Operator-Schmidt decomposition of the quantum Fourier transform on $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$

2003 J. Phys. A: Math. Gen. 36 6813

(http://iopscience.iop.org/0305-4470/36/24/317)

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

J. Phys. A: Math. Gen. **36** (2003) 6813–6819 PII: S0305-4470(03)58461-X

Operator-Schmidt decomposition of the quantum Fourier transform on $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$

Jon Tyson

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

E-mail: jonetyson@post.harvard.edu

Received 15 January 2003, in final form 17 April 2003
Published 5 June 2003
Online at stacks.iop.org/JPhysA/36/6813

Abstract

Operator-Schmidt decompositions of the quantum Fourier transform on $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ are computed for all $N_1, N_2 \geqslant 2$. The decomposition is shown to be completely degenerate when N_1 is a factor of N_2 and when $N_1 > N_2$. The first known special case, $N_1 = N_2 = 2^n$, was computed by Nielsen in his study of the communication cost of computing the quantum Fourier transform of a collection of qubits equally distributed between two parties (M A Nielsen 1998 *PhD Thesis* University of New Mexico ch 6 *Preprint* quant-ph/0011036). More generally, the special case $N_1 = 2^{n_1} \leqslant 2^{n_2} = N_2$ was computed by Nielsen *et al* in their study of strength measures of quantum operations (M A Nielsen *et al* 2002 *Preprint* quant-ph/0208077 (2003 *Phys. Rev.* A at press)). Given the Schmidt decompositions presented here, it follows that in all cases the bipartite communication cost of exact computation of the quantum Fourier transform is maximal.

PACS number: 03.67.−a

1. Introduction

Operator-Schmidt decompositions are useful for quantifying the nonlocal nature of operators on finite-dimensional bipartite Hilbert spaces. The first special cases of Schmidt decompositions of the quantum Fourier transform were computed by Nielsen [1] to illustrate his study of coherent quantum communication complexity. He considered the following problem:

> Suppose Alice is in possession of m qubits, Bob is in possession of n qubits, and they wish to perform some general unitary operation U which acts on their $m + n$ qubits. How many qubits must be communicated between Alice and Bob for them to achieve this goal?

Nielsen proved that the number $Q_0(U)$ of such qubits was bounded by

$$1/2 \times K_{\mathrm{Har}}(U) \leqslant Q_0(U) \leqslant 2\min(n, m) \tag{1}$$

where the *Hartley strength* K_{Har} satisfies

$$K_{\mathrm{Har}}(U) \equiv \log_2(\mathrm{Sch}(U))$$

where $\mathrm{Sch}(U)$, defined in definition 4 below, is the number of nonzero Schmidt coefficients of U. The upper bound of (1) is trivial, for Alice could simply send her qubits to Bob and let him send them back after performing U, or vice versa. To illustrate his theorem, Nielsen considered the quantum Fourier transform $\mathcal{F}_{2^n\times 2^n}$ on $n+n$ qubits. He showed that $K_{\mathrm{Har}}(\mathcal{F}_{2^n\times 2^n}) = 2n$, yielding $n \leqslant Q_0(\mathcal{F}_{2^n\times 2^n}) \leqslant 2n$. Subsequent work by Nielsen [2] improved the *general* lower bound of (1) by a factor of two[1], in particular implying that

$$Q_0(\mathcal{F}_{2^n\times 2^n}) = 2n.$$

In a later paper [3], Nielsen and collaborators further employ operator Schmidt decompositions in the quantitative study of *strength measures* of the nonlocal action of unitary operators[2]. Besides revisiting the Hartley strength, among the several strength measures considered is the *Schmidt strength*,

$$K_{\mathrm{Sch}}(U) = H\left(\left\{\frac{\lambda_k^2}{\dim(\mathcal{H}\otimes\mathcal{K})}\right\}\right)$$

where U is a unitary operator on $\mathcal{H}\otimes\mathcal{K}$, $\{\lambda_k\}$ are its Schmidt coefficients, and H is the Shannon entropy. They give a Schmidt decomposition of $\mathcal{F}_{2^m\times 2^n}$ on $m+n$ qubits for the case $m \leqslant n$ and conjecture that $\mathrm{Sch}\,(\mathcal{F}_{2^m\times 2^n}) = 2^{2n}$ for $m > n$.

