3\}$, $\{R_1^2, R_1, R_2, R_2^3 R_1\}$, $\{E_3, R_2 R_1, R_2^3, R_1^3\}$, $\{E_3, R_1, R_2, R_2^3 R_1\}$. For the complete set of 16 mutually unbiased bases see [19]. In order to determine the number of physically distinguishable mutually unbiased bases one has to take into account the projective structure of quantum theory implying that a pure quantum state is represented by a ray in Hilbert space. Therefore, orthonormal bases which differ by a global phase have to be identified because they are indistinguishable physically. As the basis group Q_8 has non trivial centers not all 2^4 cliques of the associated Cayley graph $K_{2,2,2,2}$ yield physically distinguishable complete sets of mutually unbiased bases.

3.4. An Icosahedral Basis Group for $d = 4$ with a Non Polytopal Cayley Graph

In four dimensional Hilbert spaces the matrices T_1 and T_2, i.e.,

$$T_1 = \frac{1}{2} \begin{pmatrix} 1 & i & i & -1 \\ -i & -1 & 1 & -i \\ -i & 1 & -1 & -i \\ -1 & i & i & 1 \end{pmatrix}, \quad T_2 = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 1 & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{21}$$

satisfying the defining relations $T_1^2 = T_2^3 = (T_1 T_2)^5 = E_4$ generate the non-Abelian basis group $I_{60} = < T_1, T_2 >$, which is isomorphic to the icosahedral group of order $| I_{60} | = N = 60$. This 4-dimensional representation of I_{60} is irreducible. This basis group is a simple group, i.e., it has no proper normal subgroups [27].

The adjacency matrix of the associated Cayley graph graph $\Gamma(I_{60}, S)$ is determined by this representation of the group I_{60} and the defining relation of Equation (6) for mutually unbiased bases. The generators S of the Cayley graph $\Gamma(I_{60}, S)$ are defined by this adjacency matrix. This Cayley graph is 48-regular so that the set S contains 48 elements. Furthermore, it is complete multipartite with $N/(N - k) = 5 = d + 1$ independent sets each containing $N - k = 12$ elements.

Although I_{60} is the group of proper three dimensional rotations of the icosahedron, the graph $\Gamma(I_{60}, S)$ is not polytopal in Euclidean 3-space. But the basis group I_{60} is a subgroup of the automorphism group of $\Gamma(I_{60}, S)$, as required by the general properties of basis groups and their associated Cayley graphs. The number of maximal mutually unbiased bases, i.e., the number of complete subgraphs K_5 of $\Gamma(I_{60}, S)$, is $(N - k)^{d+1} = 12^5 = 248,832$. As the basis group I_{60} is a simple group all these 12^5 cliques yield physically distinguishable complete sets of mutually unbiased bases.

4. Conclusions

We have discussed and generalized a recently developed group and graph theoretial approach aiming at the construction of large sets of mutually unbiased bases in finite dimensional Hilbert spaces.

In this approach the construction of mutually unbiased bases in a Hilbert space of given dimension is reformulated as a clique finding problem of a Cayley graph associated with a finite basis group. This approach offers the possibility to enlarge and possibly also to complete already known systems of mutually unbiased basis systems. As this approach is independent of prime number restrictions of previous formulations, such as the ones in [9–16], it sheds new light onto the connections between the structure of mutually unbiased bases of Hilbert spaces and other areas of mathematics.

In this manuscript we have explored a connection to geometry by classifying all the polytopal graphs in Euclidean 3-space which are the possible Cayley graphs of basis groups supporting maximal sets of mutually unbiased bases. It has been shown that apart from the degenerate case of a two dimensional triangle such polyhedral constructions can only occur in Hilbert space dimensions $d = 2$ and $d = 3$ either by octahedra in the case $d = 2$ or by tetrahedra in the case $d = 3$. The Cayley graphs of the two dimensional examples presented in Sections 3.1 and 3.2 are isomorphic octahedra exemplifying these polytopal constructions in Euclidean 3-space. In particular, these examples demonstrate that different basis groups may lead to isomorphic Cayley graphs. The Cayley graphs of the three and four dimensional examples discussed in Sections 3.3 and 3.4, however, are of a more general nature. They do not belong to the set of polytopal constructions in Euclidean 3-space and introduce new complete sets of mutually unbiased bases. In particular, these two latter examples demonstrate the general property discussed in Section 2.4 that a basis group, such as Q_8 (I_{60}), is always a subgroup of the automorphism group of the associated Cayley graph, such as $K_{2,2,2}$ ($K_{12,12,12,12}$). This property establishes an interesting general relation between the symmetry encoded in a basis group and the symmetry encoded in its associated Cayley graph which is expected to be useful for the construction of complete sets of mutually unbiased bases in higher dimensional Hilbert spaces.

