Welch Bounds and Quantum State Tomography

by

Aleksandrs Belovs

A thesis
presented to the University of Waterloo
in fulfilment of the
thesis requirement for the degree of
Master of Mathematics
in
Combinatorics and Optimization

Waterloo, Ontario, Canada, 2008

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Aleksandrs Belovs.

Abstract

In this thesis we investigate complete systems of MUBs and SIC-POVMs. These are highly symmetric sets of vectors in Hilbert space, interesting because of their applications in quantum tomography, quantum cryptography and other areas. It is known that these objects form complex projective 2-designs, that is, they satisfy Welch bounds for $k = 2$ with equality. Using this fact, we derive a necessary and sufficient condition for a set of vectors to be a complete system of MUBs or a SIC-POVM. This condition uses the orthonormality of a specific set of vectors.

Then we define *homogeneous systems*, as a special case of systems of vectors for which the condition takes an especially elegant form. We show how known results and some new results naturally follow from this construction.

Acknowledgements

I am grateful to my supervisor Ashwin Nayak for his help and support during my master's study, to the official readers of my thesis: Chris Godsil and Andrew Childs for their comments on my work, and to everyone in the Department of Combinatorics and Optimization for making my stay and research at the University of Waterloo more pleasant.

Also I would like to thank Juris Smotrovs for his participation in our joint research and Māris Ozols for useful discussions. Special thanks go to José Ignacio Rosado for bringing my attention to some errors in the early version of the paper that constitutes a part of the thesis.

Finally, I would like to thank my parents, relatives and friends in Latvia for their understanding and encouragement during my stay at Waterloo.

Contents

List of Figures

Chapter 1

Introduction

Quantum measurement is an important part of any quantum information processing task, since only through measurement is it possible to obtain any information about the system that, at the end of the day, can be interpreted by a human being. Many quantum algorithms or other quantum information processing tasks are based on transformations of a quantum state such that one specifically selected measurement reveals a lot of information about the problem being solved. In contrast, quantum state tomography is a process of applying quantum measurements in the most general settings — when nothing or almost nothing is known about the state. In this thesis we investigate two objects interesting from the point of view of quantum state tomography, however, useful in other aspects as well, — complete systems of Mutually Unbiased Bases (MUBs) and Symmetric Informationally Complete Positive Operator Valued Measures (SIC-POVMs).

A complete system of MUBs in the Hilbert space $\mathbb{C}^n$ is a set of $n+1$ orthonormal bases such that any two vectors from different bases have inner product of modulus $\frac{1}{\sqrt{n}}$. A SIC-POVM in $\mathbb{C}^n$ is a set of n^2 unit-norm vectors such that every two of them have the absolute value of their inner product equal to $\frac{1}{\sqrt{n+1}}$. These objects give the best possible measurements in corresponding classes of measurements, but it is not known whether they exist in all dimensions. Complete systems of MUBs are known to exist in prime power dimensions [58], and it is believed that they do not exist in other dimensions. SIC-POVMs are constructed numerically for all dimensions up to 47 [47, 21], and some analytical SIC-POVMs are known as well, but there is only a finite list of n's such that a SIC-POVM has been constructed in the space $\mathbb{C}^n$. However, it is widely believed that they do exist in all dimensions. Despite a considerable effort spent on proving these two conjectures, they are still open. In this thesis we also try to tackle these problems.

It is known that these optimal measurements (MUBs and SIC-POVMs) form what is called a complex projective 2-design [37]. This is a set of vectors that satisfies the Welch bounds for $k = 2$ with equality. We give a necessary and sufficient condition on the set of vectors to attain the Welch bounds, that uses the orthogonality of a particular set of vectors together with conditions on their norms. This, at first, allows us to perform the search of absolute values of the entries of vectors independently of phases, that can be seen as a task in a real vector space. Secondly, it replaces the unobvious absolute value of the inner product ($\frac{1}{\sqrt{n}}$ and $\frac{1}{\sqrt{n+1}}$) by zero, i.e., by the orthogonality condition on vectors, and that is a well studied relation.

We introduce the special case of complete systems of MUBs and SIC-POVMs, that we call *homogeneous construction*. It is a unified way to treat both complete systems of MUBs and SIC-POVMs. It includes all known examples of complete systems of MUBs and also Weyl-Heisenberg group covariant SIC-POVMs (a special class of SIC-POVMs introduced in [60, 47]). The reason for introducing this special case is that the criterion we mentioned in the previous paragraph takes an especially nice form in this special case. We give evidence that sometimes group covariant SIC-POVMs is a too narrow class (see Section 7.3), and the homogeneous construction gives SIC-POVMs that have nicer expressions than already known group covariant SIC-POVMs. This approach also gives some intuition why Fourier matrices (and, in particular, Weyl-Heisenberg group) are so useful in constructing MUBs and SIC-POVMs.

The part of the thesis concerning complete systems of MUBs mostly follows our joint paper with J. Smotrovs [6]. The part concerning SIC-POVMs represents more recent research that is not yet published.

The thesis is organized as follows. The first chapters are introductory. In Chapter 2 we define some technical concepts that we need in the next chapters: quantum states and measurements, characters of finite Abelian groups, Fourier matrices, generalized Pauli and Clifford groups. In Chapter 3 we introduce the main objects we are going to work with — MUBs and SIC-POVMs, describe some known results. In Section 3.3 we describe one known way of treating these objects as sets of vectors in real vector space — in the space of traceless Hermitian matrices. This representation also shows why these objects are so useful in quantum state estimation. In Chapter 4 we give a short excursus in the topic of sequences with low cross-correlation and show that they have a lot of common with the objects we are investigating. The main tool we gather during this excursus are the Welch bounds — the bounds on the number of vectors in a system and their cross-correlation. It turns out that both complete systems of MUBs and SIC-POVMs satisfy these bound for $k = 2$ with equality. This shows that they are complex projective 2-designs, a notion introduced in Section 4.3.

In Chapter 5 we define our criterion for attaining the Welch bounds and apply it to MUBs and SIC-POVMs. In Section 5.3 we define the special case — homogeneous systems, for which the criterion takes an especially nice form. It suffices to define two $n \times n$-matrices in order to characterize a homogeneous complete system of MUBs or a homogeneous SIC-POVM in the space $\mathbb{C}^n$. We show that, except for the absolute values of the entries of the matrices, we are interested only in one function of the matrix, namely, in what we call the L-graph of a matrix. It is a simple graph with the vertex set formed by pairs of rows of the matrix, and two vertices are adjacent if the Hadamard product of the first pair of rows is orthogonal to the Hadamard product of the second pair of rows. Roughly speaking, the more edges are there in the L-graph of the matrix, the better.

In Chapter 6 we investigate the absolute values of the entries of a homogeneous SIC-POVM. We show that they can be described by a regular simplex embedded into the fixed larger regular simplices. We also investigate circulant simplices, i.e. such simplices that a circular permutation of coordinates leaves the simplex unchanged. Such simplices, in particular, are used in the group covariant SIC-POVMs, but we will show in Chapter 7 that a more general context is also interesting.

In Section 7.2 we describe known constructions of complete systems of MUBs in the light of the criterion and show how recently obtained results about MUBs and some combinatorial structures (such as perfect nonlinear functions and relative difference sets) naturally follow from the criterion applied in the homogeneous settings. A feature of our approach is that we use extensions of characters of a finite group to a larger group that contains "non-integral elements". In particular, we consider generalisations of perfect non-linear functions to this "non-integral" group. In Section 7.3 we give a short study of SIC-POVMs in dimensions 2^k.

Finally, in Chapter 8 we summarize our work.

Chapter 2

Preliminaries

2.1 Quantum State Tomography

In this section we will mostly define notions from the quantum information science, that we will use later in the text, and studying quantum measurements. In the forthcoming we mostly follow [32] and [42].

2.1.1 General Notion of a Statistical Model

Any theoretical model of some real effect is, in the final count, based on the experience of observing this effect. Experimental data form a "skeleton" of any theoretical model. In any experimental setup two main phases can be separated. In the first, *preparation phase*, a certain experimental situation is fixed. In the next, *measurement phase*, an experimental system prepared in the previous phase is interacting with a certain *measurement device* that produces some *measurement outcomes*.

One of the main conditions that any scientific experiment must satisfy is the *reproducibility condition*. It should be possible to repeat the measurement in the same experimental situation as many times as required. Although the system is prepared each time in the identical manner, the outcome measurements usually will not be equal. Almost always the experimental data will be fluctuating, and the fluctuation amplitude depends on the experiment we are performing.

However, in some physical processes the fluctuation is so tiny, that it can be ignored. For example, mechanical movement of large objects and processes in electrical circuits have this property. Such processes are called *deterministic*, and the corresponding branches of physics assume that it is possible, at least in theory, to perform a perfect measurement of the object. And indeed, a carefully performed measurement usually reduces the fluctuation.

But there are other physical processes, in which fluctuations stay large, no matter how carefully the measurements are performed. It is assumed then that the fluctuations are not because of the imperfection of the measurement devices, but because of the very nature of the investigated process. Examples of such processes include particle scattering and quantum mechanical processes.

Although the fluctuation of the measurement outcomes in such processes cannot be ignored, the following *statistical postulate* is assumed: the measurement outcomes of different runs of the experiment can be different, but the appearance of a concrete outcome in a sufficiently long sequence of experiments can be characterized by some statistical frequency. From this point of view, the result of the experiment (that is understood as a sequence of identically prepared measurements, but not a single measurement) can be theoretically described by some *probability distribution*.

A probability distribution is a pair $(\mathcal{X}, p)$, where $\mathcal{X}$ is a set, called *sample space* and p is a function from $\mathcal{X}$ into the set of non-negative real numbers. In the context of the previous paragraph, $\mathcal{X}$ is the set of the measurement outcomes and p is the corresponding frequency. In this thesis we will work only with finite sample spaces, so let us assume the set $\mathcal{X}$ is finite. Then p must satisfy the condition $\sum_{x\in\mathcal{X}} p_x = 1$.

The experimental system after the preparation phase is described by some state S. A measurement M maps the state S into some probability distribution μ_S^M. The sample spaces of all μ_S^M for a fixed M and different S are equal. It is possible to perform different measurements on the experimental system in the same state. Each measurement results in a different probability distribution, possibly with a different sample space. If states S and S' are such that for all possible measurements M the corresponding probability distributions μ_S^M and $\mu_{S'}^M$ are the same, then this two states are indistinguishable, and usually are described by the same state.

Suppose we are able to prepare states S_α for $\alpha \in \mathcal{X}$ and let $(\mathcal{X}, p)$ be a probability distribution on the sample space $\mathcal{X}$. Consider the experiment in which at first $\alpha \in \mathcal{X}$ is chosen at random accordingly to the probability distribution $(\mathcal{X}, p)$, and then the system is prepared in the state S_α. The state of the system prepared in this way is called a *mixture* of the states S_α accordingly to the probability distribution $(\mathcal{X}, p)$. It is clear, that the probability distribution μ_S^M, for any measurement M, must satisfy

$$\mu_S^M(x) = \sum_{\alpha\in\mathcal{X}} p_\alpha \mu_{S_\alpha}^M(x)$$

for each x in the sample space of M. It turns out that it is possible to identify the set of possible states of the experimental system with a convex subset of a real vector space in such a way that the mixture S of states S_α according to the probability distribution $(\mathcal{X}, p)$ is given by $\sum_{\alpha\in\mathcal{X}} p_\alpha S_\alpha$.

2.1.2 Quantum Measurements

Let us consider now quantum measurements. Let $\mathcal{H}$ be a finite dimensional Hilbert space. We will use Dirac notation: a vector $\psi \in \mathcal{H}$ we will denote by $|\psi\rangle$ and will think of it as of a column-vector. Respectively, by $\langle\psi|$ will denote the dual row-vector (complex conjugated and transposed). Hence, $\langle\varphi|\psi\rangle$ will, naturally, denote the inner product of vectors $\varphi, \psi \in \mathcal{H}$.

Quantum state is represented by what is called a *density operator*, i.e. an operator ρ in $\mathcal{H}$ satisfying $\rho \geq 0$ (ρ is positive semidefinite) and $\operatorname{Tr}\rho = 1$. Denote by $\mathcal{S}(\mathcal{H})$ the set of all density operators over $\mathcal{H}$. It is easy to see that it is a convex set: for any $\rho_1, \rho_2 \in \mathcal{H}$ and any $0 \leq p \leq 1$, we have $p\rho_1 + (1-p)\rho_2 \in \mathcal{S}(\mathcal{H})$. The density operator $p\rho_1 + (1-p)\rho_2$ corresponds to the mixture of systems prepared in the states ρ_1 and ρ_2 in proportion p and $1-p$, respectively.

In convex sets the extreme points are of particular interest. An *extreme point* is a point of a convex set that cannot be represented as a non-trivial convex combination of other points of the convex set. In $\mathcal{S}(\mathcal{H})$ the extreme points are the so called *pure states.* These are one-dimensional projectors $\rho_\psi = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in \mathcal{H}$. States of $\mathcal{S}(\mathcal{H})$ that are not pure are called *mixed states.* Spectral decomposition

$$\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|, \quad \lambda_i \geq 0, \quad \sum_i \lambda_i = 1,$$

where λ_i are the eigenvalues, and $|e_i\rangle$ are the corresponding eigenvectors of the operator ρ, shows that any mixed state can be represented as a mixture of no more than $\dim \mathcal{H}$ pure states.

Let us now return to the measurement operation. A measurement transforms a quantum state $\rho \in \mathcal{S}(\mathcal{H})$ into a probability distribution $\mu_\rho^M(x)$ over some sample space $\mathcal{X}$. As mentioned in the previous section, any measurement maps a mixture of quantum states into the corresponding mixture of probability distributions. In other words, μ_S^M, as a function of S, must be affine. This condition turns out to be sufficient to completely characterize quantum measurements.

Theorem 2.1. *Let $\rho \mapsto \mu_\rho$ be a mapping of the space of quantum states $\mathcal{S}(\mathcal{H})$ into probability distributions over some finite probability space $\mathcal{X}$. If the mapping is affine, then there exists a set of Hermitian operators $\{M_x\}$ in $\mathcal{H}$ such that*

$$M_x \geq 0, \quad \sum_{x \in \mathcal{X}} M_x = I \quad \textit{and} \quad \mu_\rho(x) = \mathrm{Tr}(\rho M_x).$$

The set $\{M_x\}$ is called a *POVM*, i.e., ‘Positive Operator-Valued Measure’ and the operators M_x are called *POVM elements.*

Many standard books on quantum mechanics do not define quantum measurement in such generality, limiting themselves to what is known as *projective* or *orthogonal measurements.* A POVM $\{M_x\}$ is called projective if it consists of projectors, i.e., $M_x^2 = M_x$ for all x, and they are pairwise orthogonal: $M_x M_y = 0$ for all $x \neq y$. In fact, as it is easy to check, any of these two conditions implies the second.

A reason why most physicists don’t use POVM formalism is mostly because many physical systems can be measured only in a very limited number of ways, and it is enough with an orthogonal measurement to describe all interesting measurements that can be performed. From this point of view projective measurements are more suitable for practical implementation than POVMs. Moreover, any POVM can be implemented using projective measurement, as follows from the following theorem:

Theorem 2.2 (Naimark)**.** *Let $\{M_x\}_{x \in \mathcal{X}}$ be a POVM in Hilbert space $\mathcal{H}$, $\dim \mathcal{H} = n$ and $|\mathcal{X}| = m$. Then there exists a Hilbert space $\tilde{\mathcal{H}}$, $\dim \tilde{\mathcal{H}} \leq nm$, an isometry $V : \mathcal{H} \to \tilde{\mathcal{H}}$, and a projective measurement $\{E_x\}$ such that*

$$M_x = V^\dagger E_x V.$$

In other words, the space $\mathcal{H}$ can be thought as embedded into a larger space $\tilde{\mathcal{H}}$, and what looks like a POVM in $\mathcal{H}$, is in fact an orthogonal measurement in $\tilde{\mathcal{H}}$.

In many tasks of quantum computation and quantum information the measured state is prepared in a very restricted form, so that even a single measurement can give a lot of information about the problem being solved. However, in some cases we are given little or no information at all about the measured state. In this case many copies of the quantum state are identically prepared (using the reproducibility postulate) and then measured. A system of measurements $\{M_i\}$ is called *informationally complete* [46] if the state $\rho \in \mathcal{S}(\mathcal{H})$ can be uniquely determined by $\mu_\rho^{M_i}$. If an informationally complete set of measurements is performed on the state, then the statistics gathered during the experiment will give an estimate of the state. This process is known as *quantum state tomography.*

Note that we cannot get the state exactly, because it is not possible to obtain the exact outcome probabilities of the measurements using only a finite number of measurements. The main task of quantum state tomography, thus, is to reduce this vagueness as much as possible using the best possible measurements.

There are two possible paradigms of quantum tomography. In the original paradigm measurements are different and each is a projective measurement. Another method is to apply the same measurement each time. Such measurements are called *informationally complete POVMs* (IC-POVMs). In the next chapter we will give one representative for each of these two paradigms: mutually unbiased bases and symmetric informationally complete POVMs.

2.2 Fourier Matrices

A Fourier matrix is the matrix that performs the Fourier transform of a finite Abelian group. Fourier transform is widely used in many areas of mathematics, physics and computer science. For example, Shor's quantum algorithms for factoring and discrete logarithm utilize Fourier transform heavily [53]. Here, however, we will be mostly interested in some specific properties of Fourier matrices.

Let us take an Abelian group

$$G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m} \tag{2.1}$$

of order $n = d_1 d_2 \cdots d_m$. Here $\mathbb{Z}_n$ stands for the group of integers modulo n: $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. By the structure theorem for finite Abelian groups, each finite Abelian group is isomorphic to a group of this form (see, e.g., [29]), so we do not lose any generality.

Later we will be also interested in the group $\tilde{G} = \mathbb{R}_{d_1} \times \mathbb{R}_{d_2} \times \cdots \times \mathbb{R}_{d_m}$, where $\mathbb{R}_a$ is the group of real numbers modulo a with the addition operation. Note that $G_1 \cong G_2$ does not imply $\tilde{G_1} \cong \tilde{G_2}$. Indeed, if $G_1 = \mathbb{Z}_6$ and $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_3$ then $G_1 \cong G_2$, but $\tilde{G_1} = \mathbb{R}_6$ and $\tilde{G_2} = \mathbb{R}_2 \times \mathbb{R}_3$ are not isomorphic: the first one is "one-dimensional" and the second one is "two-dimensional".

Also, the group G is a subgroup of $\tilde{G}$. In addition to that we will use notation G^* for the set of non-zero elements of G, and $\tilde{G}^*$ for the set of elements of $\tilde{G}$ with at least one component being a non-zero integer. Clearly, $G^* = G \cap \tilde{G}^*$.

The Fourier transform is defined using the *dual group.* The dual group of an Abelian group G is the group $\hat{G}$ formed of all the characters of the group. A *character* of an Abelian group is its morphism to the multiplicative group of unit-modulus complex numbers. It is possible to establish an isomorphism from G to $\hat{G}$ by

$$\chi_a(b) = \exp\left(\sum_{j=1}^{m} \frac{2\pi\mathbf{i}}{d_j} a_j b_j\right), \tag{2.2}$$

where $a = (a_1, a_2, \ldots, a_m)$ and $b = (b_1, b_2, \ldots, b_m)$ are elements of G, χ_a is the element of $\hat{G}$ that corresponds to a and $\mathbf{i} = \sqrt{-1}$. Note that the expression $\chi_a(b)$ is symmetric in a and b.

We will also extend the definition (2.2) to any b in $\tilde{G}$. Although we find this definition useful, one should be careful, because because $\chi_a(b)$ is ill-defined in a if $b \notin G$. This problem can be solved if we always assume that $0 \leq a_i < d_i$ when working with non-integral b.

The following lemma is a well-known result that motivates the definition of $\tilde{G}^*$.

Lemma 2.3. *Let x be an element of $\tilde{G}$. Then $\sum\limits_{y \in G} \chi_y(x) = 0$ if and only if $x \in \tilde{G}^*$.*

Proof. Let us write $x = (x_1, x_2, \ldots, x_m)$. We have:

$$\sum_{y \in G} \chi_y(x) = \prod_{j=1}^{m} \sum_{k=0}^{d_j - 1} \exp\left(\frac{2\pi\mathbf{i}}{d_j} x_j k\right).$$

The lemma follows from the fact that the roots of the equation $\sum\limits_{k=0}^{d_j-1} \omega^k = 0$ in ω are exactly the roots of unity $\exp(\frac{2\pi\mathbf{i}}{d_j} x_j)$, with x_j an integer, $0 < x_j < d_j$. ■

A matrix with complex entries all having the same absolute value is called a *flat* matrix. If it is additionally unitary (or a scalar multiple of a unitary), it is called *complex Hadamard matrix*. It is common to rescale flat matrices in such a way that each of its elements has absolute value 1. We will usually assume that. In the case of an $n \times n$ complex Hadamard matrix it is sometimes more convenient to assume that each element has absolute value $\frac{1}{\sqrt{n}}$ (so that the matrix becomes unitary), sometimes 1. According to the situation, we will use the more suitable of these two assumptions; it will be clear from the context what is meant.

A complex Hadamard matrix is a generalization of a classical Hadamard matrix that satisfies the same requirements, but with all entries real (i.e., ±1) (see, for example, Section I.9 of [7]). We will further use term Hadamard matrix or just Hadamard to denote complex Hadamard matrices. For the classical Hadamard matrix we will use term 'real Hadamard'.

Two Hadamard matrices are called *equivalent* if one can be got from another using row and column multiplications by a scalar and row and column permutations. Some classes of equivalent Hadamards are classified. See [55] for more details. However, even in dimension 6 they are not yet completely classified [8].

