Operator-Schmidt decompositions and the Fourier transform, with applications to the operator-Schmidt numbers of unitaries

2003 J. Phys. A: Math. Gen. 36 10101

(http://iopscience.iop.org/0305-4470/36/39/309)

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **36** (2003) 10101–10114 PII: S0305-4470(03)65682-9

Operator-Schmidt decompositions and the Fourier transform, with applications to the operator-Schmidt numbers of unitaries

Jon E Tyson

Jefferson Lab, Harvard University, Cambridge, MA 02138, USA

E-mail: jonetyson@post.harvard.edu

Received 2 July 2003
Published 17 September 2003
Online at stacks.iop.org/JPhysA/36/10101

Abstract

The operator-Schmidt decomposition is useful in quantum information theory for quantifying the nonlocality of bipartite unitary operations. We construct a family of unitary operators on $\mathbb{C}^n \otimes \mathbb{C}^n$ whose operator-Schmidt decompositions are computed using the discrete Fourier transform. As a corollary, we produce unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$ with operator-Schmidt number S for every $S \in \{1, \ldots, 9\}$. This corollary was unexpected, since it contradicted reasonable conjectures of Nielsen *et al* (2003 *Phys. Rev.* A **67** 052301) based on intuition from a striking result in the two-qubit case. By the results of Dür *et al* (2002 *Phys. Rev. Lett.* **89** 057901), who also considered the two-qubit case, our result implies that there are nine equivalence classes of unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$ which are probabilistically interconvertible by (stochastic) local operations and classical communication. As another corollary, a prescription is produced for constructing maximally-entangled unitaries from biunimodular functions. Reversing tact, we state a generalized operator-Schmidt decomposition of the quantum Fourier transform considered as an operator $\mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2} \to \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$, with $M_1 M_2 = N_1 N_2$. This decomposition shows (by Nielsen's bound) that the communication cost of the QFT remains maximal when a net transfer of qudits is permitted. In an appendix, a canonical procedure is given for removing basis-dependence for results and proofs depending on the 'magic basis' introduced in S Hill and W Wootters (1997 Entanglement of a pair of quantum bits *Phys Rev. Lett.* **78** 5022–5).

PACS numbers: 03.67.Hk, 03.65.Ud

1. Introduction

This paper addresses some open problems (questions (1–3) below) concerning the operator-Schmidt decomposition [1] (see definition 1), which is useful in quantum information theory [2, 3] for quantifying nonlocality of bipartite unitary operations. Our main results are obtained by constructing a family of unitaries on $\mathbb{C}^N \otimes \mathbb{C}^N$ with computable operator-Schmidt decompositions, a result which should facilitate further study of this decomposition.

Dür *et al* [4] used operator-Schmidt numbers to determine when there exists a probabilistic[1] simulation of a unitary $\tilde{U}$ on $\mathbb{C}^d \otimes \mathbb{C}^d$ with a *single* application of a given unitary U on $\mathbb{C}^d \otimes \mathbb{C}^d$ aided by (stochastic) local operations, classical communication and ancilla. In particular, they show that this simulation can occur iff $\mathrm{Sch}\,(U) \geqslant \mathrm{Sch}(\tilde{U})$, where $\mathrm{Sch}\,(U)$ is the number of nonzero operator-Schmidt coefficients of U (see definition 1).[2]

Intriguingly, Dür *et al* observed that a unitary acting on two qubits may have operator-Schmidt number $1, 2$ or 4, but not 3.[3] Thus, there exist three equivalence classes of two-qubit unitary operations under probabilistic local interconversion (using (S)LOCC), with the successive classes represented by the identity, CNOT and SWAP operation, respectively. Their observation followed immediately from the canonical decomposition of two-qubit unitaries [6]:[4] any two-qubit unitary operation $U_{AB} \in \mathrm{SU}(4)$ can be written in the following standard form:

$$U_{AB} = (V_A \otimes W_B) \exp\left(\mathrm{i}\sum_{k=1}^{3} \mu_k \sigma_k^A \otimes \sigma_k^B\right)(\tilde{V}_A \otimes \tilde{W}_A) \tag{1}$$

where V_A, W_B, $\tilde{V}_A$ and $\tilde{W}_B$ are local unitaries and where the σ_k are the Pauli operators with $\sigma_0 \equiv 1$, and

$$\pi/4 \geqslant \mu_1 \geqslant \mu_2 \geqslant |\mu_3| \geqslant 0.$$

(Since the Schmidt coefficients of U_{AB} are unaffected by the local $V_A, \ldots, \tilde{W}_B$, their claim reduced to a simple calculation of the operator-Schmidt coefficients of the exponential.)

An interesting problem posed by Nielsen *et al* [5] is to find the allowed operator-Schmidt numbers of unitaries on $\mathbb{C}^n \otimes \mathbb{C}^m$. Since there is no known generalization of the canonical decomposition (1) to unitaries on $\mathbb{C}^n \otimes \mathbb{C}^m$ for $\max(n, m) > 2$,[5] at present a different method is required to solve this problem. (The $n = m = 3$ case is solved below.)

The operator-Schmidt decomposition was introduced by Nielsen [1] in consideration of the following problem of coherent communication complexity:

> Suppose Alice has n_a qubits and Bob has n_b qubits, and they wish to perform some general unitary operation U on their $n_a + n_b$ qubits. How many qubits of quantum communication are required to achieve this goal?

Nielsen proved that the minimum number $Q_0(U)$ of such qubits satisfies the following bound [9]:

$$K_{\mathrm{har}}(U) \leqslant Q_0(U) \leqslant 2\min(n_a, n_b) \tag{2}$$

---

[1] i.e. succeeding with a nonzero probability.

[2] Dür *et al* note that, for example, entanglement purification is a probabilistic process, so it is natural to consider probabilistic simulation of its component gates.

[3] This fact was rediscovered by Nielsen *et al* [5].

[4] Kraus and Cirac have a constructive ‘magic basis’ proof [7]. The invariants of this decomposition were first discovered by Makhlin [8].

[5] An interesting restriction of this open problem is to illuminate the nonlocal structure of maximally-entangled bipartite unitaries. (See definition 2.)

where the *Hartley strength* K_{har} satisfies

$$K_{\mathrm{har}}(U) = \log_2(\mathrm{Sch}(U))$$

where $\mathrm{Sch}(U)$, defined in definition 1, is the number of nonzero operator-Schmidt coefficients of U. It was assumed that Alice and Bob have the use of ancilla, but they must separately retain their (modified) data qubits at the end of the computation. The upper bound of (2) is trivial, for Alice could simply send all her bits to Bob and let him send them back, or vice versa. We emphasize that the communication complexity $Q_0(U)$ is the communication cost of exact computation of one application of U. An interesting open problem is to consider the communication cost of approximate computation of $U^{\otimes M}$, where the error goes to zero in some appropriate sense for large M.[6]

Nielsen applied his abstract bound to show that the communication complexity of the quantum Fourier transform is maximal, first in the case of $n_a = n_b$ [1, 9], and then (with collaborators) in the case $n_a \leqslant n_b$ [5], where Alice holds the most-significant qubits[7]. This was extended to $n_a > n_b$ and to arbitrary qudits in [10]. In section 5 we extend this result to the case that a net transfer of data qudits is permitted.

