Chapter 1

Clifford Codes

Andreas Klappenecker

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

Martin Rötteler

Institut für Algorithmen und Kognitive Systeme (Professor Thomas Beth), Universität Karlsruhe, Am Fasanengarten 5, D-76128 Karlsruhe, Germany, roettele@ira.uka.de

Abstract Quantum error control codes allow to detect and correct errors that are due to decoherence effects. We review some basic properties of these codes and give some constructions. Our main focus will be on a construction of quantum error control codes that have been introduced by Knill in 1996 with the intention to generalize stabilizer codes. These so-called Clifford codes can be constructed and analyzed with tools from representation theory of finite groups. We show that a large class of Clifford codes are actually stabilizer codes. And we construct the smallest example of a Clifford code that is not a stabilizer code.

1.1 Introduction

A quantum computer takes advantage of entangled states stored in the state of atoms, nuclear spins, photons, or other quantum systems. The interaction of the quantum computer with its environment leads to decoherence errors which alter the state of the memory. The protection of the memory against these errors is a crucial part in the construction of a resilient quantum computer. We describe in this chapter a generalization of stabilizer codes that allows to protect the encoded states.

The first quantum error correcting codes have been introduced by Shor [21] and Steane [24] about six years ago. The existence of such codes is a remarkable fact, since it shows that an infinite variety of errors affecting a single quantum bit can be corrected by a finite number of operations. Moreover, the subsequent development of fault-tolerant architectures [22] made it clear that quantum computing can overcome the imprecision problems that defeated the successful implementation of analogue computers.

The theory of quantum error control codes developed rapidly after the initial results by Shor and Steane. Calderbank and Shor showed that good quantum error correcting codes exist [7]. Their construction of a quantum error control code started from a classical binary linear code C containing its dual code $C^{\perp}$. This construction was independently discovered by Steane [23] and the quantum codes are now known as Calderbank-Shor-Steane codes or shortly CSS codes.

A more general class of quantum error control codes has been introduced by Gottesman [10] and Calderbank, Rains, Shor, and Sloane [5]. These codes are known as stabilizer codes or as additive codes. Most quantum error control codes known to date are constructed as stabilizer codes. The popularity of stabilizer codes stems from the fact that a large body of theory developed for classical error control codes can be translated into the quantum realm, as is explained in the seminal paper [6].

Some practical aspects of quantum codes have been discussed in the literature as well. For instance, Cleve and Gottesman give a construction of encoding circuits for binary stabilizer codes [8]. Grassl and Beth derive encoding and decoding circuits for cyclic codes [12].

The majority of publications on quantum error control codes is confined to the binary case: the encoding of several quantum bits into a larger set of quantum bits. This is somewhat surprising, since the

popular implementation models of quantum computing – cavity QED, trapped cold ions, or bulk spin NMR – all allow, at least in principle, to use more than just two level quantum systems. Moreover, the concatenation of codes used in fault-tolerant architectures [1] is most naturally understood in terms of quantum codes with bigger alphabets. We allow arbitrary alphabet sizes for that reason.

1.2 Motivation

A quantum computer stores its information in the state of quantum systems. The computational state space of a quantum system is a finite dimensional complex vector space $\mathbf{C}^d$, sometimes referred to as a qudit. This space is equipped with a standard orthonormal basis which is traditionally expressed in terms of Dirac's ket notation: $|0\rangle, \ldots, |d-1\rangle$.

The combination of several quantum systems yields the state space of the quantum computer

$$\mathcal{H} = \mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2} \otimes \cdots \otimes \mathbf{C}^{d_n}. \tag{1.1}$$

Notice that the quantum systems might have different dimensions d_i.

A quantum error control code is a subspace of $\mathcal{H}$. A well-designed quantum code allows to correct errors affecting only a few quantum systems, that is, a few tensor factors in (1.1). A small example will help to illustrate this feature.

Suppose that we want to protect the state of a single d-level quantum system. This can be done, for instance, by encoding the base states $|k\rangle$ into nine qudits by

$$|k\rangle \mapsto \frac{1}{d^{3/2}} \Big(\sum_{j=0}^{d-1} \omega^{kj} |jjj\rangle \Big) \otimes \Big(\sum_{j=0}^{d-1} \omega^{kj} |jjj\rangle \Big) \otimes \Big(\sum_{j=0}^{d-1} \omega^{kj} |jjj\rangle \Big), \tag{1.2}$$

where $k \in \{0, \ldots, d-1\}$ and $\omega = \exp(2\pi i/d)$. This quantum error control code is a straightforward generalization of Shor's code [21] to the nonbinary case.

The code (1.2) is able to correct an arbitrary error in one of the nine qudits. To see this, we note that the code is given by a concatenation of two codes. The inner code is a repetition code encoding a base state into three replicas

$$|k\rangle \mapsto |k\rangle \otimes |k\rangle \otimes |k\rangle \quad \text{with} \quad k \in \{0, \ldots, d-1\}.$$

This code can correct a shift error $X_\ell |k\rangle = |k + \ell \bmod d\rangle$ applied to a single qudit. The outer code protects against a single phase error $Z_\ell |k\rangle = \omega^{\ell k} |k\rangle$. It is obtained from the repetition code by applying the discrete Fourier transform to each component, that is,

$$|k\rangle \mapsto F|k\rangle \otimes F|k\rangle \otimes F|k\rangle, \quad \text{with} \quad k \in \{0, \ldots, d-1\},$$

where $F|k\rangle = d^{-1/2} \sum_{j=0}^{d-1} \omega^{kj} |j\rangle$.

