On the Monomiality of Nice Error Bases

Andreas Klappenecker and Martin Rötteler

Abstract— **Unitary error bases generalize the Pauli matrices to higher dimensional systems. Two basic constructions of unitary error bases are known: An algebraic construction by Knill, which yields nice error bases, and a combinatorial construction by Werner, which yields shift-and-multiply bases. An open problem posed by Schlingemann and Werner relates these two constructions and asks whether each nice error basis is equivalent to a shift-and-multiply basis. We solve this problem and show that the answer is negative. However, we also show that it is always possible to find a fairly sparse representation of a nice error basis.**

Keywords— **Pauli matrices, unitary error bases, monomial representations, Hadamard matrices, Latin squares.**

I. Introduction

Unitary error bases are important primitives in quantum information theory. They form the basis of quantum error-correcting codes, teleportation, and dense coding schemes. A unitary error basis is by definition an orthonormal basis of the vector space of complex $d \times d$ matrices with respect to the inner product $\langle A, B\rangle = 1/d\,\mathrm{tr}(A^\dagger B)$. Such bases have been studied in numerous works, see for instance [1–6]. However, surprisingly little is known about their general structure.

Currently, two fundamentally different constructions of unitary error bases are known: An algebraic construction due to Knill [3], which yields nice error bases, and a combinatorial construction due to Werner [7], which yields shift-and-multiply bases. The nice error bases of small dimension have been completely classified in [2]. A quick inspection of this catalogue shows that each nice error basis in dimension $d \leq 5$ is in fact equivalent to a basis of shift-and-multiply type. This motivated Schlingemann and Werner to formulate the following problem [8, 9]:

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

We will give a precise explanation of the technical terms in the next section. An affirmative answer to this problem would imply that a nice error basis can be represented by monomial matrices, which have only one nonzero entry in each row and in each column.

Do nice error bases really have such a simple structure? The answer is no, as we will show in this correspondence. However, we will prove that each nice error basis is equivalent to a unitary error basis where at least half of the entries in the basis matrices are zero. In that sense, the nice error bases are simpler than one would expect.

We will recall the definition and some properties of nice error bases and shift-and-multiply bases in the next section. We introduce a notion of equivalence for unitary error bases in Section III. We show that there exist shift-and-multiply bases which are not nice error bases. We then go on to prove that there exists an infinite number of nice error bases, which are not of shift-and-multiply type. We construct an explicit counterexample in dimension 165 in Section V.

Notations. We denote by $\mathbb{C}$ the field of complex numbers, by $\mathbb{Z}$ the ring of integers, by $\mathbb{Z}_d$ the ring of integers modulo d. The group of unitary $d \times d$ matrices is denoted by $\mathcal{U}(d)$, the general linear group by $\mathrm{GL}(d, \mathbb{C})$.

The work by A.K. was supported in part by NSF grant EIA 0218582 and a Texas A&M TITF grant. The work by M.R. was supported in part by EC grant IST-1999-10596 (Q-ACTA), by CSE and MITACS.

A. Klappenecker is with the Department of Computer Science, Texas A&M University, College Station, TX 77843-3112, USA (e-mail: klappi@cs.tamu.edu)

M. Rötteler is with the Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada, N2l 3G1 (e-mail: roettele@iqc.ca)

II. Construction of Unitary Error Bases

A unitary error basis is a set $\mathcal{E}$ of d^2 unitary $d \times d$ matrices such that $\mathrm{tr}(E^\dagger F) = 0$ for all distinct $E, F \in \mathcal{E}$. The set $\mathcal{P}$ of Pauli matrices provides the most well-known example:

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

Unitary error bases generalize this example to arbitrary dimensions. The nonbinary case is more interesting, since there exist different, non-equivalent, error bases. We review in this section the constructions of unitary error bases by Knill and by Werner.