Our investigations and the low dimensional examples presented here constitute the first steps in a systematic exploration of this group and graph-theoretical approach. They hint at interesting connections between structures of mutually unbiased bases of finite dimensional Hilbert spaces and symmetries of Cayley graphs which will be explored in future work.

Author Contributions: Conceptualization, G.A. and C.C.; methodology, G.A. and C.C.; validation, G.A. and C.C.; investigation, G.A. and C.C.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Schwinger, J. Unitary operator bases. *Proc. Natl. Acad. Sci. USA* **1960**, *46*, 570–579.
2. Ivanovic, I.D. Geometrical description of quantal state determination. *J. Phys. A: Math. Theor.* **1981**, *14*, 3241–3245.
3. Wootters, W.K.; Fields, B.D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **1989**, *191*, 363–381.
4. Yuan, H.; Zhon, Z.-W.; Guo, G.-S. Quantum state tomography via mutually unbiased measurements in driven cavity QED systems. *New J. Phys.* **2016**, *18*, 043013.
5. Gottesman, D. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **1996**, *54*, 1862–1868.
6. Calderbank, A.R.; Rains, E.M.; Shor, P.W.; Sloane, N.J.A. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **1997**, *78*, 405–408.
7. Bruß, D. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.* **1998**, *81*, 3018–3021.
8. Heath, R.W.; Strohner, T.; Paulraj, A.J. On quasi-orthogonal signatures for CDMA systems. *IEEE Trans. Inf. Theory* **2006**, *52*, 1217–1225.
9. Lawrence, J.; Brukner, C.; Zeilinger, A. Mutually unbiased binary observable sets on N qubits. *Phys. Rev. A* **2002**, *65*, 032320.

10. Šulc, P.; Tolar, J. Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions. *J. Phys. A: Math. Theor.* **2007**, *40*, 15099–15111.

11. Garcia, A.; Romero, J.L.; Klimov, A.B. Generation of bases with definite factorization for an n-qubit system and mutually unbiased sets construction. *J. Phys. A: Math. Theor.* **2010**, *43* 385301.

12. Brierley, S.; Weigert, S.; Bengtsson, I. All mutually unbiased bases in dimensions two to five. *Quantum Inf. Comp.* **2010**, *10*, 803–820.

13. van Dam, W.; Howard, M. Bipartite entangled stabilizer mutually unbiased bases as maximum cliques of Cayley graphs. *Phys. Rev. A* **2011**, *84*, 012117.

14. Klimov, A.B.; Björk, G.; Sánchez-Soto, L.L. Optimal quantum tomography of permutationally invariant qubits. *Phys. Rev. A* **2013**, *87*, 012109.

15. Spengler, C.; Kraus, B. Graph-state formalism for mutually unbiased bases. *Phys. Rev. A* **2013**, *88*, 052323.

16. García, A.; Klimov, A.B. Complete sets of mutually unbiased operators in n-qudit systems. *Phys. Scr. T* **2014**, *160*, 014012.

17. Charnes, C.; Beth, T. Groups, graphs and mutually unbiased bases. In Proceedings of ERATO conference on Quantum Information Science 2005, Tokyo, Japan, 26–30 April 2005; pp. 73–74.

18. Alber, G. Charnes, C. Mutually unbiased bases: a group and graph theoretical approach. *Phys. Scr.* **2018**, *94*, 1–8.

19. Charnes, C. Group representations, graphs and mutually unbiased bases. *Linear Algebra Appl.* **2019**, in preparation.

20. Coxeter, H.S.M. *Regular Polytopes*; Dover Publications: New York, NY, USA, 1973.

21. Holevo, A.S. *Statistical Structure of Quantum Theory*; Springer: Berlin, Germany, 2001.

22. Wilf, H.S. Spectral bounds for the clique and independence numbers in graphs. *J. Comb. Theory Ser. B* **1986**, *40*, 113–117.

23. Yildirim, E.A. A simpler characterization of a spectral lower bound on the clique number. *Math. Methods Oper. Res.* **2010**, *71*, 267–281.

24. Kalai, G. Polytope skeletons and paths. In *Handbook of Discrete and Computational Geometry-Third Edition*; Goodman, J.E., O'Rourke, J., Tóth, C.D., Eds.; CRC Press: Boca Raton, FL, USA, 2017; pp. 505–532.

25. Gonthier, G. Formal proof—The four-color theorem. *Not. Am. Math. Soc.* **2008**, *55*, 1382–1393.

26. Ziegler, G.M.; Blatter, C. Euler's polyhedron formula—A starting point of today's polytope theory. *Elem. Math.* **2007**, *62*, 184–192.

27. Murnaghan, F.D. *The Theory of Group Representations*; Dover Publications: New York, NY, USA, 2005.