1.1. Results

The main result of this paper is the construction of a family of unitaries on $\mathbb{C}^N \otimes \mathbb{C}^N$ whose Schmidt decompositions are computable using Fourier analysis. Specifically, theorem 7 gives a set $\{\Phi_{\alpha\beta}\}$ of vectors in a tensor product of two Hilbert spaces of dimension N such that the Schmidt-coefficients of the diagonal operator

$$D = \sum_{\alpha,\beta=0}^{N-1} \lambda(\alpha, \beta)|\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}| \tag{3}$$

are the nonzero values of $|\hat{\lambda}(\alpha, \beta)|$, where $\hat{\lambda}$ is the discrete Fourier transform.

Furthermore, this paper addresses the following questions concerning the operator-Schmidt decomposition:

1. What operator-Schmidt numbers S occur in unitary operators on $\mathbb{C}^3 \otimes \mathbb{C}^3$?
2. How can one construct maximally-entangled unitaries on $\mathbb{C}^N \otimes \mathbb{C}^N$?
3. Can one generalize the results of [1, 5, 9, 10] to show that the communication cost of quantum Fourier transform for data shared between two parties remains maximal if a net transfer of data qudits is allowed to occur?

The cases $S \notin \{2, 4\}$ of question 1 are resolved using (3) by considering the cardinalities of the support of Fourier transforms of phase-valued functions $\lambda(\alpha, \beta) = \exp(\mathrm{i}\theta_{\alpha\beta})$. Resolving the remaining cases $S \in \{2, 4\}$ by inspection, theorem 10 shows that there exist unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$ with arbitrary Schmidt number $S \in \{1, \ldots, 9\}$. By the work of Dür *et al* [4], this result implies that there are nine equivalence classes of unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$ which are probabilistically interconvertible by (stochastic) local operations and classical communication.

Using the diagonal operator (3), question 2 is partially answered by existing mathematical studies of *biunimodular functions*, that is phase-valued functions whose discrete Fourier transforms are also phase-valued. Using a construction of Björck and Saffari [11],

---

[6] It would be very interesting to know if this asymptotic cost for approximate computation depends only on the operator-Schmidt coefficients of U. The reader is warned that the entanglement $K_{\mathrm{Sch}}(U)$ of $U : \mathcal{A} \otimes \mathcal{B} \to \mathcal{A} \otimes \mathcal{B}$ considered as an element of the vector-space $B(\mathcal{A}) \otimes B(\mathcal{B})$ (see definition 2) was shown by Nielsen *et al* [5] not to satisfy the chaining property. In particular, there exist U, V such that $K_{\mathrm{Sch}}(UV) > K_{\mathrm{Sch}}(U) + K_{\mathrm{Sch}}(V)$.

[7] See section 5 for a precise statement of this problem.

uncountably-many maximally-entangled unitaries on $\mathbb{C}^N \otimes \mathbb{C}^N$ may be constructed for N divisible by a square. However, it remains to check whether any two of the constructed A, B are not equivalent in the sense that

$$A = (U \otimes W)B(X \otimes Y) \tag{4}$$

for local unitaries U, W, X and Y. The problem of how to verify such equivalences completely has not (to our knowledge) been worked out for general A and B, and is left as an open problem. (This is related to [12], however.)

Question 3 is answered by computing the generalized operator-Schmidt decomposition of the quantum Fourier transform as a map from $\mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2}$ to $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ and applying a slight modification of Nielsen's bound.

In the appendix we remark on the 'magic basis' of Hill and Wootters [13].

1.2. Definitions and notation

Definition 1. *Let $\mathcal{A}$, $\mathcal{A}'$, $\mathcal{B}$ and $\mathcal{B}'$ be finite-dimensional Hilbert spaces, and let $F : \mathcal{A} \otimes \mathcal{B} \to \mathcal{A}' \otimes \mathcal{B}'$ be a nonzero linear transformation. The Hilbert–Schmidt space $B(\mathcal{A} \to \mathcal{A}')$ is the Hilbert space of linear transformations from $\mathcal{A}$ to $\mathcal{A}'$ under the Hilbert–Schmidt inner product*

$$\langle C, D\rangle_{B(\mathcal{A}\to\mathcal{A}')} = \operatorname*{Tr}_{\mathcal{A}} C^\dagger D$$

where

$$\langle C^\dagger \psi, \phi\rangle_{\mathcal{A}} = \langle \psi, C\phi\rangle_{\mathcal{A}'}$$

for all $\phi \in \mathcal{A}$ and $\psi \in \mathcal{A}'$. For simplicity, we define $B(\mathcal{H}) = B(\mathcal{H} \to \mathcal{H})$. A generalized operator-Schmidt decomposition of F is a decomposition of the form

$$F = \sum_{k=1}^{\mathrm{Sch}(F)} \lambda_k A_k \otimes B_k \qquad \lambda_k > 0 \tag{5}$$

where the $\{A_k\}_{k=1\ldots\mathrm{Sch}(F)}$ and $\{B_k\}_{k=1\ldots\mathrm{Sch}(F)}$ are orthonormal subsets of $B(\mathcal{A} \to \mathcal{A}')$ and $B(\mathcal{B} \to \mathcal{B}')$, respectively[8]*. The quantity* Sch(F) *is the Schmidt number, and the λ_k are the Schmidt coefficients. Equation (5) is an operator-Schmidt decomposition when restricted to the special case $\mathcal{A} = \mathcal{A}'$ and $\mathcal{B} = \mathcal{B}'$.*

We remark that the generalized operator-Schmidt decomposition is just a special case of the well-known Schmidt decomposition [3]

$$\psi = \sum_{k=1}^{\mathrm{Sch}(\psi)} \lambda_k\, e_k \otimes f_k \qquad \lambda_k > 0 \tag{6}$$

of a vector $\psi \in \mathcal{H} \otimes \mathcal{K}$, where the $\{e_k\}$ and $\{f_k\}$ are orthonormal. In particular, one sets $\mathcal{H} = B(\mathcal{A} \to \mathcal{A}')$, $\mathcal{K} = B(\mathcal{B} \to \mathcal{B}')$ and $\psi = F \in B(\mathcal{A}\otimes\mathcal{B} \to \mathcal{A}'\otimes\mathcal{B}')$. The decomposition (5) is then obtained by identifying $B(\mathcal{A} \to \mathcal{A}') \otimes B(\mathcal{B} \to \mathcal{B}')$ with $B(\mathcal{A}\otimes\mathcal{B} \to \mathcal{A}'\otimes\mathcal{B}')$ under the natural isomorphism[9]. Note that Sch(ψ) and the set $\{\lambda_k\}_{k=1,\ldots,\mathrm{Sch}(\psi)}$ are independent of the choice of decomposition, since they are just the rank and set of singular values of the map $|f\rangle_{\mathcal{K}} \mapsto \langle\psi||f\rangle_{\mathcal{K}} : \mathcal{K} \to \mathcal{H}^*$, respectively[10]. Furthermore,

---

[8] But not necessarily bases.

