ON MUTUALLY UNBIASED BASES

THOMAS DURT
TENA-TONA Free University of Brussels, Pleinlaan 2, B-1050 Brussels, Belgium
thomdurt@vub.ac.be

BERTHOLD-GEORG ENGLERT
Centre for Quantum Technologies, National University of Singapore, Singapore 117543
Department of Physics, National University of Singapore, Singapore 117542
ctqebg@nus.edu.sg, phyebg@nus.edu.sg

INGEMAR BENGTSSON
Stockholms Universitet, Fysikum, Roslagstullsbacken 21, 106 91 Stockholm, Sweden
ingemar@physto.se

KAROL ŻYCZKOWSKI
Instytut Fizyki Uniwersytetu Jagiellońskiego, ul. Reymonta 4, 30-059 Kraków, Poland
and Centrum Fizyki Teoretycznej PAN, Al. Lotników 32/44, 02-668 Warszawa, Poland
karol@tatry.if.uj.edu.pl

Received xx XXXX 20xx

Mutually unbiased bases for quantum degrees of freedom are central to all theoretical investigations and practical exploitations of complementary properties. Much is known about mutually unbiased bases, but there are also a fair number of important questions that have not been answered in full as yet. In particular, one can find maximal sets of $N+1$ mutually unbiased bases in Hilbert spaces of prime-power dimension $N = p^{\mathrm{M}}$, with p prime and M a positive integer, and there is a continuum of mutually unbiased bases for a continuous degrees of freedom, such as motion along a line. But not a single example of a maximal set is known if the dimension is another composite number ($N = 6, 10, 12, \dots$).

In this review, we present a unified approach in which the basis states are labeled by numbers $0, 1, 2, \dots, N-1$ that are both elements of a Galois field and ordinary integers. This dual nature permits a compact systematic construction of maximal sets of mutually unbiased bases when they are known to exist but throws no light on the open existence problem in other cases. We show how to use the thus constructed mutually unbiased bases in quantum-informatics applications, including dense coding, teleportation, covariant cloning, and state tomography, all of which rely on an explicit set of maximally entangled states (generalizations of the familiar two–q-bit Bell states) that are defined with the aid of the mutually unbiased bases.

Further, we exploit the one-to-one correspondence between unbiased bases and the complex Hadamard matrices that turn the bases into each other. This offers a direct link to the mathematics of finite affine planes with the ultimate hope, presently not fulfilled, that open questions about mutually unbiased bases can be related to open questions about Hadamard matrices or affine planes, in particular the notorious existence problem

for dimensions that are not a power of a prime.

The Hadamard-matrix approach is instrumental in the very recent advance, surveyed here, of our understanding of the $N = 6$ situation. All evidence indicates that a maximal set of seven mutually unbiased bases does not exist — one can find no more than three pairwise unbiased bases — although there is presently no clear-cut demonstration of the case.

Keywords: Mutually unbiased bases, complex Hadamard matrices, generalized Bell states

Contents

Acronyms

MU	mutually unbiased
MUB	mutually unbiased bases
MUHM	mutually unbiased Hadamard matrices
POVM	positive operator valued measure
SIC	symmetric informationally complete

Introduction

Two orthonormal bases of a Hilbert space are said to be *mutually unbiased* (MU) if the transition probabilities from each state in one basis to all states of the other basis are the same irrespective of which pair of states is chosen. Put differently, if the physical system is prepared in a state of the first basis, then all outcomes are equally probable when we conduct a measurement that probes for the states of the second basis. This situation is symmetrical, it does not matter from which of the two bases we choose the prepared state and which is the other basis that is measured: unbiasedness of bases is a mutual property, possessed jointly by both bases. Familiar examples are the bases of position and momentum eigenstates for a particle moving along a line, and the spin states of a spin-$\frac{1}{2}$ particle for two perpendicular directions.

When the Hilbert space dimension N is a prime power, $N = p^{\mathrm{M}}$, there exist sets of $N + 1$ mutually unbiased bases (MUB). These sets are maximal in the sense that it is not possible to find more than $N + 1$ MUB in any N-dimensional Hilbert space, there is simply no room for the $(N + 2)$th basis. Such a maximal set of MUB is also complete because when we know all the probabilities of transition of a given quantum state towards the states of the bases of this set — exceptional situations aside, there are $(N + 1)(N - 1) = N^2 - 1$ independent probabilities — we can reconstruct the statistical operator that characterizes this quantum state; in other words we can perform full tomography or complete quantum state determination.

The existence of a maximal set of MUB for $N = p^{\mathrm{M}}$ is demonstrated by an explicit construction, not by an abstract existence proof. All known constructions rely on the fact that N is the power of a prime and, therefore, they say nothing about other dimensions, of which $N = 6$ is the smallest one and also the one that has been studied most intensely. At present, there is a widely shared conviction that one cannot have a maximal set of seven MUB for $N = 6$ and that the largest sets of MUB have no more than three bases. This conviction is strongly founded in a solid body of evidence but, strictly speaking, it is an unproven conjecture.

This situation is reminiscent of seemingly similar existence questions about finite affine planes, Graeco-Latin squares, and related geometrical structures where prime-power dimensions also play a privileged role. As suggestive as these similarities may be, there is, however, no known connection as yet between the two kinds of existence problems.

There is a plethora of applications whenever maximal sets of MUB are available, in particular when the physical system is composed of many q-bits ($N = 2^{\mathrm{M}}$), the building blocks of devices for quantum information processing. Not surprisingly, then, the rise of quantum information science has triggered fresh interest in MUB and, as a consequence, our knowledge about MUB and their applications is much richer now. But the various facts are scattered over a large number of publications, and the many pieces of the puzzle do not readily fit together and compose a uniform picture.

We are here reviewing the state of affairs in an attempt to offer a unified view, with emphasis on both the structural properties of MUB and their use in quantum-information applications. As in all constructions of MUB in prime power dimension, a crucial element is a finite commutative division ring — a Galois field of N elements.[a] Finite fields with N elements exist if and only if N is a power of a prime, and the mathematical properties of Galois fields are exploited in all constructions of MUB. Modifications of these constructions in the absence of a finite field do not yield maximal sets of MUB for other dimensions.

[a] A *ring* is a set that is closed under two operations: addition and multiplication. They obey the usual rules, associativity and commutativity of both operations, the distributive law, existence of a unique neutral element 0 for the addition and a neutral element 1 for the multiplication. A *field*, or division ring, is a ring with multiplicative inverses for every nonzero element.

We begin with a brief survey of elements of quantum kinematics in Sec. 1. The legacy of Weyl and Schwinger: the notion of complementary observables and their algebraic completeness, the MUB associated with them, and the $N \to \infty$ limit of continuous degrees of freedom — all these are central to the story told in Sec. 1.1. It is supplemented by remarks on the Heisenberg–Weyl group of unitary operators and the related Clifford group as well as, in Sec. 1.2, a geometrically motivated "measure of unbiasedness" of two bases, a distance in a real euclidean vector space.

Section 2 deals with the construction of a maximal set of MUB in prime power dimension, $N = p^{\mathrm{M}}$, systematically treated as a composite system of M p-dimensional subsystems. For the purpose of introducing some notational conventions, but also for the benefit of the typical working physicist for whom Galois fields are hardly the daily bread, we recall the most important and most relevant properties of Galois fields in Sec. 2.1. We are making extensive use of a formalism in which the numbers $0, 1, 2, \ldots, N-1$ play a dual role — they are elements of a Galois field, but also ordinary integers. This somewhat unconventional approach enables us to give a compact, transparent construction of a maximal set of MUB in Sec. 2.2–2.4. A fitting version of the discrete Heisenberg–Weyl group, also known as the generalized Pauli group, is an important tool for the construction; its abelian subgroups define the MUB. In passing, we establish the contact between these MUB and the complementary observables of the Weyl–Schwinger methodology (Sec. 2.5).

The survey of applications of the maximal set of MUB in Sec. 3 begins with the construction of a complete set of maximally entangled states, the analogs of the familiar Bell states of two–q-bit systems, in Sec. 3.1. After brief accounts of their use for quantum dense coding (Sec. 3.2) and teleportation (Sec. 3.3), we discuss in Sec. 3.4 how the generalized Bell states facilitate quantum cryptography and eavesdropping with the aid of covariant cloning machines and comment on the role of the Heisenberg–Weyl operators in error correction.

The prime-power version of the so-called Mean King's problem (Sec. 4.1) opens the section on quantum state tomography. It is, in fact, very closely related to the discrete analog of Wigner's continuous phase space function which — jointly with its Fourier partner, the analog of Weyl's characteristic function — is the subject matter of Sec. 4.2. We remark on the covariance of the Wigner-type operator basis and discuss the $N \to \infty$ limit of continuous degrees of freedom. The relation to finite affine planes in Sec. 4.3 provides further insights into the underlying geometry.

Section 5 is devoted to the matrices that transform pairs of MUB into each other: the complex Hadamard matrices. Pairs of bases may be equivalent or not, in the sense that one can map the basis states of one pair on those of the other pair by a unitary transformation in conjunction with permutations of the basis states (Sec. 5.1). The equivalence of triplets of MUB are more difficult to check (Sec. 5.2). Mutually unbiased Hadamard matrices (MUHM) are encountered when there are more than two MUB. Accordingly, one can investigate sets of MUB by studying the corresponding sets of MUHM, and vice versa. Since all Hadamard matrices of size $N \leq 5$ have been classified (Sec. 5.3), all sets of MUB are known for $N < 6$

(Sec. 5.7). The situation is not so clear, and thus more interesting, for $N = 6$; we report what is known about the families of 6×6 Hadamard matrices in Sec. 5.5, after a general discussion of affine families and tensor products in Sec. 5.4, and we deal with MUB for $N = 6$ in Secs. 5.8–5.10. Hadamard matrices for $N > 6$ get their share of attention in Sec. 5.6.

We close with a brief summary and concluding remarks (Sec. 6) and provide some additional technical details in three appendixes. The standard set of MUHM for prime dimension is given in Appendix A, and a prime-distinguishing function related to this standard set is introduced in Appendix B. Finally, Appendix C deals with MUB for the two–q-bit case of $N = 4$.

1. Elements of quantum kinematics

1.1. *The Weyl–Schwinger legacy*

1.1.1. *Complementary observables and mutually unbiased bases*

As emphasized by Bohr in his 1927 Como lecture,[1] quantum systems have properties that are *complementary*: equally real but mutually exclusive. If one such property is known accurately, then the complementary property is completely unknown. Here, "known accurately" means that the outcome of a measurement can be predicted with certainty, whereas "completely unknown" means that all outcomes are equally likely — the two properties are maximally incompatible. Familiar examples are the position and momentum of a particle moving along a line, and the x and z spin components of a spin-$\frac{1}{2}$ object. These are, in fact, the extreme cases of an infinite degree of freedom and a binary degree of freedom — the latter being the "q-bit" of recent quantum information terminology.

Intermediate are "q-nits," N-dimensional quantum degrees of freedom ($N > 1$), for which the measurement of a physical property can have at most N different outcomes. Following Weyl[2,3] and Schwinger,[4–6] we call a pair of observables, A and B, complementary if their eigenvalues are not degenerate (there is the full count of N different possible measurement results) and the sets of normalized kets $|a_j\rangle$ and $|b_k\rangle$ that describe states with predictable measurement outcomes for A and B, respectively, are MU,

$$\big|\langle a_j|b_k\rangle\big|^2 = \frac{1}{N} \quad \text{for all } j,k = 0,1,\ldots,N-1\,. \tag{1.1}$$

The important detail is not the value on the right, which is implied by the normalization to unit total probability, but that the transition probabilities on the left do not depend on the quantum numbers a_j and b_k.[b]

Technically speaking, A and B are normal operators[c] and $|a_j\rangle$, $|b_k\rangle$ are their

[b] In fact, there can be different right-hand sides for infinite degrees of freedom, when normalization is more subtle; see Sec. 1.1.8. We will mostly deal with finite degrees of freedom.

[c] A normal operator A commutes with its adjoint $A^\dagger$: $AA^\dagger = A^\dagger A$, and can be regarded either as a function of a more fundamental hermitian operator or as a function of a unitary operator.

eigenkets, which make up two bases that are orthonormal and complete,

$$\langle a_j|a_k\rangle = \delta_{j,k} = \langle b_j|b_k\rangle\,, \qquad \sum_{j=0}^{N-1} |a_j\rangle\langle a_j| = \mathbf{1} = \sum_{k=0}^{N-1} |b_k\rangle\langle k_k|\,, \tag{1.2}$$

where $\mathbf{1}$ is the identity operator. We recognize that the complementarity of A and B is in fact a property of their respective eigenket bases. The particular eigenvalues are irrelevant, we just need to know that they are not degenerate. And so we can shift the focus from the pair A, B of complementary observables to the pair $\{|a_j\rangle\}, \{|b_k\rangle\}$ of MUB.

Whenever is it expedient to be specific about the observables associated with a basis, we will follow the guidance of Weyl and Schwinger[d] and choose a unitary operator to represent the physical quantity. In the present context, these will be cyclic operators with period N,

$$A^N = \mathbf{1}\,, \quad B^N = \mathbf{1}\,, \tag{1.3}$$

with products of fewer than N factors not equaling the identity. The eigenvalues of A and B are then the N different Nth roots of unity,

$$A|a_j\rangle = |a_j\rangle\gamma_N^j\,, \quad B|b_k\rangle = |b_k\rangle\gamma_N^k \quad \text{with } \gamma_N = \mathrm{e}^{\mathrm{i}2\pi/N}\,. \tag{1.4}$$

That these cyclic operators are a pair of complementary operators can be stated as

$$\frac{1}{N}\mathrm{tr}\big\{A^m B^n\big\} = \delta_{m,0}\delta_{n,0} \qquad \text{for } m, n = 0, 1, \ldots, N-1\,, \tag{1.5}$$

which is the operator version of (1.1). Indeed, (1.1) and (1.5) imply each other.[8]

1.1.2. *Existence of a basic pair of complementary observables*

The first question we address is whether there always is a pair of complementary observables for each quantum degree of freedom. The affirmative answer begins with selecting an orthonormal reference basis $|0\rangle$, $|1\rangle$, …, $|N-1\rangle$ — we will refer to it as the *computational basis* from Sec. 2.2 onwards. Then we define a second orthonormal basis $|\underline{0}\rangle, |\underline{1}\rangle, \ldots, |\underline{N-1}\rangle$ by means of the discrete quantum Fourier transformation,

$$|\underline{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle\gamma_N^{-jk}\,, \tag{1.6}$$

so that

$$\langle \underline{j}|k\rangle = \frac{1}{\sqrt{N}}\gamma_N^{jk} \quad \text{for } j, k = 0, 1, \ldots, N-1 \tag{1.7}$$

by construction — the two bases are MU, indeed.

[d] A brief account of the history of the subject can be found in Ref. 7.

In analogy with the Pauli operators σ_x and σ_z, we introduce the cyclic operators X and Z in accordance with

$$X|\underline{j}\rangle = |\underline{j}\rangle\gamma_N^j\,, \quad X^N = \mathbf{1} \qquad \text{and} \qquad Z|k\rangle = |k\rangle\gamma_N^k\,, \quad Z^N = \mathbf{1}\,. \tag{1.8}$$

As an immediate consequence of (1.7), we note that X and Z are unitary shift operators that permute the kets or bras of the respective other basis cyclically,

$$X|k\rangle = |k+1\rangle \quad \text{for } k = 0, 1, \ldots, N-2\,, \qquad X|N-1\rangle = |0\rangle \tag{1.9}$$

as well as

$$\langle\underline{j}|Z = \langle\underline{j+1}| \quad \text{for } j = 0, 1, \ldots, N-2\,, \qquad \langle\underline{N-1}|Z = \langle\underline{0}|\,, \tag{1.10}$$

and (1.5) holds for $(A, B) = (X, Z)$, as it must. The fundamental Weyl commutation rule $ZX = \gamma_N XZ$ follows. It is the analog of the familiar $N = 2$ identity $\sigma_z\sigma_x = -\sigma_x\sigma_z$ and is more generally, and more usefully, stated as

$$X^m Z^n = \gamma_N^{-mn} Z^n X^m\,, \tag{1.11}$$

valid for all integer values of m and n, both positive and negative.

1.1.3. *Algebraic completeness of the basic pair of operators*

The second question, which also has an affirmative answer, is whether the pair X, Z of complementary observables parameterizes the degree of freedom completely. Put differently: Are all other operators functions of X and Z?

As a first step, we observe that the projectors onto the respective eigenstates are polynomials of X or Z,

$$\begin{aligned} \delta_{X,\gamma_N^j} &= |\underline{j}\rangle\langle\underline{j}| = \frac{1}{N}\sum_{n=0}^{N-1}\left(\gamma_N^{-j}X\right)^n\,, \\ \delta_{Z,\gamma_N^k} &= |k\rangle\langle k| = \frac{1}{N}\sum_{m=0}^{N-1}\left(\gamma_N^{-k}Z\right)^m\,, \end{aligned} \tag{1.12}$$

where the Kronecker delta symbols are to be understood in the usual sense of an operator function, as exemplified by

$$f(Z) = \sum_{k=0}^{N-1} |k\rangle f\big(\gamma_N^k\big)\langle k|\,. \tag{1.13}$$

The second step in writing an arbitrary operator F as a function of X and Z is to exploit the completeness of the two bases,

$$F = \sum_{j,k} |\underline{j}\rangle\langle\underline{j}|F|k\rangle\langle k| = \sum_{j,k} \delta_{X,\gamma_N^j} f_{j,k} \delta_{Z,\gamma_N^k} \quad \text{with} \quad f_{j,k} = \frac{\langle\underline{j}|F|k\rangle}{\langle\underline{j}|k\rangle}\,, \tag{1.14}$$

where the denominator is assuredly nonvanishing.[e] This answers the second question by giving an explicit expression for F as a polynomial of X and Z, here written in a unique way as an XZ-ordered function: in products, all X operators stand to the left of all Z operators. Of course, quite analogously, we can also write F in a unique ZX-ordered form — as an example recall the equivalence of the XZ-ordered operator on the left of (1.11) with the ZX-ordered product on the right. In summary, there is not just one function of X and Z that equals the given operator F, there are many such functions.

The lesson of these considerations is that the pair X, Z is algebraically complete, there are no operators that are not linear combinations of products of powers of X and Z. Accordingly, we can phrase Bohr's Principle of Complementarity, the fundamental principle of quantum kinematics, in the following technical terms: *For each degree of freedom the dynamical variables are a pair of complementary observables.*[10] For a textbook discussion, see Ref. 11.

1.1.4. *The Heisenberg–Weyl group; the Clifford group*

Supplemented with powers of γ_N, the XP-ordered products that are implicit in (1.14),

$$Y_{l,m,n} = \gamma_N^l X^m Z^n \quad \text{with} \quad l, m, n = 0, 1, \ldots, N-1\,, \tag{1.15}$$

make up the *Heisenberg–Weyl group* of unitary operators, also called the generalized Pauli group, with operator multiplication as the composition,

$$Y_{l_1,m_1,n_1} Y_{l_2,m_2,n_2} = Y_{l_1+l_2-n_1 m_2, m_1+m_2, n_1+n_2}\,, \tag{1.16}$$

where we understand all subscripts as integers modulo N, and the same convention applies in

$$Y_{l,m,n}^{-1} = Y_{l,m,n}^\dagger = Y_{mn-l,-m,-n}\,. \tag{1.17}$$

We could also use the ZX-ordered products to enumerate the group elements, or consider the set of all products of powers of X and Z without additional powers of γ_N as phase factors. Each recipe gives the same set of N^3 unitary operators, but double counting of group elements is most easily avoided when the ordered products are used. In the $N = 2$ example of $X = \sigma_x$ and $Z = \sigma_z$, the eight group elements are $\pm\mathbf{1}$, $\pm\sigma_x$, $\pm\sigma_z$, and $\pm\sigma_x\sigma_z = \mp \mathrm{i}\sigma_y$. If we use the standard real 2×2 Pauli matrices to represent σ_x and σ_z, then all eight unitary operators of the q-bit Heisenberg–Weyl group are represented by real matrices.

In addition to this notion of the Heisenberg–Weyl group as a group of unitary operators that can be multiplied, there is also the notion of the Heisenberg–Weyl group as a group of unitary transformations

$$F \to YFY^\dagger \tag{1.18}$$

[e] Numbers of the form of $f_{j,k}$ are known as "weak values" of F in the context of "weak measurements."[9]

that can be composed. There is no difference in (1.18) between $Y = X^n Z^m$ and $Y = Z^m X^n$,

$$X^m Z^n F(X,Z) Z^{-n} X^{-m} = F(\gamma_N^n X, \gamma_N^{-m} Z) = Z^n X^m F(X,Z) X^{-m} Z^{-n} \,. \quad (1.19)$$

More generally, the powers of γ_N in (1.15) are irrelevant here, and therefore the group of unitary transformations has N^2 elements and is abelian. By contrast, the group of unitary operators is nonabelian; its abelian subgroups play a crucial role in Sec. 1.1.6 below. Weyl's view of "quantum kinematics as an abelian group of rotations" with its utter disregard of phase factors in the "ray fields" should be understood in this context; see Ch. IV, Sec. 14 in Ref. 3.

We shall pay due attention to the phase factors in (1.15) where they are relevant, but otherwise remember that the physically more essential factors in (1.15) are the powers of X and Z, and thus we will not be overly pedantic when referring to the Heisenberg–Weyl group. In the given context, it will be clear whether we mean the group of unitary operators with its γ_N^l phase factors or the group of unitary transformations. An example is the observation that the Nth power of $Y_{l,m,n}$ can differ from the identity operator,

$$\big(Y_{l,m,n}\big)^N = \begin{cases} \mathbf{1} & \text{if } N \text{ is odd,} \\ (-1)^{mn}\mathbf{1} & \text{if } N \text{ is even.} \end{cases} \quad (1.20)$$

For the group of unitary operators, the appearance of $(-1)^{mn}$ is crucial, telling us that one quarter of the $Y_{l,m,n}$ have period $2N$ for even N, whereas this is of no concern for the group of unitary transformations. As an example, consider once more the $N = 2$ situation with $X = \sigma_x$ and $Z = \sigma_z$, for which

$$(\sigma_x\sigma_z)^2 = -\mathbf{1} \,, \qquad (\sigma_x\sigma_z)^2 F(\sigma_x,\sigma_z)(\sigma_x\sigma_z)^2 = F(\sigma_x,\sigma_z) \,. \quad (1.21)$$

The unitary operators C that map the Heisenberg–Weyl group onto itself under conjugation,[f] that is: $Y_{l,m,n} \to C Y_{l,m,n} C^\dagger$ equals one of the $Y_{l,m,n}$s, constitute the so-called *Clifford group*.[12] It contains the Heisenberg–Weyl group as a subgroup, but is truly larger. For example, the "q-bit Hadamard gate" $(\sigma_x + \sigma_z)/\sqrt{2}$ is an operator in the Clifford group for $N = 2$, but not in the Heisenberg–Weyl group. The Hadamard gate is represented by the familiar Hadamard matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (1.22)$$

if we use the standard 2×2 matrices for σ_x and σ_z.

1.1.5. *Composite degrees of freedom*

If N is a composite number, $N = N_1 N_2$ with $N_1 > 1$ and $N_2 > 1$, then some of the Heisenberg–Weyl operators have a shorter period, as exemplified by $(Y_{0,N_1,0})^{N_2} =$

[f] Anti-unitary operators could be, and often are, included but we have no use for them.

$(X^{N_1})^{N_2} = X^N = \mathbf{1}$. As a consequence, there are Heisenberg–Weyl operators that have different spectral properties and are not related to each other by a unitary transformation.

It is then systematic to regard the N-dimensional degree of freedom as composed of a N_1-dimensional and a N_2-dimensional degree of freedom. Accordingly, the labels k of the kets $|k\rangle$ of the reference basis are understood as pairs k_1, k_2 with $k = k_1 + k_2 N_1$ whereby $k_1 = 0, 1, \ldots, N_1 - 1$ and $k_2 = 0, 1, \ldots, N_2 - 1$. The action of the corresponding cyclic operators X_1 and X_2 is given by

$$\begin{aligned} X_1|k\rangle = X_1|k_1, k_2\rangle = |k_1 + 1, k_2\rangle = |k + 1\rangle \qquad & \text{for } k_1 = 0, 1, \ldots, N_1 - 2\,, \\ X_2|k\rangle = X_2|k_1, k_2\rangle = |k_1, k_2 + 1\rangle = |k + N_1\rangle \qquad & \text{for } k_2 = 0, 1, \ldots, N_2 - 2\,, \end{aligned} \tag{1.23}$$

and the respective $k_1 = N_1 - 1$ and $k_2 = N_2 - 1$ statements are

$$\begin{aligned} X_1|k = (k_2 + 1)N_1 - 1\rangle = X_1|N_1 - 1, k_2\rangle = |0, k_2\rangle = |k_2 N_1\rangle\,, \\ X_2|k = k_1 + N_1(N_2 - 1)\rangle = X_2|k_1, N_2 - 1\rangle = |k_1, 0\rangle = |k_1\rangle\,. \end{aligned} \tag{1.24}$$

By construction, X_1 and X_2 have periods N_1 and N_2, respectively, and as a consequence of the algebraic completeness of the pair X, Z of complementary observables, we can express X_1 and X_2 quite explicitly as functions of X and Z, with the outcome

$$X_1 = X - \big(\mathbf{1} - X^{-N_1}\big)\delta_{Z^{N_2},1} X\,, \qquad X_2 = X^{N_1}\,. \tag{1.25}$$

Clearly, X_1 commutes with X_2 because Z^{N_2} commutes with X^{N_1} when $N_1 N_2 = N$, as is the case here.

Likewise one constructs the complementary partners Z_1 and Z_2 as the operators that cyclically advance the respective quantum numbers of the common eigenbras $\langle \underline{j_1}, \underline{j_2}|$ of X_1 and X_2, which are related to the kets $|k_1, k_2\rangle$ through the analog of (1.7),

$$\langle \underline{j_1}, \underline{j_2}|k_1, k_2\rangle = \frac{1}{\sqrt{N_1}}\gamma_{N_1}^{j_1 k_1} \frac{1}{\sqrt{N_2}}\gamma_{N_2}^{j_2 k_2}\,. \tag{1.26}$$

In summary, then, the original N-dimensional degree of freedom, parameterized by the pair X, Z, is decomposed into the product of two degrees of freedom, a N_1-dimensional and a N_2-dimensional one, parameterized by the pairs X_1, Z_1 and X_2, Z_2, respectively.

In passing, we note that the two bases of product kets $|k_1, k_2\rangle$ and $|\underline{j_1}, \underline{j_2}\rangle$ are MU. This illustrates how one can construct MUB of a composite degree of freedom from such bases of its constituents.

If N_1 or N_2 are composite numbers themselves, this reasoning can be applied again, if necessary repeatedly, until one has one degree of freedom for each prime factor of N. These prime degrees of freedom are fundamental and cannot be decomposed further. As emphasized by Schwinger in his teaching,[6] they are the elementary quantum degrees of freedom.

1.1.6. *Prime degrees of freedom*

The simplest prime degree of freedom is the q-bit case $N = 2$, for which we have $X = \sigma_x$, $Z = \sigma_z$, and $XZ = -\mathrm{i}\sigma_y$. With $|0\rangle$ and $|1\rangle$ denoting the eigenkets of σ_z to eigenvalues $+1$ and -1, respectively, the eigenkets of σ_x are $2^{-\frac{1}{2}}(|0\rangle \pm |1\rangle)$, and the eigenkets of σ_y are $2^{-\frac{1}{2}}(|0\rangle\mathrm{i} \pm |1\rangle)$. These three bases are *pairwise* MU, and the three operators X, Z, and XZ are pairwise complementary.

More generally, we can consider any two components $A = \vec{a}\cdot\vec{\sigma}$ and $B = \vec{b}\cdot\vec{\sigma}$ of Pauli's vector operator $\vec{\sigma}$ whose cartesian components are σ_x, σ_y, and σ_z. Operators A and B are complementary if the nonvanishing three-dimensional numerical vectors $\vec{a}$ and $\vec{b}$ are orthogonal to each other, $\vec{a}\cdot\vec{b} = 0$. Since there are at most three pairwise orthogonal vectors, there are at most three pairwise complementary operators and at most three MUB. The choice σ_x, σ_y, σ_z for the three operators is, therefore, not particular, but typical.

If N is an odd prime, $N = 3, 5, 7, 11, 13, \ldots$, then all unitary Heisenberg–Weyl operators $Y_{l,m,n}$ of (1.15) are cyclic with period N, except for the identity $\mathbf{1} = Y_{0,0,0}$. Further, we observe that the $N + 1$ operators

$$X\,,\ XZ\,,\ XZ^2\,,\ \ldots\,,\ XZ^{N-1}\,,\ Z \tag{1.27}$$

are pairwise complementary,[8] as one verifies most directly with the aid of (1.5) in conjunction with

$$\mathrm{tr}\big\{Y_{l,m,n}\big\} = N\gamma_N^l\delta_{m,0}\delta_{n,0}\,. \tag{1.28}$$

It follows that the $N + 1$ bases of eigenkets, one for each of the operators in (1.27), are MU. In addition to the eigenbases of X and Z that we met in Sec. 1.1.2, there are thus $N - 1$ more such bases.

And there cannot be a $(N + 2)$th basis because a counting argument shows that one can at most have $N + 1$ bases that are MU.[13] One way of seeing this is presented in Sec. 1.2 below.

In this context, we note here that the powers of the operators in (1.27) make up $N + 1$ abelian subgroups of the Heisenberg–Weyl group with N unitary operators in each subgroup. Remembering that the identity is contained in each subgroup, this gives a total count of $(N + 1)(N - 1) + 1 = N^2$ operators, one representative for each set of $Y_{l,m,n}$s with common m, n values, that is: one count for each X^mZ^n product.

In summary, we can systematically construct $N + 1$ bases that are MU if N is prime. The construction does not work if N is composite. Try $N = 4$ to see what goes wrong; we return to the case of $N = 6$ in Sec. 5.10.

Yet, this is not the end of the story. If $N = p^{\mathrm{M}}$ is the power of a prime, for which $N = 8 = 2^3$ and $N = 9 = 3^2$ are examples, it is possible to modify the construction such that it does work in a closely analogous way. The clue is to replace the modulo-N shifts of (1.9) and (1.10) by shifts of a Galois field arithmetic that treats the N-dimensional degree of freedom systematically as composed of M p-dimensional constituents. This is the theme of Sec. 2, followed by applications in Secs. 3 and 4.

This Galois cure is, however, not available for $N = 6$ and $N = 10$ or other composite N values that are not powers of a prime, simply because the number of elements in a finite field is always a prime power. Section 5 contains a report on what is known about these cases, in particular about $N = 6$. Strictly speaking, the question whether there are seven MUB for $N = 6$ is presently unanswered, but there is a lot of evidence, and a growing conviction in the community, that there are no more than three such bases. And three such bases are immediately available by pairing each of the three q-bit bases ($N_1 = 2$) with one of the four q-trit bases ($N_2 = 3$) to product bases as in (1.26).

1.1.7. *The continuous limit of $N \to \infty$*

Since composite values of N refer to composite quantum degrees of freedom, we take the limit $N \to \infty$ through prime values of N, thereby dealing with a single degree of freedom of increasing complexity. The prime nature of N will not be so crucial, however, but we make use of the fact that large primes are odd numbers and relabel the kets of the reference basis $|k\rangle$ and the bras $\langle \underline{j}|$ of the Fourier-transformed basis such that now $j, k = 0, \pm 1, \pm 2, \ldots, \pm\frac{1}{2}(N-1)$.

Next, we introduce a small, eventually infinitesimal, parameter ϵ by

$$N = \frac{2\pi}{\epsilon^2} \tag{1.29}$$

to account for the fact that the basic unit of complex phase $2\pi/N$ gets arbitrarily small when $N \to \infty$. Aiming at a continuous degree of freedom in this limit, we also relabel the states in accordance with

$$\begin{aligned} j \longrightarrow j\epsilon = a = 0, \pm\epsilon, \pm 2\epsilon, \ldots, \pm\Big(\frac{\pi}{\epsilon} - \frac{\epsilon}{2}\Big)\,, \\ k \longrightarrow k\epsilon = b = 0, \pm\epsilon, \pm 2\epsilon, \ldots, \pm\Big(\frac{\pi}{\epsilon} - \frac{\epsilon}{2}\Big)\,. \end{aligned} \tag{1.30}$$

The numbers a and b will cover the real axis, $-\infty < a, b < \infty$, when $N \to \infty$, $\epsilon \to 0$.

