Quantum Latin squares and unitary error bases

Benjamin Musto
benjamin.musto@cs.ox.ac.uk

Jamie Vicary
jamie.vicary@cs.ox.ac.uk

Department of Computer Science, University of Oxford

Friday 25th September, 2015

Abstract

In this paper we introduce *quantum Latin squares*, combinatorial quantum objects which generalize classical Latin squares, and investigate their applications in quantum computer science. Our main results are on applications to *unitary error bases* (UEBs), basic structures in quantum information which lie at the heart of procedures such as teleportation, dense coding and error correction. We present a new method for constructing a UEB from a quantum Latin square equipped with extra data. Developing construction techniques for UEBs has been a major activity in quantum computation, with three primary methods proposed: *shift-and-multiply*, *Hadamard*, and *algebraic*. We show that our new approach simultaneously generalizes the shift-and-multiply and Hadamard methods. Furthermore, we explicitly construct a UEB using our technique which we prove cannot be obtained from any of these existing methods.

1 Introduction

We begin with the definition of a quantum Latin square.

Definition 1. A *quantum Latin square of order* n is an n-by-n array of elements of the Hilbert space $\mathbb{C}^n$, such that every row and every column is an orthonormal basis.

Example 2. Here is a quantum Latin square given in terms of the computational basis elements $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\} \subset \mathbb{C}^4$:

$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$
$\frac{1}{\sqrt{2}}(\|1\rangle + \|2\rangle)$	$\frac{1}{\sqrt{5}}(2\|0\rangle + i\|3\rangle)$	$\frac{1}{\sqrt{5}}(i\|0\rangle + 2\|3\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle - \|2\rangle)$
$\|3\rangle$	$\|2\rangle$	$\|1\rangle$	$\|0\rangle$

It can readily be checked that along each row, and along each column, the elements form an orthonormal basis for $\mathbb{C}^4$. We can compare this to the classical notion of Latin square [11].

Definition 3. A *classical Latin square of order* n is an n-by-n array of integers in the range $\{0, \ldots, n-1\}$, such that every row and column contains each number exactly once.

By interpreting a number $k \in \{0, \ldots, n-1\}$ as a computational basis element $|k\rangle \in \mathbb{C}^n$, we can turn an array of numbers into an array of Hilbert space elements:

$$\begin{array}{|c|c|c|c|} \hline 3 & 1 & 0 & 2 \\ \hline 1 & 0 & 2 & 3 \\ \hline 2 & 3 & 1 & 0 \\ \hline 0 & 2 & 3 & 1 \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{|c|c|c|c|} \hline |3\rangle & |1\rangle & |0\rangle & |2\rangle \\ \hline |1\rangle & |0\rangle & |2\rangle & |3\rangle \\ \hline |2\rangle & |3\rangle & |1\rangle & |0\rangle \\ \hline |0\rangle & |2\rangle & |3\rangle & |1\rangle \\ \hline \end{array} \tag{1}$$

It is easy to see that the original array of numbers is a classical Latin square if and only if the corresponding grid of Hilbert space elements is a quantum Latin square. However, as Example 2 makes clear, not every quantum Latin square is of this form.

Our main results are on the construction of *unitary error bases* (UEBs) [14], also known as unitary operator bases. These are basic structures in quantum information which play a central role in quantum teleportation [6], dense coding [13] and error correction [18]. Since UEBs are hard to find, and given their wide applicability, construction techniques for UEBs have been widely studied [12, 14, 15, 21]. In this paper, we propose a new method for construction of UEBs:

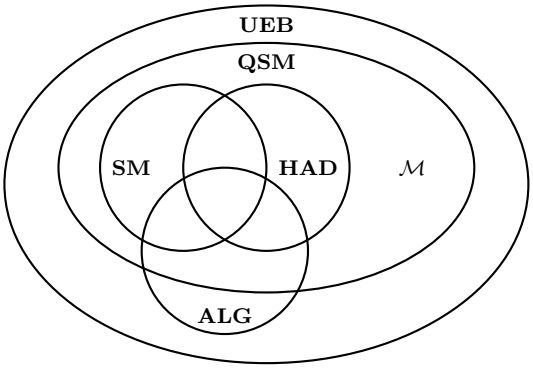
- Quantum shift-and-multiply method (**QSM**). Requires a quantum Latin square and a family of Hadamard matrices. (See Definition 17.)

We compare this to the other methods that have been proposed in the literature:

- Shift-and-multiply method (**SM**). Requires a classical Latin square and a family of Hadamard matrices. (See Definition 20.)
- Hadamard method (**HAD**). Requires a pair of mutually-unbiased bases. (See Definition 32.)
- Algebraic method (**ALG**). Requires a finite group equipped with a projective representation, satisfying certain properties. (See Definition 41.)

Our theorems concern the relationships between these constructions. In Theorems 21 and 33, we prove that **QSM** contains **SM** and **HAD** as special cases. We also use **QSM** to construct a concrete unitary error basis $\mathcal{M}$ (Example 18), and prove that it is not equivalent to one arising from **SM**, **HAD** or **ALG** (Corollaries 31, 39 and 44 respectively.)

The relationships between these constructions, up to a standard notion of equivalence of UEBs (see Definition 15), are indicated by the following Venn diagram:



(2)

Our work strongly extends previous results, in an area that has not seen progress since 2003. But there is much still to be settled: in particular, we do not know whether **ALG** is a subset of **QSM**, or whether **QSM** equals **UEB**.

Categorical quantum mechanics is a research programme in which powerful techniques of monoidal category theory are used to understand quantum computational phenomena [1, 2, 8], using a graphical notation which can make the high-level structure of computations easier to understand. The main results of this paper were originally developed using this approach (see also [17]), although we have chosen to present them here in a conventional way. We feel this is a good advert for the power of categorical quantum mechanics; certainly, we could not have developed our results without using these techniques.

There are interesting connections between Hadamard matrices, unitary error bases and quantum Latin squares. In Section 2 we show that a quantum Latin square can be constructed from any Hadamard matrix. Hadamard matrices are mathematically equivalent to the data for a pair of *mutually unbiased bases* [5], the study and classification of which is a major activity in quantum computer science [4, 10, 16, 19]. It has also been shown that in some cases a family of mutually unbiased bases can be extracted from a UEB [3]. So quantum Latin squares can be built from Hadamards, which can be built from UEBs, which can be built from quantum Latin squares; an interesting tapestry of results for which we currently lack a good intuition.

