Article

Quantum Information: A Brief Overview and Some Mathematical Aspects

Maurice R. Kibler [1,2,3]

1   CNRS/IN2P3, Institut de Physique Nucléaire, 69622 Villeurbanne, France; m.kibler@ipnl.in2p3.fr
2   Faculté des Sciences et Technologies, Université Claude Bernard Lyon 1, 69622 Villeurbanne, France
3   Université de Lyon, 69361 Lyon, France

check for updates

Abstract: The aim of the present paper is twofold. First, to give the main ideas behind quantum computing and quantum information, a field based on quantum-mechanical phenomena. Therefore, a short review is devoted to (i) *quantum bits* or qubits (and more generally *qudits*), the analogues of the usual bits 0 and 1 of the classical information theory, and to (ii) two characteristics of quantum mechanics, namely, *linearity*, which manifests itself through the superposition of qubits and the action of unitary operators on qubits, and *entanglement* of certain multi-qubit states, a resource that is specific to quantum mechanics. A, second, focus is on some mathematical problems related to the so-called *mutually unbiased bases* used in quantum computing and quantum information processing. In this direction, the construction of mutually unbiased bases is presented via two distinct approaches: one based on the group SU(2) and the other on Galois fields and Galois rings.

Keywords: linearity; superposition; entanglement; mutually unbiased bases; SU(2); Galois fields; Galois rings

1. Introduction

In the present days, there is a growing interest for the field of *quantum information* and *quantum computing*. Such a field emerged at the beginning of the 1980s when Feynman and other scientists asked the question: is it possible to simulate the behaviour of a quantum system by using a classical computer? Then, the question evolved towards how to use quantum systems to do computations. This led to the idea of a quantum computer based on quantum physics with the hope to solve problems that would be intractable or difficult to solve with a classical computer. A fact in favour of a quantum computer is the law by Moore according to which the size of electronic and spintronic devices for a classical computer should approach 10 nm in 2020, the scale where quantum effects become important. The field of quantum information and quantum computing is at the crossroads of experimental and theoretical quantum physical sciences (physics and chemistry), discrete mathematics and informatics with the aim of building a quantum computer. We note in passing that physics, mathematics, informatics and engineering have already greatly benefited from the enormous amount of works achieved along the line of quantum information and quantum computing.

The unit of classical information is the bit (possible values 0 and 1). In a quantum computer, classical bits (0 and 1) are replaced by *quantum bits* or *qubits* (that interpolate in some sense between 0 and 1). The most general qubit is a normalized vector $|\psi\rangle$ in the two-dimensional Hilbert space $\mathbb{C}^2$

$$|\psi\rangle = a|0\rangle + b|1\rangle, \quad |a|^2 + |b|^2 = 1, \quad a \in \mathbb{C}, \quad b \in \mathbb{C} \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the elements of an orthonormal basis in $\mathbb{C}^2$. The result of a measurement of $|\psi\rangle$ is not deterministic since it gives $|0\rangle$ or $|1\rangle$ with the probability $|a|^2$ or $|b|^2$, respectively. The consideration

of N qubits leads to work in the 2^N-dimensional Hilbert space $\mathbb{C}^{2^N}$. Note that the notion of qubit, corresponding to $\mathbb{C}^2$, is a particular case of the one of *qudit*, corresponding to $\mathbb{C}^d$ (d not necessarily in the form 2^N). A system of N qudits is associated with the Hilbert space $\mathbb{C}^{d^N}$. In this connection, the techniques developed for finite-dimensional Hilbert spaces are of paramount importance in quantum computation and quantum computing.

From a formal point of view, a quantum computer is a system producing qubits, the state of which can be controlled and manipulated via unitary transformations. These transformations correspond to the product of elementary unitary operators called *quantum gates* (the analogues of the logic gates of a classical computer) acting on one, two or more qubits. Measurement of the qubits out-coming from a *quantum circuit* of quantum gates yields the result of a (quantum) computation. In other words, a realization of quantum information processing can be performed by preparing a quantum system in a quantum state, then submitting this state to unitary transformations and, finally, reading the outcome from a measurement.

The two basic characteristics of quantum mechanics used in a quantum computer are *linearity* (principle of superposition of quantum states) and *entanglement*. The superposition principle gives resources: the quantum computer can be in several states at the same time. This leads to a massive quantum parallelism with a speed up of computations (for N qubits, 2^N computations can be achieved in parallel through the use of *quantum algorithms*). Entanglement, i.e., the fact that certain quantum systems made of two or more sub-systems behave as an indissociable entity, is at the root of quantum computing and *quantum teleportation*. In quantum mechanics, each measurement on a quantum system perturbs the system and the superposition principle makes impossible to duplicate a quantum state (*no-cloning theorem*). The two latter points and the use of the so-called *mutually unbiased bases* (MUBs), to be defined in Section 3, are the basic ingredients of quantum cryptography (illustrated by the BB84 protocol, the first protocol of quantum cryptography).

The aim of this paper is to present to a community of computer engineers and mathematicians the basic grounds of quantum information and quantum computing as well as some mathematical aspects and related open problems.

This paper is organized as follows. Section 2 deals with the general framework of quantum information and quantum computing (i.e., information and computing based on quantum physics): some of the concepts and ideas evoked above are further described. In Section 3, we address some mathematical aspects of quantum information; in particular, we review some of the methods for constructing mutually unbiased bases (more precisely, methods based on the group SU(2) and on Galois rings and Galois fields). Sections 2 and 3 are mainly based on References [1,2], respectively. References [3–77] constitute an incomplete list (in chronological order) of original works of relevance for an in-depth study of Sections 2 and 3. Finally, the reader will find in Reference [78] some calculations with the help of the Python language illustrating the derivation of mutually unbiased bases according to the methods described in Section 3.

2. The General Framework of Quantum Information and Quantum Computing

2.1. Quantum Mechanics in a Few Words

Classical physics does not apply in the microscopic world. It is not appropriate for describing, explaining and predicting physical and chemical phenomena at the atomic and sub-atomic level. The convenient theory for quantum systems (i.e., molecules, atoms, nuclei and elementary particles) is quantum mechanics, an extension of the old quantum theory mainly due to Planck, Einstein, Bohr and Sommerfeld (the word *quantum* comes from the fact that the energy exchanges between light and matter occur in a quantized form). Quantum mechanics, which is often used in conjunction with some other theories like relativity and quantum field theory, can be presented in two equivalent ways: *wave mechanics* initiated by de Broglie and Schrödinger and *matrix mechanics* pioneered by Heisenberg, Born and Jordan. It is not our purpose to list in detail the postulates of quantum mechanics. We shall

restrict ourselves with four aspects of the Copenhagen interpretation which are indispensable in quantum information and quantum computing.

- In both presentations of quantum mechanics, the state of a closed quantum system is described by a vector (in matrix mechanics) or a wave function (in wave mechanics), noted $|\psi\rangle$ in both cases, belonging to a finite or infinite Hilbert space $\mathcal{H}$.

- In quantum information and quantum computing, the space $\mathcal{H}$ is finite-dimensional (isomorphic to $\mathbb{C}^2$ for qubits or $\mathbb{C}^d$ for qudits) and the (normalized) vector $|\psi\rangle$, defined up to a phase factor, can be the result (arising from an evolution or transformation of a vector $|\psi'\rangle$)

$$|\psi\rangle = U|\psi'\rangle$$

  of the action of a unitary operator U (or quantum gate) on $|\psi'\rangle$. (We are not concerned here with dynamical systems for which the time evolution of ψ in the wave picture is given by the Schrödinger equation, in the non-relativistic case, or the Dirac equation, in the relativistic case, two linear equations.)

- In quantum information and quantum computing, $|\psi\rangle$ is given by a linear combination of the eigenvectors of an observable in the matrix formulation. An observable $\mathcal{A}$ is associated with a measurable physical quantity (energy, position, impulsion, spin, etc.). It is represented by a self-adjoint operator A acting on the space $\mathcal{H}$. The possible outcomes of a measurement of an observable $\mathcal{A}$ are the real eigenvalues of the operator A. Measurement in quantum mechanics exhibits a probabilistic nature. More precisely, if (in the case of the finite-dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$)

$$|\psi\rangle = \sum_{n=0}^{d-1} c_n |\varphi_n\rangle, \quad c_n \in \mathbb{C} \tag{2}$$

where the φ_n given by

$$A|\varphi_i\rangle = \lambda_i |\varphi_i\rangle, \quad i = 0, 1, \cdots, d-1$$

are the orthormalized eigenvectors of A, then a measurement of $\mathcal{A}$ will give λ_k with the probability

$$|c_k|^2 = |\langle \varphi_k | \psi \rangle|^2$$

where $\langle \varphi_k | \psi \rangle$ stands for the inner product of $|\psi\rangle$ by $|\varphi_k\rangle$ (we suppose that the spectrum of A is non-degenerate). Hence, before measurement, the quantum system is in several states being a linear combination of the states $|\varphi_n\rangle$ and, after measurement, the quantum system is in a well-defined state $|\varphi_k\rangle$. Measurement leads to a reduction of the wave packet or wave function collapse. In terms of measurement of qudits, what precedes can be formulated as follows. Let $|\psi\rangle$ as given by Equation (2) be a qudit describing a quantum system before measurement. A measurement of $|\psi\rangle$ in a basis $\{\varphi_i : i = 0, 1, \cdots, d-1\}$ of $\mathbb{C}^d$ yields the state

$$\frac{\langle \varphi_i | \psi \rangle}{\sqrt{\langle \psi | \varphi_i \rangle \langle \varphi_i | \psi \rangle}} |\varphi_i\rangle = \frac{\langle \varphi_i | \psi \rangle}{|\langle \varphi_i | \psi \rangle|} |\varphi_i\rangle$$

with the probability

$$p(i) = |\langle \psi | \varphi_i \rangle|^2$$

Observe that the factor $\langle \varphi_i | \psi \rangle |\langle \varphi_i | \psi \rangle|^{-1}$ is a simple phase factor without importance. By way of example, in the case of $\mathbb{C}^2$, measurement of the qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ in the basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$ yields $|0\rangle$ or $|1\rangle$ (up to unimportant phase factors) with the probabilities $|a|^2$ or $|b|^2$, respectively.

- A postulate of quantum mechanics of considerable interest in quantum information and quantum computing concerns the description of a system composed of several sub-systems. The state vector for the system is build from tensors products of the state vectors of the various sub-systems. This may lead to entangled vector states for the composite system. Entanglement constitutes another important resource for quantum information and quantum computing besides the linearity and the non deterministic nature of quantum mechanics. As an example, suppose we have a system of qubits made of two two-level sub-systems. The Hilbert space for the system is $\mathcal{H} = \mathbb{C}^4 \sim \mathbb{C}^2 \otimes \mathbb{C}^2$, where the first and second $\mathbb{C}^2$ corresponds to the first and second sub-systems, respectively. By the tensor product, we can take

$$\{|0\rangle_1 \otimes |0\rangle_2, \ |0\rangle_1 \otimes |1\rangle_2, \ |1\rangle_1 \otimes |0\rangle_2, \ |1\rangle_1 \otimes |1\rangle_2\}$$

as a basis for $\mathbb{C}^4$, where the indices 1 and 2 refer to the first and the second qubits, respectively. Two kinds of states can be considered in $\mathbb{C}^4$, namely separable or non entangled states as

$$|\psi_s\rangle = |0\rangle_1 \otimes \frac{1}{2}(|0\rangle_2 + \sqrt{3}|1\rangle_2)$$

and non separable or entangled states as

$$|\psi_{ns}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2)$$

For the non entangled state $|\psi_s\rangle$, measurement of the qubit 1 yields $|0\rangle_1$ with the probability 1 while measurement of the qubit 2 leads either to $|0\rangle_2$ with the probability $\frac{1}{4}$ or to $|1\rangle_2$ with the probability $\frac{3}{4}$; therefore, the result of a measurement for one qubit does not depend on the result of a measurement for the other qubit. The situation turns out to be entirely different for the entangled state $|\psi_{ns}\rangle$: a measurement of the first qubit leads either to $|0\rangle_1$ with the probability $\frac{1}{2}$ or to $|1\rangle_1$ with the probability $\frac{1}{2}$; once one of the two results has been obtained, we immediately know what would be the result if we perform a measurement on the second qubit; it is thus unnecessary to make a measurement on the second qubit and this may be sum up as follows:

$$\text{result of a measurement of qubit 1} \quad \Rightarrow \quad \text{state of qubit 2 (without measurement)}$$
$$|0\rangle_1 \quad \Rightarrow \quad |1\rangle_2$$
$$|1\rangle_1 \quad \Rightarrow \quad |0\rangle_2$$

and conversely

$$\text{result of a measurement of qubit 2} \quad \Rightarrow \quad \text{state of qubit 1 (without measurement)}$$
$$|1\rangle_2 \quad \Rightarrow \quad |0\rangle_1$$
$$|0\rangle_2 \quad \Rightarrow \quad |1\rangle_1$$

Entanglement may also occur for more than two qubits. For entangled states, there are strong correlations between the results of measurements of the qubits. This effect is essential for quantum information and quantum computing.

Unfortunately, "something is rotten in the state of Denmark" (where the Copenhagen interpretation developed). In fact, entanglement is also an inconvenience: entanglement of qubits with their environment leads to errors. This is known as the effect of decoherence an important drawback for the building of a quantum computer. One way to fight against errors due to decoherence and other effects of noise is to develop *quantum error-correcting codes*.

2.2. Qubits and Qudits

2.2.1. Qubits

Let

$$B_2 = \{|0\rangle, |1\rangle\}$$

be an orthonormal basis called the computational basis of the Hilbert space $\mathbb{C}^2$. Any normalized (to unity) vector $|\psi\rangle$, see Equation (1), in $\mathbb{C}^2$ is called a quantum bit or qubit. From the quantum mechanical point of view, a qubit describes a state of a two-level quantum system. In the absence of measurement (and decoherence), the state $|\psi\rangle$ is a superposition of $|0\rangle$ and $|1\rangle$. A measurement of the state $|\psi\rangle$ yields either $|0\rangle$ (with the probability $|a|^2$) or $|1\rangle$ (with the probability $|b|^2$). Therefore, the superposition of the states $|0\rangle$ and $|1\rangle$ is lost after the measurement. In matrix form, we take

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

From a group-theoretical point of view, $|0\rangle$ and $|1\rangle$ can be considered as the basis vectors for the fundamental irreducible representation $\left(\frac{1}{2}\right)$ of SU(2), in the chain SU(2) $\supset$ U(1), with

$$|0\rangle = |\tfrac{1}{2}, \tfrac{1}{2}\rangle, \quad |1\rangle = |\tfrac{1}{2}, -\tfrac{1}{2}\rangle \tag{3}$$

in the notations of quantum angular momentum theory.

The state $|\psi\rangle$ can be associated with a point (x, y, z, t) of the sphere S^3 in $\mathbb{R}^4$ according to

$$\mathbb{C}^2 \to S^3 \; : \; a|0\rangle + b|1\rangle \mapsto (x, y, z, t)$$

with $a = x + iy$ and $b = z + it$. In fact, the point (x, y, z, t) can be visualized as a point $(1, \theta, \varphi)$ of the sphere S^2 in $\mathbb{R}^3$, referred to as the Bloch sphere, since ψ can be re-written as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle, \quad 0 \le \theta \le \pi, \quad 0 \le \varphi < 2\pi \tag{4}$$

up to a global multiplicative phase factor. The application

$$S^3 \to S^2 \; : \; (x, y, z, t) \mapsto (1, \theta, \varphi)$$

corresponds to the first Hopf fibration $S^3 \xrightarrow{S^1} S^2$ of compact fibre S^1. Any qubit as given by Equation (4) can be represented by a point on the Bloch sphere. Table 1 gives the correspondence between some remarkable qubits $|\psi\rangle$ and points on the Bloch sphere. Any unitary transformation acting on a qubit $|\psi\rangle$ corresponds to a rotation around an axis passing through the centre of the Bloch sphere.

Table 1. Correspondence between qubits $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ and points ($\xi = \sin\theta\cos\varphi$, $\eta = \sin\theta\sin\varphi$, $\zeta = \cos\theta$) of the Bloch sphere S^2 in $\mathbb{R}^3$.

