Mutually Unbiased Bases in Low Dimensions

Stephen Brierley

PhD thesis

University of York

Department of Mathematics

November 2009

Abstract

The density matrix of a qudit may be reconstructed with optimal efficiency if the expectation values of a specific set of observables are known. The required observables only exist if it is possible to identify d mutually unbiased (MU) complex $(d \times d)$ Hadamard matrices, defining a complete set of $d + 1$ MU bases.

This thesis is an exploration of sets of $r \leq d + 1$ MU bases in low dimensions. We derive all inequivalent sets of MU bases in dimensions two to five confirming that in these dimensions, the complete sets of $(d + 1)$ MU bases are unique. In dimension six, we prescribe a first Hadamard matrix and construct all others mutually unbiased to it, using algebraic computations performed by a computer program. We repeat this calculation many times, sampling all known complex Hadamard matrices, and never find more than two that are mutually unbiased. We also study subsets of a complete set of MU bases by considering sets of pure states which satisfy the desired properties. We use this concept to provide the strongest numerical evidence so far that no seven MU bases exist in dimension six.

In the final part of the thesis, we introduce a new quantum key distribution protocol that uses d-level quantum systems to encode an alphabet with c letters. It has the property that the error rate introduced by an intercept-and-resend attack is higher than the BB84 or six-state protocols when the legitimate parties use a complete set of MU bases.

Contents

List of Figures

List of Tables

Preface

Two quantum tests are called complementary when the outcomes of one test reveal no information about the outcome of the other test. Mathematically, this concept is captured by the notion of mutually unbiased bases. Two complementary quantum tests are described by a pair of mutually unbiased (MU) bases. In recent years, the construction of sets of two or more MU bases has been an active topic of research. Perhaps because the problem appears so innocent to state, the challenge of finding a complete set of $d + 1$ MU bases in any dimension, d, has fascinated me and many other mathematicians and physicists. That is not to say that the problem is purely mathematical: it relates to some of the fundamental aspects of quantum mechanics. A complete set of MU bases enables one to determine an unknown quantum state with optimal efficiency and allows two parties to implement a quantum key distribution protocol that is sensitive to eavesdropping.

For prime-power dimensions there are several ingenious methods to construct a complete set of MU bases making use of, for example, finite fields, the Heisenberg-Weyl group, generalised angular momentum operators, and identities from number theory. However, even for the smallest composite dimension $d = 6$, the existence of such a set remains an open problem. It is unknown for a qubit-qutrit system whether there exists a set of observables that would realise optimal state tomography. This distinction between composite and prime-power dimensions poses a potentially

deep question about the structure of quantum systems. For example, one would expect that the kinematics of systems of dimension $d = 2 \times 3$ to be structurally similar to those of dimension $d = 3 \times 3$. The notion of mutually unbiased bases appears to invalidate that expectation.

I begin Chapter 1 with a detailed account of MU bases and their role in quantum mechanics. Emphasis is given to the two main applications of sets of MU bases since they motivate the claim that complementary quantum tests are special in the formalism of quantum mechanics. Chapter 1 ends with a review of the current state of research on MU bases and explains how my work fits into this setting. There are many approaches to this problem and although I have not attempted to include them all, I hope to have summarised the main results.

Sets of MU bases are intimately linked to complex Hadamard matrices. Any set of $r + 1$ MU bases can be written in a standard form consisting of r complex Hadamard matrices and the identity matrix, I. The main thrust of this thesis is provided by a simple idea: given a Hadamard matrix, H, one can construct sets of MU bases by extending the pair of bases $\{I, H\}$ to a larger set of MU bases $\{I, H, K, \ldots\}$.

All complex Hadamard matrices in dimensions two to five are known. In Chapter 2, I make use this fact to derive all inequivalent sets of MU bases in low dimensions. This classification leads to some interesting conclusions such as the fact that a complete set of $d + 1$ MU bases is unique in dimensions below six. In dimension six, the landscape of complex Hadamard matrices is far more complicated and the classification of all Hadamards is incomplete. However, we can still ask if any *known* Hadamard matrix can be part of a complete set of MU bases in dimension six? The results presented in Chapter 3 suggest that the answer to this question is likely to be negative. That is, in order to construct a complete set of MU bases in dimension six, it is probable that we must find six new complex Hadamard matrices.

In Chapters 4 and 5 I try to address the *global* nature of the problem. First, in Chapter 4, by numerical means where we search for subsets of MU bases. I feel that this numerical evidence makes it highly unlikely that a complete set of MU bases exist in dimension six. Then in Chapter 5, I explore three algorithms that *could* provide a no-go theorem in dimension six if they were successfully implemented. Unfortunately, the computational difficulty of these methods means that, for now at least, the existence of seven MU bases in dimension six remains an open problem.

I was first attracted to the field of Quantum Information by the applications such as quantum computation and quantum cryptography which perform tasks using quantum systems. In particular, the beautifully simple idea of Bennett and Brassard (now called the BB84 protocol), allows two parties to share a key in such a way that an eavesdropper can be detected. Hence I was very pleased to come across a new quantum key distribution protocol which is presented in Chapter 6. It fits nicely into the thesis because the protocol is *optimal* when the legitimate parties use a complete set of mutually unbiased bases.

Acknowledgements

I would particularly like to thank my supervisor Stefan Weigert who has been encouraging throughout the three years of my Ph.D. I appreciate the freedom he gave me to find my own research topic and have enjoyed our many discussions in the department and over lunch. He has always found time to meet or comment on written notes despite having many departmental duties. I am also very grateful to Tony Sudbery for many interesting and illuminating conversations and for introducing me to mutually unbiased bases.

It has been a pleasure spending the last three years in the Department of Mathematics at the University of York. Discussions with the various participants of the Quantum Information Seminar over the years are gratefully acknowledged and in particular with the other Ph.D. students in the group; Paul Butterley, Leon Loveridge and Bill Hall. I would also like to thank my office mates Nassraddin Ghroda, Lubna Shaheen and Phil Walker for making the experience all the more enjoyable. There have been three visitors to the Department who have particularly influenced my research; Ingemar Bengtsson and Marcus Appleby who both spoke about mutually unbiased bases and a related topic, SIC POVMs; and Subhash Chaturvedi whose question got me started on the numerical search presented in Chapter 4. I am also grateful for e-mail correspondence with Mate Matolcsi.

The calculations in Chapter 4 have been performed on the White Rose Grid provided by the Universities of Leeds, Sheffield and York. I would like to thank Mark Hewitt and Aaron Turner, who run its node at York, for their help in using the grid.

Author's declaration

The classification of all mutually unbiased bases in dimensions two to five as presented in Chapter 2, is available as a preprint at arXiv.org [34]. This paper was written in collaboration with S. Weigert and I. Bengtsson. The results relating to dimensions two to four were found by myself and S. Weigert, and independently by I. Bengtsson. The classification of all mutually unbiased bases in dimension five was found by myself and S. Weigert in roughly equal proportions. The material of Chapter 3 has been published in [33]. The numerical search for sets of mutually unbiased states presented in Chapter 4 has been published in [32]. These two papers where written in collaboration with S. Weigert with the ideas being roughly equal between the two of us. The ideas of Chapter 5 came from myself. The new quantum key distribution protocol in Chapter 6 has been obtained by myself and has been presented as a paper on the lanl pre-print server arXiv.org [31]. The computer programs and the computations of Chapters 3, 4 and 5 were written and performed my myself. The results of Chapter 5 and the two programs for MatLab and Python in the Appendix have not been published before.

CHAPTER 1

Introduction and background

The mathematical formalism of finite-dimensional quantum systems is surprisingly rich. In recent years, this setting has led to many important discoveries such as the no-cloning theorem [151], quantum teleportation [19], dense coding [20], quantum computing [50] and quantum cryptography [17, 148]. These examples are interesting from a foundational perspective because they explore the nature of quantum systems and the difference between quantum and classical mechanics. Many of these applications at the intersection of quantum mechanics and information theory also have the potential to be enormously useful.

Two-dimensional quantum systems are often called qubits in analogy to bits, their classical counterparts in computer science. As with classical bits, qubits have the property that the outcomes of any measurement are either zero or one. What makes qubits different is that quantum mechanics allows the existence of a superposition of the states labelled by 0 and 1. Systems consisting of many qubits can be used as the computational register for a quantum computer. The ability to realise such systems and perform certain operations on the qubits would allow one to implement a quantum algorithm. A particularly important quantum algorithm was provided by Shor in 1995 [134]. Shor's algorithm factorises an integer, N, into the product of primes in *polynomial* time; the number of operations in the algorithm is bounded by a polynomial

in the number of digits in N. Since there is no known classical algorithm that can achieve this, quantum mechanics appears to offer an exponential speed-up for this computational task.

There are many difficulties involved in realising a quantum computer in practice despite the considerable efforts reviewed in [113]. The preparation of a quantum register that remains coherent throughout the computation is very hard. The necessity of adding additional qubits in order to perform quantum error correction means that it is unlikely that a quantum computer will outperform a classical computer in the near future.

An application of quantum mechanics for discrete systems that is closer to wholesale realization is quantum cryptography. This beautifully simple idea is perhaps the first application of quantum mechanics at a microscopic level that has a commercial potential (see [70] for a review of the state of the art). A quantum key distribution protocol allows two parties to generate a shared key. In an ideal experiment, the properties of quantum systems mean that the legitimate parties can be certain that any eavesdropper has no knowledge of the key. This is in stark contrast to classical methods of distributing a key in which the security of the protocol is based on the computational difficulty of solving certain mathematical problems. The security of classical key distribution protocols is therefore conditional on a lack of future mathematical and computational advances. We will return to this subject later in this chapter: the key point is that by examining the mathematical setting of quantum mechanics, it is possible to find applications that go beyond classical results.

We begin with a property of quantum measurements found in any good text book on quantum mechanics [115]. The outcomes of a non-degenerate measurement of a discrete quantum system are described by an orthogonal basis $\mathcal{B} = \{|\psi_1\rangle, \ldots, |\psi_d\rangle\}$ of the complex linear space $\mathbb{C}^d$. There are many other sets of vectors that span $\mathbb{C}^d$ but quantum mechanics uses *orthogonal* vectors. We will be interested in the properties of one basis relative to another. In Section 1.1, we will argue that quantum mechanics prefers sets of bases which have a certain orthogonality property.

The space of density operators is a vector space provided we choose the origin to be the totally mixed state, $\frac{1}{d}I \equiv \frac{1}{d}\sum_{j=1}^{d} |j\rangle\langle j|$. In this setting, a basis of $\mathbb{C}^d$ defines a $d-1$ dimensional hyperplane spanned by the projectors $|\psi_j\rangle\langle\psi_j|$, $j = 1 \ldots d$. If two such hyperplanes are totally orthogonal we call the corresponding bases *mutually unbiased (MU)*. Writing this condition in

terms of the basis vectors leads to the usual definition of MU bases [16]: two orthonormal bases $\mathcal{B}^0 = \{|\psi_j^0\rangle, j = 1 \dots d\}$ and $\mathcal{B}^1 = \{|\psi_j^1\rangle, j = 1 \dots d\}$ of $\mathbb{C}^d$ are mutually unbiased if the modulus of the inner product of vectors from different bases is uniform,

$$|\langle\psi_i^0|\psi_j^1\rangle| = \frac{1}{\sqrt{d}}, \quad \text{for all} \quad i, j = 1 \dots d. \tag{1.1}$$

For example, in dimension $d = 2$, the bases defined by

$$\mathcal{B}^0 = \{|0\rangle, |1\rangle\} \text{ and } \mathcal{B}^1 = \left\{ \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right) \right\}, \tag{1.2}$$

are mutually unbiased.

Mutually unbiased (MU) bases are not purely a mathematical construct; they have a direct physical interpretation. The observables that correspond to two MU bases are *complementary*. A measurement of one of the observables reveals no information about the outcomes of the other. Following a measurement of observable $\mathcal{O}_1$, the outcomes of a complementary observable, $\mathcal{O}_2$, are all equally likely. For example, measuring the polarization of a photon in the vertical versus horizontal linear directions, reveals no information about the polarization in either the $\pm 45^\circ$ diagonal or circular polarizations. These three measurements are described by the three Pauli operators σ_x, σ_y and σ_z and have the property that the eigenstates of the operators form a set of MU bases. A natural question is to ask how many MU bases are there for quantum systems of arbitrary dimensions? We would like to understand the mathematical structure of quantum systems comprising of n qubits, $d = 2^n$, or more generally n qu*dits*, $d = d_1 \dots d_n$, with possibly different dimensions $d_1, \dots, d_n$.

Each basis in the space $\mathbb{C}^d$ consists of d orthogonal unit vectors which, collectively, will be thought of as a unitary $d \times d$ matrix. Two (or more) MU bases thus correspond to two (or more) unitary matrices, one of which can always be mapped to the identity, I, acting on the space $\mathbb{C}^d$, using an overall unitary transformation. It then follows from the conditions (1.1) that the remaining unitary matrices must be *complex Hadamard matrices*: the moduli of all their matrix elements equal $1/\sqrt{d}$.

A *complete set of MU bases* consists of d complex Hadamard matrices that are pair-wise mutually unbiased plus the standard basis, I. For example, in dimension $d = 3$, the four bases

$$\mathcal{B}^0 \simeq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \mathcal{B}^1 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$
$$\mathcal{B}^2 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} \qquad \mathcal{B}^3 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix} \tag{1.3}$$

where $\omega = e^{2\pi i/3}$ is a third root of unity, constitute a complete set of MU bases. Here, the columns of the matrix $\mathcal{B}^x$ correspond to the vectors $|\psi_i^x\rangle$, $i = 1 \ldots d$ of each basis.

It is not possible to find more than $d + 1$, totally orthogonal $d - 1$ dimensional hyperplanes in the space of density matrix since it has dimension $d^2 - 1$. Hence in any dimension a complete set contains the maximum number of MU bases [16]. Interestingly, given any set, $\mathcal{S}$, of d MU bases, it is always possible to construct an additional basis. The additional basis is given by the orthogonal complement of the d hyperplanes corresponding to the elements of $\mathcal{S}$. It has been shown that a basis constructed in this way is indeed a basis of d orthogonal vectors MU to each basis in $\mathcal{S}$ [147].

Here is the catch: as of today, complete sets of MU bases have been constructed only in spaces $\mathbb{C}^d$ of prime or prime-power dimension. If the dimension is a *composite* number, $d = 6, 10, 12, \ldots$, the existence of a complete set of MU bases in $\mathbb{C}^d$ has neither been proved nor disproved. Addressing this problem has led mathematicians and physicists to consider interesting connections between physics and mathematical structures. For example, constructing a complete set of MU bases in $\mathbb{C}^d$ is equivalent to finding an orthogonal decomposition of the Lie algebra $sl_d(\mathbb{C})$ [27]. This poses a long-standing open problem whenever d is not a power of a prime [93].

Sets of mutually unbiased bases are the primary subject of this thesis. In the next section we will give two important applications of MU bases that serve to motivate the claim that they

are "special" in the framework of quantum mechanics. We will explore the classification of all possible sets of MU bases for quantum systems of dimensions two to five. In dimension six, we find that such a classification is highly non-trivial and will address the open problem concerning the existence of seven MU bases. In the final part of the thesis, we will further explore the mathematical setting of quantum mechanics for discrete systems to find a new way of generating a shared key. An analysis of this new protocol reveals that it is more sensitive to an attack by a third party when the legitimate parties use a complete set of MU bases.

1.1 Using mutually unbiased bases

In this section, we present two applications which serve to demonstrate the role mutually unbiased bases play in quantum mechanical systems. The intuition is that MU bases are useful for *finding* and *hiding* quantum information. First we will show that a complete set of $d+1$ MU bases are optimal in quantum state tomography; they minimise the statistical uncertainty of the estimated density matrix. Second, we will see that sets of MU bases can be used to hide information from an eavesdropper during a quantum key distribution protocol. An amusing additional application of MU bases is in the so called Mean King's problem where a stranded physicist must escape a king by correctly guessing the outcome of a quantum measurement [6, 59, 144].

1.1.1 Optimal state determination

Pairs of MU bases represent measurements that were called "maximally non-commuting" by Schwinger [130]: a measurement in one of the bases reveals no information about the outcome of measurements in the other basis. Ivanović [83] was the first to realise that a set of $d+1$ bases that are all pair-wise mutually unbiased could be applied to quantum state reconstruction.

Suppose there is a source producing identical copies of some unknown quantum state described by a density matrix, ρ. Since ρ is a $d\times d$ Hermitian matrix with $\mathrm{Tr}\,\rho = 1$, we must determine d^2-1 real variables [63]. A non-degenerate projective measurement yields d probabilities which sum to one so that each measurement performed on a sub-ensemble of states can be used to determine $d-1$ variables. A quick calculation reveals that we require at least $(d^2-1)/(d-1) = d+1$

projective measurements.

Ivanović demonstrated that $d+1$ MU bases are also *sufficient* to determine any density matrix [83]. For example, in dimension two, any density matrix may be expressed as

$$\rho = \frac{1}{d} I + \mathbf{r} \cdot \boldsymbol{\sigma}, \tag{1.4}$$

where $\mathbf{r}$ is a vector in the 3-sphere of radius one (called the Bloch ball) and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)^T$ is a vector of the Pauli matrices σ_x, σ_y and σ_z. By performing measurements corresponding to the three Pauli matrices on multiple copies of ρ, we are able to determine the vector $\mathbf{r}$ up to some statistical accuracy. Therefore this set of $2 + 1$ bases, whose eigenvectors form a complete set of MU bases, are sufficient to estimate any 2×2 density matrix ρ.

Eq. (1.4) also demonstrates that there are many other possible choices for an *informationally complete* set of measurements. In fact, any set of three bases can replace the Pauli operators $\boldsymbol{\sigma}$, provided their corresponding vectors in the Bloch ball are not coplanar. The key step forward in understanding the power of MU bases in state tomography was provided by Wootters and Fields. They showed that a complete set of MU bases are the *optimal* choice of measurement settings in any dimension because they minimise the statistical uncertainty of the estimated state [150]. Intuitively, this can be seen as follows. Any finite set of measurement outcomes always results in some statistical uncertainty; there is some imprecision in determining the d probabilities corresponding to each measurement. Hence we should visualise each measurement not as a definite $d-$dimensional hyperplane but as some "pancake" with volume defined by the uncertainty in the measurement outcomes. The precision in the re-constructed state is then described by the overlap of the "pancakes" corresponding to each measurement. Wootters and Fields proved that in order to minimise this overlap we must perform $d + 1$ measurements that correspond to orthogonal hyperplanes, i.e. a complete set of MU bases [150].

1.1.2 Quantum key distribution

By sharing a random string of numbers, two parties can encrypt a message in such a way that it appears completely random to an eavesdropper. The "one-time pad" is an unbreakable method

of encryption provided the string is truly random and only used once [131]. The problem comes in having sufficiently many strings, called keys, with which to encrypt all messages you wish to send. This is called the key distribution problem.

By allowing the security of the key distribution protocol to be *computationally* impossible rather than unconditional, several ingenious methods to distribute keys have been developed. Assuming that an eavesdropper does not posses an infinitely large computer, cryptographic systems can make use of mathematical problems that are very hard to solve. For example, there is no known efficient algorithm to factorize large integers into a product of primes (used in the Rivest-Shamir-Adleman algorithm [121]) or to compute the discrete logarithm (used in the Diffe-Hellman-Merkle key exchange [52, 77]). However, solving these problems is only difficult, not impossible, so that the security of such public key protocols relies on the lack of future developments in mathematics and technology.

In 1970, Wiesner proposed a totally new approach to cryptography [148] that was developed by Bennet and Brassard: they presented a key distribution protocol [17], now known as BB84, that uses properties of quantum systems to ensure its security. This protocol allows two parties, Alice and Bob, to distribute a key such that anyone who attempts to listen in on the quantum signals can, in theory, be detected. The eavesdropper, Eve, is constrained by the physical laws of quantum mechanics. She cannot perform a measurement without introducing a disturbance (Heisenberg's uncertainty principle), copy states (no cloning) or split the signal, since it consists of single photons or particles. Other protocols such as Ekert's [57] use *entangled* particles in such a way that Eve essentially introduces hidden variables destroying the quantum correlations. It is possible to prove that these quantum key distribution (QKD) protocols are secure against all future technological and mathematical advances [106, 135]. Except possibly a new theory of physics that allows operations beyond quantum mechanics (cf. Popescu-Rohrlich boxes [118]).

The original BB84 protocol and its subsequent generalisation to d-dimensional systems exploit the complementarity of MU bases in order to ensure their security. By defining a protocol that uses *any* bases, Phoenix argues that the MU bases used in the original BB84 are the best choice of bases for the legitimate parties to detect an eavesdropper [117]. In other words, MU bases are optimal for this quantum key distribution protocol. In Chapter 6, we will formulate a new

protocol that allows Alice and Bob to use d-level quantum systems in order to generate a key with elements taken from an alphabet containing c letters. By considering a suitable measure of distance between the bases used by all three parties, we will see that, again, $d+1$ MU bases are optimal in a well defined sense.

1.2 Existing results and overview

In this section, we review what is known about mutually unbiased bases in $\mathbb{C}^d$ and explain how the results included in this thesis fit into this background. Roughly speaking, the results about sets of MU bases fall in to one of four groups. First, there are efforts to construct sets of r MU bases in particular dimensions such as a prime-power or square dimensions. The second type of result concerns ruling out sets of MU bases that have a certain form; for example, it has been shown that a complete set of MU bases cannot be constructed in dimension six using 12^{th} roots of unity alone. Next, there are numerical results which search for a set of MU bases such as four MU bases in dimension six, where none have been found analytically. Finally, there are algorithmic methods of of finding or proving the non-existence of a complete set of MU bases. They work in theory but as yet have been unsuccessful in practice due to the computational complexity of the algorithm. Under these broad headings, we now summarise existing results and explain how each of the four Chapters 2-5 adds an extra piece of the puzzle to this long-standing problem. We have not attempted to provide an exhaustive review of all results but hope to have included the main contributions.

1.2.1 Constructing MU bases in particular dimensions

We begin with existing methods of constructing a set of $r \leq d+1$ mutually unbiased bases. As noted in the previous discussion, there is no construction which provides a complete set of MU bases in all dimensions. We find that existing constructions are either restricted to dimensions that take a certain form or do not provide $d+1$ bases.

The first construction is due to Ivanović [83] and Alltop [3] who independently found that there exists a complete set of MU bases in prime dimension $d = p$, for any prime $p \neq 2$. A set

of $p+1$ MU bases consists of the standard basis plus p bases whose matrix elements (which run from 0 to $p-1$) are given by

$$(H^a)_{kl} = \frac{1}{\sqrt{p}}\omega^{al^2+kl} \tag{1.5}$$

where $a = 0 \ldots p-1$ labels the basis and $\omega = \exp(2\pi i/p)$ is a root of unity. Applying this construction to dimension three gives the set of 4 bases in Eq. (1.3). Note that, by defining the discrete Fourier matrix, F, whose elements are given by $F_{kl} = \frac{1}{\sqrt{d}}\omega^{kl}$, there is a neat way of writing this formula that will be useful later. The complete set of MU bases given by Eq. (1.5) can be written in matrix form as [62]

$$\{I, F, DF, D^2F, \ldots D^{p-1}F\},$$

where the diagonal matrix D that pre-multiplies F has non-zero entries ω^{l^2}, for $l = 0 \ldots p-1$.

Using the theory of finite fields, Wootters and Fields extended the construction of Ivanović and Alltop to all dimensions that are a power of an odd prime, $d = p^n$ [150]. Their construction essentially uses the same formulae as Eq. (1.5) but the expression $al^2 + kl$ is replaced by its number theoretic generalisation, $\mathrm{Tr}(al^2+kl)$. Here, we use the field theory trace (see for example [100]) and the indices, a, k and l take values from a field with p^n elements. An important addition is that Wootters and Fields also give a construction for n qubits, that is, for dimensions that are a power of two, $d = 2^n$. A complete set of MU bases for systems consisting of multiple qubits is very useful as it allows for typical applications in quantum information. Interestingly, the set of $d+1$ MU bases constructed by Wootters and Fields can also be expressed in terms of characters of the cyclic group, G of order p [45].

An alternative construction for prime powers $p^n \geq 5$ is obtained by replacing the polynomial al^2+kl, the exponent of ω in Eq. (1.5), by $\mathrm{Tr}((l+a)^3+k(l+a))$ [89]. Klappenecker and Roetteler also found that the formula $\mathrm{Tr}((a+2k)l)$ where a, k and l are now elements of a subset of the Galois ring called a Teichmüller set, gives a complete set of MU bases in dimensions that are a power of two [89].

Bandyopadhyay et al. [9] provide an alternative proof that a complete set of MU bases exists

in all prime-power dimensions. They construct sets of MU bases from the eigenvectors of special unitary operators. In fact, Schwinger noted that the eigenvectors of the operators Z and X, defined by the actions $Z|j\rangle = \omega^j|j\rangle$ and $X|j\rangle = |j+1\rangle$, are mutually unbiased [130]. In prime dimensions $d = p$, this set of two MU bases can be extended to a complete set of $p+1$ bases given by the eigenvectors of the generalised Pauli matrices [9]

$$\left\{Z, X, XZ, \ldots, XZ^{d-1}\right\}.$$

The resulting set of bases is equal to the construction of Ivanović given in Eq. (1.5). In prime-power dimensions $d = p^n$, this approach also yields a complete set of MU bases. The operators are now elements of the *Pauli group* that act on the n-fold tensor product space $\mathbb{C}^p \otimes \mathbb{C}^p \otimes \cdots \otimes \mathbb{C}^p$. More explicitly, they have the form

$$\omega^j X(\alpha) Z(\beta), \tag{1.6}$$

where $j = 0 \ldots p-1$, the field elements $\alpha = (\alpha_1, \ldots, \alpha_n), \beta = (\beta_1, \ldots, \beta_n) \in \mathbb{F}_{p^n}$ and the operators labeled by α and β are given by $X(\alpha) = X^{\alpha_1} \otimes \cdots \otimes X^{\alpha_n}$ and $Z(\alpha) = Z^{\alpha_1} \otimes \cdots \otimes Z^{\alpha_n}$. The condition for the eigenvectors of elements of this group to form a complete set of MU bases is expressed in terms of α and β and leads to a direct representation of the corresponding complementary observables [9].

Durt has found a simple expression of the group elements (1.6) in terms of the additive characters of a field [55]. This allows one to relate multiplication of the MU bases to composition of group elements and construct the same complete set of MU bases in prime-power dimensions.

The group SU(2) can also be used to construct a complete set of MU bases in prime-power dimensions [88]. Again, the bases vectors are eigenvectors of a set of operators but in this approach the operators come from the theory of angular momentum. The study of subgroups of U(2) and their connection to MU bases is further developed in [2].

An alternative construction of the $d+1$ bases given in Eq. (1.5) in prime dimensions is provided by Combescure [46]. A complete set of MU bases follows if one is able to find a circulant

matrix, C, such that its powers are also circulant matrices. The bases are given explicitly as

$$\{I, F_d, C, C^2, ..., C^{d-1}\}, \tag{1.7}$$

where F_d is the discrete Fourier matrix and C has the property that it commutes with X and diagonalises XZ. The approach can also be applied to prime-power dimensions where it recovers the bases found by Wootters and Fields [47]. Interestingly, various properties of Gauss and quadratic Weil sums which were used by Wootters and Fields in their construction, follow from this construction of a complete set of MU bases [46, 47].

We say that a set of n vectors $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ in $\mathbb{C}^d$ span *equiangular* lines if $|\langle\psi_i|\psi_j\rangle| = \kappa$ for some constant κ and all $i, j = 1 \ldots n$. Hence the condition for two orthonormal bases to be mutually unbiased, Eq. (1.1), is the requirement that vectors from different bases be equiangular with $\kappa = 1/\sqrt{d}$. The value of the constant κ, is not arbitrary, it is implied by the relation $\sum_{j=1}^{d} |\psi_j\rangle\langle\psi_j| = I$. Another physically relevant set of equiangular lines corresponds to a symmetric informationally complete positive operator value measure (SIC POVM). Such a set of $d^2 - 1$ lines is as close to being an orthonormal basis for the space of quantum states as possible and are useful for quantum cryptography [68]. They also naturally appear when representing quantum states in terms of probabilities for the outcomes of a fixed counterfactual reference measurement [69].

Constructions of equiangular lines can be used to find a complete set of MU bases in prime-power dimensions [71]. This approach also allows Godsil and Roy [71] to prove that all *known* sets of d+1 MU bases in prime-power dimensions are special cases of a construction due to Calderbank et al. [42].

We have seen that there are several methods of constructing MU bases in dimensions of the form $d = p^n$ but what can be said about *composite* dimensions $d = 6, 10, 12, \ldots$? The first point is that we can always reduce the dimension to its prime-power constituents. We can write $d = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$ and use the prime-power construction to form $p_i^{n_i} + 1$ bases for each of the

subsystems. Then by forming the tensor product of these bases we can construct

$$\min(p_1^{n_1}, \ldots, p_r^{n_r}) + 1 \tag{1.8}$$

MU bases in any dimension [89].

At this point, one might have the feeling that all constructions essentially involve the prime-power decomposition of the dimension. However, this is not the case: in some square dimensions, $d = s^2$, one can do better than Eq. (1.8) [149]. For example, if $d = 2^2 \times 13^2$, a total of $6 > 2^2 + 1$ MU bases have been identified. The construction used by Wocjan and Beth differs from the prime-power constructions since it links sets of MU bases to orthogonal Latin squares [22, 23].

In addition, whilst Eq. (1.8) implies that there are at least three MU bases in all dimensions, it is also possible to construct *three* MU bases in $\mathbb{C}^d$ without reference to the value of d. The eigenvectors of the operators X, Z and XZ^k, where $\gcd(k, d) = 1$ form a set of three MU bases in any dimension d [72].

In Chapter 2 we will provide a new method of constructing MU bases that does not rely on any dimension dependent results as it uses only planar geometry. Unfortunately, the complexity of the resulting trigonometric equations means that we can only find their solutions in dimensions two to five. This approach has the added benefit that it *exhaustively* lists all possible sets of MU bases; we are thus able to provide a complete classification of all sets of $r \leq d + 1$ MU bases in dimensions $d \leq 5$.

1.2.2 MU bases of a specific form

The maximum number of MU bases in composite dimensions remains unknown. A natural approach to this problem is to search for sets of MU bases of a specific form. For example, one might notice that the constructions presented in [83], [150] and [89] are all based on number theoretic formulae and so search for similar or generalised formulae that work in composite dimensions. Alternatively, we might spot that all existing constructions of complete sets use roots of unity and so search through "sensible" choices of other roots of unity to find MU bases. Although none of these approaches have been successful in constructing $d + 1$ MU bases in

composite dimensions, one can say that they rule out a subset of all possible MU bases. As we become more convinced that complete sets in composite dimensions do not exist, we make the *exclusion* of MU bases of a certain form the goal that would ultimately lead to a complete solution to this long-standing problem. Many of the results that follow are directed at the first composite dimension, $d = 6$.

The constructions of complete sets of MU bases due to Ivanović, Wootters and Fields, and Klappenecker and Roetteler described above all have the form

$$(\mathcal{B}^a)_{kl} = \frac{1}{\sqrt{p}}\omega^{f(a,k,l)} \tag{1.9}$$

where $\omega = \exp(2\pi i/p)$ is a root of unity and $f(a, k, l)$ is a number theoretic function defined over a finite field or finite ring. Archer has shown that a natural generalisation of Eq. (1.9) can be used to construct a complete set of MU bases if and only if d is a power of a prime [7].

Eq. (1.5) and the subsequent generalization to prime-power dimensions by Wootters and Fields as well as the construction for dimensions of powers of two all have one thing in common: The components of the vectors are roots of unity. In prime-power dimensions the appropriate roots are $\omega = \exp(2\pi i/p)$ and for dimensions of the form 2^n we need to use 4^{th} roots. Therefore, in dimension 6, it is natural to suppose that a complete set of MU bases can be constructed using $3 \times 4 = 12^{\text{th}}$ roots of unity. By exhaustively listing all possible matrices with components that are 12^{th} roots, Bengtsson et al. [16] prove than no such combinations can form a complete set of MU bases. They further extend this result by considering all 48^{th}, 60^{th} and 72^{nd} roots of unity (and some algebraic numbers that appear when considering triples of MU bases in dimension six). However, none of the resulting plausible matrices form more than three MU bases in $\mathbb{C}^6$.

Grassl [72] has shown that only *finitely* many vectors exist which are MU with respect to the eigenvectors of the Pauli operators X and Z in $\mathbb{C}^6$. Again, no more than three MU bases emerge; it is thus impossible to base the construction of a complete set on the Pauli group in dimension six. The strategy of Chapter 3 will be to generalize Grassl's approach by removing the restriction that the second MU basis is related to the Heisenberg-Weyl group. Instead, we will consider many different choices for the second MU basis, thoroughly sampling the set of

candidates in $\mathbb{C}^6$. We will find that none of the matrices studied can be used to construct a complete set of MU bases.

Since the publication of [33], Jaming et al. have ruled out complete sets of MU bases that contain a two parameter extension of the basis related to the Heisenberg-Weyl group [84]. This was achieved by using an alternative global method. They are able to discretise the space of possible MU bases by finding suitable error bounds for two approximate bases to be MU. This allows one to exhaustively search a discrete set of phases which make up the components of potentially MU bases.

1.2.3 Numerical searches

We have seen that attempts to find a complete set of MU bases in composite dimensions by *analytical* methods have so far been unsuccessful. It is possible to cast the existence of sets of MU bases as a minimization problem. This is done by defining a positive function of appropriate parameters that equals zero if and only if the values of the parameters correspond to a set of MU bases. Approaching this global minimization problem by *numerical* means allowed Butterley and Hall to provide evidence for the non-existence of *four* MU bases in $\mathbb{C}^6$ [38].

In Chapter 4 we will strengthen the evidence of Butterley and Hall by searching for various MU *constellations* which correspond to *subsets* of four MU bases in dimension six. Taking these negative results together, we argue that this evidence makes the existence of a complete set of MU bases highly unlikely [32].

The general idea behind this approach is that by performing a search for *local* minima many times, we hope to cover the relevant parameter space sufficiently so that there is a low probability of missing the true *global* minimum. There are established techniques for finding a global minimum or at least a global lower bound. The application of these ideas to the existence of a complete set of MU bases is what we will discuss next.

1.2.4 Analytic solutions

The existence of sets of MU bases in dimension d concerns the global properties of the space $\mathbb{C}^d$. In Chapter 5, we make this explicit by providing three algorithmic methods which decide if a

complete set of MU bases exist in dimension d.

First, we express the problem as a system of coupled polynomials and use powerful techniques from commutative algebra to either find a solution or try to prove that none exists. These equations define an ideal and the construction of a Gröbner bases through Buchberger's algorithm simplifies its representation. If the equations have no solution over the algebraic closure of the real numbers then the ideal will be empty and Buchberger's algorithm will prove this. The second idea is to find a global lower bound on any of the functions used in the numerical search. This can be achieved using semidefinite programming after a suitable transformation of the problem and if the algorithm were to terminate the dual problem would provide a certificate of non-existence. The final approach is inspired by Jaming et al. who discretise the space of all possible bases so that it is possible to exhaustively check for MU bases.

If these algorithms were to terminate, we would have a proof that a complete set of MU bases do not exist in dimension six, for example. Unfortunately, these approaches appear to require a substantial amount of computational resources. We will provide a rough analysis of how they perform in Chapter 5, but for now at least the number of MU bases in composite dimensions remains unknown.

CHAPTER 2

All mutually unbiased bases in low dimensions

Traditionally, a Hadamard matrix H in dimension d is understood to have elements ± 1 only and to satisfy the condition $H^\dagger H = dI$, where I is the identity. In the context of MU bases, it is customary to call H a *Hadamard* matrix if it is unitary and its matrix elements are of the form

$$|H_{ij}| = \frac{1}{\sqrt{d}}\,, \qquad i,j = 0,1,\ldots,d-1\,. \tag{2.1}$$

The d vectors formed by the columns of such a matrix provide an orthonormal basis of $\mathbb{C}^d$. Each of these vectors is mutually unbiased with respect to the standard basis, naturally associated with the identity matrix I.

Two Hadamard matrices are *equivalent* to each other, $H' \approx H$, if one can be obtained from the other by permutations of its columns and its rows, and by the multiplication of its columns and rows with individual phase factors. Explicitly, the equivalence relation reads

$$H' = M_1 H M_2\,, \tag{2.2}$$

where M_1 and M_2 are *monomial* matrices, i.e. they are unitary and have only one nonzero element in each row and column. Consequently, each Hadamard matrix is equivalent to a *dephased*

Hadamard matrix, the first row and column of which have entries $1/\sqrt{d}$ only.

It is possible to list all pairs of MU bases $\{I, H\}$ in $\mathbb{C}^d$ once all complex Hadamard matrices are known. Using this observation as a starting point, we will extend the classification from pairs to sets of $r \leq (d+1)$ MU bases. As complex Hadamard matrices have been classified for $d \leq 5$, we expect to obtain an exhaustive list of sets of r MU bases in these low dimensions.

The task to find all MU bases is complicated by the fact that, actually, many sets of apparently different MU bases are identical to each other. For the desired classification, it is sufficient to enumerate all *dephased* sets of $(r+1)$ MU bases in analogue to dephased Hadamard matrices. This *standard form* [141] is given by

$$\{I, H_1, \ldots, H_r\}, \quad r \in \{1, \ldots, d\}, \tag{2.3}$$

where I is the identity in $\mathbb{C}^d$ and the other matrices are dephased Hadamard matrices. See Eqs. (1.3) for an explicit example with $d = 3$ and Eqs. (2.33) and (2.35) when $d = 5$. The possibility of dephasing is based on the notion of *equivalence classes* for MU bases, explained in more detail in Appendix A.

The results of this chapter have been arranged as follows. In Section 2.1 we deal with dimensions two and three. The complete list of sets of MU bases in dimension four is derived in Section 2.2. Then, all sets of MU bases of $\mathbb{C}^5$ are constructed, and in Section 2.4 we summarize and discuss our results.

2.1 Dimensions $d = 2$ and $d = 3$

In this section, we construct all sets of MU bases in dimensions two and three using only planar geometry. The direct approach to construct all MU bases for $d = 4$ in Section 2.2 will be based on similar arguments.

2.1.1 Dimension $d = 2$

The matrices consisting of the eigenvectors of the Heisenberg-Weyl operators form a set of three MU bases in dimension two which are unique up to the equivalences specified in Appendix A. We present a simple proof of this well-known fact.

Let us begin by noting that there is only one dephased complex Hadamard matrix in $d = 2$ (up to equivalences) [74], the discrete (2×2) Fourier matrix

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{2.4}$$

A vector $v \in \mathbb{C}^2$ is MU to the standard basis I (constructed from the eigenstates of the z-component of a spin 1/2) if its components have modulus $1/\sqrt{d}$. Applying the transformation given in Eq. (A.3), the dephased form of such a a vector reads $v = (1, e^{i\alpha})^T/\sqrt{2}$, with a real parameter $\alpha \in [0, 2\pi]$. The vector v is MU to the columns of F_2 if the phase α satisfies two conditions,

$$\left|1 \pm e^{i\alpha}\right| = \sqrt{2} . \tag{2.5}$$

These equations hold simultaneously only if $e^{i\alpha} = \pm i$. Thus, there are only two vectors which are MU to both I and F_2, given by $v_\pm = (1, \pm i)^T /\sqrt{2}$. Since this is a pair of orthogonal vectors, they form a Hadamard matrix $H_2 = (v_+|v_-)$ and, therefore, the three sets

$$\{I\} , \{I, F_2\} , \{I, F_2, H_2\} \tag{2.6}$$

represent all (equivalence classes of) one, two, or three MU bases in dimension two.