Acknowledgements. The authors are grateful to Dominic Verdon for useful discussions, and to EPSRC for financial support.

2 Quantum Latin squares from Hadamard matrices

In this section we introduce some basic properties of quantum Latin squares, show how to construct a quantum Latin square from a Hadamard matrix, and prove that our quantum Latin square of Example 2 is not equivalent to one arising in this way.

We begin by developing a precise notation for working with quantum Latin squares. Throughout, we assume we are working with a quantum Latin square of order n, and that indices i, j, k, p, q range from 0 to $n-1$.

Definition 4. For a quantum Latin square Q, we define the following:

- Q_i is the matrix whose columns are the entries of the ith row of Q;
- $Q_{ij} \in \mathbb{C}^n$ is the Hilbert space element at the ith row and jth column of Q;
- $Q_{ijk} := (Q_{ij})_k = \langle k|Q_{ij}\rangle \in \mathbb{C}$ is the coefficient of the basis vector $|k\rangle$.

For a matrix M, it is a standard notation to write M_{ij} for the element at the ith row and jth column. Combining this with Definition 4, we have the following:

$$(Q_i)_{jk} = Q_{ikj} \tag{3}$$

Note that the order of the final two indices changes.

Given a collection of numbers $Q_{ijk} \in \mathbb{C}$, we can easily identify when they arise from a quantum Latin square. For a matrix M, we write M^* for the conjugate matrix, M^{T} for the transpose matrix, and $M^\dagger = (M^*)^\dagger = (M^\dagger)^*$ for the conjugate transpose matrix.

Lemma 5. *A family of numbers $Q_{ijk} \in \mathbb{C}$ arise from a quantum Latin square if and only if they satisfy the following properties for all i, p, q:*

$$\sum_j Q^*_{ipj} Q_{iqj} = \delta_{pq}, \text{ or equivalently the matrices } Q_i \text{ are unitary} \tag{4}$$

$$\sum_j Q^*_{pij} Q_{qij} = \delta_{pq} \tag{5}$$

Proof. Equations (4) and (5) are exactly the condition that the rows and columns, respectively, of the quantum Latin square form orthonormal bases. Unitarity of Q_i means precisely $(Q_i^\dagger \circ Q_i)_{pq} = \delta_{pq}$, which expands to $\sum_j (Q_i^\dagger)_{pj} (Q_i)_{jq} = \sum_j Q^*_{ipj} Q_{iqj} = \delta_{pq}$. (Recall that for an operator Q on a finite-dimensional Hilbert space, $Q \circ Q^\dagger = \mathbb{I}_n$ if and only if $Q^\dagger \circ Q = \mathbb{I}_n$.) □

The condition (5) equivalently says that the matrices formed by the *columns* of the Latin square are unitary, but this is not a fact that we will need directly.

There are certain trivial ways to transform a quantum Latin square into a different quantum Latin square, which we use to define a notion of equivalence.

Definition 6. Two quantum Latin squares are *equivalent* when one can be obtained from the other by permuting rows and columns, multiplying rows and columns by unit complex numbers, and applying a fixed unitary to every element. Algebraically, quantum Latin squares Q and Q' are equivalent when there exists some unitary U, diagonal unitary D, permutation matrix P, permutation ϕ, and a family of unit complex numbers c_j, such that the following holds:

$$Q'_j = c_j U \circ Q_{\phi(j)} \circ P \circ D \tag{6}$$

We now give the standard definition of a Hadamard matrix, as a square matrix with entries of absolute value 1 which is proportional to a unitary matrix.

Definition 7 (See [20], Definition 2.1)**.** A *Hadamard matrix of order n* is an n-by-n matrix H with the following properties for all i, j, which we write in both matrix and index form:

$$|H_{ij}| = 1 \qquad H_{ij} H^*_{ij} = 1 \tag{7}$$

$$H \circ H^\dagger = n\, \mathbb{I}_n \qquad \sum_p H_{ip} H^*_{jp} = n\, \delta_{ij} \tag{8}$$

$$H^\dagger \circ H = n\, \mathbb{I}_n \qquad \sum_p H^*_{pi} H_{pj} = n\, \delta_{ij} \tag{9}$$

We now give the construction of a quantum Latin square from a Hadamard matrix.

Definition 8. For a square matrix M, let $\mathrm{diag}(M, i)$ be the diagonal matrix whose diagonal entries are given by the ith row of M:

$$\mathrm{diag}(M, i)_{jk} := \delta_{jk} M_{ij} \tag{10}$$

Definition 9. For a Hadamard matrix H of order n, its *associated quantum Latin square* Q_H of order n is defined as follows:

$$(Q_H)_j := \tfrac{1}{n} H \circ \mathrm{diag}(H, j)^\dagger \circ H^\dagger \tag{11}$$

We will refer to a quantum Latin square constructed in this way as a *Hadamard quantum Latin square*.

Theorem 10. *The associated quantum Latin square construction is correct.*

Proof. To establish property (4), we note that $(Q_H)_j$ is the composite of three unitary matrices, and is therefore unitary. To verify (5), we write expression (11) in index form:

$$\begin{aligned}(Q_H)_{qij} &\overset{(3)}{=} ((Q_H)_q)_{ji} \overset{(11)}{=} \tfrac{1}{n}\textstyle\sum_{rs} H_{jr}\mathrm{diag}(H,q)^\dagger_{rs}H^\dagger_{si} \\ &\overset{(10)}{=} \tfrac{1}{n}\textstyle\sum_{rs} H_{jr}H^*_{qr}\delta_{rs}H^*_{is} = \tfrac{1}{n}\textstyle\sum_{r} H_{jr}H^*_{qr}H^*_{ir} \end{aligned} \tag{12}$$

We then perform the following calculation:

$$\begin{aligned}&\textstyle\sum_j (Q_H)^*_{pij}(Q_H)_{qij} \overset{(12)}{=} \tfrac{1}{n^2}\textstyle\sum_j \big(\sum_r H^*_{jr}H_{pr}H_{ir}\big)\big(\sum_s H_{js}H^*_{qs}H^*_{is}\big) \\ &= \tfrac{1}{n^2}\textstyle\sum_{rs}\big(\sum_j H^*_{jr}H_{js}\big)H_{pr}H_{ir}H^*_{qs}H^*_{is} \overset{(9)}{=} \tfrac{1}{n}\textstyle\sum_{rs}\delta_{rs}H_{pr}H_{ir}H^*_{qs}H^*_{is} \\ &= \tfrac{1}{n}\textstyle\sum_r H_{pr}H^*_{qr}H_{ir}H^*_{ir} \overset{(7)}{=} \tfrac{1}{n}\textstyle\sum_r H_{pr}H^*_{qr} \overset{(8)}{=} \delta_{pq}\end{aligned} \tag{13}$$

In the second equality here, the sum is being reorganized. □

We now establish a lemma which we will use to prove Lemma 12 and later Proposition 36.