A. 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 1: 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 an arbitrary unitary error basis in dimension 2. 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 $\mathcal{A} \equiv \mathcal{P}$. ■

B. 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 $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n) \mid g \in G\}$ 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 2 (Knill) A nice error basis is a unitary error basis.

Proof: Let $\mathcal{E} = \{\rho(g) \in \mathcal{U}(n) \mid g \in G\}$ 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 3: Let $d \geq 2$ be a integer, $\omega = \exp(2\pi i/d)$. Let X_d denote the cyclic shift $X_d\,|x\rangle = |x - 1 \bmod d\rangle$, and let Z_d denote 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 [10].

C. 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

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

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 $\operatorname{tr}(E_{ij}^\dagger E_{kl}) = 0$ when $(i,j) \neq (k,l)$. If $j \neq l$, then the matrix $P_j^\dagger P_l$ has a vanishing diagonal, whence $\operatorname{tr}(E_{ij}^\dagger E_{kl}) = 0$ for any choice of i and k. If $j = l$ and $i \neq k$, then $\operatorname{tr}(E_{ij}^\dagger E_{kj})$ is equal to the inner product of the ith and kth row of the complex Hadamard matrix $H^{(j)}$, hence $\operatorname{tr}(E_{ij}^\dagger E_{kj}) = 0$. ■

Example 5: The nice error basis $\mathcal{E}_d$ in Example 3 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}.

D. 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 6: The abstract error group H_d associated with the nice error basis $\mathcal{E}_d$ from Example 3 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 [2] 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.

III. Wicked Error Bases

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 7: 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 $\{c_{ij} A U_{ij} B : i, j = 1, \ldots, 4\}$ 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 the unitary error basis $\mathcal{E}_\alpha$ 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 individual 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 $\alpha \in \mathbb{Q}^\times$. ■

IV. Sparsity of Nice Error Bases

A matrix is said to be monomial if and only if it contains exactly one nonzero entry in each row and in each column. If a nice error basis $\mathcal{E}$ is also a shift-and-multiply basis, then all matrices $M \in \mathcal{E}$ are monomial. This does not have to be the case. However, our next result shows that a nice error basis is always equivalent to a fairly sparse error basis:

Theorem 8: Let $\mathcal{E}$ be a nice error basis. There exists an equivalent nice error basis $\mathcal{E}_s \equiv \mathcal{E}$ such that at least half of the entries of each matrix $M \in \mathcal{E}_s$ are zero.

Proof: There exists a nice error basis $\mathcal{E}' \equiv \mathcal{E}$ such that the abstract error group H of $\mathcal{E}'$ is finite. The group generated by the matrices of $\mathcal{E}'$ is an irreducible matrix group isomorphic to H. In other words, H has an irreducible unitary representation ρ such that

$$\mathcal{E}' = \{\rho(t) \,|\, t \in T\},$$

where T is a transversal of H modulo $Z(H)$.

Recall that a character χ of H is said to be induced from an irreducible character ψ of a proper subgroup K of H if χ is of the form

$$\chi(x) = \frac{1}{|K|} \sum_{\substack{h \in H \\ hxh^{-1} \in K}} \psi(hxh^{-1}).$$

Let χ be the irreducible character of H corresponding to the representation ρ. If χ is induced by an irreducible character of a proper subgroup of H, then there exists a base change $A \in \mathcal{U}(d)$ such that at least half of the entries of the matrices $A\rho(h)A^{-1}$ are zero.

Seeking a contradiction, we assume that χ is not induced by an irreducible character of some proper subgroup of H. In other words, we assume that χ is a primitive character. Notice that the degree of χ is large, $\chi(1) = \sqrt{(H:Z(H))}$. It follows that the multiple $\chi(1)\chi$ of the character χ is induced from a character from the center $Z(H)$, see [11]. Since H is an abstract error group, it is in particular a solvable group [2]. It has been shown by Ferguson and Isaacs [12] that the multiple of a primitive character of a solvable group can never be induced from an irreducible character of a proper subgroup, contradiction.