2.1.2 Dimension $d = 3$

In dimension three there is also only one dephased complex Hadamard matrix up to equivalence [74]. It is given by the (3×3) discrete Fourier matrix

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \tag{2.7}$$

defining $\omega = e^{2\pi i/3}$ which equals the basis $\mathcal{B}^1$ in Eq. (1.3). Again, we search for dephased vectors $v = (1, e^{i\alpha}, e^{i\beta})^T/\sqrt{3}$, $0 \leq \alpha, \beta \leq 2\pi$, which are MU with respect to the matrix F_3. This leads to the following three conditions

$$\begin{aligned} \left|1 + e^{i\alpha} + e^{i\beta}\right| &= \sqrt{3}\,, \\ \left|1 + \omega e^{i\alpha} + \omega^2 e^{i\beta}\right| &= \sqrt{3}\,, \\ \left|1 + \omega^2 e^{i\alpha} + \omega e^{i\beta}\right| &= \sqrt{3}\,. \end{aligned} \tag{2.8}$$

Removing an overall factor of $e^{i\alpha/2}$, they can be rewritten

$$\begin{aligned} \left|\zeta + \cos\frac{\alpha}{2}\right| &= \frac{\sqrt{3}}{2}\,, \\ \left|\zeta + \cos\left(\frac{\alpha}{2} \pm \frac{2\pi}{3}\right)\right| &= \frac{\sqrt{3}}{2}\,, \end{aligned} \tag{2.9}$$

where $2\zeta = e^{i(\beta - \alpha/2)}$. By considering a plot in the complex plane, Fig. 2.1, we see that these three equations hold simultaneously only if two of the cosine terms are equal. This implies that the only possible values of the parameter α are $0, \pi/3$, or $2\pi/3$, leading to the requirement

$\pm 1/2 = \cos\beta$. Consequently, the Eqs. (2.8) have exactly six solutions which give rise to vectors

$$\begin{aligned} v_1 &\propto \begin{pmatrix} 1 \\ \omega \\ \omega \end{pmatrix}, \quad v_2 \propto \begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \quad v_3 \propto \begin{pmatrix} 1 \\ 1 \\ \omega^2 \end{pmatrix}, \\ v_4 &\propto \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}, \quad v_5 \propto \begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix}, \quad v_6 \propto \begin{pmatrix} 1 \\ 1 \\ \omega \end{pmatrix}. \end{aligned} \tag{2.10}$$

Examining their inner products shows that there is only one way to arrange them (after normalization) into two orthonormal bases, namely $H_3^{(1)} = (v_1|v_2|v_3)$ and $H_3^{(2)} = (v_4|v_5|v_6)$. Hence, we have obtained the remaining two bases, $\mathcal{B}^2$ and $\mathcal{B}^3$, from Eq. (1.3). As noted in the introduction, one can write

$$H_3^{(1)} = DF_3 \quad \text{and} \quad H_3^{(2)} = D^2F_3\,, \tag{2.11}$$

where $D = \mathrm{diag}(1, \omega, \omega)$ is a diagonal unitary matrix with entries identical to the components of the vector v_1, i.e. the first column of $H_3^{(1)}$. The triples obtained from adding either $H_3^{(1)}$ or $H_3^{(2)}$ to the pair $\{I, F_3\}$ are equivalent,

$$\{I, F_3, H_3^{(1)}\} \sim \{D^2ID, D^2F_3, D^2H_3^{(1)}\} = \{I, H_3^{(2)}, F_3\} \sim \{I, F_3, H_3^{(2)}\}\,,$$

as follows from first applying the unitary D^2 globally from the left, rephasing the first basis with $D^{-2} \equiv D$, and finally rearranging the last two bases. We therefore conclude that the sets

$$\{I\}\,, \{I, F_3\}\,, \{I, F_3, H_3^{(1)}\}\,, \{I, F_3, H_3^{(1)}, H_3^{(2)}\}$$

constitute a complete classification of all sets of MU bases in dimension $d = 3$. Therefore, the set of bases given in Eq. (1.3) is the unique complete set of MU bases in dimension three.

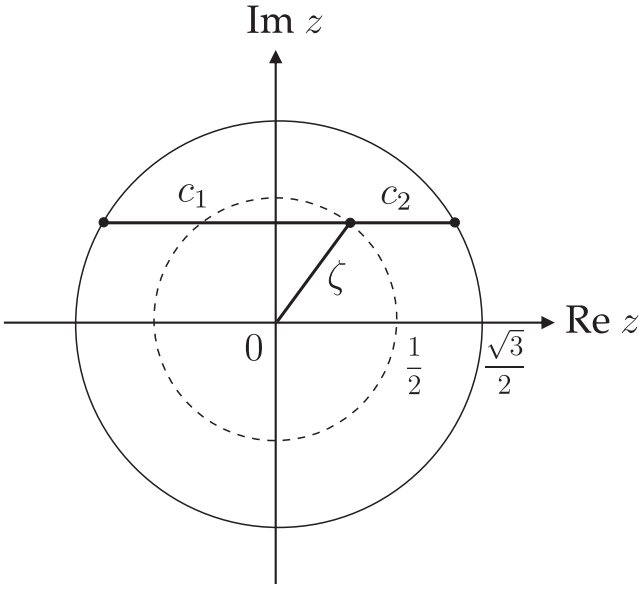

Figure 2.1: Plot of Eqs. (2.9) in the complex z-plane. The real numbers c_1 and c_2 each represent one of the three numbers $\cos(\alpha/2)$ and $\cos(\alpha/2 \pm 2\pi/3)$; it follows that at least two of these three expressions must be equal.

2.2 Dimension $d = 4$

In dimension $d = 4$, a one-parameter family [74] of complex Hadamard matrices exists,

$$F_4(x) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & ie^{ix} & -ie^{ix} \\ 1 & -1 & -ie^{ix} & ie^{ix} \end{pmatrix}, \quad x \in [0, \pi)\,. \tag{2.12}$$

When $x = 0$, the resulting matrix is equivalent to the discrete Fourier transform F_4 on the space $\mathbb{C}^4$, with matrix elements given by $\omega^{jk}, j, k = 0 \ldots 3, \omega \equiv i$. The matrix $F_4(\pi/2)$ is equivalent to a direct product of the matrix F_2 with itself while for other values of x it can be written as a Hadamard product of F_4 with an x-dependent matrix.

2.2.1 Constructing vectors MU to $F_4(x)$

After dephasing, any vector MU to the standard basis takes the form $v = (1, e^{i\alpha'}, e^{i\beta'}, e^{i\gamma'})^T/2$ where $0 \leq \alpha', \beta', \gamma' < 2\pi$. For convenience, we will use an *enphased* variant of v. Multiplying through by the phase factor $e^{-i\alpha'/2}$ and defining $\alpha = \alpha'/2 \in [0, \pi]$, $\beta = \beta' - \alpha'/2 \in [0, 2\pi)$, and similarly for γ, we consider the parametrization $v = (e^{-i\alpha}, e^{i\alpha}, e^{i\beta}, e^{i\gamma})^T/2$ instead. The conditions for $v(\alpha, \beta, \gamma)$ to be MU to the columns of $F_4(x)$ lead to four equations,

$$\left|\cos\alpha \pm \zeta_+\right| = 1\,, \tag{2.13}$$

$$\left|\sin\alpha \pm e^{-ix}\zeta_-\right| = 1\,, \tag{2.14}$$

where complex numbers $\zeta_\pm = (e^{i\beta} \pm e^{i\gamma})/2$ have been introduced. We will now construct all solutions of these equations as a function of the value of x. We treat the cases (i) $\alpha = 0$, (ii) $\alpha = \pi/2$, and (iii) $\alpha \neq 0, \alpha \neq \pi/2$ separately since the Eqs. (2.13) and (2.14) take different forms for these values.

(i): $\alpha = 0$

Eqs. (2.14) simplify to the pair $\left|\pm e^{-ix}\zeta_-\right| = 1$, which only hold simultaneously if $|\zeta_-| = 1$ or $e^{i\gamma} = -e^{i\beta}$, implying that $\zeta_+ = 0$ so that Eqs. (2.13) are satisfied automatically. Thus, solutions exist for any value of x whenever $\beta = \gamma + \pi \pmod{2\pi}$, and the resulting vectors can be written as $v(\beta) = \left(1, 1, e^{i\beta}, -e^{i\beta}\right)^T/2$, with $\beta \in [0, 2\pi)$. It will be convenient to divide this family of states into two sets,

$$h_1(y) = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ e^{iy} \\ -e^{iy} \end{pmatrix},\ h_2(y') = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -e^{iy'} \\ e^{iy'} \end{pmatrix}, \qquad 0 \leq y, y' < \pi, \tag{2.15}$$

introducing $y = \beta$ and $y' = \pi + \beta$.

(ii): $\alpha = \pi/2$

Eqs. (2.13) and (2.14) now reverse their roles: the conditions $|\pm\zeta_+| = 1$ require $e^{i\gamma} = e^{i\beta}$, with (2.13) being satisfied since $|\zeta_-| = 1$ follows immediately. Hence, there is another one-parameter family of mutually unbiased vectors for all values of x if $\beta = \gamma$. This family can be written as $v(\varphi) = \left(1, -1, e^{i\varphi}, e^{i\varphi}\right)^T/2$, $\varphi \in [0, 2\pi)$, after dephasing and absorbing a factor of i in the definition of the phase, $\varphi = \pi/2 + \beta$. Again, we express these solutions as a set of pairs,

$$h_3(z) = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ e^{iz} \\ e^{iz} \end{pmatrix}, \; h_4(z') = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -e^{iz'} \\ -e^{iz'} \end{pmatrix}, \qquad 0 \le z, z' < \pi, \tag{2.16}$$

where $z = \varphi$ and $z' = \pi + \varphi$.

(iii) $\alpha \neq 0, \alpha \neq \pi/2$

A plot in the complex plane (see Fig. 2.2) reveals that one must have $\zeta_+ = \pm \mathrm{i} \sin\alpha$ if Eqs. (2.13) are to hold with $\cos\alpha \neq 0$. Thus, the real part of ζ_+ vanishes,

$$\cos\beta + \cos\gamma = 0 \tag{2.17}$$

with $\gamma = \pi - \beta \pmod{2\pi}$ being the only acceptable solution: the other solution, $\gamma = \pi + \mathrm{mod}\ 2\pi)$ leads to $0 = \zeta_+ = \pm \mathrm{i} \sin\alpha$, producing a contradiction since $\alpha \neq 0$. Thus, using $\gamma = \pi - \beta \pmod{2\pi}$, we obtain $\zeta_+ = i \sin\beta$ find the following relation between α and β:

$$\pm \sin\alpha = \sin\beta\,. \tag{2.18}$$

Similarly, Eqs. (2.14) for $\sin\alpha \neq 0$ imply that $e^{-ix}\zeta_- = \pm i \cos\alpha$. Using $\gamma = \pi - \beta \pmod{2\pi}$ in the definition of ζ_-, we find $\zeta_- = \cos\beta$, so that

$$i(\pm\cos\alpha + \sin x \cos\beta) = \cos x \cos\beta. \tag{2.19}$$

The right-hand-side of this equation only vanishes if $x = \pi/2$: both $\beta = \pi/2$ and $\beta = 3\pi/2$ would, according to (2.18), require $\alpha = \pi/2$ which we currently exclude. Therefore, solutions to Eqs. (2.13,2.14) with $\alpha \neq 0$ or $\alpha \neq \pi/2$ only exist for $x = \pi/2$ if a second relation between α and β holds,

$$\pm \cos\alpha = \cos\beta \,. \tag{2.20}$$

The form of the additional MU vectors is determined by Eqs. (2.18) and (2.20) which have four solutions. First, for $\beta = \alpha$ we obtain MU vectors of the form $(e^{-i\alpha}, e^{i\alpha}, e^{i\alpha}, -e^{ia})^T/2$ or $\left(1, e^{2i\alpha}, e^{2i\alpha}, -1\right)^T/2$ after dephasing. Splitting this family into two subsets as before, we find

$$k_1 = \frac{1}{2}\begin{pmatrix} 1 \\ e^{it} \\ e^{it} \\ -1 \end{pmatrix}, \; k_2 = \frac{1}{2}\begin{pmatrix} 1 \\ -e^{it'} \\ -e^{it'} \\ -1 \end{pmatrix}, \quad 0 \leq t, t' < \pi \,. \tag{2.21}$$

Similarly, the choice $\beta = \pi + \alpha \pmod{2\pi}$ leads to two sets of dephased MU vectors,

$$k_3 = \frac{1}{2}\begin{pmatrix} 1 \\ e^{iu} \\ -e^{iu} \\ -1 \end{pmatrix}, \; k_4 = \frac{1}{2}\begin{pmatrix} 1 \\ -e^{iu'} \\ e^{iu'} \\ -1 \end{pmatrix}, \quad 0 \leq u, u' < \pi \,. \tag{2.22}$$

Next, when proceeding in an entirely analogous manner for the remaining two choices $\beta = \pi - \alpha \pmod{2\pi}$ and $\beta = 2\pi - \alpha \pmod{2\pi}$, we obtain the following four families of dephased vectors MU to $F_4(\pi/2)$,

$$j_1 = \frac{1}{2}\begin{pmatrix} 1 \\ e^{ir} \\ -1 \\ e^{ir} \end{pmatrix}, \; j_2 = \frac{1}{2}\begin{pmatrix} 1 \\ -e^{ir'} \\ -1 \\ -e^{ir'} \end{pmatrix}, \; j_3 = \frac{1}{2}\begin{pmatrix} 1 \\ e^{is} \\ 1 \\ -e^{is} \end{pmatrix}, \; j_4 = \frac{1}{2}\begin{pmatrix} 1 \\ -e^{is'} \\ 1 \\ e^{is'} \end{pmatrix}, \tag{2.23}$$

with $0 \leq r, r', s, s' < \pi$.

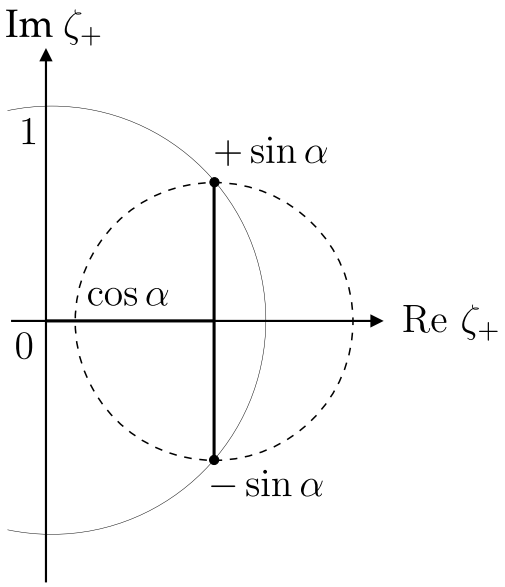

Figure 2.2: Plot of Eqs. (2.13) in the ζ_+-plane implying that, for $\cos\alpha \neq 0$, their solutions are given by $\zeta_+ = \pm \mathrm{i} \sin\alpha$.

2.2.2 Forming MU bases

Knowing all vectors that are MU to both the identity and F_4, we now determine those combinations which allow us to form other bases.

Triples of MU bases in $\mathbb{C}^4$

To begin, consider the MU vectors $h_1, \ldots, h_4$, in Eqs. (2.15) and (2.16) which exist for all values of $x \in [0, \pi)$. Calculating their inner products, one finds that they only form an *orthonormal* basis of $\mathbb{C}^4$ if $y = y'$ and $z = z'$. Thus, for each value of x, the pair $\{I, F_4(x)\}$ may be complemented

by a third MU basis taken from the two-parameter family

$$H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \end{pmatrix}. \tag{2.24}$$

In other words, there is a *three parameter-family of triplets* of MU bases $\{I, F_4(x), H_4(y,z)\}$ in dimension $d = 4$. This agrees with the result obtained by Zauner by other means [152].

If $x = \pi/2$, additional MU vectors $j_1, \ldots, j_4$, and $k_1, \ldots, k_4$, have been identified, cf. Eqs. (2.21-2.23). Calculating the scalar products within each group, one sees that two further orthonormal two-parameter bases emerge,

$$J_4(r,s) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ e^{ir} & -e^{ir} & e^{is} & -e^{is} \\ -1 & -1 & 1 & 1 \\ e^{ir} & -e^{ir} & -e^{is} & e^{is} \end{pmatrix}, \tag{2.25}$$

$$K_4(t,u) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ e^{it} & -e^{it} & e^{iu} & -e^{iu} \\ e^{it} & -e^{it} & -e^{iu} & e^{iu} \\ -1 & -1 & 1 & 1 \end{pmatrix}, \tag{2.26}$$

if the conditions $r = r'$, $s = s'$, and $t = t'$, $u = u'$, respectively, are satisfied. No other combinations of the MU vectors can form inequivalent bases so that the matrices in Eqs. (2.24-2.26) represent all possible choices of a MU basis. Permuting appropriate rows and columns of the matrices J_4 and K_4 transforms them into H_4; thus, the triples $\{I, F_4(\pi/2), J_4(r,s)\}$ and $\{I, F_4(\pi/2), K_4(t,u)\}$ are equivalent to $\{I, F_4(\pi/2), H_4(y,z)\}$.

Quadruples and quintuples of MU bases in $\mathbb{C}^4$

Let us begin by noting that sets of four MU bases cannot exist away from $x = \pi/2$. No two matrices $H_4(y, z)$ and $H_4(y', z')$ are MU since

$$\left|h_1^\dagger(y)h_1(y')\right| = \left|h_1^\dagger(y)h_2(y')\right| = \frac{1}{2} \tag{2.27}$$

only hold if

$$\left|1 \pm e^{i(y-y')}\right| = 1\,; \tag{2.28}$$

however, these equations have no solution for any values of y and y'. A similar argument shows that there are no values of z and z' such that the matrices $H_4(y, z)$ and $H_4(y, z')$ are MU.

We now show that for $x = \pi/2$ the bases $H_4(y, z), J_4(r, s)$ and $K_4(t, u)$ give rise to four and five MU bases if the free parameters are chosen appropriately. An argument similar to the one just presented shows that no two bases within either the family $J_4(r, s)$ or $K_4(t, u)$ are MU. Thus, any quadruple of MU bases must contain bases from different families.

The inner products $\left|h_1^\dagger(y)j_1(r)\right|, \left|h_1^\dagger(y)j_2(r)\right|, \left|h_2^\dagger(y)j_1(r)\right|$ and $\left|h_2^\dagger(y)j_2(r)\right|$ have modulus $1/2$ if there are values for y and r such that the equations

$$\left|1 + e^{ir} \pm (e^{-iy} + e^{i(r-y)})\right| = 2 \tag{2.29}$$

$$\left|1 - e^{ir} \pm (e^{-iy} - e^{i(r-y)})\right| = 2 \tag{2.30}$$

hold simultaneously. Upon introducing a factor of $e^{-ir/2}$, Eqs. (2.29) are equivalent to the constraints

$$\left|\cos\frac{r}{2}\right| = \frac{1}{|1 \pm e^{-iy}|} = \left|\sin\frac{r}{2}\right|. \tag{2.31}$$

Consequently, one must have $r = \pi/2$, and thus $e^{-iy} = \pm i$ or $y = \pi/2$ since $0 \leq r, y < \pi$. An entirely analogous argument restricts the values of s and z: checking the inner products $\left|h_1(r)^\dagger j_3(z)\right|, \left|h_1(r)^\dagger j_4(z)\right|$ etc. tells us that the matrices $H_4(y, z)$ and $J_4(r, s)$ are mutually unbiased only if $y = z = r = s = \pi/2$. We also find that the pairs $\{J_4(r, s),\ K_4(t, u)\}$ and

$\{K_4(t,u), H_4(x,y)\}$ are MU only when all six parameters take the value $\pi/2$.

We are now in the position to list all possible sets of MU bases in $\mathbb{C}^4$ beyond $\{I, F_4(x)\}$,

$$\begin{aligned} &\{I, F_4(x), H_4(y,z)\}\,, \\ &\{I, F_4(\pi/2), H_4(\pi/2,\pi/2), J_4(\pi/2,\pi/2)\}\,, \\ &\{I, F_4(\pi/2), H_4(\pi/2,\pi/2), J_4(\pi/2,\pi/2), K_4(\pi/2,\pi/2)\}\,. \end{aligned} \tag{2.32}$$

There is one three-parameter family of *triples* consisting of the one-parameter Fourier family $F_4(x)$ combined with two-parameter set $H_4(y,z)$; neither $J_4(r,s)$ nor $K_4(t,u)$ give rise to other triples since each of these sets of Hadamard matrices is equivalent to $\{I, F, H_4(y,z)\}$. The three-dimensional set (2.32) of MU bases in dimension $d = 4$ may be visualized as a cuboid defined by defined by $0 \le x, y < \pi$ and $0 \le z < \pi/2$. The reduction in the parameter range of z is due to the equivalence $\{I, F_4(x), H_4(y,z)\} \sim \{I, F_4(\pi - x), H_4(\pi - y, \pi - z)\}$ which follows from an overall complex conjugation. Each of the points i nthe cuboid correspond to one triple while both the quadruple and the quintuple are located at the point, $x = y = z = \pi/2$.

Only one set of *four* MU bases exists, since the other two candidates obtained by combining $K_4(\pi/2,\pi/2)$ with either $J_4(\pi/2,\pi/2)$ or $H_4(\pi/2,\pi/2)$ are a permutation of this quadruple. Finally, there is a unique way to a construct *five* MU bases which is easily seen to be equivalent to the standard construction of a complete set of MU bases in dimension four.

2.3 Dimension $d = 5$

As in dimensions two and three, there is a unique choice of a (5×5) dephased complex Hadamard matrix [74],

$$F_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{2.33}$$

equal to the discrete (5×5) Fourier matrix, with $\omega = \exp(2\pi i/5)$ denoting a fifth root of unity.

We have not found an elementary method to obtain a list of all vectors which are MU to the Fourier matrix F_5. Instead, we will rely on the work presented in Chapter 3 where the vectors have been constructed *analytically* by means of a computer program.

2.3.1 Constructing vectors MU to F_5

The vector $v = (1, e^{i\alpha_1}, \ldots, e^{i\alpha_4})/\sqrt{5} \in \mathbb{C}^5$ is MU to F_5 if it satisfies the conditions

$$\left| \sum_{j=0}^{4} \omega^{jk} e^{i\alpha_j} \right| = \sqrt{5}\,, \quad k = 0 \ldots 4\,, \tag{2.34}$$

defining $\alpha_0 \equiv 0$. The solutions of these equations give rise to 20 vectors which can be arranged in four MU bases,

$$H_5^{(1)} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & \omega^3 & \omega^4 & 1 \\ \omega^4 & \omega & \omega^3 & 1 & \omega^2 \\ \omega^4 & \omega^2 & 1 & \omega^3 & \omega \\ \omega & 1 & \omega^4 & \omega^3 & \omega^2 \end{pmatrix}, \; H_5^{(2)} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^2 & \omega^3 & \omega^4 & 1 & \omega \\ \omega^3 & 1 & \omega^2 & \omega^4 & \omega \\ \omega^3 & \omega & \omega^4 & \omega^2 & 1 \\ \omega^2 & \omega & 1 & \omega^4 & \omega^3 \end{pmatrix},$$

$$H_5^{(3)} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^3 & \omega^4 & 1 & \omega & \omega^2 \\ \omega^2 & \omega^4 & \omega & \omega^3 & 1 \\ \omega^2 & 1 & \omega^3 & \omega & \omega^4 \\ \omega^3 & \omega^2 & \omega & 1 & \omega^4 \end{pmatrix}, \; H_5^{(4)} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^4 & 1 & \omega & \omega^2 & \omega^3 \\ \omega & \omega^3 & 1 & \omega^2 & \omega^4 \\ \omega & \omega^4 & \omega^2 & 1 & \omega^3 \\ \omega^4 & \omega^3 & \omega^2 & \omega & 1 \end{pmatrix}. \tag{2.35}$$

To obtain this result, Eqs. (2.34) have been expressed as a set of coupled quadratic polynomials in eight real variables. Using an implementation [124] of Buchberger's algorithm [36, 37] on the computer program Maple [102], a Gröbner basis of these equations has been constructed which leads to the 20 vectors given by the columns of the four Hadamard matrices above. It is important to note that no other solutions of Eqs. (2.34) exist, a result which does *not* follow

from the known methods to construct a complete set of six MU bases in $\mathbb{C}^5$. Further details of this approach will be presented in Chapter 3.

Each of the four matrices in (2.35) is related to the Fourier matrix in a remarkably simple manner. In analogy to the unitary diagonal matrix used in Eq. (2.11), define a diagonal unitary matrix

$$D = \mathrm{diag}(1, \omega, \omega^4, \omega^4, \omega)\,, \tag{2.36}$$

with entries given by the first column of $H_5^{(1)}$ and you find that

$$H_5^{(k)} = D^k F_5\,, \quad k = 1, \ldots, 4\,. \tag{2.37}$$

Using this observation, we can express the unique complete set of six MU bases for dimension $d = 5$ as follows

$$\{I, F_5, H_5^{(1)}, \ldots, H_5^{(4)}\} \equiv \{I, F_5, DF_5, D^2F_5, D^3F_5, D^4F_5\}\,, \tag{2.38}$$

which will be useful later on.

Next, we proceed to classify all smaller sets of MU bases of $\mathbb{C}^5$ by combining subsets of the four Hadamard matrices $H_5^{(k)}$ in (2.35) with the pair $\{I, F_5\}$. For clarity, we now list the set of inequivalent classes which we will obtain. In addition to the pair $\{I, F_5\}$ and the complete set given in (2.38) there are *two* inequivalent triples as well as *one* quadruple and *one* quintuple:

$$\begin{gathered} \{I, F_5, H_5^{(1)}\}\,, \{I, F_5, H_5^{(2)}\}\,, \\ \{I, F_5, H_5^{(1)}, H_5^{(2)}\}\,, \\ \{I, F_5, H_5^{(1)}, H_5^{(2)}, H_5^{(3)}\}\,. \end{gathered} \tag{2.39}$$

Triples of MU bases in $\mathbb{C}^5$

Select one of the four matrices given in (2.35) and adjoin it to the pair $\{I, F_5\}$. You obtain four triples of MU bases with two immediate equivalences, namely,

$$\{I, F_5, H_5^{(1)}\} \equiv \{I, F_5, DF_5\} \sim \{I, F_5, D^4F_5\} \equiv \{I, F_5, H_5^{(4)}\} \tag{2.40}$$

on the one hand, and

$$\{I, F_5, H_5^{(2)}\} \equiv \{I, F_5, D^2F_5\} \sim \{I, F_5, D^3F_5\} \equiv \{I, F_5, H_5^{(3)}\} \tag{2.41}$$

on the other. The equivalence (2.40) follows from multiplying the set $\{I, F_5, DF_5\}$ with D^4 from the left, rephasing the first basis with D from the right, using $D^5 = I$ and swapping the last two matrices. A similar argument establishes the equivalence (2.41), using D^3 instead of D^4.

Thus, it remains to check whether the triples $\mathcal{T}^{(1)} \equiv \{I, F_5, H_5^{(1)}\}$ and $\mathcal{T}^{(2)} \equiv \{I, F_5, H_5^{(2)}\}$ are equivalent to each other. It turns out that these two triples are, in fact, *inequivalent*. More explicitly, this means that no unitary matrix U and no monomial matrices M_0, M_1 and M_2 can be found which would map $\mathcal{T}^{(1)}$ into $\mathcal{T}^{(2)}$ according to

$$\{I, F_5, H_5^{(1)}\} \to \{UIM_0, UF_5M_1, UH_5^{(1)}M_2\}\,. \tag{2.42}$$

A proof of this statement is given in Appendix B.

Quadruples of MU bases in $\mathbb{C}^5$

There are six possibilities to form quadruples by selecting two of the four matrices in Eq. (2.35) and adding them to the pair $\{I, F_5\}$. Recalling that $H_5^{(k)} = D^kF_5$, we identify the following equivalences which relate three quadruples each,

$$\{I, F_5, DF_5, D^2F_5\} \sim \{I, F_5, D^3F_5, D^4F_5\} \sim \{I, F_5, DF_5, D^4F_5\}\,, \tag{2.43}$$

and

$$\{I, F_5, DF_5, D^3F_5\} \sim \{I, F_5, D^2F_5, D^4F_5\} \sim \{I, F_5, D^2F_5, D^3F_5\}\,. \tag{2.44}$$

To show the first equivalence in Eq. (2.43), for example, multiply its left-hand-side with D^3 from the left, use the identity $D^5 = 1$ and rearrange the bases appropriately. The other equivalences follow from analogous arguments. Thus, there are at most two inequivalent sets of four MU bases in $\mathbb{C}^5$, with representatives $\{I, F_5, H_5^{(1)}, H_5^{(2)}\}$ and $\{I, F_5, H_5^{(1)}, H_5^{(3)}\}$, say.

Interestingly, these two classes of MU bases are *equivalent* to each other leaving us with a single equivalence class of quadruples in dimension five, with representative $\{I, F_5, H_5^{(1)}, H_5^{(2)}\}$, say. To show this equivalence, we multiply the first quadruple with the adjoint of F_5 from the left

$$F_5^\dagger\{I, F_5, H_5^{(1)}, H_5^{(2)}\} \sim \{I, F_5, F_5^\dagger H_5^{(1)}, F_5^\dagger H_5^{(2)}\}\,. \tag{2.45}$$

using the identity $F^\dagger = FP$, with some permutation matrix P, and swapping the first two bases. The action of $F_5^\dagger$ on the other two elements is surprisingly simple: the Hadamard matrix $H_5^{(1)}$ is mapped to itself,

$$F_5^\dagger H_5^{(1)} = H_5^{(1)} M\,, \tag{2.46}$$

up to a monomial matrix M, while $H_5^{(2)}$ is sent to $H_5^{(3)}$,

$$F_5^\dagger H_5^{(2)} = H_5^{(3)} M'\,, \tag{2.47}$$

again up to some monomial matrix M'. Both relations simply follow from working out the product on the left and factoring the result, e.g.

$$F_5^\dagger H_5^{(2)} = \frac{1}{\sqrt{5}} \begin{pmatrix} s(1) & s(2) & s(3) & s(4) & s(5) \\ \omega^3 s(1) & \omega^2 s(2) & \omega s(3) & s(4) & \omega^4 s(5) \\ \omega^2 s(1) & s(2) & \omega^3 s(3) & \omega s(4) & \omega^4 s(5) \\ \omega^2 s(1) & \omega^4 s(2) & \omega s(3) & \omega^3 s(4) & s(5) \\ \omega^3 s(1) & \omega^4 s(2) & s(3) & \omega s(4) & \omega^2 s(5) \end{pmatrix} = H_5^{(3)} D^{(2)}\, P, \tag{2.48}$$

where the k^{th} entry of the diagonal matrix $D^{(2)}$ is given by the sum of the k^{th} column of $H_5^{(2)}$, denoted by $s(k) = \sum_i H_{ik}^{(2)}$, and P permutes the columns. Using these identities in Eq. (2.45) we find that

$$\{I, F_5, H_5^{(1)}, H_5^{(2)}\} \sim \{I, F_5, H_5^{(1)}, H_5^{(3)}\} \tag{2.49}$$

the two quadruples are equivalent.

Quintuples of MU bases in $\mathbb{C}^5$

Four sets of MU bases can be obtained by adding any three of the four matrices in Eq. (2.35) to the pair $\{I, F_5\}$. It is not difficult to show that the four resulting sets of quintuples are equivalent to each other. Thus, there is effectively only one possibility to choose five MU bases in $\mathbb{C}^5$, with representative $\{I, F_5, H_5^{(1)}, H_5^{(2)}, H_5^{(3)}\}$.

Let us show now that this representative, which has been obtained by leaving out $H_5^{(4)}$, is equivalent to the set $\{I, F_5, H_5^{(1)}, H_5^{(2)}, H_5^{(4)}\}$, for example. Indeed, the equivalence

$$\{I, F_5, DF_5, D^2F_5, D^3F_5\} \sim \{I, F_5, DF_5, D^2F_5, D^4F_5\}\,, \tag{2.50}$$

follows immediately from multiplying the second set by D from the left and using $D^5 = I$,

$$\{I, F_5, DF_5, D^3F_5, D^4F_5\} \sim \{I, DF_5, D^2F_5, D^3F_5, F_5\}\,. \tag{2.51}$$

Reordering the set of five matrices on the right reveals the desired equivalence with the quintuple $\{I, F_5, H_5^{(1)}, H_5^{(2)}, H_5^{(3)}\}$. Effectively, the four matrices different from I undergo a cyclic shift under multiplication with D, and the remaining equivalences follow from shifts induced by D^2 and D^3, respectively.

2.4 Summary of MU bases in dimensions two to five

We have constructed all inequivalent sets of mutually unbiased bases in dimension two to five. Our approach is based on the fact that all complex Hadamard matrices are known in these

dimensions. For dimensions up to $d = 4$, elementary arguments suffice to classify the existing sets of MU bases while dimension five requires some analytic results which have been found using algebraic computer software (cf. Chapter 3).

d	2	3	4	5	6
pairs	1	1	∞^1	1	$\geq \infty^2$
triples	1	1	∞^3	2	$\geq \infty^2$
quadruples	-	1	1	1	?
quintuples	-	-	1	1	?
sextuples	-	-	-	1	?

Table 2.1: The number of inequivalent MU bases for dimensions two to six where ∞^k denotes a k-parameter set; see text for details.

The first four columns of Table 2.1 summarize the results obtained in this chapter. All *pairs* of MU bases in dimensions two to five are listed in the first row, effectively reflecting the known classification of inequivalent Hadamard matrices; a continuous (one-parameter) set of inequivalent MU pairs only exists in dimension four.

The main results concern *triples* of MU bases in dimension four where we find a *three-parameter family* and in dimension five where we obtain *two* inequivalent triples. Finally, we have shown that there is only one class of both MU *quadruples* and MU *quintuples* in dimensions four and five. In all dimensions considered, there is a unique d-tuple which can be extended to a complete set of $(d + 1)$ MU bases using a construction presented in [147].

The last column of Table 2.1 contrasts these results with dimension six where the classification of all complex Hadamard matrices is not known to be complete. The first entry shows that there are two-parameter families of pairs of MU bases [74, 139] (it has been conjectured that the parameter space has, in fact, four dimensions [136]). One of the families of pairs can be extended to a two-parameter family of triples [139] using an idea taken from [152]. In the next chapter we will attempt to complete this final column by applying the same method of constructing set of $r \leq d + 1$ MU bases starting from a pair $\{I, H\}$ in dimensions six.

CHAPTER 3

Constructing mutually unbiased bases in dimension six

We have seen that in dimensions two to five we are able to give a full classification of sets of MU bases. In dimension six it is not known whether there are any sets of more than 3 MU bases, and in fact there is a long standing conjecture due to Zauner [152]

Conjecture 3.0.1 *There are no more than 3 MU bases in dimension 6.*

There have been two main attempts to obtain rigorous results in support of this conjecture by restricting the search to MU bases of a specific form:

- selecting a first Hadamard matrix and then searching for MU bases with components given by suitable roots of unity leads to no more than two MU complex Hadamard matrices, or three MU bases in $\mathbb{C}^6$ [16];
- Grassl [72] has shown that only *finitely* many vectors exist which are MU with respect to the identity and the discrete Fourier matrix F_6. Again, no more than two MU Hadamard matrices emerge, giving rise to at most three MU bases; it is thus impossible to base the construction of a complete set on the Heisenberg-Weyl group.

The strategy of this chapter will be to generalize Grassl's approach by removing the restriction that the second MU basis be F_6. Instead, we will consider many different choices for the second

MU basis, thoroughly sampling the set of currently known complex Hadamard matrices in $\mathbb{C}^6$. We will find that none of the matrices studied can be used to construct a complete set of MU bases. Taken together, these negative instances provide further strong support for the conjecture that no seven MU bases exist in dimension six.

Let us now present the outline of our argument. In Section 3.1, we briefly describe the set of known complex Hadamard matrices in dimension six. Then, we explain in Section 3.2 how to construct all vectors that are MU with respect to both the standard basis of $\mathbb{C}^6$ and a second basis, defined by an arbitrary fixed Hadamard matrix. We illustrate the algorithm for $d = 3$ only to rediscover the known complete set of four MU bases given in Eq. (1.3) and found in Section 2.1.2. Then, whilst re-deriving Grassl's result for $d = 6$, we will explain the subtle interplay between algebraic and numerical calculations in this approach. Section 3.3 presents our findings which we obtain by applying the algorithm to nearly 6000 Hadamard matrices of dimension six.

3.1 Complex Hadamard matrices in dimension six

All (complex) Hadamard matrices are known for dimensions $d \leq 5$ but there is no exhaustive classification for $d = 6$. It is useful to briefly describe the Hadamard matrices known to exist in dimension six since we will 'parametrize' the search for MU bases in terms of Hadamard matrices. We use the notation introduced in [141] the authors of which maintain an online catalog of Hadamard matrices [140].

Each point in Fig. 3.1, an updated version of a figure presented in [16], corresponds to one Hadamard matrix of dimension six, except for the interior of the upper circle where a point represents two Hadamard matrices (cf. below). There is one *isolated point*, representing the spectral matrix S given in [108], also known as Tao's matrix [143]. Three sets of Hadamard matrices labeled by a *single parameter* are known: the Diţă family $D(x)$ introduced in [51], a family of symmetric matrices denoted by $M(t)$ [105] and the family of all Hermitean Hadamard matrices $B(\theta)$ [11]. Two *two-parameter* families of Hadamard matrices are known to arise from discrete Fourier-type transformations $F(x_1, x_2)$ in $\mathbb{C}^6$, and from their transpositions, $F^T(x_1, x_2)$ [74]. The Szöllősi family $X(a, b)$ is the only other known two-parameter set [139]. Interestingly,

the matrix $X(0,0)$ can be shown to be equivalent to $F(1/6,0)$, and there is a second possibility to define a matrix at this point, giving rise to $X^T(0,0) \approx F^T(1/6,0)$ [15]. We have noticed that such a doubling actually occurs for *all* values of the parameters (a,b) leading to a set of Hadamard matrices $X^T(a,b)$ inequivalent to $X(a,b)$. Hence, the interior of the upper circle in Fig. 3.1 represents two layers of Hadamard matrices which are glued together at its boundary. Topologically, the Szöllősi family $X(a,b)$ and the set $X^T(a,b)$ thus combine to form the surface of a sphere. Appendix C lists the explicit forms of Hadamard matrices as well as the parameter ranges which have been reduced to their *fundamental regions* using the equivalence relation (2.2).

Fig. 3.1 also shows *equivalences* between Hadamard matrices simultaneously belonging to different families. The circulant Hadamard matrix C [24], for example, embeds into the Hermitean family which in turn is given by the boundary of the Szöllősi families; interestingly, the Diţă matrices are also contained therein. Lining up some of the points where different families overlap suggests that we arrange the Hadamard matrices in a symmetrical way. Then, a reflection about the line passing through the points $F(0,0)$ and S maps $H(\mathbf{x})$ to $H(-\mathbf{x})$ if $H(\mathbf{x})$ is a member of the Diţă, Hermitean or symmetric families; furthermore, the same reflection sends $H(\mathbf{x})$ to $H^T(\mathbf{x})$ if the matrix $H(\mathbf{x})$ is taken from Diţă, Hermitean or Fourier families. For the Szöllősi family, the reflection about the vertical axis must be supplemented by a change of layer in order to get from $X(a,b)$ to $X^T(a,b)$. We will see that the findings presented in Section 3.3 echo this symmetry which we will explain in the conclusion.