We have given all these definitions in order to state the following important corollary of Lemma 2.3:

Corollary 2.4. *The matrix $F = (f_{i,j})$, indexed by the elements of G and with $f_{i,j} = \chi_j(i)$, is a Hadamard matrix.*

Proof. Clearly, all elements of the matrix have absolute value 1. The inner product of the rows indexed by a and b with $a \neq b$ is

$$\sum_{y\in G} \overline{\chi_y(a)}\chi_y(b) = \sum_{y\in G} \chi_y(b-a) = 0.$$

Hence, two distinct rows are orthogonal and the matrix F is Hadamard. ■

Matrix F from the last corollary is called the *Fourier matrix* of the group G. As an example, if we take $G = \mathbb{Z}_n$, we obtain the matrix:

$$F_n = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_n & \omega_n^2 & \dots & \omega_n^{n-1} \\ 1 & \omega_n^2 & \omega_n^4 & \dots & \omega_n^{2n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_n^{n-1} & \omega_n^{2n-2} & \dots & \omega_n^{n^2-2n+1} \end{pmatrix} \tag{2.3}$$

with $\omega_n = e^{2\pi \mathbf{i}/n}$. If we wish to consider Fourier matrix as a unitary operation, it is enough to rescale it by $\frac{1}{\sqrt{n}}$. Unlike the usual convention in quantum computing, we define the Fourier matrix F_n as in (2.3), i.e., we do not rescale by $\frac{1}{\sqrt{n}}$. An arbitrary Fourier matrix is equal to a tensorial product of such matrices. For instance, if $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$ then the Fourier matrix of G is given by $F = F_{d_1} \otimes F_{d_2} \otimes \cdots \otimes F_{d_m}$. The *Fourier transform* of a vector $|x\rangle$ with components indexed by the elements of the group G is defined as $F|x\rangle$.

It is straightforward to check that $F_n^2 = nR_n$, where R_n is the matrix exchanging i-th basis vector with the $(-i)$-th modulo n:

$$R_n = \begin{pmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \dots & 0 & 0 \end{pmatrix}. \tag{2.4}$$

Since $R_n^2 = I$, we have $F_n^{-1} = \frac{1}{n}R_nF_n = \frac{1}{n}F_nR_n$. Because F_n is symmetric, we have also $F_n^{-1} = \frac{1}{n}\overline{F_n}$.

Let $A = (a_{ij})$ and $B = (b_{ij})$ be two matrices of equal size. The *Hadamard product* (see, for example, Chapter 7 of [33]) is the matrix of the same size (denoted by $A \circ B$) with its (i,j)-th entry equal to $a_{ij}b_{ij}$. In other words, multiplication is performed component-wise. The k-th Hadamard power of the matrix A is again the matrix of the same size (denoted by $A^{(k)}$) with its (i,j)-th entry equal to a_{ij}^k. The following result is obvious.

Proposition 2.5. *The Fourier matrix of the group G is symmetric. Denote by R_i the row of the matrix that corresponds to the element $i \in G$. Then $R_i \circ R_j = R_{i+j}$, i.e., the set of rows (the set of columns) with Hadamard multiplication operation forms a group, that it is isomorphic to the original group G.*

Remark 2.6. Note that the statement of Corollary 2.4 holds with more general assumptions. Take any subset $X \subset \tilde{G}$ of size $|G|$ such that for any $a, b \in X$ with $a \neq b$ we have $a - b \in \tilde{G}^*$. Then the matrix $F = (f_{xj})$ $(x \in X,\ j \in G)$, with $f_{xj} = \chi_j(x)$, is Hadamard.

For example, if we take $G = \mathbb{Z}_3 \times \mathbb{Z}_2$ and $X = \{(0,0),(0,1),(1,a),(1,1+a),(2,b),(2,1+b)\}$ where $0 \le a, b \le 1$ are some reals, then we get the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & z_1 & -z_1 & z_2 & -z_2 \\ 1 & 1 & \omega_3 & \omega_3 & \omega_3^2 & \omega_3^2 \\ 1 & -1 & \omega_3 z_1 & \omega_6^5 z_1 & \omega_3^2 z_2 & \omega_6 z_2 \\ 1 & 1 & \omega_3^2 & \omega_3^2 & \omega_3 & \omega_3 \\ 1 & -1 & \omega_3^2 z_1 & \omega_6 z_1 & \omega_3 z_2 & \omega_6^5 z_2 \end{pmatrix}$$

where $z_1 = e^{\mathbf{i}\pi a}$ and $z_2 = e^{\mathbf{i}\pi b}$. This matrix is equivalent to one given in equation (4) of [8]. In that paper such matrices are also called Fourier matrices. We prefer, however, to reserve name 'Fourier matrix' for matrices that perform Fourier transform of a finite Abelian group.

2.3 Pauli Group and Circulant Matrices

Define two unitary matrices (we enumerate rows and columns of matrices with elements of $\mathbb{Z}_n$ from 0 to $n-1$)

$$X_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad Z_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega_n & 0 & \cdots & 0 \\ 0 & 0 & \omega_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega_n^{n-1} \end{pmatrix}. \tag{2.5}$$

The first operator maps a basis vector $|i\rangle$ to the vector $|i+1\rangle$ modulo n. The second operator multiplies a basis vector $|i\rangle$ by the phase ω_n^i. The group generated by these two operators is known as the *Weyl-Heisenberg* or *generalized Pauli group*.

Let us state some properties of operators X_n and Z_n. At first, $Z_n X_n = \omega_n X_n Z_n$, since

$$Z_n X_n |i\rangle = Z_n |i+1\rangle = \omega_n^{i+1} |i+1\rangle = \omega_n X_n \omega_n^i |i\rangle = \omega_n X_n Z_n |i\rangle$$

for all basis vectors $|i\rangle$. Also, it is easy to see that $X_n^n = Z_n^n = I$. So, the Weyl-Heisenberg group in n dimensions consists of n^3 elements $\{\omega_n^k X_n^i Z_n^j \mid 0 \le k, i, j \le n-1\}$.

Recall that the *unitary group* $\mathrm{U}(n)$ is the group of unitary matrices in the space $\mathbb{C}^n$ with matrix multiplication as the group operation. However, in quantum mechanics the global phase often is not important, so, define $\mathrm{I}(n)$ as $\{\alpha I \mid \alpha \in \mathbb{C}, |\alpha| = 1\}$ where I is the identity matrix in $\mathbb{C}^n$. Then define the *generalized Pauli group* $\mathrm{GP}(n)$ as the subgroup of $\mathrm{U}(n)/\,\mathrm{I}(n)$ consisting of equivalence classes containing elements of $\{X_n^i Z_n^j \mid 0 \le i, j < n\}$.

The *Clifford group* $\mathrm{C}(n)$ is defined as the subgroup of $\mathrm{U}(n)/\,\mathrm{I}(n)$ that normalizes the generalized Pauli group via conjugation. I.e.,

$$\mathrm{C}(n) = \{U \in \mathrm{U}(n)/\,\mathrm{I}(n) \mid U\,\mathrm{GP}(n) U^\dagger = \mathrm{GP}(n)\}.$$

Also we will be interested in tensorial products of generalized Pauli groups, so let us define $\mathrm{GP}(G)$ where G is a finite Abelian group like in (2.1) in the following manner. Set $\mathrm{GP}(\mathbb{Z}_n) =$

$\mathrm{GP}(n)$ and for groups G_1 and G_2, define $\mathrm{GP}(G_1 \times G_2) = \{U_1 \otimes U_2 \mid U_1 \in \mathrm{GP}(G_1), U_2 \in \mathrm{GP}(G_2)\}$. It is easy to see that $|\,\mathrm{GP}(G)| = |G|^2$.

Let us return to operators X_n and Z_n. Operator X_n has eigenvalues $\lambda_k = \omega_n^{n-k}$ for $k = 0, 1, \ldots, n-1$ and the corresponding eigenvectors are

$$t_k = (1, \omega_n^k, \omega_n^{2k}, \ldots, \omega_n^{(n-1)k}).$$

The Fourier matrix F_n defined in (2.3) has exactly these vectors as columns and Z_n^{-1} has exactly the same eigenvalues on the diagonal, hence,

$$Z_n^{-1} = F_n^{-1} X_n F_n.$$

Replacing F_n by F_n^{-1}, we get in a similar fashion that $Z_n = F_n X_n F_n^{-1}$. From the last two identities, the following fact easily follows.

Proposition 2.7. *The Fourier matrix $\frac{1}{\sqrt{n}} F_n$ belongs to the Clifford group $\mathrm{C}(n)$.*

Recall that a square matrix $C = (c_{ab})$ with rows and columns indexed with elements of an Abelian group G, is called *circulant* over G if $c_{a+d,b+d} = c_{a,b}$ for all $a, b, d \in G$. If $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$, then, as it is easy to see, a matrix is circulant if and only if it is a linear combination of matrices

$$\{X_{d_1}^{a_1} \otimes X_{d_2}^{a_2} \otimes \cdots \otimes X_{d_m}^{a_m} \mid 0 \leq a_i < d_i\}. \tag{2.6}$$

Since F_n diagonalizes X_n, the Fourier matrix $F = F_{d_1} \otimes F_{d_2} \otimes \cdots \otimes F_{d_m}$ of G diagonalizes any matrix from (2.6), hence, any circulant matrix over G. Let us take an arbitrary element of the set (2.6): $X = X_{d_1}^{a_1} \otimes X_{d_2}^{a_2} \otimes \cdots \otimes X_{d_m}^{a_m}$. Note that the diagonal of $F^{-1}XF$ is equal to the column of F indexed with the element $(-a_1, -a_2, \ldots, -a_m) \in G$, and it is the index of the only non-zero element in the first row of X (i.e., in the row indexed by $(0, 0, \ldots, 0)$). Hence, by linearity, we have the following theorem:

Theorem 2.8. *Any circulant matrix C over G is diagonalizable using the Fourier transform F of G. The diagonal of $F^{-1}CF$ (and, hence, the spectrum of C) is equal to the Fourier transform of the first row of C. Up to the order of elements, it is equal to the Fourier transform of the first column of C as well.*

From this it immediately follows that a circulant matrix is a scalar multiple of a unitary if and only if the Fourier transform of its first row (or column) is flat, i.e. all its elements have the same absolute value (note that this value is equal to the norm of the first row).

Recall that the *convolution* of two vectors u and v (indexed with elements of G) is defined as $w = u \star v$ with

$$w_k = \sum_{i+j=k} u_i v_j. \tag{2.7}$$

This operation is commutative and linear in both arguments. Using the result of Theorem 2.8, we have

$$F(u \circ v) = F \operatorname{diag}(u) v = \operatorname{circ}\left(F^{-1}u\right) Fv = \operatorname{circ}\left(\frac{1}{|G|} RFu\right) Fv = \frac{1}{|G|}(Fu) \star (Fv),$$

with diag(u) being the diagonal matrix with diagonal given by u, circ(u) being the circulant matrix over G with the first row equal to u, and $R = R_{d_1} \otimes R_{d_2} \otimes \cdots \otimes R_{d_m}$. In a similar way we have

$$F(u \star v) = (Fu) \circ (Fv).$$

This property is widely deployed in physics and computer science. For example, the calculation of a convolution (that is an important operation in computer graphics, sound processing and other areas) is performed by executing what is called Fast Fourier Transform (FFT), multiplying two lists element-wise, and performing inverse FFT. This happens to be much faster than the naïve calculation using (2.7).

Chapter 3

MUBs and SIC-POVMs

In this chapter we introduce the objects we are going to work with in the remaining part of the thesis: mutually unbiased bases (MUBs) and symmetric informationally complete POVMs (SIC-POVMs). We give the corresponding definitions, state main properties and applications of these objects. Additionally we discuss some conjectures on the existence of SIC-POVMs.

In Section 3.3 we define a mapping of the quantum states into the real vector space. This mapping is a generalization of the well-known Bloch sphere representation to higher dimensions. This mapping gives a nice geometrical description of both MUBs and SIC-POVMs. Some properties of these objects follow easily from this representation.

3.1 Mutually Unbiased Bases

Two vectors $x, y \in \mathbb{C}^n$ are called *unbiased* if the absolute value of the scalar product $|\langle x|y\rangle|$ is equal to $\frac{1}{\sqrt{n}}$. For the sake of brevity the square of an absolute value of a scalar product of two vectors sometimes is called the *angle* between these vectors (see, e.g., [37]). Thus, two vectors are unbiased if and only if the angle between them is $\frac{1}{n}$.

A set of *mutually unbiased bases* (MUBs) in the Hilbert space $\mathbb{C}^n$ is defined as a set of orthonormal bases $\{B_0, B_1, \ldots, B_r\}$ of the space such that any two vectors from different bases are unbiased. We will often group vectors of a basis into a matrix and say that two unitary matrices are mutually unbiased iff the bases obtained from their columns are. Bases with such properties were first observed by Schwinger in [51]. The name 'mutually unbiased bases' is due to Fields and Wootters [58]. For instance, the following three bases in $\mathbb{C}^2$ are mutually unbiased:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ \mathbf{i} & -\mathbf{i} \end{pmatrix} \right\} \tag{3.1}$$

The applications of MUBs includes quantum state determination [35, 58], and we are going to talk about this application in Section 3.3. Another application is quantum cryptography. For example, the well-known protocol BB84 due to Bennet and Brassard [9] uses the first two bases of (3.1). The idea behind this usage is that the measurement of a state in one of these bases provides absolutely no information about what the outcomes would be if the state had been measured in the second basis. Yet other applications are the Mean King's problem [1] and Wigner functions [59]. A good source of an up-to-date information on MUBs can be found in [20].

Clearly, if $n = 1$ then any number of unit vectors (in fact, scalars) gives a set of MUBs. This result does not seem very useful, so we will further assume the dimension of the space n is at least 2. In this case it can be proved that the number of bases in any set of MUBs in $\mathbb{C}^n$ doesn't exceed $n+1$ (see Theorem 4.3 later in the text). A set of bases that achieves this bound is called a *complete set of MUBs.* For example, the three MUBs given in (3.1) form a complete system of MUBs in $\mathbb{C}^2$. An interesting question is whether such a set exists for any given dimension n. The answer is positive if n is a prime power [35, 58]. The corresponding constructions are listed in Sections 3.1.1 and 7.2.1. In all other cases (even for $n = 6$) the question is still open, despite a considerable effort spent on solving this problem (see, e.g., [8]).

Suppose we have a complete system of MUBs: $\{B_0, B_1, \dots, B_n\}$. We can always represent them in the first basis B_0 (i.e., multiply all bases by B_0^{-1} from the left), thus we can assume that the first basis is the standard basis (the identity matrix). Then the matrices representing all other bases are unitary and have all their entries equal in absolute value $\frac{1}{\sqrt{n}}$, i.e. they are Hadamards.

A system of Hadamards such that any two are mutually unbiased is called a *system of mutually unbiased Hadamards* or *MUHs* for short. The following result is obvious.

Proposition 3.1. *A complete system of MUBs exists in the space $\mathbb{C}^n$ if and only if there is a system of n MUHs in the same space.*

A system of n MUHs in $\mathbb{C}^n$ is called a *complete system of MUHs.* It is more convenient to study complete systems of MUHs, and we will usually do so in the remaining part of the thesis.

The search for a complete system of MUBs is complicated because of the number of bases we should find and because of the non-obviousness of the angle $\frac{1}{n}$. Using the Welch bounds (as described in the next chapter) we will give a necessary and sufficient condition that uses solely the orthogonality of vectors. Clearly, it is a much more studied and intuitive relation. This is not the first attempt to substitute the angle $\frac{1}{n}$ by zero. An alternative approach that uses the projections of the corresponding density operators into the space of traceless Hermitian operators appears in the classical paper [58]. We will describe it in Section 3.3.

Our approach is slightly different. Using any collection of $n+1$ Hadamards in $\mathbb{C}^n$ we build n flat vectors (with all entries having the same absolute value), each in $\mathbb{C}^{n^2}$. Next, from each pair of these vectors we obtain a new vector from the same space. We prove that the bases of the original collection are MUHs if and only if the latter vectors are pairwise orthogonal. It is not a problem to find $\binom{n}{2}$ orthogonal flat vectors in $\mathbb{C}^{n^2}$, but, in general, they won't be decomposable back to pairs.

Moreover, if we restrict our attention to homogeneous systems of MUHs (see Section 5.3 for the definition), it is possible to reduce the criterion to only two matrices from $\mathbb{C}^n$ and orthogonality conditions obtained in a similar fashion. In order to show the usability of our result we show how it sheds light on the known constructions of complete sets of MUBs. In particular, we give slightly easier proofs that these constructions do result in complete sets of MUBs.

We also show how this approach naturally leads to some applications of combinatorial structures to MUBs that were obtained recently. In particular, we extend the correspondence between planar functions and splitting semiregular relative difference sets (see Section 7.2.2) to the case of non-splitting ones.

3.1.1 Known constructions of MUBs

In this section we give some known construction of complete systems of MUHs in dimension p^k where p is an odd prime. This construction was first obtained in the case $k = 1$ by Ivanović in [35] and then generalized for an arbitrary k by Wootters and Fields in [58]. The reason for the prime power dimension is that this construction uses finite fields that, as is well-known, are of prime power sizes. As said earlier, we will consider the odd case only. The case of $p = 2$, as well as another interpretation of the odd case will be given in Section 7.2.1. We refer the reader to any standard text on (finite) fields (e.g., [40]) for the notions related to finite fields.

Let $GF(p^k)$ be a finite field with p^k elements. Recall that a character of a group is its morphism to the multiplicative group of unit-modulus complex numbers. We will use ψ to denote characters of the additive group of the field, and ϕ for characters of the multiplicative group of the field. We will assume that multiplicative characters are non-trivial (i.e., they attain a non-identity value for at least one element of the field) and assume that $\phi(0) = 0$.

There exists a canonical way of representing additive characters of the finite field using its multiplicative structure. Namely, the character ψ_a associated with the element $a \in GF(p^k)$ is defined as

$$\psi_a(x) = \omega_p^{\mathrm{Tr}(ax)} \tag{3.2}$$

where Tr is the trace function $GF(p^k) \to GF(p)$. It is defined as

$$\mathrm{Tr}(x) = x + x^p + x^{p^2} + \cdots + x^{p^{k-1}}.$$

The trace is a linear function, and this makes $\psi_a(x)$ a character. Using this assignment the Fourier transform of a function $f : GF(p^k) \to \mathbb{C}$ is defined as the function $\hat{f} : GF(p^k) \to \mathbb{C}$ with

$$\hat{f}(x) = \frac{1}{\sqrt{p^k}} \sum_{a \in GF(p^k)} \psi_a(x) f(a).$$

If $x \neq 0$ we have the following calculations

$$\sum_{a \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax)} \phi(a) = \overline{\phi(x)} \sum_{a \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax)} \phi(ax) = \overline{\phi(x)} \sum_{a \in GF(p^k)} \psi_1(a) \phi(a)$$

that give the elegant formula

$$\hat{\phi}(x) = \overline{\phi(x)} \hat{\phi}(1). \tag{3.3}$$

The formula holds for any non-trivial multiplicative character ϕ and any x (if $x = 0$, the formula follows from Lemma 2.3). Using this formula and the fact that the Fourier transform is a unitary operation, it is not hard to deduce that $|\hat{\phi}(x)| = 1$ for any $x \neq 0$, and $\hat{\phi}(0) = 0$.

Now consider the following *quadratic* multiplicative character

$$\tau(a) = \begin{cases} 0 & , \quad a = 0; \\ 1 & , \quad a \neq 0 \text{ is a square in } GF(p^k); \\ -1 & , \quad a \text{ is not a square in } GF(p^k). \end{cases}$$

and the function $\kappa_a(x) = \psi_a(x^2)$. Using these two objects it is easy to show that

$$|\hat{\kappa}_a(b)| = 1 \tag{3.4}$$

for any non-zero a. Indeed, $|\hat{\kappa}_a(b)|$ is equal to

$$\left| \frac{1}{\sqrt{p^k}} \sum_{x \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax^2+bx)} \right| = \left| \frac{1}{\sqrt{p^k}} \sum_{x \in GF(p^k)} \omega_p^{\mathrm{Tr}(ax^2)} \right| = \left| \frac{1}{\sqrt{p^k}} \sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} (1 + \tau(y)) \right|$$

$$= \left| \frac{1}{\sqrt{p^k}} \left(\sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} + \sum_{y \in GF(p^k)} \omega_p^{\mathrm{Tr}(ay)} \tau(y) \right) \right| = |\hat{\tau}(a)| = 1.$$

In the second equality, the transformation $x \mapsto x - \frac{b}{2a}$ is applied, in the third step the fact that each non-zero square in a field of odd characteristic has two square roots, is used. In the fifth step we make use of Lemma 2.3.

Theorem 3.2. *The bases*

$$(v_b^{(r)})_\ell = \frac{1}{\sqrt{p^k}} \omega_p^{\mathrm{Tr}(r\ell^2+b\ell)}$$

(where r is a base index, b is a vector index and ℓ is a component index, all elements of $GF(p^k)$, where p is an odd prime) form a complete set of MUHs in $\mathbb{C}^{p^k}$.

Proof. Let us take two vectors from different bases, say $v_{b_1}^{(r_1)}$ and $v_{b_2}^{(r_2)}$, $r_1 \neq r_2$. It is easy to see that

$$\left| \langle v_{b_1}^{(r_1)} | v_{b_2}^{(r_2)} \rangle \right| = \left| \frac{1}{p^k} \sum_{\ell \in GF(p^k)} \omega_p^{\mathrm{Tr}((r_2-r_1)\ell^2+(b_2-b_1)\ell)} \right| = \left| \frac{1}{\sqrt{p^k}} \hat{\kappa}_{r_2-r_1}(b_2 - b_1) \right| = \frac{1}{\sqrt{p^k}}.$$

Other inner products can be checked easily. ■

3.2 Symmetric Informationally Complete POVMs

A symmetric informationally complete POVM, or SIC-POVM, is defined as a set $\{x_i\}$ of n^2 unit vectors in the n dimensional complex space $\mathbb{C}^n$ such that

$$|\langle x_i | x_j \rangle| = \frac{1}{\sqrt{n+1}}$$

whenever $i \neq j$. Thus defined, this set, of course, is not a POVM. The corresponding POVM is made of projectors $\{\frac{1}{n}|x_i\rangle\langle x_i|\}$. It is not apparent at the first glance that this is indeed a POVM, but we will show this later in Section 5.1. But already now it is clear that a SIC-POVM is merely a set of n^2 equiangular lines in $\mathbb{C}^n$, and as such has been studied outside the framework of quantum information science (see, e.g., [39]).

In the scope of quantum information science, this notion was first studied by Zauner in his doctoral thesis [60]. Aside from quantum state tomography [12], SIC-POVMs are used also in quantum cryptography [23] and theoretical foundations of quantum mechanics [24], where they are used as a kind of "standard quantum measurement", similar to standard kilogram and standard meter that are kept in France and used to calibrate other measuring apparatus.

