Unitary Error Bases: Constructions, Equivalence, and Applications

Andreas Klappenecker[1] and Martin Rötteler[2]

[1] Department of Computer Science
Texas A&M University, College Station, TX 77843-3112, USA
klappi@cs.tamu.edu
[2] Department of Combinatorics and Optimization
University of Waterloo, Waterloo, Ontario, Canada, N2l 3G1
roettele@ira.uka.de

Abstract. Unitary error bases are fundamental primitives in quantum computing, which are instrumental for quantum error-correcting codes and the design of teleportation and super-dense 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 answer this question by giving an explicit counterexample in dimension 165 which has been constructed with the help of a computer algebra system.

Keywords: Quantum codes, unitary error bases, monomial representations, Hadamard matrices, Latin squares.

1 Introduction

Orthonormal bases of unitary matrices are a recurring theme in quantum information processing. The most well-known example is provided by the Pauli basis

$$\mathcal{P} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \right\},$$

which is a unitary basis for the vector space $\mathbb{C}^{2\times 2}$. More generally, a set $\mathcal{E}$ of d^2 unitary $d \times d$ matrices is called a *unitary error basis* if and only if $\mathcal{E}$ is orthonormal with respect to the inner product $\langle A, B\rangle = \operatorname{tr}(A^\dagger B)/d$. These bases of $\mathbb{C}^{d\times d}$ play a fundamental role for quantum error-correcting codes and other typical applications of quantum information processing, like e.g. super-dense coding and teleportation schemes.

Unitary error bases have been studied in numerous works, even before the advent of quantum computing [6, 8–10, 12], yet surprisingly little is known about their general structure. Currently, there are two fundamentally different constructions of unitary error bases: An algebraic construction due to Knill [9], which yields so-called nice error bases, and a combinatorial construction due to Werner [14], which yields so-called shift-and-multiply bases. Schlingemann and Werner posed the following problem [11]:

Is every nice error basis equivalent to a basis of shift-and-multiply type?

We solve this problem.

2 Two Constructions of Unitary Error Bases

We begin by giving a simple characterization of unitary error bases. Suppose that U is a unitary matrix of dimension d^2. Let $E_i(U) = \sqrt{d}(U_{i,nd+m})_{n,m=0,\ldots,d-1}$ be the matrix obtained by arranging the ith row of U into a matrix. We call a matrix $U \in \mathcal{U}(d^2)$ a *UEB-matrix* if and only if $E_i(U)$ is a unitary matrix for all i in the range $0 \leq i < d^2$. The UEB-matrices characterize the unitary error bases:

Lemma 1. *If U is a UEB-matrix, then $\mathcal{E} = \{E_i \,|\, 0 \leq i < d^2\}$ is a unitary error basis. Conversely, if $\mathcal{E}$ is a unitary error basis in dimension d, then the matrix $\frac{1}{\sqrt{d}}(\mathrm{vec}(E))_{E\in\mathcal{E}} \in \mathcal{U}(d^2)$ is a UEB-matrix.*

Here we denote by $\mathrm{vec}(M)$ the row vector $(\mathrm{vec}(M))_\mu = M_{(\mu \,\mathrm{div}\, d, \mu \bmod d)}$ for any $d\times d$ matrix M. The proof of the lemma is a direct consequence of the definitions. If U is a UEB-matrix, then $\mathrm{diag}(c_E : E \in \mathcal{E})U(A^t \otimes B)$ is a UEB-matrix for all $A, B \in \mathcal{U}(d)$. This motivates the following notion of equivalence of unitary error bases given in the next paragraph.

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 $\mathcal{E} \equiv \mathcal{E}'$, if and only if there exist unitary matrices $A, B \in \mathcal{U}(d)$ and constants $c_E \in \mathcal{U}(1)$, $E \in \mathcal{E}$, such that

$$\mathcal{E}' = \{c_E AEB : E \in \mathcal{E}\}.$$

One readily checks that $\equiv$ is an equivalence relation.

