Unitary Error Bases: Constructions, Equivalence, and Applications

Andreas Klappenecker
Department of Computer Science
Texas A&M University, College Station, TX 77843-3112, USA
Email: klappi@cs.tamu.edu

Martin Rötteler (contact author)
Department of C&O
University of Waterloo, Waterloo, Ontario, Canada, N2l 3G1
Email: roettele@ira.uka.de

Abstract — **Unitary error bases are fundamental primitives in quantum computing, which are instrumental in the design of quantum error-correcting codes, teleportation and superdense coding schemes. There are two prominent constructions of such bases: an algebraic construction using projective representations of finite groups, and a combinatorial construction using Latin squares and Hadamard matrices. An open problem posed by Schlingemann and Werner relates these two constructions, and asks whether each algebraic construction is equivalent to a combinatorial construction. We solve this problem by giving an explicit counterexample in dimension 165, which has been constructed using computer algebra systems.**

I. Introduction

A unitary error basis (UEB) in dimension d is a set $\mathcal{E}$ of d^2 unitary $d\times d$ matrices such that $\mathcal{E}$ is orthonormal with respect to the inner product $\langle A,B\rangle = \mathrm{tr}(A^\dagger B)/d$.

The most famous example is the Pauli basis, a UEB in 2 dimensions, which is given by the four Pauli matrices $\mathbf{1}_2$, σ_x, σ_y, and σ_z. UEBs are crucial in teleportation, super-dense coding, and quantum error-correction applications.

II. UEBs from Projective Representations

Nice error bases have been introduced by E. Knill, see also [1]. Let G be a group of order d^2 with identity element 1. A nice error basis in d dimensions is given by a set $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n) \,|\, g\in G\}$ of unitary matrices such that

(i) $\rho(1)$ is the identity matrix,

(ii) $\mathrm{tr}\,\rho(g) = 0$ for all $g\in G\setminus\{1\}$,

(iii) $\rho(g)\rho(h) = \omega(g,h)\,\rho(gh)$ for all $g,h\in G$,

where $\omega(g,h)$ is a phase factor. Conditions (i) and (iii) state that ρ is a projective representation of the group G.

Lemma 1 (Knill) *Nice error bases are UEBs.*

The following example shows that UEBs exist in all dimensions:

Example 2 *Let $d\geq 2$ be a integer, $\omega = \exp(2\pi i/d)$. Let X_d be the shift $X_d\,|x\rangle = |x-1 \bmod d\rangle$, and let Z_d be the diagonal matrix* $\mathrm{diag}(1,\omega,\omega^2,\dots,\omega^{d-1})$. *Then $\mathcal{E}_d := \{X_d^i Z_d^j | (i,j) \in \mathbb{Z}_d\times\mathbb{Z}_d\}$ is a nice error basis.*

III. Hadamard Matrices and Latin Squares

A complex Hadamard matrix H of order d is a matrix in $\mathrm{GL}(d,\mathbb{C})$ such that $H_{ik}\in\mathcal{U}(1)$, $0\leq i,k<d$, and $H^\dagger H = d\mathbf{1}$.

Let $\mathbf{H} = (H^{(i)} : 0\leq i<d)$ be a sequence of complex Hadamard matrices, and let L be a Latin square L of order d. A shift-and-multiply basis $\mathcal{E}$ associated with $L,\mathbf{H}$ is given by the unitary matrices

$$E_{ij} = P_j\,\mathrm{diag}(H^{(j)}_{ik} : 0\leq k<d),\quad i,j\in\mathbb{Z}_d, \tag{1}$$

where P_j is the matrix defined by $P_j(L(j,k),k) = 1$, for $0\leq k<d$, and 0 otherwise. In short, E_{ij} is determined by the ith row of the jth Hadamard matrix $H^{(j)}$, and by the entries of the jth row of the Latin square L; briefly $E_{ij}\,|k\rangle = H^{(j)}_{ik}\,|L(j,k)\rangle$.

Lemma 3 (Werner) *Shift-and-multiply bases are UEBs.*

Example 4 *The nice error basis $\mathcal{E}_d$ in Example 2 is a shift-and-multiply basis. Indeed, choose the Latin square $L = (j-i \bmod d)_{i,j\in\mathbb{Z}_d}$ and the complex Hadamard matrix $H = (\omega^{k\ell})_{k,\ell\in\mathbb{Z}_d}$, with $\omega = \exp(2\pi i/d)$. For example, if $d=3$, then*

$$L := \begin{pmatrix} 0 & 1 & 2\\ 2 & 0 & 1\\ 1 & 2 & 0\end{pmatrix},\ H = \begin{pmatrix} 1 & 1 & 1\\ 1 & \omega & \omega^2\\ 1 & \omega^2 & \omega\end{pmatrix},$$

where $\omega = \exp(2\pi i/3)$.

IV. Equivalence

Equivalence. Let $\mathcal{E}$ and $\mathcal{E}'$ be two unitary error bases in d dimensions. We say that $\mathcal{E}$ and $\mathcal{E}'$ are equivalent, in signs $\mathcal{E}\equiv\mathcal{E}'$, iff there exist unitary matrices $A,B\in\mathcal{U}(d)$ and constants $c_E\in\mathcal{U}(1)$, $E\in\mathcal{E}$, such that $\mathcal{E}' = \{c_E AEB : E\in\mathcal{E}\}$.

Schlingemann and Werner asked whether each nice error basis is equivalent to a shift-and-multiply basis. The main contribution of the paper is to show that the bases introduced in Sections II and III really give rise to different UEBs.

Theorem 5 *There exist shift-and-multiply UEBs which are not equivalent to nice error basis UEBs.*

The other direction is more involved. The proof uses a construction of Everett Dade for groups of central type having a nonmonomial irreducible representation of large degree.

Theorem 6 *There exist nice error basis UEBs which are not equivalent to shift-and-multiply UEBs.*

Acknowledgements

We would like to thank Thomas Beth, Everett Dade, Marty Isaacs, and Reinhard Werner for helpful discussions and remarks. Research supported by NSF grant EIA 0218582, Texas A&M TITF, and by the EC project Q-ACTA (IST-1999-10596).

References

[1] A. Klappenecker and M. Rötteler. Beyond Stabilizer Codes I: Nice Error Bases. *IEEE Trans. Inform. Theory*, 48(8):2392–2395, 2002.

[2] R. Werner. All teleportation and dense coding schemes. *J. Phys. A*, 34:7081–7094, 2001.