Beyond Stabilizer Codes II: Clifford Codes

Andreas Klappenecker, Martin Rötteler

Abstract

Knill introduced a generalization of stabilizer codes, in this note called Clifford codes. It remained unclear whether or not Clifford codes can be superior to stabilizer codes. We show that Clifford codes *are* stabilizer codes provided that the abstract error group has an abelian index group. In particular, if the errors are modelled by tensor products of Pauli matrices, then the associated Clifford codes are necessarily stabilizer codes.

Keywords

Quantum error correcting codes, stabilizer codes, Clifford codes, abstract error groups, index groups.

I. Introduction

Quantum error control codes allow to protect the computational states of a quantum computer against decoherence errors. Almost all quantum codes known today have been constructed as stabilizer codes, cf. [1], [2], [3], [4]. Allowing the protection of quantum systems of arbitrary finite dimension, we are led to modify the notion of a stabilizer code in the following way:

Let $\varrho\colon E \to \mathcal{U}(n)$ be a faithful unitary irreducible ordinary representation of an abstract error group E [5]. A *stabilizer code* is defined to be the joint eigenspace Q of the representing matrices $\varrho(n)$ for all $n \in N$, where N is a normal subgroup of E. If Q is nontrivial, then N is necessarily an *abelian* normal subgroup of E.

We recover the definition of binary stabilizer codes as used in [2], [3] by taking E to be the generalized extraspecial 2-group which is generated by k-fold tensor products of Pauli matrices. The stabilizer codes derived within this error model have been studied in great detail, see [2], [3].

The definition of stabilizer codes forces the normal subgroup to be abelian. A more general class of quantum error correcting codes – in this note called Clifford codes – has been introduced by Knill in [6]. Clifford codes are derived with the help of normal subgroups which are not necessarily abelian.

A.K. thanks the Santa Fe Institute for support through their Fellow-at-Large program, and the European Community for support through the grant IST-1999-10596 (Q-ACTA). M.R. thanks the DFG for support through the Graduiertenkolleg GRK-209/3-98. Part of this work has been done at the Tacheles, Berlin, during a concert of Remember the Day.

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 Institut für Algorithmen und Kognitive Systeme, Forschungsgruppe Quantum Computing (Professor Thomas Beth), Universität Karlsruhe, Am Fasanengarten 5, D-76 128 Karlsruhe, Germany (e-mail: roettele@cs.tamu.edu).

It remained unclear, whether or not it is possible to construct Clifford codes that are better than stabilizer codes. We found surprisingly good Clifford codes by computer search. However, we were never able to beat the stabilizer codes. The main result of this note partly explains this phenomenon: we find that each Clifford code is actually a stabilizer code given that the error group has an abelian index group. Therefore, the error models discussed in [1], [2], [3] cannot lead to Clifford codes which are not stabilizer codes.

II. Clifford Codes

We will construct a quantum code Q from a normal subgroup N of an abstract error group E. The main properties of such a code Q are determined by applying results from Clifford theory, hence the name Clifford code. The relevant results from Clifford theory can be found in Huppert [7, Chapter 5] or any other standard text on representation theory of finite groups.

Let E be an abstract error group. Recall that the group E has a faithful irreducible ordinary representation $\varrho\colon E \to \mathcal{U}(n)$ of large degree $\deg \varrho = (E : Z(E))^{1/2}$. The errors are expressed as linear combinations of the unitary $n \times n$ matrices $\varrho(g)$ representing elements g of the abstract error group E.

The action of the representation ϱ on $\mathbf{C}^n$ induces an irreducible $\mathbf{C}E$-module structure on the ambient space $\mathbf{C}^n$. Let N be a normal subgroup of E, denoted by $N \trianglelefteq E$. If we view the ambient space $\mathbf{C}^n$ as a $\mathbf{C}N$-module, then we obtain a decomposition into irreducible $\mathbf{C}N$-modules gW of the form

$$\mathbf{C}^n \cong \bigoplus_{i=1}^{m} \left\{ \bigoplus_{g \in R} gW \right\},$$

where R is a transversal of the inertia group $T(W)$ in E, and m is the multiplicity of the module gW in this decomposition. Recall that the inertia group is defined by

$$T(W) = \{ g \in E \,|\, gW \cong W \}.$$

We define a quantum code Q to be a homogeneous component

$$Q \cong \underbrace{W \oplus \cdots \oplus W}_{m\text{-times}}$$

of this decomposition. Thus, Q is a subspace of $\mathbf{C}^n$ which is also endowed with the structure of a $\mathbf{C}N$-module. We call any quantum code Q that can be obtained by such a construction a *Clifford code*.