1.1. Results

Schmidt decompositions of the quantum Fourier transform $\mathcal{F}_{N_1\times N_2} : \mathbb{C}^{N_1}\otimes\mathbb{C}^{N_2} \to \mathbb{C}^{N_1}\otimes\mathbb{C}^{N_2}$ are given for all $N_1, N_2 > 1$, with no requirement that either N_1 or N_2 be a power of two. As a special case, the conjecture of Nielsen and collaborators is affirmed. In all cases, the results of Nielsen imply that the bipartite communication cost of exact computation of the quantum Fourier transform is maximal. Once stated, the decomposition is easily verified; a short derivation is given in the appendix.

1.2. Definitions and notation

Definition 1. *Let N, N_1, N_2 be integers greater than one satisfying $N = N_1N_2$. The* ***quantum Fourier transformation***[3] *$\mathcal{F}_N : \mathbb{C}^N \to \mathbb{C}^N$ is the unitary operator satisfying*

$$\mathcal{F}_N|s\rangle_N = \frac{1}{\sqrt{N}}\sum_{t=0}^{N-1}\exp\left(\frac{2\pi\mathrm{i}}{N}ts\right)|t\rangle_N \qquad s \in \{0,\ldots,N-1\}$$

[1] See also footnote for a brief outline of an alternative proof. We remark that Nielsen considers qubits for convenience only. In particular, let V be a unitary on $\mathbb{C}^{N_1}\otimes C^{N_2}$, where N_1 and N_2 are the respective dimensions of Alice and Bob's quantum states, with no requirement that N_1 and N_2 be a powers of two. Then any quantum computation of V employing some combination of qudit communication and ancillae, possibly of varying dimension, satisfies the following bound: $\sum_{d=2}^{\infty} N_d \log_2(d) \geqslant K_{\mathrm{Har}}(V)$, where N_d is the number of qudits of dimension d communicated between Alice and Bob. It is assumed at the end of the computation that Alice and Bob retain possession of their (now altered) data qudits, although the bound holds whether or not a given net transfer of the (restored) ancillae is allowed.

[2] They also consider more general quantum operations than unitaries.

[3] This is unitarily equivalent to the discrete Fourier transform.

where each $|s\rangle_N$ is a standard basis element. The ***quantum Fourier transformation $\mathcal{F}_{N_1 \times N_2}$*** *on $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ is obtained by identifying $\mathbb{C}^N$ with $\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2}$ under the mixed-decimal representation, which asserts the equalities*

$$|s\rangle_N = |k\ell\rangle_{N_1,N_2} = |k\rangle_{N_1} \otimes |\ell\rangle_{N_2}$$

when

$$s = kN_2 + \ell \ldots k \in \{0, \ldots, N_1 - 1\} \qquad \ell \in \{0, \ldots, N_2 - 1\}.$$

Remark 2. In the case that $N_1 \neq N_2$, the reader is warned that the operator $\mathcal{F}_{N_1 \times N_2}$ is not equivalent in what follows to $\mathcal{F}_{N_2 \times N_1}$. Specifically, $\mathcal{F}_N$ does not commute with the unitary operator $R_{N_1,N_2} : \mathbb{C}^N \to \mathbb{C}^N$ given by

$$R_{N_1,N_2}|kN_2 + \ell\rangle = |\ell N_1 + k\rangle \qquad k \in \{0, \ldots, N_1 - 1\} \qquad \ell \in \{0, \ldots, N_2 - 1\}$$

which interchanges the digits of the mixed-decimal representation.

Notation 3. *Let $\mathcal{H}$ be a finite-dimensional Hilbert space. Then $B(\mathcal{H})$ is the Hilbert space of linear transformations on $\mathcal{H}$ with the Hilbert–Schmidt inner product $\langle A, B\rangle_{B(\mathcal{H})} = \operatorname{Tr} A^\dagger B$.*[4]

Definition 4. *Let $\mathcal{H}$ and $\mathcal{K}$ be finite-dimensional Hilbert spaces, and let F be a nonzero linear transformation on $\mathcal{H} \otimes \mathcal{K}$. An* ***(operator) Schmidt decomposition*** *of F is a decomposition of the form*

$$F = \sum_{k=1}^{\operatorname{Sch}(F)} \lambda_k A_k \otimes B_k \qquad \lambda_k > 0 \tag{2}$$

where $\{A_k\}_{k=1\cdots\operatorname{Sch}(F)}$ and $\{B_k\}_{k=1\cdots\operatorname{Sch}(F)}$ are orthonormal sets[5] *of operators on $\mathcal{H}$ and $\mathcal{K}$, respectively, under the Hilbert–Schmidt inner product. The quantity* $\operatorname{Sch}(F)$ *is called the* ***Schmidt number****, and the λ_k are called the* ***Schmidt coefficients****. Such a decomposition is said to be* ***completely degenerate*** *if* $\operatorname{Sch}(F) = (\min(\dim \mathcal{H}, \dim \mathcal{K}))^2$ *and all the λ_k are equal*[6].