Most of the research papers on SIC-POVMs deal with the special cases of SIC-POVMs we are now about to describe.

3.2.1 Group Covariant SIC-POVMs

In contrast to MUBs, numerical SIC-POVMs have been found in any dimension that is small enough to allow such a search. However few analytical SIC-POVMs are known, and no analytical construction working in an infinite number of dimensions has been found. Much effort has been spent on trying to narrow the search space, i.e., give a stronger conjecture than merely the existence of a SIC-POVM. Such a conjecture, if it held in all small dimensions, could give enough intuition to deduce a formula that would work in an infinite number of dimensions. Also, a computer search is easier for a special case of the problem, that makes it possible to find SIC-POVMs in large dimensions numerically. In this section we will give some of these conjectures.

A vector $|\psi\rangle \in \mathbb{C}^n$ is called *fiducial with respect to* K where K is a subgroup of $\mathrm{U}(n)/\,\mathrm{I}(n)$ if the set $\{U|\psi\rangle \mid U \in K\}$ forms a SIC-POVM (see Section 2.3 for the definitions of $\mathrm{U}(n)$, $\mathrm{I}(n)$ and other groups used in this section). A SIC-POVM that can be formed in such a way is called *group covariant with respect to* K. The name reflects the fact that any element of the group K permutes, up to a phase, the elements of the SIC-POVM.

Usually this notion is used with $K = \mathrm{GP}(n)$. So, if the group K is not specified we will always assume that it is the generalized Pauli group. For example, in $\mathbb{C}^2$ fiducial vectors are given by

$$\frac{1}{\sqrt{6}}\begin{pmatrix}\sqrt{3+\sqrt{3}}\\ \omega_8\sqrt{3-\sqrt{3}}\end{pmatrix} \qquad \text{and} \qquad \frac{1}{\sqrt{6}}\begin{pmatrix}-\sqrt{3-\sqrt{3}}\\ \omega_8\sqrt{3+\sqrt{3}}\end{pmatrix}. \tag{3.5}$$

We will give more examples in Chapter 7. Another choice for K we will sometimes use is $\mathrm{GP}(G)$ where G is a finite Abelian group.

The notion of a group covariant SIC-POVM is due to Renes *et al*, see [47]. The following conjecture is also due to them:

Open Problem 3.3. *Do group covariant SIC-POVMs exist in all dimensions?*

In the same paper they have numerically found fiducial vectors in all dimensions up to 45. The list can be found at [48].

For $n = 5$ the following fiducial vector is given in [48]:

$$\begin{pmatrix} 0.1630948960 - 0.3554098551\mathbf{i} \\ 0.3048387097 + 0.0113254913\mathbf{i} \\ 0.2784270686 + 0.3836760386\mathbf{i} \\ 0.6479623659 - 0.2829656308\mathbf{i} \\ 0.1544552195 - 0.0742890175\mathbf{i} \end{pmatrix}. \tag{3.6}$$

A good question is: what operations preserve "fiduciality". The first answer to this question could be:

Proposition 3.4. *If C is an element of the Clifford group $\mathrm{C}(n)$ and $|\psi\rangle \in \mathbb{C}^n$ is a fiducial vector, then $C|\psi\rangle$ is also a fiducial vector.*

Proof. Indeed, for any $U \in \mathrm{GP}(n)$ such that $U \notin \mathrm{I}(n)$, we have:

$$|\langle C\psi|UC\psi\rangle| = |\langle C\psi|CU'\psi\rangle| = |\langle\psi|\alpha U'\psi\rangle|,$$

for some $U' \in \mathrm{GP}(n)$. It is important to note that $U' \notin \mathrm{I}(n)$, because otherwise we would have $U = CU'C^\dagger \in \mathrm{I}(n)$, that is impossible. Hence, the inner product is equal to $\frac{1}{\sqrt{n+1}}$. ■

This was stressed by Grassl in [27]. For instance, if x is a fiducial vector, and a, b are some elements of $\mathbb{Z}_n$ with $\gcd(a, n) = 1$, then the vector y with components $y_j = x_{aj+b}$ is also a fiducial vector. In other words, permuting elements of a fiducial vector with an invertible affine operation (that works in the index set $\mathbb{Z}_n$) preserves "fiduciality". This operation falls within the scope of Proposition 3.4 as such permutations belong to the Clifford group.

However, there is one important operation that does not. Namely, it easy to see that if $|\psi\rangle \in \mathbb{C}^n$ is a fiducial vector then

$$|\langle\overline{\psi}|X_n^i Z_n^j \overline{\psi}\rangle| = \overline{|\langle\psi|X_n^i Z_n^{n-j}\psi\rangle|} = \frac{1}{\sqrt{n+1}}$$

for any integeres $0 \le i, j < n$ not equal to zero simultaneously (here $|\overline{\psi}\rangle$ is a component-wise complex conjugate of $|\psi\rangle$). Hence, complex conjugation also preserves "fiduciality".

This observation led Appleby to define the extended Clifford group in [3] as follows. An *anti-linear* operator $L : \mathbb{C}^n \to \mathbb{C}^n$ is defined as a linear operator over $\mathbb{R}$ with an additional property $L(\alpha|\psi\rangle) = \bar{\alpha}L|\psi\rangle$ for any vector $|\psi\rangle$ and scalar α. An anti-linear operator L is called *anti-unitary* if it is invertible and its inverse satisfies $\langle\varphi|L^{-1}|\psi\rangle = \langle\psi|L|\varphi\rangle$ for all $|\varphi\rangle, |\psi\rangle \in \mathbb{C}^n$.

The *extended Clifford group* $\mathrm{EC}(n)$ is defined as the group consisting of all unitary and anti-unitary operators U such that $U\,\mathrm{GP}(n)U^{-1} = \mathrm{GP}(n)$. Proposition 3.4 can be strengthened in the following way:

Proposition 3.5. *If C is an element of the extended Clifford group $\mathrm{EC}(n)$ and $|\psi\rangle \in \mathbb{C}^n$ is a fiducial vector, then $C|\psi\rangle$ is also a fiducial vector.*

3.2.2 Zauner's Conjecture

As we have seen in the previous subsection, any element of the Clifford group transforms a fiducial vector into a fiducial vector. Since there are not so many fiducial vectors, it is quite possible that some element U of the Clifford group leaves some fiducial vector unchanged up to a phase, i.e. that this fiducial vector is an eigenvector of U.

Something of this kind was conjectured by Zauner in his doctoral thesis [60].

Conjecture A. *Let U_z be the element of the Clifford group $\mathrm{C}(n)$ that satisfies $U_z Z_n^i X_n^j = Z_n^{j-i} X_n^{-i} U_z$ for all i, j. Then, in any finite dimension, U_z has an eigenvector that is a fiducial vector.*

(Usually the operator U_z is denoted by Z, but we do not use this notation in order to not confuse it with the operator Z_n). Note that U_z has order 3, i.e., $U_z^3 = I$. Note also that if $|\psi\rangle$ is a fiducial vector and simultaneously an eigenvector of $U \in \mathrm{EC}(n)$, and U' is a conjugate of U in $\mathrm{EC}(n)$ (say, $U' = VUV^{-1}$, $V \in \mathrm{EC}(n)$), then $V|\psi\rangle$ is an eigenvector of U' and also a fiducial vector because of Proposition 3.5.

Regarding Conjecture A, it is worth mentioning that the spectrum of U_z is highly degenerate, which is part of the reason it is not so easy to decide whether it has a fiducial eigenvector.

Appleby in [3] by careful analysis of numerical fiducial vectors found by Renes *et al.* in [47], defined a special class of order 3 unitaries of $\mathrm{C}(n)$, that he called *canonical order 3 unitaries*, and stated the following two conjectures.

Conjecture B. *A fiducial vector exists in every finite dimension. Each fiducial vector is an eigenvector of a canonical order 3 unitary.*

Conjecture C. *A fiducial vector exists in every finite dimension. Each fiducial vector is an eigenvector of an element of $\mathrm{C}(n)$ which is conjugate to U_z.*

In fact, U_z is a canonical order 3 unitary, and each element of $\mathrm{C}(n)$ that is conjugate to a canonical order 3 unitary, is a canonical order 3 unitary itself. Hence, Conjecture C implies both Conjectures A and B. No counterexamples to Conjectures A and B have been found. Grassl [28] constructed a counterexample to Conjecture C in dimension 12, however, for prime dimensions greater than 3, Conjectures A, B and C are known to be equivalent [21].

Thus, the leading tendency is to narrow the class of SIC-POVMs as much as possible. We, however, are going to define in Section 5.3 a bit wider class than group covariant SIC-POVMs, that borrows many ideas from the constructions of complete sets of MUHs.

3.3 The Space of Traceless Hermitian Matrices

We are now going to take a closer look at the space in which density matrices live and describe how MUBs and SIC-POVMs look in this representation. We mostly follow [58] when talking about MUBs, and [47] when talking about SIC-POVMs. We also used [52].

As we have seen in Section 2.1.2, a density matrix ρ is a positive semidefinite matrix in $\mathbb{C}^n$ of trace 1. Consider the mapping

$$\beta(S) = S - \frac{\operatorname{Tr} S}{n} I$$

from the set of Hermitian matrices to the set of traceless Hermitian matrices $\mathcal{H}_0$. As easy to check, the latter set is a real vector space of dimension $n^2 - 1$.

The *Hilbert-Schmidt inner product* is defined by $(A|B) = \mathrm{Tr}(A^\dagger B)$ (in $\mathcal{H}_0$ this is, of course, equal to $\mathrm{Tr}(AB)$). Note that this quantity is equal to the sum of all entries of $\overline{A} \circ B$. In other words, this is nothing else but the inner product of A and B if we represent them as elements of $\mathbb{C}^{n^2}$ by packing entries of a matrix into one long vector. Since A and B are Hermitian, the (i,j)-th and (j,i)-th entries of $\overline{A} \circ B$ are complex conjugates of each other for all i and j, hence $(A|B)$ is a *real* inner product in $\mathcal{H}_0$.

The norm induced by $(A|B)$ is called *Euclidean* norm (see chapter 5 of [33], also known as *Frobenius* norm) $\|A\|_E = \sqrt{\mathrm{Tr}(A^\dagger A)}$. It is easy to see that unitary operators, applied both from the left and the right, do not change the Euclidean norm of a matrix. Hence, from the singular value decomposition it follows that $\|A\|_E$ is equal to $\sqrt{\sum_i \sigma_i^2}$, where $\{\sigma_i\}$ are the singular values of A. For Hermitian matrices, that are the only ones we consider here, the singular values are equal to the absolute values of the eigenvalues.

Any normalized vector $|\psi\rangle \in \mathbb{C}^n$ can also be embedded in $\mathcal{H}_0$ by $\psi \mapsto |\psi\rangle\langle\psi| - I/n$. The eigenvalues of the latter matrix are $1 - \frac{1}{n}$ with multiplicity 1, and $-\frac{1}{n}$ with multiplicity $n-1$. Hence,

$$\||\psi\rangle\langle\psi| - I/n\|_E = \frac{1}{n}\sqrt{(n-1)^2 + (n-1)} = \sqrt{(n-1)/n}.$$

Mixed states, as mixtures of pure states, have strictly smaller norm. The zero point corresponds to the maximally mixed state.

If $n = 2$ this embedding *beta* is equivalent to the well-known Bloch sphere representation. In this case it is bijective, i.e., any point within the ball of radius $1/\sqrt{2}$ corresponds to a density matrix. If $n > 2$, the mapping is injective, but not surjective. It is easy to see, since otherwise every mixed state would be a mixture of no more than two pure states. That clearly is not the case.

Let $\{M_x\}$ be a POVM. Suppose we are measuring a density matrix ρ with this POVM. Then the probability of an outcome x is

$$\mathrm{Tr}(\rho M_x) = \mathrm{Tr}\left(\left(\beta(\rho) + \frac{I}{n}\right)\left(\beta(M_x) + \frac{\mathrm{Tr}\, M_x}{n} I\right)\right) = (\beta(\rho)|\beta(M_x)) + \frac{\mathrm{Tr}\, M_x}{n}.$$

Thus, orthogonal projections of $\beta(\rho)$ on $\beta(M_x)$ are uniquely determined by the measurement outcome probabilities and vice versa. If we know the outcome probabilities exactly, then the image of the density matrix in $\mathcal{H}_0$ is determined up to a vector orthogonal to $\mathrm{span}\{\beta(M_x)\}$. Hence the POVM $\{M_x\}$ is informationally complete if and only if $\{\beta(M_x)\}$ span $\mathcal{H}_0$.

Note that the condition $\sum_x M_x = I$ implies $\sum_x \beta(M_x) = 0$, hence, the images of elements of any POVM are always linearly dependent. Since the dimension of $\mathcal{H}_0$ is $n^2 - 1$, the number of elements in an informationally complete POVM is at least n^2. An example, that this bound can be achieved, is provided by SIC-POVMS. Any SIC-POVM contains n^2 elements and is informationally complete. Let us describe how SIC-POVMs look in this representation. The image of an element of a SIC-POVM looks like

$$\frac{1}{n}|\psi\rangle\langle\psi| - \frac{I}{n^2}$$

where $|\psi\rangle$ is the corresponding normalized vector. The norm of this matrix is $\sqrt{(n-1)/n^3}$. The inner product of images of two different elements of SIC-POVM (with $|\psi_1\rangle$ and $|\psi_2\rangle$ being the corresponding normalized vectors) is

$$\operatorname{Tr}\left(\left(\frac{1}{n}|\psi_1\rangle\langle\psi_1| - \frac{I}{n^2}\right)\left(\frac{1}{n}|\psi_2\rangle\langle\psi_2| - \frac{I}{n^2}\right)\right) = \frac{1}{n^2}\operatorname{Tr}(\langle\psi_2|\psi_1\rangle\langle\psi_1|\psi_2\rangle) - \frac{2}{n^3} + \frac{\operatorname{Tr} I}{n^3}$$

$$= \frac{1}{n^2(n+1)} - \frac{1}{n^3} = -\frac{1}{n^3(n+1)}.$$

Recall that a *regular simplex* in the real vector space $\mathbb{R}^n$ is the convex hull of a set of $n+1$ normalized vectors $\{x_i\}$ such that the inner product of any two of them is equal to $-1/n$. And, as is usual in geometry, translations, rotations and dilatations of this object are also called regular simplices. The point that corresponds to the origin in the original formulation is called the *centre* of the simplex. We will call the distance from the centre to the vertices of the simplex *radius* of the simplex. A regular simplex is a very symmetric object: any permutation of its vertices can be realized as an orthogonal affine operator.

A regular simplex can be constructed recursively. In zero dimension it is just a point. To get an n-dimensional regular simplex, put an $(n-1)$-dimensional simplex of radius $\sqrt{1-1/n^2}$ in the hyperplane $x_n = -1/n$, centred at $(0,0,\ldots,0,-1/n)$ and connect its vertices to the point $(0,0,\ldots,0,1)$.

It is easy to see now that the images of the elements of a SIC-POVM form a regular simplex of radius $\sqrt{(n-1)/n^3}$ in $\mathcal{H}_0$.

Let us now consider the images of the elements of MUBs. Each element of an MUB is a normalized vector, hence, its image has norm $\sqrt{(n-1)/n}$. If $|\psi_1\rangle$ and $|\psi_2\rangle$ are two different vectors from a system of MUBs, then the inner product of $\beta(\psi_1)$ and $\beta(\psi_2)$ is

$$\operatorname{Tr}\left(\left(|\psi_1\rangle\langle\psi_1| - \frac{I}{n}\right)\left(|\psi_2\rangle\langle\psi_2| - \frac{I}{n}\right)\right) = \operatorname{Tr}(\langle\psi_2|\psi_1\rangle\langle\psi_1|\psi_2\rangle) - \frac{2}{n} + \frac{\operatorname{Tr} I}{n^2}$$

$$= \begin{cases} -1/n & , \quad \psi_1 \text{ and } \psi_2 \text{ are from the same basis;} \\ 0 & , \quad \text{otherwise.} \end{cases}$$

Hence, each base of a system of MUBs is mapped to a regular simplex in an $(n-1)$-dimensional subspace of $\mathcal{H}_0$. There are $n+1$ MUBs that, in total, give $n+1$ subspaces. These $(n-1)$-dimensional subspaces are pairwise orthogonal, hence, they together span the whole space $\mathcal{H}_0$. This also proves that no system of MUBs can contain more than $n+1$ bases. We will give another proof of this fact in Theorem 4.3. Moreover, for any set of $n+1$ MUBs, no vector can be unbiased to all of them.

This also allows to give an informal argument why MUBs are useful in quantum state tomography. Suppose we perform quantum tomography of the mixed state ρ by repeatedly performing orthogonal measurements in $n+1$ orthonormal bases $B_0, B_1, \ldots, B_n$ that are together informationally complete. As we have said before, the measurement outcome probabilities for each base determine the projection of $\beta(\rho)$ onto the $(n-1)$-dimensional space spanned by the images of the elements of the base. But, if we perform only a finite number of measurements, we cannot get the outcome probabilities exactly. In reality, the outcomes of the measurement will give a kind of Gaussian distribution centered on the projection of $\beta(\rho)$.

To make the demonstration more apparent, assume that from the measurement statistics we get to know that the projection of $\beta(\rho)$ is located somewhere in a box of $(n-1)$-dimensional measure S for each of $n+1$ bases. Then we know that $\beta(\rho)$ is located somewhere in (n^2-1)-dimensional box, and its measure is minimal possible (equal to S^{n+1}) if the subspaces spanned by the images of elements of each of the bases are pairwise orthogonal. And this happens if and only if these bases are pairwise unbiased.

This, of course, is an informal argument. Refer to [58] for a more formal reasoning.

Nice representations of SIC-POVMs and MUBs in $\mathcal{H}_0$ as a regular (n^2-1)-dimensional simplex and $n+1$ pairwise orthogonal $(n-1)$-dimensional simplices, respectively, may lead one to expect that it is easy to find MUBs ans SIC-POVMs using this representation. In fact, this is easy only for $n=2$. For larger dimensions this is not easy because only a small fraction of all vectors of $\mathcal{H}_0$ with norm $\sqrt{(n-1)/n}$ are images of pure states.

Also, based on the observation that a SIC-POVM is represented by a regular simplex in $\mathcal{H}_0$, and it has the symmetric group S_{d^2} as its automorphism group, Renes *et al.* motivate in [47] why we should search for group covariant SIC-POVMs as described in Section 3.2.1.

Chapter 4

Welch Bounds

In this chapter we give a short exposition on the topic of sequences with low cross-correlation and show that they have a lot of common with the objects we defined in Chapter 3. The main tool we gather during this exposition are the Welch bounds — the bounds on the number of vectors in a system and their cross-correlation.

Welch bounds are applicable to our problem as well. Namely, it turns out that both complete systems of MUBs and SIC-POVMs satisfy these bound for $k = 2$ with equality. This shows that they are complex projective 2-designs, a notion introduced in Section 4.3.

4.1 Welch Bounds and Crosscorrelation

Welch bounds are the inequalities from the following theorem:

Theorem 4.1. *For any finite sequence $\{x_i\}$ of vectors in Hilbert space $\mathbb{C}^n$ and any integer $k \geq 1$ the following inequality holds:*

$$\binom{n+k-1}{k} \sum_{i,j} |\langle x_i | x_j \rangle|^{2k} \geq \left(\sum_i \langle x_i | x_i \rangle^k \right)^2 . \tag{4.1}$$

The proof will be given in Section 5.1, but for now let us note that these inequalities were first derived (in the case of all vectors having the same norm) by Welch in [57]. It is worth becoming acquainted with his motivation.

In order to do this we should define sequences with low correlation. For a systematic treatment of the topic see [30]. Let u and v be complex periodic sequences of equal period n. Usually the sequences are defined as $u_i = \omega_q^{a_i}$ with a_i from $\mathbb{Z}_q$. The binary case (with $q = 2$) is the most common. The *(periodic) correlation* of u and v is defined as (where L stands for the left cyclic shift function)

$$\theta_{u,v}(\tau) = \langle L^\tau(u) | v \rangle = \sum_{i=1}^{n} \overline{u_i} v_{i+\tau}.$$

The correlation of a sequence with itself is called its *autocorrelation* $\theta_u(\tau) = \langle L^\tau(u) | u \rangle$. The correlation of two shift-distinct sequences is usually called *crosscorrelation.*

Informally, the correlation of binary sequences characterizes the number of places two sequences coincide minus the number of places they differ. For random sequences magnitude of this value is small, so it can be used as a measure of the pseudorandomness of a sequence. The correlation is called *ideal* if it is as small as possible (0 or ±1). It is considered low, if it is $O(\sqrt{n})$ (an expected value for random sequences). For example, *m-sequences* (the maximal length sequences generated by a linear feedback shift register (LFSR) [50]) have ideal autocorrelation, since for them $\theta(\tau) = -1$ for any $\tau \not\equiv 0 \pmod{n}$. This, among other properties, explains why they are used in cryptography (as a main building block of nearly every stream cipher) and electronic engineering (e.g., in radars).

Families of sequences with low crosscorrelation are also well-studied. A nice property of these sequences is that they can be transmitted through the same channel simultaneously without mutual disturbance. By the time Welch was writing his paper there were some good families of sequences with low auto- and cross-correlation and he got interested in obtaining upper bounds on the number of sequences in a family.

For example, one family of sequences was proposed by Gold in [25]. For any integer k he constructed a family of $2^k + 1$ binary sequences of period $2^k - 1$ and correlation between any two of them takes only three possible values: $-1, -(2^{(k+1)/2} + 1)$ and $2^{(k+1)/2} - 1$.

Similarity of this family and a complete family of MUBs is apparent. Both are built of vectors from $\mathbb{C}^n$, vectors are joined in blocks of size n, the number of blocks is approximately the same and the ratios of possible inner products and norms of vectors also almost agree. So, an attempt to apply Welch bounds to the problem of MUBs seems quite reasonable.

