World Scientific
www.worldscientific.com

ON MUTUALLY UNBIASED BASES

THOMAS DURT

TONA Vrije Universiteit Brussel,
Pleinlaan 2, B-1050 Brussels, Belgium
thomdurt@vub.ac.be

BERTHOLD-GEORG ENGLERT

Centre for Quantum Technologies,
National University of Singapore,
3 Science Drive 2, Singapore 117543, Singapore

Department of Physics, National University of Singapore,
2 Science Drive 3, Singapore 117542, Singapore
cqtebg@nus.edu.sg

INGEMAR BENGTSSON

Stockholms Universitet, Fysikum, Alba Nova,
106 91 Stockholm, Sweden
ingemar@physto.se

KAROL ŻYCZKOWSKI

Instytut Fizyki Uniwersytetu Jagiellońskiego,
ul. Reymonta 4, 30-059 Kraków, Poland

Centrum Fizyki Teoretycznej PAN, Al. Lotników 32/44,
02-668 Warszawa, Poland
karol@tatry.if.uj.edu.pl

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 $N = p^{\text{M}}$, with p prime and M a positive integer, and there is a continuum of mutually unbiased bases for a continuous degree 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 ($N = 6, 10, 12, \ldots$).

In this review, we present a unified approach in which the basis states are labeled by numbers $0, 1, 2, \ldots, N - 1$ 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, entanglement swapping, 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 related to the mutually unbiased bases.

There is a link to the mathematics of finite affine planes. We also exploit the one-to-one correspondence between unbiased bases and the complex Hadamard matrices that turn the bases into each other. The ultimate hope, not yet fulfilled, is 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 currently 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-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. Various methods have been used for the construction of maximal sets of MUB, including the Galois−Fourier approach of this review. Other constructions are based on generalized Pauli matrices, discrete Wigner functions, abelian subgroups, mutually orthogonal Latin squares, and finite-geometry methods.

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 ($N = 2^M$), 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 do not 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 maximal sets of MUB. Modifications of these constructions in the absence of a finite field do not yield maximal sets of MUB for other dimensions.

The paper is structured as follows. 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 Hei-senberg−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, $N = p^M$, 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 Secs. 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.

---

[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 non-zero element.

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. Section 3 closes with a brief discussion of entanglement swapping (Sec. 3.5).

The prime-power version of the so-called Mean King's problem (Sec. 4.1) opens the section on quantum state tomography. The Mean King's problem 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 comment 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 is 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. All Hadamard matrices of size $N \leq 5$ have been classified (Sec. 5.3), and 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 four appendixes. The standard set of MUHM for prime dimension is given in Appendix B, and a prime-distinguishing function related to this standard set is introduced in Appendix C. Finally, Appendix D 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,[1,2] 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-1/2 object. These are, in fact, the extreme cases of a continuous 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 exclusive outcomes. Following Weyl[3,4] and Schwinger,[5−7] 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,

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

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

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

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. It follows in particular that, if A and B are complementary, then αA and βB with $\alpha\beta \neq 0$ are complementary as well. And if a unitary transformation turns A into A' and B into B', then the pair A', B' is complementary if the pair A, B is. Therefore, 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 unitary operators to represent physical quantities. In the present context, these will be

---

[b]In fact, there can be different right-hand sides for infinite degrees of freedom, when normalization is more subtle; see Secs. 1.1.8−1.1.11. 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.
[d]A brief account of the history of the subject can be found in Ref. 8.

nondegenerate 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,

$$A|a_j\rangle = |a_j\rangle\gamma_N^j, \quad B|b_k\rangle = |b_k\rangle\gamma_N^k \quad \text{with } \gamma_N = e^{i2\pi/N}. \tag{1.4}$$

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

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

which is the operator version of (1.1). Indeed, (1.1) and (1.5) imply each other.[9]

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 $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ — we will refer to it as the *computational basis* from Sec. 2.2 onwards. Then we define a second orthonormal basis $|\widehat{0}\rangle, |\widehat{1}\rangle, \ldots, |\widehat{N-1}\rangle$ by means of the discrete quantum Fourier transformation,

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

so that

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

by construction — the two bases are MU, indeed.

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

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

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,

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

as well as

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

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.

When we change the kets of the reference basis by phase factors, $|k\rangle \to |k\rangle e^{i\phi_k}$, the resulting second basis will change accordingly and we get another complementary partner X to the same observable Z. This freedom to adjust phases that do not affect the projectors $|k\rangle\langle k|$ of the reference basis but modify the projectors $|\widehat{j}\rangle\langle\widehat{j}|$ of the Fourier transformed basis is crucial for quantifying Einstein's[10,11] and de Broglie's[12] wave-particle duality in the context of two-path[13,14] and multi-path[15] interferometers.

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,

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

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

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

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,

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

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.

---

[e] Numbers of the form of $f_{j,k}$ are known as "weak values" of F in the context of "weak measurements."[16]

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.*[17] For a textbook discussion, see Ref. 18.

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

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

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

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 $\pm\sigma_x\sigma_z = \mp i\sigma_y$. 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 are composed by multiplication, there is also the notion of the Heisenberg−Weyl group as a group of unitary transformations

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

that are composed by sequential execution. There is no difference in (1.18) between $Y = X^n Z^m$ and $Y = Z^m X^n$,

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

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. 4.

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,

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

For the group of unitary operators, the appearance of $(-1)^{mn}$ is crucial, telling us that one quarter of the $Y_{l,m,n}$s 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

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

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*.[19−22] It contains the Heisenberg−Weyl group as a subgroup, but is truly larger. For $N = 2$, the Clifford group contains 24 unitary transformations (and is isomorphic to the symmetry group of the cube) whereas the Heisenberg−Weyl group contains only four unitary transformations. An example of a transformation belonging to the former but not the latter is the "q-bit Hadamard gate" $(\sigma_x + \sigma_z)/\sqrt{2}$ that is represented by the familiar Hadamard matrix

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

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 $(Y_{0,N_1,0})^{N_2} = (X^{N_1})^{N_2} = X^N = \mathbf{1}$. 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 methodical 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

---

[f]Anti-unitary operators could be, and often are, included — see Ref. 19, for example — but we have no use for them here.

$k = k_1 + k_2 N_1$ 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

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

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

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

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 $\langle \widehat{j}_1, \widehat{j}_2|$ of X_1 and X_2, which are related to the kets $|k_1, k_2\rangle$ through the analog of (1.7),

$$
\langle \widehat{j}_1, \widehat{j}_2 | k_1, k_2\rangle = \frac{1}{\sqrt{N_1}} \gamma_{N_1}^{j_1 k_1} \frac{1}{\sqrt{N_2}} \gamma_{N_2}^{j_2 k_2}.
\tag{1.26}
$$

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 $|\widehat{j}_1, \widehat{j}_2\rangle$ 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,[7] 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

$$X, XZ, XZ^2, \ldots, XZ^{N-1}, Z \qquad (1.27)$$

are pairwise complementary,[9] as one verifies most directly with the aid of (1.5) and (1.16) in conjunction with

$$\mathrm{tr}\{Y_{l,m,n}\} = N\gamma_N^l \delta_{m,0}\delta_{n,0}. \qquad (1.28)$$

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.[23] 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 cyclic 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 $X^m Z^n$ product.

Explicitly, ket $|i, k\rangle$, the kth eigenket of the ith basis, $XZ^i|i, k\rangle = |i, k\rangle\gamma_N^k$, is given by

$$N \text{ odd}: |i, k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |l\rangle\gamma_N^{-kl}\gamma_N^{il(l-1)/2} \quad \text{for } i = 0, 1, 2, \ldots, N - 1 \qquad (1.29)$$

in terms of the reference basis of eigenkets of Z. For $i = 0$ we have the eigenstates of X, $|\widehat{k}\rangle = |0, k\rangle$. While (1.29) correctly states the eigenkets of XZ^i for all odd N, these bases are pairwise MU only if N is prime. With due attention to the extra phase factors required by (1.20) one can give a similar expression for $|i, k\rangle$ when N is even.

In summary, we can systematically construct $N + 1$ bases that are MU if N is prime. As noted, the construction based on the cyclic operators in (1.27) 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, and a general discussion for arbitrary $N \geq 2$ is given in Appendix C.

Yet, this is not the end of the story. If $N = p^M$ 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 $N = 6$. The question whether there are seven MUB for $N = 6$ is currently 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 $\langle \widehat{j}|$ of the Fourier-transformed basis such that now $j, k = 0, \pm 1, \pm 2, \ldots, \pm 1/2(N - 1)$.

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

$$N = \frac{2\pi}{\epsilon^2} \tag{1.30}$$

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

$$
\begin{aligned}
j &\to j\epsilon = a = 0, \pm\epsilon, \pm 2\epsilon, \ldots, \pm\left(\frac{\pi}{\epsilon} - \frac{\epsilon}{2}\right), \\
k &\to k\epsilon = b = 0, \pm\epsilon, \pm 2\epsilon, \ldots, \pm\left(\frac{\pi}{\epsilon} - \frac{\epsilon}{2}\right).
\end{aligned}
\tag{1.31}
$$

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 unity, so that it effects $b \to b + \epsilon$. Likewise Z applied to $\langle \widehat{j}|$ results in $a \to a + \epsilon$. This suggests the identification of hermitian operators A and B such that

$$
\begin{aligned}
X &= \mathrm{e}^{\mathrm{i}\epsilon A} \quad \text{with } A = A^\dagger, \\
Z &= \mathrm{e}^{\mathrm{i}\epsilon B} \quad \text{with } B = B^\dagger.
\end{aligned}
\tag{1.32}
$$

The Weyl commutation relation (1.11) then appears as

$$X^k Z^j = \mathrm{e}^{-\mathrm{i}\frac{2\pi}{N}jk} Z^j X^k \to \mathrm{e}^{\mathrm{i}k\epsilon A}\mathrm{e}^{\mathrm{i}j\epsilon B} = \mathrm{e}^{-\mathrm{i}j\epsilon k\epsilon}\mathrm{e}^{\mathrm{i}j\epsilon B}\mathrm{e}^{\mathrm{i}k\epsilon A} \tag{1.33}$$

or

$$e^{ibA}e^{iaB} = e^{-iab}e^{iaB}e^{ibA}. \tag{1.34}$$

The two equivalent versions

$$\begin{aligned}
e^{ib(A-a\mathbf{1})} &= e^{-iaB}e^{ibA}e^{iaB} = e^{ib\,e^{-iaB}A\,e^{iaB}}, \\
e^{ia(B-b\mathbf{1})} &= e^{ibA}e^{iaB}e^{-ibA} = e^{ia\,e^{ibA}B\,e^{-ibA}}
\end{aligned} \tag{1.35}$$

seem to imply that

$$\begin{aligned}
e^{-iaB}A\,e^{iaB} &= A - a\mathbf{1}, \\
e^{ibA}B\,e^{-ibA} &= B - b\mathbf{1},
\end{aligned} \tag{1.36}$$

but this does not follow without imposing a restricting condition, just as $e^{i\alpha} = e^{i\beta}$ 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,

$$\langle a|e^{ia'B} = \langle a + a' \ (\mathrm{mod}\ 2\pi/\epsilon)|, \quad e^{ib'A}|b\rangle = |b + b' \ (\mathrm{mod}\ 2\pi/\epsilon)\rangle, \tag{1.37}$$

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 (1.36) hold with continuous values for a and b. We can, therefore, exhibit the terms that are linear in a or b and arrive at

$$AB - BA = [A, B] = i\mathbf{1}. \tag{1.38}$$

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

$$\langle a| = \frac{1}{\sqrt{\epsilon}}\langle \widehat{j}| \Big|_{\epsilon \to 0} \quad \text{with } j\epsilon = a, \quad \text{and} \quad |b\rangle = |k\rangle\frac{1}{\sqrt{\epsilon}}\Big|_{\epsilon \to 0} \quad \text{with } k\epsilon = b, \tag{1.39}$$

and then get

$$\langle a|b\rangle = \frac{1}{\sqrt{2\pi}}e^{iab} \tag{1.40}$$

as the analog of (1.7) as well as

$$\langle a|a'\rangle = \delta(a - a'), \quad \langle b|b'\rangle = \delta(b - b') \tag{1.41}$$

and

$$\int_{-\infty}^{\infty} da\, |a\rangle\langle a| = \mathbf{1} = \int_{-\infty}^{\infty} db\, |b\rangle\langle b| \tag{1.42}$$

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. 7; see also Sec. 1.2.5 in Ref. 18. It should be appreciated that $N \to \infty$ is not a limit in the precise sense that one has in calculus. Rather, it is a systematic method for inferring the properties of the basic operators for continuous degrees of freedom, but these operators then stand on their own and the consistency of the inferred algebraic properties must be verified.

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 (position and momentum for motion along a line), there are also asymmetric limits. For instance, if the position variable — the analog of the Hermitian A of (1.32) — is kept periodic over a finite range in the limit, one obtains the pair of azimuth-angle operator and angular-momentum operator for motion on a circle,[24] with which we deal in Sec. 1.1.9. In a third way of taking the $N \to \infty$ limit, the Hermitian position variable is kept positive throughout and one arrives at a continuous quantum degree of freedom of the kind that parameterizes radial motion; see Sec. 1.1.10. Finally, there is a fourth procedure, in which the position values cover a finite range without, however, retaining the cyclic nature by identifying the boundaries with each other; this results in a degree of freedom of the kind associated with the polar angle in spherical coordinates (Sec. 1.1.11).

1.1.8. *Continuous degree of freedom 1: Motion along a line*

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, although an interesting complication can be observed too.[25]

Harking back to Sec. 1.1.6, we recall that each basis in the set of MUB consists of the joint eigenstates of the unitary operators that one gets by taking products of *one* of the unitary operators in the list (1.27) with itself. Translated into the continuum case of Sec. 1.1.7, the corresponding unitary operators are those of (1.34), and since

$$\mathrm{e}^{\mathrm{i}b_1 A}\mathrm{e}^{\mathrm{i}a_1 B}\,\mathrm{e}^{\mathrm{i}b_2 A}\mathrm{e}^{\mathrm{i}a_2 B} = \mathrm{e}^{\mathrm{i}(a_1 b_2 - b_1 a_2)}\,\mathrm{e}^{\mathrm{i}b_2 A}\mathrm{e}^{\mathrm{i}a_2 B}\,\mathrm{e}^{\mathrm{i}b_1 A}\mathrm{e}^{\mathrm{i}a_1 B} \tag{1.43}$$

tells us that two of these unitary operators commute if $a_1 b_2 = b_1 a_2$, the operators $\mathrm{e}^{\mathrm{i}bA}\mathrm{e}^{\mathrm{i}aB}$ for which $(a, b) = (\alpha t, \beta t)$ with common values of α and β make up an abelian subgroup of Heisenberg−Weyl operators. The elements of the subgroup specified by the pair (α, β) are labeled by parameter t, which takes on all real values. For $\alpha = \beta = 0$, we have the one-element subgroup of the identity; this case is of no further interest and excluded from the following considerations.

It is expedient to choose the single-exponent form

$$Y(\alpha, \beta; t) = \mathrm{e}^{\mathrm{i}t(\beta A + \alpha B)} \tag{1.44}$$

for the subgroup elements, so that the subgroup composition rule

$$Y(\alpha, \beta; t_1) Y(\alpha, \beta; t_2) = Y(\alpha, \beta; t_1 + t_2) \tag{1.45}$$

involves no additional phase factors, and we denote the common eigenkets and eigenbras of all unitary operators in the (α, β) subgroup by $|\alpha, \beta; y\rangle$ and $\langle \alpha, \beta; y|$,

$$Y(\alpha, \beta; t)|\alpha, \beta; y\rangle = |\alpha, \beta; y\rangle e^{ity}, \quad \langle \alpha, \beta; y|\, Y(\alpha, \beta; t) = e^{ity}\langle \alpha, \beta; y|. \tag{1.46}$$

If one wishes, one can regard $|\alpha, \beta; y\rangle$ and $\langle \alpha, \beta; y|$ as eigenstates of the Hermitian operator $\beta A + \alpha B$ with eigenvalue y, but we prefer to work with the sets of bounded unitary operators rather than the unbounded Hermitian operators.

As usual, the eigenstates are normalized to the Dirac delta function,

$$\langle \alpha, \beta; y \,|\, \alpha, \beta; y' \rangle = \delta(y - y'), \tag{1.47}$$

which implies that, up to a phase factor of no consequence,

$$|\lambda\alpha, \lambda\beta; \lambda y\rangle \sqrt{|\lambda|} = |\alpha, \beta; y\rangle \tag{1.48}$$

for $\lambda \neq 0$, consistent with $Y(\lambda\alpha, \lambda\beta; t/\lambda) = Y(\alpha, \beta; t)$. The subgroup for $(\lambda\alpha, \lambda\beta)$ is identical with the subgroup for (α, β), with the elements parameterized differently. The respective eigenstates are in one-to-one correspondence, but differ from each other by a normalization factor (except when $\lambda = -1$).

These statements have no analogs for finite N, when the normalization of states is unambiguous and the parameterization of the abelian subgroups is essentially unique. In the continuous case, by contrast, there is more than one way of parameterizing the continuous abelian subgroups, and one would have to impose constraints on α and β to avoid this innocuous ambiguity, such as insisting on $\alpha = \cos\theta$ and $\beta = \sin\theta$ with $0 \leq \theta < \pi$ or, equivalently, permitting only $(\alpha, \beta) = (0, 1)$ and $\alpha = 1$ with arbitrary β. Clearly, constraints of this sort are a bit awkward, and they are not necessary.

The projector $|\alpha, \beta; y\rangle\langle\alpha, \beta; y|$ is given by

$$|\alpha, \beta; y\rangle\langle\alpha, \beta; y| = \int_{-\infty}^{\infty} \frac{dt}{2\pi} Y(\alpha, \beta; t) e^{-ity} \tag{1.49}$$

as one verifies by, for instance, checking that

$$(|\alpha, \beta; y\rangle\langle\alpha, \beta; y|)|\alpha, \beta; y'\rangle = |\alpha, \beta; y\rangle\delta(y - y'). \tag{1.50}$$

The completeness relation

$$\int_{-\infty}^{\infty} dy\, |\alpha, \beta; y\rangle\langle\alpha, \beta; y| = Y(\alpha, \beta; 0) = \mathbf{1} \tag{1.51}$$

follows and confirms that we have a basis for each of the abelian subgroups.

Next, we consider two different abelian subgroups, specified by (α, β) and (α', β'), respectively, with $\alpha\beta' \neq \beta\alpha'$, and evaluate the transition probability density[g]

---

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

between their respective eigenstates by means of

$$
\begin{aligned}
|\langle \alpha, \beta; y \,|\, \alpha', \beta'; y' \rangle|^2 &= \mathrm{tr}\{(|\alpha, \beta; y\rangle\langle \alpha, \beta; y|)(|\alpha', \beta'; y'\rangle\langle \alpha', \beta'; y'|)\} \\
&= \int \frac{\mathrm{d}t\,\mathrm{d}t'}{(2\pi)^2}\,\mathrm{tr}\{Y(\alpha, \beta; t)Y(\alpha', \beta'; t')\}\,\mathrm{e}^{-\mathrm{i}(ty+t'y')} \\
&= \int \frac{\mathrm{d}t\,\mathrm{d}t'}{(2\pi)^2}\,\frac{2\pi\delta(t)\delta(t')}{|\alpha\beta' - \beta\alpha'|}\,\mathrm{e}^{-\mathrm{i}(ty+t'y')} \\
&= \frac{1}{2\pi|\alpha\beta' - \beta\alpha'|},
\end{aligned}
\tag{1.52}
$$

which is Eq. (11) in Ref. 25. Since the value of $|\langle \alpha, \beta; y \,|\, \alpha', \beta'; y' \rangle|^2$ does not depend on the quantum numbers y and y' that label the states of the two bases, the two bases are MU. This is true for the bases to any two different abelian subgroups. Indeed, we have a continuum of MUB for a continuous degree of freedom.

As a consequence, the Hermitian operators $\beta A + \alpha B$ and $\beta' A + \alpha' B$ are complementary observables if their commutator $\mathrm{i}[\beta A + \alpha B, \beta' A + \alpha' B] = (\alpha\beta' - \beta\alpha')\mathbf{1}$ does not vanish. The absolute value of this commutator appears in the denominator of (1.52). Not unexpectedly, for a continuous degree of freedom, there is a continuum of pairwise complementary observables.

We could have arrived at the same conclusion by the following more direct argument that exploits the observations made after (1.2). There are unitary transformations that turn $\beta A + \alpha B$ into κA and $\beta' A + \alpha' B$ into $\kappa' B$ with $\kappa\kappa' = \alpha\beta' - \beta\alpha' \neq 0$. Now, since the pair A, B is complementary, so is the pair $\kappa A, \kappa' B$, which implies that the pair $\beta A + \alpha B, \beta' A + \alpha' B$ is complementary as well, and their bases of eigenstates are MU.

Whereas the right-hand side of (1.1) has the same value of N^{-1} for any pair of MUB for a N-dimensional degree of freedom, this is not the case for the right-hand side of (1.52); recall footnote 'b'. For a given pair of bases specified by the coefficients (α, β) and (α', β'), we can either choose $(\alpha'', \beta'') = (\alpha + \alpha', \beta + \beta')$ or $(\alpha'', \beta'') = (\alpha - \alpha', \beta - \beta')$ to supplement them with a third basis such that these three MUB have the same numerical value for the constant transition probability densities between each pair of bases. The basis for any fourth choice (α''', β''') will have a different value for one or more of its transition probability densities with the earlier three bases. This observation by Weigert and Wilkinson[25] means that the continuous set of MUB, composed of the bases of (1.46), contains three-element subsets that are polytopes of MUB in the sense of Sec. 1.2.