Let us finally mention that the known families of Hadamard matrices come in two different types, *affine* and *non-affine* ones. The set $H(\mathbf{x})$ is affine if it can be written in the form

$$H(\mathbf{x}) = H(0) \circ \mathrm{Exp}[R(\mathbf{x})] \tag{3.1}$$

for some matrix R; the open circle denotes the Hadamard (elementwise) product of two matrices, $(A \circ B)_{ij} = A_{ij}B_{ij}$, and $\mathrm{Exp}[R]$ represents the matrix R elementwise exponentiated: $(\mathrm{Exp}[R])_{ij} = \exp R_{ij}$. Both Fourier-type families and the Diţă matrices are affine (cf. Appendix C) while the symmetric, Hermitean and Szöllősi families are not.

3.2 Constructing MU vectors

In this section, we modify the approach taken in Chapter 2. As before, we make explicit the conditions on a vector $|v\rangle \in \mathbb{C}^d$ to be MU with respect to the standard matrix and a fixed Hadamard matrix, i.e. to the pair $\{I, H\}$. However, we parameterise the vector $|v\rangle$ using real variables so that the MU conditions result in a system of multivariate *polynomial* equations. Then we outline an algorithm to construct *all* solutions of the resulting equations, allowing us to check how many additional MU Hadamard matrices do exist. We illustrate this approach by constructing a complete set of *four* MU bases in dimension $d = 3$, reproducing the result of Sec 2.1.2. We also reproduce Grassl's result for $d = 6$ in order to explain that this approach produces rigorous results in spite of inevitable numerical approximations.

3.2.1 MU vectors and multivariate polynomial equations

A vector $|v\rangle \in \mathbb{C}^d$ is MU with respect to the standard basis (associated with the columns of the identity I) if each of its components has modulus $1/\sqrt{d}$. Furthermore, $|v\rangle$ is MU with respect to a fixed Hadamard matrix H if $|\langle h(k)|v\rangle|^2 = 1/d$, where $|h(k)\rangle$ is the state associated with the k^{th} column $h(k)$ of H, $k = 0, \ldots, d-1$.

Let us express these conditions on $|v\rangle$ in terms of its components v_j, written as

$$\sqrt{d}v_j = \begin{cases} 1 & j = 0\,, \\ x_j + iy_j & j = 1, \ldots, d-1\,, \end{cases} \tag{3.2}$$

where x_j, y_j are $2(d-1)$ real parameters. The overall phase of the state $|v\rangle$ is irrelevant which allows us to fix the phase of its first component. Then, the first set of constraints on the state $|v\rangle$ reads

$$x_j^2 + y_j^2 = 1\,, \quad j = 1, \ldots, d-1\,, \tag{3.3}$$

and the second set is given by

$$\left|\sum_{j=0}^{d-1} h_j^*(k) v_j\right|^2 \equiv \left|\sum_{j=0}^{d-1} H_{kj}^\dagger (x_j + iy_j)\right|^2 = \frac{1}{d}\,, \quad k = 0, \ldots, d-2\,, \tag{3.4}$$

where the state $|h(k)\rangle$ has components $h_j(k) \equiv H_{jk}$, $0 = 1, \ldots, d-1$. The completeness relation of the orthonormal basis $\{|h(k)\rangle,\, k = 0, \ldots, d-1\}$, implies that if a state $|v\rangle$ is MU with respect to $(d-1)$ of its members, it is also MU with respect to the remaining one. Therefore, it is not necessary to include $k \equiv d-1$ in Eqs. (3.4).

For each given Hadamard matrix H, Eqs. (3.3) and (3.4) represent $2(d-1)$ simultaneous coupled quadratic equations for $2(d-1)$ real variables. Once we know *all* solutions of these equations, we know *all* vectors $|v\rangle$ MU with respect to the chosen pair of bases $\{I, H\}$. Analysing the set of solutions will reveal whether they form additional MU Hadamard matrices, or, equivalently, MU bases.

If Eqs. (3.3) and (3.4) were *linear*, one could apply Gaussian elimination to bring them into 'triangular' form. The resulting equations would have the same solutions as the original ones but the solutions could be obtained easily by successively solving for the unknowns.

The solutions of Eqs. (3.3) and (3.4) can be found using *Buchberger's algorithm* [36] which generalizes Gaussian elimination to *(nonlinear) multivariate polynomial* equations. In this approach, a set of polynomials $\mathcal{P} \equiv \{p_n(\mathbf{x}), n = 1, \ldots, N\}$ is transformed into a different set of polynomials $\mathcal{G} \equiv \{g_m(\mathbf{x}), m = 1, \ldots, M\}$ (usually with $M \neq N$) such that the equations $\mathcal{P} = 0$ and $\mathcal{G} = 0$ possess the *same* solutions; here $\mathcal{P} = 0$ is short for $p_n(\mathbf{x}) = 0, n = 1, \ldots, N$. Technically, one constructs a *Gröbner basis* $\mathcal{G}$ of the polynomials $\mathcal{P}$ which requires a choice of variable ordering [36]. The transformed equations $\mathcal{G} = 0$ will be straightforward to solve due their 'triangular' form: one can find all possible values of a first unknown by solving for the zeros of a polynomial in a *single* variable; using each of these solutions will reduce one or more of the remaining equations to single-variable polynomials, allowing one to solve for a second unknown, etc. This process iteratively generates all solutions of $\mathcal{G} = 0$ and, therefore, all solutions of the original set of equations, $\mathcal{P} = 0$.

A Gröbner basis exists for any set of polynomial equations with a finite number of variables. However, the number of steps required to construct a Gröbner basis tends to be large even for polynomials of low degrees and a small number of unknowns. Thus, Buchberger's algorithm is most conveniently applied by means of algebraic software programs. We have used the implementation [124] of this algorithm suitable for the computational algebra system Maple [102] since

we found it to be particularly fast for the system of equations under study.

Let us now make explicit how to construct all vectors MU with respect to a pair $\{I, H\}$ by solving the multivariate polynomial equations (3.3) and (3.4) using Buchberger's algorithm. We will consider two cases in dimensions $d = 3$ and $d = 6$, respectively, which have been solved before but they are suitable to illustrate the construction and to discuss some of its subleties.

3.2.2 Four MU bases in $\mathbb{C}^3$

In dimension $d = 3$, four MU bases are known to exist. We will now show how to construct two MU Hadamard matrices H_2 and H_3 given a pair $\{I, H\}$. The resulting three MU Hadamard matrices plus the identity provide a complete set of four MU bases in $\mathbb{C}^3$ thus reproducing the result of Sec 2.1.2.

1. Choose a Hadamard In dimension three, all Hadamard matrices are known and there is only one choice for a dephased Hadamard matrix [74] given by the Fourier matrix,

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

where $\omega = \exp(2\pi i/3)$ is a third root of unity.

2. List the constraints We want to find all states $|v\rangle \in \mathbb{C}^3$ which are MU with respect to the columns of the identity matrix I and the Fourier matrix F_3. Using the four real parameters x_1, x_2, y_1, and y_2 introduced in (3.2), the constraints (3.3) and (3.4) read explicitly

$$\begin{aligned} 1 - x_1^2 - y_1^2 &= 0\,, \\ 1 - x_2^2 - y_2^2 &= 0\,, \\ x_1 + x_2 + x_1x_2 + y_1y_2 &= 0\,, \\ x_1 + x_2 - \sqrt{3}y_1 + \sqrt{3}y_2 + x_1x_2 - \sqrt{3}x_1y_2 + \sqrt{3}y_1x_2 + y_1y_2 &= 0\,. \end{aligned} \tag{3.5}$$

The solutions of these four coupled quadratic equations in four real variables, $\mathcal{P} = 0$, will tell us whether additional Hadamard matrices exist which are MU with respect to the Fourier matrix F_3.

3. Construct the solutions By running Buchberger's algorithm, we find the Gröbner basis $\mathcal{G}$ associated with the polynomials in Eqs. (3.5). Equating the resulting four polynomials $g_n(\mathbf{x}), n = 1, \ldots, 4$, to zero, gives rise to the equations

$$\begin{aligned} 3y_2 - 4y_2^3 &= 0\,, \\ 1 - x_2 - 2y_2^2 &= 0\,, \\ 1 + 2x_1 + 4y_1y_2 - 4y_2^2 &= 0\,, \\ 3 - 4y_1^2 + 4y_1y_2 - 4y_2^2 &= 0\,. \end{aligned} \tag{3.6}$$

This set is 'triangular' in the sense that solutions can be found by iteratively determining the roots of polynomials for single variables only. The first equation has three solutions,

$$y_2 \in \{0\,, \pm\sqrt{3}/2\}\,;$$

next, the second equation implies that

$$x_2 = \begin{cases} 0 & \text{if } y_2 = 0\,, \\ 2 & \text{if } y_2 = \pm\sqrt{3}/2\,; \end{cases}$$

etc. Altogether, there are six solutions,

$$\begin{aligned} \mathbf{s}_1 &= \tfrac{1}{2}(-1, -1, \sqrt{3}, \sqrt{3})\,, & \mathbf{s}_2 &= \tfrac{1}{2}(-1, 2, -\sqrt{3}, 0)\,, \\ \mathbf{s}_3 &= \tfrac{1}{2}(2, -1, 0, -\sqrt{3})\,, & \mathbf{s}_4 &= \tfrac{1}{2}(-1, -1, -\sqrt{3}, -\sqrt{3})\,, \\ \mathbf{s}_5 &= \tfrac{1}{2}(2, -1, 0, \sqrt{3})\,, & \mathbf{s}_6 &= \tfrac{1}{2}(-1, 2, \sqrt{3}, 0)\,, \end{aligned}$$

defining $\mathbf{s} = (x_1, x_2, y_1, y_2)$.

Since the degrees of the polynomials $\mathcal{G}$ in Eqs. (3.6) do not exceed three, we are able to

obtain analytic expressions for its solutions. This, however, is a fortunate coincidence due to the simplicity of the problem: in general, we will need to determine the roots of higher-order polynomials (cf. the example presented in Section 3.2.3) which requires numerical methods. The resulting complications will be discussed in Section 3.2.4.

4. List all MU vectors Upon substituting the solutions $\mathbf{s}_1$ to $\mathbf{s}_6$ into (3.2), one obtains the six vectors, v_1 to v_6 given in Eq. (2.10) which are MU with respect to the columns of both the matrices I and F_3. No other vectors with this property exist, leaving us with $v_1, \ldots, v_6$, as the only candidates for the columns of additional MU Hadamard matrices.

5. Analyse the vectors The six vectors in (2.10) allow us to define an additional Hadamard matrix only if any three of them are orthogonal; for a second Hadamard matrix the remaining three must be orthogonal among themselves *and* MU to the first three. As before, calculating the inner products between all pairs of the vectors v_1 to v_6 shows that they indeed fall into two groups with the required properties. Consequently, we have constructed a complete set of four MU bases in $\mathbb{C}^3$, corresponding to the set $\{I, F_3, H_2, H_3\}$ where the columns of the matrices H_2 and H_3 are given by $\{v_1, v_2, v_3\}$ and $\{v_4, v_5, v_6\}$, respectively.

We have also checked that the construction procedure works in dimensions $d = 2, 5$ and $d = 7$ where it correctly generates complete sets of $(d+1)$ MU bases. The results produced here allowed the classification of all MU bases in dimension five given in Section 2.3 which would not have been possible without the aid of Buchberger's algorithm.

3.2.3 Three MU bases in $\mathbb{C}^6$

In $d = 6$, the existence of seven MU bases is an open problem. We will search for all states $|v\rangle$ which are MU with respect to the identity I and the six-dimensional equivalent of F_3 given in

(2.7), the dephased Fourier matrix

$$F_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 \\ 1 & \omega^2 & \omega^4 & 1 & \omega^2 & \omega^4 \\ 1 & \omega^3 & 1 & \omega^3 & 1 & \omega^3 \\ 1 & \omega^4 & \omega^2 & 1 & \omega^4 & \omega^2 \\ 1 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \tag{3.7}$$

with $\omega = \exp(\pi i/3)$ now being the sixth root of unity. This problem has been studied in the context of biunimodular sequences [24] and in relation to MU bases [72]. It is impossible to complement the pair $\{I, F_6\}$ by more than one Hadamard matrix MU with respect to F_6. Thus, the construction method of MU bases in prime-power dimensions which is based on the Heisenberg-Weyl group, has no equivalent in the composite dimension $d = 6$. We will now reproduce this negative result.

Having chosen the first Hadamard matrix to be F_6, we can write down the conditions which the components of a state $|v\rangle$ must satisfy, $\mathcal{P} = 0$. After some algebraic operations detailed in Appendix D, one obtains the equations

$$\begin{aligned} x_1 + x_5 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + y_1y_2 + y_2y_3 + y_3y_4 + y_4y_5 &= 0\,, \\ y_1 - y_5 + x_1y_2 - x_2y_1 + x_2y_3 - x_3y_2 + x_3y_4 - x_4y_3 + x_4y_5 - x_5y_4 &= 0\,, \\ x_3 + x_1x_4 + x_2x_5 + y_1y_4 + y_2y_5 &= 0\,, \\ x_2 + x_4 + x_1x_3 + x_1x_5 + x_2x_4 + x_3x_5 + y_1y_3 + y_1y_5 + y_2y_4 + y_3y_5 &= 0\,, \\ y_2 - y_4 + x_1y_3 - x_1y_5 + x_2y_4 - x_3y_1 + x_3y_5 - x_4y_2 + x_5y_1 - x_5y_3 &= 0\,, \end{aligned} \tag{3.8}$$

which must be supplemented by the five conditions (3.3) arising for $d = 6$.

We need to find all solutions of these ten coupled equations $\mathcal{P} = 0$ which are quadratic in ten real variables. The Gröbner basis $\mathcal{G}$ associated with the set $\mathcal{P}$ consists of 36 polynomials of

considerably higher degrees. We reproduce only the first one of the new set of equations, $\mathcal{G} = 0$,

$$\begin{aligned} -245025\, y_5 + 4318758\, {y_5}^3 - 28135161\, {y_5}^5 + 89685000\, {y_5}^7 - 158611892\, {y_5}^9 \\ +177275680\, {y_5}^{11} - 150745472\, {y_5}^{13} + 104333824\, {y_5}^{15} - 43667456\, {y_5}^{17} \\ +2351104\, {y_5}^{19} + 4882432\, {y_5}^{21} - 1703936\, {y_5}^{23} + 262144\, {y_5}^{25} \quad = \quad 0\,, \end{aligned}$$

being of order 25 in the single variable y_5. This equation admits 15 real solutions,

$$y_5 \in \{0, \pm 1, \pm\frac{1}{2}, \pm\frac{\sqrt{3}}{2}, \pm\frac{1}{2}(1+\sqrt{3}), \pm\frac{1}{2}(1-\sqrt{3}), \pm 0.988940\ldots, \pm 0.622915\ldots\}\,, \tag{3.9}$$

the last four of which we only find numerically. Due to the triangular structure resulting from Buchberger's algorithm, there will be equations (at least one) containing only y_5 and one other single variable. For each value of y_5 taken from (3.9), they reduce to single-variable polynomials the roots of which can be determined to desired numerical accuracy; etc. Keeping track of all possible branches we obtain 48 vectors that satisfy the Eqs. (3.8).

Having determined the candidates for columns of MU Hadamard matrices, we calculate the inner products among all pairs of the 48 vectors. It turns out that there are 16 different ways to group them into bases of $\mathbb{C}^6$. However, no two of these bases are MU with respect to each other. Consequently, it is possible to form at most 16 different *triples* of MU bases which include F_6. It also follows that the Fourier matrix F_6 (or any other unitarily equivalent element of the Heisenberg-Weyl group [72]) *cannot* be supplemented by two MU Hadamard matrices–no four MU bases can exist.

There are, however, many choices other than $H = F_6$ for a dephased Hadamard matrix in dimension six. In Section 4.3, we will repeat the calculations just presented for a large sample of currently known Hadamard matrices. Before doing so, we will discuss the fact that we are able to construct the desired vectors only approximately. In the following section we show that sufficiently high numerical accuracy allows us to draw *rigorous* conclusions about the properties of the exact vectors.

3.2.4 The impact of numerical approximations

The previous section illustrated that the problem of finding MU vectors with respect to the identity I and a given Hadamard matrix H can be reduced to successively solving for the roots of polynomials of a single variable. These roots, however, can only be found approximately. Does the approximation prevent us from drawing rigorous conclusions about the properties of the MU vectors we construct? We will argue now that it remains possible to find upper bounds on the number of MU vectors with the desired properties.

Consider the system of polynomials $\mathcal{P} = \{p_n(\mathbf{x}), n = 1, \ldots, 10\}$ in the variables $\mathbf{x} \in \mathbb{R}^{10}$ resulting from some chosen Hadamard matrix H, and calculate a Gröbner basis, $\mathcal{G} = \{g_m(\mathbf{x}), m = 1, \ldots, M\}$. The roots of the equations $\mathcal{P} = 0$ and $\mathcal{G} = 0$ are identical by construction. Since $\mathcal{G} = 0$ corresponds to a 'triangular' set, its roots can be found iteratively but, in general, no closed form will exist. The implementation of Buchberger's algorithm which we have chosen finds these roots with user-specified accuracy, relying on the theory presented in [123].

Suppose that $\mathcal{G} = 0$ has two roots $\mathbf{s}_a$ and $\mathbf{s}_b$, to which we have found approximations, $\mathbf{s}_A$ and $\mathbf{s}_B$. The associated approximate exact states, $|v_a\rangle$ and $|v_b\rangle$, differ from the approximate states, $|v_A\rangle$ and $|v_B\rangle$, by error terms $|\delta v_a\rangle = |v_A\rangle - |v_a\rangle$ and similarly for the second solution. The components of the vectors $|\delta v_a\rangle$ all have moduli smaller than the user-defined accuracy of 10^{-r}, say. If the inner product of the exact states $|v_a\rangle$ and $|v_b\rangle$ has a non-zero modulus, $\Delta > 0$, then they are *not* orthogonal. We can detect this by calculating the inner product of the *approximate* states,

$$\begin{aligned} |\langle v_A|v_B\rangle| &= |\langle v_a|v_b\rangle + \langle v_a|\delta v_b\rangle + \langle \delta v_a|v_b\rangle + \langle \delta v_a|\delta v_b\rangle| \\ &\leq |\langle v_a|v_b\rangle| + |\langle v_a|\delta v_b\rangle| + |\langle \delta v_a|v_b\rangle| + \mathcal{O}(10^{-2r}) \\ &\leq |\langle v_a|v_b\rangle| + 10\sqrt{2} \times 10^{-r} + \mathcal{O}(10^{-2r})\,, \end{aligned}$$

using $|||\delta v_a\rangle|| \leq 5\sqrt{2} \times 10^{-r}$ and $|||v_a\rangle|| = 1$. Thus, a non-zero lower bound for the exact scalar product follows if the approximate inner product is *larger* than $\sqrt{2} \times 10^{-r+1}$. In other words, we may conclude that the exact states are non-orthogonal if we ensure that the error in the

approximate scalar product is negligible, i.e. $\Delta \geq |\langle v_A|v_B\rangle| - \sqrt{2} \times 10^{-r+1} > 0$. A similar argument allows us to exclude that two approximate states are MU with respect to each other.

We determine the roots of $\mathcal{G} = 0$ to $r = 20$ significant digits which proves sufficient to put relevant limits on the properties of the vectors constructed in dimension six. The results presented in the Sections 3.3.1 and 3.3.2 thus represent rigorous limits on the number of vectors MU with respect to specific Hadamard matrices and hence on the number of MU bases.

3.3 Constructing MU bases in dimension six

We are now in a position to present the main results of this chapter. We will consider one Hadamard matrix H at a time constructing all additional Hadamard matrices MU with respect to the chosen one. Picking matrices both systematically and randomly, we will find that not a single one is compatible with the existence of four MU bases.

More specifically, we will determine two quantities for each chosen Hadamard matrix H. The number N_v equals the number of vectors MU with the pair $\{I, H\}$, and the number N_t provides an upper bound on how many different triples of MU bases $\{I, H, H'\}$ exist.

3.3.1 Special Hadamard matrices

To begin, we consider the Hadamard matrices on the symmetry axis of Fig. (3.1): the Fourier matrix $F_6 \equiv F(0,0)$ being invariant under transposition, the Diţă matrix $D_0 \equiv D(0)$ which is both symmetric and Hermitean, the circulant matrix C, and the Spectral matrix S. These matrices are special in the sense that they are either isolated or belong to different Hadamard families simultaneously.

The first row of Table 3.1 completes the findings of Section 3.2.3 obtained for the *Fourier* matrix F_6: there are $N_v = 48$ vectors MU with respect to both I and F_6 that can be arranged in $N_t = 16$ different ways to form a second Hadamard matrix H' being MU with respect to F_6. However, no two of these 16 Hadamard matrices are MU between themselves, limiting the number of MU bases containing F_6 to three.

A similar analysis for the *Diţă* matrix D_0 reveals that there are 120 vectors MU to its columns

H	N_v	N_t
F_6	48	16
D_0	120	10
C	56	4
S	90	0

Table 3.1: The number of MU vectors and their properties for *special* Hadamard matrices: there are N_v vectors being MU with respect to the pair of matrices $\{I, H\}$ that form N_t additional Hadamard matrices i.e. there are N_t different *triples* of MU bases.

and those of the identity, 60 of which form ten bases but none of these are MU with respect to each other. Whilst ten triples of MU bases exist, sets of four MU bases which include D_0 do *not* exist.

Interestingly, the components of the 120 vectors have phases ϕ which take values in a small set only,

$$\phi_D \equiv \{0, \pi, \pm\pi/12, \ldots, \pm 11\pi/12, \pm\alpha\},$$

where $\tan\alpha = 2$. This result agrees with the one obtained by Bengtsson et al. [16] (note, however, that the descriptions given in the last two entries of the list in their Section 7 must be swapped). What is more, our approach *proves* that these authors have been able to identify *all* vectors MU with the pair $\{I, D_0\}$ by means of their ansatz for the form of MU vectors. In fact, the value of N_t in Table 3.1 given for D_0 is *exact*, not an upper bound since the phases of the MU states $|v\rangle$ are known in closed form. Interestingly, a restricted set of phases also occurs for other members of the Diţă family. For example, all 48 vectors MU with the pair $\{I, D(1/8)\}$ have phases limited to the set $\phi_D \cup \{\pm\beta\}$ where $\tan\beta = 3$.

The *circulant* matrix C permits 56 MU vectors, which can be arranged into 4 different bases, $N_t = 4$. The *spectral* matrix S is the only known *isolated* Hadamard matrix. We find 90 MU vectors but not a single sextuple of orthonormal ones among them. Thus, the pair $\{I, S\}$ cannot even be extended to a triple of MU bases.

H	$\mathbf{x}$	$\#(\mathbf{x})$	N_v	N_t
$D(x)$	Γ_D	36	48/72/120	4
	random	500	72/120	4
$F(\mathbf{x})$	Γ_F	168	48	8/70
	random	2,000	48	8
$F^T(\mathbf{x})$	Γ_F	168	48	8/70
	random	2,000	48	8

Table 3.2: The number of MU vectors and their properties for *affine* Hadamard matrices: the second column indicates which values have been chosen for the parameters $\mathbf{x}$; the grids of points Γ_M and Γ_F are defined in Eqs. (3.10) and (3.11), respectively; the third column displays the number of Hadamard matrices considered in a sample; N_v and N_t are defined as in Table 3.1 and vary as a function of the parameter values (cf. Section 3.3.2).

3.3.2 Affine families

Table 3.2 collects the properties of vectors MU with respect to the pair $\{I, H\}$ where H is an affine Hadamard matrix, i.e. taken either from the one-parameter set discovered by Diţă or from the two-parameter Fourier families. Again, we have sampled the relevant parameter spaces both systematically and randomly.

The set of *Diţă* matrices $D(x)$ depends on a single continuous parameter x, with $|x| \leq 1/8$. We have sampled the interval in steps of size $1/144$ making sure that the resulting grid of points include the 24^{th} roots of unity which play an important role for D_0, so

$$\Gamma_D = \{a/144 : a = \pm 1, \pm 2 \ldots, \pm 18\}\,; \tag{3.10}$$

note that the matrix D_0 has been left out. The number of vectors MU with the pair $\{I, D(x)\}$ depends on the *value* of the parameter x: the Diţă matrices $D(x)$ on the grid Γ_D allow for 48, 72 or 120 MU vectors which can be grouped into into four additional Hadamard matrices. Since they are not MU between themselves, there are at most three MU bases containing any of these Diţă matrices.

The results obtained from *randomly* picking points in the fundamental interval are in line with the observations made for grid points. Fig. 3.2 shows N_v, the number of vectors MU with respect to the pair $\{I, D(x)\}$ for all 536 values of the parameter x which we have considered. The

function $N_v(x)$ appears to be symmetric about $x = 0$ and piecewise constant, dropping from 120 for small values of x to 72 at $x \simeq \pm 0.0177$, and to 48 at the end points of the interval, $x = \pm 1/8$. The values for N_v can be found in Table 3.2.

The results for members of *Fourier* family $F(\mathbf{x})$ are qualitatively similar. Picking values of $\mathbf{x} \equiv (x_1, x_2)$ either randomly in the fundamental area or from the two-dimensional grid

$$\Gamma_F = \{(a, b)/144 : a = 1, 2, \ldots, 24,\ b = 0, 1, \ldots, 12,\ a \geq 2b\}\,, \tag{3.11}$$

invariably leads to 48 vectors being MU to the columns of the pair $\{I, F(\mathbf{x})\}$. There are eight different ways to form additional Hadamard matrices for each point considered except for the matrix $F(1/6, 0)$ with an upper bound of 70 triples. It is important to realize that Grassl's result—the construction of complete sets of MU bases cannot be based on the Heisenberg-Weyl group in dimension $d = 6$—also holds for the 2,168 other Fourier matrices we have considered.

The situation is similar when turning to the family of *transposed Fourier* matrices, $F^T(\mathbf{x})$. The number N_v equals 48 throughout and a second Hadamard matrix can be formed in eight different ways, and only matrix $F^T(1/6, 0)$ allows for 70 different triples, eight being the norm.

3.3.3 Non-affine families

The equations $\mathcal{P} = 0$ encoding MU vectors for the symmetric $M(t)$, Hermitean $B(\theta)$ and Szöllősi $X(a, b)$ families turn out to be more challenging from a computational perspective: the program has, in general, not been able to construct the associated Gröbner bases $\mathcal{G}$. The problem is not a fundamental one—the desired Gröbner bases do exist but it appears that their construction requires more memory than the 16GB available to us.

We suspect that the difficulties are due to the fact that, for non-affine matrices, the coefficients of the polynomials $\mathcal{P} = 0$ are no longer equal to fractions or simple roots of integers. When approximating the coefficients in question by fractions we obtain different sets of polynomials, $\tilde{\mathcal{P}}$, and the program indeed succeeds in constructing the corresponding Gröbner bases, $\tilde{\mathcal{G}}$, outputting (approximate) MU vectors $|\tilde{v}\rangle$. Being continuous functions of the coefficients, the approximate vectors will resemble the exact ones, $|\tilde{v}\rangle \simeq |v\rangle$. However, the *number* of MU vectors may change

discontinuously if $\tilde{\mathcal{P}} = 0$ is considered instead of $\mathcal{P} = 0$, similar to the discontinuous change in the number N_v for the family $D(x)$ near $x \simeq 0.0177$, shown in Fig. 3.2. In other words, it could happen that we 'lose' some solutions due to a geometric instability as a consequence of modifying the defining polynomials.

To determine the impact of such an approximation, we have studied how the number N_v of MU vectors changes in a case for which we know rigorous bounds. We retain only five significant digits of the coefficients in the equations $\mathcal{P} = 0$ associated with the family $D(t)$ and solve for the approximate MU vectors. The inset of Fig. 3.2 shows that the plateaus of 120 and 72 MU vectors continue to be well-defined away from the discontinuity at $x \simeq 0.0177$ while the values of N_v fluctuate close to it. Assuming that a qualitatively similar behaviour will also occur for symmetric and Hermitean matrices, we now simplify the equations $\mathcal{P} = 0$ associated with them. Retaining only five significant digits of the coefficients in these equations, we determine the number of MU vectors $|\tilde{v}\rangle$ and their inner products.

Fig. 3.3 shows that the family of *symmetric* Hadamard matrices $M(t)$ comes with 48 MU vectors $|\tilde{v}\rangle$ close to the point $t = 0$, while there are 120 near $t = 1/4$. These numbers are consistent with the rigorous bounds obtained in Section 3.3.2 if we recall that $M(0) = M(1/2) \approx F(0,0)$ and $M(1/4) \approx D(0)$ holds (cf. Fig. 3.1). Across the entire parameter range, the number of MU vectors is a piecewise constant function symmetric about $x = 1/4$, with distinct plateaus of $48, 52, 120$ and possibly 96 MU vectors. We suspect that the other values of N_v near the discontinuities are spurious. An analysis of the scalar products among the approximate MU vectors shows that they can be arranged into between 1 and 16 additional bases; a plot of which also resembles a step function. Crucially, they can never be arranged to form two bases that are MU to each other and therefore the points in Fig. 3.3 cannot be included in a set of four MU bases. Table 3.3 lists the results obtained for both a regular grid

$$\Gamma_M = \{a/144 : a = 1, 2, \ldots, 71; a \neq 36\}\,; \tag{3.12}$$

and 300 randomly selected points in the fundamental interval; the reason for leaving out $a = 36$ is the equivalence $M(1/4) \approx D_0$ just mentioned. We are confident that a more rigorous approach

will confirm the absence of a set of four MU bases containing a single symmetric Hadamard matrix $M(t)$.

H	$\mathbf{x}$	$\#(\mathbf{x})$	N_v	N_t
$M(t)$	Γ_M	70	48-120	1-16
	random	300	48-120	1-16
$B(\theta)$	Γ_B	34	56-120	1/4/8/16
	random	300	56-120	1/4/8/16
$X(a,b)$	Λ	50	48/56	4/16/70
	Λ'	50	48-60	4/8/16/70
	random	300	48-120	1-70

Table 3.3: The number of MU vectors and their properties for *non-affine* Hadamard matrices: the grids Γ_M and Γ_B are defined in Eqs. (3.12) and (3.13), respectively; see Eqs. (3.14) and (3.15) for the definition of the lines Λ and Λ'; other notation as in Table 3.2; preliminary results for the family $X^T(a,b)$ resemble those obtained for $X(a,b)$.

The results obtained for *Hermitean* Hadamard matrices $B(\theta)$, shown in Fig. 3.3, are similar to those of the symmetric family. The observed plateaus conform with the rigorous bounds found for $N_v = 120$ and $N_v = 56$ due to the equivalences $B(1/2) \approx D(0)$ and $B(\theta_0) \approx C$ (cf. Table 3.1). We consider the plateaus at 56, 58, 60, 72, 84 and 108 to be genuine while spurious values for N_v proliferate near their ends, where N_v is likely to vary discontinuously. Once more, Table 3.3 reveals that both regularly spaced points on the grid

$$\Gamma_B = \{a/144 : a = 55, 56, \ldots, 89; a \neq 72\}\,; \tag{3.13}$$

and randomly chosen values of the parameter θ define Hadamard matrices $B(\theta)$ which allow the construction of three MU bases but not four.

Finally, let us consider the *Szöllősi* family, the non-affine two-parameter set of Hadamard matrices $X(a,b)$. Fig. 3.4 shows the values of N_v for randomly chosen parameters on two cuts through parameter space, namely along the line

$$\Lambda = \{(a,b) : \arg(a+ib) = \pi/6\} \tag{3.14}$$

which connects $X(0,0) \approx F(1/6,0)$ to the circulant matrix C, and the randomly chosen line

$$\Lambda' = \{(a,b) : \arg(a+ib) = 0.3510\} \tag{3.15}$$

connecting $X(0,0)$ to $B(\theta')$, a Hermitean Hadamard matrix on the boundary. The values of N_v at the end points of the lines are, in both cases, consistent with results obtained above for $F(1/6,0)$, C, and $B(\theta')$; broadly speaking, the number of solutions again represents a step function. However, the plateaus at $48, 52, 54, 56, 58$ and 60 in Fig. 3.4 (b) show considerable overlap: the effect of approximating the coefficients in the relevant polynomials is even more pronounced for the Szöllősi family than for the other non-affine families. The results for the 300 randomly chosen parameter values sampling the two-dimensional parameter space resemble those of the symmetric and Hermitean families: we find $48 \leq N_v \leq 120$ throughout which allow for triples of MU bases but never for a quadruple. Preliminary calculations show that the properties of the new family of transposed Szöllősi matrices $X^T(a,b)$ are similar to those of the set $X(a,b)$.

While not being exact, the results for the symmetric, Hermitean and Szöllősi families provide bounds on the number of MU bases which can be constructed from their members. None of the Hadamard matrices considered can be extended to a set of four MU bases. We consider it unlikely that the approximation made would systematically suppress other MU vectors with properties invalidating this conclusion.

3.4 Summary of calculations

We have searched for MU bases related to pairs $\{I, H\}$ where I is the unit matrix and H runs through a discrete subset of known (6×6) complex Hadamard matrices. Using Buchberger's algorithm, we have obtained upper bounds on the number of MU bases; the bounds are *rigorous* in many cases and *approximate* in others. Each of the 5,980 calculations required between 4 and 16 GB of memory and, altogether, would have lasted approximately 29,000 hours on a single 2.2 GHz processor.

Each point in Fig. 3.5 represents one of the Hadamard matrices H we have been investigating.

We find that the Spectral matrix S is the only Hadamard matrix which cannot be extended to a triple of MU bases. Furthermore, if four (seven) MU bases were to exist in dimension six three (six) Hadamard matrices different from the ones shown in Fig. 3.5 would be required. This clearly conforms with Conjecture 3.0.1.

There is one caveat that we must make regarding the results for the non-affine families. In general, the program was unable to construct the associated Gröbner bases for the symmetric, Hermitean and Szöllősi families. For these Hadamard matrices, we cannot guarantee that we have found *all* MU vectors although we consider it unlikely that the approximation made would systematically suppress the missing vectors.

The symmetrical presentation of known Hadamard matrices in Fig 3.1 is justified by the results of our calculations: both the number of vectors N_v and the values of their inner products (i.e. the number N_t) are symmetric about the line passing through $F(0,0)$ and S. We will now explain why this symmetry exists.

First, let H be a member of the Diţă, symmetric or Fourier families and consider a vector $|v\rangle$ that is MU to both I and H. Since multiplication by an overall unitary leaves the MU conditions (4.1) invariant, we have the equivalence between sets

$$\{I, H, |v\rangle\} \approx \{H^\dagger, I, H^\dagger|v\rangle\} = \{I, H^\dagger, |v'\rangle\} \tag{3.16}$$

where $|v'\rangle = H^\dagger|v\rangle$. It follows that $|v'\rangle$ is MU to I and $H^\dagger$, and since $D^\dagger(x) \approx D(-x)$, $M^\dagger(t) \approx M(-t)$ and $F^\dagger(x_1, x_2) \approx F^T(x_1, x_2)$, the number of solutions N_v is symmetric about the line through $F(0,0)$ and S. Further, since $H^\dagger$ is unitary and it is applied to all vectors, this transformation leaves the inner products between two MU vectors invariant and therefore, the number of triples N_t is also symmetric.

We need an additional transformation to explain the symmetry found for the Hermitean matrices since $B^\dagger(\theta) = B(\theta)$: under complex conjugation a Hermitean matrix transforms according to

$$B^*(\theta) = B(1-\theta)\,,$$

as follows from the explicit form of $B(\theta)$ given in Eq. (C.7). Now consider a vector $|v\rangle$ which is MU to the columns $b(\theta)$ of the matrix $B(\theta)$; then

$$|\langle b(\theta)|v\rangle|^2 = |\langle b(\theta)|v\rangle^*|^2 = |\langle b^*(\theta)|v^*\rangle|^2 = |\langle b(1-\theta)|v^*\rangle|^2 \ ,$$

and therefore $|v^*\rangle$ is MU to each column of $B(1-\theta)$. Thus, the vectors MU to $B(\theta)$ are the complex conjugates of those MU to $B(1-\theta)$ which implies that the number N_v of MU vectors (and their properties) will not change upon a reflection about the point $\theta = 1/2$. Although we did not pay attention to the existence of these exact symmetries when introducing the approximations for the non-affine Hadamard matrices, the results obtained do respect them.

The set of Hadamard matrices in $\mathbb{C}^6$ may depend on four parameters [16], a conjecture which recently gained some numerical support [136]. It remains difficult to draw general conclusions about the number of MU bases in dimension $d = 6$. However, we would like to point out that the approach presented here is *future-proof*: it will work for any Hadamard matrix - including currently unknown ones.

We have found 48 vectors MU to $F(x_1, x_2)$ and $F^T(x_1, x_2)$ for each of the 4,336 values of (x_1, x_2) sampled from the corresponding fundamental regions. Since the work contained in this chapter was presented in [33], Jaming et. al. have shown that this in fact holds for *all* members of the Fourier and Fourier transpose families [84]. That is, for all (x_1, x_2) there are 48 solutions to the equations defined by Eqs. (3.3) and (3.4). Furthermore, Jaming et al. prove that no member of the Fourier or Fourier transpose family can be contained in a triple of MU bases [84]; thus generalising some of the results presented here. In the Chapter 7 we will discuss how one might extend the approach presented in this chapter to exclude parameter dependent families of complex Hadamard matrices from a complete set of MU bases in dimension six.

In summary, we have shown that the construction of more than three MU bases in $\mathbb{C}^6$ is not possible starting from nearly 6,000 different Hadamard matrices. This result adds significant weight to the conjecture that a complete set of seven MU bases does not exist in dimension six. It becomes ever more likely that only prime-power dimensions allow for optimal state reconstruction.

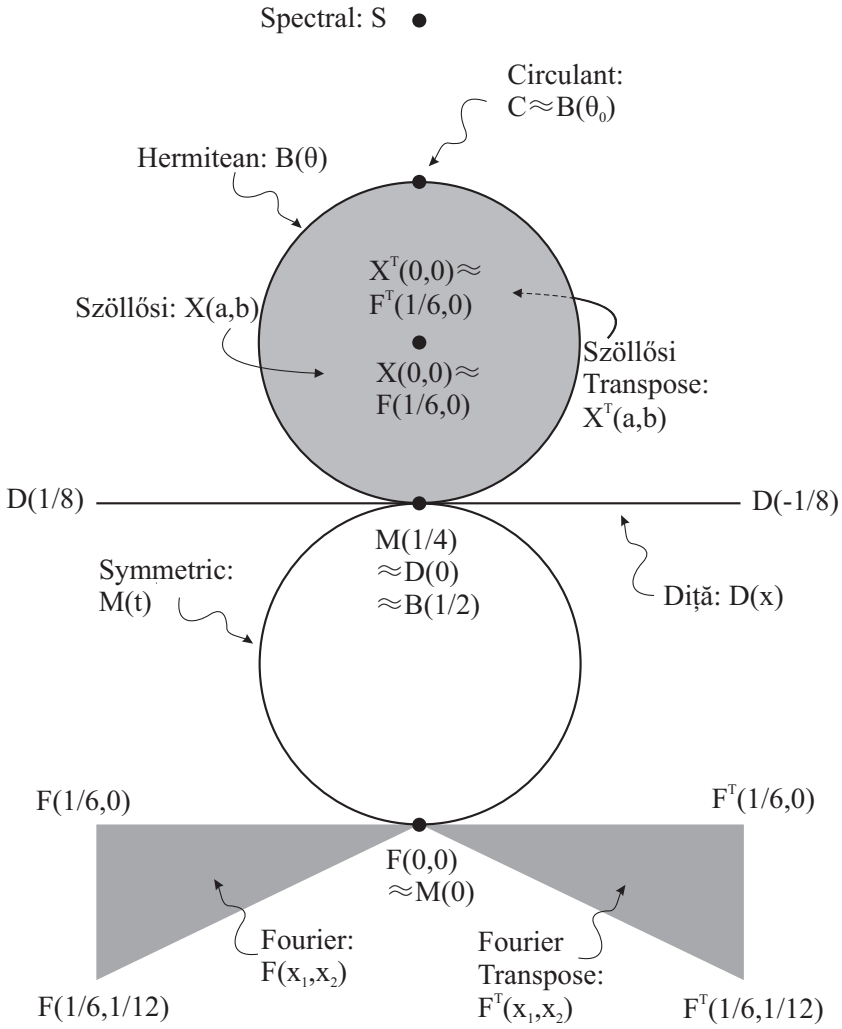

Figure 3.1: The set of known Hadamard matrices in dimension six consists of *special* Hadamard matrices $F(0,0) \equiv F_6, D(0) \equiv D_0, C$, and S, located on the vertical symmetry axis; of the *affine* families $D(x)$, $F(\mathbf{x})$, and $F^T(\mathbf{x})$; and of the *non-affine* families $M(t)$, $B(\theta)$, $X(a,b)$, and $X^T(a,b)$ (see Appendix C for definitions). Note that the sets $X(a,b)$ and $X^T(a,b)$ cover the interior of the upper circle twice and that the Diţă family, $D(x)$, is contained in $X(a,b)$.