Lemma 11. *The following equations hold:*

$$\mathrm{diag}(P\circ H, i) = \mathrm{diag}(H, p(i)) = \mathrm{diag}(H_{p(i),0}, ..., H_{p(i),n-1}) \tag{14}$$

$$\mathrm{diag}(H\circ P, i) = \mathrm{diag}(H_{i,p(0)}, ..., H_{i,p(n-1)}) \tag{15}$$

$$\mathrm{diag}(D\circ H, i) = D_{ii}\,\mathrm{diag}(H, i) \tag{16}$$

$$\mathrm{diag}(H\circ D, i) = D\circ\mathrm{diag}(H, i) = \mathrm{diag}(H, i)\circ D \tag{17}$$

Proof. Straightforward calculation. □

Lemma 12. *Equivalent Hadamards give rise to equivalent quantum Latin squares.*

Proof. We will prove equivalence on a case-by-case basis. Suppose $H' = P\circ H$. Then we have the following, where we use the fact that $P^{-1} = P^\dagger = P^T$:

$$\begin{aligned}(Q_{H'})_j &\overset{(11)}{=} \tfrac{1}{n}P\circ H\circ\mathrm{diag}(P\circ H, j)^\dagger\circ H^\dagger\circ P^{-1} \\ &\overset{(14)}{=} \tfrac{1}{n}P\circ H\circ\mathrm{diag}(H, p(j))^\dagger\circ H^\dagger\circ P^{-1} \\ &\overset{(6)}{\sim} \tfrac{1}{n}H\circ\mathrm{diag}(H, j)^\dagger\circ H^\dagger \overset{(11)}{=} (Q_H)_j\end{aligned}$$

We now consider $H' = H\circ P$:

$$\begin{aligned}(Q_{H'})_j &\overset{(11)}{=} \tfrac{1}{n}H\circ P\circ\mathrm{diag}(H\circ P, j)^\dagger\circ P^{-1}\circ H^\dagger \\ &\overset{(15)}{=} \tfrac{1}{n}H\circ P\circ\mathrm{diag}(H_{j,p(0)}, ..., H_{j,p(n-1)})^\dagger\circ P^{-1}\circ H^\dagger \\ &\overset{(27)}{=} \tfrac{1}{n}H\circ P\circ P^{-1}\circ\mathrm{diag}(H, j)^\dagger\circ H^\dagger \\ &= \tfrac{1}{n}H\circ\mathrm{diag}(H, j)^\dagger\circ H^\dagger \overset{(11)}{=} (Q_H)_j\end{aligned}$$

Finally, suppose $H' = D_1\circ H\circ D_2$, with $D_1 = \mathrm{diag}(c_1, \ldots, c_n)$, where $|c_i| = 1$. Then we calculate as follows:

$$\begin{aligned}(Q_{H'})_j &\overset{(11)}{=} \tfrac{1}{n}D_1\circ H\circ D_2\circ\mathrm{diag}(D_1\circ H\circ D_2, j)^\dagger D_2^\dagger\circ H^\dagger\circ D_1^\dagger \\ &\overset{(16)}{=} \tfrac{1}{n}D_1\circ H\circ D_2\circ c_j\mathrm{diag}(H\circ D_2, j)^\dagger\circ D_2^\dagger\circ H^\dagger\circ D_1 \\ &\overset{(17)}{=} \tfrac{1}{n}D_1\circ H\circ D_2\circ c_j\mathrm{diag}(H, j)^\dagger D_2\circ D_2^\dagger\circ H^\dagger\circ D_1 \\ &= \tfrac{1}{n}D_1\circ H\circ D_2\circ c_j\mathrm{diag}(H, j)^\dagger\circ H^\dagger\circ D_1 \\ &\overset{(6)}{\sim} \tfrac{1}{\sqrt{n}}\mathrm{diag}(H, j)^\dagger\circ H^\dagger \\ &\overset{(6)}{\sim} \tfrac{1}{n}H\circ\mathrm{diag}(H, j)^\dagger\circ H^\dagger \overset{(11)}{=} (Q_H)_j\end{aligned}$$

This completes the proof. □

Finally, we prove that our example quantum Latin square does not arise in this way, even up to equivalence. This makes use of some results that we prove later in the paper.

Proposition 13. *The quantum Latin square given in Example 2 is not equivalent to a quantum Latin square constructed from a Hadamard.*

Proof. Let H_α be the family of Hadamard matrices as defined in equation (32), let $(Q_{H_\alpha})_j := \frac{1}{n} H_\alpha \circ \mathrm{diag}(H_\alpha, j)^\dagger \circ H_\alpha^\dagger$ be the associated quantum Latin squares, and let Q be the quantum Latin square of Example 2. By Lemma 12 and Proposition 37, any quantum Latin square arising from a Hadamard matrix in the manner of Definition 9 is equivalent to Q_{H_α} for some value of α.

For a contradiction, suppose that Q and Q_{H_α} are equivalent in the manner of Definition 6, for some fixed value of α. So there exists some unitary matrix U, diagonal unitary matrix D, permutation matrix P, permutation ϕ, and a family of unit complex numbers c_j, such that the following holds:

$$(Q_{H_\alpha})_j = c_j U \circ Q_{\phi(j)} \circ P \circ D$$

Note that the composite $P \circ D$ is unitary; so the families of matrices $(Q_{H_\alpha})_j$ and Q_j, which are unitary by Lemma 5, are equivalent families in the sense of Definition 15.

