Optimal qudit operator bases for efficient characterization of quantum gates

2014 J. Phys. A: Math. Theor. 47 385305

(http://iopscience.iop.org/1751-8121/47/38/385305)

IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor **47** (2014) 385305 (13pp) doi:10.1088/1751-8113/47/38/385305

Optimal qudit operator bases for efficient characterization of quantum gates

Daniel M Reich[1], Giulia Gualdi[2,3] and Christiane P Koch[1]

[1] Theoretische Physik, Universität Kassel, Heinrich-Plett-Str. 40, D-34132 Kassel, Germany
[2] Dipartimento di Fisica ed Astronomia, Università di Firenze, Via Sansone 1, I-50019 Sesto Fiorentino, Italy
[3] QSTAR, Largo Enrico Fermi 2, I-50125 Firenze, Italy

E-mail: christiane.koch@uni-kassel.de

Received 14 April 2014, revised 7 August 2014
Accepted for publication 11 August 2014
Published 10 September 2014

Abstract

For target unitary operations which preserve the basis of measurement operators, the average fidelity of the corresponding N-qubit gate can be determined efficiently. That is, the number of required experiments is independent of system size and the classical computational resources scale only polynomially in the number N of qubits. Here we address the question of how to optimally choose the measurement basis for fidelity estimation when replacing two-level qubits by d-level qudits. We define optimality in terms of the maximal number of unitaries that preserve the measurement basis. Our definition allows us to construct the optimal measurement basis in terms of their spectra and eigenbases: the measurement operators are unitaries with d-nary spectrum and partition into $d + 1$ Abelian groups whose eigenbases are mutually unbiased.

Keywords: quantum process tomography, quantum protocols, qudit operations
PACS numbers: 03.65.Wj, 03.67.Ac

1. Introduction

The development and maintenance of quantum devices requires the capability to verify their proper functioning. This is quantified by suitable performance measures such as the average gate fidelity which compares the actual evolution of the quantum system to the desired unitary [1]. In order to determine the gate fidelity in a given experimental setup, no matter what is the specific protocol, one needs to define a set, or, more precisely, a complete and orthonormal basis, of measurement operators [1]. The choice of measurement operators is typically

dictated by considerations of experimental convenience such as the requirement of local measurements, in the sense that each operator can be measured in a separable eigenbasis.

Additional considerations become important for certain classes of quantum operations, namely those that map a suitable basis of measurement operators onto itself, up to a phase factor. For qubits, Pauli measurements represent such an operator basis. The corresponding unitary operations are termed Clifford gates; they facilitate fault-tolerant computation [2] and yield a universal set for quantum computation when augmented by a single non-Clifford gate, such as a local phasegate [3]. The property of Clifford gates to map the operator basis onto itself, up to a phase factor, can be exploited to obtain protocols for determining the average gate fidelity that require a number of experiments that is independent of system size and classical computational resources that scale only polynomially in the number of information carriers [4–6].

When replacing two-level qubits by d-level qudits, one is faced with the problem that the d-dimensional generalizations of the Pauli measurement basis cannot be Hermitian and unitary at the same time. Qudits have attracted interest in both quantum communication and quantum computation and often occur naturally, for example in superconducting devices. Since device characterization is an important prerequisite for any practical application, it is important to identify the most suitable measurement bases. Different choices exist that correspond to different numbers of unitaries for which efficient characterization is possible [7]. This raises the question of the optimal choice for the measurement basis.

Here we address this question by defining optimality in terms of the maximal number of unitaries that can be efficiently characterized and use this definition to construct the optimal measurement basis in terms of their spectra and eigenbases. We find the optimal measurement basis to consist of unitaries with d-nary spectrum that partition into $d + 1$ Abelian groups whose eigenbases are mutually unbiased. Our result motivates the use of the generalized Pauli group [2, 8] as an optimal measurement basis, not least because of its close connection to mutually unbiased bases [9–11].

The paper is organized as follows: we first define optimality of an operator basis for estimating the average fidelity of quantum gates in section 2. In the following, we use this definition of optimality in sections 3 and 4 to construct the operators that make up the optimal set in terms of their spectra and eigenbases for the case that the Hilbert space dimension d is a prime number. The construction will allow us to show that the optimal operator basis consists of unitaries with d-nary spectrum (i.e., the spectrum is made up of the dth roots of unity) and partitions into $(d + 1)$ Abelian groups whose eigenbases are mutually unbiased. The latter is demonstrated in section 5. For the case that d is not prime, we construct the measurement operators as tensor products and can thus reuse our results obtained for d prime in section 6. Section 7 concludes.

2. Problem statement

We consider a Hilbert space of dimension p with p prime, that is a qupit Hilbert space. Any suitable operator basis $\mathcal{M}$ defined on this Hilbert space must be complete and orthonormal. Unitaries that map the operator basis onto itself, up to a phase factor, can be efficiently characterized, for example, by employing Monte–Carlo estimation of the average fidelity [4, 5] or by using randomized benchmarking [6]. Here, we take the perspective of Monte–Carlo estimation of the average fidelity [4, 5, 12]. In a nutshell, it consists in rewriting the average fidelity as expectation value of a random variable which is characterized by a relevance (or probability) distribution, see [7] for a detailed discussion of three different choices

of the random variable. The expectation value is evaluated by selecting, according to the relevance distribution, pairs of input states and measurement operators and carrying out the respective experiment. Monte–Carlo estimation thus requires classical computational resources for the selection procedure and a certain number of experiments. While both scale exponentially in the number of qubits for general unitaries, they become independent of system size for unitaries which, up to a phase factor, map the operator basis onto itself [4, 5, 12].

Correspondingly, we define the set of unitaries $\mathcal{U}_{\mathcal{M}}$ by the property that for all $U \in \mathcal{U}_M$ and $M_i \in \mathcal{M}$ there exists a $M_j \in \mathcal{M}$ such that $UM_iU^\dagger = \mathrm{e}^{i\phi_i}M_j$ with $\phi_i \in \mathbb{R}$ some phase. This property guarantees a relevance distribution for the Monte–Carlo sampling with p^2 non-vanishing entries which is the minimal amount [7]. Furthermore, these entries all have equal magnitude.