The unitary operator X acting on $|k\rangle$ increases k by 1, so that it effects $b \to b + \epsilon$. Likewise Z applied to $\langle \underline{j}|$ results in $a \to a + \epsilon$. This suggests the identification of hermitian operators A and B such that

$$\begin{aligned} X = \mathrm{e}^{\mathrm{i}\epsilon A} \quad \text{with } A = A^\dagger\,, \\ Z = \mathrm{e}^{\mathrm{i}\epsilon B} \quad \text{with } B = B^\dagger\,. \end{aligned} \tag{1.31}$$

The Weyl commutation relation (1.11) then appears as

$$X^k Z^j = \mathrm{e}^{-\mathrm{i}\frac{2\pi}{N}jk} Z^j X^k \longrightarrow \mathrm{e}^{\mathrm{i}k\epsilon A}\mathrm{e}^{\mathrm{i}j\epsilon B} = \mathrm{e}^{-\mathrm{i}jk\epsilon\epsilon}\mathrm{e}^{\mathrm{i}j\epsilon B}\mathrm{e}^{\mathrm{i}k\epsilon A} \tag{1.32}$$

or

$$\mathrm{e}^{\mathrm{i}bA}\mathrm{e}^{\mathrm{i}aB} = \mathrm{e}^{-\mathrm{i}ab}\mathrm{e}^{\mathrm{i}aB}\mathrm{e}^{\mathrm{i}bA}\,. \tag{1.33}$$

The two equivalent versions

$$\begin{aligned} \mathrm{e}^{\mathrm{i}b(A-a\mathbf{1})} &= \mathrm{e}^{-\mathrm{i}aB}\mathrm{e}^{\mathrm{i}bA}\mathrm{e}^{\mathrm{i}aB} = \mathrm{e}^{\mathrm{i}b\,\mathrm{e}^{-\mathrm{i}aB}A\,\mathrm{e}^{\mathrm{i}aB}}\,, \\ \mathrm{e}^{\mathrm{i}a(B-b\mathbf{1})} &= \mathrm{e}^{\mathrm{i}bA}\mathrm{e}^{\mathrm{i}aB}\mathrm{e}^{-\mathrm{i}bA} = \mathrm{e}^{\mathrm{i}a\,\mathrm{e}^{\mathrm{i}bA}B\,\mathrm{e}^{-\mathrm{i}bA}} \end{aligned} \tag{1.34}$$

seem to imply that

$$\begin{aligned} \mathrm{e}^{-\mathrm{i}aB}A\,\mathrm{e}^{\mathrm{i}aB} &= A - a\mathbf{1}\,, \\ \mathrm{e}^{\mathrm{i}bA}B\,\mathrm{e}^{-\mathrm{i}bA} &= B - b\mathbf{1}\,, \end{aligned} \tag{1.35}$$

but this does not follow without imposing a restricting condition, just as $\mathrm{e}^{\mathrm{i}\alpha} = \mathrm{e}^{\mathrm{i}\beta}$ does not imply $\alpha = \beta$, but only that $\alpha - \beta$ is an integer multiple of 2π.

The said restriction is that, for large N, only a, b values from a finite vicinity of 0 matter, which is to say that we break the cyclic nature of the labels a, b,

$$\langle a|\mathrm{e}^{\mathrm{i}a'B} = \langle a + a' \,(\mathrm{mod}\, 2\pi/\epsilon)|\,, \qquad \mathrm{e}^{\mathrm{i}b'A}|b\rangle = |b + b' \,(\mathrm{mod}\, 2\pi/\epsilon)\rangle\,, \tag{1.36}$$

and take for granted that all relevant values of a, a' and b, b' are such that we stay inside the range $-(\pi/\epsilon - \epsilon/2)\cdots(\pi/\epsilon - \epsilon/2)$. Put differently, we give up the periodicity that would force us to identify $a = +\infty$ with $a = -\infty$ in the $\epsilon \to 0$ limit.

After performing the $N \to \infty$, $\epsilon \to 0$ limit with this restriction, the statements of (1.35) hold with continuous values for a and b. We can, therefore, exhibit the terms that are linear in a or b and arrive at

$$AB - BA = [A, B] = \mathrm{i}\mathbf{1}\,. \tag{1.37}$$

We recognize, of course, Heisenberg's commutation relation for a pair of complementary hermitian observables of a continuous degree of freedom, such as position A and momentum B (in natural units) for the motion along a line.

These $N \to \infty$ considerations for X and Z have to be supplemented by counterparts for their respective kets and bras. We need to identify

$$\langle a| = \frac{1}{\sqrt{\epsilon}}\langle \underline{j}|\Big|_{\epsilon\to 0} \quad \text{with } j\epsilon = a, \text{ and} \quad |b\rangle = |k\rangle\frac{1}{\sqrt{\epsilon}}\Big|_{\epsilon\to 0} \quad \text{with } k\epsilon = b, \tag{1.38}$$

and then get

$$\langle a|b\rangle = \frac{1}{\sqrt{2\pi}}\mathrm{e}^{\mathrm{i}ab} \tag{1.39}$$

as the analog of (1.7) as well as

$$\langle a|a'\rangle = \delta(a - a')\,, \quad \langle b|b'\rangle = \delta(b - b') \tag{1.40}$$

and

$$\int_{-\infty}^{\infty} \mathrm{d}a\, |a\rangle\langle a| = \mathbf{1} = \int_{-\infty}^{\infty} \mathrm{d}b\, |b\rangle\langle b| \tag{1.41}$$

as the continuum versions of the orthogonality and completeness relations in (1.2).

This discussion of the $N \to \infty$ limit is a variant of Schwinger's treatment in Sec. 1.16 of Ref. 6; see also Sec. 1.2.5 in Ref. 11. In passing we note that, in addition

to the standard symmetric limit that treats X and Z on equal footing and results in the Heisenberg pair of A and B, there are also asymmetric limits. For instance, if the position variable is kept periodic over a finite range in the limit, one obtains the pair of azimuth-angle operator and angular-momentum operator.[14]

1.1.8. *Continuous degree of freedom*

Knowing that there are $N+1$ pairwise complementary observables for prime degrees of freedom, we expect to find an infinite number of them for a continuous degree of freedom. Indeed, there is a continuum of pairwise complementary observables and, therefore, a continuum of MUB.

Consider the family of hermitian operators $Y(\vartheta)$ with eigenkets $|y,\vartheta\rangle$ that we introduce in accordance with

$$Y(\vartheta) = A\cos\vartheta + B\sin\vartheta\,,$$
$$Y(\vartheta)|y,\vartheta\rangle = |y,\vartheta\rangle y\,, \quad \langle y,\vartheta|y',\vartheta\rangle = \delta(y-y')\,, \quad \int_{-\infty}^{\infty} \mathrm{d}y\, |y,\vartheta\rangle\langle y,\vartheta| = \mathbf{1}\,. \tag{1.42}$$

Since $Y(\vartheta+\pi) = -Y(\vartheta)$, we need only deal with ϑ values in the range $0 \le \vartheta < \pi$. For given $Y(\vartheta)$, the corresponding abelian subgroup of unitary Heisenberg–Weyl operators comprises all operators $\mathrm{e}^{\mathrm{i}tY(\vartheta)}$ with real t.

For each value of ϑ the kets $|y,\vartheta\rangle$ make up a complete orthonormal basis, with the usual normalization to Dirac's delta function as stated in (1.42). The transition amplitude between states from two bases is given by

$$\langle y,\vartheta|y',\vartheta'\rangle = \frac{1}{\sqrt{\mathrm{i}2\pi\sin(\vartheta-\vartheta')}}\mathrm{e}^{\mathrm{i}\frac{1}{2}(y^2+y'^2)\cot(\vartheta-\vartheta') - \mathrm{i}yy'\csc(\vartheta-\vartheta')}\,, \tag{1.43}$$

where we recognize the familiar time-transformation function of the one-dimensional harmonic oscillator.[15] The commutator

$$\big[Y(\vartheta), Y(\vartheta')\big] = \mathrm{i}\sin(\vartheta'-\vartheta) \tag{1.44}$$

tells us that all pairs $Y(\vartheta), Y(\vartheta+\frac{1}{2}\pi)$ are on equal footing with the pair A, B, and indeed we have

$$\langle y,\vartheta|y',\vartheta+\tfrac{1}{2}\pi\rangle = \frac{1}{\sqrt{\mathrm{i}2\pi}}\mathrm{e}^{\mathrm{i}yy'} \tag{1.45}$$

as a generalization of the $\vartheta = 0$ statement in (1.39). The factor $\sqrt{\mathrm{i}}$, which appears here naturally and ensures the correct $\vartheta' \to \vartheta$ limit of (1.43), could have been included as well in (1.39) or earlier in (1.6), but the usual phase conventions have no such factors there.

Accordingly, the transition probability density[g]

$$\big|\langle y,\vartheta|y',\vartheta'\rangle\big|^2 = \frac{1}{2\pi\big|\sin(\vartheta-\vartheta')\big|} \tag{1.46}$$

[g]It is a *density* because we need to multiply with $\mathrm{d}y\,\mathrm{d}y'$ to get the probabilities referring to infinitesimal intervals of y and y'.

is the same, irrespective of the particular states chosen from the ϑ basis and the ϑ' basis — the right-hand side does not depend on the quantum numbers y and y'. The two bases are, therefore, MU for all pairs ϑ, ϑ', and the operators $Y(\vartheta)$ are pairwise complementary.

The factor $\big|\sin(\vartheta-\vartheta')\big|$ in the denominator in (1.46) originates in the $\sin(\vartheta-\vartheta')$ factor in the commutator (1.44) and is an artifact of the way we normalize the eigenstates of $Y(\vartheta)$ to the Dirac delta function; this illustrates the remark in footnote 'b'. Other normalization conventions would give different numerical values on the right-hand side of (1.46) but, of course, $Y(\vartheta)$ and $Y(\vartheta')$ are a pair of complementary observables irrespective of such normalization conventions. We, therefore, disagree with the approach in Ref. 16 where the authors first insist on identical numerical values on the right-hand sides of (1.46) for sets of MUB and then conclude that there are at most three such bases.

1.2. *A geometrically motivated measure of mutual unbiasedness*

The kets $|\,\rangle$ in N-dimensional Hilbert state, and their adjoint bras $\langle\,| = |\,\rangle^\dagger$, are rather abstract geometrical objects, and so are the linear operators that map kets on kets and bras on bras, among them the statistical operator ρ that summarizes our knowledge about the state of the physical N-dimensional degree of freedom under consideration. With reference to a specified basis, the kets are represented by numerical column vectors ψ ($N\times 1$ matrices), the bras by row vectors $\psi^\dagger$ ($1\times N$ matrices), and the linear operators by $N\times N$ matrices, among them the density matrix ϱ for the statistical operator ρ. We denote these relationships by $\psi \mathrel{\widehat{=}} |\,\rangle$, $\psi^\dagger \mathrel{\widehat{=}} \langle\,|$, and $\varrho \mathrel{\widehat{=}} \rho$, respectively.

There are many density matrices, one for each reference basis, to one and the same statistical operator, much like there are many trios of components for the velocity vector of the moon, one trio for each coordinate system. One should not confuse the velocity vector with its components, or the statistical operator with the density matrix used to represent it numerically.

When they exist, maximal sets of MUB form a very distinct geometrical pattern in the set of hermitian matrices of unit trace — the real euclidean space that contains the set of density matrices. This is where we begin our story about maximal sets of MUB, although in most of what follows we will prefer to work directly in Hilbert space. The two pictures ought to be considered as complementary, each of them possessing advantages and drawbacks.

The set $\{\varrho\}$ of density matrices is a convex body in the set of hermitian matrices of unit trace. Its pure states are the one-dimensional projectors. The set of its pure states has real dimension $2(N-1)$, and can be identified with the complex projective Hilbert space. The dimension of $\{\varrho\}$ is N^2-1, and the space in which it sits can be regarded as a vector space, with its origin at the maximally mixed state

$$\varrho_\star = \frac{1}{N}\mathbb{1} \mathrel{\widehat{=}} \frac{1}{N}\mathbf{1} = \rho_\star\,, \tag{1.47}$$

where $\mathbf{1}$ is the identity operator of (1.2) and $\mathbb{1}$ is the unit matrix that represents it.

With any hermitian matrix M of unit trace we associate a traceless matrix

$$\mathbf{m} = M - \varrho_\star \,. \tag{1.48}$$

The set of these traceless matrices forms a vector space, and we will think of them as vectors. The matrix representation is used to define the inner product

$$\mathbf{m}_1 \cdot \mathbf{m}_2 = \frac{1}{2}\mathrm{tr}\big\{(M_1 - \varrho_\star)(M_2 - \varrho_\star)\big\} \,. \tag{1.49}$$

Thus the squared distance between the tips of the two vectors $\mathbf{m}_1$ and $\mathbf{m}_2$ is

$$D(\mathbf{m}_1, \mathbf{m}_2)^2 = \frac{1}{2}\mathrm{tr}\big\{(M_1 - M_2)^2\big\} \,. \tag{1.50}$$

With any unit ket $|e\rangle$ in Hilbert space we associate a vector $\mathbf{e}$ in $\mathbf{R}^{N^2-1}$, the space of (N^2-1)-component real vectors, through

$$\mathbf{e} = \psi_e\psi_e^\dagger - \varrho_\star \mathrel{\widehat{=}} |e\rangle\langle e| - \rho_\star \tag{1.51}$$

so that the squared length of $\mathbf{e}$ is

$$|\mathbf{e}|^2 = \frac{N-1}{2N} \,. \tag{1.52}$$

All vectors in $\mathbf{R}^{N^2-1}$ with this specific length sit on the surface of the outsphere of the body $\{\varrho\}$, the smallest sphere containing the body. But it is important to realize that it is only a small $2(N-1)$-dimensional subset of this outsphere that corresponds to vectors in Hilbert space — most of the outsphere lies outside the body. The case $N = 2$ is an exception: in this case the outsphere is the familiar Bloch sphere, which is identical to the boundary of the body of density matrices.

Note furthermore that the orthonormality relations

$$\langle e_i|e_j\rangle = \delta_{j,k} \,, \qquad \mathbf{e}_i \cdot \mathbf{e}_j = \frac{1}{2}\delta_{j,k} - \frac{1}{2N} \tag{1.53}$$

imply each other. If $|e_i\rangle$ is an orthonormal basis of kets, the corresponding vectors $\mathbf{e}_i$ form a regular simplex that spans an $(N-1)$-plane, and clearly

$$\sum_{i=0}^{N-1} \mathbf{e}_i = 0 \,. \tag{1.54}$$

Hence the simplex is centered at the origin. We have normalized its edge lengths to unity.

Next consider two MUB with kets $|e_i\rangle$ and $|f_j\rangle$, respectively, represented by the vectors $\mathbf{e}_i$ and $\mathbf{f}_j$. The two equations

$$\big|\langle e_i|f_j\rangle\big|^2 = \frac{1}{N} \,, \qquad \mathbf{e}_i \cdot \mathbf{f}_j = 0 \tag{1.55}$$

are equivalent ways of stating that the bases are MU and, therefore, the two planes spanned by a pair of MUB are totally orthogonal: each vector in one plane is orthogonal to all vectors in the other plane. Since the dimension of our space is

$N^2-1=(N+1)(N-1)$, we can fit at most $N+1$ totally orthogonal $(N-1)$-planes into it. This is one way of seeing that the maximal number of MUB is $N+1$.

Let us now momentarily forget that our vectors $\mathbf{e}_i$, $\mathbf{f}_i$, and so on, are supposed to come from unit vectors in Hilbert space. Whatever the value of N, we can always find $N+1$ totally orthogonal $(N-1)$-planes in $\mathbf{R}^{N^2-1}$, and if we place a regular simplex in each we will obtain a quite interesting convex polytope with $N(N+1)$ corners.[17] When $N=2$, it is in fact a regular octahedron, but for other values of N it needs a name of its own. We will call it the MUB polytope, without implying that there exists a maximal set of MUB in the N-dimensional Hilbert space. The MUB polytope and the body of density matrices share the same outsphere and, in this manner, the existence problem for MUB can be turned into the problem of rotating the MUB polytope in such a way that all its corners fit into the small subset of pure quantum states that are present in that outsphere. This is a hard problem (unless $N=2$). Indeed, from this perspective it is not obvious that we can find even one pair of MUB but, as we have seen in Sec. 1.1.2, we can always do this. It is the existence of a *maximal* set, with $N+1$ bases that are pairwise MU, which is in doubt for general N.

Viewing bases as $(N-1)$-planes in $\mathbf{R}^{N^2-1}$ gives us the means to quantify how close a given pair of bases is to being MU. The trick is to regard n-planes in $\mathbf{R}^m$ as rank-n projectors in a vector space of real $m\times m$ matrices, in analogy to the way we go from vectors in Hilbert space to density matrices. This gives us an embedding of the Grassmannian of n-planes into a flat vector space equipped with a natural euclidean distance, and hence a natural notion of distance between vectors in Hilbert space. To derive it, consider the N vectors $\mathbf{e}_i$. Then form the $(N^2-1)\times N$ matrix

$$B=\big[\mathbf{e}_1\ \mathbf{e}_2\ \ldots\ \mathbf{e}_N\big]\,. \tag{1.56}$$

It has rank $N-1$ because of (1.54). Next form the projector onto the $(N-1)$-plane spanned by the linearly dependent vectors $\mathbf{e}_i$. It is

$$\Pi=2BB^{\mathrm{T}}\,. \tag{1.57}$$

Finally, the square of the chordal Grassmannian distance between a pair of planes is

$$\begin{aligned} D_c(\Pi_e,\Pi_f)^2\equiv\frac{1}{2}\mathrm{tr}\big\{(\Pi_e-\Pi_f)^2\big\} &= N-1-\sum_{a,b}\left(\big|\langle e_a|f_b\rangle\big|^2-\frac{1}{N}\right)^2 \\ &= \sum_{a,b}\big|\langle e_a|f_b\rangle\big|^2\Big(1-\big|\langle e_a|f_b\rangle\big|^2\Big)\,, \end{aligned} \tag{1.58}$$

where the kets $|e_a\rangle$ are related to Π_e through (1.51), (1.56), and (1.57), and the kets $|f_b\rangle$ are analogously related to Π_f. The last expression of (1.58) shows that $D_c=0$ if the projectors $|f_b\rangle\langle f_b|$ are a permutation of the projectors $|e_a\rangle\langle e_a|$, in which case we have the same basis twice, possibly with different labeling.

One can check that

$$0 \leq D_c^2 \leq N-1\,, \tag{1.59}$$

and that the distance is maximal if and only if the two bases are MU. This notion of distance has been used to study packing problems for n-planes,[18] and as a measure of "MUness".[19] If we pick our bases at random, using the unitarily invariant Fubini–Study measure to define "random," we find that the average squared distance is given by

$$\langle D_c^2 \rangle_{\rm FS} = \frac{N}{N+1}(N-1)\,. \tag{1.60}$$

If the dimension is large, $N \gg 1$, two bases picked at random are likely to be almost MU.

2. Construction of mutually unbiased bases in prime power dimensions

2.1. *Galois fields*

In what follows, we work in a Hilbert space of prime power dimension $N = p^{\rm M}$ with p a prime number and M a positive integer. These are the dimensions for which maximal sets of MUB are known to exist. Moreover, and not coincidentally, there is a finite Galois field with $N = p^{\rm M}$ elements. We shall label these elements by integer numbers i, $0 \leq i \leq N-1$, or, equivalently, by M-tuples $(i_0, i_1, \ldots, i_{{\rm M}-1})$ of integers, each integer running from 0 to $p-1$, that we get from the p-ary expansion of i:

$$i = (i_0, i_1, \ldots, i_{{\rm M}-1}) \qquad \text{if} \qquad i = \sum_{n=0}^{{\rm M}-1} i_n p^n\,. \tag{2.1}$$

Each field is characterized by two operations, a multiplication and an addition, that we shall denote by $\odot$ and $\oplus$ respectively. As in footnote 'a', we shall use the symbols 0 and 1 for the neutral elements of addition and multiplication, respectively, throughout the paper, consistent with their meaning as integers.

Further, we adopt the particular convention that the elements of the field are labeled in such a way that the addition is equivalent to the component-wise addition modulo p, that is

$$i = j \oplus k \text{ is tantamount to } i_n = j_n + k_n \,(\mathrm{mod}\ p) \tag{2.2}$$

for $n = 0, 1, \ldots, {\rm M}-1$, where i_n, j_n, k_n are the respective coefficients of (2.1). As a consequence, the summation in (2.1) is also a field summation,

$$i = (i_0 p^0) \oplus (i_1 p^1) \oplus \cdots \oplus (i_{{\rm M}-1} p^{{\rm M}-1}) = \bigoplus_{n=0}^{{\rm M}-1} i_n p^n\,. \tag{2.3}$$

All fields with the same number of elements are equivalent up to a relabeling, and there is no strict obligation for the convention (2.2), but it is natural and

convenient in the present context, because it allows us to regard the elements of the field both as labels of basis states and as integer numbers that we can use for getting powers of complex numbers in accordance with the usual computation rules.

Actually, that there exists a relabeling such that the addition is equivalent to the addition modulo p component-wise is a direct consequence of the fact that for all finite fields the characteristics of the field — the smallest number of times that we must add the element 1 (neutral for the multiplication) to itself before we obtain the element 0 (neutral for the addition) — is always equal to a prime number (p when $N = p^{\mathrm{M}}$).

Unfortunately, there is no similarly simple convention for the field multiplication $\odot$, and — the exceptions $N = p$ and $N = 4$ aside — one has a choice between several equally good ways of defining the field multiplication $\odot$ such that it is consistent with the component-wise definition of the field addition $\oplus$. In view of the associative and distributive nature of $\odot$, that is: $(a \odot b) \odot c = a \odot (b \odot c)$ and $(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$, respectively, we only need to state the values of $p^j \odot p^k$, the products of powers of p, with $j, k = 0, 1, \ldots, \mathrm{M} - 1$.

For $\mathrm{M} = 1$, $N = p$, the field multiplication is just multiplication modulo p. For $\mathrm{M} > 1$, we have

$$p^j \odot p^k = \begin{cases} p^{j+k} & \text{if } j + k < \mathrm{M}\,, \\ \displaystyle\sum_{l=0}^{\mathrm{M}-1} \mu_l p^l = (\mu_0, \mu_1, \ldots, \mu_{\mathrm{M}-1}) & \text{if } j + k = \mathrm{M}\,, \\ p \odot (p^{j-1} \odot p^k) & \text{recursively, if } j + k > \mathrm{M}\,. \end{cases} \tag{2.4}$$

Hereby, the coefficients that define the $j + k = \mathrm{M}$ products are restricted by the requirement that

$$x \mapsto x^{\mathrm{M}} - \sum_{l=0}^{\mathrm{M}-1} \mu_l x^l \tag{2.5}$$

is an *irreducible polynomial* over the Galois field with p elements, which is to say that it cannot be factored into two nonconstant polynomials whose coefficients are modulo-p integers.

For instance, the choice $2 \odot 2 = 3$ is unique for $N = 4$, and for p odd and $N = p^2$, one can always choose $p \odot p = \mu_0$ with μ_0 not a square, such as $3 \odot 3 = 2$, $5 \odot 5 = 2$ or $5 \odot 5 = 3$, $7 \odot 7 = 3$ or $7 \odot 7 = 5$ or $7 \odot 7 = 6$, and so forth. For higher powers of $p = 2$, there are several choices too; they include $2 \odot 4 = 5$ for $N = 8$, $2 \odot 8 = 3$ for $N = 16$, and $2 \odot 16 = 5$ for $N = 32$.

As a final example, we mention $3 \odot 9 = (1, 2, 2) = 25$ for $N = 3^3$.[h] This implies

[h] The choice $3 \odot 9 = 25$ is the largest one of the eight permissible values. The other seven values for (μ_0, μ_1, μ_2) are $(1, 1, 0) = 4$, $(2, 1, 0) = 5$, $(2, 0, 1) = 11$, $(1, 1, 1) = 13$, $(2, 2, 1) = 17$, $(1, 0, 2) = 19$, and $(2, 1, 2) = 23$. Each of them yields a consistent implementation of the field multiplication.

first $9 \odot 9 = (2,2,0) = 8$ and then

$$\begin{aligned} N = 27: \quad & (a_0,a_1,a_2) \odot (b_0,b_1,b_2) = a \odot b = c = (c_0,c_1,c_2) \\ & \text{with} \quad \begin{aligned} c_0 &= a_0b_0 + a_1b_2 + a_2b_1 - a_2b_2 \pmod 3 , \\ c_1 &= a_0b_1 + a_1b_0 - a_1b_2 - a_2b_1 - a_2b_2 \pmod 3 , \\ c_2 &= a_0b_2 + a_1b_1 + a_2b_0 - a_1b_2 - a_2b_1 \pmod 3 , \end{aligned} \end{aligned} \tag{2.6}$$

for the multiplication of two arbitrary field elements. The special cases $3 \odot 13 = 1$ and $9 \odot 17 = 1$ may serve as illustrations.

More generally, when writing

$$p^j \odot p^k = \big(M_0^{(j+k)}, M_1^{(j+k)}, \ldots, M_{\mathrm{M}-1}^{(j+k)}\big) , \tag{2.7}$$

we have

$$M_m^{(j+k)} = \delta_{j+k,m} \quad \text{for } j+k = 0,1,\ldots,\mathrm{M}-1 , \text{ and} \quad M_m^{(\mathrm{M})} = \mu_m , \tag{2.8}$$

and the coefficients for $j+k = \mathrm{M}+1, \mathrm{M}+2, \ldots, 2\mathrm{M}-2$ are successively calculated with the aid of the recurrence relation

$$M_m^{(j+k)} = (1-\delta_{m,0}) M_{m-1}^{(j+k-1)} + \mu_m M_{\mathrm{M}-1}^{(j+k-1)} \pmod p , \tag{2.9}$$

which is valid for $j+k = 1,2,\ldots,2\mathrm{M}-2$. The field product of two arbitrary elements is then given by

$$a \odot b = \big(a\mathcal{M}_0 b^T, a\mathcal{M}_1 b^T, \ldots, a\mathcal{M}_{\mathrm{M}-1} b^T\big) , \tag{2.10}$$

where $\mathcal{M}_m = \mathcal{M}_m^T$ is the symmetric $\mathrm{M} \times \mathrm{M}$ matrix

$$\mathcal{M}_m = \begin{pmatrix} M_m^{(0)} & M_m^{(1)} & M_m^{(2)} & \cdots & \cdots & & \\ M_m^{(1)} & M_m^{(2)} & & & & & \\ M_m^{(2)} & & & & & \vdots & \\ \vdots & & & \ddots & & \vdots & \\ \vdots & & & & & M_m^{(2\mathrm{M}-4)} & \\ & & & & M_m^{(2\mathrm{M}-4)} & M_m^{(2\mathrm{M}-3)} & \\ & & \cdots & \cdots & M_m^{(2\mathrm{M}-4)} & M_m^{(2\mathrm{M}-3)} & M_m^{(2\mathrm{M}-2)} \end{pmatrix} , \tag{2.11}$$

and in the products $a\mathcal{M}_m b^T$ we regard $a = (a_0, a_1, \ldots)$ as a row of p-ary coefficients and b^T as a column. These row × matrix × column products are ordinary matrix products with the outcome evaluated modulo p. The matrices $\mathcal{M}_0, \mathcal{M}_1, \ldots, \mathcal{M}_{\mathrm{M}-1}$ are invertible, in the sense of modulo-p arithmetic, because there is a unique multiplicative inverse for each non-zero field element. For instance, we have

$$\mathcal{M}_0 = \begin{pmatrix} 1&0&0 \\ 0&0&1 \\ 0&1&2 \end{pmatrix} , \qquad \mathcal{M}_1 = \begin{pmatrix} 0&1&0 \\ 1&0&2 \\ 0&2&2 \end{pmatrix} , \qquad \mathcal{M}_2 = \begin{pmatrix} 0&0&1 \\ 0&1&2 \\ 1&2&0 \end{pmatrix} , \tag{2.12}$$

and

$$\mathcal{M}_0^{-1} = \begin{pmatrix} 1\,0\,0 \\ 0\,1\,1 \\ 0\,1\,0 \end{pmatrix}, \quad \mathcal{M}_1^{-1} = \begin{pmatrix} 2\,1\,2 \\ 1\,0\,0 \\ 2\,0\,2 \end{pmatrix}, \quad \mathcal{M}_2^{-1} = \begin{pmatrix} 1\,1\,1 \\ 1\,1\,0 \\ 1\,0\,0 \end{pmatrix}, \tag{2.13}$$

for the $N = 27$ example in (2.6).

For notational simplicity, let us denote by γ the basic pth root of unity,

$$\gamma = \mathrm{e}^{\mathrm{i}2\pi/p}\,, \tag{2.14}$$

rather than writing γ_p as in (1.4). Exponentiating γ with elements g of the field — regarding now, as noted above, the field elements as integers — we obtain complex phase factors of the type γ^g with $0 \le g \le N-1$. As g is an integer, such phase factors can only take p different values. Their value depends solely on the value of the first component g_0 of the p-ary expansion of g because g_0 is just the remainder of g when dividing by p in the usual sense. The phase factor γ^g can be considered as a p-tuple generalization of the (binary) parity operation $\mathrm{e}^{\mathrm{i}(2\pi/2)g} = (-1)^g$ of the q-bit case (that is $p = 2$).

The following identity plays a fundamental role:

$$\sum_{j=0}^{N-1} \gamma^{j\odot i} = N\delta_{i,0}\,. \tag{2.15}$$

Indeed, if $i = 0$, then $\displaystyle\sum_{j=0}^{N-1} \gamma^{j\odot i} = \sum_{j=0}^{N-1} 1 = N$. Otherwise,

$$i \neq 0\,: \qquad \sum_{j=0}^{N-1} \gamma^{j\odot i} = \sum_{j'=0}^{N-1} \gamma^{j'} \tag{2.16}$$

because the field multiplication is invertible. Now, the exponentiation of γ by elements of the field does only depend on the remainder after division by p, so that

$$\sum_{j'=0}^{N-1} \gamma^{j'} = p^{\mathrm{M}-1} \sum_{j'_0=0}^{p-1} \gamma^{j'_0} = p^{\mathrm{M}-1}\frac{(1-\gamma^p)}{(1-\gamma)} = 0\,. \tag{2.17}$$

In virtue of the fact that the field addition is the component-wise addition modulo p, we also have the following useful identity:

$$\gamma^i\gamma^j = \gamma^{i+j} = \gamma^{i_0+j_0} = \gamma^{(i\oplus j)_0} = \gamma^{i\oplus j}\,. \tag{2.18}$$

Consistent with (2.1), here we represent by the symbol x_0 the remainder of x after division by p, where x is an element of the field, identified as an integer between 0 and $p^{\mathrm{M}} - 1 = N - 1$, and the division of x by p is taken in the usual sense. In the final expression on the right, the sum $i \oplus j$ is the Galois sum of i and j, which is then regarded as an integer, just as we regard the result of the Galois multiplication $j \odot i$ in (2.15) and (2.16) as an integer, and so get integer powers of γ. Relation

Table 1. (a) Addition and multiplication tables for the field with $N = 4$ elements. (b) Addition and multiplication modulo $N = 4$.

(a)

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

(b)

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(2.18) expresses, in the language of mathematicians, that the pth roots of unity are additive characters of the Galois field.[20]

It is important to note, in order to avoid confusions, that different types of operations are present at this level: the internal field operations ($\oplus$ and $\odot$) must not be confused with the modulo-N operations. As an illustration of the differences between these operations, we consider the case $p = 2$, $\mathrm{M} = 2$, $N = p^{\mathrm{M}} = 4$ and give the tables for field addition ($\oplus$) and field multiplication ($\odot$) in Table 1(a) as well as the tables for modulo-N addition and multiplication ($\oplus_4$ and $\odot_4$, respectively) in Table 1(b).

One can check that the field and modulo-4 multiplications are distributive with respect to the associated addition, but that there are no dividers of 0, 0 excepted, only in the case of the field multiplication, whereas we have $0 = 2 \odot_4 2$ for the modulo-4 multiplication. As a consequence, the field multiplication table exhibits an invertible group structure when the first line and first column are removed. All operations are commutative as can be seen from the invariance of all four tables under transposition.

Let us express q-quarts as products of two q-bits, in accordance with the binary encoding of $i = (i_0, i_1)$ for $i = 0, 1, 2, 3$ as stated by

$$\begin{aligned} |i\rangle_4 = |i_0\rangle_2 \otimes |i_1\rangle_2 \,:\quad & |0\rangle_4 = |0\rangle_2 \otimes |0\rangle_2\,, \\ & |1\rangle_4 = |1\rangle_2 \otimes |0\rangle_2\,, \\ & |2\rangle_4 = |0\rangle_2 \otimes |1\rangle_2\,, \\ & |3\rangle_4 = |1\rangle_2 \otimes |1\rangle_2\,. \end{aligned} \tag{2.19}$$

With the aid of the $\oplus$ subtable in Table 1, it is easy to verify that

$$\begin{aligned} |i \oplus j\rangle_4 &= |i_0 \oplus_2 j_0\rangle_2 \otimes |i_1 \oplus_2 j_1\rangle_2 \\ &\text{for } i = (i_0, i_1) \text{ and } j = (j_0, j_1)\,. \end{aligned} \tag{2.20}$$

This illustrates that the field addition is equivalent to the component-wise modulo-p addition.