Lemma 2. *Any unitary error basis in dimension 2 is equivalent to the Pauli basis.*

Proof: Let $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$ be the unitary error basis. This basis is equivalent to a basis of the form $\{\mathbf{1}_2, \mathrm{diag}(1,-1), B_3, B_4\}$. The diagonal elements of B_3 and B_4 are necessarily zero, because of the trace orthogonality relations. We may assume that B_3 and B_4 are of the form $B_3 = \mathrm{antidiag}(1, a)$ and $B_4 = \mathrm{antidiag}(1, -a)$, where $a = \exp(i\phi)$ for some $\phi \in \mathbb{R}$, since we are allowed to multiply the matrices with scalars. Conjugating the basis elements with the matrix $\mathrm{diag}(1, \exp(-i\phi/2))$ yields the matrices of Pauli basis up to scalar multiples, hence $\mathcal{A} \equiv \mathcal{P}$. □

In higher dimensions, we have an ubiquity of nonequivalent unitary error bases. In what follows we give a brief description of the two known constructions of unitary error bases.

Nice error bases. 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) $\operatorname{tr} \rho(g) = 0$ 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 3 (Knill). *A nice error basis is a unitary error basis.*

Proof: Let $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n) \,|\, g \in G\}$ be a nice error basis. Notice that $\rho(g)^\dagger = \omega(g^{-1},g)^{-1}\rho(g^{-1})$. Assume that g,h are distinct elements of G, then $g^{-1}h \neq 1$, hence $\operatorname{tr}(\rho(g)^\dagger\rho(h)) = \omega(g^{-1},g)^{-1}\omega(g^{-1},h)\operatorname{tr}(\rho(g^{-1}h)) = 0$ by property (ii) of a nice error basis. □

The next example shows that nice error bases exist in arbitrary dimensions:

Example 1. 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 $\operatorname{diag}(1,\omega,\omega^2,\ldots,\omega^{d-1})$. 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. This has been shown by an explicit calculation in [2].

Shift-and-Multiply Bases. Recall that a Latin square of order d is a $d \times d$ matrix such that each element of the set $\mathbb{Z}_d$ is contained exactly once in each row and in each column. 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

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

where P_j denotes the permutation matrix with entries 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 $E_{ij}\,|k\rangle = H^{(j)}_{ik}\,|L(j,k)\rangle$.

If all matrices in $\mathbf{H}$ are equal to a single Hadamard matrix H, then we refer to this basis as the shift-and-multiply basis associated with L, H.

Lemma 4 (Werner). *A shift-and-multiply basis is a unitary error basis.*

Proof: We have to show that $\operatorname{tr}(E^\dagger_{ij}E_{kl}) = 0$ when $(i,j) \neq (k,l)$. If $j \neq l$, then the matrix $P^\dagger_j P_l$ has a vanishing diagonal, whence $\operatorname{tr}(E^\dagger_{ij}E_{kl}) = 0$ for any choice of i and k. If $j = l$ and $i \neq k$, then $\operatorname{tr}(E^\dagger_{ij}E_{kj})$ is equal to the inner product of the ith and kth row of the complex Hadamard matrix $H^{(j)}$, hence $\operatorname{tr}(E^\dagger_{ij}E_{kj}) = 0$. □

Example 2. The nice error basis $\mathcal{E}_d$ in Example 1 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 $\omega = \exp(2\pi i/3)$. According to equation (1), the basis matrices E_{01} and E_{12} are respectively given by

$$E_{01} = \begin{pmatrix} 0\,1\,0 \\ 0\,0\,1 \\ 1\,0\,0 \end{pmatrix}, \; E_{12} = \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}.$$

The entries of the middle row of the Latin square L and the first row of the complex Hadamard matrix H determine the matrix E_{01}.