The concatenated code (1.2) is then able to correct a single shift error, a single phase error, or a combination of both. In fact, the code is even able to correct all linear combinations of these errors, since the error recovery is a linear operation. Therefore, Shor's code (1.2) is able to correct an *arbitrary* error in one of the nine qudits.

Our point-of-view in the following sections will slighly differ from our approach taken in this motivating example. The error-correcting properties of a quantum error control code do not depend on the particular choice of basis nor on the choice of encoding map. Thus, we prefer a basis free approach in the following sections, since an analogue of (1.2) would be awkward in larger dimensions.

1.3 Quantum Error Control Codes

A *quantum error control code* is a subspace Q of a finite dimensional Hilbert space

$$\mathcal{H} = \mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2} \otimes \cdots \otimes \mathbf{C}^{d_n}. \tag{1.3}$$

We refer to $\mathcal{H}$ as the *ambient space* of Q. The *dimension* of the code Q is its dimension as a complex vector space.

Let E be an error operator acting on a quantum code Q. We say that E is *detectable* by Q if and only if

$$\langle w| E |w\rangle = \langle u| E |u\rangle \tag{1.4}$$

holds for all $u, w \in Q$ with $\|u\| = \|w\|$.

LEMMA 1.1
Let E be a detectable error on a quantum error control code Q. Then

$$\langle w|E|u\rangle = 0 \tag{1.5}$$

holds for all $w, u \in Q$ with $\langle w|u\rangle = 0$.

PROOF The statement is clearly true if $u = 0$ or $w = 0$. So, without loss of generality, we can assume that u and w are nonzero and normalized to the same length $\|w\| = \|u\|$. A simple calculation shows that $\langle w|E|u\rangle$ can be expressed in terms of the polarization identity

$$\begin{aligned}\langle w|E|u\rangle = \frac{1}{4}[\langle u+w|E|u+w\rangle - \langle u-w|E|u-w\rangle] \\ + \frac{i}{4}[\langle u+iw|E|u+iw\rangle - \langle u-iw|E|u-iw\rangle].\end{aligned}$$

However, $\|u+w\| = \|u-w\|$ and $\|u+iw\| = \|u-iw\|$ and therefore the terms in the brackets are zero by the length condition (1.4). ∎

Denote by P_Q the orthogonal projection from the ambient space $\mathcal{H}$ onto the quantum error control code Q. A simple consequence of the previous result is that an error operator E is detectable by Q if and only if the projection condition

$$P_Q E P_Q = \lambda_E P_Q, \qquad \lambda_E \in \mathbf{C}^\times \tag{1.6}$$

holds.

Suppose that we want to be able to correct for a certain set S of errors acting on Q. We want to be able to reliably distinguish between different encoded states that have been affected by correctable errors. Therefore, it is necessary that orthogonal states $u, w \in Q$ remain orthogonal

$$\forall u, w \in Q\colon \langle u|w\rangle = 0 \Longrightarrow \langle u|E_1^\dagger E_2|w\rangle = 0$$

for all possible errors E_1 and E_2 in S. However, this simply means that $E = E_1^\dagger E_2$ must be a detectable error:

LEMMA 1.2
Suppose that an error operator E acting on a quantum error control code Q satisfies

$$\forall u, w \in Q\colon \langle u|w\rangle = 0 \implies \langle u|E|w\rangle = 0. \tag{1.7}$$

Then E is a detectable error.

PROOF Let B be an orthonormal basis of Q. Suppose that u and w are distinct elements of B, then $\langle u+w|u-w\rangle = 0$, hence

$$0 = \langle u+w|E|u-w\rangle = \langle u|E|u\rangle - \langle w|E|w\rangle.$$

Therefore, $\langle u|E|u\rangle = \langle w|E|w\rangle$ for all $u, w \in B$. It follows that (1.4) holds for arbitrary $u, w \in Q$ with $\|u\| = \|w\|$. ∎

It has been shown by Knill and Laflamme [17] (see also Bennett *et al.* [4]) that this error correction condition is not only necessary but also sufficient. Thus, to summarize, a set of errors S can be *corrected* by a quantum error control code Q if and only if all errors in the set

$$S^\dagger S = \{E_1^\dagger E_2 \,|\, E_1, E_2 \in S\}$$

are detectable by Q. An elementary proof of this fact is given in the chapter by M. Grassl in this volume [11].

The detectable errors also lead us to the notion of minimum distance of a quantum error control code. The minimum distance is an essential parameter of a code, since it determines how many localized errors can be corrected by this code.