It is also worth reminding that the properties

$$\gamma_N^i \gamma_N^j = \gamma_N^{i \oplus_N j} \quad \text{and} \quad \sum_{p=0}^{N-1} \gamma_N^{p \odot_N q} = N\delta_{q,0} \tag{2.21}$$

with $\gamma_N = \mathrm{e}^{\mathrm{i}2\pi/N}$ as in (1.4) are true for the modulo-N addition and multiplication as well, but note that γ_N is the basic Nth root of unity in these analogs of (2.18) and (2.15). In prime dimensions ($\mathrm{M} = 1$, $N = p^1 = p$) we have $\gamma = \gamma_N$ so that the characteristics of the modulo-p ring and the Galois field coincide. Indeed, both structures are rigorously identical in prime dimensions. In prime-power but non-prime dimensions, for instance when $N = 4$, this is not true.

2.2. *The computational basis*

Consider now a quantum degree of freedom of prime-power dimension $N = p^{\mathrm{M}}$ — a *q-nit* composed of M *q-pits*. The corresponding Hilbert space of kets has a conveniently chosen orthonormal reference basis consisting of $|0\rangle, |1\rangle, \ldots, |N-1\rangle$, which we regard as the *computational basis* of kets. The adjoint basis of bras comprises all $\langle n| = |n\rangle^\dagger$ with $n = 0, 1, \ldots, N-1$. As usual, the inner products $(\,\cdot\,,\,\cdot\,)$ of two kets or two bras are given by Dirac brackets ($\equiv$ bra-kets), for which the orthonormality relations

$$\big(|i\rangle, |j\rangle\big) = \big(\langle i|, \langle j|\big) = \langle i|j\rangle = \delta_{i,j} \tag{2.22}$$

are an elementary illustration.

2.3. *The dual basis*

Let us now consider the unitary transformations V_l^0 that shift each label of the states of the computational basis $\{|0\rangle, |1\rangle, \ldots, |i\rangle, \ldots, |N-1\rangle\}$ by l,

$$|i\rangle \to V_l^0 |i\rangle = |i \oplus l\rangle\,, \tag{2.23}$$

so that each V_l^0 implements a permutation among the kets of the computational basis, but does not change the basis as a whole. The shift in (2.23) is a shift modulo N in prime dimensions only (N=p) and then V_l^0 is identical with X^l of Sec. 1.1.2; in prime power dimensions ($N = p^{\mathrm{M}}$, $\mathrm{M} > 1$) the shift consists of M shifts modulo p, component-wise. The transformations effected by V_l^0 with $l = 0, 1, \ldots, N-1$ make up a commutative group of permutations with N elements that is isomorphic to the Galois addition.

Generalizing the procedure outlined in Ref. 21, we employ a suitable discrete Fourier-type transformation — the inverse *Galois–Fourier* transformation — to define the dual basis as follows:

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \gamma^{\ominus k \odot j} \tag{2.24}$$

where the symbol $\ominus$ represents the inverse of the Galois addition $\oplus$, that is: $x = \ominus y$ if $x \oplus y = 0$. It is easy to check that these dual kets are joint eigenkets of the unitary permutation operators V_l^0. Indeed, we have

$$V_l^0|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k \oplus l\rangle \gamma^{\ominus k \odot j} = \frac{1}{\sqrt{N}} \sum_{k'=0}^{N-1} |k'\rangle \gamma^{\ominus(k' \ominus l)\odot j} = |\tilde{j}\rangle \gamma^{l \odot j}\,, \tag{2.25}$$

which identifies the eigenvalues $\gamma^{l\odot j}$. These are p different eigenvalues, each occurring M times.

Obviously, the dual basis and the computational basis are MU by construction,

$$\left|\langle\tilde{j}|k\rangle\right|^2 = \left|\frac{1}{\sqrt{N}}\gamma^{j\odot k}\right|^2 = \frac{1}{N} \qquad \text{for all } j,k = 0,1,\ldots,N-1\,. \tag{2.26}$$

When the dimension is prime ($N = p$), the dual basis is the standard discrete Fourier transform of the computational basis, as in (1.6); when N is a power of 2, it is a real Hadamard transform.[21]

Let us denote by V_0^l the unitary transformations that shift each label of the states of the dual basis $\{|\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |\tilde{i}\rangle, \ldots, |\widetilde{N-1}\rangle\}$ by $\ominus l$,

$$|\tilde{i}\rangle \to V_0^l|\tilde{i}\rangle = |\widetilde{i \ominus l}\rangle\,, \qquad \langle\tilde{i}| \to \langle\tilde{i}|V_0^l = \langle\widetilde{i \oplus l}|\,, \tag{2.27}$$

so that each V_0^l implements a permutation among the kets of the dual basis, but does not change the basis as a whole. In perfect analogy with the permutation operators V_l^0 of (2.23), the transformations effected by V_0^l with $l = 0,1,\ldots,N-1$ upon the bras $\langle\tilde{i}|$ also compose a commutative group of permutations with N elements that is isomorphic to the Galois addition.

These permutation operators are diagonal in the computational basis,

$$V_0^l = \sum_{k=0}^{N-1} |\widetilde{k}\rangle\langle\widetilde{k \oplus l}| = \sum_{k=0}^{N-1} |k\rangle \gamma^{k\odot l}\langle k|\,. \tag{2.28}$$

This is the dual counterpart of the analogous expression for the shifts in the computational basis,

$$V_l^0 = \sum_{k=0}^{N-1} |k \oplus l\rangle\langle k| = \sum_{k=0}^{N-1} |\tilde{k}\rangle \gamma^{k\odot l}\langle\tilde{k}|\,, \tag{2.29}$$

which is equivalent to (2.25) and follows from that eigenket statement.

The unitary operators V_l^0 and V_0^l are obviously analogs of the operators X^l and Z^l of Sec. 1.1.2, but for M > 1 these operators are markedly different. In particular, the period of V_1^0 and V_0^1 is p, not $N = p^{\mathrm{M}}$. We indicate the difference by writing $\langle\tilde{i}|$ for the dual basis here, whereas the notation $\langle\underline{i}|$ is employed in Sec. 1.1.2.

As mentioned above, it is immediately clear that $|k\rangle \to V_l^0|k\rangle = |k \oplus l\rangle$ is a component-wise addition, where the components of the q-nit ket $|k\rangle$ are the M

q-pits that compose it, as is illustrated by (2.19) and (2.20) for $p = 2$ and $\mathrm{M} = 2$. More generally,

$$V_l^0|k\rangle = V_l^0|k_0\rangle\otimes|k_1\rangle\otimes\cdots\otimes|k_{\mathrm{M}-1}\rangle = |k_0{+}l_0\rangle\otimes|k_1{+}l_1\rangle\otimes\cdots\otimes|k_{\mathrm{M}-1}{+}l_{\mathrm{M}-1}\rangle\,, \quad (2.30)$$

where each factor $|k_m\rangle$ in the tensor product is a q-pit ket, and the sums $k_m{+}l_m$ are modulo-p sums. It follows that V_l^0 is a product of factors, each of which referring to one of the q-pits,

$$V_l^0 = \left(V_1^0\right)^{l_0}\left(V_p^0\right)^{l_1}\left(V_{p^2}^0\right)^{l_2}\cdots = \prod_{m=0}^{\mathrm{M}-1}\left(V_{p^m}^0\right)^{l_m}\,, \quad (2.31)$$

where the mth factor affects the mth q-pit only, with $V_{p^m}^0$ giving a unit shift of the mth modulo-p label.

In order to see that $\langle\tilde{k}| \to \langle\tilde{k}|V_0^l = \langle\widetilde{k\oplus l}|$ is a q-pit–wise shift as well, we first observe that the Galois–Fourier transformation (2.24) factorizes,

$$\begin{aligned}\langle\tilde{k}| &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\gamma^{k\odot j}\langle j| = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\gamma^{k\mathcal{M}_0 j^T}\langle j_0|\otimes\langle j_1|\otimes\langle j_2|\otimes\cdots\otimes\langle j_{\mathrm{M}-1}|\\ &= \frac{1}{\sqrt{p}}\sum_{j_0=0}^{p-1}\gamma^{(k\mathcal{M}_0)_0 j_0}\langle j_0|\otimes\frac{1}{\sqrt{p}}\sum_{j_1=0}^{p-1}\gamma^{(k\mathcal{M}_0)_1 j_1}\langle j_1|\otimes\cdots\\ &= \langle\widetilde{\underline{k}_0}|\otimes\langle\widetilde{\underline{k}_1}|\otimes\cdots\otimes\langle\widetilde{\underline{k}_{\mathrm{M}-1}}|\,, \end{aligned} \quad (2.32)$$

where $\mathcal{M}_0$ is the 0th multiplication matrix in (2.10) and $\underline{k}_m$ is the mth component of $k\mathcal{M}_0 = (\underline{k}_0, \underline{k}_1, \ldots)$. Since $\mathcal{M}_0$ is invertible, we can parameterize the field element k in terms of the coefficients $\underline{k}_m$,

$$k = (\underline{k}_0, \underline{k}_1, \ldots)\mathcal{M}_0^{-1} = (\underline{k}_0, \underline{k}_1, \ldots)\begin{pmatrix} g_0\\ g_1\\ \vdots\\ g_{\mathrm{M}-1}\end{pmatrix} = \sum_{m=0}^{\mathrm{M}-1}\underline{k}_m g_m\,, \quad (2.33)$$

with the field elements g_m defined such that their p-ary coefficients make up the rows of the $\mathrm{M}\times\mathrm{M}$ matrix $\mathcal{M}_0^{-1}$. Alternatively, we could define the g_ms by their basic property

$$\gamma^{p^m\odot g_n} = \gamma^{\delta_{m,n}} = \begin{cases}\gamma \text{ if } m = n\,,\\ 1 \text{ if } m \neq n\,.\end{cases} \quad (2.34)$$

Therefore, a unit increase of $\underline{k}_m$ means the addition of g_m to k, and the shift operator V_0^l factorizes accordingly into a product of powers of single–q-pit Fourier operators, each of which (the mth, say) acting on the single–q-pit bras $\langle\widetilde{j_m}|$ only and leaving the other $\mathrm{M}-1$ q-pit bras in the products of (2.32) unaffected,

$$V_0^l = (V_0^{g_0})^{\underline{l}_0}\,(V_0^{g_1})^{\underline{l}_1}\,(V_0^{g_2})^{\underline{l}_2}\cdots = \prod_{m=0}^{\mathrm{M}-1}(V_0^{g_m})^{\underline{l}_m}\,, \quad (2.35)$$

with the mth factor affecting the mth q-pit only. For instance, we have $g_0 = 1$, $g_1 = 12$, $g_2 = 3$, and $\underline{k}_0 = k_0$, $\underline{k}_1 = k_2$, $\underline{k}_2 = k_1 - k_2$ for the $N = 27$ example of (2.6), (2.12), and (2.13).

The respective unitary operator factors for unit shifts in (2.31) and (2.35) commute if they refer to different q-pits,

$$V_{p^m}^0 V_0^{g_n} = V_0^{g_n} V_{p^m}^0 \quad \text{if } m \neq n\,, \tag{2.36}$$

which essentially states that the Galois shifts with their component-wise addition are consistent with the factorization of the $N = p^{\mathrm{M}}$-dimensional degree of freedom into M p-dimensional degrees of freedom, as discussed in Sec. 1.1.5. And for the pair of operators to the same q-pit, one easily verifies the Weyl commutation rule

$$V_{p^m}^0 V_0^{g_m} = \gamma^{-1} V_0^{g_m} V_{p^m}^0\,. \tag{2.37}$$

Equations (2.36) and (2.37) are particular cases of (2.39) below.

2.4. *Construction of the remaining N-1 mutually unbiased bases*

In the previous section we established a pair of MUB, the computational basis, which can be chosen arbitrarily, and its dual basis, defined by (2.24). In this section, we shall generalize this construction in order to obtain the other $N - 1$ bases that complement the computational basis and its dual basis such that the bases of each of the $N(N + 1)/2$ pairs are MU.

2.4.1. *Heisenberg–Weyl group*

Let us denote by V_i^j the compositions of the shifts in the computational and the dual bases, obtained by ordinary operator multiplication of V_0^j and V_i^0,

$$V_i^j = V_0^j V_i^0 = \sum_{k=0}^{N-1} |k \oplus i\rangle \gamma^{(k\oplus i)\odot j} \langle k| \quad \text{for } i, j = 0, 1, \ldots, N-1\,, \tag{2.38}$$

the building blocks of the Heisenberg–Weyl group. This is consistent with the previous expressions for $i = 0$ or $j = 0$ because V_0^0 is the identity. In particular, for $i = 0$ and $j = l$ we get the second sum of (2.28), and for $i = l$ and $j = 0$ we have the first sum of (2.29).

We note that the order of multiplication of V_0^j and V_j^0 matters in the definition (2.38) because these unitary shift operators do not commute,

$$V_i^0 V_0^j = \gamma^{\ominus i\odot j} V_0^j V_i^0\,. \tag{2.39}$$

We recognize here the Weyl commutation rule for the two unitary operators V_0^j and V_i^0, which is their basic algebraic relation.[2,3]

In dimension $N = p = 2$, the commutation relation (2.39) is that of the Pauli group (identify V_0^1 with σ_x and V_1^0 with σ_z once more). When the dimension is a prime number, the field operations are the addition and multiplication modulo

p, and the properties of MUB are well-known;[22] recall the discussion in Sec. 1.1.6 with its emphasis on the Heisenberg–Weyl group.

Presently, we consider the Heisenberg–Weyl group associated with the Galois addition and multiplication rather than the Heisenberg–Weyl group associated with the usual modulo-N operations. These groups coincide in prime dimensions but differ for non-prime but prime-power dimensions. Notably, the Galois field is isomorph to the modulo-N ring in prime dimensions only ($N = p$). Nevertheless, the Heisenberg–Weyl group factorizes in dimension p^{M} into products of operators that belong to the local q-pit Heisenberg–Weyl group. In the case of translations of the computational basis, the factorization is straightforward and given above in (2.31). And in the case of translations of the dual basis, where the mapping from global operator labels to local operator labels is more intricate, see (2.32)–(2.34), the factorization is stated in (2.35).

The composition law of the N^2 unitary operators introduced in (2.38) is

$$\begin{aligned} V_i^j V_k^l &= V_0^j V_i^0 V_0^l V_k^0 \\ &= \gamma^{\ominus i\odot l} V_0^j V_0^l V_i^0 V_k^0 = \gamma^{\ominus i\odot l} V_{i\oplus k}^{j\oplus l} \,, \end{aligned} \tag{2.40}$$

which implies

$$V_k^{l\,-1} = V_k^{l\,\dagger} = \gamma^{\ominus k\odot l} V_{\ominus k}^{\ominus l} \tag{2.41}$$

and

$$V_k^l V_i^j V_k^{l\,\dagger} = \gamma^{l\odot i\ominus j\odot k} V_i^j \tag{2.42}$$

for example. Another implication is

$$\big(V_i^j\big)^p = \begin{cases} (-1)^{i\odot j}\mathbf{1} & \text{for } p = 2\,, \\ \mathbf{1} & \text{for } p = 3, 5, 7, 11, \ldots\,, \end{cases} \tag{2.43}$$

which is reminiscent of (1.20) and once again shows a difference between the single even prime $p = 2$ and the odd primes $p > 2$.

Yet another implication is the orthonormality relation for the V_i^js, with respect to the Hilbert–Schmidt inner product,

$$\big(V_i^j, V_k^l\big) = \mathrm{tr}\big\{V_i^{j\,\dagger} V_k^l\big\} = N\delta_{i,k}\delta_{j,l}\,, \tag{2.44}$$

because all V_i^js are traceless, except $V_0^0 = \mathbf{1}$. The other side of this coin is the ergodicity relation,[4]

$$\sum_{m,n=0}^{N-1} V_m^n\, A\, V_m^{n\,\dagger} = N\mathrm{tr}\big\{A\big\}\mathbf{1}\,, \tag{2.45}$$

which one may regard as a manifestation of Schur's lemma.

Equation (2.40) is the discrete analog of the familiar Baker–Campbell–Hausdorff relation for exponentiated position and momentum operators that we encountered in (1.33). An immediate consequence of (2.40) is

$$V_i^j V_l^k = V_l^k V_i^j \quad \text{if } (i\odot k)_0 = (j\odot l)_0 \text{ and only then,} \tag{2.46}$$

where $(\ )_0$ has the same meaning as in (2.18). In particular, (2.46) is fulfilled if $i \odot k = j \odot l$, which we note for later reference.

2.4.2. *Abelian subgroups*

Up to a global phase, (2.40) looks like a group composition law. Indeed, one can show[23] that there is a true analog of what we observed in Sec. 1.1.6 for prime N: the N^2 unitary operators V_i^j with $i, j = 0, 1, \ldots, N-1$ make up $N+1$ commuting sets (abelian subgroups of the Heisenberg–Weyl group) of N elements each that have only the identity V_0^0 in common. For each of these commuting sets, there is a basis of joint eigenkets of all V_i^js in the set. The $N+1$ bases thus identified are pairwise MU. In passing, we note that this property can be shown, following an alternative approach developed in Ref. 24, to be a consequence of the fact that the V_i^j operators form what is called "a maximally commuting basis of orthogonal unitary matrices."

It is expedient to introduce a fitting notation and terminology before we proceed. We shall denote by U_l^i the elements of these abelian subgroups, where i labels the subgroup and runs from 0 to N to account for $N+1$ subgroups, while l labels the N elements in the subgroup and runs from 0 to $N-1$. For the basis kets associated with the subgroups we use the convention that the kth basis ket for the ith subgroup is denoted by $|e_k^i\rangle$.

The abelian subgroups for $i = N$ and $i = 0$ are composed of the two sets of commuting permutation operators of Sec. 2.3, respectively,

$$\begin{aligned} U_l^N = V_0^l &= \sum_{k=0}^{N-1} |k\rangle\gamma^{k\odot l}\langle k| = \sum_{k=0}^{N-1} |e_k^N\rangle\gamma^{k\odot l}\langle e_k^N|\,, \\ U_l^0 = V_l^0 &= \sum_{k=0}^{N-1} |\tilde{k}\rangle\gamma^{k\odot l}\langle \tilde{k}| = \sum_{k=0}^{N-1} |e_k^0\rangle\gamma^{k\odot l}\langle e_k^0|\,, \end{aligned} \tag{2.47}$$

with $l = 0, 1, \ldots, N-1$. As indicated, we identify $|k\rangle$ with $|e_k^N\rangle$, and $|\tilde{k}\rangle$ with $|e_k^0\rangle$. In other words, we choose the convention that the computational basis is the Nth basis, and the dual basis is the 0th basis.

This suggests strongly that the other $N-1$ sets can be chosen such that

$$U_l^i = \sum_{k=0}^{N-1} |e_k^i\rangle\gamma^{k\odot l}\langle e_k^i| \tag{2.48}$$

with $i = 1, 2, \ldots, N-1$ and $l = 0, 1, \ldots, N-1$. To complete the picture, we need to find the kets $|e_l^i\rangle$, such that those with common label i make up orthonormal sets, and the sets with different i labels are MU. These requirements are compactly summarized by

$$\left|\langle e_k^i|e_l^j\rangle\right|^2 = \delta_{i,j}\delta_{k,l} + \frac{1-\delta_{i,j}}{N} = \begin{cases} \delta_{k,l} \ \text{ for } i = j \text{ (orthonormal)}, \\ 1/N \text{ for } i \neq j \text{ (mutually unbiased)}, \end{cases} \tag{2.49}$$

which have to hold for $i, j = 0, 1, \ldots, N$ and $k, l = 0, 1, \ldots, N-1$.

Irrespective of the choice for the ith orthonormal set of kets and bras in (2.48), the U_l^i are unitary and commute with each other,

$$U_l^i U_{l'}^i = U_{l'}^i U_l^i = U_{l\oplus l'}^i \,, \tag{2.50}$$

which is an immediate consequence of distributivity and the identity (2.18). In view of (2.46), we can guess that the U_l^i of the ith set are operators V_l^k such that the Galois ratio $k\oslash l$ has the same i-dependent value for all of them.[i] For, if $k\oslash l = k'\oslash l'$, then $k' \odot l = k \odot l'$, and (2.46) implies that V_l^k and $V_{l'}^{k'}$ commute.

We are thus invited to try the ansatz

$$U_l^i = \alpha_l^i V_l^{i\odot l} \quad \text{for } i = 0, 1, \ldots, N-1 \,, \tag{2.51}$$

where the phase factors α_l^i have to be chosen consistently. In particular we have

$$\begin{aligned} \alpha_l^0 = 1 \,: \quad & U_l^0 = V_l^0 \quad \text{for } l = 0, 1, \ldots, N-1 \\ \text{and } \ \alpha_0^i = 1 \,: \quad & U_0^i = V_0^0 \quad \text{for } i = 0, 1, \ldots, N-1 \,, \end{aligned} \tag{2.52}$$

and the said consistency with (2.50) requires

$$\alpha_k^i \alpha_l^i = \alpha_{k\oplus l}^i \gamma^{i\odot k\odot l} \,, \tag{2.53}$$

where (2.18) and (2.40) have been used repeatedly. We note that all U_l^i of (2.47) and (2.48) have period p, which tells us that the inclusion of α_l^i in (2.51) removes the even-odd distinction of (2.43).

The orthonormality relation (2.44) carries over to the U_l^is in the form

$$\mathrm{tr}\big\{{U_k^i}^\dagger U_l^j\big\} = N\delta_{k,l}\delta_{i\odot k, j\odot l} = \begin{cases} N & \text{for } k = l = 0 \,, \\ N\delta_{i,j} & \text{for } k = l \neq 0 \,, \\ 0 & \text{for } k \neq l \,. \end{cases} \tag{2.54}$$

This is, of course, (1.5) in the present context.

Any choice for the phase factors α_l^i that obeys (2.52) and (2.53) is permissible in (2.51), but these conditions do not determine the phase factors uniquely (except for $i = 0$). Just as (2.50) remains valid when we replace U_l^i by $\gamma^{b_i\odot l} U_l^i$ with an arbitrary field element b_i, the replacement $\alpha_l^i \to \alpha_l^i \gamma^{b_i\odot l}$ has no effect in (2.52) and (2.53), and in (2.51) it amounts to a permutation of the states in the ith basis: $|e_k^i\rangle \to |e_{k\ominus b_i}^i\rangle$, but leaves the basis as a whole unchanged.[23]

It remains to be shown, though, that there *are* consistent choices for all phase factors. This task has been successfully completed in Ref. 23, from where we take the following explicit solutions.

In odd prime-power dimensions ($p = 3, 5, 7, \ldots$), where $1 \oplus 1 = 2$, the self-suggesting choice

$$p \text{ odd:} \quad \alpha_l^i = \gamma^{\ominus(i\odot l\odot l)\oslash 2} \tag{2.55}$$

[i] For $l \neq 0$, one naturally defines $k \oslash l$ by $(k \oslash l) \odot l = k$.

is simplest and indeed possible. But in even prime-power dimensions ($p = 2$), where $1 \oplus 1 = 0 \neq 2$, (2.55) does not work.

That the situation is more complicated for $p = 2$ could perhaps be anticipated because finite fields with even and odd cardinality are known to possess very different structures. In the present context, the structural difference between $p = 2$ and $p = 3, 5, 7, \ldots$ manifests itself in the observation that

$$\left(\alpha_l^j\right)^p = \begin{cases} (-1)^{j\odot l\odot l} = 1 \text{ or } -1 & \text{for } p = 2\,, \\ 1 & \text{for } p > 2\,, \end{cases} \tag{2.56}$$

which combines with (2.43) to ensure the p-periodicity of all U_l^is. As a consequence, we can systematically write α_l^j as a power of γ for odd p, as we do in (2.55). For $p = 2$ this is not possible but, instead, we can systematically write α_l^j as a power of $\mathrm{i} = \sqrt{-1} = \mathrm{e}^{\mathrm{i}\frac{\pi}{2}}$ because, in virtue of (2.56), α_l^j is the square root of a power of $\gamma = -1$ for $p = 2$.

Now, such a square root is only determined up to a global sign. Some extra work is thus necessary in order to fix these signs, which will enable us to derive a $p = 2$ counterpart of (2.55). As a consequence of the group property (2.53), for each j it is sufficient to fix M well chosen phases such that then the values of all the $N = 2^{\mathrm{M}}$ phases are determined.

The M values of the signs of the phases α_l^j that we choose by convention are $\alpha_0^j, \alpha_2^j, \ldots, \alpha_{2^{\mathrm{M}-1}}^j$ and we require, in agreement with (2.56), that they obey

$$p = 2: \quad \alpha_{2^n}^j = \mathrm{i}^{j\odot 2^n\odot 2^n} \quad \text{or} \quad \alpha_{l_n 2^n}^j = \mathrm{i}^{j\odot(l_n 2^n)\odot(l_n 2^n)}\,, \tag{2.57}$$

where the latter version, with $l_n = 0$ or $l_n = 1$, incorporates $\alpha_0^j = 1$ as well. For

$$l = \sum_{n=0}^{\mathrm{M}-1} l_n 2^n = \bigoplus_{n=0}^{\mathrm{M}-1} l_n 2^n\,, \tag{2.58}$$

we then have two ways of evaluating the product of all $\alpha_{l_n 2^n}^j$, namely

$$\prod_{n=0}^{\mathrm{M}-1} \alpha_{l_n 2^n}^j = \prod_{n=0}^{\mathrm{M}-1} \mathrm{i}^{j\odot(l_n 2^n)\odot(l_n 2^n)} \tag{2.59}$$

as an immediate consequence of (2.57), and

$$\begin{aligned} \prod_{n=0}^{\mathrm{M}-1} \alpha_{l_n 2^n}^j &= (-1)^{j\odot l_0\odot(l_1 2)} \alpha_{l_0\oplus l_1 2}^j \prod_{n=2}^{\mathrm{M}-1} \alpha_{l_n 2^n}^j \\ &= (-1)^{j\odot l_0\odot(l_1 2)} (-1)^{j\odot(l_0\oplus l_1 2)\odot(l_2 2^2)} \alpha_{l_0\oplus l_1 2\oplus l_2 2^2}^j \prod_{n=3}^{\mathrm{M}-1} \alpha_{l_n 2^n}^j \\ &= \cdots \\ &= \alpha_l^j \prod_{m=0}^{\mathrm{M}-2} \prod_{n=m+1}^{\mathrm{M}-1} (-1)^{j\odot(l_m 2^m)\odot(l_n 2^n)} \end{aligned} \tag{2.60}$$

or

$$\prod_{n=0}^{M-1} \alpha_{l_n 2^n}^{j} = \alpha_l^j \prod_{\substack{m,n=0 \\ m\neq n}}^{M-1} (-\mathrm{i})^{j\odot(l_m 2^m)\odot(l_n 2^n)} \tag{2.61}$$

by repeated application of (2.53). The $n = m$ terms missing in (2.61) make up the product in (2.59), so that we arrive at[j]

$$p = 2: \quad \alpha_l^j = \prod_{m,n=0}^{M-1} \mathrm{i}^{j\odot(l_m 2^m)\odot(l_n 2^n)} \tag{2.62}$$

as the suitable square root of $(-1)^{j\odot l\odot l}$. The additional option of replacing α_l^j by $\gamma^{b_j\odot l}\alpha_l^j$, see the paragraph after (2.54), amounts to extra factors of $(-1)^{l_n}$ in (2.57) for some n values. Examples of evaluating the product in (2.62) can be found in Appendix C.

Irrespective of the conventions adopted for the phase factors α_l^i, we note that the symmetry property

$$\alpha_l^i = \alpha_{\ominus l}^i \tag{2.63}$$

holds when N is even, because $l = \ominus l$ for $p = 2$. It is also true for odd N if the phases of (2.55) are chosen, but not for all permissible choices. If one imposes (2.63) as an additional condition, then

$$\left(\alpha_l^i\right)^2 = \alpha_l^i \alpha_{\ominus l}^i = \gamma^{\ominus i\odot l\odot l} \tag{2.64}$$

for all N and all $i = 0, 1, \ldots, N-1$, and (2.55) and (2.62) show how the proper square root of the right-hand side can be defined. Unless explicitly stated, the symmetry (2.63) is not assumed for $p > 2$ in what follows, and neither are the explicit expressions (2.55) and (2.62) for the phase factors.

2.4.3. *The remaining $N-1$ bases*

Having thus at our disposal the unitary operators U_l^i of (2.48) and (2.51), we can also state quite explicitly the $N-1$ dual bases associated with the abelian subgroups for $i = 1, 2, \ldots, N-1$. For this purpose we exploit the analog of (1.12),

$$|e_k^i\rangle\langle e_k^i| = \frac{1}{N}\sum_{l=0}^{N-1} \gamma^{\ominus k\odot l} U_l^i\,, \tag{2.65}$$

which is an immediate consequence of (2.48) and (2.15), and from its implication

$$\langle e_l^N|e_k^i\rangle\langle e_k^i|e_m^N\rangle = \frac{1}{N}\left(\gamma^{k\odot l}\alpha_{\ominus l}^i\right)^*\left(\gamma^{k\odot m}\alpha_{\ominus m}^i\right) \tag{2.66}$$

[j]Owing to an oversight that was pointed out by Eusebi and Mancini,[25] the expression given in Ref. 23 is incorrect, but this inadvertence is of no consequence because the general properties (2.52) and (2.53) matter, not the explicit convention chosen for the values of the α_l^js. The derivation (2.57)–(2.62) is essentially identical with the reasoning in Ref. 25.

we find

$$|e_k^i\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |e_l^N\rangle \gamma^{\ominus k\odot l} {\alpha_{\ominus l}^i}^* \,. \tag{2.67}$$

As a consequence, the unitary shift operators V_m^n of the Heisenberg–Weyl group, turn states of one basis into each other, but do not relate the bases to one another,

$$V_m^n |e_0^i\rangle = |e_{i\odot m\ominus n}^i\rangle {\alpha_m^i}^* \quad \text{for } i = 0, 1, \ldots, N-1\,, \qquad V_m^n |e_0^N\rangle = |e_m^N\rangle\,. \tag{2.68}$$

Statements (2.66), (2.67), and (2.68), as well as (2.71)–(2.74) below, are valid both for odd prime powers and even prime powers, whether the respective phase factors of (2.55) and (2.62) are used or any other permissible choice, and apply also for $i = 0$ when $|e_k^0\rangle = |\tilde{k}\rangle$ as required by the conventions chosen in (2.47) and (2.52).

Indeed, it is easy to establish the validity of the requirement (2.49) for the projectors in (2.65) by exploiting (2.65) and without relying on (2.67):

$$\begin{aligned} \left|\langle e_k^i | e_l^j\rangle\right|^2 = \mathrm{tr}\left\{ \left(|e_k^i\rangle\langle e_k^i|\right) \left(|e_l^j\rangle\langle e_l^j|\right)\right\} &= \frac{1}{N^2} \sum_{m,n=0}^{N-1} \gamma^{k\odot m} \gamma^{\ominus l\odot n} \mathrm{tr}\left\{ {U_m^i}^\dagger U_n^j \right\} \\ &= \frac{1}{N} \sum_{m,n=0}^{N-1} \gamma^{k\odot m\ominus l\odot n} \delta_{m,n} \delta_{i\odot m, j\odot n} = \frac{1}{N} \sum_{m=0}^{N-1} \gamma^{(k\ominus l)\odot m} \delta_{i\odot m, j\odot m} \\ &= \frac{1}{N} + \delta_{i,j} \frac{1}{N} \sum_{m=1}^{N-1} \gamma^{(k\ominus l)\odot m} = \frac{1}{N} + \delta_{i,j} \left(\delta_{k,l} - \frac{1}{N} \right)\,, \end{aligned} \tag{2.69}$$

where the orthonormality relation (2.54) and the identity (2.15) are the main ingredients. The eigenvalue equations

$$U_l^i |e_k^i\rangle\langle e_k^i| = |e_k^i\rangle\langle e_k^i| U_l^i = |e_k^i\rangle \gamma^{k\odot l} \langle e_k^i| \tag{2.70}$$

also follow for (2.65) directly from (2.50).

But it cannot be a mistake to check, for consistency, that $|e_k^i\rangle$ as given in (2.67) is the eigenket of U_l^i of (2.51) to eigenvalue $\gamma^{k\odot l}$. Starting from

$$\begin{aligned} U_l^i |e_m^N\rangle = V_l^{i\odot l} |m\rangle \alpha_l^i &= |m\oplus l\rangle \gamma^{i\odot(m\oplus l)\odot l} \alpha_l^i \\ &= |m\oplus l\rangle {\alpha_{\ominus(m\oplus l)}^i}^* \alpha_{\ominus m}^i \end{aligned} \tag{2.71}$$

we have

$$\begin{aligned} U_l^i |e_k^i\rangle \gamma^{\ominus k\odot l} &= \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} U_l^i |e_m^N\rangle \gamma^{\ominus(m\oplus l)\odot k} {\alpha_{\ominus m}^i}^* \\ &= \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |m\oplus l\rangle {\alpha_{\ominus(m\oplus l)}^i}^* \gamma^{\ominus(m\oplus l)\odot k} = |e_k^i\rangle\,, \end{aligned} \tag{2.72}$$

indeed.