Even more, it turns out that Alltop in his work [2] of 1980 (i.e., one year before the work [35] of Ivanović) for any prime $p \geq 5$ gave a set of p sequences with period p with elements of modulus $\frac{1}{\sqrt{p}}$, such that the crosscorrelation is given by

$$|\theta_{uv}(\tau)| = \begin{cases} 1 & , \quad u = v \text{ and } \tau = 0; \\ 0 & , \quad u \neq v \text{ and } \tau = 0; \\ \frac{1}{\sqrt{p}} & , \quad \tau \neq 0. \end{cases}$$

The corresponding sequences are defined as

$$b_\ell^{(r)} = \frac{1}{\sqrt{p}} \omega_p^{\ell^3 + r\ell}$$

(where r is the sequence number and ℓ is the component index). The proof is very similar to that of Theorem 3.2. These sequences with different shifts and the standard basis give a complete set of MUBs in $\mathbb{C}^p$. Another way to say this is that the vector $\{\omega_p^{\ell^3}\}_{\ell \in \mathbb{Z}_p}$ is a "fiducial vector" for a complete system of MUHs, as the ones we considered for SIC-POVMs in Section 3.2.1.

This result was generalized to prime power dimensions in [38] as Wootters and Fields [58] generalized the result of Ivanović.

Theorem 4.2. *Let $p \geq 5$ be a prime. The bases*

$$(v_b^{(r)})_\ell = \frac{1}{\sqrt{p^k}} \omega_p^{\mathrm{Tr}((\ell-b)^3 + r(\ell-b))},$$

where $r, b, \ell \in GF(p^k)$, r is the basis index, b is the vector index and ℓ is the component index, form a complete set of MUHs in $\mathbb{C}^{p^k}$.

These bases do not give sequences, as in the construction of Alltop, if $k > 1$, because ℓ is not longer an integer. But each Hadamard is still circulant, only with respect to $\mathbb{Z}_p^k$.

4.2 Link between MUBs and the Welch Bounds

As our first application of the Welch bounds to MUBs we can apply the original approach of Welch in the new settings. It is easy to check that a union of orthonormal bases satisfy the Welch bound for $k = 1$ (it can be done either directly using (4.1) or using Theorem 5.1 further in the text). So, we should use $k = 2$.

Theorem 4.3. *If $n \geq 2$ then the maximal number of mutually unbiased bases in $\mathbb{C}^n$ does not exceed $n + 1$.*

Proof. Suppose we have a system of $n+2$ MUBs. Join all vectors of the system into one big sequence $\{x_i\}$ of size $n(n+2)$. Let us fix $k = 2$ and calculate the left hand side of (4.1). We have $n(n+2)$ vectors, each giving the scalar product 1 with itself and $n(n+1)$ scalar products of absolute value $\frac{1}{\sqrt{n}}$ with vectors from other bases. Summing up, we have:

$$\binom{n+1}{2} \sum_{i,j} |\langle x_i | x_j \rangle|^4 = \frac{n(n+1)}{2} \left[n(n+2) \left(1 + n(n+1) \cdot \frac{1}{n^2} \right) \right]$$
$$= \frac{n(n+1)(n+2)(2n+1)}{2}.$$

For the right hand side we have:

$$\left(\sum_i \langle x_i | x_i \rangle^2 \right)^2 = n^2(n+2)^2 > \frac{n(n+1)(n+2)(2n+1)}{2}$$

if $n \geq 2$, in a contradiction with the Welch bound for $k = 2$. ■

If we reduce the number of MUBs from $n+2$ to $n+1$ we don't get an apparent contradiction. However, even in this case the Welch bounds prove themselves to be useful.

Theorem 4.4. *Let $\{B_i\}$ be a set of $n+1$ orthonormal bases in an n-dimensional Hilbert space and X be the union of these bases (that is the sequence of vectors, each of them appearing in the sequence the same number of times it appears in the bases). Then X satisfies the Welch bound for $k = 2$ with equality if and only if $\{B_i\}$ form a complete system of MUBs.*

Proof. If $\{B_i\}$ is a complete system of MUBs and $X = \{x_i\}$ is the union of its bases, then calculations similar to ones in the proof of Theorem 4.3 show

$$\binom{n+1}{2} \sum_{i,j} |\langle x_i | x_j \rangle|^4 = \frac{n(n+1)}{2} \left[n(n+1) \left(1 + n^2 \cdot \frac{1}{n^2} \right) \right] = n^2(n+1)^2$$

and

$$\left(\sum_i \langle x_i | x_i \rangle^2 \right)^2 = n^2(n+1)^2.$$

And vice versa, suppose X, being a union of orthonormal bases, attains the Welch bound for $k = 2$. Then, $|\langle x|x\rangle|^4 = 1$ for each x in X, $|\langle x|y\rangle|^4 = 0$ for two different vectors of the same basis, and by the inequality between square and arithmetic means (Cauchy-Schwartz inequality between the vector of all 1's and the vector $(\langle x|y\rangle)_x$) we get:

$$\sum_{x\in B_i} |\langle x|y\rangle|^4 \geq \frac{1}{n}\left(\sum_{x\in B_i} |\langle x|y\rangle|^2\right)^2 = \frac{1}{n}.$$

for any vector y of unit length. To attain the Welch bound, this inequality must actually be an equality, which is achieved only if $|\langle x|y\rangle|^2$ has the same value for all vectors x from B_i. This means that the bases $\{B_i\}$ form a complete system of MUBs. ■

Analysis of links between complex projective 2-designs (defined in the next section) and MUBs was initiated in Zauner's dissertation [60] and obtained a finished form in the work by Klappenecker and Rötteler [37]. In particular, the 'if' part of Theorem 4.4 is due to them. Also they proved that any complex projective 2-design in $\mathbb{C}^n$ with $n^2 + n$ elements, such that angle between any two distinct vectors is in $\{0, \frac{1}{n}\}$, is the union of $n + 1$ MUBs in $\mathbb{C}^n$. However, this result is not what we are really interested in. It seems that the 'only if' part of Theorem 4.4 first appeared later, in [49]. It is also worth mentioning the paper by Barnum [5] where Theorem 4.4 appeared first, but in a very special case.

4.3 Complex Projective t-designs

In the previous section we saw that the vectors from a complete system of MUBs satisfy the Welch bounds for $k = 1$ and $k = 2$ with equality. In fact, systems of vectors attaining the Welch bounds have been investigated before. In the majority of papers on the subject, such an object, i.e., a system of complex vectors attaining the Welch bounds for $k = t$, is called a *complex projective t-design.* Because of this, we find it useful to introduce this object, although we are not going to use it in the thesis.

Consider the $(n - 1)$-dimensional complex projective space $\mathbb{C}P^{n-1}$. Its points are the 1-dimensional subspaces of $\mathbb{C}^n$, and its k-dimensional subspace is defined as a set of 1-dimensional subspaces contained in some $(k + 1)$-dimensional subspace of $\mathbb{C}^n$. Another possible visualization of this space is the unit sphere $\mathbb{C}S^{n-1}$ in $\mathbb{C}^n$ factorized under the relation $\equiv$, where $x \equiv y$ if and only if there is an $\alpha \in \mathbb{C}^*$ such that $x = \alpha y$. An equivalence class forms a "circle" in $\mathbb{C}S^{n-1}$. The 1-dimensional subspace of $\mathbb{C}P^{n-1}$ corresponds to the circle of $\mathbb{C}S^{n-1}/\equiv$ it cuts in $\mathbb{C}S^{n-1}$.

Since any unitary operator acting on $\mathbb{C}^n$ transforms 1-dimensional subspaces into 1-dimensional subspaces, we may consider unitaries as acting on $\mathbb{C}P^{n-1}$. There is a unique normalized measure μ on $\mathbb{C}P^{n-1}$ that is invariant under the action of all unitaries on $\mathbb{C}^n$. For any measurable function $f : \mathbb{C}P^{n-1} \to \mathbb{R}$ it can be defined as

$$\int_{\mathbb{C}P^{n-1}} f(x)d\mu(x) = \frac{1}{\sigma(\mathbb{C}S^{n-1})}\int_{\mathbb{C}S^{n-1}} \tilde{f}(y)d\sigma(y)$$

where σ is $(n-1)$-dimensional cubature on $\mathbb{C}S^{n-1}$ and $\tilde{f} : \mathbb{C}S^{n-1} \to \mathbb{R}$ is the function that equals $f(x)$ on all points of $\mathbb{C}S^{n-1} \cap x$.

Denote by $\hom(k,k)$ the set of polynomials in $\mathbb{C}[x_1,x_2,\dots,x_n;y_1,y_2,\dots,y_n]$ homogeneous of degree k in both $\{x_i\}$ and $\{y_i\}$. For any $p\in\hom(k,k)$ and $x\in\mathbb{C}S^{n-1}$ define

$$p(x)=p(x_1,x_2,\dots,x_n;\bar{x}_1,\bar{x}_2,\dots,\bar{x}_n)$$

where $(x_1,x_2,\dots,x_n)$ are coordinates of x in the standard basis. Note that $x\equiv y$ implies $p(x)=p(y)$, hence we can consider p as a function defined on $\mathbb{C}P^{n-1}$.

We define *weighted set* as a pair (X,w) where X is a finite set and $w:X\to\mathbb{R}$ is a *weight function* such that $w(x)\geq 0$ for all x and $\sum_{x\in X}w(x)=1$. (This can be seen as a probability space on X.) A weighted set (X,w) with $X\subset\mathbb{C}P^{n-1}$ is called a *weighted complex projective t-design* if

$$\sum_{x\in X}w(x)p(x)=\int_{\mathbb{C}P^{n-1}}p(x)d\mu(x)$$

for all polynomials $p\in\hom(t,t)$. In other words, a weighted complex projective t-design is a Chebyshev-type averaging set in $\mathbb{C}P^{n-1}$.

If we restrict the weight function to be $w(x)=1/X$ for all x, we obtain a more known concept of (unweighted) complex projective t-design. Thus defined, complex projective t-designs were first considered by Neumaier [43] as a generalization of a spherical t-design [15].

The following result shows why complex projective t-designs falls within the scope of our thesis.

Theorem 4.5. *A weighted set (X,w), $X\subset\mathbb{C}P^{n-1}$ is a weighted complex projective t-design if and only if the set $\{\sqrt[2t]{w(x)}\tilde{x}\mid x\in X\}\in\mathbb{C}^n$ satisfies the Welch bounds for $k=t$ with equality, where $\tilde{x}$ is any vector from $\mathbb{C}S^{n-1}\cap x$.*

The following result is also interesting, and it is easier to formulate in the terms of weighted designs.

Proposition 4.6. *Any weighted complex projective t-design is also a weighted complex projective $(t-1)$-design.*

For the proof of these two results refer, e.g, to [52].

So, we see that unweighted complex projective t-designs are exactly the sets of unit vectors satisfying the Welch bounds for $k=t$ (the normalization factor $\sqrt[2t]{w(x)}$ can be, obviously, omitted). The case of weighted complex projective t-designs is more tricky. The normalization factor $\sqrt[2t]{w(x)}$ depends on t, so, in particular, it is not possible to deduce from Proposition 4.6 that if $X\subset\mathbb{C}^n$ satisfies the Welch bounds for $k=t$, it does so for $k=t-1$ as well. In order to get a similar result, we should renormalise the vectors accordingly to Theorem 4.5. This possibly makes weighted complex projective t-designs a more natural object to investigate. However, in the case of unweighted designs this distinction disappears, and we are going to work only with unweighted designs in the thesis.

Complex projective t-designs are well-studied objects, so it is worth being aware of the equivalence provided by Theorem 4.5. We prefer to talk about Welch bounds, because it is also a well-known object (especially in the engineering literature), it is more elementary (does not require any measure theory) and is adequate for the applications we are interested in. Also it is pretty hard to check that a system of vectors is a complex t-design using just the definition, and this fact is usually checked using the Welch bounds (see [37], for example).

4.4 Link between SIC-POVMs and the Welch Bounds

It turns out that SIC-POVMs also satisfy the Welch bounds for $k = 2$ with equality. In fact an even stronger result holds:

Theorem 4.7. *The vectors from a SIC-POVM satisfy the Welch bounds for $k = 1$ and for $k = 2$ with equality. Conversely, any set X, of normalized vectors of $\mathbb{C}^n$ that attains the Welch bounds for $k = 2$, consists of at least n^2 elements, and if it contains n^2 elements, it is a SIC-POVM.*

Proof. The first part of the theorem is a counting argument. Let $\{x_i\}$ be a SIC-POVM in $\mathbb{C}^n$. It has n^2 vectors, each giving the scalar product 1 with itself and $n^2 - 1$ scalar products of absolute value $\frac{1}{\sqrt{n+1}}$ with other vectors. Summing up, we have for $k = 1$:

$$n \sum_{i,j} |\langle x_i | x_j \rangle|^2 = n \cdot n^2 \left(1 + (n^2 - 1)\frac{1}{n+1}\right) = n^4 = \left(\sum_i \langle x_i | x_i \rangle\right)^2 .$$

And for $k = 2$:

$$\binom{n+1}{2} \sum_{i,j} |\langle x_i | x_j \rangle|^4 = \frac{n(n+1)}{2} n^2 \left(1 + (n^2 - 1)\frac{1}{(n+1)^2}\right) = n^4 = \left(\sum_i \langle x_i | x_i \rangle^2\right)^2 .$$

Conversely, suppose the set $X = \{x_i\} \subset \mathbb{C}^n$ satisfies the Welch bounds for $k = 2$ with all x_i having the unit norm. From Proposition 4.6 is follows that it attains the Welch bounds for $k = 1$ as well. These two equalities give

$$n \sum_{i,j} |\langle x_i | x_j \rangle|^2 = |X|^2 \quad \text{and} \quad \frac{n(n+1)}{2} \sum_{i,j} |\langle x_i | x_j \rangle|^4 = |X|^2.$$

Hence:

$$\sum_{i \neq j} |\langle x_i | x_j \rangle|^2 = \frac{1}{n}|X|^2 - |X| \quad \text{and} \quad \sum_{i \neq j} |\langle x_i | x_j \rangle|^4 = \frac{2}{n(n+1)}|X|^2 - |X|. \tag{4.2}$$

by the inequality between square and arithmetic means (Cauchy-Schwartz) we have:

$$\frac{2}{n(n+1)}|X|^2 - |X| = \sum_{i \neq j} |\langle x_i | x_j \rangle|^4 \geq \frac{1}{|X|(|X| - 1)} \left(\sum_{i \neq j} |\langle x_i | x_j \rangle|^2\right)^2 = \frac{(|X|^2 - n|X|)^2}{n^2|X|(|X| - 1)}. \tag{4.3}$$

This inequality yields that $|X| \geq n^2$ and if $|X| = n^2$ then there is actually an equality in (4.3). This is possible only if all $|\langle x_i | x_j \rangle|$ are all equal for $i \neq j$. It is straightforward then to get from (4.2) that the moduli of these inner products are equal to $\frac{1}{\sqrt{n+1}}$. ■

Remark 4.8. The proof we gave resembles the proof of the same result given in [47]. In fact, this result holds also if we release the condition on the elements of X to be of unit norm (i.e., consider a weighted design). In this case, if X is a set attaining Welch bounds for $k = 2$ with n^2 elements, it is a scalar multiple of a SIC-POVM. In [52] it is shown how this result can be proved using more general results of complex projective t-design theory.

Chapter 5

The Criterion

In this chapter we state the criterion for attaining the Welch bounds and apply it to MUBs and SIC-POVMs. In Section 5.3 we define the special case — homogeneous systems, for which the criterion takes an especially nice form. It suffices to define two $n \times n$-matrices in order to characterize a homogeneous complete system of MUBs or a homogeneous SIC-POVM in the space $\mathbb{C}^n$. For both these matrices we define L-graph of the matrix. It is a simple graph that describes how good is this matrix for constructing homogeneous systems. In Section 5.4 we show that Fourier matrices have very good (in some sense, the best) L-graphs. This explains, to some extent, why Fourier matrices are used in constructions of MUBs and SIC-POVMs.

5.1 Criterion for Attaining the Welch Bounds

We will at first give a proof of the Welch bounds and then extract the equality criterion from the proof.

Proof of Theorem 4.1. Let us construct the Gram matrix $G = (a_{ij})$ with $a_{ij} = \langle x_i | x_j \rangle$ and consider its k-th Hadamard power $G^{(k)}$ (with k being a positive integer). The square of its Euclidean norm is equal to

$$\left(\|G^{(k)}\|_E \right)^2 = \sum_{i,j} |\langle x_i | x_j \rangle|^{2k} = \sum_{\lambda \in \sigma(G^{(k)})} \lambda^2 \tag{5.1}$$

here σ is the spectrum (the multiset of the eigenvalues of a matrix). By the inequality between square and arithmetic means, we have (let us recall that the rank of a matrix is equal to the number of its non-zero eigenvalues):

$$\sum_{\lambda \in \sigma(G^{(k)})} \lambda^2 \geq \frac{1}{\operatorname{rank}(G^{(k)})} (\operatorname{Tr} G^{(k)})^2 \geq \frac{1}{\binom{n+k-1}{k}} \left(\sum_i \langle x_i | x_i \rangle^k \right)^2 . \tag{5.2}$$

We prove the upper bound on the rank of $G^{(k)}$ used above in the proof of Theorem 5.1. ■

Theorem 5.1. *Let B be a matrix and $X \subset \mathbb{C}^n$ be the sequence of its columns. Let $w_1, w_2, \dots, w_n$ be the rows of the matrix. Then X attains the Welch bound for a fixed k if and only if all vectors from*

$$W = \left\{ \sqrt{\binom{k}{k_1, \dots, k_n}} w_1^{(k_1)} \circ w_2^{(k_2)} \circ \cdots \circ w_n^{(k_n)} \mid k_i \in \mathbb{N}_0, k_1 + \cdots + k_n = k \right\}$$

are of equal length and pairwise orthogonal.

In other words, each vector of W is a Hadamard product of a k-multiset of rows of B with a coefficient that is the square root of the multinomial coefficient of the multiset

$$\binom{k}{k_1, \dots, k_n} = \frac{k!}{k_1! k_2! \cdots k_n!}.$$

Proof. At first, let us note that matrix G in (5.1) is equal to $B^\dagger B$. So (if each w_i is treated as a row vector):

$$G = w_1^\dagger w_1 + w_2^\dagger w_2 \cdots + w_n^\dagger w_n.$$

By the formula for a power of a sum, we obtain

$$G^{(k)} = \sum_{k_1 + \cdots + k_n = k} \binom{k}{k_1, \dots, k_n} \left(w_1^{(k_1)} \circ \cdots \circ w_n^{(k_n)} \right)^\dagger \left(w_1^{(k_1)} \circ \cdots \circ w_n^{(k_n)} \right).$$

In other words, $G^{(k)} = C^\dagger C$, where the rows of C are exactly the vectors from W. This gives the bound on the rank of $G^{(k)}$ used in (5.2), because the number of k-multisets of an n-set equals $\binom{n+k-1}{k}$ (see, e.g., Section 1.2 of [54]).

By observing the inequality between (5.1) and (5.2), we see that X satisfies the Welch bound for a fixed k with equality if and only if $G^{(k)}$ has $\binom{n+k-1}{k}$ equal non-zero eigenvalues (all other eigenvalues are automatically zeros due to the rank observations).

It is a well-known fact that for any matrices P and Q the set of non-zero eigenvalues of matrices PQ and QP are equal whenever these two products are defined (see Section 1.3 of [33]). Hence, $CC^\dagger$ has $\binom{n+k-1}{k}$ equal non-zero eigenvalues, and because it is a Hermitian matrix of the same size it is a scalar multiple of the identity matrix. And the latter is equivalent to the requirement on the set W. ■

We haven't hitherto seen the pair of Theorems 4.1 and 5.1 appearing in such a general form, however all ideas involved in the proof have already appeared in the proofs of other results. As we have already said, Welch was the first who derived the bounds (4.1) in the case when all vectors have unit norm and k is arbitrary. It was done in [57]. The variant of Theorem 5.1, with $k = 1$ and all vectors of equal length, seems first to appear in [41]. Our proof is a generalization of an elegant proof found in [56]. In the latter paper the Welch bounds are stated in the case of vectors of different length, but it deals with the case of $k = 1$ only. The definition of a complex projective design in [52] also is quite close to our criterion.

A system $\{x_i\}$ of vectors in $\mathbb{C}^n$ is called a *tight frame* if $\sum_i |x_i\rangle\langle x_i| = aI$ for some $a \in \mathbb{R}$. By taking trace of both parts, it becomes clear that a must be equal to $\frac{1}{n}\sum_i \|x_i\|^2$. In fact, we have seen this object before: the set $\{\frac{1}{a}|x_i\rangle\langle x_i|\}$ is a POVM consisting of rank-one operators for any tight frame $\{x_i\}$, and vice versa.

Proposition 5.2. *Any set $\{x_i\} \subset \mathbb{C}^n$ attaining the Welch Bounds for $k = 1$ is a tight frame.*

Proof. Using the notations of the proof of Theorem 5.1, we have $CC^\dagger = BB^\dagger = aI$ for some $a \in \mathbb{R}$. It remains to notice that $BB^\dagger = \sum_i |x_i\rangle\langle x_i|$. ■

From this proposition and Theorem 4.7 we have the following corollary, which we promised to prove:

Corollary 5.3. *If $\{|x_i\rangle\}$ is a SIC-POVM in $\mathbb{C}^n$ then $\{\frac{1}{n}|x_i\rangle\langle x_i|\}$ is a POVM.*

5.2 Application of the Criterion to MUBs

At first let us state the following easy consequence of Theorem 5.1:

Corollary 5.4. *Let B be a matrix and $X \subset \mathbb{C}^n$ be the sequence of its columns. Let $w_1, w_2, \ldots, w_n$ be the rows of the matrix. Then X satisfy the Welch bound for $k = 2$ with equality if and only if all vectors from $W = \{w_i^{(2)}\} \cup \{\sqrt{2} w_i \circ w_j \mid 1 \leq i < j \leq n\}$ are of*

- *equal length (length condition) and*
- *pairwise orthogonal (orthogonality condition).*

Now we are able to prove the following theorem:

Theorem 5.5. *Let $\{B_i\}$ $(i = 1, 2 \ldots, n)$ be a set of n Hadamards in $\mathbb{C}^n$ and B be a concatenation of these matrices (i.e., an $n \times n^2$-matrix having as columns all columns appearing in $\{B_i\}$). Then $\{B_i\}$ form a complete set of MUHs if and only if all vectors from $W' = \{w_i \circ w_j \mid 1 \leq i \leq j \leq n\}$ are pairwise orthogonal, where $\{w_i\}$ are the rows of B.*

Proof. Let us denote the $n \times n$ identity matrix by B_0. By Theorem 4.4, we see that the set $\{B_0, B_1, \ldots, B_n\}$ is a complete set of MUBs if and only if the set of columns of all these matrices attains the Welch bound for $k = 2$. Now from Corollary 5.4 it follows that it only remains to show that vectors from W, as defined in Corollary 5.4, are of equal length and orthogonal if vectors of W' are orthogonal.