Abstract Error Groups. Let $\mathcal{E} = \{\rho(g) : g \in G\}$ be a nice error basis. A group H isomorphic to the group generated by the matrices $\rho(g)$ is called an abstract error group of $\mathcal{E}$.

The group H is not necessarily finite. However, if we multiply the representing matrices $\rho(g)$ by scalars c_g such that $c_g\rho(g)$ has determinant 1, then the resulting nice error basis $\mathcal{E}' = \{c_g\rho(g) : g \in G\}$ is equivalent to $\mathcal{E}$, and its abstract error group H' is finite.

Thus, if we consider a nice error basis up to equivalence, then we may assume without loss of generality that the associated abstract error group is finite.

Example 3. The abstract error group H_d associated with the nice error basis $\mathcal{E}_d$ from Example 1 is by definition isomorphic to the group generated by X_d and Z_d. An element of the group $\langle X_d, Z_d\rangle$ is of the form $\omega^z Z_d^y X_d^x$, because $X_d Z_d = \omega Z_d X_d$. Notice that H_d is isomorphic to the unitriangular subgroup of $\mathrm{GL}(3, \mathbb{Z}_d)$ given by

$$H_d \cong \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{Z}_d \right\}.$$

We prefer to describe the group H_d abstractly by the set of elements $(x, y, z) \in \mathbb{Z}_d^3$ with composition given by $(x, y, z)\circ(x', y', z') = (x+x', y+y, z+z'+xy')$, where all operation are modulo d.

Recall that a finite group H which has an irreducible representation of large degree $d = \sqrt{(H\!:\!Z(H))}$ is called a group of central type. It has been shown in [8] that a finite group H is an abstract error group if and only if it is a group of central type with cyclic center. A somewhat surprising consequence is that an abstract error group has to be a solvable group [8].

3 An Application of UEBs: Teleportation Schemes

Teleportation is an effect predicted by quantum mechanics, which allows to communicate the state of a quantum system from one location to another [3]. Teleportation has been demonstrated in experiments for binary quantum systems [5]. We give a description of teleportation schemes systems in *arbitrary dimensions* as an application of unitary error bases.

Let $\mathcal{E} = \{U_{i,j} : i, j = 0, \dots d-1\}$ be a unitary error basis in d dimensions. Denote by $|\varepsilon\rangle$ the quantum state $|\varepsilon\rangle := \sum_{i=0}^{d-1} |i\rangle |i\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$. This state is a maximally entangled, meaning that the partial traces satisfy $\mathrm{tr}_1 |\varepsilon\rangle\langle\varepsilon| = \mathrm{tr}_2 |\varepsilon\rangle\langle\varepsilon| = \frac{1}{d}\mathbf{1}_d$. Therefore, a local measurement of one of the subsystems of $|\varepsilon\rangle$ does not yield any information about the global state.

Next, we construct a unitary operator $U_\mathcal{E}$ starting from the unitary error basis $\mathcal{E}$. We denote by $U_{i,j}[n,m]$ the matrix entry at position (n,m) of the matrix $U_{i,j} \in \mathcal{E}$. Then $U_\mathcal{E}$ is defined as the UEB matrix which has the flattened and transposed matrices contained in $\mathcal{E}$ as rows: $U_\mathcal{E} = \frac{1}{\sqrt{d}}(\mathrm{vec}(E))_{E\in\mathcal{E}} \in \mathcal{U}(d^2)$. As mentioned in the introduction this matrix is unitary. Alternatively, we can write $U_\mathcal{E}$ in the form $U_\mathcal{E} = \sum_{i,j}\sum_{m,n} U_{i,j}[n,m] |i,j\rangle\langle m,n|$. The following lemma is the essential ingredient for the teleportation circuit.