For later reference, we further observe that

$$\mathrm{tr}\left\{ {U_l^i}^\dagger V_m^n \right\} = N \delta_{i\odot l, n}\, \delta_{l,m}\, {\alpha_l^i}^*\,, \tag{2.73}$$

which follows from (2.51) and (2.44) and in turn implies

$$\langle e_k^i|V_m^n|e_k^i\rangle = \delta_{i\odot m,n}\,\gamma^{k\odot m}\alpha_m^{i\,*}\,, \tag{2.74}$$

upon invoking the adjoint version of (2.65). And finally we note that the unitary mapping of the computational basis ($i = N$) onto the ith basis is accomplished by the Clifford operator C_i whose defining property, that is: $C_i|e_k^N\rangle = |e_k^i\rangle$ for all k, implies

$$C_i = \sum_{k=0}^{N-1} |e_k^i\rangle\langle e_k^N|\,. \tag{2.75}$$

This includes $C_N = \mathbf{1}$. The terminology "Clifford operators" refers to the Clifford group,[12] which consists of all unitary operators that map the Heisenberg–Weyl group onto itself under conjugation, that is: $V_l^i \to C^\dagger V_l^i C$ equals one of the V_l^is for each C in the Clifford group, in full analogy to the discussion in Sec. 1.1.4.

2.5. *Complementary period-N observables*

In a sense, the $N+1$ abelian subgroups replace the $N+1$ complementary observables of Sec. 1.1.6 whose powers constitute the $N+1$ abelian subgroups for prime N. But there are much closer analogs in the form of $N+1$ pairwise complementary period-N observables for which (1.5) applies immediately, rather than the analog we have in (2.54).

For each abelian subgroup, $i = 0, 1, 2, \ldots, N$, we introduce a period-N observable by means of

$$Z_i = \sum_{k=0}^{N-1} |e_k^i\rangle\gamma_N^k\langle e_k^i| = \frac{1}{N}\sum_{k,l=0}^{N-1} \gamma_N^k\gamma^{\ominus k\odot l}U_l^i\,. \tag{2.76}$$

By construction, these observables constitute a maximal set of pairwise complementary observables for the N-dimensional degree of freedom. See Table 2 in Sec. 5.7 for an example of five such observables for $N = 4$.

3. Generalized Bell states and their applications

There is a one-to-one correspondence between generalized Bell states and the Heisenberg–Weyl group.[21,26] This correspondence is a key concept for a uniform view of several important applications in quantum information science, such as quantum dense coding (Sec. 3.2), quantum teleportation (Sec. 3.3), and quantum cloning (Sec. 3.4).

The construction that we use here employs the Heisenberg–Weyl group of Sec. 2 whose shift operators (2.38) change state labels via field addition. In the context of generalized Bell states, the analogous construction based on the modulo-N Heisenberg–Weyl operators of Sec. 1.1.4 works equally well. The deep connection between Bell states and displacement operators was already underlined in Ref. 27:

With the necessary changes, all applications in Secs. 3.2–3.4 can be implemented by these other Bell states.[28]

3.1. *Generalized Bell states*

Following Refs. 21, 26, and 29, we can define the generalized Bell states by the following procedure. First, for all kets $|\psi\rangle$ and bras $\langle\phi|$ we introduce *conjugate* kets $|\psi^*\rangle$ and bras $\langle\phi^*|$ whose defining property is

$$\langle\psi^*|\phi^*\rangle = \langle\psi|\phi\rangle^* = \langle\phi|\psi\rangle\,. \tag{3.1}$$

Although this does not identify the conjugate kets and bras uniquely, any two implementations of the map $|\psi\rangle \to |\psi^*\rangle$ are related to each other by a unitary transformation and, therefore, it does not matter which convention we employ for the implementation of our choosing.

Since the conjugate kets transform like the original bras, we have a very useful one-to-one correspondence of one–q-nit operators $|\psi\rangle\langle\phi|$ and two–q-nit states,[k]

$$|\psi\rangle\langle\phi| \longleftrightarrow |\phi^*,\psi\rangle\,, \tag{3.2}$$

which is linear in the ket part of the one–q-nit operator and antilinear in the bra part. As a consequence, we have relations such as

$$\text{if } A \longleftrightarrow |a\rangle \text{ and } B \longleftrightarrow |b\rangle, \text{ then } \mathrm{tr}\big\{A^\dagger B\big\} = \langle a|b\rangle \tag{3.3}$$

as well as

$$\text{if } A \longleftrightarrow |a\rangle, \text{ then } BA \longleftrightarrow (\mathbf{1}\otimes B)|a\rangle \tag{3.4}$$

and

$$\text{if } A \longleftrightarrow |a\rangle, \text{ then } AB^\dagger \longleftrightarrow (B^*\otimes \mathbf{1})|a\rangle\,, \tag{3.5}$$

where $B^*|\phi^*\rangle = |\psi^*\rangle$ if $B|\phi\rangle = |\psi\rangle$. Take, for instance,

$$A = |\psi_1\rangle\langle\phi_1| \longrightarrow |a\rangle = |\phi_1^*,\psi_1\rangle \quad\text{and}\quad B = |\psi_2\rangle\langle\phi_2| \longrightarrow |b\rangle = |\phi_2^*,\psi_2\rangle\,, \tag{3.6}$$

for which

$$\mathrm{tr}\big\{A^\dagger B\big\} = \langle\phi_2|\phi_1\rangle\langle\psi_1|\psi_2\rangle = \langle\phi_1^*|\phi_2^*\rangle\langle\psi_1|\psi_2\rangle = \langle a|b\rangle \tag{3.7}$$

as well as

$$BA = |\psi_2\rangle\langle\phi_2|\psi_1\rangle\langle\phi_1| \longrightarrow |\phi_1^*,\psi_2\rangle\langle\phi_2|\psi_1\rangle = \Big(\mathbf{1}\otimes|\psi_2\rangle\langle\phi_2|\Big)|\phi_1^*,\psi_1\rangle \tag{3.8}$$

and

$$AB^\dagger = |\psi_1\rangle\langle\phi_1|\phi_2\rangle\langle\psi_2| \longrightarrow |\psi_2^*,\psi_1\rangle\langle\phi_2^*|\phi_1^*\rangle = \Big(|\psi_2^*\rangle\langle\phi_2^*|\otimes\mathbf{1}\Big)|\phi_1^*,\psi_1\rangle\,. \tag{3.9}$$

[k]In an experimental realization, the two different N-ary quantum degrees of freedom, the two q-nits, could just as well be carried by one physical object or by several.

Quite generally, the mapping (3.2) turns statements about one–q-nit operators into statements about two–q-nit kets.

An important example is the observation that irrespective of the basis used in the completeness relation, the identity operator is mapped onto one and the same ket $|B_{0,0}\rangle$,

$$\mathbf{1} = \sum_k |k\rangle\langle k| = \sum_k |e_k^i\rangle\langle e_k^i| \longleftrightarrow \sum_k |k^*, k\rangle = \sum_k |e_k^{i*}, e_k^i\rangle = |B_{0,0}\rangle\sqrt{N}\,, \quad (3.10)$$

here illustrated for the computational basis and either one of the bases of (2.67). The factor $\sqrt{N}$ normalizes $|B_{0,0}\rangle$ to unit length, consistent with (3.3) and $\mathrm{tr}\{\mathbf{1}\} = N$. Owing to its basis independence, the ket $|B_{0,0}\rangle$ plays a central role in tomographic protocols for quantum key distribution; see, e.g., Ref. 30.

As an example, consider the case $N = 2$ of a single q-bit, and the following four alternative ways, four of many, of defining the map $|\psi\rangle \to |\psi^*\rangle$:

$$|\psi\rangle = |0\rangle\alpha + |1\rangle\beta \to |\psi^*\rangle = \begin{cases} |0\rangle\alpha^* + |1\rangle\beta^*\,, \\ |0\rangle\alpha^* - |1\rangle\beta^*\,, \\ |0\rangle\beta^* + |1\rangle\alpha^*\,, \\ |0\rangle\beta^* - |1\rangle\alpha^*\,. \end{cases} \quad (3.11)$$

The respective two–q-bit kets $|B_{0,0}\rangle$,

$$|B_{0,0}\rangle = \begin{cases} \frac{1}{\sqrt{2}}\big(|0,0\rangle + |1,1\rangle\big)\,, \\ \frac{1}{\sqrt{2}}\big(|0,0\rangle - |1,1\rangle\big)\,, \\ \frac{1}{\sqrt{2}}\big(|0,1\rangle + |1,0\rangle\big)\,, \\ \frac{1}{\sqrt{2}}\big(|0,1\rangle - |1,0\rangle\big)\,, \end{cases} \quad (3.12)$$

are the familiar standard Bell states.[31] The four maps in (3.11) differ by simple unitary transformations, and the same unitary transformations (of the first qubit) relate the four Bell states to each other. For instance, $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ turns the first and second versions of $|\psi^*\rangle$ into each other, and also the third and fourth versions. Likewise, $\sigma_z \otimes \mathbf{1}$ interchanges the first and second Bell states, and the third and fourth. These observations for q-bits invite us to call $|B_{0,0}\rangle$ a *generalized Bell state*.

In view of $V_0^0 = \mathbf{1}$, we recognize that $N^{-1/2}V_0^0 \longleftrightarrow |B_{0,0}\rangle$, which identifies $|B_{0,0}\rangle$ as one of the N^2 members of the set composed of the kets $|B_{m,n}\rangle$ that correspond to the unitary shift operators V_m^n,

$$V_m^n = \sum_{k=0}^{N-1} |k\oplus m\rangle\gamma^{(k\oplus m)\odot n}\langle k| \longleftrightarrow \sum_{k=0}^{N-1} |k^*, k\oplus m\rangle\gamma^{(k\oplus m)\odot n} = |B_{m,n}\rangle\sqrt{N}\,. \quad (3.13)$$

These make up the set of *generalized Bell states*. Their orthonormality follows from (3.3) and (2.44),

$$\langle B_{m,n}|B_{m',n'}\rangle = \frac{1}{N}\mathrm{tr}\big\{V_m^{n\dagger}V_{m'}^{n'}\big\} = \delta_{m,m'}\delta_{n,n'}\,, \tag{3.14}$$

and (3.4) implies that the shift operators V_m^n permute the Bell states,

$$\begin{aligned}(\mathbf{1}\otimes V_r^s)|B_{m,n}\rangle &= |B_{m\oplus r,n\oplus s}\rangle\gamma^{\ominus(r\odot n)}\,,\\ (V_r^{s*}\otimes\mathbf{1})|B_{m,n}\rangle &= |B_{m\ominus r,n\ominus s}\rangle\gamma^{(m\ominus r)\odot s}\,,\end{aligned} \tag{3.15}$$

where (2.40) enters. In particular, we have

$$\begin{aligned}|B_{m,n}\rangle &= (\mathbf{1}\otimes V_m^n)|B_{0,0}\rangle\,,\\ |B_{\ominus m,\ominus n}\rangle &= (V_m^{n*}\otimes\mathbf{1})|B_{0,0}\rangle\gamma^{m\odot n}\,,\end{aligned} \tag{3.16}$$

which relate all generalized Bell states to their "seed" $|B_{0,0}\rangle$ of (3.10).

We note the identity

$$(V_m^{n*}\otimes V_m^n)|B_{0,0}\rangle = |B_{0,0}\rangle\,, \tag{3.17}$$

which states the invariance of the seed under simultaneous shifts of both q-nits. And the analog of the ergodicity relation (2.45) is

$$\frac{1}{N}\sum_{m,n=0}^{N-1}(V_m^{n*}\otimes V_m^n)|\phi^*,\psi\rangle = |B_{0,0}\rangle\sqrt{N}\langle\phi|\psi\rangle\,, \tag{3.18}$$

which once more emphasizes the particularity of the invariant Bell seed.

Since all Bell states are related to the maximally entangled seed by a local unitary transformation ("local" because $\mathbf{1}\otimes V_m^n$ affects the second q-nit only in the two–q-nit state to which $|B_{0,0}\rangle$ refers), each of them is maximally entangled, and since they are orthonormal and N^2 in number, they constitute an orthonormal, maximally entangled basis in the Hilbert space of two–q-nit kets. Technically speaking, this N^2-dimensional Hilbert space is obtained by taking the tensor product of the N-dimensional Hilbert space, in which we have the computational basis and all that, with itself.

Owing to the correspondence $|B_{m,n}\rangle \longleftrightarrow N^{-1/2}V_m^n$ in (3.13), the expansion of any N-dimensional single–q-nit operator in the operator basis of the V_m^n shift operators, is equivalent to the decomposition of a N^2-dimensional two–q-nit state ket in the orthonormal Bell-state basis. This is at the heart of the quantum tomography that we present in Sec. 4.2 below.

The Bell states in (3.16) refer explicitly to the computational basis because (2.38) expresses V_m^n in terms of the $|k\oplus m\rangle\langle k| = |e^N_{k\oplus m}\rangle\langle e^N_k|$ ket-bra products. We get the Bell states relative to the ith basis by applying the Clifford operator C_i of (2.75) to the second q-nit and its dual analog C_i^*, which we define by $C_i^*|e_k^{N*}\rangle = |e_k^{i*}\rangle$, to the first q-nit. In view of (3.4) and (3.5), the analog of the correspondence (3.13) for the computational basis, is then

$$(C_i^*\otimes C_i)|B_{m,n}\rangle \longleftrightarrow \frac{1}{\sqrt{N}}C_iV_m^nC_i^\dagger\,, \tag{3.19}$$

and as a consequence of the trace rule (3.3) we have

$$\langle B_{m,n}|(C_i^* \otimes C_i)|B_{m',n'}\rangle = \frac{1}{N}\mathrm{tr}\left\{V_m^{n\,\dagger} C_i V_{m'}^{n'} C_i^\dagger\right\}. \tag{3.20}$$

Upon employing (2.67) to express $C_i V_m^n C_i^\dagger$ in terms of the computational basis,

$$\begin{aligned} C_i V_m^n C_i^\dagger &= \sum_{k=0}^{N-1} |e^i_{k\oplus m}\rangle \gamma^{(k\oplus m)\odot n} \langle e^i_k| \\ &= \sum_{l=0}^{N-1} |n\oplus l\rangle \alpha^i_{\ominus(n\oplus l)}{}^* \gamma^{\ominus l\odot m} \alpha^i_{\ominus l} \langle l|\,, \end{aligned} \tag{3.21}$$

the trace is readily evaluated, and we find

$$\begin{aligned} \langle B_{m,n}|(C_i^* \otimes C_i)|B_{m',n'}\rangle &= \delta_{m,n'}\,\delta_{i\odot m\ominus n,m'}\,\gamma^{\ominus m\odot n}\alpha^i_{\ominus m}{}^* \\ &= \delta_{m,n'}\,\delta_{n,i\odot n'\ominus m'}\,\gamma^{m'\odot n'}\alpha^i_{n'}\,. \end{aligned} \tag{3.22}$$

The two Kronecker delta symbols tell us that the application of the unitary operator $C_i^* \otimes C_i$ to the Bell basis permutes the Bell states, but leaves the basis as a whole unaltered.

Quite explicitly, we have

$$\begin{aligned} |B_{m,n}\rangle &= (C_i^* \otimes C_i)|B_{i\odot m\ominus n,m}\rangle \gamma^{m\odot n}\alpha^i_{\ominus m}\,, \\ (C_i^* \otimes C_i)|B_{m,n}\rangle &= |B_{n,i\odot n\ominus m}\rangle \gamma^{m\odot n}\alpha^i_n\,, \end{aligned} \tag{3.23}$$

where the mappings of the indices,

$$\begin{pmatrix} m \\ n \end{pmatrix} \to \begin{pmatrix} i & \ominus 1 \\ 1 & 0 \end{pmatrix} \odot \begin{pmatrix} m \\ n \end{pmatrix}, \qquad \begin{pmatrix} m \\ n \end{pmatrix} \to \begin{pmatrix} 0 & 1 \\ \ominus 1 & i \end{pmatrix} \odot \begin{pmatrix} m \\ n \end{pmatrix}, \tag{3.24}$$

are each other's inverse. The particular case of $m = n = 0$,

$$(C_i^* \otimes C_i)|B_{0,0}\rangle = |B_{0,0}\rangle\,, \tag{3.25}$$

states the invariance of the Bell seed when switching from one bases to another, which we have observed earlier in the context of (3.10).

3.2. *Quantum dense coding*

The generalization of q-bit quantum dense coding[32] to an arbitrary dimension N is an immediate application of (3.16). It goes at follows.[28] Alice and Bob initially share the seed state $|B_{0,0}\rangle$ of the Bell basis, with q-nit 1 in Alice's possession and q-nit 2 in Bob's. Bob applies one of the N^2 unitary shift operators V_m^n to his q-nit 2 and then sends it to Alice who, according to (3.16), has the q-nit pair in the Bell state $|B_{m,n}\rangle$. She finds out which of the states is the case by performing a von Neumann measurement in the Bell basis.

The measurement result tells her which one of the N^2 shifts was implemented by Bob, and so she receives $2\log_2 N$ bits of information, as much as two classical N-valued signals could convey. In a manner of speaking, Bob has transmitted two

c-nits by sending one q-nit. This is the essence of dense coding; quite like the teleportation of the following section, it has no classical counterpart.

3.3. *Quantum teleportation*

The relation between maximal sets of orthogonal families of unitary matrices and teleportation was already emphasized several years ago in the q-bit case[27,33] and has been generalized to arbitrary dimension N along the following lines.[28] A central ingredient of the q-nit teleportation process is the three–q-nit–states identity

$$\begin{aligned}\sum_{k=0}^{N-1} |k^*, j, k\rangle &= \sum_{k,m,n} |B_{m,n}, k\rangle\langle B_{m,n}|k^*, j\rangle \\ &= \sum_{k,m,n} |B_{m,n}, k\rangle \,\mathrm{tr}\big\{N^{-1/2} V_m^{n\dagger}\, |j\rangle\langle k|\big\} \\ &= \frac{1}{\sqrt{N}} \sum_{k,m,n} |B_{m,n}, k\rangle\langle k|V_m^{n\dagger}|j\rangle \\ &= \frac{1}{\sqrt{N}} \sum_{m,n} (\mathbf{1}\otimes\mathbf{1}\otimes V_m^{n\dagger})|B_{m,n}, j\rangle\,, \end{aligned} \tag{3.26}$$

where the completeness of the Bell basis, the trace relation (3.3), and the completeness of the computational basis are exploited.

Now, to teleport an unknown state $|\psi\rangle = \sum_j |j\rangle\psi_j$ from q-nit 2 to q-nit 3, we prepare q-nits 1 and 3 in their Bell seed state, so that the initial three–q-nit state is

$$\frac{1}{\sqrt{N}} \sum_{j,k} |k^*, j, k\rangle\psi_j = \frac{1}{N} \sum_{m,n} (\mathbf{1}\otimes\mathbf{1}\otimes V_m^{n\dagger})|B_{m,n}, \psi\rangle\,. \tag{3.27}$$

A von Neumann measurement in the Bell basis for q-nits 1 and 2 will find one of the generalized Bell states, $|B_{m,n}\rangle$ say, all N^2 outcomes being equally probable. Conditioned on the said measurement result, the state ket for q-nit 3 is then $V_m^{n\dagger}|\psi\rangle$, which is turned into $|\psi\rangle$ by performing the unitary transformation described by the shift operator V_m^n. In effect, the unknown state $|\psi\rangle$ has been teleported successfully and without any distortion from q-nit 2 to q-nit 3. If, at the time of the Bell measurement on q-nits 1 and 2, they are separated from q-nit 3 by a space-like distance, there exists no classical counterpart for this quantum teleportation.

3.4. *Quantum cryptography, covariant cloning machines, and error operators*

In quantum cryptography, MUB play an important role because they maximize uncertainty relations which ensures the confidentiality of protocols for quantum key distribution.[34–36] For instance, the celebrated BB84 protocol[34] consists of encrypting the message in a q-bit state that is chosen at random between four states

that belong to two MUB. The relevance of MUB for quantum cloning has also been recognized,[21,37,38] which is not unexpected in view of the close link between cloning and the security of key distribution protocols: as a rule, the most dangerous eavesdropping attacks can be realized with the aid of optimized one-to-two cloners — the so-called phase-covariant cloner,[39–41] for instance, when attacking the BB84 protocol.

The symmetry properties of the Bell states have important implications in the theory of cloning machines,[21,38] as we shall sketch briefly now. Under very general conditions,[29] optimal cloning states obey Cerf's ansatz,[37]

$$|\Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} |B_{m,n}, B_{\ominus m,\ominus n}\rangle \gamma^{\ominus m\odot n} a_{m,n} \\ = \sum_{m,n=0}^{N-1} (\mathbf{1}\otimes V_m^n \otimes \mathbf{1} \otimes V_m^{n\dagger}) |B_{0,0}, B_{0,0}\rangle a_{m,n}\,, \tag{3.28}$$

which is a four–q-nit state that is constructed as a linear superposition of states that have q-nits 0 and 1 in the m,n Bell state and q-nits 2 and 3 in the $\ominus m, \ominus n$ Bell state. The coefficients $a_{m,n}$ are arbitrary, their values specify the particular cloning state. Q-nit 0 will be measured and thus projected onto one of a set of chosen states, q-nits 1 and 3 will be the clones, and q-nit 2 the anticlone (or "machine").

The expansion of the state ket (3.28) in the biorthogonal double-Bell basis, with only N^2 of the N^4 basis states appearing in (3.28), emphasizes a generic property of such cloning states, namely their covariance when passing from one of the MUB to another. This covariance property, which we discussed at the end of Sec. 3.1, is of considerable importance in various contexts, such as cryptography protocols that treat all single–q-nit MUB on the same footing[30,34,38,41] and phase-covariant cloning,[39,40] and also has a bearing on the Mean King's problem of Sec. 4.1.

In the present context, we need yet another symmetry property, namely that the two clones — q-nits 1 and 3 — play complementary roles. To establish this point, we first recall the definition of the generalized Bell states in (3.13) and note that

$$|B_{m,n}^{(01)}, B_{\ominus m,\ominus n}^{(23)}\rangle = \frac{1}{N}\sum_{k,l=0}^{N-1} |k^*, k\oplus m, l^*, l\ominus m\rangle \gamma^{(k\oplus m)\odot n} \gamma^{\ominus(l\ominus m)\odot n}\,, \tag{3.29}$$

where we now employ a notation that indicates which q-nits are paired in the Bell states: 0 with 1, and 2 with 3, as it is the case in (3.28). Alternatively, we can pair 0 with 3 and 2 with 1, which gives

$$|B_{m,n}^{(03)}, B_{\ominus m,\ominus n}^{(21)}\rangle = \frac{1}{N}\sum_{k,l=0}^{N-1} |k^*, l\ominus m, l^*, k\oplus m\rangle \gamma^{(k\oplus m)\odot n} \gamma^{\ominus(l\ominus m)\odot n}\,. \tag{3.30}$$

In fact, the states of (3.29) span the same N^2-dimensional subspace as the states of (3.30) in the N^4-dimensional four–q-nit Hilbert space.

To justify this remark, we evaluate the transition amplitudes,

$$\begin{aligned}\langle B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'} | B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle \\ &= \frac{1}{N^2}\sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\oplus m)\odot n\ominus(l\ominus m)\odot n\ominus(k'\oplus m')\odot n'\oplus(l'\ominus m')\odot n'} \\ &\qquad\qquad \times \langle k'^*, l'\ominus m', l'^*, k'\oplus m' | k^*, k\oplus m, l^*, l\ominus m\rangle \\ &= \frac{1}{N^2}\sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\ominus l\oplus m\oplus m')\odot n}\gamma^{\ominus(k'\ominus l'\oplus m'\oplus m)\odot n'}\gamma^{(m\ominus m')\odot(n\oplus n')} \\ &\qquad\qquad \times \delta_{k',k}\delta_{k'\oplus m',l\ominus m}\delta_{l',l}\delta_{l'\ominus m',k\oplus m}\,, \end{aligned} \tag{3.31}$$

where this product of four Kronecker delta symbols equals $\delta_{k,k'}\delta_{l,l'}\delta_{m\oplus m',l\ominus k}$, a product of only three, with the consequence that

$$\langle B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'} | B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = \frac{1}{N}\gamma^{(m\ominus m')\odot(n\oplus n')}\,. \tag{3.32}$$

For given $|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle$ these are N^2 transition amplitudes, each of modulus N, and therefore no other $B^{(03)}B^{(21)}$ kets can appear on the right-hand side of

$$|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = \frac{1}{N}\sum_{m',n'=0}^{N-1} |B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'}\rangle\gamma^{(m\ominus m')\odot(n\oplus n')}\,. \tag{3.33}$$

It follows that $\langle B^{(03)}_{m',n'}, B^{(21)}_{m'',n''} | B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = 0$ unless both $m'\oplus m''=0$ and $n'\oplus n''=0$, which can be verified directly. In particular, we have

$$|B_{0,0}, B_{0,0}\rangle = |B^{(01)}_{0,0}, B^{(23)}_{0,0}\rangle = \frac{1}{N}\sum_{m,n=0}^{N-1} (\mathbf{1}\otimes V^n_m\otimes\mathbf{1}\otimes V^{n\dagger}_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle\,, \tag{3.34}$$

which we use in (3.28) to arrive at the alternative expansion

$$|\Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} (\mathbf{1}\otimes V^{n\dagger}_m\otimes\mathbf{1}\otimes V^n_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle b_{m,n}\,, \tag{3.35}$$

where the coefficients $b_{m,n}$ are the double Galois–Fourier transforms of the $a_{m,n}$s,

$$b_{m,n} = \frac{1}{N}\sum_{m',n'=0}^{N-1} \gamma^{m\odot n'\ominus n\odot m'} a_{m',n'}\,. \tag{3.36}$$

The stage is now set for a discussion of cloning. When q-nit 0 is measured and found in the state described by the bra $\langle\psi^*|$, the resulting state of q-nits 1–3 is

$$\begin{aligned}|\Psi_{1-3}\rangle &= \sum_{m,n=0}^{N-1} (V^n_m\otimes\mathbf{1}\otimes V^{n\dagger}_m)|\psi, B^{(23)}_{0,0}\rangle a_{m,n} \\ &= \sum_{m,n=0}^{N-1} (V^{n\dagger}_m\otimes\mathbf{1}\otimes V^n_m)|B^{(21)}_{0,0}, \psi\rangle b_{m,n}\,. \end{aligned} \tag{3.37}$$

The resulting statistical operator for q-nit 1, the first clone, is

$$\rho_1 = \mathrm{tr}_{2\&3}\big\{|\Psi_{1-3}\rangle\langle\Psi_{1-3}|\big\} = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle\big|a_{m,n}\big|^2\langle\psi_{m,n}| \tag{3.38}$$

with $|\psi_{m,n}\rangle = V_m^n|\psi\rangle$, and for q-nit 3, the second clone, we obtain

$$\rho_3 = \mathrm{tr}_{1\&2}\big\{|\Psi_{1-3}\rangle\langle\Psi_{1-3}|\big\} = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle\big|b_{m,n}\big|^2\langle\psi_{m,n}|\,. \tag{3.39}$$

The displacement operators V_m^n appear as error operators in (3.38) and (3.39).

There are two extreme complementary situations: if $a_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $\big|b_{m,n}\big|^2 = 1/N^2$, then $\rho_1 = |\psi\rangle\langle\psi|$ is the projector on the target state $|\psi\rangle$ and $\rho_3 = \mathbf{1}/N$ is the completely mixed state, as implied by the ergodicity relation (2.45); but if $b_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $\big|a_{m,n}\big|^2 = 1/N^2$, we get $\rho_1 = \mathbf{1}/N$ and $\rho_3 = |\psi\rangle\langle\psi|$. In intermediate situations, both ρ_1 and ρ_3 are imperfect copies of $|\psi\rangle\langle\psi|$.

We see that, as a consequence of the Galois–Fourier relation (3.36), the two clones are complementary to each other in the sense that if one of them projects on the target state $|\psi\rangle$, then the other is completely mixed. More generally, if one clone is in a pure state (not necessarily the target state), then the other clone is in the completely mixed state.

This complementarity is important because it helps us to understand the main idea underlying quantum cryptography: if the first clone is received by Bob, to whom it appears as the target state with an admixture of noise, and the second clone is eavesdropper Eve's imperfect copy (she also has access to the anticlone), then the more Eve knows about Alice's or Bob's signals, the less strongly their signals are correlated. In other words, when the entanglement between two of the three parties becomes stronger, the entanglement with the third party weakens, an idea that was already central to the first entanglement-based protocol, the 1991 Ekert protocol.[42] For obvious reasons, this property is sometimes referred to as the "monogamy of quantum entanglement."

We further note that the Heisenberg–Weyl group is not only related to the error operators that describe the imperfections of the clones, it is also directly related to error correcting codes.[43,44] For instance, the Shor code for q-bits (see, e.g., Ref. 44) exploits the fact that the Pauli σ operators are an operator basis in the q-bit space. Higher-dimensional generalizations of this code likewise exploit that the Heisenberg–Weyl operators, essentially the shift operators of (2.38), constitute an operator basis, especially in the many–q-bit case ($N = 2^{\mathrm{M}}$).

4. The Mean King's problem and quantum state tomography

4.1. *The Mean King's problem in prime power dimensions*

The "Mean King's Problem" originated in the 1987 paper by Vaidman, Aharonov, and Albert,[45] which deals with the $N = 2$ case. Generalizations first to $N = 3$,[46]

then to N prime,[8] and finally to prime-power values of N,[47,48] were completed some 15 years later. In the simplest case ($N = 2$), the problem can be presented as in Ref. 8:

> The Mean King challenges a physicist, Alice, who got stranded on the remote island ruled by the king, to prepare a spin-$\frac{1}{2}$ atom in any state of her choosing and to perform a control measurement of her liking. Between her preparation and her measurement, the king's men determine the value of either σ_x, σ_y, or σ_z. Only after she completed the control measurement, the physicist is told which spin component has been measured, and she must then state the result of that intermediate measurement correctly.

In dimension N, where N is a prime power, the challenge can be summarized in this way: Alice prepares a q-nit system in any state of her choosing and performs a control measurement of her liking. Between her preparation and her measurement, the king's men measure the q-nit in one of the $N + 1$ MUB. The particular basis chosen for the intermediate measurement is communicated to Alice only after she has completed the control measurement, and she must then state the result of that intermediate measurement correctly.

The power of entanglement enables Alice to raise to this challenge. Her solution consists of four stages:

(i) She prepares q-nit 1, which will be handed to the king's men, jointly with q-nit 0, which she will keep for herself, in the Bell state $|B_{0,0}\rangle$ of (3.10).

(ii) The king's men measure q-nit 1 in the ith basis of the MUB and find it in the kth state, whereafter the state ket of the q-nit pair is $|e_k^{i*}, e_k^i\rangle$; there is a total of $N(N + 1)$ states of this kind.

(iii) Alice measures the q-nit pair in the entangled basis composed of the N^2 pairwise orthogonal states $|(m, n)\rangle$ that are given by

$$|(m,n)\rangle = (V_m^{n*} \otimes V_m^n)|(0,0)\rangle \quad \text{for } m,n = 0,1,\ldots,N-1$$
$$\text{with the "seed"} \quad |(0,0)\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N} |e_0^{i*}, e_0^i\rangle - |B_{0,0}\rangle\,. \tag{4.1}$$

Alice's measurement outcome is an ordered pair of field elements (m, n).

(iv) Now, being told that the ith basis was measured at the intermediate stage (ii), and having her outcome (m, n) of the control measurement of stage (iii) at hand, Alice *correctly* infers that the king's men found q-nit 1 in state $|e_k^i\rangle$ with

$$k = \begin{cases} i \odot m \ominus n & \text{for } i = 0,1,\ldots,N-1\,, \\ m & \text{for } i = N\,. \end{cases} \tag{4.2}$$

As shown in Ref. 48, this solution is a special case of Aravind's very general solution,[47] which is formulated without a particular choice for the maximal set of MUB; Our solution exploits the specific MUB of Secs. 2.2–2.4. For $N = 2$, 3, 4, and 5, all maximal sets of MUB are equivalent,[49,50] in the sense that they can be

turned into each other by unitary transformations combined with permutations of the basis kets; more about this in Sec. 5. This equivalence could be true for all prime N, but it is surely not the case for $N = 8$ and $N = 16$.[51,52]

The explanation how Alice's scheme works begins with first noting the explicit form of the two–q-nit states $|(m,n)\rangle$ of Alice's measurement basis,

$$|(m,n)\rangle = \frac{1}{\sqrt{N}} \left(|e_m^{N*}, e_m^N\rangle + \sum_{i=0}^{N-1} |e_{i\odot m\ominus n}^{i*}, e_{i\odot m\ominus n}^{i}\rangle \right) - |B_{0,0}\rangle \,, \tag{4.3}$$

where the sum over i does not include the computational basis ($i = N$), as it does for the seed in (4.1). With the aid of (2.49), the invariance property (3.17), and $\langle e_k^{i*}, e_k^i | B_{0,0}\rangle = N^{-1/2}$, we then establish

$$\langle B_{0,0}|(m,n)\rangle = \frac{1}{N} \tag{4.4}$$

and

$$\langle e_k^{i*}, e_k^i|(m,n)\rangle = \begin{cases} \delta_{k,i\odot m\ominus n}/\sqrt{N} & \text{for } i = 0,1,\ldots,N-1\,, \\ \delta_{k,m}/\sqrt{N} & \text{for } i = N\,, \end{cases} \tag{4.5}$$

from which follows the orthonormality

$$\langle (m,n)|(m',n')\rangle = \delta_{m,m'}\,\delta_{n,n'}\,, \tag{4.6}$$

thus confirming that the kets $|(m,n)\rangle$ constitute an orthonormal basis in the N^2-dimensional space of two–q-nit kets.