We define an operator basis set $\mathcal{M}$ to be optimal, $\mathcal{M}^\star$, if $\left|\mathcal{U}_{\mathcal{M}}\right| = u_{\max}$ where $u_{\max} = \max_{\mathcal{M}'}\left|\mathcal{U}_{\mathcal{M}'}\right|$ and $|\cdot|$ denotes the cardinality of a set. That is to say that an operator basis $\mathcal{M}$ is optimal if the number of unitaries that map the basis onto itself is maximal amongst all possible operator bases. The map here is to be understood as the conjugation U: $M \mapsto UMU^\dagger$.

3. Spectral properties

Completeness of the operator basis implies that the set $\mathcal{M}$ contains p^2 elements. We include the identity in $\mathcal{M}$ since $\mathbb{1}$ is mapped onto itself by *all* unitaries. This provides a good starting point for the construction of $\mathcal{M}^\star$ which requires all M_i to be mapped to some $M_j \in \mathcal{M}^\star$ by as *many* unitaries as possible. We can thus restrict the following discussion to the $d^2 - 1$ traceless operators in $\mathcal{M}$. Tracelessness of the remaining operators $M_1, M_2, \ldots, M_{p^2-1}$ in $\mathcal{M}$ follows from their orthogonality to the identity. We denote this set by $\tilde{\mathcal{M}}$, i.e., $\tilde{\mathcal{M}} = \mathcal{M}\backslash\mathbb{1}$.

By assumption, $M_1 \in \tilde{\mathcal{M}}$ is mapped to some $M_j \in \tilde{\mathcal{M}}$ for any unitary $U \in \mathcal{U}_{\mathcal{M}}$, i.e., $UM_1U^\dagger = \mathrm{e}^{i\phi_1}M_j$ with ϕ_1 a phase. M_j can either be M_1 itself, and we speak of a cycle of degree 1, or some other element of $\tilde{\mathcal{M}}$. In the latter case, we take $j = 2$ without loss of generality. Applying the map to M_2, $UM_2U^\dagger = UUM_1U^\dagger U^\dagger = U^2M_1\left(U^\dagger\right)^2$ yields either a result proportional to M_1, in which case we have a cycle of degree 2, or a result proportional to another M_j for which we can set $j = 3$. Note that the outcome of $UM_2U^\dagger$cannot be M_2 if $M_2 = UM_1U^\dagger$ due to the bijectivity of rotations. The cycle will necessarily be closed after a number of repeated applications of the map since this always leads to an element of $\tilde{\mathcal{M}}$, and there are only $p^2 - 1$ elements in $\tilde{\mathcal{M}}$. We define the cycle to be of degree n on the set $\tilde{\mathcal{M}}$ if $U^nM_1\left(U^\dagger\right)^n = \mathrm{e}^{i\phi_n}M_1$ with $n \leqslant p^2 - 1$ and ϕ_n a phase.

An iterative argument shows that every operator M in the set $\tilde{\mathcal{M}}$ is contained in at least one cycle. To see this, choose the lowest i such that M_i is not contained in a previously considered cycle and apply U repeatedly on M_i until $U^nM_i\left(U^\dagger\right)^n = \mathrm{e}^{i\phi_n}M_i$. This procedure can be repeated until the complete set $\tilde{\mathcal{M}}$ is exhausted. In fact, for a specific $U \in \mathcal{U}_{\mathcal{M}}$, every operator $M \in \tilde{\mathcal{M}}$ appears exactly once in all the cycles generated by this U. As a consequence, the sum over the degrees of all cycles generated by U needs to be $p^2 - 1$. This can be seen follows: Since rotations are bijective, U: $M_i \mapsto UM_iU^\dagger = \mathrm{e}^{i\phi_i}M_j$ induces a mapping between the integers i and j which is also bijective. Therefore each i can also only occur in one cycle. The degree of a cycle measures how many indices i are present in this cycle. Since the total number of indices is $p^2 - 1$, summing over the degrees of all cycles must amount to

$p^2 - 1$. The two extreme cases are that there are $p^2 - 1$ cycles of degree 1 (e.g. when U is the identity) or that there is one cycle of degree $p^2 - 1$.

For the operator basis to be optimal, the unitary mappings on $\tilde{\mathcal{M}}$ should allow for arbitary cycle structures, i.e., cycles of degree 1, a single cycle of degree $p^2 - 1$, and anything in between. This guarantees that the number of unitaries in $\mathcal{U}_{\mathcal{M}}$ is not limited by the cycle structure. While we do not prove this to be a strict requirement on the optimal set, it represents a very reasonable assumption in terms of avoiding unnecessary restrictions on the unitaries that map the operator basis onto itself. Specifically, for a cycle of degree $p^2 - 1$ to exist, all operators in the set $\tilde{\mathcal{M}}$ must have the same spectrum[4]. This is due to all elements in this cycle emerging from one another by unitary transformation which leaves the spectrum invariant. The requirement of an identical spectrum for all $M_i \in \tilde{\mathcal{M}}^\star$ automatically also allows for the existence of cycles of all other degrees. We denote the spectrum of the operators in the set $\tilde{\mathcal{M}}$ by $\mathrm{spec}\left(\tilde{\mathcal{M}}\right)$.