A *local error operator* is a linear operator E of the form

$$E = M_1 \otimes M_2 \otimes \cdots \otimes M_n,$$

where M_i is a linear operator acting on the tensor component $\mathbf{C}^{d_i}$ in the ambient space (1.3). A local error operator is thus compatible with the tensor product structure of the ambient space $\mathcal{H}$. The *weight* of the local error operator is given by the number of elements M_i that are not scalar multiples of the identity.

The code Q has *minimum distance* at least d if and only if all local errors of weight less than d are detectable by Q. A quantum error control code with minium distance $d = 2t+1$ allows to correct decoherence errors affecting up to t qudits.

REMARKS

(a) A detailed analysis of general quantum error control codes can be found in Knill and Laflamme [17]. Another early account is given by Bennett *et al.* [4]. We refer to articles by Knill, Laflamme, and Viola [18] and by Zanardi [25] for more recent discussions of the general theory of quantum error control codes.

(b) The notion of detectable errors has been explicitly introduced in [17] in the form (1.6). The equivalent form (1.4) has been used by Rains [19] in his definition of minimum distance of a quantum

code. Alternatively, one can define a detectable error by the orthogonality condition (1.7), as is shown by Lemma 1.1 and 1.2. Detectable errors have been studied in detail by Ashikhmin, Barg, Knill, and Litsyn in [2, 3].

1.4 Nice Error Bases

We introduced the notion of detectable errors in the previous section. The detectability condition (1.4) is linear in the error operators. This suggest the following approach: choose a basis of the linear operators that is particularly convenient for the construction of quantum error control codes. We will be able to characterize the operators in this basis that can be detected by the constructed code. Hence, the code will be able to detect all linear combinations of these error operators. The main benefit is that we have only a discrete number of conditions to check, and the code constructions resemble (and sometimes mimick) constructions of classical codes.

Let us motivate the definition of a nice error basis by way of a familiar example. Consider the set of Pauli matrices σ_x, σ_y, σ_z together with the identity matrix $\mathbf{1}_2$:

$$\mathbf{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \ \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (1.8)$$

This set forms an orthonormal basis of the vector space of complex 2×2 matrices $\mathrm{Mat}_2(\mathbf{C})$ with respect to the normalized trace inner product $\langle A|B\rangle = \mathrm{tr}(A^\dagger B)/2$. Thus, we can express a 2×2 matrix A conveniently in the form

$$A = \frac{1}{2}\left(\mathrm{tr}(A)\mathbf{1} + \mathrm{tr}(\sigma_x^\dagger A)\sigma_x + \mathrm{tr}(\sigma_y^\dagger A)\sigma_y + \mathrm{tr}(\sigma_z^\dagger A)\sigma_z\right).$$

Moreover, the multiplication of the matrices (1.8) resembles the composition operation in the Kleinian group of four elements $V_4 = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ if we ignore phase factors. Indeed, if we assign the Pauli matrices to the elements of V_4 in the following way

$$\hat{p}(0,0) = \mathbf{1}_2, \quad \hat{p}(1,0) = \sigma_x, \quad \hat{p}(0,1) = \sigma_z, \quad \hat{p}(1,1) = \sigma_y,$$

then the product of the representing matrices $\hat{p}$ of the elements (a, b) and (c, d) yields – up to a scalar factor – the representing matrix of $(a, b) +$

(c, d). In other words, the matrices (1.8) form a projective representation $\hat{p}$ of the group V_4.

This example motivates the following definition:

DEFINITION 1.1 *Let G be a finite group of square order d^2. The identity of this group is denoted by 1. A* nice error basis *on $\mathbf{C}^d$ is a set $\mathcal{E} = \{\hat{p}(g) \,|\, g \in G\}$ of unitary matrices such that*

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

(ii) $\operatorname{tr} \hat{\rho}(g) = 0$ for all elements $g \in G$ with $g \neq 1$,

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

where $\omega(g, h)$ is a nonzero complex number depending on $g, h \in G$. We call G the index group *of the nice error basis $\mathcal{E}$.*

The condition (i) and (iii) simply state that $\hat{\rho}$ is a projective representation with factor system ω. The conditions (i) – (iii) imply that $\mathcal{E}$ is an orthonormal basis of the vector space of linear operators acting on $\mathbf{C}^d$ with respect to the normalized trace inner product $\langle A|B\rangle = \operatorname{tr}(A^\dagger B)/d$.

Notice that a nice error basis for $\mathcal{H} = \mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2} \otimes \cdots \otimes \mathbf{C}^{d_n}$ can be obtained by choosing nice error bases for each component and taking tensor products. The corresponding index group is then given by the direct product of the index groups of the components.

We give some more examples of nice error bases before proceeding with the construction of quantum error control codes. The first example is given by the error operators that we have seen in Section 1.2 in the discussion of Shor's code.