It follows that $\mathcal{E}_s = \{A\rho(t)A^{-1} \,|\, t \in T\}$ is a nice error basis, and half of the entries of $A\rho(t)A^\dagger$ are zero. By construction, $\mathcal{E} \equiv \mathcal{E}' \equiv \mathcal{E}_s$, hence $\mathcal{E} \equiv \mathcal{E}_s$ as claimed. ■

V. Nonmonomial Abstract Error Groups

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

Theorem 9: 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 10 (Dade, Isaacs) There exist a group H of central type with cyclic center, which has a nonmonomial irreducible character χ of degree $\chi(1) = \sqrt{(H:Z(H))}$.

Proof of Theorem 9: We actually show a stronger statement, namely that there are nice error bases which are not equivalent to monomial bases.

By Theorem 10, 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,

$$\mathcal{E} = \{\rho(t) \,|\, t \in T\}$$

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 the equivalence $\equiv$.

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_t/c_1 cannot result in a monomial matrix, leading to a contradiction. ■

Remark. We have shown in the proof of Theorem 8 that an irreducible character χ of large degree of an abstract error group H is always induced from an irreducible character ψ of a proper subgroup. The essence of Theorem 10 is that in general we cannot choose ψ to be a linear character.

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 10 for that purpose. Theorem 10 was independently proved by Everett Dade and by Martin Isaacs, but unfortunately their results remained unpublished. Our exposition is a variation of Dade's approach, which we include here with the kind permission of Professor Dade.

A. 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 $(n_1, h_1)(n_2, h_2) = (n_1\,\varphi(h_1)(n_2), h_1h_2)$. If the center of H acts trivially on N, then the center of the semidirect product is given by $Z(G) = Z(N) \times Z(H)$. A detailed discussion of semidirect products can be found for instance in [13].

B. Automorphisms of the Heisenberg group H_p

Let p be an odd prime. The Heisenberg group H_p defined in Example 6 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

$$\begin{aligned} \alpha(x, y, z) &= (-y, x, z - xy), \\ \beta(x, y, z) &= (x, x + y, z + \tfrac{(p+1)}{2}\, x^2). \end{aligned}$$

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.

Recall that a matrix M is said to act irreducibly on a vector space V if and only if $\{0\}$ and V are the only M-invariant subspaces of V.

Lemma 11: Let r, p be odd prime numbers such that $r|(p+1)$. The group $\mathrm{SL}(2, \mathbb{F}_p)$ contains matrices of order r, and all such matrices act irreducibly on $\mathbb{F}_p \times \mathbb{F}_p$.

Proof: It is known that the group $\mathrm{SL}(2, \mathbb{F}_p)$ has a cyclic subgroup of order $p + 1$, hence contains matrices of order r, see [14, p. 42]. Let $g \in \mathrm{SL}(2, \mathbb{F}_p)$ be an element of order r. The subgroup $R = \langle\, g\, \rangle$ of order r acts on the vector space $V = \mathbb{F}_p \times \mathbb{F}_p$. The orbit length $|Rv| \in \{1, r\}$ for all $v \in V$. If we denote by U the centralizer of R, then r divides $|V| - |U| = p^2 - p^k$, where $k \in \{0, 1\}$. Since r does not divide $p - 1$ or p, it follows that k has to be 0. Thus, $0 \in V$ is the only fixed point. It follows that $\{0\}$ and V are the only R-invariant subspaces of V. Indeed, suppose that V' is an R-invariant subspace with p elements, then the number of elements in $V' - \{0\}$ must be a multiple of r, contradicting $r \nmid (p - 1)$. ∎

Remark: The preceding lemma also follows from Theorem 3.5 in Hering [15].

C. A nonmonomial nice error group

We take now the Heisenberg groups as a starting point to construct an abstract error group G of a nice error basis, which is not equivalent to a shift-and-multiply basis.