Now, after the king's men find q-nit 1 in the kth state of the ith basis, the q-nit pair is in the state described by the bra $\langle e_k^{i*}, e_k^i|$. Clearly then, the Kronecker delta symbols in (4.5) enable Alice to infer the k value in accordance with (4.2). For, only a single k value is possible for the actual outcome (m,n) of Alice's control measurement and the ith basis chosen by the king's men.

It is important that Alice can always infer the correct k value with certainty. This aspect can be understood, or illustrated, by a geometrical picture, in the sense of affine geometry (more about this in Sec. 4.3). When the king's men find the kth state of the ith basis (where i runs from 0 to N, and k from 0 to $N-1$) N of the N^2 detectors fire with equal probability in Alice's control measurement, namely the detectors whose (m,n) values appear in

$$|e_k^{i*}, e_k^i\rangle = \begin{cases} \dfrac{1}{\sqrt{N}} \displaystyle\sum_{m=0}^{N-1} |(m, i\odot m\ominus k)\rangle & \text{for } i = 0,1,\ldots,N-1\,, \\ \dfrac{1}{\sqrt{N}} \displaystyle\sum_{n=0}^{N-1} |(k,n)\rangle & \text{for } i = N\,. \end{cases} \tag{4.7}$$

Accordingly, in the $N \times N$ discrete plane (grid) spanned by the pairs (m,n) the labels of these detectors are on the straight lines $m \mapsto n = i\odot m\ominus k$ with slope i when $i = 0,1,\ldots,N-1$, and on the "vertical" lines $m = k$ when $i = N$. Figure 1 shows the five grids for $N = 4$.

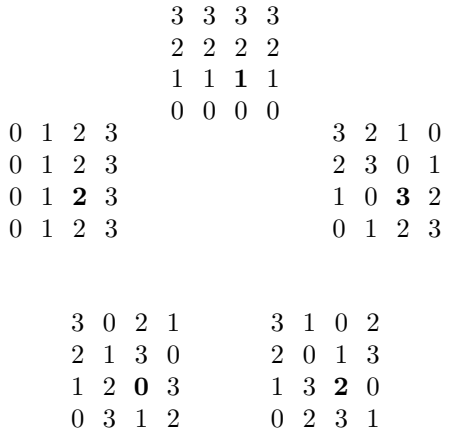

Fig. 1. Mean King Problem for $N = 4$. The five 4×4 grids show the k values for $i = 0, \ldots, 4$ clockwise, with $i = 0$ at the top. In each (m, n) grid, the columns are labeled by m from left to right, and the rows are labeled by n from bottom to top. For example, we have $k = 2$ for $(m, n) = (2, 1)$ in the grid for $i = 2$.

As emphasized by Aravind,[47] the existence of a finite field with N elements is absolutely necessary for the solution. This is also true in this geometrical picture: because the addition $\oplus$ and multiplication $\odot$ form a field, exactly one straight line of given slope passes through each point of the grid, which is a sine qua non condition for unambiguously inferring which detector fired during the king's men's measurement.

In Alice's measurement bases (4.3), the $N(N+1)$ two–q-nit states $|e_k^{i*}, e_k^i\rangle$ are grouped into N^2 sets of $N+1$ states, each state appearing in N sets, and each set composed of one state from each of the $N+1$ MUB. The states of the set associated with a measurement outcome (m, n) correspond to the respective $N+1$ grid points; such as the highlighted grid points for $(m, n) = (2, 1)$ in Fig. 1.

The normalized superposition states of the N^2 sets that appear in (4.3),

$$\frac{1}{\sqrt{2N+2}}\left(|e_m^{N*}, e_m^N\rangle + \sum_{i=0}^{N-1} |e_{i\odot m\oplus n}^{i*}, e_{i\odot m\oplus n}^{i}\rangle\right) = \sqrt{\frac{N}{2N+2}}\Big(|(m,n)\rangle + |B_{0,0}\rangle\Big)\,, \tag{4.8}$$

are linearly independent, but they are not pairwise orthogonal. Rather they are the edges of an acute N^2-dimensional pyramid, with angle $\arccos\frac{N+2}{2N+2}$ between each pair of edges, and the invariant Bell state $|B_{0,0}\rangle$ as the symmetry axis of the pyramid. Alice's measurement is the so-called "square-root measurement" for this pyramid, the natural von Neumann measurement associated with the pyramid.[53,54]

4.2. *State tomography with discrete Weyl and Wigner phase-space functions*

Owing to the correspondence (3.2), the expansion of any operator in a one–q-nit operator basis, which is at the heart of quantum tomography, is related to the expansion of a two–q-nit state ket in the corresponding ket basis. In the general situation, we have a positive-operator-valued measure (POVM)[1] for the two–q-nit states,

$$\sum_k |a_k\rangle\langle a_k| = \mathbf{1}\,, \tag{4.9}$$

a sum of N^2 or more hermitian, rank-1, two–q-nit operators. In accordance with the mapping of (3.2)–(3.5), there is a single–q-nit operator A_k for each ket $|a_k\rangle$,

$$|a_k\rangle \longleftrightarrow A_k\,, \tag{4.10}$$

and, in view of the trace rule (3.3), the expansion

$$|x\rangle = \sum_k |a_k\rangle\langle a_k|x\rangle \tag{4.11}$$

of a generic ket $|x\rangle$ then implies the corresponding expansion for the operator X associated with $|x\rangle$,

$$|x\rangle \longleftrightarrow X = \sum_k A_k \,\mathrm{tr}\big\{A_k^\dagger X\big\}\,, \tag{4.12}$$

which is valid for any single–q-nit operator X. This identity is the completeness relation for the operators basis composed of the A_ks.

In the more particular case of an orthonormal basis of N^2 kets (and its adjoint basis of bras), $\langle a_j|a_k\rangle = \delta_{j,k}$, the POVM in (4.9) refers to an ideal von Neumann measurement, and we have the corresponding orthonormality statement for the operator basis: $\mathrm{tr}\big\{A_j^\dagger A_k\big\} = \delta_{j,k}$. This is the situation for the two specific two–q-nit bases that we encountered in Secs. 3.1 and 4.1, respectively: the basis made up by the generalized Bell states $|B_{m,n}\rangle$ of (3.13), and the basis composed of Alice's "mean king states" $|(m,n)\rangle$ of (4.3). The operator basis corresponding to the ket basis of Bell states is the Galois field version of Weyl's unitary operator basis[2,3] of Sec. 1.1, and the operator basis associated with the ket basis of mean-king states is a candidate for a discrete analog of the familiar hermitian Wigner basis for a continuous degree of freedom.[55]

[1]POVM, with its emphasis on "measure" and the connotations of measure theory, is mathematical terminology. The corresponding quantum-physics terms POM (probability operator measurement) refers to the physical significance.

4.2.1. *Discrete Weyl-type unitary operator basis and phase-space function*

When we identify the Bell kets $|B_{m,n}\rangle$ with the basis kets $|a_k\rangle$ in (4.10), the mapping (3.13) tells us that $N^{-1/2}V_m^n$ corresponds to A_k, and the completeness relation (4.12) acquires the form

$$X = \frac{1}{N}\sum_{m,n=0}^{N-1} V_m^n\, x_m^n \qquad \text{with} \quad x_m^n = \mathrm{tr}\big\{V_m^{n\,\dagger}\, X\big\}\,. \tag{4.13}$$

The unitary shift operators V_m^n compose the operator basis, and the coefficients x_m^n make up the discrete phase-space function $(m,n) \mapsto x_m^n$ of Weyl-type. The mapping of the operator X to its Weyl-type phase-space function is one-to-one: there is a unique single–q-nit operator X to the given set of coefficients $\{x_m^n\}_{m,n=0}^{N-1}$, and all x_m^ns are uniquely specified by the given operator X. In particular, we have

$$x_0^0 = \mathrm{tr}\big\{X\big\}\,. \tag{4.14}$$

Since the unitary operators U_l^i of the abelian subgroups of Sec. 2.4 comprise all the shift operators V_m^n, with the identity $\mathbf{1} = V_0^0 = U_0^i$ appearing $N+1$ times, once for each subgroup ($i = 0, 1, \ldots, N$), an alternative way of presenting (4.13) is

$$X = \frac{\mathbf{1}}{N}\mathrm{tr}\big\{X\big\} + \frac{1}{N}\sum_{i=0}^{N}\sum_{l=1}^{N-1} U_l^i \bar{x}_l^i \qquad \text{with} \quad \bar{x}_l^i = \mathrm{tr}\big\{U_l^{i\,\dagger}\, X\big\}\,. \tag{4.15}$$

The coefficients in (4.13) and (4.15) are related to each other by

$$\bar{x}_l^i = \begin{cases} \alpha_l^{i\,*}\, x_l^{i\odot l} & \text{for } i = 0, 1, \ldots, N-1\,, \\ x_0^l & \text{for } i = N\,, \end{cases} \tag{4.16}$$

which is an immediate consequence of (2.47) and (2.51). The two expansions (4.13) and (4.15) are really the same expansion twice, differing solely be the labeling of the terms.

Weyl tomography, on many identically prepared q-nits with statistical operator ρ, amounts to measuring equal fractions of the q-nits in the $N+1$ MUB of Secs. 2.2–2.4. The measurements provide the probabilities $\langle e_k^i|\rho|e_k^i\rangle$,[m] from which the expansion coefficients

$$\bar{r}_l^i = \mathrm{tr}\big\{U_l^{i\,\dagger}\rho\big\} = \sum_{k=0}^{N-1} \gamma^{\ominus k\odot l}\langle e_k^i|\rho|e_k^i\rangle \tag{4.17}$$

can then be computed, as follows from (2.48). With $X \to \rho$, $\mathrm{tr}\big\{X\big\} \to 1$, $\bar{x}_l^i \to \bar{r}_l^i$ in (4.16), the statistical operator ρ is parameterized in terms of the unitary Weyl basis U_l^i and the measured coefficients $\bar{r}_l^i$.

[m] This is an idealization of the real physical situation. Any actual experiment will give the relative frequencies from which the probabilities can be estimated. The subtleties of *quantum state estimation* are the subject matter of Ref. 56.

There are N measurement outcomes for each of the $N+1$ MUB, so that one is measuring a total of $N(N+1)$ probabilities (or relative frequencies) in order to determine the N^2-1 parameters of the statistical operator. Clearly, there is some redundancy in the data, namely that $\vec{r}_0^{\,i}=1$ for all $N+1$ values of i. Nevertheless, the measurement of the $N+1$ MUB realizes state tomography that is optimal in the sense of Ref. 13: Other choices of $N+1$ von Neumann measurements, not composed of bases that are pairwise MU, give estimates for the statistical operator with larger statistical errors when measuring finite samples, as is always the situation in practice.

Yet, when we regard the measurements of the $N+1$ bases, on equal fractions of the q-nits, as jointly defining a POVM with $N(N+1)$ outcomes, then these are more outcomes than are really needed to determine N^2-1 parameters. More economic, and thus optimal in a different sense, are POVMs with the minimal number of N^2 outcomes (the one constraint of unit total probability is always there). And among those, a particularly good choice is the "symmetric informationally complete" (SIC) POVM.[57] This is a different story, however, which does not need the structure of an underlying Galois field, a ring structure suffices; see Refs. 58 and 59 for further information.

4.2.2. *The limit $N\to\infty$ of continuous degrees of freedom*

At the end of Sec. 2.3 — recall (2.30) and (2.31) — we observed that the unitary shift operators $V_m^n=V_0^nV_m^0$ are products of M factors, one for each constituent q-pit,[n]

$$V_m^n=\prod_{j=0}^{\mathrm{M}-1}\left(V_0^{g_j}\right)^{\underline{n}_j}\left(V_{p^j}^0\right)^{m_j}=\prod_{j=0}^{\mathrm{M}-1}V_{\underline{n}_jg_j\,m_jp^j}^{\phantom{\underline{n}_jg_j}}\,, \tag{4.18}$$

where the m_js are the p-ary coefficients of m as in (2.1), and the $\underline{n}_j$s are the conjugate coefficients of n in the sense of (2.33). There are p^2 unitary shift operators $V_{\underline{n}_jg_j\,m_jp^j}^{\phantom{\underline{n}_jg_j}}$ for each j value, and those referring to different j values commute with each other. Accordingly, the factorization (4.18) is a decomposition of V_m^n into the Weyl operator bases of the individual M q-pits that make up the q-nit.

It is, therefore, systematic to regard the q-nit as a system of M q-pit degrees of freedom, rather than a single q-nit degree of freedom. The limit $N\to\infty$ is then understood as $p\to\infty$ for the given value of M, so that we obtain M continuous degrees of freedom or, put differently, a M-dimensional continuous system.

In view of the factorization observed above, the limit $p\to\infty$ is carried out for each of the M q-pits individually. The details, and the subtleties, of this $p\to\infty$ limit are discussed in Sec. 1.1.7.

[n] As in (2.33), read the product $\underline{n}_jg_j$ as the number $\underline{n}_j$ multiplying the row of p-ary coefficients for g_j, so that the outcome is the field element $\underline{n}_j\odot g_j$. A similar remark applies to the product m_jp^j, except that in this case there is no difference between the number product of m_j and p^j and the field product.

4.2.3. *Discrete Wigner-type hermitian operator basis and phase-space function*

When we identify the two–q-nit kets $|(m,n)\rangle$ of Alice's mean-king basis in (4.3) with the basis kets $|a_k\rangle$ of (4.9), the corresponding single–q-nit operator basis is composed of the operators $W_{m,n}$ that we get from the correspondence (3.2),[48]

$$|(m,n)\rangle\sqrt{N} \leftrightarrow W_{m,n} = |e^N_m\rangle\langle e^N_m| + \sum_{i=0}^{N-1} |e^i_{i\odot m\ominus n}\rangle\langle e^i_{i\odot m\ominus n}| - \mathbf{1}\,, \tag{4.19}$$

with a conventional removal of the factor $1/\sqrt{N}$ from the definition of the $W_{m,n}$s. These operators are hermitian, normalized to unit trace, and pairwise orthogonal,

$$W^\dagger_{m,n} = W_{m,n}\,, \quad \mathrm{tr}\big\{W_{m,n}\big\} = 1\,, \quad \mathrm{tr}\big\{W_{m,n}W_{m',n'}\big\} = N\delta_{m,m'}\delta_{n,n'}\,, \tag{4.20}$$

and their completeness relation is stated by

$$\rho = \frac{1}{N}\sum_{m,n=0}^{N-1} r_{m,n}W_{m,n} \qquad \text{with} \quad r_{m,n} = \mathrm{tr}\big\{\rho W_{m,n}\big\} \tag{4.21}$$

for the statistical operator ρ, but is equally valid for any single–q-nit operator X. The coefficients $r_{m,n}$ are the discrete analog of the familiar Wigner phase-space function for a continuous degree of freedom.

According to Wootters and his collaborators,[60–62] an operator basis is acceptable as a discrete analog of the continuous basis underlying Wigner's phase space function[55] if it meets five criteria:

(W1) each basis operator is hermitian;
(W2) each basis operator has unit trace;
(W3) the basis operators are pairwise orthogonal;
(W4) the basis as a whole, that is: the set of N^2 basis operators, is invariant under the unitary tranformations of the N^2 Weyl operators;
(W5) the marginals of the operator basis are rank-1 projectors, whereby the N projectors associated with parallel lines are mutually orthogonal and thus compose a basis for the kets and bras, with MUB for different sets of parallel lines.

(4.22)

To these we add a sixth criterion:

(W6) in the limit $N \to \infty$ the sequence of discrete bases converges to the standard continuous Wigner basis. (4.23)

It seems to us that (W6) is necessary to justify the term "discrete Wigner-type basis."

Criteria (W1)–(W3) are the three statements in (4.20), and criterion (W4) is an immediate consequence of (2.68) , that is:

$$W_{m,n} = V^n_m\, W_{0,0}\, V^{n\,\dagger}_m = V^{n\ominus n'}_{m\ominus m'}\, W_{m',n'}\, V^{n\ominus n'\,\dagger}_{m\ominus m'} \tag{4.24}$$

for all m, n and all m', n'. Just like $|(0,0)\rangle$ is the seed for the ket basis (4.1), $W_{0,0}$ is the seed of the operator basis (4.19).

Regarding criterion (W5), we first note that a *marginal operator*, or simply: marginal, of the basis is the equal-weight average of all basis operators on an affine straight line. We specify a particular straight line by requiring that all m, n values on the line obey $a \odot m = b \odot n \oplus c$ where a, b, c is any trio of field elements, excluding solely the choice of $a = b = 0$. Clearly, the trio $a \odot d, b \odot d, c \odot d$ with $d \neq 0$ specifies the same line, and the lines for a_1, b_1, c_1 and a_2, b_2, c_2 are parallel if $a_1 \odot b_2 = a_2 \odot b_1$, whereas they intersect in one m, n point if $a_1 \odot b_2 \neq a_2 \odot b_1$.

Accordingly, the marginal operators are

$$M_{a,b,c} = \frac{1}{N} \sum_{m,n=0}^{N-1} W_{m,n} \delta_{a\odot m, b\odot n\oplus c} = \begin{cases} |e^{a\oslash b}_{c\oslash b}\rangle\langle e^{a\oslash b}_{c\oslash b}| & \text{if} \quad b \neq 0\,, \\ |e^{N}_{c\oslash a}\rangle\langle e^{N}_{c\oslash a}| & \text{if} \quad b = 0 \text{ and } a \neq 0\,, \end{cases} \tag{4.25}$$

and the not-a-marginal case $a = b = 0$, for which $M_{0,0,c} = \delta_{c,0}\mathbf{1}$, illustrates an ergodic property of the Wigner basis,

$$\frac{1}{N} \sum_{m,n=0}^{N-1} W_{m,n} = \mathbf{1}\,. \tag{4.26}$$

Another way of stating the explicit projector values of the marginals is

$$|e^i_k\rangle\langle e^i_k| = \begin{cases} M_{i,1,k} = \dfrac{1}{N} \displaystyle\sum_{m=0}^{N-1} W_{m,i\odot m\ominus k} & \text{for} \quad i = 0, 1, 2, \ldots, N-1\,, \\ M_{1,0,k} = \dfrac{1}{N} \displaystyle\sum_{n=0}^{N-1} W_{k,n} & \text{for} \quad i = N\,, \end{cases} \tag{4.27}$$

which we recognize as the single–q-nit operator version of the two–q-nit identities in (4.7). Indeed, the projectors for the N parallel lines with slope $a \oslash b = i$ make up the ith basis for $i = 0, 1, \ldots, N-1$, while the computational basis ($i = N$) is obtained for the "vertical" lines with $b = 0$. These are, of course, the sets of parallel lines that we encountered in Sec. 4.1, as illustrated in Fig. 1. One could say that the relations (4.19) and (4.25) are reciprocals of each other: the projectors $|e^i_k\rangle\langle e^i_k|$ are marginals of the basis operators $W_{m,n}$, and the $W_{m,n}$s are marginals of the projectors (up to a subtraction of the identity operator).

The reciprocity of the relations (4.19) and (4.25) is even more striking if, following the geometrical approach emphasized in Sec. 1.2, we define the vectors of $\mathbf{R}^{N^2-1}$ that are naturally associated with the Wigner operators $W_{m,n}$ and the projectors $|e^i_k\rangle\langle e^i_k|$,

$$\begin{aligned} \mathbf{w}_{m,n} &= \mathcal{W}_{m,n} - \varrho_\star \mathrel{\widehat{=}} W_{m,n} - \rho_\star\,, \\ \mathbf{p}^i_j &= \psi^i_k {\psi^i_k}^\dagger - \varrho_\star \mathrel{\widehat{=}} |e^i_k\rangle\langle e^i_k| - \rho_\star\,, \end{aligned} \tag{4.28}$$

where the matrix $\mathcal{W}_{m,n}$ represents $W_{m,n}$, and ψ_k^i is the column for $|e_k^i\rangle$. It clearly results from the ergodicity condition (4.26) that the $\mathbf{w}_{m,n}$s obey

$$\sum_{m,n=0}^{N-1} \mathbf{w}_{m,n} = 0\,. \tag{4.29}$$

The $\mathbf{w}_{m,n}$s are thus the corners of a regular simplex in $\mathbf{R}^{N^2-1}$, and this is how we want to think about them now. We refer to the $\mathbf{w}_{m,n}$s as the face points.

Equations (4.19) and (4.27) now appear as

$$\mathbf{w}_{m,n} = \mathbf{p}_m^N + \sum_{i=0}^{N-1} \mathbf{p}_{i\odot m\ominus n}^i\,, \tag{4.30}$$

and

$$\begin{aligned} \mathbf{p}_k^i &= \mathcal{M}_{i,1,k} = \frac{1}{N}\sum_{m=0}^{N-1} \mathbf{w}_{m,i\odot m\ominus k} \quad \text{for } i = 0,1,2,\ldots,N-1\,,\\ \mathbf{p}_k^N &= \mathcal{M}_{1,0,k} = \frac{1}{N}\sum_{n=0}^{N-1} \mathbf{w}_{k,n}\,, \end{aligned} \tag{4.31}$$

where matrix $\mathcal{M}_{a,b,c}$ represents $M_{a,b,c}$ of (4.25).

There is a natural interpretation of (4.31) in $\mathbf{R}^{N^2-1}$: it says that the corners of the MUB polytope lie at the centers of certain specially selected faces of the face point operator simplex. The former has been inscribed into the latter in a special way. Alternatively, (4.30) says that the corners of this simplex lie right above the centers of certain special faces of the MUB polytope. These faces are orthocomplemented to the facets (the highest dimensional faces). To see this, note that $\mathrm{tr}\{W_{m,n}M\}$ = constant defines a hyperplane in $\mathbf{R}^{N^2-1}$, the space of vectors $\mathbf{m}$ that (1.48) associates with the unit-trace hermitian matrices M. All the corners of the MUB polytope lie either in the hyperplane $\mathrm{tr}\{W_{m,n}M\} = 0$, where they span a facet, or in the hyperplane $\mathrm{tr}\{W_{m,n}M\} = 1$, which is the orthocomplemented face. All points in the polytope obey $0 \le \mathrm{tr}\{W_{m,n}M\} \le 1$, for all values of m and n. This underlies the construction of Wootters' analogs of Wigner's function, and it explains why we refer to the vectors $\mathbf{w}_{m,n}$ as face points, and to their unit trace versions $W_{m,n}$ as face point operators.

In passing we note that one can prove a remarkable result in prime dimensions:[63] all statistical operators such that $0 \le \mathrm{tr}\{W_{mn}\rho\}$, which says that their Wigner coefficients are positive, necessarily are convex combinations of projectors onto the states $|e_k^i\rangle$ of the MUB, for which

$$\langle e_k^i|W_{m,n}|e_k^i\rangle = \left\{ \begin{matrix} \delta_{k\oplus n,i\odot m} & \text{for } i = 0,1,\ldots,N-1 \\ \delta_{k,m} & \text{for } i = N \end{matrix} \right\} = 0 \text{ or } 1\,. \tag{4.32}$$

In other words, the statistical operators $|e_k^i\rangle\langle e_k^i|$ belong to the polytope. So, the equation $0 \le \mathrm{tr}\{W_{m,n}M\} \le 1$ is necessary and *sufficient* for belonging to the MUB polytope. We conjecture that this is also true in prime power dimensions.

With criteria (W1)–(W5) taken care of, we finally turn to (W6). As noted in Sec. 4.2.2, the limit $N = p^{\mathrm{M}} \to \infty$ is the limit $p \to \infty$ with a fixed value of M, so that we are consistently dealing with a system composed of M q-pits and arrive at a M-dimensional continuous system in the limit. Contact with the standard Wigner basis is, therefore, established if we get[o]

$$W_{0,0} \to \int \mathrm{d}^{\mathrm{M}}x \,|-x\rangle 2^{\mathrm{M}}\langle x| = P \otimes P \otimes \cdots \otimes P \tag{4.33}$$

in the limit, that is: M copies of the one-dimensional parity operator

$$P = \int_{-\infty}^{\infty} \mathrm{d}x \,|-x\rangle 2\langle x|\,, \tag{4.34}$$

the seed of the Wigner basis,[64,65] where the factor of 2 ensures proper normalization to unit trace, $\mathrm{tr}\{P\} = 1$.

Now, after expressing the projectors in

$$W_{0,0} = \sum_{i=0}^{N} |e_0^i\rangle\langle e_0^i| - \mathbf{1} \tag{4.35}$$

in terms of the unitary shift operators, we have

$$W_{0,0} = \frac{1}{N} \sum_{i=0}^{N-1} \left(V_0^i + \sum_{j=1}^{N-1} \alpha_j^{i\oslash j} V_j^i \right), \tag{4.36}$$

where (2.51) and the $k = 0$ version of (2.65) are the main ingredients. This shows that the seed $W_{0,0}$ — and, therefore, also all other $W_{m,n}$s — is an equal-weight sum of all N^2 operators of the unitary Weyl basis, whereby the phase factors $\alpha_j^{i\oslash j}$ ensure that $W_{0,0}$ is hermitian.

This is illustrated by the $N = 2$ example for which

$$\begin{aligned} W_{0,0} &= \frac{1}{2}(\mathbf{1} + \sigma_x + \sigma_y + \sigma_z)\,, \qquad W_{0,1} = \frac{1}{2}(\mathbf{1} - \sigma_x - \sigma_y + \sigma_z)\,, \\ W_{1,0} &= \frac{1}{2}(\mathbf{1} + \sigma_x - \sigma_y - \sigma_z)\,, \qquad W_{1,1} = \frac{1}{2}(\mathbf{1} - \sigma_x + \sigma_y - \sigma_z)\,, \end{aligned} \tag{4.37}$$

are well-known q-bit analogs of the Wigner basis operators. In an ill-fated attempt, Feynman used the expectation values of these operators to introduce probabilities of "$\sigma_x = 1$ *and* $\sigma_z = 1$" and the like. But since the eigenvalues of the four operators in (4.37) are $\frac{1}{2}(1 \pm \sqrt{3})$, he was forced to resort to the dubious notion of "negative probabilities" which, in fact, gave his last paper its title.[66] A direct measurement of the said expectation values, for the polarization q-bit of a photon, is reported in Ref. 67.

[o]The integration in (4.33) is over the M-dimensional real space, $x = (x_0, x_1, \ldots, x_{\mathrm{M}-1})$ with each coefficient x_j taking on all real values.

In the limit $p \to \infty$, only odd values of p are relevant, and for those $j = (j \oslash 2) \oplus (j \oslash 2)$ is true, which allows us to write

$$V_j^i = \gamma^{i \odot j \oslash 2} V_{j \oslash 2}^0 V_0^i V_{j \oslash 2}^0 \tag{4.38}$$

with the aid of (2.40) and, *if* we choose the symmetric value of (2.55) for α_l^i, we have

$$\alpha_j^{i \oslash j} \gamma^{i \odot j \oslash 2} = 1 \tag{4.39}$$

for the product of phase factors, that is: *if* we enforce the symmetry property (2.63). With this symmetry in place, then, the seed is $(j \to 2 \odot k)$

$$\begin{aligned} W_{0,0} &= \frac{1}{N} \sum_{i,k=0}^{N-1} V_k^0 V_0^i V_k^0 = \sum_{k=0}^{N-1} V_k^0 |0\rangle\langle 0| V_k^0 \\ &= \sum_{k=0}^{N-1} |k\rangle\langle \ominus k| = \sum_{k=0}^{N-1} |e_k^i\rangle\langle e_{\ominus k}^i| \,, \end{aligned} \tag{4.40}$$

where the value of the last summation does not depend on the basis label i. This is clearly the discrete analog of the continuous M-dimensional parity operator P in (4.33),

$$W_{0,0} = \sum_{k=0}^{N-1} |\ominus k\rangle\langle k| = \sum_{k_0=0}^{p-1} |-k_0\rangle\langle k_0| \otimes \sum_{k_1=0}^{p-1} |-k_1\rangle\langle k_1| \otimes \cdots \,, \tag{4.41}$$

the product of M factors of the analog of the one-dimensional parity operator in (4.34). And since the unitary shift operators factorize in accordance with (4.18), this factorization of the Wigner seed carries over to all operators of the Wigner basis. The limit $p \to \infty$, then, gives us the right-hand side of (4.33) as desired.[P]

In summary, the basis composed of the operators $W_{m,n}$ as defined in (4.19) obeys criteria (W1)–(W5) by construction, and also criterion (W6) if the symmetry property (2.63) is imposed on the phase factors α_l^i of (2.51). We then have a genuine analog of the standard Wigner basis for continuous degrees of freedom, and it is fair terminology to call the $W_{m,n}$s the elements of the N-dimensional Wigner basis, as we have already been doing above.

It is worth remembering, however, that *all* permissible choices for the α_l^i give a good hermitian operator basis for which (W1)–(W5) are true, and the limit $p \to \infty$ is of little concern for any particular value of $N = p^{\mathrm{M}}$ at hand. If one makes use of the option discussed in the paragraph after (2.54) and multiplies the right-hand side

[P]This limit has its subtleties (see the references cited in Sec. 1.1.7) and requires careful attention to the factor of 2^{M} in (4.27) which, roughly speaking, originates in

$$\mathrm{tr}\{|\ominus k\rangle\langle k|\} = \delta_{2 \odot k, 0} = \delta_{k,0} \to \delta(x) = 2^{\mathrm{M}} \delta(2x) = \mathrm{tr}\{|-x\rangle 2^{\mathrm{M}} \langle x|\} \,.$$

of (2.55) by $\gamma^{b_i \odot l}$ with $b_0 = 0$ and arbitrary field elements b_i for $i = 1, 2, \ldots, N-1$, then

$$W_{0,0}^{(b)} = \frac{1}{N} \sum_{i,k=0}^{N-1} \gamma^{2 \odot b_i \odot k} V_k^0 V_0^i V_k^0 \tag{4.42}$$

replaces the $b_i \equiv 0$ version of (4.40). If one or more of the b_is are nonzero, $W_{0,0}^{(b)}$ is different from all $W_{m,n}$s and, therefore, the hermitian operator basis generated from the seed $W_{0,0}^{(b)}$ is different from the Wigner basis — the parity operator (4.41) is not one of the basis operators. There are in total N^{N-1} different seeds $W_{0,0}^{(b)}$ and as many hermitian operator bases and with suitable $N \to \infty$ limits for the b_is the seeds will have well-defined limits themselves, but in our understanding only the $b \equiv 0$ basis is a true finite-dimensional analog of the Wigner basis.[q]

We thus observe that the symmetric choice of (2.55) is the right choice for obtaining a proper analog of the Wigner basis. It also endows the Wigner basis with certain elegant covariance properties[48] that will be discussed in Sec. 4.2.4.

We further note that the property (W5) is sufficient to derive that each Wigner operator is equal to the sum of projectors onto states from different bases minus the identity operator as expressed by (4.19); the explicit choice of MUB that we made in Sec. 2 is not crucial. Indeed, the sum of all the Wigner operators that belong to the $N+1$ (nonparallel) straight lines passing through a phase space point (m, n) is also equal to the sum of all Wigner operators plus N times $W_{m,n}$; as a consequence of (W5) it also equals N times a sum of the projectors onto states from different bases; now, the sum of all Wigner operators equals N times the identity as noted in (4.26). It follows that each Wigner operator plus the identity operator is equal to a sum of projectors onto states from different bases.

This is how Wootters *et al.* derived an expression for (loosely analogous) Wigner operators similar to (4.19),[62] which may or may not possess property (W6). Their approach is somewhat more general than ours in the sense that theirs is valid whichever set of $N+1$ MUB is adopted, whereas the expression (4.19) refers explicitly to the bases defined in (2.67) and specified unambiguously by the phase factors α_l^i that obey the constraints (2.52) and (2.53).

In view of the properties (W1) to (W5) in (4.22), in particular the marginals property (W5), it is natural to interpret the Wigner operators as discrete phase-space localization operators.[61,62] Indeed, when the system is in a "position" eigenstate $|e_k^N\rangle$, the expectation value of $W_{m,n}$ equals 0 for $k \neq m$, and $1/N$ for $k = m$, irrespective of the "momentum label" n. Similarly, when the system is prepared in a "momentum" eigenstate $|e_l^0\rangle$, the expectation value is 0 for $l \neq \ominus n$, and $1/N$ for $l = \ominus n$, whatever the value of the "position label" m. This situation is reminiscent

[q]In arbitrary odd dimensions N, one can also introduce a Wigner-type operator basis by modifying the parity operator of (4.43) through a replacement of the field arithmetic by modulo-N arithmetic ($\ominus \to \ominus_N$). Consult Refs. 48, 63, 68 for details.

of the uncertainty principle:[69] when we have a state of sharp position, here: $|e_k^N\rangle$, then the value of the position is definite while all values of the momentum label are equally probable; and the analogous reverse case applies to states $|e_l^0\rangle$ of sharp momentum.