Example 1.1
Denote by ω the primitive dth root of unity $\omega = \exp(2\pi i/d)$. Let $X_\ell \,|k\rangle = |k + \ell \bmod d\rangle$ and $Z_\ell \,|k\rangle = \omega^{\ell k} \,|k\rangle$. Then

$$\mathcal{E} = \{\, X_k Z_\ell \,|\, (k, \ell) \in G\}$$

is a nice error basis on $\mathbf{C}^d$ with index group $G = \mathbf{Z}/d\,\mathbf{Z} \times \mathbf{Z}/d\,\mathbf{Z}$. In particular, we obtain in the four-dimensional case $d = 4$ the error matrices

$$X_1 = \begin{pmatrix} . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \\ . & . & 1 & . \end{pmatrix}, \quad Z_1 = \begin{pmatrix} 1 & . & . & . \\ . & \omega & . & . \\ . & . & \omega^2 & . \\ . & . & . & \omega^3 \end{pmatrix},$$

which generate the nice error basis (i.e., one can obtain all other basis elements by forming the products $X_1^k Z_1^\ell$). □

In dimension 4, there also exist error bases with *non-abelian* index groups. This is the smallest dimension where this can happen, since all groups of order p^2, with p prime, are abelian. Therefore, there do not exist any non-abelian index groups in dimensions 2 or 3. We will see in the following sections that these non-abelian index groups will allow us to unravel some interesting properties of quantum error control codes.

Example 1.2
In this example, we consider a finite group G generated by three elements a, b, c subject to the relations

$$a^2 = b^2 = [a, b] = 1 \qquad \text{and} \qquad a^c = b, \quad b^c = a, \quad c^4 = 1,$$

where $[a, b] = a^{-1}b^{-1}ab$ denotes the group-theoretical commutator. This is a group of order 16. It is the extension of a cyclic group $\langle c\rangle$ of order 4 by the direct product $\langle a\rangle \times \langle b\rangle$ of two cyclic groups of order 2. The representing matrices of the generators of G are given by

$$\hat\rho(a) = \begin{pmatrix} . & . & -1 & . \\ . & . & . & -1 \\ -1 & . & . & . \\ . & -1 & . & . \end{pmatrix} \hat\rho(b) = \begin{pmatrix} . & . & . & -i \\ . & . & i & . \\ . & -i & . & . \\ i & . & . & . \end{pmatrix} \hat\rho(c) = \begin{pmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & -i & . \\ . & . & . & i \end{pmatrix},$$

where . is an abbreviation for 0. These representing matrices generate a nice error basis in 4 dimensions. The group G has the property that it is non-abelian, but all proper subgroups of G are abelian. □

Example 1.3
Let G be the finite group generated by a, b, c subject to the relations

$$a^4 = b^2 = (ab)^2 = 1 \qquad \text{and} \qquad c^2 = [a, c] = [b, c] = 1.$$

It is the direct product of the dihedral group $D_8 \cong \langle a, b\rangle$ of order 8 and the cyclic group $C_2 \cong \langle c\rangle$. The group G is the index group of a nice error basis in 4 dimensions, which is generated by

$$\hat\rho(a) = \begin{pmatrix} \omega & . & . & . \\ . & \omega^7 & . & . \\ . & . & \omega^5 & . \\ . & . & . & \omega^3 \end{pmatrix} \hat\rho(b) = \begin{pmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{pmatrix} \hat\rho(c) = \begin{pmatrix} . & . & 1 & . \\ . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \end{pmatrix}$$

where . and ω are abbreviations for 0 and $\exp(2\pi i/8)$ respectively. □

REMARKS

(a) Rather surprisingly, the definition of a nice error basis severly restricts the possible index groups. It is shown in [15] that an index group of a nice error basis has to be a solvable group. A complete classification of all nice error bases up to dimensions 11 is also derived in that paper.

(b) A nice error basis can also be defined as a faithful irreducible unitary projective representation of degree n of a finite group of order n^2.

1.5 Stabilizer Codes

The most well-known construction of quantum error control codes is given by the so-called stabilizer construction. Stabilizer codes have been introduced by Gottesman [10] and Calderbank, Rains, Shor, and Sloane [5] for two-level quantum systems. This approach is particularly appealing, since the construction of the quantum codes can be reduced to the construction of classical error control codes over the finite field with four elements [6]. We will discuss a more general setting that allows to combine quantum systems with a different numbers of levels.

We have introduced the concept of a nice error basis in the last section. Notice that the matrices of a nice error basis do *not* form a group, since they are not closed under multiplication. For instance, the set of matrices (1.8) does not contain the product $\sigma_x\sigma_y$. However, we can obtain a matrix group in a canonical way from a nice error basis by taking the closure under multiplication and inverse operations. We call this group the *error group* associated with a nice error basis.

Unfortunately, the error group of a nice error basis can be infinite, a situation we would like to avoid. We say that two nice error bases $\mathcal{E}_1$, $\mathcal{E}_2$ are equivalent if and only if we can find a unitary matrix U such that

$$\mathcal{E}_1 = \{\hat{\rho}(g) \,|\, g \in G\} \quad \text{and} \quad \mathcal{E}_2 = \{U\hat{\rho}(g)U^\dagger \,|\, g \in G\}.$$

It turns out that for each nice error basis there exists an equivalent error basis with finite error group [15]. We call a finite group that is isomorphic to a finite error group an *abstract error group*. Abstract error groups allow us to work with ordinary representations instead of projective representations, which is very convenient. In fact, an abstract error group is a so-called ω-covering group of the index group, hence there corresponds to each projective representation of the index group an ordinary representation of the abstract error group.