$|\psi\rangle$	$|0\rangle$	$|1\rangle$	$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$	$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$	$\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$	$\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$
(ξ, η, ζ)	$(0,0,1)$	$(0,0,-1)$	$(1,0,0)$	$(-1,0,0)$	$(0,1,0)$	$(0,-1,0)$

Note that the sets

$$B_0 = \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}, \quad B_1 = \left\{ \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \right\}, \quad B_2 = \{|0\rangle, |1\rangle\} \tag{5}$$

appearing in Table 1 are three orthonormal bases of the space $\mathbb{C}^2$. In addition, the vectors in B_0, B_1 and B_2 are eigenvectors of the Pauli matrices σ_1, σ_2 and σ_3 (defined in Equation (9) below), respectively. The bases B_0, B_1 and B_2 constitute the simplest example of the so-called MUBs to be studied in Section 3.

2.2.2. Qudits

The generalisation from the two-dimensional Hilbert space $\mathbb{C}^2$ to the d-dimensional Hilbert space $\mathbb{C}^d$ $(d > 2)$ is immediate. Given an orthonormal basis (called the computational basis)

$$B_d = \{|n\rangle : n = 0, 1, \cdots, d - 1\} \tag{6}$$

of $\mathbb{C}^d$, any normalized vector

$$|\psi\rangle = \sum_{n=0}^{d-1} c_n |n\rangle, \quad \sum_{n=0}^{d-1} |c_n|^2 = 1, \quad c_i \in \mathbb{C}, \quad i = 0, 1, \cdots, d - 1$$

is called a qudit. From the point of view of quantum mechanics, the states $|n\rangle$ can be realized as generalized angular momentum states with

$$|n\rangle = |j, m\rangle, \quad n = j - m, \quad d = 2j + 1 \tag{7}$$

where for fixed j, the index m takes the values $-j, -j + 1, \cdots, j$. This yields the correspondence

$$|0\rangle = |j, j\rangle, \quad |1\rangle = |j, j - 1\rangle, \quad \cdots, \quad |d - 1\rangle = |j, -j\rangle$$

between qudits and angular momentum states. (Let us recall that the *angular momentum state* $|j, m\rangle$ is a common eigenstate of the square J^2 of a generalized angular momentum and of the z-component J_z of the angular momentum.) Therefore, $|\psi\rangle$ can be re-written

$$|\psi\rangle = \sum_{m=-j}^{j} d_{j-m} |j, m\rangle$$

in the angular momentum basis $\{|j, m\rangle : m = -j, -j + 1, \cdots, j\}$. For instance, a qutrit $|\psi\rangle$ can be written

$$|\psi\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle$$

in the ternary basis $\{|0\rangle, |1\rangle, |2\rangle\}$ or

$$|\psi\rangle = d_2 |1, -1\rangle + d_1 |1, 0\rangle + d_0 |1, 1\rangle$$

in the balanced basis $\{|1, -1\rangle, |1, 0\rangle, |1, 1\rangle\}$ associated with the angular momentum $j = 1$.

2.2.3. Qudits with $d = 2^N$

In the case where $d = 2^N$, the corresponding qudits can be obtained from tensor products. For example, for $d = 4$ a basis of $\mathbb{C}^4 \sim \mathbb{C}^2 \otimes \mathbb{C}^2$ is

$$|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Then, the most general quartit $|\psi\rangle$ is made of the superposition of tensor products of two qubits. In detail, we have

$$|\psi\rangle = a|0\rangle \otimes |0\rangle + b|0\rangle \otimes |1\rangle + c|1\rangle \otimes |0\rangle + d|1\rangle \otimes |1\rangle$$

where $a, b, c, d \in \mathbb{C}$ (usually, in $|i\rangle \otimes |j\rangle$ the state $|i\rangle$ refers to the first qubit and $|j\rangle$ to the second).

It is interesting to remark that the vectors $|\psi\rangle$ for $d = 2, 2^2$ and 2^3 are associated with the Hopf fibrations $S^3 \xrightarrow{S^1} S^2$ (connected to complex numbers), $S^7 \xrightarrow{S^3} S^4$ (connected to quaternions) and $S^{15} \xrightarrow{S^7} S^8$ (connected to octonions). Entanglement for $d = 2^2$ and 2^3 can be discussed in terms of fibrations on spheres [21]. In the same vein, we may ask the question of the interest for entanglement of Cayley-Dickson algebras for $d = 2^N$ with $N > 3$ and of fibrations on hyperboloids [13].

2.3. Physical Realizations of Qubits

According to R. Landauer, information is physical so that qubits are realised by quantum systems, more specifically by two-level quantum systems, the qubits $|0\rangle$ and $|1\rangle$ corresponding to two different (energy) levels. We shall not be concerned here with the physical realization of qubits (and qudits). It is enough to say that any two-level quantum system may be considered as a qubit. Therefore, qubits can be carried out by nuclear spins, ultra-cold trapped ions, neutral atoms and Bose-Einstein condensates, two different polarizations of a photon, and Josephson tunnel nanojunctions. For instance, in nuclear magnetic resonance, the nuclear spins of an atom in an organic molecule can be aligned (giving the state $|0\rangle$) or anti-aligned (giving the state $|1\rangle$) with an applied constant magnetic field; in generalized angular momentum terminology, we have the quantum states given by Equation (3) and corresponding to the spin $j = \frac{1}{2}$. Similarly, for an ion cooled and trapped by electric fields in a cavity, qubits can be implemented as electronic states (ground state for $|0\rangle$, excited state for $|1\rangle$). Vibrational states can also be used for realizing qubits (zero-phonon state for $|0\rangle$, one-phonon state for $|1\rangle$).

2.4. Entanglement

2.4.1. Generalities

Entanglement occurs only in quantum physics. It has no analogue in classical physics. The notion of entanglement goes back to the famous paper by Einstein, Poldosky and Rosen. In quantum physics, two (or more than two) particles are said to be entangled if the quantum state of each particle depends of the quantum state(s) of the other(s) or cannot be described independently of the quantum state(s) of the other(s). In other words, there exist correlations between the physical properties of a system of entangled particles. More generally, two entangled sub-systems S_1 and S_2 are not independent so that the global system $\{S_1, S_2\}$ must be considered as a whole even after separation by an arbitrary distance. Then, a measurement made on one sub-system gives an information on the other (without

measurement on the other sub-system). On the contrary, for a non entangled system consisting of two sub-systems, a measurement on one sub-system does not give in general an information on the other sub-system.

As an example, let us consider a system consisting of two particles, system having a total spin equal to 0. If the spin of one particle is measured to be $\frac{1}{2}$ on a certain axis, then we know (without any measurement) that the spin on the other particle on the same axis is $-\frac{1}{2}$ because

$$0 = \frac{1}{2} - \frac{1}{2}$$

The two particles are not independent, even after separation. They still behave like an indivisible system of spin 0.

Entanglement contradicts the principle of locality. There is non locality in the sense that what happens in some place depends of what happens in another place. Indeed, quantum mechanics is a non local, non deterministic and linear physical theory.

2.4.2. Entanglement of Qubits

In quantum information, the notion of entanglement occurs for multi-qubit systems. Let us consider a two-qubit system. There are two possibilities.

- The system is non entangled (or separable); it is then described by a state $|\psi_s\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ such that

$$|\psi_s\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

  which can be re-written as

$$|\psi_s\rangle = ac|0\rangle \otimes |0\rangle + ad|0\rangle \otimes |1\rangle + bc|1\rangle \otimes |0\rangle + bd|1\rangle \otimes |1\rangle$$

  where $a|0\rangle + b|1\rangle$ and $c|0\rangle + d|1\rangle$ refer to the first and second qubit, respectively.
- The system is entangled (or non separable); it is then described by a state $|\psi_{ns}\rangle \in \mathbb{C}^4$ such that

$$|\psi_s\rangle = A|0\rangle \otimes |0\rangle + B|0\rangle \otimes |1\rangle + C|1\rangle \otimes |0\rangle + D|1\rangle \otimes |1\rangle$$

  cannot be written as the tensor product of two qubits in $\mathbb{C}^2$.

It is clear that a necessary and sufficient condition for an arbitrary two-qubit state

$$|\psi\rangle = \alpha|0\rangle \otimes |0\rangle + \beta|0\rangle \otimes |1\rangle + \gamma|1\rangle \otimes |0\rangle + \delta|1\rangle \otimes |1\rangle$$

of $\mathbb{C}^4$ to be non entangled is

$$\alpha\delta - \beta\gamma = 0$$

Therefore, if $\alpha\delta - \beta\gamma \neq 0$, then the state is entangled. The degree of entanglement of an arbitrary normalized two-qubit state $|\psi\rangle$ is characterized by the concurrence defined by

$$C = |\alpha\delta - \beta\gamma|, \quad 0 \leq C \leq \frac{1}{2} \tag{8}$$

Non entangled states correspond to $C = 0$, maximally entangled states to $C = \frac{1}{2}$. (A maximally entangled state is such that the density operator for each qubit is half the identity operator; it corresponds to a maximum value of the entropy.) Equation (8) can be straightforwardly generalized to the case

$$|\psi\rangle = \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} a_{ij} |i\rangle \otimes |j\rangle$$

of two qudits for which the concurrence C is defined as

$$C = \det(a_{ij}), \quad 0 \leq C \leq \frac{1}{\sqrt{d^d}}$$

in agreement with Equation (8) for $d = 2$.

Example 1. *Let us consider the four states ($\oplus$ stands for the addition modulo 2)*

$$|\beta_{xy}\rangle = \frac{1}{\sqrt{2}}[|0\rangle \otimes |y\rangle + (-1)^x|1\rangle \otimes |y \oplus 1\rangle], \quad x, y = 0, 1$$

called Bell states (in reference to the work on the so-called Bell inequalities) or EPR pairs (in reference to the paper by Einstein, Poldosky and Rosen). As a particular case

$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_2 + |1\rangle_1 \otimes |0\rangle_2)$$

where the first qubit (qubit 1) and the second one (qubit 2) are clearly emphasized in order to avoid confusion. The result of a measurement of the qubit 1 gives

- *either $|0\rangle_1$ (with the probability $\frac{1}{2}$) so that the qubit 2 is a priori (without measurement) in the state $|1\rangle_2$*
- *or $|1\rangle_1$ (with the probability $\frac{1}{2}$) so that the qubit 2 is a priori (without measurement) in the state $|0\rangle_2$*

but no measurement can lead to both qubits 1 and 2 in the same state ($|0\rangle$ or $|1\rangle$). The result of a measurement of the qubit 1 provides information on the qubit 2 and reciprocally. It is then unnecessary to make a measurement of one qubit once the result of the measurement of the other is known. Similar conclusions can be obtained for the three other Bell states β_{00}, β_{10} and β_{11}. The four Bell states are maximally entangled (they correspond to $C = \frac{1}{2}$).

　In passing note that

$$|\beta_{xy}\rangle = (-1)^{xy}[(\sigma_1)^y(\sigma_3)^x] \otimes \sigma_0|\beta_{00}\rangle$$

where σ_0, σ_1 and σ_3 are three of the four Pauli matrices

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma_2 = i\sigma_1\sigma_3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{9}$$

Thus, any Bell state $|\beta_{xy}\rangle$ can be obtained from $|\beta_{00}\rangle$.

Example 2. *Let us consider the separable state*

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{5}}(|0\rangle + 2|1\rangle) = \frac{1}{\sqrt{5}}(a|0\rangle \otimes |0\rangle + 2a|0\rangle \otimes |1\rangle + b|1\rangle \otimes |0\rangle + 2b|1\rangle \otimes |1\rangle)$$

tensor product of two normalized qubits. A measurement of the first qubit gives either $|0\rangle$ with the probability $|a|^2 = |\frac{a}{\sqrt{5}}|^2 + |\frac{2a}{\sqrt{5}}|^2$ or $|1\rangle$ with the probability $|b|^2 = |\frac{b}{\sqrt{5}}|^2 + |\frac{2b}{\sqrt{5}}|^2$ while a measurement of the second qubit gives either $|0\rangle$ with the probability $\frac{1}{5} = |\frac{a}{\sqrt{5}}|^2 + |\frac{b}{\sqrt{5}}|^2$ or $|1\rangle$ with the probability $\frac{4}{5} = |\frac{2a}{\sqrt{5}}|^2 + |\frac{2b}{\sqrt{5}}|^2$. Therefore, a measurement on one qubit does not provide information on the other qubit (the state $|\psi\rangle$ corresponds to $C = 0$).

　　It is important to realize that entanglement of qubits (as in Example 1) and more generally of qudits has no analogue for classical bits. To be clear, the bits in 00 or 01 or 10 or 11 are not correlated. This is not the case for the quantum bits in any of the Bell states β_{xy}.

2.5. Quantum Gates

2.5.1. One-Qubit Gates

In a classical computer, bits are handled with the help of logic gates (there exist seven basic logic gates: AND, OR, XOR, NOT, NAND, NOR, and XNOR). A quantum computer processes qubits arranged in registers. It is equipped with quantum gates which perform unitary transformations on qubits. Quantum gates can be represented by unitary matrices. Table 2 gives some examples of quantum gates [G] for one-qubit systems together with their matrix representations G. The actions of the one-qubit gates of Table 2 on the qubit $|x\rangle$ (with $x = 0$ or 1) are given by

$$|x\rangle \rightarrow [\mathrm{I}] \rightarrow |x\rangle, \quad |x\rangle \rightarrow [\mathrm{NOT}] \rightarrow |x \oplus 1\rangle$$

$$|x\rangle \rightarrow [\mathrm{S}_\theta] \rightarrow \mathrm{e}^{\mathrm{i}x\theta}|x\rangle, \quad |x\rangle \rightarrow [\mathrm{H}] \rightarrow \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle) \equiv \tfrac{1}{\sqrt{2}}(|x \oplus 1\rangle + (-1)^x|x\rangle)$$

(as an example, the quantum circuit $|x\rangle \rightarrow [\mathrm{S}_\theta] \rightarrow \mathrm{e}^{\mathrm{i}x\theta}|x\rangle$ is described by the action $S_\theta|x\rangle = \mathrm{e}^{\mathrm{i}x\theta}|x\rangle$). Therefore, by linearity

$$a|0\rangle + b|1\rangle \rightarrow [\mathrm{NOT}] \rightarrow b|0\rangle + a|1\rangle$$

$$a|0\rangle + b|1\rangle \rightarrow [\mathrm{S}_\theta] \rightarrow a|0\rangle + \mathrm{e}^{\mathrm{i}\theta}b|1\rangle$$

$$a|0\rangle + b|1\rangle \rightarrow [\mathrm{H}] \rightarrow \tfrac{1}{\sqrt{2}}(a+b)|0\rangle + \tfrac{1}{\sqrt{2}}(a-b)|1\rangle$$

$$a|0\rangle + b|1\rangle \rightarrow [\mathrm{H}] \rightarrow [\mathrm{H}] \rightarrow a|0\rangle + b|1\rangle$$

(the last circuit reflects that $H^2 = I$). Note that the most general qubit can be obtained from the sequence $[\mathrm{H}] \rightarrow [\mathrm{S}_{2\theta}] \rightarrow [\mathrm{H}] \rightarrow [\mathrm{S}_{\frac{\pi}{2}+\varphi}]$ of one-qubit gates since

$$|0\rangle \rightarrow [\mathrm{H}] \rightarrow [\mathrm{S}_{2\theta}] \rightarrow [\mathrm{H}] \rightarrow [\mathrm{S}_{\frac{\pi}{2}+\varphi}] \rightarrow \cos\theta|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\theta|1\rangle$$

or

$$S_{\frac{\pi}{2}+\varphi}HS_{2\theta}H|0\rangle = \cos\theta|0\rangle + \mathrm{e}^{\mathrm{i}\varphi}\sin\theta|1\rangle$$

up to the phase factor $\mathrm{e}^{\mathrm{i}\theta}$.

Table 2. Four basic quantum gates for one-qubit systems; the gates [I] and [NOT] also denoted [X] are associated with the Pauli matrices σ_0 or I and σ_1 or σ_x, respectively; the two other Pauli matrices σ_2 or σ_y and σ_3 or σ_z define two further one-qubit gates denoted as [Y] and [Z], respectively.