Lemma 5. *Let $|\varepsilon\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be the maximally entangled state defined above and let $|\psi\rangle \in \mathbb{C}^d$ a quantum state. Furthermore let $U_\mathcal{E}$ be the unitary operation corresponding to the error basis $\mathcal{E} = \{U_{i,j}\}$. Then the identity $(U_\mathcal{E} \otimes \mathbf{1}_d)|\psi\rangle|\varepsilon\rangle = \sum_{i,j} |i,j\rangle U_{i,j} |\psi\rangle$. holds.*

Proof: Let $|\psi\rangle = \sum_\mu \alpha_\mu |\mu\rangle$. We make the following computation which is a mere juggling with the bra and ket notation.

$$\begin{aligned}
(U_\mathcal{E} \otimes \mathbf{1}_d)|\psi\rangle|\varepsilon\rangle &= \left(\sum_{i,j}\sum_{m,n} U_{i,j}[n,m]\,|i,j,k\rangle\langle m,n,k|\right) \sum_{\mu,\nu} \alpha_\mu |\mu\rangle|\nu\rangle|\nu\rangle \\
&= \sum_{i,j} |i,j\rangle \left(\sum_{m,n} U_{i,j}[n,m]\,|n\rangle\langle m|\right)\left(\sum_\mu \alpha_\mu |\mu\rangle\right) \\
&= \sum_{i,j} |i,j\rangle U_{i,j} |\psi\rangle . \square
\end{aligned}$$

We obtain the following theorem which generally is called "teleportation" of an unknown quantum state. The context in which this theorem applies is a two party protocol. We call the parties "Alice" and "Bob" and assume that they share an EPR pair, i. e., they both have one part of the state $|\varepsilon\rangle$, but they might be separated from each other. In particular we assume that Alice and Bob cannot perform joint operations on the state $|\varepsilon\rangle$, however they are allowed to perform local operations and to send classical messages.

Theorem 1. *Let $|\psi\rangle \in \mathbb{C}^d$ be an unknown quantum state, let $|\varepsilon\rangle = \sum_i |i\rangle\,|i\rangle$ be a maximally entangled state, and let $U_{\mathcal{E}}$ be the unitary transformation corresponding to the unitary error basis $\mathcal{E}$. Then the following protocol will transfer the state $|\psi\rangle$ from Alice to Bob:*

1. *Alice applies the operation $U_{\mathcal{E}} \in \mathcal{U}(d^2)$ to $|\psi\rangle$ and her part of $|\varepsilon\rangle$.*
2. *Alice performs a measurement in the standard basis. Let (i_0, j_0) with $i_0, j_0 \in \{0, \dots, d-1\}$ be the outcome of this measurement.*
3. *Alice sends the classical information (i_0, j_0) to Bob. This can be encoded using $2\log_2 d$ bits.*
4. *Bob performs $U^\dagger_{i_0,j_0}$ on his part of the state $|\varepsilon\rangle$ and retrieves the state $|\psi\rangle$.*

Proof: The hard part was already shown in Lemma 5. The operation affected by Alice prior to the measurement yield the state $(U_{\mathcal{E}} \otimes \mathbf{1}_d)\,|\psi\rangle\,|\varepsilon\rangle = \sum_{i,j} |i,j\rangle\, U_{i,j}\,|\psi\rangle$. A measurement of the first two registers, which are in Alice's possession, gives a random outcome (i_0, j_0). However, by this measurement the entangled quantum state $\sum_{i,j} |i,j\rangle\, U_{i,j}\,|\psi\rangle$ will collapse into just the term $U_{i_0,j_0}\,|\psi\rangle$ of this superposition. After Alice has send the information (i_0, j_0) about the outcome of the measurement to Bob, he in turn is able to apply U_{i_0,j_0} to recoup the original quantum state. □

Remark 1. It takes a potentially infinite amount of information to completely characterize the state $|\psi\rangle$ since it involve complex numbers in the description of the amplitudes. A remarkable feature of Theorem 1 is still it is possible to transmit $|\psi\rangle$ to a remote location by sending $2\log_2 d$ bits of classical information.