[9] In particular, there exists a unique unitary $\Xi : B(\mathcal{A} \to \mathcal{A}') \otimes B(\mathcal{B} \to \mathcal{B}') \to B(\mathcal{A}\otimes\mathcal{B} \to \mathcal{A}'\otimes\mathcal{B}')$ such that $(\Xi(A \tilde{\otimes} B))(f \otimes g) = (Af) \otimes (Bg)$ for all $f \in \mathcal{A}$ and $g \in \mathcal{B}$. Here $\tilde{\otimes}$ denotes the defining formal tensor product of $B(\mathcal{A} \to \mathcal{A}') \otimes B(\mathcal{B} \to \mathcal{B}')$, considering the factors as abstract Hilbert spaces.

[10] See definition 3 for the Hilbert-space structure of the dual space $\mathcal{H}^*$.

Definition 2. *The Schmidt strength* $K_{\mathrm{Sch}}(F)$ *of* $F : \mathcal{A}\otimes\mathcal{B} \to \mathcal{A}'\otimes\mathcal{B}'$ *[5] is the entanglement of* F *considered as an element of* $B(\mathcal{A} \to \mathcal{A}')\otimes B(\mathcal{B} \to \mathcal{B}')$.[11] F *is said to be maximally entangled if* $K_{\mathrm{Sch}}(F)$ *is maximized or, equivalently, if* $\mathrm{Sch}(F) = \min(\dim(\mathcal{A})\dim(\mathcal{A}'), \dim(\mathcal{B})\dim(\mathcal{B}'))$ *and all the operator-Schmidt coefficients are equal.*

We note that the Schmidt-number condition on maximally-entangled operators implies that they have maximal communication cost by Nielsen's bound (2) (see also the slight modification (24), below).

2. Schmidt decompositions given by the Fourier transform

The goal of this section is to construct the family of diagonal operators (3), whose operator-Schmidt coefficients are computed using the discrete Fourier transform. There are two ingredients in this construction:

1. The well-known isomorphism between $\mathcal{H}\otimes\mathcal{H}^*$ (defined below) and $B(\mathcal{H})$, which allows application of the tools of operator theory to the study of bipartite Hilbert spaces.
2. The characterization (up to a scalar) of the discrete Fourier transform by its action by conjugation on the Heisenberg–Weyl algebra.

Definition 3. *Let* $\mathcal{H}$ *be a Hilbert space of dimension* N *with inner product*[12] $\langle\bullet, \bullet\rangle_{\mathcal{H}}$, *and let* $\mathcal{H}^*$ *be its dual*[13]. *Define the natural antilinear map* $f \mapsto \bar{f} : \mathcal{H} \to \mathcal{H}^*$ *by*

$$\overline{|\psi\rangle} = \langle\psi| \tag{7}$$

and endow $\mathcal{H}^*$ *with the inner product* $\langle\bar{f}, \bar{g}\rangle_{\mathcal{H}^*} = \langle g, f\rangle_{\mathcal{H}}$. *For a linear operator* $A : \mathcal{H} \to \mathcal{H}$, *define the conjugate* $\bar{A} : \mathcal{H}^* \to \mathcal{H}^*$ *by*[14]

$$\bar{A}\bar{f} = \overline{Af}. \tag{8}$$

The natural isomorphism $A \mapsto |A\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*} : B(\mathcal{H}) \to \mathcal{H}\otimes\mathcal{H}^*$ *is the unitary map satisfying*

$$A = |f\rangle\langle g| \Longrightarrow |A\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*} = f \otimes \bar{g}$$

for all $f, g \in \mathcal{H}$, *where* $\otimes$ *on the right-hand side is the defining formal Hilbert-space tensor product of* $\mathcal{H}\otimes\mathcal{H}^*$.[15] *Let* $\mathbb{Z}_N = \{0, \ldots, N-1\}$ *and* $\mathbb{Z}_N^2 = \mathbb{Z}_N \times \mathbb{Z}_N$. *The computational basis is denoted by* $\{|j\rangle\}_{j\in\mathbb{Z}_N} \subseteq \mathcal{H}$.

The following lemma is a basis-free version of equations (6) and (10) of [15], with a similar proof:

Lemma 4. *Let* $A, B, C \in B(\mathcal{H})$. *Then* $(A \otimes \bar{B})|C\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*} = |ACB^\dagger\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*}$. *Furthermore,* $|C\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*}$ *is maximally entangled iff* C *is a nonzero scalar multiple of a unitary.*

---

[11] Hence $K_{\mathrm{Sch}}(F) = S(\mathrm{Tr}_{B(\mathcal{A}\to\mathcal{A}')}|F\rangle\langle F|)$, where S is the von-Neumann entropy $S(\rho) = -\mathrm{Tr}\rho\log\rho$.

[12] We take inner products to be linear in the second argument.

[13] The dual space $\mathcal{H}^*$ is the set of linear functionals $\ell : \mathcal{H} \to \mathbb{C}$. In Dirac notation, $\mathcal{H}^*$ is the space of bras.

[14] The suggestive use of bar-notation in (7)–(8) is motivated by the following formulae: $\psi = \sum_k a_k|k\rangle \to \bar{\psi} = \sum_k \bar{a}_k\overline{|k\rangle}$ and $A|j\rangle = \sum_k a_{jk}|k\rangle \to \bar{A}\,\overline{|j\rangle} = \sum_k \bar{a}_{jk}\overline{|k\rangle}$.

[15] The double-ket notation goes back to [14]. Equivalently, $\langle f\otimes\bar{g}|\cdot|A\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*} = \langle f, Ag\rangle_{\mathcal{H}}$ for all $f, g \in \mathcal{H}$, where $\cdot$ is the inner product on $\mathcal{H}\otimes\mathcal{H}^*$.