1.1.9. *Continuous degree of freedom 2: Motion along a circle*

We parameterize the position around the circle by the 2π-periodic azimuth φ — with $|\varphi\rangle = |\varphi + 2\pi\rangle$, for instance — and normalize the corresponding bras and kets in accordance with the orthogonality and completeness relations

$$
\langle\varphi|\varphi'\rangle = 2\pi\delta^{(2\pi)}(\varphi - \varphi'), \quad \int_{(2\pi)} \frac{\mathrm{d}\varphi}{2\pi}\,|\varphi\rangle\langle\varphi| = \mathbf{1},
\tag{1.53}
$$

where the integration range is any 2π interval and $\delta^{(2\pi)}(\ )$ denotes the 2π-periodic version of Dirac's delta function,

$$\delta^{(2\pi)}(\varphi - \varphi') = \frac{1}{2\pi} \sum_{l=-\infty}^{\infty} e^{il(\varphi - \varphi')}. \tag{1.54}$$

We regard the azimuthal states $|\varphi\rangle$ as eigenstates of a unitary operator E,

$$E|\varphi\rangle = |\varphi\rangle e^{i\varphi}, \quad E = \int_{(2\pi)} \frac{d\varphi}{2\pi} |\varphi\rangle e^{i\varphi} \langle\varphi|. \tag{1.55}$$

This E is the proper $N \to \infty$ limit of X in the present context.

All azimuthal wave functions $\psi(\varphi) = \langle\varphi| \ \rangle = \psi(\varphi + 2\pi)$ are periodic, and the Fourier series of $\langle\varphi|$ identifies the eigenstates of the associated angular momentum operator L,

$$\langle\varphi| = \sum_{l=-\infty}^{\infty} e^{il\varphi}\langle l|, \quad L|l\rangle = |l\rangle l. \tag{1.56}$$

Their orthonormality and completeness relations are

$$\langle l|l'\rangle = \delta_{l,l'}, \quad \sum_{l=-\infty}^{\infty} |l\rangle\langle l| = \mathbf{1}, \tag{1.57}$$

consistent with (1.53).

In view of

$$\langle\varphi|l\rangle = e^{il\varphi}, \quad |\langle\varphi|l\rangle|^2 = 1, \tag{1.58}$$

the φ-basis and the l-basis are MU. The respective unitary shift operators are powers of E and exponential functions of L,

$$E^m|l\rangle = |l+m\rangle, \quad \langle\varphi|e^{i\phi L} = \langle\varphi + \phi|. \tag{1.59}$$

Their products $E^m e^{i\alpha L}$ make up the Heisenberg−Weyl group with the basic Weyl commutation relation given by

$$E^m e^{i\phi L} = e^{-im\phi} e^{i\phi L} E^m, \tag{1.60}$$

which is the analog of (1.34). For each modulo-2π value of ϕ, there is an abelian subgroup composed of the unitary operators $(E e^{i\phi L})^m$ with $m = 0, \pm 1, \pm 2, \ldots$.

Despite these analogies and the great structural similarities with the situation of Sec. 1.1.8, there is a striking difference: there is no third basis that is MU with respect to both the φ-basis and the l-basis.

To make this point, let us assume that ket $| \ \rangle$ belongs to such a third basis. Then it must be true that

$$|\langle\varphi| \ \rangle|^2 = \lambda > 0 \quad \text{for all } \varphi \quad \text{and} \quad |\langle l| \ \rangle|^2 = \mu > 0 \quad \text{for all } l. \tag{1.61}$$

The completeness relations in (1.53) and (1.57) then imply

$$\langle\,|\,\rangle = \int_{(2\pi)} \frac{\mathrm{d}\varphi}{2\pi} |\langle\varphi|\,\rangle|^2 = \int_{(2\pi)} \frac{\mathrm{d}\varphi}{2\pi} \lambda = \lambda \quad\text{and}$$

$$\langle\,|\,\rangle = \sum_{l=-\infty}^{\infty} |\langle l|\,\rangle|^2 = \sum_{l=-\infty}^{\infty} \mu = \infty, \tag{1.62}$$

which contradict each other. It follows that there is not even a single ket with the properties (1.61); indeed, there is no third basis.

This situation of a missing third basis is a unique feature of the E, L-type continuous degree of freedom. There is always a third basis for finite N — the three eigenbases to X, Z, and XZ of (1.27) are pairwise MU for all $N > 1$ — and there is a continuum of MUB for the continuous degrees of freedom of the three other types. It appears that the combination of the continuous position variable E with the discrete momentum variable L is at the heart of the matter. For the other continuous degrees of freedom, the respective position and momentum variables are both continuous, as will be discussed below.

The nonexistence of a third basis that supplements the φ-basis and the l-basis does not exclude the possibility that there are other bases that are MU, perhaps with sets of MUB that have more than two elements. Currently, we are not aware of any such set, however, but its bases would have to be rather unusual. For two different discrete bases (such as the l-basis) cannot be MU, nor can two different continuous bases (such as the φ-basis) be MU. And if one basis is discrete and the other continuous, the dilemma of (1.62) cannot be avoided.

1.1.10. *Continuous degree of freedom 3: Radial motion*

In spherical coordinates, radial motion is characterized by a positive position operator $R > 0$,

$$R|r\rangle = |r\rangle r \quad\text{with } r > 0, \quad \langle r|r'\rangle = r\delta(r - r'), \quad \int_0^\infty \frac{\mathrm{d}r}{r}|r\rangle\langle r| = \mathbf{1}, \tag{1.63}$$

whereas the eigenvalues of its complementary partner S are all real numbers,

$$S|s\rangle = |s\rangle s \quad\text{with} -\infty < s < \infty, \quad \langle s|s'\rangle = \delta(s - s'), \quad \int_{-\infty}^\infty \mathrm{d}s\,|s\rangle\langle s| = \mathbf{1}. \tag{1.64}$$

The transition amplitudes

$$\langle r|s\rangle = \frac{r^{\mathrm{i}s}}{\sqrt{2\pi}} \tag{1.65}$$

confirm that the r-basis and the s-basis are MU and that R and S are a pair of complementary observables.

The unitary shift operators R^{it} and $e^{i\lambda S}$ have the expected effect when applied to the states of the other basis,

$$\langle r | e^{i\lambda S} = \langle e^\lambda r |, \qquad R^{it} | s \rangle = | s + t \rangle, \tag{1.66}$$

as follows from (1.65). The resulting Weyl commutation relation

$$R^{it} e^{i\lambda S} = e^{-i\lambda t} e^{i\lambda S} R^{it} \tag{1.67}$$

and the Heisenberg commutator

$$[R, S] = iR \tag{1.68}$$

tell us that S is the Hermitian generator of scaling transformations,

$$e^{-i\lambda S} R \, e^{i\lambda S} = e^{-\lambda} R, \tag{1.69}$$

fitting to the positive nature of R.

The unitary operator products in (1.67) make up the Heisenberg−Weyl group here, and the abelian subgroups can be characterized by common values of τ and μ in $(t, \lambda) = \kappa(\tau, \mu)$. In full analogy with (1.46)−(1.52), then, the bases defined by

$$e^{i\kappa^2 \tau\mu/2} R^{i\kappa\tau} e^{i\kappa\mu S} | \tau, \mu; \alpha \rangle = | \tau, \mu; \alpha \rangle e^{i\kappa\alpha} \tag{1.70}$$

for $(\tau, \mu) \neq (0, 0)$ are pairwise MU,

$$| \langle \tau, \mu; \alpha \, | \, \tau', \mu'; \alpha' \rangle |^2 = \frac{1}{2\pi | \tau\mu' - \mu\tau' |}. \tag{1.71}$$

Just as in Sec. 1.1.8, here too we have a continuum of pairwise complementary observables and a continuum of MUB, and the set of MUB has three-element polytopes in the sense of Ref. 25. The R, S-type degree of freedom is really quite similar to the A, B-type degree of freedom of the Heisenberg kind, because $\log R$ and S are a Heisenberg pair of operators: $[\log R, S] = i\mathbf{1}$. This commutator is a particular case of

$$[f(R), S] = iR \frac{\partial f(R)}{\partial R}, \tag{1.72}$$

which follows from (1.68) or from (1.69).

1.1.11. *Continuous degree of freedom 4: Motion within a segment*

After dealing with the azimuthal and radial degrees of freedom in Secs. 1.1.9 and 1.1.10, we now turn to the degree of freedom associated with the polar angle ϑ of spherical coordinates, $(x, y, z) = (r \sin\vartheta \, \cos\varphi, r \sin\vartheta \, \sin\varphi, r \cos\vartheta)$. Since the values of ϑ are restricted to a finite interval $0 \leq \vartheta \leq \pi$, where the endpoints are not identified with each other as is the case for the periodic azimuth φ, we speak of "motion within a segment," very much like the popular textbook example of the "particle in a box," about which some non-textbook material is reported in Ref. 26. The relations between the position and momentum operators for cartesian and spherical coordinates are discussed in Appendix A.

The eigenstates of the position variable Θ and its complementary partner Ω are related to each other by

$$\langle\vartheta|\omega\rangle = \frac{1}{\sqrt{2\pi}}\left(\tan\frac{\vartheta}{2}\right)^{\mathrm{i}\omega} \quad \text{with } 0 < \vartheta < \pi \quad \text{and} \quad -\infty < \omega < \infty, \tag{1.73}$$

and the respective orthonormality and completeness relations are

$$\langle\vartheta|\vartheta'\rangle = \sin\vartheta \, \delta(\vartheta - \vartheta'), \quad \int_0^\pi \frac{\mathrm{d}\vartheta}{\sin\vartheta} \, |\vartheta\rangle\langle\vartheta| = \mathbf{1} \tag{1.74}$$

for the ϑ-basis as well as

$$\langle\omega|\omega'\rangle = \delta(\omega - \omega'), \quad \int_{-\infty}^\infty \mathrm{d}\omega \, |\omega\rangle\langle\omega| = \mathbf{1} \tag{1.75}$$

for the ω-basis. Accordingly, the unitary shift operators are specified by

$$\langle\vartheta|\mathrm{e}^{\mathrm{i}\lambda\Omega} = \langle\vartheta'|\big|_{\vartheta'=2\arctan(\mathrm{e}^\lambda\tan\frac{\vartheta}{2})}, \quad \left(\tan\frac{\Theta}{2}\right)^{\mathrm{i}\omega'}|\omega\rangle = |\omega + \omega'\rangle, \tag{1.76}$$

telling us that the unitary transformation effected by $\mathrm{e}^{\mathrm{i}\lambda\Omega}$ has no simple geometrical meaning.

The Weyl commutation relation reads

$$\left(\tan\frac{\Theta}{2}\right)^{\mathrm{i}\omega}\mathrm{e}^{\mathrm{i}\lambda\Omega} = \mathrm{e}^{-\mathrm{i}\omega\lambda}\mathrm{e}^{\mathrm{i}\lambda\Omega}\left(\tan\frac{\Theta}{2}\right)^{\mathrm{i}\omega}, \tag{1.77}$$

from which we get the Heisenberg commutator

$$[\Theta, \Omega] = \mathrm{i} \, \sin\Theta. \tag{1.78}$$

More generally, we have the analog of (1.72),

$$[f(\Theta), \Omega] = \mathrm{i} \, \sin\Theta \frac{\partial f(\Theta)}{\partial\Theta}, \tag{1.79}$$

and the particular case

$$\left[\log\tan\frac{\Theta}{2}, \Omega\right] = \mathrm{i}\,\mathbf{1} \tag{1.80}$$

identifies $\log\tan(\Theta/2)$ and Ω as a Heisenberg pair of complementary observables. Remembering the lessons of Secs. 1.1.8 and 1.1.10, we conclude that the abelian subgroups of the Heisenberg−Weyl group composed of the unitary operators of (1.77) define a continuum of MUB, with the set of MUB having three-element subsets that are MUB polytopes in the sense of Ref. 25.

We close this excursion into the realm of continuous degrees of freedom with a comment on the completeness and orthonormality relations (1.63) and (1.74). Why did we not absorb the factors r and $\sin\vartheta$ into the normalization of the respective bras

and kets? There are two good reasons: (i) Such a change of normalization would spoil the relations (1.65) and (1.73); (ii) these factors would re-appear in a disturbing way when the orthonormality and completeness relations are rewritten in terms of the eigenstates for the Heisenberg partners $\log R$ and $\log \tan (\Theta/2)$ of S and Ω, respectively. In other words, it is very natural to have the factors r and $\sin \vartheta$ in (1.63) and (1.74).

In view of the various subtle issues regarding the normalization of eigenkets and eigenbras for continuous degrees of freedom, the definition of what constitutes a pair of complementary observables — given above in the context of (1.1) — should perhaps be modified to state more carefully that two nondegenerate observables A and B are complementary if one can normalize their respective eigenstates consistently such that $|\langle a|b\rangle|^2$ has the same value for all eigenbras $\langle a|$ of A and all eigenkets $|b\rangle$ of B.

1.2. *A geometrically motivated measure of mutual unbiasedness*

The kets $|\ \rangle$ in N-dimensional Hilbert space, 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

$$\varrho_\star = \frac{1}{N}\mathbb{1} \mathrel{\widehat{=}} \frac{1}{N}\mathbf{1} = \rho_\star, \tag{1.81}$$

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

$$\mathbf{m} = M - \varrho_\star. \tag{1.82}$$

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

$$\mathbf{m}_1 \cdot \mathbf{m}_2 = \frac{1}{2}\text{tr}\{(M_1 - \varrho_\star)(M_2 - \varrho_\star)\}. \tag{1.83}$$

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

$$D(\mathbf{m}_1, \mathbf{m}_2)^2 = \frac{1}{2}\text{tr}\{(M_1 - M_2)^2\}. \tag{1.84}$$

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

$$\mathbf{e} = \psi_e \psi_e^\dagger - \varrho_\star \,\widehat{=}\, |e\rangle\langle e| - \rho_\star \tag{1.85}$$

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

$$|\mathbf{e}|^2 = \frac{N-1}{2N}. \tag{1.86}$$

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 relations

$$\langle e_i|e_j\rangle = \delta_{i,j}, \quad \mathbf{e}_i \cdot \mathbf{e}_j = \frac{1}{2}\delta_{i,j} - \frac{1}{2N} \tag{1.87}$$

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

$$\sum_{i=0}^{N-1} \mathbf{e}_i = 0. \tag{1.88}$$

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

$$|\langle e_i|f_j\rangle|^2 = \frac{1}{N}, \quad \mathbf{e}_i \cdot \mathbf{f}_j = 0 \tag{1.89}$$

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 $N(N+1)$ vertices.[27] 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 vertices 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

$$B = [\mathbf{e}_1 \mathbf{e}_2 \cdots \mathbf{e}_N]. \tag{1.90}$$

It has rank $N-1$ because of (1.88). Next, form the projector onto the $(N-1)$-plane spanned by the linearly dependent vectors $\mathbf{e}_i$. It is

$$\Pi = 2BB^{\mathrm{T}}. \tag{1.91}$$

Finally, the square of the chordal Grassmannian distance between a pair of planes is[28]

$$D_c(\Pi_e, \Pi_f)^2 \equiv \frac{1}{2}\mathrm{tr}\{(\Pi_e - \Pi_f)^2\} = N - 1 - \sum_{a,b}\left(|\langle e_a|f_b\rangle|^2 - \frac{1}{N}\right)^2$$

$$= \sum_{a,b}|\langle e_a|f_b\rangle|^2(1 - |\langle e_a|f_b\rangle|^2), \tag{1.92}$$

where the kets $|e_a\rangle$ are related to Π_e through (1.85), (1.90) and (1.91), and the kets $|f_b\rangle$ are analogously related to Π_f. The last expression of (1.92) 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

$$0 \le D_c^2 \le N - 1, \tag{1.93}$$

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,[29] and as a measure of "MUness".[28] 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

$$\langle D_c^2 \rangle_{\mathrm{FS}} = \frac{N}{N+1} (N-1). \tag{1.94}$$

If the dimension is large, $N \gg 1$, two bases picked at random are likely to be almost MU. Let us finally mention that entropic uncertainty relations in effect provide an interesting alternative measure of "MUness".[30−32]

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 $N = p^{\mathrm{M}}$ 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 $N = p^{\mathrm{M}}$ elements. We shall label these elements by integer numbers i, $0 \le i \le N - 1$, or, equivalently, by M-tuples $(i_0, i_1, \ldots, i_{\mathrm{M}-1})$ of integers, each integer running from 0 to $p - 1$, that we get from the p-ary expansion of i:

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

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

$$i = j \oplus k \text{ is tantamount to } i_n = j_n + k_n \pmod{p} \tag{2.2}$$

for $n = 0, 1, \ldots, \mathrm{M} - 1$, 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,

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

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 $N = p^{\text{M}}$).

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 $j, k = 0, 1, \ldots, \text{M} - 1$.

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

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

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

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

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.

In a standard textbook parameterization of the Galois field with $N = p^{\text{M}}$ elements,[33] one identifies the field elements with polynomials that are defined by the coefficients of the p-ary expansion of (2.1),

$$
i = (i_0, i_1, \ldots, i_{\text{M}-1}) \longleftrightarrow \sum_{m=0}^{\text{M}-1} i_m x^m.
\tag{2.6}
$$

Addition and multiplication of the field elements are then carried out as addition and multiplication of the corresponding polynomials modulo the polynomial of (2.5), with the resulting sums and products stated as polynomials of degree $\text{M} - 1$ with modulo-p integer coefficients. Clearly, this gives the component-wise addition of (2.2) and multiplication in accordance with (2.4). Since the field multiplication is not familiar to readers with a typical theoretical-physics background, we now discuss it in some detail.

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

$$
N = 27: \quad (a_0, a_1, a_2) \odot (b_0, b_1, b_2) = a \odot b = c = (c_0, c_1, c_2)
$$
$$
\text{with} \quad c_0 = a_0 b_0 + a_1 b_2 + a_2 b_1 - a_2 b_2 \pmod 3,
$$
$$
c_1 = a_0 b_1 + a_1 b_0 - a_1 b_2 - a_2 b_1 - a_2 b_2 \pmod 3,
$$
$$
c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 - a_1 b_2 - a_2 b_1 \pmod 3,
$$

$$(2.7)$$

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

$$
p^j \odot p^k = (M_0^{(j+k)}, M_1^{(j+k)}, \ldots, M_{\mathrm{M}-1}^{(j+k)}),
\tag{2.8}
$$

we have

$$
M_m^{(j+k)} = \delta_{j+k,m} \quad \text{for } j + k = 0, 1, \ldots, \mathrm{M} - 1, \quad \text{and} \quad M_m^{(\mathrm{M})} = \mu_m,
\tag{2.9}
$$

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

$$
M_m^{(j+k)} = (1 - \delta_{m,0}) M_{m-1}^{(j+k-1)} + \mu_m M_{\mathrm{M}-1}^{(j+k-1)} \pmod p,
\tag{2.10}
$$

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

$$
a \odot b = \left(a\mathcal{M}_0 b^T, a\mathcal{M}_1 b^T, \ldots, a\mathcal{M}_{\mathrm{M}-1} b^T \right),
\tag{2.11}
$$

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

$$
\mathcal{M}_m =
\begin{pmatrix}
M_m^{(0)} & M_m^{(1)} & M_m^{(2)} & \cdots & \cdots & & \\
M_m^{(1)} & M_m^{(2)} & & & & & \\
M_m^{(2)} & & & & & & \vdots \\
\vdots & & & \ddots & & & \vdots \\
\vdots & & & & & & M_m^{(2\mathrm{M}-4)} \\
& & & & & M_m^{(2\mathrm{M}-4)} & M_m^{(2\mathrm{M}-3)} \\
& \cdots & \cdots & M_m^{(2\mathrm{M}-4)} & M_m^{(2\mathrm{M}-3)} & M_m^{(2\mathrm{M}-2)}
\end{pmatrix},
\tag{2.12}
$$

---

[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.

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 $\times$ matrix $\times$ 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

$$\mathcal{M}_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix}, \quad \mathcal{M}_1 = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix}, \quad \mathcal{M}_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \quad (2.13)$$

and

$$\mathcal{M}_0^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{M}_1^{-1} = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}, \quad \mathcal{M}_2^{-1} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad (2.14)$$

for the $N = 27$ example in (2.7).

Having thus established how the field addition $a \oplus b$ and the field multiplication $a \odot b$ are implemented for any two field elements $a, b = 0, 1, \ldots, N-1$ with $N = p^{\mathrm{M}}$, we can put the Galois field to use. For notational simplicity, let us denote by γ the basic pth root of unity,

$$\gamma = \mathrm{e}^{\mathrm{i}2\pi/p}, \quad (2.15)$$

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 take on only p different values, which are completely determined by the first component g_0 of the p-ary expansion of g,

$$\gamma^g = \gamma^{g_0} \quad \text{for } g = \sum_{m=0}^{\mathrm{M}-1} g_m p^m, \quad (2.16)$$

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:

$$\sum_{j=0}^{N-1} \gamma^{j\odot i} = N\delta_{i,0}. \quad (2.17)$$

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

$$i \ne 0 : \sum_{j=0}^{N-1} \gamma^{j\odot i} = \sum_{j'=0}^{N-1} \gamma^{j'} \quad (2.18)$$

because the field multiplication is invertible, and then

$$\sum_{j'=0}^{N-1} \gamma^{j'} = p^{M-1} \sum_{j'_0=0}^{p-1} \gamma^{j'_0} = p^{M-1} \frac{(1-\gamma^p)}{(1-\gamma)} = 0, \tag{2.19}$$

where the first step exploits (2.16) and recognizes that there are p^{M-1} field elements j' with the same value of j'_0.

The fact that the field addition is the component-wise addition modulo p, combined with the rule (2.16), implies the following useful identity:

$$\gamma^i \gamma^j = \gamma^{i+j} = \gamma^{i_0+j_0} = \gamma^{(i\oplus j)_0} = \gamma^{i\oplus j}. \tag{2.20}$$

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 (2.17) and (2.18) as an integer, and so get integer powers of γ. Relation (2.20) expresses, in the language of mathematicians, that the pth roots of unity are additive characters of the Galois field.[33]

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 $p = 2$, M $= 2$, $N = p^M = 4$ 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 non-zero dividers of 0 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.