4 Error Bases That Are Not Nice

A unitary error basis, which is not equivalent to a nice error basis, is called wicked. We show now that there exist an abundance of wicked shift-and-multiply bases.

Theorem 2. *Let $\mathcal{E}_\alpha$ be the shift-and-multiply basis associated with L, H_α, where*

$$L = \begin{pmatrix} 0\,1\,2\,3 \\ 3\,0\,1\,2 \\ 2\,3\,0\,1 \\ 1\,2\,3\,0 \end{pmatrix}, \; H_\alpha = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{i\alpha} & -e^{i\alpha} \\ 1 & -1 & -e^{i\alpha} & e^{i\alpha} \end{pmatrix}.$$

If $\alpha \in \mathbb{Q}^\times$, then $\mathcal{E}_\alpha$ is not equivalent to a nice error basis.

Proof: Suppose there exist $A, B \in \mathcal{U}(4)$, and scalars c_{ij} such that the set $\{c_{ij} A U_{ij} B : i, j = 1, \dots, 4\}$ is a nice error basis. Without loss of generality, we may assume that the group G generated by the matrices $c_{ij} A U_{ij} B$ is finite.

Notice that $\mathcal{E}_\alpha$ contains the matrices $M_1 = \mathrm{diag}(1, -1, e^{i\alpha}, -e^{i\alpha})$, and $M_2 = \mathbf{1}_4$. Consequently, $(c_1 A M_1 B)(c_2 A M_2 B)^{-1} = c_1 c_2^{-1} A M_1 M_2^\dagger A^\dagger = c_1 c_2^{-1} A M_1 A^{-1}$ is an element of the group G. Since G is finite, it follows that $c_1 c_2^{-1} A M_1 A^{-1}$ and hence also that $c_1 c_2^{-1} M_1$ is of finite order. Looking at the entries of this matrix this implies that $c_1 c_2^{-1}$ and $c_1 c_2^{-1} e^{i\alpha}$ are roots of unity. It follows that $e^{i\alpha}$ would have to be a root of unity as well, contradicting the assumption $\alpha \in \mathbb{Q}^\times$. □

5 Nonmonomial Abstract Error Groups

In this section, we will answer the question raised by Schlingemann and Werner:

Theorem 3. *There exist nice error bases which are not equivalent to bases of shift-and-multiply type.*

We will prove this result with the help of abstract error groups. The following result will play a key role in our proof:

Theorem 4 (Dade, Isaacs). *There exists a group H of central type with cyclic center, with nonmonomial irreducible character χ of degree $\chi(1) = \sqrt{(H : Z(H))}$.*

Proof of Theorem 3: We actually show a stronger statement, namely that there are nice error bases which are not equivalent to monomial bases. By Theorem 4, there exists an abstract error group H that has a non-monomial irreducible unitary representation ρ of degree $d = \sqrt{(H : Z(H))}$. Denote by $\mathcal{E}$ a nice error basis associated with ρ, that is, $\mathcal{E} = \{\rho(t) \mid t \in T\}$, where T is a transversal of H modulo $Z(H)$, with $1 \in T$. Since ρ is nonmonomial, it is impossible to find a base change A such that $A\rho(t)A^\dagger$ is monomial for all $t \in T$. We show next that this property is even preserved with respect to $\equiv$.

Seeking a contradiction, we suppose that there exist unitary matrices A, B and scalars c_t such that $c_t A\rho(t)B$ is a monomial unitary error basis. Since the identity matrix $\mathbf{1}_d = \rho(1)$ is part of the nice error basis, we can conclude that the matrix $C = c_1 AB$ is monomial. But $c_t A\rho(t)B = c_t A\rho(t)(A^\dagger A)B = c_t/c_1 A\rho(t)A^\dagger C$ shows that the resulting equivalent error basis is nonmonomial. Indeed, among the matrices $A\rho(t)A^\dagger$ is at least one nonmonomial matrix U. Multiplying U with the monomial matrix C and the scalar prefactor c_i/c_1 cannot result in a monomial matrix, leading to a contradiction. $\square$

In the next section, we want to construct an explicit example of a nice error basis that is not equivalent to a shift-and-multiply basis. We will need an explicit example of a group H satisfying the assumptions of Theorem 4 for that purpose. Theorem 4 was independently proved by Everett Dade and by Martin Isaacs, but unfortunately their results remained unpublished. We construct H, following Dade's approach, and use MAGMA to construct an explicit counterexample.