The condition of an identical spectrum together with the property that the operator basis is mapped onto itself by $U \in \mathcal{U}_{\mathcal{M}}$ implies that the eigenvalues must form a closed cycle: From $UM_iU^\dagger = \mathrm{e}^{i\phi_i} M_j$ it follows that the spectrum needs to obey the condition $\mathrm{e}^{i\phi_i}\mathrm{spec}\left(M_j\right) = \mathrm{spec}\left(M_j\right)$, i.e., if $\lambda \in \mathrm{spec}\left(\tilde{\mathcal{M}}^\star\right)$ then $\mathrm{e}^{i\phi_i}\lambda \in \mathrm{spec}\left(\tilde{\mathcal{M}}^\star\right)$. Multiplication by a complex number $\mathrm{e}^{i\phi_i}$ corresponds to rotating the eigenvalue by an angle ϕ_i in the complex plane. Unless ϕ_i is a multiple of 2π, a new eigenvalue $\mu = \mathrm{e}^{i\phi_i}\lambda$ is obtained. Each application of U thus rotates an eigenvalue onto the next one until the cycle is closed. The degree of the cycle on the eigenvalues can be at most p since the operators in $\tilde{\mathcal{M}}$ can at most have p distinct eigenvalues. Similarly to asking above for the existence of operator cycles of all degrees, asking for the longest eigenvalue cycle ensures that the number of unitaries in $\mathcal{U}_{\mathcal{M}}$ is not unnecessarily restricted. This implies $\left(\mathrm{e}^{i\phi_i}\right)^p = 1$, i.e., the smallest possible rotation angle between two distinct eigenvalues is $\phi_i = \frac{2\pi}{p}$. As a consequence the spectrum in polar representation $\lambda_i = r_i\mathrm{e}^{i\phi_i}$ needs to fulfill $r_i = r = \text{const.}$ and $\phi_i = \frac{2\pi k}{p} + \phi_0$ with ϕ_0 arbitrary such that any rotation by $\frac{2\pi}{p}$ leaves the spectrum invariant. The normalization condition on the operator basis $\mathcal{M}$ yields $r = 1$. Since a global phase on the spectrum is physically irrelevant we can choose $\phi_0 = 0$.

To summarize, for an operator basis $\mathcal{M}$ not to restrict the number of unitaries that map $\mathcal{M}$ onto itself, the spectrum is identical for all $M \in \mathcal{M}\backslash\mathbb{1}$ and p-nary, i.e., it consists of the pth roots of unity:

$$\mathrm{spec}\left(\mathcal{M}^\star\right) = \left\{ \lambda_k = \mathrm{e}^{i\frac{2\pi k}{p}} \;\middle|\; k = 0, \ldots, p-1 \right\}. \tag{1}$$

In particular, this requires all measurement operators in $\mathcal{M}^\star$ to be unitary. As can be seen from equation (1), the operators in $\mathcal{M}^\star$ cannot be unitary and Hermitian at the same time for $p > 2$. For a discussion of non-Hermitian, unitary measurements please see [7] and references therein.

[4] There is always the freedom of a global phase on the spectrum of each measurement operator. It does not influence the relevance distribution and thus does not affect the property of efficient characterizability in any Monte–Carlo protocol. For this reason we set the global phase to zero. Our term 'the same spectrum' therefore corresponds to, strictly speaking, 'the same spectrum up to a global phase'.

4. Properties of the eigenbases

In the previous section, we have used the transformation of the operators $M \in \mathcal{M}$ under a special class of rotations together with the requirement not to restrict the number of unitaries in this class to derive the spectral properties of the operator basis. We can now use orthogonality of the operator basis,

$$\mathrm{Tr}\left[M_a M_b^\dagger\right] = \delta_{ab} \quad \forall \; M_a, M_b \in \mathcal{M}\,, \tag{2}$$

to obtain information about the eigenbases of the operators in $\mathcal{M}$[5]. Since any orthogonal basis of the underlying Hilbert space is an eigenbasis of the identity, i.e., the eigenbasis of $\mathbb{1}$ is undetermined, we only consider the $p^2 - 1$ traceless operators in $\tilde{\mathcal{M}} = \mathcal{M}\backslash\mathbb{1}$.

We order the eigensystem according to the complex phase in the spectrum, equation (1), i.e., $\lambda_k = \mathrm{e}^{i\frac{2\pi k}{d}}$ for $k = 0, \ldots, p-1$ and consider two distinct arbitary measurement operators M_a and M_b, $a \neq b$, with corresponding eigenbases $\left\{|\psi_k^a\rangle\right\}_{k=1,\ldots,p}$ and $\left\{|\psi_k^b\rangle\right\}_{k=1,\ldots,p}$. Employing a spectral decomposition, $M_a = \sum_k \lambda_k |\psi_k^a\rangle\langle\psi_k^a|$, and expanding the trace in equation (2) in the eigenbasis of M_a, we obtain

$$\mathrm{Tr}\left[M_a M_b^\dagger\right] = \sum_{klm} \lambda_k \lambda_l^* \left\langle \psi_m^a \middle| \psi_k^a \right\rangle \left\langle \psi_k^a \middle| \psi_l^b \right\rangle \left\langle \psi_l^b \middle| \psi_m^a \right\rangle = \sum_{kl} \lambda_k \lambda_l^* \left| \left\langle \psi_k^a \middle| \psi_l^b \right\rangle \right|^2 = 0.$$

Inserting the ordered eigenvalues yields for the trace

$$\begin{aligned} \mathrm{Tr}\left[M_a M_b^\dagger\right] &= \sum_{kl} \mathrm{e}^{i\frac{2\pi k}{p}} \mathrm{e}^{-i\frac{2\pi l}{p}} \left| \left\langle \psi_k^a \middle| \psi_l^b \right\rangle \right|^2 = \sum_{kl} \mathrm{e}^{i\frac{2\pi (k-l)}{p}} \left| \left\langle \psi_k^a \middle| \psi_l^b \right\rangle \right|^2 \\ &= \sum_s \mathrm{e}^{i\frac{2\pi s}{p}} \sum_k \left| \left\langle \psi_{k \oplus s}^a \middle| \psi_k^b \right\rangle \right|^2, \end{aligned} \tag{3}$$

where in the last step we have shifted the index s to run from 0 to $p-1$ and $\oplus$ denotes addition modulo d corresponding to the group Z_p on the eigenbasis indices. Equation (3) can be interpreted as a change of basis between the eigenbases of M_a and M_b,

$$U^{ab} = \sum_k \left|\psi_k^b\right\rangle\left\langle\psi_k^a\right|, \tag{4a}$$

together with a right-shift by s in the eigenbasis of M_a,

$$S^a(s) = \sum_k \left|\psi_{k \oplus s}^a\right\rangle\left\langle\psi_k^a\right|. \tag{4b}$$