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	$\odot$	0	1	2	3
	0	0	1	2	3	0	0	0	0	0
	1	1	0	3	2	1	0	1	2	3
	2	2	3	0	1	2	0	2	3	1
	3	3	2	1	0	3	0	3	1	2
(b)	$\oplus_4$	0	1	2	3	$\odot_4$	0	1	2	3
	0	0	1	2	3	0	0	0	0	0
	1	1	2	3	0	1	0	1	2	3
	2	2	3	0	1	2	0	2	0	2
	3	3	0	1	2	3	0	3	2	1

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

$$
\begin{aligned}
|i\rangle_4 = |i_0\rangle_2 \otimes |i_1\rangle_2 : |0\rangle_4 &= |0\rangle_2 \otimes |0\rangle_2, \\
|1\rangle_4 &= |1\rangle_2 \otimes |0\rangle_2, \\
|2\rangle_4 &= |0\rangle_2 \otimes |1\rangle_2, \\
|3\rangle_4 &= |1\rangle_2 \otimes |1\rangle_2.
\end{aligned}
\tag{2.21}
$$

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

$$
|i \oplus j\rangle_4 = |i_0 \oplus_2 j_0\rangle_2 \otimes |i_1 \oplus_2 j_1\rangle_2 \quad \text{for } i = (i_0, i_1) \quad \text{and} \quad j = (j_0, j_1). \tag{2.22}
$$

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

It is also worth reminding that the properties

$$
\gamma_N^i \gamma_N^j = \gamma_N^{i \oplus_N j} \quad \text{and} \quad \sum_{p=0}^{N-1} \gamma_N^{p \odot_N q} = N \delta_{q,0} \tag{2.23}
$$

with $\gamma_N = e^{i2\pi/N}$ 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 (2.20) and (2.17). In prime dimensions ($\text{M} = 1$, $N = p^1 = p$) 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 $N = p^{\text{M}}$ — 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

$$
(|i\rangle, |j\rangle) = (\langle i|, \langle j|) = \langle i \,|\, j \rangle = \delta_{i,j} \tag{2.24}
$$

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,

$$
|i\rangle \rightarrow V_l^0 |i\rangle = |i \oplus l\rangle, \tag{2.25}
$$

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 (2.25) 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 ($N = p^{\text{M}}$, $\text{M} > 1$) 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. 34, we employ a suitable discrete Fourier-type transformation — the inverse *Galois−Fourier* transformation — to define the dual basis as follows:

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \gamma^{\ominus k \odot j} \tag{2.26}$$

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

$$
\begin{aligned}
V_l^0 |\tilde{j}\rangle &= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k \oplus l\rangle \gamma^{\ominus k \odot j} \\
&= \frac{1}{\sqrt{N}} \sum_{k'=0}^{N-1} |k'\rangle \gamma^{\ominus (k' \ominus l) \odot j} = |\tilde{j}\rangle \gamma^{l \odot j},
\end{aligned}
\tag{2.27}
$$

which identifies the eigenvalues $\gamma^{l \odot j}$. These are p different eigenvalues, each occurring $p^{\text{M}-1}$ times.

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

$$|\langle \tilde{j}|k\rangle|^2 = \left| \frac{1}{\sqrt{N}} \gamma^{j \odot k} \right|^2 = \frac{1}{N} \quad \text{for all } j, k = 0, 1, \ldots, N-1. \tag{2.28}$$

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, the Galois−Fourier transform is a real Hadamard transform.[34]

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 $\ominus l$,

$$|\tilde{i}\rangle \to V_0^l |\tilde{i}\rangle = |\widetilde{i \ominus l}\rangle, \quad \langle \tilde{i}| \to \langle \tilde{i}|V_0^l = \langle \widetilde{i \oplus l}|, \tag{2.29}$$

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 (2.25), 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,

$$V_0^l = \sum_{k=0}^{N-1} |\tilde{k}\rangle \langle \widetilde{k \oplus l}| = \sum_{k=0}^{N-1} |k\rangle \gamma^{k \odot l} \langle k|. \tag{2.30}$$

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

$$V_l^0 = \sum_{k=0}^{N-1} |k \oplus l\rangle\langle k| = \sum_{k=0}^{N-1} |\widetilde{k}\rangle \gamma^{k \odot l}\langle\widetilde{k}|, \tag{2.31}$$

which is equivalent to (2.27) 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 $\mathrm{M} > 1$ 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 $\langle\,\widehat{i}\,|$ 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 (2.21) and (2.22) for $p = 2$ and $\mathrm{M} = 2$. More generally,

$$\begin{aligned}
V_l^0|k\rangle &= V_l^0(|k_0\rangle \otimes |k_1\rangle \otimes \cdots \otimes |k_{\mathrm{M}-1}\rangle) \\
&= |k_0 + l_0\rangle \otimes |k_1 + l_1\rangle \otimes \cdots \otimes |k_{\mathrm{M}-1} + l_{\mathrm{M}-1}\rangle,
\end{aligned} \tag{2.32}$$

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,

$$V_l^0 = (V_1^0)^{l_0}(V_p^0)^{l_1}(V_{p^2}^0)^{l_2}\cdots = \prod_{m=0}^{\mathrm{M}-1}(V_{p^m}^0)^{l_m}, \tag{2.33}$$

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 (2.26) factorizes,

$$\begin{aligned}
\langle\tilde{k}| &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\gamma^{k \odot j}\langle j| = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\gamma^{k\mathcal{M}_0 j^T}\langle j_0| \otimes \langle j_1| \otimes \langle j_2| \otimes \cdots \otimes \langle j_{\mathrm{M}-1}| \\
&= \frac{1}{\sqrt{p}}\sum_{j_0=0}^{p-1}\gamma^{(k\mathcal{M}_0)_0 j_0}\langle j_0| \otimes \frac{1}{\sqrt{p}}\sum_{j_1=0}^{p-1}\gamma^{(k\mathcal{M}_0)_1 j_1}\langle j_1| \otimes \cdots \\
&= \langle\widetilde{\underline{k}_0}| \otimes \langle\widetilde{\underline{k}_1}| \otimes \cdots \otimes \langle\widetilde{\underline{k}_{\mathrm{M}-1}}|,
\end{aligned} \tag{2.34}$$

where $\mathcal{M}_0$ is the 0th multiplication matrix in (2.11) 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 $\underline{k}_m$,

$$k = (\underline{k}_0, \underline{k}_1, \ldots)\mathcal{M}_0^{-1} = (\underline{k}_0, \underline{k}_1, \ldots)\begin{pmatrix} g_0 \\ g_1 \\ \vdots \\ g_{\mathrm{M}-1} \end{pmatrix} = \sum_{m=0}^{\mathrm{M}-1}\underline{k}_m g_m, \tag{2.35}$$

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

$$\gamma^{p^m \odot g_n} = \gamma^{\delta_{m,n}} = \begin{cases} \gamma & \text{if } m = n, \\ 1 & \text{if } m \neq n. \end{cases} \tag{2.36}$$

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 $\langle \tilde{j}_m |$ only and leaving the other $\mathrm{M} - 1$ q-pit bras in the products of (2.34) unaffected,

$$V_0^l = (V_0^{g_0})^{\underline{l}_0} (V_0^{g_1})^{\underline{l}_1} (V_0^{g_2})^{\underline{l}_2} \cdots = \prod_{m=0}^{\mathrm{M}-1} (V_0^{g_m})^{\underline{l}_m}, \tag{2.37}$$

with the mth factor affecting the mth q-pit only,

$$(V_0^{g_m})^{\underline{l}_m} |k_m\rangle = |k_m\rangle \gamma^{k_m \underline{l}_m}. \tag{2.38}$$

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 (2.7), (2.13) and (2.14).

The respective unitary operator factors for unit shifts in (2.33) and (2.37) commute if they refer to different q-pits,

$$V_{p^m}^0 V_0^{g_n} = V_0^{g_n} V_{p^m}^0 \quad \text{if } m \neq n, \tag{2.39}$$

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

$$V_{p^m}^0 V_0^{g_m} = \gamma^{-1} V_0^{g_m} V_{p^m}^0. \tag{2.40}$$

Equations (2.39) and (2.40) are particular cases of (2.42) 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 (2.26). 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,

$$V_i^j = V_0^j V_i^0 = \sum_{k=0}^{N-1} |k \oplus i\rangle \gamma^{(k \oplus i) \odot j} \langle k| \quad \text{for } i, j = 0, 1, \ldots, N-1, \tag{2.41}$$

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 (2.30), and for $i = l$ and $j = 0$ we have the first sum of (2.31).

We note that the order of multiplication of V_0^j and V_j^0 matters in the definition (2.41) because these unitary shift operators do not commute,

$$V_i^0 V_0^j = \gamma^{\ominus i \odot j} V_0^j V_i^0. \tag{2.42}$$

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.[3,4]

In dimension $N = p = 2$, the commutation relation (2.42) 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[23]; recall the discussion in Sec. 1.1.6 with its emphasis on the Heisenberg−Weyl group.

Currently, 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 isomorphic 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 (2.33). 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 (2.34)−(2.36), the factorization is stated in (2.37).

The composition law of the N^2 unitary operators introduced in (2.41) is

$$\begin{aligned} V_i^j V_k^l &= V_0^j V_i^0 V_0^l V_k^0 \\ &= \gamma^{\ominus i \odot l} V_0^j V_0^l V_i^0 V_k^0 = \gamma^{\ominus i \odot l} V_{i \oplus k}^{j \oplus l}, \end{aligned} \tag{2.43}$$

which implies

$$V_k^{l-1} = V_k^{l\dagger} = \gamma^{\ominus k \odot l} V_{\ominus k}^{\ominus l} \tag{2.44}$$

and

$$V_k^l V_i^j V_k^{l\dagger} = \gamma^{l \odot i \ominus j \odot k} V_i^j \tag{2.45}$$

for example. Another implication is

$$\begin{aligned} (V_i^j)^p &= (\gamma^{\ominus i \odot j})^{1+2+\cdots+(p-1)} V_0^0 = (\gamma^{\ominus i \odot j})^{\frac{1}{2}p(p-1)} \mathbf{1} \\ &= \begin{cases} (-1)^{i \odot j} \mathbf{1} & \text{for } p = 2, \\ \mathbf{1} & \text{for } p = 3, 5, 7, 11, \ldots, \end{cases} \end{aligned} \tag{2.46}$$

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,

$$(V_i^j, V_k^l) = \mathrm{tr}\{V_i^{j\,\dagger} V_k^l\} = N \delta_{i,k} \delta_{j,l}, \tag{2.47}$$

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

$$\frac{1}{N^2} \sum_{m,n=0}^{N-1} V_m^n A V_m^{n\,\dagger} = \frac{1}{N} \mathrm{tr}\{A\} \mathbf{1}, \tag{2.48}$$

which one may regard as a manifestation of Schur's lemma, inasmuch as the right-hand side follows after observing that the sum on the left commutes with all V_j^i and must therefore be a multiple of the identity. Schwinger[5] calls such statements about equal-weight averages over the whole phase space *ergodic relations*.

Equation (2.43) is the discrete analog of the familiar Baker−Campbell−Hausdorff relation for exponentiated position and momentum operators that we encountered in (1.34). An immediate consequence of (2.43) is

$$V_i^j V_l^k = V_l^k V_i^j \quad \text{if } (i \odot k)_0 = (j \odot l)_0 \text{ and only then}, \tag{2.49}$$

where $(\ )_0$ has the same meaning as in (2.20). In particular, (2.49) 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, (2.43) looks like a group composition law. Indeed, one can show[35] 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. 36, 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 operators of Sec. 2.3, respectively,

$$U_l^N = V_0^l = \sum_{k=0}^{N-1} |k\rangle \gamma^{k \odot l} \langle k| = \sum_{k=0}^{N-1} |e_k^N\rangle \gamma^{k \odot l} \langle e_k^N|,$$
$$U_l^0 = V_l^0 = \sum_{k=0}^{N-1} |\tilde{k}\rangle \gamma^{k \odot l} \langle \tilde{k}| = \sum_{k=0}^{N-1} |e_k^0\rangle \gamma^{k \odot l} \langle e_k^0|, \tag{2.50}$$

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

$$U_l^i = \sum_{k=0}^{N-1} |e_k^i\rangle \gamma^{k \odot l} \langle e_k^i| \tag{2.51}$$

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

$$|\langle e_k^i | e_l^j \rangle|^2 = \delta_{i,j} \delta_{k,l} + \frac{1 - \delta_{i,j}}{N} = \begin{cases} \delta_{k,l} & \text{for } i = j \text{ (orthonormal)}, \\ 1/N & \text{for } i \neq j \text{ (mutually unbiased)}, \end{cases} \tag{2.52}$$

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 (2.51), the U_l^i are unitary and commute with each other for fixed i,

$$U_l^i U_{l'}^i = U_{l'}^i U_l^i = U_{l \oplus l'}^i, \tag{2.53}$$

which is an immediate consequence of distributivity and the identity (2.20). In view of (2.49), 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 (2.49) implies that V_l^k and $V_{l'}^{k'}$ commute.

We are thus invited to try the ansatz[j]

$$U_l^i = \alpha_l^i V_l^{i \odot l} \quad \text{for } i = 0, 1, \ldots, N-1, \tag{2.54}$$

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

$$\alpha_l^0 = 1 : U_l^0 = V_l^0 \quad \text{for } l = 0, 1, \ldots, N-1 \quad \text{and}$$
$$\alpha_0^i = 1 : U_0^i = V_0^0 \quad \text{for } i = 0, 1, \ldots, N-1, \tag{2.55}$$

---

[i] For $l \neq 0$, one naturally defines $k \oslash l$ by $(k \oslash l) \odot l = k$.
[j] For $N = p$ odd, we make contact with Sec. 1.1.6 for $U_l^i = (XZ^i)^l$, that is $\alpha_l^i = \gamma^{-il(l+1)/2}$.

and the said consistency with (2.53) requires

$$\alpha_k^i \alpha_l^i = \alpha_{k \oplus l}^i \gamma^{i \odot k \odot l}, \tag{2.56}$$

where (2.20) and (2.43) have been used repeatedly. We note that all U_l^is of (2.50) and (2.51) have period p, which tells us that the inclusion of α_l^i in (2.54) removes the even-odd distinction of (2.46).

The orthonormality relation (2.47) carries over to the U_l^is in the form

$$\mathrm{tr}\{U_k^{i\,\dagger} U_l^j\} = N \delta_{k,l} \delta_{i \odot k, j \odot l} = \begin{cases} N & \text{for } k = l = 0, \\ N \delta_{i,j} & \text{for } k = l \neq 0, \\ 0 & \text{for } k \neq l. \end{cases} \tag{2.57}$$

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

Any choice for the phase factors α_l^i that obeys (2.55) and (2.56) is permissible in (2.54), but these conditions do not determine the phase factors uniquely (except for $i = 0$). Just as (2.53) remains valid when we replace U_l^i by $\gamma^{b_i \odot l} U_l^i$ with an arbitrary field element b_i,[k] the replacement $\alpha_l^i \rightarrow \alpha_l^i \gamma^{b_i \odot l}$ has no effect in (2.55) and (2.56), and in (2.54) it amounts to a permutation of the states in the ith basis: $|e_k^i\rangle \rightarrow |e_{k \ominus b_i}^i\rangle$, but leaves the basis as a whole unchanged.[35] Indeed, irrespective of the particular choice made for the phase factors in (2.54), the set of common eigenkets $|e_k^i\rangle$ of the N unitary operators in the ith abelian subgroup must always be the same — a different phase convention can only result in a different labeling of the eigenkets.

It remains to be shown, though, that there *are* consistent choices for all phase factors. This task has been completed in Ref. 35, 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[l]

$$p \text{ odd}: \alpha_l^i = \gamma^{\ominus(i \odot l \odot l) \oslash 2} \tag{2.58}$$

is simplest and indeed possible. But in even prime-power dimensions $(p = 2)$, where $1 \oplus 1 = 0 \neq 2$, (2.58) 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

$$(\alpha_l^j)^p = \begin{cases} (-1)^{j \odot l \odot l} = 1 \text{ or } -1 & \text{for } p = 2, \\ 1 & \text{for } p > 2, \end{cases} \tag{2.59}$$

which combines with (2.46) 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 (2.58). For $p = 2$ this is not possible but, instead, we can systematically write α_l^j as a power

---

[k] Analogously, we could introduce a phase factor $e^{ib(\alpha,\beta)t}$ in (1.44) without affecting (1.45).

[l] Note that $l \odot l \oslash 2 = l(l + p)/2 \pmod{p}$ for $N = p$ odd.

of $i = \sqrt{-1} = e^{i\frac{\pi}{2}}$ because, in virtue of (2.59), 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 (2.58). As a consequence of the group property (2.56), for each j it is sufficient to fix M well chosen phases such that then the values of all the $N = 2^M$ phases are determined.

The M values of the signs of the phases α_l^j that we choose by convention are $\alpha_1^j, \alpha_2^j, \ldots, \alpha_{2^{M-1}}^j$ and we require, in agreement with (2.59), that they obey

$$p = 2 : \alpha_{2^n}^j = i^{j \odot 2^n \odot 2^n} \quad \text{or} \quad \alpha_{l_n 2^n}^j = i^{j \odot (l_n 2^n) \odot (l_n 2^n)}, \tag{2.60}$$

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

$$l = \sum_{n=0}^{M-1} l_n 2^n = \bigoplus_{n=0}^{M-1} l_n 2^n, \tag{2.61}$$

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

$$\prod_{n=0}^{M-1} \alpha_{l_n 2^n}^j = \prod_{n=0}^{M-1} i^{j \odot (l_n 2^n) \odot (l_n 2^n)} \tag{2.62}$$

as an immediate consequence of (2.60), and

$$\begin{aligned}
\prod_{n=0}^{M-1} \alpha_{l_n 2^n}^j &= (-1)^{j \odot l_0 \odot (l_1 2)} \alpha_{l_0 \oplus l_1 2}^j \prod_{n=2}^{M-1} \alpha_{l_n 2^n}^j \\
&= (-1)^{j \odot l_0 \odot (l_1 2)} (-1)^{j \odot (l_0 \oplus l_1 2) \odot (l_2 2^2)} \alpha_{l_0 \oplus l_1 2 \oplus l_2 2^2}^j \prod_{n=3}^{M-1} \alpha_{l_n 2^n}^j \\
&= \cdots \\
&= \alpha_l^j \prod_{m=0}^{M-2} \prod_{n=m+1}^{M-1} (-1)^{j \odot (l_m 2^m) \odot (l_n 2^n)}
\end{aligned} \tag{2.63}$$

or

$$\prod_{n=0}^{M-1} \alpha_{l_n 2^n}^j = \alpha_l^j \prod_{\substack{m,n=0 \\ m \neq n}}^{m-1} (-i)^{j \odot (l_m 2^m) \odot (l_n 2^n)} \tag{2.64}$$

by repeated application of (2.56). The $n = m$ terms missing in (2.64) make up the product in (2.62), so that we arrive at[m]

$$p = 2 : \alpha_l^j = \prod_{m,n=0}^{M-1} i^{j \odot (l_m 2^m) \odot (l_n 2^n)} \tag{2.65}$$

---

[m] Owing to an oversight that was pointed out by Eusebi and Mancini,[37] the expression given in Ref. 35 is incorrect, but this inadvertence is of no consequence because the general properties (2.55) and (2.56) matter, not the explicit convention chosen for the values of the α_l^js. The derivation (2.60)−(2.65) is essentially identical with the reasoning in Ref. 37.

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 (2.57), amounts to extra factors of $(-1)^{l_n}$ in (2.60) for some n values. Examples of evaluating the product in (2.65) can be found in Appendix D.

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

$$\alpha_l^i = \alpha_{\ominus l}^i \tag{2.66}$$

holds when N is even, because $l = \ominus l$ for $p = 2$. It is also true for odd N if the phases of (2.58) are chosen, but not for all permissible choices. If one imposes (2.66) as an additional condition, then

$$(\alpha_l^i)^2 = \alpha_l^i \alpha_{\ominus l}^i = \gamma^{\ominus i \odot l \odot l} \tag{2.67}$$

for all N and all $i = 0, 1, \dots, N-1$, and (2.58) and (2.65) show how the proper square root of the right-hand side can be defined. Unless explicitly stated, the symmetry (2.66) is not assumed for $p > 2$ in what follows, and neither are the explicit expressions (2.58) and (2.65) for the phase factors.

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

Having thus at our disposal the unitary operators U_l^i of (2.51) and (2.54), we can also state quite explicitly the $N - 1$ bases associated with the abelian subgroups for $i = 1, 2, \dots, N - 1$. For this purpose we exploit the analog of (1.12),

$$|e_k^i\rangle\langle e_k^i| = \frac{1}{N} \sum_{l=0}^{N-1} \gamma^{\ominus k \odot l} U_l^i, \tag{2.68}$$

which is an immediate consequence of (2.51) and (2.17), and from its implication

$$\langle e_l^N \,|\, e_k^i\rangle\langle e_k^i \,|\, e_m^N\rangle = \frac{1}{N} (\gamma^{k \odot l} \alpha_{\ominus l}^i)^* (\gamma^{k \odot m} \alpha_{\ominus m}^i) \tag{2.69}$$

we find

$$|e_k^i\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} |e_l^N\rangle \gamma^{\ominus k \odot l} \alpha_{\ominus l}^{i\,*}. \tag{2.70}$$

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,

$$V_m^n |e_0^i\rangle = |e_{i \odot m \ominus n}^i\rangle \alpha_m^{i\,*} \quad \text{for } i = 0, 1, \dots, N-1, \quad V_m^n |e_0^N\rangle = |e_m^N\rangle. \tag{2.71}$$

Statements (2.69), (2.70) and (2.71), as well as (2.74)−(2.77) below, are valid both for odd prime powers and even prime powers, whether the respective phase factors of (2.58) and (2.65) 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 (2.50) and (2.55).

Indeed, it is easy to establish the validity of the requirement (2.52) for the projectors in (2.68) by just exploiting (2.68) itself and without relying on (2.70):

$$|\langle e_k^i | e_l^j \rangle|^2 = \mathrm{tr}\{(|e_k^i\rangle\langle e_k^i|)\,(|e_l^j\rangle\langle e_l^j|)\} = \frac{1}{N^2} \sum_{m,n=0}^{N-1} \gamma^{k\odot m} \gamma^{\ominus l\odot n} \mathrm{tr}\{U_m^{i\,\dagger} U_n^j\}$$

$$= \frac{1}{N} \sum_{m,n=0}^{N-1} \gamma^{k\odot m\ominus l\odot n} \delta_{m,n} \delta_{i\odot m, j\odot n} = \frac{1}{N} \sum_{m=0}^{N-1} \gamma^{(k\ominus l)\odot m} \delta_{i\odot m, j\odot m}$$

$$= \frac{1}{N} + \delta_{i,j} \frac{1}{N} \sum_{m=1}^{N-1} \gamma^{(k\ominus l)\odot m} = \frac{1}{N} + \delta_{i,j}\left(\delta_{k,l} - \frac{1}{N}\right), \tag{2.72}$$

where the orthonormality relation (2.57) and the identity (2.17) are the main ingredients. The eigenvalue equations

$$U_l^i |e_k^i\rangle\langle e_k^i| = |e_k^i\rangle\langle e_k^i|\,U_l^i = |e_k^i\rangle \gamma^{k\odot l} \langle e_k^i| \tag{2.73}$$

also follow for (2.68) directly from (2.53).