6 An Explicit Counterexample

We construct now a nice error basis in dimension $165 = 3 \cdot 5 \cdot 11$, which is not equivalent to a shift-and-multiply basis. First, we recall some basic facts on semidirect products and the representations and automorphism groups of the finite Heisenberg groups.

Semidirect Products. Let N, H be finite groups, and let φ be a group homomorphism from H to $\mathrm{Aut}(N)$. Recall that the (outer) semidirect product $G = N \rtimes_\varphi H$ is a group defined on the set $N \times H$, with composition given by $(n_1, h_1)(n_2, h_2) = (n_1\, \varphi(h_1)(n_2), h_1 h_2)$. If the center of H acts trivially on N, then the center of the semidirect product is given by $Z(G) = Z(N) \times Z(H)$. Recall that a group G is said to be an *inner* semidirect product of the two subgroups H and N if and only if N is a normal subgroup of G such that $HN = G$ and $H \cap N = \{1_G\}$. A detailed discussion of semidirect products can be found for instance in [1].

An Irreducible Representation of H_p. Let p be an odd prime. The Heisenberg group H_p has an irreducible representation $\rho_p \colon H_p \to \mathcal{U}(p)$, which associates to an element $(x, y, z) \in H_p$ the matrix $\rho_p((x, y, z)) = \omega^z Z_p^y X_p^x$. Here ω denotes the primitive root of unity $\omega = \exp(2\pi i/p)$, and X_p and Z_p denote the generalized Pauli matrices, as defined in Example 1. We will derive a faithful irreducible matrix representation of degree 165 of the group $G = (H_5 \times H_{11}) \rtimes_\varphi H_3$ by a suitable composition of the representations ρ_3, ρ_5, and ρ_{11}.

Automorphisms of the Heisenberg group H_p. Let p be an odd prime. The Heisenberg group H_p defined in Example 3 has p^3 elements. Recall that the special linear group $\mathrm{SL}(2, \mathbb{F}_p)$ is a matrix group of order $(p+1)p(p-1)$, which is generated by the matrices

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \beta = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

The special linear group acts as an automorphisms group on the Heisenberg group H_p. Indeed, define $\alpha(x, y, z) = (-y, x, z - xy)$ and $\beta(x, y, z) = (x, x + y, z + \frac{(p+1)}{2} x^2)$. It is straightforward to check that $\alpha, \beta \in \mathrm{Aut}(H_p)$. We will construct the abstract error group by semidirect products of Heisenberg groups. We will need some more detailed knowledge about these automorphisms to tailor this construction to our needs.

Making the Automorphisms of H_5 and H_{11} explicit. The matrix group representing $G = (H_5 \times H_{11}) \rtimes_\varphi H_3$ is an inner semidirect product. This means that the action of the automorphism is realized by a conjugation with a matrix. It suffices to find matrices which realize the action of the generators α and β of $\mathrm{SL}(2, \mathbb{F}_p)$. Recall that $\alpha(1, 0, 0) = (0, 1, 0)$ and $\alpha(0, 1, 0) = (-1, 0, 0)$. This means we need to find a matrix $A \in \mathcal{U}(p)$ such that