With the definitions of equation (4), we can rewrite the orthogonality condition as

$$\mathrm{Tr}\left[M_a M_b^\dagger\right] = \sum_s \mathrm{e}^{i\frac{2\pi s}{p}} \sum_k \left| \left\langle \psi_k^a \middle| S^a(s) U^{ab} \middle| \psi_k^a \right\rangle \right|^2 = 0. \tag{5}$$

To derive from equation (5) requirements that the operator eigenbases of operators in the optimal set $\mathcal{M}^\star$ must meet, we first assume M_a and M_b to commute and analyze the case of non-commuting operators in section 4.2 below.

[5] To be precise, the two properties that we have not yet exploited are orthogonality and completeness. However, completeness immediately follows from orthogonality and the fact that $\mathcal{M}$ contains (by definition) p^2 elements.

4.1. Commuting measurement operators

We first show that a change of basis U^{ab} between the eigenbases of two measurement operators which commute, $\left[M_a, M_b\right] = 0$, is a permutation. Next, we derive, from the spectral properties obtained in the previous section, the structure of the matrix U^{ab}. The corresponding constraints allow for the existence of only $p-2$ such permutation operators. This implies that there are p orthogonal, pairwise commuting measurement operators with their spectrum given by equation (1), namely M_a plus the $p-2$ operators obtained by applying U^{ab} to M_a plus identity.

Due to the spectral condition (1), all operators in $\tilde{\mathcal{M}}$ are non-degenerate. This together with the assumption of commutativity implies that for each index k enumerating the eigenbasis of M_a there exists an index l enumerating the eigenbasis of M_b such that $|\psi_k^a\rangle = |\psi_l^b\rangle$ and the mapping between k and l is bijective. That is to say that the eigenbases of M_a and M_b are the same up to reordering which means that certain eigenvectors can correspond to different eigenvalues. In this case, the change of basis U^{ab} between the eigenbases of M_a and M_b, defined by equation (4*b*), is a permutation operator.

In the eigenbasis of M_a, the matrix elements of U^{ab} are either zero or one and the total number of one's is p. $S^a(s)$ is also a permutation operator which shifts the columns of U^{ab} in this representation by s to the right. This means that for all s, the sum over k in equation (5) is a non-negative integer,

$$\sum_k \left| \left\langle \psi_k^a \right| S^a(s) U^{ab} \left| \psi_k^a \right\rangle \right|^2 = c_s. \tag{6}$$

Since U^{ab} and $S^a(s)$ are both permutation operators, so is their product, $P^{ab}(s) = S^a(s)U^{ab}$. Note that $S^a(s=0) = \mathbb{1}$, and c_0 is given by the sum over the diagonal elements squared of U^{ab}. For $s = 1$, all columns of U^{ab} are shifted to the right by one, i.e., the first upper diagonal of U^{ab} becomes the diagonal of P^{ab}, and the sum over its elements squared yields c_1. In other words, each c_s corresponds to the sum over the diagonal of $P^{ab}(s)$, that is the sth secondary diagonal of U^{ab}, and thus takes a value between 0 and p. Due to orthogonality of the operator basis, equation (5), the set of integers $\{c_s\}_{s=0,\ldots,p-1}$ has to fulfill the condition

$$\sum_{s=0}^{d-1} c_s \mathrm{e}^{i\frac{2\pi s}{p}} = 0. \tag{7}$$

Note that, $\sum_{s=0}^{p-1} c_s = p$ since summing over all c_s corresponds to summing over all elements squared of $P(s)$, or U^{ab}. We show in appendix A that for p prime no linear combination with non-negative integers c_s can exist that makes the sum go to zero except if $c_s = 1$ for all s.

Since c_s corresponds to the sum over the sth secondary diagonal of U^{ab}, we have thus restricted all possible matrices U^{ab} for a change of basis between the eigenbases of commuting measurement operators $M_a, M_b \in \tilde{\mathcal{M}}$ to those that contain exactly one entry equal to one on each (secondary) diagonal with all other entries being zero. In addition, each row and each column of U^{ab} also contains exactly one entry equal to one with all other entries being zero since U^{ab} is a permutation operator.

We now show that under these constraints there exist $p-2$ distinct permutation operators U^{ab}, demonstrating first how one can construct $p-2$ such unitaries and then proving in a second step that these are indeed *all* unitaries that fulfill the given constraints. In order to construct the $p-2$ matrices U^{ab} for a change of basis, we reorder the eigenbases of M_a and M_b such that the main diagonal always contains one as its first entry for all b: $U_{11}^{ab} = 1$, $U_{ii}^{ab} = 0$ for $i = 2,\ldots, p$. This reordering does not interfere with ordering the eigenbases of M_a

and M_b in terms of the eigenvalues, equation (1), since M_a and M_b can be multiplied by $e^{i\frac{2\pi t}{p}}$ for some t without changing the orthogonality condition. This multiplication performs exactly the shift in the eigenbases required to ensure $U_{11}^{ab} = 1$ for all b. In other words: The ordering of the eigenvalues determines the indexing of the eigenbasis of M_b while now in addition the global phase of M_b is fixed. Then, for p prime, a set of $p - 2$ permutation operators that have on each of their diagonals exactly one entry equal to one with all others being zero and $U_{11}^{ab} = 1$ is given by

$$\left(U^{ab}\right)_{ik} = \delta_{k,(i-1)\cdot b\oplus 1} \quad \text{with} \quad b = 2, \ldots, p-1. \tag{8}$$