As appealing as this picture is, it has a flaw: the expectation value of $W_{m,n}$ can be negative. In fact, for odd N, we have

$$W_{0,0}\big(|k\rangle \pm |\ominus k\rangle\big) = \pm\big(|k\rangle \pm |\ominus k\rangle\big) \tag{4.43}$$

for $k = 0, 1, \ldots, N-1$, so that $W_{0,0}$ has the $(N+1)/2$-fold eigenvalue $+1$ and the $(N-1)/2$-fold eigenvalue -1. In view of the unitary equivalence property (W4), explicitly stated in (4.24), these are also the eigenvalues of all other $W_{m,n}$s. It follows that the operators of the Wigner basis are not projectors, but each of them is rather the difference between a projector onto a $(N+1)/2$-dimensional subspace and a projector on a $(N-1)/2$-dimensional subspace.

In (4.19) we have one projector for each of the $N+1$ MUB, and it follows from (4.32) that the expectation value of $W_{m,n}$ is maximal for these states,

$$\langle e_m^N|W_{m,n}|e_m^N\rangle = 1 \quad \text{and} \quad \langle e^i_{i\odot m\ominus n}|W_{m,n}|e^i_{i\odot m\ominus n}\rangle = 1 \quad \text{for } i = 0, 1, \ldots, N-1\,. \tag{4.44}$$

They are, therefore, eigenstates to eigenvalue $+1$, and since they are $N+1$ states in a $(N+1)/2$-dimensional subspace, they are clearly linearly dependent. They are also assuredly complete because the projector on the $+1$ subspace of $W_{m,n}$,

$$\frac{\mathbf{1} + W_{m,n}}{2} = \frac{1}{2}\left(|e_m^N\rangle\langle e_m^N| + \sum_{i=0}^{N-1} |e^i_{i\odot m\ominus n}\rangle\langle e^i_{i\odot m\ominus n}|\right), \tag{4.45}$$

is clearly spanned by those $N+1$ eigenstates, one from each basis.

A direct measurement of the expectation values of all Wigner basis operators — or, put differently, the experimental determination of the N^2 Wigner coefficients $r_{m,n}$ of (4.21) — would thus require the realization of the N^2 binary observables (eigenvalues ± 1) that distinguish the respective subspaces. While possible in principle, such a procedure is not economic in practice, because two different $W_{m,n}$s do not commute, and each $W_{m,n}$ must be measured separately. Indeed, with one exception, all reports of experimentally determined Wigner functions (in the one-dimensional continuous case) are actually Wigner functions that are inferred from measured marginal distributions. The said exception is the experiment of Refs. 70 and 71, which implemented the scheme introduced in Ref. 72.

The geometrical picture offered by the marginals and the corresponding sums over affine straight lines, recall (4.25) and (4.27), sheds some light on the solution of the mean king's problem in Sec. 4.1. As noted above, the correspondence (3.2) links (4.27) to (4.7), and so we understand why the preparation of the state $|e_k^{i\,*}, e_k^i\rangle$ by the king's men is accompanied by the equiprobable firing of N detectors that correspond to the states $|(i_1, i_2)\rangle$ with $i_2 = k$ when $i = N$ and $\ominus i_1 \oplus i \odot i_2 = k$ otherwise. The other detectors do not fire at all. If we re-express this property

in terms of localization operators, in the sense of the paragraph preceding (4.43), we find that the N detectors that have a nonzero probability of firing correspond to localization operators located on a straight line for which the marginal is the projector $|e^i_k\rangle\langle e^i_k|$.

4.2.4. *Covariance of the Wigner-type basis*

Upon projecting (4.3) onto the Bell basis we get

$$|(i_1,i_2)\rangle = \frac{1}{N}\sum_{m,n=0}^{N-1} |B_{m,n}\rangle\gamma^{i_2\odot m\ominus i_1\odot n}\Gamma_{m,n}$$
$$\text{with}\quad \Gamma_{m,n} = \begin{cases} 1 & \text{for } m=0\,,\\ \alpha_m^{n\oslash m} & \text{for } m>0\,, \end{cases} \tag{4.46}$$

where α^i_m is the phase factor of (2.51), explicitly stated in (2.62) for N even and in (2.55) for N odd, provided the symmetry property (2.63) is imposed, as we assume throughout the present discussion. Then ${\Gamma^n_m}^2 = \gamma^{\ominus m\odot n}$, and we can regard the phase factors Γ^n_m as the appropriate square roots of $\gamma^{\ominus m\odot n}$.

Making use of the transformation (3.13) that transforms Bell states into displacement operators we get an alternative expression for the Wigner operator W_{i_1,i_2},

$$W_{i_1,i_2} = \frac{1}{N}\sum_{m,n=0}^{N-1} \gamma^{\ominus i_1\odot n\oplus i_2\odot m}\Gamma_{m,n}V^n_m\,. \tag{4.47}$$

In view of the symmetric choice (2.55), we can rewrite (3.21) for odd N in the form

$$\Gamma_{m,n}V^n_m = C_i\Gamma_{m',n'}V^{n'}_{m'}C_i^\dagger \quad \text{with } i\odot m\ominus n = m' \text{ and } m = n'\,. \tag{4.48}$$

This is the transformation-law of the displacement operators under a change of the underlying basis, the main ingredient on the right-hand side of (4.47). It is sometimes referred to as the *covariance* of the Heisenberg–Weyl group.

Similarly, the permutation invariance (3.23) of the Bell basis under the action of $C_i^*\otimes C_i$ is sometimes referred to as the covariance of the Bell basis. The other permutation invariance, noted in (3.15), is of quite a different kind. But both reflect a general property: the Clifford group of unitary operators is the stabilizer of the Heisenberg–Weyl group.

In addition, the affine transformation (3.24) that maps (m,n) onto (m',n') is a symplectic transformation in the sense that it preserves the symplectic form $m_1\odot n_2\ominus n_1\odot m_2$. Indeed, $m'_1\odot n'_2\ominus n'_1\odot m'_2 = m_1\odot n_2\ominus n_1\odot m_2$ so that

$$C_iW_{i_1,i_2}C_i^\dagger = W_{i'_1,i'_2} \quad \text{with } i\odot i_1\ominus i_2 = i'_1 \text{ and } i_1 = i'_2\,, \tag{4.49}$$

which shows that the Clifford transformations C_i correspond to affine reparameterizations of the phase-space labels of the operators in the Wigner basis, the phase-space localization operators.

The elegant transformation laws (4.48) and (4.49) hold for odd N with the symmetric choice (2.55). What about even prime power dimensions, $N = 2^{\mathrm{M}}$? Here, the expression (2.62) of the phase factors α_l^i is rather intricate and we do not know whether (4.48) and (4.49) are valid. It is an open question whether there is a set of field elements b_i such that, after supplementing the α_l^is of (2.62) by factors $(-1)^{b_i \odot l}$, they conspire to produce (4.48) and (4.49).

But one does know that other properties of Wigner operators, such as the factorization (4.41) into a product of M Wigner operators of dimension p, can only be had for odd p, not for $p = 2$ and $\mathrm{M} > 2$.[73,74] The two–q-bit case $N = 2^2$ is an exception; there are q-quart Wigner operators that factorize into products of two q-bit Wigner operators. They have been realized experimentally for the purpose of biphoton polarimetry.[67]

We emphasize that the requirements (W1) to (W5) in (4.22) are obeyed by the $W_{m,n}$s for all prime power dimensions, even or odd, irrespective of the convention chosen for the α_l^is. And (W6) is of no concern for even N.

4.3. *Mutually unbiased bases and finite affine planes*

The combinatorial structure that underlies the solution of the mean king's problem is known as a finite affine plane of order N. By definition an affine plane is an ordered pair of two sets, the first of which consists of elements a_α, called points, and the second of which consists of subsets L_ω of the first, called lines. Two lines whose intersection is empty are called parallel. The following axioms hold:

A1: If a_α and a_β are distinct points, there is a unique line L_ω such that $a_\alpha \in L_\omega$ and $a_\beta \in L_\omega$.
A2: If a_α is a point not contained in the line L_ω, there is a unique line L_σ such that $a_\alpha \in L_\sigma$ and $L_\sigma \cap L_\omega = \emptyset$.
A3: There are at least two points on each line, and there are at least two lines. (4.50)

To see how this works, think of an ordinary affine plane, and think of it as two sets, the set of points and the set of lines. Two points determine a unique line, while two lines either intersect in a unique point, or else they are parallel and do not intersect at all. This is what the axioms (4.50) say.

If the number of points is finite the affine plane is also said to be finite, and it is assigned a finite number N, called its order. A finite affine plane of order N has exactly N^2 points and $N^2 + N$ lines. Each line contains N points, and $N + 1$ lines intersect in each point. There are altogether $N + 1$ *pencils* of parallel lines containing N lines each. If we label the lines of every pencil with a set of N letters, we can use two of the pencils to provide a "coordinate system" for the affine plane. Each remaining pencil then defines what is known as a Latin square — a square array of N^2 symbols, such that there are N different kinds of symbols, and such

that the same symbol never occurs twice in a row or in a column of the array.[r] Examples can be found in Table 1.

Starting from any pair of pencils, every entry of the array receives an ordered pair of two symbols, and the intersection properties of the affine plane guarantee that these ordered pairs can be used as an alternative coordinate system for the array. Pairs of Latin squares that have this property are said to be orthogonal, or Graeco-Latin.[75] Finite affine planes come with an existence problem of their own; indeed already Euler raised the question whether it is at all possible to find Graeco-Latin squares when $N = 6$. More than a hundred years later it was proved that the answer is "no." This important result was reported in 1900 by the mathematician Terry[76] who proved by combinatoric techniques that Euler's so-called "36 officers problem" did not possess a solution, in agreement with Euler's conjecture.

Finite affine planes do exist if $N = p^{\mathrm{M}}$, where p is a prime number. They do not exist if $N = 4k+1$ or $N = 4k+2$ and N is not the sum of two squares, or if $N = 10$. All other cases are open. If $N = p^{\mathrm{M}}$, a finite affine plane can be constructed using the methods of analytical geometry, with the finite field of order p^{M} as the field of scalars, but examples not of this form are known as well.

A finite affine plane can be turned into a finite projective plane through the addition of an extra line "at infinity." It should be emphasised that finite planes, whether affine or projective, are much more than just interesting toys — in classical computer science they play prominent roles, for instance in the theory of error correcting codes, and we have already seen that they have quantum mechanical applications.

The relation between MUB and finite affine planes can be seen already at the level of the MUB polytope discussed in Sec. 1.2. The idea is to represent the lines by the $N^2 + N$ corners of the polytope, and the points by a subset of its N^{N+1} facets. Two points are to lie on a line if the corresponding corners are corners of the same facets, and two lines intersect in a point if the corresponding facets share a common corner. It turns out[17] that if an affine plane exists such a correspondence can always be set up, and the N^2 selected facets will then be placed in such a way that their centers form a regular simplex in $\mathbf{R}^{N^2-1}$. This construction needs neither finite fields nor the special feature that the corners of the polytope correspond to one-dimensional projectors on Hilbert space. But when they do, it is possible to choose — following Wootters — the special set of Wigner operators that we have discussed, and to relate the construction to the partition of the Heisenberg–Weyl group that is associated with the MUB: then each basis is associated with a straight line that passes through the origin in the plane.

Whether there is a deeper relation between the existence problem for MUB and the existence problem for finite affine planes is not known today, although it has been conjectured that such a relation exists.[77] In the 19th century, the combinatorial structures now known as finite geometries were studied more concretely by

[r] Sudokus are 9×9 Latin squares.

geometers, who realized them as configurations of lines and points, or more generally as configurations of subspaces of complex projective space.[78] In 1844 Hesse, following earlier work by Plücker, studied a configuration of 9 lines and 12 points in the projective plane, such that each line contains 4 points and each point lies on 3 lines.[79] Translated into the language of quantum theory, where the projective plane is the set of rays in a three-dimensional Hilbert space ($N = p = 3$), Hesse's twelve points are indeed the twelve kets that compose the four MUB of three kets each. His construction was generalized to the case of arbitrary prime N by Segre,[80] who therefore in a sense discovered the maximal sets of MUB in prime dimensions — although some necessary ingredients, including the quantum mechanical significance of the construction, were very naturally missing.

Segre's starting point was an elliptic curve in complex projective space,[81] whose symmetry group consists of the Heisenberg–Weyl group together with an extra reflection, an element of order 2. In fact, there are N^2 such reflections, since the Heisenberg–Weyl group acts on them in accordance with (4.24), which corresponds to the condition (W4) in (4.22). In our terminology this means that he introduced a discrete parity operator with the matrix representation[s]

$$[W_{0,0}]_{a,b} = \delta_{0,a\oplus b}\,. \tag{4.51}$$

This operator is both hermitian and unitary, with eigenvalues ± 1, and in fact it splits the Hilbert space into two subspaces, of dimension n and $n-1$ respectively, where $N = 2n-1$. There are altogether N^2 such subspaces of dimension n, and Segre observed that there exists N^2+N vectors such that each subspace contains $N+1$ of the vectors, and each vector lies in exactly N of the subspaces. In the notation used to describe such things, we have a configuration of type

$$\left(N^2_{N+1}, N(N+1)_N\right). \tag{4.52}$$

These incidence relations are exactly those of a finite affine plane. They are clearly quite remarkable: in $N = 2n-1$ dimensions two n-dimensional subspaces intersect in (at least) a single vector, but the remarkable thing is that only N^2+N distinct vectors are needed for the entire configuration. And, of course, once we have chosen the standard representation of the Heisenberg–Weyl group, these N^2+N vectors are precisely the kets that make up the MUB.

To see why this is so, let us go back to the definition of the face point operators in (4.30). The first face point operator is defined by picking one projector from each MUB. Any choice will do. Then the combinatorics of the affine plane — or alternatively the action of the Heisenberg–Weyl group — will define a definite N^2-plet of face point operators. Now consider the kets corresponding to the $N+1$ projectors we picked. Typically, $N+1$ kets will span the N-dimensional Hilbert space. But let us pick "the first vector in each basis" (referring to the standard set

[s]Since N is an odd prime, the field addition $\oplus$ is modulo-N addition.

of MUB of Appendix A), that is: the kets represented by the columns

$$\psi^{(0)} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \qquad \psi^{(r)} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \gamma_N^{r1^2} \\ \gamma_N^{r2^2} \\ \vdots \\ \gamma_N^{r(N-2)^2} \\ \gamma_N^{r(N-1)^2} \end{pmatrix}, \quad 1 \le r \le N\,. \tag{4.53}$$

By inspection we see that they span an n-dimensional subspace only, and indeed that they are all eigenvectors of $W_{0,0}$ to eigenvalue $+1$. Since the face point operators, and the choices of MU vectors made for them, are related by the Heisenberg–Weyl group, there will be altogether N^2 subspaces of this kind, and they will necessarily have the intersection properties discovered by Segre. But to him this was a statement about the geometry of an elliptic curve in projective space, not about quantum mechanics — the latter was still several decades into his future.

Segre's observation holds true in all odd prime power dimensions. In particular, as observed above in the context of (4.43)–(4.45), all Wigner basis operators in odd prime power dimensions possess a $n = \frac{1}{2}(N+1)$-dimensional subspace to eigenvalue $+1$ and a $n-1 = \frac{1}{2}(N-1)$-dimensional subspace to eigenvalue -1.

In marked contrast, no similar construction is known for even N. In this case there is no extra symmetry of order 2 available, a fact that also causes well studied complications when one tries to define analogs of the Wigner function.[82]

5. Mutually unbiased Hadamard matrices

5.1. *Pairs of mutually unbiased bases and Hadamard matrices*

Let us look at the problem of finding MUB from a different perspective. As in Sec. 1.2 we represent kets as column vectors. The kets $|u_0\rangle, |u_1\rangle, \ldots, |u_{N-1}\rangle$ of an orthonormal basis then correspond to the N columns of a unitary matrix U. By convention, the computational basis is represented by the unit matrix $\mathbb{1}$. Then,

$$U = \begin{pmatrix} \langle 0| \\ \langle 1| \\ \vdots \\ \langle N-1| \end{pmatrix} \big(|u_0\rangle, |u_1\rangle, \ldots, |u_{N-1}\rangle\big) \tag{5.1}$$

turns the basis kets into the unitary matrix, and

$$\big(|u_0\rangle, |u_1\rangle, \ldots, |u_{N-1}\rangle\big) = \big(|0\rangle, |1\rangle, \ldots, |N-1\rangle\big)U \tag{5.2}$$

recovers the basis from U.

If the columns of a unitary matrix are permuted, or multiplied with phase factors, the corresponding basis as a whole is unaffected. Therefore, we say that

two matrices are equivalent if and only if they can be related in this way,

$$U_1 \sim U_2 \qquad \Leftrightarrow \qquad U_2 = U_1 P E \,. \tag{5.3}$$

Here P is a permutation matrix and E is a diagonal unitary matrix.

There is a second, stronger notion of equivalence in which matrices that are related by permutations and rephasings of rows are also regarded as equivalent,

$$U_1 \approx U_2 \qquad \Leftrightarrow \qquad U_2 = E_1 P_2 U_1 P_1 E_1 \,. \tag{5.4}$$

In particular this means that we can present every unitary matrix in *dephased form*: with all entries in the first row and the first column chosen to be real and nonnegative. In this respect, the second equivalence relation reminds us of how particle physicists treat their Kobayashi–Maskawa mixing matrix. If the matrix is not dephased it is said to be *enphased*. The *core* of a dephased matrix is its lower right square submatrix of size $N-1$.

Any basis that is unbiased with respect to the computational basis is now represented by a complex *Hadamard matrix* H. This is a rescaled unitary matrix all of whose matrix elements have unit modulus,

$$|H_{i,j}|^2 = 1 \,, \quad i,j = 0,\ldots,N-1 \quad \text{and} \quad H H^\dagger = N \mathbb{1} \,. \tag{5.5}$$

An example which works for any N is the *Fourier matrix* whose matrix elements are

$$[F_N]_{j,k} = \gamma_N^{jk} \,, \qquad j,k = 0,1,\ldots,N-1 \,, \tag{5.6}$$

with $\gamma_N = \mathrm{e}^{2\pi \mathrm{i}/N}$ as in (1.4). This matrix is used to define the discrete Fourier transform. We recall from Sec. 1.1.2 that its existence means that pairs of MUB exist in all dimensions. Another example, for $N = p^{\mathrm{M}}$, is the Galois–Fourier matrix $[G_N]_{j,k} = \gamma^{j \odot k}$ with $\gamma = \mathrm{e}^{\mathrm{i}2\pi/p}$ that plays a central role in the construction of the dual basis in Sec. 2.3.

Yet another example are the Hadamard matrices $H_i^{(p)}$ for the prime-dimensional bases associated with the unitary operators XZ^i of (1.27) with $i = 0,1,\ldots,p-1$. Their matrix elements are

$$\bigl[H_i^{(p)}\bigr]_{j,k} = \gamma^{-jk} \gamma^{\frac{1}{2} ij(j-1)} \tag{5.7}$$

and their dephased forms

$$\bigl[H_i^{(p)}\bigr]_{j,k} \Big/ \bigl[H_i^{(p)}\bigr]_{j,0} = \gamma^{-jk} \tag{5.8}$$

are all equal to the inverse Fourier matrix. As a set, the matrices in (5.7) are equivalent to the *standard set* of Appendix A in the stronger sense of (5.4).

Our terminology is a bit unusual: in most of the literature an Hadamard matrix is required to have real entries only. Such *real Hadamard matrices* have many applications in computer science, and in quantum information too. Sylvester[83] constructed examples for all $N = 2^{\mathrm{M}}$, and Hadamard[84] proved that real Hadamard matrices do not exist unless $N = 2$ or $N = 4k$. It was conjectured by Paley[85] that

they do exist in all cases not excluded by Hadamard. This conjecture has been verified for all $N \leq 664$.[86] By the way, the non-existence of real Hadamard matrices in dimensions not divisible by 4 means that pairs of real MUB do not exist in real Hilbert spaces unless their dimension equals 2 or $4k$.[87] Another special class of Hadamard matrices are those of *Butson type*,[88] which by definition have all matrix elements equal to rational roots of unity. The Fourier matrix, the Galois–Fourier matrix, and the matrices $H_i^{(p)}$ of (5.7) are obvious examples.

For our purposes a pair of MUB that can be transformed into each other by an overall unitary matrix will be regarded as equivalent. It will be convenient to distinguish ordered and unordered pairs. Let (M_0, M_1) denote an *ordered pair* of MUB, with each basis represented as the columns of a unitary matrix. We identify pairs that can be transformed into each other by means of a single unitary matrix. Therefore, two ordered pairs of bases will be considered equivalent, written

$$(M_0', M_1') \sim (M_0, M_1)\,, \tag{5.9}$$

if and only if there exist permutations P_0, P_1, diagonal unitary matrices E_0, E_1, and a unitary matrix U such that

$$(UM_0'P_0E_0, UM_1'P_1E_1) = (M_0, M_1)\,. \tag{5.10}$$

By using the freedom to perform overall unitary transformations, we can bring any pair of MUB into the *standard form* $(\mathbb{1}, H)$, where H stands for a complex Hadamard matrix. But this still leaves some freedom to perform permutations and rephasings from the left, because

$$(\mathbb{1}, H_1) \sim (EP\mathbb{1}P^{-1}E^{-1}, EPH_1P_1E_1) = (\mathbb{1}, EPH_1P_1E_1)\,. \tag{5.11}$$

The conclusion is that two pairs of ordered MUB, written in standard form, are equivalent if and only if the two Hadamard matrices are equivalent in the sense of (5.4),

$$(\mathbb{1}, H_1) \sim (\mathbb{1}, H_2) \qquad \Leftrightarrow \qquad H_1 \approx H_2\,. \tag{5.12}$$

Haagerup[89] devised a useful way of testing for this kind of equivalence. The matrices $H_i^{(p)}$ of (5.7) are equivalent to each other.

Now consider *unordered pairs* of MUB, denoted by $\{M_0, M_1\}$. The freedom to perform overall unitaries implies that $(\mathbb{1}, H) \sim (H^\dagger, \mathbb{1})$. It follows that

$$\{\mathbb{1}, H\} \sim \{\mathbb{1}, H^\dagger\}\,. \tag{5.13}$$

Therefore unordered pairs of MUB may be equivalent even when the ordered pairs are not. Indeed

$$\{\mathbb{1}, H_1\} \sim \{\mathbb{1}, H_2\} \qquad \Leftrightarrow \qquad \begin{cases} \text{either } H_1 \approx H_2\,, \\ \text{or } H_1 \approx H_2^\dagger\,. \end{cases} \tag{5.14}$$

5.2. *Triplets of mutually unbiased bases and circulant matrices*

The question when two MUB triplets, say, are equivalent is a little bit involved. In an *ordered triplet* the first two bases are kept fixed, one of them being the standard basis and the other some fixed Hadamard matrix H_1. Then the freedom to perform further permutations and rephasings from the left is severely restricted, and we can only say that

$$(\mathbb{1}, H_1, H_2) \sim (\mathbb{1}, H_1, H_3) \qquad \Rightarrow \qquad H_2 \approx H_3\,. \tag{5.15}$$

The converse is false. Equivalence of *unordered sets* of $k+1$ MUB can be discussed similarly, but becomes harder and harder to check in practice because there are $k+1$ different choices of the basis to be represented by the unit matrix. Keeping this limitation in mind, a collection of $k+1$ ordered MUB $(\mathbb{1}, H_1, \ldots, H_k)$ is called *homogeneous* if all the Hadamard matrices H_i, $i = 1, \ldots, k$, are equivalent, and *heterogeneous* if there is a pair of inequivalent matrices among the Hadamard matrices.[19]

Two Hadamard matrices H_1 and H_2 are said to be MUHM if

$$\frac{1}{\sqrt{N}} H_1^\dagger H_2 = H_3\,, \tag{5.16}$$

where H_3 is an Hadamard matrix too. This is interesting because it implies that the triplet $(\mathbb{1}, H_1, H_2)$ represents three MUB. More generally a set of N MUHM is equivalent to a collection of $N+1$ MUB.

Triplets of MUB that include the Fourier matrix have an interesting interpretation in terms of the discrete Fourier transform. Given a sequence of complex numbers z_i, $0 \le i \le N-1$, its Fourier transform is

$$\tilde{z} = Fz \qquad \Leftrightarrow \qquad z = F^\dagger \tilde{z}\,. \tag{5.17}$$

The column vector whose components are $\tilde{z}_i/\sqrt{N}$ is unbiased with respect to the Fourier basis if and only if the sequence z_i is unimodular, $|z_i|^2 = 1$, and it is unbiased with respect to the standard basis if and only if $\tilde{z}_i$ is unimodular. Hence vectors that are unbiased with respect to both the standard basis and the Fourier basis are in one-to-one correspondence to sequences obeying

$$|z_i|^2 = |\tilde{z}_i|^2 = 1 \tag{5.18}$$

for all values of i. Such sequences are called *biunimodular*.[89,90] The first examples were produced by Gauss:

$$z_j^{(n,m)} = \begin{cases} \mathrm{e}^{\frac{2\pi \mathrm{i}}{N}\left(n(j+\frac{1}{2})+m\right)} & \text{for } N \text{ even}, \\ \mathrm{e}^{\frac{2\pi \mathrm{i}}{N}(nj+m)} & \text{for } N \text{ odd}, \end{cases} \tag{5.19}$$

where $j = 0, \ldots, N-1$ while $n \neq 0$ and m are integers modulo N.

Biunimodular sequences have an interesting property that emerges when one studies the autocorrelation function

$$\Gamma_a = \frac{1}{N}\sum_{i=0}^{N-1} \tilde{z}_i^* \tilde{z}_{a+i}\,. \tag{5.20}$$

An easy calculation shows that

$$\Gamma_a = \frac{1}{N}\sum_{i=0}^{N-1} |z_i|^2 \gamma_N^{ai}\,. \tag{5.21}$$

Hence, if the sequence is biunimodular it obeys

$$\Gamma_a = \delta_{a,0}\,. \tag{5.22}$$

Therefore $\tilde{z}_i$ and $\tilde{z}_{a+i}$, with a fixed and nonzero, are orthogonal vectors.

Any column vector can be used to define a *circulant matrix*, where each column is obtained from the preceding one by shifting all its elements cyclically in such a way that all the diagonal elements are the same.[91] For an explicit example see (5.34) below. The matrix elements are

$$C_{ij} = \tilde{z}_{i-j\,(\mathrm{mod}\,N)}\,. \tag{5.23}$$

With this definition a circulant matrix is a Hadamard matrix if and only if the sequence z_i is biunimodular. It follows that all vectors unbiased with respect to both the standard and the Fourier bases can be collected into a set of circulant Hadamard matrices whose columns form bases that are unbiased with respect to the standard and Fourier bases. There can be no "stray" unbiased vectors not belonging to an unbiased basis. We observe that any circulant matrix is diagonalized by the Fourier matrix. More precisely, if the first column of the circulant matrix C is defined by the sequence $\tilde{z}_i$, then

$$F^\dagger C F = \mathrm{diag}(z_0, z_1, \ldots, z_{N-1})\,. \tag{5.24}$$

It follows that all circulant matrices commute. Moreover, via (5.16) this confirms that F and C represent a pair of unbiased bases.

An example of a MUB triplet of this type is the triplet consisting of the eigenvectors of the three cyclic subgroups of the Heisenberg–Weyl group which exist in all dimensions. When $N = p$, a prime number, the known solution for a complete set of MUB consists of $\mathbb{1}$, F, and $N-1$ circulant matrices constructed from the biunimodular sequences (5.19) given by Gauss.

It is natural to ask if there are other solutions. In fact this is a discrete version of the Pauli problem:[92] given the modulus of a function and that of its Fourier transform, is the function uniquely determined? Björck and coworkers looked into this question,[90] and they found all biunimodular sequences for $N \leq 8$. Equivalently, they found all vectors unbiased to the Fourier matrix in these dimensions. For $N = 5$ there are 20 vectors, all of them given by Gauss' formula, for $N = 6$ there are 48

vectors, including 12 given by Gauss, for $N = 7$ there are 532 vectors, including 42 given by Gauss, and for $N = 8$ there is an infinite number of solutions.

There are also MUB triplets that do not include the Fourier or the Galois–Fourier matrix. We will see examples later.

5.3. *Classification of Hadamard matrices of size* $N \leq 5$

For $N \leq 5$ the classification of all Hadamard matrices under the equivalence relation (5.4) is complete. All complex 2×2 Hadamard matrices are equivalent to the Fourier matrix F_2, here without the $1/\sqrt{2}$ factor of (1.22),

$$F_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} . \tag{5.25}$$

This is a real Hadamard matrix. When $N = 3$, the set of all inequivalent Hadamard matrices contains the only element

$$F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \gamma & \gamma^2 \\ 1 & \gamma^2 & \gamma \end{pmatrix} , \tag{5.26}$$

where $\gamma = \mathrm{e}^{2\pi\mathrm{i}/3}$ as usual.[89] When $N = 5$, all complex Hadamard matrices are again equivalent to the Fourier matrix F_5.[89] The known maximal sets of MUB in these dimensions, and indeed in all prime dimensions, consist of the standard basis together with equivalent Hadamard matrices of the form $H = EF$, for p different choices of a diagonal unitary matrix E.

This remark about prime dimensions is illustrated by the matrices in (5.7) except that the inverse Fourier matrix appears there, but that is only one permutation away from the Fourier matrix itself. Indeed, we could have the Fourier matrix just as well, simply by interchanging the roles of X and Z in (1.27) and using the eigenstates of X as the computational basis. Since X and Z are unitarily equivalent, the two sets of MUB are as well.

For $N = 4$ the situation is different: there exists a one-parameter family of equivalence classes,

$$F_4(a) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \mathrm{e}^{\mathrm{i}a} & -1 & -\mathrm{e}^{\mathrm{i}a} \\ 1 & -1 & 1 & -1 \\ 1 & -\mathrm{e}^{\mathrm{i}a} & -1 & \mathrm{e}^{\mathrm{i}a} \end{pmatrix} . \tag{5.27}$$

Hadamard[84] himself proved that all $N = 4$ Hadamard matrices are equivalent to a member of this family, for some value $0 \leq a < \pi$ of the phase a. If $a = \frac{\pi}{2}$, this is the standard Fourier matrix F_4. Choosing $a = 0$ produces the Galois–Fourier matrix $F_4(0) \approx F_2 \otimes F_2$, which is a real Hadamard matrix.

5.4. *Affine families and tensor products*

Why does the continuous family appear when $N = 4$? To analyze this question we keep N arbitrary, multiply the matrix elements of the core of the dephased form of a given Hadamard matrix by arbitrary phase factors, and expand to first orders in the angles:

$$H_{ij} \to H_{ij}\mathrm{e}^{\mathrm{i}\phi_{ij}} \simeq H_{ij}(1 + \mathrm{i}\phi_{ij})\,, \qquad 1 \le i, j \le N-1\,. \tag{5.28}$$

Then we solve the unitarity equations to first order in the angles ϕ_{ij}. This is a linear system, but the number of equations exceeds the number of unknowns. The number of free parameters in the solution is called the *defect* of the matrix H.[93] The defect gives an upper bound on the dimension of any continuous set of inequivalent Hadamard matrices containing H. If the defect is nonzero it can happen that the solution to the linearized unitarity equations holds to all orders, in which case we speak of an *affine family* of Hadamard matrices.[94] It can also happen that the full unitarity equations are obeyed if the angles become nonlinear functions of each other, and then we have a *nonaffine* family. If the defect is zero the matrix is said to be *isolated*.

It is known that the defect of the Fourier matrix is zero whenever N is a prime number, hence there are no continuous families containing the Fourier matrix in these dimensions.[93] On the other hand, whenever $N = N_1N_2$ is a composite number one can produce continuous affine families from any choice of Hadamard matrices in dimensions N_1 and N_2.[89,95] If both N_1 and N_2 are prime, $N = p_1p_2$, the construction gives a $(p_1 - 1)(p_2 - 1)$-dimensional orbit of inequivalent Hadamard matrices including the Fourier matrix, which explains what happens for $N = 4$.

A more basic, and quite important, fact about tensor product Hilbert spaces is the following: Let $\{H_1^A, \ldots, H_k^A\}$ be a set of k MUHM of size N_A, while $\{H_1^B, \ldots, H_k^B\}$ denotes a set of k MUHM of size N_B. Then the tensor products $\{H_1^A \otimes H_1^B, \ldots, H_k^A \otimes H_k^B\}$ form a set of k unbiased Hadamard matrices in $\mathbf{C}^{N_AN_B}$. To prove this it is enough to check that condition (5.16) is obeyed. When $k = 2$, we have

$$\frac{1}{\sqrt{N}}(H_1^A \otimes H_1^B)^\dagger(H_2^A \otimes H_2^B) = \frac{1}{\sqrt{N_A}}H_1^{A\dagger}H_2^A \otimes \frac{1}{\sqrt{N_B}}H_1^{B\dagger}H_2^B\,. \tag{5.29}$$

The matrix on the right-hand side is an Hadamard matrix by assumption, and we are done. Note that the pair with cross terms $\{H_1^A \otimes H_2^B, H_2^A \otimes H_1^B\}$ is also unbiased, but these Hadamard matrices are not unbiased with respect to the pair used in (5.29). Hence by tensoring two sets of k MUHM of dimension N_A and N_B we will obtain exactly k MUHM of the product structure in the extended space of size $N = N_AN_B$, but not more of them. This is the construction mentioned at the end of Sec. 1.1.6 for $N_A = 2$, $N_B = 3$, and $k = 3$.