Let E be an abstract error group. This group has an irreducible faithful unitary resentation ρ of degree $\sqrt{[E : Z(E)]}$. Denote by N a normal subgroup of E. A *stabilizer code* is defined as a joint eigenspace Q of the representing matrices $\{\rho(n) \,|\, n \in N\}$ of this normal subgroup. In other words, there exist eigenvalues $\chi(n)$ such that

$$\rho(n)v = \chi(n)v \tag{1.9}$$

for all $v \in Q$, and all $n \in N$. For non-trival codes Q, the normal subgroup N must be abelian – a condition which we will assume in the following.

Note that the eigenvalues $\chi(n)$ in (1.9) constitute a character of the group N. Indeed, we have $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in N$, since

$$\chi(nm)v = \rho(nm)v = \rho(n)\rho(m)v = \chi(n)\chi(m)v$$

holds for any nonzero vector $v \in Q$.

We can give another characterization of a stabilizer code in terms of an orthogonal projector. The projector P onto the code space Q can be made explicit in the following way:

$$P = \frac{1}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n). \tag{1.10}$$

The relation $P^2 = P$ is basically a consequence of the orthogonality relations of characters, and we can immediately see that $P^\dagger = P$. Thus P is an orthogonal projection operation. We claim that the image of P is the stabilizer code Q. Indeed, if v is an element of Q, then $Pv = v$, because the character is defined by the eigenvalues of the representing matrices; hence $Q \subseteq \mathrm{im}(P)$. On the other hand, if $v \in \mathrm{im}(P)$, then we obtain

$$\rho(m)Pv = \frac{1}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(mn)v = \chi(m)\frac{1}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n)v$$

by the multiplicativity of the character χ. Thus, Q is the image of the orthogonal projector P.

Equation (1.10) is the starting point for a more general construction of quantum error control codes, which will be described in the next section.

1.6 Clifford Codes

The projection formula (1.10) suggests an immediate extension: replace the abelian normal subgroup by an arbitrary normal subgroup N. The joint eigenspace of the representing matrices is trivial in the case of non-abelian normal subgroups, but the projection formulae can still have a non-trivial images. We call the resulting class of codes 'Clifford codes', since the construction relies on tools of representation theory developed by Clifford [9].

DEFINITION 1.2 *Let E be an abstract error group with a faithful irreducible unitary representation ρ of degree $\sqrt{[E : Z(E)]}$. Denote by ϕ the character of E corresponding to this representation, that is, $\phi(g) = \operatorname{tr}\rho(g)$ for all $g \in E$. Let N be a normal subgroup of the abstract error group E. Denote by χ an irreducible character of N that is a constituent of the restriction of the character ϕ to N. Then the* Clifford code *with data (E, ρ, N, χ) is defined as the image of the orthogonal projector*

$$P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n). \tag{1.11}$$

Clifford codes have been introduced by Knill in [16]. Some remarks concerning this definition are in order. Denote by ϕ_N the restriction of the character ϕ to the normal subgroup N. In general, this restricted character is not irreducible. The character χ is one of the irreducible constituents of ϕ_N. The latter condition ensures that the projector P has a nonzero image.

We want to characterize the error correcting properties of a Clifford code. It turns out that the detectable errors can be determined from the characters alone. In order to give a concise characterization, we need two definitions. The *inertia subgroup* $T(\chi)$ of the character χ is defined

by

$$T(\chi) = \{g \in E \,|\, \chi(gxg^{-1}) = \chi(x) \text{ for all } x \in N\}.$$

The *quasikernel* of a character ϑ of a group T is by definition given by

$$Z(\vartheta) = \{n \in T \,|\, |\vartheta(n)| = \vartheta(1)\}.$$

The significance of these definitions can be seen as follows. Errors corresponding to elements of the abstract error group E, which are not contained in the inertia subgroup $T(\chi)$, map the code Q to an orthogonal complement. Hence, these errors can be detected by a suitable measurement. On the other hand, we are also interested in errors that act trivially by scalar multiplication on the code Q, hence do not affect the encoded information. We note that the image of P is not only a vector space but also an irreducible $T(\chi)$-module. Denote by ϑ the irreducible character of the group $T(\chi)$ afforded by this module. Then the quasikernel $Z(\vartheta)$ of this character contains all elements m of the abstract error group E such that the matrix $\rho(m)$ acts by scalar multiplication on Q.

We summarize the error correcting properties of Clifford codes in the following theorem:

THEOREM 1.1
Let Q be a Clifford code with the data (E, ρ, N, χ). Denote by ϑ the irreducible character of $T(\chi)$ described above. The code Q is able to correct a set of errors $S \subseteq E$ if and only if the condition $s_1^{-1}s_2 \notin T(\chi) \setminus Z(\vartheta)$ holds for all $s_1, s_2 \in S$.

A detailed proof of this result can be found in [14].