The construction that leads to equation (8) proceeds as follows: The first row is given by the assumption $\left(U^{ab}\right)_{11} = 1$ for all b. In the second row, $\left(U^{ab}\right)_{21}$ and $\left(U^{ab}\right)_{22}$ need to be zero due to the constraints of each column and the main diagonal containing exactly one entry equal to one. The smallest j for which $\left(U^{ab}\right)_{2j}$ can be non-zero is thus $j = 3$. Analogously, in the third row, the smallest entry that can be non-zero is $j = 5$ (with $j = 4$ being excluded by the condition on the first upper diagonal). This construction is similar to the movement of a knight on a chess board: one step down, two steps to the right. It is continued until the last row is reached to yield the first U^{ab} (with b set to 2). The second U^{ab} is obtained by choosing $j = 4$ in the construction of the second row. This implies a modified movement of the knight with one step down, $b = 3$ steps to the right. Once the right boundary on the matrix is reached, the movement is simply continued by counting from the left, as implied by the modulo algebra in equation (8). For a $p\times p$ matrix U^{ab}, there are $p - 2$ distinct knight-type movements since in the construction of the second row, $\left(U^{ab}\right)_{21}$ and $\left(U^{ab}\right)_{22}$ are always fixed and one can choose at most $j = p$, i.e., move at most $p - 1$ steps to the right. As shown in appendix A.2, for p prime, the construction rule, equation (8), yields proper unitary permutation operators which have on each (secondary) diagonal only one entry equal to one. This holds only for prime $d = p$. For non-prime d, the above construction leads to a contradiction to the unitarity constraint of each column having exactly one entry equal to one with all others being zero.

When applied to M_a, the U^{ab} constructed according to equation (8) yield $p - 2$ operators M_b that are orthogonal to M_a. We now show that equation (8) represents *all* the unitaries that fulfill the constraint of having exactly one entry equal to one on each (secondary) diagonal, i.e., there are exactly p commuting measurement operators (including identity). As a side result, we obtain that all M_b obtained from applying the U^{ab} to M_a are not only orthogonal to M_a but also to each other.

The fact that, for p prime, *all* permutation operators, that have on each of their diagonals exactly one entry equal to one with all other entries being zero and $U_{11}^{ab} = 1$, are given by equation (8) and that there are thus $p - 2$ such unitaries can be seen as follows: since U^{ab} maps the eigenvectors of M_a onto the eigenvectors of M_b, it also corresponds to a mapping between the eigenvalues λ_k^a and $\lambda_{k'}^b$. The fact that we fixed $\left(U^{ab}\right)_{11} = 1$ together with equation (1) implies $\lambda_0^a = \lambda_0^b = 1$. The other eigenvalues are redistributed according to $\lambda_k^b = \mathrm{e}^{i\frac{2\pi}{p}\cdot k} \mapsto \lambda_{kb}^a = \mathrm{e}^{i\frac{2\pi}{p}\cdot kb}$ where the product kb is to be understood modulo p. Since the eigenvalue λ_{kb}^a shows up in the spectral decomposition of the bth power of M_a,

$$\left(M_a\right)^b = \left(\sum_k \mathrm{e}^{i\frac{2\pi}{p}k}\left|\psi_k^a\right\rangle\left\langle\psi_k^a\right|\right)^b = \sum_k \mathrm{e}^{i\frac{2\pi}{p}kb}\left|\psi_k^a\right\rangle\left\langle\psi_k^a\right|, \tag{9}$$

we find

$$M_b = \left(M_a\right)^b \quad \text{with} \quad b = 2, \ldots, p-1. \tag{10}$$

Moreover, $\left(M_a\right)^p = \mathbb{1}$ since $kp = 1$ when interpreted modulo d for all k. Then all powers of M_a are orthonormal since, for all b,

$$\mathrm{Tr}\left[M_a\left(M_a^\dagger\right)^b\right] = \mathrm{Tr}\left[M_a M_a^\dagger\left(M_a^\dagger\right)^{b-1}\right] = \mathrm{Tr}\left[\left(M_a^\dagger\right)^{b-1}\right] = \begin{cases} 1 & \text{if } b \bmod p = 1 \\ 0 & \text{otherwise} \end{cases}.$$

The last step follows from the fact that M_a^{b-1} has the same spectrum as M_a and is consequently traceless, unless $b - 1 = p$ where we obtain identity. This is evident from equation (9). Adjungation of the operator just returns the complex conjugated result for the trace. Since this result is real in either case, it is unaffected by adjungation. Finally, the maximal number of commuting, pairwise orthogonal unitaries M_a defined on a p-dimensional Hilbert space is p. This can be seen by considering their common eigenbasis $\left\{|\psi_k\rangle\right\}_{k=1,\ldots,p}$. Any linear combination of the commuting, pairwise orthogonal unitaries M_a also has this eigenbasis. We can thus employ the common eigenbasis to construct a representation of any operator M with this eigenbasis, $M = \sum_{k=0}^{p-1}\lambda_k |\psi_k\rangle\langle\psi_k|$. This is a linear combination of p orthonormal operators $|\psi_k\rangle\langle\psi_k|$ with coefficients corresponding to the eigenvalues of M. Consequently no orthonormal basis of the space of operators with common eigenbasis to M_a can have more than p elements and as such the maximal number of commuting, pairwise orthogonal unitaries M_a is p.

As a corollary, we obtain that the set $\tilde{\mathcal{M}}_a = \left\{\left(M_a\right)^b\right\}_{b=1,\ldots,p-1}$ with the spectrum of all elements given by equation (1) together with the identity forms an Abelian group of pairwise orthonormal operators with matrix multiplication as group operation. $\tilde{\mathcal{M}}_a$ contains all the unitaries that share an eigenbasis with M_a while having the same spectrum as M_a and being pairwise orthogonal.

4.2. Complete set of measurement operators

After constructing p commuting measurement operators from the spectral conditions and orthogonality, we now identify the remaining $p^2 - p$ measurement operators that are required to complete the optimal operator basis. Since we have also shown in section 4.1 that there are only p commuting measurement operators, the remaining ones are necessarily non-commuting.