But it cannot be a mistake to check, for consistency, that $|e_k^i\rangle$ as given in (2.70) is the eigenket of U_l^i of (2.54) to eigenvalue $\gamma^{k\odot l}$. Starting from

$$U_l^i |e_m^N\rangle = V_l^{i\odot l} |m\rangle \alpha_l^i = |m \oplus l\rangle \gamma^{i\odot(m\oplus l)\odot l} \alpha_l^i$$
$$= |m \oplus l\rangle \alpha_{\ominus(m\oplus l)}^{i\ *} \alpha_{\ominus m}^i \tag{2.74}$$

we have

$$U_l^i |e_k^i\rangle \gamma^{\ominus k\odot l} = \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} U_l^i |e_m^N\rangle \gamma^{\ominus(m\oplus l)\odot k} \alpha_{\ominus m}^{i\ *}$$
$$= \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |m \oplus l\rangle \alpha_{\ominus(m\oplus l)}^{i\ *} \gamma^{\ominus(m\oplus l)\odot k} = |e_k^i\rangle, \tag{2.75}$$

indeed.

For later reference, we further observe that

$$\mathrm{tr}\{U_l^{i\,\dagger} V_m^n\} = N\delta_{i\odot l, n}\,\delta_{l,m}\,\alpha_l^{i\ *}, \tag{2.76}$$

which follows from (2.54) and (2.47) and in turn implies

$$\langle e_k^i | V_m^n | e_k^i \rangle = \delta_{i\odot m, n}\,\gamma^{k\odot m} \alpha_m^{i\ *}, \tag{2.77}$$

upon invoking the adjoint version of (2.68). 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

$$C_i = \sum_{k=0}^{N-1} |e_k^i\rangle\langle e_k^N|. \tag{2.78}$$

This includes $C_N = \mathbf{1}$. The terminology "Clifford operators" refers to the Clifford group,[38] 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 (2.57).

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

$$Z_i = \sum_{k=0}^{N-1} |e_k^i\rangle \gamma_N^k \langle e_k^i| = \frac{1}{N} \sum_{k,l=0}^{N-1} \gamma_N^k \gamma^{\ominus k \odot l} U_l^i. \tag{2.79}$$

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 the elements of an orthonormal basis of generalized Bell states and the Heisenberg−Weyl group of unitary transformations.[20,34,39] 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), quantum cloning (Sec. 3.4), and entanglement swapping (Sec. 3.5).

The construction that we use here employs the Heisenberg−Weyl group of Sec. 2 whose shift operators (2.41) change state labels via field addition.[34,39] 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.[20] With the necessary changes, all applications in Secs. 3.2−3.5 can be implemented by these other Bell states.[40]

3.1. *Generalized Bell states*

Following Refs. 34, 39, and 41, 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,[n]

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

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

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

as well as

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

and

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

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

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

as well as

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

and

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

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 $|B_{0,0}\rangle$,

$$\mathbf{1} = \sum_k |k\rangle\langle k| = \sum_k |e_k^i\rangle\langle e_k^i| \leftrightarrow \sum_k |k^*, k\rangle = \sum_k |e_k^{i*}, e_k^i\rangle = |B_{0,0}\rangle\sqrt{N}, \tag{3.10}$$

here illustrated for the computational basis and either one of the bases of (2.70). The factor $\sqrt{N}$ normalizes $|B_{0,0}\rangle$ to unit length, consistent with (3.3) and $\text{tr}\{\mathbf{1}\} = N$. 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. Refs. 42−44.

While $|B_{0,0}\rangle$ is basis independent in the sense of (3.10) for a given implementation of the conjugation $|\psi\rangle \to |\psi^*\rangle$, one should realize that different definitions of this map do result in different forms of $|B_{0,0}\rangle$ as expressed in the original bases. As an example, consider the case $N = 2$ of a single q-bit, and the following four alternative ways, four

---

[n] 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.

of many, of defining the map $|\psi\rangle \rightarrow |\psi^*\rangle$:

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

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

$$|B_{0,0}\rangle = \frac{1}{\sqrt{2}}(|0^*,0\rangle + |1^*,1\rangle) = \begin{cases} \dfrac{1}{\sqrt{2}}(|0,0\rangle + |1,1\rangle), \\[2mm] \dfrac{1}{\sqrt{2}}(|0,0\rangle - |1,1\rangle), \\[2mm] \dfrac{1}{\sqrt{2}}(|0,1\rangle + |1,0\rangle), \\[2mm] \dfrac{1}{\sqrt{2}}(|0,1\rangle - |1,0\rangle), \end{cases} \qquad (3.12)$$

are the familiar standard Bell states.[45] 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 $N^{-1/2}V_0^0 \leftrightarrow |B_{0,0}\rangle$, 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,

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

These make up the set of *generalized Bell states*. Their orthonormality follows from (3.3) and (2.47),

$$\langle B_{m,n} \mid B_{m',n'}\rangle = \frac{1}{N}\operatorname{tr}\{V_m^{n\dagger}V_{m'}^{n'}\} = \delta_{m,m'}\delta_{n,n'}, \qquad (3.14)$$

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

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

where (2.43) enters. In particular, we have

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

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 (2.48) 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 $|B_{m,n}\rangle \leftrightarrow N^{-1/2}V_m^n$ 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 techniques that we present in Sec. 4.2 below.

The Bell states in (3.16) refer explicitly to the computational basis because (2.41) expresses V_m^n in terms of the $|k \oplus m\rangle\langle k| = |e_{k\oplus m}^N\rangle\langle e_k^N|$ ket-bra products. We get the Bell states relative to the ith basis by applying the Clifford operator C_i of (2.78) 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

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

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

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

Upon employing (2.70) to express $C_i V_m^n C_i^\dagger$ in terms of the computational basis,

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

the trace is readily evaluated, and we find

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

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

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

where the mappings of the indices,

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

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 basis 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[46] to an arbitrary dimension N is an immediate application of (3.16). It goes as follows.[40] 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.

Despite this "manner of speaking," quantum dense coding does not violate the *Holevo bound*,[47,48] which states that a single q-nit can only transmit one c-nit, because of the earlier distribution of q-nit 1 to Alice that is entangled with Bob's q-nit 2 from the beginning. At the time when Alice carries out the measurement that discriminates the Bell states, she has received both q-nits.

3.3. *Quantum teleportation*

The relation between maximal sets of orthogonal families of unitary matrices and teleportation was already emphasized several years ago.[49] Several generalizations of

the teleportation scheme to arbitrary dimension that were proposed in the past[40,50,51] are close in spirit to the generalization that we proceed to describe now.

A central ingredient of the q-nit teleportation process is the three−q-nit−states identity

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

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,[42,43,52−54] although MUB are not really needed in arbitrary dimensions.[44] For instance, the celebrated BB84 protocol[52] 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,[34,55−58] 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,[59−62] for instance, when attacking the BB84 protocol.

The symmetry properties of the Bell states have important implications in the theory of cloning machines,[34,58] as we shall sketch briefly now. Under very general conditions,[41] optimal cloning states obey Cerf's ansatz,[55−57]

$$
|\Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} |B_{m,n}, B_{\ominus m, \ominus n}\rangle \gamma^{\ominus m \odot n} a_{m,n}
$$

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

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. Except for the normalization constraint,

$$
\langle \Psi_{0-3} \,|\, \Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} |a_{m,n}|^2 = 1, \tag{3.29}
$$

the probability amplitudes $a_{m,n}$ are arbitrary, their values specify the particular cloning state. In one standard scenario (see below), 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[44,52,58,62] and phase-covariant cloning,[59−61] 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

$$
|B_{m,n}^{(01)}, B_{\ominus m, \ominus n}^{(23)}\rangle = \frac{1}{N} \sum_{k,l=0}^{N-1} |k^*, k \oplus m, l^*, l \ominus m\rangle \gamma^{(k \oplus m) \odot n} \gamma^{\ominus (l \ominus m) \odot n}, \tag{3.30}
$$

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

$$
|B_{m,n}^{(03)}, B_{\ominus m, \ominus n}^{(21)}\rangle = \frac{1}{N} \sum_{k,l=0}^{N-1} |k^*, l \ominus m, l^*, k \oplus m\rangle \gamma^{(k \oplus m) \odot n} \gamma^{\ominus (l \ominus m) \odot n}. \tag{3.31}
$$

In fact, the states of (3.30) span the same N^2-dimensional subspace as the states of (3.31) in the N^4-dimensional four−q-nit Hilbert space.

To justify this remark, we evaluate the transition amplitudes,

$$
\langle B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'} \,|\, B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle
$$

$$
= \frac{1}{N^2} \sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\oplus m)\odot n \ominus (l\ominus m)\odot n \ominus (k'\oplus m')\odot n' \oplus (l'\ominus m')\odot n'}
$$

$$
\times \langle k'^*, l'\ominus m', l'^*, k'\oplus m' \,|\, k^*, k\oplus m, l^*, l\ominus m\rangle
$$

$$
= \frac{1}{N^2} \sum_{k,k',l,l'=0}^{N-1} \gamma^{(k\ominus l\oplus m\oplus m')\odot n}\gamma^{\ominus(k'\ominus l'\oplus m'\oplus m)\odot n'}\gamma^{(m\ominus m')\odot(n\oplus n')}
$$

$$
\times\, \delta_{k',k}\delta_{k'\oplus m',l\ominus m}\delta_{l',l}\delta_{l'\ominus m',k\oplus m}, \tag{3.32}
$$

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

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

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

$$
|B^{(01)}_{m,n}, B^{(23)}_{\ominus m,\ominus n}\rangle = \frac{1}{N}\sum_{m',n'=0}^{N-1} |B^{(03)}_{m',n'}, B^{(21)}_{\ominus m',\ominus n'}\rangle\gamma^{(m\ominus m')\odot(n\oplus n')}. \tag{3.34}
$$

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

$$
|B_{0,0}, B_{0,0}\rangle = |B^{(01)}_{0,0}, B^{(23)}_{0,0}\rangle = \frac{1}{N}\sum_{m,n=0}^{N-1} (\mathbf{1}\otimes V^n_m \otimes \mathbf{1}\otimes V^{n\,\dagger}_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle, \tag{3.35}
$$

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

$$
|\Psi_{0-3}\rangle = \sum_{m,n=0}^{N-1} (\mathbf{1}\otimes V^{n\,\dagger}_m \otimes \mathbf{1}\otimes V^n_m)|B^{(03)}_{0,0}, B^{(21)}_{0,0}\rangle b_{m,n}, \tag{3.36}
$$

where the probability amplitudes $b_{m,n}$ are the double Galois−Fourier transforms of the $a_{m,n}$s,

$$
b_{m,n} = \frac{1}{N}\sum_{m',n'=0}^{N-1} \gamma^{m\odot n'\ominus n\odot m'} a_{m',n'}. \tag{3.37}
$$

The stage is now set for a discussion of cloning. We consider two standard scenarios. In the first scenario, Alice and Bob believe that they share the Bell state described by ket $|B^{(01)}_{0,0}\rangle$, but in fact eavesdropper Eve controls the two−q-nit source and has replaced $|B^{(01)}_{0,0}\rangle$ by $|\Psi_{0-3}\rangle$. Alice measures her q-nit 0 and finds it in the state described by the bra $\langle\psi^*|$, so that the state of Bob's q-nit 1 would be described by ket

$|\psi\rangle$, but the ket for the resulting state of q-nits $1-3$ is actually given by

$$
\begin{aligned}
|\Psi_{1-3}\rangle &= \sum_{m,n=0}^{N-1} (V_m^n \otimes \mathbf{1} \otimes V_m^{n\,\dagger})|\psi, B_{0,0}^{(23)}\rangle a_{m,n} \\
&= \sum_{m,n=0}^{N-1} (V_m^{n\,\dagger} \otimes \mathbf{1} \otimes V_m^n)|B_{0,0}^{(21)}, \psi\rangle b_{m,n}.
\end{aligned} \tag{3.38}
$$

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

$$
\rho_1 = \mathrm{tr}_{2\&3}\{|\Psi_{1-3}\rangle\langle\Psi_{1-3}|\} = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle |a_{m,n}|^2 \langle\psi_{m,n}| \tag{3.39}
$$

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

$$
\rho_3 = \mathrm{tr}_{1\&2}\{|\Psi_{1-3}\rangle\langle\Psi_{1-3}|\} = \sum_{m,n=0}^{N-1} |\psi_{m,n}\rangle |b_{m,n}|^2 \langle\psi_{m,n}|. \tag{3.40}
$$

The displacement operators V_m^n appear as error operators in (3.39) and (3.40).

There are two extreme complementary situations: if $a_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $|b_{m,n}|^2 = 1/N^2$, 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 (2.48); but if $b_{m,n} = \delta_{m,0}\delta_{n,0}$ and thus $|a_{m,n}|^2 = 1/N^2$, 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 (3.37), 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 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.[63] For obvious reasons, this property is sometimes referred to as the "monogamy of quantum entanglement."

The second scenario is that of BB84-type[52] schemes for quantum cryptography: Alice prepares q-nit 1 in the state described by ket $|\psi\rangle$ and sends it to Bob. Eve gets hold of the q-nit in transmission, combines it with her q-nits 2 and 3 that she had earlier prepared in the "00" Bell state, and realizes a unitary transformation that

effects

$$|k, B_{0,0}^{(23)}\rangle \rightarrow \sum_{m,n=0}^{N-1} (V_m^n \otimes \mathbf{1} \otimes V_m^{n\,\dagger})|k, B_{0,0}^{(23)}\rangle a_{m,n}$$

$$= \sum_{m,n=0}^{N-1} |k \oplus m, B_{\ominus m, \ominus n}^{(23)}\rangle \gamma^{k \odot n} a_{m,n} \qquad (3.41)$$

for all kets $|k\rangle$ of q-nit 1, so that $|\psi, B_{0,0}^{(23)}\rangle$ is turned into the ket of (3.38),

$$|\psi, B_{0,0}^{(23)}\rangle \rightarrow |\Psi_{1-3}\rangle. \qquad (3.42)$$

Then q-nit 1, the first clone, is forwarded to Bob and Eve keeps the second clone and the anticlone.

The unitary property of the map (3.41) is confirmed by

$$\delta_{k,k'} = \langle k, B_{0,0}^{(23)}|k', B_{0,0}^{(23)}\rangle$$

$$\rightarrow \sum_{m,n}^{N-1} \sum_{m',n'}^{N-1} a_{m,n}{}^* \gamma^{\ominus k \odot n} \delta_{k \oplus m, k' \oplus m'} \delta_{m,m'} \delta_{n,n'} \gamma^{k' \odot n'} a_{m',n'}$$

$$= \delta_{k,k'}. \qquad (3.43)$$

Accordingly, Eve can — in principle, at least, if not in practice — implement (3.41) by a suitable interaction between q-nits 1 and 3.

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.[64−67] For instance, the Shor code for q-bits (see, e.g. Ref. 66) 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 (2.41), constitute an operator basis, especially in the many−q-bit case ($N = 2^{\mathrm{M}}$).

3.5. *Entanglement swapping*

A system of four q-nits, prepared in the state described by one of the kets $|B_{m,n}^{(01)}, B_{\ominus m, \ominus n}^{(23)}\rangle$ of (3.34), has the q-nit pairs (01) and (23) in maximally entangled states while there is no entanglement between the two pairs. If one then performs a Bell basis measurement on the pair (12) and finds it in the Bell state $|B_{\ominus m', \ominus n'}^{(21)}\rangle$, the state of the pair (03) is reduced to the Bell state $|B_{m',n'}^{(03)}\rangle$. In a manner of speaking, half of the original entanglement between the pairs (01) and (23) is used up in the Bell measurement on the pair (12) and the other half is transferred to the pair (03) which emerges maximally entangled.

At the time when the pair (12) is measured, q-nits 0 and 3 can be far away, possibly at space-like separations from each other and from pair (12), and q-nits 0

and 3 may never have been close to each other in the past. What matters is that their partners, q-nits 1 and 2, with which they share the maximally entangled initial Bell states, are brought into contact during the Bell-basis measurement on the pair (12). As soon as the outcome of the measurement on pair (12) is communicated (through a classical channel) to the experimenters in possession of q-nits 0 and 3, they can exploit the entanglement in the resulting Bell state $|B_{m',n'}^{(03)}\rangle$.

This *entanglement swapping*[68] has been demonstrated for q-bits carried by photons in different experiments; see Refs. 69 and 70, for example. In conjunction with quantum repeaters, entanglement swapping offers a practical way of creating strong entanglement between q-nits that are far apart.[71]

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,[72] which deals with the $N = 2$ case. Generalizations first to $N = 3$,[73] then to N prime,[9] and finally to prime-power values of N,[74,75] were completed some 15 years later. For further generalizations see Refs. 76 and 77. In the simplest case ($N = 2$), the problem can be presented as in Ref. 9:

> The Mean King challenges a physicist, Alice, who got stranded on the remote island ruled by the king, to prepare a spin-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 rise 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

$$|(m,n)\rangle = (V_m^{n*} \otimes V_m^n)|(0,0)\rangle \quad \text{for } m,n = 0,1,\ldots,N-1$$

with the "seed" $\quad |(0,0)\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N} |e_0^{i*}, e_0^i\rangle - |B_{0,0}\rangle.$ (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

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

As shown in Ref. 75, this solution is a special case of Aravind's very general solution,[74] 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,[78,79] 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. A finer notion of equivalence which takes entanglement properties into account, is possible in composite dimensions. In this finer sense there are inequivalent MUB for $N = 8$ and $N = 16$.[80,81,156]

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,

$$|(m,n)\rangle = \frac{1}{\sqrt{N}} \left(|e_m^{N*}, e_m^N\rangle + \sum_{i=0}^{N-1} |e_{i\odot m\ominus n}^{i*}, e_{i\odot m\ominus n}^i\rangle \right) - |B_{0,0}\rangle,$$ (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 (2.52), the invariance property (3.17), and $\langle e_k^{i*}, e_k^i | B_{0,0}\rangle = N^{-1/2}$, we then establish

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

and

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

from which follows the orthonormality

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

$$
|e_k^{i*}, e_k^i\rangle = \begin{cases} \dfrac{1}{\sqrt{N}} \displaystyle\sum_{m=0}^{N-1} |(m, i \odot m \ominus k)\rangle & \text{for } i = 0, 1, \ldots, N-1, \\[2ex] \dfrac{1}{\sqrt{N}} \displaystyle\sum_{n=0}^{N-1} |(k, n)\rangle & \text{for } i = N. \end{cases} \tag{4.7}
$$

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 $N = 4$ as they result from the multiplication and addition tables in Table 1(a).

In Aravind's construction,[74] the combinatorial properties offered by an affine plane of order N (properly defined in Sec. 4.3 below) are a crucial ingredient. 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),

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

are linearly independent, but they are not pairwise orthogonal. Rather they are the edges of an acute N^2-dimensional pyramid, with angle $\arccos((N + 2)/(2N + 2))$ 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.[82,83]

```
                        3 3 3 3
                        2 2 2 2
                        1 1 1 1
                        0 0 0 0
      0 1 2 3                       3 2 1 0
      0 1 2 3                       2 3 0 1
      0 1 2 3                       1 0 3 2
      0 1 2 3                       0 1 2 3


        3 0 2 1           3 1 0 2
        2 1 3 0           2 0 1 3
        1 2 0 3           1 3 2 0
        0 3 1 2           0 2 3 1
```

Fig. 1. The Mean King's 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 $i = 2$.

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)[o] 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 $|x\rangle$,

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

---

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

which is valid for any single$-$q-nit operator X. This identity is the completeness relation for the operator 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: $\mathrm{tr}\{A_j^\dagger A_k\} = \delta_{j,k}$. 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[3,4] 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.[84,85]

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

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

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

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

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

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

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 (2.50) and (2.54). The two expansions (4.13) and (4.15) are really the same expansion twice, differing solely by 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 $\langle e^i_k|\rho|e^i_k\rangle$,[p] from which the expansion coefficients

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

can then be computed, as follows from (2.51). With $X \to \rho$, $\mathrm{tr}\{X\} \to 1$, $\bar{x}^{\,i}_l \to \bar{r}^{\,i}_l$ in (4.16), the statistical operator ρ is parameterized in terms of the unitary Weyl basis U^i_l and the measured coefficients $\bar{r}^{\,i}_l$.

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 $\bar{r}^{\,i}_0 = 1$ 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. 87: 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 economical, 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.[88] This is a different story, however, which does not need the structure of an underlying Galois field, a ring structure suffices; see Refs. 89 and 19 for further information. The recent comprehensive account by Scott and Grassl[90] is recommended reading.

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

At the end of Sec. 2.3 — recall (2.32) and (2.33) — we observed that the unitary shift operators $V^n_m = V^n_0 V^0_m$ are products of M factors, one for each constituent q-pit,[q]

$$V^n_m = \prod_{j=0}^{\mathrm{M}-1} (V^{g_j}_0)^{\underline{n}_j} (V^0_{p^j})^{m_j} = \prod_{j=0}^{\mathrm{M}-1} V^{\underline{n}_j g_j}_{m_j p^j}, \tag{4.18}$$

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 (2.35). There are p^2 unitary shift operators $V^{\underline{n}_j g_j}_{m_j p^j}$ 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^n_m into the Weyl operator bases of the individual M q-pits that make up the q-nit.

---

[p] 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. 86.

[q] As in (2.35), read the product $\underline{n}_j g_j$ 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 $m_j p^j$, except that in this case there is no difference between the number product of m_j and p^j and the field product.

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.

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),[75]

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

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,

$$W_{m,n}^{\dagger} = W_{m,n}, \quad \mathrm{tr}\{W_{m,n}\} = 1, \quad \mathrm{tr}\{W_{m,n}W_{m',n'}\} = N\delta_{m,m'}\delta_{n,n'}, \qquad (4.20)$$

and their completeness relation is stated by

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

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.