The second ingredient in our construction is the following:

Theorem 5 (H Weyl)**.** *Let $\mathcal{H}$ and N be as in definition 3. Then any irreducible unitary representation of the group generated by the discrete Weyl relations*

$$R^n = I \quad \text{iff } n \in N\mathbb{Z} \tag{9}$$

$$T^n = I \quad \text{iff } n \in N\mathbb{Z} \tag{10}$$

$$RT = \exp\left(-\frac{2\pi \mathrm{i}}{N}\right) TR \tag{11}$$

is unitarily equivalent to one in which R and T are represented on $\mathcal{H}$ as the right-shift operator and twist operator, respectively:

$$R|j\rangle = |j + 1 \bmod N\rangle \qquad j \in \mathbb{Z}_N \tag{12}$$

$$T|j\rangle = \exp\left(\frac{2\pi \mathrm{i} j}{N}\right)|j\rangle. \tag{13}$$

Furthermore, if F satisfies the associated Fourier relations

$$FRF^{-1} = T$$
$$FTF^{-1} = R^{-1}$$

then F will be simultaneously represented (up to a scalar factor λ) as the discrete Fourier transform:

$$\langle j|F|k\rangle = \frac{\lambda}{\sqrt{N}} \exp\left(\frac{2\pi \mathrm{i}}{N} jk\right).$$

The first part of the theorem is given in [16]. The second part follows trivially from Schur's lemma. Weyl considered the representations of the discrete Weyl relations because they are a finite-dimensional analogue of the canonical commutation relation $[P, Q] = -\mathrm{i}$ for self-adjoint P and Q.[16]

Definition 6. *The discrete Fourier transform of functions on $\mathbb{Z}_N^2$ is given by*

$$\hat{\lambda}(a, b) = \frac{1}{N} \sum_{\alpha,\beta=0}^{N-1} \exp\left(\frac{2\pi \mathrm{i}}{N}(\alpha a + \beta b)\right) \lambda(\alpha, \beta).$$

Theorem 7. *Take $R, T \in B(\mathcal{H})$ to be given by (12)–(13). Let*

$$\Phi_{\alpha\beta} = N^{-1/2} |T^\alpha R^{-\beta}\rangle\rangle_{\mathcal{H}\otimes\mathcal{H}^*}$$

for $\alpha, \beta \in \mathbb{Z}_N$. Then the $\Phi_{\alpha\beta}$ form a maximally-entangled orthonormal basis of $\mathcal{H} \otimes \mathcal{H}^*$. Furthermore, for an arbitrary function $\lambda : \mathbb{Z}_N^2 \to \mathbb{C}$, the diagonal operator D

$$D = \sum_{\alpha,\beta=0}^{N-1} \lambda(\alpha, \beta) |\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}| : \mathcal{H} \otimes \mathcal{H}^* \to \mathcal{H} \otimes \mathcal{H}^* \tag{14}$$

---

[16] See [18] for the representations of the infinite-dimensional Weyl relations (due to von Neumann). See [17] for their relationship to the CCR, and for an example (essentially due to Ed Nelson) of an irreducible representation of the CCR on $L^2(\mathbb{R})$ that is *not* unitarily equivalent to $Q = x$, $P = -\mathrm{i}\, \mathrm{d}/\mathrm{d}x$.

satisfies the relation

$$D = \frac{1}{N}\sum_{a,b=0}^{N-1} \hat{\lambda}(a,b) \times (R^a T^b) \otimes \overline{(R^a T^b)}. \tag{15}$$

In particular, a Schmidt decomposition of D is given by

$$D = \sum_{a,b} |\hat{\lambda}(a,b)| \times \left(\frac{\hat{\lambda}(a,b)}{|\hat{\lambda}(a,b)|}\frac{1}{\sqrt{N}}R^a T^b\right) \otimes \overline{\left(\frac{1}{\sqrt{N}}R^a T^b\right)} \tag{16}$$

where the summation is over the $a, b \in \mathbb{Z}_N$ *such that* $\hat{\lambda}(a,b) \neq 0$.

Proof. It was observed by Schwinger [19] that the set $\{N^{-1/2}T^\alpha R^{-\beta}\}_{\alpha,\beta\in\mathbb{Z}_N}$ is an orthonormal basis of $B(\mathcal{H})$. That the $\Phi_{\alpha\beta}$ form an orthonormal basis of $\mathcal{H}\otimes\mathcal{H}^*$ follows by the natural isomorphism. Maximal entanglement follows from the second part of lemma 4.

By lemma 4 and the Weyl relations (11), each $\Phi_{\alpha\beta}$ is an eigenvector of each $(R^a T^b) \otimes \overline{(R^a T^b)}$:

$$\begin{aligned}(R^a T^b) \otimes \overline{(R^a T^b)}\Phi_{\alpha\beta} &= N^{-1/2}|R^a T^b T^\alpha R^{-\beta}(R^a T^b)^\dagger\rangle\rangle \\ &= \exp\left(-\frac{2\pi \mathrm{i}}{N}(a\alpha + b\beta)\right)\Phi_{\alpha\beta}.\end{aligned} \tag{17}$$

Since the $\Phi_{\alpha\beta}$ form an orthonormal basis, (17) becomes

$$(R^a T^b) \otimes \overline{(R^a T^b)} = \sum_{\alpha\beta=0}^{N-1} \exp\left(-\frac{2\pi \mathrm{i}}{N}(a\alpha + b\beta)\right)|\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}|.$$

By the Fourier inversion theorem,

$$|\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}| = \frac{1}{N^2}\sum_{a,b=0}^{N-1} \exp\left(\frac{2\pi \mathrm{i}}{N}(a\alpha + b\beta)\right)(R^a T^b) \otimes \overline{(R^a T^b)}.$$

Hence

$$\begin{aligned}D &= \sum_{\alpha,\beta=0}^{N-1} \lambda(\alpha,\beta)|\Phi_{\alpha\beta}\rangle\langle\Phi_{\alpha\beta}| \\ &= \sum_{\alpha,\beta=0}^{N-1} \lambda(\alpha,\beta)\frac{1}{N^2}\sum_{a,b=0}^{N-1} \exp\left(\frac{2\pi \mathrm{i}}{N}(a\alpha + b\beta)\right)(R^a T^b) \otimes \overline{(R^a T^b)} \\ &= \frac{1}{N}\sum_{a,b=0}^{N-1} \hat{\lambda}(a,b)(R^a T^b) \otimes \overline{(R^a T^b)}.\end{aligned}$$

By the orthonormality of the $N^{-1/2}R^a T^b$, (16) is a Schmidt decomposition. □

Remark 8. By the lemmas used in [7] to prove the canonical decomposition (1) one has the following fact: up to local unitaries in the sense of (4), for $N = 2$ every unitary on $\mathcal{H}\otimes\mathcal{H}^*$ is of the form (14) even if the $\Phi_{\alpha\beta}$ are replaced by an arbitrary maximally-entangled basis.

3. Application to Schmidt numbers of unitaries

In this section we produce the allowed Schmidt numbers of unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$, solving a special case of the problem of Nielsen *et al* [5] which prompted our investigations here. By theorem 7, one may produce a unitary of Schmidt number S from a 'unimodular' function $\lambda : \mathbb{Z}_N^2 \to \{|z| = 1\}$ whose Fourier transform $\hat{\lambda}$ has support of cardinality S.