Let p, q, and r be three distinct odd primes such that r divides $p + 1$ and $q + 1$. Define

$$G = (H_p \times H_q) \rtimes_\varphi H_r,$$

where the action φ is chosen such that $\varphi(g)$ acts trivially on $H_p \times H_q$ for all $g \in Z(H_r)$.

Lemma 12: The group G is of central type with cyclic center. The center $Z(G)$ is of order pqr.

Proof: The three Sylow subgroups H_p, H_q, and H_r of the group G are of central type. Since the center of H_r acts trivially on $H_p \times H_q$, we have $Z(G) = Z(H_p) \times Z(H_q) \times Z(H_r)$. In particular, $H_\ell \cap Z(G) = Z(H_\ell)$ for $\ell \in \{p, q, r\}$. It follows from Theorem 2 of [16] that G is a group of central type.

The center of a Heisenberg group H_d is given by the cyclic subgroup $Z(H_d) = \{(0, 0, z) \,|\, z \in \mathbb{Z}_d\}$. The center of G is thus a direct product of cyclic groups of coprime orders, hence $Z(G)$ is a cyclic group of order pqr. ∎

We want to choose φ such that G does not contain a subgroup of index pqr. If this is the case, then a character $\chi \in \mathrm{Irr}(G)$ of degree $\chi(1) = \sqrt{(G\!:\!Z(G))} = pqr$ cannot be monomial, because a monomial character is induced from a linear character of a subgroup of index pqr.

Lemma 13: If G has a subgroup H of index $(G : H) = pqr$, then there exists a conjugate subgroup $K = H^g$ such that $|K \cap H_p| = p^2$, $|K \cap H_q| = q^2$, and $|K \cap H_r| = r^2$,

Proof: The Sylow subgroups H_p and H_q of G are normal, hence respectively contain the subgroups of order p^2 and of order q^2 of H^g for any $g \in G$. The subgroup of order r^2 of H is contained in some Sylow subgroup of G. The claim follows, since the r-Sylow subgroups in G are all conjugate by Sylow's theorem. ∎

Theorem 14: Let p, q, r be distinct odd primes such that r divides $p + 1$ and $q + 1$. It is possible to choose φ such that $G = (H_p \times H_q) \rtimes_\varphi H_r$ is a group of central type that does not contain a subgroup of index pqr.

Proof: First, we define the action φ of H_r on $H_p \times H_q$. Recall that the Heisenberg group H_r is generated by the two elements $a = (1, 0, 0)$ and $b = (0, 1, 0)$. Let $A, B \in \mathrm{SL}(2, \mathbb{F}_p)$ be matrices of order r. The element a acts with A on H_p, and trivially on H_q. Similarly, the element b acts trivially on H_p, and with B on H_p.

Notice that $c = (0, 0, 1) = aba^{-1}b^{-1}$ generates the center of H_r. It follows that c acts trivially on $H_p \times H_q$, hence $Z(H_r)$ acts trivially on $H_p \times H_q$. An immediate consequence is that the center of G is given by $Z(G) = Z(H_p) \times Z(H_q) \times Z(H_r)$.

The Sylow subgroups of G are isomorphic to the Heisenberg groups H_p, H_q, and H_r, whence all Sylow subgroups of G are of central type. Moreover, the construction of G ensures that the intersection of a Sylow subgroup P of G with the center $Z(G)$ gives $Z(P)$. It follows from Theorem 2 of [16] that G is a group of central type.

Seeking a contradiction, we suppose that G has a subgroup of index pqr. Lemma 13 shows that G must then have a subgroup K such that the intersection of K with H_p, H_q, and H_r contains p^2, q^2, and r^2 elements, respectively.