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

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

of a vector $\psi \in \mathcal{H}_0 \otimes \mathcal{K}_0$, where the $\{e_k\}$ and $\{f_k\}$ are orthonormal[7]. In particular, one sets $\mathcal{H}_0 = B(\mathcal{H})$, $\mathcal{K}_0 = B(\mathcal{K})$ and $\psi = F \in B(\mathcal{H} \otimes \mathcal{K})$. The decomposition (2) is then obtained by identifying $B(\mathcal{H}) \otimes B(\mathcal{K})$ with $B(\mathcal{H} \otimes \mathcal{K})$ under the natural isomorphism[8]. It follows that

[4] If A is a linear operator on $\mathcal{H}$, then $A^\dagger$ is defined by $\langle x, Ay\rangle_{\mathcal{H}} = \langle A^\dagger x, y\rangle_{\mathcal{H}}$ for all $x, y \in \mathcal{H}$. Here $\langle \bullet, \bullet\rangle_{\mathcal{H}}$ is the inner product on $\mathcal{H}$, and we will always take inner products to be linear in the second argument.

[5] But not necessarily bases.

[6] More generally, if $F : \mathcal{H} \otimes \mathcal{K} \to \mathcal{H}' \otimes \mathcal{K}'$, then one may consider decompositions of the form (2), where now the $A_k : \mathcal{H} \to \mathcal{H}'$ and $B_k : \mathcal{K} \to \mathcal{K}'$ are orthornormal. Such a useful decomposition exists for the *communication operator* $C : (\mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2}) \otimes \mathbb{C}^{n_3} \to \mathbb{C}^{n_1} \otimes (\mathbb{C}^{n_2} \otimes \mathbb{C}^{n_3})$, defined by $C(a \otimes b) \otimes c = a \otimes (b \otimes c)$. One may check that $C = \sum_{k=1}^{n_2} \sqrt{n_1 n_3} A_k \otimes B_k$, where $A_k = n_1^{-1/2} \sum_{i=1}^{n_1} |i\rangle\langle ik| : \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \to \mathbb{C}^{n_1}$ and $B_k = n_3^{-1/2} \sum_{i=1}^{n_3} |ki\rangle\langle i| : \mathbb{C}^{n_3} \to \mathbb{C}^{n_2} \otimes \mathbb{C}^{n_3}$. Replacing the swap operators in section III.B.3 of [3] by communication operators, one obtains the aforementioned sharp quantum communication complexity bound of [2].

[7] See [4] for a discussion of the Schmidt decomposition.

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

F and G in $B(\mathcal{H}\otimes\mathcal{K}) \simeq B(\mathcal{H})\otimes B(\mathcal{K})$ have the same operator-Schmidt coefficients, counting multiplicity, iff

$$A = (\mathbb{U}\otimes\mathbb{V})B$$

for some unitary 'super-operators' $\mathbb{U} \in B\,(B(\mathcal{H}))$ and $\mathbb{V} \in B\,(B(\mathcal{K}))$.[9]

The well-known procedure for computing Schmidt decompositions is reviewed in theorem 8 of the appendix. We content ourselves here with the statement that the Schmidt coefficients of $\psi \in \mathcal{H}_0 \otimes \mathcal{K}_0$ are the square roots of the nonzero eigenvalues of the reduced density matrix

$$\rho_\psi = \operatorname*{Tr}_{\mathcal{K}_0} |\psi\rangle\langle\psi|.$$

Equivalently, the Schmidt coefficients are the nonzero singular values of the operator $B_\psi : \mathcal{H}_0 \to \mathcal{K}_0^*$ given by

$$(B_\psi f)(g) = \langle \psi,\, f\otimes g\rangle_{\mathcal{H}_0\otimes\mathcal{K}_0}$$

where $\mathcal{K}_0^*$ is the dual space of continuous linear functionals on $\mathcal{K}_0$.[10]