If a vector from W is multiplied by itself using the Hadamard product, the result has one 1 and all other entries equal to 0 in the part corresponding to B_0, and all entries in other parts in absolute value are equal to $\frac{1}{n}$. Hence, the length of the vector is $\sqrt{1 + n^2 \frac{1}{n^2}} = \sqrt{2}$.

If two distinct vectors are multiplied, the result has only zeroes in the first part, and its length is $\sqrt{n^2 \frac{1}{n^2}} = 1$. We thus see that all vectors from W have the same length.

Moreover, the part of B_0 contributes zero to the inner product of 2 distinct vectors of W, hence vectors of W are orthogonal if and only if the corresponding vectors of W' are. ■

Let us restate the last theorem. Suppose B is a flat $n \times n$-matrix. Construct the weighted graph $K(B)$ as follows. Its vertices are all multisets of size 2 from $\{1, ..., n\}$. Semantically, a vertex $\{i, j\}$ represents the Hadamard product of the i-th and the j-th row of B. The weight of an edge is the inner product of the vertices it joins. (Of course, thus defined, the weight depends on the order of the vertices, but let us fix a direction of each edge, say lexicographical). Then Theorem 5.5 can be restated by saying that Hadamards $B_1, \ldots, B_n$ form a set of MUHs in $\mathbb{C}^n$ if and only if for each edge the sum of its weights in $K(B_1), \ldots, K(B_n)$ equals 0. In fact, there is no need to consider edges between vertices that have an element in common, since they will be weighted by 0 in each of $K(B_i)$.

It does not seem that this restatement makes the problem much easier comparing to the initial formulation. However, careful examination of the possible configurations of weights that can be achieved in $K(B)$ may shed some light on the problem. In the next section we consider a special case of systems of MUHs for which Theorem 5.5 yields a considerable simplification.

5.3 Homogeneous Systems

In this section we will describe a special case of systems of MUHs and SIC-POVMs for which the criterion given by corollary 5.4 gains a significant simplification. For SIC-POVMs this construction is a generalization of group covariant SIC-POVMs we have seen in section 3.2.1.

Suppose we have two $n \times n$-matrices $A = (a_{i,j})$ and $B = (b_{i,j})$. Consider the following system of matrices (we do not assume normalization for a moment)

$$(v_k^{(r)})_\ell = a_{\ell,r} b_{\ell,k} \tag{5.3}$$

with r being a matrix index, k being a column index and ℓ being a row index ($r, k, \ell \in \{1, \ldots, n\}$). In other words, the i-th matrix is given by $\operatorname{diag}(v_i)B$, where v_i is the i-th column of A. We will call such a set of matrices a *homogeneous system*. For MUHs, each matrix is a Hadamard. For SIC-POVMs each matrix is a union of n elements of the SIC-POVM, taken as columns. The name is borrowed from [8], where a set of MUHs built of equivalent Hadamards is called a *homogeneous systems of MUHs*.

Note that the complete system of MUHs given in Theorem 3.2 and all group covariant SIC-POVMs are homogeneous systems. In all of them one of matrices A, B is a Fourier matrix. This motivates why we are interested in this construction.

Recall the result of corollary 5.4. Forget for a moment the length condition, and consider only the orthogonality condition. We have:

$$\begin{aligned}\langle w_{\ell_1} \circ w_{\ell_2} | w_{\ell_3} \circ w_{\ell_4} \rangle &= \frac{1}{n} \sum_{r,k} \overline{a_{\ell_1,r} b_{\ell_1,k} a_{\ell_2,r} b_{\ell_2,k}} a_{\ell_3,r} b_{\ell_3,k} a_{\ell_4,r} b_{\ell_4,k} = \\ &= \frac{1}{n} \left(\sum_r \overline{a_{\ell_1,r} a_{\ell_2,r}} a_{\ell_3,r} a_{\ell_4,r} \right) \left(\sum_k \overline{b_{\ell_1,k} b_{\ell_2,k}} b_{\ell_3,k} b_{\ell_4,k} \right)\end{aligned} \tag{5.4}$$

should be equal to zero for all ℓ_1, ℓ_2, ℓ_3 and ℓ_4 such that $\{\ell_1, \ell_2\} \neq \{\ell_3, \ell_4\}$.

Let us define the *L-graph* (denoted $L(A)$) of a matrix A as follows. It is a simple graph with the same set of vertices as $K(A)$, i.e., each vertex is an unordered pair of rows of the matrix A, the pair may consist of the same row counted twice. We will denote vertices of $L(A)$ by unordered pair of indices of rows. Two vertices $\{a, b\}$ and $\{c, d\}$ are adjacent if ond only if $R_a \circ R_b \perp R_c \circ R_d$ where R_a is the row of A with index a. We will call two L-graphs

$L(A)$ and $L(B)$ *isomorphic* if there is a bijection σ from the set of rows of A onto the set of rows of B such that, for all a, b, c, d, vertices $\{a, b\}$ and $\{c, d\}$ of $L(A)$ are connected if and only if the vertices $\{\sigma(a), \sigma(b)\}$ and $\{\sigma(c), \sigma(d)\}$ are connected in $L(B)$.

Identity (5.4) leads to the following observation:

Proposition 5.6. *The homogeneous system given by (5.3) satisfies the orthogonality condition of Corollary 5.4 if and only if the graphs $L(A)$ and $L(B)$ together cover the complete graph.*

If we consider the complete systems of MUHs, Theorem 5.5 says what matrices A and B should be. We will fix B to be a complex Hadamard matrix, and A to be an ordinary flat matrix. Then Theorem 5.5 and Proposition 5.6 tell us that the system given by (5.3) gives a complete system of MUHs if and only if $L(A)$ and $L(B)$ cover the complete graph.

In the case of SIC-POVMs we are not that restricted, however we will restrict us ourselves by fixing B to be a flat matrix. We will work out conditions on A in the next chapter.

Sometimes it is more convenient to use graph $\tilde{L}(A)$ instead of $L(A)$. Its vertices are *ordered* pairs of rows and two vertices are adjacent if and only if the Hadamard product of rows in the first pair is orthogonal to the Hadamard product of rows in the second pair. Graph-theoretically, the graph $\tilde{L}(A)$ can be obtained from $L(A)$ by splitting each vertex $\{a, b\}$ with $a \neq b$ into two non-adjacent vertices: (a, b) and (b, a).

If matrices A and B satisfy the conditions of Proposition 5.6 and A' and B' are such that $L(A)$ is a spanning subgraph of $L(A')$ and the same holds for $L(B)$ and $L(B')$, then A' and B' also satisfy the conditions of Proposition 5.6. Hence, if the length condition of Corollary 5.4 is satisfied, we may consider only matrices with maximal L-graphs. We will call them *L-maximal matrices.* We will use notion *L-maximal Hadamard matrix* (*L-maximal flat matrix*) for a matrix A that is Hadamard (respectively, flat) and such that $L(A)$ is not a proper subgraph of $L(B)$ for any Hadamard (respectively, flat) matrix B.

Clearly, a matrix A is L-maximal if and only if $\tilde{L}(A)$ is maximal. For the study of homogeneous systems of MUHs the following question is of great importance:

Open Problem 5.7. *Describe L-maximal flat and Hadamard matrices and the corresponding graphs.*

In the case of homogeneous SIC-POVMs we are interested in the maximal flat matrices. Anyway, it is already clear that L-maximal matrices cover L-maximal flat matrices, and they cover L-maximal Hadamard matrices (because a Hadamard matrix is a special case of a flat matrix, and the latter is a special case of a general matrix).

There is an important class of L-maximal Hadamard (and even general) matrices. These are the Fourier matrices we have introduced in Section 2.2.

5.4 Fourier Matrices in Homogeneous Systems

Let A be a $n \times n$-matrix and $L(A)$ be its L-graph. The vertices of the graph correspond to vectors of $\mathbb{C}^n$ and two vertices are adjacent if and only if the corresponding vectors are orthogonal. A more general notion would be of a graph T whose vertices are arbitrary vectors of $\mathbb{C}^n$ and two vertices are adjacent if and only if the vectors are orthogonal.

Let G be a graph. Let us recall some concepts from graph theory (see, e.g. [17]). An *independent set* of G is an induced edgeless subgraph of G, i.e. a subset of vertices such that no two vertices in it are connected by an edge. On contrary, a *clique* is an induced complete subgraph of G, i.e. a set of vertices that are all pairwise connected. The *independence number* $\alpha(G)$ is the size of a largest independent set of G and the *clique number* $\omega(G)$ is the size of a largest clique of G.

The minimal number of colours that can be assigned to the vertices of the graph in such a way that any two adjacent vertices are coloured in different colours, is called the *chromatic number* $\chi(G)$ of the graph. It is easy to see that $\chi(G) \geq \omega(G)$, because all vertices of a clique must be coloured in different colours.

The following lemma is obvious.

Lemma 5.8. *Let T be a graph whose vertices are arbitrary non-zero vectors of $\mathbb{C}^n$ and two vertices are adjacent if and only if the vectors are orthogonal. Then $\omega(G) \leq n$.*

Let F be the Fourier matrix of a group G, and $\{R_i\}$ be the set of its rows. Recall (Proposition 2.5) that the rows of F are pairwise orthogonal and form a group under Hadamard product isomorphic to G. Hence, vertices $\{a, b\}$ and $\{c, d\}$ of $L(F)$ are connected if and only if $a + b \neq c + d$.

Theorem 5.9. *A Fourier matrix F is an L-maximal matrix. In particular, it is an L-maximal Hadamard matrix. Moreover, $\tilde{L}(F)$ has maximal possible number of edges among $\tilde{L}(A)$ for all $n \times n$-matrices A.*

For any Hadamard matrix H, such that $\tilde{L}(H)$ has that many edges, the graph $L(H)$ is isomorphic to an L-graph of a Fourier matrix.

Proof. Let A be any $n \times n$-matrix and F be a Fourier $n \times n$-matrix. From Lemma 5.8 we have $\omega(\tilde{L}(A)) \leq n$. Recall that *Turán graph* $T^r(n)$ (see Section 7.1 of [17]) is the unique complete r-partite graph on n-vertices whose partition sets differ in size by at most 1. In particular, if r divides n then all partition sets are of size $\frac{n}{r}$. Turán graph $T^r(n)$ has the largest number of edges among all graphs on n vertices with clique number r.

So, the L-maximality of a Fourier matrix follows from the fact that $\tilde{L}(F)$ is a Turán graph $T^n(n^2)$.

Let H be a Hadamard $n \times n$-matrix. Denote the rows of H by $\{R_i\}$, $i = 0, 1, \ldots, n-1$. Rescaling of columns by unit modulus scalars does not change the L-graph, so we may always assume that R_0 consists only of ones.

For a fixed i the set $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$ is an orthogonal basis of $\mathbb{C}^n$. Hence, any $R_a \circ R_b$ is not orthogonal to at least one of $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$. If H is a Fourier matrix, then $R_a \circ R_b$ is not orthogonal to exactly one of $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$: the one with $i + j = a + b$.

If $\tilde{L}(H)$ has maximal possible number of edges, then it is a Turán graph $T^n(n^2)$, hence each vertex is not adjacent to exactly n vertices (including itself). Thus, any $R_a \circ R_b$ is not orthogonal to exactly one of $\{R_i \circ R_j \mid j = 0, \ldots, n-1\}$ for each i and, in particular, is not orthogonal to exactly one of $\{R_i\}$ (since R_0 consists solely of ones). This means that $R_a \circ R_b = \alpha R_i$ for some i and $\alpha \in \mathbb{C}^*$.

Let G be the set of directions (equivalence classes of collinear vectors) defined by rows of H with the Hadamard product operation. The set is finite, it is closed under the operation,

R_0 is the identity element, the operation is commutative and associative and for any fixed i the operation $R_j \mapsto R_i \circ R_j$ is a bijection. Hence, G is a finite Abelian group, and $L(H)$ is isomorphic to the L-graph of the Fourier matrix of G. ■

This result explains why Fourier matrices are so useful in the constructions of MUBs and SIC-POVMs. Indeed, the L-graph of a Fourier matrix covers a fraction of roughly $\frac{n-1}{n}$ edges of the complete graph, so it remains to find the second matrix A that covers the remaining fraction of $\frac{1}{n}$ edges. It can be conjectured that Fourier matrices are the only L-maximal Hadamard matrices. However, it is not hard to show that there are other L-maximal flat matrices. For example, consider the Fourier matrix F and a flat matrix A in $\mathbb{C}^3$ given by

$$F = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3 \end{pmatrix} \quad A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3 & \omega_3^2 \end{pmatrix}. \tag{5.5}$$

The corresponding L-graphs are given in Figure 5.1. The bold edges in the second graph are the only edges not covered by $L(F)$. Thus, these two graphs cover the complete graph. Note that none of bold edges can be covered by the L-graph of a Hadamard matrix. Indeed, suppose edge $\{0,0\}\{1,2\}$ belongs to the L-graph of a Hadamard matrix. Then these two vertices together with $\{0,1\}$ and $\{0,2\}$ form K_4 — a complete graph on 4 vertices, but this is impossible.

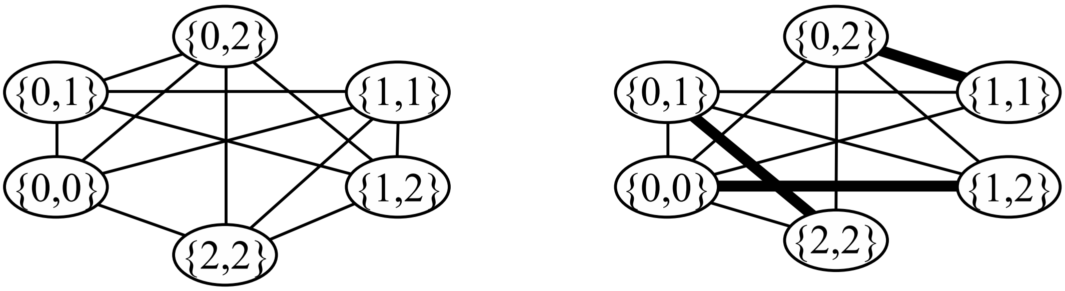

Figure 5.1: The L-graphs of matrices F (on the left) and A (on the right) given in (5.5).

In this case $L(F)$ is a Turán graph itself, but this is not always the case. For example, $L(F_2^{\otimes k})$ has an independent set of size 2^k, where F_2 is as in (2.3). That is why we considered the graph $\tilde{L}(F)$ in the proof of Theorem 5.9.

Inspired by the number of edges in $L(F)$, it may seem that the task of finding the second matrix should be easy, but it is not. A notable property of a Fourier matrix F is that $\chi(L(F)) = n$ (a colour of a vertex $\{a, b\}$ is $a + b$). In particular, it means that if one found an $n \times n$ Hadamard matrix H such that $\chi(L(H)) > n$, it would not be covered by any Fourier matrix, and the conjecture that Fourier matrices are the only L-maximal Hadamard matrices would be false. But we do not know any Hadamard matrix with such a property.

For a general graph G the inequality $\alpha(G) \geq \frac{n(G)}{\chi(G)}$ holds ($n(G)$ is the number of vertices in G; the inequality follows from the fact that vertices with the same colour form an independent set). Thus, small chromatic number implies large independence number, and, hence, the second matrix, in order to satisfy the conditions of Proposition 5.6 should have large clique number. And that may result in troubles finding the second matrix. We will make this observation more robust in Proposition 5.10. Thus, Hadamard matrices H with large $\chi(L(H))$ and small $\alpha(L(H))$ (if there are any) could be useful while constructing complete systems of MUHs.

It seems worth mentioning some constructions that are similar to the notion of L-graphs (i.e., when the adjacency relation on the set of vectors is generated using the orthogonality relation). One example known to us is *Hadamard graph* defined in [34]. The set of vertices of the Hadamard graph $S(n)$ of order n is the set of all ± 1-component vectors of length n, and two vectors are adjacent iff they are orthogonal. The famous Hadamard conjecture is equivalent to the statement that $\omega(S(4n)) = 4n$ for any positive integer n. It is proved in [22] that there is an exponential gap between $4n$ and $\chi(S(4n))$. So, it is quite possible that for some Hadamard matrix H we would have $\chi(L(B)) > n$, and it would not be possible to covered it by a Fourier matrix.

In the absence of a better alternative we will assume further that B is the Fourier matrix of a finite Abelian group G. In this case, it is easy to see that a matrix A and B satisfy the conditions of Proposition 5.6 if and only if

$$\forall g_1, g_2, g_3, g_4 \in G : \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow R_{g_1} \circ R_{g_2} \perp R_{g_3} \circ R_{g_4}, \tag{5.6}$$

where R_i is the i-th row of A. This condition can be rewritten in the following way.

Proposition 5.10. *Let B be the Fourier matrix of a group G and A be a matrix with rows $\{R_i\}_{i \in G}$. These two matrices satisfy the conditions of Proposition 5.6 if and only if for any non-zero $\Delta \in G$ the rows*

$$\{R_{i+\Delta} \circ \overline{R_i} \mid i \in G\}$$

of matrix D_Δ are pairwise orthogonal.

Proof. Suppose A and B satisfy the conditions. Let us take $g_1 \neq g_3$. Then

$$\langle R_{g_1+\Delta} \circ \overline{R_{g_1}} | R_{g_3+\Delta} \circ \overline{R_{g_3}} \rangle = \langle R_{g_1+\Delta} \circ R_{g_3} | R_{g_3+\Delta} \circ R_{g_1} \rangle.$$

Moreover, $(g_1 + \Delta) + g_3 = (g_3 + \Delta) + g_1$, $g_3 \neq g_1$ and $g_3 \neq g_3 + \Delta$. Using (5.6) with $g_2 = g_3 + \Delta$ and $g_4 = g_1 + \Delta$, we have $R_{g_1+\Delta} \circ \overline{R_{g_1}} \perp R_{g_2+\Delta} \circ \overline{R_{g_2}}$.

The proof of the converse statement is similar. ■

Note that if D_Δ has orthogonal rows then $D_{-\Delta}$ has orthogonal rows as well. This allows to reduce the search in some cases.

Chapter 6

Searching for Moduli

In this chapter we will give conditions on the absolute values of elements of matrices A and B in (5.3) in order to satisfy the length condition of Corollary 5.4. As it was noticed in the previous chapter, Theorem 5.5 implies that in the case of homogeneous system of MUHs it suffices to assume that A is a flat matrix and B is a complex Hadamard matrix, and the question on the absolute values of A and B is exhausted. So, in this chapter we will concentrate on SIC-POVMs.

Theorem 6.1. *Suppose we are looking for a SIC-POVM in the homogeneous settings (5.3) with B being the Fourier matrix of a group G. In this case matrix A must satisfy*

1. *each column of A is of unit norm;*

2. *each row R_i is of unit norm;*

3. *for all i, j, k such that $j \neq k$: $\|R_i^{(2)}\| = \sqrt{2}\|R_j \circ R_k\|$;*

4. *for all $g_1, g_2, g_3, g_4 \in G$ such that $g_1 + g_2 = g_3 + g_4$ and $\{g_1, g_2\} \neq \{g_3, g_4\}$ the vectors $R_{g_1} \circ R_{g_2}$ and $R_{g_3} \circ R_{g_4}$ are orthogonal;*

where, as usually, R_i is the row of A indexed with element $i \in G$.

Proof. Condition 1 must be satisfied because of the definition of a SIC-POVM. In notations of Corollary 5.4 let w_i be the row of B corresponding to $i \in G$. From (5.3), since each element of B has absolute value 1, it follows that $\|w_i \circ w_j\| = \sqrt{n}\|R_i \circ R_j\|$ (each entry of $R_i \circ R_j$ is repeated, up to a phase, n times, one for each column of B). Then Condition 3 follows from the length condition of Corollary 5.4. Condition 4 is a paraphrasing of (5.6).

Condition 2 possibly requires more comments. As stated in Theorem 4.7, vectors of a SIC-POVM attain the Welch bound for $k = 1$. From Theorem 5.1 we have $\|w_i\| = \|w_j\|$ for all $i, j \in G$. Then, as for Condition 3, we have $\|R_i\| = \|R_j\|$. Since each column of A has norm 1, it follows that each row is also of norm 1.■

Let us make the following remark that binds homogeneous SIC-POVMs with another special case of SIC-POVMs.

Remark 6.2. If matrix A satisfies the conditions of Theorem 6.1 and is, moreover, circulant with respect to G, then the SIC-POVM given by (5.3) is group covariant with respect to $\mathrm{GP}(G)$.

As already said, in this chapter we are not interested in Condition 4, leaving it for the next chapter. Since all other conditions only deal with norms of vectors, we may replace $A = (a_{ij})$ by the matrix $M = (m_{ij})$ composed of its element-wise absolute values: $m_{ij} = |a_{ij}|$. All entries of M are non-negative real numbers.

From Remark 4.8 and Corollary 5.4, Conditions 3 and 4 are sufficient for the the constructed system of vectors to be a scalar multiple of a SIC-POVM. We have added Conditions 1 and 2 to the list in order to narrow the class of matrices M, that corresponds to some A satisfying Condition 4, as much as possible.