The family $(Q_{H_\alpha})_j$ are simultaneously monomializable, by the matrix Y defined in equation (33). (This follows from Theorem 38, in which we show that the members of $\mathcal{F}_\alpha$, which include the $(Q_{H_\alpha})_j$ as a subset, are simultaneously monomializable.) So all together, the family of matrices Q_j contains the identity, and is equivalent in the sense of Definition 15 to a monomial family. So by Proposition 26, the family Q_j is simultaneously monomializable, and thus by Proposition 28, their 12th powers must all commute. But as established in the proof of Theorem 29, the 12th powers of $Q_1 = \mathcal{M}_{01}$ and $Q_2 = \mathcal{M}_{02}$ do not commute. This gives us our contradiction. □

3 Unitary error bases from quantum Latin squares

In this section we define unitary error bases, and present our new *quantum shift-and-multiply* construction, which produces a unitary error basis from a quantum Latin square equipped with a family of Hadamard matrices. We then introduce an example UEB $\mathcal{M}$, which will play an important role in later sections where we show that it cannot arise from the shift-and-multiply, Hadamard or algebraic methods, even up to equivalence.

We begin with the definition of unitary error basis. As remarked in the introduction, these structures play a central role in quantum computation.

Definition 14 (See [14], Section 1)**.** For a Hilbert space H of dimension n, a *unitary error basis* (or *unitary operator basis*) is a family of n^2 unitary matrices $U_{ij} : H \to H$ which form an orthogonal basis:

$$\mathrm{Tr}(U_{ij}^\dagger \circ U_{i'j'}) = \delta_{ii'}\delta_{jj'}n \tag{18}$$

There is a standard notion of equivalence of unitary error bases, which we recall here.

Definition 15 (See [14], Section 2)**.** Two families of unitary matrices $\mathcal{A}$, $\mathcal{B}$ are *equivalent* if there are unitary matrices U and V, such that for any element $A \in \mathcal{A}$, there is an element $B \in \mathcal{B}$ and a unit complex number c such that the following holds:

$$B = c\,U \circ A \circ V \tag{19}$$

The following technical lemma will be useful later.

Lemma 16. *Let D be a diagonal matrix, and A be a square matrix which is zero along the main diagonal, such that D and A are composable. Then $D \circ A$ is zero along the main diagonal.*

Proof. We perform the following calculation of the diagonal elements of $D \circ A$:

$$(D \circ A)_{ii} = \sum_k D_{ik} A_{ki} = \sum_k \delta_{ik} D_{ii} A_{ki} = D_{ii} A_{ii} = 0 \tag{20}$$

Here we apply the definition of matrix composition, the diagonal property of D, the properties of the sum, and the hypothesis that A is zero along the main diagonal. □

We now define the main construction of focus in this paper. This construction is similar to Werner's shift-and-multiply method [21], the difference being that ours is in terms of *quantum* Latin squares. As usual, we take all indices in the range 0 to $n-1$.

Definition 17 (Quantum shift-and-multiply method)**.** Let Q be a quantum Latin square of order n, and H_j be a family of n Hadamard matrices of order n. Then the associated *quantum shift-and-multiply basis* has the following elements:

$$S_{ij} := Q_j \circ \mathrm{diag}(H_j, i) \tag{21}$$

In words, the (i, j) entry of the quantum shift-and-multiply basis is the matrix given by the jth row of the quantum Latin square, composed with the diagonal matrix formed from the ith row of the jth Hadamard matrix.

We illustrate this with an example. This example will play a central role, as we will show in the remainder of the paper that it cannot be obtained, even up to equivalence, by any of the existing methods of unitary error basis construction.

Example 18. The quantum shift-and-multiply basis $\mathcal{M}$ is constructed from the quantum Latin square of Example 2, and from the following family of Hadamard matrices:

$$H_0 = H_1 = H_2 = H_3 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} \tag{22}$$

The resulting family of 16 matrices is listed in Appendix A.1.

We now show that quantum shift-and-multiply bases are unitary error bases. This has similarities with Werner's original proof [21] for standard shift-and-multiply bases (see Section 4), but our use of quantum Latin squares requires nontrivial extra ideas.

Theorem 19. *Quantum shift-and-multiply bases are unitary error bases.*

Proof. First, we note that the elements $S_{ij} = Q_j \circ \mathrm{diag}(H_j, i)$ are unitary, since they are composites of unitary matrices: the matrix Q_j is the jth row of a quantum Latin square, and hence unitary by Lemma 5; and $\mathrm{diag}(H_j, i)$ is a diagonal matrix with unit complex numbers along the diagonal, and hence unitary.

We must establish the following trace property:

$$\mathrm{Tr}(S_{ij}^\dagger \circ S_{i'j'}) = n\,\delta_{ii'}\delta_{jj'} \tag{23}$$

We first consider the case that $j = j'$ and $i = i'$. By unitarity of S_{ij} we have $S_{ij} \circ S_{i'j'}^\dagger = \mathbb{I}_n$, with $\mathrm{Tr}(\mathbb{I}_n) = n$, and so the condition follows.

Next we consider the case that $j = j'$ and $i \neq i'$. We perform the following calculation:

$$\begin{aligned}\mathrm{Tr}(S_{ij}^\dagger \circ S_{i'j}) &\overset{(21)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \circ Q_j^\dagger \circ Q_j \circ \mathrm{diag}(H_j, i')\right) \\ &\overset{(4)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \circ \mathrm{diag}(H_j, i')\right)\end{aligned}$$

The final expression is equal to the inner product of rows i and i' of the Hadamard H_j. Since distinct rows of a Hadamard are orthogonal, the result is zero as required.

It remains to consider the case that $j \neq j'$. We use the cyclic property of the trace to rearrange our trace expression:

$$\begin{aligned}\mathrm{Tr}(S_{ij}^\dagger \circ S_{i'j'}) &\overset{(21)}{=} \mathrm{Tr}\left(\mathrm{diag}(H_j, i)^\dagger \circ Q_j^\dagger \circ Q_{j'} \circ \mathrm{diag}(H_{j'}, i')\right) \\ &= \mathrm{Tr}\left(\mathrm{diag}(H_{j'}, i') \circ \mathrm{diag}(H_j, i)^\dagger \circ Q_j^\dagger \circ Q_{j'}\right)\end{aligned} \tag{24}$$

Inside the trace there is the composite $\mathrm{diag}(H_{j'}, i') \circ \mathrm{diag}(H_j, i)^\dagger$, which is diagonal. There is also $Q_j^\dagger \circ Q_{j'}$, which by the following argument is zero along the diagonal:

$$(Q_j^\dagger \circ Q_{j'})_{kk} = \textstyle\sum_l (Q_j^\dagger)_{kl}(Q_{j'})_{lk} = \sum_l (Q_j^*)_{lk}(Q_{j'})_{lk} \overset{(3)}{=} \sum_l Q_{jkl}^* Q_{j'kl} \overset{(5)}{=} \delta_{jj'} = 0 \tag{25}$$

Hence by Lemma 16, expression (24) is zero as required. □

4 Shift-and-multiply method

The shift-and-multiply method of Werner [21], which was a direct inspiration for our own results, can straightforwardly be seen as a special case of our quantum shift-and-multiply method. Our focus in this section is the proof that the unitary error basis $\mathcal{M}$ of Example 18 is not equivalent to a shift-and-multiply basis, and thus that the shift-and-multiply bases are *strictly* contained within the quantum shift-and-multiply bases.