Gate [G]	Identity Gate [I]	Not Gate [NOT]	Phase Gate [S_θ]	Hadamard Gate [H]
matrix form G	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$S_\theta = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta} \end{pmatrix}$	$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

2.5.2. Multi-Qubit Gates

Quantum gates for two-qubit systems are important. For example, let us mention the controlled-NOT gate [C_{NOT}] defined via

$$|x\rangle \otimes |y\rangle \rightarrow [C_{\mathrm{NOT}}] \rightarrow |x\rangle \otimes |y \oplus x\rangle$$

or in operator form

$$C_{NOT}|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus x\rangle$$

where the first input qubit $|x\rangle$ and the second input qubit $|y\rangle$ are called control qubit and target qubit, respectively. Here, the corresponding quantum circuit has two inputs ($|x\rangle$ and $|y\rangle$) and two outputs ($|x\rangle$ and $|y \oplus x\rangle$). In matrix form, we have the permutation matrix

$$
C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
$$

Clearly, $(C_{NOT})^2 = I$. Note that

$$
C_{NOT}|x\rangle \otimes |0\rangle = |x\rangle \otimes |x\rangle \tag{10}
$$

where $x = 0$ or 1; however, this result does not mean that an arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ can be cloned by using the gate [C_{NOT}] since we generally have (see Section 2.6)

$$
C_{NOT}|\psi\rangle \otimes |0\rangle \neq |\psi\rangle \otimes |\psi\rangle
$$

to be compared with Equation (10). Note also that

$$
|x\rangle \otimes |y\rangle \to [H \otimes I] \to [C_{NOT}] \to |\beta_{xy}\rangle
$$

or

$$
|\beta_{xy}\rangle = C_{NOT}(H \otimes I)|x\rangle \otimes |y\rangle
$$

that shows the interest of the gate [C_{NOT}] for producing Bell states (i.e., entangled states) from non entangled states. (By [$H \otimes I$], we mean that the quantum gates [H] and [I] act on $|x\rangle$ and $|y\rangle$, respectively. Hence, $H \otimes I$ stands for the direct product of the matrices H and I.)

More generally, the quantum gate [U_f] is defined through

$$
|x\rangle \otimes |y\rangle \to [U_f] \to |x\rangle \otimes |y \oplus f(x)\rangle
$$

or in an equivalent way

$$
U_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle
$$

where f stands for the function $f : \{0,1\} \to \{0,1\}$. Clearly, $(U_f)^2 = I$.

Another important two-qubit gate is the controlled phase gate [CP_θ] such that

$$
|x\rangle \otimes |y\rangle \to [CP_\theta] \to |x\rangle \otimes e^{ixy\theta}|y\rangle
$$

or

$$
CP_\theta|x\rangle \otimes |y\rangle = |x\rangle \otimes e^{ixy\theta}|y\rangle
$$

with

$$
CP_\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}
$$

Note that

$$
[C_{NOT}] = [I \otimes H] \to [CP_{\frac{\pi}{2}}] \to [CP_{\frac{\pi}{2}}] \to [I \otimes H]
$$

so that the gate [C_{NOT}] can be obtained from the gates [$I \otimes H$] and [$CP_{\frac{\pi}{2}}$].

There exist other two-qubit gates. Moreover, use is also made of n-qubit gates ($n > 2$). The advantage of the quantum gates over the classical logic gates is that all the quantum gates

are reversible or invertible due to the unitary property of the matrices representing quantum gates; this is not always the case for classical logic gates.

The preceding examples are sufficient for illustrating how works the algorithm set up by Deutsch and Jozsa [1].

2.5.3. Quantum Computing Algorithms

The Deutsch-Jozsa algorithm addresses the following problem: to find with only one measurement if the function

$$f : \{0,1\}^{\otimes n} \rightarrow \{0,1\}$$

is constant or balanced (f is balanced means either $f(0) = 0$ and $f(1) = 1$ or $f(0) = 1$ and $f(1) = 0$; f is constant means $f(0) = f(1) = 0$ or 1). The classical algorithm requires $2^{n-1} + 1$ evaluations of f whereas only one measurement is necessary in order to get the answer. For $n = 1$, the proof based on the quantum circuit $[H \otimes H] \rightarrow [U_f] \rightarrow [H \otimes I]$ of two-qubit gates is as follows. It is easy to show that

$$|0\rangle \otimes |1\rangle \rightarrow [H \otimes H] \rightarrow [U_f] \rightarrow [H \otimes I] \rightarrow |x\rangle \otimes |y\rangle$$

alternatively

$$|x\rangle \otimes |y\rangle = (H \otimes I)U_f(H \otimes H)|0\rangle \otimes |1\rangle$$

where

$$|x\rangle \otimes |y\rangle = \pm|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ if } f \text{ is constant}$$

$$|x\rangle \otimes |y\rangle = \pm|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ if } f \text{ is balanced}$$

Then, the result of a single measurement of the first output qubit can be

$$\begin{cases} |0\rangle \Rightarrow f \text{ is constant} \\ \text{or} \\ |1\rangle \Rightarrow f \text{ is balanced} \end{cases}$$

Therefore, a single measurement (instead of two in the classical case) is sufficient for getting the answer. The Deutsch-Jozsa algorithm is of little interest. However, it shows the superiority of the quantum approach on the classical one (namely, only one measurement instead of $2^{n-1} + 1$ evaluations in the general case where $f : \{0,1\}^{\otimes n} \rightarrow \{0,1\}$).

Let us briefly mention two other historical algorithms, viz, the Shor algorithm and the Grover algorithm [1]. The Shor algorithm concerns the search of the period of a periodic function and is used for the factorization of a composite integer into prime factors. It constitutes an alternative to the classical RSA code. The Grover algorithm makes it possible to find an item in an unstructured data basis consisting of n entries; the quantum speed up for this algorithm is $n \rightarrow \sqrt{n}$ (O(n) researches for the classical case and O($\sqrt{n}$) for the quantum case). The two preceding algorithms are based on the massive quantum parallelism. They formally show the superiority of a (still hypothetical) quantum computer on a classical one. The present evolution is towards quantum cryptography.

2.6. No-Cloning Theorem

We may ask the question: does there exist a unitary operator (or quantum gate) U such that

$$U|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle \tag{11}$$

where $|\psi\rangle = a|0\rangle + b|1\rangle$ is an arbitrary qubit. As a consequence of the linearity of quantum mechanics, the answer is no: it is not possible to clone an arbitrary qubit $|\psi\rangle$ [8]. This result can be proved in the following way. Suppose that there exists U such that Equation (11) is true. Then, by linearity

$$
\begin{aligned}
U|\psi\rangle \otimes |0\rangle &= U(a|0\rangle + b|1\rangle) \otimes |0\rangle \\
&= U(a|0\rangle \otimes |0\rangle + b|1\rangle \otimes |0\rangle) \\
&= aU|0\rangle \otimes |0\rangle + bU|1\rangle \otimes |0\rangle \\
&= a|0\rangle \otimes |0\rangle + b|1\rangle \otimes |1\rangle
\end{aligned}
\tag{12}
$$

On another side, we have

$$
\begin{aligned}
U|\psi\rangle \otimes |0\rangle &= |\psi\rangle \otimes |\psi\rangle \\
&= (a|0\rangle + b|1\rangle) \otimes (a|0\rangle + b|1\rangle) \\
&= a^2|0\rangle \otimes |0\rangle + ab(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle) + b^2|1\rangle \otimes |1\rangle
\end{aligned}
\tag{13}
$$

Compatibility between Equations (12) and (13) yields

$$
a^2 = a \ (\Rightarrow \ a = 0, 1), \quad b^2 = b \ (\Rightarrow \ b = 0, 1), \quad ab = 0 \ (\Rightarrow \ a = 0 \text{ or } b = 0)
$$

The sole solutions are ($a = 1$, $b = 0$) and ($a = 0$, $b = 1$) in agreement with Equation (10). There are no solution in the general case. This proves the no-cloning theorem (a theorem that does not have an analogue in classical information).

Another way to understand this result is to realize that in order to clone an arbitrary state $|\psi\rangle = a|0\rangle + b|1\rangle$ one must measure it so that one gets $|0\rangle$ or $|1\rangle$, two states that differ from $|\psi\rangle$ in general.

2.7. Quantum Teleportation

It is not possible to clone an arbitrary quantum state. However, it is feasible to teleporte it, i.e., to transfer it from one place to another without an effective transportation. In other words, without a material transportation of a qubit, it is possible to transmit at distance the information contained in the qubit. We shall not deal here with some physical device making teleportation possible. We shall rather limit ourselves to the corresponding quantum algorithm [15].

Suppose someone, Alice, wants to send a qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ (for which she does not know a and b) to somebody, Bob, by a quantum circuit and the possibility of using a classical communication channel. The only requirement for Bob and Alice is to dispose of and EPR pair $|\beta_{00}\rangle$, the first qubit of which belongs to Alice and the second one to Bob. Thus, the entry $|\varphi_0\rangle$ of the quantum circuit is

$$
\begin{aligned}
|\varphi_0\rangle &= |\psi\rangle \otimes |\beta_{00}\rangle \\
&= (a|0\rangle_1 + b|1\rangle_1) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3) \\
&= \frac{1}{\sqrt{2}}\left[a|0\rangle_1 \otimes (|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3) + b|1\rangle_1 \otimes (|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3) \right] \\
&= \frac{1}{\sqrt{2}}\left[a(|0\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3 + |0\rangle_1 \otimes |1\rangle_2 \otimes |1\rangle_3) + b(|1\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3 + |1\rangle_1 \otimes |1\rangle_2 \otimes |1\rangle_3) \right]
\end{aligned}
$$

where qubits 1 and 2 refer to the Alice qubit and qubit 3 to the Bob qubit. Then, Alice sends her qubits to a controlled-NOT gate producing the state

$$
\begin{aligned}
|\varphi_1\rangle &= \frac{1}{\sqrt{2}}\left[a(|0\rangle_1 \otimes |0\rangle_2 \otimes |0\rangle_3 + |0\rangle_1 \otimes |1\rangle_2 \otimes |1\rangle_3) + b(|1\rangle_1 \otimes |1\rangle_2 \otimes |0\rangle_3 + |1\rangle_1 \otimes |0\rangle_2 \otimes |1\rangle_3)\right] \\
&= \frac{1}{\sqrt{2}}\left[a|0\rangle_1 \otimes (|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3) + b|1\rangle_1 \otimes (|1\rangle_2 \otimes |0\rangle_3 + |0\rangle_2 \otimes |1\rangle_3)\right]
\end{aligned}
$$

Next, qubit 1 goes to an Hadamard gate giving

$$
|\varphi_2\rangle = \frac{1}{2}\left[a(|0\rangle_1 + |1\rangle_1) \otimes (|0\rangle_2 \otimes |0\rangle_3 + |1\rangle_2 \otimes |1\rangle_3) + b(|0\rangle_1 - |1\rangle_1) \otimes (|1\rangle_2 \otimes |0\rangle_3 + |0\rangle_2 \otimes |1\rangle_3)\right]
$$

which can be re-arranged as

$$
\begin{aligned}
|\varphi_2\rangle &= \frac{1}{2}\left[(|0\rangle_1 \otimes |0\rangle_2) \otimes (a|0\rangle_3 + b|1\rangle_3) + (|0\rangle_1 \otimes |1\rangle_2) \otimes (a|1\rangle_3 + b|0\rangle_3)\right. \\
&\quad + \left.(|1\rangle_1 \otimes |0\rangle_2) \otimes (a|0\rangle_3 - b|1\rangle_3) + (|1\rangle_1 \otimes |1\rangle_2) \otimes (a|1\rangle_3 - b|0\rangle_3)\right]
\end{aligned}
$$

Measurement of qubits 1 and 2 by Alice can give

$$|0\rangle_1 \otimes |0\rangle_2 \text{ with the probability } \tfrac{1}{4}, \quad |0\rangle_1 \otimes |1\rangle_2 \text{ with the probability } \tfrac{1}{4}$$
$$|1\rangle_1 \otimes |0\rangle_2 \text{ with the probability } \tfrac{1}{4}, \quad |1\rangle_1 \otimes |1\rangle_2 \text{ with the probability } \tfrac{1}{4}$$

Suppose Alice gets $|0\rangle_1 \otimes |0\rangle_2$. Then, she communicates this result to Bob by a classical channel (telephone or mail). Thus, Bob knows that $|\psi\rangle$ is $a|0\rangle_3 + b|1\rangle_3$. Should Alice have got $|0\rangle_1 \otimes |1\rangle_2$ or $|1\rangle_1 \otimes |0\rangle_2$ or $|1\rangle_1 \otimes |1\rangle_2$, then Bob would obtain $a|0\rangle_3 + b|1\rangle_3$ after the use of the gates [X] or [Z] or [T] with $T = ZX$ on the states $a|1\rangle_3 + b|0\rangle_3$ or $a|0\rangle_3 - b|1\rangle_3$ or $a|1\rangle_3 - b|0\rangle_3$, respectively. In all cases, the qubit $|\psi\rangle = a|0\rangle + b|1\rangle$ has been teleported. This proof shows that entanglement (via the EPR pair) plays a crucial role in teleportation.

3. Some Mathematical Aspects: Mutually Unbiased Bases

3.1. Introducing MUBs

3.1.1. Generalities about MUBs

Unitary operator bases in the Hilbert space $\mathbb{C}^d$ are of pivotal importance for quantum information and quantum computing as well as for quantum mechanics in general. The interest for unitary operator bases started with the seminal work by Schwinger [5]. In this connection, MUBs play a key role in quantum information and quantum computing. Two distinct orthonormal bases of $\mathbb{C}^d$ are said to be unbiased if and only if the modulus of the inner product of any vector of one basis with any vector of the other one is equal to $\frac{1}{\sqrt{d}}$ (see the detailed definition in Section 3.1.2).

MUBs proved to be useful in classical information theory (network communication protocols) [17,47]. They play an important role in quantum mechanics as for the discrete Wigner function [11,29,34,42,43,55,62], for the solution of the Mean King problem [20,26,33,34,43], for the understanding of the Feynman path integral formalism [57,63] and potentially for studies of the Weyl-Heisenberg group in connection with quantum optics. MUBs are of central importance in quantum information theory as for instance in quantum state tomography (deciphering an unknown quantum state) [38,56,77], quantum cryptography (secure quantum key exchange) [9,25] and quantum teleportation [15]. Along this line, measurements corresponding to MUBs are appropriate for an optimal determination of the density matrix of a quantum system and the use of MUBs ensure the maximum of security for quantum communication (especially in the BB84 quantum cryptography

protocol). Let us also mention that MUBs are connected with the notion of maximal entanglement of quantum states a result of great importance for quantum computing.

Here, it is not our purpose to give some details about all the applications listed above. The interested reader may consult the quoted original references for a full description of each application. It is enough to say that a central common point to all the applications is given by Equation (15) that reflects the uniform probability nature of the results of measurements using MUBs. This is especially obvious in the BB84 protocol where the probability of detection of Eve (a spy) on a quantum communication channel between Alice and Bob is maximum when Alice and Bob use MUBs.

There exist numerous ways of constructing sets of MUBs (e.g., see [58,64,65]). Most of them are based on discrete Fourier transform over Galois fields and Galois rings [2,14,17,28–30,36,41,72], discrete Wigner distribution [11,29,34,42,55], generalized Pauli spin matrices [22,23,27,30], mutually orthogonal Latin squares [33,35], graph theory [74], finite and projective geometries [49,61], convex polytopes [40], complex projective 2-designs [19,39,67], quantum angular momentum theory [44], group theoretical methods [24,45,50,53], discrete phase states [68] and Hadamard matrices [73]. In this section, from quantum theory of angular momentum theory (or, in mathematical terms, from the Lie algebra A_1 of the group $SU(2)$ or $SU(2, \mathbb{C})$ or $SL(2, \mathbb{C})$) we shall derive a formula for a complete set of MUBs in dimension p with p prime. Moreover, we shall construct complete sets of MUBs in dimension p^m with p prime and m positive integer from the additive characters of the Galois field $\mathbb{GF}(p^m)$ for p odd and of the Galois ring $\mathbb{GR}(2^2, m)$ for $p = 2$.

3.1.2. Definition of MUBs

Definition 1. *Let B_a and B_b two distinct orthonormal bases*

$$B_a = \{|a\alpha\rangle \ : \ \alpha = 0, 1, \cdots, d-1\}, \quad B_b = \{|b\beta\rangle \ : \ \beta = 0, 1, \cdots, d-1\}$$

of the Hilbert space $\mathbb{C}^d$. The bases B_a and B_b ($a \neq b$) are said to be unbiased if and only if

$$\forall \alpha \in \mathbb{Z}_d, \ \forall \beta \in \mathbb{Z}_d : |\langle a\alpha | b\beta \rangle| = \frac{1}{\sqrt{d}} \tag{14}$$

where $\langle \ | \ \rangle$ denotes the inner product of $\mathbb{C}^d$ [5,6,10,11]. In other words, the inner product $\langle a\alpha | b\beta \rangle$ has a modulus independent of α and β. The relation

$$|\langle a\alpha | b\beta \rangle| = \delta_{a,b}\delta_{\alpha,\beta} + \frac{1}{\sqrt{d}}(1 - \delta_{a,b})$$

makes it possible to describe both the cases $B_a = B_b$ and $B_a \neq B_b$.