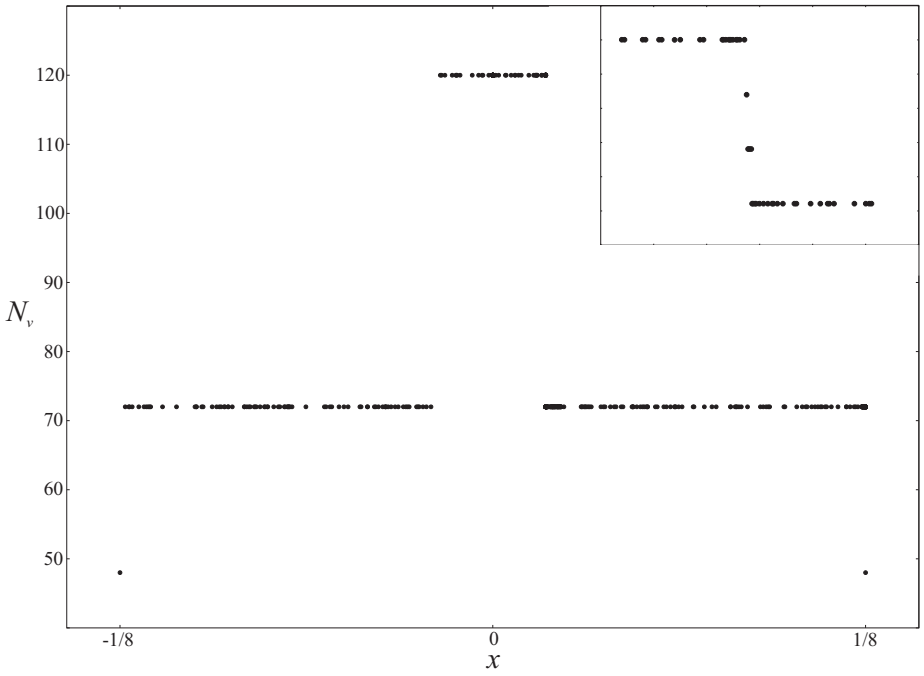

Figure 3.2: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and Diţă matrices $D(x)$; the parameter x assumes 72 parameter values $x \in \Gamma_D$, and 500 randomly chosen ones in the fundamental interval $[-1/8, 1/8]$ of the parameter x. The inset illustrates the impact on N_v near the discontinuity $x \simeq 0.0177$ if an *approximate* set of equations is used (cf. Section 3.3.3).

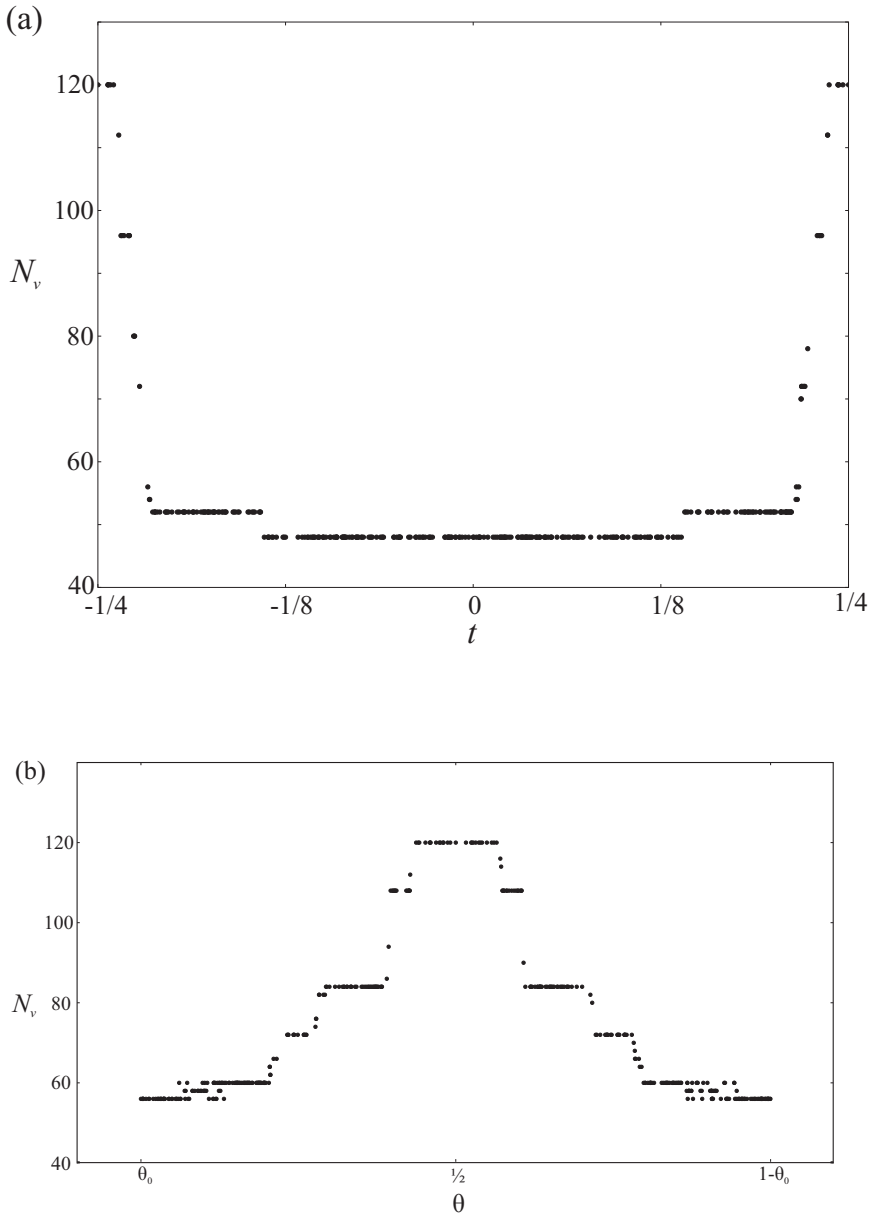

Figure 3.3: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and (a) symmetric Hadamard matrices $M(t)$; the parameter t assumes 60 parameter values $t \in \Gamma_M$, and 300 randomly chosen ones in the fundamental interval $[0, 1/2]$, and of (b) Hermitean matrices $B(\theta)$; the parameter θ assumes 34 parameter values $\theta \in \Gamma_B$, and 300 randomly chosen ones in the fundamental interval $[\theta_0, 1 - \theta_0]$. The phase θ_0 has been defined in equation (C.8).

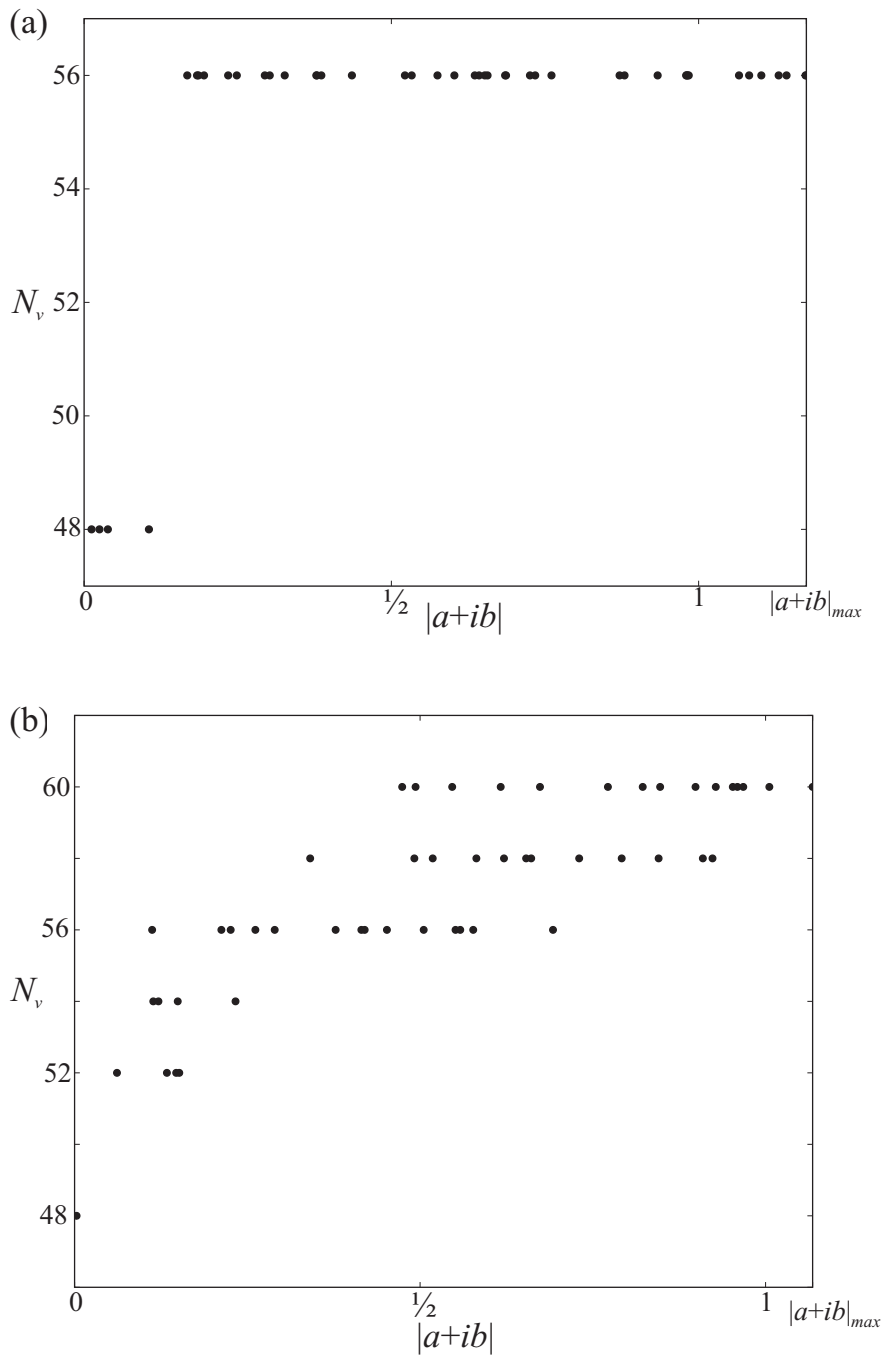

Figure 3.4: The number N_v of vectors $|v\rangle$ which are MU with respect to the columns of the identity I and Szöllősi Hadamard matrices $X(a,b)$ for 50 randomly chosen parameter values (a) on the line Λ connecting $F(1/6,0)$ to C, and (b) on the line Λ' connecting $F(1/6,0)$ to $B(\theta')$; in both figures, the maximum modulus $|a+ib|_{\max}$ is defined by Eq. (C.14).

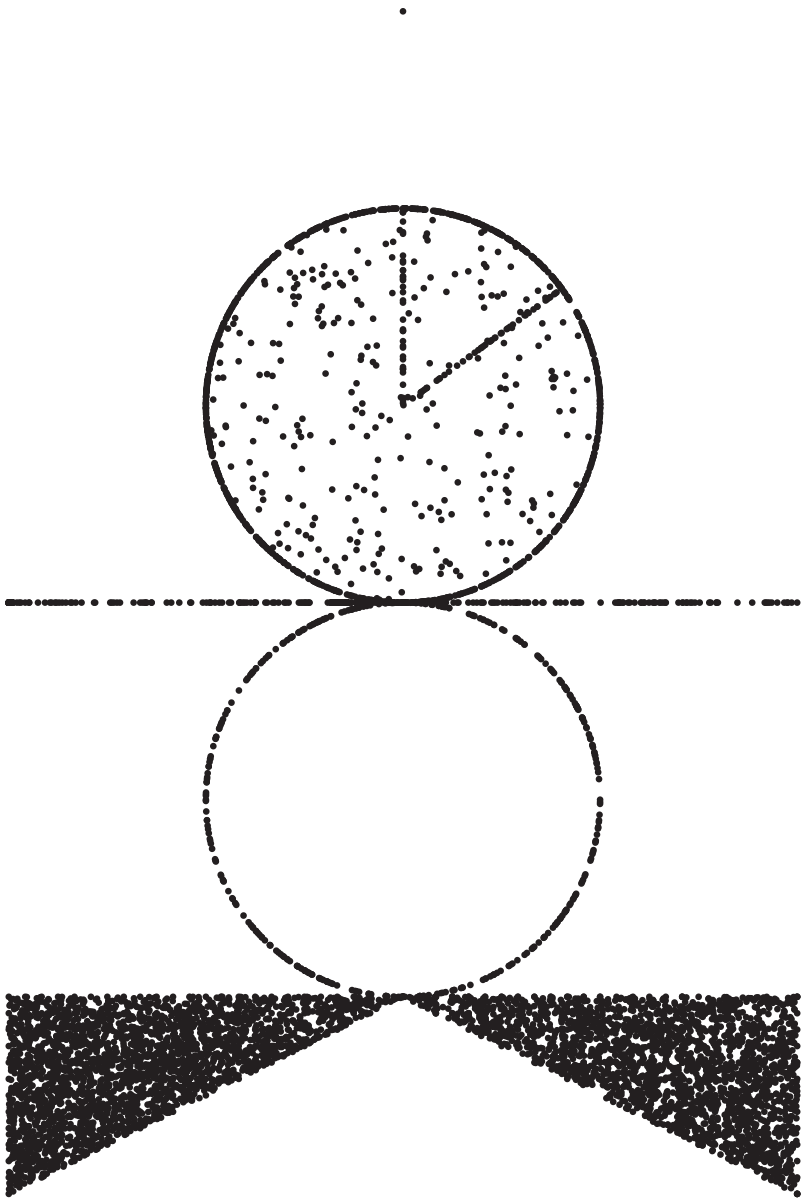

Figure 3.5: The set of all Hadamard matrices H which have been considered (cf. Fig. 3.1 and Tables 3.1-3.3): for each H, a second MU Hadamard matrix can always be found except for the isolated spectral matrix S; consequently, triples of MU bases are the norm while quartets of MU bases do not exist.

CHAPTER 4

Maximal sets of mutually unbiased states in dimension six

In the previous chapter, we were unable to find more than three MU bases in dimension six by systematically sampling all known complex Hadamard matrices. However, the classification of Hadamard matrices in dimension six is incomplete leaving open the possibility that we may have missed some (crucial) part of the Hilbert space $\mathbb{C}^6$. In this chapter, we drop the reliance on existing constructions of Hadamard matrices and search for MU bases numerically.

We begin by re-writing the conditions for a set of vectors to form a complete set of MU bases. Given a quantum system of dimension d, a *complete set of MU bases* in $\mathbb{C}^d$ is a set of $d(d+1)$ pure states $|\psi_j^x\rangle$, $x = 0, 1, \ldots, d$, $j = 1, \ldots, d$, which satisfy the conditions

$$\left|\langle\psi_i^x|\psi_j^y\rangle\right| = \begin{cases} \delta_{ij} & \text{if } x = y\,, \\ \frac{1}{\sqrt{d}} & \text{if } x \neq y\,. \end{cases} \tag{4.1}$$

In this chapter we systematically search for *subsets* of complete sets of MU bases which we will call *MU constellations*. Essentially, a MU constellation consists of groups of d or fewer vectors having scalar products as in (4.1). Three MU bases, known to exist in any dimension d, are a well-known example of a MU constellation, and as seen in Chapter 3, it has been conjectured that no more than three MU bases exist in dimension six [152]. Conjecture 3.0.1 is supported by

numerical evidence given in [38] reporting *unsuccessful* searches for four MU bases, another MU constellation. Similarly, no four MU bases have been found within a set of vectors determined by the assumption that their components have a specific form such as being certain roots of unity [16]. The non-existence of a MU constellation consisting of three MU bases plus one additional vector, related to the Heisenberg-Weyl group, has been shown in [72]. And finally, in Chapter 3, we have seen how Grassl's result can be extended to exclude 6,000 complex Hadamard matrices sampled from the set of all known Hadamards. There are, however, many other entirely unexplored MU constellations.

The chapter is organised as follows. In the next section, we introduce the concept of MU constellations and embed them in well-defined searchable spaces. Then, in Section 4.2 the search for MU constellations is cast into the form of a numerical minimisation. Section 4.3 describes the results of the searches, and they will be discussed in the final section.

4.1 Constellations of quantum states in $\mathbb{C}^d$

In this section we define *mutually unbiased constellations* of quantum states and embed them in appropriate spaces to search for them.

4.1.1 Mutually unbiased constellations

A *MU constellation* in $\mathbb{C}^d$ consists of $(d+1)$ sets of λ_x pure states $|\psi_j^x\rangle$, $x = 0, 1, \ldots, d$, $j = 1, \ldots, \lambda_x$, which satisfy the conditions (4.1). The $(d+1)$ integers $\lambda_x \in \{0, \ldots, d-1\}$ specify all possible types of MU constellations which will be denoted by

$$\{\lambda\}_d \equiv \{\lambda_0, \lambda_1, \ldots, \lambda_d\}_d\,, \quad \lambda \in (\mathbb{Z} \bmod (d-1))^{d+1}\,. \tag{4.2}$$

If the number λ_x in a MU constellation $\{\lambda\}_d$ equals zero, it corresponds to an empty set and will be suppressed. For example, $\{2,1,2,0\}_4 \equiv \{2,1,2\}_4$ denotes a MU constellation in $\mathbb{C}^4$ which consists of two pairs of orthonormal vectors and one single vector. Since the ordering of the bases within a constellation will be irrelevant, we arrange them in decreasing order, using the

shorthand λ^a if there are a bases with λ elements: $\{2,1,2\}_4$ thus becomes $\{2^2,1\}_4$.

The numbers λ_x are limited to $(d-1)$ since there is only one way to complete $(d-1)$ orthonormal vectors to a basis of the space $\mathbb{C}^d$, apart from an irrelevant phase factor. More explicitly, the complement of $(d-1)$ orthonormal vectors $|\psi_j\rangle \in \mathbb{C}^d, j = 1,\ldots,d-1$, is a unique one-dimensional subspace spanned by $|\psi_\perp\rangle$, say. Due to the completeness relation for an orthonormal basis, the projector on this subspace must have the form

$$|\psi_\perp\rangle\langle\psi_\perp| = \mathbb{I}_d - \sum_{j=1}^{d-1} |\psi_j\rangle\langle\psi_j|\,, \tag{4.3}$$

where $\mathbb{I}_d$ is the identity in $\mathbb{C}^d$.

The completion of $(d-1)$ orthonormal vectors into a basis is *consistent* with the conditions of mutual unbiasedness (4.1). The identity (4.3) implies that the state $|\psi_\perp\rangle$ is MU with respect to any vector $|v\rangle$ satisfying $|\langle\psi_j|v\rangle| = 1/\sqrt{d}$, hence any MU constellation containing the states $\{|\psi_j\rangle\}$ remains MU if the state $|\psi_\perp\rangle$ is added to the set.

MU constellations in $\mathbb{C}^d$ are a *partially ordered set* with respect to the relation $\leq$ defined by

$$\{\lambda\}_d \leq \{\mu\}_d \Longleftrightarrow \lambda_x \leq \mu_x\,, \qquad \text{for all } x = 0,1,\ldots,d\,. \tag{4.4}$$

The ordering refers only to the *number* of vectors in each basis; it does not imply any relation between the subspaces spanned by the vectors in corresponding 'partial bases' of the constellations $\{\lambda\}_d$ and $\{\mu\}_d$. If (4.4) holds, we will say that $\{\mu\}_d$ *contains* $\{\lambda\}_d$; alternatively, $\{\lambda\}_d$ is said to be *smaller* than $\{\mu\}_d$. For example, the MU constellation $\{2^2,1\}_4$ is contained in four MU bases $\{3^4\}_4$ because

$$\{2^2,1\}_4 \leq \{3^4\}_4 \tag{4.5}$$

is true. The ordering induced by (4.4) is only partial since constellations such as $\{3,1\}_4$ and $\{2^2\}_4$ cannot be compared to each other. Thus, MU constellations possess a *lattice structure* with a unique minimal element, $\emptyset$, and $(d+1)$ MU bases $\{(d-1)^{d+1}\}_d$, if existing, provide a unique maximal element.

Here is an important consequence of the lattice structure. A set of $k \in \{2,\ldots,d+1\}$ complete

MU bases $\{(d-1)^k\}_d$ in dimension d exists only if all *smaller* MU constellations $\{\lambda\}_d$ exist, i.e. those with

$$\{\lambda_0, \lambda_1, \ldots, \lambda_{k-1}\}_d \leq \{(d-1)^k\}_d\,, \quad 0 \leq \lambda_x \leq d-1\,, \quad x = 0, 1, \ldots, k-1\,. \tag{4.6}$$

Hence, if any MU constellation $\{\lambda_0, \lambda_1, \ldots, \lambda_k\}_d$ is found missing then k complete MU bases cannot exist. This observation has been exploited in [38] where the unsuccessful numerical search for four MU bases, i.e. the MU constellations $\{5^4\}_6$, is used to argue that no seven MU bases exist for $d = 6$. Similarly, it has been shown in [72] that it is impossible in $\mathbb{C}^6$ to extend two MU bases $\{5^2\}_6$ *of a specific type* to the MU constellation $\{5^3, 1\}_6$, excluding thus the existence of seven MU bases based on a specific construction.

Evidence for the non-existence of any small MU constellation is evidence for the non-existence of the corresponding complete set of MU bases. This observation is crucial for the main thrust of this chapter.

4.1.2 Constellation spaces

In Section 4.3, we will numerically search for all MU constellations $\{\lambda\}_6$ in $\mathbb{C}^6$ contained in $\{5^4\}_6$, i.e. in *four* MU bases. To do this, we need to search through a space which is guaranteed to contain a specific MU constellation if it exists; at the same time, the search space should be as small as possible to maximize computational efficiency. From now on, we will only consider MU constellations which contain at least one complete basis,

$$\{\lambda\}_d \equiv \{d-1, \lambda_1, \ldots, \lambda_d\}_d\,, \tag{4.7}$$

which is a mild restriction that allows considerable simplifications.

To associate an appropriate space with a given MU constellation $\{\lambda\}_d$ of type (4.7), we will need to write it in *dephased* form. Once dephased, its first $(d-1)$ vectors are given by those of the standard basis $\mathcal{B}_z$, while the components of the first vector of the second basis and the first component of each remaining vector are equal to $1/\sqrt{d}$. For example, upon dephasing a MU

constellation $\{2^3,1\}_3$, it takes the form

$$\left\{\begin{pmatrix}1&0\\0&1\\0&0\end{pmatrix},\frac{1}{\sqrt{3}}\begin{pmatrix}1&1\\1&e^{i\alpha_{11}}\\1&e^{i\alpha_{21}}\end{pmatrix},\frac{1}{\sqrt{3}}\begin{pmatrix}1&1\\e^{i\beta_{11}}&e^{i\beta_{12}}\\e^{i\beta_{21}}&e^{i\beta_{22}}\end{pmatrix},\frac{1}{\sqrt{3}}\begin{pmatrix}1\\e^{i\gamma_{11}}\\e^{i\gamma_{21}}\end{pmatrix}\right\}, \tag{4.8}$$

with specific values for the eight angles $\alpha_{11},\ldots,\gamma_{21}$. It is shown in Appendix A that any given MU constellation of type (4.7) can be written in dephased form by applying transformations which leave invariant the conditions (4.1).

Now it is straightforward to associate a *space of constellations* with the MU constellation $\{2^3,1\}_4$: the space $\mathcal{C}_4(2^3,1)$ is defined as the set of vectors one obtains from (4.8) if the eight angles $\alpha_{11},\ldots,\gamma_{21}$, are allowed to vary freely between 0 and 2π. Each point in this space will be called a *constellation* $[2^3,1]_4$, and it corresponds to a set of seven (not necessarily different) pure states in $\mathbb{C}^4$. Not all constellations $[2^3,1]_4$ are a MU constellation $\{2^3,1\}_4$, but each MU constellation $\{2^3,1\}_4$ is represented by at least one point of the space $\mathcal{C}_4(2^3,1)$.

In general, each MU constellation $\{\lambda\}_d$ is embedded in space $\mathcal{C}_d(\lambda)$ of constellations $[\lambda]_d$, defined in analogy to $\mathcal{C}_4(2^3,1)$. Simply write down the dephased form of the MU constellation $\{\lambda\}_d$ at hand; then, varying the angles $\alpha_{11},\ldots$ between 0 and 2π, generates the space of constellations

$$\mathcal{C}_d(\lambda)\ni[\lambda]_d=[d-1,\lambda_0,\ldots,\lambda_d]_d\,. \tag{4.9}$$

The space $\mathcal{C}_d(\lambda)$ has the structure of a multi-dimensional *torus* due to the periodicity of the angles used to parameterize it.

Let us now determine the dimension of the space $\mathcal{C}_d(\lambda)$ associated with a MU constellation (4.7). It contains

$$S=d-1+s \tag{4.10}$$

quantum states where

$$s=\sum_{b=1}^{d}x_b \tag{4.11}$$

is the number of states in all groups but the first one. Since each of these vectors except the first

one brings $(d-1)$ phases, the entire constellation $[\lambda]_d$ depends on

$$p_d \equiv p\left([d-1, \lambda_1, \lambda_2, \ldots, \lambda_d]_d\right) = (d-1)(s-1) \tag{4.12}$$

independent real parameters. For example, the constellation space $\mathcal{C}_d((d-1)^{d+1})$ associated with $(d+1)$ complete MU bases has dimension $(d-1)(d^2-d-1)$.

How many constraints does the requirement of mutual unbiasedness in (4.1) impose on the parameters of a constellation $[\lambda]_d$? The states of a constellation are normalized, and the conditions on scalar products involving vectors of the first basis are satisfied by construction. Hence, there remains one condition for each pair of different states taken from the last d bases plus an additional condition for each pair of vectors from the same basis. The extra condition resulting from the orthogonality of two vectors is due to the fact that both the real *and* imaginary parts of their inner product are required to be zero. Consequently, the number of *constraints* is given by

$$\begin{aligned} c_d &\equiv c_d\left([d-1, \lambda_1, \lambda_2, \ldots, \lambda_d]_d\right) \\ &= \frac{1}{2}s(s-1) + \frac{1}{2}\sum_{x=1}^{d}\lambda_x(\lambda_x - 1) \\ &= \frac{1}{2}s(s-2) + \frac{1}{2}\sum_{x=1}^{d}\lambda_x^2. \end{aligned} \tag{4.13}$$

Note that the number of constraints, c_d, presented in [32] is corrected by Eq. (4.13). The error being due to counting the real and imaginary parts of the inner product of two orthogonal vectors as only one equation.

4.2 Numerical search for MU constellations

This section explains the numerical method we use to identify MU constellations. The basic idea is to define a continuous function on the space of constellations $\mathcal{C}$ that takes the value zero if and only if the input is a MU constellation. We then search for the zeros of this function in the neighborhood of a large number of randomly chosen points in $\mathcal{C}$, using standard numerical

methods.

4.2.1 MU constellations as global minima

Suppose you want to find the MU constellation $\{\lambda\}_d$. To do so, consider the associated space of constellations $\mathcal{C}_d(\lambda)$ which can be parameterized by p_d angles denoted by $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{p_d})^T$. Defining

$$\chi_{ij}^{xy} = \begin{cases} \delta_{ij} & \text{if } x = y\,, \\ \frac{1}{\sqrt{d}} & \text{if } x \neq y\,, \end{cases} \tag{4.14}$$

the non-negative function $F : \mathbb{R}^{p_d} \to \mathbb{R}$

$$F(\boldsymbol{\alpha}) = \sum_{1 \leq x \leq y}^{d} \sum_{i=1}^{\lambda_x} \sum_{\substack{j=1 \\ \text{if } x=y, \\ i<j}}^{\lambda_y} \Big(|\langle \psi_i^x(\boldsymbol{\alpha}) | \psi_j^y(\boldsymbol{\alpha}) \rangle| - \chi_{ij}^{xy} \Big)^2, \tag{4.15}$$

equals zero if and only if the input $[\lambda]_d$ coincides with a MU constellation $\{\lambda\}_d$.

It is thus possible, in principle, to prove the (non-) existence of a MU constellation by determining whether the smallest value of the function $F(\boldsymbol{\alpha})$ is non-zero. This means to identify its (possibly degenerate) *global* minimum which, unfortunately, is not simple: the global minimisation of a nonlinear function such as a polynomial of fourth order in sufficiently many variables may already pose a NP-hard problem [112]. A well-known strategy is to search for minima by starting from random initial points which, however, may turn out to be *local* ones. By repeating the process sufficiently often, one will detect global minima as well—if they exist.

A numerical search along similar lines has been reported in [38], restricted, however, to the MU constellations $\{5^4\}_6$ and $\{5^7\}_6$, that is, four or seven MU bases. This limitation allows for a different parametrization which exploits the fact that complete bases in dimension d are associated with d-dimensional unitary matrices.

Note that the choice of the function $F(\boldsymbol{\alpha})$ is not unique[1]. The expression (4.15) is convenient because efficient minimisation tools are available for a sum of squares. In particular, the

[1] We have also considered an everywhere differentiable variant of (4.15) obtained by subtracting the square of χ_{ij}^{xy} from $|\langle \psi_i^x | \psi_j^y \rangle|^2$. We noticed, however, that the success rate to find existing MU constellations is systematically lower.

Levenberg-Marquardt algorithm [99, 103], often used in Regressional Analysis, cleverly switches between the method of steepest descent and the Gauss-Newton algorithm to speed up convergence. To search for zeros of the function $F(\boldsymbol{\alpha})$, we use the function `optimize.leastsq` from the Open-Source Python package SciPy [86] which implements the LM-algorithm.

The function $F(\boldsymbol{\alpha})$ achieves its maximum

$$F_{\max} = \frac{1}{2}\sum_{x=1}^{d}\lambda_x(\lambda_x - 1) + \left(\frac{\sqrt{d}-1}{\sqrt{d}}\right)^2 \sum_{1\le x<y}^{d}\lambda_x\lambda_y\,, \tag{4.16}$$

if all states coincide, each having components equal to $1/\sqrt{d}$ only. For typical constellations such as $\{5^2, 4, 1\}_6$ or $\{5, 3^3\}_6$, one finds $F_{\max} = 33.2$ and $F_{\max} = 25.0$, respectively. Fig. 4.1(a) shows a two-dimensional contour plot of $F(\boldsymbol{\alpha})$ in the 45-dimensional constellation space $\mathcal{C}_6(5, 4^2, 2)$. Ranging between 2.6 and 3.6, the function $F(\boldsymbol{\alpha})$ exhibits one maximum, one minimum, and two saddle points. This structure is consistent with (4.15) because $F(\boldsymbol{\alpha})$ reduces to a simple trigonometric polynomial of two variables if all but the first two angles $\alpha_1 \equiv u, \alpha_2 \equiv v$, are fixed.

Considering the range of the function F, it appears reasonable to say that a MU constellation $[\lambda]_d$ parameterized by $\boldsymbol{\alpha}$ has been found if $F(\boldsymbol{\alpha})$ assumes a value below

$$F_{\rm c} = 10^{-7}\,. \tag{4.17}$$

This criterion, stronger than the one used in [38] is entirely arbitrary, and smaller values could be used at the expense of computational time. The numerical data presented below will retrospectively justify the chosen value of the threshold for zeros of $F_{\rm c}$.

4.2.2 Testing the numerical search

We begin by presenting searches for MU constellations which are known to exist. The data provide evidence that the numerical minimization of $F(\boldsymbol{\alpha})$ defined in Eq. (4.15) is a reliable tool to identify MU constellations.

Three complete MU bases

It is known that one can construct *three* complete MU bases in the space $\mathbb{C}^d$ without referring to the prime decomposition of d [72]. Let us check the proposed minimisation method by searching for the MU constellations $\{(d-1)^3\}_d$ in dimensions $d = 2, 3, \ldots, 8$. Table 4.1 displays the success rates obtained for a total of 1,000 searches in each of these dimensions. The input consists of constellations $[(d-1)^3]_d$ chosen randomly in the constellation space $\mathcal{C}_d((d-1)^3) \equiv [0, 2\pi)^{p_d}$, with $p_d = (d-1)(2d-3)$. Each dephased constellation $[(d-1)^3]_d$ corresponds to $3(d-1)$ pure states in $\mathbb{C}^d$.

d	2	3	4	5	6	7	8
p_d	1	6	15	28	45	66	91
%	100.0	81.9	96.6	49.3	67.9	24.0	48.5

Table 4.1: Success rates for searches of three MU bases $\{(d-1)^3\}_d$ in dimensions $d = 2, 3, \ldots, 8$, based on 1,000 initial points randomly chosen in the p_d-dimensional space $\mathcal{C}_d((d-1)^3)$.

The searches are successful in all dimensions. The rate of success systematically decreases for larger dimensions if even and odd dimensions are considered separately. This overall trend is not surprising in view of the constant number of samples taken in ever bigger spaces $\mathcal{C}_d$. The success rate is consistently higher in even dimensions which might be attributed to the possibility of constructing different types of triples of MU bases resulting from the factor of two in $d = 4, 6, 8$.

MU constellations in dimension five

Next, we test the minimisation procedure by systematically searching for MU constellations of the form $\{4, \lambda, \mu, \nu\}_5$, i.e. all MU constellations in dimension $d = 5$ contained in four MU bases. The results from 1,000 searches for each MU constellation have been collected in Table 4.2. The success rate gradually decreases from 100% for MU constellations with 16 or fewer parameters to 10% for MU constellations with 44 parameters. All MU constellations are identified. In view of later developments the table also makes explicit the number of free parameters for each dephased constellation.

To judge the quality of the minimisation procedure, it is instructive to plot the distribution

$d=5$	parameters p_5				success rate			
λ,μ	ν				ν			
	1	2	3	4	1	2	3	4
1,1	8	-	-	-	100.0	-	-	-
2,1	12	-	-	-	100.0	-	-	-
2,2	16	20	-	-	100.0	96.4	-	-
3,1	16	-	-	-	100.0	-	-	-
3,2	20	24	-	-	92.0	35.7	-	-
3,3	24	28	32	-	68.3	38.0	29.0	-
4,1	20	-	-	-	99.0	-	-	-
4,2	24	28	-	-	56.2	37.0	-	-
4,3	28	32	36	-	55.8	31.8	21.8	-
4,4	32	36	40	44	37.4	20.1	14.9	9.7

Table 4.2: Success rates for searches of MU constellations $\{4,\lambda,\mu,\nu\}_5$ in dimension five, based on 1,000 initial points randomly chosen in the p_5-dimensional space $\mathcal{C}_5(4,\lambda,\mu,\nu)$.

of the minimal values of $F(\boldsymbol{\alpha})$ obtained in the space $\mathcal{C}_5(4^3,2)$, say. The histogram in Fig. 4.2(a) shows that *global* minima, defined by $F < 10^{-7}$, are separated from *local* minima by several orders of magnitude, justifying the criterion (4.17). For a random sample of these 'zeros,' we have been able to reduce the value of $F(\boldsymbol{\alpha})$ to less than 10^{-20}, simply by running the search for longer.

Note that by detecting one MU constellation in a particular run, all MU constellations contained in it have also been found. Thus, Table 4.2 does not only report 370 incidences of the MU constellation $\{4^2,2^2\}_5$ but since MU constellations form a lattice due to (4.4), all successful searches to the right and below this entry also confirm its presence, adding a further 983 detected cases.

Fig. 4.1(b) shows a contour plot of the function $F(\boldsymbol{\alpha})$ in a two-dimensional neighbourhood of a zero, i.e. of a MU constellation of type $\{4^3,2\}_5$. Qualitatively, it resembles the random cross-section depicted above it.

MU constellations in dimension seven

In dimension seven, a complete set of eight MU bases exists. Thus, we expect a numerical search to successfully identify all MU constellations with no more than four partial bases. The largest

$d=7$	parameters p_7						success rate					
λ,μ	ν						ν					
	1	2	3	4	5	6	1	2	3	4	5	6
1,1	12	-	-	-	-	-	100.0	-	-	-	-	-
2,1	18	-	-	-	-	-	100.0	-	-	-	-	-
2,2	24	30	-	-	-	-	100.0	100.0	-	-	-	-
3,1	24	-	-	-	-	-	100.0	-	-	-	-	-
3,2	30	36	-	-	-	-	100.0	100.0	-	-	-	-
3,3	36	42	48	-	-	-	100.0	100.0	99.3	-	-	-
4,1	30	-	-	-	-	-	100.0	-	-	-	-	-
4,2	36	42	-	-	-	-	100.0	100.0	-	-	-	-
4,3	42	48	54	-	-	-	99.9	95.6	0.0	-	-	-
4,4	48	54	60	66	-	-	52.3	0.0	0.0	0.0	-	-
5,1	36	-	-	-	-	-	100.0	-	-	-	-	-
5,2	42	48	-	-	-	-	100.0	37.9	-	-	-	-
5,3	48	54	60	-	-	-	2.6	0.0	0.1	-	-	-
5,4	54	60	66	72	-	-	0.0	0.0	0.0	0.1	-	-
5,5	60	66	72	78	84	-	0.2	0.2	0.2	0.1	0.2	-
6,1	42	-	-	-	-	-	57.5	-	-	-	-	-
6,2	48	54	-	-	-	-	1.1	0.0	-	-	-	-
6,3	54	60	66	-	-	-	0.0	0.1	0.0	-	-	-
6,4	60	66	72	78	-	-	0.2	0.0	0.1	0.3	-	-
6,5	66	72	78	84	90	-	0.3	0.4	0.1	0.1	0.1	-
6,6	72	78	84	90	96	102	0.5	0.2	0.2	0.0	0.4	0.3

Table 4.3: Success rates for searches of MU constellations $\{6,\lambda,\mu,\nu\}_7$ in dimension seven, based on 1,000 initial points randomly chosen in the p_7-dimensional space $\mathcal{C}_7(6,\lambda,\mu,\nu)$.

constellation, $\{6^4\}_7$, now depends on 102 parameters, more than double the number occurring in dimension five. Due to this substantial expansion of the parameter space, however, the search for zeros of the function $F(\boldsymbol{\alpha})$ is likely to succeed less frequently.

These expectations are confirmed by the results collected in Table 4.3. As in dimension five, the success rates decrease if we search for MU constellations containing more states. Although the spaces searched are considerably larger, we still find four out of five MU constellations of the form $\{6,x,y,z\}_7$ after 1,000 attempts. Overall, the success rates show a feature not observed in dimension five: the high detection rate for small MU constellations drops sharply when the number of parameters, p_7, is greater than 48. Importantly, 22 of the 34 MU constellations $\{x\}_7$ beyond the 'line' of constellations with 54 or more parameters have been identified. Taken

together, the success rate for the $34,000$ searches for constellations with $p_7 \geq 51$ was $\sim 0.13\%$. It is true that the success rate is small but the basin of attraction for global minima is likely to be only a tiny region in the high-dimensional search space.