Definition 20. A *shift-and-multiply basis* is a quantum shift-and-multiply basis where the quantum Latin square is a classical Latin square.

Theorem 21. *Every shift-and-multiply basis is a quantum shift-and-multiply basis.*

Proof. Follows immediately from Definitions 3 and 20. □

Monomial matrices will be crucial to our proof strategy.

Definition 22. A *monomial matrix* is a square matrix with exactly one nonzero entry in each row and each column. Equivalently, it is any matrix A which can be expressed as $A = D_A \circ P_A$, where D_A is a diagonal matrix and P_A is a permutation matrix.

Lemma 23. *The set of monomial matrices is closed under composition, taking inverses, taking adjoints, and multiplication by nonzero complex scalars.*

Proof. Straightforward. □

Definition 24. A square matrix A is *monomializable* if there exists a unitary matrix U such that $U \circ A \circ U^\dagger$ is monomial.

Definition 25. A family of square matrices $A_1, ..., A_n$ are *simultaneously monomializable* if they are all monomializable by the same unitary matrix U.

We establish the following propositions, the first of which is adapted and generalized to suit our purposes from the literature.

Proposition 26 (See [14], final part of the proof of Theorem 3)**.** *If a family $\mathcal{S}$ of unitary matrices containing the identity is equivalent (in the sense of Definition 15) to a family of monomial matrices, then the members of $\mathcal{S}$ are simultaneously monomializable.*

Proof. Let $\mathcal{S} = \{S_i\}$ be a family of unitary matrices with $S_0 = \mathbb{I}_n$. Suppose S_i is equivalent to some monomial family $\mathcal{T} = \{T_i\}$ with $T_i = c_i U S_i V$, such that each c_i is a complex number of norm 1, and U, V are unitary matrices. We then perform the following calculation:

$$\frac{c_0}{c_j} T_j T_0^\dagger = \frac{c_0}{c_j}(c_j U S_j V)(c_0 U S_0 V)^\dagger = c_0 c_0^* U S_j V V^\dagger \mathbb{I}_n U^\dagger = U S_j U^\dagger \tag{26}$$

The left hand side is monomial by Lemma 23, and hence U simultaneously monomializes S_i. □

Lemma 27. *Let p be a permutation, $P = \sum_k |p(k)\rangle\langle k|$ be the corresponding permutation matrix, and $D = \sum_k d_k |k\rangle\langle k|$ and $D' = \sum_k d_{p(k)} |k\rangle\langle k|$ be diagonal matrices. Then the following holds:*

$$D \circ P = P \circ D', \tag{27}$$

Proof. We perform the following calculation:

$$\begin{aligned} D \circ P &= P \circ P^\dagger \circ D \circ P = P \circ \left(\textstyle\sum_{ijk} |i\rangle\langle p(i)|d_j|j\rangle\langle j|p(k)\rangle\langle k| \right) \\ &= P \circ \left(\textstyle\sum_{ik} d_{p(k)} |i\rangle\langle p(i)|p(k)\rangle\langle k| \right) = P \circ \left(\textstyle\sum_i d_{p(i)} |i\rangle\langle i| \right) = P \circ D' \end{aligned}$$

This completes the proof. □

Proposition 28. *Let A, B be square matrices of size n, and let μ_n be the lowest common multiple of $\{1, 2, ..., n\}$. If A and B are simultaneously monomializable, then A^{μ_n} and B^{μ_n} commute.*

Proof. Suppose A, B are simultaneously monomializable, with μ_n defined as above. Then there exists a unitary matrix U such that $UAU^\dagger = D_A P_A$ and $UBU^\dagger = D_B P_B$ where D_A, D_B are diagonal matrices and P_A, P_B are permutation matrices. Note that $A = U^\dagger D_A P_A U$, so we have the following:

$$A^{\mu_n} = U^\dagger (D_A P_A)^{\mu_n} U = U^\dagger \widetilde{D}_A P_A^{\mu_n} U \tag{28}$$

Here $\widetilde{D}_A$ is some diagonal matrix, and the last equality is obtained by repeated application of Lemma 27 and the fact that diagonal matrices are closed under composition. Since

P_A is a permutation matrix of dimension n it has order k, where k is the lowest common multiple of the lengths of the permutation's cycles. Each cycle has length $\in \{1, 2, ..., n\}$. Thus k divides μ_n, and so $P_A^{\mu_n} = \mathbb{I}_n$. So $A^{\mu_n} = U^\dagger \widetilde{D}_A U$, and by the same argument, $B^{\mu_n} = U^\dagger \widetilde{D}_B U$ for some diagonal matrix $\widetilde{D}_B$. We then demonstrate that A^{μ_n} and B^{μ_n} commute:

$$A^{\mu_n} B^{\mu_n} = U^\dagger \widetilde{D}_A U U^\dagger \widetilde{D}_B U = U^\dagger \widetilde{D}_A \widetilde{D}_B U = U^\dagger \widetilde{D}_B \widetilde{D}_A U = U^\dagger \widetilde{D}_B U U^\dagger \widetilde{D}_A U = B^{\mu_n} A^{\mu_n}$$

The central equality here holds because diagonal matrices commute. □

We are now ready to prove the necessary properties of our example basis.