Wigner functions for finite-dimensional systems have been defined in several different ways.[91−93] Here we choose to follow Wootters and his collaborators,[94−96] who regard an operator basis as an acceptable discrete analog of the continuous basis underlying Wigner's phase space function[84,85] 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.

$$(4.22)$$

The notions of "marginals" and "parallel lines" will be explained shortly. To the five criteria of (4.22) we add a sixth criterion:

(W6)   in the limit $N \to \infty$ the sequence of discrete bases converges
to the standard continuous Wigner basis. $\hspace{3cm}$ (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 (2.71) , that is:

$$W_{m,n} = V_m^n \, W_{0,0} V_m^{n\,\dagger} = V_{m\ominus m'}^{n\ominus n'} \, W_{m',n'} \, V_{m\ominus m'}^{n\ominus n'\,\dagger} \qquad (4.24)$$

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 given 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

$$M_{a,b,c} = \frac{1}{N} \sum_{m,n=0}^{N-1} W_{m,n} \delta_{a\odot m, b\odot n \oplus c} = \begin{cases} |e_{c\oslash b}^{a\oslash b}\rangle \langle e_{c\oslash b}^{a\oslash b}| & \text{if } b \neq 0, \\[2mm] |e_{c\oslash a}^{N}\rangle \langle e_{c\oslash a}^{N}| & \text{if } b = 0 \text{ and } a \neq 0, \end{cases} \qquad (4.25)$$

and the case $a = b = 0$, for which $M_{0,0,c} = \delta_{c,0}\mathbf{1}$, illustrates an ergodic property of the Wigner basis,

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

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

$$|e_k^i\rangle \langle e_k^i| = \begin{cases} M_{i,1,k} = \dfrac{1}{N} \sum_{m=0}^{N-1} W_{m,i\odot m \ominus k} & \text{for } i = 0, 1, 2, \ldots, N-1, \\[4mm] M_{1,0,k} = \dfrac{1}{N} \sum_{n=0}^{N-1} W_{k,n} & \text{for } i = N, \end{cases} \qquad (4.27)$$

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 $|e_k^i\rangle\langle e_k^i|$ 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 $|e_k^i\rangle\langle e_k^i|$,

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

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 vertices 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 vertices 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 vertices 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 (1.82) associates with the unit-trace hermitian matrices M. All the vertices 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's 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[97]: 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

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

In other words, the statistical operators $|e_k^i\rangle\langle e_k^i|$ belong to the polytope. So, the equation $0 \leq \operatorname{tr}\{W_{m,n}M\} \leq 1$ 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 $N = p^{\text{M}} \to \infty$ 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[r]

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

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,[98,99] where the factor of 2 ensures proper normalization to unit trace, $\operatorname{tr}\{P\} = 1$.

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 (2.54) and the $k = 0$ version of (2.68) 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

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

---

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

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 $(1/2)(1 \pm \sqrt{3})$, he was forced to resort to the dubious notion of "negative probabilities" which, in fact, gave this paper its title.[100] A direct measurement of the said expectation values, for the polarization q-bit of a photon, is reported in Ref. 101.

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 (2.43) and, *if* we choose the symmetric value of (2.58) 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 (2.66). With this symmetry in place, then, the seed is ($j \to 2 \odot k$)

$$W_{0,0} = \frac{1}{N} \sum_{i,k=0}^{N-1} V_k^0 V_0^i V_k^0 = \sum_{k=0}^{N-1} V_k^0 |0\rangle\langle 0| V_k^0$$

$$= \sum_{k=0}^{N-1} |k\rangle\langle \ominus k| = \sum_{k=0}^{N-1} |e_k^i\rangle\langle e_{\ominus k}^i|, \tag{4.40}$$

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 in virtue of property (W4). The limit $p \to \infty$, then, gives us the right-hand side of (4.33) as desired.[s]

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 (2.66) is imposed on the phase factors α_l^i of (2.54). 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.

---

[s]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

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

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 (2.57) and multiplies the right-hand side of (2.58) by $\gamma^{b_i \odot l}$ with $b_0 = 0$ and arbitrary field elements b_i for $i = 1, 2, \ldots, N-1$, then

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

replaces the $b_i \equiv 0$ version of (4.40). If one or more of the b_is are non-zero, $W_{0,0}^{(b)}$ 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.[t]

We thus observe that the symmetric choice of (2.58) is the right choice for obtaining a proper analog of the Wigner basis. It also endows the Wigner basis with certain elegant covariance properties[75] 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),[96] 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 (2.70) and specified unambiguously by the phase factors α_l^i that obey the constraints (2.55) and (2.56).

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.[95,96] 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

---

[t]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. 75, 92, 97 for details.

$k = m$, 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 of the uncertainty principle:[102] 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

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

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 onto 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,

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

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 $W_{m,n}$,

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

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 economical 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. 103 and 104, which implemented the scheme introduced in Ref. 105. The measurements, reported in Ref. 101, of the single−q-bit Wigner basis

(4.37) and a particular two−q-bit Wigner basis of product form, exploited an optical implementation of a one−q-bit SIC POVM that is optimal for single−q-bit tomography.[106]

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 non-zero probability of firing correspond to localization operators located on a straight line for which the marginal is the projector $|e_k^i\rangle\langle e_k^i|$.

4.2.4. *Covariance of the Wigner-type basis*

Upon projecting (4.3) onto the Bell basis we get

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

where α_m^i is the phase factor of (2.54), explicitly stated in (2.65) for N even and in (2.58) for N odd, provided the symmetry property (2.66) is imposed, as we assume throughout the present discussion. Then $\Gamma_m^{n\,2} = \gamma^{\ominus m \odot n}$, and we can regard the phase factors Γ_m^n 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},

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

In view of the symmetric choice (2.58), we can rewrite (3.21) for odd N in the form

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

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

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

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 (2.58). What about even prime power dimensions, $N = 2^M$? Here, the expression (2.65) 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 (2.65) 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 M > 2.[107,108] 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.[101]

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.

Actually, it is easy to show that the different phase choices compatible with (2.57) preserve the MUB as a whole but shift the labels of their basis states.[35] The covariance of the Heisenberg−Weyl group (4.48) as well as the transformation law (4.49) are guaranteed, in odd prime power dimensions, only for the symmetric phase-choice (2.58). This also concerns the phase point operators within the framework laid out by Gibbons *et al.*,[96] for which the bijection between MUB and Wigner operators (4.27) also holds by construction, independently of the choice of MUB and of the labeling of the MUB states. This result can be inferred in prime dimensions, for instance, from the study[109] of the properties of the Wigner operators that correspond to different quantum nets in Wootters's terminology, or to different phase-choices compatible with (2.57) in ours.

Another elegant feature that singles out the symmetric phase-choice (2.58) is that the corresponding Wigner function is well-behaved with regard to the composition law of Wigner operators, a property that was remarked upon by Gibbons *et al.* in Ref. 96, who noted that among all N^{N-1} possible choices of quantum nets, there

exists a particular net that exhibits "more than the required symmetry." This singled-out net corresponds to our symmetric phase choice in (2.58).

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[110]:

$$
\begin{aligned}
&\text{A1:} \quad \text{If } a_\alpha \text{ and } a_\beta \text{ are distinct points, there is a unique line } L_\omega \\
&\qquad \text{such that } a_\alpha \in L_\omega \text{ and } a_\beta \in L_\omega. \\
&\text{A2:} \quad \text{If } a_\alpha \text{ is a point not contained in the line } L_\omega, \text{ there is a unique} \\
&\qquad \text{line } L_\sigma \text{ such that } a_\alpha \in L_\sigma \text{ and } L_\sigma \cap L_\omega = \emptyset. \\
&\text{A3:} \quad \text{There are at least two points on each line, and there are at} \\
&\qquad \text{least two lines.}
\end{aligned}
\tag{4.50}
$$

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.[u] Examples for such arrays are the two addition tables in Table 1, but by no means all Latin squares arise in such an orderly manner.

To see how this works, consider $N = 3$. Pick two pencils of parallel lines, and label their lines with $0, 1, 2$ and $0', 1', 2'$. The nine points of the affine plane can then be arranged in an array with points on the lines of the first pencil making up the columns, and those of the second pencil making up the rows. The lines of the remaining two pencils of parallel lines are labeled by A, B, C and α, β, γ. Marking all points in the array that occur on line A with this letter, and so on for the other lines, will give rise to two Latin squares:

---

[u]Sudokus are 9×9 Latin squares of a restricted kind.

$$
\begin{array}{c|ccc}
 & 0 & 1 & 2 \\
\hline
0' & A & B & C \\
1' & B & C & A \\
2' & C & A & B
\end{array}
\qquad
\begin{array}{c|ccc}
 & 0 & 1 & 2 \\
\hline
0' & \alpha & \gamma & \beta \\
1' & \beta & \alpha & \gamma \\
2' & \gamma & \beta & \alpha
\end{array}
\tag{4.51}
$$

The squares must be Latin because the line labeled A, say, intersects each of the lines in the two pencils we started out with exactly once, and similarly for all other lettered lines. Now recall that the line labeled A intersects the line labeled α in a unique point. This explains why the two Latin squares we obtain must have the interesting property of being orthogonal Latin squares; another name for such a pair is a Graeco-Latin pair.[110] By definition this means that picking a pair of symbols, one Latin and one Greek — one from each of the two Latin squares — determines a unique point in the original array. To check that we did things right we simply superpose the two squares, and check that the pair of symbols $A\alpha$ occurs once and once only, and similarly for all other pairs. Incidentally, we see another interesting thing, namely that we could just as well have used the Latin letters to label the columns and the Greek letters to label the rows. The symbols we used in the first place will then distribute themselves into another Graeco-Latin pair:

$$
\begin{array}{c|ccc}
 & 0 & 1 & 2 \\
\hline
0' & A\alpha & B\gamma & C\beta \\
1' & B\beta & C\alpha & A\gamma \\
2' & C\gamma & A\beta & B\alpha
\end{array}
\qquad \leftrightarrow \qquad
\begin{array}{c|ccc}
 & A & B & C \\
\hline
\alpha & 00' & 22' & 11' \\
\beta & 12' & 01' & 20' \\
\gamma & 21' & 10' & 02'
\end{array}
\tag{4.52}
$$

Given the facts about finite affine planes that were recited above, it is clear that all of this works for every finite affine plane, and regardless of what pencils of parallel lines we pick. Setting two of the pencils aside to define the array, the remaining $N-1$ pencils always define $N-1$ mutually orthogonal Latin squares. This much is guaranteed by the intersection properties of the affine plane. Conversely, $N-1$ mutually orthogonal Latin squares will define an affine plane of order N.

But finite affine planes come with an existence problem of their own; indeed already Euler raised the question whether it is at all possibe to find a pair of orthogonal Latin squares when $N = 6$. He phrased it as a problem concerning 36 officers. More than a hundred years later it was proved that the answer is "no." This important result was reported in 1900 by the mathematician Tarry,[111] who proved by means of an exhaustive calculation that Euler's problem does not possess a solution, in agreement with Euler's conjecture. It follows that finite affine planes of order 6 do not exist. Progress since then has been slow. Finite affine planes do exist if $N = p^M$, 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 $N = p^M$, 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 emphasized 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 $N^2 + N$ vertices 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 vertices are vertices of the same facets, and two lines intersect in a point if the corresponding facets share a common vertex. It turns out[27] 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 vertices of the polytope correspond to one-dimensional projectors on Hilbert space. But when they do, it is possible to choose — following Wootters[94−96] — the special set of Wigner operators that we have discussed in Sec. 4.2.3, and to relate the construction to the partition of the Heisenberg−Weyl group that is associated with the MUB[36]: 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. It has been conjectured that such a relation exists,[112,113] but a recent attempt to use a pair of Graeco-Latin squares that does exist when $N = 10$ to construct a set of four MUB in this dimension failed.[114] It is interesting to notice that if N mutually orthogonal Latin squares exist, then there always exist $N + 1$ of them. Similarly, if N MUB exist, then there always exist $N + 1$ of them.[115]

In the 19th century, the combinatorial structures now known as finite geometries were studied more concretely by geometers, who realized them as configurations of lines and points, or more generally as configurations of subspaces of a complex projective space.[116] In 1844 Hesse, following earlier work by Plücker, studied a configuration of nine lines and 12 points in the projective plane, such that each line contains four points and each point lies on three lines.[117] 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 12 points are indeed the 12 kets that compose the four MUB of three kets each. His construction was generalized to the case of arbitrary prime N by Segre,[118] 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,[119] whose symmetry group consists of the Heisenberg−Weyl group together with an extra

reflection, an element of order 2. When N is an odd prime, 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[v]

$$[W_{0,0}]_{a,b} = \delta_{0,a\oplus b}. \qquad (4.53)$$

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 $N = 2n - 1$ is an odd prime. 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

$$(N^2_{N+1}, N(N+1)_N). \qquad (4.54)$$

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

$$\psi^{(0)} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \quad \psi^{(r)} = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ \gamma_N^{r1^2} \\ \gamma_N^{r2^2} \\ \vdots \\ \gamma_N^{r(N-2)^2} \\ \gamma_N^{r(N-1)^2} \end{pmatrix}, \quad 1 \leq r \leq N. \qquad (4.55)$$

By inspection we see that they span an n-dimensional subspace only, and indeed that they are all eigenvectors of $W_{0,0}$ with 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

---

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

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 $n = (1/2)(N+1)$-dimensional subspace to eigenvalue $+1$ and a $n-1 = (1/2)(N-1)$-dimensional subspace to eigenvalue -1.

In marked contrast, no similar construction is known for even N. In this case there is no parity operator available, a fact that also causes well-studied complications when one tries to define analogs of the Wigner function.[93]

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,

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

turns the basis kets into the unitary matrix, and

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

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

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

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,

$$U_1 \approx U_2 \Leftrightarrow U_2 = E_2 P_2 U_1 P_1 E_1. \tag{5.4}$$

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 non-negative. 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,

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

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

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

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.

Further examples include the Hadamard matrices $H_i^{(p)}$ for the prime-dimensional bases associated with the unitary operators XZ^i of (1.27) with $i = 0, 1, \ldots, p-1$. In accordance with (1.29), their matrix elements are

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

and their unique dephased forms

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

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

Our terminology is a bit unusual: in most of the literature a 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[120] constructed examples for all $N = 2^{\mathrm{M}}$, and Hadamard[121] proved that real Hadamard matrices do not exist unless $N = 2$ or $N = 4k$. It was conjectured by Paley[122] that they do exist in all cases not excluded by Hadamard. This conjecture has been verified for all $N \leq 664$.[123] 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 $4k$.[124] Another special class of Hadamard matrices are those of *Butson type*,[125] 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 an overview of the theory of Hadamard matrices and their many applications, consult Horadam's book.[126]

For our purposes a pair of MUB that can be transformed into each other by an overall unitary matrix will be regarded as equivalent. The problem of classifying all such unbiased bases was first raised by Kraus.[127] 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),

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

Haagerup[128] 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 unitary transformations 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

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

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

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

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.[28]

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 a 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

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

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*.[128,129] The first examples were in effect produced by Gauss. When N is odd they are

$$z_j^{(n,m)} = e^{\frac{2\pi i}{N}(mj^2+nj)} \tag{5.19}$$

where m, n are integers modulo N and the greatest common divisor of m and N equals 1. To prove that these sequences are biunimodular we must perform a Gauss sum, as discussed in Appendix C.

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, make up orthogonal columns.

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.[130] For an explicit example see (5.49) 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 basis and the Fourier basis 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: the three abelian subgroups composed of the powers of X, Z, and XZ of Sec. 1.1.6, for instance. When $N = p$ is prime, one known solution for a complete set of MUHM consists of $\mathbb{1}$, F, and $N - 1$ circulant matrices constructed from the biunimodular sequences (5.19) given by Gauss; see Appendix B.

It is natural to ask if there are other solutions. In fact this is a discrete version of the Pauli problem[131]: Given the modulus of a function and that of its Fourier transform, is the function uniquely determined? Björck and coworkers looked into this question,[129] 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's 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. This is true whenever N contains a square factor,[132] while the number of solutions is always finite for prime N.[133]

There are also MUHM 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 $N \le 5$*

For $N \le 5$ 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 $\gamma = e^{2\pi i/3}$ as usual.[128] When $N = 5$, all complex Hadamard matrices are again
equivalent to the Fourier matrix F_5.[128] 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,

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

Hadamard[121] himself proved that all $N = 4$ Hadamard matrices are equivalent to a
member of this family, for some value $0 \le a < \pi$ of the phase a. If $a = \pi/2$, 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 order in the angles:

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

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 of this linearized problem is called the *defect* of the matrix H. It can be explicitly determined by computing the rank of a certain matrix.[134] 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.[135] 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.[134] On the other hand, whenever $N = N_1 N_2$ is a composite number, one can produce continuous affine families from any choice of Hadamard matrices in dimensions N_1 and N_2.[128,136] If both N_1 and N_2 are prime, $N = p_1 p_2$, 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 $\mathbf{C}^{N_A N_B}$. 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 a 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 $N = N_A N_B$, 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. But the hunt for $N = 6$ Hadamard matrices is ongoing, and was brought to a sunny plateau recently by Karlsson.[137,138]

We begin by defining an H_2-*reducible* Hadamard matrix as a Hadamard matrix for which all its 2×2 submatrices are themselves Hadamard matrices. Karlsson proved the theorem that a 6×6 Hadamard matrix is H_2-reducible if and only if it contains a single 2×2 Hadamard submatrix. As a simple corollary, H_2-reducible Hadamard matrices are very easy to recognize: a 6×6 Hadamard matrix is H_2-reducible if and only if its dephased form contains a matrix element equal to -1.[137] With the sole exception of the Tao matrix,[139] all analytically known examples take this form. Moreover, the set of such Hadamard matrices belong to a three-parameter family that was explicitly constructed by Karlsson.[138]

Karlsson starts with the ansatz

$$
H = \left(
\begin{array}{cc|cc|cc}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & z_1 & -z_1 & z_2 & -z_2 \\
\hline
1 & z_3 & \bullet & \bullet & \bullet & \bullet \\
1 & -z_3 & \bullet & \bullet & \bullet & \bullet \\
\hline
1 & z_4 & \bullet & \bullet & \bullet & \bullet \\
1 & -z_4 & \bullet & \bullet & \bullet & \bullet
\end{array}
\right),
\tag{5.31}
$$

where the z_i are phase factors and the 2×2 blocks that have not been written out are guaranteed to be Hadamard matrices. We used the fact that four phase factors that add to zero form a rhombus in the complex plane, which is why they pair up in the way indicated. This ansatz is rewritten as

$$
H = \left(
\begin{array}{ccc}
F_2 & Z_1 & Z_2 \\
Z_3 & \dfrac{1}{2} Z_3 A Z_1 & \dfrac{1}{2} Z_3 B Z_2 \\
Z_4 & \dfrac{1}{2} Z_4 B Z_1 & \dfrac{1}{2} Z_4 A Z_2
\end{array}
\right).
\tag{5.32}
$$

This matrix will be unitary if and only if

$$A + B = F_2, \quad A - B = \sqrt{3} F_2 i \Lambda, \quad \Lambda^\dagger \Lambda = \mathbb{1}, \quad \Lambda^\dagger = \Lambda. \tag{5.33}$$

The unitary 2×2 matrix Λ, and *a fortiori* the matrices A and B, will therefore depend on two free parameters that parameterize a sphere — which can be thought of as the equator of the group $SU(2)$. We find

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{12}^* & -A_{11}^* \end{pmatrix} \tag{5.34}$$

with

$$A_{11} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}(x_1 + ix_2 + x_3), \quad A_{12} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}(x_1 - ix_2 - x_3) \tag{5.35}$$

and

$$B(x_1, x_2, x_3) = A(-x_1, -x_2, -x_3), \tag{5.36}$$

where the three real parameters (x_1, x_2, x_3) are constrained by

$$x_1^2 + x_2^2 + x_3^2 = 1. \tag{5.37}$$

Actually, another solution is $\Lambda = \pm \mathbb{1}$, but in the end this gives only Hadamard matrices that are equivalent to one of the above.

It remains to ensure that all matrix elements are unimodular. The conditions for this can be written in an elegant form using Möbius transformations that take the unit circle to the unit circle. Indeed

$$z_3^2 = \mathcal{M}_A(z_1^2) = \mathcal{M}_B(z_2^2), \quad z_4^2 = \mathcal{M}_A(z_2^2) = \mathcal{M}_B(z_1^2), \tag{5.38}$$

where

$$\mathcal{M}(z) = \frac{\alpha z - \beta}{\beta^* z - \alpha^*} \tag{5.39}$$

with the respective parameter values

$$\alpha_A = A_{12}^2, \quad \beta_A = A_{11}^2, \quad \alpha_B = B_{12}^2, \quad \beta_B = B_{11}^2 \tag{5.40}$$

for $\mathcal{M}_A$ and $\mathcal{M}_B$. Provided that at least one of these Möbius transformations is non-degenerate, these equations can be solved (up to a sign) for z_2, z_3, z_4 in terms of z_1, say, so together they contribute only one real parameter to the family of H_2-reducible Hadamard matrices. There are four points where both transformations are degenerate, namely

$$(x_1, x_2, x_3) = (0, 0, \pm 1) \quad \text{and} \quad (x_1, x_2, x_3) = (\pm 1, 0, 0). \tag{5.41}$$

Hence the parameter space has three dimensions, and can be roughly described as a circle bundle over a two-dimensional sphere, but with four special points where the circle has been blown up to a torus.

It would be desirable to work out exactly what choices of the three parameters lead to equivalent Hadamard matrices. This problem has been solved only partially. Changing the sign of any z_i leads to equivalent Hadamard matrices. It is also known that the transformations

$$(x_1, x_2, x_3) \rightarrow (-x_1, -x_2, x_3) \rightarrow (x_1, -x_2, -x_3) \rightarrow (-x_1, -x_2, -x_3) \qquad (5.42)$$

lead to equivalent Hadamard matrices if supplemented by appropriate transformations of the phase factors z_i. Hence at most one octant of the sphere is needed in the parameterization.