2. Schmidt decomposition of $\mathcal{F}$

Notation 5. *Let* $\mathbb{Z}_{N_1} = \{0,\ldots,N_1-1\}, \mathbb{Z}_{N_2} = \{0,\ldots,N_2-1\}, \mathbb{Z}_{N_2}^2 = \mathbb{Z}_{N_2}\times\mathbb{Z}_{N_2}$, $N_1\mathbb{Z}^2 = \{(N_1x, N_1y)|x, y\in\mathbb{Z}\}$, $\lceil x\rceil = \min\{n\in\mathbb{Z}|n > x\}$ *and* $\lfloor x\rfloor = -\lceil -x\rceil$. *Denote the cardinality of a set* C *by* $|C|$. *Its characteristic function* χ_C *satisfies*

$$\chi_C(x) = \begin{cases} 1 & \text{if} \quad x\in C \\ 0 & \text{if} \quad x\notin C \end{cases}.$$

Adopt the convention $n \bmod m \in \mathbb{Z}_m$.

Theorem 6. *Define an equivalence relation* $\sim$ *on* $\mathbb{Z}_{N_2}^2$ *by*

$$\vec{\ell}\sim\vec{m} \iff \vec{\ell}-\vec{m}\in N_1\mathbb{Z}^2$$

where the subtraction is not modular, and define $\mathcal{M} = \mathbb{Z}_{N_2}^2\big/\sim$ *to be the set of equivalence classes*[11]. *Then a Schmidt decomposition of* $\mathcal{F}_{N_1\times N_2}$ *is given by*

$$\mathcal{F}_{N_1\times N_2} = \sum_{C\in\mathcal{M}} \sqrt{\frac{N_1}{N_2}|C|}\,A_C\otimes B_C \tag{3}$$

where the matrices of $A_C : \mathbb{C}^{N_1}\to\mathbb{C}^{N_1}$ *and* $B_C : \mathbb{C}^{N_2}\to\mathbb{C}^{N_2}$ *are defined by*

$$(A_C)_{k_1k_2} = \frac{1}{N_1}\exp\left[\frac{2\pi\mathrm{i}}{N_1}(N_2k_1k_2 + k_1\tilde{c}_2 + k_2\tilde{c}_1)\right] \qquad k_1,k_2\in\mathbb{Z}_{N_1}$$

$$(B_C)_{\ell_1\ell_2} = \tfrac{1}{|C|^{1/2}}\exp\left(\frac{2\pi\mathrm{i}}{N}\ell_1\ell_2\right)\chi_C((\ell_1,\ell_2)) \qquad \ell_1,\ell_2\in\mathbb{Z}_{N_2}$$

with each $(\tilde{c}_1,\tilde{c}_2)\in C$ *arbitrarily chosen. (*A_C *does not depend on this choice.)*

[9] See exercise 2.80 of [4]. One would like to know much more, i.e. invariants which specify when there are local unitaries $U, Y\in B(\mathcal{H})$ and $V, Z\in B(\mathcal{K})$ such that $A = (U\otimes V)B(Y\otimes Z)$. Such invariants are known only in the two-qubit case [5], where one has the corresponding canonical decomposition of Khaneja *et al* [6] (see also Kraus and Cirac [7] for a simple 'magic basis' proof.)

[10] See [4] for a proof that the Schmidt decomposition is a consequence of the singular value decomposition. In fact they are mathematically equivalent.

[11] The reader may check that for $N_1 = 2$ and $N_2 = 3$ $\mathcal{M}$ consists of $\{(0,0),(0,2),(2,0),(2,2)\}$, $\{(1,0),(1,2)\}$, $\{(0,1),(2,1)\}$ and $\{(1,1)\}$.

Proof. It is trivial to check that $\{A_C\}$ and $\{B_C\}$ are orthonormal sets. Furthermore, for $k_1, k_2 \in \mathbb{Z}_{N_1}$ and $\ell_1, \ell_2 \in \mathbb{Z}_{N_2}$,