Lemma 9. *There exists a function* $\lambda : \mathbb{Z}_3^2 \to \{|z| = 1\}$ *such that the support of* $\hat{\lambda}$ *has cardinality* S *iff* $S \in \{1, 3, 5, 6, 7, 8, 9\}$.

Proof. Define g_1 and $g_3 : \mathbb{Z}_3 \to \{|z| = 1\}$ by declaring $g_1 = 1$ identically and choosing g_3 such that $\operatorname{supp} \hat{g}_3 = \mathbb{Z}_3$. Then the support of the Fourier transform of $(g_a \otimes g_b)(j, k) = g_a(j) g_b(k)$ has cardinality $S = ab \in \{1, 3, 9\}$. For a function $\lambda : \mathbb{Z}_3^2 \to \mathbb{C}$, let $\Gamma\lambda$ be the 3×3 matrix whose j, k entry is $\lambda(j, k)$, $j, k \in \mathbb{Z}_3$. Setting

$$\omega = \exp\left(\frac{2\pi \mathrm{i}}{3}\right)$$

one has the following table of unimodular λ_S such that the support of $\hat{\lambda}_S$ has cardinality S:

S	$\Gamma\lambda_S$	$\Gamma\hat{\lambda}_S$
5	$\begin{bmatrix} 1 & -1 & 1 \\ \omega & -\omega & \omega^2 \\ \omega^2 & -\omega^2 & \omega \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 1 & \omega^2 & \omega \\ 0 & 1-\omega & 1-\omega^2 \end{bmatrix}$
6	$\begin{bmatrix} 1 & 1 & 1 \\ \omega & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{bmatrix}$	$\begin{bmatrix} 0 & 0 & 0 \\ 1 & \omega^2 & \omega \\ 2 & 1+\omega & 1+\omega^2 \end{bmatrix}$
7	$\begin{bmatrix} 1 & \omega & \omega^2 \\ 1 & -\omega^2 & \omega \\ -1 & \omega^2 & -\omega \end{bmatrix}$	$\frac{1}{3}\begin{bmatrix} 0 & 0 & 3 \\ -2+2\omega & 1+2\omega & 7+2\omega \\ 2-2\omega & -1-2\omega & -1-2\omega \end{bmatrix}$
8	$\begin{bmatrix} \omega & \omega & \omega^2 \\ 1 & -\omega^2 & \omega^2 \\ -1 & 1 & -\omega \end{bmatrix}$	$\frac{1}{3}\begin{bmatrix} 0 & -3+3\omega & 3 \\ -2+2\omega & 1+2\omega & 4+5\omega \\ -1+\omega & -1-2\omega & -1-2\omega \end{bmatrix}$

Now let $P \subseteq \mathbb{Z}_3^2$ have cardinality $S = 2$ or 4. We claim that there exists a nonzero $v \in \mathbb{Z}_3^2$ such that there exists a unique $x \in P$ such that $x + v \bmod 3\mathbb{Z}^2 \in P$. For $S = 2$ this fact is trivial. For $S = 4$, by a modular translation and a rotation, one can assume without loss of generality that the points $(0, 0)$ and $(0, 1)$ are in P. But then either $(0, 2) \in P$ or there is another adjacent pair (s, t) and $(s, t + 1) \in P$. In either case a contradiction follows by inspection.

Now suppose λ is unimodular and $\hat{\lambda}$ has cardinality 2 or 4. Let P be the support of $\hat{\lambda}$ and take v and x to be as in the previous paragraph. Then

$$\begin{aligned} 0 = \delta_{v,0} &= \widehat{(\bar{\lambda}\lambda)}(-v \bmod 3\mathbb{Z}^2) \\ &= \frac{1}{N} \sum_{w \in \mathbb{Z}_3^2} \bar{\hat{\lambda}}(v + w \bmod 3\mathbb{Z}^2)\hat{\lambda}(w) \\ &= \frac{1}{N} \bar{\hat{\lambda}}(v + x \bmod N\mathbb{Z}^2)\hat{\lambda}(x) \neq 0 \end{aligned}$$

yielding a contradiction. □

Theorem 10. *There exist unitary operators on $\mathbb{C}^3 \otimes \mathbb{C}^3$ with Schmidt number S, for every $S \in \{1, \ldots, 9\}$.*

Proof. By theorem 7 and lemma 9, all that remains is to check that there exist unitaries on $\mathbb{C}^3 \otimes \mathbb{C}^3$ with the Schmidt numbers 2 and 4. Setting

$$P_1 = \mathrm{diag}(1, 0, 0) \qquad P_2 = \mathrm{diag}(0, 1, 1)$$

both of the following unitary operators have Schmidt number 2:

$$U = P_1 \otimes R + P_2 \otimes I$$
$$V = R \otimes P_1 + I \otimes P_2$$

where R is given by (12). Furthermore, their product

$$UV = P_1R \otimes RP_1 + P_1 \otimes RP_2 + P_2R \otimes P_1 + P_2 \otimes P_2$$

has Schmidt number 4, since this is already a Schmidt decomposition, except for normalizations. □

4. A connection between maximally-entangled unitaries and biunimodular functions

Theorem 7 gives some insight into the problem of constructing maximally-entangled unitaries on $\mathbb{C}^N \otimes \mathbb{C}^N$. The best-known example of such a unitary is the SWAP operator $f \otimes g \mapsto g \otimes f$ on $\mathbb{C}^N \otimes \mathbb{C}^N$, with Schmidt decomposition

$$\mathrm{SWAP} = \sum_{j=1}^{N^2} A_j \otimes A_j^\dagger \tag{18}$$

where $\{A_j\}_{j=1\ldots N^2}$ is *any* orthonormal basis of $B(\mathbb{C}^N)$.[17] Furthermore, corollary 15 shows that the quantum Fourier transform $\mathcal{F}_{M_1M_2\to N_1N_2} : \mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2} \to \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ is maximally entangled in many cases, including the case where only one species of qudit is present[18].

Theorem 7 shows that the diagonal operator D on $\mathbb{C}^N \otimes \mathbb{C}^N$ (14) is maximally entangled and unitary iff $\lambda : \mathbb{Z}_N^2 \to \mathbb{C}$ is *biunimodular* [20], i.e. both λ and $\hat{\lambda}$ have ranges lying in the circle $\{|z| = 1\}$. To characterize the biunimodular functions on $\mathbb{Z}_N^2$ is a generalization of a studied problem of considerable difficulty: to characterize the biunimodular functions on $\mathbb{Z}_N$.