As a typical example, the bases B_0, B_1 and B_2 of $\mathbb{C}^2$, see Equation (5), constitute a set of three MUBS whose basis vectors are specific qubits.

3.1.3. Well-Known Results about MUBs

The main results concerning MUBs are [6,14,19,35,37]:

1. MUBs are stable under unitary or anti-unitary transformations. More precisely, if two unbiased bases undergo the same unitary or anti-unitary transformation, they remain mutually unbiased.
2. The number $N(d)$ of MUBs in $\mathbb{C}^d$ cannot exceed $d + 1$. Thus

$$N(d) \leq d + 1$$

3. The maximum number $d + 1$ of MUBs is attained when d is a power p^m ($m \geq 1$) of a prime number p. Thus

$$N(p^m) = p^m + 1$$

4.   When d is a composite number, $N(d)$ is not known but it can be shown that

$$3 \leq N(d) \leq d+1$$

As a more accurate result, for $d = \prod_i p_i^{m_i}$ with p_i prime and m_i positive integer, we have

$$\min(p_i^{m_i}) + 1 \leq N(d) \leq d+1$$

By way of illustration, let us mention the following cases.

- In the particular composite case $d = 6 = 2 \times 3$, we have

$$3 \leq N(6) \leq 7$$

and it was conjectured that $N(6) = 3$. Indeed, in spite of an enormous amount of computational works, no more than three MUBs were found for $d = 6$.
- For $d = 15 = 3 \times 5$ and $d = 21 = 3 \times 7$, there are at least four MUBs.
- For $d = 676 = 2^2 \times 13^2$, we have

$$2^2 + 1 = 5 \leq N(676) \leq 677$$

but it is known how to construct at least six MUBs.

A set of $d+1$ MUBs in $\mathbb{C}^d$ is referred to as a complete set. Such sets exist for $d = p^m$ (p prime, m positive integer) and this result opens the way to establish a link between MUBs and Galois fields and/or Galois rings.

For d composite (different from a power of a prime), the question to know if there exist complete sets in dimension d, i.e., to know if $N(d)$ can be equal to $d+1$, is still an open problem (in 2018). Indeed, for d different from a power of a prime, it was conjectured (SPR conjecture [32]) that the problem of the existence of a set of $d+1$ MUBs in $\mathbb{C}^d$ is equivalent to the problem of whether there exist a projective plane of order d. As another conjecture for d composite (different from a power of a prime), the problem of the existence of a set of $d+1$ MUBs in $\mathbb{C}^d$ is equivalent to the one of the existence of a decomposition of the Lie algebra of SU(d) into $d+1$ Cartan subalgebras of dimension $d-1$.

3.1.4. Interests of MUBs

MUBs are or relevance in advanced quantum mechanics. From a very general point of view, MUBs are closely connected to the principle of complementarity introduced by Bohr in the early days of quantum mechanics. This principle, quite familiar in terms of observables like position and momentum, tells that for two non-commuting observables, if we have a complete knowledge of one observable, then we have a total uncertainty of the other. Equation (14) indicates that the development in the basis B_a of any vector of the basis B_b is such that each vector of B_a appears in the development with the probability $\frac{1}{d}$. This is especially interesting when translated in terms of measurements, the bases B_a and B_b corresponding to the (non-degenerate) eigenvectors of two non-commuting observables.

A significance of MUBs in terms of quantum measurements can be seen as follows. Let A and B be two non-degenerate (i.e., with multiplicity-free eigenvalues) self-adjoint (or hermitian) operators associated with two observables $\mathcal{A}$ and $\mathcal{B}$ of a quantum system with the Hilbert space $\mathbb{C}^d$ of dimension d. Suppose that the eigenvectors of A and B yield two unbiased bases B_a and B_b, respectively. When the quantum system is prepared in an eigenvector $|b\beta\rangle$ of the observable B, no information can be obtained from a measurement of the observable A. This result follows from the development in the basis B_a of any vector of the basis B_b

$$|b\beta\rangle = \sum_{\alpha=0}^{d-1} |a\alpha\rangle \langle a\alpha|b\beta\rangle$$

which shows that the d probabilities

$$|\langle a\alpha|b\beta\rangle|^2 = \frac{1}{d}, \quad \alpha, \beta = 0, 1, \cdots, d-1 \tag{15}$$

of obtaining any state vector $|a\alpha\rangle$ in a measurement of A are equal.

Indeed, the two operators A and B do not commute. The two corresponding observables $\mathcal{A}$ and $\mathcal{B}$ are said to be complementary (Bohr's principle of complementarity introduced in the early days of quantum mechanics): a precise knowledge of one of them implies a total uncertainty of the other (or, all possible results of measurements of the other one are equally probable). This can be made more explicit through the generalized Heisenberg uncertainty principle. Let A and B be two hermitian operators associated with two observables and $|\psi\rangle$ a vector of $\mathbb{C}^d$. The generalized Heisenberg uncertainty principle can be expressed as

$$\Delta A \Delta B \geq \frac{1}{2} |\langle \psi | [A, B]_- | \psi \rangle|$$

where $[A, B]_- = AB - BA$ and ΔO stands for the standard deviation

$$\Delta O = \sqrt{\langle \psi | O^2 | \psi \rangle - \langle \psi | O | \psi \rangle^2}$$

of the operator $O = A$ or B. (The most familiar example is for d infinite. The position $A = x$ and the momentum $B = p_x$, along the x direction, of a particle are complementary observables. They satisfy the commutation relations $[x, p_x]_- = i\hbar$, where $\hbar$ is the Planck constant. Hence, $\Delta x \Delta p_x \geq \frac{1}{2}\hbar$ so that more precise is Δx more imprecise is Δp_x and *vice versa*.) Therefore, if A and B correspond to observables generating MUBs, then a precise knowledge of A yields a complete indeterminacy of B and *vice versa*.

Note that

$$d + 1 = \frac{d^2 - 1}{d - 1}$$

is the number of different measurements to fully determine a quantum state for a quantum system in dimension d. (This follows from the fact that a $d \times d$ density matrix, that is to say an Hermitian matrix with a trace equal to 1, contains $d^2 - 1$ real parameters and each measurement gives $d - 1$ real parameters.) Note also that $d^2 - 1$ and $d - 1$ are the number of generators and the rank of the special unitary group $\mathrm{SU}(d)$ in d dimensions, respectively, and that for $d = p$ (prime number) their ratio $p + 1$ is the number of disjoint sets of $p - 1$ commuting generators of $\mathrm{SU}(p)$.

The rest of the paper is structured in the following way. In Section 3.2, we give a complete solution, based on a nonstandard approach to the Lie algebra of the group $\mathrm{SU}(2)$ (equivalently, to the quantum theory of angular momentum), for the construction of MUBs in the case where $d = p$ is a prime number. Further developments are discussed in Section 3.3 in relation with Weyl pairs. Sections 3.4 and 3.5 are concerned with the construction of MUBs from Galois fields (for $d = p^m$, a power of an odd prime number) and Galois rings (for $d = 2^m$, a power of the even prime number), respectively. (See Refs. [31,46,48] for the formalism of Galois quantum systems.)

3.2. Group-Theoretical Construction of MUBs

3.2.1. Standard Basis for SU(2)

Equation (7) shows that the vectors $|n\rangle$ (with $n = 0, 1, \cdots, d-1$) of the computational basis (6) can be viewed as the basis vectors $|j, m\rangle$ (with $m = j, j-1, \cdots, -j$) for the irreducible representation (j) of $\mathrm{SU}(2)$ in the chain $\mathrm{SU}(2) \supset \mathrm{U}(1)$. In the language of group theory (and quantum angular momentum theory), the vector $|j, m\rangle$ is a common eigenvector of the Casimir operator J^2 (the square of

an angular momentum) and of a Cartan generator J_z (the z component of the angular momentum) of the Lie algebra A_1 of the group SU(2). More precisely, we have the eigenvalue equations

$$J^2|j,m\rangle = j(j+1)|j,m\rangle, \quad J_z|j,m\rangle = m|j,m\rangle$$

with the orthonormality relations

$$\langle j,m|j,m'\rangle = \delta_{m,m'}, \quad m,m' = j, j-1, \cdots, -j$$

In other words, the computational basis B_d can be visualized as the basis

$$B_{2j+1} = \{|j,m\rangle \ : \ m = j, j-1, \cdots, -j\}$$

known as the standard basis for the irreducible representation (j) of SU(2) or the angular momentum basis corresponding to the angular momentum quantum number j, referred to as spin angular momentum for $j = \frac{1}{2}$.

3.2.2. Nonstandard Bases for SU(2)

As far as the representation theory of SU(2) is concerned, we can replace the complete set $\{J^2, J_z\}$ by another complete set of two commuting operators. For instance, we may consider the set $\{J^2, v_a\}$, where the unitary operator v_a is defined by

$$v_a|j,m\rangle = \begin{cases} |j,-j\rangle & \text{if} \quad m = j \\[2mm] \omega^{(j-m)a}|j,m+1\rangle & \text{if} \quad m = j-1, j-2, \cdots, -j \end{cases}$$

where

$$\omega = e^{i\frac{2\pi}{2j+1}}$$

is a primitive $(2j+1)$-th root of unity and a is a fixed parameter in the ring $\mathbb{Z}_{2j+1}$. The operator v_a takes its origin in a polar decomposition of the two generators $E_\pm = J_\pm$ of the group SU(2). For fixed a, the common eigenvectors of J^2 and v_a provide an alternative basis to that given by the common eigenstates of J^2 and J_z. This can be made precise by the following result.

Proposition 1. *For fixed j and a (with $2j \in \mathbb{N}^*$ and $a \in \mathbb{Z}_{2j+1}$), the $2j+1$ common eigenvectors of J^2 and v_a can be taken in the form*

$$|j\alpha; a\rangle = \frac{1}{\sqrt{2j+1}} \sum_{m=-j}^{j} \omega^{\frac{1}{2}(j+m)(j-m+1)a+(j+m)\alpha}|j,m\rangle$$

with $\alpha = 0, 1, \cdots, 2j$. The corresponding eigenvalues of v_a are given by

$$v_a|j\alpha; a\rangle = \omega^{ja-\alpha}|j\alpha; a\rangle$$

Then, the spectrum of v_a is non-degenerate.

The inner product

$$\langle j\alpha; a|j\beta; a\rangle = \delta_{\alpha,\beta}, \quad \alpha, \beta = 0, 1, \cdots, 2j$$

shows that for fixed j and a

$$B_a = \{|j\alpha;a\rangle \; : \; \alpha = 0, 1, \cdots, 2j\}$$

is an orthonormal set which provides a nonstandard basis for the irreducible representation (j) of SU(2). For fixed j, there exists $2j + 1$ orthonormal bases B_a since a can take $2j + 1$ distinct values $(a = 0, 1, \cdots, 2j)$.

3.2.3. Bases in Quantum Information

We now go back to quantum information. By introducing

$$|a\alpha\rangle = |j\alpha;a\rangle$$

together with the change of notations (7), the eigenvectors of v_a can be written as

$$|a\alpha\rangle = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \omega^{\frac{1}{2}(n+1)(d-n-1)a-(n+1)\alpha} |n\rangle$$

where $\omega = e^{i\frac{2\pi}{d}}$. The vector $|a\alpha\rangle$ satisfies the eigenvalue equation

$$v_a|a\alpha\rangle = \omega^{\frac{1}{2}(d-1)a-\alpha} |a\alpha\rangle$$

For fixed d and a, each eigenvector $|a\alpha\rangle$ is a linear combination of the qudits $|0\rangle, |1\rangle, \cdots, |d-1\rangle$ and the basis

$$B_a = \{|a\alpha\rangle \; : \; \alpha = 0, 1, \cdots, d-1\}$$

is an alternative to the computational basis B_d. For fixed d, we therefore have $d + 1$ remarkable bases of the d-dimensional space $\mathbb{C}^d$, namely, B_d and B_a for $a = 0, 1, \cdots, d-1$.

The operator v_a can be represented by a d-dimensional unitary matrix V_a. The matrix V_a, built on the basis B_d with the ordering $0, 1, \cdots, d-1$ for the lines and columns, reads

$$V_a = \begin{pmatrix} 0 & \omega^a & 0 & \cdots & 0 \\ 0 & 0 & \omega^{2a} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{(d-1)a} \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

The eigenvectors of V_a are

$$\phi(a\alpha) = \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} \omega^{\frac{1}{2}(n+1)(d-n-1)a-(n+1)\alpha} \phi_n$$

with $\alpha = 0, 1, \cdots, d-1$, where ϕ_n with $n = 0, 1, \cdots, d-1$ are the column vectors

$$\phi_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \phi_1 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \cdots, \quad \phi_{d-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

representing the qudits $|0\rangle, |1\rangle, \cdots, |d-1\rangle$, respectively. The vectors $\phi(a\alpha)$ satisfy the eigenvalue equation

$$V_a \phi(a\alpha) = \omega^{\frac{1}{2}(d-1)a-\alpha} \phi(a\alpha)$$

with the orthonormality relation

$$\phi(a\alpha)^\dagger \phi(a\beta) = \delta_{\alpha,\beta}$$

for $\alpha, \beta = 0, 1, \cdots, d-1$.

The matrix V_a can be diagonalized by means of the d-dimensional matrix H_a of elements

$$(H_a)_{n\alpha} = \frac{1}{\sqrt{d}} \omega^{\frac{1}{2}(n+1)(d-n-1)a-(n+1)\alpha}$$

with the lines and columns of H_a arranged from left to right and from top to bottom in the order $n, \alpha = 0, 1, \cdots, d-1$. Indeed, by introducing the $d \times d$ permutation matrix

$$P = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{pmatrix}$$

we can check that

$$(H_a P)^\dagger V_a (H_a P) = \omega^{\frac{1}{2}(d-1)a} \begin{pmatrix} \omega^0 & 0 & \cdots & 0 \\ 0 & \omega^1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}$$

from which we recover the eigenvalues of V_a. Note that the complex matrix H_a is a unitary matrix for which each entry has a modulus equal to $\frac{1}{\sqrt{d}}$. Thus, H_a is a generalized Hadamard matrix. This establishes a connection between MUBs and Hadamard matrices [35,51,52,60,64,66,73].

3.2.4. MUBs for $d = p$ (p Prime)

Going back to the case where d is arbitrary, we now examine an important property for the couple (B_a, B_d) and its generalization to couples (B_a, B_b) with $b \neq a$ ($a, b = 0, 1, \cdots, d-1$). For fixed d and a, we verify that

$$|\langle n | a\alpha \rangle| = \frac{1}{\sqrt{d}}, \quad n, \alpha = 0, 1, \cdots, d-1$$

which shows that B_a and B_d are two unbiased bases of the Hilbert space $\mathbb{C}^d$.

Other examples of unbiased bases can be obtained for $d = 2$ and 3. We easily check that the bases B_0 and B_1 for $d = 2$ are unbiased. Similarly, the bases B_0, B_1 and B_2 for $d = 3$ are mutually unbiased. Therefore, by taking into account the computational basis B_d, we end up with $d + 1 = 3$ MUBs for $d = 2$ and $d + 1 = 4$ MUBs for $d = 3$. This is in agreement with the general result according to which, in dimension d, the maximum number $d + 1$ of MUBs is attained when d is a prime number or a power of a prime number. The results for $d = 2$ and 3 can be generalized through the following proposition.

Proposition 2. *For $d = p$, p a prime number, the bases $B_0, B_1, \cdots, B_p$ form a complete set of $p + 1$ MUBs. The p^2 vectors $|a\alpha\rangle$, with $a, \alpha = 0, 1, \cdots, p - 1$, of the bases $B_0, B_1, \cdots, B_{p-1}$ are given by a single formula, namely*

$$|a\alpha\rangle = \frac{1}{\sqrt{p}} \sum_{n \in \mathbb{F}_p} \omega^{\frac{1}{2}(n+1)(p-n-1)a - (n+1)\alpha} |n\rangle, \quad \omega = e^{i\frac{2\pi}{p}} \tag{16}$$

that gives the p basis vectors for each basis B_a. In matrix form, $|a\alpha\rangle$ and $|n\rangle$ are replaced by $\phi(a\alpha)$ and ϕ_n, respectively.