1.7 Clifford Codes that are Stabilizer Codes

We have seen in the previous section that a Clifford code Q is given by the image of a projection operator

$$Q = \text{im}\left(\frac{\chi(1)}{|N|}\sum_{n\in N}\chi(n^{-1})\rho(n)\right).$$

In the case of an abelian normal subgroup N, we obtain a stabilizer code. It is a little bit more surprising that a non-abelian normal subgroup N might still lead to a stabilizer code. We show in the next theorem that many abstract error groups cannot produce *any* non-stabilizer code:

THEOREM 1.2
Let E be an abstract error group. If the index group $G = E/Z(E)$ is an abelian group or a Redei group (i.e., a non-abelian group where all proper subgroups are abelian), then all Clifford codes in E are stabilizer codes.

The remainder of this section is devoted to the proof of this theorem. We say that a normal subgroup N of an abstract error group is *large* if and only if

$$N/(Z(E) \cap N) \cong E/Z(E) \tag{1.12}$$

holds, that is, if we factor out the central elements $Z(E) \cap N$, then we still get a group isomorphic to the full index group $E/Z(E)$.

PROPOSITION 1.1
Let (E, ρ, N, χ) be the data of a Clifford code Q with ambient space $\mathcal{H}$. If the normal subgroup N is large, then Q coincides with its ambient space $\mathcal{H}$ and the projection operation

$$P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n)$$

is the identity map. In particular, the Clifford code Q is a stabilizer code.

PROOF We want to exploit the largeness property of N to show that the projector P is the identity map. We do this in two steps. Our first step is to show that the normal subgroup N and the center $Z(E)$ of E generate the error group E. First, we observe that

$$N/(Z(E) \cap N) \cong NZ(E)/Z(E)$$

holds by the second isomorphism theorm, cf. [20, p. 56, Theorem 3.40]. Now $NZ(E)$ is a subgroup of E, and

$$|NZ(E)| = \frac{|N| \cdot |Z(E)|}{|N \cap Z(E)|} \overset{\text{by } (1.12)}{=} \frac{|E|}{|Z(E)|}|Z(E)| = |E|$$

holds, therefore $E = NZ(E)$.

In the second step we show that $\rho(g)P\rho(g^{-1}) = P$ holds for all $g \in E$; this implies – by Schur's lemma [13, Lemma 1.5] – that P is a scalar multiple of the identity. Our previous discussion shows that we can write an arbitrary group element $g \in E$ in the form $g = nz$ with $n \in N$ and $z \in Z(E)$. Thus we obtain

$$\begin{aligned}\rho(nz)P\rho((nz)^{-1}) &= \frac{\chi(1)}{|N|}\sum_{m\in N}\chi(m^{-1})\rho(nzmz^{-1}n^{-1}) \\ &= \frac{\chi(1)}{|N|}\sum_{m\in N}\chi(m^{-1})\rho(nmn^{-1}) \\ &= \frac{\chi(1)}{|N|}\sum_{m\in N}\chi((n^{-1}mn)^{-1})\rho(m) = P\end{aligned}$$

The last equality follows from the fact that the character χ is a class function, hence $\chi((n^{-1}mn)^{-1}) = \chi(m^{-1})$. Therefore, $P = \alpha\mathbf{1}$ for some scalar α. Since we have $P^2 = P$, we either have $\alpha = 0$ or $\alpha = 1$. However, χ is by definition a constituent of the restricted character $\operatorname{tr}\rho_N$, and thus the projector P is a nonzero map, which proves the claim $P = \mathbf{1}$. ∎

PROPOSITION 1.2

Let E be an abstract error group and $\phi \in \mathrm{Irr}(E)$ a faithful character of degree $\phi(1)^2 = [E\colon Z(E)]$. Denote by N a normal subgroup of E and let $\chi \in \mathrm{Irr}(\phi|N)$ be an irreducible constituent of the restricted character ϕ_N. Note that the restriction of χ to the center $Z(N)$ is a multiple of a linear character $\chi_{Z(N)} = \chi(1)\varphi$ with $\varphi \in \mathrm{Irr}(Z(N))$. If $N/(Z(E)\cap N)$ is abelian, then

$$\frac{\chi(1)}{|N|}\sum_{n\in N}\chi(n^{-1})\rho(n) = \frac{1}{|Z(N)|}\sum_{n\in Z(N)}\varphi(n^{-1})\rho(n).$$

Thus, in particular, the Clifford code (N,χ) coincides with the stabilizer code $(Z(N),\varphi)$.

PROOF Denote by $Z = Z(E)\cap N$ the intersection of N with the center of E. We recall that the support of ϕ is the center $Z(E)$ and that by definition $(\phi_N,\chi) \neq 0$. These two facts imply that χ coincides – up to a nonzero constant factor – with ϕ on Z, hence χ_Z is a faithful character. Thus we can invoke the following lemma:

LEMMA 1.3
Let $\chi \in \mathrm{Irr}(N)$, $Z = N \cap Z(E)$, N/Z *abelian, and* χ_Z *a faithful character. Then* $\mathrm{supp}(\chi) = Z(N)$.