The quality of the zeros is excellent: they correspond to values of $F(\boldsymbol{\alpha})$ below 10^{-12}, being clearly different from the vast majority of local minima producing values in the order of 10^{-3}. This is illustrated in the histogram Fig. 4.3(a) which combines all the minima obtained for constellations $\{\lambda\}_7$ defined by 66 or more parameters. We associate the clusters of values at 10^{-13} and at 10^{-3} with global and local minima, respectively.

It is straightforward to check that the numerically identified MU constellations reproduce the numbers χ_{ij}^{xy} in (4.14), correct to seven significant digits. We are thus confident to have identified these MU constellations in dimension seven.

4.3 MU constellations in dimension six

Knowing that the numerical procedure to minimise $F(\boldsymbol{\alpha})$ defined in (4.15) generates reliable data, we now turn to the main findings of this chapter which are related to dimension six.

In Table 4.4, we present the success rates to identify all MU constellations contained in four MU bases $\{5^4\}_6$, i.e.

$$\{5, \lambda, \mu, \nu\}_6\,, \quad 1 \leq \lambda, \mu, \nu \leq d-1\,. \tag{4.18}$$

We will proceed as in dimensions $d = 5$ and $d = 7$ but, in order to give our results additional weight, we have performed 10,000 searches for each MU constellation.

The results exhibit a structure which differs qualitatively from the findings in neighboring dimensions. The success rates decrease as before if the search aims at MU constellations with increasing numbers of free parameters. However, after dropping to zero when the number of parameters exceeds 40, there is no evidence for a single MU constellation $\{\lambda\}_6$.

It is true that only a few of these MU constellations had been identified in dimension seven; considering their abundance in $d = 5$, however, their complete absence in $d = 6$ is a striking feature which we consider to be statistically relevant. Note that the lattice structure due to (4.4) allows us to conclude that unsuccessful searches for MU constellations *contained* in $\{5^4\}_6$ also

$d=6$	parameters p_6					success rate				
λ,μ	ν					ν				
	1	2	3	4	5	1	2	3	4	5
1,1	10	-	-	-	-	100.00	-	-	-	-
2,1	15	-	-	-	-	100.00	-	-	-	-
2,2	20	25	-	-	-	100.00	100.00	-	-	-
3,1	20	-	-	-	-	100.00	-	-	-	-
3,2	25	30	-	-	-	99.95	100.00	-	-	-
3,3	30	35	40	-	-	99.42	39.03	0.00	-	-
4,1	25	-	-	-	-	100.00	-	-	-	-
4,2	30	35	-	-	-	92.92	44.84	-	-	-
4,3	35	40	45	-	-	12.97	0.00	0.00	-	-
4,4	40	45	50	55	-	0.74	0.00	0.00	0.00	-
5,1	30	-	-	-	-	95.40	-	-	-	-
5,2	35	40	-	-	-	76.71	10.96	-	-	-
5,3	40	45	50	-	-	1.47	0.00	0.00	-	-
5,4	45	50	55	60	-	0.00	0.00	0.00	0.00	-
5,5	50	55	60	65	70	0.00	0.00	0.00	0.00	0.00

Table 4.4: Success rates for searches of MU constellations $\{5,\lambda,\mu,\nu\}_6$ in dimension six, based on 10,000 initial points randomly chosen in the p_6-dimensional space $\mathcal{C}_6(5,\lambda,\mu,\nu)$.

count against its existence. Since none of the constellations it contains have been found, Table 4.4 effectively reports a total of 170,000 *negative* instances for the MU constellation $\{5^4\}_6$.

The minimal values of $F(\boldsymbol{\alpha})$ obtained for most of the constellations on and near the critical line are not below 1.1×10^{-4} except for $\{5,4,3,2\}_6, \{5,4^2,2\}_6$, and $\{5,3^3\}_6$, where values close to 10^{-6} have been obtained. We have not been able to push the these values below the threshold of 10^{-7}, even by running the search considerably longer. The histogram Fig. 4.2(b) shows that the minima obtained for $\{5,4^2,2\}_6$ cluster at values of 10^{-3}, orders of magnitude away from the criterion (4.17) for a global minimum. The histogram Fig. 4.3(b) combines the results for all constellations $\{\lambda\}_6$ with 45 or more parameters, showing that throughout the minimal values found are well above the threshold of 10^{-7}.

As an aside, the absence of the MU constellations $\{5^2,4,1\}_6$ and $\{5^3,1\}_6$ from Table 4.4 suggests that no three complete MU bases plus one additional mutually unbiased state exist. This result generalizes the impossibility of extending two MU bases $\{5^2\}_6$ equal to the identity plus a fixed Hadamard matrix, $\{I,H\}$, to a MU constellation $\{5^3,1\}_6$. We therefore pose the

following conjecture.

Conjecture 4.3.1 *If H and K are mutually unbiased 6×6 complex Hadamard matrices then there are no vectors $|v\rangle$ MU to I, H and K.*

Our conclusions are based on a total of 433,000 searches in dimensions five to seven which would take approximately 16,000 hours on a single Pentium 4 desktop PC. The results of the searches performed in dimension six provide strong evidence that not all MU constellations of the form $\{5, \lambda, \mu, \nu\}_6$ exist. Here are our main conclusions drawn from Table 4.4:

- the *largest existing* MU constellations are $\{5, 4^2, 1\}_6$ and $\{5^2, 3, 1\}_6$ both containing 15 ($\equiv S + 1$) mutually unbiased states;
- the *smallest non-existing* MU constellations are $\{5, 3^3\}_6$ and $\{5, 4, 3, 2\}_6$ each consisting of 14 ($\equiv S$) states;
- We have been able to positively identify 18 out of 35 MU constellations in dimension six. On the basis of the numerical data, we consider it highly unlikely that the 15 unobserved MU constellations do exist, making the existence of four MU bases exceedingly improbable.

The existence of a MU constellation $\{\lambda\}_d$ in the space of constellations $C_d[\lambda]$ is determined by the zeros of a set of equations. Many of the non-existing constellations in dimension six correspond to constellations where there are more equations than free parameters. Therefore, it is natural to ask whether one would expect such *overdetermined* constellations to exist in general? We will discuss this point in more detail in Chapter 7 but now we turn our attention to attempts at proving the non-existence of a complete set of MU bases in dimension six.

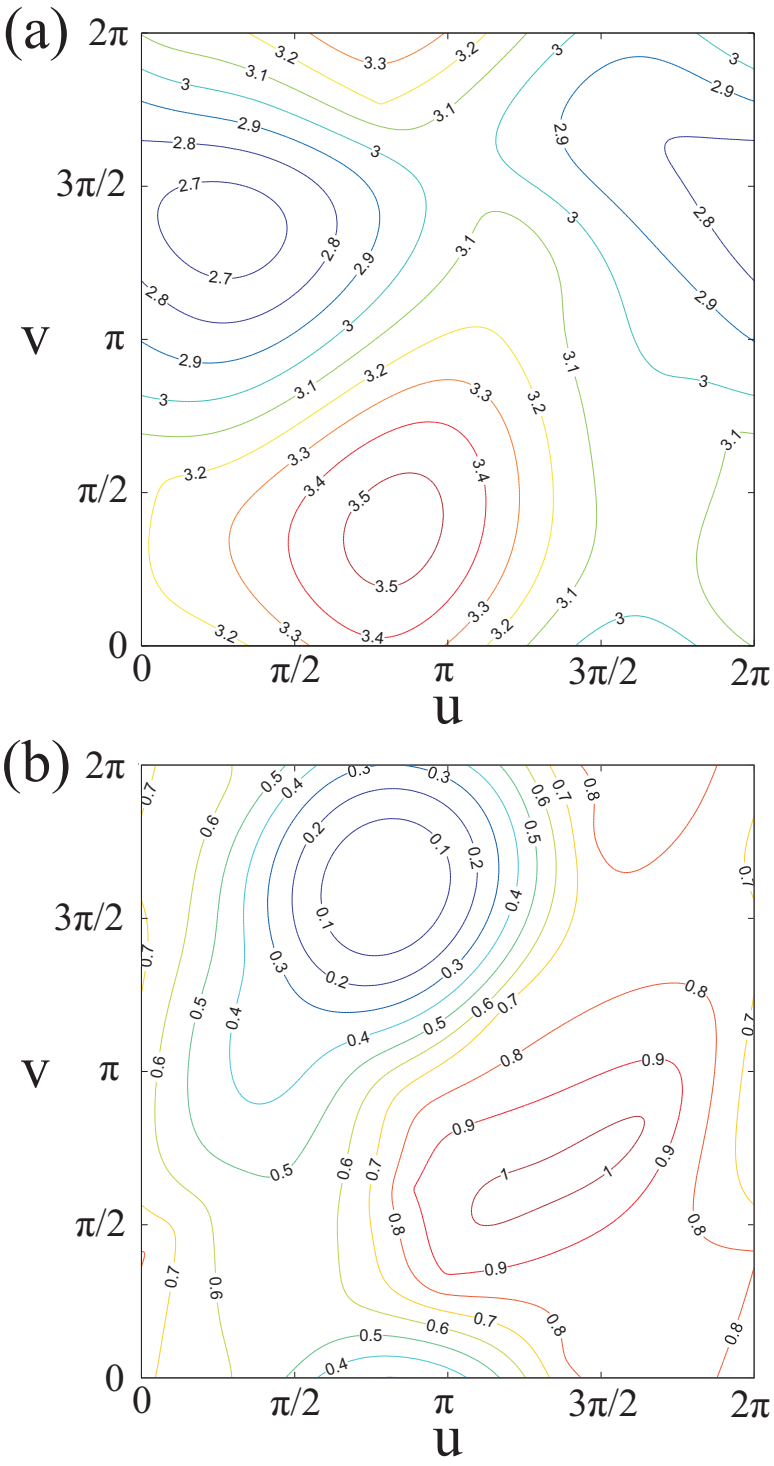

Figure 4.1: Contour plots of the function $F(\boldsymbol{\alpha})$ in the uv-plane (see text) of (a) the constellation space $\mathcal{C}_6(5, 4^2, 2)$ in dimension six, and of (b) the constellation space $\mathcal{C}_5(4^3, 2)$ in dimension five near a zero indicating a MU constellation $\{4^3, 2\}_5$.

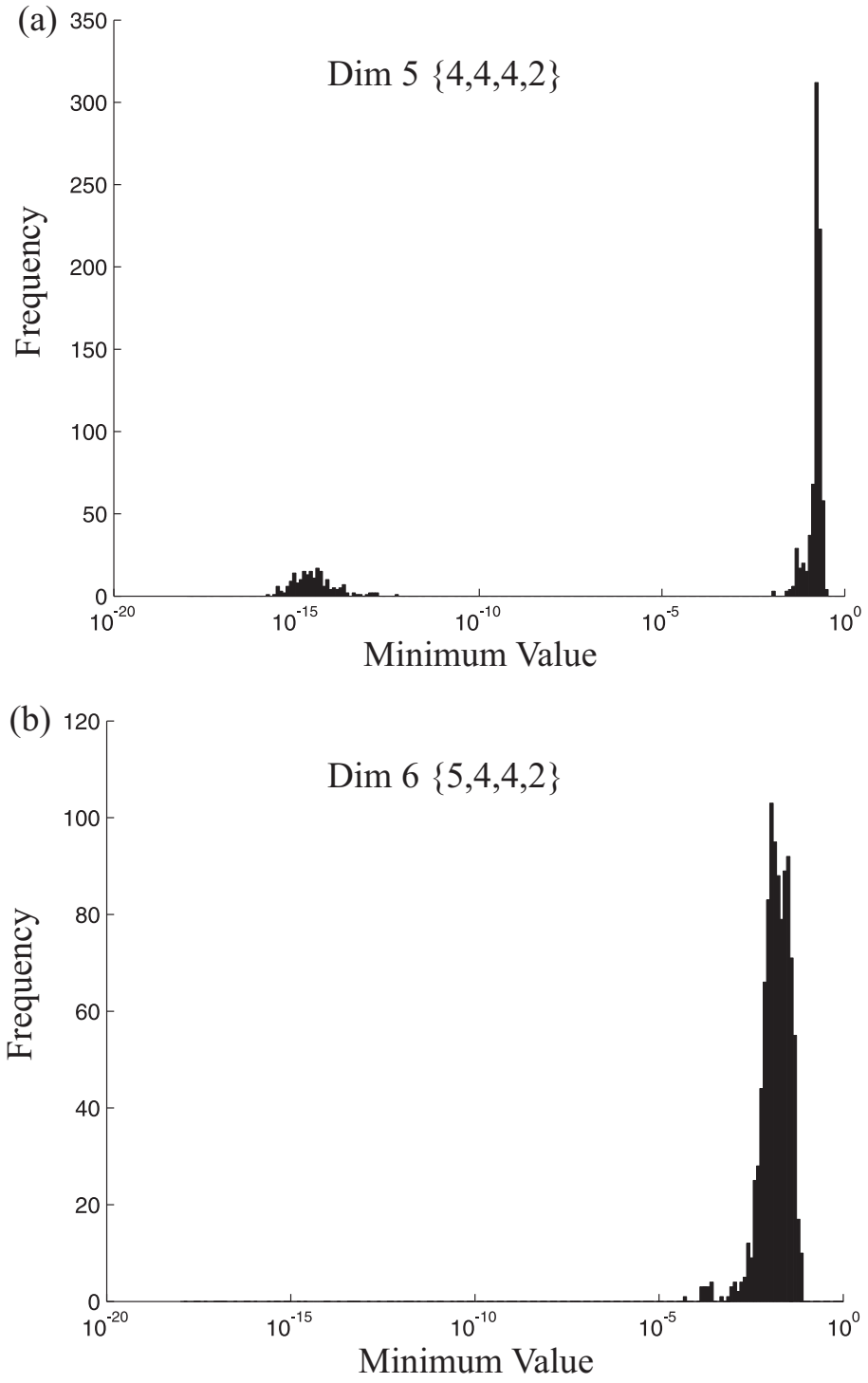

Figure 4.2: Distribution of the values obtained by minimising the function $F(\boldsymbol{\alpha})$ for 1,000 initial points chosen randomly (a) in the 36-dimensional space $\mathcal{C}_5(4^3, 2)$ and (b) in the 45-dimensional constellation space $\mathcal{C}_6(5, 4^2, 2)$.

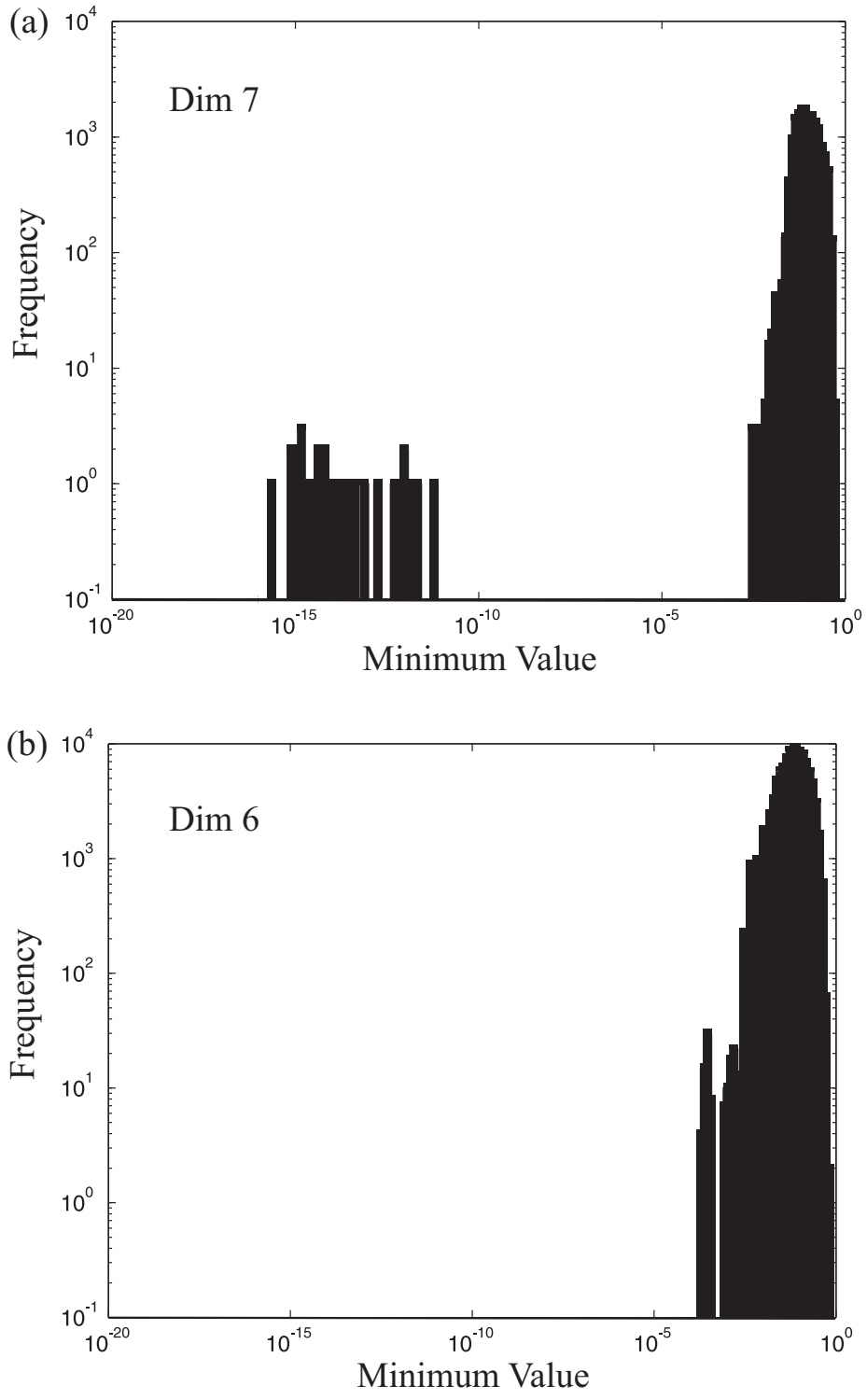

Figure 4.3: Distribution of the values obtained by minimising the function $F(\boldsymbol{\alpha})$ for (a) 16,000 points combining the results of the 16 constellations with $p_7 \geq 66$ in Table 4.3, and for (b) 110,000 points combining the results of the 11 constellations with $p_6 \geq 45$ in Table 4.4.

CHAPTER 5

Towards a no-go theorem in dimension six

In this chapter we examine potential methods of proving Conjecture 3.0.1; that there cannot be more than three MU bases in dimension six. We present three alternative approaches to this problem about the geometry of state space in $\mathbb{C}^6$. We will also consider other dimensions, using the complete classification of all MU bases in dimensions two to five as a test bed for these ideas. First we show how the construction of a Gröbner basis could be used to prove that the set of equations defining an MU constellation have no solution. We then consider global optimization techniques and apply them to suitably defined functions. Finally we examine an approach used by Jaming et al. in [84] which uses error bounds and an exhaustive search of a discrete space.

We should say from the outset that none of these approaches have been successful in practice. The three ideas outlined below are algorithms for proving the non-existence (or finding) a set of four MU bases in dimension d. However, the *computational* resources required to implement the algorithms in dimension six were beyond those available.

Throughout this chapter, we will use the notation of Chapter 4 and consider MU constellations $\{d-1, \lambda, \mu, \nu\}_d$. The non-existence of any MU constellation smaller than $\{5^4\}_6$, proves the non-existence of four (or more) MU bases in dimension six. The number of vectors, $s-1 = \lambda+\mu+\nu-1$, which are not fixed by the equivalence relations given in Appendix A, determine the number of

variables and equations needed to define a MU constellation. The value of $s-1$ determines the *size* of the original problem and therefore the difficulty of the resulting algorithms. In order to reduce the problem as much as possible, we will use the small constellations not found by the numerical searches presented in Chapter 4. For example, the MU constellation $\{5,3,3,3\}_6$ contains $s-1=8$ free vectors, whereas attacking the full set of 7 MU bases in dimension six would involve the parametrisation of $s-1=89$ vectors.

For each of the algorithms described below, we will demonstrate how they can be used to prove the non-existence of a set of four MU bases in dimension two. This fact is of course well known; but it allows us to explicitly demonstrate how each method could be used to provide a no-go theorem in dimension six.

5.1 Using Gröbner bases

The first idea we consider is to extend the method used in Chapter 3. We parametrise the vectors in a constellation $[d-1,\lambda,\mu,\nu]_d$ using real variables. For these variables to define a mutually unbiased constellation, they must satisfy a system of coupled polynomial equations, $\{p_1=0,\ldots,p_N=0\}$. A proof that there is no MU constellation $\{d-1,\lambda,\mu,\nu\}_d$ follows directly from a proof that these equations have no real solutions.

Following Chapter 4, any constellation $\{d-1,\lambda,\mu,\nu\}_d$ can be parametrised using $s(d-1)$ real phases. However, since we wish to define a system of *polynomial* equations, we must write each complex number $e^{i\theta_j}=x_j+iy_j$, adding the condition $x_j^2+y_j^2=1$. In order to parametrise all of the s vectors, $|\psi^v\rangle$, $v=1\ldots s$, in the constellation, $\{d-1,\lambda,\mu,\nu\}_d$, that are not determined by the equivalence relations, we require $2s(d-1)$ real variables.

The conditions for vectors in the constellation space $\mathcal{C}_d(d-1,\lambda,\mu,\nu)$ to be mutually unbiased represent a total of

$$N\equiv c_d+(d-1)(s-1),$$

polynomials, where

$$c_d=\frac{1}{2}s(s-2)\ +\frac{1}{2}(\lambda^2+\mu^2+\nu^2),$$

has been derived in Eq. (4.13). The polynomials

$$p_j : \mathbb{R}^{2s(d-1)} \to \mathbb{R},$$

for $j = 1 \ldots N$ determine whether there exist variables $\mathbf{x} \in \mathbb{R}^{2s(d-1)}$ which form a MU constellation $\{d-1, \lambda, \mu, \nu\}_d$. The solution set of these multivariate polynomial equations $p_j = 0$, $j = 1 \ldots N$, is the variety

$$V \equiv \{\mathbf{x} \in \mathbb{R}^{2s(d-1)} : p_1 = 0, \ldots, p_N = 0\}.$$

a subset of $\mathbb{R}^{2s(d-1)}$. Hence, proving that no MU constellation of the form $\{d-1, \lambda, \mu, \nu\}_d$ exists, is equivalent to proving that the corresponding variety is empty, $V = \emptyset$.

The geometric object, V, can be described algebraically in terms of an ideal $I = \langle p_1, \ldots, p_N \rangle$, generated by the polynomials p_1 to p_N. The ideal, I, consists of all linear combinations of the polynomials p_j with coefficients polynomial in the variables $\mathbf{x} \in \mathbb{R}^{2s(d-1)}$. That is, every element $a \in I$ has the form

$$a = \sum_{j=1}^{S} r_j(\mathbf{x}) p_j(\mathbf{x}),$$

where r_j are polynomials in $\mathbf{x}$. Note that the ideal corresponds to the variety over the algebraic closure of the coefficient field, here the complex numbers.

Having re-cast the problem as the description of an ideal, we can now apply the methods from commutative algebraic geometry. In particular, no solutions exist over the complex numbers if the polynomial 1 is contained in I. The construction of a Gröbner basis, G, would allow us to prove this fact since G will described simply by the set $G = \{1\}$. The converse is not necessarily true; this provides only a sufficient condition. It could be that the equations defining a MU constellation have no solutions over the real numbers but the ideal is non-empty. For example, the equation $x^2 + 1$ has no *real* solutions but the ideal $I = \langle x^2 + 1 \rangle$ is not generated by $\{1\}$. We may, however, be fortunate and find that the variety is also empty over the complex numbers. In which case, we would have a proof that a complete set of MU bases does not exist in dimension six.

5.1.1 Testing the Gröbner basis algorithm

Dimension two

In order to test the algorithm for proving the non-existence of a MU constellation, $\{d-1, x, y, z\}_d$, we consider the case of four MU bases in dimension two which are known not to exist. We begin by writing down a system of coupled polynomial equations, the solutions to which define the MU constellation $\{1^4\}_2$. The constellation space $\mathcal{C}_2[1^4]$ is parametrised by the four real variables $\{x_1, x_2, y_1, y_2\}$, so that the vectors are given by

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ x_1 + iy_1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ x_2 + iy_2 \end{pmatrix}.$$

The conditions which define an MU constellation in the space $\mathcal{C}_2(1^4)$ are given by the five equations

$$\begin{aligned} p_1(\mathbf{x}) &\equiv x_1^2 + y_1^2 - 1 = 0 \\ p_2(\mathbf{x}) &\equiv x_2^2 + y_2^2 - 1 = 0 \\ p_3(\mathbf{x}) &\equiv (1 + x_1)^2 + y_1^2 - 2 = 0 \\ p_4(\mathbf{x}) &\equiv (1 + x_2)^2 + y_2^2 - 2 = 0 \\ p_5(\mathbf{x}) &\equiv (1 + x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2 - 2 = 0. \end{aligned} \tag{5.1}$$

We will now prove that the variety $V = \{\mathbf{x} \in \mathbb{R}^4 : p_1(\mathbf{x}) = 0, \ldots, p_5(\mathbf{x}) = 0\}$ is empty. One might argue that this is trivial since the equations are not complicated and could be solved by hand. However, the corresponding equations defining the MU constellation $\{5^3, 1\}_6$ are certainly not simple and an algorithmic method is required. We therefore prove the non-existence of the MU constellation $\{1^4\}_2$ in an entirely general manner that can be applied to dimension six.

We have constructed the Gröbner basis for the system of equations given in Eqs. (5.1). Using the FGb package developed by Faugère et al. [64] and implemented in Maple [102], a desktop PC outputs the Gröbner basis in 0.016 seconds. The ideal generated by Eqs. (5.1) is indeed equal

to all polynomials over the complex numbers,

$$\langle p_1(\mathbf{x}), \ldots, p_5(\mathbf{x}) \rangle = \langle 1 \rangle.$$

A proof of which is obtained by writing down the polynomials calculated when constructing a Gröbner basis,

$$\begin{aligned} r_1(\mathbf{x}) &\equiv -\frac{1}{2}\left(y_1 y_2 + x_1 + 2\right) \\ r_2(\mathbf{x}) &\equiv -\frac{1}{2}\left(x_1^2 y_2 + y_1^2 y_2 - x_1 y_2 + x_2 y_1 + 2y_1\right) y_1 \\ r_3(\mathbf{x}) &\equiv \frac{1}{2} x_1 \\ r_4(\mathbf{x}) &\equiv -\frac{1}{2}\left(x_1 y_2 - x_2 y_1\right) y_1 \\ r_5(\mathbf{x}) &\equiv \frac{1}{2} y_1 y_2, \end{aligned} \tag{5.2}$$

which are the coefficients in the equation

$$\sum_{j=1}^{5} r_j(\mathbf{x}) p_j(\mathbf{x}) = 1.$$

Towards dimension six

Unfortunately, 16GB of memory was insufficient to decide if the Gröbner basis corresponding to the equations generated by the constellations $\{5, 3, 3, 3\}$, $\{5, 5, 4, 1\}$ or $\{5, 5, 5, 5\}$ contains the element 1. The computation runs out of memory before the algorithm terminates. In general, this is known to be a hard problem and the number of variables and equations even for these "small" constellations is high. For example, the constellation $\{5, 5, 4, 1\}$ requires the construction of a Gröbner basis of the ideal generated by 61 equations of degree 4 in 90 real variables.

5.2 Using semidefinite programming

A powerful tool called semidefinite programming [145] has already been applied to problems in quantum information theory. For example, a semidefinite program can be used to decide if a

given mixed state, ρ, is entangled or not [53]. The success of semidefinite programmes in quantum information and in other applied areas such as control theory and combinatorial optimization stems from the fact that semidefinite problems are *efficiently* solvable by a computer. In addition, there is a powerful duality theorem which gives a *certificate* of the result. For example, when applied to the separability problem, a semidefinite program decides if a given mixed state is entangled and if it is, provides an entanglement witness. An entanglement witness is a hyperplane separating the entangled state from the set of all separable states (see [81] for a review).

Another interesting application of semidefinite programing to problems about finite dimensional Hilbert spaces is to the compatibility problem. Here the question is to decide if there exists a single state of the entire system given the states of all proper subsystems. Hall [75] has cast the compatibility problem in the form a semidefinite program and used it to disprove a conjecture of Butterley et al. [39]. The duel problem then outputs a certificate, called an incompatibility witness, which proves that the reduced states are not compatible with any multipartite state.

A *semidefinite program* (SDP) is an algorithm for solving an optimization problem of the form

$$\begin{aligned} &\text{minimise } \mathbf{c}^T\mathbf{x} \\ &\text{subject to } F(\mathbf{x}) \geq 0 \end{aligned}$$

where, $\mathbf{c}$ is a fixed vector and the variables, $\mathbf{x}$, are constrained by the requirement that the matrix $F(\mathbf{x}) \equiv x_1F_1 + \cdots + x_nF_n - B$ be positive semidefinite [145]. It is a *convex* optimization problem since the constants $F_1, \ldots, F_n$ are required to be symmetric $n \times n$ matrices. A linear program, where the constrains have the form $F(\mathbf{x}) = \text{diag}(A\mathbf{x} - \mathbf{b})$, is an example of a SDP with many important applications such as finding optimal network flows [21] and in problems from economics [104]. A SDP can also be used to solve non-linear problems provided they are convex. For example, the problem

$$\begin{aligned} &\text{minimise } \frac{(\mathbf{c}^T\mathbf{x})^2}{\mathbf{d}^T\mathbf{x}} \\ &\text{subject to } A\mathbf{x} \geq \mathbf{b} \end{aligned}$$

can be re-written as the SDP [145]

$$\begin{array}{ll} \text{minimise } t & \\ \text{subject to} & \begin{pmatrix} \text{diag}(A\mathbf{x}-\mathbf{b}) & 0 & 0 \\ 0 & t & \mathbf{c}^T\mathbf{x} \\ 0 & \mathbf{c}^T\mathbf{x} & \mathbf{d}^T\mathbf{x} \end{pmatrix} \geq 0. \end{array}$$

The idea is to cast the existence of a complete set of MU bases in dimension six as a semidefinite program. The dual problem would then provide a certificate of non-existence. Unfortunately, the system of equations which define MU constellations are not convex; they have the form $p_j(\mathbf{x}) = 0$, where p is a fourth order polynomial. However, all is not lost; one may apply methods from non-convex optimization such as those presented in [91, 133]. By relaxing the non-convex constraints we can obtain an approximation to the original problem. Lasserre has shown that one can define a *hierachy* of semidefinite programs, each step of which is a better approximation to the true solution [95]. This is called the method of *relaxations*. At each step in the hierachy one can either be certain that a MU constellation does or does not exist or one has to go on one more step of the computation. Each step is inevitably more computationally difficult than the previous step but the remarkable work of Lasserre [95] ensures that at some point in the process the *exact* solution will be obtained. In other words, the hierachy is asymptotically complete. A similar approach has already been successfully applied to the separability problem [28, 29, 53, 54] and to other problems from quantum information [56].

The existence of an constellation satisfying the MU conditions can be expressed as an optimization problem. This is achieved by choosing one of the polynomials, say $p_1(\mathbf{x})$ and finding the minimum value of $(p_1(\mathbf{x}))^2$ subject to the constraints that the variables solve the other polynomials $p_2(\mathbf{x}), \ldots, p_N(\mathbf{x})$. In other words, we wish to minimise $(p_1(\mathbf{x}))^2$ in the feasible region defined by the remaining polynomials. Lasserre's relaxations allows us to find a lower bound on the function $(p_1(\mathbf{x}))^2$, $B_L(r)$, where r is the relaxation order. If at any point in the hierachy, $r = 2 \ldots$ we find that $B_L(r) > 0$, then no MU constellation exists in the relevant space.

SDP Algorithm

We summarise the algorithm which determines whether a MU constellation $\{d-1, \lambda, \mu.\nu\}_d$, exists in demission d as follows.

1. Define the constellation space and write down the equations which define an MU constellation.
2. Generate a SDP at the lowest possible level of relaxation ($r = 2$)
3. Solve the resulting SDP
4. If the global lower bound, $B_L(r)$, is positive then we are done otherwise repeat steps 2 and 3 at the next level of relaxation, $r := r + 1$.

Provided the constellation does not exist, the algorithm is guaranteed to find a positive lower bound. As r increases, the global lower bounds $B_L(r)$ monotonically converge to the exact global minimum of the function, B_L^{opt}. Note that if a MU constellation does exist, this algorithm will find an explicit parametrisation up to a high level of numerical accuracy.

5.2.1 Testing the SDP algorithm

Dimension two

The first successful application of the algorithm is to prove that there are no more than three MU bases in dimension two. We find a global lower bound, $B_L(r)$, on the polynomial

$$(p_1(\mathbf{x}))^2 = \left(x_1^2 + y_1^2 - 1\right)^2$$

subject to all of the other polynomials defined in Eq. (5.1) being equal to zero, $p_j(\mathbf{x}) = 0$ for $j = 2 \ldots 5$. In other words, we wish to solve the following minimization problem

$$\begin{aligned} \min \quad & \left(x_1^2 + y_1^2 - 1\right)^2 \\ \text{subject to} \quad & p_2(\mathbf{x}) = 0 \\ & p_3(\mathbf{x}) = 0 \\ & p_4(\mathbf{x}) = 0 \\ & p_5(\mathbf{x}) = 0. \end{aligned} \tag{5.3}$$

A MU constellation $\{1^4\}_2$ exists if and only if all global lower bounds are *not* strictly positive, $B_L(r) \leq 0$ for all r.

r	B_L	N_d	F
2	1.4038×10^{-8}	69	15×15
3	0.5359	209	35×35
4	0.5359	494	70×70

Table 5.1: Table of the lower bounds of the minimization problem defined in Eq. 5.3. The level of relaxation is denoted by r. The labels N_d and F denote the number of decision variables and the size of the semidefinite inequalities in the resulting SDP respectively.

Using the Matlab package `gloptipoly3` [78] which is based on the theory presented in [96], we have converted the problem (5.3) into a semidefinite program. The resulting SDP can then be solved using the `SeDuMi` MatLab package developed by Strum et al. [138]. The results of the computations at three levels of relaxation, $r = 2, 3, 4$, are presented in Table 5.1. We find that even at the lowest level of relaxation $r = 2$, the polynomial $(p_1(\mathbf{x}))^2$ has a positive lower bound, $B_L(2) > 0$, and hence four MU bases do not exist in dimension two. At $r = 3$, the lower bound $B_L(3)$ is clearly distinct from zero and in fact is already guaranteed to equal the exact minimum value of $(p_1(\mathbf{x}))^2$.

The high level of numerical accuracy used by the optimization program `SeDuMi` allows us to find an analytical expression for the lower bound, $B_L^{opt} = (1 - \sqrt{3})^2$. The third and fourth columns of Table 5.1 show how the size of the SDP grows as we increase the level of relaxation.

The number of decision variables, N_d, grows from 69 to 494 as the level of relaxation increases. Similarly, the size of the semidefinite constraint $F(\mathbf{x}) \geq 0$ is almost five times larger at $r = 4$ than at the lowest level of relaxation, $r = 2$. The algorithm proves to be very efficient taking only 0.11 seconds on a desktop PC to convert the original problem and solve the SDP for $r = 2$. The time rises to 1.67 seconds when $r = 4$.

At the third and fourth levels of relaxation, the lower bound is optimal in that the function $(p_1(\mathbf{x}))^2$ reaches the value B_L. It is possible to output the parameter values, $\mathbf{x}$, which achieves this lower bound in the feasible region. There are two sets of vectors corresponding to the global minimum value $B_L^{opt} = B_L(3) = B_L(4) = (1 - \sqrt{3})^2$ given by

$$V_{\pm} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \alpha(1 \mp i) \end{pmatrix} \right\},$$

where $\alpha = (\sqrt{3} - 1)/2$. Interestingly, the two sets V_+ and V_- correspond to a set of three MU bases plus one additional vector.

Towards dimension six

In Chapter 4, we proved that the Spectral matrix, S, cannot be part of a triple of MU bases (see Appendix C.1 for a definition of S). An analysis of the vectors MU to both I and S reveals that, in fact a stronger statement is true: there is no pair of orthogonal vectors $\{|v\rangle, |u\rangle\}$ MU to the bases I and S. This reduction in the number of vectors makes it a good candidate to test our SDP algorithm. The original problem has 20 real variables which must satisfy 21 constraints given by 4^{th} order polynomials. At the lowest level of relaxation, $r = 2$, the equivalent SDP has $10,625$ decision variables which must satisfy $4,851$ linear constraints and semidefinite inequalities of size 231×231. It took approximately three and a half hours and used 5.4G of memory to solve the SDP. A global lower bound for the square of one of the polynomials defined by the MU conditions is given by

$$B_L(2) = 2.28 \times 10^{-8}.$$

Since $B_L(2) > 0$ the algorithm confirms the result of Chapter 4; no two orthonormal vectors can be mutually unbiased to the pair $\{I, S\}$. At the next level of relaxation, $r = 3$, the resulting SDP is too large to solve; it has $230,229$ variables and 1771×1771 semidefinite constraints so it was not possible to improve this lower bound.

Unfortunately, we have been unable to construct the SDP for the constellation $\{5^3, 1\}_6$ even at the lowest level of relaxation. Judging by the increase in the number of decision variables and the size of the semidefinite constraints seen in the previous examples, it is likely to be very large. Solving the resulting SDP would seem optimistic. However, it maybe that some clever programing could be applied, for example, making further use of techniques such as sparse matrices.

5.3 An exhaustive search with error bounds

Jaming et al. have shown that the Fourier family cannot be a member of a quadruple of MU bases [84]. The restriction to consider sets of the form $\{I, F(x_1, x_2), \mathcal{B}^2, \mathcal{B}^3\}$, for any bases $\mathcal{B}^2$ and $\mathcal{B}^3$, is in order to reduce the computational complexity rather than any inherent restriction on their method. Following an argument similar to [84], we now explain how their idea could be used to obtain a general no-go theorem in dimension six.

We assume that there exists a MU constellation $C \equiv \{d-1, \lambda, \mu, \nu\}_d$ in the constellation space $\mathcal{C}_d[d-1, \lambda, \mu, \nu]$ and attempt to find a contradiction. As explained in Chapter 4, any constellation can be parametrised by p_d phases (cf. Eq. (4.8)) so there exist phases $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{p_d})^T$ which parametrise C. The first step is to *approximate* this MU constellation by the closest constellation in $\mathcal{C}_d$ whose elements are N^{th} roots of unity only. The approximation is achieved by partitioning the interval $[0, 2\pi)$ into N subintervals modulo 2π; $I_j = [(2j-1)/2N, (2j+1)/2N)$ for $j = 0, \ldots, N$. If the phase α_k lies in the interval I_j, we approximate it by the mid-point of I_j, $\alpha_k \to \widetilde{\alpha}_k \equiv 2\pi j/N$. The mapping $\boldsymbol{\alpha} \to \widetilde{\boldsymbol{\alpha}}$, thus sends the MU constellation C to a new constellation, $\widetilde{C}$, whose vectors do not necessarily satisfy the MU conditions (4.1).

The approximation of the MU constellation C by $\widetilde{C}$, can be controlled by increasing the value of N. The key step forward made by Jaming et al. [84] is to find bounds on this accuracy. In order

to obtain a contradiction, one can exhaustively search the discrete space of constellations whose elements are given by N^{th} roots of unity only. For a given N, if we find that no constellations $\widetilde{C}$, satisfy the error bounds then it follows that there are no MU constellations, C, in the space $\mathcal{C}_d$. If N is small, the search is easy to perform as not many points need to be checked. However, for small values of N, the error bounds are loose and so it is likely that no violation will be found.

Jaming et al. have used this method to exclude the entire Fourier family from a complete set of MU bases. This was achieved by discretising the fundamental region of the Fourier family using $N = 180$ and two other complete bases using $N' = 19$. Interestingly, the non-existence of a finite projective plane was shown by an exhaustive search [94]. Since the existence of a complete set of MU bases shares some properties with the existence of finite projective planes [125] this appears a promising avenue.