The complete set of measurement operators $\tilde{\mathcal{M}}$ is obtained iteratively: That is, one chooses a starting point, i.e., an operator M_a with spectrum according to equation (1). M_a defines the commmuting set $\tilde{\mathcal{M}}_a$ with all operators in $\tilde{\mathcal{M}}_a$ given by equation (10). Next one needs to find another matrix $M_{a'}$ with the same spectrum, equation (1), but orthogonal to all $M_a \in \tilde{\mathcal{M}}_a$. By construction, $M_{a'}$ does not share an eigenbasis with the $M_a \in \tilde{\mathcal{M}}_a$. Rather, it defines, according to equation (10), its own set of commuting operators, $\tilde{\mathcal{M}}_{a'}$ which, together with the identity, forms another Abelian group. A constructive method to determine $M_{a'}$ is obtained by exploiting mutual unbiasedness of the eigenbases of the sets $\tilde{\mathcal{M}}_a$ for different a, as we show below in section 5.The step of identifying $M_{a'}$ and its commuting set needs to be repeated until $p + 1$ Abelian groups $\tilde{\mathcal{M}}_a \cup \mathbb{1}$ have been found. The procedure of identifying $p + 1$ sets of p commuting, pairwise orthogonal measurement operators yields, without double-counting the identity which is an element of all the Abelian groups, p^2 orthogonal measurement operators, i.e., the complete operator basis $\mathcal{M}$.

Clearly, one cannot find more than $p+1$ Abelian groups of orthogonal operators since there exist only p^2 orthogonal operators on a p-dimensional Hilbert space. Note that we know of the existence of at least one such set of Abelian groups–the generalized Pauli operator basis $\mathcal{P}$ and its separation into mutually commuting subsets. The operators belonging to the generalized Pauli basis are given by [2, 10, 11, 13]

$$X^a Z^b, \quad a, b \in [0, p-1], \tag{11a}$$

where $\omega = \exp(2i\pi/p)$ and

$$X = |n \oplus 1\rangle\langle n|, \tag{11b}$$

$$Z = \omega^n |n\rangle\langle n|, \tag{11c}$$

with $n \in [0, p-1]$ and addition is modulo p.

5. Mutually unbiased bases

The existence of $p+1$ Abelian groups $\tilde{\mathcal{M}}_a \cup \mathbb{1}$ of orthogonal measurement operators is in a one-to-one correspondence to the existence of $p+1$ mutually unbiased bases [10]. This is easily seen using our constructions of section 3 and 4: the common eigenbasis of $\tilde{\mathcal{M}}_a$, $\{|\psi_k^a\rangle\}$, can be used to construct an operator basis,

$$M_{au} = (M_a)^u = \sum_k \mathrm{e}^{i\frac{2\pi}{p}uk} \left|\psi_k^a\right\rangle\left\langle\psi_k^a\right|.$$

Projectors can be defined in terms of the operator basis, that is,

$$P_n^a = \left|\psi_n^a\right\rangle\left\langle\psi_n^a\right| = \frac{1}{p}\sum_u \mathrm{e}^{-i\frac{2\pi}{p}un}(M_a)^u.$$

Then

$$\left|\left\langle\psi_n^a\middle|\psi_{n'}^b\right\rangle\right|^2 = \mathrm{Tr}\left[P_n^a\left(P_{n'}^b\right)^\dagger\right] = \frac{1}{p^2}\sum_{uu'}\mathrm{e}^{-i\frac{2\pi}{p}\left(un-u'n^{prime}\right)}\mathrm{Tr}\left[M_{au}M_{bu'}^\dagger\right].$$

If M_a and M_b are from different Abelian groups, only identity ($u = u' = 0$) contributes due to orthogonality of all other measurement operators. In this case

$$\left|\left\langle\psi_n^a\middle|\psi_{n'}^b\right\rangle\right|^2 = \frac{1}{p^2}\mathrm{Tr}\,[\mathbb{1}] = \frac{1}{p}. \tag{12}$$

If M_a and M_b are from the same set $\tilde{\mathcal{M}}_a \cup \mathbb{1}$, all $u = u'$ contribute and then

$$\left|\left\langle\psi_n^a\middle|\psi_{n'}^a\right\rangle\right|^2 = \frac{1}{p^2}\sum_u \mathrm{e}^{-i\frac{2\pi}{p}u(n-n')}\mathrm{Tr}\left[M_{au}M_{au}^\dagger\right] = \frac{1}{p}\sum_u \mathrm{e}^{-i\frac{2\pi}{p}u(n-n')} = \delta_{nn'}.$$

These findings allow us to construct the set of measurement operators as mentioned above in section 4.2. After identifying the first set $\tilde{\mathcal{M}}_a$ of p commuting measurement operators by picking an M_a and employing equation (10), a new measurement operator $M_{a'}$is found by choosing its eigenvectors as a MUB with respect to the eigenbases of $\tilde{\mathcal{M}}_a$ (in the subsequent steps of the iterative procedure, the eigenvectors have to be mutually unbiased with respect to *all* previously constructed sets). The eigenvectors of $M_{a'}$ are assigned a spectrum analogously to equation (9), using equation (1). Thus $M_{a'}$ and all of its powers form a commuting set with proper spectrum that is orthogonal to all matrices from $\tilde{\mathcal{M}}_a$ (or, in the subsequent steps of the iterative procedure, to *all* previously constructed sets $\tilde{\mathcal{M}}_a$, $\tilde{\mathcal{M}}_{a'}$, …). It

is indeed possible to construct a complete basis of measurement operators with this method since the maximal number of $p + 1$ MUB does exist for prime dimension p.