PROOF We can assume without loss of generality that the group N is non-abelian. Let $x \in N - Z(N)$, then there exists an element $h \in N$ such that $xh \neq hx$. We have $[x,h] = z$ for some $z \in Z$ with $z \neq 1$, since N/Z is abelian. Keeping in mind that $[x,h] = z$ is equivalent to $xz = h^{-1}xh$, we get $\chi(x) = \chi(h^{-1}xh) = \chi(xz) = \omega\chi(x)$, with $\omega \neq 1$, since χ is faithful on the center Z; hence, $\chi(x) = 0$. It follows that $\mathrm{supp}(\chi) = Z(N)$, as claimed. ∎

It is known that the minimal support condition $\mathrm{supp}(\chi) = Z(N)$ is equivalent to the extremal degree condition $\chi(1)^2 = [N : Z(N)]$, cf. Isaacs [13], Corollary 2.30. Moreover, $\chi_{Z(N)}(n) = \chi(1)\varphi(n)$ for a linear character of $Z(N)$. Therefore,

$$\begin{aligned}\frac{\chi(1)}{|N|}\sum_{n\in N}\chi(n^{-1})\rho(n) &= \frac{\chi(1)^2}{|N|}\sum_{n\in Z(N)}\varphi(n^{-1})\rho(n)\\ &= \frac{1}{|Z(N)|}\sum_{n\in Z(N)}\varphi(n^{-1})\rho(n)\end{aligned}$$

which concludes the proof of Proposition 1.2. ∎

PROOF (of Theorem 1.2) We have shown that a normal subgroup N of an error group E can produce only stabilizer codes in case $N/(Z(E) \cap N)$ is large or is abelian. Thus, an index group which is a Redei group or an abelian group cannot produce any Clifford code that is not a stabilizer code. ∎

REMARKS

(a) The proof of Proposition 1.1 showed that the character χ of a large normal subgroup is extendible to a character of E. We can derive similar results whenever the character χ extends to E. This leads to an even larger class of error groups admitting only stabilizer codes.

(b) A different proof of the statement of Theorem 1.2 for the case of error groups with abelian index groups has been given in [14]. It

is an interesting open problem to characterize all abstract error groups that admit only stabilizer codes.

1.8 A Remarkable Error Group

Let G be the finite group generated by three elements a, b, c subject to the relations

$$a^2 = b^2 = [a, b] = 1 \qquad \text{and} \qquad a^c = b, \quad b^c = a, \quad c^4 = 1.$$

This is the index group that we have introduced in Example 1.2.

An abstract error group E is obtained by a central extension of the index group G by a cyclic group of order 2. More explicitly, E is presented by four generators a, b, c, d that are subject to the relations

$$a^2 = b^2 = [a, b] = 1, \qquad d^2 = [a, d] = [b, d] = [c, d] = 1$$

and $c^4 = 1$, $a^c = b$, $b^c = ad$.

The group E is nilpotent of class 3 and of order 32. A faithful irreducible representation of E is given by

$$\rho(a) = \begin{pmatrix} . & . & -1 & . \\ . & . & . & -1 \\ -1 & . & . & . \\ . & -1 & . & . \end{pmatrix} \rho(b) = \begin{pmatrix} . & . & . & -i \\ . & . & i & . \\ . & -i & . & . \\ i & . & . & . \end{pmatrix} \rho(c) = \begin{pmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & -i & . \\ . & . & . & i \end{pmatrix}$$

and the generator d of the center of E is represented by $\rho(d) = -\mathbf{1}$.

What is so remarkable about this error group? It has a nonabelian index group and yet all its Clifford codes are stabilizer codes. This follows from the fact that all nontrivial normal subgroups of G are abelian.

1.9 A Weird Error Group

Let G be the finite group generated by a, b, c subject to the relations

$$a^4 = b^2 = (ab)^2 = 1 \qquad \text{and} \qquad c^2 = [a, c] = [b, c] = 1.$$

This is the index group that we have introduced in Example 1.3.

Let E be the group generated by a, b, c, d subject to the relations

$$a^4 d = b^2 = (ab)^2 = 1, \qquad c^2 = [a, c]d = [b, c] = 1,$$

and

$$d^2 = [a, d] = [b, d] = [c, d] = 1.$$

This is a group of order 32. The construction ensured that the center of E is generated by d and that the factor group $E/Z(E)$ is isomorphic to G. A faithful irreducible representation ρ of the group E is given by

$$\rho(a) = \begin{pmatrix} \omega & . & . & . \\ . & \omega^7 & . & . \\ . & . & \omega^5 & . \\ . & . & . & \omega^3 \end{pmatrix} \rho(b) = \begin{pmatrix} . & 1 & . & . \\ 1 & . & . & . \\ . & . & . & 1 \\ . & . & 1 & . \end{pmatrix} \rho(c) = \begin{pmatrix} . & . & 1 & . \\ . & . & . & 1 \\ 1 & . & . & . \\ . & 1 & . & . \end{pmatrix}$$

where . and ω are abbreviations for 0 and $\exp(2\pi i/8)$ respectively. Notice that $\rho(d) = -\mathbf{1}$ is a consequence of the relation $a^4 = d$.