We say that the Hadamard matrix H is *separable* if it is equivalent to any matrix of the product form

$$H \approx H_{N_1} \otimes H_{N_2}\,, \tag{5.30}$$

where H_{N_1} and H_{N_2} are $N_1 \times N_1$ and $N_2 \times N_2$ Hadamard matrices, respectively. If this is not the case, the Hadamard matrix H of size $N_1 N_2$ will be called *entangled*. This concept requires that a concrete tensor product decomposition is given beforehand. One may find a Hadamard matrix of size $N = 12$ which is separable with respect to the 2×6 factorization, but entangled with respect to the 3×4 splitting. An example is the matrix $F_2 \otimes S_6$, where S_6 is the Tao matrix that will be discussed in the next section.

5.5. *Hadamard matrices of size N = 6*

$N = 6$ is the smallest composite number for which the two factors are different, the smallest integer that is not a power of a prime. It is the smallest dimension for which the MUB existence problem is open, and it is also the smallest dimension for which the classification of all Hadamard matrices is an unsolved question. In fact, the hunt for $N = 6$ Hadamard matrices is a lively research subject. So far, two pairs of two-parameter families of Hadamard matrices have been found.

The affine *Fourier family* reads[89]

$$F(a,b) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma z_1 & \gamma^2 z_2 & \gamma^3 & \gamma^4 z_1 & \gamma^5 z_2 \\ 1 & \gamma^2 & \gamma^4 & 1 & \gamma^2 & \gamma^4 \\ 1 & \gamma^3 z_1 & z_2 & \gamma^3 & z_1 & \gamma^3 z_2 \\ 1 & \gamma^4 & \gamma^2 & 1 & \gamma^4 & \gamma^2 \\ 1 & \gamma^5 z_1 & \gamma^4 z_2 & \gamma^3 & \gamma^2 z_1 & \gamma z_2 \end{pmatrix} \tag{5.31}$$

with $\gamma = \gamma_6 = \mathrm{e}^{\mathrm{i}2\pi/6}$ here while $z_1 = \mathrm{e}^{\mathrm{i}2\pi a}$ and $z_2 = \mathrm{e}^{\mathrm{i}2\pi b}$. The two free parameters a, b arise because a six-dimensional space can be written as a tensor product. They can take any value, but there exist several equivalence relations connecting different matrices within the family. The result is that the original square parameterized by a, b is divided into 144 equivalent triangles of equal area. One of them has corners at $(0,0)$, $(\frac{1}{6},0)$ and $(\frac{1}{6},\frac{1}{12})$, and every affine $F(a,b)$ is equivalent to one for which (a,b) lies within this triangle.[19]

The twin family of transposed matrices $F^{\mathrm{T}}(a,b)$ can be parameterized in an analogous way. These two families intersect at the Fourier matrix itself,

$$F_6 = F(0,0) = F^{\mathrm{T}}(0,0) \approx F_2 \otimes F_3 \approx F_3 \otimes F_2 \,. \tag{5.32}$$

The equivalence happens because the factors of $6 = 2 \cdot 3$ are relatively prime; see Ref. 96 for a general discussion of equivalences between tensor products of Fourier matrices.

A recent discovery is the two-parameter family of *bicirculant* Hadamards found by Szöllősi.[97] By definition, a bicirculant matrix is divided into four blocks of equal size, each block being a circulant matrix in itself. Szöllősi's family contains all bicirculant matrices with two independent blocks only, according to the pattern

$$H = \begin{pmatrix} A & B \\ B^\dagger & -A^\dagger \end{pmatrix} , \tag{5.33}$$

where H is bicirculant because A and B are circulant,

$$A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} , \qquad B = \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix} . \tag{5.34}$$

The individual entries are unimodular phase factors. Since any two circulant matrices commute, H is an Hadamard matrix if and only if

$$AA^\dagger + BB^\dagger = 6\,\mathbb{1} \qquad \Leftrightarrow \qquad \frac{a}{c} + \frac{b}{a} + \frac{c}{b} + \frac{d}{f} + \frac{e}{d} + \frac{f}{e} = 0\,. \tag{5.35}$$

Now introduce the function

$$\Phi(\mathrm{e}^{\mathrm{i}\phi}, \mathrm{e}^{\mathrm{i}\phi_0}) = \mathrm{e}^{\mathrm{i}\phi} + \mathrm{e}^{\mathrm{i}\phi_0} + \mathrm{e}^{-\mathrm{i}(\phi\,-\,\phi_0)}\,. \tag{5.36}$$

Clearly

$$\Phi\left(\frac{a}{c}, \frac{b}{a}\right) = \frac{a}{c} + \frac{b}{a} + \frac{c}{b}\,. \tag{5.37}$$

Hence we get an Hadamard matrix if we can find phase factors s, t, u, v such that

$$\Phi(s,t) = -\Phi(u,v) = \alpha\,, \tag{5.38}$$

where $\pm\alpha$ is some complex number in the range of Φ. But the function Φ has a simple geometric interpretation. If its two arguments coincide, the resulting curve in the complex plane is a *deltoid*, a 3-hypocycloid defined as the curve traced out if you place the tip of your pen at the rim of a wheel, and then let this wheel roll inside a larger wheel whose inner rim has three times the radius of the rolling wheel. For non-coinciding arguments the range of Φ is precisely the interior of the deltoid. Since we require that $\pm\alpha$ belongs to the range of Φ we conclude that any block circulant Hadamard matrix defines a point in the intersection of the interiors of two deltoids related by a reflection, as shown in Fig. 2.

The construction gives rise to a two-parameter family of Hadamard matrices because we can also go the other way. Given a complex number α belonging to the appropriate region we can find unimodular numbers s, t that solve (5.38). It turns out that they are roots of the cubic equation

$$z^3 - \alpha z^2 + \alpha^* z - 1 = 0\,. \tag{5.39}$$

All three roots are unimodular. If we are inside the deltoid, we must choose two different roots for s, t. We obtain u, v similarly. This leaves us with $6 \cdot 6$ possible choices of roots, and will lead to a discrete ambiguity in the specification of the Hadamard matrix. Recalling that s, t, u, v are defined as quotients of the entries of the Hadamard matrix, we solve for the latter, and we are done.

Note that (5.39) is invariant under the substitution

$$z \to \mathrm{e}^{\mathrm{i}2\pi/3} z\,, \qquad \alpha \to \mathrm{e}^{\mathrm{i}2\pi/3}\alpha\,. \tag{5.40}$$

Moreover, the interchange $\alpha \to -\alpha$ will interchange the roles of the two deltoids and leads to an equivalent Hadamard matrix. Taken together, these observations

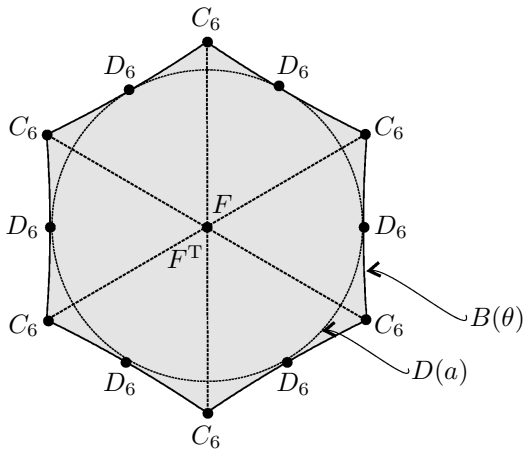

Fig. 2. Szöllősi's two-dimensional family of $N = 6$ complex Hadamard matrices interpolates between the generalized Fourier matrix $F = F\left(\frac{1}{6}, 0\right)$ and the hermitian family $B(\theta)$, which includes C_6 and D_6. It is parametrized by the common interior of two deltoids. There are actually several "leaves" over the interior, and it is divided into six equivalent sectors. Diţă's affine family $D(a)$, see (5.41), is represented by a circle inscribed into the figure.

mean that the parameter space is divided into six sectors representing equivalent Hadamard matrices, so the final picture is that of an umbrella. In fact two superposed umbrellas, because among the 36 matrices obtained from a given choice of α there are exactly two inequivalent ones, and they can be represented as the transposes of each other. Thus we have two two-parameter families $X_6(\alpha)$ and $X_6^{\mathrm{T}}(\alpha)$.

Two previously known one-parameter families are included in the bicirculant families. One of them is the affine Diţă family,[95] which in dephased form is given by

$$D(a) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \\ 1 & \mathrm{i} & -1 & \mathrm{i}z & -\mathrm{i}z & -\mathrm{i} \\ 1 & -\mathrm{i} & \mathrm{i}z^* & -1 & \mathrm{i} & -\mathrm{i}z^* \\ 1 & -\mathrm{i} & -\mathrm{i}z^* & \mathrm{i} & -1 & \mathrm{i}z^* \\ 1 & \mathrm{i} & -\mathrm{i} & -\mathrm{i}z & \mathrm{i}z & -1 \end{pmatrix} \qquad \text{with } z = \mathrm{e}^{\mathrm{i}2\pi a}\,. \tag{5.41}$$

We obtain all inequivalent examples if we impose the restriction $-\frac{1}{8} \le a \le \frac{1}{8}$. These matrices trace out the largest inscribed circle in the umbrella and touch the boundary in six equivalent points representing the Butson-type matrix $D_6(0)$, known as the Diţă matrix, and composed of fourth roots of unity. The boundary itself represents a one-parameter family including all hermitian Hadamard matrices. The hermitian family was in fact the first nonaffine family of Hadamard matrices ever constructed (by Beauchamp and Nicoara[98]); its explicit form is rather involved.

It includes the Diţă matrix as well as the circulant matrix[90]

$$C_6 = \begin{pmatrix} 1 & \mathrm{i}d & -d & -\mathrm{i} & -d^* & \mathrm{i}d^* \\ \mathrm{i}d^* & 1 & \mathrm{i}d & -d & -\mathrm{i} & -d^* \\ -d^* & \mathrm{i}d^* & 1 & \mathrm{i}d & -d & -\mathrm{i} \\ -\mathrm{i} & -d^* & \mathrm{i}d^* & 1 & \mathrm{i}d & -d \\ -d & -\mathrm{i} & -d^* & \mathrm{i}d^* & 1 & \mathrm{i}d \\ \mathrm{i}d & -d & -\mathrm{i} & -d^* & \mathrm{i}d^* & 1 \end{pmatrix}, \tag{5.42}$$

where

$$d = \frac{1-\sqrt{3}}{2} + \mathrm{i}\sqrt{\frac{\sqrt{3}}{2}}, \quad d^*d = 1\,. \tag{5.43}$$

The unimodular number d solves the equation $d^2 - (1-\sqrt{3})d + 1 = 0$. This matrix is represented by the extreme points on the boundary. It is known that every circulant Hadamard matrix is equivalent to either F_6 or C_6. Finally, the point at the center of the umbrella corresponds to the two inequivalent matrices $F(\frac{1}{6}, 0)$ and $F^{\mathrm{T}}(\frac{1}{6}, 0)$.

The bicirculant family is not yet fully understood. In particular, it is believed, but not known, that $F(\frac{1}{6}, 0)$ is their only point of intersection with the Fourier family. As we will see below, $F(\frac{1}{6}, 0)$ has a special status in the MUB existence problem, so perhaps its appearance here is natural.

The elegance of the whole construction is very encouraging, but it is not the end of the story. There exists a nonaffine family of symmetric Hadamard matrices,[99]

$$M(x) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & x & x & -x & -x \\ 1 & x & d & a & b & c \\ 1 & x & a & d & c & b \\ 1 & -x & b & c & p & q \\ 1 & -x & c & b & q & p \end{pmatrix}, \tag{5.44}$$

where $x = \mathrm{e}^{\mathrm{i}t}$ and the remaining entries are nonlinear algebraic functions of x. It happens that $M(1) \approx F_6$ while $M(\mathrm{i}) \approx D_6$, which means that this family connects all the two-parameter families. In fact, it has been conjectured[19] that all these families belong to one single four-parameter family. One reason for this is that the defect of all included matrices was found to be four, whenever it was checked. Moreover, there is some concrete perturbative evidence that the set really is four-dimensional around the matrices D_6,[19] C_6,[100] and F_6.[101]

Yet, the set of inequivalent $N = 6$ Hadamard matrices is disconnected, because there is also an isolated matrix that does not belong to any continuous family. This is a symmetric Butson-type Hadamard matrix composed of third roots of unity only, known as *Tao's matrix*.[102,103] It is isolated because its defect vanishes. One does not known if other isolated matrices exist.

5.6. *Hadamard matrices for $N \geq 7$*

Some general facts are known also in higher dimensions, in particular affine families stemming from known Hadamard matrices have been much studied. As we have already mentioned, the Fourier matrix is an isolated matrix if and only if N is a prime number.[93] When N is a power of a prime, $N = p^{\mathrm{M}}$, all affine orbits stemming from the Fourier matrix are explicitly known. The dimension of these orbits reads $d = p^{\mathrm{M}-1}[(p-1)\mathrm{M} - p] + 1$ and is equal to the defect of F_N.[93] It is also known that every real Hadamard matrix admits an affine orbit if $N \geq 12$.[104] In prime dimensions, affine orbits cannot pass through the Fourier matrix, but Petrescu found an example for $N = 7$ which contains a Butson-type matrix built from sixth roots of unity.[105]

All circulant Hadamard matrices up to $N \leq 8$ have been found.[90] When $N = 8$ this includes a continuous family. Many block circulant examples are also known.[106] Special methods for constructing Hadamard matrices include one based on tiling abelian groups,[107] one based on N equiangular vectors in $N/2$ dimensions,[108] and one based on inverse orthogonal conference matrices[109] of size $N/2$. And, of course, there are many ad hoc constructions. A catalog of known Hadamard matrices for $N \leq 16$ is available,[94] also as an updated internet version.[110]

5.7. *All mutually unbiased bases for $N \leq 5$*

Since we know that the Hadamard matrix in dimensions 2, 3, and 5 is unique up to equivalences it seems reasonable to expect that the maximal set of MUB is also unique up to an overall unitary transformation. When $N = 2$ a maximal set of MUB can be thought of — as we did in Sec. 1.2 — as a regular octahedron inscribed in the Bloch sphere, and the uniqueness follows from the fact that all such octahedra are related by a rotation, corresponding to a unitary transformation in the $N = 2$ Hilbert space. Alternatively, there is the observation of Sec. 1.1.6 that q-bit operators are associated with directions in $\mathbf{R}^3$ and complementary observables must refer to orthogonal directions.

Uniqueness continues to hold for $N = 3$ and $N = 5$, although a complicated calculation is needed to see this.[49] The explicit form of unbiased Hadamard matrices forming one maximal set of MUHM for any prime $N = p$ is provided in Appendix A. Another, equivalent, maximal set is composed of the matrices $H_i^{(p)}$ in (5.7).

The case $N = 4$ is more interesting because of its one-parameter family of inequivalent Hadamard matrices. It is also simple enough that the calculations can be done by hand.[50] We begin by looking for ordered MUB triplets of the form $(\mathbb{1}, F_4(a), H)$, where $F_4(a)$ is written in the standard form (5.27) and H is some Hadamard matrix obtained by enphasing $F_4(a)$, possibly with its rows permuted. After going through all the possibilities, one finds that there are exactly three families of ordered triplets of MUB, with 2 or $1 + 2$ free parameters each:

$$\left(\mathbb{1}, F_4(a), H^{(1)}(\phi_1; \alpha_1)\right), \quad \left(\mathbb{1}, F_4(0), H^{(2)}(\phi_2; \alpha_2)\right), \quad \left(\mathbb{1}, F_4(0), H^{(3)}(\phi_3; \alpha_3)\right). \tag{5.45}$$

The third members of these triplets are given by

$$H^{(1)}(\phi_1;\alpha_1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \mathrm{e}^{\mathrm{i}\alpha_1} & \mathrm{e}^{\mathrm{i}(\alpha_1+\phi_1)} & -\mathrm{e}^{\mathrm{i}\alpha_1} & -\mathrm{e}^{\mathrm{i}(\alpha_1+\phi_1)} \\ -1 & 1 & -1 & 1 \\ \mathrm{e}^{\mathrm{i}\alpha_1} & -\mathrm{e}^{\mathrm{i}(\alpha_1+\phi_1)} & -\mathrm{e}^{\mathrm{i}\alpha_1} & \mathrm{e}^{\mathrm{i}(\alpha_1+\phi_1)} \end{pmatrix},$$

$$H^{(2)}(\phi_2;\alpha_2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \mathrm{e}^{\mathrm{i}\alpha_2} & \mathrm{e}^{\mathrm{i}(\alpha_2+\phi_2)} & -\mathrm{e}^{\mathrm{i}\alpha_2} & -\mathrm{e}^{\mathrm{i}(\alpha_2+\phi_2)} \\ -\mathrm{e}^{\mathrm{i}\alpha_2} & \mathrm{e}^{\mathrm{i}(\alpha_2+\phi_2)} & \mathrm{e}^{\mathrm{i}\alpha_2} & -\mathrm{e}^{\mathrm{i}(\alpha_2+\phi_2)} \\ 1 & -1 & 1 & -1 \end{pmatrix},$$

$$H^{(3)}(\phi_3;\alpha_3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ -\mathrm{e}^{\mathrm{i}\alpha_3} & -\mathrm{e}^{\mathrm{i}(\alpha_3+\phi_3)} & \mathrm{e}^{\mathrm{i}\alpha_3} & \mathrm{e}^{\mathrm{i}(\alpha_3+\phi_3)} \\ \mathrm{e}^{\mathrm{i}\alpha_3} & -\mathrm{e}^{\mathrm{i}(\alpha_3+\phi_3)} & -\mathrm{e}^{\mathrm{i}\alpha_3} & \mathrm{e}^{\mathrm{i}(\alpha_3+\phi_3)} \end{pmatrix}, \tag{5.46}$$

respectively. Regarded as unordered triplets, the last two are actually special cases of the first, so there is a single $1+2$ parameter family of unordered triplets.

It is straightforward to check that none of these families contains a quartet of MUB. The only way to obtain a quartet is to pick the third member of two different ordered triplets. Moreover, there is only one way in which this can be done, namely to set

$$\alpha_1 = \alpha_2 = \alpha_3 = \frac{\pi}{2}\,, \qquad a = \phi_1 = \phi_2 = \phi_3 = 0\,. \tag{5.47}$$

This leads to the standard solution for a maximal set of MUB, which is thereby shown to be unique up to an overall unitary transformation.

Since $N = 4$ gives the Hilbert space for two q-bits it is interesting to ask how the MUB behave with respect to entanglement. In fact three of them can be chosen to consist of separable states only, while the remaining two are constructed out of maximally entangled Bell states.[111,112] One can understand these five MUB as bases composed of the common eigenstates to three two–q-bit observables with period 2 or, equivalently, as the eigenstate bases of complementary period-4 operators; see Table 2.[113] Alternatively we can use the magic basis for Hilbert space, so that real vectors are maximally entangled.[114] It is easy to see that there is a MUB triplet consisting of three real bases, although this is a triplet that cannot be extended to a maximal set. Incidentally the three real MUB form a maximal set for a real four-dimensional Hilbert space, and this observation is closely related to the existence of a platonic body in $\mathbf{R}^4$, called the 24-cell.

5.8. *Triplets of mutually unbiased bases in dimension* 6

Since a complete list of all possible sets of five MUB in $N = 4$ can be constructed by hand one might guess that the case of $N = 6$ could easily be settled with a computer. Numerical searches have been performed by many, but it seems that

Table 2. One choice for the five MUB of a two–q-bit system ($N = 2^2$) can be characterized as the bases of common eigenstates to five sets of three commuting period-2 observables each, or as the eigenstate bases of five period-4 observables. Bases 1–3 consist of product states; bases 4 and 5 consist of maximally entangled states. Together with the identity $\mathbf{1} \otimes \mathbf{1}$ and phase factors ± 1, the 15 observables in the middle column constitute the two–q-bit Heisenberg–Weyl group; their 15 expectation values determine the state of the two–q-bit system uniquely. The five observables in the right column are pairwise complementary.

Basis	Set of three commuting period-2 observables	Complementary period-4 observables
1	$\sigma_x \otimes \mathbf{1} \quad \mathbf{1} \otimes \sigma_x \quad \sigma_x \otimes \sigma_x$	$\frac{1+\mathrm{i}}{2}\sigma_x \otimes (\mathbf{1} - \mathrm{i}\sigma_x)$
2	$\sigma_y \otimes \mathbf{1} \quad \mathbf{1} \otimes \sigma_y \quad \sigma_y \otimes \sigma_y$	$\frac{1+\mathrm{i}}{2}\sigma_y \otimes (\mathbf{1} - \mathrm{i}\sigma_y)$
3	$\sigma_z \otimes \mathbf{1} \quad \mathbf{1} \otimes \sigma_z \quad \sigma_z \otimes \sigma_z$	$\frac{1+\mathrm{i}}{2}\sigma_z \otimes (\mathbf{1} - \mathrm{i}\sigma_z)$
4	$\sigma_x \otimes \sigma_y \quad \sigma_y \otimes \sigma_z \quad \sigma_z \otimes \sigma_x$	$\frac{1+\mathrm{i}}{2}(\sigma_x \otimes \sigma_y + \mathrm{i}\sigma_z \otimes \sigma_x)$
5	$\sigma_y \otimes \sigma_x \quad \sigma_z \otimes \sigma_y \quad \sigma_x \otimes \sigma_z$	$\frac{1+\mathrm{i}}{2}(\sigma_y \otimes \sigma_x + \mathrm{i}\sigma_x \otimes \sigma_z)$

the first published account is the one by Zauner,[115] who was led to conjecture that at most three MUB can be found. By now the evidence for his conjecture is overwhelming, but not quite conclusive, which tells us something about how fast the complexity of a Hilbert space grows with dimension.

The problem of classifying all pairs of MUB is equivalent to the problem of classifying Hadamard matrices. With partial results on this problem available, one can go on to ask what pairs can be extended to triplets of MUB, and in how many ways this can be done. For the Fourier family of Hadamard matrices (and its transpose), a clear picture has emerged.[116–118] There is very strong evidence that the number of kets unbiased to the bases represented by the pair $\big(\mathbb{1}, F(a,b)\big)$ equals 48, regardless of the values taken by the parameters a, b. For generic values of the parameters these vectors can be collected into eight different unbiased bases which, however, are not MU. Some values of the parameters are special in this regard: the Fourier matrix $F(0,0)$ admits 16 unbiased bases,[58] and $F(\frac{1}{6}, 0)$ admits up to 70. Note that these values of the parameters are special also because they correspond to singular points in the moduli space of all Hadamard matrices of this type, and that $F(\frac{1}{6}, 0)$ is very special because it is also included in the bicirculant family $X_6(\alpha)$.

The evidence consists in computer calculations for a large number of members of the family,[116] and also a proof that there exists a vicinity of $(a,b) = (0,0)$ where the number of unbiased vectors is constant[117] and equal to 48. In one version, the procedure begins with the observation that the condition for a ket to be unbiased with respect to the bases pair corresponding to $(\mathbb{1}, H)$, for some Hadamard matrix H, is a set of multivariate polynomial equations that can in principle be brought to "diagonal" form (in the way one would do Gauss elimination for linear equations) by

Table 3. Number $N_{\rm v}$ of kets unbiased with respect to a given complex Hadamard matrix and the number $N_{\rm t}$ of bases (not mutually unbiased) which can be formed out of them.

Matrix	$F(a,b)$	$F(0,0)$	$F(\frac{1}{6},0)$	$D(0)$	$D(b)$	$D(c)$	S_6
$N_{\rm v}$	48	48	48	120	120	48	90
$N_{\rm t}$	8	16	70	10	4	4	0

means of Gröbner bases for the polynomials. In the end one has to solve polynomial equations in single variables, to high enough accuracy. The procedure works nicely for all of the affine families, while results for the nonaffine families are somewhat uncertain because of more stringent demands on computer memory.

In Table 3, we show the number $N_{\rm v}$ of kets unbiased to the computational basis and one additional listed basis, as well as the number $N_{\rm t}$ of bases (or triplets of MUB) that can be formed from these vectors. The results for the twin families $F(a,b)$ and $F^{\rm T}(a,b)$ are similar, and hence results for the latter are not given explicitly. For the Diţă family $D(a)$ one finds that the result depends on the parameter value;[116] if $|a| \leq 0.0177$ there are 120 unbiased vectors, and if $0.0177 \leq |a| \leq \frac{1}{8}$ there are 48 of them. This takes care of all inequivalent values of a. Note that the Butson-type matrix $D(0)$ is quite exceptional; moreover, in this case the phases that define the unbiased kets are known exactly. The isolated Butson-type matrix S_6 does not admit even a single triplet of MUB.

Exactly what makes the unbiased vectors collect into bases in some, but not all cases, is imperfectly understood. For triplets of MUB involving $F(0,0)$, we have given the explanation in terms of the discrete Fourier transform,[19] and for the affine family $F(a,b)$ some partial understanding exists.

Some continuous families of triplets of MUB are known. In particular, Zauner showed that any bicirculant Hadamard matrix gives rise to a triplet because (5.16) can be solved for H_1 and H_2 if H_3 is a specified bicirculant Hadamard matrix.[115] In fact, the entire set of triplets in $N = 4$ dimensions can be shown to arise in this way. For $N = 6$, this means that Szöllősi's bicirculant family $X_6(\alpha)$ gives rise to a two-parameter set of triplets. Another continuous family of the form $\big(\mathbb{1}, F(0,b(t)), H(t)\big)$ has been constructed by Jaming *et al.*;[117] the third member of their triplet family belongs to the Fourier family.

5.9. *A maximal set of mutually unbiased bases when* $N = 6$*?*

We now ask whether any of the explicitly known triplets of MUB can be extended to a quartet. The answer is that none of them can, and the failure can be expressed quantitatively. If a quartet involving the Fourier matrix did exist, one would be able to find a pair of bases among the 16 bases unbiased with respect to $(\mathbb{1}, F)$ such that the Grassmannian distance between them is equal to unity.[58] However, the best one can do is $D_c^2 = 0.93$.[19] Remembering that a random pair of bases are situated at a distance given by $D_c^2 = 0.86$, this is not impressive. Other pairs of MUB have not

been treated in quite that much detail, but it is a rigorous theorem that no quartets of MUB including any member of the Fourier family $F(a, b)$ can exist. The proof involves approximations of the elements of the columns that represent the kets by rational roots of unity, exhaustive computer searches, and careful estimates of the errors involved.

Direct numerical searches for maximal sets have been carried out,[115,119] but relatively few such investigations have been published. Butterley and Hall[120] have conducted a search based on the minimization of a suitable function. The minimization proceeds by picking a point at random in some parameter space, and changing it until a minimum is reached. The problem is that this minimum may not be the global minimum, so the procedure could miss its target even if the target — in this case a quartet of MUB — is there. Indeed, the success rate was 60.4% when $N = 5$, but only 0.9% when $N = 7$. No quartets were found for $N = 6$. This result is suggestive but not definitive.

Brierley and Weigert[121] concentrated on finding *MU constellations*, defined as $N + 1$ sets of orthogonal kets that are MU with respect to each other. It is not required that the sets have N members. In fact, for $N = 6$ they were able to find seven sets with two members each. This constellation is denoted by $\{2^7\}_6$, while a quartet of MUB is the constellation $\{6^4\}_6$, in a notation that should now be obvious (given the fact that six orthogonal vectors automatically define a seventh, unbiased to all vectors that are unbiased with respect to the original six). They then proceeded to search for constellations that necessarily exist if the quartet exists, such as $\{6, 3, 3, 3\}_6$, $\{6, 4, 3, 2\}_6$, and so on. Altogether they found 17 examples of such constellations for which their success rate in dimension 6 was zero. The advantage of the procedure is that the parameter spaces in which the search is conducted are comparatively small — in the two quoted examples there are 40 parameters, as opposed to 70 parameters for a quartet of MUB. The success rates for similar calculations in $N = 7$ were high.

Hence we feel that the answer to the question in the title of this subsection must be "no." It is fair to say, however, that a structural understanding of this negative result is missing. A precise translation into Euler's problem of the 36 officers (see Sec. 4.3) could provide this — if there is one, and if the translation provides a structural understanding of the latter problem.

5.10. *Heisenberg–Weyl group approach for* $N = 6$

We have seen how the abelian subgroups of the Heisenberg–Weyl group identify the maximal set of MUB if N is a power of a prime, whereby the construction of the MUB relies heavily on the properties of the Galois field with N elements. As noted earlier, this construction is not applicable for other values of N, simply because there is no corresponding Galois field. The failure of this approach, therefore, say nothing about the existence of maximal sets of MUB in non–prime-power dimensions. As noted repeatedly, this existence problem is open, even in the most intensely studied

Table 4. The twelve abelian subgroups of the modulo-6 Heisenberg–Weyl group of unitary operators. The six elements of each subgroup are given by the powers of the period-6 unitary operator that generates the subgroup. These generators X^mZ^n are listed in the second column without, however, displaying the phase factors $e^{i(\pi/6)mn}$ that are needed when the product mn is odd to compensate for the $(-1)^{mn}$ factor in (1.20). The last column shows which six other generators are complementary partners.

Subgroup	Period-6 observable	Complementary partners
0	X	1, 5, 6, 7, 9, 10
1	XZ	0, 2, 6, 7, 8, 11
2	XZ^2	1, 3, 6, 8, 9, 10
3	XZ^3	2, 4, 6, 7, 9, 11
4	XZ^4	3, 5, 6, 7, 8, 10
5	XZ^5	0, 4, 6, 8, 9, 11
6	Z	0, 1, 2, 3, 4, 5
7	X^2Z	0, 1, 3, 4, 10, 11
8	X^2Z^3	1, 2, 4, 5, 10, 11
9	X^2Z^5	0, 2, 3, 5, 10, 11
10	X^3Z	0, 2, 4, 7, 8, 9
11	X^3Z^2	1, 3, 5, 7, 8, 9

case of $N = 6$.[19, 58, 120–122]

Since the Galois–Fourier construction of the Heisenberg–Weyl group, which works so well for prime power dimensions, cannot be applied for $N = 6, 10, 12, 14, \ldots$, one could try to repeat the procedure with operations that do not form a field; for instance, we could try to use distributive rings with N elements, possibly the modulo-N ring that suffices for statements like (1.5).[t] For $N = 6$ the only ring is the modulo-6 ring, and we have the usual $N^2 = 36$ Heisenberg–Weyl unitary operators of Sec. 1.1.4.

Let us see. The powers of the $N + 1 = 7$ operators of (1.27) do form seven abelian subgroups, but they do not exhaust all 36 products X^jZ^k because quite a few of these products belong to more than one subgroup. For example, we have $X^2Z^2 = (XZ)^2 = (XZ^4)^2$ and, therefore, the operators XZ and XZ^4 are not complementary.

In total, there are twelve abelian subgroups of six elements each, the identity plus five more interesting ones, obtained as powers of period-6 unitary operators. In Table 4 we see that each of the these twelve "generators" has six complementary partners, so that the corresponding bases are MU. But there are not more than three bases that are pairwise MU. For instance, the bases '0' and '1' are MU and are both MU with bases '6' and '7', but these are not MU themselves, so that '0,1,6' and '0,1,7' are MUB triplets whereas '0,1,6,7' is *not* a MUB quartet. As an alternative to this counting of MUB, one can evaluate the prime-distinguishing

[t] Recall footnote 'a': In marked contrast to a field, a ring may have zero products of nonzero elements, such as $2 \odot_6 3 = 0$.

function of Appendix B for $N = 6$ to find that it does not take the value 0.

Similarly, the modulo-4 ring construction fails for $N = 4$.[26] The modification that replaces the Galois field shifts by modulo-N shifts simply does not work, except when N is prime (Sec. 1.1.6) and the two ways of shifting coincide.

6. Brief summary and concluding remarks

We used the Galois-shift based Heisenberg–Weyl group to construct first maximal sets of MUB in prime power dimensions and then the generalized Bell states associated with them. Several applications to quantum information processing were discussed, some in considerable detail: dense coding and teleportation, quantum cryptography and cloning machines, the Mean King's problem and state tomography. Owing to the somewhat unconventional parameterization in terms of numbers that are both field elements and ordinary integers, the approach we presented is relatively new, and some results are rather recent.[23,26] There are yet other applications of these techniques, including the discrete phase operators[123] (that would correspond to the dual group in our terminology) and the SIC POVMs[58,59] that present appealing applications in the framework of tomography.

Some of these applications do not require the basic operations (addition and multiplication) of a field, a ring structure suffices, as is the case for instance for the SIC POVMs, teleportation, dense coding, or the discrete Weyl-type phase space function. All of them can be realized by use of the usual modulo-N operations for Hilbert spaces of arbitrary dimension. For the construction of maximal sets of MUB, the modulo-N rings are good enough in prime dimensions only, and this fact inspired the design of the prime-distinguishing function described in Appendix B.

For what concerns the construction of MUB, the dimensionality seems to play a crucial role. The reasons why prime power dimensions are so special are not clearly understood as yet,[111,112] and it is certainly worth investigating this problem in the future. We offer a speculation below that is suggested by the significance of the Hilbert space dimension in quantum physics.