The identification of the eigenbases of the measurement operators with mutually unbiased bases allows us to determine which unitaries can be efficiently characterized with this operator basis. The candidate unitaries need to map any measurement operator onto another measurement operator from the set, modulo a phase corresponding to a pth root of unity. Consider a specific measurement operator M from an optimal set $\tilde{\mathcal{M}}^\star$. M is mapped by the candidate unitaries either to the same or to a different Abelian group in $\tilde{\mathcal{M}}^\star$. Given the spectral decomposition of M in terms of its eigenbasis, $\{|\psi_k^a\rangle\}$, with eigenvalues λ_a, we can write

$$UMU^\dagger = \sum_a \lambda_a U \left|\psi_k^a\right\rangle\left\langle\psi_k^a\right| U^\dagger = \sum_a \lambda_a \left|U\psi_k^a\right\rangle\left\langle U\psi_k^a\right|$$

which must be equal to M' where $M' \in \tilde{\mathcal{M}}^\star$ by definition of U. Since the $\{|\psi_k^a\rangle\}$ are orthonormal, so are the $\{|U\psi_k^a\rangle\}$; hence they correspond to the eigenbasis of M'. Consequently, the set $\{|U\psi_k^a\rangle\}$ must either be identical to the set $\{|\psi_k^a\rangle\}$ modulo phasefactors on the individual states or correspond to a basis which is mutually unbiased to $\{|\psi_k^a\rangle\}$. Therefore a unitary U is efficiently characterizable if and only if it keeps the partitioning of the $p + 1$ mutually unbiased bases in a Hilbert space of prime dimension p intact.

6. Tensor products

We now consider N qupits ($N > 1$) and assume the measurement operators to be tensor products of single-qupit operators. This choice is motivated by the requirement to allow for product input states since the preparation of these states is experimentally much easier. Product input states imply a tensor product structure for the measurement basis since, in Monte–Carlo estimation of the average fidelity, the input states are the eigenstates of the measurement basis [4, 5, 7].

Assuming the measurement basis to be given by tensor products, we obtain a natural partition of the total Hilbert space into a tensor product of smaller Hilbert spaces. It corresponds to the direct product structure imposed on the measurement basis. A natural approach to identify optimal measurement bases on the total Hilbert space starts from maximizing the number of efficiently characterizable unitaries on each subspace [7]. This is achieved by finding an optimal measurement basis on each subspace as discussed above, provided the dimension of the subspace is prime. The optimal measurement basis of the total Hilbert space is then constructed in terms of tensor products of the operators defined on the subspaces. This yields indeed an orthonormal basis of measurement operators on the total Hilbert space.

The dimension of each subspace is prime for N identical qupits but also for mixtures of e.g. qubits and qutrits ($p = 3$). If a subspace has non-prime dimension, we suggest to perform a prime decomposition of the dimension and construct the measurement basis as tensor products of the optimal bases defined on the resulting prime dimension subspaces, analogously to the discussion above. Most likely, this yields an optimal measurement basis. However, it remains an open question whether the explicit use of non-prime dimension subspaces can be used to increase the number of efficiently characterizable unitaries beyond the one following from the prime factor decomposition approach. Nonetheless, our conjecture that a measurement basis constructed from the prime factor decomposition represents indeed an optimal choice is motivated by the fact that existence of $p + 1$ mutually unbiased bases is

not guaranteed for non-prime dimension Hilbert spaces but seems to be a central prerequisiste for obtaining efficiently characterizable unitaries [7].

7. Conclusions

Efficient estimation of the average fidelity of Clifford gates relies on the property of these unitaries to map the basis of measurement operators onto itself, up to a phase factor. We have used this property to define optimality of a measurement basis in terms of the maximum number of unitaries that can be efficiently characterized. For Hilbert spaces of prime dimension, we have shown that this definition yields a constructive proof for the optimal measurement basis and also allows for identifying the unitaries which can be efficiently characterized. For N identical qudits, an optimal measurement basis is obtained in terms of tensor products of the single-qudit operators making up the optimal single-qudit operator basis. This choice guarantees that the measurements are local in the sense that only separable input states are required.

Our construction of an optimal set of measurement operators with the corresponding set of measurement bases is determined only up to a global rotation. In other words, the choice of the eigenbasis for the first Abelian group of measurement operators is arbitrary. This corresponds to mutual unbiasedness being defined only in relation of one basis to another. If, in a given experimental setting, it is possible to perform measurements and prepare input states relative to a rotated set of mutually unbiased bases, this can be used to also rotate the set of efficiently characterizable unitaries. Specifically, for any unitary U there exists a measurement basis in which U can be efficiently characterized. This is essentially the idea underlying randomized benchmarking [6] where arbitrary unitaries are rotated into identity. The corresponding rotation on the input states requires, however, application of the inverse of the unitary that shall be characterized. This is in general not practical. In other words, the freedom of choice for the global rotation of the measurement can in principle be used to tune the set of efficiently characterizable unitaries. Typically, however, the choice of the eigenbasis for the first Abelian group of measurement operators is dictated by experimental convenience such as the requirement of a separable eigenbasis. This fixes the set of unitaries that can be characterized efficiently.

The fact that our proof relies on the dimension of the Hilbert (sub)spaces to be prime highlights the intimate relation between finding efficiently characterizable unitaries and the existence of mutually unbiased bases. In particular, for prime dimensions we have proven that the optimal basis of measurement operators can be partitioned into $p + 1$ commuting sets, i.e., it gives rise to a maximal partitioning. The generalized Pauli operators [2, 10, 11, 13] represent one example of such an optimal measurement basis. Generalized Pauli operators can also be defined for Hilbert spaces whose dimension cannot be expressed as p^N with p prime [8].

Acknowledgements

GG acknowledges support from a MIUR-PRIN grant (2010LLKJBX). QSTAR is the MPQ, LENS, IIT, UniFi Joint Center for Quantum Science and Technology in Arcetri.