Denote by N the normal subgroup in E generated by ab and ac, a dihedral group of order 16. Let χ be an irreducible character of N of degree 2 with $\chi(d) = -2$. There exist two such characters and both are constituents of the restriction of the character $\phi(x) = \operatorname{tr} \rho(x)$ to the normal subgroup N. One choice yields the orthogonal projection matrix

$$P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1}) \rho(n) = \frac{1}{2} \begin{pmatrix} 1 & . & i & . \\ . & 1 & . & -i \\ -i & . & 1 & . \\ . & i & . & 1 \end{pmatrix}.$$

The image of this projector yields a 2-dimensional Clifford code $Q = \operatorname{im}(P)$. The stabilizer of this code Q is by definition the set

$$S = \{g \in E \mid \exists s_g \in \mathbf{C} \text{ such that } \rho(g)v = s_g v \text{ for all } v \in \operatorname{im}(P)\}.$$

It is not difficult to check that S is given by the center $\langle d \rangle$ of E. The joint eigenspace (containing Q) of S is the full four-dimensional space $\mathbf{C}^4$, which shows that Q is not a stabilizer code. In fact, the code Q is the smallest example of a Clifford code that is not a stabilizer code.

1.10 Conclusions

Clifford codes are highly structured and have many interesting properties. We have demonstrated here for the first time that the concept

of Clifford codes goes truly beyond the stabilizer code concept. We discussed the concept of nice error bases and abstract error groups, following the seminal work of Knill. This allowed us to obtain a more flexible definition of stabilizer codes. We have shed some light on the relation between Clifford codes and the class of stabilizer codes, the hitherto most popular code construction. There are many interesting open problems concerning the constructive aspects of the theory developed in this chapter.

Acknowledgments. This chapter has been completed during the European workshop on Quantum Computer Theory, Villa Gualino, Torino, June 2001. We thank Mario Rasetti and Paolo Zanardi of the Institute for Scientific Interchange Foundation for their kind hospitality. A.K. thanks the Santa Fe Institute for support through their Fellow-at-Large program. M.R. has been supported by the European Community under contract IST-1999-10596 (Q-ACTA).

References

[1] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error. In *Proc. of the 29th Annual ACM Symposium on Theory of Computation (STOC)*, pages 176–188, New York, 1997. ACM.

[2] A.E. Ashikhmin, A.M. Barg, E. Knill, and S.N. Litsyn. Quantum error detection I: Statement of the problem. *IEEE Trans. on Information Theory*, 46(3):778–788, 2000.

[3] A.E. Ashikhmin, A.M. Barg, E. Knill, and S.N. Litsyn. Quantum error detection II: Bounds. *IEEE Trans. on Information Theory*, 46(3):789–800, 2000.

[4] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters. Mixed state entanglement and quantum error correction. *Physical Review A*, 54:3824–3851, 1996.

[5] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.*, 76:405–409, 1997.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory*, 44:1369–1387, 1998.

[7] A.R. Calderbank and P. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996.

[8] R. Cleve and D. Gottesman. Efficient computations of encodings for quantum error correction. *Phys. Rev. A*, 56(1):76–82, 1997.

[9] A.H. Clifford. Representations induced in an invariant subgroup. *Ann. Math.*, 38(2):533–550, 1937.

[10] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.

[11] M. Grassl. Algorithmic aspects of error-correcting codes. In R. Brylinski and G. Chen, editors, *The Mathematics of Quantum Computing*, pages –. CRC Press, 2001.

[12] M. Grassl and Th. Beth. Cyclic quantum error-correcting codes and quantum shift registers. *Proc. Royal Soc. London Series A*, 456(2003):2689–2706, 2000.

[13] I.M. Isaacs. *Character Theory of Finite Groups*. Academic Press, New York, 1976.

[14] A. Klappenecker and M. Rötteler. Beyond stabilizer codes. Eprint quant/ph/0010076, 2000.

[15] A. Klappenecker and M. Rötteler. A remark on unitary error bases. Eprint quant-ph/0010082, 2000.

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

[17] E. Knill and R. Laflamme. A theory of quantum error–correcting codes. *Physical Review A*, 55(2):900–911, 1997.

[18] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *Phys. Rev. Lett.*, 84(11):2525–2528, 2000.

[19] E.M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, 45:1827–1832, 1999.

[20] J.S. Rose. *A Course on Group Theory*. Dover, New York, 1994.

[21] P. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, 2:2493–2496, 1995.

[22] P. Shor. Fault-tolerant quantum computation. In *Proceedings of the 37th Symposium on the Foundations of Computer Science*, Los Alamitos, 1996. IEEE Computer Society Press.

[23] A.M. Steane. Multiple-particle interference and quantum error correction. *Proc. Roy. Soc. London A*, 452:2551–2577, 1996.

[24] A.M. Steane. Simple quantum error correcting codes. *Phys. Rev. Lett.*, 77:793–797, 1996.

[25] P. Zanardi. Stabilizing quantum information. *Phys. Rev. A*, 63(1):012301, 2001.