CHAPTER 6

Quantum key distribution highly sensitive to eavesdropping

When attempting to implement a QKD protocol a key factor in determining its *practical* success is the error rate introduced by Eve: if it is small, her presence may be masked by the system noise. This error rate thus determines the level of technology required to implement the protocol and the distance over which Alice and Bob can establish a secure key. We will present a protocol that extends the one proposed by Khan et al. [87]. The new approach ensures that eavesdropping causes a large error rate and therefore, from an experimental point of view, offers a modification that could improve the implementation of existing QKD technology.

The new protocol allows Alice and Bob a great deal of freedom: the elements of the key that they form can be taken from an alphabet of arbitrary size, and encoded using any bases of $\mathbb{C}^d$. It is equivalent to the protocol presented in [87] when Alice and Bob use a two-letter alphabet and corresponds to the SARG protocol [126] when in addition, they use two-dimensional quantum systems.

In order to better understand the freedom in the choice of bases used by all three parties, Alice, Bob and Eve, we will introduce a measure of distance between two bases and show how this relates to the error rate. It gives a simple interpretation of the optimal setup for all parties: Alice and Bob should use a set of c bases, $\mathcal{S}$, that are as far apart as possible; whilst Eve should

choose her basis, $\mathcal{E}$, so it minimises the average distance between $\mathcal{E}$ and the elements of $\mathcal{S}$. The conclusion then is that for the legitimate parties, the optimal settings correspond to *mutually unbiased bases*. MU bases have been used before in other QKD protocols [17, 25, 44]; making use of the fact that a measurement in one of the bases reveals no information about the state in all other bases.

The chapter is organised as follows. In Section 6.1, we will introduce a key distribution protocol that encodes a c-letter alphabet using quantum systems of dimension d. In Sec 6.2, we will examine the effect of an eavesdropper by calculating two error rates that allow the legitimate parties to detect Eve's intercept-and-resend attack. Section 6.3 will show how one of these error rates can be understood as a measure of the distance between the bases used by all three parties. We will consider some examples of specific sets of bases in Section 6.4. In Section 6.5, we compare this new protocol to the six-state protocol in an experimental setting and consider a general method of implementing the protocol for any choice of c and d. Finally, we summarise the results and compare the new protocol to existing quantum key distribution methods in Section 6.6.

6.1 General form of the protocol

In quantum cryptography, there are two legitimate parties who wish to establish a shared sequence of letters from an alphabet such as a string of zeros and ones. Typically, these two parties have different roles: Alice prepares and sends quantum states, and Bob performs measurements on the states he receives and records the outcomes. At the end of this quantum part of the protocol, the two parties then exchange information via a classical communication channel. A third party, Eve, attempts to gain information about some or all of the shared key without being detected. Eve can perform any operation allowed by quantum mechanics and can listen in on the classical part of the communication without being detected. We also assume that she has access to a high level of technology so that she can hide behind any system noise by replacing parts of the implementation by better components. The aim is to find protocols and implementations such that Eve is easily detected.

We begin by presenting a new protocol that enables Alice and Bob to share a key and then discuss the effect Eve has on the states received by Bob. We will assume that Eve uses an intercept-and-resend attack and calculate error rates that allow the legitimate parties to detect her presence. There are other more sophisticated forms of attack available to Eve but we will not analyse them here; we simply remark that this form of attack provides a useful guide to the security of the protocol against more general attacks.

We first present the *highly-sensitive-to-eavesdropping (HSE)* protocol in its general form; encoding an alphabet, $\mathcal{A}$, containing $c \equiv |\mathcal{A}|$ elements using d dimensional quantum systems. In Section 6.1.1, we give an explicit example of the protocol when used to encode a 4-letter alphabet, say $\{0, 1, 2, 3\}$, using 3-dimensional quantum systems. A further example is provided in Section 6.5.1 where we discus the case of $c = 3$ and $d = 2$ in an experimental setting.

The HSE-Protocol Alice and Bob agree publicly on a method of encoding the c elements of $\mathcal{A}$ using states in $\mathbb{C}^d$ by choosing bases $\mathcal{B}^x = \{|\psi_i^x\rangle \in \mathbb{C}^d : i = 1 \dots d\}$ for all $x \in \mathcal{A}$. They are free to choose any bases provided they are different (in the sense that no two bases have any state in common). We will discuss the optimum choice in Section 6.3. Alice generates a random string, S, of letters from $\mathcal{A}$ that form the raw data she will attempt to share with Bob. For each element, $x \in S$, Alice and Bob perform the following procedure.

- Alice generates $c - 1$ random numbers, $\mathbf{a} \equiv (a_1, \dots a_{c-1})$, between 1 and d. The numbers $\mathbf{a}$ serve as indices for states chosen from basis $\mathcal{B}^x$ as she now prepares and sends the $c - 1$ states $|\psi_{a_k}^x\rangle \in \mathcal{B}^x$, $k = 1 \dots c - 1$, to Bob.

- Bob chooses *one* of the letters of $\mathcal{A}$ and uses the remaining $c - 1$ letters, $x_1, \dots, x_{c-1}$. When he receives the k^{th} state, $|\psi_{a_k}^x\rangle$, he measures it in the bases $\mathcal{B}^{x_k}$ and records the measurement outcomes, $\mathbf{b} \equiv (b_1, \dots b_{c-1})$.

- After Bob's measurements, Alice publicly announces the indices $\mathbf{a}$ keeping her choice of basis a secret. Using this information, Bob is (sometimes) able to deduce which basis Alice used and therefore to determine the element of S.

- Bob tells Alice for which elements he was able to determine x. Unsuccessful attempts are discarded, leaving only the shared key.

An element $x \in S$ is successfully shared between Alice and Bob when for every state $|\psi^x_{a_k}\rangle \in \mathcal{B}^x$, $k = 1 \ldots c-1$, the index measured by Bob does *not* equal the index announced by Alice, $a_k \neq b_k$ for all k. If this happens Bob knows that *none* of his measurements were in basis $\mathcal{B}^x$ and so his missing basis corresponds to the correct letter of the string, x. If Bob's measurement does equal the announced index for any k, he does not know if this was because he measured in the same basis as Alice or because of the non-zero overlap between vectors from different bases. This element of the string then fails.

The protocol presented in [87] is then a special case of this protocol applied to a two-letter alphabet $\{0, 1\}$ so that Alice needs only to send one state for each letter of S. Khan et al.'s protocol is interesting because it has a high error rate that approaches 50% for higher dimensional quantum systems if Alice and Bob use two mutually unbiased bases. Starting with the probability that the transmission of the element x is successful, we will analyse the performance of the general protocol in the following sections. We find that this general protocol has an error rate that approaches 100% when Alice and Bob use high-dimensional systems and a complete set of $(d+1)$ mutually unbiased bases. In Section 6.3 we will use a natural measure of distance between bases to argue that the optimal settings for Alice and Bob are indeed mutually unbiased bases.

6.1.1 A four-letter alphabet encoded using qutrits

We now make the protocol explicit when applied to a four-letter alphabet, say $\mathcal{A} = \{0, 1, 2, 3\}$, encoded using three-dimensional quantum systems. Note that we can think of $0, 1, 2, 3$ as representing 00, 01, 10, 11 and therefore the key that Alice and Bob share as pairs of bits, for example, the string $S = 213101$ becomes 100111010001; this makes it easier to compare the bit efficiency of different protocols. We examine the case where Alice and Bob encode $\mathcal{A}$ using the

bases defined in Eq. (1.3),

$$\mathcal{B}^0 \simeq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \mathcal{B}^1 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$
$$\mathcal{B}^2 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix}, \mathcal{B}^3 \simeq \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}, \tag{6.1}$$

where the columns of the matrix $\mathcal{B}^x$ correspond to the vectors $|\psi_i^x\rangle, i = 1, 2, 3$ of each basis.

In order to send the first element of the string, say $x = 2$, Alice generates three random numbers $a_1, a_2, a_3 \in \{1, 2, 3\}$ and sends the states $|\psi_{a_1}^2\rangle$, $|\psi_{a_2}^2\rangle$ and $|\psi_{a_3}^2\rangle$. Bob now measures in three different, randomly chosen bases resulting in the measurement outcomes b_1, b_2 and b_3. The element x is successfully transmitted if and only if $a_1 \neq b_1$, $a_2 \neq b_2$ and $a_3 \neq b_3$ since if this happens, Bob can be certain that he did not use the same basis as Alice. Bob must have performed measurements in the bases $\mathcal{B}^0$, $\mathcal{B}^1$ and $\mathcal{B}^3$ so that his missing basis corresponds to the correct element $x = 2$. The probability that an element is shared for each run of the protocol is given by

$$\mathcal{R}_s \equiv \frac{1}{4}\left(1 - \frac{1}{3}\right)^3 = \frac{2}{27},$$

since there is a 1/4 chance that Bob does *not* use $\mathcal{B}^2$ and a 2/3 chance that he does *not* measure index a_k when using basis $\mathcal{B}^x$, $x \neq 2$, for $k = 1 \ldots 3$.

Each element of the string represents two bits and so, on average, in order to share one bit of information Alice and Bob need to perform this procedure $27/4 \approx 7$ times so that Alice has to send a total of $3 \times 27/4 \approx 20.3$ states. This is relatively high, for example in the BB84 protocol, Alice needs to send an average of only two states in order to successfully transmit one bit of information. However, as we will see in Sec 6.2, the presence of an eavesdropper causes a much higher error rate. The present protocol therefore remains secure even if there is a very high level of system noise.

6.1.2 Probability of success

Having calculated the success rate for the protocol in the case of a four-letter alphabet encoded using a specific choice of bases of $\mathbb{C}^3$, we now consider the general probability of success. The protocol results in a letter, x, forming part of the shared key whenever the indices measured by Bob are all different from those announced by Alice, that is whenever $a_k \neq b_k$ for $k = 1, \ldots, c-1$. For each state, indexed by k, Bob makes a measurement in basis B^{x_k} so that the probability of measuring index a_k is given by

$$q_k \equiv \text{prob}(a_k = b_k) = \left|\langle \psi_{a_k}^{x_k} | \psi_{a_k}^{x} \rangle\right|^2 .$$

Hence the success rate of the protocol is

$$\mathcal{R}_s \equiv \frac{1}{c} \prod_{k=1}^{c-1} (1 - q_k), \tag{6.2}$$

the chance that none of the $c-1$ bases chosen by Bob equal the one selected by Alice, $\mathcal{B}^x$, multiplied by the probability of never measuring the same index even though all of Bob's measurements are different to $\mathcal{B}^x$. In order to get a success rate *per bit* of information shared between Alice and Bob, called the *bit transmission rate,*

$$\mathcal{R}_t \equiv \log_2(c) \mathcal{R}_s, \tag{6.3}$$

we multiply $\mathcal{R}_s$ by $\log_2(c)$.

This general formula depends on the choice of bases used to encode the alphabet, and in particular the modulus of the overlap between states from different bases. We will consider different bases used in the protocol in Section 6.4 and compare the bit transmission rate, $\mathcal{R}_t$, with existing QKD protocols in the conclusion.

6.2 Error rate introduced by an eavesdropper

We have seen how the protocol allows Alice and Bob to create a shared key, we now consider the effect of an eavesdropper. In particular, we analyse the effect of an intercept-and-resend attack. That is, for each state sent by Alice, an eavesdropper performs a measurement on the system and then prepares and sends a new state to Bob. In effect, we can imagine the attack as being performed in two stages. Eve measures the state of the system and then discards it completely. Using the classical information corresponding to her measurement outcome, she then prepares a new system in a state that is as "close as possible" to the original.

In general, Eve is free to use different measurements for each state sent by Alice. She can also send Bob a system in any state regardless of the measurement outcome. However, since the states $|\psi^x_{a_k}\rangle$ have indices, a_k, that are uniformly distributed, each subsequent measurement made by Eve is independent from the previous measurement outcomes. Therefore, there is no loss of generality in assuming that Eve always uses the same measurement basis, $\mathcal{E} = \{|e_i\rangle \in \mathbb{C}^d, i = 1 \dots d\}$, corresponding to her optimal one. In addition, we assume that Eve sends the state corresponding to her measurement outcome since it is likely to be the state closest to $|\psi^x_{a_k}\rangle$.

Alice and Bob can detect Eve's attack in one of two different ways; by detecting a change in the index of the state received by Bob, called the *index transmission error rate* (ITER); and by errors in the final shared key, called the *quantum bit error rate* (QBER). We begin by considering the ITER, which can be detected whenever Alice and Bob use the *same* bases, $\mathcal{B}^x$, and has been used in other QKD protocols to detect an eavesdropper [87, 14, 13].

6.2.1 The index transmission error rate

Suppose Alice sends the state $|\psi^x_i\rangle$, Bob can detect Eve if he happens to perform a measurement in basis $\mathcal{B}^x$ and his measurement outcome, j, does not equal i. This occurs with probability $p_i(x, x)$, where we define

$$p_i(x, y) \equiv \sum_{k=1}^{d} \sum_{\substack{j=1 \\ j \neq i}}^{d} |\langle \psi^x_i | e_k \rangle|^2 |\langle e_k | \psi^y_j \rangle|^2, \tag{6.4}$$

to be the probability that the index i changes when Alice prepares a state in basis $\mathcal{B}^x$ and Bob measures the system he receives in basis $\mathcal{B}^y$. Since for any y and k, Bob measures one of the possible outcomes with certainty,

$$\sum_{j=1}^{d} |\langle e_k|\psi_j^y\rangle|^2 = 1, \tag{6.5}$$

Eq. (6.4) can be written as

$$p_i(x,y) = 1 - \sum_{k=1}^{d} |\langle \psi_i^x|e_k\rangle|^2 |\langle e_k|\psi_i^y\rangle|^2,$$

one minus the probability that Bob measures a state with index i.

The rate at which Alice and Bob can detect an index transmission error, $\mathcal{R}_{IT}$, is calculated by averaging $p_i(x,x)$ over all indices, i, and letters of the alphabet, $x \in \mathcal{A}$. That is,

$$\begin{aligned} \mathcal{R}_{IT} &\equiv \frac{1}{cd}\sum_{x=0}^{c-1}\sum_{i=1}^{d} p_i(x,x) \\ &= 1 - \frac{1}{cd}\sum_{x=0}^{c-1}\sum_{i=1}^{d}\sum_{k=1}^{d} |\langle \psi_i^x|e_k\rangle|^4. \end{aligned} \tag{6.6}$$

As with the probability of success, $\mathcal{R}_{IT}$ depends on the choice of bases. We will see how this measure of the sensitivity of the protocol to eavesdropping can be understood as a measure of distance between the bases used by all three parties in Section 6.3. Then in Section 6.4 we will consider some interesting examples of specific bases.

6.2.2 The quantum bit error rate

In addition to the index transmission error rate, Alice and Bob can detect an eavesdropper by calculating the error rate of the final shared key. Eve's intercept-and-resend attack may cause a change in the index in such a way that Bob adds an incorrect letter to his key. Just as in the original BB84 protocol, the legitimate parties can detect quantum bit errors by selecting a random subset of the key and openly comparing its elements.

To see how an error in the key is created, suppose Alice attempts to share the letter $x \in \mathcal{A}$. If none of the indices measured by Bob equal the indices announced by Alice, $a_k \neq b_k$ for all

$k = 1 \ldots c-1$, Alice adds x to her key and Bob adds $\widetilde{x}$. The letters, x and $\widetilde{x}$, correctly coincide provided one of Bob's measurements was not in the basis $\mathcal{B}^x$ since he adds the letter corresponding to his missing basis. If however, Bob did use $\mathcal{B}^x$, he adds the letter $\widetilde{x} \neq x$ to his key and there is an error in the shared key. Therefore, the proportion of key elements that contain an error, is given by the *quantum bit error rate*

$$\mathcal{R}_{QB} \equiv \frac{c-1}{c} \frac{\mathcal{R}_{BE}}{\mathcal{R}_K}, \tag{6.7}$$

where: the factor $\frac{c-1}{c}$ is the probability that Bob uses the same basis as Alice in one of his $c-1$ measurements; $\mathcal{R}_{BE}$ is the rate at which Bob adds incorrect letters to his key given that he used the same basis as Alice, called *Bob's error rate*; and $\mathcal{R}_K$ is the average probability that a bit is added to the key regardless of Bob's choice of basis, called the *key rate*.

We now calculate the terms in Eq. (6.7) starting with $\mathcal{R}_K$. Given any vector of indices, $\mathbf{a} = (a_1, \ldots, a_{c-1})$, chosen by Alice and bases with indices $\mathbf{y} = (y_1, \ldots, y_{c-1})$ chosen by Bob, the probability that $a_k \neq b_k$ for all $k = 1 \ldots c-1$ is given by

$$\prod_{k=1}^{c-1} p_{a_k}(x, y_k). \tag{6.8}$$

where $p_i(x, y)$ has been defined in Eq. (6.4). Alice uses vectors from the set $I \equiv \{(a_1, \ldots, a_{c-1}) : a_k \in \mathbb{Z}_d\}$ since she is free to repeat an index. Bob, however is more restricted, he must use each basis only once and therefore, choose a vector

$$\mathbf{y} \in Y \equiv \{(y_1, \ldots, y_{c-1}) : y_k \in \mathcal{A} \text{ and } y_k \neq y_l \text{ for all } k, l\}.$$

Hence, $\mathcal{R}_K$ is the average over all bases $\mathcal{B}^x$ and elements of the sets I and Y,

$$\mathcal{R}_K = \frac{1}{c|Y||I|} \sum_{x=0}^{c-1} \sum_{\mathbf{y} \in Y} \sum_{\mathbf{a} \in I} \prod_{k=1}^{c-1} p_{a_k}(x, y_k), \tag{6.9}$$

where $|Y| = c!$ and $|I| = d^{c-1}$.

The numerator in Eq. (6.7), $\mathcal{R}_{BE}$, is the average probability that Bob adds an incorrect

letter to his key. Such a bit error occurs when Bob uses the same basis as Alice *and* measures indices that are all different to those announced by Alice. To help calculate Bob's error rate, we define the set Z to be

$$Z \equiv \{(x, z_2, \ldots, z_{c-1}) : z_k \in \mathcal{A},\ z_k \neq x \text{ and } z_k \neq z_l \text{ for all } k, l\},$$

that is, the first component of every $\mathbf{z} \in Z$ corresponds to the letter x used by Alice to encode the states. Therefore, Bob's error rate is given by

$$\mathcal{R}_{BE} = \frac{1}{c|Z||I|} \sum_{x=0}^{c-1} \sum_{\mathbf{z}\in Z} \sum_{\mathbf{a}\in I} \prod_{k=1}^{c-1} p_{a_k}(x, z_k), \tag{6.10}$$

where we average over all outcomes that correspond to Bob adding an incorrect letter to his key and the set Z contains $|Z| = (c-1)!$ elements.

The rather complicated formula for $\mathcal{R}_{QB}$ given by Eqns. (6.7), (6.9) and (6.10) has a simple form when Alice and Bob use only two bases in the protocol. The simplification is due to the fact that when $c = 2$, Bob's error rate $\mathcal{R}_{BE} = \mathcal{R}_{IT}$ and hence

$$\mathcal{R}_{QB} = \frac{\mathcal{R}_{IT}}{2\mathcal{R}_K} \quad \text{for } c = 2,$$

corresponding to the QBER obtained in [87]. We will also see that the general form of $\mathcal{R}_{QB}$ simplifies when applied to a specific choice of bases in Section 6.4. Before doing so, we show how the error rate $\mathcal{R}_{IT}$ relates to a natural measure of distance between the bases of $\mathbb{C}^d$ used by the three parties.

6.3 Distance between bases

In this section we consider the bases used in the QKD protocol as points in a higher-dimensional space. This setting allows us to understand the optimal strategy for the legitimate parties in terms of a natural measure of distance between two bases. We follow an approach similar to that presented in [16]; here, however, we will consider an alternative choice of origin so that the

resulting space is an *affine* space rather than a vector space.

We begin by associating to every normalised vector, $|\psi\rangle \in \mathbb{C}^d$, the operator

$$|\psi\rangle \to \boldsymbol{\psi} = |\psi\rangle\langle\psi|$$

that lives in a d^2-1 dimensional space consisting of Hermitian operators of trace one. Equipped with the inner product

$$\boldsymbol{\psi} \cdot \boldsymbol{\phi} = \mathrm{Tr}\boldsymbol{\psi}\boldsymbol{\phi},$$

this is an affine space in which a basis $\mathcal{B} = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$ of $\mathbb{C}^d$ is identified with a set of operators $\{\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots, \boldsymbol{\psi}_d\}$ spanning a $d-1$ dimensional plane. To define a distance between two such planes, we perform a similar procedure and embed them in an even larger space so that to each basis $\mathcal{B}$ we associate the matrix

$$\Psi = \frac{1}{\sqrt{d}}[\boldsymbol{\psi}_1\boldsymbol{\psi}_2\ldots\boldsymbol{\psi}_d]\begin{bmatrix} \boldsymbol{\psi}_1^T \\ \boldsymbol{\psi}_2^T \\ \vdots \\ \boldsymbol{\psi}_d^T \end{bmatrix},$$

that projects onto the plane spanned by the basis vectors $\{\boldsymbol{\psi}_1, \boldsymbol{\psi}_2, \ldots \boldsymbol{\psi}_d\}$. Acting on an arbitrary pure state, $\boldsymbol{\phi}$, the operator Ψ describes the action of performing a measurement in basis $\mathcal{B}$ since the non-zero elements of $\Psi\boldsymbol{\phi}$ are $|\langle\psi_i|\phi\rangle|^2 \boldsymbol{\psi}_i$ for $i = 1 \ldots d$.

The matrices Ψ are elements of a $(d^2-1)^2$ dimensional space (called an affine Grassmannian), in which a natural measure of distance between two points, Φ and Ψ, is the chordal Grassmannian distance

$$D^2(\Phi, \Psi) = 1 - \mathrm{Tr}\Phi\Psi. \tag{6.11}$$

Applying this distance measure to two points, Φ and Ψ, associated with two bases reads

$$\begin{aligned} D^2(\Phi,\Psi) &= 1-\frac{1}{d}\mathrm{Tr}\left\{[\boldsymbol{\psi}_1\boldsymbol{\psi}_2\ldots\boldsymbol{\psi}_d]\begin{bmatrix}\boldsymbol{\psi}_1^T\\ \boldsymbol{\psi}_2^T\\ \vdots\\ \boldsymbol{\psi}_d^T\end{bmatrix}[\boldsymbol{\varphi}_1\boldsymbol{\varphi}_2\ldots\boldsymbol{\varphi}_d]\begin{bmatrix}\boldsymbol{\varphi}_1^T\\ \boldsymbol{\varphi}_2^T\\ \vdots\\ \boldsymbol{\varphi}_d^T\end{bmatrix}\right\} \\ &= 1-\frac{1}{d}\sum_{i=1}^{d}\sum_{j=1}^{d}(\boldsymbol{\psi}_i\cdot\boldsymbol{\varphi}_j)^2 \\ &= 1-\frac{1}{d}\sum_{i=1}^{d}\sum_{j=1}^{d}\left|\langle\psi_i|\varphi_j\rangle\right|^4. \end{aligned}$$

Hence the average distance, $D_{average}$, between Eve's basis E and the bases chosen by Alice and Bob, B^x, $x=0\ldots c-1$, is given by

$$\begin{aligned} D_{average} &= \frac{1}{c}\sum_{x=0}^{c-1}D^2(B^x,E) \\ &= 1-\frac{1}{cd}\sum_{x=0}^{c-1}\sum_{i=1}^{d}\sum_{k=1}^{d}|\langle e_k|\psi_j^x\rangle|^4 \\ &= \mathcal{R}_{IT}, \end{aligned} \tag{6.12}$$

the index transmission error rate caused by Eve's intercept-and-resend attack.

This distance measure provides an intuitive feel as to how the three parties in the protocol should behave: Alice and Bob aim to maximize the error rate $\mathcal{R}_{IT}$ by separating their bases as much as possible; whilst Eve chooses a basis that minimises the average distance between all of the bases chosen by Alice and Bob. We will begin the next section by making these statements more precise and find that they lead to the conclusion that Alice and Bob should use a complete set of mutually unbiased bases.

6.4 Optimal choice of bases

In this section we consider specific choices of bases used by Alice and Bob in the HSE-protocol. The protocol is entirely general and any set of bases can be used to encode the alphabet. There

are likely to be many considerations in choosing a suitable set such as the ease of preparing and measuring states in each of the prescribed bases. In this section we will not worry about experimental difficulties but simply consider the optimal choice from a theoretical perspective. Motivated by the distance measure in Section 6.3 we begin by considering a set of mutually unbiased (MU) bases.

6.4.1 Mutually unbiased bases

The distance measure introduced in Eq. (6.11) has the following property. The distance between any two bases Φ and Ψ, is bounded by

$$0 \leq D^2(\Phi, \Psi) \leq 1 - \frac{1}{d},$$

where the lower bound is obtained when Φ and Ψ span the same subspace and the upper bound is realised when they are mutually unbiased. Since Alice and Bob wish to maximize the average distance between their bases, a natural strategy is to use as many MU bases as possible. They cannot use more than a complete set of $d+1$, since it is impossible to fit any more $d-1$ dimensional planes with the correct overlap into a space of dimension $d^2 + 1$ [16].

We now turn our attention to the optimal strategy of an eavesdropper. As before, we assume that she uses an intercept-and-resend attack and following the arguments of Section 6.2, only uses one basis corresponding to her optimal choice. Eve's optimal strategy is essentially a minimisation problem subject to some constraints. The functions she wishes to minimise are the error rates $\mathcal{R}_{QB}$ and $\mathcal{R}_{IT}$, and the constraints come from the fact that Eve must use a set of d orthonormal vectors. By approaching this problem numerically, Khan et. al. provide evidence that for $c = 2$, the index transmission error rate has a global minimum when Eve's basis spans the same subspace as one of the bases chosen by Alice and Bob [87]. In other words, Eve's optimal strategy is to simply pick one of the bases used by the legitimate parties.

Eve has many alternative eavesdropping strategies at her disposal. For example, for the case when $d = c = 2$, Eve could use the so-called Breidbart basis that is halfway between the two bases used by the legitimate parties [40]. In the BB84 protocol, such a strategy has been shown

to increase the chance that Eve reads the bit correctly although it does not reduce her chance of being detected [18]. However, when the legitimate parties use a complete set of MU bases, there is no basis that is "halfway" between all of them. There are many issues concerned with finding the optimal strategy of an eavesdropper [58, 82, 67, 12]. In the following, we will assume that Eve picks one of the bases used by the legitimate parties and consider the protocol when Alice and Bob use a set of c MU bases.

There is no loss of generality in assuming that Eve's basis is given by $\mathcal{E} \equiv \{|e_i\rangle \in \mathbb{C}^d, i = 1 \dots d\} = \mathcal{B}^0$. Under this assumption, the distance between the bases used by all three parties is

$$D^2(E, B^x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 - \frac{1}{d} & \text{if } x \neq 0, \end{cases}$$

zero if $\mathcal{B}^x$ corresponds to $\mathcal{E}$ or maximal otherwise. Hence, the index transmission error rate for a set of c MU bases is given by

$$\begin{aligned} \mathcal{R}_{IT}^{MUB} &= \frac{1}{c} \sum_{x=1}^{c-1} \left(1 - \frac{1}{d}\right) \\ &= \frac{(c-1)(d-1)}{cd}. \end{aligned} \tag{6.13}$$

We see that the error rate is an increasing function of both c and d and that Eq. (6.13) is indeed maximized if Alice and Bob use a complete set of MU bases. In which case, the index transmission error rate of the protocol equals

$$\mathcal{R}_{IT}^{MUB} = \frac{d-1}{d+1}$$

and therefore tends to 100% as d tends to infinity.

The index transmission error rate introduced by an intercept-and-resend attack in Eq. (6.13) is equal to the quantum bit error rate of the BKB01-protocol of Bourennane et al. [25]. It is a natural generalisation of the BB84 protocol and has been further analysed in [26, 44]. The BKB01-protocol, the d letters of an alphabet are encoded into the indices of one of c mutually

unbiased bases. Alice sends a state $|\psi_x^a\rangle$, where $x = 1 \ldots d$ and $a = 0 \ldots c-1$, and after Bob's measurement, announces the basis, a, which she used to prepare the states. Hence, whenever Bob performs a measurement in the same basis $\mathcal{B}^b$, they share the letter $x \in \mathcal{A}$. Note that in contrast to the HSE-protocol, the roles of the bases labels and indices are reversed. In the conclusion, the error rates and the number of states needed to successfully share one bit of the key for the BKB01 protocol are compared to the HSE-protocol.

The quantum bit error rate, $\mathcal{R}_{QB}$, given in Eq. (6.7), also simplifies significantly when Alice and Bob use a set of c MU bases and we assume that Eve's basis equals $\mathcal{E} = \mathcal{B}^0$, say. Under these assumptions, the probability that an index changes is zero if all three parties use the same bases and one minus the probability of measuring the correct index if any one of the parties uses a different basis

$$p_i(x,y) = \begin{cases} 0 & \text{if } (x,y) = (0,0) \\ 1 - \frac{1}{d} & \text{if } (x,y) \neq (0,0). \end{cases}$$

Therefore, the product of probabilities given in Eq. (6.8),

$$\prod_{k=1}^{c-1} p_{a_k}(x, y_k),$$

depends solely on whether any of the terms correspond to $(x, y_k) = (0,0)$.

To calculate the number of non-zero terms in $\mathcal{R}_{BE}$, given in Eq. (6.10), note that one of Bob's bases is always equal to $\mathcal{B}^x$ and therefore $(x, y_k) = (0,0)$ for some k, if and only if $x = 0$. Hence, the proportion of non-zero terms in Eq. (6.10) is equal to $(1 - 1/c)$. Similarly, when the vectors $\mathbf{y} \in Y$, the number of non-zero terms in Eq. (6.9) is $\left(1 - \frac{1}{c} + \frac{1}{c^2}\right)|Y||I|c$, so that Bob's error rate and the key rate are given by

$$\begin{aligned} \mathcal{R}_{BE} &= \left(1 - \frac{1}{c}\right)\left(1 - \frac{1}{d}\right)^{c-1} \\ \mathcal{R}_K &= \left(1 - \frac{1}{c} + \frac{1}{c^2}\right)\left(1 - \frac{1}{d}\right)^{c-1}, \end{aligned}$$

respectively. Therefore, for a set of c mutually unbiased bases, the error rate $\mathcal{R}_{QB}$ is given by

$$\mathcal{R}_{QB}^{MUB} = \left(1 - \frac{1}{c}\right)^2 \left(1 - \frac{1}{c} + \frac{1}{c^2}\right)^{-1} \tag{6.14}$$

which, surprisingly, does *not* depend on the dimension of the quantum systems used in the protocol. However, it is of course limited by the number of MU bases that can be constructed in a given dimension $c \leq d + 1$ and may also be limited by the conjectured non-existence of complete sets of MU bases in composite dimensions.

Whilst constructions of complete sets of MU bases are known for prime power dimensions, and are well understood in low dimensions [34] their existence is an open problem for composite dimensions. In fact, there is considerable numerical [38, 32] and analytical [33, 84] evidence to suggest that there are no more than three MU bases in dimension six. Hence restricting the measurements to MU bases could mean that the protocol is more efficient in prime power dimensions than in composite dimensions, for example, using six MU bases in dimension five the error rate $\mathcal{R}_{IT}$ is $2/3 \approx 66.7\%$ were as if only three MU bases are available in dimension six the maximum error rate is $5/9 \approx 55.6\%$. The situation for the QBER is even more pronounced since $\mathcal{R}_{QB}^{MUB}$ depends only on the number of MU bases available and not on the dimension. As such it would be better to use quantum systems of dimension three since it is possible to construct four MU bases than to use systems of dimension $d = 6$, for which we only know how to construct three bases with the required overlap.

6.4.2 Approximate mutually unbiased bases

It is not clear that a complete set of $d + 1$ mutually unbiased bases exists in all dimensions. Therefore, in order to consider the limiting behaviour of the protocol, we consider an alternative choice of bases for which constructions are known in all dimensions. As with a complete set of MU bases, they have the property that the error rate $\mathcal{R}_{IT}$ tends to 100% as the dimension of the quantum systems used by Alice and Bob increases.

Two bases $\mathcal{B}^x = \{|\psi_1^x\rangle, \ldots, |\psi_d^x\rangle\}$ and $\mathcal{B}^y = \{|\psi_1^x\rangle, \ldots, |\psi_d^x\rangle\}$, are mutually unbiased when

their elements satisfy the uniform modulus condition

$$|\langle\psi_i^x|\psi_j^y\rangle| = \kappa, \tag{6.15}$$

for all $i, j = 1, \ldots, d$. In finite dimensions, this condition implies that $\kappa = 1/\sqrt{d}$ but one might ask if there are sets of bases which almost satisfy Eq. (6.15)? Klappenecker et al. [90] define approximate mutually unbiased bases (abbreviated as AMU bases) which have the property that the modulus of the inner product between vectors from different bases is small. In particular they define a set of d^2 bases such that

$$|\langle\psi_i^x|\psi_j^y\rangle| \leq \frac{2 + O(d^{-1/10})}{\sqrt{d}} \quad \text{for } x \neq y,$$

and for all i, j, where $f(d) = O(d^{-1/10})$ means that there exists a constant $K > 0$ such that $|f(d)| \leq Kd^{-1/10}$ for all $d \geq 1$. Hence if Alice and Bob use all d^2 bases, and Eve uses one of the bases in her intercept-and-resend attack, the index transmission error rate is bounded from below by

$$\mathcal{R}_{IT}^{AMUB} \geq 1 - \frac{1}{d^3}\left[d + (d^2 - 1)(2 + Kd^{-1/10})^4\right]. \tag{6.16}$$

The unknown constant in Eq. (6.16) prevents us from saying anything in specific dimensions, but we can still consider the protocol when Alice and Bob use a set of AMU bases in the limit as d tends to infinity. We see that such a set of approximate MU bases defined so that they minimise the value of κ in Eq. (6.15) and therefore maximise the distance measure defined by Eq. (6.12) are good at detecting the eavesdropping by Eve. Even though a complete set of MU bases may not exist in every dimension, we can at least define a set of AMU bases that do exist in all dimensions and for which the ITER tends to 100%.

6.5 Implementations

In this section, we present a specific example of how Alice and Bob can use the HSE-protocol to form a shared key. We also calculate the quantum bit and index transmission error rates that

allow Alice and Bob to detect an eavesdropper for this choice of c and d. Finally, we discuss a practical implementation of the protocol that could be used for any values of c and d using photon states and multiport beam splitters.

6.5.1 An alternative "six-state" protocol using qubits

In the six-state protocol [12, 35], Alice prepares and sends one of six states corresponding to the points on the Bloch ball $(\pm 1, 0, 0)$, $(0, \pm 1, 0)$ and $(0, 0, \pm 1)$. These six states form three MU bases $\mathcal{B}^0$, $\mathcal{B}^1$, and $\mathcal{B}^2$ corresponding to

$$\{|0\rangle, |1\rangle\}, \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}, \text{ and } \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

respectively. After receiving a state from Alice, Bob performs a measurement in one of the three bases and records his outcome. Alice announces which of the bases she used to prepare the state and if Bob used the *same* basis they are able to share an element of the key. When the bases used by Alice and Bob coincide, Bob can correctly determine the letter because his measurement outcome must correspond to the state prepared by Alice (in the absence of an eavesdropper).

Using the polarization of photons to encode the states, Enzer et. al. have implemented the six-state protocol experimentally [60]. The three bases in their scheme correspond to horizontal/vertical (H/V), diagonal $+45°/-45°$ (D/d) and left/right circular (L/R) polarization; the three states H,D and L encoding a zero and V,d,R a one. By simulating an intercept-and-resend attack Enzer et. al. find a bit error rate of $34.0 \pm 1.4\%$ in agreement with the theoretical value of 33.3%.

In order to implement the HSE-protocol, the six-state scheme presented in [60] requires only a slight modification. The preparation and measurement of the states remains the same; the difference being the method of encoding the alphabet. Here, we will use the polarizations H/V to encode a zero, D/d a one and L/R a two. That is, our scheme uses a three letter alphabet $\mathcal{A} = \{0, 1, 2\}$ encoded into the choice of basis; $\mathcal{B}^0$, $\mathcal{B}^1$, or $\mathcal{B}^2$. The indices of the states are either zero or one corresponding to H,D, and L or V,d and R respectively.

As before, Alice chooses one of the bases $\mathcal{B}^0$, $\mathcal{B}^1$, or $\mathcal{B}^2$ but this time sends *two* states. That is,

suppose Alice chooses to encode the bits in the H/V basis, then she sends either HH, HV, VH or VV. Bob now makes a measurement in two *different* bases and records the indices corresponding to his outcomes. Alice announces the indices, either 00, 01, 10 or 11, equal to her choice of prepared states. She does not announce the basis. Using the indices announced by Alice and his measurement outcomes, Bob hopes to determine the basis used by Alice.

An element of the key is shared whenever Bob's indices both differ from the indices announced by Alice. For example, if Alice sends states with indices 01, an element of the key is shared if and only if Bob's measurement outcomes are 10. For this scheme, the average rate at which a bits are shared between Alice and Bob is given by

$$\mathcal{R}_t = \log_2(3)\frac{1}{3}\left(1-\frac{1}{2}\right)^2 \approx 13.2\%,$$

since the probability that Bob does not use the same basis as Alice in both of his measurements is 1/3 and there is a 1/2 chance that he does not measure the announced index when using a different basis. The pre-factor of $\log_2(3)$ is due to the fact that when an element of the key is shared it corresponds to an element of of a *three* letter alphabet.

Whilst the bit rate is 13.2%, compared to 33% for the six-state protocol, the number of sates Alice must send in order to share one bit of information is much higher than in the six-state protocol. For each attempt at sharing a letter of the alphabet, Alice must send two states. Therefore the average number of states, $\mathcal{N}_s = 2 \times 100/13.2 \approx 15.2$ which is five times more than the 3 states needed to share one bit when implementing the six-state protocol.

We find that although this protocol is more expensive than the six-state protocol, it is also more sensitive to an eavesdropper. The quantum bit error rate of an intercept-and-resend attack of this new protocol is given by

$$\mathcal{R}_{QB}^{MUB} = \left(1-\frac{1}{3}\right)^2\left(1-\frac{1}{3}+\frac{1}{3^2}\right)^{-1} = \frac{4}{7} \approx 57.1\%,$$

following Eq. (6.14); representing a significant improvement over the 33.3% error rate of the six-state protocol. We have used the *same* six states as the six-state protocol but this new method

of encoding the letters of an alphabet is more sensitive to an intercept-and-resend attack.

6.5.2 Possible implementation using multiport beam splitters

A recent experiment has implemented quantum state tomography using a complete set of MU bases in dimension $d = 4$ [1]. It demonstrates that tomography with MU bases is not only optimal in theory, but is more efficient than standard measurement strategies in practice. The scheme presented in [1] therefore provides a way of measuring two-qubit photon states in one of five mutually unbiased bases in dimension four. However, to implement the QKD presented in Section 6.1 a set of c MU bases, we also need to reliably *prepare* the relevant states. Such a scheme for $c = 2$ MU bases has been provided by Khan et al. [87] and can be extended to any number of mutually unbiased bases. This follows from the fact that *any* discrete unitary operator can be realised using a series of beam splitters and mirrors [120]. These so called *multiport beam splitters* are symmetric when they correspond to MU bases [153].