$$\begin{aligned}
\langle k_1, \ell_1| \left(\sum_{C\in\mathcal{M}} \sqrt{\frac{N_1}{N_2}|C|} A_C \otimes B_C \right) |k_2, \ell_2\rangle &= \sum_{C\in\mathcal{M}} \sqrt{\frac{N_1}{N_2}|C|} \langle k_1|A_C|k_2\rangle \langle \ell_1|B_C|\ell_2\rangle \\
&= \sum_{C\in\mathcal{M}} \frac{1}{\sqrt{N}} \exp\left[\frac{2\pi \mathrm{i}}{N}\left(N_2^2 k_1 k_2 + N_2 k_1 \tilde{c}_2 + N_2 k_2 \tilde{c}_1 + \ell_1 \ell_2\right)\right] \chi_C((\ell_1, \ell_2)) \\
&= \sum_{C\in\mathcal{M}} \frac{1}{\sqrt{N}} \exp\left[\frac{2\pi \mathrm{i}}{N}\left(N_2^2 k_1 k_2 + N_2 k_1 \ell_2 + N_2 k_2 \ell_1 + \ell_1 \ell_2\right)\right] \chi_C((\ell_1, \ell_2)) \\
&= \frac{1}{\sqrt{N}} \exp\left[\frac{2\pi \mathrm{i}}{N}(N_2 k_1 + \ell_1)(N_2 k_2 + \ell_2)\right] \\
&= \langle k_1 \ell_1 | \mathcal{F}_{N_1 \times N_2} | k_2, \ell_2\rangle
\end{aligned}$$

as desired. □

The reader may find it instructive to compute the linear spans of the matrices B_C corresponding to each of the Schmidt coefficients.

Corollary 7. *The Schmidt decompositions of $\mathcal{F}_{N_1 \times N_2}$ fall into three categories:*

(i) If N_1 is a factor of N_2, then there is only one Schmidt coefficient, $\sqrt{N_2/N_1}$, with multiplicity N_1^2.
(ii) If $N_1 \geqslant N_2$, there is only one Schmidt coefficient, $\sqrt{N_1/N_2}$, with multiplicity N_2^2.
(iii) Otherwise, $\mathcal{F}_{N_1 \times N_2}$ has three distinct nonzero Schmidt coefficients:

$$\begin{aligned}
&\sqrt{\left\lceil \frac{N_2}{N_1} \right\rceil^2 \frac{N_1}{N_2}} && \text{multiplicity } (N_2 \bmod N_1)^2 \\
&\sqrt{\left\lceil \frac{N_2}{N_1} \right\rceil \left\lfloor \frac{N_2}{N_1} \right\rfloor \frac{N_1}{N_2}} && \text{multiplicity } 2\ (N_2 \bmod N_1)((-N_2) \bmod N_1) \\
&\sqrt{\left\lfloor \frac{N_2}{N_1} \right\rfloor^2 \frac{N_1}{N_2}} && \text{multiplicity } ((-N_2) \bmod N_1)^2.
\end{aligned}$$

In all cases, the Schmidt number of $\mathcal{F}_{N_1 \times N_2}$ is $\min\left(N_1^2, N_2^2\right)$. In particular, the Schmidt decomposition is completely degenerate in Cases 1 and 2.

We remark that the previously known cases fall under Case 1. Case 2 verifies the Schmidt numbers conjectured in [3]. Since the Schmidt decomposition in Case 1 (or Case 2) is completely degenerate, theorem 8 (below), may be used to find a Schmidt decomposition of the form of equation (2) for *any* orthonormal basis $\{A_k\}$ (or $\{B_k\}$, in case 2)[12].

Acknowledgments

Michael Nielsen's correspondence is greatly appreciated. I would like to thank Mary Beth Ruskai for her comments, which were most useful in making the paper more readable. This research was carried out for the Clay Mathematics Institute.

[12] Note that cases 1 and 2 overlap for $N_1 = N_2$.

Appendix. A derivation

It will soon be apparent that the crucial fact which allows easy calculation of a Schmidt decomposition of $\mathcal{F}$ is the following: *No two of the B_C have a nonzero matrix entry in the same place*.

The well-known computational recipe needed here is summarized in

Theorem 8. *Let $\psi \in \mathcal{H} \otimes \mathcal{K}$ be nonzero. If*

$$\rho_{\mathcal{K}} \equiv \operatorname*{Tr}_{\mathcal{H}} |\psi\rangle\langle\psi| = \sum_{\ell \in L} \mu_\ell |f_\ell\rangle\langle f_\ell|$$

is a spectral decomposition of the reduced density matrix, then a Schmidt decomposition of ψ is given by

$$\psi = \sum_{\{\ell | \mu_\ell > 0\}} \sqrt{\mu_\ell} e_\ell \otimes f_\ell \tag{4}$$

where each e_ℓ is defined by the requirement that

$$\langle \psi, v \otimes f_\ell \rangle_{\mathcal{H}\otimes\mathcal{K}} = \sqrt{\mu_k} \langle e_\ell, v \rangle_{\mathcal{H}} \tag{5}$$

for all $v \in \mathcal{H}$. Furthermore, all Schmidt decompositions of ψ may be exhibited in this manner.