It remains to describe some examples of special interest. The first family to be discovered was the affine *Fourier family*[128]

$$F(a,b) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \gamma z_1 & \gamma^2 z_2 & \gamma^3 & \gamma^4 z_1 & \gamma^5 z_2 \\ 1 & \gamma^2 & \gamma^4 & 1 & \gamma^2 & \gamma^4 \\ 1 & \gamma^3 z_1 & z_2 & \gamma^3 & z_1 & \gamma^3 z_2 \\ 1 & \gamma^4 & \gamma^2 & 1 & \gamma^4 & \gamma^2 \\ 1 & \gamma^5 z_1 & \gamma^4 z_2 & \gamma^3 & \gamma^2 z_1 & \gamma z_2 \end{pmatrix} \qquad (5.43)$$

with $\gamma = \gamma_6 = e^{i2\pi/6}$ here while $z_1 = e^{i2\pi a}$ and $z_2 = e^{i2\pi b}$. In the construction the two free parameters a, b arise because a six-dimensional space can be written as a tensor product. For this subfamily the equivalence problem has been fully understood.[28] Thus there is a discrete group acting on the square, or torus, parameterized by a, b. It is a semi-direct group of a dihedral group with a discrete translation group. This dihedral group is the symmetry group of a regular hexagon. The result is that the original square is divided into 144 equivalent triangles of equal area. One of them has corners at $(0, 0)$, $(1/6, 0)$ and $(1/6, 1/12)$, and every affine $F(a, b)$ is equivalent to one for which (a, b) lies within this triangle.

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,

$$F_6 = F(0, 0) = F^{\mathrm{T}}(0, 0) \approx F_2 \otimes F_3 \approx F_3 \otimes F_2. \qquad (5.44)$$

The equivalence happens because the factors of $6 = 2 \cdot 3$ are relatively prime; see Ref. 140 for a general discussion of equivalences between tensor products of Fourier matrices.

In the family of H_2-reducible Hadamard matrices, one finds the Fourier family at the special point $(x_1, x_2, x_3) = (0, 0, 1)$, while the transposed Fourier family sits at $(x_1, x_2, x_3) = (1, 0, 0)$; recall that both Möbius transformations of (5.38)−(5.40) become degenerate at these points. Curiously, the one parameter family $F^{\mathrm{T}}(0, b)$ also sits at $(0, 0, 1)$, and similarly $F(a, 0)$ also sits at $(1, 0, 0)$.

One more affine family is known, namely the Diţă family,[136] which in dephased form is given by

$$
D(a) = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & i & -i & -i & i \\
1 & i & -1 & iz & -iz & -i \\
1 & -i & iz^* & -1 & i & -iz^* \\
1 & -i & -iz^* & i & -1 & iz^* \\
1 & i & -i & -iz & iz & -1
\end{pmatrix} \quad \text{with } z = e^{i2\pi a}. \quad (5.45)
$$

We obtain all inequivalent examples if we impose the restriction $-1/8 < a \leq 1/8$. It includes the Butson-type matrix $D_6(0)$, known as the Diţă matrix, and composed of fourth roots of unity. This can be found in several different places within the three-parameter family, reflecting the fact that the equivalence problem for the latter is unsolved. One possibility is to set $x_1 = x_2 = x_3$, in which case the Diţă family is parameterized by the phase factor z_1.

Another Hadamard matrix of special interest is the circulant matrix[129]

$$
C_6 = \begin{pmatrix}
1 & id & -d & -i & -d^* & id^* \\
id^* & 1 & id & -d & -i & -d^* \\
-d^* & id^* & 1 & id & -d & -i \\
-i & -d^* & id^* & 1 & id & -d \\
-d & -i & -d^* & id^* & 1 & id \\
id & -d & -i & -d^* & id^* & 1
\end{pmatrix}, \quad (5.46)
$$

where

$$
d = \frac{1-\sqrt{3}}{2} + i\sqrt{\frac{\sqrt{3}}{2}}, \quad d^*d = 1. \quad (5.47)
$$

The unimodular number d solves the equation $d^2 - (1-\sqrt{3})d + 1 = 0$. It is known that every circulant Hadamard matrix is equivalent to either F_6 or C_6.

Before Karlsson's work, several nonlinear subfamilies of Hadamard matrices were known. The first to be found (by Beauchamp and Nicoara[141]) was the one-parameter family $B(\theta)$ containing all Hadamard matrices equivalent to a hermitian matrix. It interpolates between C_6 and $D_6(0)$ in a complicated way. It is included as the boundary of a two-parameter family of *bicirculant* Hadamard matrices found by Szöllősi.[142] 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

$$
X_6 = \begin{pmatrix} A & B \\ B^\dagger & -A^\dagger \end{pmatrix}, \quad (5.48)
$$

where H is bicirculant because A and B are circulant,

$$A = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}, \quad B = \begin{pmatrix} d & e & f \\ f & d & e \\ e & f & d \end{pmatrix}. \tag{5.49}$$

The individual entries are unimodular phase factors. Since any two circulant matrices commute the unitarity conditions are quite simple to state. Szöllősi ended up with an appealing picture of the resulting two-parameter family. In the complex plane, the parameter space is bounded by two *deltoids* related by a reflection. By definition a deltoid is a 3-hypocycloid, that is 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; see Fig. 2. The picture is that of an umbrella, and in fact of two superposed umbrellas because above each point there are two inequivalent matrices that can be represented as the transposes of each other. Thus we have two two-parameter families $X_6(\alpha)$ and $X_6^{\mathrm{T}}(\alpha)$ coming together at their common boundary. One can easily check that they are subfamilies of Karlsson's family.

Another one-parameter family of symmetric Hadamard matrices[143] was extended to a two-parameter family by Karlsson.[144] This family can be obtained by setting $z_1 = z_2$ and $z_3 = z_4$ in the ansatz (5.32). Interestingly it is then possible to solve explicitly for the matrices A and B in terms of the phases z_1 and z_3.

The elegance of the available constructions is very encouraging, but they are not the end of the story. It has been conjectured[28] that a four-parameter family exists. One reason for this is that the defect of all included matrices has been found to be four, whenever it has been checked,[28] and moreover there is by now strong numerical
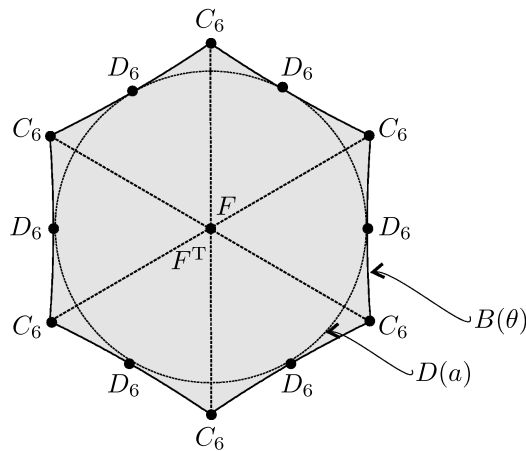
Fig. 2.   Szöllősi's two-dimensional family of $N = 6$ complex Hadamard matrices interpolates between the generalized Fourier matrix $F = F(1/6, 0)$ and the hermitian family $B(\theta)$, which includes C_6 and D_6. It is parametrized by the common interior of two deltoids. There are actually several "leaves" over the interior, and it is divided into six equivalent sectors. Diţă's affine family $D(a)$, see (5.45), is represented by a circle inscribed into the figure.

evidence for the conjecture.[145,146] 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*.[139,147] It is isolated because its defect vanishes. One does not know 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.[134] 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.[134] It is also known that every real Hadamard matrix admits an affine orbit if $N \geq 12$.[148] 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.[149]

All circulant Hadamard matrices up to $N \leq 9$ have been found.[129] When N contains a square factor this includes a continuous family,[132] whereas the number is finite for all prime N.[133] Many block circulant examples are also known.[150] Special methods for constructing Hadamard matrices include one based on tiling abelian groups,[151] one based on N equiangular vectors in $N/2$ dimensions,[152] as well as a method for constructing Hadamard matrices of size N from matrices of size $N/2$. This gives a rich supply of examples with $N = 8$.[153,154] And, of course, there are many ad hoc constructions. A catalog of known Hadamard matrices for $N \leq 16$ is available,[135] also as an updated internet version.[155]

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. Equivalently, 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.[78] The explicit form of unbiased Hadamard matrices forming one maximal set of MUHM for any prime $N = p$ is provided in Appendix B. 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.[79] 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:

$$(\mathbb{1}, F_4(a), H^{(1)}(\phi_1; \alpha_1)), \quad (\mathbb{1}, F_4(0), H^{(2)}(\phi_2; \alpha_2)), \quad (\mathbb{1}, F_4(0), H^{(3)}(\phi_3; \alpha_3)). \quad (5.50)$$

The third members of these triplets are given by

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

$$H^{(2)}(\phi_2; \alpha_2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ e^{i\alpha_2} & e^{i(\alpha_2+\phi_2)} & -e^{i\alpha_2} & -e^{i(\alpha_2+\phi_2)} \\ -e^{i\alpha_2} & e^{i(\alpha_2+\phi_2)} & e^{i\alpha_2} & -e^{i(\alpha_2+\phi_2)} \\ 1 & -1 & 1 & -1 \end{pmatrix}, \quad (5.51)$$

$$H^{(3)}(\phi_3; \alpha_3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ -e^{i\alpha_3} & -e^{i(\alpha_3+\phi_3)} & e^{i\alpha_3} & e^{i(\alpha_3+\phi_3)} \\ e^{i\alpha_3} & -e^{i(\alpha_3+\phi_3)} & -e^{i\alpha_3} & e^{i(\alpha_3+\phi_3)} \end{pmatrix},$$

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

$$\alpha_1 = \alpha_2 = \alpha_3 = \frac{\pi}{2}, \quad a = \phi_1 = \phi_2 = \phi_3 = 0. \quad (5.52)$$

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. For $N = 5$ there are two inequivalent triplets.[79]

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.[156,157] 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 pairwise complementary period-4 operators; see Table 2.[158] Alternatively we can use the magic basis for the two−q-bit Hilbert space, so that real vectors are maximally entangled.[159] 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

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 0−2 consist of product states; bases 3 and 4 consist of maximally entangled states. Together with the identity $\mathbf{1} \otimes \mathbf{1}$ and phase factors ± 1, $\pm \mathrm{i}$, 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 unitary observables in the right column are pairwise complementary; see Sec. 2.5. The period-5 unitary transformation of (5.52) permutes the five period-4 observables cyclically: $0 \to 1 \to 2 \to 3 \to 4 \to 0$.

Basis	Set of three commuting period-2 observables			Complementary period-4 observables
0	$\sigma_z \otimes \mathbf{1}$	$\mathbf{1} \otimes \sigma_z$	$\sigma_z \otimes \sigma_z$	$\dfrac{1+\mathrm{i}}{2}\left(\sigma_z \otimes \mathbf{1} - \mathrm{i}\,\mathbf{1} \otimes \sigma_z\right)$
1	$\sigma_x \otimes \mathbf{1}$	$\mathbf{1} \otimes \sigma_x$	$\sigma_x \otimes \sigma_x$	$\dfrac{1+\mathrm{i}}{2}\left(\mathbf{1} \otimes \sigma_x - \mathrm{i}\,\sigma_x \otimes \sigma_x\right)$
2	$\sigma_y \otimes \mathbf{1}$	$\mathbf{1} \otimes \sigma_y$	$\sigma_y \otimes \sigma_y$	$\dfrac{1+\mathrm{i}}{2}\left(\sigma_y \otimes \mathbf{1} - \mathrm{i}\,\mathbf{1} \otimes \sigma_y\right)$
3	$\sigma_x \otimes \sigma_y$	$\sigma_y \otimes \sigma_z$	$\sigma_z \otimes \sigma_x$	$\dfrac{1+\mathrm{i}}{2}\left(\sigma_y \otimes \sigma_z - \mathrm{i}\,\sigma_z \otimes \sigma_x\right)$
4	$\sigma_y \otimes \sigma_x$	$\sigma_z \otimes \sigma_y$	$\sigma_x \otimes \sigma_z$	$\dfrac{1+\mathrm{i}}{2}\left(\sigma_z \otimes \sigma_y - \mathrm{i}\,\sigma_y \otimes \sigma_x\right)$

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. The Segre configuration (mentioned in Sec. 4.3) has an analog known as Reye's configuration: if we pick a pair of vectors from two distinct bases, there is a unique vector in the third basis which is linearly dependent on the first two.[160]

We note that the unitary transformation which is defined by the mapping

$$(\sigma_x \otimes \mathbf{1}, \sigma_z \otimes \mathbf{1}, \mathbf{1} \otimes \sigma_x, \mathbf{1} \otimes \sigma_z) \to (\sigma_y \otimes \sigma_y, \mathbf{1} \otimes \sigma_x, \sigma_y \otimes \mathbf{1}, \sigma_x \otimes \sigma_x) \qquad (5.53)$$

is of period 5 and permutes the period-4 observables in the last column of Table 2 cyclically, which is why the five bases are listed in this particular order. We have here an illustration of the observation[161−163] that, in the case of M−q-bit systems ($N = 2^\mathrm{M}$), a maximal set of $N + 1$ MUB can be generated from the computational basis by repeated application of a suitable unitary operator with period $N + 1$. When $N = p^\mathrm{M}$ with $p = 3 \pmod 4$ this can be done with an anti-unitary operator.[164]

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 the first published account is the one by Zauner,[22] 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.[165−167] There is very strong evidence that the number of kets unbiased to the bases represented by the pair $(\mathbb{1}, F(a, b))$ equals 48, regardless of the values taken by the parameters a, b, with $F(a, b)$ as introduced in (5.43). 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,[89] and $F(1/6, 0)$ 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 $F(1/6, 0)$ 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,[165] and also a proof that there exists a vicinity of $(a, b) = (0, 0)$ where the number of unbiased vectors is constant[166] 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 means of Gröbner bases for the polynomials. In the end polynomial equations in single variables are solved 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_v of kets unbiased to the computational basis and one additional listed basis, as well as the number N_t of bases (or triplets of MUB) that can be formed from these vectors.[165] The results for the twin families $F(a, b)$ and $F^T(a, b)$ are the same, and hence results for the latter are not given explicitly. For the Diță family $D(a)$ of (5.44) one finds that the result depends on the parameter value; if $|a| < a_* \simeq 0.0177$ there are 120 unbiased vectors, and if $a_* < |a| \le 1/8$ 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

Table 3.   Number N_v of kets unbiased with respect to a given complex Hadamard matrix and the number N_t of bases (not mutually unbiased) which can be formed out of them, obtained for generic values of the parameters a and b as well as for $|a_1| < a_* < |a_2| \le 1/8$ with $a_* \simeq 0.0177$.

Matrix	$F(a, b)$	$F(0, 0)$	$F(\frac{1}{6}, 0)$	$D(0)$	$D(a_1)$	$D(a_2)$	S_6
N_v	48	48	48	120	120	48	90
N_t	8	16	70	10	4	4	0

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,[28] and for the affine family $F(a,b)$ some partial understanding exists.[166]

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.[22] 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 $(\mathbb{1}, F(0, b(t)), H(t))$ has been constructed by Jaming *et al.*[166]; 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,[89] and the failure can be expressed quantitatively.[28] 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. However, the best one can do is $D_c^2 = 0.93$. 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 Jaming *et al.* recently proved that no quartets of MUB including any member of the Fourier family $F(a,b)$ can exist.[166] 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,[22,168] but relatively few such investigations have been published. Butterley and Hall[169] 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[170] concentrated on finding *MU constellations*, defined as up to $N + 1$ 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 $\{5^4\}_6$, in a notation that should now be obvious (given the fact that five orthogonal vectors automatically define a sixth, unbiased to all

vectors that are unbiased with respect to the original five). 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, says 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 case of $N = 6$.[28,89,166,169−171]

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).[w] 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 $X^j Z^k$ because quite a few of these products belong to more than one subgroup. For example, we have $\gamma_6 X^2 Z^2 = (XZ)^2 = -(XZ^4)^2$ and, therefore, the operators XZ and XZ^4 are not complementary.

In total, there are 12 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 12 "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

---

[w]Recall footnote 'a': In marked contrast to a field, a ring may have zero products of nonzero elements, such as $2 \odot_6 3 = 0$.

Table 4. The 12 abelian subgroups of order six 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 $X^m Z^n$ 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

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.

Similarly, the modulo-4 ring construction fails for $N = 4$.[39] 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.[35,39] There are yet other applications of these techniques, including the discrete phase operators[172] (that would correspond to the dual group in our terminology), and there are interesting connections between MUB and SIC POVMs[22,88,89,173−175] that present appealing applications in the framework of tomography and deserve further study.

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, that is: when they are fields. This fact enables us to design the prime-distinguishing function described in Appendix C.

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, 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, beside the aforementioned constructions that use orthogonal unitary matrices[36,176,177] and discrete phase space,[81,96,178] an abundance of valuable papers on the MUB problem related to group theory,[36,96,179−181] angular momentum,[182,183] finite fields and affine planes,[27,172] and mutually orthogonal Latin squares.[114,184] Nearly all of these constructions rely on properties of primes and prime powers and on an underlying finite field.[87,183,185−189] After some translation, the problem is equivalent to that of finding mutually orthogonal Cartan subalgebras in the Lie algebra of $SL(N)$.[78,190] The problem also occurs in radar science,[191] operator algebra,[192] and coding theory.[65] Geometric approaches to the problem are developed in Refs. 27, 193 and 194.

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).

(a) Maximal sets of MUB exist for all prime power dimensions, $N = p^M$.

(b) If the dimension is not a power of a prime, $N \neq p^M$, 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 $N > 3$, there are certain sets of MUHM that cannot be extended to a maximal set.

(f) In prime dimension, $N = p$, all known sets of MUHM are equivalent to the standard set of Appendix B. 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.

(g) The case of a prime power dimension, $N = p^M$, can be naturally interpreted as a system of M quantum degrees of freedom, each described in its own p-dimensional Hilbert space. In this case several sets of MUB may exist with different

entanglement properties of the basis states. A complete set of MUB represented by block-circulant Hadamard matrices was constructed by Combescure.[195] For two, three, or four q-bits ($N = 4$, 8, or 16) the number of sets of MUB obtained from the Heisenberg–Weyl group but differing in their entanglement properties is one, four, and seventeen, respectively.[80,81,156]

(h) In certain square dimensions, $N = d^2$, the known sets of MUB are larger than would follow from the factorization of d. Wocjan and Beth[184] show that k mutually orthogonal Latin squares of order N enable one to construct $k + 2$ MUB in dimension N^2. For $N = 26^2$ this yields six MUB. On the other hand, the product-ket construction described at the end of Sec. 1.1.5 yields at most $p_1^{a_1} + 1$ MUB in dimension $N = p_1^{a_1} \cdots p_n^{a_n}$ with $p_1 < p_2 < \cdots < p_n$, whenever the dimension is not a prime power. It has been established[196] that one cannot do better by using any other group to replace the Galois-shift Heisenberg–Weyl group.

Finally, a list entry about continuous degrees of freedom:

(i) Continuous degrees of freedom have, as a rule, a continuum of MUB. An exception is the periodic degree of freedom ("motion along a circle") for which only one pair of MUB is known.

Items (a), (b), and (g) invite a speculation about the difference between Hilbert space dimensions N that are a power of a prime and those that are other composite numbers. In the spirit of Sec. 1.1.5, we follow Schwinger's[5–7] guidance and 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 (g) is artificial because the labels $m = 0, 1, \ldots, \text{M} - 1$ 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 $N \neq p^{\text{M}}$ is surely desirable.

Acknowledgments

already known. Sincere thanks to P. Cara for patiently answering our questions about finite fields, and to A. Eusebi for attracting our attention to a sign error in Ref. 35 and correspondence on this subject.

Appendix A. Generalized Position and Momentum Operators for Spherical Coordinates

We denote the cartesian coordinate operators by A_1, A_2, and A_3, and their complementary partners are the (linear) momentum operators B_1, B_2, and B_3. The Heisenberg commutation relations

$$[A_j, B_k] = \mathrm{i}\delta_{j,k}\mathbf{1} \tag{A.1}$$

state that we have three independent copies of the A, B pair of Secs. 1.1.7 and 1.1.8. The operators R, Θ, E for the spherical coordinates, introduced in Secs. 1.1.9−1.1.11 are related to the cartesian A_js in the familiar way,

$$
\begin{aligned}
A_1 &= R\,\sin\Theta\,\frac{E + E^\dagger}{2}, \\
A_2 &= R\,\sin\Theta\,\frac{E - E^\dagger}{2\mathrm{i}}, \\
A_3 &= R\,\cos\Theta,
\end{aligned}
\tag{A.2}
$$

so that the relations

$$
\begin{aligned}
R &= \sqrt{A_1^2 + A_2^2 + A_3^2}, \\
\tan\frac{\Theta}{2} &= \sqrt{\frac{R - A_3}{R + A_3}}, \\
E &= \frac{A_1 + \mathrm{i}A_2}{\sqrt{A_1^2 + A_2^2}}
\end{aligned}
\tag{A.3}
$$

express the spherical coordinate operators in terms of the cartesian coordinate operators.

Their complementary partners are linear functions of the cartesian momenta,

$$S = \sum_{j=1}^{3} \frac{1}{2} (A_j B_j + B_j A_j),$$

$$\Omega = \frac{1}{R} [(A_1 B_1 + B_2 A_2) A_3 - (A_1^2 + A_2^2) B_3], \tag{A.4}$$

$$L = A_1 B_2 - A_2 B_1.$$

Of these, the generator S of scaling transformations and the generator L of rotations around the A_3 axis are familiar operators, whereas Ω is not standard textbook fare.

Of the 15 commutators that involve two different ones of the operators in (A.3) and (A.4) all vanish except for

$$[R, S] = iR, \quad \left[\tan\frac{\Theta}{2}, \Omega\right] = i\tan\frac{\Theta}{2}, \quad [E, L] = -E, \tag{A.5}$$

as one can verify with the aid of

$$[f(A_1, A_2, A_3), B_k] = i\frac{\partial}{\partial A_k} f(A_1, A_2, A_3). \tag{A.6}$$

The numerical spherical coordinates $(x, y, z) = (r \sin\vartheta \cos\varphi, r \sin\vartheta \sin\varphi, r \cos\vartheta)$ are singular for $z = \pm r$ and, in particular, for $r = 0$ and these singularities are inherited by the corresponding operators. The factors R in (1.72) and $\sin\Theta$ in (1.79) bear witness thereof.