The protocol could be implemented as follows. Alice uses a single photon source such as a spontaneous parametric down conversion crystal. She now chooses one of $c-1$ multiport beam splitters, or to bypass the beam splitters altogether. This gives one of the c bases labeled by the letters of $\mathcal{A}$ required for the protocol. Each vector $|\psi_i^x\rangle$ of her chosen basis, $\mathcal{B}^x$, is encoded into the output paths of the corresponding beam splitter by sending a single photon into the input port i. Bob uses the same beam splitters in order to measure the state of each photon he receives. He does this by first sending it through one of the beam splitters (or bypasses them to measure $\mathcal{B}^0$) and then detecting it in one of the d output ports. When $c = 2$, a natural choice for the two MU bases is to use the standard basis $\mathcal{B}^0 = \{|i\rangle, i = 0 \ldots d-1\}$ and the so called Fourier matrix which has entries $F_{ij} = \omega^{ij}/\sqrt{d}$, for $i, j = 0 \ldots d-1$ where $\omega = \exp(2\pi i/d)$ is the d^{th} root of unity (which for $d = 3$ is given by $\mathcal{B}^1$ in Eq. (6.1)). This scheme corresponds to the one presented in [87] and could be realised using Bell multiport beam splitters [101].

6.6 Comparison with other QKD protocols

We have presented a novel protocol that enables two parties to generate a shared key. It is special in that the presence of an eavesdropper who uses an intercept-and-resend attack creates a *high error rate*. This has the practical advantage of allowing Alice and Bob to detect Eve even if the system noise in their implementation is high. We have analysed two error rates that allow for the detection of an eavesdropper; the *index transmission error rate* (ITER) and the *quantum bit error rate* (QBER). Both of these measures of the sensitivity to eavesdropping tend to one as the parties use more bases to encode the elements of the key and, in the case of the ITER, if they use higher dimensional systems.

Protocol	(d, c)	$\mathcal{R}_{QB}$	$\mathcal{R}_{IT}$	$\mathcal{R}_t$	N_s
BB84	$(2, 2)$	25.0%	n/a	50.0%	2.0
KMB09	$(2, 2)$	33.3%	25.5%	25.0%	4.0
BKB01 (6-state)	$(2, 3)$	33.3%	n/a	33.3%	3.0
HSE	$(2, 3)$	57.1%	33.3%	13.2%	15.1
BKB01	$(3, 2)$	33.3%	n/a	79.2%	1.3
KMB09	$(3, 2)$	33.3%	33.3%	33.3%	3.0
BKB01	$(3, 4)$	50.0%	n/a	39.6%	2.5
HSE	$(3, 4)$	69.2%	50.0%	14.8%	20.3
BKB01	$(7, 2)$	42.9%	n/a	140.4%	0.7
KMB09	$(7, 2)$	33.3%	42.9%	42.9%	2.3
BKB01	$(7, 8)$	75.0%	n/a	35.1%	2.8
HSE	$(7, 8)$	86.0%	75.0%	12.7%	54.9

Table 6.1: Table comparing different QKD protocols in dimensions $d = 2, 3$ and 7; $\mathcal{R}_{QB}$ and $\mathcal{R}_{IT}$ are the quantum bit and index transmission error rates of an intercept-and-resend attack, respectively; $\mathcal{R}_t$ is the bit transmission rate defined in Eqn (6.3); finally, N_s is the average number of states Alice must send in order to share one bit with Bob. Note that the KMB09-protocol is a special case of the HSE-protocol.

Table 6.1 compares the essential features of the HSE-protocol to existing QKD protocols: the original quantum key distribution protocol of Bennett and Brassard [17] is referred to as BB84; the generalisation of BB84 to a protocol that uses c mutually unbiased bases and d-dimensional quantum systems [25] is called BKB01; the case where three MU bases are used in dimension two corresponds to the six-state protocol (6-state) [12, 35]; the protocol presented in Section 6.1 is

denoted HSE (which stands for *highly sensitive to eavesdropping*); the case where only two bases are used corresponding to the protocol of Khan et al. (KMB09) [87]. Throughout the table, we assume that the HSE-protocol is applied to a set of c mutually unbiased bases. The pair of numbers, (d, c), in the second column correspond to the dimension of the quantum systems used in the protocol and the number of elements in the classical alphabet.

The third and forth columns of Table 6.1 show the QBER and the ITER respectively. The error rates, which have been calculated using Eqns. (6.13) and (6.14), show that by using $d+1$ MU bases, Alice and Bob can increase the QBER beyond that of BKB01. The fifth column displays the rate at which the two legitimate parties sharing one bit of information; that is $\mathcal{R}_s$ has been normalised so that it gives a *per bit* success rate[1]. The last column then shows the average number of states Alice needs to send in order to successfully share one bit of her key with Bob. This final column clearly demonstrates the trade-off between the error rate and the "cost" of producing a shared key. It is possible to make it easier to detect Eve but this comes at the expense of reducing the bit transmission rate.

[1] Note that when the BKB01 protocol is applied to two MU bases in dimension $d = 7$, the rate at which bits are shared between Alice and Bob is larger than 100%. In this case, the legitimate parties use 7-dimensional quantum systems so that each time they are successful, they share an element of a 7 letter alphabet. Hence, the number of states Alice needs to send in order to share one *bit* is 0.7, i.e. less than one.

CHAPTER 7

Summary and outlook

The *dynamics* of an autonomous Hamiltonian system with a single degree of freedom differs considerably from that of a system with two or more degrees of freedom. Nontrivial interactions among the degrees of freedom usually lead to an effectively unpredictable time evolution. From a *kinematical* point of view, however, there is not much of a difference: the composite system simply inherits the structure of its constituents.

Schwinger associates one degree of freedom with a quantum system whenever the dimension d of its Hilbert space is a prime number [130]. Quantum systems with two or more degrees of freedom are obtained by tensoring copies of these building blocks. Our classically trained intuition wants to make us believe that the kinematics of composite quantum systems will not depend on the dimensions of the building blocks. In other words, we expect that composite quantum systems with dimensions $d_1 = 2 \times 3$ and $d_2 = 3 \times 3$, for example, are structurally identical. The concept of *mutually unbiased* (MU) bases appears to invalidate this expectation since complete sets of MU bases seem to exist in prime-power dimensions only. They are an important, physically motivated tool allowing one to reconstruct quantum states with optimal efficiency or implement a quantum key distribution protocol.

7.1 Sets of MU bases

The traditional approach to find *complete* sets of MU bases in prime-power dimensions via the Heisenberg-Weyl group or by using finite fields is constructive and, therefore, does not exclude the existence of other inequivalent complete sets. The approach presented in Chapter 2 is, in contrast, *exhaustive*: we are able to affirm that the known complete sets for $2 \leq d \leq 5$ are unique (up to equivalence). Their uniqueness has been shown earlier for $d \leq 4$ [61] while [27] contains a proof for $2 \leq d \leq 5$ in a Lie algebraic setting. We find it appealing that it is possible to prove the uniqueness of complete sets of MU bases in low dimensions by *elementary* methods.

The *Clifford group* is the normalizer of the Heisenberg-Weyl group in the group of all unitaries. It can be written as a semi-direct product of the Heisenberg-Weyl group and $SL(2, F_d)$, the group of (2×2) matrices with entries integers modulo d. Triples of MU bases are interesting in this context because there is a conjecture [152] which states that all SIC-POVM vectors are invariant under an element of the Clifford group of order 3. The conjecture has been verified in all dimensions for which SIC-POVMs are known [4]. Any triple of MU bases is the orbit of an order 3 element of $SL(2, F_d)$. Thus, the existence of two inequivalent triples in dimension five may lead to some structural insight into the relation between MU bases and SIC-POVMs going beyond the results of [5].

The constructive method of extending a pair of bases $\{I, H\}$ to a larger set can also be used to prove that a given Hadamard matrix cannot be part of a complete set of MU bases. In Chapter 3, we have shown that the construction of more than three MU bases in $\mathbb{C}^6$ is not possible starting from nearly 6,000 different Hadamard matrices. This result adds significant weight to the conjecture that a complete set of seven MU bases does not exist in dimension six. In this approach, the idea to construct a Gröbner basis was vital since the resulting equations appear intractable to solve by hand.

The landscape of known Hadamard matrices (given in Appendix B and pictured in Fig. 3.1) contains parameter dependent families such as the Fourier family $F(\mathbf{x})$. These parameters determine the coefficients of the equations which define a vector MU to the pair $\{I, H(\mathbf{x})\}$. Hence by changing the parameter values by a small amount the solutions of the equations will also only

change by a small amount. Obviously, these terms need to be made explicit but one might hope to extend each point considered in Chapter 3 to a small ball by obtaining a suitable error bound. There is, however, one problem with this argument. The *number* of solutions may change when varying the parameter values (cf. the step changes in Figs. 3.2 and 3.3).

In a recent work by Faugère et al., the idea of constructing a *parameter dependent* Gröbner basis was proposed [66]. A parameter space such as $\{(\alpha, \beta) : 0 \leq \alpha \leq 1/6, 0 \leq \beta \leq 2\alpha\}$ which defines the fundamental region of the Fourier family, is divided into cells where the number of solutions in each cell remains constant. Just as the discriminant of a polynomial in one variable distinguishes regions of a differing number of solutions, it is possible to construct a *discriminant variety* of a system of multivariate polynomials. Finding a discriminant variety would allow one to study each cell one at a time in the knowledge that the number of solutions remains constant.

In Chapter 4, we address the existence of a complete set of MU bases in dimension six by defining constellations of quantum states in the space $\mathbb{C}^d$ which are mutually unbiased. The search for these MU constellations has been cast in the form of a global minimisation problem which can be approached by standard numerical methods. Our conclusions are based on a total of 433,000 searches in dimensions five to seven which would take approximately 16,000 hours on a single Pentium 4 desktop PC. The results of the numerical searches performed in dimension six provide strong evidence that not all MU constellations of the form $\{5, \lambda, \mu, \nu\}_6$ exist. We have been able to positively identify 18 out of 35 MU constellations in dimension six. On the basis of the numerical data, we consider it highly unlikely that the 15 unobserved critical and overdetermined MU constellations do exist, making the existence of four MU bases exceedingly improbable.

Let us discuss these results in a general framework. *Critical* constellations $[\boldsymbol{\lambda}]_d$ are defined by the equality $p_d = c_d$. If p_d parameters need to satisfy $c_d \equiv p_d$ equations, one would expect some isolated solutions to exist in a generic situation. In the overdetermined case, there are more constraints than free parameters, $c_d > p_d$, and no MU constellations are expected. The counting of parameters indicates how special large sets of mutually unbiased states are. For any $d > 2$, the $d(d+1)$ quantum states of a complete set of MU bases possess too few parameters to generically satisfy the conditions imposed on them by mutual unbiasedness. In dimension seven,

for example, such a set consists of 56 pure states depending on 288 independent parameters which need to satisfy 1,323 constraints. This is only possible if the constraints conform to some fundamental structure prevailing in the space $\mathbb{C}^7$ - obviously, the number-theoretic consequences of $d = 7$ being a prime number spring to mind. In other words, the constraints must *degenerate* at one or more points of the constellation space $\mathcal{C}_7$ so that sufficiently many MU bases can arise.

We conclude by emphasizing that the results of algebraic and numerical searches presented in Chapters 3 and 4 provide strong evidence for the absence of seven MU bases in dimension six. It is thus likely that the kinematics of quantum systems with dimensions $d_1 = 2 \times 3$ and $d_2 = 3 \times 3$, respectively, will differ structurally.

7.2 Applications of MU bases

We have seen that there are two main applications for sets of mutually unbiased bases: quantum state tomography and quantum key distribution. In a tomographic procedure the optimal measurement settings constitute a complete set of MU bases. Likewise, it is possible to argue that sets of MU bases are "optimal" in some quantum key distribution protocols such as BB84, the six-state protocol and the new protocol presented in Chapter 6. From a practical perspective MU bases are useful for finding and hiding information about quantum states.

At first sight, the new protocol presented in Chapter 6 appears to have no special features relating to the dimension of the quantum systems used by Alice and Bob. However, an analysis of the optimal bases reveals that it is more efficient when the legitimate parties use systems of prime-power dimensions. In prime-power dimensions Alice and Bob can use constructions of $d+1$ mutually unbiased bases. In addition, in some dimensions, *inequivalent* sets of c MU bases are available. For example in dimension $d = 4$, there exits a three-parameter family of triples of MU bases or in dimension $d = 16$ there is a 17-parameter family of pairs of MU bases [141]. It may be that within these families there are some bases that are experimentally more accessible than others. For example, the notion of equivalence considered by Romero et al. [122] involves the entanglement content of the bases and therefore, one aspect of the experimental difficulty in measuring and preparing systems in the corresponding bases.

If an experimenter finds that a particular measurement is easy to implement and that quantum systems prepared in the corresponding basis are readily available, they can use the HSE-protocol to distribute shared keys. Given the analytical form of the bases, we have shown how to calculate the error rate and the rate at which elements of a key are generated. Hence, to some extent, the protocol can be made to fit around experimental conditions, the question is then if the system noise enables an eavesdropper to disguise their presence. It may be that in practice it is better to search for measurements that can be performed efficiently in the laboratory (or in a purpose built device) than to find the analytical optimal bases.

In recent years, quantum physicists have realised that finite dimensional complex linear spaces are surprisingly rich both in physical content and from a mathematical perspective. This setting has led to many important physical discoveries and in particular, the ability to distribute keys in a secure way. In this thesis, we have explored this mathematical structure further and found that, at least in principle, Alice and Bob can make it very hard for Eve to hide. An interesting question is what further applications of MU bases are there; either in existing quantum information tasks or in new applications of quantum systems?

7.3 Gröbner bases in Quantum Information

The application of Gröbner bases to the problem of mutually unbiased bases suggests that they could be used as a powerful tool in other problems from quantum information. By its very nature, many problems in this field are formulated relative to finite-dimensional Hilbert spaces and, mathematically, boil down to solving coupled polynomial equations. The construction of Gröbner bases through Buchberger's algorithm [36] transforms these equations into a form suitable to identify their solutions. In most cases, the required algebraic operations will be lengthy and cannot be carried out manually. Appropriate symbolic computer programs, however, often allow one to compute them analytically. In fact the construction of Gröbner bases has already been extremely useful in other applied fields such as cryptography [65], error correcting codes [8, 48], robotics [98], and in biological systems [114]. In recent years, this application of commutative algebraic geometry has been helped by the increased availability of computational

resources such as memory and computing time. We now briefly describe how the construction of a Gröbner basis could be used in three applications from Quantum Information.

The Geometric measure of entanglement.

A natural way to measure the entanglement of a k-party state, $|\psi\rangle$, is its "distance" to the nearest separable state. This geometric measure of entanglement [132],

$$E(\psi) = \min_{|a_1 a_2 \ldots a_k\rangle} |\langle a_1 a_2 \ldots a_k | \psi \rangle| \,,$$

is widely used [10, 146], and equals the coefficient of the first term in the multi-partite generalization of the Schmidt decomposition [43]. It is possible to find an analytic expression for many two party states [146] but is already very challenging for three-qubit states.

The general n-party case can be expressed as a system of coupled multivariate polynomial equations [43] and by restricting the form of the states $|\psi\rangle$, some progress has been made for three-qubit systems [79, 142]. However, as one considers systems composed of more qubits or qudits, the resulting polynomial equations become difficult to solve by hand. The application of Buchberger's algorithm and the subsequent algorithms for the construction of a Gröbner basis are a promising method of studying the geometric measure of entanglement. As an interesting aside, it may be that the approach presented in [79] is effectively the construction of a Gröbner basis.

Separability

The investigation of entanglement has been a particularly lively and fruitful strand in the field of quantum information. Described by Schrödinger as not one but rather *the* characteristic trait of quantum mechanics [129], it distinguishes quantum states from states with purely classical correlations and is a key resource in many of the exciting applications of quantum systems.

Unfortunately, understanding the complex structure of entanglement in quantum systems is not an easy problem. In fact, it is known that the separability problem cannot be efficiently solved with a classical computer [73]. A key result in the field is that a separable state remains a valid

density matrix under partial transposition [116] and that this is an example of a positive map [80]. Positive maps provide a necessary and sufficient condition of separability. In order to find new ways of detecting entanglement, we need to find operators that are not a sum of a symmetric operator and an operator symmetric under partial transposition. These "indecomposable maps" are intimately linked to the problem of finding biquadratic forms that are not sums of squares, a link that has recently been extended in [137]. Simple examples can be solved by hand but the application of Gröbner bases and the surrounding techniques would allow one to tackle more general and interesting cases. In fact, the authors of the paper [137] mention themselves that the construction of a Gröbner basis would be a hopeful strategy to extend their results.

In addition to finding new entanglement witnesses through the construction of indecomposable maps, Gröbner basis methods could be directly applied to the separability problem. The condition for a state to be separable can be formulated in terms of a set of polynomial inequalities [92] developed using Lagrange multipliers. However, due to the complexity of the resulting equations, the authors of [92] were only able to consider simple subsets of all states in low dimensions. Using this or other potential ways of formulating the separability problem as a system of equations it would be possible to apply the powerful methods developed since the introduction of Buchberger's algorithm.

Classification of graph states.

Graph states are a subset of all possible pure multipartite states which can be described by the nodes and connections of a graph [76, 127]. They are used in quantum error correction [128] and in one-way quantum computation [30, 119]. There are two types of quantum operations which leave a graph state invariant: local unitary (LU) operations and local Clifford (LC) operations. Hence it is natural to define equivalence classes of graph states using these two types of operation. It has been conjectured that these equivalence classes of graph states under LU and LC operations are the same [111]. There is numerical evidence to support this claim for states that consist of only a few qubits. However, a 27-qubit state for which the LU and LC equivalence classes are *not* equal acts as a counter example of this conjecture [85].

The equivalence classes of LU and LC states can be characterized in terms of a set of poly-

nomial invariants [41, 109, 110]. Hence the relationship between LU- and LC- invariant graph states can be studied at the level of invariants. Gröbner bases can be used to provide a canonical description of the invariants and have already been applied to problems relating to polynomials which are invariant under matrix groups [49]. By simplifying the description of the invariants, it is possible to address the question of uniqueness and therefore equivalence of two sets of invariants.

APPENDIX A

Equivalent sets of MU bases

Many sets of MU bases are identical to each other. To simplify the enumeration of all sets of MU bases we introduce *equivalence classes* and a *standard form* of sets of MU bases.

Each set of $(r+1)$ MU bases in $\mathbb{C}^d$ corresponds to a list of $(r+1)$ (with $r \leq d$) complex matrices H_ρ, $\rho = 0, 1, \ldots, r$ of size $(d \times d)$. Two such lists $\{H_0, H_1, \ldots, H_r\}$ and $\{H'_0, H'_1, \ldots, H'_r\}$ are *equivalent* to each other,

$$\{H_0, H_1, \ldots, H_r\} \sim \{H'_0, H'_1, \ldots, H'_r\} \tag{A.1}$$

if they can be transformed into each other by a succession of the following four transformations:

1. an *overall unitary* transformation U applied from the left,

$$\{H_0, H_1, \ldots, H_r\} \to U\{H_0, H_1, \ldots, H_r\} \equiv \{UH_0, UH_1, \ldots, UH_r\}\,, \tag{A.2}$$

   which leaves invariant the value of all scalar products;

2. $(r+1)$ *diagonal unitary* transformations D_ρ from the right which attach phase factors to

each column of the $(r+1)$ matrices,

$$\{H_0, H_1, \ldots, H_r\} \to \{H_0 D_0, H_1 D_1, \ldots, H_r D_r\}\,; \tag{A.3}$$

these transformations exploits the fact that the overall phase of a quantum state drops out from the conditions of MU bases;

3. $(r+1)$ *permutations* of the elements within each basis,

$$\{H_0, H_1, \ldots, H_r\} \to \{H_0 P_0, H_1 P_1, \ldots, H_r P_r\}\,, \tag{A.4}$$

which amount to relabeling the elements within each basis by means of unitary permutation matrices P_n satisfying $PP^T = I$;

4. *pairwise exchanges* of two bases,

$$\{\ldots, H_\rho, \ldots, H_{\rho'}, \ldots\} \to \{\ldots, H_{\rho'}, \ldots, H_\rho, \ldots\}\,, \tag{A.5}$$

which amounts to relabeling the bases.

5. an *overall complex conjugation*

$$\{H_0, H_1, \ldots, H_r\} \to \{\overline{H}_0, \overline{H}_1, \ldots, \overline{H}_r\} \tag{A.6}$$

which leaves the values of all scalar products invariant.

These equivalence relations 1-4, allow us to *dephase* a given set of MU bases. The resulting *standard form* $\{I, H_1, \ldots, H_r\}$ is characterized by four properties: (i) the first basis is chosen to be the standard basis of $\mathbb{C}^d$ described by $H_0 \equiv I$, where I is the $(d \times d)$ identity matrix; (ii) the remaining bases are described by (complex) *Hadamard* matrices: each of their matrix elements has modulus $1/\sqrt{d}$; (iii) the components of the first column of the matrix H_1 are given by $1/\sqrt{d}$; (iv) the first row of each of the Hadamard matrices H_1 to H_r has entries $1/\sqrt{d}$ only.

Let us illustrate the dephasing in dimension $d = 3$ where a given complete set of four MU bases can be brought into the form

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & e^{i\alpha_{11}} & e^{i\alpha_{12}} \\ 1 & e^{i\alpha_{21}} & e^{i\alpha_{22}} \end{pmatrix}, \right.$$
$$\left. \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{i\beta_{11}} & e^{i\beta_{12}} & e^{i\beta_{13}} \\ e^{i\beta_{21}} & e^{i\beta_{22}} & e^{i\beta_{23}} \end{pmatrix}, \quad \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ e^{i\gamma_{11}} & e^{i\gamma_{12}} & e^{i\gamma_{13}} \\ e^{i\gamma_{21}} & e^{i\gamma_{22}} & e^{i\gamma_{23}} \end{pmatrix} \right\}. \tag{A.7}$$

The second unitary matrix obtained here is (proportional to) a *dephased* complex Hadamard matrix [16] motivating our terminology. Note that the vectors of the last three bases (except for $(1, 1, 1)^T/\sqrt{3}$) may be rearranged using (A.4).

MU constellations $\{\lambda\}_d$ with at least one complete basis as in (4.7) also come in equivalence classes if one applies suitably restricted variants of the symmetry transformations (A.2) to (A.5). Thus, they can be brought to *dephased* form as well. If a complete set of MU bases exists, such as $\{3^4\}_4$ in $\mathbb{C}^d$, the dephased form of smaller MU constellations is simply obtained by removing an appropriate number of the vectors. Eq. (4.8) shows the dephased form of the MU constellation $\{2^3, 1\}_4$ contained in $\{3^4\}_4$, given in (A.7).

The notion of equivalence defined by Eqs. (A.2) to (A.6) is mathematical in nature; it captures all possible operations that leave invariant the conditions (4.1) for two bases to be mutually unbiased. Motivated by experiments, there is a finer equivalence of complete sets of MU bases based on the entanglement structure of the states contained in each basis [97, 122]. For dimensions that are a power of two, a complete set of MU bases can be realized using Pauli operators acting on each two-dimensional subsystem. Two sets of MU bases are then called equivalent when they can be factored into the same number of subsystems. For $d = 2, 4$ this notion of equivalence also leads to a unique set of $(d + 1)$ MU bases. However, for $d = 8, 16, \ldots$ complete sets of MU bases can have different entanglement structures even though they are equivalent up to an overall unitary transformation [97, 122].

APPENDIX B

Inequivalent triples of MU bases in $\mathbb{C}^5$

We show that the two classes of triples of MU bases given by $\mathcal{T}^{(1)} \equiv \{I, F_5, H_5^{(1)}\}$ and $\mathcal{T}^{(2)} \equiv \{I, F_5, H_5^{(2)}\}$ are *inequivalent*. In a first step, we explain that it is sufficient to search for equivalence transformations generated by matrices of a special form. In a second step we show that a contradiction arises if one assumes that the triples $\mathcal{T}^{(1)}$ and $\mathcal{T}^{(2)}$ are equivalent.

Let us begin with a general remark about the structure of equivalence classes of sets of MU bases $\mathcal{M} = \{I, B_1, \ldots, B_r\}$ of $\mathbb{C}^d$ for all $r \in \{1, \ldots, d-1\}$. For convenience, we assume that the first basis equals the identity, i.e. the set is given in standard form. As explained in Appendix A all sets of MU bases equivalent to $\mathcal{M}$ are obtained as follows,

$$\mathcal{M} \to \mathcal{M}' = \{UM_0, UB_1M_1, \ldots, UB_rM_r\}\,; \tag{B.1}$$

with a unitary U and $(r+1)$ monomial matrices M_i being a product of diagonal unitaries with permutation matrices; to keep the notation simple we do not reorder the $(r+1)$ bases within $\mathcal{M}'$. For the set $\mathcal{M}'$ to be in standard form, one of the bases in $\mathcal{M}$, say B_ρ, must be mapped to the identity. As a consequence, the overall unitary transformation U must have a particular

form, namely

$$U = NB_\rho^\dagger\,, \tag{B.2}$$

where N is some monomial matrix and B_ρ is one of the matrices contained in the set $\mathcal{M}$.

In view of Eq. (B.2) we are led to determine the action of $F_5^\dagger$ and $(H_5^{(1)})^\dagger$ on the triple $\mathcal{T}^{(1)}$ as well as the action of $F_5^\dagger$ and $(H_5^{(2)})^\dagger$ on the triple $\mathcal{T}^{(2)}$. It turns out that both triples are *invariant* under these global transformations as we have the equivalences

$$NF_5^\dagger\mathcal{T}^{(1)} \sim N\mathcal{T}^{(1)} \sim N(H_5^{(1)})^\dagger\mathcal{T}^{(1)}\,, \tag{B.3}$$

and

$$NF_5^\dagger\mathcal{T}^{(2)} \sim N\mathcal{T}^{(2)} \sim N(H_5^{(2)})^\dagger\mathcal{T}^{(2)}\,. \tag{B.4}$$

The first equivalence in (B.3) follows from using $F_5^\dagger = F_5P$ and Eq. (2.46) while the second one also requires the identity

$$(H_5^{(1)})^\dagger F_5 = H_5^{(4)}M\,, \tag{B.5}$$

with some monomial matrix M. The equivalences (B.4) are derived in a similar way.

Consequently, we can always remove the effect of the matrices $B_\rho^\dagger$ in the global transformations (B.2) which leaves us with

$$\{I, F_5, H_5^{(j)}\} \to \{NIM_0, NF_5M_1, NH_5^{(j)}M_2\}\,, \quad j = 1, 2\,, \tag{B.6}$$

where N, M_1 and M_2 are monomial matrices, and up to rearranging terms. The non-zero entries of the monomial matrix N must, in fact, be fifth roots of unity[1] but we will not need this fact.

Using the restricted transformations shown in Eqs. (B.6), the triples $\{I, F_5, H_5^{(1)}\}$ and $\{I, F_5, H_5^{(2)}\}$ are equivalent to each other only if either

$$NF_5 = F_5M_1 \text{ and } H_5^{(2)}M_2 = NH_5^{(1)}\,, \tag{B.7}$$

[1] Assume that N has a nonzero element different from a fifth root, say $e^{i\alpha}$. This makes it impossible to transform $\mathcal{T}^{(1)}$ into standard form using right multiplication by monomial matrices unless the other nonzero elements of N also equal $e^{i\alpha}$. It follows that N must be a permutation matrix P apart from a phase factor, $N = e^{i\alpha}P$. Thus the matrices M_ρ must have a common factor of $e^{-i\alpha}$ which, however, is irrelevant for the definition of MU bases.

or

$$NF_5 = H_5^{(2)} M_1 \text{ and } F_5 M_2 = N H_5^{(1)}\,, \tag{B.8}$$

hold for some monomial matrices M_1 and M_2. The choice $M_0 = N^{-1} = N^\dagger$ in Eqs. (B.6) ensures that the identity will be mapped to the identity.

Eqs. (B.7) will now be shown to imply the identity

$$\Delta F_5 = F_5 M \tag{B.9}$$

for some monomial matrix M while Δ is a diagonal matrix with fifth roots of unity as nonzero entries, *not* proportional to the identity, $\Delta \neq cI, c \in \mathbb{C}$. However, Eq. (B.9) only holds if Δ *is* a multiple of the identity. This contradiction implies that there are no matrices N, M_1, M_2 such that Eqs. (B.7) hold. Since Eqs. (B.8) also imply Eq. (B.9) with a (possibly different) diagonal matrix $\Delta \neq cI, c \in \mathbb{C}$, the triples $\mathcal{T}^{(1)}$ and $\mathcal{T}^{(2)}$ cannot be equivalent.

Use $H_5^{(j)} = D^j F_5, j = 1, 2$, to express the second equation in (B.7) as

$$D^2 F_5 M_2 = NDF_5 = NDN^\dagger N F_5 \equiv \tilde{D} N F_5\,, \tag{B.10}$$

introducing $\tilde{D} \equiv NDN^\dagger = PDP^T$. Thus, the matrix $\tilde{D}$ is obtained from D by reordering its diagonal elements according to the permutation P defined via $N = PE$, with some unitary diagonal matrix E. Combining this equation with the first one in (B.7) leads to $D^2 F_5 M_2 = \tilde{D} F_5 M_1$, or

$$\tilde{D}^\dagger D^2 F_5 = F_5 M_1 M_2^\dagger \tag{B.11}$$

which is identical to (B.9) upon defining $\Delta = \tilde{D}^\dagger D^2$ and $M = M_1 M_2^\dagger$ which, as a product of two monomial matrices, is another monomial matrix. Since no permutation of the elements on the diagonal of $D^\dagger = \mathrm{diag}(1, \omega^4, \omega, \omega, \omega^4)$ produces the inverse of D^2 or a multiple thereof, we have $\Delta \neq cI$. Using the pair (B.8) instead of (B.7) also leads to an equation of the form (B.9) with $\tilde{D}^\dagger$ replaced by $\tilde{D}$ which, however, cannot be a multiple of the inverse of D^2, leading again to $\Delta \neq cI$.

We now show that Eq. (B.9) only holds if the matrix Δ is proportional to the identity. Write the monomial matrix M in (B.9) in the form

$$M = P\Delta'' \,, \tag{B.12}$$

where P is a permutation matrix and Δ'' is a *diagonal* matrix with entries having modulus one only. Denoting the inverse of Δ'' by Δ', Eq. (B.9) takes the form

$$\Delta F_5 \Delta' = F_5 P \,. \tag{B.13}$$

Let us write $\Delta = \mathrm{diag}(\alpha, \beta, \ldots, \epsilon)$ with phase factors α, β, etc., and similarly for Δ', and consider the simplest case $P \equiv I$. Then the matrix relation (B.13) reads explicitly

$$\begin{pmatrix} \alpha\alpha' & \alpha\beta' & \alpha\gamma' & \alpha\delta' & \alpha\epsilon' \\ \beta\alpha' & & & & \cdot \\ \gamma\alpha' & & & & \cdot \\ \delta\alpha' & & & & \cdot \\ \epsilon\alpha' & \cdot & \cdot & \cdot & \epsilon\epsilon'\omega \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix} , \tag{B.14}$$

The conditions resulting from the first row immediately imply that the elements on the diagonal of Δ' are all equal to α^*, or $\Delta' = \alpha^* I$. The conditions of the first column imply that the matrix Δ is also a multiple of the identity, namely $\Delta = \alpha I$. This contradicts the fact that the matrix Δ is different from a multiple of the identity.

Let us now drop the restriction the $P = I$. The effect of P acting on F_5 from the right is to permute its columns. The first row of F_5 will not change under this operation. Under the action of P, the first column will either stay where is is or it will be mapped to one of the four others. In the first case, we can immediately apply the argument given above to derive a contradiction. In the second case, it it straightforward to see that a similar argument still applies involving the first row of the matrices and that column which is the image of the first column. Thus, all possible choices of the monomial matrix M in (B.9) require Δ to be a multiple of the identity -

which it is not.

Finally, we consider the action of an overall complex conjugation (A.6) on either of the triples. We find that the set of three MU bases, $\mathcal{T}^{(1)}$, remains invariant after complex conjugation

$$\begin{aligned} \overline{\mathcal{T}}^{(1)} &= \{I, \overline{F_5}, \overline{H}_5^{(1)}\} \\ &\sim \{I, F_5, H_5^{(4)}\} \\ &\sim \mathcal{T}^{(1)}. \end{aligned}$$

Similarly, complex conjugation maps $\mathcal{T}^{(2)}$ to itself, $\overline{\mathcal{T}}^{(2)} \sim \mathcal{T}^{(2)}$. In summary, then we have shown that the equivalence relations (A.2) to (A.6) cannot transform the triple $\mathcal{T}^{(1)}$ into $\mathcal{T}^{(2)}$ or vice versa.

APPENDIX C

Known complex Hadamards matrices in dimension six

This Appendix lists the currently known complex Hadamard matrices for easy reference and to establish notation. For more details the reader is referred to [16] and to the online catalogue [140].

C.1 Special Hadamard matrices

The *Fourier matrix* F_6 has been introduced in Eq. (3.7); it is contained in both the Fourier family $F(\mathbf{x})$ and the transposed Fourier family $F^T(\mathbf{x})$ for $\mathbf{x} = 0$, where $F_6 \equiv F(0,0) \approx F^T(0,0)$ holds (cf. Section C.2).

The *Diţă matrix* D_0 is an example of a complex symmetric Hadamard matrix,

$$D_0 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & i & -i & -i & i \\ 1 & i & -1 & i & -i & -i \\ 1 & -i & i & -1 & i & -i \\ 1 & -i & -i & i & -1 & i \\ 1 & i & -i & -i & i & -1 \end{pmatrix}, \tag{C.1}$$

embedded in a continuous one-parameter set of Hadamard matrices, the Diţă family (cf. C.2).

Björck's *circulant matrix* [24] is defined by

$$C = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & iz & -z & -i & -z^* & iz^* \\ iz^* & 1 & iz & -z & -i & -z^* \\ -z^* & iz^* & 1 & iz & -z & -i \\ -i & -z^* & iz^* & 1 & iz & -z \\ -z & -i & -z^* & iz^* & 1 & iz \\ iz & -z & -i & -z^* & iz^* & 1 \end{pmatrix}, \tag{C.2}$$

where

$$z = \frac{1-\sqrt{3}}{2} + i\sqrt{\frac{\sqrt{3}}{2}}\,. \tag{C.3}$$

It was originally thought to be isolated but it is now known to be part of the family of Hermitean Hadamard matrices, $C \approx B(\theta_0)$ (cf. C.3).

The only known isolated Hadamard matrix is the *spectral matrix*,

$$S = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega^2 & \omega^2 \\ 1 & \omega & 1 & \omega^2 & \omega^2 & \omega \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega^2 & \omega & 1 & \omega \\ 1 & \omega^2 & \omega & \omega^2 & \omega & 1 \end{pmatrix}, \tag{C.4}$$

where ω is a third root of unity, $\omega = e^{2\pi i/3}$. It has been discovered by Moorhouse [108] and, independently, by Tao [143].

C.2 Affine families

There are three affine families of Hadamard matrices, characterized by the property (3.1) that they can be written as a non-trivial Hadamard product. The *Diţă family* [51] is given by $D(x) =$

$D_0 \circ \mathrm{Exp}[2\pi i R(x)]$, $|x| \leq 1/8$, with D_0 from Eq. (C.1) and

$$R(x) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x & x & 0 \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & -x & 0 & 0 & -x \\ 0 & 0 & 0 & x & x & 0 \end{pmatrix}; \tag{C.5}$$

the componentwise exponential Exp[·] of a matrix has been defined after Eq. (3.1).

The Fourier matrix F_6 has been embedded in a similar way into a *two*-parameter set, namely the Fourier family $F(\mathbf{x}) = F_6 \circ \mathrm{Exp}[2\pi i R(\mathbf{x})]$, where

$$R(\mathbf{x}) \equiv R(x_1, x_2) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_1 & x_2 & 0 & x_1 & x_2 \end{pmatrix}; \tag{C.6}$$

the parameters (x_1, x_2) take values in a fundamental region given by a triangle with vertices $(0, 0)$, $(1/6, 0)$ and $(1/6, 1/12)$.

Upon transposing the matrices $F(\mathbf{x})$ one obtains a different two-parameter set of Hadamard matrices, called the *transposed Fourier family* $F^T(\mathbf{x})$. It has the same fundamental region as the Fourier family.

C.3 Non-affine families

Non-affine Hadamard matrices are not parametrised in the form (3.1). The *Hermitean family* [11] provides a one-parameter example of such a set,

$$B(\theta) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x^* & -y & y & x^* \\ 1 & -x & 1 & y & z^* & t^* \\ 1 & y^* & y^* & 1 & t^* & t^* \\ 1 & y^* & z & -t & 1 & x^* \\ 1 & x & -t & t & -x & 1 \end{pmatrix}, \tag{C.7}$$

where $y = e^{2\pi i\theta}$ and $t = xyz$, with

$$\begin{aligned} z &= \frac{1+2y-y^2}{y(-1+2y+y^2)}\,, \\ x &= \frac{1+2y+y^2 \pm \sqrt{2(1+2y+2y^3+y^4)}}{1+2y-y^2}\,; \end{aligned}$$

the free parameter θ is restricted to vary within the fundamental interval $[\theta_0, 1-\theta_0]$, and the number θ_0 is defined by the condition

$$2\pi\theta_0 = \cos^{-1}\left(1-\sqrt{3}\right)\,. \tag{C.8}$$

Note that this is a smaller fundamental region than was previously known; the reduction is due to equivalences that have become apparent since the discovery of the Szöllősi family (cf. below).

Another non-affine one-parameter set of Hadamard matrices is given by the *symmetric family*

[105],

$$M(t) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & d & a & b & c \\ 1 & x & a & d & c & b \\ 1 & -x & b & c & p & q \\ 1 & -x & c & b & q & p \end{pmatrix}, \tag{C.9}$$

where $x = e^{2\pi i t}$, and the complex numbers a, b, c, d, p, q are the unique solutions of the equations

$$\begin{aligned} 1 + x + d + a + b + c &= 0\,, \\ x^2 - 2x - 2a - 2d - 1 &= 0\,, \\ 1 - x + b + c + p + q &= 0\,, \\ x^2 + 2b + 2c + 1 &= 0\,. \end{aligned} \tag{C.10}$$

In addition, one needs the fact that given a row $(r_1, \ldots, r_6)$ of a Hadamard matrix, the last two elements are determined by $\Sigma = (r_1 + r_2 + r_3 + r_4)/2$, since

$$r_{5,6} = -\Sigma \pm i \frac{\Sigma}{|\Sigma|} \sqrt{1 - |\Sigma|^2} \tag{C.11}$$

if $\Sigma \neq 0$. The fundamental region is given by $t \in [0, 1/2]$.

Finally, there is the non-affine *Szöllősi family* [139]

$$X(a,b) \equiv H(x,y,u,v) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & x^2y & xy^2 & \frac{xy}{uv} & uxy & vxy \\ 1 & \frac{x}{y} & x^2y & \frac{x}{u} & \frac{x}{v} & uvx \\ 1 & uvx & uxy & -1 & -uxy & -uvx \\ 1 & \frac{x}{u} & vxy & -\frac{x}{u} & -1 & -vxy \\ 1 & \frac{x}{v} & \frac{xy}{uv} & -\frac{xy}{uv} & -\frac{x}{v} & -1 \end{pmatrix}. \tag{C.12}$$

The entries x, y and u, v are solutions to the equations $f_\alpha = 0$ and $f_{-\alpha} = 0$, respectively, where

$$f_\alpha(z) \equiv z^3 - \alpha z^2 + \alpha^* z - 1\,, \tag{C.13}$$

and $\alpha \equiv a + ib$ is restricted to the region $\mathbb{D}$ defined by $D(\alpha) \leq 0$ and $D(-\alpha) \leq 0$, with

$$D(\alpha) \equiv |\alpha|^4 + 18|\alpha|^2 - 8\mathrm{Re}[\alpha^3] - 27\,. \tag{C.14}$$

It is possible to reduce $\mathbb{D}$ to a smaller fundamental region [15] since, firstly, the transformation $\alpha \to -\alpha$ maps Hadamard matrices to equivalent ones and, second, Eq. (C.13) is invariant under the substitutions $\alpha \to \omega\alpha$ and $y \to \omega y$ with $\omega = \exp(2\pi i/3)$. As the second transformation leaves the dephased Hadamard matrix invariant, this establishes an equivalence between the Hadamard matrices associated with points in $\mathbb{D}$ and in $\mathbb{D}'$ (which one obtains from $\mathbb{D}$ through a rotation by $2\pi/3$). As a result, the region $\mathbb{D}$ is found to consist of six equivalent sectors, and one may restrict α by

$$0 \leq \arg(\alpha) \leq \frac{\pi}{3}\,. \tag{C.15}$$

The *transposed Szöllősi family*, $X^T(a,b)$ is obtained by transposing $X(a,b)$ or by using the equivalence $H(x,y,u,v)^T \approx H(x,y,v,u)$. Fig. 3.1 illustrates that the points on the boundary of the reduced fundamental region for both $X(a,b)$ and $X^T(a,b)$ correspond to the members of the Hermitean family.