Let us start with a more detailed treatment of the problem. Denote by y_{ij} the (i, j)-th element of the matrix $M^{(2)}$, i.e., $y_{ij} = m_{ij}^2$. Then Conditions 1 and 2 of Theorem 6.1 imply, respectively,

$$\sum_i y_{ij} = 1 \quad \text{and} \quad \sum_j y_{ij} = 1. \tag{6.1}$$

Condition 3 means that

$$\sum_j y_{ij}^2 = 2 \sum_j y_{kj} y_{\ell j}$$

for all i, k, ℓ such that $k \neq \ell$. Combining it together, we get

$$n = \sum_j \left(\sum_i y_{ij} \right)^2 = \sum_{i,j} y_{ij}^2 + 2 \sum_{i<k} \sum_j y_{ij} y_{kj} = \left(n + \frac{n(n-1)}{2} \right) \sum_j y_{ij}^2. \tag{6.2}$$

Hence,

$$\sum_j y_{ij}^2 = \frac{2}{n+1}, \quad \text{and} \quad \sum_j y_{kj} y_{\ell j} = \frac{1}{n+1}. \tag{6.3}$$

Denote by y_i the vector $(y_{i1}, y_{i2}, \dots, y_{in})$, define a vector $e = \left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}\right)$ and set $\tilde{y}_i = y_i - e$. It is easy to see that (6.1) implies $\tilde{y}_i \perp e$ for all i. So,

$$\frac{2}{n+1} = \langle y_i | y_i \rangle = \langle \tilde{y}_i + e | \tilde{y}_i + e \rangle = \langle \tilde{y}_i | \tilde{y}_i \rangle + \frac{1}{n}$$

for all i. And for any $i \neq j$:

$$\frac{1}{n+1} = \langle y_i | y_j \rangle = \langle \tilde{y}_i + e | \tilde{y}_j + e \rangle = \langle \tilde{y}_i | \tilde{y}_j \rangle + \frac{1}{n}.$$

Hence,

$$\langle \tilde{y}_i | \tilde{y}_i \rangle = \frac{n-1}{n(n+1)} \quad \text{and} \quad \langle \tilde{y}_i | \tilde{y}_j \rangle = -\frac{1}{n(n+1)} \quad \text{for any } i \neq j.$$

So, it is easy to see that $\{\tilde{y}_i\}$ are vertices of a regular $(n-1)$-dimensional simplex embedded in the hyperplane orthogonal to e, and scaled by $\sqrt{\frac{n-1}{n(n+1)}}$. The simplex $\mathcal{Y}$, spanned by $\{y_i\}$, is additionally translated by e. Because all y_i should be non-negative, $\mathcal{Y}$

must be contained in the larger regular simplex $\mathcal{S}$ spanned by the elements of the standard basis of $\mathbb{R}^n$. The latter simplex is also centred at e and its radius is

$$\sqrt{(n-1)\frac{1}{n^2}+\frac{(n-1)^2}{n^2}}=\sqrt{\frac{n-1}{n}}.$$

Since the size of $\mathcal{Y}$ is smaller than the size of $\mathcal{S}$, the former can always be put in the latter. An easy way to do that is to scale $\mathcal{S}$ by $1/\sqrt{n+1}$ with centre in e. The resulting simplex is spanned by

$$\left(\frac{1}{n}+\frac{n-1}{n\sqrt{n+1}},\frac{1}{n}-\frac{1}{n\sqrt{n+1}},\frac{1}{n}-\frac{1}{n\sqrt{n+1}},\dots,\frac{1}{n}-\frac{1}{n\sqrt{n+1}}\right) \tag{6.4}$$

and its circular permutations.

Careful analysis of the calculations we have just made reveals the following

Theorem 6.3. *Let M be a matrix satisfying Conditions 1, 2 and 3 of Theorem 6.1. Then the rows of the Hadamard square of M form a regular $(n-1)$-dimensional simplex $\mathcal{Y}$, of radius $\sqrt{\frac{n-1}{n(n+1)}}$, centred at $\left(\frac{1}{n},\frac{1}{n},\dots,\frac{1}{n}\right)$ and contained in the $(n-1)$-dimensional simplex $\mathcal{S}$ spanned by the elements of the standard basis. And conversely, any such simplex $\mathcal{Y}$ corresponds to a matrix M satisfying Conditions 1, 2 and 3.*

Proof. We have just shown one direction of the Theorem. For the converse statement, note that Condition 2 follows from the fact all vertices of the simplex $\mathcal{Y}$ are located in the hyperplane $\sum_j y_j = 1$. Condition 3 follows from reversing our calculations after (6.3). Then by (6.2) we have $\sum_j\left(\sum_i y_{ij}\right)^2 = n$. And by the inequality between square and arithmetic means we have

$$\sum_j\left(\sum_i y_{ij}\right)^2 \geq \frac{1}{n}\left(\sum_{i,j} y_{ij}\right)^2 = n$$

with equality if and only if all $\sum_i y_{ij}$ are equal. Hence, Condition 1 is also satisfied. ■

Let us now consider circulant matrices M satisfying Conditions 1,2 and 3. We are interested in circulant matrices because, for one, such matrices appear in group covariant SIC-POVMs. Secondly, the case of circulant M sometimes makes the analysis of Condition 4 that we do in the next chapter easier.

Let $G = \mathbb{Z}_{d_1}\times\mathbb{Z}_{d_2}\times\cdots\times\mathbb{Z}_{d_m}$. We will call simplex $\mathcal{Y}$ *circulant over* G, if the corresponding matrix M is circulant over G (we assume also that M is non-negative). Such simplices always exist. In particular, the simplex given by (6.4) is circulant for any group G. We will now show how to obtain all other circulant simplices from this one.

The rows and columns of matrix M are indexed by elements of G, so we may suppose that the standard basis of the space in which simplex $\mathcal{Y}$ is located is also indexed with elements of G. Let V_i be the transformation that maps the vector of the standard basis that corresponds to the element $(a_1, a_2, \dots, a_m)\in G$ to the vector of the standard basis corresponding to $(a_1, a_2, \dots, a_{i-1}, a_i + 1, a_{i+1}, \dots, a_m)\in G$. In other words,

$$V_i = I_{d_1}\otimes I_{d_2}\otimes\cdots\otimes I_{d_{i-1}}\otimes X_{d_i}\otimes I_{d_{i+1}}\otimes\cdots\otimes I_{d_m} \tag{6.5}$$

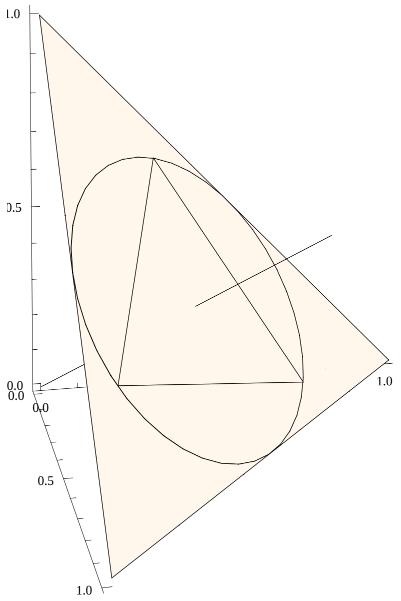

Figure 6.1: Circulant simplices for $G = \mathbb{Z}_3$. The circulant simplex $\mathcal{Y}$ is embedded in the larger simplex $\mathcal{S}$. The simplex $\mathcal{Y}$ can be rotated around the vector e by an arbitrary angle, and vertices of $\mathcal{Y}$ fill out the circle $\mathcal{C}$. In this case, $\mathcal{Y}$ stays in $\mathcal{S}$ for any rotation, and any simplex $\mathcal{Y}$ as in Theorem 6.3 is circulant.

where I_n is the $n \times n$ identity matrix, and X_n is as defined in Section 2.3. Note that all $\{V_i\}$ are orthogonal linear operations and they commute.

Let $\mathcal{Y}$ be a circulant simplex with respect to G (for example, one given by (6.4)). For simplicity, we will consider simplices $\tilde{\mathcal{Y}} = \mathcal{Y} - e$ and $\tilde{\mathcal{S}} = \mathcal{S} - e$, both centred at zero (i.e., consider vectors $\tilde{y}$ instead of y). Denote by $\mathcal{H}$ the hyperplane perpendicular to the vector e. Note that all operators V_i have e as an eigenvector with eigenvalue 1. Hence, $\mathcal{H}$ is an invariant subspace for all V_i and we may consider the induced operators $V_i|_{\mathcal{H}}$. For simplicity, we will still denote them by V_i.

Fix an arbitrary vertex v of $\tilde{\mathcal{Y}}$. Clearly, using operators $V_1, V_2, \ldots, V_m$ we can map v to any other vertex of the simplex. Now suppose that w is a vertex of another circulant simplex $\tilde{\mathcal{Y}}' = \mathcal{Y}' - e$ centred at zero. Let U be the linear operator that maps $V_1^{a_1} V_2^{a_2} \cdots V_m^{a_m} v$ to $V_1^{a_1} V_2^{a_2} \cdots V_m^{a_m} w$ for any $(a_1, a_2, \ldots, a_m) \in G$. This is an orthogonal operator and it commutes with all V_i. And vice versa, if U is an orthogonal operator that commutes with all V_i, then $U\tilde{\mathcal{Y}}$ is also a circulant simplex as long as it fits in $\tilde{\mathcal{S}}$. It is enough to assure that all components of $Uv + e$ are non-negative, because the components of other vertices of $\mathcal{Y}$ are just permutations of $Uv + e$. In addition, we may always assume that $Ue = e$. This gives the following theorem.

Theorem 6.4. *Suppose U is an orthogonal operator in $\mathbb{R}^n$ such that $Ue = e$, and $\mathcal{Y}$ is a*

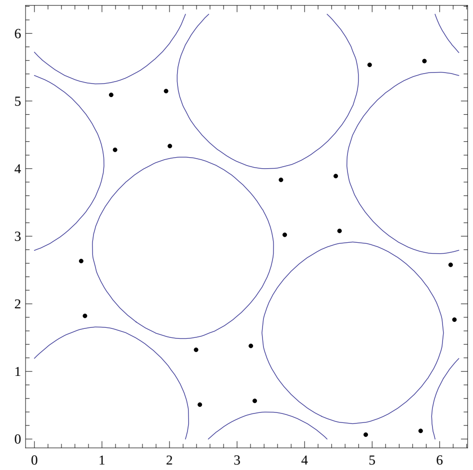

Figure 6.2: Circulant simplices for $G = \mathbb{Z}_5$. As we have seen, in this case all circulant simplices can be parametrized using two real parameters φ_1 and φ_2 that correspond to rotation angles in two planes. On the axes the values of φ_1 and φ_2 are represented. The points inside 'circles' correspond to simplices that do not fit in $\mathcal{S}$. Also vectors, that correspond to a fiducial vector in (3.6) and its linear permutations, are marked.

circulant simplex in $\mathbb{R}^n$ with respect to G (e.g., one given by (6.4)). Then $U\mathcal{Y}$ is circulant if and only if it fits in $\mathcal{S}$ and U commutes with all V_i defined in (6.5).

Consider the case of $\mathbb{Z}_n$ that appears in the case of group covariant SIC-POVMs. In this case we have just one operator $V_1 = X_n$. It is well known that as a real linear operator X_n performs rotations by angle $2\pi/k$ in the planes spanned by

$$\left(1, \cos\frac{2\pi k}{n}, \cos\frac{4\pi k}{n}, \ldots, \cos\frac{2(n-1)\pi k}{n}\right) \quad \text{and} \quad \left(0, \sin\frac{2\pi k}{k}, \sin\frac{4\pi k}{n}, \ldots, \sin\frac{2(n-1)\pi k}{n}\right)$$

for $k = 1, \ldots, \left\lfloor \frac{n-1}{2} \right\rfloor$ and, if n is even, negation in the space spanned by

$$(1, -1, 1, -1, \ldots, 1, -1).$$

Hence, $U\tilde{\mathcal{Y}}$ will give a circulant simplex for a unitary U that performs a rotation by an arbitrary angle in the same planes and possibly, if n is even, negation in the space spanned by $(1, -1, 1, -1, \ldots, 1, -1)$. So, all circulant simplices with respect to $\mathbb{Z}_n$ can be parametrised using $\left\lfloor \frac{n-1}{2} \right\rfloor$ real parameters. The case of $\mathbb{Z}_3$ is illustrated in Figure 6.1.

As n grows, the ratio between radii of $\mathcal{S}$ and $\mathcal{Y}$ grows as $O(\sqrt{n})$. However, the ratio of radius of $\mathcal{S}$ and the distance between the centre of $\mathcal{S}$ and the border of $\mathcal{S}$ grows faster — as $O(n)$. Indeed, $(\frac{1}{n}, -\frac{1}{n}, 0, 0, \ldots, 0)$ is the shortest vector that can be added to e to get a point on the border of $\mathcal{S}$. This means that for large n rotations of $\mathcal{Y}$ often will not fit in $\mathcal{S}$. As we have seen in Figure 6.1, for $n = 3$ the simplex $\mathcal{Y}$ is always contained in $\mathcal{S}$, but for $n = 5$ this is not always the case. See Figure 6.2.

In a similar way circulant simplices for other groups can be described.

Chapter 7

Searching for Phases

In this chapter we will be interested in the following question. Given an $n \times n$-matrix M consisting of non-negative real numbers and a finite Abelian group G, we want to construct a flat matrix P such that $A = M \circ P$ satisfies the condition (5.6). If such a matrix P exists, we call matrix M *satisfiable* over G. Moreover, as motivated in the previous chapter, we will consider only matrices M that are circulant with respect to G. Then matrix A is circulant if and only if the flat matrix P is circulant over G. So, if we say that a circulant matrix M is satisfiable over G we implicitly assume that M is circulant with respect to G.

The motivation for searching the matrix P is as follows. Suppose we want to build a complex projective 2-design using a homogeneous construction as in (5.3). We use the Fourier matrix of a group G as the matrix B because of its good properties. We apply Corollary 5.4 to get the conditions on the absolute values of the entries in the second matrix (as in the previous chapter). Suppose M satisfies these conditions. Then we want to finish the construction by finding phases such that the conditions of Corollary 5.4 hold to the full extent.

In particular, if we take M to have all entries equal to 1, we get a complete system of MUHs if M is satisfiable. If M is like a matrix in the previous chapter, we get a SIC-POVM. So, for MUHs we get one possible matrix M of very simple structure, for SIC-POVMs we have a larger choice of matrices M, but not that simple. This is in agreement with the actual situation. Complete systems of MUHs have been constructed in all dimensions in which they are believed to exist; SIC-POVMs are not, but they are believed to exist in all dimensions, which is not true for MUHs.

Let us start with a simple example of satisfiability.

Proposition 7.1. *A circulant matrix with the first row (a, b, c) is satisfiable over $\mathbb{Z}_3$ if and only if either one of $\{a, b, c\}$ is equal to 0, or a, b, c satisfy the triangle inequality, i.e., $2\max\{a, b, c\} \le a + b + c$. Moreover, if these conditions are satisfied, P can be taken to be circulant.*

Proof. In the group G_3 we have $g_1 + g_2 = g_3 + g_4$ and $\{g_1, g_2\} \ne \{g_3, g_4\}$ if and only if $g_1 = g_2$ and $\{g_3, g_4\} = \mathbb{Z}_3 \setminus \{g_2\}$ or vice versa. For the matrix to satisfy (5.6), the vector $\overline{R_{g_1} \circ R_{g_2}} \circ R_{g_3} \circ R_{g_4}$ should sum up to zero. The vector of the absolute values of the elements of this vector is, up to a permutation, $abc(a, b, c)$.

If $abc = 0$ then $M \circ P$ satisfies the condition for *any* flat matrix P.

Otherwise, it is clear that a, b, c must satisfy the triangle inequality. Suppose they do. In this case let $\varphi_0, \varphi_1, \varphi_2 \in [0, 2\pi)$ be such that $ae^{\mathbf{i}\varphi_0} + be^{\mathbf{i}\varphi_1} + ce^{\mathbf{i}\varphi_2} = 0$. It is now easy to check that the circulant matrix P with the first row $(e^{\mathbf{i}\varphi_0/3}, e^{\mathbf{i}\varphi_1/3}, e^{\mathbf{i}\varphi_2/3})$ satisfies the condition. Indeed, suppose $g_1 = g_2 = 0$, $g_3 = 1$ and $g_4 = 2$. Then

$$\langle R_0 \circ R_0 | R_1 \circ R_2 \rangle = abc\left(ae^{(\mathbf{i}/3)(\varphi_1+\varphi_2-2\varphi_0)} + be^{(\mathbf{i}/3)(\varphi_0+\varphi_2-2\varphi_1)} + ce^{(\mathbf{i}/3)(\varphi_0+\varphi_1-2\varphi_2)}\right) =$$

$$= abce^{(\mathbf{i}/3)(\varphi_0+\varphi_1+\varphi_2)}\left(ae^{-\mathbf{i}\varphi_0} + be^{-\mathbf{i}\varphi_1} + ce^{-\mathbf{i}\varphi_2}\right) = 0.$$

Other cases can be checked similarly. ■

Using this proposition and the analysis at the end of the previous chapter, it is possible to build some SIC-POVMs in dimension 3. As we have seen in Figure 6.1, the vector of squares of the absolute values of the elements of the first row of M lies on the circle $\mathcal{C}$ of radius $\frac{1}{\sqrt{6}}$ centred at $e = (\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ and perpendicular to e. Moreover, this circle lies completely inside $\mathcal{S}$, hence all components of any point on the circle are non-negative. Now we will show that the circle $\mathcal{C}$ consists of extreme points, whose square roots satisfy the triangle inequality. In other words, for all points $(x, y, z) \in \mathcal{S}$, inside or on the border of $\mathcal{C}$, the inequality $\sqrt{x} + \sqrt{y} + \sqrt{z} \geq 2\max\{\sqrt{x}, \sqrt{y}, \sqrt{z}\}$ is satisfied, for all points outside the circle — is not.

Indeed, from equalities $\sqrt{x} + \sqrt{y} + \sqrt{z} = 2\max\{\sqrt{x}, \sqrt{y}, \sqrt{z}\}$ and $x + y + z = 1$ we have

$$\sqrt{x} = \pm(\sqrt{y} \pm \sqrt{z}).$$

Taking the square, rearranging and taking the square once more:

$$\begin{aligned} & x - y - z = \pm 2\sqrt{yz} \\ \Longrightarrow\quad & x^2 + y^2 + z^2 = 2xy + 2xz + 2yz \\ \Longrightarrow\quad & 2x^2 + 2y^2 + 2z^2 = 1, \end{aligned}$$

because $(x + y + z)^2 = 1$. Dividing by 2 and rearranging the terms, we have

$$x^2 + y^2 + z^2 - \frac{2}{3}(x + y + z) + 3\frac{1}{9} = \frac{1}{6}$$

$$\left(x - \frac{1}{3}\right)^2 + \left(y - \frac{1}{3}\right)^2 + \left(z - \frac{1}{3}\right)^2 = \frac{1}{6}.$$

Thus, we can get a SIC-POVM from any point on $\mathcal{C}$ using Proposition 7.1. For points on the intersection of $\mathcal{C}$ and the border of $\mathcal{S}$, we can even take an arbitrary P. Because we can always take a circulant P, any point on $\mathcal{C}$ gives a fiducial vector.

7.1 Group Covariant SIC-POVMs

Let us return to group covariant SIC-POVMs for a moment. To get a group covariant SIC-POVM, not only must the matrix M be circulant, so should P as well. Let x be the first row of $A = P \circ M$. If we reverse this vector, we get a column of A, so if the SIC-POVM is group covariant, x is a fiducial vector.

By denoting $g_1 = j, g_2 = j + k + l, g_3 = j + k, g_4 = j + l$ in Condition 4 of Theorem 6.1 and using (6.3), it is not hard to deduce that $x = (x_i)$ is a fiducial vector if and only if

$$\sum_{j=0}^{n-1} \overline{x_j} x_{j+k} x_{j+l} \overline{x_{j+k+l}} = \frac{1}{n+1}(\delta_{k,0} + \delta_{l,0})$$

where $\delta_{a,b}$ is Kronecker delta, that is equal to 1, if $a = b$, and equal to 0, otherwise. This was proved independently in [4] and [36] using another techniques.

Denote $X = X_n$, $Z = Z_n$, $F = F_n$, $R = R_n$ as in Section 2.3. From Proposition 5.10 we know that matrices $D_\triangle$ have orthogonal rows. In the case of group covariant SIC-POVMs, the rows of $D_\triangle$ are given by $\{(X^{i+\triangle}x) \circ \overline{(X^i x)} \mid i \in \mathbb{Z}_n\}$. Notice that $D_\triangle$ is circulant. Hence (by Theorem 2.8), it has orthogonal rows if and only if the Fourier transform of the 0-th row $\bar{x} \circ (X^\triangle x)$ is flat. Let us calculate the Fourier transform:

$$F(\bar{x} \circ (X^\triangle x)) = \frac{1}{n}(F\bar{x}) \star (FX^\triangle x) = \frac{1}{n}(R\overline{Fx}) \star (Z^\triangle Fx).$$

The k-th component of this vector is nothing else but $\frac{1}{n}\langle X^k Fx | Z^\triangle Fx\rangle$. So, the condition on phases (Condition 4 of Theorem 6.1) says that the absolute value of the inner product of Fx with any shift of $Z^\ell Fx$ depends only on ℓ. But (6.3) implies that the norm of the vector $\bar{x} \circ (X^\triangle x)$ is $\sqrt{\frac{1}{n+1}}$. So, it says that the absolute value of the inner product does not depend on ℓ as well, hence $\frac{1}{\sqrt{n}}Fx$ is a fiducial vector. But we already know this from Propositions 2.7 and 3.4.

Hence, Condition 4 of Theorem 6.1 in the case of group covariants SIC-POVMs turns out to be closely related to the fact that the Fourier transform of a fiducial vector is also a fiducial vector.

7.2 Adjusting Phases for MUHs

As we have said before, in order to get a complete system of MUHs, we use construction (5.3) with the Fourier matrix of a group G as matrix B. We have seen some nice properties of this matrix in Section 5.4. Let us begin this section by giving one more property of Fourier matrices, noted to be "striking" in [8]. Namely, any vector v, unbiased with respect both to the standard basis and a Fourier matrix, can be collected into a whole unbiased basis. It is easy to prove this if one notices that a Fourier matrix F is symmetric and, hence, its columns $\{R_i\}$ also form a group with Hadamard multiplication as the operation. The vector v can be extended to a basis $\{R_a \circ v \mid a \in G\}$, and

$$|\langle R_b | R_a \circ v\rangle| = |\langle R_{b-a} | v\rangle| = \frac{1}{\sqrt{n}}.$$

But let us return to the search of phases. In the case of MUHs we are looking for a flat matrix A satisfying (5.6). Hence, we may consider the matrix M, as described in the beginning of the chapter, to have all entries equal to 1. It is worth mentioning that in this case matrices D_Δ from Proposition 5.10 are complex Hadamard matrices.

Hadamard matrices are quite rare, and here from one flat matrix one should extract $n-1$ Hadamards. It explains, to some extent, why it is not so easy to find a convenient matrix A. In practice, matrices D_Δ are chosen to be (up to some equivalence) equal to the same Fourier matrix. Now we will give three possible kinds of restrictions on D_Δ and describe the corresponding constructions in terms of functions acting from one Abelian group into another.