Proof. First, the computational basis B_p is clearly unbiased to any of the p bases $B_0, B_1, \cdots, B_{p-1}$. Second, let us consider

$$\langle a\alpha | b\beta \rangle = \frac{1}{p} \sum_{k=0}^{p-1} e^{i\frac{\pi}{p}\{(a-b)k^2 + [(b-a)p + 2(\beta-\alpha)]k\}}$$

for $b \neq a$. The inner product $\langle a\alpha | b\beta \rangle$ can be rewritten by making use of the generalized quadratic Gauss sum [18]

$$S(u, v, w) = \sum_{k=0}^{|w|-1} e^{i\frac{\pi}{w}(uk^2 + vk)}$$

where u, v and w are integers such that u and w are co-prime, uw is non-vanishing and $uw + v$ is even. This leads to

$$\langle a\alpha | b\beta \rangle = \frac{1}{p} S(u, v, w), \quad u = a - b, \quad v = -(a - b)p - 2(\alpha - \beta), \quad w = p$$

It can be shown that $|S(u, v, w)| = \sqrt{p}$. Consequently

$$|\langle a\alpha | b\beta \rangle| = \frac{1}{\sqrt{p}}$$

for $b \neq a$ and $\alpha, \beta = 0, 1, \cdots, p - 1$. This completes the proof. $\square$

In many of the papers dealing with the construction of MUBs for $d = p$ a prime number or $d = p^m$ a power of a prime number, the explicit derivation of the bases requires the diagonalization of a set of matrices. Equation (16) arises from the diagonalization of a single matrix. It allows to derive in one step the $p(p + 1)$ vectors (or qupits, i.e., qudits with $d = p$) of a complete set of $p + 1$ MUBs in $\mathbb{C}^p$ via a single formula easily encodable on a classical computer.

Note that, for d arbitrary, the inner product $\langle a\alpha | b\beta \rangle$ can be rewritten as

$$\langle a\alpha | b\beta \rangle = \left(H_a^\dagger H_b \right)_{\alpha\beta}$$

in terms of the generalized Hadamard matrices H_a and H_b. In the case where $d = p$ is a prime number, we find that

$$\left| \left(H_a^\dagger H_b \right)_{\alpha\beta} \right| = |\langle a\alpha | b\beta \rangle| = \frac{1}{\sqrt{p}}$$

Therefore, the product $H_a^\dagger H_b$ is another generalized Hadamard matrix [64].

Finally note that the passage, given by Equation (16), from the computational basis $B_p = \{|n\rangle : n = 0, 1, \cdots, p - 1\}$ to the the basis $B_0 = \{|0\alpha\rangle : \alpha = 0, 1, \cdots, p - 1\}$ corresponds to a discrete Fourier transform. Similarly, the passage from the basis B_p to the the basis $B_a = \{|a\alpha\rangle : \alpha = 0, 1, \cdots, p - 1\}$ with $a = 1, 2, \cdots, p - 1$ corresponds to a *quadratic discrete Fourier transform*.

Example 3. $d = 2$. *In this case, relevant for a spin $j = \frac{1}{2}$ or for a qubit, we have $\omega = e^{i\pi}$ and $a, \alpha \in \mathbb{F}_2$. The matrices of the operators v_a are*

$$V_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_1, \quad V_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\sigma_2$$

The $d + 1 = 3$ MUBs B_0, B_1 and B_2 are the following:

$$B_0 : \quad |00\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |01\rangle = -\frac{|0\rangle - |1\rangle}{\sqrt{2}} = -\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$B_1 : \quad |10\rangle = i\frac{|0\rangle - i|1\rangle}{\sqrt{2}} = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}, \quad |11\rangle = -i\frac{|0\rangle + i|1\rangle}{\sqrt{2}} = -\frac{i}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}$$

$$B_2 : \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

to be compared with Equation (5).

Example 4. $d = 3$. *This case corresponds to an angular momentum $j = 1$ or to a qutrit. Here, we have $\omega = e^{i\frac{2\pi}{3}}$ and $a, \alpha \in \mathbb{F}_3$. The matrices of the operators v_a are*

$$V_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad V_1 = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & \omega^2 \\ 1 & 0 & 0 \end{pmatrix}, \quad V_2 = \begin{pmatrix} 0 & \omega^2 & 0 \\ 0 & 0 & \omega \\ 1 & 0 & 0 \end{pmatrix}$$

The $d + 1 = 4$ MUBs B_0, B_1, B_2 and B_3 are the following:

$$B_0 : \quad |00\rangle = \frac{|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \quad |01\rangle = \frac{\omega^2|0\rangle + \omega|1\rangle + |2\rangle}{\sqrt{3}}, \quad |02\rangle = \frac{\omega|0\rangle + \omega^2|1\rangle + |2\rangle}{\sqrt{3}}$$

$$B_1 : \quad |10\rangle = \frac{\omega|0\rangle + \omega|1\rangle + |2\rangle}{\sqrt{3}}, \quad |11\rangle = \frac{|0\rangle + \omega^2|1\rangle + |2\rangle}{\sqrt{3}}, \quad |12\rangle = \frac{\omega^2|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}$$

$$B_2 : \quad |20\rangle = \frac{\omega^2|0\rangle + \omega^2|1\rangle + |2\rangle}{\sqrt{3}}, \quad |21\rangle = \frac{\omega|0\rangle + |1\rangle + |2\rangle}{\sqrt{3}}, \quad |22\rangle = \frac{|0\rangle + \omega|1\rangle + |2\rangle}{\sqrt{3}}$$

$$B_3 : \quad |0\rangle, \quad |1\rangle, \quad |2\rangle$$

This can be transcribed in terms of column vectors as follows:

$$B_0 : \quad |00\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad |01\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega^2 \\ \omega \\ 1 \end{pmatrix}, \quad |02\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega \\ \omega^2 \\ 1 \end{pmatrix}$$

$$B_1 : \quad |10\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega \\ \omega \\ 1 \end{pmatrix}, \quad |11\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \quad |12\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega^2 \\ 1 \\ 1 \end{pmatrix}$$

$$B_2 : \quad |20\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega^2 \\ \omega^2 \\ 1 \end{pmatrix}, \quad |21\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} \omega \\ 1 \\ 1 \end{pmatrix}, \quad |22\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix}$$

$$B_3 : \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

To close this section, note that it is not necessary to treat separately the cases p odd and p even: Equation (16) for $|a\alpha\rangle$ is valid both for p even prime ($p = 2$) and for p odd prime. In the case where p is odd, there exists a useful alternative formula to Equation (16) as shown in the next section.

3.2.5. MUBs for $d = p$ (p Odd Prime)

In the special case where $d = p$ is an odd prime number, the formula

$$|a\alpha\rangle' = \frac{1}{\sqrt{p}} \sum_{n \in \mathbb{F}_p} \omega^{(an+\alpha)n} |n\rangle, \quad \omega = e^{i\frac{2\pi}{p}} \tag{17}$$

provides an alternative to Equation (16). Indeed, it can be shown that

$$B_a' = \{|a\alpha\rangle' \ : \ \alpha = 0, 1, \cdots, p-1\}$$

where a can take any of the values $0, 1, \cdots, p-1$ constitutes an orthonormal basis of $\mathbb{C}^d$ and that the p bases B_a' ($a = 0, 1, \cdots, p-1$) form, with the computational basis B_p, a complete set of $p+1$ MUBs. The proof, based on the properties of Gauss sums, is analogous to that given in Section 3.2.4.

It is to be emphasized that for p even prime ($p = 2$) the bases B_0', B_1' and B_2 do not form a complete set of MUBs while the proposition given in Section 3.2.4 is valid for p odd prime and equally well for p even prime. The interest of Equation (17) is that it can be easily extended in the case where $\mathbb{F}_p$ is replaced by the Galois field $\mathrm{GF}(p^m)$ with $m > 1$.

3.2.6. MUBs for d Power of a Prime

We may ask what becomes the proposition in Section 3.2.4 when the prime number p is replaced by an arbitrary (not prime) number d. In this case, Equation (16), with p replaced by d, does not provide a complete set of $d+1$ MUBs. However, it is easy to verify that the bases B_0, B_1 and B_d are three MUBs in $\mathbb{C}^d$, in agreement with the well-known result according to which the number of MUBs in $\mathbb{C}^d$, with d arbitrary, is greater than or equal to 3.

Equation (16) for $\mathbb{C}^p$ can be used for deriving a complete set of $p^m + 1$ MUBs in $\mathbb{C}^{p^m}$ (p prime and $m \geq 2$) by tensor products of order m of vectors in $\mathbb{C}^p$. The general case is very much involved. Hence, we shall limit ourselves to the case $d = 2^2$.

The case $d = 4$ corresponds to the spin angular momentum $j = \frac{3}{2}$. The four bases B_a for $a = 0, 1, 2, 3$ consisting of the vectors $|a\alpha\rangle$ calculated for $d = 4$ from Section 3.2.3 and the computational basis B_4 do not constitute a complete set of $d+1 = 5$ MUBs. Nevertheless, it is possible to find $d+1 = 5$ MUBs because $d = 2^2$ is the power of a prime number. Indeed, another way to deal with the search for MUBs in $\mathbb{C}^4$ is to consider two systems of qubits associated with the spin angular momenta $j_1 = \frac{1}{2} \Leftrightarrow d_1 = p = 2$ and $j_2 = \frac{1}{2} \Leftrightarrow d_2 = p = 2$. Then, bases of $\mathbb{C}^4$ can be constructed from tensor products $|a\alpha\rangle \otimes |b\beta\rangle$ which are eigenvectors of the operator $v_a \otimes v_b$, where v_a corresponds to the first system of qubits and v_b to the second one. Obviously, the set

$$B_{ab} = \{|a\alpha\rangle \otimes |b\beta\rangle \ : \ \alpha, \beta = 0, 1\}$$

is an orthonormal basis of $\mathbb{C}^4$. Four of the five MUBs for $d = 2^2 = 4$ can be constructed from the various bases B_{ab}. It is evident that B_{00} and B_{11} are two unbiased bases since the modulus of the inner product of $|1\alpha'\rangle \otimes |1\beta'\rangle$ by $|0\alpha\rangle \otimes |0\beta\rangle$ is

$$|\langle 0\alpha|1\alpha'\rangle \langle 0\beta|1\beta'\rangle| = \frac{1}{\sqrt{4}} = \frac{1}{\sqrt{d}}$$

A similar result holds for the two bases B_{01} and B_{10}. However, the four bases B_{00}, B_{11}, B_{01} and B_{10} are not mutually unbiased. A possible way to overcome this no-go result is to keep the bases B_{00}

and B_{11} intact and to re-organize the vectors inside the bases B_{01} and B_{10} in order to obtain four MUBs. We are thus left with the four bases

$$W_{00} \equiv B_{00}, \quad W_{11} \equiv B_{11}, \quad W_{01}, \quad W_{10}$$

which together with the computational basis B_4 give five MUBs. In detail, we have

$$
\begin{aligned}
W_{00} &= \{|0\alpha\rangle \otimes |0\beta\rangle \ : \ \alpha, \beta = 0, 1\} \\
W_{11} &= \{|1\alpha\rangle \otimes |1\beta\rangle \ : \ \alpha, \beta = 0, 1\} \\
W_{01} &= \{\lambda|0\alpha\rangle \otimes |1\beta\rangle + \mu|0\alpha \oplus 1\rangle \otimes |1\beta \oplus 1\rangle \ : \ \alpha, \beta = 0, 1\} \\
W_{10} &= \{\lambda|1\alpha\rangle \otimes |0\beta\rangle + \mu|1\alpha \oplus 1\rangle \otimes |0\beta \oplus 1\rangle \ : \ \alpha, \beta = 0, 1\}
\end{aligned}
$$

where the addition $\oplus$ should be understood modulo 4; furthermore

$$\lambda = \frac{1 - i}{2}, \quad \mu = \frac{1 + i}{2}$$

and the vectors of type $|a\alpha\rangle$ are given by Equation (16). As a résumé, only two formulas are necessary for obtaining the $d^2 = 16$ vectors $|ab; \alpha\beta\rangle$ for the bases W_{ab}, namely

$$
\begin{aligned}
W_{00}, W_{11} \ &: \ |aa; \alpha\beta\rangle = |a\alpha\rangle \otimes |a\beta\rangle \\
W_{01}, W_{10} \ &: \ |aa \oplus 1; \alpha\beta\rangle = \lambda|a\alpha\rangle \otimes |a \oplus 1\beta\rangle + \mu|a\alpha \oplus 1\rangle \otimes |a \oplus 1\beta \oplus 1\rangle
\end{aligned}
$$

for all a, α, β in $\mathbb{F}_2$. A simple development of W_{00}, W_{11}, W_{01} and W_{10} gives the following expressions.

The W_{00} basis:

$$
\begin{aligned}
|00; 00\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\
|00; 01\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\
|00; 10\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\
|00; 11\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)
\end{aligned}
$$

or in column vectors

$$
\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}
$$

The W_{11} basis:

$$
\begin{aligned}
|11; 00\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + i|0\rangle \otimes |1\rangle + i|1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\
|11; 01\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - i|0\rangle \otimes |1\rangle + i|1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\
|11; 10\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + i|0\rangle \otimes |1\rangle - i|1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\
|11; 11\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - i|0\rangle \otimes |1\rangle - i|1\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle)
\end{aligned}
$$

or in column vectors

$$
\frac{1}{2}\begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}
$$

The W_{01} basis:

$$
\begin{aligned}
|01;00\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle - i|1\rangle \otimes |0\rangle + i|1\rangle \otimes |1\rangle) \\
|01;11\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle + i|1\rangle \otimes |0\rangle + i|1\rangle \otimes |1\rangle) \\
|01;01\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle - i|1\rangle \otimes |0\rangle - i|1\rangle \otimes |1\rangle) \\
|01;10\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + i|1\rangle \otimes |0\rangle - i|1\rangle \otimes |1\rangle)
\end{aligned}
$$

or in column vectors

$$
\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -i \\ i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ i \\ i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -i \\ -i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ i \\ -i \end{pmatrix}
$$

The W_{10} basis:

$$
\begin{aligned}
|10;00\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - i|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + i|1\rangle \otimes |1\rangle) \\
|10;11\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + i|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle + i|1\rangle \otimes |1\rangle) \\
|10;01\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle + i|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle - i|1\rangle \otimes |1\rangle) \\
|10;10\rangle &= \frac{1}{2}(|0\rangle \otimes |0\rangle - i|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle - i|1\rangle \otimes |1\rangle)
\end{aligned}
$$

or in column vectors

$$
\frac{1}{2}\begin{pmatrix} 1 \\ -i \\ 1 \\ i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ i \\ -1 \\ i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix}, \quad
\frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -1 \\ -i \end{pmatrix}
$$

The computational basis:

$$
|0\rangle \otimes |0\rangle, \quad |0\rangle \otimes |1\rangle, \quad |1\rangle \otimes |0\rangle, \quad |1\rangle \otimes |1\rangle
$$

or in column vectors

$$
\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad
\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad
\begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad
\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
$$

It is to be noted that the vectors of the bases W_{00} and W_{11} are not entangled (i.e., each vector is the tensor product of two vectors) while the vectors of the bases W_{01} and W_{10} are entangled (i.e., each vector

is not the tensor product of two vectors). In fact, all the state vectors for W_{01} and W_{10} are maximally entangled (the entanglement entropy is maximum for W_{01} and W_{10} and vanishes for W_{00} and W_{11}).

Generalization of the formulas given above for two systems of qubits can be obtained in more complicated situations (two systems of qupits, three systems of qubits, etc.). The generalization of the bases W_{00} and W_{11} is immediate. The generalization of W_{01} and W_{10} can be achieved by taking linear combinations of vectors such that each linear combination is made of vectors corresponding to the same eigenvalue of the relevant tensor product of operators of type v_a.

3.3. Weyl Pairs

3.3.1. Shift and Phase Operators

Let us go back to the case d arbitrary. The matrix V_a can be decomposed as

$$V_a = XZ^a, \quad a = 0, 1, \cdots, d-1$$

where

$$X = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}, \quad \omega = e^{i\frac{2\pi}{d}}$$

The matrices X and Z satisfy

$$Z\phi_n = \omega^n \phi_n, \; n = 0, 1, \cdots, d-1, \quad X\phi_n = \phi_{n-1 \bmod d} = \begin{cases} \phi_{d-1}, \; n = 0 \\ \\ \phi_{n-1}, \; n = 1, 2, \cdots, d-1 \end{cases}$$

The linear operators corresponding to the matrices X and Z are known in quantum information as flip or shift and clock or phase operators, respectively. The unitary matrices X and Z ω-commute in the sense that

$$XZ - \omega ZX = O_d$$

In addition, they satisfy

$$X^d = Z^d = I_d$$

where I_d and O_d are the d-dimensional unity and zero matrices, respectively. The last two equations show that X and Z constitute a so-called Weyl pair [3].