It is worth emphasizing that the search for maximal sets of inequivalent MUB in each dimension is related to several different mathematical problems. The literature contains an abundance of valuable papers on the MUB problem related to group theory,[62,124–126] angular momentum,[127] finite fields and projective planes,[17,123,128] and mutually orthogonal Latin squares.[24] A geometric approach to the problem is developed in Refs. 17, 129, and 130.

Let us try to collect here the information concerning the number of known MUB, which depends on the number-theoretic properties of the dimension N. The following list, which by its nature is unavoidably incomplete, contains statements about MUB and MUHM, which are easily translated into the respectively other terminology with the aid of (5.1) and (5.2). In particular, if the maximal number of known MUHM is k, then there are $k + 1$ MUB.

(a) Maximal sets of MUB exist for all prime power dimensions, $N = p^{\mathrm{M}}$.

(b) If the dimension is not a power of a prime, $N \neq p^{\mathrm{M}}$, maximal sets of MUB are not known. It is highly unlikely that there are sets of MUB for $N = 6$ with more than three bases.
(c) For any $N \geq 2$ there exists at least one triplet of MUB. This is equivalent to the statement that there exists at least a pair of MUHM.
(d) For $N = 2$, 3, 4, and 5, all maximal sets of $N + 1$ MUB are equivalent.
(e) For $N = 2$, one can find a corresponding Hadamard matrix H_2 to any, possibly enphased, Hadamard matrix H_1 such that they are MU.
(f) For $N \geq 3$, there are certain sets of MUHM that cannot be extended to a maximal set.
(g) In prime dimension, $N = p$, all known sets of MUHM are equivalent to the standard set of Appendix A. It seems unlikely that there are other nonequivalent sets of MUHM, but we are not aware of a formal proof that they do not exist.
(h) The case of a prime power dimension, $N = p^{\mathrm{M}}$, can be naturally interpreted as a system of M particles, each described in its own p-dimensional Hilbert space. In this case several inequivalent sets of MUHM may exists. For instance, for two, three, or four q-bits ($N = 4$, 8, or 16) the number of inequivalent sets of MUB constructed out of the Heisenberg–Weyl group is one, four, and seventeen, respectively.[51,52,131]
(i) In the case of M–q-bit systems, $N = 2^{\mathrm{M}}$, the maximal set of $N + 1$ MUB can be generated by choosing an appropriate unitary $N \times N$ matrix U with period $N + 1$ and raising it to integer powers to obtain a maximal set of MUHM: $H_m = 2^{\mathrm{M}/2} U^m$, with $m = 1, 2, \ldots, N$.[132]
(j) In certain square dimensions, $N = d^2$, the known sets of MUB are larger than would follow from the factorization of d. For instance Wocjan and Beth[133] found six MUB for $N = 26^2$, which is one more than the five bases obtained due to the solution of the problem for $N = 4$ and $N = 169$, the factorization $N = 2^2 \cdot 13^2$, and the construction of Sec. 1.1.5.

Items (a), (b), and (h) invite a speculation about the difference between Hilbert space dimensions N that are the power of a prime and those that are other composite numbers. In the spirit of Sec. 1.1.5, we associate one quantum degree of freedom with each prime factor of N. If different primes occur, we surely have a physical system composed of different components. But if there is only one prime, we could have indistinguishable components, in which case the physical system behaves as one whole and the separation into the M subsystems of (h) is artificial because the labels $m = 0, 1, \ldots, \mathrm{M} - 1$ are physically meaningless. From this physical point of view, then, it is quite satisfactory that prime power dimensions are not so different from prime dimensions (maximal sets of MUB for both) while other dimensions are not on the same footing (relatively few bases that are MU). A clear-cut demonstration that, indeed, there are no maximal sets of MUB for $N \neq p^{\mathrm{M}}$ is surely desirable.

Acknowledgments

It is a pleasure to thank W. Bruzda, Å. Ericsson, J.-A. Larsson, and W. Tadej for a long-term collaboration on research projects related to mutually unbiased bases and for allowing us to mention some of their unpublished results. We are also grateful to V. Cappellini, M. Matolcsi, A. Scott, and A. Uhlmann for inspiring discussions and to P. Diţă, R. Nicoara, A. J. Skinner, and F. Szöllősi for helpful correspondence and a permission to use their results prior to publication. Sincere thanks to P. Cara for patiently answering our questions about finite fields, and to A. Eusebi for attracting our attention to a typo in Ref. 23.

The authors acknowledge support from the ICT Impulse Program of the Brussels Capital Region (Project Cryptasc), the IUAP programme of the Belgian government, the grant V-18, and the Solvay Institutes for Physics and Chemistry (TD), the A*Star Grant 012-104-0040 (BGE), the research network LFPPI financed by the Polish Ministry of Science and an European research project SCALA (KŻ). Centre for Quantum Technologies is a Research Centre of Excellence funded by Ministry of Education and National Research Foundation of Singapore.

Appendix A. Standard sets of mutually unbiased Hadamard matrices for prime dimension

For completeness we provide here an explicit form of a maximal set of N MUHM in the case of an arbitrary odd prime dimension, $N = p \geq 3$. It is different from, and supplements, the example of (5.7).

As a first element in the set of MUHM let us choose the Fourier matrix (5.6), $H^{(0)} = F_N$. Then introduce the diagonal unitary $N \times N$ matrix E_N with matrix elements

$$[E_N]_{jk} = \delta_{jk}\, \mathrm{e}^{\mathrm{i}\frac{2\pi}{N}j^2} \quad \text{where} \quad j,k = 0,1,2,\ldots,N-1\,. \tag{A.1}$$

It allows us to define a sequence of N matrices $\big(H^{(0)},\ H^{(1)},\ \ldots,\ H^{(N-1)}\big)$, where

$$H^{(r)} = E_N^r H^{(0)} \quad \text{for} \quad r = 0,1,2,\ldots,N-1\,. \tag{A.2}$$

By construction all these matrices are complex Hadamard matrices. Furthermore, the products

$$X_{r-s} = \frac{1}{\sqrt{N}} {H^{(s)}}^\dagger H^{(r)} = \frac{1}{\sqrt{N}} F_N^\dagger E_N^{r-s} F_N \tag{A.3}$$

are Hadamard matrices for all $r \neq s$ from the set $\{0,1,\ldots,N-1\}$ if and only if the dimension N is an odd prime.

Hence the set $\{H^{(0)}, H^{(1)}, \ldots, H^{(N-1)}\}$ is a set of N MUHM, referred to as the *standard set of MUHM*, which generates the *standard set of* $N+1$ *MUB*, according to (5.16). We observe that, just like the set (5.7), this set of Hadamard matrices is homogeneous, since all its members arise by enphasing the same Fourier matrix F_N,

hence they are equivalent and share the same core. The equivalence of the standard set of MUHM and the set of (5.7) is shown with the aid of the identity

$$\frac{1}{2}j(j-1) = \frac{1}{2}q(q-1) + q(j-q)^2 \pmod N \qquad \text{with } q = \frac{1}{2}(N+1)\,, \tag{A.4}$$

which is valid for all odd N values.

Appendix B. A prime-distinguishing function

In this appendix we provide a prime-distinguishing function of an integer argument n, related to the standard maximal set of MUB, which exists if n is prime.

Consider the following function of integer $n > 1$:

$$g(n) = \frac{1}{n-1}\sum_{r=1}^{n-1}\frac{1}{\sqrt{n}}\left|\sum_{j=0}^{n-1}\mathrm{e}^{\mathrm{i}\frac{2\pi}{n}rj^2}\right| - 1\,. \tag{B.1}$$

Let us then analyze the inner sum in this expression for n an odd prime, $n = p$, and $\gamma = \mathrm{e}^{2\pi\mathrm{i}/p}$ as usual. Making use of the Gauss sum (see Ref. 134, for instance), one can evaluate this expression and finds that it does not depend on the value of summation variable r,[u]

$$\left|\sum_{j=0}^{p-1}\gamma^{rj^2}\right| = \sqrt{p}\,. \tag{B.2}$$

After substituting this into (B.1), we see that

$$g(p) = \frac{1}{p-1}\sum_{r=1}^{p-1}\frac{1}{\sqrt{p}}\left|\sum_{j=0}^{p-1}\gamma^{rj^2}\right| - 1 = \frac{1}{p-1}\sum_{r=1}^{p-1}\frac{1}{\sqrt{p}}\sqrt{p} - 1 = 0\,. \tag{B.3}$$

Therefore we can conclude that *for any prime $p \geq 3$ the function $g(n)$ is equal to zero.*

This property is stronger than the known fact that the products in (A.3) are Hadamard matrices if and only if N is an odd prime. This is because the definition of $g(n)$ in (B.1) is equivalent to

$$g(n) = \frac{1}{n-1}\sum_{r=1}^{n-1}\Big|[X_r]_{ii}\Big| - 1 = \sum_{r=1}^{n-1}\left|\frac{1}{\sqrt{n}}[F_n^\dagger E^r F_n]_{ii}\right| - 1\,, \tag{B.4}$$

in accordance with (A.3); the index i is arbitrary here because the X_rs are circulant matrices. The function $g(n)$ is thus equal to zero if n is prime, see Fig. 3, but beyond that it may still be zero even if diagonal elements of X_r's are not unimodular. This simple example indicates that the problem of existence of MUB and MUHM of size N could be related to number-theoretical properties of the dimension.

[u]This Gauss sum plays a fundamental role in the derivation of the MUness condition in prime power dimensions; see, for instance, Ref. 23. It is also a key ingredient for conceiving a maximally entangling quantum gate that generalizes the two–q-bit cnot gate in arbitrary dimension.[135]

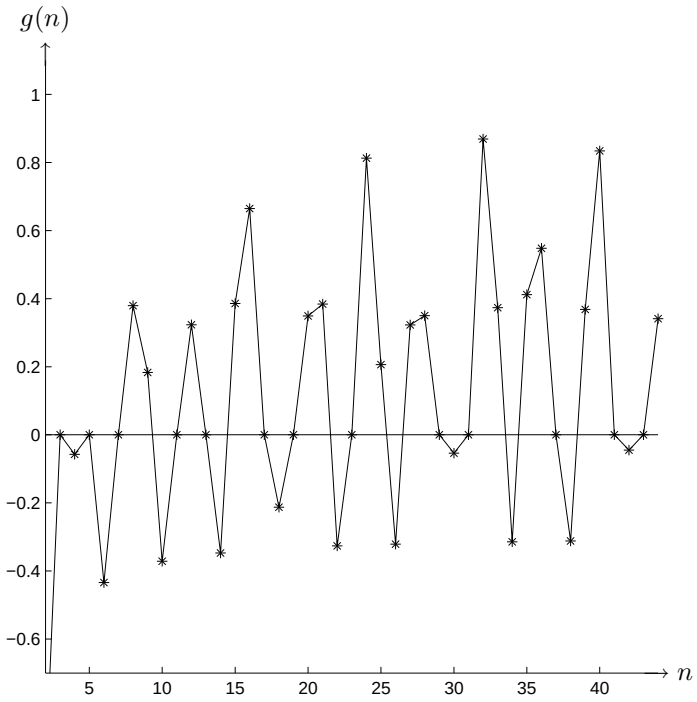

Fig. 3. The function $g(n)$ is defined for integer values and the solid line is only provided to guide the eye. Observe that the integer roots of this function are prime.

Appendix C. Mutually unbiased bases for $N = 4$

In accordance with (2.67), the set of MUHM for the maximal set of MUB for $N = p^{\mathrm{M}}$ of Sec. 2 is given by

$$\left[H_j^{(N)}\right]_{k,l} = \sqrt{N}\langle e_k^N | e_l^j\rangle = {\alpha_{\ominus k}^j}^* \gamma^{\ominus k \odot l} \tag{C.1}$$

for $j, k, l = 0, 1, \ldots, N-1$, so that $H_j^{(N)} = A_j^{(N)} G_N^{-1}$ is the product of the inverse Galois–Fourier matrix with matrix elements

$$\left[G_N^{-1}\right]_{k,l} = \gamma^{\ominus k \odot l} \tag{C.2}$$

and the diagonal matrix of phase factors

$$\left[A_j^{(N)}\right]_{k,l} = \delta_{k,l} {\alpha_{\ominus k}^j}^* \tag{C.3}$$

with $A_0^{(N)} = \mathbb{1}_N$ and $H_0^{(N)} = G_N^{-1}$ in particular for the 0th basis, the dual bases. The conventional choices for α_l^j are found in (2.55) for odd N and in (2.62) for even N. For even $N = 2^{\mathrm{M}}$, we note that $\ominus l = l$ for all field elements and $G_N^{-1} = G_N$ since $\gamma = -1$.

As an example, we consider $N = 4$ with the field addition and multiplication tables of Table 1(a). The Fourier–Galois matrix G_4 is the tensor product of G_2 with

itself,

$$H_0^{(4)} = G_4^{-1} = G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} G_2 & G_2 \\ G_2 & -G_2 \end{pmatrix} = G_2 \otimes G_2 \,, \tag{C.4}$$

where G_2 is the 2×2 Hadamard matrix of (1.22). [Are you reminded of the sign sequences in (4.37)?] The binary components $l = (l_0, l_1)$ of the four field elements $0 = (0,0)$, $1 = (1,0)$, $2 = (0,1)$, and $3 = (1,1)$ are needed for the calculation of the phase factors

$$N = 4: \qquad {\alpha^j_{\ominus l}}^* = \alpha_l^{j\,*} = \prod_{m,n=0}^{1} (-\mathrm{i})^{j \odot (l_m 2^m) \odot (l_n 2^n)} \tag{C.5}$$

along with $2^0 \odot 2^0 = 1$, $2^0 \odot 2^1 = 2^1 \odot 2^0 = 2$, $2^1 \odot 2^1 = 3$. This gives

$$\alpha_0^{j\,*} = 1 \,, \quad \alpha_1^{j\,*} = (-\mathrm{i})^{j \odot 1} = (-\mathrm{i})^j \,, \quad \alpha_2^{j\,*} = (-\mathrm{i})^{j \odot 3} \,, \tag{C.6}$$

and

$$\alpha_3^{j\,*} = (-\mathrm{i})^{j \odot 1} \big[(-\mathrm{i})^{j \odot 2}\big]^2 (-\mathrm{i})^{j \odot 3} = (-\mathrm{i})^{j + j \odot 3} (-1)^{j \odot 2} \,. \tag{C.7}$$

The resulting phase matrices are $A_0^{(4)} = \mathbb{1}_4$ and

$$A_1^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\mathrm{i} & 0 & 0 \\ 0 & 0 & \mathrm{i} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -\mathrm{i} & 0 \\ 0 & 0 & 0 & -\mathrm{i} \end{pmatrix}, \quad A_3^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{i} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \mathrm{i} \end{pmatrix}, \tag{C.8}$$

and the Hadamard matrices are $H_0^{(4)} = G_4$ as well as

$$H_1^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -\mathrm{i} & \mathrm{i} & -\mathrm{i} & \mathrm{i} \\ \mathrm{i} & \mathrm{i} & -\mathrm{i} & -\mathrm{i} \\ 1 & -1 & -1 & 1 \end{pmatrix}, \; H_2^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -\mathrm{i} & -\mathrm{i} & \mathrm{i} & \mathrm{i} \\ -\mathrm{i} & \mathrm{i} & \mathrm{i} & -\mathrm{i} \end{pmatrix}, \; H_3^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \mathrm{i} & -\mathrm{i} & \mathrm{i} & -\mathrm{i} \\ -1 & -1 & 1 & 1 \\ \mathrm{i} & -\mathrm{i} & -\mathrm{i} & \mathrm{i} \end{pmatrix}. \tag{C.9}$$

Multiplied by $\frac{1}{\sqrt{N}} = \frac{1}{2}$ the columns of $A_j^{(4)}$ represent the kets of the jth bases with reference to the computational basis, the 4th basis.[v] Up to relabeling, they coincide with those derived by Bandyopadhyay *et al.* in a similar fashion.[24]

References

1. N. Bohr, Naturwissenschaften **16**, 245 (1928); English version: Nature **121**, 580 (1928).
2. H. Weyl, Z. Phys. **46**, 1 (1927).

[v] $A_4^{(4)} = \mathbb{1}_4$, so to say, but no factor of $\frac{1}{2}$ for the 4th basis.

3. H. Weyl, *Gruppenthorie und Quantenmechanik* (Hirzel, Leipzig, 1928), English translation by H.P. Robertson, (E.P. Dutton, New York, 1932).
4. J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).
5. J. Schwinger, *Quantum Kinematics and Dynamics* (1st edition: Benjamin, 1970; 2nd edition: Addison-Wesley, 1991; 3rd edition: Perseus Books Group, 2000).
6. J. Schwinger, *Quantum Mechanics — Symbolism of Atomic Measurements* (Springer Verlag, Berlin, 2nd printing, 2003).
7. J. Schwinger, in: *Exact Sciences and Their Philosophical Foundations*, edited by W. Deppert, K. Hübner, A. Oberschelp, and V. Weidemann (Verlag Peter Lang, Frankfurt, 1985).
8. B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001).
9. Y. Aharonov, D.Z. Albert, and L. Vaidman, Phys. Rev. Lett. **60**, 1351 (1988).
10. M.O. Scully, B.-G. Englert, and H. Walther, Nature **351**, 111 (1991).
11. B.-G. Englert, *Lectures on Quantum Mechanics — Perturbed Evolution* (World Scientific, Singapore, 2006).
12. M. Planat and P. Jorrand, J. Phys. A: Math. Theor. **41**, 182001 (2008).
13. W.K. Wootters and B.D. Fields, Ann. Phys. **191**, 363 (1989).
14. See Problems 2-12a–c in Ref. 6 and Sec. 1.2.6 in Ref. 11.
15. See, for example, equation (6.1.31) in Ref. 6.
16. S. Weigert and M. Wilkinson, Phys. Rev. A **78**, 020303 (2008).
17. I. Bengtsson and Å. Ericsson, Open Syst. Inf. Dyn. **12**, 107 (2005).
18. J.H. Conway, R.H. Hardin, and N.J.A. Sloane, Exp. Math. **5**, 93 (1996).
19. I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski J. Math. Phys. **48**, 052106 (2007).
20. G. Karpilovski, *Field theory* (Marcel Dekker Inc., New York and Basel, 1988).
21. B. Nagler and T. Durt, Phys. Rev. A **66**, 042323 (2003).
22. I.D. Ivanovic, J. Phys. A, **14**, 3241 (1981).
23. T. Durt, J. Phys. A: Math. Gen. **38**, 5267 (2005).
24. S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
25. A. Eusebi and S. Mancini, e-print arXiv:0802.4160[quant-ph] (2008).
26. T. Durt, e-print arXiv:quant-ph/0401046 (2004).
27. D.I. Fivel, Phys. Rev. Lett. **74**, 835 (1995).
28. T. Durt, COSMOS, **2**, 21 (2006).
29. T. Durt, D. Kaszlikowski, J.-L. Chen, and L.C. Kwek, Phys. Rev. A **69**, 032313 (2004).
30. Y.C. Liang, D. Kaszlikowski, B.-G. Englert, L.C. Kwek, and C.H. Oh, Phys. Rev. A **68**, 022324 (2003).
31. S.L. Braunstein, A. Mann, and M. Revzen, Phys. Rev. Lett. **68**, 3259 (1992).
32. C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
33. R.F. Werner, J. Phys. A: Math. Gen. **34**, 7081 (2001).
34. C.H. Bennett, and G. Brassard, in: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.
35. P. Boykin and V. Roychowdhury, Phys. Rev. A **67**, 042317 (2003).
36. H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
37. N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); N.J. Cerf, Acta Phys. Slov. **48**, 115 (1998); N.J. Cerf, J. Mod. Opt. **47**, 187 (2000).
38. N.J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002).
39. C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163

(1997); R.B. Griffiths and C.-S. Niu, Phys. Rev. A **56**, 1173 (1997).
40. C.-S. Niu and R.B. Griffiths, Phys. Rev. A **60**, 2764 (1999).
41. D. Bruss, M. Cinchetti, G.M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
42. A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
43. R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Phys. Rev. Lett. **78**, 405 (1997).
44. M.A. Nielsen, and I.L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, 2000).
45. L. Vaidman, Y. Aharonov, and D.Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).
46. Y. Aharonov and B.-G. Englert, Z. Naturforsch. **56a**, 16 (2001).
47. P.K. Aravind, Z. Naturforsch. **58a**, 2212 (2003).
48. T. Durt, Int. J. Mod. Phys. B **20**, 1742 (2006); and e-print arXiv:quant-ph/0401037 (2004).
49. A.I. Kostrikin and P.H. Tiep, *Orthogonal Decompositions and Integral Lattices*, de Gruyter Expositions in Mathematics **15** (Walter de Gruyter, Berlin, 1994).
50. S. Brierley, S. Weigert, and I. Bengtsson, to appear.
51. J.L. Romero, G. Björk, A.B. Klimov and L.L. Sanchez-Soto, Phys. Rev. A **72**, 062310 (2005).
52. G. Björk, J.L. Romero, A.B. Klimov, and L.L. Sanchez-Soto, JOSA **B 24**, 371 (2007).
53. D. Kaszlikowski, A. Gopinathan, Y.C. Liang, L.C. Kwek, and B.-G. Englert, Phys. Rev. A **70**, 032306 (2004).
54. B.-G. Englert and J. Řeháček, e-print arXiv:0905.2292[quant-ph] (2009).
55. E.P. Wigner, Phys. Rev. **40**, 749 (1932); M. Hillery, R.F. O'Connell, M.O. Scully, and E.P. Wigner, Phys. Rep. **106**, 121 (1984).
56. M.G.A. Paris and J. Řeháček, eds., *Quantum State Estimation*, Lecture Notes in Physics **649** (Springer Verlag, Berlin, 2004).
57. J.M. Renes, R. Blume-Kohout, A.J. Scott, and C.M. Caves J. Math. Phys. **45**, 2171 (2004).
58. M. Grassl, in: Proceedings ERATO Conference on Quantum Information Science 2004 (EQIS 2004); also: e-print arXiv:quant-ph/0406175 (2004).
59. M. Appleby, J. Math. Phys. **46**, 052107 (2005).
60. W.K. Wootters, Ann. Phys. (NY) **176**, 1 (1987).
61. W.K. Wootters, IBM J. Res. Dev. **48**, 99 (2004).
62. K.S. Gibbons, M.J. Hoffman, and W.K. Wootters, Phys. Rev. A **70**, 062101 (2004).
63. D. Gross, Appl. Phys. B **86**, 367 (2007).
64. R.J. Glauber, Phys. Rev. **131**, 2766 (1963).
65. B.-G. Englert, J. Phys. A: Math. Gen. **22**, 625 (1989).
66. R.P. Feynman, in: *Quantum Implications*, edited by B.J. Hiley and F.D. Peat (Routledge & Kegan Paul, London and New York, 1987).
67. T. Durt, C. Kurtsiefer, A. Lamas-Linares, and A. Ling, Phys. Rev. A **78**, 1 (2008).
68. A. Vourdas, Rep. Progr. Phys. **67**, 267 (2004).
69. A.O. Pittenger and M.H. Rubin, J. Phys. A: Math. Gen., **38**, 6005 (2005).
70. G. Nogues, A. Rauschenbeutel, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond, S. Haroche, L.G. Lutterbach, and L. Davidovich, Phys. Rev. A **62**, 054101 (2000).
71. P. Bertet, A. Auffeves, P. Maioli, S. Osnaghi, T. Meunier, M. Brune, J.M. Raimond, and S. Haroche, Phys. Rev. Lett. **89**, 200402 (2002).
72. B.-G. Englert, N. Sterpi, and H. Walther, Opt. Commun. **100**, 526 (1993).
73. T. Durt, J. Laser Phys. **11**, 1557 (2006).
74. T. Durt, Open Syst. Inf. Dyn. **13**, 403 (2006).

75. M.K. Bennett, *Affine and Projective Geometry* (Wiley, New York, 1995).
76. G. Terry, C. R. Ass. Fr. Av. Sci. Naturelles **1**, 122 & 2170 (1900).
77. M. Saniga, M. Planat, and H. Rosu, J. Opt. B: Quantum Semiclass. **6**, L19 (2004).
78. F. Klein, *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert* (Springer, Berlin, 1926).
79. O. Hesse, Crelle's J. **28**, 68 (1844).
80. C. Segre, Math. Ann. **27**, 296 (1886).
81. K. Hulek, Asterisque **137**, 1 (1986).
82. S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda, and R. Simon, Pramana **65**, 981 (2005).
83. J.J. Sylvester, Phil. Mag. **34**, 461 (1867).
84. J. Hadamard, Bull. Sci. Math. **17**, 240 (1893).
85. R.E.A.C. Paley, J. Math. Phys. **12**, 311 (1933).
86. H. Kharaghani and B. Tayfeh-Rezaie, J. Comb. Des. **13**, 435(2005).
87. P.O. Boykin, M. Sitharam, M. Tarifi and P. Wocjan, e-print arXiv:quant-ph/0502024 (2005).
88. A. T. Butson, Can. J. Math. **15**, 42 (1963).
89. U. Haagerup, in: Operator Algebras and Quantum Field Theory (Rome) (International Press, Cambridge, MA, 1996), p. 296.
90. G. Björck and B. Saffari, C. R. Acad. Sci. Paris, Sér. I **320**, 319 (1995).
91. M. L. Mehta, *Elements of Matrix Theory* (Hindustan Publishing Corporation, Delhi, 1977).
92. W. Pauli, in: Handbuch der Physik **24** (H. Geiger and K. Scheel, eds., Springer, Berlin, 1933), pt. 1, p. 98.
93. W. Tadej and K. Życzkowski, Lin. Alg. Appl. **429** 447 (2008).
94. W. Tadej and K. Życzkowski, Open Syst. Inf. Dyn. **13**, 133 (2006).
95. P. Diţă, J. Phys. A: Math. Gen. **37**, 5355 (2004).
96. W. Tadej, Lin. Alg. Appl. **418**, 719 (2006).
97. F. Szöllősi, e-print arXiv:0811.3930[quant-ph] (2008).
98. K. Beauchamp and R. Nicoara, Lin. Alg. Appl. **428**, 1833 (2008).
99. M. Matolcsi and F. Szöllősi, Open Syst. Inf. Dyn. **15**, 93 (2008).
100. R. Nicoara, private communication with I.B.
101. A.J. Skinner, V.A. Newell, and R. Sanchez, J. Math. Phys. **50**, 012107 (2009).
102. G.E. Moorhouse, *The 2-transitive complex Hadamard matrices*, preprint available at `http://www.uwyo.edu/moorhouse/pub/` (2001).
103. T. Tao, Math. Res. Lett. **11**, 251 (2004).
104. F. Szöllősi, Eur. J. Combin. **29**, 1219 (2008).
105. M. Petrescu, Ph.D thesis, UCLA (1997).
106. R. Craigen, W.H. Holzmann, and H. Kharaghani, J. Combin. Design **5** 319 (1998).
107. M. Matolcsi, J. Reffy, and F. Szöllősi, Open Syst. Inf. Dyn. **14**, 247 (2007).
108. R.B. Holmes and V.I. Paulsen, Lin. Alg. Appl. **377**, 31 (2004).
109. P. Diţă, *One method for construction of inverse orthogonal matrices*, preprint (November 2008).
110. The URL is `http://chaos.if.uj.edu.pl/~karol/hadamard` .
111. J. Lawrence, Č. Bruckner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).
112. Č. Bruckner and A. Zeilinger, Phys. Rev. Lett. **83**, 3354 (1999).
113. B.-G. Englert and N. Metwally, J. Mod. Opt. **47**, 2221 (2000).
114. C.H. Bennett, D.P. DiVincenzo, J. Smolin, and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).
115. G. Zauner, Ph.D. Thesis, Universität Wien (1999).

116. S. Brierley and S. Weigert, Phys. Rev. A **79**, 052316 (2009).
117. P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner, J. Phys. A: Math. Theor. **42**, 275209 (2009).
118. W. Bruzda, Master Thesis, Jagiellonian University, Cracow (2006); available online at `http://chaos.if.uj.edu.pl/~karol/prace/Br06.pdf`.
119. W. Bruzda, private communication (2008).
120. P. Butterley and W. Hall, Phys. Lett. A **369**, 5 (2007).
121. S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008).
122. C. Archer, J. Math. Phys. **46**, 022106 (2005).
123. M. Planat, H. Rosu, and M. Saniga, AIP Conf. Proc. **734**, 315 (2004).
124. M.R. Kibler, Int. J. Mod. Phys. **B 20**, 1802 (2006).
125. P. Sulc and J. Tolar, J. Phys. A: Math. Gen. **40**, 15099 (2007).
126. O. Albouy and M.R. Kibler, SIGMA **3**, 076 (2007).
127. M.R. Kibler, Int. J. Mod. Phys. **B 20**, 1792 (2006).
128. I. Bengtsson, in: Proceedings of the Växö Conference on Foundations of Probability and Physics, edited by G. Adenier, C. Fuchs, and A. Khrennikov, AIP Conf. Proc. **889** (New York 2007); available as e-print arXiv:quant-ph/0610216 (2006).
129. A.B. Klimov, J.L. Romero, G. Bjork, and L.L. Sanchez-Soto, J. Phys. A: Math. Gen. 40 3987 (2007).
130. A.B. Klimov, J.L. Romero, G. Bjork, and L.L. Sanchez-Soto, Ann. Phys. (NY) **324**, 53 (2009).
131. J. Lawrence, Č. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).
132. R. Gow, e-print arXiv:math/0703333 (2007).
133. P. Wocjan and T. Beth, Quant. Inf. Comp. **5**, 93 (2005).
134. A. Erderlyi, W. Magnus, F. Oberhettinger, and F.G. Tricomi, *Higher Transcendental Functions*, Vol. III, (McGraw–Hill, New York, 1955).
135. T. Durt, L.C. Kwek, and D. Kaszlikowski, Phys. Rev. A **77**, 042318 (2008).

*** **References that may need updates: 25, 26, 48, 54, 87, 97, 102, 109, 132**

Logical labels

Sections, equations, figures, etc.

References

Bohr27 [1]
Weyl1 [2]
Weyl2 [3]
Schwinger [4]
KinDyn [5]
SchwingerQMbook [6]
SchwingerOnWeyl [7]
Englert [8]
weakvalue [9]
SEW91 [10]
QMnotes-PE [11]
planat08 [12]
Wootters [13]
asymLimit [14]
TTF-HO [15]
WeigertWilkinson [16]
BE05 [17]
conway96 [18]
BBELTZ07 [19]
Karpilovski [20]
DurtNagler [21]
Ivanovic [22]

Durtsept [23]
india [24]
eusebi [25]
Durtmutu [26]
Fivel [27]
cosmos [28]
DurtKwek [29]
tomocrypt [30]
bellstate [31]
dense [32]
werner [33]
BB84 [34]
optimalencrypt [35]
Bechmann [36]
CERFPRL [37]
qutrits [38]
FGGNP [39]
NG [40]
bruss [41]
Ekert [42]
errorcorr [43]
nielsen [44]
vaid [45]
MK3 [46]
2003 [47]
Durtmean [48]
Kostrikin [49]
BeBrWe [50]
RBKS05 [51]
BRKS07 [52]
pyramids1 [53]
pyramids2 [54]
wigner1 [55]
QuStateEstimation [56]
Renes+al [57]
Grassl [58]
Appleby [59]
Wootters87 [60]
Wootters2 [61]
discretewigner [62]
gross [63]
Glauber [64]
wigner2 [65]
negprobFeyn [66]
wignerdurtsing [67]
Vourdas2 [68]
uncertainty [69]
Wigner-exp1a [70]
Wigner-exp1b [71]
Wigner-exp2 [72]

laser [73]
durtarxive [74]
bennett95 [75]
Terry [76]
saniga04 [77]
klein26 [78]
hesse44 [79]
segre86 [80]
hulek86 [81]
chatu05 [82]
Sy67 [83]
Ha93 [84]
Paley [85]
KT04 [86]
BSTW05 [87]
Bu63 [88]
Ha96 [89]
Bjorck [90]
mehta77 [91]
PauliProblem [92]
TZ08 [93]
TZ06a [94]
Di04 [95]
Ta07 [96]
Sz09 [97]
BN08 [98]
MS08 [99]
Nicoara [100]
SNS08 [101]
Moorhouse [102]
Tao [103]
Sz08 [104]
Pe97 [105]
Craigen [106]
MRS07 [107]
HP04 [108]
Di08 [109]
TZ06b [110]
Zeil [111]
Qinfo [112]
EngMet [113]
magi [114]
Zauner [115]
BW09 [116]
JMM09 [117]
Brthesis [118]
Br08 [119]
BH07 [120]
BW08 [121]
Archer [122]

Planat2 [123]
Ki06a [124]
ST07 [125]
AK07 [126]
Ki06b [127]
Be06 [128]
KRBS07 [129]
KRBS08 [130]
LBZ02 [131]
Go07 [132]
Beth [133]
Er55 [134]
DKK08 [135]

Analysis of references

There are no multiply defined tags.

All references are cited.

All citations are defined.

The references are ordered correctly.