Suppose matrix B (as in (5.3)) is the Fourier matrix of the group $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$ and let $N = \mathbb{Z}_{d'_1} \times \mathbb{Z}_{d'_2} \times \cdots \times \mathbb{Z}_{d'_{m'}}$ be a group of the same size. Suppose all matrices D_Δ are equal (up to a permutation of rows) to the Fourier matrix F of N and each row of A (that we want to construct) is a row of F. Define the function $f : G \to N$ as assigning to the index of a row of A the index of the row of F that stands in that place. It is easy to see that this construction satisfies the condition of Proposition 5.6 if and only f satisfies

$$\forall g_1, g_2, g_3, g_4 \in G : \quad \left.\begin{array}{r} g_1 + g_2 = g_3 + g_4 \\ f(g_1) + f(g_2) = f(g_3) + f(g_4) \end{array}\right\} \Longrightarrow \{g_1, g_2\} = \{g_3, g_4\}. \tag{7.1}$$

This is not the most general case. If we allow D_Δ to be equal to the matrix F with rows permuted and each column multiplied by $\chi_a(x_\Delta)$ where a is the index of the column and x_Δ is some element of $\tilde{N}$ (recall the definition from Section 2.2), then we can take the matrix $A = (a_{\ell r})$, $(\ell \in G, r \in N)$ defined by $a_{\ell r} = \chi_r(f(\ell))$, where function $f : G \to \tilde{N}$ satisfies

$$\forall g_1, g_2, g_3, g_4 \in G : \quad \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow f(g_1) + f(g_2) - f(g_3) - f(g_4) \in N^*. \tag{7.2}$$

Finally, from Lemma 2.3 it follows that this approach gives a complete system of MUHs if and only if $f : G \to \tilde{N}$ satisfies

$$\forall g_1, g_2, g_3, g_4 \in G : \quad \left.\begin{array}{c} g_1 + g_2 = g_3 + g_4 \\ \{g_1, g_2\} \neq \{g_3, g_4\} \end{array}\right\} \Longrightarrow f(g_1) + f(g_2) - f(g_3) - f(g_4) \in \tilde{N}^*. \tag{7.3}$$

However, in this case the matrices D_Δ are not longer equivalent to a Fourier matrix, but rather to a matrix mentioned in Remark 2.6.

Summarizing everything, we have the following result:

Theorem 7.2. *Condition (7.3) is more general than the one in (7.2) that, in turn, is more general than the one in (7.1). Formula*

$$(v_k^{(r)})_\ell = \frac{1}{\sqrt{n}} \chi_k(\ell) \chi_r(f(\ell)), \tag{7.4}$$

(with $k, \ell \in G$ and $r \in N$) gives a complete system of MUHs if and only if the function f (mapping from G to $\tilde{N}$) satisfies (7.3).

A similar result appeared in [49]. We postpone a discussion of related topics till Section 7.2.2. In the next section we demonstrate known constructions of complete systems of MUBs from Section 3.1.1 in the light of Theorem 7.2.

7.2.1 Known Constructions

Now we will give two known examples of complete sets of MUHs in the terms of the previous corollary.

A construction essentially corresponding to the following one was first obtained for $GF(p)$ by Ivanović in [35] and in the general case by Fields and Wootters in [58].

Lemma 7.3. *If $n = p^k$ is a power of an odd prime, then the function $f(x) = x^2$ with $G = N$ being the additive group of $GF(n)$ (i.e. $\mathbb{Z}_p^k$) satisfies (7.1).*

Proof. Let us suppose $g_1 + g_2 = g_3 + g_4$ and $g_1^2 + g_2^2 = g_3^2 + g_4^2$. Then $g_1 - g_3 = g_4 - g_2$ and $(g_1 - g_3)(g_1 + g_3) = (g_4 - g_2)(g_4 + g_2)$. If $g_1 = g_3$, we are done. Otherwise, we can cancel $g_1 - g_3$ out from the last equality and get $g_1 + g_3 = g_4 + g_2$. Together with the first equality it gives $2(g_2 - g_3) = 0$. Because 2 does not divide p, $g_2 = g_3$ and we are done. ■

This construction gives almost the same construction as in Theorem 3.2 except that we do not use characters defined by (3.2), but ones defined in (2.2). The first definition uses the trace function, that is specific for additive characters of $GF(p^k)$; the second one uses a "scalar product", that is specific for characters of the group $\mathbb{Z}_p^k$. It is justified because this does not change the characters, only the correspondence between elements of the group and characters, and this results in a mere permutation of rows. Sometimes identities like (3.3) are needed (for an example of its usage in quantum computation see [14]), but not in our case, and we may choose any representation of characters that we like.

Remark 7.4. Thus, we have shown that for $G = \mathbb{Z}_p^k$ where p is an odd prime, the matrix M consisting of all ones is satisfiable. In fact, from Theorem 4.2 it follows that M is satisfiable with a circulant P if $p \geq 5$.

If n is even we have to be a bit cleverer. Let us recall that a common construction of the finite field $GF(2^k)$ is as polynomials with degree smaller than k and coefficients from $\{0, 1\}$. All operations are performed modulo 2 and h, where h is a polynomial of degree k irreducible over $GF(2)$. We will treat these polynomials as integral polynomials. The next lemma also leads to the construction first obtained by Fields and Wootters in [58].

Lemma 7.5. *Let G be the additive group of $GF(2^k)$. Then the function $f : G \to \tilde{G}$ defined with*

$$f(x) = \frac{x^2}{2} \bmod (2, h)$$

satisfies (7.2) with $N = G$.

Proof. Suppose $g_1 + g_2 \equiv g_3 + g_4 \pmod{2, h}$. Then $(g_1 + g_2)^2 \equiv (g_3 + g_4)^2 \pmod{2, h}$. Hence, $g_1^2 + g_2^2 - g_3^2 - g_4^2 \equiv 0 \pmod{2, h}$. This means that

$$f(g_1) + f(g_2) - f(g_3) - f(g_4) = \frac{g_1^2 + g_2^2 - g_3^2 - g_4^2}{2} \bmod (2, h)$$

is an integer polynomial. The only way it could not belong to N^* is if it was equal to 0. Let us suppose it is equal to zero and prove that in this case $\{g_1, g_2\} = \{g_3, g_4\}$.

Define $s = (g_1 + g_2) \bmod 2$. Then also $g_1^2 + g_2^2 \equiv s^2 \pmod 2$. Consider the following equation in x:

$$\frac{g_1^2 + g_2^2 - x^2 - (s-x)^2}{2} \equiv 0 \pmod{h, 2}.$$

Both g_1 and g_2 are its roots. The polynomial of x can be rewritten as $\frac{g_1^2+g_2^2-s^2}{2} + sx - x^2$. One may notice that $\frac{g_1^2+g_2^2-s^2}{2}$ is an integer polynomial, so taking it modulo h and 2 we obtain an equation of the second degree in $GF(2^k)$:

$$x^2 - sx - \frac{g_1^2 + g_2^2 - s^2}{2} = 0.$$

If $g_1 \neq g_2$, no other element except these can satisfy it. If $g_1 = g_2$ then $s = 0$ and this equation has only one root, because $x \mapsto x^2$ is a bijection in $GF(2^k)$ (the Frobenius map). Thus, f satisfies (7.2). ■

Remark 7.6. Permuting the columns of the matrix A does not break the property (5.6). Also, in $GF(2^k)$ the mapping $x \mapsto x^2$ is a bijection. Hence, if we define $A = (a_{ij})$ as

$$a_{ij} = \chi_{j^2}\left(\frac{i^2}{2} \bmod (2, h)\right),$$

we still get a matrix satisfying (5.6). But note that $a_{ij}^2 = \chi_{j^2}(i^2) = \chi_{i^2}(j^2) = a_{ji}^2$, so, additionally, $A^{(2)}$ is a symmetric real Hadamard matrix.

For example, if we take $k = 2$, $h = x^2 + x + 1$, we get the matrix

$$A' = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & \mathbf{i} & 1 \\ 1 & -\mathbf{i} & -1 & -\mathbf{i} \\ 1 & 1 & \mathbf{i} & \mathbf{i} \end{pmatrix}, \tag{7.5}$$

where rows and columns are indexed by $0, 1, x, x+1$. We will use this matrix in Section 7.3.

The last two lemmas can be combined into the following well-known result:

Theorem 7.7. *If n is a prime power then there exists a complete set of MUBs in $\mathbb{C}^n$.*

7.2.2 Related Combinatorial Structures

Observing formulas (7.1), (7.2) and (7.3) one can conclude that they, especially (7.1), are of highly combinatorial nature. It turns out that they indeed have a strong link with some well-studied combinatorial structures.

Suppose G and N are Abelian groups with $|G| \leq |N| < \infty$. Functions $f : G \to N$ such that the equation $f(x+a) - f(x) = b$ has no more than 1 solution, for all $a, b \in G$ not equal to zero simultaneously, are called *differentially 1-uniform* [44]. If N satisfies $|G|/|N| = m \in \mathbb{N}$ and function $f : G \to N$ is such that $|\{x \in G \mid f(x+a) - f(x) = b\}| = m$ for any $b \in N$ and non-zero $a \in G$, the function is called *perfect non-linear* [11]. These functions are used in cryptography to construct S-boxes that are not vulnerable to differential cryptanalysis.

If $|G| = |N|$ as in (7.1), these two notions coincide and function f is sometimes called a *planar function*. This name is given because any planar function gives rise to an affine plane [16]. For functions satisfying (7.2) we will use the name *fractional planar*.

The following planar functions from $GF(p^k)$, with p odd, to itself are known:

- $f(x) = x^{p^\alpha+1}$, where α is a non-negative integer with $k/\gcd(k,\alpha)$ being odd. See [16].
- $f(x) = x^{(3^\alpha+1)/2}$ only for $p = 3$, α is odd, and $\gcd(k,\alpha) = 1$. See [13].
- $f(x) = x^{10} - ux^6 - u^2x^2$ only for $p = 3$, k is odd, and u is a non-zero element of $GF(p^k)$. The special case of $u = -1$ was obtained in [13], the general case is due to [18].

The construction with $f(x) = x^2$ from the previous section is from the first class.

Let K again be an Abelian group and N be its subgroup. A subset $R \subset K$ is called a *relative* (m, n, r, λ)*-difference set* if $|K| = nm$, $|N| = n$, $|R| = r$ and

$$|\{r_1, r_2 \in R \mid r_1 - r_2 = b\}| = \begin{cases} r & , \quad b = 0; \\ 0 & , \quad b \in N \setminus \{0\}; \\ \lambda & , \quad b \in K \setminus N. \end{cases}$$

A relative difference set is a generalization of a classical difference set and it was introduced in [19]. If $r = m$ the difference set is called *semiregular*. A relative difference set is called *splitting* if $K = G \times N$, i.e. if N has a complement in K.

This notion is interesting to us because of the following easy observation (see, e.g., [45]). Let G and N be arbitrary finite groups and f be a function from G to N. The set $\{(x, f(x)) \mid x \in G\}$ is a semiregular splitting $(|G|, |N|, |G|, |G|/|N|)$-difference set in $G \times N$ relative to $\{1\} \times N$ if and only if f is perfect nonlinear. Thus, planar functions correspond to splitting relative $(n, n, n, 1)$-difference sets. We extend this result a bit:

Theorem 7.8. *Let K be an Abelian group of size n^2 having a subgroup $N = \mathbb{Z}_{d'_1} \times \mathbb{Z}_{d'_2} \times \cdots \times \mathbb{Z}_{d'_{m'}}$ of size n. The following two statements are equivalent:*

(a) There exists a semiregular $(n, n, n, 1)$-difference set R in K relative to N.

(b) There exists a fractional planar function $f : G \to \tilde{N}$ where $G \cong K/N$.

Proof. Suppose we have a relative difference set. Fix any $G = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_m}$ such that $G \cong K/N$. Let $k_1, \ldots, k_m \in K$ be representatives of the elements of the basis of G. Denote by $(s_{1i}, s_{2i}, \ldots, s_{m'i})$ the element $d_i k_i \in N$, $i = 1, \ldots m$.

Define an Abelian group K' as follows. Its elements are from the direct product $G \times N$ and the sum of two elements $(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots, y_{m'})$ and $(z_1, z_2, \ldots, z_m; t_1, t_2, \ldots, t_{m'})$ is defined as $(a_1, a_2, \ldots, a_m; b_1, b_2, \ldots, b_{m'})$ where $a_i = x_i + z_i$ and

$$\begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_{m'} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{m'} \end{pmatrix} + \begin{pmatrix} t_1 \\ t_2 \\ \vdots \\ t_{m'} \end{pmatrix} + \begin{pmatrix} s_{11} & s_{12} & \cdots & s_{1m} \\ s_{21} & s_{22} & \cdots & s_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ s_{m'1} & s_{m'2} & \cdots & s_{m'm} \end{pmatrix} \begin{pmatrix} [x_1 + z_1 \geq d_1] \\ [x_2 + z_2 \geq d_2] \\ \vdots \\ [x_m + z_m \geq d_m] \end{pmatrix} \tag{7.6}$$

where $[x_i + z_i \geq d_i]$ is equal to 1 if the sum of x_i and z_i, taken as integers, exceeds d_i and is equal to 0 otherwise. It is not hard to check that $\varphi : K' \to K$, defined with

$$(x_1, x_2, \dots, x_m; y) \mapsto y + \sum_{i=1}^{m} x_i k_i,$$

is an isomorphism. As usual, we identify elements of G with the set $\{(x, 0) \mid x \in G\}$ and N with $\{(0; y) \mid y \in N\}$.

Denote by S the $m' \times m$-matrix whose (i, j)-th element is equal to s_{ij}/d_i. Clearly, $\psi : K' \to \tilde{N}$ defined by

$$\psi(x, y) = y + Sx$$

is a morphism. Since R is a semiregular relative difference set, for any $x \in K/N$ we can find a unique element $r_x \in R$ with projection on K/N equal to x. Define $f(x) = \psi(\varphi^{-1}(r_x))$.

Let us prove that f is fractional planar. At first, note that for any $x \in G$: $\varphi^{-1}(r_x) = (x, y)$ for some $y \in N$. Then suppose that $g_1, g_2, g_3, g_4 \in G$ are such that $g_3 - g_1 = g_2 - g_4 \neq 0$ and $g_1 \neq g_4$. Denote $(x_1, y_1) = \varphi^{-1}(r_{g_3} - r_{g_1})$ and $(x_2, y_2) = \varphi^{-1}(r_{g_2} - r_{g_4})$. We have $x_1 = x_2$ (because $g_3 - g_1 = g_2 - g_4$) and $y_1 \neq y_2$ (because $r_{g_3} - r_{g_1} \neq r_{g_2} - r_{g_4}$). From the definition of ψ we have $(f(g_3) - f(g_1)) - (f(g_2) - f(g_4)) \in N^*$.

Suppose conversely that we have a fractional planar function $f : G \to \tilde{N}$ with the same expressions for G and N. Define the function $\{\cdot\}$ that takes the fractional part of every component of an element of $\tilde{N}$. Define also $\tilde{f}(x) = \{f(x)\}$. Then (7.2) yields

$$(a + b = c + d) \Longrightarrow (\tilde{f}(a) + \tilde{f}(b) - \tilde{f}(c) - \tilde{f}(d) \in N).$$

Since the condition on f is invariant under adding a constant to the function, we may assume that $\tilde{f}(0) = 0$. Then $\tilde{f}(a + b) = \{\tilde{f}(a) + \tilde{f}(b)\}$. Now it is easy to deduce that $\tilde{f}(x) = \{Sx\}$ where S is defined in the same way as before for some integers s_{ij}.

Define K' as in (7.6) and define

$$R = \{(x; f(x) - Sx) \mid x \in G\}.$$

Similar reasoning as before shows that R is semiregular difference set relative to N. ■

So, we have proved that if matrix B in (5.3) is a Fourier matrix, and all D_Δ are equivalent (in some sense) Fourier matrices, then the existence of a complete system of MUHs in $\mathbb{C}^n$ is equivalent to the existence of a relative $(n, n, n, 1)$-difference set. In fact, a more general result [26] is known: the existence of a relative (n, k, n, λ)-difference set implies the existence of a set of k MUHs in $\mathbb{C}^n$. And all known constructions of complete systems of MUBs are special cases of this construction.

It is proved in [10] that a relative $(n, n, n, 1)$-difference set exists only if n is a prime power. Thus, using the approach with f satisfying (7.2) it is not possible to construct a complete system of MUBs for any new dimension. It is still not clear what can be said in the case of general D_Δ and, in particular, in the case of f satisfying (7.3).

7.3 SIC-POVMs in dimensions 2^k

In this section we will talk about SIC-POVMs in dimensions 2^k and consider some possible construction ideas.

Analytical constructions of SIC-POVMs are known for dimensions 2, 4 and 8. In $\mathbb{C}^2$ this is the SIC-POVM given by (3.5). The known SIC-POVM in $\mathbb{C}^4$ is quite complicated and it is group covariant with respect to $\mathrm{GP}(\mathbb{Z}_4)$. We give a complete list of fiducial vectors [47].

Let

$$r_0 = \frac{1-1/\sqrt{5}}{2\sqrt{2-\sqrt{2}}}, \qquad r_1 = (\sqrt{2}-1)r_0, \qquad r_\pm = \frac{1}{2}\sqrt{1+\frac{1}{\sqrt{5}} \pm \sqrt{\frac{1}{5}+\frac{1}{\sqrt{5}}}},$$

and

$$a = \arccos\frac{2}{\sqrt{5+\sqrt{5}}}, \qquad b = \arcsin\frac{2}{\sqrt{5}}.$$

Define the functions

$$\theta_+(j,m,n) = (-1)^m\left(\frac{b}{4}+\frac{a}{2}\right) + \frac{(m+2n+7j+1)\pi}{4}, \qquad \theta_1(k) = \frac{(2k+1)\pi}{2},$$

$$\text{and} \qquad \theta_-(j,k,m,n) = (-1)^m\left(\frac{b}{4}-\frac{a}{2}\right) + \frac{(m+2n+3j+4k+1)\pi}{4}.$$

Then the complete list of fiducial vectors in $\mathbb{C}^4$ is given by

$$\left\{ \alpha X_4^i R_4^\ell \begin{pmatrix} r_0 \\ r_+ e^{\mathbf{i}\theta_+(j,m,n)} \\ r_1 e^{\mathbf{i}\theta_1(k)} \\ r_- e^{\mathbf{i}\theta_-(j,k,m,n)} \end{pmatrix} \middle| \; \alpha \in \mathbb{C}, |\alpha| = 1, \quad i,n = 0,\ldots,3 \;\text{ and }\; j,k,\ell,m = 0,1 \right\}$$

where X_4 and R_4 are as in (2.5) and (2.4), respectively.

In $\mathbb{C}^8$ the construction is rather nice [31], and and the resulting SIC-POVM can be made group covariant with respect to $\mathrm{GP}(\mathbb{Z}_2^3)$ [26]. We will give a description of an equivalent SIC-POVM. Take $G = \mathbb{Z}_2^3$ and

$$A = \begin{pmatrix} \frac{1}{\sqrt{3}}I & \frac{1}{\sqrt{6}}A' \\ \frac{1}{\sqrt{6}}A' & \frac{i}{\sqrt{3}}I \end{pmatrix},$$

where I is the 4×4 identity matrix and A' is the matrix from (7.5). Let us prove that matrix A satisfies all conditions of Theorem 6.1. Suppose the rows and columns of A are indexed as $(0,0,0), (0,0,1), \ldots, (1,1,0), (1,1,1)$.

Conditions 1 and 2 are trivial. For Condition 3, note that

$$\|R_i^{(2)}\| = \sqrt{\frac{1}{9}+4\frac{1}{36}} = \frac{\sqrt{2}}{3}$$

and

$$\|R_i \circ R_j\| = \begin{cases} \sqrt{4\frac{1}{36}} & , \quad i \text{ and } j \text{ are from the same block} \\ \sqrt{2\left(\frac{1}{3}\right)\left(\frac{1}{6}\right)} & , \quad \text{otherwise} \end{cases} = \frac{1}{3}.$$

For Condition 4 we will describe what the vector $R = \overline{R_{g_1} \circ R_{g_2}} \circ R_{g_3} \circ R_{g_4}$ looks like and prove that it sums up to zero. There are two possibilities.

- If all g_1, g_2, g_3, g_4 are from the same, say the first, block then R looks like

  $$(0, 0, 0, 0, a_{(0,0)}, a_{(0,1)}, a_{(1,0)}, a_{(1,1)})$$

  and the condition is satisfied because A' satisfies (5.6) for $\mathbb{Z}_2^2$. (This is similar to the proof of Theorem 5.5).

- Suppose they are from different blocks, say g_1, g_2 are from the first block, and g_3, g_4 are from the second block. Note that $g_1 + g_2 = g_3 + g_4$. Denote this value by d. Then if $d \neq 0$, then R consists only of zeroes. If $g_1 = g_2$ and $g_3 = g_4$ then R has exactly two non-zero elements, one at position g_1 and equal to $a^2_{g_3', g_1}$, and second at position g_3 and equal to $-a^2_{g_1, g_3'}$, where $A = (a_{ij})$ and $g_3' = g_3 + (1, 0, 0)$. Then R sums up to zero because $A'^{(2)}$ is symmetric.

Unfortunately such a nice reduction from MUHs to SIC-POVMs is possible only for $\mathbb{Z}_2^3$ because of Condition 3. Also, it was proved in [26] that there exist no group covariant SIC-POVM with respect to $\mathbb{Z}_2^k$ if $k \neq 1$ and $k \neq 3$.

This is what was previously known. Let us give now some results that can be obtained using our techniques. In Theorem 7.1 a necessary and sufficient condition for a circulant matrix over $\mathbb{Z}_3$ to be satisfiable is given. In the case of $G = \mathbb{Z}_2$ and $G = \mathbb{Z}_2^2$ the condition is even simpler.