APPENDIX D

Simplification of the Fourier equations in dimension six

The conditions for a state $|v\rangle \in \mathbb{C}^6$ to be MU with respect to F_6 are given by $\mathcal{P} = 0$ where $\mathcal{P} = \{p_\pm, q_\pm, r_\pm\}$ with

$$
\begin{aligned}
p_\pm \;=\;& -5 \pm 2\,x_5 + 2\,x_4 \pm 2\,x_3 + 2\,x_2 \pm 2\,x_1 + {x_5}^2 \pm 2\,x_4x_5 + {x_4}^2 + 2\,x_3x_5 \pm 2\,x_3x_4 \\
& + {x_3}^2 \pm 2\,x_2x_5 + 2\,x_2x_4 \pm 2\,x_2x_3 + {x_2}^2 + 2\,x_1x_5 \pm 2\,x_1x_4 + 2\,x_1x_3 \pm 2\,x_1x_2 \\
& + {x_1}^2 + {y_5}^2 \pm 2\,y_4y_5 + {y_4}^2 + 2\,y_3y_5 \pm 2\,y_3y_4 + {y_3}^2 \pm 2\,y_2y_5 + 2\,y_2y_4 \pm 2\,y_2y_3 \\
& + {y_2}^2 + 2\,y_1y_5 \pm 2\,y_1y_4 + 2\,y_1y_3 \pm 2\,y_1y_2 + {y_1}^2\,, \\
q_\pm \;=\;& -5 + x_5 - x_4 - 2\,x_3 - x_2 + x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \pm \sqrt{3}y_1 + {x_5}^2 + x_4x_5 \\
& + {x_4}^2 - x_3x_5 + x_3x_4 + {x_3}^2 - 2\,x_2x_5 - x_2x_4 + x_2x_3 + {x_2}^2 - x_1x_5 - 2\,x_1x_4 \\
& - x_1x_3 + x_1x_2 + {x_1}^2 \pm \sqrt{3}y_5x_4 \pm \sqrt{3}y_5x_3 \mp \sqrt{3}y_5x_1 + {y_5}^2 \mp \sqrt{3}y_4x_5 \pm \sqrt{3}y_4x_3 \\
& \pm \sqrt{3}y_4x_2 + y_4y_5 + {y_4}^2 \mp \sqrt{3}y_3x_5 \mp \sqrt{3}y_3x_4 \pm \sqrt{3}y_3x_2 \pm \sqrt{3}y_3x_1 - y_3y_5 \\
& + y_3y_4 + {y_3}^2 \mp \sqrt{3}y_2x_4 \mp \sqrt{3}y_2x_3 \pm \sqrt{3}y_2x_1 - 2\,y_2y_5 - y_2y_4 + y_2y_3 + {y_2}^2 \\
& \pm \sqrt{3}y_1x_5 \mp \sqrt{3}y_1x_3 \mp \sqrt{3}y_1x_2 - y_1y_5 - 2\,y_1y_4 - y_1y_3 + y_1y_2 + {y_1}^2\,,
\end{aligned}
$$

and

$$\begin{aligned} r_{\pm} \;=\; & -5 - x_5 - x_4 + 2\,x_3 - x_2 - x_1 \mp \sqrt{3}y_5 \mp \sqrt{3}y_4 \pm \sqrt{3}y_2 \mp \sqrt{3}y_1 + {x_5}^2 - x_4 x_5 \\ & + {x_4}^2 - x_3 x_5 - x_3 x_4 + {x_3}^2 + 2\,x_2 x_5 - x_2 x_4 - x_2 x_3 + {x_2}^2 - x_1 x_5 + 2\,x_1 x_4 \\ & - x_1 x_3 - x_1 x_2 + {x_1}^2 \pm \sqrt{3}y_5 x_4 \mp \sqrt{3}y_5 x_3 \pm \sqrt{3}y_5 x_1 + {y_5}^2 \mp \sqrt{3}y_4 x_5 \pm \sqrt{3}y_4 x_3 \\ & \mp \sqrt{3}y_4 x_2 - y_4 y_5 + {y_4}^2 \pm \sqrt{3}y_3 x_5 \mp \sqrt{3}y_3 x_4 \pm \sqrt{3}y_3 x_2 \mp \sqrt{3}y_3 x_1 - y_3 y_5 \\ & - y_3 y_4 + {y_3}^2 \pm \sqrt{3}y_2 x_4 \mp \sqrt{3}y_2 x_3 \pm \sqrt{3}y_2 x_1 + 2\,y_2 y_5 - y_2 y_4 - y_2 y_3 + {y_2}^2 \\ & \mp \sqrt{3}y_1 x_5 \pm \sqrt{3}y_1 x_3 \mp \sqrt{3}y_1 x_2 - y_1 y_5 + 2\,y_1 y_4 - y_1 y_3 - y_1 y_2 + {y_1}^2 \,. \end{aligned} \tag{D.1}$$

Upon substituting the normalization condition $\langle v|v\rangle = 1$, or

$${x_1}^2 + {y_1}^2 + {x_2}^2 + {y_2}^2 + {x_3}^2 + {y_3}^2 + {x_4}^2 + {y_4}^2 + {x_5}^2 + {y_5}^2 = 5\,, \tag{D.2}$$

one finds

$$\begin{aligned} p_+ + p_- &= 0\,, \\ p_+ - p_- - q_+ + q_- + r_+ - r_- &= 0\,, \\ 2p_+ - 2\,p_- + q_+ - q_- - r_+ + r_- &= 0\,, \\ p_+ \pm p_- \mp r_+ - r_- &= 0\,, \end{aligned} \tag{D.3}$$

giving Eqs. (3.8).

APPENDIX E

Maple and Python programs

E.1 Maple program to construct MU vectors

In this Appendix, we given an example of the Maple program used to find all vectors mutually unbiased to a given Hadamard matrix. In particular, the Hadamard matrix is a member of the Fourier family $F(\mathbf{x})$ for some randomly generated $\mathbf{x}$ contained in the fundamental region defined in App C.2. The program can be easily modified to find vectors MU to the identity and other Hadamard matrices by changing the matrix defined by the command line starting "`B := Matrix`..." The solutions to the resulting equations are found up to a user defined accuracy, set here to be 10^{-20}. That is, the solutions satisfy the equations up to 20 decimal places. After finding all solutions, the program analyses the vectors to see if they can form a third MU basis. As explained in Section 3.2.4, in order to draw rigours conclusions dispite the numerical approximation of the solutions, we cacluate the inner products of the MU vectors at a level less than the accuracy of the solutions. In this example, we calculate the inner products up to 8 decimal places.

```
with(LinearAlgebra):  with(RootFinding):  with(RandomTools):
Seed:=randomize():
```

```
v := (Vector(5, symbol = x) + I*Vector(5, symbol = y))/sqrt(6):
seq(assume((x[j])::real, (y[j])::real), j = 1 ..  5):
var := [seq(x[k], k = 1 ..  5), seq(y[k], k = 1 ..  5)]:

uniform := proc (a, b) local f; f := rand(a*10^Digits ..  b*10^Digits)/
10^Digits; (‘@‘(evalf, f))() end proc:
E := 0:  while E = 0 do a := uniform(0, 2); b := uniform(0, 1); if 2*b < a
then E := 1 end if end do:
alpha := (1/12)*a; beta := (1/12)*b;
w := exp(I*Pi*(1/3)); z1 := exp((2*Pi*I)*alpha):  z2 := exp((2*Pi*I)*beta):
B := Matrix(6, 6, {(1, 1) = 1, (1, 2) = 1, (1, 3) = 1, (1, 4) = 1,
(1, 5) = 1, (1, 6) = 1, (2, 1) = 1, (2, 2) = w*z1, (2, 3) = w^2*z2,
(2, 4) = w^3, (2, 5) = w^4*z1, (2, 6) = w^5*z2, (3, 1) = 1, (3, 2) = w^2,
(3, 3) = w^4, (3, 4) = 1, (3, 5) = w^2, (3, 6) = w^4, (4, 1) = 1,
(4, 2) = w^3*z1, (4, 3) = z2, (4, 4) = w^3, (4, 5) = z1, (4, 6) = w^3*z2,
(5, 1) = 1, (5, 2) = w^4, (5, 3) = w^2, (5, 4) = 1, (5, 5) = w^4,
(5, 6) = w^2, (6, 1) = 1, (6, 2) = w^5*z1, (6, 3) = w^4*z2, (6, 4) = w^3,
(6, 5) = w^2*z1, (6, 6) = w*z2})/sqrt(6):

for k to 5 do eq[k] := 1/6+add(HermitianTranspose(v)[j]*B[j+1,k],j=1..5)
end do:
for k to 5 do abseq[k] := simplify(evalf(evalc(Re(eq[k])^2+Im(eq[k])^2-1/6)))
end do:
for k to 5 do eq2[k] := x[k]^2+y[k]^2-1 end do:
equations := {seq(eq2[k],k=1..5), seq(abseq[k],k=1..5)}:

Sol := Isolate(equations, var, digits = 20);
N := nops(Sol);

Vecs := Matrix(6, N, 1); for j to N do for k to 5 do Vecs[k+1, j]
:= RootOf(op(k, op(j, Sol)))+I*RootOf(op(k+5, op(j, Sol))) end do end do;
```

```
abs(evalf(HermitianTranspose(Vecs).B));
Mabs := evalf(abs(HermitianTranspose(Vecs).Vecs)/sqrt(6));
Mabsr := Matrix(N); for i to N do for j to N do Mabsr[i, j]
:= evalf(round(Mabs[i, j]*10^8)/10^8) end do end do;

count := 1; for a to N-5 do for b from a+1 to N-4 do for c from b+1 to N-3
do for d from c+1 to N-2 do for e from d+1 to N-1 do for f from e+1 to N do
if Mabsr[a, b] = 0 and Mabsr[a, c] = 0 and Mabsr[a, d] = 0 and
Mabsr[a, e] = 0 and Mabsr[a, f] = 0 and Mabsr[b, c] = 0 and Mabsr[b, d] = 0
and Mabsr[b, e] = 0 and Mabsr[b, f] = 0 and Mabsr[c, d] = 0 and
Mabsr[c, e] = 0 and Mabsr[c, f] = 0 and Mabsr[d, e] = 0 and Mabsr[d, f] = 0
and Mabsr[e, f] = 0 then BasisIndex[count] := [a, b, c, d, e, f];
count := count+1 end if end do end do end do end do end do end do:  count-1;
for i to count-1 do print(BasisIndex[i]) end do;
for j to N do if Mabsr[op(6, BasisIndex[1]), j] = 1 then print(j) end if
end do;
```

E.2 Python search for MU constellations

This Python program searches for local minima in the space of constellations $\mathcal{C}_d(v)$, where $v = [d-1, \lambda, \mu, \nu]_d$ as defined in Eqn (4.9). The program uses the phyton packages `numpy`, `scipy`, `time` and `pickle` all freely available from various sources on the internet [107, 86]. The program prompts the user to input the dimension, the constellation space, the maximum number of searches and the maximum number of hours the program is to run for. For example, to perform a search for the MU constellation $\{5, 4, 3, 2\}_6$, 1,000 times or for less than 2 hours, input the parameters `6`, `[4,3,2]`, `1000` and `2` respectively. The search results are saved to the variables `val` and `para`; `para[r]` is a vector of the parameters at the minimum value `val[r]`. The program also creates a file containing the search results and the input information.

```
from numpy import *
import minpack
```

```
from time import *
dim=input('Plese enter the dimension ')
d=float(dim)
v=array(input('Plese input constellation space in vector form [λ,μ,ν] '))
notests=input('What is the max number of tests?  ')
runfor=input('What is the max number of hours the prog should run for?  ')
t0=time()

def paravec(X,dim,v):
   # this function constructs the complex vectors from the real parameters
   # INPUTs
   # X is a column vector of real parameters
   # dim is the dimension
   # v is a row vector of the number of vectors in each of the bases.
   # Note, basis0 is the identity and is always full and the first vector
of the second basis is given.
   angles1=zeros((dim , v[0]), float) # parametrises the angles of basis 1.
   for q in range(v[0]-1):
     for p in range(dim-1):
       angles1[p+1,q+1]=X[p + q*(dim-1)]
       angles2=zeros((dim,v[1]), float) # parametrises the angles of basis 2
   for q in range(v[1]):
     for p in range(dim-1):
       angles2[p+1,q]=X[p + (q+v[0]-1)*(dim-1)]
       angles3=zeros((dim,v[2]), float) # parametrises the angles of basis 3
   for q in range(v[2]):
     for p in range(dim-1):
       angles3[p+1,q]=X[p + (q+v[0]-1+v[1])*(dim-1)]
   basis1 = exp(2j*pi*angles1)
```

```
    basis2 = exp(2j*pi*angles2)
    basis3 = exp(2j*pi*angles3)
    M=hstack((basis1,basis2,basis3))/sqrt(dim)
    return M

def sumterm(X,dim,v):
    # this function calculates the terms that go into the sum.
    # INPUTS as above
    M=paravec(X,dim,v)
    Gram = abs(dot(M.conj().T,M)) #array of all inner products.
    A=eye( sum(v) );
    for p in range(v[0]):
      for q in range(v[0] , v[0]+v[1]):
        A[p,q]=1/d;
    for p in range(v[0]+v[1]):
      for q in range(v[0]+v[1] , v[0]+v[1]+v[2]):
        A[p,q]=1/d;
    index=0
    Out=zeros(max([(sum(v)-1)*(dim-1),sum(v)*(sum(v)-1)/2]))
    for p in range(sum(v)-1):
      for q in range(p+1,sum(v)):
        Out[index]=(Gram-A)[p,q]
        index=index+1
    return Out

if (v[0]>dim):
    print 'error, the number of vectors in the bases exceeds the dimension'
else:
    count=0
    t=0
```

```
    val=[]
    para=[]
    while (t < runfor*60*60) & (count<notests):
      x0=random.rand((sum(v)-1)*(dim-1))
      (xlsq,p) = optimize.leastsq(sumterm, x0, args=(dim,v), ftol=1.49012e-16,
      \xtol=1.49012e-16, maxfev=10**8, warning=False)
    if dim==2:
      xlsq=[xlsq]
    para.append(xlsq)
    val.append(sum(sumterm(xlsq,dim,v)**2))
    count=count+1
    t=time()-t0
    val=array(val)
    print 'It took', (time()-t0), 'seconds to perform', count, 'searches.
The
    \best min was'
    print val.min(0)

import pickle
# create a dictionary of the values and the parameters
pickleresults = {'dim':dim,'PMUB vector':v,'values':val, 'parameters':para}
# now create a file with an suitable name
file = open('[directory]\\'+'dim'+`dim`+'_'+`v[0]`+`v[1]`+`v[2]`+'_'
+`count`,\'w')
pickle.dump(pickleresults,file)
file.close()
```

Bibliography

[1] R. Adamson and A. Steinberg, *Improving quantum state estimation with mutually unbiased bases*, 2008, arXiv:0808.0944.

[2] O. Albouy and M. Kibler, *SU(2) nonstandard bases: The case of mutually unbiased bases*, Symmetry, Integrability and Geometry: Methods and Applications **3** (2007), 076, arXiv:quant-ph/0701230.

[3] W. Alltop, *Complex sequences with low periodic correlations*, IEEE Transactions on Information Theory **26** (1980), 350.

[4] D. Appleby, *Sic-povms and the extended clifford group*, Journal of Mathematical Physics **46** (2005), 052107, arXiv:quant-ph/0412001.

[5] D. Appleby, H. Dang, and C. Fuchs, *Physical significance of symmetric informationally-complete sets of quantum states*, 2007, arXiv:0707.2071.

[6] P. Aravind, *Solution to the king's problem in prime dimensions*, Zeitschrift für Naturforschung **58** (2003), 2212, arXiv:quant-ph/0210007.

[7] C. Archer, *There is no generalization of known formulas for mutually unbiased bases*, Journal of Mathematical Physics **46** (2005), 022106, arXiv:quant-ph/0312204.

[8] D. Augot, M. Bardet, and J.-C. Faugere, *On formulas for decoding binary cyclic codes*, 2007, arXiv:cs/0701070.

[9] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, *A new proof for the existence of mutually unbiased bases*, Algorithmica **34** (2002), 512, arXiv:quant-ph/0103162.

[10] H. Barnum and N. Linden, *Monotones and invariants for multi-particle quantum states*, Journal of Physics A **34** (2001), 6787, arXiv:quant-ph/0103155.

[11] K. Beauchamp and R. Nicoara, *Orthogonal maximal abelian subalgebras of the* 6×6 *matrices*, 2006, arXiv:math/0609076.

[12] H. Bechmann-Pasquinucci and N. Gisin, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography*, Physical Review A **59** (1999), 4238, arXiv:quant-ph/9807041.

[13] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, *Secure communication with a publicly known key*, Acta Physica Polonica A **101** (2002), 357, arXiv:quant-ph/0111106.

[14] ———, *Secure communication with single-photon two-qubit states*, Journal of Physics A **35** (2002), L407, arXiv:quant-ph/0101066.

[15] I. Bengtsson, private communication.

[16] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-A. Larsson, W. Tadej, and K. Życzkowski, *Mubs and hadamards of order six*, Journal of Mathematical Physics **48** (2007), 052106, arXiv:quant-ph/0610161.

[17] C. Bennet and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proc. Of the IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore), 1984, p. 175.

[18] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental quantum cryptography*, Journal of Cryptology **5** (1992), 3.

[19] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Physical Review Letters **70** (1993), 1895.

[20] C. Bennett and S. Wiesner, *Communication via one- and two-particle operators on einstein-podolsky-rosen states*, Physical Review Letters **69** (1992), 2881.

[21] D. Bertsimas and M. Sim, *Robust discrete optimization and network flows*, Mathematical Programming **98** (2003), 49.

[22] T. Beth, D. Jungnickel, and H. Lenz., *Design theory*, Encyclopedia of Mathematics and Its Applications, vol. 1, Cambridge University Press, 1999.

[23] T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, Encyclopedia of Mathematics and Its Applications, vol. 2, Cambridge University Press, 1999.

[24] G. Björck and B. Saffari, *New classes of finite unimodular sequences with unimodular fourier transforms. circulant hadamard matrices with complex entries*, Comptes Rendus de l'Académie des Sciences - Series I **320** (1995), 319.

[25] M. Bourennane, A. Karlsson, and G. Björk, *Quantum key distribution using multilevel encoding*, Physical Review A **64** (2001), 012306.

[26] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. Cerf, *Quantum key distribution using multilevel encoding: Security analysis*, Journal of Physics A **35** (2002), 10065, arXiv:quant-ph/0106049.

[27] P. Boykin, M. Sitharam, P. Tiep, and P. Wocjan, *Mutually unbiased bases and orthogonal decompositions of lie algebras*, Quantum Information and Computation **7** (2005), 371, arXiv:quant-ph/0506089.

[28] F. Brandão and R. Vianna, *A robust semidefinite programming approach to the separability problem*, Physical Review A **70** (2004), 062309, arXiv:quant-ph/0405008.

[29] ———, *Separable multipartite mixed states - operational asymptotically necessary and sufficient conditions*, Physical Review Letters **93** (2004), 220503, arXiv:quant-ph/0405063.

[30] H. Briegel and R. Raussendorf, *Persistent entanglement in arrays of interacting particles*, Physical Review Letters **86** (2001), 910, arXiv:quant-ph/0004051.

[31] S. Brierley, *Quantum key distribution highly sensitive to eavesdropping*, 2009, arXiv:0910.2578.

[32] S. Brierley and S. Weigert, *Maximal sets of mutually unbiased quantum states in dimension six*, Physical Review A **78** (2008), 042312, arXiv:0808.1614.

[33] ———, *Constructing mutually unbiased bases in dimension six*, Physical Review A **79** (2009), 052316, arXiv:0901.4051.

[34] S. Brierley, S. Weigert, and I. Bengtsson, *All mutually unbiased bases in dimensions two to five*, 2009, arXiv:0907.4097.

[35] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states*, Physical Review Letters **81** (1998), 3018, arXiv:quant-ph/9805019.

[36] B. Buchberger, *An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal*, Ph.D. thesis, University of Innsbruck, 1965, English translation by M. Abramson in Journal of Symbolic Computation 41, 471 (2006).

[37] ———, *Introduction to gröbner bases*, Lecture Note Series 251: Gröbner Bases and Applications, London Mathematical Society, 1998, ed: B. Buchberger and F. Winkler.

[38] P. Butterley and W. Hall, *Numerical evidence for the maximum number of mutually unbiased bases in dimension six*, Physics Letters A **369** (2007), 5, arXiv:quant-ph/0701122.

[39] P. Butterley, A. Sudbery, and J. Szulc, *Compatibility of subsystem states*, Foundations of Physics **36** (2006), 83, arXiv:quant-ph/0407227.

[40] S. Breidbart C. Bennett, G. Brassard and S. Wiesner, *Quantum cryptography, or unforgeable subway tokens*, Advances in Cryptology: Proceedings of Crypto "82 (New York), Plenum, 1982, p. 267.

[41] A. Cabello, A. López-Tarrida, P. Moreno, and J. Portillo, *Compact set of invariants characterizing graph states of up to eight qubits*, Physical Review A **80** (2009), 012102, arXiv:0904.3551.

[42] A. Calderbank, P. Cameron, W. Kantor, and J. Seidel, *Z_4-Kerdock Codes, Orthogonal Spreads, and Extremal Euclidean Line-Sets*, Proceedings London Mathematical Society **75** (1997), 436.

[43] H. Carteret, A. Higuchi, and A. Sudbery, *Multipartite generalisation of the schmidt decomposition*, Journal of Mathematical Physics **41** (2000), 7932, arXiv.org:quant-ph/0006125.

[44] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, *Security of quantum key distribution using d-level systems*, Physical Review Letters **88** (2002), 127902, arXiv:quant-ph/0107130.

[45] S. Chaturvedi, *Aspects of mutually unbiased bases in odd-prime-power dimensions*, Physical Review A **65** (2002), 044301.

[46] M. Combescure, *Circulant matrices, gauss sums and mutually unbiased i. the prime number case*, 2007, arXiv:0710.5642.

[47] ———, *Block circulant matrices with circulant blocks, weil sums and mutually unbiased bases, ii. the prime power case*, Journal of Mathematical Physics **50** (2009), 032104, arXiv:0710.5643.

[48] A. Cooper III, *Direct solution of BCH syndrome equations*, 1990 Bilkent Conference on New Trends in Communications, Control, and Signal Processing (Bilkent University, Ankara), Elservier, 1990.

[49] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms*, Springer, 2007.

[50] D. Deutsch, *Quantum-theory, the church-turing principle and the universal quantum computer*, Proceedings of the Royal Society of London Series A **400** (1985), 97.

[51] P. Diţă, *New results on the parametrisation of complex hadamard matrices*, Journal of Physics A **37** (2002), 5355, arXiv:quant-ph/0212036.

[52] W. Diffie and M. Hellman, *New directions in cryptography,*, IEEE Transactions on Information Theory **22** (1976), 644.

[53] A. Doherty, P. Parrilo, and F. Spedalieri, *Distinguishing separable and entangled states*, Physical Review Letters **88** (2002), 187904, arXiv:quant-ph/0112007.

[54] ———, *Complete family of separability criteria*, Physical Review A **69** (2004), 022308, arXiv:quant-ph/0308032.

[55] T. Durt, *About mutually unbiased bases in even and odd prime power dimensions*, Journal of Physics A **38** (2005), 5267, arXiv.org:quant-ph/0409090.

[56] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, *Complete hierarchies of efficient approximations to problems in entanglement theory*, Physical Review A **70** (2004), 062317, arXiv:quant-ph/0407135.

[57] A. Ekert, *Quantum cryptography based on bell's theorem,*, Physical Review Letters **67** (1991), 661.

[58] A. Ekert, B. Huttner, M. Palma, and A. Peres, *Eavesdropping on quantum-cryptographical systems*, Physical Review A **50** (1994), 1047.

[59] B.-G. Englert and Y. Aharonov, *The mean king's problem: prime degrees of freedom*, Physics Letters A **284** (2001), 1, arXiv:quant-ph/0101134.

[60] D. Enzer, P. Hadley, R. Hughes, C. Peterson, and P. Kwiat, *Entangled-photon six-state quantum cryptography*, New Journal of Physics **4** (2002), 45.

[61] Å. Ericsson, unpublished, 2004.

[62] ———, *Exploring the set of quantum states*, Ph.D. thesis, Department of Physics, Stockholm University, 2009.

[63] U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques*, Reviews of Modern Physics **29** (1957), 74.

[64] J.-C. Faugère, *A new efficient algorithm for computing gröbner bases (f4)*, Journal of Pure and Applied Algebra **139** (1999), 61.

[65] J.-C. Faugère and A. Joux., *Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using gröbner bases*, Crypto 2003 (2003), 44.

[66] J.-C. Faugère, G. Moroz, F. Rouillier, and M. El Din, *Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities*, ISSAC '08: Proceedings of the twenty-first international symposium on Symbolic and algebraic computation (New York, USA), ACM, 2008, p. 79.

[67] C. Fuchs, N. Gisin, R. Griffiths, C.-S. Niu, and A. Peres, *Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy*, Physical Review A **56** (1997), 1163, arXiv:quant-ph/9701039.

[68] C. Fuchs and M. Sasaki, *Squeezing quantum information through a classical channel: Measuring the "quantumness" of a set of quantum states*, Quantum Information and Computation **3** (2003), 377, arXiv:quant-ph/0302092.

[69] C. Fuchs and R. Schack, *Quantum-bayesian coherence*, 2009, arXiv:0906.2187.

[70] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Reviews of Modern Physics **74** (2002), 145, arXiv:quant-ph/0101098.

[71] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics **30** (2009), 246.

[72] M. Grassl, *On sic-povms and mubs in dimension 6*, Proceedings: ERATO Conference on Quantum Information Science (Tokyo) (J. Gruska, ed.), 2004, arXiv:quant-ph/0406175, p. 60.

[73] L. Gurvits, *Classical deterministic complexity of edmonds problem and quantum entanglement*, Proceedings of the Thirty-Fifth ACM Symposium on Theory of Computing (New York), ACM, 2003, arXiv:quant-ph/0303055, p. 10.

[74] U. Haagerup, *Orthogonal maximal abelian *- subalgebras of the $n \times n$ matrices and cyclic n-roots*, Proceedings: Operator Algebras and Quantum Field Theory (Rome) (S. Doplicher, ed.), 1996, p. 296.

[75] W. Hall, *Compatibility of subsystem states and convex geometry*, Physical Review A **75** (2007), 032102, arXiv:quant-ph/0610031.

[76] M. Hein, J. Eisert, and H. Briegel, *Multiparty entanglement in graph states*, Physical Review A **69** (2004), 062311, arXiv:quant-ph/0307130.

[77] M. Hellman, B. Diffie, and R. Merkle, *Cryptographic apparatus and method*, US Patent 4200770, 1980.

[78] D. Henrion, J.-B. Lasserre, and J. Loefberg, *GloptiPoly 3: Moments, optimization and semidefinite programming v3.4*, 2008, available at http://www.laas.fr/~henrion/software/gloptipoly3/.

[79] J. Hilling and A. Sudbery, *The geometric measure of multipartite entanglement and the singular values of a hypermatrix*, 2009, arXiv:0905.2094.

[80] M. Horodecki, P. Horodecki, and R. Horodecki, *Separability of mixed states: Necessary and sufficient conditions*, Physics Letters A **223** (1996), 1, arXiv:quant-ph/9605038.

[81] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Reviews of Modern Physics **81** (2009), 865, arXiv:quant-ph/0702225.

[82] B. Huttner and A. Ekert, *Information gain in quantum eavesdropping*, Journal of Modern Optics **41** (1994), 2455.

[83] I. Ivanović, *Geometrical description of quantal state determination*, Journal of Physics A **14** (1981), 3241.

[84] P. Jaming, M. Matolcsi, P. Mora, F. Szöllősi, and M. Weiner, *A generalized pauli problem and an infinite family of mub-triplets in dimension 6*, Journal of Physics A **42** (2009), 245305, arXiv:0902.0882.

[85] Z. Ji, J. Chen, Z. Wei, and M. Ying, *The LU-LC conjecture is false*, 2007, arXiv:0709.1266.

[86] E. Jones, T. Oliphant, and P. Peterson et Al., *SciPy: Open source scientific tools for python 4.0 (version 2.5)*, http://www.scipy.org/.

[87] M. Khan, M. Murphy, and A. Beige, *High error-rate quantum key distribution for long-distance communication*, New Journal of Physics **11** (2009), 063043, arXiv:0901.3909.

[88] M. Kibler and M. Planat, *A $SU(2)$ recipe for mutually unbiased bases*, International Journal of Modern Physics B **20** (2006), 1802, arXiv:quant-ph/0601092.

[89] A. Klappenecker and M. Röetteler, *Constructions of mutually unbiased bases*, Lecture Notes in Computer Science **2948** (2004), 262, arXiv:quant-ph/0309120.

[90] A. Klappenecker, M. Rötteler, I. Shparlinski, and A. Winterhof, *On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states*, Journal of Mathematical Physics **46** (2005), 082104, arXiv:quant-ph/0503239.

[91] M. Kojima and L. Tunçel, *Cones of matrices and successive convex relaxations of nonconvex sets*, SIAM Journal on Optimization **10** (2000), 750.

[92] J. Korbicz, F. Hulpke, A. Osterloh, and M. Lewenstein, *A statistical-mechanical description of quantum entanglement*, Journal of Physics A **41** (2008), 375301, arXiv:0704.3357.

[93] A. Kostrikin and P. Tiep, *Orthogonal decompositions and integral lattices*, De Gruyter Expositions in Mathematics 15, Walter de Gruyter, Berlin, 1994.

[94] C. Lam, L. Thiel, and S. Swiercz, *The non-existence of finite projective planes of order 10*, Canadian Journal of Mathematics **41** (1989), 1117.

[95] J. Lasserre, *Global optimization with polynomials and the problem of moments*, SIAM Journal on Optimization **11** (2001), 796.

[96] ———, *A semidefinite programming approach to the generalized problem of moments*, Mathematical Programming **112** (2008), 65.

[97] J. Lawrence, C. Brukner, and A. Zeilinger, *Mutually unbiased binary observable sets on n qubits*, Physics Review A **65** (2002), 032320, arXiv:quant-ph/0104012.

[98] D. Lazard, *Stewart platforms and gröbner basis*, Proceedings of Advances in Robotics Kinematics, 1992, p. 136.

[99] K. Levenberg, *A method for the solution of certain non-linear problems in least squares*, Quarterly of Applied Mathematics **2** (1944), 164.

[100] R. Lidl and H. Niederreiter, *Finite fields*, Addison Wesley, Reading, MA, 1983.

[101] Y. Lim and A. Beige, *Multiphoton entanglement through a bell-multiport beam splitter*, Physical Review A **71** (2005), 062311, arXiv:quant-ph/0406047.

[102] *Maple 11*, Waterloo Maple Inc. Waterloo, Ontario, Canada.

[103] D. Marquardt, *An algorithm for least-squares estimation of nonlinear parameters*, SIAM Journal on Applied Mathematics **11** (1963), 431.

[104] L. Mathiesen, *Computation of economic equilibria by a sequence of linear complementarity problems*, Mathematical Programming Studies **23** (1985), 144.

[105] M. Matolcsi and F. Szöllősi, *Towards a classification of* 6×6 *complex hadamard matrices*, 2007, arXiv:math/0702043.

[106] D. Mayers, *Unconditional security in quantum cryptography,*, Journal of the ACM **48** (2001), 351, arXiv:quant-ph/9802025.

[107] J. Millman, E. Jones, R. Kern, T. Oliphant, and Et. Al. S. Van der Walt, *Numpy: Package for scientific computing with python (version 1.3)*, http://numpy.scipy.org/.

[108] G. Moorhouse, *The 2-transitive complex hadamard matrices*, http://www.uwyo.edu/ moorhouse/pub, 2001.

[109] M. Van den Nest, J. Dehaene, and B. De Moor, *Local invariants of stabilizer codes*, Physical Review A **70** (2004), 032323, arXiv:quant-ph/0404106.

[110] M. Van den Nest, J. Dehaene, and B. De Moor, *Finite set of invariants to characterize local clifford equivalence of stabilizer states*, Physical Review A **72** (2005), 014307, arXiv:quant-ph/0410165.

[111] ———, *Local unitary versus local clifford equivalence of stabilizer states*, Physical Review A **71** (2005), 062323, arXiv:quant-ph/0411115.

[112] Y. Nesterov, *Squared functional systems and optimization problems*, High Performance Optimization (Dordrecht) (K. Roos, T. Terlaky, and S. Zhang, eds.), Kluwer, 2000.

[113] M. Nielsen and I. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[114] W. Niu and D. Wang., *Algebraic approaches to stability analysis of biological systems*, Mathematics in Computer Science **1** (2008), 507.

[115] A. Peres, *Quantum theory: Concepts and methods*, Kluwer Academic Publishers, 1995.

[116] A. Peres, *Collective tests for quantum nonlocality*, Physical Review A **54** (1996), 2685.

[117] S. Phoenix, *Quantum cryptography without conjugate coding*, Physical Review A **48** (1993), 96.

[118] S. Popescu and D. Rohrlich, *Quantum nonlocality as an axiom*, Foundations of Physics **24** (1994), 379.

[119] R. Raussendorf and H. Briegel, *A one-way quantum computer*, Physical Review Letters **86** (2001), 5188.

[120] M. Reck, A. Zeilinger, H. Bernstein, and P. Bertani, *Experimental realization of any discrete unitary operator*, Physical Review Letters **73** (1994), 58.

[121] R Rivest, A Shamir, and L Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM **21** (1978), 120.

[122] J. Romero, G. Björk, A. Klimov, and L. Sánchez-Soto, *Structure of the sets of mutually unbiased bases for n qubits*, Physical Review A **72** (2005), 062310, arXiv:quant-ph/0508129.

[123] F. Rouillier, *Solving zero-dimensional systems through the rational univariate representation*, Journal of Applicable Algebra in Engineering, Communication and Computing **9** (1999), 433.

[124] *SALSA: Solvers for algebraic systems and applications*, software available from http://fgbrs.lip6.fr/salsa/.

[125] M. Saniga, M. Planat, and H. Rosu, *Mutually unbiased bases and finite projective planes*, Journal of Optics B **6** (2004), L19, arXiv:math-ph/0403057.

[126] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations*, Physical Review Letters **92** (2004), 057901, arXiv:quant-ph/0211131.

[127] D. Schlingemann, *Cluster states, algorithms and graphs*, Quantum Information and Computation **4** (2004), 287, arXiv:quant-ph/0305170.

[128] D. Schlingemann and R. Werner, *Quantum error-correcting codes associated with graphs*, Physical Review A **65** (2001), 012308, arXiv:quant-ph/0012111.

[129] E. Schrödinger, *Discussion of probability relations between separated systems*, Mathematical Proceedings of the Cambridge Philosophical Society **31** (1935), 555.

[130] J. Schwinger, *Unitary operator bases*, Proceedings of the National Academy of Sciences **46** (1960), 560.

[131] C. Shannon, *Communication theory of secrecy systems*, Bell System Technical Journal **28** (1949), 656.

[132] A. Shimony, *Degree of entanglement*, Annals of the New York Academy of Sciences **755** (1995), 675.

[133] N. Shor, *Quadratic optimization problems*, Soviet Journal of Circuits and Systems Sciences **25** (1987), 1.

[134] P. Shor, *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings of the 35th Annual Symposium on Foundations of Computer Science (Santa Fe), 1995, arXiv:quant-ph/9508027, p. 124.

[135] P. Shor and J. Preskill, *Simple proof of security of the BB84 quantum key distribution protocol*, Physical Review Letters **85** (2000), 441, arXiv:quant-ph/00030004.

[136] A. Skinner, V. Newell, and R. Sanchez, *Unbiased bases (hadamards) for 6-level systems: Four ways from fourier*, Journal of Mathematical Physics **50** (2009), 012107, arXiv:0810.1761.

[137] L. Skowronek and K. Życzkowski, *Positive maps, positive polynomials and entanglement witnesses*, Journal of Physics A **42** (2009), 325302, arXiv:0903.3042.

[138] J. Strum, *Using SeDuMi: A matlab toolbox for optimization over symmetric cones*, Optimization Methods and Software **11** (1999), 625, available at www.sedumi.ie.lehigh.edu/.

[139] F. Szöllősi, *A two-parameter family of complex hadamard matrices of order 6 induced by hypocycloids*, 2008, arXiv:0811.3930.

[140] On-Line Catalgue of Known Hadamard Matrices Maintained by W. Tadej and K. Życzkowski at http://chaos.if.uj.edu.pl/ karol/hadamard/.

[141] W. Tadej and K. Życzkowski, *A concise guide to complex hadamard matrices*, Open Systems and Information Dynamics **13** (2006), 133, arXiv:quant-ph/0512154.

[142] L. Tamaryan, D. Park, J.-W. Son, and S. Tamaryan, *Geometric measure of entanglement and shared quantum states*, Physical Review A **78** (2008), 032304, arXiv:0803.1040.

[143] T. Tao, *Fuglede's conjecture is false in 5 and higher dimensions*, Mathematical Research Letters **11** (2004), 251, arXiv:math/0306134.

[144] L. Vaidman, Y. Aharonov, and D. Albert, *How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle*, Physical Review Letters **58** (1987), 1385.

[145] L. Vandenberghe and S. Boyd, *Semidefinite programming*, SIAM Review **38** (1996), no. 1, 49–95.

[146] T.-C. Wei and P. Goldbart, *Geometric measure of entanglement and applications to bipartite and multipartite quantum states*, Physical Review A **68** (2003), 042307, arXiv:quant-ph/0307219.

[147] M. Weiner, *A gap for the maximum number of mutually unbiased bases*, 2009, arXiv:0902.0635.

[148] S. Wiesner, *Conjugate coding*, SIGACT News **15** (1983), 78, originally written circa 1970.

[149] P. Wocjan and T. Beth, *New construction of mutually unbiased bases in square dimensions*, Quantum Information and Computation **5** (2005), 93, arXiv:quant-ph/0407081.

[150] W. Wootters and B. Fields, *Optimal state-determination by mutually unbiased measurements*, Annals of Physics **191** (1989), 363.

[151] W. Wootters and W. Zurek, *a single quantum cannot be cloned*, Nature **299** (1982), 802.

[152] G. Zauner, *Quantendesigns. grundzuge einer nichtkommunikativen designtheorie.*, Ph.D. thesis, University of Wien, 1999.

[153] M. Żukowski, A. Zeilinger, and M. Horne, *Realizable higher-dimensional two-particle entanglements via multiport beam splitters*, Physical Review A **55** (1997), 2564.