Note that the Weyl pair (X, Z) can be deduced from the master matrix V_a via

$$X = V_0, \quad Z = V_0^\dagger V_1$$

which shows a further interest of the matrix V_a. Indeed, the matrix V_a condensates all that can be done with the matrices X and Z. This has been seen in Section 3.2.4 with the derivation of a single formula for the determination from V_a of a complete set of $p + 1$ MUBs when $d = p$ is prime whereas many other determinations of such a complete set needs repeated use of the matrices X and Z.

A connection between X and Z can be deduced from the expression of $(H_a P)^\dagger V_a (H_a P)$ given in Section 3.2.3. By taking $a = 0$, we obtain

$$(H_0 P)^\dagger X (H_0 P) = Z \iff X = (H_0 P) Z (H_0 P)^\dagger$$

where H_0 is the matrix of a discrete Fourier transform that allows to pass from the vectors ϕ_n ($n = 0, 1, \cdots, d-1$) to the vector $\phi(0, \alpha)$ according to

$$\phi(0, \alpha) = \sum_{n \in \mathbb{Z}_d} (H_0)_{n\alpha} \, \phi_n = (-1)^\alpha \frac{1}{\sqrt{d}} \sum_{n \in \mathbb{Z}_d} e^{-i \frac{2\pi}{d} n \alpha} \phi_n$$

cf. the expression of $\phi(a, \alpha)$ in Section 3.2.3.

3.3.2. Generalized Pauli Matrices

For d arbitrary, let us define the matrices

$$U_{ab} = X^a Z^b, \quad a, b \in \mathbb{Z}_d$$

The matrices U_{ab} belong to the unitary group $U(d)$. The d^2 matrices U_{ab} are called *generalized Pauli matrices* in dimension d. They satisfy the trace relation

$$\mathrm{tr}\left(U_{ab}{}^\dagger U_{a'b'} \right) = d \, \delta_{a,a'} \, \delta_{b,b'}$$

Thus, the set $\{U_{ab} \ : \ a, b \in \mathbb{Z}_d\}$ of unitary matrices is an orthogonal set with respect to the Hilbert-Schmidt inner product. Consequently, the d^2 pairwise orthogonal matrices U_{ab} can be used as a basis of $\mathbb{C}^{d \times d}$.

Example 5. *The case $d = 2 \iff j = \frac{1}{2}$ ($\Rightarrow \omega = e^{i\pi}$ and $a, b = 0, 1$) corresponds to the two-dimensional ordinary Pauli matrices of quantum mechanics. The matrices $X^a Z^b$ are*

$$I_2 = X^0 Z^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ X = X^1 Z^0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Z = X^0 Z^1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ Y = X^1 Z^1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

so that the matrices X and Z generate the ordinary Pauli matrices. Indeed, we have

$$I_2 = \sigma_0, \quad X = V_0 = \sigma_1, \quad Y = XZ = V_1 = -i\sigma_2, \quad Z = \sigma_3$$

in terms of the usual (Hermitian and unitary) Pauli matrices.

Example 6. *The case $d = 3 \iff j = 1$ ($\Rightarrow \omega = e^{i\frac{2\pi}{3}}$ and $a, b = 0, 1, 2$) yields nine three-dimensional matrices. More precisely, the matrices X and Z generate $I_3 = X^0 Z^0$ and*

$$X = V_0, \quad X^2, \quad Z, \quad Z^2, \quad XZ = V_1, \quad X^2 Z^2, \quad XZ^2 = V_2, \quad X^2 Z$$

In the detail, the matrices $X^a Z^b$ are

$$
X^0 Z^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \ X^0 Z^1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \ X^0 Z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix}
$$

$$
X^1 Z^0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \ X^1 Z^1 = \begin{pmatrix} 0 & \omega & 0 \\ 0 & 0 & \omega^2 \\ 1 & 0 & 0 \end{pmatrix}, \ X^1 Z^2 = \begin{pmatrix} 0 & \omega^2 & 0 \\ 0 & 0 & \omega \\ 1 & 0 & 0 \end{pmatrix}
$$

$$
X^2 Z^0 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \ X^2 Z^1 = \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \ X^2 Z^2 = \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix}
$$

They constitute a natural extension in dimension $d = 3$ of the usual Pauli matrices.

3.3.3. Weyl Pair and Groups

For arbitrary d, the Weyl pair $(X = V_0, Z = V_0^\dagger V_1)$ is a basic ingredient for generating the Pauli group P_d in d dimensions and the Lie algebra of the linear group $\mathrm{GL}(d, \mathbb{C})$ in d dimensions, groups of central interest in group theory, quantum mechanics and quantum information.

The Pauli group. For arbitrary d, let us define the matrices

$$
V_{abc} = \omega^a U_{bc} = \omega^a X^b Z^c, \quad a, b, c \in \mathbb{Z}_d, \quad \omega = \mathrm{e}^{\mathrm{i}\frac{2\pi}{d}}
$$

The matrices V_{abc} are unitary and satisfy

$$
\mathrm{tr} \left(V_{abc}{}^\dagger V_{a'b'c'} \right) = \omega^{a'-a} \, d \, \delta_{b,b'} \, \delta_{c,c'}
$$

In addition, we have the following result.

Proposition 3. *The set $\{V_{abc} \ : \ a, b, c \in \mathbb{Z}_d\}$ is a finite group of order d^3, denoted P_d, for the internal law (matrix multiplication)*

$$
V_{abc} V_{a'b'c'} = V_{a''b''c''}, \quad a'' = a + a' - cb', \quad b'' = b + b', \quad c'' = c + c'
$$

It is a non-commutative (for $d \geq 2$) nilpotent group with nilpotency class equal to 3.

The group P_d is called the Pauli group in dimension d. It is of considerable importance in quantum information, especially for quantum computation and for quantum error-correcting codes. The group P_d is a sub-group of the unitary group $\mathrm{U}(d)$. The normalizer of P_d in $\mathrm{U}(d)$ is called Clifford group (denoted as $\mathcal{C}_d$) in d dimensions. More precisely, $\mathcal{C}_d$ is the set $\{U \in \mathrm{U}(d) \ : \ U P_d U^\dagger = P_d\}$ endowed with matrix multiplication. The Pauli group P_d as well as any other invariant sub-group of $\mathcal{C}_d$ are useful for quantum error-correcting codes in the case of N-qubit systems corresponding to $d = 2^N$.

Moreover, the Pauli group is connected to the Heisenberg-Weyl group. In fact, the group P_d corresponds to a discretization of the Heisenberg-Weyl group $HW(\mathbb{R})$. From an abstract point of view, the group $HW(\mathbb{R})$ is the set $S = \{(x, y, z) \ : \ x, y, z \in \mathbb{R}\}$ equipped with the internal law $S \times S \to S$ defined via

$$
(x, y, z)(x', y', z') = (x + x' - zy', y + y', z + z')
$$

This group is a non-commutative Lie group of order 3. It is non-compact and nilpotent with a nilpotency class equal to 3. The passage from $HW(\mathbb{R})$ to P_d amounts to replace the infinite field $\mathbb{R}$ by the finite ring $\mathbb{Z}_d$ so that $HW(\mathbb{R})$ gives $HW(\mathbb{Z}_d) \equiv P_d$.

The three generators of $HW(\mathbb{R})$ are

$$H = \frac{1}{i}\frac{\partial}{\partial x}, \quad Q = \frac{1}{i}\frac{\partial}{\partial y}, \quad P = \frac{1}{i}\left(\frac{\partial}{\partial z} - y\frac{\partial}{\partial x}\right)$$

They satisfy the commutation relations

$$[Q, P]_- = iH, \quad [P, H]_- = 0, \quad [H, Q]_- = 0$$

Therefore, the Lie algebra $hw(\mathbb{R})$ of $HW(\mathbb{R})$ is a three-dimensional nilpotent Lie algebra with nilpotency class equal to 3. The commutation relations of Q, P and H are reminiscent of the Heisenberg commutation relations. As a matter of fact, the Heisenberg commutation relations correspond to an infinite-dimensional irreducible representation by Hermitian matrices of $hw(\mathbb{R})$. The Lie algebra $hw(\mathbb{R})$ also admits finite-dimensional irreducible representations at the price to abandon the Hermitian character of the representation matrices.

The linear group. The Weyl pair consisting of the generalized Pauli matrices X and Z in d dimensions can be used for constructing a basis of the Lie algebra of $U(d)$. More precisely, we have the two following propositions.

Proposition 4. *For arbitrary d, the set $\{X^a Z^b : a, b \in \mathbb{Z}_d\}$ forms a basis for the Lie algebra $gl(d, \mathbb{C})$ of the linear group $GL(d, \mathbb{C})$ or for the Lie algebra $u(d)$ of the unitary group $U(d)$. The Lie brackets of $gl(d, \mathbb{C})$ in such a basis are*

$$[X^a Z^b, X^e Z^f]_- = \sum_{i \in \mathbb{Z}_d} \sum_{j \in \mathbb{Z}_d} (ab, ef; ij) X^i Z^j$$

with the structure constants

$$(ab, ef; ij) = \delta_{i,a+e}\delta_{j,b+f}\left(\omega^{-be} - \omega^{-af}\right)$$

where $a, b, e, f, i, j \in \mathbb{Z}_d$.

Note that the commutator $[U_{ab}, U_{ef}]_- = U_{ab}U_{ef} - U_{ef}U_{ab}$ and the anti-commutator $[U_{ab}, U_{ef}]_+ = U_{ab}U_{ef} + U_{ef}U_{ab}$ of U_{ab} and U_{ef} are given by

$$[U_{ab}, U_{ef}]_{\pm} = \left(\omega^{-be} \pm \omega^{-af}\right) U_{ij}, \quad i = a + e, \quad j = b + f$$

Consequently, $[U_{ab}, U_{ef}]_- = 0$ if and only if $af - be = 0 \pmod d$ and $[U_{ab}, U_{ef}]_+ = 0$ if and only if $af - be = \frac{1}{2}d \pmod d$. Therefore, all anti-commutators $[U_{ab}, U_{ef}]_+$ are different from 0 if d is an odd integer.

Proposition 5. *For $d = p$, with p a prime number, the simple Lie algebra $sl(p, \mathbb{C})$ of the special linear group $SL(p, \mathbb{C})$ or its compact real form $su(d)$ of the special unitary group $SU(d)$ can be decomposed into a sum of $p + 1$ Abelian subalgebras of dimension $p - 1$*

$$sl(p, \mathbb{C}) = \mathcal{V}_0 \oplus \mathcal{V}_1 \oplus \cdots \oplus \mathcal{V}_p$$

where each of the $p + 1$ subalgebras $\mathcal{V}_0, \mathcal{V}_1, \cdots, \mathcal{V}_p$ is a Cartan subalgebra generated by a set of $p - 1$ commuting matrices.

A similar result holds for $d = p^m$, a power of a prime number [7,12,16,53,64].

The decomposition of $\text{sl}(p, \mathbb{C})$, called orthogonal decomposition of $\text{sl}(p, \mathbb{C})$, is trivial for $p = 2$. In fact, for $p = 2$ we have the following decomposition

$$\text{su}(2) = \sigma_1 \oplus \sigma_2 \oplus \sigma_3$$

in terms of vector space sum.

3.3.4. MUBs and the Special Linear Group

According to the orthogonal decomposition proposition, in the case where $d = p$ is a prime number (even or odd), the set $\{X^a Z^b : a, b \in \mathbb{Z}_p\} \setminus \{X^0 Z^0\}$ of cardinality $p^2 - 1$ can be partitioned into $p + 1$ subsets containing each $p - 1$ commuting matrices.

As an example, let us consider the case $d = 5$. For this case, we are left with the six following sets of four commuting matrices

$$\mathcal{V}_0 = \{01, 02, 03, 04\}, \quad \mathcal{V}_1 = \{10, 20, 30, 40\}, \quad \mathcal{V}_2 = \{11, 22, 33, 44\}$$
$$\mathcal{V}_3 = \{12, 24, 31, 43\}, \quad \mathcal{V}_4 = \{13, 21, 34, 42\}, \quad \mathcal{V}_5 = \{14, 23, 32, 41\}$$

where ab is used as an abbreviation of $X^a Z^b$.

More generally, for $d = p$ with p prime, the $p + 1$ sets of $p - 1$ commuting matrices are easily seen to be

$$
\begin{aligned}
\mathcal{V}_0 &= \{X^0 Z^a : a = 1, 2, \cdots, p - 1\} \\
\mathcal{V}_1 &= \{X^a Z^0 : a = 1, 2, \cdots, p - 1\} \\
\mathcal{V}_2 &= \{X^a Z^a : a = 1, 2, \cdots, p - 1\} \\
\mathcal{V}_3 &= \{X^a Z^{2a} : a = 1, 2, \cdots, p - 1\} \\
&\vdots \\
\mathcal{V}_{p-1} &= \{X^a Z^{(p-2)a} : a = 1, 2, \cdots, p - 1\} \\
\mathcal{V}_p &= \{X^a Z^{(p-1)a} : a = 1, 2, \cdots, p - 1\}
\end{aligned}
$$

Each of the $p + 1$ sets $\mathcal{V}_0, \mathcal{V}_1, \cdots, \mathcal{V}_p$ can be put in a one-to-one correspondence with one basis of the complete set of $p + 1$ MUBs. In fact, $\mathcal{V}_0$ is associated with the computational basis while $\mathcal{V}_1, \mathcal{V}_2, \cdots, \mathcal{V}_p$ are associated with the p remaining MUBs in view of

$$V_a \in \mathcal{V}_{a+1} = \{X^b Z^{ab} : b = 1, 2, \cdots, p - 1\}, \quad a = 0, 1, \cdots, p - 1$$

More precisely, we have

$$Z \in \mathcal{V}_0, \quad X \in \mathcal{V}_1, \quad XZ \in \mathcal{V}_2, \quad \cdots, \quad XZ^{p-1} \in \mathcal{V}_p$$

The eigenvectors of the $p + 1$ unitary operators

$$Z, \quad X, \quad XZ, \quad \cdots, \quad XZ^{p-1}$$

generate $p + 1$ MUBs (one basis is associated with each of the $p + 1$ operators).

3.4. Galois Field Approach to MUBs

The existence of a complete set of $p^m + 1$ MUBS in $\mathbb{C}^{p^m}$ (p prime and m positive integer) is an indication of a possible utility of Galois fields and Galois rings for the construction of MUBs in $\mathbb{C}^{p^m}$ (p prime, $m \geq 2$). Indeed, the passage from the case $d = p$ to the case $d = p^m$ (p prime, $m \geq 2$) can be

achieved by considering the Galois field $\mathbb{GF}(p^m)$ for p odd prime and the Galois ring $\mathbb{GR}(2^2, m)$ for $p = 2$ [2,28]. In this section, we shall deal with the construction of a complete set of $p^m + 1$ MUBs in $\mathbb{C}^{p^m}$, corresponding to the case of m qupits, via the use of the Galois field $\mathbb{GF}(p^m)$ for p odd prime and m greater than 1.

3.4.1. The Computational Basis

We first have to define the computational basis B_{p^m} in the framework of $\mathbb{GF}(p^m)$, p odd prime and $m \geq 2$. The vectors of the basis B_{p^m} of the Hilbert space $\mathbb{C}^{p^m}$ can be labeled by the elements x of the Galois field $\mathbb{GF}(p^m)$. This can be done in two ways according to as the elements x are taken in the monomial form ($x = 0$, α^ℓ with $\ell = 1, 2, \cdots, p^m - 1$) or in the polynomial form ($x = [x_0 x_1 \cdots x_{m-1}]$ with $x_0, x_1, \cdots, x_{m-1} \in \mathbb{F}_p$). In both cases, we have

$$B_{p^m} = \{|0\rangle \text{ or } \phi_0, \quad |1\rangle \text{ or } \phi_1, \quad \cdots, \quad |p^m - 1\rangle \text{ or } \phi_{p^m-1}\}$$

in terms of vectors or column vectors. More precisely, this can be achieved as follows.