Theorem 29. *The basis $\mathcal{M}$ of Example 18 is not equivalent to a monomial basis.*

Proof. For a contradiction, suppose that $\mathcal{M}$ is equivalent to a monomial basis. Note that $\mathcal{M}$ contains the identity matrix, so by Proposition 26 the elements of the UEB are simultaneously monomializable. The least common multiple of $\{1, 2, 3, 4\}$ is $\mu_4 = 12$; thus by Proposition 28 the 12th powers of the elements of $\mathcal{M}$ will commute. To exhibit the contradiction, we compute the following commutator:

$$(\mathcal{M}_{01})^{12}(\mathcal{M}_{02})^{12} - (\mathcal{M}_{02})^{12}(\mathcal{M}_{01})^{12} = \frac{12168}{15625} \begin{pmatrix} -i & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -2 & 0 & 0 & i \end{pmatrix} \neq 0 \tag{29}$$

This completes the proof. □

Proposition 30. *Shift-and-multiply bases are monomial bases.*

Proof. Recall from Definition 20 of a shift-and-multiply basis that each matrix is the product of a diagonal matrix with the permutation matrix given by a row of a classical Latin square. By definition, the result is a monomial matrix. □

Corollary 31. *The basis $\mathcal{M}$ of Example 18 is not equivalent to a shift-and-multiply basis.*

Proof. Immediate from Theorem 29 and Proposition 30. □

5 Hadamard method

In this section we study the *Hadamard method*, a direct construction of a unitary error basis from a Hadamard matrix. While this is certainly known, we cannot find a clear description of it in full generality, although a special case is worked out in detail in [7]. The main results of this section are Theorem 33, where we show that the quantum shift-and-multiply method contains the Hadamard method as a special case, and Corollary 39, in which we show that this containment is proper.

Definition 32 (Hadamard method; folklore)**.** For a Hadamard matrix H of order n, its associated *Hadamard basis* $\{(U_H)_{ij}\}$ is defined as follows:

$$(U_H)_{ij} = \tfrac{1}{n} H \circ \mathrm{diag}(H, j)^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T, i) \tag{30}$$

Theorem 33. *A Hadamard basis is a quantum shift-and-multiply basis.*

Proof. By Definition 9 and Theorem 10 we have $(U_H)_{ij} = (Q_H)_j \circ \mathrm{diag}(H^T, i)$. Since the transpose of a Hadamard is also a Hadamard, the result follows. □

Corollary 34. *A Hadamard basis is a unitary error basis.*

Proof. Follows from Theorems 19 and 33. □

Definition 35 (See [21], Section 4)**.** Two Hadamard matrices are *equivalent* when one can be obtained from the other by permuting rows and columns, and multiplying rows and columns by unit complex numbers. Algebraically, H, H' are equivalent if there exist P_1, P_2 permutation matrices and D_1, D_2 unitary diagonal matrices such that:

$$H' = D_1 \circ P_1 \circ H \circ P_2 \circ D_2 \tag{31}$$

Proposition 36. *If two Hadamard matrices are equivalent by Definition 35, then their associated unitary error bases are equivalent by Definition 15.*

Proof. We will once again prove equivalence on a case-by-case basis. Again suppose $H' = P \circ H$. Then we have the following:

$$(U_{H'})_{ij} \overset{(30)}{=} \tfrac{1}{n} P \circ H \circ \mathrm{diag}(P \circ H, j)^\dagger \circ H^\dagger \circ P^{-1} \circ \mathrm{diag}(H^T \circ P^{-1}, i)$$

Again using the fact that P is real and unitary so, $P^{-1} = P^\dagger = P^T$. We continue:

$$\begin{aligned}
(U_{H'})_{ij} &\overset{(14)(15)}{=} \tfrac{1}{n} P \circ H \circ \mathrm{diag}(H, p(j))^\dagger \circ H^\dagger \circ P^{-1} \circ \mathrm{diag}(a_{p(0),i}, ..., a_{p(n-1),i}) \\
&\overset{(27)}{=} \tfrac{1}{n} P \circ H \circ \mathrm{diag}(H, p(j))^\dagger \circ H^\dagger \circ \mathrm{diag}(a_{p^{-1}p(0),i}, ..., a_{p^{-1}p(n-1),i}) \circ P^{-1} \\
&\overset{(10)}{=} \tfrac{1}{n} P \circ H \circ \mathrm{diag}(H, p(j))^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T, i) \circ P^{-1} \\
&\overset{(19)}{\sim} \tfrac{1}{n} H \circ \mathrm{diag}(H, p(j))^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T, i) \\
&\overset{(30)}{=} (U_H)_{i,p(j)}
\end{aligned}$$

The case that $H' = H \circ P$ is similar. Now suppose $H' = D \circ H$, with $D = \mathrm{diag}(c_1, \ldots, c_n)$, where $|c_i| = 1$. Then we calculate as follows:

$$\begin{aligned}
(U_{H'})_{ij} &\overset{(30)}{=} \tfrac{1}{n} D \circ H \circ \mathrm{diag}(D \circ H, j)^\dagger \circ H^\dagger \circ D^\dagger \circ \mathrm{diag}(H^T \circ D^\dagger, i) \\
&\overset{(16)}{=} \tfrac{1}{n} D \circ H \circ c_j \mathrm{diag}(H, j)^\dagger \circ H^\dagger \circ c_i^{-1} \mathrm{diag}(H^T \circ D^\dagger, i) \circ D^\dagger \\
&\overset{(17)}{=} \tfrac{c_j c_i^{-1}}{n} D \circ H \circ \mathrm{diag}(H, j)^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T, i) \circ D^\dagger \circ D^\dagger \\
&\overset{(19)}{\sim} \tfrac{1}{n} H \circ \mathrm{diag}(H, j)^\dagger \circ H^\dagger \circ \mathrm{diag}(H^T, i) \\
&\overset{(30)}{=} (U_H)_{ij}
\end{aligned}$$

The case $H' = H \circ D$ is similar. □

Proposition 37 (See [9], Theorem 1)**.** *All Hadamard matrices on $\mathbb{C}^4$ are equivalent to one of the following Fourier matrices, parameterised by $\alpha \in [0, \frac{\pi}{2}]$:*

$$H_\alpha := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{i\alpha} & -e^{i\alpha} \\ 1 & -1 & -e^{i\alpha} & e^{i\alpha} \end{pmatrix} \tag{32}$$

Theorem 38. *Every unitary error basis for $\mathbb{C}^4$ arising from the Hadamard method is equivalent to a monomial basis.*