Known examples of biunimodular functions on $\mathbb{Z}_N^2$ come as tensor products $f(x)g(y)$ of biunimodular functions f and g on $\mathbb{Z}_N$. The first examples of biunimodular functions on $\mathbb{Z}_N$ were known to Gauss: for odd N there are the biunimodular Gaussians $g_{N,a,b} : \mathbb{Z}_N \to \mathbb{C}$, for $a, b \in \mathbb{Z}_N$ with a coprime to N, given by

$$g_{N,a,b}(k) = \exp\left(\frac{2\pi \mathrm{i}}{N}(ak^2 + bk)\right)$$

and for even N one has

$$g_N(k) = \exp\left(\frac{2\pi \mathrm{i}}{N}k^2\right).$$

For N divisible by a square, these Gaussian examples are special cases of the following theorem:

---

[17] Since $\langle A_j \otimes A_k^*, \mathrm{SWAP}\rangle_{B(\mathbb{C}^n\otimes\mathbb{C}^n)} = \langle A_j, A_k\rangle_{B(\mathbb{C}^n\otimes\mathbb{C}^n)} = \delta_{jk}$, equation (18) is just the coordinate expansion of SWAP in the orthonormal basis $\{A_j \otimes A_k^*\}$ of $B(\mathbb{C}^n \otimes \mathbb{C}^n)$.

[18] Special cases of the general result (22) were given in [1, 5, 10].

Theorem 11 (Björck and Saffari [11])**.** *Let* n^2 *be the largest square dividing N. If* $n > 1$ *then there exist infinitely many biunimodular functions on* $\mathbb{Z}_N$*. In particular, setting* $m = N/n$*,*

Case 1: Either n is even or m is odd. An infinite set of biunimodular functions $f_{\tau,\mathcal{C},\rho} : \mathbb{Z}_N \to \mathbb{C}$ *is given by*

$$f_{\tau,\mathcal{C},\rho}(k) = c_h \rho^{r\tau(h)+nr(r-1)/2} \tag{19}$$

where k has 'mixed-decimal' expansion $k = nr + h$ *(with* $0 \leqslant h < n, 0 \leqslant r < m$*), where* $\mathcal{C} = (c_0, \ldots, c_{n-1})$ *is an arbitrary unimodular sequence of length n,* τ *is any permutation of* $\{0, 1, \ldots, n-1\}$ *and* ρ *is any primitive mth root of unity.*

Case 2: n is odd and m is even. Each function $g_{\tau,\mathcal{C},\rho} : \mathbb{Z}_N \to \mathbb{C}$ *of the following form is biunimodular:*

$$g_{\tau,\mathcal{C},\rho}(k) = z_{k \bmod 2} \times f_{\tau,\mathcal{C},\rho}(k \bmod (N/2))$$

where z is the sequence $z = (1, i)$ *and where* $f_{\tau,\mathcal{C},\rho} : \mathbb{Z}_{N/2} \to \mathbb{C}$ *is a biunimodular function generated using case 1.*

For further results on biunimodular functions, see [20–23].

5. Generalized Schmidt decomposition of the quantum Fourier transform

In this section, we consider the communication complexity of the bipartite quantum Fourier transform when a net transfer of data is allowed to occur between the two parties, generalizing the decompositions of [1, 5, 10].

Definition 12. *The quantum Fourier transform* $\mathcal{F}_{M_1M_2\to N_1N_2} : \mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2} \to \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$*, with* $N = N_1N_2 = M_1M_2$*, is the unitary map satisfying*

$$_{N_1}\langle j|\, _{N_2}\langle k|\, \mathcal{F}_{M_1M_2\to N_1N_2}\, |\ell\rangle_{M_1}\, |m\rangle_{M_2} = \frac{1}{\sqrt{N}} \exp\left(\frac{2\pi \mathrm{i}}{N}(jN_2 + k)(\ell M_2 + m)\right).$$

The communication cost of a unitary operation $U : \mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2} \to \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ *is given by*

$$Q_0(U) = \min \sum_{d=2}^{\infty} N_d \log_2(d)$$

where the minimum is over all protocols to compute U using ancilla, local operations and the transmission of N_d *qudits of dimension d, for* $d \geqslant 2$*. The communication cost of U is said to be maximal if* $Q_0(U) = \log_2 \min(M_1N_1, M_2N_2)$*.*

This is just the usual quantum Fourier transform, with the data shared by Alice and Bob using mixed decimals $|\ell\rangle_{M_1}|m\rangle_{M_2} \leftrightarrow |\ell M_2 + m\rangle_N$ before (and $|j\rangle_{N_1}|k\rangle_{N_2} \leftrightarrow |jN_2 + k\rangle_N$ after) the computation. We note that the dimensions of Alice and Bob's local Hilbert spaces change upon each communication of a qudit, although the product of the dimensions remains constant. Furthermore, the trivial bound

$$Q_0(U) \leqslant \log_2 \min(M_1N_1, M_2N_2) \tag{20}$$

for any $U : \mathbb{C}^{M_1} \otimes \mathbb{C}^{M_2} \to \mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ follows from the fact that Alice could send all her qudits to Bob, who would perform the computation and send back the required ones (or vice versa).

We now state the generalized Schmidt decomposition of $\mathcal{F}_{M_1M_2\to N_1N_2}$. A proof and derivation are not included, as they scarcely differ from those in [10].

Definition 13. *Let* $\mathbb{Z}_N = \{0, \ldots, N-1\}$*. The equivalence classes of* $\mathbb{Z}_{N_2} \times \mathbb{Z}_{M_2}$ *mod* (M_1, N_1) *consist of all sets of the form*

$$C = \{(a + M_1 k_1, b + N_1 k_2) | a \in \mathbb{Z}_{N_2}, b \in \mathbb{Z}_{M_2}, k_1, k_2 \in \mathbb{Z}\} \cap \left(\mathbb{Z}_{N_2} \times \mathbb{Z}_{M_2}\right)$$

where addition is NOT modular.

Note that we do not consider equivalence classes of $\mathbb{Z}_{N_2} \times \mathbb{Z}_{M_2}$ mod (N_1, M_1): the order of the N and M switches.

Theorem 14. *Let* $N = N_1 N_2 = M_1 M_2$*. Then* $\mathcal{F}_{M_1 M_2 \to N_1 N_2}$ *has generalized Schmidt decomposition*

$$\mathcal{F}_{M_1 M_2 \to N_1 N_2} = \sum_C \lambda_c A_C \otimes B_C$$

where the summation is over equivalence classes C *of* $\mathbb{Z}_{N_2} \times \mathbb{Z}_{M_2}$ *mod* (M_1, N_1)*, and where*

$$\begin{aligned} \lambda_C &= \sqrt{\frac{N_1 M_1 \mathrm{Card}(C)}{N}} \\ (A_C)_{jk} &= \frac{1}{\sqrt{N_1 M_1}} \exp\left[\frac{2\pi \mathrm{i}}{N}(N_2 M_2 jk + M_2 k\hat{s} + N_2 j\hat{t})\right] \qquad \mathit{for} (\hat{s}, \hat{t}) \in C \\ (B_C)_{jk} &= \frac{1}{\sqrt{\mathrm{Card}(C)}} \times \begin{cases} \exp\left(\frac{2\pi \mathrm{i}}{N} jk\right) & \text{if } (j,k) \in C \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

with $\mathrm{Card}(C)$ *denoting the cardinality of* C*. Note that the definition of* A_C *is independent of the choice of* $(\hat{s}, \hat{t}) \in C$*.*