Appendix B. 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

$$[E_N]_{jk} = \delta_{j,k} \, e^{i\frac{2\pi}{N}j^2} \quad \text{where } j, k = 0, 1, 2, \ldots, N-1. \tag{B.1}$$

It allows us to define a sequence of N matrices $(H^{(0)}, H^{(1)}, \ldots, H^{(N-1)})$, where

$$H^{(r)} = E_N^r H^{(0)} \quad \text{for } r = 0, 1, 2, \ldots, N-1. \tag{B.2}$$

By construction, all these matrices are complex Hadamard matrices. Furthermore, the products

$$X_{r-s} = \frac{1}{\sqrt{N}} H^{(s)\dagger} H^{(r)} = \frac{1}{\sqrt{N}} F_N^\dagger E_N^{r-s} F_N \tag{B.3}$$

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

$$\frac{1}{2}j(j-1) = \frac{1}{2}q(q-1) + q(j-q)^2 \pmod{N} \quad \text{with } q = \frac{1}{2}(N+1), \qquad \text{(B.4)}$$

which is valid for all odd N values.

Appendix C. A Prime-Distinguishing Function

We return to Sec. 1.1.6, but now consider the $N+1$ operators of (1.27) for arbitrary values of $N \geq 2$. In accordance with

$$(XZ^n)^N = \left\{ \begin{array}{ll} \mathbf{1} & \text{if } N \text{ is odd} \\ (-1)^n \mathbf{1} & \text{if } N \text{ is even} \end{array} \right\} = (-1)^{(N-1)n} \qquad \text{(C.1)}$$

for $n = 0, 1, 2, \ldots, N-1$, the eigenkets $|n, k\rangle$ of XZ^n obey the eigenvalue equation

$$XZ^n|n, k\rangle = |n, k\rangle \beta_N(n) \gamma_N^k \quad \text{with } \beta_N(n)^N = (-1)^{(N-1)n}. \qquad \text{(C.2)}$$

For $n = 0$, we have the eigenkets of X and choose $\beta_N(0) = 1$ to enforce consistency with (1.6)−(1.8), that is: $|0, j\rangle = |\widehat{j}\rangle$; for $n = 1, 2, \ldots, N-1$ we choose a convenient convention for $\beta_N(n)$ in (C.11) below. As always, we have $\gamma_N = \mathrm{e}^{\mathrm{i}2\pi/N}$ here, and we recall the Weyl commutation rule $\gamma_N XZ = ZX$, the central algebraic property of the period-N unitary operators X and Z introduced in Sec. 1.1.2.

The projector on the kth eigenstate of XZ^n is given by the appropriate analog of (1.12),

$$|n, k\rangle\langle n, k| = \frac{1}{N} \sum_{l=0}^{N-1} \left(\frac{XZ^n}{\beta_N(n)\gamma_N^k} \right)^l. \qquad \text{(C.3)}$$

We use this to evaluate the transition probability between $|n, k\rangle$ and $|0, j\rangle$ in terms of a trace,

$$|\langle 0, j|n, k\rangle|^2 = \mathrm{tr} \left\{ \frac{1}{N^2} \sum_{l,l'=0}^{N-1} \left(\frac{XZ^n}{\beta_N(n)\gamma_N^k} \right)^l \left(\frac{X}{\gamma_N^j} \right)^{l'} \right\}$$

$$= \frac{1}{N^2} \sum_{l=0}^{N-1} \beta_N(n)^{-l} \gamma_N^{(j-k)l} \mathrm{tr}\{(XZ^n)^l X^{-l}\}, \qquad \text{(C.4)}$$

where we have recognized that only terms with $l + l' = 0 \pmod{N}$ contribute to the double sum.

As an immediate consequence of $(XZ^n)^l = \gamma_N^{\frac{1}{2}nl(l-1)} X^l Z^{nl}$, we get

$$\mathrm{tr}\{(XZ^n)^l X^{-l}\} = N\gamma_N^{\frac{1}{2}nl(l-1)}\delta_{nl,0}^{(N)}, \tag{C.5}$$

where we meet the modulo-N Kronecker symbol that is defined by

$$\delta_{j,k}^{(N)} = \begin{cases} 1 & \text{if } j = k \ (\mathrm{mod}\ N), \\ 0 & \text{if } j \neq k \ (\mathrm{mod}\ N). \end{cases} \tag{C.6}$$

To proceed further, we write

$$\begin{aligned} N &= N_1 N_2 \geq 2, \\ n &= mN_1 \geq 1, \end{aligned} \tag{C.7}$$

where N_1 is the greatest common divisor of n and N, $N_1 = \gcd(n,N) \geq 1$, which implies that m and N_2 are co-prime, $\gcd(m, N_2) = 1$. For $l = l_1 N_2 + l_2$ with $l_1 = 0, 1, \ldots, N_1 - 1$ and $l_2 = 0, 1, \ldots, N_2 - 1$, we then have

$$\delta_{nl,0}^{(N)} = \delta_{ml_2 N_1,0}^{(N)} = \delta_{ml_2,0}^{(N_2)} = \delta_{l_2,0}^{(N_2)}, \tag{C.8}$$

so that

$$\begin{aligned} \mathrm{tr}\{(XZ^n)^l X^{-l}\} &= N\gamma_N^{\frac{1}{2}ml_1 N(l_1 N_2-1)}\delta_{l_2,0}^{(N_2)} \\ &= N(-1)^{ml_1(l_1 N_2-1)}\delta_{l_2,0}^{(N_2)} \\ &= N(-1)^{(N_2-1)l_1}\delta_{l_2,0}^{(N_2)}, \end{aligned} \tag{C.9}$$

where we encounter a distinction between even and odd N_2 values that is quite similar to the even-odd distinction in (C.1). The last equality in (C.9) recognizes that $l_1(l_1 N_2 - 1)$ is even when N_2 is odd and that m is odd when N_2 is even.

After combining the various ingredients, (C.4) turns into

$$|\langle 0,j|n,k\rangle|^2 = \frac{1}{N}\sum_{l_1=0}^{N_1-1}(-1)^{(N_2-1)l_1}\beta_N(n)^{-l_1 N_2}\gamma_{N_1}^{(j-k)l_1}, \tag{C.10}$$

and upon imposing

$$\beta_N(n)^{N_2} = (-1)^{N_2-1} \tag{C.11}$$

we arrive at

$$|\langle 0,j|n,k\rangle|^2 = \frac{1}{N_2}\delta_{j,k}^{(N_1)}, \tag{C.12}$$

with the slightly frivolous convention of $\delta_{j,k}^{(1)} = 1$ for all j,k. In as much as

$$\beta_N(n) = \begin{cases} \gamma_{2N_2} = \gamma_{2N}^{N_1} = e^{i\pi/N_2} & \text{if } N_2 \text{ is even} \\ 1 & \text{if } N_2 \text{ is odd} \end{cases} \quad \text{for } n = 1, 2, \ldots, N-1 \tag{C.13}$$

obeys the requirement in (C.2) and also meets the constraint (C.11), it is indeed permissible to impose the latter. Other choices for $\beta_N(n)$, as permitted by (C.2), differ

from this $\beta_N(n)$ by a power of γ_N, equivalent to a cyclic relabeling of the states in the nth basis.

In summary, we have

$$\sqrt{N}\,|\langle 0,j|n,k\rangle| = \sqrt{N_1}\delta_{j,k}^{(N_1)} \quad \text{with } N_1 = \gcd(n,N) \tag{C.14}$$

for $n = 1, 2, \ldots, N - 1$. It follows that the 0th basis and the nth basis are MU only if $\gcd(n,N) = 1$, which can be true for all n only if N is prime: the $N + 1$ bases of eigenstates of the operators in (1.27) do not constitute a maximal set of MUB if N is composite.

The general-N version of (1.29) is

$$\langle l|n,k\rangle = \frac{1}{\sqrt{N}}\beta_N(n)^{-l}\gamma_N^{-kl}\gamma_N^{\frac{1}{2}nl(l-1)}, \tag{C.15}$$

which follows from (C.2) upon recalling that $\langle l|Z = \gamma_N^l\langle l|$ and $\langle l+1|X = \langle l|$. This agrees with (1.29) for odd N values, for which $\beta_N(n) = 1$. For $k = j + a$ in (C.14) we then have

$$\sqrt{N}\,|\langle 0,j|n,j+a\rangle| = \frac{1}{\sqrt{N}}\left|\sum_{l=0}^{N-1}[\beta_N(n)\gamma_N^a]^{-l}\gamma_N^{\frac{1}{2}nl(l-1)}\right| = \sqrt{N_1}\delta_{a,0}^{(N_1)}, \tag{C.16}$$

where we choose

$$a = \begin{cases} \dfrac{1}{2}(N-1)n & \text{if } N_2 \text{ is odd,} \\[2mm] \dfrac{1}{2}(N-1)n - \dfrac{1}{2}N_1 & \text{if } N_2 \text{ is even,} \end{cases} \tag{C.17}$$

so that

$$\beta_N(n)\gamma_N^a = \gamma_{2N}^{(N-1)n} \tag{C.18}$$

and, therefore,

$$\frac{1}{\sqrt{N}}\left|\sum_{l=0}^{N-1}\gamma_{2N}^{-(N-1)nl}\gamma_N^{\frac{1}{2}nl(l-1)}\right| = \frac{1}{\sqrt{N}}\left|\sum_{l=0}^{N-1}\gamma_{2N}^{(l-N)ln}\right| = \sqrt{N_1}\delta_{a,0}^{(N_1)} \tag{C.19}$$

for all $N = 2, 3, 4, \ldots$ and $n = 1, 2, \ldots, N - 1$. After taking into account that

$$\begin{aligned} a &\neq 0 \pmod{N_1} && \text{if } N \text{ is even and } N_2 \text{ is odd and } m \text{ is odd} \\ \text{whereas}\quad a &= 0 \pmod{N_1} && \text{otherwise,} \end{aligned} \tag{C.20}$$

this states that

$$\frac{1}{\sqrt{N}}\left|\sum_{l=0}^{N-1}\gamma_{2N}^{(N-l)ln}\right| = \begin{cases} 0 & \text{if } N \text{ even with both } \dfrac{N}{\gcd(n,N)} \text{ and } \dfrac{n}{\gcd(n,N)} \text{ odd,} \\[3mm] \sqrt{\gcd(n,N)} & \text{else,} \end{cases} \tag{C.21}$$

which can also be verified by expressing the sum over l in terms of standard Gauss sums[197]; see, for example, pages $85-90$ in Ref. 198.

It follows from (C.21) that the function $N \mapsto g(N)$ that is defined by

$$g(N) = \sum_{n=1}^{N-1} \left(\frac{1}{\sqrt{N}} \left| \sum_{l=0}^{N-1} \gamma_{2N}^{(N-l)ln} \right| - 1 \right) \tag{C.22}$$

for $N > 1$ can be evaluated as

$$g(N) = \sum_{n=1}^{N-1}{}' \sqrt{\gcd(n,N)} - (N-1), \tag{C.23}$$

where the primed summation omits all even-N terms for which both $N/\gcd(n,N)$ and $n/\gcd(n,N)$ are odd. There are no omissions if N is odd or a power of 2.

The $g(\ )$ of (C.22) is a *prime-distinguishing function* in the sense of

$$\begin{aligned} g(N) &= 0 \quad \text{if } N \text{ is prime,} \\ g(N) &\neq 0 \quad \text{if } N \text{ is composite,} \end{aligned} \tag{C.24}$$

because $\gcd(n,N) = 1$ for all n when N is prime, whereas $\gcd(n,N) > 1$ for some n when N is composite. In the latter situation, the right-hand side of (C.23) contains a sum of the irrational square roots of the prime factors of N, and possibly products of these square roots, with positive integer weights, and no such sum can be rational, so that $g(N)$ is irrational and $g(N) = 0$ is impossible.[x]

For odd N, equivalent forms of $g(N)$ are

$$\begin{aligned} g(N) &= \sum_{n=1}^{N-1} \left(\frac{1}{\sqrt{N}} \left| \sum_{l=0}^{N-1} \gamma_N^{\frac{1}{2}(l-1)ln} \right| - 1 \right) \\ &= \sum_{r=1}^{N-1} \left(\frac{1}{\sqrt{N}} \left| \sum_{l=0}^{N-1} \gamma_N^{rl^2} \right| - 1 \right), \end{aligned} \tag{C.25}$$

of which the first is obtained from (C.22) by the shift $l \to l + (1/2)(N-1)$ in the sum over l, and the second identity follows from (B.4) with $r = nq$. Here we make contact with Appendix B, inasmuch as

$$g(N) = \sum_{r=1}^{N-1} (|[X_r]_{ii}| - 1) = \sum_{r=1}^{N-1} \left(\frac{1}{\sqrt{N}} |[F_N^\dagger E_N^{r-s} F_N]_{ii}| - 1 \right), \tag{C.26}$$

in accordance with (B.3); the index i is arbitrary here because the X_rs are circulant matrices. For $N = p$, an odd prime, we encounter in (C.25) the well-known Gauss sum[198]

$$\left| \sum_{j=0}^{p-1} \gamma^{rj^2} \right| = \sqrt{p}. \tag{C.27}$$

---

[x]We owe this argument to M. Grassl.

As just demonstrated, it is needed to check explicitly that the Hadamard matrices given in Appendix B really are MU when the dimension is prime (see, for instance, Refs. 23 and 35), and (C.27) is also a key ingredient for conceiving a maximally entangling quantum gate that generalizes the two−q-bit CNOT gate in arbitrary dimension.[199]

Concerning the composite-N case of (C.24), we can be more specific about $g(N) \neq 0$. In fact,

$$g(N) > 0 \quad \begin{array}{l} \text{if } N \text{ is odd and composite} \\ \text{or } N \text{ is a multiple of 4,} \end{array} \tag{C.28}$$

and $g(N) < 0$ can only occur when N is an odd multiple of 2. The case of composite odd N is immediate because there are no terms omitted in (C.23). For even N, we exploit the identity

$$g(2^{\mathrm{M}}\nu) = g(2^{\mathrm{M}}) + \frac{2^{\mathrm{M}} - 2^{(\mathrm{M}-1)/2}}{2 - \sqrt{2}} g(\nu) + \frac{2^{\mathrm{M}} - 2^{\mathrm{M}/2}}{2 - \sqrt{2}} (\sqrt{\nu} - 1)$$
$$+ 2^{(\mathrm{M}-1)/2}(2^{\mathrm{M}/2} - 1 - 2^{-1/2})(\nu - 1), \tag{C.29}$$

which is valid for $\mathrm{M} = 1, 2, \dots$ and odd $\nu \geq 3$; it holds also for $\nu = 1$ if we adopt the convention that $g(1) = 0$. The first three summands on the right-hand side of (C.29) cannot be negative, whereas the fourth is positive for $\mathrm{M} > 1$ and negative for $\mathrm{M} = 1$. Indeed, we have

$$g(2p) = \frac{\sqrt{p} - 1}{2 + \sqrt{2}} (\sqrt{2} + 1 - \sqrt{p}) \tag{C.30}$$

when p is an odd prime.

The value of $g(2^{\mathrm{M}})$, needed in (C.29), is available as the $p = 2$ version of the general prime-power value of $g(N)$ that is given by

$$g(p^{\mathrm{M}}) = (p^{\mathrm{M}/2} - 1)(p^{(\mathrm{M}-1)/2} - 1) \quad \text{for } p \text{ prime.} \tag{C.31}$$

We have, in particular, $g(2p) < 0$ for $p \geq 7$, $g(2p^2) < 0$ for $p \geq 29$, and $g(2p^{\mathrm{M}}) < 0$ for $p \geq 37$ when $\mathrm{M} > 2$. A survey for N up to 2×10^6 established that there are 92, 676, 6,949, 77,310, and 155,150N values not exceeding 10^3, 10^4, 10^5, 10^6, and 2×10^6, respectively, for which $g(N) < 0$. These matters are illustrated in Fig. 3.

Equations (C.29) and (C.30) are particular cases of the general factorization formula

$$h(N_1 N_2) = h(N_1)h(N_2) \quad \text{if } \gcd(N_1, N_2) = 1, \tag{C.32}$$

where the auxiliary function $N \mapsto h(N)$ is defined by

$$h(N) = g(N) + \left\{ \begin{array}{ll} N + \sqrt{N} - 1 & \text{if } N \text{ is odd} \\ N + \dfrac{1}{2}\sqrt{N} - 1 & \text{if } N \text{ is even} \end{array} \right\}$$
$$= \frac{1}{4}(3 - (-1)^N)\sqrt{N} + \sum_{n=1}^{N-1} \frac{1}{\sqrt{N}} \left| \sum_{l=0}^{N-1} \gamma_{2N}^{(N-l)ln} \right| \tag{C.33}$$
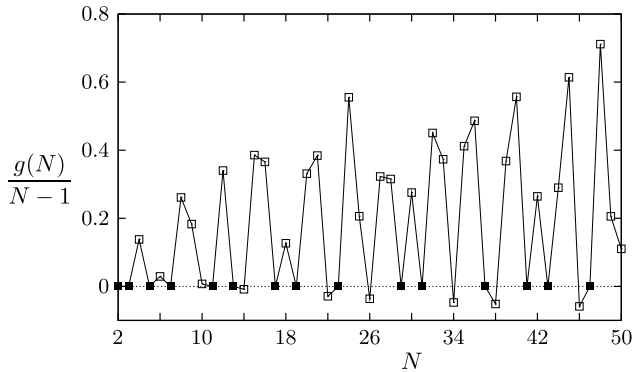
Fig. 3.   The prime-distinguishing function $g(N)$ of (C.21) for $2 \le N \le 50$; for normalization, the function values are divided by $N-1$. Straight lines connect successive values of $g(N)/(N-1)$ to guide the eye. Filled squares show where $g(N) = 0$, which happens when N is prime. Empty squares indicate $g(N) \ne 0$ and so identify composite N values. Consistent with (C.28), we have $g(N) < 0$ for $N = 14, 22, 26, 34, 38$, and 46, with the respective $g(N)$ values given by (C.30).

for $N = 1, 2, 3, \ldots$; consistent with the convention $g(1) = 0$, we have $h(1) = 1$. One establishes (C.32) by an exercise in counting that exploits the explicit form of $g(N)$ in (C.23).

We observe, as an immediate consequence of (C.32), that

$$h(N) = h(p_1^{\mathrm{M}_1})h(p_2^{\mathrm{M}_2})h(p_3^{\mathrm{M}_3})\cdots \tag{C.34}$$

if $N = p_1^{\mathrm{M}_1} p_2^{\mathrm{M}_2} p_3^{\mathrm{M}_3} \cdots$ is the prime-factor decomposition of N. In conjunction with (C.31) this facilitates the computation of $g(N)$ without an actual evaluation of the summations in (C.22) or (C.23).

As a final remark we note that the derivation of (C.21) with quantum-mechanical reasoning in the context of searching for MUB in dimension N seems to indicate that the existence problem of maximal sets of MUB and MUHM is related to number-theoretical properties of the dimension. We leave the matter at that.

Appendix D. Mutually Unbiased Bases for $N = 4$

In accordance with (2.70), the set of MUHM for the maximal set of MUB for $N = p^{\mathrm{M}}$ of Sec. 2 is given by

$$[H_j^{(N)}]_{k,l} = \sqrt{N}\langle e_k^N | e_l^j \rangle = \alpha_{\ominus k}^{j\ \ *}\gamma^{\ominus k \odot l} \tag{D.1}$$

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

$$[G_N^{-1}]_{k,l} = \gamma^{\ominus k \odot l} \tag{D.2}$$

and the diagonal matrix of phase factors

$$[A_j^{(N)}]_{k,l} = \delta_{k,l} \alpha_{\ominus k}^{j}{}^{*}$$ (D.3)

with $A_0^{(N)} = \mathbb{1}_N$ and $H_0^{(N)} = G_N^{-1}$ in particular for the 0th basis, the dual basis. The conventional choices for α_l^j are found in (2.58) for odd N and in (2.65) 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,

$$H_0^{(4)} = G_4^{-1} = G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} G_2 & G_2 \\ G_2 & -G_2 \end{pmatrix} = G_2 \otimes G_2,$$ (D.4)

where G_2 is the 2×2 Hadamard matrix of (1.22). We are reminded here 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

$$N = 4: \quad \alpha_{\ominus l}^{j}{}^{*} = \alpha_l^{j}{}^{*} = \prod_{m,n=0}^{1} (-\mathrm{i})^{j \odot (l_m 2^m) \odot (l_n 2^n)}$$ (D.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

$$\alpha_0^{j}{}^{*} = 1, \quad \alpha_1^{j}{}^{*} = (-\mathrm{i})^{j \odot 1} = (-\mathrm{i})^j, \quad \alpha_2^{j}{}^{*} = (-\mathrm{i})^{j \odot 3},$$ (D.6)

and

$$\alpha_3^{j}{}^{*} = (-\mathrm{i})^{j \odot 1}[(-\mathrm{i})^{j \odot 2}]^2(-\mathrm{i})^{j \odot 3} = (-\mathrm{i})^{j+j \odot 3}(-1)^{j \odot 2}.$$ (D.7)

The resulting phase matrices are $A_0^{(4)} = \mathbb{1}_4$ and

$$A_1^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -\mathrm{i} & 0 & 0 \\ 0 & 0 & \mathrm{i} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_2^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -\mathrm{i} & 0 \\ 0 & 0 & 0 & -\mathrm{i} \end{pmatrix},$$ (D.8)

$$A_3^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \mathrm{i} & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & \mathrm{i} \end{pmatrix},$$

and the Hadamard matrices are $H_0^{(4)} = G_4$ as well as

$$
H_1^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -i & i & -i & i \\ i & i & -i & -i \\ 1 & -1 & -1 & 1 \end{pmatrix}, \quad H_2^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -i & -i & i & i \\ -i & i & i & -i \end{pmatrix},
$$

$$
\text{(D.9)}
$$

$$
H_3^{(4)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ i & -i & i & -i \\ -1 & -1 & 1 & 1 \\ i & -i & -i & i \end{pmatrix}.
$$

When multiplied by $1/\sqrt{N} = 1/2$, the columns of $H_j^{(4)}$ represent the kets of the jth bases with reference to the computational basis, the 4th basis.[y] Up to relabeling, they coincide with those derived by Bandyopadhyay *et al.* in a similar fashion.[36]

References

1. N. Bohr, *Naturwissenschaften* **16** (1928) 245.
2. N. Bohr, *Nature* **121** (1928) 580.
3. H. Weyl, *Z. Phys.* **46** (1927) 1.
4. H. Weyl, *Gruppenthorie und Quantenmechanik* (Hirzel, Leipzig, 1928), English translation by H. P. Robertson (E. P. Dutton, New York, 1932).
5. J. Schwinger, *Proc. Natl. Acad. Sci. U. S. A.* **46** (1960) 570.
6. J. Schwinger, *Quantum Kinematics and Dynamics* (1st edn.: Benjamin, 1970; 2nd edn.: Addison-Wesley, 1991; 3rd edn.: Perseus Books Group, 2000).
7. J. Schwinger, *Quantum Mechanics — Symbolism of Atomic Measurements* (Springer-Verlag, Berlin, 2nd printing, 2003).
8. J. Schwinger, in *Exact Sciences and Their Philosophical Foundations*, eds. W. Deppert, K. Hübner, A. Oberschelp and V. Weidemann (Verlag Peter Lang, Frankfurt, 1985), pp. 107−129.
9. B.-G. Englert and Y. Aharonov, *Phys. Lett. A* **284** (2001) 1.
10. A. Einstein, *Ann. Physik* **17** (1905) 132.
11. A. Einstein, *Ann. Physik* **20** (1906) 199.
12. L. de Broglie, *Recherches sur la Théorie des Quanta*, PhD thesis, Paris (1924).
13. B.-G. Englert, *Phys. Rev. Lett.* **77** (1996) 2154.
14. B.-G. Englert and J. A. Bergou, *Opt. Commun.* **179** (2000) 337.
15. B.-G. Englert, D. Kaszlikowski, L. C. Kwek, and W. H. Chee, *Int. J. Quant. Inf.* **6** (2008) 129.
16. Y. Aharonov, D. Z. Albert, and L. Vaidman, *Phys. Rev. Lett.* **60** (1988) 1351.
17. M. O. Scully, B.-G. Englert, and H. Walther, *Nature* **351** (1991) 111.
18. B.-G. Englert, *Lectures on Quantum Mechanics — Perturbed Evolution* (World Scientific, Singapore, 2006).
19. M. Appleby, *J. Math. Phys.* **46** (2005) 052107.
20. D. I. Fivel, *Phys. Rev. Lett.* **74** (1995) 835.