$$X_p^A = Z_p \quad \text{and} \quad Z_p^A = X_p^{-1}.$$

The action of the automorphism β is determined by $\beta(1, 0, 0) = (1, 1, (p+1)/2)$ and $\beta(0, 1, 0) = (0, 1, 0)$. Hence we need to find a matrix $B \in \mathcal{U}(p)$ such that

$$X_p^B = \omega^{(p+1)/2} Z_p X_p \quad \text{and} \quad Z_p^B = Z_p.$$

We can choose A to be the discrete Fourier transform (DFT) of length p, i.e., $F_p = \frac{1}{\sqrt{p}}(\omega^{k\ell})_{k,\ell=0,\dots,p-1}$, with $\omega = \exp(2\pi i/p)$. Notice that the diagonal matrix $D_p = \mathrm{diag}(\omega^{i(i-1)/2} : 0 \leq i < p)$ satisfies $X_p^{D_p} = Z_p X_p$ and $Z_p^{D_p} = Z_p$. It follows that the matrix B can be chosen to be $B = D_p Z_p^{(p+1)/2}$.

A Nonmonomial Error Basis in Dimension 165. We need an element of order 3 of $\mathrm{SL}(2,\mathbb{F}_p)$ to specify the action of H_3 on $H_5 \times H_{11}$. We can choose for instance the element $\gamma = \beta\alpha\beta\alpha$ in $\mathrm{SL}(2,\mathbb{F}_p)$, i.e.,

$$\gamma = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The action of γ on the matrix representation $\rho_5(H_5)$ of the Heisenberg group H_5 is realized by conjugation with the matrix $R_5 = D_5 Z_5^3 \cdot F_5 \cdot D_5 Z_5^3 \cdot F_5 \in \mathcal{U}(5)$. Similarly, the action of γ on the matrix version of H_{11} is given by conjugation with $R_{11} = D_{11} Z_{11}^3 \cdot F_{11} \cdot D_{11} Z_{11}^3 \cdot F_{11} \in \mathcal{U}(11)$.

Recall that H_3 is generated by the two elements $(1,0,0)$ and $(0,1,0)$. According to the construction of Section 5, the action of H_3 is chosen such that the generator $(1,0,0)$ acts with γ on H_5 and trivially on H_{11}, and the generator $(0,1,0)$ acts trivially on H_5 and by γ on H_{11}. Explicitly, we obtain the matrix group:

$$\begin{aligned} G = \langle & \mathbf{1}_3 \otimes X_5 \otimes \mathbf{1}_{11},\ \mathbf{1}_3 \otimes Z_5 \otimes \mathbf{1}_{11},\ \mathbf{1}_3 \otimes \mathbf{1}_5 \otimes X_{11}, \\ & \mathbf{1}_3 \otimes \mathbf{1}_5 \otimes Z_{11},\ X_3 \otimes R_5 \otimes \mathbf{1}_{11},\ Z_3 \otimes \mathbf{1}_5 \otimes R_{11} \rangle. \end{aligned}$$

The group G is an inner semidirect product of the form $H_3 \ltimes (H_5 \times H_{11})$. Indeed, the subgroup generated by the first four generators is isomorphic to $N = H_5 \times H_{11}$ since the irreducible representations of a direct product are given by tensor products of the irreducible representations of the factors. We have $N \lhd G$ because of the choice of R_5 and R_{11}. The complement H of N is given by the group generated by the to remaining generators. Obviously the intersection $H \cap N$ is trivial and $G = HN$ by definition. This shows that $G = H \ltimes N$.