Proof. Write $\mathcal{F}_\alpha$ for the unitary error basis arising from H_α by the Hadamard method, for some fixed $\alpha \in [0, \frac{\pi}{2}]$. By Propositions 36 and 37 all unitary error bases arising from Hadamards in dimension 4 are equivalent to $\mathcal{F}_\alpha$, for some value of α. But the following unitary matrix simultaneously monomializes $\mathcal{F}_\alpha$, for all values of α:

$$Y := \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \tag{33}$$

The basis $\mathcal{F}'_\alpha = \{Y \circ F_{ij} \circ Y^\dagger | F_{ij} \in \mathcal{F}\}$ is listed in Section A.2, and is monomial and equivalent to $\mathcal{F}_\alpha$. This completes the proof. □

Corollary 39. *The basis $\mathcal{M}$ of Example 18 is not equivalent to a Hadamard basis.*

Proof. Follows from Theorems 29 and 38. □

6 Algebraic method

Another technique for constructing UEBs is the *algebraic method*, due to Knill [15]. UEBs obtained using this technique are called *nice error bases*. The main result in this section is Corollary 44, that the basis $\mathcal{M}$ of Example 18 is not equivalent to a nice error basis. Throughout this section, we use '$\propto$' to denote equality up to multiplication by a unit complex number.

Recall that for a finite group G, an *n-dimensional unitary projective representation* is a function $\rho : G \to U(n)$, valued in the group of n-by-n unitary matrices, and for any $g, g' \in G$ a complex number $\omega_{g,g'} \in \mathbb{C}$ with unit norm, such that we have $\rho(gg') = \omega_{g,g'}\rho(g)\rho(g')$ and $\rho(1) = \mathbb{I}_n$ where 1 is the group identity. We therefore have the following:

$$\rho(g)\rho(g') \propto \rho(gg') \text{ for all } g, g' \in G \tag{34}$$

The following result will also be useful.

Lemma 40. *Given a unitary projective representation ρ of a group G, the following holds:*

$$\rho(g)^\dagger \propto \rho(g^{-1}) \text{ for all } g \in G \tag{35}$$

Proof. As follows: $\rho(g)^\dagger = \rho(g)^\dagger\rho(1) = \rho(g)^\dagger\rho(gg^{-1}) \overset{(34)}{\propto} \rho(g)^\dagger\rho(g)\rho(g^{-1}) = \rho(g^{-1})$. □

We now give the definition of a nice error basis, and show that a nice error basis is a unitary error basis.

Definition 41 (Nice error basis. See [15], Section 2)**.** Let G be a finite group of order n^2, and let ρ be an n-dimensional unitary projective representation of G, such that for all $g \in G$ not equal to the identity, we have the following:

$$\mathrm{Tr}(\rho(g)) = 0 \tag{36}$$

Then a *nice error basis* $\mathcal{R}_{G,\rho} := \{\rho(g) \,|\, g \in G\}$ is the image of ρ.

Lemma 42 (See [14], Lemma 3)**.** *A nice error basis is a unitary error basis.*

We now prove a key proposition, which we will use to establish that our example basis $\mathcal{M}$ of Example 18 is not equivalent to a nice error basis.

Proposition 43. *Let $\mathcal{S}$ be a unitary error basis containing the identity matrix $\mathbb{I}_n$, such that $\mathcal{S}$ is equivalent to a nice error basis. Then up to multiplication by a unit complex number, $\mathcal{S}$ is closed under taking adjoints.*

Proof. Let $\mathcal{R}_{G,\rho}$ be a nice error basis, and let $\mathcal{S} = \{c_g U\rho(g)V \mid g \in G\}$ be an equivalent unitary error basis, with elements $\mathcal{S}_g := c_g U\rho(g)V$. Since by hypothesis $\mathbb{I}_n \in \mathcal{S}$, there is some $h \in G$ with $\mathcal{S}_h = c_h U\rho(h)V = \mathbb{I}_n$. In particular, writing '$\propto$' to indicate equality up to multiplication by a unit complex number, we have the following:

$$\mathbb{I}_n \propto U\rho(h)V \tag{37}$$
$$\mathcal{S}_g \propto U\rho(g)V \text{ for all } g \in G \tag{38}$$

We now perform the following calculation, for any $g \in G$:

$$(\mathcal{S}_g)^\dagger \overset{(38)}{\propto} V^\dagger\rho(g)^\dagger U^\dagger = \mathbb{I}_n V^\dagger\rho(g)^\dagger U^\dagger \mathbb{I}_n \overset{(37)}{\propto} U\rho(h)VV^\dagger\rho(g)^\dagger U^\dagger U\rho(h)V$$
$$= U\rho(h)\rho(g)^\dagger\rho(h)V \overset{(35)}{\propto} U\rho(h)\rho(g^{-1})\rho(h)V \overset{(34)}{\propto} U\rho(hg^{-1}h)V \overset{(38)}{\propto} \mathcal{S}_{hg^{-1}h}$$

So $\mathcal{S}$ is closed under adjoints, up to multiplication by a unit complex number. □

Corollary 44. *The basis $\mathcal{M}$ of Example 18 is not equivalent to a nice error basis.*

Proof. By inspection of the elements of $\mathcal{M}$, as listed in Section A.1. For a contradiction, let us assume that $\mathcal{M}$ is equivalent to a nice error basis. Note that $\mathcal{M}$ contains the identity matrix; then by Proposition 43, it must be closed under taking adjoints, up to a unit complex number. But this is clearly false: for example, the second element of the first row of $\mathcal{M}_{01}$ has absolute value $\frac{1}{\sqrt{5}}$, but no member of $\mathcal{M}$ has an element with the same absolute value in the second element of the first column. □

References

[1] Samson Abramsky and Bob Coecke. A categorical semantics of quantum protocols. In *Proceedings of the 19th Annual IEEE Symposium on Logic in Computer Science*, pages 415–425. IEEE, 2004. arXiv:quant-ph/0402130. doi:10.1109/LICS.2004.1319636.

[2] Samson Abramsky and Bob Coecke. Categorical quantum mechanics. *Handbook of quantum logic and quantum structures: quantum logic*, pages 261–324, 2008.

[3] Somshubhro Bandyopadhyay, Oscar P. Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002. arXiv:quant-ph/0103162. doi:10.1007/s00453-002-0980-7.