---

[y] $H_4^{(4)} = \mathbb{1}_4$, so to say, but no factor of $1/2$ for the 4th basis.

21. D. Gottesman, *Phys. Rev. A* **57** (1998) 127.
22. G. Zauner, PhD thesis, Universität Wien (1999).
23. I. D. Ivanovic, *J. Phys. A: Math. Gen.* **14** (1981) 3241.
24. See Problems 2-12a−c in Ref. 6 and Sec. 1.2.6 in Ref. 17.
25. S. Weigert and M. Wilkinson, *Phys. Rev. A* **78** (2008) 020303.
26. B.-G. Englert, *Found. Phys.* **28** (1998) 375.
27. I. Bengtsson and Å. Ericsson, *Open Syst. Inf. Dyn.* **12** (2005) 107.
28. I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej and K. Życzkowski, *J. Math. Phys.* **48** (2007) 052106.
29. J. H. Conway, R. H. Hardin and N. J. A. Sloane, *Exp. Math.* **5** (1996) 93.
30. D. Deutsch, *Phys. Rev. Lett.* **50** (1983) 631.
31. I. Białynicki-Birula, *Phys. Lett. A* **103** (1984) 253.
32. S. Wehner and A. Winter, *New J. Phys.* **12** (2010) 025009.
33. G. Karpilovski, *Field Theory* (Marcel Dekker Inc., New York and Basel, 1988).
34. B. Nagler and T. Durt, *Phys. Rev. A* **68** (2003) 042323.
35. T. Durt, *J. Phys. A: Math. Gen.* **38** (2005) 5267.
36. S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, *Algorithmica* **34** (2002) 512.
37. A. Eusebi and S. Mancini, *Quant. Inf. Comp.* **9** (2009) 950.
38. M. Planat and P. Jorrand, *J. Phys. A: Math. Theor.* **41** (2008) 182001.
39. T. Durt, e-print arXiv:quant-ph/0401046 (2004).
40. T. Durt, *Cosmos* **2** (2006) 21.
41. T. Durt, D. Kaszlikowski, J.-L. Chen and L. C. Kwek, *Phys. Rev. A* **69** (2004) 032313.
42. D. Bruß, *Phys. Rev. Lett.* **81** (1998) 3018.
43. D. Bruß and C. Macchiavello, *Phys. Rev. Lett.* **88** (2002) 127901.
44. Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L. C. Kwek and C. H. Oh, *Phys. Rev. A* **68** (2003) 022324.
45. S. L. Braunstein, A. Mann and M. Revzen, *Phys. Rev. Lett.* **68** (1992) 3259.
46. C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69** (1992) 2881.
47. A. S. Holevo, *Probl. Peredachi Inf.* **9** (1973) 3.
48. A. S. Holevo, *Probl. Inf. Transm. (USSR)* **9** (1973) 177.
49. R. F. Werner, *J. Phys. A: Math. Gen.* **34** (2001) 7081.
50. M. S. Zubairy, *Phys. Rev. A* **54** (1998) 4368.
51. Z. Zhang, Y. Liu and D. Wang, *Phys. Lett. A* **372** (2007) 28.
52. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Bangalore, India (1984), p. 175.
53. P. Boykin and V. Roychowdhury, *Phys. Rev. A* **67** (2003) 042317.
54. H. Bechmann-Pasquinucci and W. Tittel, *Phys. Rev. A* **61** (2000) 062308.
55. N. J. Cerf, *Acta Phys. Slov.* **48** (1998) 115.
56. N. J. Cerf, *Phys. Rev. Lett.* **84** (2000) 4497.
57. N. J. Cerf, *J. Mod. Opt.* **47** (2000) 187.
58. N. J. Cerf, T. Durt and N. Gisin, *J. Mod. Opt.* **49** (2002) 1355.
59. C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu and A. Peres, *Phys. Rev. A* **56** (1997) 1163.
60. R. B. Griffiths and C.-S. Niu, *Phys. Rev. A* **56** (1997) 1173.
61. C.-S. Niu and R. B. Griffiths, *Phys. Rev. A* **60** (1999) 2764.
62. D. Bruss, M. Cinchetti, G. M. D'Ariano and C. Macchiavello, *Phys. Rev. A* **62** (2000) 012302.
63. A. K. Ekert, *Phys. Rev. Lett.* **67** (1991) 661.
64. D. Gottesman, *Phys. Rev. A* **54** (1996) 1862.

65. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, *Phys. Rev. Lett.* **78** (1997) 405.

66. M. A. Nielsen and I. L. Chuang, *Quantum Computing and Quantum Information* (Cambridge University Press, Cambridge, 2000).

67. D. Gottesman, Quantum Error Correction and Fault-Tolerance, in *Encyclopedia of Mathematical Physics*, Vol. 4, eds. J.-P. Francoise, G. L. Naber and S. T. Tsou (Elsevier, Oxford, 2006); available as e-print arXiv:quant-ph/0507174 (2005).

68. M. Żukowski, A. Zeilinger, M. A. Horne and A. K. Ekert, *Phys. Rev. Lett.* **71** (1993) 4287.

69. J.-W. Pan, D. Bouwmeester, H. Weinfurter and A. Zeilinger, *Phys. Rev. Lett.* **80** (1998) 3891.

70. M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon and H. Zbinden, *Nature Phys.* **3** (2007) 692.

71. H.-J. Briegel, W. Dür, J. I. Cirac and P. Zoller, *Phys. Rev. Lett.* **81** (1998) 5932.

72. L. Vaidman, Y. Aharonov and D. Z. Albert, *Phys. Rev. Lett.* **58** (1987) 1385.

73. Y. Aharonov and B.-G. Englert, *Z. Naturforsch.* **56a** (2001) 16.

74. P. K. Aravind, *Z. Naturforsch.* **58a** (2003) 2212.

75. T. Durt, *Int. J. Mod. Phys. B* **20** (2006) 1742; e-print arXiv:quant-ph/0401037 (2004).

76. A. Klappenecker and M. Rötteler, e-print arXiv:quant-ph/0502138 (2005).

77. M. Reimpell and R. F. Werner, *Phys. Rev. A* **75** (2007) 062334.

78. A. I. Kostrikin and P. H. Tiep, *Orthogonal Decompositions and Integral Lattices*, de Gruyter Expositions in Mathematics, Vol. 15 (Walter de Gruyter, Berlin, 1994).

79. S. Brierley, S. Weigert and I. Bengtsson, e-print arXiv:0907.4097[math-ph] (2009).

80. J. L. Romero, G. Björk, A. B. Klimov and L. L. Sanchez-Soto, *Phys. Rev. A* **72** (2005) 062310.

81. G. Björk, J. L. Romero, A. B. Klimov and L. L. Sanchez-Soto, *J. Opt. Soc. Am. B* **24** (2007) 371.

82. D. Kaszlikowski, A. Gopinathan, Y. C. Liang, L. C. Kwek and B.-G. Englert, *Phys. Rev. A* **70** (2004) 032306.

83. B.-G. Englert and J. Řeháček, *J. Mod. Opt.* **57** (2010) 218.

84. E. P. Wigner, *Phys. Rev.* **40** (1932) 749.

85. M. Hillery, R. F. O'Connell, M. O. Scully and E. P. Wigner, *Phys. Rep.* **106** (1984) 121.

86. M. G. A. Paris and J. Řeháček (eds.), *Quantum State Estimation*, Lecture Notes in Physics, Vol. 649 (Springer-Verlag, Berlin, 2004).

87. W. K. Wootters and B. D. Fields, *Ann. Phys. (NY)* **191** (1989) 363.

88. J. M. Renes, R. Blume-Kohout, A. J. Scott and C. M. Caves, *J. Math. Phys.* **45** (2004) 2171.

89. M. Grassl, in *Proc. ERATO Conf. on Quantum Information Science 2004 (EQIS 2004)*; also: e-print arXiv:quant-ph/0406175 (2004).

90. A. J. Scott and M. Grassl, *J. Math. Phys.* **51** (2010) 042203.

91. U. Leonhardt, *Measuring the Quatum State of Light* (Cambridge University Press, United Kingdom, 1997).

92. A. Vourdas, *Rep. Progr. Phys.* **67** (2004) 267.

93. S. Chaturvedi, E. Ercolessi, G. Marmo, G. Morandi, N. Mukunda and R. Simon, *Pramana* **65** (2005) 981.

94. W. K. Wootters, *Ann. Phys. (NY)* **176** (1987) 1.

95. W. K. Wootters, *IBM J. Res. Dev.* **48** (2004) 99.

96. K. S. Gibbons, M. J. Hoffman and W. K. Wootters, *Phys. Rev. A* **70** (2004) 062101.

97. D. Gross, *Appl. Phys. B* **86** (2007) 367.

98. R. J. Glauber, *Phys. Rev.* **131** (1963) 2766.

99. B.-G. Englert, *J. Phys. A: Math. Gen.* **22** (1989) 625.
100. R. P. Feynman, in *Quantum Implications*, eds. B. J. Hiley and F. D. Peat (Routledge & Kegan Paul, London and New York, 1987).
101. T. Durt, C. Kurtsiefer, A. Lamas-Linares and A. Ling, *Phys. Rev. A* **78** (2008) 1.
102. A. O. Pittenger and M. H. Rubin, *J. Phys. A: Math. Gen.* **38** (2005) 6005.
103. 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** (2000) 054101.
104. P. Bertet, A. Auffeves, P. Maioli, S. Osnaghi, T. Meunier, M. Brune, J. M. Raimond and S. Haroche, *Phys. Rev. Lett.* **89** (2002) 200402.
105. B.-G. Englert, N. Sterpi and H. Walther, *Opt. Commun.* **100** (1993) 526.
106. J. Řeháček, B.-G. Englert and D. Kaszlikowski, *Phys. Rev. A* **70** (2004) 052321.
107. T. Durt, *J. Laser Phys.* **11** (2006) 1557.
108. T. Durt, *Open Syst. Inf. Dyn.* **13** (2006) 403.
109. D. M. Appleby, I. Bengtsson and S. Chaturvedi, *J. Math. Phys.* **49** (2008) 012102.
110. M. K. Bennett, *Affine and Projective Geometry* (Wiley, New York, 1995).
111. G. Tarry, *C. R. Ass. Fr. Av. Sci. Naturelles* **1** (1900) 122 & 2170.
112. M. Saniga, M. Planat and H. Rosu, *J. Opt. B: Quantum Semiclass.* **6** (2004) L19.
113. T. Paterek, B. Dakić and Č. Brukner, *Phys. Rev. A* **79** (2009) 012109.
114. T. Paterek, M. Pawłowski, M. Grassl and Č. Brukner, e-print arXiv:0910.1439[quant-ph] (2009).
115. M. Weiner, e-print arXiv:0902.0635[math-ph] (2009).
116. F. Klein, *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert* (Springer, Berlin, 1926).
117. O. Hesse, *Crelle's J.* **28** (1844) 68.
118. C. Segre, *Math. Ann.* **27** (1886) 296.
119. K. Hulek, *Asterisque* **137** (1986) 1.
120. J. J. Sylvester, *Phil. Mag.* **34** (1867) 461.
121. J. Hadamard, *Bull. Sci. Math.* **17** (1893) 240.
122. R. E. A. C. Paley, *J. Math. Phys.* **12** (1933) 311.
123. H. Kharaghani and B. Tayfeh-Rezaie, *J. Comb. Des.* **13** (2005) 435.
124. P. O. Boykin, M. Sitharam, M. Tarifi and P. Wocjan, e-print arXiv:quant-ph/0502024 (2005).
125. A. T. Butson, *Can. J. Math.* **15** (1963) 42.
126. K. J. Horadam, *Hadamard Matrices and their Applications* (Princeton University Press, USA, 2007).
127. K. Kraus, *Phys. Rev. D* **35** (1987) 3070.
128. U. Haagerup, in *Operator Algebras and Quantum Field Theory (Rome)* (International Press, Cambridge, MA, 1996), p. 296.
129. G. Björck and B. Saffari, *C. R. Acad. Sci. Paris, Sér. I* **320** (1995) 319.
130. M. L. Mehta, *Elements of Matrix Theory* (Hindustan Publishing Corporation, Delhi, 1977).
131. W. Pauli, in *Handbuch der Physik*, Vol. 24, eds. H. Geiger and K. Scheel (Springer, Berlin, 1933), pt. 1, p. 98.
132. J.-C. Faugère, Finding all the solutions of Cyclic 9 using Gröbner basis techniques, in *Lecture Notes Series on Computing*, Vol. 9, eds. K. Shirayanagi and K. Yokoyama (World Scientific, Singapore, 2001), p. 1.
133. U. Haagerup, e-print arXiv:0803.2629[math.AC] (2008).
134. W. Tadej and K. Życzkowski, *Lin. Alg. Appl.* **429** (2008) 447.
135. W. Tadej and K. Życzkowski, *Open Syst. Inf. Dyn.* **13** (2006) 133.
136. P. Diţă, *J. Phys. A: Math. Gen.* **37** (2004) 5355.

137. B. R. Karlsson, e-print arXiv:1003.4133[math-ph] (2010).
138. B. R. Karlsson, e-print arXiv:1003.4177[math-ph] (2010).
139. T. Tao, *Math. Res. Lett.* **11** (2004) 251.
140. W. Tadej, *Lin. Alg. Appl.* **418** (2006) 719.
141. K. Beauchamp and R. Nicoara, *Lin. Alg. Appl.* **428** (2008) 1833.
142. F. Szöllősi, *Proc. Am. Math. Soc.* **138** (2010) 921.
143. M. Matolcsi and F. Szöllősi, *Open Syst. Inf. Dyn.* **15** (2008) 93.
144. B. R. Karlsson, *J. Math. Phys.* **50** (2009) 082104.
145. A. J. Skinner, V. A. Newell and R. Sanchez, *J. Math. Phys.* **50** (2009) 012107.
146. B. R. Karlsson, private communication with IB (2010).
147. G. E. Moorhouse, *The 2-transitive Complex Hadamard Matrices*, preprint available at http://www.uwyo.edu/moorhouse/pub/ (2001).
148. F. Szöllősi, *Eur. J. Combin.* **29** (2008) 1219.
149. M. Petrescu, PhD thesis, University of California at Los Angeles (1997).
150. R. Craigen, W. H. Holzmann and H. Kharaghani, *J. Combin. Design* **5** (1998) 319.
151. M. Matolcsi, J. Reffy and F. Szöllősi, *Open Syst. Inf. Dyn.* **14** (2007) 247.
152. R. B. Holmes and V. I. Paulsen, *Lin. Alg. Appl.* **377** (2004) 31.
153. P. Diţă, e-print arXiv:0901.0982[math-ph] (2009).
154. P. Diţă, e-print arXiv:1002.4933[math-ph] (2010).
155. The URL is http://chaos.if.uj.edu.pl/~karol/hadamard.
156. J. Lawrence, Č. Brukner and A. Zeilinger, *Phys. Rev. A* **65** (2002) 032320.
157. Č. Brukner and A. Zeilinger, *Phys. Rev. Lett.* **83** (1999) 3354.
158. B.-G. Englert and N. Metwally, *J. Mod. Opt.* **47** (2000) 2221.
159. C. H. Bennett, D. P. DiVincenzo, J. Smolin and W. K. Wootters, *Phys. Rev. A* **54** (1996) 3824.
160. P. K. Aravind, *Found. Phys. Lett.* **13** (2000) 499.
161. R. Gow, e-print arXiv:math/0703333 (2007).
162. W. K. Wootters and D. M. Sussman, e-print arXiv:0704.1277[quant-ph] (2007).
163. O. Kern, K. S. Ranade and U. Seyfarth, e-print arXiv:0912.4661[quant-ph] (2009).
164. D. M. Appleby, e-print arXiv:0909.5233[quant-ph] (2009).
165. S. Brierley and S. Weigert, *Phys. Rev. A* **79** (2009) 052316.
166. P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner, *J. Phys. A: Math. Theor.* **42** (2009) 245305.
167. W. Bruzda, MSc thesis, Jagiellonian University, Cracow (2006); available online at http://chaos.if.uj.edu.pl/~karol/prace/Br06.pdf.
168. W. Bruzda, private communication with KŻ (2008).
169. P. Butterley and W. Hall, *Phys. Lett. A* **369** (2007) 5.
170. S. Brierley and S. Weigert, *Phys. Rev. A* **78** (2008) 042312.
171. C. Archer, *J. Math. Phys.* **46** (2005) 022106.
172. M. Planat, H. Rosu and M. Saniga, *AIP Conf. Proc.* **734** (2004) 315.
173. S. Colin, J. Corbett, T. Durt and D. Gross, *J. Opt. B: Quantum Semiclass. Opt.* **7** (2005) S778.
174. D. M. Appleby, H. B. Dang and C. A. Fuchs, e-print arXiv:0707.2071[quant-ph] (2007).
175. D. M. Appleby, in *Proc. Växjö Conf. on Foundations of Probability and Physics−5*, eds. L. Accardi *et al.*, *AIP Conf. Proc.*, Vol. 1101 (New York 2009); available as e-print arXiv:0905.1428[quant-ph] (2009).
176. A. Yu. Vlasov, in *Gravitation, Cosmology and Elementary Particles*, eds. V. Dorofeev, A. Yu. Pavlov and E. Poberii (SPb UEF Publishing, St. Petersburg, 2004), p. 147 ; available as e-print arXiv:quant-ph/0302064 (2003).
177. A. O. Pittenger and M. H. Rubin, *Lin. Alg. Appl.* **390** (2004) 255.

178. J. P. Paz, A. J. Roncaglia and M. Saraceno, *Phys. Rev. A* **72** (2005) 012309.
179. M. R. Kibler, *Int. J. Mod. Phys. B* **20** (2006) 1802.
180. P. Sulc and J. Tolar, *J. Phys. A: Math. Gen.* **40** (2007) 15099.
181. O. Albouy and M. R. Kibler, *Sigma* **3** (2007) 076.
182. M. R. Kibler, *Int. J. Mod. Phys. B* **20** (2006) 1792.
183. M. R. Kibler, *J. Phys. A: Math. Theor.* **42** (2009) 353001.
184. P. Wocjan and T. Beth, *Quant. Inf. Comp.* **5** (2005) 93.
185. M. Daoud and M. R. Kibler, *J. Phys. A: Math. Theor.* **43** (2010) 115303.
186. H. F. Chau, e-print arXiv:quant-ph/0212055 (2002).
187. S. Chaturvedi, *Phys. Rev. A* **65** (2002) 044301.
188. A. Klappenecker and M. Roetteler, *Lecture Notes in Computer Science*, Vol. 2948 (Springer-Verlag, Berlin, 2004), p. 137.
189. A. Vourdas, *J. Phys. A: Math. Theor.* **40** (2007) R285.
190. P. O. Boykin, M. Sitharam, P. H. Tiep and P. Wojcan, *Quant. Inf. Comp.* **7** (2007) 371.
191. W. O. Alltop, *IEEE Trans. Inform. Theory* **26** (1980) 350.
192. S. Popa, *J. Operator Theory* **9** (1983) 253.
193. A. B. Klimov, J. L. Romero, G. Björk and L. L. Sanchez-Soto, *J. Phys. A: Math. Gen.* **40** (2007) 3987.
194. A. B. Klimov, J. L. Romero, G. Björk and L. L. Sanchez-Soto, *Ann. Phys. (NY)* **324** (2009) 53.
195. M. Combescure, *J. Math. Phys.* **50** (2009) 032104.
196. M. Aschbacher, A. M. Childs and P. Wocjan, *J. Algebr. Comb.* **25** (2007) 111.
197. C. W. Chin, private communication with BGE (2010).
198. S. Lang, *Algebraic Number Theory*, Grad. Texts in Math., Vol. 110 (Springer-Verlag, New York, 2nd edn. 1994, 3rd printing 2000).
199. T. Durt, L. C. Kwek and D. Kaszlikowski, *Phys. Rev. A* **77** (2008) 042318.