Derivation of theorem 6. We follow the prescription of theorem 8, and employ the natural isomorphism $B(\mathbb{C}^{N_1}) \otimes B(\mathbb{C}^{N_2}) \simeq B(\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2})$, as explained in section 1.2. The reduced density superoperator $\rho \in B(B(\mathbb{C}^{N_2}))$ is defined by the equation

$$\langle A, \rho B \rangle_{B(\mathbb{C}^{N_2})} = \sum_E \langle E \otimes A, \mathcal{F} \rangle_{B(\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2})} \langle \mathcal{F}, E \otimes B \rangle_{B(\mathbb{C}^{N_1} \otimes \mathbb{C}^{N_2})}$$

for arbitrary $A, B \in B(\mathbb{C}^{N_2})$, where E runs over a basis of $B(\mathbb{C}^{N_1})$. For $\vec{j} \in \mathbb{Z}^2_{N_1}$ and $\vec{\ell} \in \mathbb{Z}^2_{N_2}$ define the standard basis elements

$$E_{\vec{j}} = |j_1\rangle\langle j_2| \in B(C^{N_1}) \qquad F_{\vec{\ell}} = |\ell_1\rangle\langle \ell_2| \in B(\mathbb{C}^{N_2}).$$

We compute ρ by studying its matrix coordinates

$$\rho_{\vec{\ell}\vec{m}} = \langle F_{\vec{\ell}}, \rho F_{\vec{m}} \rangle_{B(\mathbb{C}^{N_2})}.$$

Similarly, let

$$\mathcal{F}_{\vec{j}\vec{\ell}} = \langle E_{\vec{j}} \otimes F_{\vec{\ell}}, \mathcal{F} \rangle_{B(\mathbb{C}^N)}.$$

Then

$$\begin{aligned}
\rho_{\vec{\ell}\vec{m}} &= \sum_{\vec{j} \in \mathbb{Z}^2_{N_1}} \mathcal{F}_{\vec{j}\vec{\ell}} \bar{\mathcal{F}}_{\vec{j}\vec{m}} \\
&= \frac{1}{N} \sum_{j_1=0}^{N_1-1} \sum_{j_2=0}^{N_1-1} \begin{pmatrix} \exp\left(\frac{2\pi \mathrm{i}}{N}(N_2 j_1 + \ell_1)(N_2 j_2 + \ell_2)\right) \\ \times \exp\left(-\frac{2\pi \mathrm{i}}{N}(N_2 j_1 + m_1)(N_2 j_2 + m_2)\right) \end{pmatrix} \\
&= \frac{1}{N} \exp\left(\frac{2\pi \mathrm{i}}{N}(\ell_1 \ell_2 - m_1 m_2)\right) \\
&\quad \times \sum_{j_1=0}^{N_1-1} \exp\left(\frac{2\pi \mathrm{i}}{N_1}(\ell_2 - m_2) j_1\right) \times \sum_{j_2=0}^{N_1-1} \exp\left(\frac{2\pi \mathrm{i}}{N_1}(\ell_1 - m_1) j_2\right).
\end{aligned}$$

Evaluating the appropriate inverse-Fourier transforms,

$$\rho_{\vec{\ell}\vec{m}} \equiv \frac{N_1}{N_2} \exp\left(\frac{2\pi \mathrm{i}}{N}(\ell_1 \ell_2 - m_1 m_2)\right) \times \chi_{N_1 \mathbb{Z}^2}(\vec{\ell} - \vec{m}). \tag{6}$$

The spectral decomposition of ρ into a linear combination of projections may be simply read off from the asymptotic $n \to \infty$ behaviour of (6) to the power of $n \in \mathbb{Z}^+$.[13] One need not do this, however, for using the identity

$$\chi_{N_1\mathbb{Z}^2}(\vec{\ell} - \vec{m}) = \sum_{C \in \mathcal{M}} \chi_C(\vec{\ell})\chi_C(\vec{m})$$

equation (6) may be rewritten as

$$\rho = \sum_{C \in \mathcal{M}} \frac{N_1}{N_2} |C| \times |B_C\rangle\langle B_C|$$

where the B_C are orthonormal, as noted before. The A_C are easily computed using (5). □

References

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

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

[3] 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 2002 Quantum dynamics as a physical resource *Phys. Rev.* A *Preprint* quant-ph/0208077

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

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

[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 (*Preprint* quant-ph/0011050)

[13] Using matrix multiplication.