Corollary 15. *In all cases*

$$\mathrm{Sch}\left(\mathcal{F}_{M_1 M_2 \to N_1 N_2}\right) = \min(M_1 N_1, M_2 N_2). \tag{21}$$

In particular, the communication cost of $Q_0\left(\mathcal{F}_{M_1 M_2 \to N_1 N_2}\right)$ *is maximal in all cases. Furthermore,* $\mathcal{F}_{M_1 M_2 \to N_1 N_2}$ *is maximally entangled iff*

$$(M_1 \textit{ is a factor of } N_2 \textit{ or } M_1 > N_2)$$

or equivalently

$$(N_1 \textit{ is a factor of } M_2 \textit{ or } N_1 > M_2). \tag{22}$$

Otherwise $\mathcal{F}_{M_1 M_2 \to N_1 N_2}$ *has at most three distinct Schmidt coefficients (of various multiplicities), taking values of the form*

$$\sqrt{\frac{N_1 M_1}{N} ab}$$

where we ignore Schmidt coefficients stated as zero, and where

$$a, b \in \{\lfloor N_2/M_1 \rfloor, \lceil N_2/M_1 \rceil\} = \{\lfloor M_2/N_1 \rfloor, \lceil M_2/N_1 \rceil\}$$

Proof. Equation (21) follows by a simple counting argument. That the communication cost is maximal then follows from a slight modification of the work of Nielsen *et al* in [5], as follows[19]. Replacing the Schmidt decomposition by the generalized Schmidt decomposition in the definition of the Hartley strength [5] and replacing the SWAP operator in section $III.B.3$ of [5] by communication operators[20]

$$C : (\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}) \otimes \mathbb{C}^{d_3} \to \mathbb{C}^{d_1} \otimes (\mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3})(f \otimes g) \otimes h \mapsto f \otimes (g \otimes h) \tag{23}$$

---

[19] This idea was mentioned vaguely in footnote 10 of [5] and in footnotes 1 and 6 of [10].

[20] As stated in [10], the communication operator has generalized Schmidt-decomposition $C = \sum_{k=1}^{d_2} \sqrt{d_1 d_3} A_k \otimes B_k$, where $A_k = d_1^{-1/2} \sum_{i=1}^{d_1} |i\rangle\langle ik| : \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2} \to \mathbb{C}^{d_1}$ and $B_k = d_3^{-1/2} \sum_{i=1}^{d_3} |ki\rangle\langle i| : \mathbb{C}^{d_3} \to \mathbb{C}^{d_2} \otimes \mathbb{C}^{d_3}$.

one immediately obtains the following version of Nielsen's bound (2):

$$K_{\mathrm{har}}\big(\mathcal{F}_{M_1M_2\to N_1N_2}\big) \leqslant Q_0\big(\mathcal{F}_{M_1M_2\to N_1N_2}\big). \tag{24}$$

Hence the left-hand side of (24) equals the right-hand side of (20), proving the communication cost is maximal, as claimed. The rest of this corollary is trivial. □

Acknowledgment

We would like to thank Mike Nielsen, Andreas Klappenecker, Bahman Saffari, Harold Shapiro and Petre Dita for their correspondence, J I Cirac and G Vidal for pointing out their interesting reference and Arthur Jaffe for his encouragement.

Appendix. The magic basis, without the basis

The natural isomorphism $A \mapsto |A\rangle\rangle : B(\mathcal{H}) \to \mathcal{H} \otimes \mathcal{H}^*$ has allowed us application of the tools of operator theory on $B(\mathcal{H})$ to the study of bipartite tensor product spaces in a natural manner. In this spirit we list below the properties of the gradient of the determinant, which we will relate to 'conjugation in the magic basis' of Hill and Wootters [13]:

Theorem 16. *The determinant is everywhere-differentiable on* $B(\mathcal{H})$. *In particular, the determinant has a gradient* $\mathcal{G} : B(\mathcal{H}) \to B(\mathcal{H})$ *such that*

$$\frac{\mathrm{d}}{\mathrm{d}t}\det(A) = \left\langle \mathcal{G}(A), \frac{\mathrm{d}A}{\mathrm{d}t} \right\rangle_{B(\mathcal{H})}$$

for differentiable functions $A : \mathbb{R} \to B(\mathcal{H})$. *Define the corresponding map* $\mathfrak{D} : \mathcal{H} \otimes \mathcal{H}^* \to \mathcal{H} \otimes \mathcal{H}^*$ *by*

$$\mathfrak{D}|A\rangle\rangle = |\mathcal{G}(A)\rangle\rangle.$$

Taking $\lambda \in \mathbb{C}$, $A, B \in B(\mathcal{H})$, $\psi \in \mathcal{H} \otimes \mathcal{H}^*$ *and* $N = \dim(\mathcal{H})$, *the functions* $\mathcal{G}$ *and* $\mathfrak{D}$ *have the following properties:*

1. $\mathcal{G}$ *is the continuous extension of the map* $A \mapsto ((\det A)A^{-1})^{\dagger}$ *from invertible* A *to all* A.
2. $\mathcal{G}(AB) = \mathcal{G}(A)\mathcal{G}(B)$ *and* $\mathcal{G}(A^{\dagger}) = (\mathcal{G}(A))^{\dagger}$. *In particular,* $\mathcal{G}$ *acts independently on the factors of the polar decomposition.*
3. $\mathfrak{D}((A \otimes \bar{B})\psi) = (\mathcal{G}(A) \otimes \overline{\mathcal{G}(B)})\mathfrak{D}(\psi)$. *In particular, if* A *and* B *are unitary then* $\mathfrak{D}((A \otimes \bar{B})\psi) = (\det A^{\dagger}B)(A \otimes \bar{B})\mathfrak{D}(\psi)$.
4. $\mathfrak{D}(\psi) = \alpha\psi$ *for some* $\alpha \in \mathbb{C}$ *iff* ψ *is maximally entangled or zero. Furthermore, for* $N \geqslant 3$ *the maximizers of* $\|\mathfrak{D}(\psi)\|_{\mathcal{H}\otimes\mathcal{H}^*}/\|\psi\|_{\mathcal{H}\otimes\mathcal{H}^*}$ *are precisely the maximally-entangled states.*
5. *Temporarily allowing Schmidt coefficients to vanish, the product of the Schmidt coefficients of* ψ *is given by* $N^{-1}|\langle\psi, \mathfrak{D}\psi\rangle_{\mathcal{H}\otimes\mathcal{H}^*}|$.
6. *Furthermore, if* $N = 2$ *then*
   (a) $\mathcal{G}$ *and* $\mathfrak{D}$ *are conjugations, i.e. antiunitary maps squaring to the identity.*
   (b) ψ *is separable iff* $\langle\psi, \mathfrak{D}\psi\rangle = 0$.
   (c) *Denote* $|i\bar{j}\rangle \equiv |i\rangle \otimes \overline{|j\rangle} \in \mathcal{H} \otimes \mathcal{H}^*$. *Then each of the following vectors are invariant under* $\mathfrak{D}$:

$$\{|0\bar{0}\rangle + |1\bar{1}\rangle, i|0\bar{0}\rangle - i|1\bar{1}\rangle, i|0\bar{1}\rangle + i|1\bar{0}\rangle, |0\bar{1}\rangle - |1\bar{0}\rangle\}. \tag{A1}$$

Furthermore, they form an orthonormal basis.