Let $X = \langle a, c\rangle$ and $Y = \langle b, c\rangle$; both are subgroups of order r^2 of the Heisenberg group H_r. The subgroup $K_r = H_r \cap K$ cannot coincide with both X and Y. Suppose that $K_r \neq X$. Since $H_r = \langle K_r, X\rangle$, the group K_r must act irreducibly on $H_q/Z(H_q)$. The subgroup $K_q = K \cap H_q$ cannot exist, because K_r would have to normalize $K_q/Z(K_q)$, which is impossible. Similarly, if $K_r \neq Y$, then the subgroup $K_p = K \cap H_p$ cannot exist. Therefore, the group K cannot exist. This proves that G does not contain a subgroup of index pqr. ■

VI. An Explicit Counterexample

We take now a closer look at the examples given in the previous section. Specifically, it is our goal is to make the construction explicit for the smallest possible choice of parameters. This will give us a concrete example of a nice error basis in dimension $165 = 3 \cdot 5 \cdot 11$ that is not equivalent to a shift-and-multiply basis.

A. A 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 3.

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}.

B. Automorphisms of H_p

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 $H \cap N = \{1_G\}$.

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

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

Similarly, 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 $F_p = \frac{1}{\sqrt{p}}(\omega^{k\ell})_{k,\ell=0,\dots,p-1}$, 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 $B = D_p Z_p^{(p+1)/2}$.

C. 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.,

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

One easily verfies that $\gamma^3 = \mathbf{1}$.

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 V, 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 $G = H \ltimes N$.

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.

VII. Conclusions

We have studied unitary error bases for higher-dimensional systems. 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 solves an open problem posed by Schlingemann and Werner.

Acknowledgments

We thank Everett Dade and Marty Isaacs for discussions on non-monomial representations of groups of central type. The construction of the nonmonomial character of extremal degree given in Section V is due to Everett Dade. We thank Thomas Beth for his encouragement and support.

References

[1] R. Frucht, “Über die Darstellung endlicher Abelscher Gruppen durch Kollineationen,” *J. Reine Angew. Math.*, vol. 166, pp. 16–28, 1931.

[2] A. Klappenecker and M. Rötteler, "Beyond Stabilizer Codes I: Nice Error Bases," *IEEE Trans. Inform. Theory*, vol. 48, no. 8, pp. 2392–2395, 2002.

[3] E. Knill, "Group representations, error bases and quantum codes," Los Alamos National Laboratory Report LAUR-96-2807, 1996.

[4] J. Schwinger, "Unitary operator bases," *Proc. Nat. Acad. Sci.*, vol. 46, pp. 570–579, 1960.

[5] J. Schwinger, *Quantum Mechanics - Symbolism of Atomic Measurements,* (edited by B.-G. Englert), Springer, Heidelberg, 2001.

[6] 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.*, vol. 29, no. 3, pp. 665–673, 1988.

[7] R. Werner, "All teleportation and dense coding schemes," *J. Phys. A*, vol. 34, pp. 7081–7094, 2001.

[8] D. Schlingemann, "Problem 6 in Open Problems in Quantum Information Theory," http://www.imaph.tu-bs.de/qi/problems/.

[9] R.F. Werner, "Personal communication," November 16, 2000.

[10] A. Ashikhmin and E. Knill, "Nonbinary quantum stabilizer codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 3065–3072, 2001.

[11] I.M. Isaacs, *Character Theory of Finite Groups*, Dover, New York, 1976.

[12] P. Ferguson and I.M. Isaacs, "Induced characters which are multiples of irreducible characters," *J. Algebra*, vol. 124, pp. 149–157, 1989.

[13] J. L. Alperin and R. B. Bell, *Groups and representations*, vol. 162 of *Graduate texts in mathematics*, Springer, 1995.

[14] D. Gorenstein, *Finite Groups*, Chelsea, New York, 1980.

[15] C. Hering, "Transitive linear groups and linear groups which contain irreducible subgroups of prime order," *Geom. Dedicata*, vol. 2, pp. 425–460, 1974.

[16] F. R. DeMeyer and G. J. Janusz, "Finite groups with an irreducible representation of large degree," *Math. Z.*, vol. 108, pp. 145–153, 1969.