Proposition 7.9. *Any circulant over $\mathbb{Z}_2$ or $\mathbb{Z}_2^2$ matrix M is satisfiable. For $\mathbb{Z}_2$ the matrix P can be taken to be circulant.*

Proof. Use matrices

$$P = \begin{pmatrix} 1 & \omega_8 \\ \omega_8 & 1 \end{pmatrix} \quad \text{and} \quad P = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathbf{i} & 1 & \mathbf{i} \\ 1 & -\mathbf{i} & -\mathbf{i} & 1 \\ 1 & 1 & \mathbf{i} & -\mathbf{i} \end{pmatrix},$$

respectively. In the second matrix index the rows and columns as $(0,0), (0,1), (1,0), (1,1) \in \mathbb{Z}_2^2$. Straightforward but bulky computations show that this indeed works. We omit them. ∎

In particular, if we take M as given by (6.4) for $n = 4$ and the matrix P from the previous theorem, we get a SIC-POVM in $\mathbb{C}^4$. We will give a complete expression for it as the columns of the matrix

$$\begin{pmatrix} b & a & a & a & b & a & a & a & b & a & a & a & b & a & a & a \\ a & \mathbf{i}b & a & \mathbf{i}a & -a & -\mathbf{i}b & -a & -\mathbf{i}a & a & \mathbf{i}b & a & \mathbf{i}a & -a & -\mathbf{i}b & -a & -\mathbf{i}a \\ a & -\mathbf{i}a & -\mathbf{i}b & a & a & -\mathbf{i}a & -\mathbf{i}b & a & -a & \mathbf{i}a & \mathbf{i}b & -a & -a & \mathbf{i}a & \mathbf{i}b & -a \\ a & a & \mathbf{i}a & -\mathbf{i}b & -a & -a & -\mathbf{i}a & \mathbf{i}b & -a & -a & -\mathbf{i}a & \mathbf{i}b & a & a & \mathbf{i}a & -\mathbf{i}b \end{pmatrix}$$

where

$$a = \frac{1}{2}\sqrt{1 - \frac{1}{\sqrt{5}}} \qquad \text{and} \qquad b = \frac{1}{2}\sqrt{1 + \frac{3}{\sqrt{5}}}.$$

This expression is much simpler than the expression for the known SIC-POVM in $\mathbb{C}^4$. It is very close to being group covariant with respect to $\mathbb{Z}_2^2$, but is not, because P is not circulant. This shows that our approach with homogeneous systems can lead to simple constructions of SIC-POVMs in some cases.

Matrices P that do not depend on the matrix M, as in Theorem 7.9, are interesting, because their entries can be very simple, even if the entries in M are complicated, that in the case of SIC-POVMs is quite possible. Let, up to the end of the section, denote by $P = (p_{ij})$ a flat matrix such that $M \circ P$ satisfies (5.6) for all circulant matrices M.

Let us give a reason why for $G = \mathbb{Z}_2^k$ it becomes possible to construct such a matrix P. Denote $Q = P^{(2)}$ and let $M = (M_{ij})$ be a circulant matrix over G. Note that if $A = M \circ P$ satisfies (5.6) then $A^{(2)} = M^{(2)} \circ Q$ must be a scalar multiple of a unitary matrix. So let us, up to the end of this section, denote by $Q = (q_{ij})$ a flat matrix such that $M \circ Q$ is a scalar multiple of a unitary matrix for all circulant matrices M.

Consider rows of Q indexed by a and b. Note that for any d we have $m_{a,d} = m_{b,d+a+b}$ and $m_{b,d} = m_{a,d+a+b}$. Hence, if Q satisfies $q_{a,d}\overline{q_{b,d}} = -q_{a,d+a+b}\overline{q_{b,d+a+b}}$ for all $a, b, d \in G$, then $M \circ Q$ has orthogonal rows for any circulant matrix M. Hence, at least theoretically, Q may not depend on M.

Similarly, let $g_1, g_2, g_3, g_4 \in G$ be such that $g_1 + g_2 = g_3 + g_4$ and d be an arbitrary element of G. Consider the 4×4-submatrix M' of M given by the intersection of

$$\text{rows } \{g_1, g_2, g_3, g_4\} \text{ and columns } \{d, d + g_1 + g_2, d + g_1 + g_3, d + g_1 + g_4\}. \tag{7.7}$$

Matrix M' is circulant over $\mathbb{Z}_2^2$. If for any such choice of g_1, g_2, g_3, g_4 and d the submatrix P' of P at the intersection of rows and columns with the same indices, is like the matrix P in Theorem 7.9 (i.e., $M' \circ P'$ satisfies (5.6) for any circulant matrix M'), then $M \circ P$ satisfies the same condition.

Unfortunately, it is possible to show that for $G = \mathbb{Z}_2^3$ and larger groups such a matrix P does not exist. The proof we have is computer aided. We will give a sketch of it, omitting most of the details.

In order to prove this result, let us start with the matrix $Q = P^{(2)}$. For any circulant M the matrix $M \circ Q$ must have orthogonal rows. Denote $q_{ab} = e^{2\pi \mathbf{i} q'_{ab}}$ with $q'_{ab} \in \mathbb{R}$. For any $a, b, d \in G$ with $a \neq b$, we must have

$$q'_{a,d} - q'_{a,d} \equiv 1/2 + q'_{a,d+a+b} - q'_{b,d+a+b} \pmod 1.$$

This gives a system of linear equations over reals modulo 1 with integer coefficients. Without loss of generality we may assume that $q'_{0,i} = q'_{i,0} = 0$ for all $i \in G$. Solving this system for $G = \mathbb{Z}_2^4$, we find that this system has no solutions, hence such a matrix Q (and a fortiori P) does not exist for $G = \mathbb{Z}_2^k$ with $k \geq 4$. For $G = \mathbb{Z}_2^3$, however, we get 16 solutions. One of them gives Q equal to

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \end{pmatrix}.$$

But from the system we still get that all these solutions have entries in $\{0, 1/2\}$. Hence, we may assume, without loss of generality, that matrix P for $G = \mathbb{Z}_2^3$ has entries in $\{\pm 1, \pm \mathbf{i}\}$. Then by exhaustive search it is possible to show that such P does not exist.

One possible complaint we would expect is that in a simple matrix M given by (6.4) (it gives a circulant simplex for all groups) all off-diagonal elements are equal. Thus, in the case of SIC-POVMs, we do not need to consider the most general case, and may assume that M is the circulant matrix with the first row given by $(a, b, b, \ldots, b)$ where a, b are arbitrary non-negative real numbers. In this case we may state the same questions: does there exist a matrix Q such that $M \circ Q$ is a scalar multiple of a unitary matrix and does there exist a matrix P such that $M \circ P$ satisfies (5.6), where M is an arbitrary matrix of the given form and P, Q do not depend on M.

It turns out, that such matrix Q exists for all $G = \mathbb{Z}_2^k$. Indeed, take

$$Q_1 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

and define

$$Q_{k+1} = \begin{pmatrix} Q_k^T & Q_k \\ -Q_k^T & Q_k \end{pmatrix}.$$

Both Q_k and Q_k^T work for $G = \mathbb{Z}_2^k$. These are "antisymmetric" (except for the diagonal that consists only of 1's) real Hadamard matrices.

But we get no new matrices P is such way. Indeed, such a matrix P should satisfy (5.6), because one can take M consisting only of 1's. Take distinct $g_1, g_2, g_3, g_4 \in G$ such that $g_1 + g_2 = g_3 + g_4$, and define matrix P' as the submatrix of P at the intersection of rows and columns indexed by $\{g_1, g_2, g_3, g_4\}$. Index rows and columns of $P' = (p'_{ij})$ by elements of $\mathbb{Z}_2^2$. Then for any permutation (a, b, c, d) of $\mathbb{Z}_2^2$, P' must satisfy $(p'_{a,a})^2\overline{(p'_{b,a})^2} = -(p'_{a,b})^2\overline{(p'_{b,b})^2}$ and $R_a \circ R_b \perp R_c \circ R_d$, where R_i is the i-th row of P'. It is possible to check using a computer that then P' satisfies (5.6) (we do not know an analytical proof of this fact). In particular it means that $Q = P^{(2)}$ is a general Q, i.e. $M \circ Q$ has orthogonal rows for *any* circulant matrix M over G. Hence, P cannot exist for $G = \mathbb{Z}_2^4$ or larger.

For $G = \mathbb{Z}_2^3$, a matrix P and any P', as defined in the previous paragraph, must satisfy (5.6). By subtracting, it follows that any submatrix P' at the intersection given in (7.7) must satisfy (5.6). From this it follows that $M \circ P$ satisfies (5.6) for any circulant matrix M. But we already know that such a matrix P does not exist.

Thus, it is not possible to construct a matrix P that works for any choice of matrix M. However, this does not mean that it is not possible to combine the ideas from this section with some others to give nice constructions of homogeneous SIC-POVMs in dimensions 2^k.

Chapter 8

Conclusion

In this thesis we have shown that constructions used in quantum state tomography (with applications in other areas as well) have some common aspects with sequences with low correlation. So, it turns out that classical information processing and quantum information processing are not as distinct as it may seem. In particular, one of the famous lower bounds in the topic of sequences with low correlation (the Welch bounds) gives a nice characterisation of MUBs and SIC-POVMs. This connection has been known before in the terms of complex projective t-designs. Also a construction by Alltop which was aimed to produce sequences with low correlation, in fact, results in a construction of MUHs. It could be interesting to try to use other constructions and bounds from one area in another.

Also, we have formulated the criterion that reduces the existence of a complete system of MUBs or a SIC-POVM (or, more generaly, any complex projective t-design) to the condition on orthonormality of a certain collection of vectors. We can mention the following advantages of this approach:

Orthogonality Both definitions of MUBs and SIC-POVMs involve unobvious angles like $\frac{1}{n}$ or $\frac{1}{n+1}$. Our criterion allows to define them solely in the terms of orthogonal vectors. Clearly, orthogonality is a much more studied notion than the angles like $\frac{1}{n}$ and $\frac{1}{n+1}$.

Modularity This approach makes it possible to characterize the contribution of each part of the system in a concise way. This allows replacing some parts of the system by other. For example, some Hadamards in a complete system of MUHs can be replaced by others, if and only if the sums of weights on each arc in their K-graphs are the same.

Homogeneous systems The modularity principle becomes most obvious in the homogeneous setting. In this setting which allows a unified treatment of complete systems of MUHs and SIC-POVMs, we have only two matrices, and for each of them we are mostly interested in the L-graph.

Separation of moduli and phases The problem of finding vectors breaks into the problem of finding the absolute values of the elements of these vectors, and then searching phases for these vectors. Both these problems can be solved independently, that simplifies the search in some cases.

The main drawback of our approach is the complicated dependency between the elements of a complex projective design and the system of vectors we are using in the criterion.

Another disadvantage of our criterion is that it seems not to work for non-complete systems of MUBs. However, there are many other areas where the criterion is applicable. For example, Scott in [52] proposes to use IC-POVMs that are simultaneously complex projective 2-designs (he calls them *tight IC-POVMs*) and it is claimed that they are "as close as possible to orthonormal bases for the space of quantum states". In particular, in the joint work with Roy [49], weighted complex projective 2-designs consisting of orthonormal bases are investigated. The problem is to find such orthonormal bases $B_0, B_1, \ldots, B_k$ of $\mathbb{C}^n$ and weights $w_0, w_1, \ldots, w_k$ that are non-negative real numbers so that the set $\{w_i x \mid x \in B_i, i = 0, 1, \ldots, k\}$ attains the Welch bound for $k = 2$. Such designs are proposed for use in spaces where no complete systems of MUBs are known, i.e., in all dimensions that are not prime powers. The following theorem is proved in [49]:

Theorem 8.1. *The existence of a differentially 1-uniform function f from an Abelian group G into an Abelian group N with $|G| = n$ and $|N| = m$ implies the existence of a weighted 2-design in $\mathbb{C}^n$ formed from $m + 1$ orthonormal bases.*

This allows us to build a complex weighted 2-design of $n + 2$ orthonormal bases in $\mathbb{C}^n$ when $n + 1$ is a prime power. This is one basis more than in the complete system of MUBs. Our criterion is applicable in these settings as well, in particular, Theorem 8.1 can be proved in a manner similar to the proof of Theorem 7.2.

8.1 Open problems

The main open problem that motivated this research and still remains open is the existence problem of complete systems of MUBs and SIC-POVMs. So, what are the smaller problems that arises from our thesis? It is hard to mention all of them, we will state ones that we think are the most interesting.

It is interesting whether homogeneous systems of MUHs exist only in prime power dimensions. This question gives rise to two subquestions:

- Describe all dimensions in which the matrix consisting only of 1's is satisfiable in the sense of Section 7. In particular, are there interesting functions that satisfy condition (7.3), but does not satisfy (7.2).
- Decide whether Fourier matrices are the only L-maximal complex Hadamard matrices. If they are not, what are other L-maximal Hadamard matrices and are they useful in the constructions of complex projective 2-designs using the homogeneous systems approach?

Another problem is to give a nice criterion for a circulant matrix M to be satisfiable. This may a be complicated question, because the non-satisfiability of a matrix consisting only of 1's alone implies some deep combinatorial non-existence results.

A more promising area of investigation is construction of homogeneous SIC-POVMs that are not group covariant. Because most of the research in the area deals with group covariant

SIC-POVMs, some simple constructions may have been overlooked. Dimensions of the form 2^k may be the easiest cases to start with.

It is also not clear to us at the moment how to deal with non-homogeneous SIC-POVMs and systems of MUHs.

Bibliography

[1] Aharonov, Y., Englert, B.-G.: The mean kings problem: Spin 1. Zeitschrift für Naturforschung 56a, 16–19 (2001)

[2] Alltop, W.O.: Complex sequences with low periodic correlations. IEEE Transactions on Information Theory 26(3), 350–354 (1980)

[3] Appleby, D.M.: SIC-POVMs and the Extended Clifford Group. Journal of Mathematical Physics 46, 052107, arXiv:quant-ph/0412001 (2004)

[4] Appleby, D.M., Dang, H.B., Fuchs, C.A.: Physical significance of symmetric informationally complete sets of quantum states. arXiv:0707.2071v1 (2007)

[5] Barnum, H.: Information-disturbance tradeoff in quantum measurement on the uniform ensemble. Proceedings of IEEE International Symposium on Information Theory 2001, 277, arXiv:quant-ph/0205155v1 (2002)

[6] Belovs, A., Smotrovs, J.: A Criterion for Attaining the Welch Bounds with Applications for Mutually Unbiased Bases. arXiv:0802.0855v2, to apper in the proceedings of Mathematical Methods in Computer Science 2008 (2008)

[7] Beth, T., Jungnickel, D., Lenz, H.: Design Theory (Second Edition). Cambridge University Press (1999)

[8] Bengtsson, I., Bruzda, W., Ericsson, A., Larsson, J.-A., Tadej, W., Zyczkowski, K.: MUBs and Hadamards of Order Six. arXiv:quant-ph/0610161 v1 (2006)

[9] Bennett, C.H., Brassard, G.: Quantum Cryptography : Public Key Distribution and Coin Tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, New York, 175–179 (1984)

[10] Blokhuis, A., Jungnickel, D., Schmidt, B.: Proof of the Prime Power Conjecture for Projective Planes of Order n with Abelian Collineation Groups of Order n^2. Proceedings of AMS 130(5), 1473–1476 (2001)

[11] Carlet C., Ding C.: Highly nonlinear mappings. Journal of Complexity 20, 205–244 (2004)

[12] Caves, C.M., Fuchs, C.A., Schack R.: Unknown Quantum States: The Quantum de Finetti Representation. Journal of Mathematical Physics 43, 4537–4559, arXiv:quant-ph/0104088v1 (2002)

[13] Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II. Designs, Codes and Cryptography 10, 167–184 (1997)

[14] van Dam, W., Hallgren, S., Ip, L.: Quantum algorithms for some hidden shift problems. Proceedings of the ACM-SIAM Symposium on Discrete Algorithms, 489–498, arXiv:quant-ph/0211140 (2003)

[15] Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geometriae Dedicata 6, 363 (1977)

[16] Dembowski, P., Ostrom, T.G.: Planes of order n with collineation groups of order n^2. Mathematische Zeitschrift 103, 239–258 (1968)

[17] Diestel, R.: Graph theory (Third edition). Springer-Verlag (2005)

[18] Ding, C., Yuan J.: A family of skew Hadamard difference sets. Journal of Combinatorial Theory, Series A 113 1526–1535 (2006)

[19] Elliott, J.E.H., Butson, A.T.: Relative difference sets. Illinois Journal of Mathematics 10, 517–531 (1966)

[20] Englert, B.-G.: Mutually unbiased bases. Problem page in Quantum Information at TU Braunschweig, http://www.imaph.tu-bs.de/qi/problems/13.html.

[21] Flammia, S.T.: On SIC-POVMs in Prime Dimensions. Journal of Physics A: Mathematical and General 39, 13483-13493, arXiv:quant-ph/0605050v3 (2006)

[22] Frankl, P.: Orthogonal vectors in the n-dimensional cube and codes with missing distances. Combinatorica 6(3), 279–285 (1986)

[23] Fuchs, C.A., Sasaki, M. : Squeezing Quantum Information through a Classical Channel: Measuring the 'Quantumness' of a Set of Quantum States. Quantum Information & Computation 3(5), 377-404, arXiv:quant-ph/0302092v3 (2003)

[24] Fuchs, C.A.: Quantum Mechanics as Quantum Information (and only a little more). arXiv:quant-ph/0205039 (2002)

[25] Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Transactions on Information Theory, IT-14, 154–156 (1967)

[26] Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. European Journal of Combinatorics 30(1), 246–262, arXiv:quant-ph/0511004 v2 (2005)

[27] Grassl, M.: On SIC-POVMs and MUBs in dimension 6. arXiv:quant-ph/0406175 (2004)

[28] Grassl, M.: Tomography of Quantum States in Small Dimensions. Electronic Notes in Discrete Mathematics 20, 151–164 (2005)

[29] Hall, M. Jr: The theory of groups. The Macmillan Company (1968)

[30] Helleseth, T., Kumar, V.J.: Sequences with low correlation. in Handbook of Coding Theory, V. Pless, C. Huffman Eds., Elsevier (1998)

[31] Hoggar, S.G.: 64 lines from a quaternionic polytope. Geometriae Dedicata 69(3), 287–289 (1998)

[32] Holevo, A.S.: Probabilistic and statistical aspects of quantum theory (in Russian). Nauka (1980)

[33] Horn, R.A., Johnson, C.R.: Matrix Analysis. Cambridge University Press (1985)

[34] Ito, N.: Hadamard graphs. Graphs and Combinatorics 1, 57–64 (1985)

[35] Ivanović, I.D.: Geometrical description of quantal state determination. Journal of Physics A: Mathematical and General 14, 3241–3245 (1981)

[36] Khatirinejad, M.: On Weyl-Heisenberg orbits of equiangular lines. Journal of Algebraic Combinatorics 28(3), 333–349 (2007)

[37] Klappenecker, A., Rötteler, M.: Mutually Unbiased Bases are Complex Projective 2-Designs. Proceedings of ISIT International Symposium on Information Theory 2005, 1740–1744, arXiv:quant-ph/0502031 v2 (2005)

[38] Klappenecker, A., Rötteler, M.: Constructions of Mutually Unbiased Bases. Finite Fields and Applications 2004, Lecture Notes in Computer Science 2948, 262–266, arXiv:quant-ph/0309120 (2003)

[39] Lemmens, P.W.H., Seidel J.J.: Equiangular Lines. Journal of Algebra 24, 494-512 (1973)

[40] Lidl, R., Niederreiter, H.: Finite fields. 2nd ed. Cambridge University Press (1997)

[41] Massey, J.L., Mittelholzer, T.: Welch's bound and sequence sets for code-division multiple-access systems. Sequences II: Methods in Communication, Security and Computer Sciences. Springer-Verlag, 63–78 (1993)

[42] Nielsen, M.A., Chuang I.L.: Quantum Computation and Quantum Information. Cambridge University Press (2000)

[43] Neumaier, A.: Combinatorial configurations in terms of distances. Departement of Mathematics Memorandum 81-09, Eindhoven University of Technology (1981)

[44] Nyberg, K.: Differentially uniform mappings for cryptography. Advances in cryptology EUROCRYPT 93 (Lofthus), Lecture Notes in Computer Science 765, 55–64 (1994)

[45] Pott, A.: Nonlinear functions in abelian groups and relative difference sets. Discrete Applied Mathematics 138, 177–193 (2004)

[46] Prugovečki, E.: Information-theoretic aspects of quantum measurement. International Journal of Theoretical Physics 16, 321–331 (1977)

[47] Renes, J., Blume-Kohout, R., Scott, A.J., Caves, C.: Symmetric Informationally Complete Quantum Measurements. Journal of Mathematical Physics 45, 2171–2180, quant-ph/0310075v1 (2003)

[48] Renes, J., Blume-Kohout, R., Scott, A.J., Caves, C.: A list of fiducial vector up to dimension 45. Available at http://info.phys.unm.edu/papers/reports/sicpovm.html.

[49] Roy, A., Scott, A.J.: Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements. Journal of Mathematical Physics 48, 072110, quant-ph/0703025v2 (2007)

[50] Rueppel, R.: Analysis and Design of Stream Ciphers. Springer-Verlag (1986)

[51] Schwinger, J.: Unitary operator bases. Proceedings of the National Academy of Sciences USA 46, 570–579 (1960)

[52] Scott, A.J: Tight informationally complete quantum measurements. Journal of Physics A: Mathematical and General 39, 13507-13530, arXiv:quant-ph/0604049v6 (2006)

[53] Shor, P.W: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Scientific Computing 26, 1484–1509, arXiv:quant-ph/9508027v2 (1997)

[54] Stanley, R.: Enumerative Combinatorics (Volume 1). Cambridge University Press (1997)

[55] Tadey, W., Zyczkowski, K.: A concise guide to complex Hadamard matrices. Open Systems & Information Dynamics 13(2), 133–177, arXiv:quant-ph/0512154v2 (2006)

[56] Waldron, S.: Generalized Welch Bound Equality Sequences Are Tight Frames. IEEE Transactions on Information Theory 49(9), 2307–2309 (2003)

[57] Welch, L.R.: Lower bounds on the maximum cross correlations of signals. IEEE Transactions on Information Theory 20(3), 397–399 (1974)

[58] Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Annals of Physics 191, 363 – 381 (1989)

[59] Wootters, W.K.: Picturing qubits in phase space. IBM Journal of Research and Development 48(1), 99–110 (2004)

[60] Zauner, G.: Quantendesigns Grundzüge einer nichtkommutativen Designtheorie (in German). PhD thesis, Universität Wien (1999)