(d) If $A = \mathrm{e}^{\mathrm{i}\theta} UP$, *where* $U \in SU(2)$ *and* $P = \mathrm{diag}(\lambda_1, \lambda_2)$ *is positive, then* $\mathcal{G}(A) = \mathrm{e}^{-\mathrm{i}\theta} U \mathrm{diag}(\lambda_2, \lambda_1)$. *In particular,* $\mathfrak{D}$ *preserves Schmidt coefficients.*

For $N = 2$, $\mathfrak{D}$ is an analogue of conjugation of coordinates in the so-called 'magic basis' of [13], which is recovered by simply removing the bars from (A1).[21] We note that Vollbrecht and Werner [24] make the following point:

> The remarkable properties of the [magic] basis ... are in some sense not so much a property of that basis, but of the antiunitary operation of *complex conjugation* in [that] basis.

In particular, one may canonically translate the results and the magic basis or magic-conjugation proofs of [7, 8, 13, 25] on $\mathbb{C}^2 \otimes \mathbb{C}^2$ into basis-free results and proofs on $\mathcal{H} \otimes \mathcal{H}^*$. Hence, it is apparent that choice of a basis (or of a basis-dependent conjugation) is necessary in the cited proofs because choice is necessary to select an isomorphism between $\mathcal{H} \otimes \mathcal{H}$ and $\mathcal{H} \otimes \mathcal{H}^*$.

References

[1] Nielsen M A 1998 *PhD Thesis* University of New Mexico *Preprint* quant-ph/0011036 ch 6

[2] Preskill J 1998 Online course notes *Physics 229: Quantum Computation and Information* California Institute of Technology http://www.theory.caltech.edu/people/preskill/

[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) pp 109–11

[4] Dür W, Vidal G and Cirac J I 2002 Optimal conversion of nonlocal unitary operations *Phys. Rev. Lett.* **89** 057901 (*Preprint* quant-ph/0112124)

[5] Nielsen M A, Dawson C M, Dodd J L, Gilchrist A, Mortimer D, Osborne T J, Bremmer M J, Harrow A W and Hines A 2003 Quantum dynamics as a physical resource *Phys. Rev.* A **67** 052301 (The published version is preferred, since the communication bound in the January 2003 arXiv version had a typo. This could confuse the reader of Nielsen's *stronger* bound of [9] or of section 5 here)

[6] Khaneja N, Brockett R and Glaser S J 2001 Time optimal control of spin systems *Phys. Rev.* A **63** 032308 (*Preprint* quant-ph/0006114)

[7] Kraus B and Cirac J I 2001 Optimal creation of entanglement using a two-qubit gate *Phys. Rev.* A **63** 062309 (LANL *Preprint* quant-ph/0011050)

[8] Makhlin Y 2000 Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations LANL *Preprint* quant-ph/0002045

[9] Nielsen M A 2000 Entanglement and distributed quantum computation *Talk at the Benasque Center for Physics, July 19, 2000* http://www.qinfo.org/talks/index.html

[10] Tyson J 2003 Operator-Schmidt decomposition of the quantum Fourier transform on $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ *J. Phys. A: Math. Gen.* **36** 6485–91 (*Preprint* quant-ph/0210100)

[11] Björck G and Saffari B 1995 New classes of finite unimodular sequences with unimodular Fourier transforms. Circulant Hadamard matrices with complex entries *C. R. Acad. Sci. Paris Sér. I Math.* **320** 319–24

[12] Grassl M, Rötteler M and Beth T 1998 Computing local invariants of qubit systems *Phys. Rev.* A **58** 1833–9 (*Preprint* quant-ph/9712040)

[13] Hill S and Wootters W K 1997 Entanglement of a pair of quantum bits *Phys. Rev. Lett.* **78** 5022–5 (*Preprint* quant-ph/9703041)

[14] Baranger M 1958 Problem of overlapping lines in the theory of pressure broadening *Phys. Rev.* **111** 494–504

[15] D'Ariano G M, Lo Presti P and Sacchi M 2000 Bell measurements and observables *Phys. Lett.* A **272** 32–8 (*Preprint* quant-ph/0005121)

[16] Weyl H 1950 *Theory of Groups and Quantum Mechanics* (New York: Dover) pp 272–80 ch 4 sections 14–15 (translation of the second rev. German ed H P Robinson)

[17] Reed M and Simon B 1980 *Methods of Modern Mathematical Physics I: Functional Analysis* revised and enlarged edition (New York: Academic) p 275

---

[21] For $N = 2$ the properties 4, 5, 6a and 6b are just the $\mathcal{H} \otimes \mathcal{H}^*$ analogues of the useful properties of the magic basis.

[18] Reed M and Simon B 1983 *Methods of Modern Mathematical Physics III: Scattering Theory* (New York: Academic) pp 217–8

[19] Schwinger J 1960 Unitary operator bases *Proc. Natl. Acad. Sci.* **46** 570–9

[20] Björck G 1990 Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and 'cyclic n-roots *Recent Advances in Fourier Analysis and its Applications* ed J S Byrnes and J L Byrnes (Dordrecht: Kluwer) pp 131–40

[21] Backelin J and Fröberg R 1991 How we proved that there are exactly 924 cyclic 7-roots *Proc. ISAAC '91* ed S M Watt (New York: ACM) pp 103–11

[22] Björck G and Fröberg R 1991 A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots *J. Symb. Comput.* **12** 329–36

[23] Björck G and Fröberg R 1994 Methods to 'divide out' certain solutions from systems of algebraic equations, applied to find all cyclic 8-roots *Analysis, Algebra, and Computers in Math. Research* ed M Gyllenberg and L E Persson (New York: Dekker) pp 57–70

[24] Vollbrecht K G H and Werner R F 2000 Why two qubits are special *J. Math. Phys.* **41** 6772–82 (*Preprint* quant-ph/9910064)

[25] Wootters W 1998 Entanglement of formation of an arbitrary state of two qubits *Phys. Rev. Lett.* **80** 2245–8 (*Preprint* quant-ph/9709029)