- In the monomial form, we define the vectors of B_{p^m} via the correspondences

$$x = 0 \mapsto |0\rangle \text{ or } \phi_0, \quad x = \alpha^\ell \mapsto |\ell\rangle \text{ or } \phi_\ell \text{ with } \ell = 1, 2, \cdots, p^m - 1$$

  where α is a primitive element of $\mathbb{GF}(p^m)$.
- In the polynomial form, we can range the vectors of B_{p^m} in the order $0, 1, \cdots, p^m - 1$ by adopting the lexicographical order for the elements $[x_0 x_1 \cdots x_{m-1}]$.

These notations are reminiscent of those employed for the computational basis

$$B_p = \{|0\rangle \text{ or } \phi_0, \quad |1\rangle \text{ or } \phi_1, \quad \cdots, \quad |p - 1\rangle \text{ or } \phi_{p-1}\}$$

corresponding to the limit case $m = 1$.

3.4.2. Shift and Phase Operators for $\mathbb{GF}(p^m)$

The notion of Weyl pair can be extended to any Galois field $\mathbb{GF}(p^m)$ with p (even or odd) prime and $m \geq 2$. Let x and y be two elements of $\mathbb{GF}(p^m)$ and ϕ_y be the basis column vector of B_{p^m} associated with y. For fixed x, we define the matrices $\hat{X}_x$ (shift operators) and $\hat{Z}_x$ (phase operators) via the actions

$$\hat{X}_x \phi_y = \phi_{y-x}, \quad \hat{Z}_x \phi_y = \chi(xy)\phi_y = e^{i\frac{2\pi}{p}\text{Tr}(xy)}\phi_y$$

where y is arbitrary. One easily verifies the properties

$$\hat{X}_{x+y} = \hat{X}_x \hat{X}_y = \hat{X}_y \hat{X}_x, \quad \hat{Z}_{x+y} = \hat{Z}_x \hat{Z}_y = \hat{Z}_y \hat{Z}_x$$

and

$$\hat{X}_x \hat{Z}_y - \chi(xy)\hat{Z}_y \hat{X}_x = O_{p^m}, \quad \chi(xy) = e^{i\frac{2\pi}{p}\text{Tr}(xy)}$$

In the limit case $m = 1$ (i.e., for the base field $\mathbb{F}_p$) the matrices

$$X = \hat{X}_1, \quad Z = \hat{Z}_1$$

corresponding to $x = y = 1$ satisfy

$$XZ - e^{i\frac{2\pi}{p}}ZX = O_p$$

to be compared with the relations satisfied by the Weyl pair (X, Z) defined in Section 3.3.1.

3.4.3. Bases in the Frame of $\mathbb{GF}(p^m)$

We might use the Weyl pair (X_x, Z_y) defined in the framework of $\mathbb{GF}(p^m)$, see Section 3.4.2, for determining a complete set of $p^m + 1$ MUBs in $\mathbb{C}^{p^m}$ in a way similar to that used for $m = 1$ with the help of the matrix V_a for a in $\mathbb{F}_p$. However, it is quicker to start from Equation (17) giving MUBs in $\mathbb{C}^p$ in order to generate a formula for $\mathbb{C}^{p^m}$ giving back Equation (17) in $\mathbb{C}^p$ in the limit case $m = 1$. In this direction, a possible way to pass from the basis vector

$$\frac{1}{\sqrt{p}} \sum_{x \in \mathbb{F}_p} e^{i\frac{2\pi}{p}(ax+\alpha)x} |x\rangle$$

of $\mathbb{C}^p$ to a basis vector of $\mathbb{C}^{p^m}$ is to replace

$$e^{i\frac{2\pi}{p}(ax+\alpha)x}, \quad a, \alpha, x \in \mathbb{F}_p$$

by

$$\chi(ax^2 + \alpha x) = e^{i\frac{2\pi}{p}\operatorname{Tr}(ax^2+\alpha x)}, \quad a, \alpha, x \in \mathbb{GF}(p^m)$$

where χ is the canonical additive character of $\mathbb{GF}(p^m)$. This yields the two following propositions.

Proposition 6. *For p odd prime and $m \geq 2$, the set*

$$B_a = \{ |a\alpha\rangle \ : \ \alpha \in \mathbb{GF}(p^m) \}$$

where

$$|a\alpha\rangle = \frac{1}{\sqrt{p^m}} \sum_{x \in \mathbb{GF}(p^m)} e^{i\frac{2\pi}{p}\operatorname{Tr}(ax^2+\alpha x)} |x\rangle, \quad a \in \mathbb{GF}(p^m)$$

constitutes an orthonormal basis of $\mathbb{C}^{p^m}$.

Proof. See the proof of the next proposition. □

Note that for $m = 1$

$$\operatorname{Tr}(ax^2 + \alpha x) = ax^2 + \alpha x$$

so that the vector $|a\alpha\rangle$ coincides with the vector $|a\alpha\rangle'$ derived in Section 3.2.5. This explains why we chose to extend Equation (17) valid for $\mathbb{C}^p$ to the case $\mathbb{C}^{p^m}$. Indeed, the same kind of extension applied to Equation (16) is not possible since $\operatorname{Tr}[\frac{1}{2}n(p-n)a + n\alpha]$ does not make sense.

3.4.4. MUBs in the Frame of $\mathbb{GF}(p^m)$

Proposition 7. *For p odd prime and $m \geq 2$, the p^m bases B_a, a ranging in $\mathbb{GF}(p^m)$, constitute with the computational basis B_{p^m} a complete set of $p^m + 1$ MUBs in $\mathbb{C}^{p^m}$.*

Proof. Let $|a\alpha\rangle$ and $|b\beta\rangle$ two vectors belonging to the bases B_a and B_b, respectively. We have

$$\langle a\alpha|b\beta\rangle = \frac{1}{p^m} \sum_{x \in \mathbb{GF}(p^m)} e^{i\frac{2\pi}{p}\operatorname{Tr}[(b-a)x^2+(\beta-\alpha)x]}, \quad a, b, \alpha, \beta \in \mathbb{GF}(p^m)$$

By using [2,4,18]

$$\left| \sum_{x \in \mathbb{GF}(p^m)} e^{i\frac{2\pi}{p}\operatorname{Tr}(ux^2+vx)} \right| = \sqrt{p^m}, \quad u \in \mathbb{GF}(p^m)^*, \quad v \in \mathbb{GF}(p^m)$$

(valid for p odd prime), we obtain

$$|\langle a\alpha|b\beta\rangle| = \begin{cases} \delta_{\alpha,\beta} \text{ if } b = a \\[2ex] \frac{1}{\sqrt{p^m}} \text{ if } b \neq a \end{cases}$$

or in compact form

$$|\langle a\alpha|b\beta\rangle| = \delta_{a,b}\delta_{\alpha,\beta} + \frac{1}{\sqrt{p^m}}(1 - \delta_{a,b})$$

which shows that B_a is an orthonormal basis and that the couple (B_a, B_b) with $b \neq a$ is a couple of unbiased bases. Of course, each basis B_a is unbiased to the computational basis B_{p^m}. We thus end up with a total of $p^m + 1$ MUBs as desired. $\square$

The previous result applies in the limit case $m = 1$ for which we recover the $p + 1$ MUBs in $\mathbb{C}^p$.

3.5. Galois Ring Approach to MUBs

In dimension $d = 2^m$, $m \geq 2$, the use of the Galois field $\mathbb{GF}(2^m)$ for constructing a complete set of $2^m + 1$ MUBs in $\mathbb{C}^{2^m}$ according to the method employed in Section 3.4 for $d = p^m$, p odd prime, would lead to a no-win situation because $\gcd(2, 2^m) \neq 1$ (while $\gcd(2, p^m) = 1$ for p odd prime). For $d = 2^m$, which corresponds to the case of m qubits, we can use the Galois ring $\mathbb{GR}(2^2, m)$, denoted R_{4^m} too, for constructing MUBs in $\mathbb{C}^{2^m}$.

3.5.1. Bases in the Frame of $\mathbb{GR}(2^2, m)$

We start with the residue class ring

$$\mathbb{GR}(2^2, m) = \mathbb{Z}_{2^2}[\xi]/\langle P_m(\xi)\rangle$$

where $P_m(x)$ is a monic basic irreducible polynomial of degree m (i.e., its restriction $\overline{P_m(x)} = P_m(x)$ modulo 2 is irreducible over $\mathbb{Z}_2$). The 2^m vectors of the computational basis B_{2^m} are labeled by the 2^m elements of the Teichmüller set T_m associated with the ring $\mathbb{Z}_{2^2}[\xi]/\langle P_m(\xi)\rangle$. Thus

$$B_{2^m} = \{|x\rangle \ : \ x \in T_m\}$$

(the set T_m and the ring $\mathbb{GR}(2^2, m)$ contain 2^m and 4^m elements, respectively).

Proposition 8. *For a and α in T_m, let*

$$|a\alpha\rangle = \frac{1}{\sqrt{2^m}}\sum_{x \in T_m}\chi[(a + 2\alpha)x]|x\rangle = \frac{1}{\sqrt{2^m}}\sum_{x \in T_m}e^{i\frac{2\pi}{4}\operatorname{Tr}(ax+2\alpha x)}|x\rangle = \frac{1}{\sqrt{2^m}}\sum_{x \in T_m}i^{\operatorname{Tr}(ax+2\alpha x)}|x\rangle$$

where χ is an additive character vector of $\mathbb{GR}(2^2, m)$ and the trace takes its values in $\mathbb{Z}_4$. For fixed a in T_m, the set

$$B_a = \{|a\alpha\rangle \ : \ \alpha \in T_m\}$$

constitutes an orthonormal basis of $\mathbb{C}^{2^m}$.

Proof. See the proof of the next proposition. $\square$

Note that for $m = 1$

$$\operatorname{Tr}(ax + 2\alpha x) = ax + 2\alpha x$$

so that

$$|a\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \mathbb{F}_2} i^{ax+2\alpha x} |x\rangle \tag{18}$$

to be compared with the vector

$$|a\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \mathbb{F}_2} e^{i\frac{2\pi}{2}[\frac{1}{2}ax(2-x)+\alpha x]} |1-x\rangle = \frac{1}{\sqrt{2}} \sum_{x \in \mathbb{F}_2} i^{ax(2-x)+2\alpha x} |1-x\rangle \tag{19}$$

given by Equation (16). In view of the fact that

$$i^{ax+2\alpha x} = i^{ax(2-x)+2\alpha x}$$

for $x = 0$ and $x = 1$, the two vectors $|a\alpha\rangle$ in Equations (18) and (19) are the same up to an interchange of the vectors $|0\rangle$ and $|1\rangle$. $\quad\square$

3.5.2. MUBs in the Frame of $\mathbb{GR}(2^2, m)$

Proposition 9. *The 2^m bases B_a, with $m \geq 2$ and a ranging in the Teichüller set T_m associated with the Galois ring $\mathbb{GR}(2^2, m)$, constitute with the computational basis B_{2^m} a complete set of $2^m + 1$ MUBs in $\mathbb{C}^{2^m}$.*

Proof. Let $|a\alpha\rangle$ and $|b\beta\rangle$ two vectors belonging to the bases B_a and B_b, respectively. We have

$$\langle a\alpha | b\beta \rangle = \frac{1}{2^m} \sum_{x \in T_m} e^{i\frac{\pi}{2}\text{Tr}[(b-a+2\beta-2\alpha)x]}$$

By using [2,4,18]

$$\left| \sum_{x \in T_m} e^{i\frac{\pi}{2}\text{Tr}(ux)} \right| = \begin{cases} 0 \text{ if } u \in 2T_m, \ u \neq 0 \\ \\ 2^m \text{ if } u = 0 \\ \\ \sqrt{2^m} \text{ otherwise} \end{cases}$$

we obtain

$$|\langle a\alpha | b\beta \rangle| = \begin{cases} \delta_{\alpha,\beta} \text{ if } b = a \\ \\ \frac{1}{\sqrt{2^m}} \text{ if } b \neq a \end{cases}$$

or in compact form

$$|\langle a\alpha | b\beta \rangle| = \delta_{a,b}\delta_{\alpha,\beta} + \frac{1}{\sqrt{2^m}}(1 - \delta_{a,b})$$

which shows that B_a is an orthonormal basis and that the couple (B_a, B_b) with $b \neq a$ is a couple of unbiased bases. Of course, each basis B_a is unbiased to the computational basis B_{2^m}. We thus end up with a total of $2^m + 1$ MUBs and we are done. $\quad\square$

The previous result applies in the limit case $m = 1$ for which we can recover the $2 + 1$ MUBs in $\mathbb{C}^2$.

3.5.3. One-Qubit System

For $m = 1$, the $2^m = 2$ vectors of the computational basis B_2 are labeled with the help of the two elements of the Teichmüller set $T_1 = \mathbb{Z}_2$ of the Galois ring $\mathbb{GR}(2^2, 1) = \mathbb{Z}_{2^2}$. Thus, the basis B_2 is

$$B_2 \quad : \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

The vectors $|a\alpha\rangle$ of the basis B_a ($a \in T_1$) are given by (see Section 3.5.1)

$$|a\alpha\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{1} \mathrm{i}^{(a+2\alpha)x} |x\rangle, \quad \alpha \in T_1 = \{0, 1\}$$

This yields the two unbiased bases

$$B_0 \quad : \quad |00\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |01\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$B_1 \quad : \quad |10\rangle = \frac{|0\rangle + \mathrm{i}|1\rangle}{\sqrt{2}}, \quad |11\rangle = \frac{|0\rangle - \mathrm{i}|1\rangle}{\sqrt{2}}$$

which, together with the computational basis B_2, form a complete set of $2 + 1 = 3$ MUBs in $\mathbb{C}^2$. Note that the bases B_0 and B_1 are in agreement (up to phase factors and a rearrangement of the vectors inside B_1) with the bases B_0 and B_1 derived in Section 3.2.4.

3.5.4. Two-Qubit System

For $m = 2$, the $2^m = 4$ vectors of the computational basis B_4 are labeled with the help of the four elements of the Teichmüller set $T_2 = \{0, \beta^1, \beta^2 = 3 + 3\beta, \beta^3 = 1\}$ of the Galois ring $\mathbb{GR}(2^2, 2)$ (here, we use β instead of α in order to avoid confusion with the index α in $|a\alpha\rangle$). Thus, the basis B_4 is

$$B_4 \quad : \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |\beta^1 \text{ or } 1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |\beta^2 \text{ or } 2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |\beta^3 \text{ or } 3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

The vectors $|a\alpha\rangle$ of the basis B_a ($a = 0$, β^1 or 1, β^2 or 2, β^3 or 3) are given by (see Section 3.5.1)

$$|a\alpha\rangle = \frac{1}{2} \sum_{x \in T_2} \mathrm{i}^{\mathrm{Tr}(ax + 2\alpha x)} |x\rangle, \quad \alpha \in T_2 = \{0, \beta^1, \beta^2 = 3 + 3\beta, \beta^3 = 1\}$$

with

$$\mathrm{Tr}(ax + 2\alpha x) = ax + 2\alpha x + \phi(ax + 2\alpha x)$$

where ϕ is the generalized Frobenius map $\mathbb{GR}(2^2, 2) \rightarrow \mathbb{GR}(2^2, 2)$. The correspondence between the indexes a, α in $|a\alpha\rangle$ and the elements $0, \beta^1, \beta^2, \beta^3$ of T_2 is as follows

$$0 \leftrightarrow a \text{ or } \alpha = 0, \ \beta^1 \leftrightarrow a \text{ or } \alpha = 1, \ \beta^2 \leftrightarrow a \text{ or } \alpha = 2, \ \beta^3 \leftrightarrow a \text{ or } \alpha = 3$$

This yields the four unbiased bases

$$
B_0 \quad : \quad |00\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \ |01\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \ |02\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \ |03\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}
$$

$$
B_1 \quad : \quad |12\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ 1 \\ i \end{pmatrix}, \ |11\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -1 \\ i \end{pmatrix}, \ |13\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ 1 \\ -i \end{pmatrix}, \ |10\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -1 \\ -i \end{pmatrix}
$$

$$
B_2 \quad : \quad |21\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -i \\ i \end{pmatrix}, \ |22\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ i \\ i \end{pmatrix}, \ |20\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -i \\ -i \end{pmatrix}, \ |23\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ i \\ -i \end{pmatrix}
$$

$$
B_3 \quad : \quad |33\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}, \ |32\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \ |31\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix}, \ |30\rangle = \frac{1}{2}\begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}
$$

We thus end up with $4 + 1 = 5$ bases (B_0 to B_4) which form a complete set of MUBs in $\mathbb{C}^4$. Note that the bases B_0, B_1, B_2 and B_3 coincide with the bases W_{00}, W_{10}, W_{01} and W_{11} derived from tensor products, respectively; for the purpose of comparison, the vectors $|a\alpha\rangle$ are listed in the same order for each of the couples (B_0, W_{00}), (B_1, W_{10}), (B_2, W_{01}) and (B_3, W_{11}), see Section 3.2.6.