[4] Karol Bartkiewicz, Antonín Černoch, Karel Lemr, Adam Miranowicz, and Franco Nori. Experimental temporal steering and security of quantum key distribution with mutually-unbiased bases. quant-ph/1503.00612, 2015.

[5] Ingemar Bengtsson, Wojciech Bruzda, Asa Ericsson, Jan-Ake Larsson, Wojciech Tadej, and Karol Zyczkowski. MUBs and Hadamards of order six. *Journal of Mathematical Physics*, 48(5):052106, 2007. quant-ph/0610161. doi:10.1063/1.2716990.

[6] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895, 1993. doi:10.1103/PhysRevLett.70.1895.

[7] Bob Coecke and Ross Duncan. Interacting quantum observables: categorical algebra and diagrammatics. *New Journal of Physics*, 13(4):043016, 2011. arXiv:0906.4725. doi:10.1088/1367-2630/13/4/043016.

[8] Bob Coecke and Aleks Kissinger. Quantum computer science, lecture notes, 2013.

[9] Robert Craigen. Equivalence classes of inverse orthogonal and unit Hadamard matrices. *Bulletin of the Australian Mathematical Society*, 44(01):109–115, 1991. doi:10.1017/s0004972700029506.

[10] Vincenzo D'Ambrosio, Filippo Cardano, Ebrahim Karimi, Eleonora Nagali, Enrico Santamato, Lorenzo Marrucci, and Fabio Sciarrino. Test of mutually unbiased bases for six-dimensional photonic quantum systems. *Scientific reports*, 3, 2013. quant-ph/1304.4081. doi:10.1038/srep02726.

[11] Ronald Aylmer Fisher and Frank Yates. The 6×6 Latin squares. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 30.04, pages 492–507. Cambridge Univ Press, 1934. doi:10.1017/s0305004100012731.

[12] Sibasish Ghosh and Ajit Iqbal Singh. Invariants for maximally entangled vectors and unitary bases. arXiv:1401.0099, 2014.

[13] Mile Gu, Helen M Chrzanowski, Syed M Assad, Thomas Symul, Kavan Modi, Timothy C Ralph, Vlatko Vedral, and Ping Koy Lam. Observing the operational significance of discord consumption. *Nature Physics*, 8(9):671–675, 2012. arXiv:1203.0011. doi:10.1038/NPHYS2376.

[14] Andreas Klappenecker and Martin Rötteler. Unitary error bases: Constructions, equivalence, and applications. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 139–149. Springer, 2003. doi:10.1007/3-540-44828-4_16.

[15] Emanuel Knill. Group representations, error bases and quantum codes. Technical Report LAUR-96-2807, LANL, 1996. arXiv:quant-ph/9608049. doi:10.2172/373768.

[16] Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, and Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3):032305, 2013. doi:10.1103/physreva.88.032305.

[17] Benjamin Musto. Exploring quantum teleportation through unitary error bases. Master's thesis, Department of Computer Science, University of Oxford, 2014. Download.

[18] Peter Shor. Fault-tolerant quantum computation. In *Proceedings of 37th Symposium on Foundations of Computing*, pages 56–65. IEEE Computer Society Press, 1996. arXiv:quant-ph/9605011. doi:10.1007/978-0-387-30162-4_143.

[19] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C Hiesmayr. Entanglement detection via mutually unbiased bases. *Physical Review A*, 86(2):022311, 2012. quant-ph/1202.5058. doi:10.1103/physreva.86.022311.

[20] Wojciech Tadej and Karol Życzkowski. A concise guide to complex Hadamard matrices. *Open Systems & Information Dynamics*, 13(02):133–177, 2006. arXiv:quant-ph/0512154. doi:10.1007/s11080-006-8220-2.

[21] Reinhard Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, 2001. arXiv:quant-ph/0003070. doi:10.1088/0305-4470/34/35/332.

A Lists of unitary error bases

Here we list the unitary error bases that we make use of in the main text.

A.1 The unitary error basis $\mathcal{M}$

Here we list the unitary error basis $\mathcal{M}$ defined in Example 18.

$$\mathcal{M}_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{M}_{01} = \begin{pmatrix} 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{02} = \begin{pmatrix} 0 & \frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & \frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{03} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{10} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -i \end{pmatrix} \quad \mathcal{M}_{11} = \begin{pmatrix} 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{12} = \begin{pmatrix} 0 & \frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{13} = \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & -1 & 0 \\ 0 & i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{20} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \mathcal{M}_{21} = \begin{pmatrix} 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{22} = \begin{pmatrix} 0 & -\frac{2}{\sqrt{5}} & \frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & -\frac{i}{\sqrt{5}} & \frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{23} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{M}_{30} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix} \quad \mathcal{M}_{31} = \begin{pmatrix} 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{32} = \begin{pmatrix} 0 & -\frac{2i}{\sqrt{5}} & -\frac{i}{\sqrt{5}} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{i}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{5}} & -\frac{2}{\sqrt{5}} & 0 \end{pmatrix} \quad \mathcal{M}_{33} = \begin{pmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -1 & 0 \\ 0 & -i & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

A.2 The unitary error basis $\mathcal{F}'$

Here we list the unitary error basis $\mathcal{F}'$ defined in the proof of Theorem 38.

$$\mathcal{F}'_{00} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{01} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{02} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \mathcal{F}'_{03} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{10} = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \mathcal{F}'_{12} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} \quad \mathcal{F}'_{13} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ e^{-2ia} & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{20} = \begin{pmatrix} 0 & 0 & -e^{ia} & 0 \\ 0 & 0 & 0 & -1 \\ -e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{21} = \begin{pmatrix} 0 & 0 & e^{ia} & 0 \\ 0 & 0 & 0 & 1 \\ -e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{22} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ -e^{ia} & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{23} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ -e^{ia} & 0 & 0 & 0 \end{pmatrix}$$

$$\mathcal{F}'_{30} = \begin{pmatrix} 0 & 0 & e^{ia} & 0 \\ 0 & 0 & 0 & -1 \\ e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{31} = \begin{pmatrix} 0 & 0 & -e^{ia} & 0 \\ 0 & 0 & 0 & 1 \\ e^{ia} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{32} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ e^{ia} & 0 & 0 & 0 \end{pmatrix} \quad \mathcal{F}'_{33} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -e^{-ia} & 0 \\ 0 & -1 & 0 & 0 \\ e^{ia} & 0 & 0 & 0 \end{pmatrix}$$