Appendix A. Details of the proofs

A.1. The solution to equation (7) is $c_s = 1$

We show here that the only solution of equation (7) for $c_s = 0, 1, \ldots \in \mathbb{N}$ under the additional constraint

$$\sum_{s=0}^{p-1} c_s = p \tag{A.1}$$

is

$$c_s = 1$$

for all s. To prove this we use the fact that $e^{i\frac{2\pi s}{p}}$ is a pth root of unity for all s and then apply a theorem of [14] about sums over roots of unity. Abbreviating $e^{i\frac{2\pi}{p}} = \omega$, equation (7) becomes

$$\sum_{s=0}^{p-1} c_s \omega^s = 0. \tag{A.2}$$

Since all c_s are non-negative integers, this can be rewritten as

$$\sum_{t=0}^{p-1} \Omega_t = 0, \tag{A.3}$$

where Ω_t is a pth root of unity. We absorbed the integer values of c_s into the Ω_t by allowing for repetitions in the sum. So for example if a c_s was greater than one, there would be multiple indices t in equation (A.3) with $\Omega_t = \omega^s$. Furthermore, some c_s could be zero which means that the corresponding root of unity ω^s does not appear in the set of Ω_t. Note furthermore that since we know that the c_s sum up to p, the sum in equation (A.3) indeed has $p - 1$ elements.

Consider now the general situation of sums over pth roots of unity with an arbitrary number of summands, n. As in equation (A.3), the same root of unity may appear multiple times. Lam and Leung in [14] showed that if p is prime, such a sum can only be equal to zero if n is equal to a multiple of p. As a consequence there exists no proper subsum of the sum in equation (A.3) that goes to zero by itself. This property is called minimal. Moreover, corollary 3.4. from [14] implies that for p prime the only minimal vanishing sum of p roots of unity, including repetitions, is given by

$$\sum_{t=0}^{p-1} \omega^t = e^{i\frac{2\pi t}{p}} = 0. \tag{A.4}$$

This translates into the sum in equation (A.3) having no repetitions but every root of unity appears exactly once. Consequently, $c_s = 1$ in for all s in equation (7) and the statement is proven.

A.2. All matrices constructed according to equation (8) are unitary for p prime

We show here that all matrices constructed according to equation (8) are unitary for p prime and contain on each (secondary) diagonal only one entry equal to one.

For simplicity we use normal addition symbols in this section but all algebraic manipulations are to be understood modulo p. We first show that each (secondary) diagonal contains only one entry equal to one with all others being zero. Consider a fixed b and a fixed diagonal t. An element on this (secondary) diagonal, $(U^{ab}_{i,\,i+t})$ with $i = 1,\ldots,p$, is non-zero according to equation (8) if and only if $\delta_{i+t,(i-1)\cdot b+1} = 1$. To prove that, given b and t, there is

exactly one i for which this can happen, we consider the solutions of the equation

$$(i-1)\cdot(b-1)=t, \tag{A.5}$$

which follows directly from $(i-1)\cdot b+1=i+t$. If we keep b fixed, showing that for each t there is one i for which equation (A.5) is fulfilled is equivalent to showing that for each i there is exactly one t for which equation (A.5) is fulfilled, i.e. $t(i)$ is bijective. Then in each row a different diagonal acquires the value 1. Since the map $t(i)$ maps the finite set $1,...,p$ onto itself, injectivity implies surjectivity. Hence we only need to prove that $t(i)$ is injective.

To do this, we need to find out how many solutions i are allowed for equation (A.5) with $t\in\{0,...,p-1\}$. At least one solution to equation (A.5) must exist since by construction of U_{ab}, there is one entry equal to 1 on each row. According to the rules of modulo algebra, if one solution exists, then there are g solutions with $g=\gcd(b-1,p)$ where gcd denoting the greatest common divisor. Since $b<p$ and p is a prime number, $g=1$ and there exists only one solution. This proves injectivity of $t(i)$. Therefore the map $t(i)$ is bijective and so is $i(t)$ which implies that the construction of U_{ab}, equation (8), indeed fulfills the condition of exactly one entry equal to 1 on each (secondary) diagonal.

Next we show unitarity of U_{ab}. By construction, there exists exactly one entry equal to 1 in each row. It remains to be shown that in each column there exists also only one entry equal to 1. Unitarity of U_{ab} then follows immediately.

Let us consider for fixed b a column k. According to equation (8), an entry in the ith row is non-zero if and only if $\delta_{k,(i-1)\cdot b+1}=1$. To show that for fixed b and k there is exactly one i for which this can happen, we consider the solutions of the equation

$$(i-1)\cdot b+1=k. \tag{A.6}$$

Equation (A.6) defines a map $k(i)$. Showing that $k(i)$ is bijective implies that for each k there exists only one i as a solution and vice versa, i.e., for each column there is only one row with an entry equal to 1. Employing the same argument as above, there exist g solutions to equation (A.6) with $g=\gcd(b,p)$ and, since $b<p$ and p is prime, $g=1$ and there exists only one solution. As a consequence the map $k(i)$ is bijective and so is the map $i(k)$, i.e., the U_{ab} constructed according to equation (8) are indeed unitary.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Gottesman D 1999 *Chaos Solitons Fractals* **10** 1749
[3] Boykin P, Mor T, Pulver M, Roychowdhury V and Vatan F 2000 *Inf. Process. Lett.* **75** 101
[4] Flammia S T and Liu Y-K 2011 *Phys. Rev. Lett.* **106** 230501
[5] da Silva M P, Landon-Cardinal O and Poulin D 2011 *Phys. Rev. Lett.* **107** 210404
[6] Magesan E, Gambetta J M and Emerson J 2011 *Phys. Rev. Lett.* **106** 180504
[7] Gualdi G, Licht D, Reich D M and Koch C P 2014 *Phys. Rev.* (at press) arXiv:1404.1608
[8] Bermejo-Vega J and van DenNest M 2014 *Quant. Inf. Comput.* **14** 0181
[9] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
[10] Bandyopadhayay S, Boykin P O and Roychowdhury V V F 2002 *Algorithmica* **34** 512
[11] Lawrence J 2004 *Phys. Rev.* A **70** 012302
[12] Reich D M, Gualdi G and Koch C P 2013 *Phys. Rev. Lett.* **111** 200401
[13] Lawrence J, Brukner C and Zeilinger A 2002 *Phys. Rev.* A **65** 032320
[14] Lam T and Leung K 2000 *J. Algebra* **224** 91