4. Closing Remarks

During the last two decades, quantum information and quantum computing have been the object of considerable progresses both in theoretical and experimental physical sciences, scientific engineering, discrete mathematics and quantum informatics. In the present days, there exit several quantum computer languages and, although quantum devices are mainly developed in academic and private laboratories, the scientific community has access to some quantum computers (e.g., access to the 5-qubit quantum computer of the IBM Quantum Experience [79]) and to quantum simulators (e.g., access to the 41-qubit ATOS Quantum Learning Machine [80]). In the medium term, the accent shall be put, among others, on (i) the development of new quantum algorithms that outperform classical ones, (ii) the production of qubits robust to decoherence (with coherence time greater than 500 ms), (iii) the increase of the lifetime of quantum memories, (iv) the development of quantum networks working over a few thousands of kilometres (v) the realization of 50–100 qubit computers, and (vi) the test of quantum supremacy. There is a long way before the realization of a universal quantum computer!

From the side of the mathematical aspects of MUBs, some further developments and a few open problems should be mentioned. It would be interesting to see if Cayley-Dickson algebras of dimension $d = 2^N$ could be used for providing a geometrical approach to entanglement of N qubits with $N > 3$. Furthermore, the problem of the determination of the maximum number $N(d)$ of MUBs in composite dimension d is still an unsolved problem (except in the case where d is a power of a prime number). The two conjectures listed in Section 3.1.3 do not very much help, probably because they lead to two equivalent problems for which the solutions are as difficult to find as those of the initial problem. As far as the second conjecture is concerned, the recent work [76] on orthogonal decompositions of $sl(n, R)$ over a finite commutative ring with identity R is very appealing. Finally, even in the simplest case where $d = 6$, the maximum number $N(6)$ of MUBs is not known (to the best of the author knowledge). However, for $d = 6$ there are numerous numerical evidences that $N(6) = 3$ [19,37,52,54,59,60,70,71]. The number $N(6) = 3$ is equal indeed to the number of *weak* mutually unbiased bases associated

with the smallest prime divisor of 6 (the recently introduced notion of weak MUBs in dimension d corresponds to the Definition (14) where $\sqrt{d}$ is replaced by $\sqrt{f}$ where f is a prime divisor of d [69,75]).

References

1. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2003.
2. Kibler, M.R. *Galois Fields and Galois Rings Made Easy*; ISTE Press–Elsevier: London/Oxford, UK, 2017.
3. Weyl, H. *The Theory of Groups and Quantum Mechanics*; Dover Publications: New York, NY, USA, 1931.
4. Weil, A. On some exponential sums. *Proc. Natl. Acad. Sci. USA* **1948**, *34*, 204–207. [CrossRef] [PubMed]
5. Schwinger, J. Unitary operator bases. *Proc. Natl. Acad. Sci. USA* **1960**, *46*, 570–579. [CrossRef] [PubMed]
6. Ivanović, I.D. Geometrical description of quantal state determination. *J. Phys. A Math. Gen.* **1981**, *14*, 3241–3245. [CrossRef]
7. Kostrikin, A.I.; Kostrikin, I.A.; Ufnarovskiĭ, V.A. Orthogonal decompositions of simple Lie algebras (type A_n). *Trudy Mat. Inst. Steklov* **1981**, *158*, 105–120. (In Russian)
8. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802. [CrossRef]
9. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
10. Wootters, W.K. Quantum mechanics without probability amplitudes. *Found. Phys.* **1986**, *16*, 391–405. [CrossRef]
11. Wootters, W.K. A Wigner function formulation of finite-state quantum mechanics. *Ann. Phys. (N. Y.)* **1987**, *176*, 1–21. [CrossRef]
12. Patera, J.; Zassenhaus, H. The Pauli matrices in n dimensions and finest gradings of simple Lie algebras of type A_{n-1}. *J. Math. Phys.* **1988**, *29*, 665–673. [CrossRef]
13. Lambert, D.; Kibler, M. An algebraic and geometric approach to non-bijective quadratic transformations. *J. Phys. A Math. Gen.* **1988**, *21*, 307–343. [CrossRef]
14. Wootters, W.K.; Fields, B.D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys. (N. Y.)* **1989**, *191*, 363–381. [CrossRef]
15. Bennett, C.H.; Brassard, G.; Crépeau, C.; Jozsa, R.; Peres, A.; Wootters, W.K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895. [CrossRef] [PubMed]
16. Kostrikin, A.I.; Tiep, P.H. *Orthogonal Decompositions and Integral Lattices*; Walter de Gruyter: Berlin, Germany, 1994.
17. Calderbank, A.R.; Cameron, P.J.; Kantor, W.M.; Seidel, J.J. $\mathbb{Z}_4$–Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. Lond. Math. Soc.* **1997**, *75*, 436–480. [CrossRef]
18. Berndt, B.C.; Evans, R.J.; Williams, K.S. *Gauss and Jacobi Sums*; Wiley: New York, NY, USA, 1998.
19. Zauner, G. Quantendesigns: Grundzüge einer Nichtcommutativen Designtheorie. Bachelor's Thesis, University of Wien, Wien, Austria, 1999.
20. Englert, B.-G.; Aharonov, Y. The mean king's problem: Prime degrees of freedom. *Phys. Lett. A* **2001**, *284*, 1–5. [CrossRef]
21. Mosseri, R.; Dandoloff, R. Geometry of entangled states, Bloch spheres and Hopf fibrations. *J. Phys. A Math. Gen.* **2001**, *34*, 10243–10252. [CrossRef]
22. Bandyopadhyay, S.; Boykin, P.O.; Roychowdhury, V.; Vatan, F. A new proof for the existence of mutually unbiased bases. *Algorithmica* **2002**, *34*, 512–528.

23. Lawrence, J.; Brukner, C.; Zeilinger, A. Mutually unbiased binary observable sets on N qubits. *Phys. Rev. A* **2002**, *65*, 032320. [CrossRef]

24. Chaturvedi, S. Aspects of mutually unbiased bases in odd prime power dimensions. *Phys. Rev. A* **2002**, *65*, 044301. [CrossRef]

25. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of quantum key distribution using *d*-level systems. *Phys. Rev. Lett.* **2002**, *88*, 127902. [CrossRef] [PubMed]

26. Aravind, P.K. Solution to the King's problem in prime power dimensions. *Z. Naturforsch.* **2003**, *58*, 85–92. [CrossRef]

27. Lawrence, J. Mutually unbiased bases and trinary operator sets for N qutrits. *Phys. Rev. A* **2004**, *70*, 012302. [CrossRef]

28. Klappenecker, A.; Rötteler, M. Constructions of mutually unbiased bases. *Lect. Notes Comput. Sci.* **2004**, *2948*, 137–144.

29. Gibbons, K.S.; Hoffman, M.J.; Wootters, W.K. Discrete phase space based on finite fields. *Phys. Rev. A* **2004**, *70*, 062101. [CrossRef]

30. Pittenger, A.O.; Rubin, M.H. Mutually unbiased bases, generalized spin matrices and separability. *Linear Algebr. Appl.* **2004**, *390*, 255–278. [CrossRef]

31. Vourdas, A. Quantum systems with finite Hilbert space. *Rep. Prog. Phys.* **2004**, *67*, 267–320. [CrossRef]

32. Saniga, M.; Planat, M.; Rosu, H. Mutually unbiased bases and finite projective planes. *J. Opt. B Quantum Semiclass. Opt.* **2004**, *6*, L19–L20. [CrossRef]

33. Hayashi, A.; Horibe, M.; Hashimoto, T. Mean king's problem with mutually unbiased bases and orthogonal Latin squares. *Phys. Rev. A* **2005**, *71*, 052331. [CrossRef]

34. Paz, J.P.; Roncaglia, A.J.; Saraceno, M. Qubits in phase space: Wigner-function approach to quantum-error correction and the mean-king problem. *Phys. Rev. A* **2005**, *72*, 012309. [CrossRef]

35. Wocjan, P.; Beth, T. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.* **2005**, *5*, 93–101.

36. Archer, C. There is no generalization of known formulas for mutually unbiased bases. *J. Math. Phys.* **2005**, *46*, 022106. [CrossRef]

37. Grassl, M. On SIC-POVMs and MUBs in dimension 6. In Proceedings of the ERATO Conference on Quantum Information Science (EQIS'04), Tokyo, Japan, 1–5 September 2004; pp. 60–61.

38. Grassl, M. Tomography of quantum states in small dimensions. *Electron. Notes Discret. Math.* **2005**, *20*, 151–164. [CrossRef]

39. Klappenecker, A.; Rötteler, M. Mutually unbiased bases are complex projective 2-designs. In Proceedings of the 2005 IEEE International Symposium on Information Theory, Adelaide, Australia, 4–9 September 2005; pp. 1740–1744.

40. Bengtsson, I.; Ericsson, A.A. Mutually unbiased bases and the complementary polytope. *Open Syst. Inf. Dyn.* **2005**, *12*, 107–120. [CrossRef]

41. Durt, T. About mutually unbiased bases in even and odd prime power dimensions. *J. Phys. A Math. Gen.* **2005**, *38*, 5267–5283. [CrossRef]

42. Pittenger, A.O.; Rubin, M.H. Wigner functions and separability for finite systems. *J. Phys. A Math. Gen.* **2005**, *38*, 6005–6036. [CrossRef]

43. Durt, T. About the Mean King's problem and discrete Wigner distributions. *Int. J. Mod. Phys. B* **2006**, *20*, 1742–1760. [CrossRef]

44. Kibler, M.R. Angular momentum and mutually unbiased bases. *Int. J. Mod. Phys. B* **2006**, *20*, 1792–1801. [CrossRef]

45. Kibler, M.R.; Planat, M. A SU(2) recipe for mutually unbiased bases. *Int. J. Mod. Phys. B* **2006**, *20*, 1802–1807. [CrossRef]

46. Vourdas, A. Galois quantum systems, irreducible polynomials and Riemann surfaces. *J. Math. Phys.* **2006**, *47*, 092104. [CrossRef]

47. Heath, R.W.; Strohmer, T.; Paulraj, A.J. On quasi-orthogonal signatures for CDMA systems. *IEEE Trans. Inf. Theory* **2006**, *52*, 1217–1226. [CrossRef]

48. Vourdas, A. Quantum systems in finite Hilbert space: Galois fields in quantum mechanics. *J. Phys. A Math. Theor.* **2007**, *40*, R285–R331. [CrossRef]

49. Klimov, A.B.; Romero, J.L.; Björk, G.; Sánchez-Soto, L.L. Geometrical approach to mutually unbiased bases. *J. Phys. A Math. Theor.* **2007**, *40*, 3987–3998. [CrossRef]

50. Šulc, P.; Tolar, J. Group theoretical construction of mutually unbiased bases in Hilbert spaces of prime dimensions. *J. Phys. A Math. Theor.* **2007**, *40*, 15099. [CrossRef]

51. Aschbacher, M.; Childs, A.M.; Wocjan, P. The limitations of nice mutually unbiased bases. *J. Algebr. Comb.* **2007**, *25*, 111–123. [CrossRef]

52. Bengtsson, I.; Bruzda, W.; Ericsson, A.A.; Larsson, J.-A.A.; Tadej, W.; Zyczkowski, K. Mutually unbiased bases and Hadamard matrices of order six. *J. Math. Phys.* **2007**, *48*, 052106. [CrossRef]

53. Boykin, P.O.; Sitharam, M.; Tiep, P.H.; Wocjan, P. Mutually unbiased bases and orthogonal decompositions of Lie algebras. *Quantum Inf. Comput.* **2007**, *7*, 371–382.

54. Butterley, P.; Hall, W. Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Phys. Lett. A* **2007**, *369*, 5–8. [CrossRef]

55. Björk, G.; Romero, J.L.; Klimov, A.B.; Sánchez-Soto, L.L. Mutually unbiased bases and discrete Wigner functions. *J. Opt. Soc. Am. B* **2007**, *24*, 371–378. [CrossRef]

56. Klimov, A.B.; Muñoz, C.; Fernández, A.; Saavedra, C. Optimal quantum-state reconstruction for cold trapped ions. *Phys. Rev. A* **2008**, *77*, 060303(R). [CrossRef]

57. Svetlichny, G. Feynman's integral is about mutually unbiased bases. *arXiv* **2008**, arXiv:0708.3079v3.

58. Kibler, M.R. Variations on a theme of Heisenberg, Pauli and Weyl. *J. Phys. A Math. Theor.* **2008**, *41*, 375302. [CrossRef]

59. Brierley, S.; Weigert, S. Maximal sets of mutually unbiased quantum states in dimension six. *Phys. Rev. A* **2008**, *78*, 042312. [CrossRef]

60. Brierley, S.; Weigert, S. Constructing mutually unbiased bases in dimension six. *Phys. Rev. A* **2009**, *79*, 052316. [CrossRef]

61. Appleby, D.M. SIC-POVMS and MUBS: Geometrical relationships in prime dimension. In Proceedings of the AIP Conference, Foundations of Probability and Physics-5, San Diego, CA, USA, 26–31 May 2009; Volume 1101, pp. 223–232.

62. Albouy, O. The isotropic lines of $\mathbb{Z}_d^2$. *J. Phys. A Math. Theor.* **2009**, *42*, 072001. [CrossRef]

63. Tolar, J.; Chadzitaskos, G. Feynman's path integral and mutually unbiased bases. *J. Phys. A Math. Theor.* **2009**, *42*, 245306. [CrossRef]

64. Kibler, M.R. An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, the unitary group and the Pauli group. *J. Phys. A Math. Theor.* **2009**, *42*, 353001. [CrossRef]

65. Durt, T.; Englert, B.-G.; Bengtsson, I.; Zyczkowski, K. On mutually unbiased bases. *Int. J. Quantum Inf.* **2010**, *8*, 535–640. [CrossRef]

66. Diţă, P. Hadamard matrices from mutually unbiased bases. *J. Math. Phys.* **2010**, *51*, 072202. [CrossRef]

67. Zauner, G. Quantum designs: Foundations of a noncommutative design theory. *Int. J. Quantum Inf.* **2011**, *9*, 445–507. [CrossRef]

68. Daoud, M.; Kibler, M.R. Phase operators, phase states and vector phase states for SU_3 and $SU_{2,1}$. *J. Math. Phys.* **2011**, *52*, 082101. [CrossRef]

69. Shalaby, M.; Vourdas, A. Weak mutually unbiased bases. *J. Phys. A Math. Theor.* **2012**, *45*, 052001. [CrossRef]

70. McNulty, D.; Weigert, S. The limited role of mutually unbiased product bases in dimension six. *J. Phys. A Math. Theor.* **2012**, *45*, 102001. [CrossRef]

71. McNulty, D.; Weigert, S. All mutually unbiased product bases in dimension six. *J. Phys. A Math. Theor.* **2012**, *45*, 135307. [CrossRef]

72. Ghiu, I. Generation of all sets of mutually unbiased bases for three-qubit systems. *Phys. Scr.* **2013**, *153*, 014027. [CrossRef]

73. Goyeneche, D. Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6. *J. Phys. A Math. Theor.* **2013**, *46*, 105301. [CrossRef]

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

75. Olupitan, T.; Lei, C.; Vourdas, A. An analytic function approach to weak mutually unbiased bases. *Ann. Phys. (N. Y.)* **2016**, *371*, 1–19. [CrossRef]

76. Sriwongsa, S.; Zou, Y.M. Orthogonal abelian Cartan subalgebra decomposition of sl_n over a finite commutative ring. *Linear Multilinear Algebra* **2018**. [CrossRef]

77. Rao, H.S.S.; Sirsi, S.; Bharath, K. Mutually disjoint, maximally commuting set of physical observables for optimum state determination. *arXiv* **2018**, arXiv:1809.06762.

78. Trifa, Y. Utilisation et construction de bases mutuellement non biaisées en théorie de l'information quantique. In *Rapport de Stage, IPN Lyon—ENS Lyon*; IPN: Lyon, France; ENS: Lyon, France, 2018.

79. IBM Quantum Experience. Available online: https://quantumexperience.ng.bluemix.net/qx/experience (accessed on 21 November 2018).

80. ATOS Quantum Learning Machine. Available online: https://atos.net/en/insights-and-innovation/quantum-computing/atos-quantum (accessed on 21 November 2018).