This also shows that $|G| = 4492125 = 3^3 5^3 11^3$, that the centre is of order $\zeta(G) = 165 = 3 \cdot 5 \cdot 11$ and that G itself defines an irreducible representation. This can also be obtained by an enumeration of G using Magma [4]. Starting from this a pc-group presentation [13] of G can be computed and we obtain

$$\begin{aligned} G = \langle a_1, \ldots, a_9 | & a_1^3 = a_9^9,\ a_2^3 = a_8^3,\ a_3^3 = a_4^5 = a_5^5 = a_6^{11} = a_7^{11} = a_8^5 = a_9^{11} = 1, \\ & [a_2, a_1] = a_3^2,\ [a_4, a_2] = a_5, [a_5, a_2] = a_5^{-1} a_4^2 a_5^3 a_8^3, [a_5, a_4] = a_8, \\ & [a_6, a_1] = a_7 a_9^{10},\ [a_7, a_1] = a_7^{-1} a_6^8 a_7^9 a_9^8,\ [a_7, a_6] = a_9^{10} \rangle. \end{aligned}$$

Once a finite group is given as a pc-group many computational tasks can be accomplished easily. For instance using computer algebra systems like Gap [7] or Magma [4] we can check that G and $\zeta(G)$ indeed have the desired orders. Using the command `CharacterDegrees` in Gap we can check that G has irreducible representations of degree 165. One of these representations is given by the generators above. The fact that this representation of degree 165 is nonmonomial can be verified by computing the whole subgroup lattice of G. It turns out that G does not have subgroups of index 165 (in Gap this can be checked using the command `Lattice(G)`). Since each monomial representation χ is induced by a linear character from a subgroup H of index $\chi(1) = [G : H]$, and no such subgroup exists in the subgroup lattice of G, we can conclude that G is nonmonomial.

We obtain a non-monomial nice error basis by choosing a transversal of $Z(G)$ in G. This nice error basis is in particular not equivalent to a shift-and-multiply basis.

7 Conclusions

We have studied unitary error basis for d dimensional systems, for $d \geq 2$. We have shown that all such bases are equivalent in dimension 2. This changes dramatically in higher dimensions. We have shown that nice error bases are in general not equivalent to shift-and-multiply bases, and vice versa. This answers an open problem posed by Schlingemann and Werner. Also the use of unitary error bases for the construction of general nonbinary teleportation schemes has been described.

Acknowledgments. This research was supported by NSF grant EIA 0218582, Texas A&M TITF, and by the EC project Q-ACTA (IST-1999-10596). We thank Everett Dade and Martin Isaacs for discussions about groups of central types with nonmonomial representations. The construction of the nonmonomial character of extremal degree given in Section 5 is due to Everett Dade. We thank Thomas Beth for supporting this work.

References

1. J. L. Alperin and R. B. Bell. *Groups and representations*, volume 162 of *Graduate texts in mathematics*. Springer, 1995.
2. A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.
3. 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):1895–1899, 1993.
4. W. Bosma, J.J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24:235–266, 1997.
5. D. Bouwmeester, J. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.
6. R. Frucht. Über die Darstellung endlicher Abelscher Gruppen durch Kollineationen. *J. Reine Angew. Math.*, 166:16–28, 1931.
7. The GAP Team, Lehrstuhl D für Mathematik, RWTH Aachen, Germany and School of Mathematical and Computational Sciences, U. St. Andrews, Scotland. GAP – *Groups, Algorithms, and Programming, Version 4*, 1997.
8. A. Klappenecker and M. Rötteler. Beyond Stabilizer Codes I: Nice Error Bases. *IEEE Trans. Inform. Theory*, 48(8):2392–2395, 2002.
9. E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.
10. J. Patera and H. Zassenhaus. The Pauli matrices in n dimensions and finest gradings of simple Lie algebras of type A_{n-1}. *J. Math. Phys.*, 29(3):665–673, 1988.
11. D. Schlingemann. Problem 6 in Open Problems in Quantum Information Theory. http://www.imaph.tu-bs.de/qi/problems/.
12. J. Schwinger. Unitary operator bases. *Proc. Nat. Acad. Sci.*, 46:570–579, 1960.
13. Ch. Sims. *Computation with finitely presented groups.* Cambridge University Press, 1994.
14. R. Werner. All teleportation and dense coding schemes. *J. Phys. A*, 34:7081–7094, 2001.