We need to introduce some more notation before we can discuss the error correcting properties of a Clifford code Q. We define $Z(W)$ to be the set of elements that act on Q by scalar multiplication

$$Z(W) = \{g \in T(W) \,|\, \exists \lambda \in \mathbf{C}\, \forall v \in Q : gv = \lambda v\}.$$

The error correcting properties of the code Q are summarized by the following theorem. Although this theorem is essentially contained in [6], we include it here to make this note self-contained:

Theorem 1: We keep the notation introduced above. Let χ be the character of N afforded by W. Then

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

is an orthogonal projector onto Q. The code Q is able to correct a set of errors $\Sigma \subset E$ precisely when the condition $e_1^{-1} e_2 \notin T(W) - Z(W)$ holds for all $e_1, e_2 \in \Sigma$. The dimension of Q is $m\chi(1)$.

Proof: We divide the proof into several steps.

Step 1. The matrix group $\varrho(N)$ is isomorphic to the abstract group N, since ϱ is a faithful representation. Since χ is an irreducible character of N, it follows that e_χ is an idempotent in the group algebra $\mathbf{C}[\varrho(N)] \cong \mathbf{C}N$, cf. [8, p. 209]. The idempotent e_χ is hermitian, since ϱ is unitary, hence an orthogonal projection operator. That e_χ projects onto Q is a well-known fact, cf. Theorem 8 in [9, p. 21]. The dimension of the module W is $\chi(1)$, whence $\dim_{\mathbf{C}}(Q) = m\chi(1)$.

Step 2. Let $g, h \in E$. The characters of gW and hW are $\psi(x) = \chi(gxg^{-1})$ and $\varphi(x) = \chi(hxh^{-1})$ respectively, cf. Chap. V, §17, Theorem 17.3 c) in [7]. Suppose that g and h are not in the same coset of $T(W)$ in E. Then ψ and φ are different irreducible characters. Thus the idempotents e_ψ and e_φ satisfy $e_\chi e_\psi = 0 = e_\psi e_\chi$, hence project on orthogonal subspaces. We have $\mathrm{im}(e_\psi) = gQ$, $\mathrm{im}(e_\varphi) = hQ$, and thus, in particular, $gQ \perp hQ$.

Step 3. It remains to show the error correcting properties of Q. Recall that an error w can be detected if and only if $e_\chi \varrho(w) e_\chi$ is a scalar multiple of e_χ, cf. [6]. The code Q is Σ-correcting if and only if Q is able to detect all errors in $\{e_1^{-1} e_2 \,|\, e_1, e_2 \in \Sigma\}$, cf. [10], [11]. Hence it remains to show that an error w can be detected if and only if $w \notin T(W) - Z(W)$.

(a) An error $w \in Z(W)$ can be detected, since, by definition, there exists a scalar $\lambda \in \mathbf{C}$ such that $e_\chi \varrho(w) e_\chi = \lambda e_\chi$.

(b) An error $w \in E - T(W)$ can be detected, since Step 2 shows that $e_\chi \varrho(w) e_\chi = 0$ holds.

(c) An error $w \in T(W) - Z(W)$ cannot be detected. Indeed, $\varrho(w)$ maps Q into itself, since $w \in T(W)$. However, $e_\chi \varrho(w) e_\chi$ cannot be a multiple of e_χ, since this would imply that w is an element of $Z(W)$. This proves the claim. $\square$

The error correcting properties of a Clifford code Q are fully determined by the inertia group $T(W)$ and the group $Z(W)$. It is often more convenient to use characters rather than modules to compute these groups. The inertia group $T(W)$ coincides with the inertia group $T(\chi)$ of the character χ in G:

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

The group $Z(W)$ can also be determined by a character. Clifford theory shows that Q is an irreducible $\mathbf{C}T$-module, where $T = T(W)$. Denote by ϑ the irreducible character of T afforded by Q. Then $Z(W)$ is determined by the values of the character ϑ:

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

III. Characters

We have seen that the inertia group of χ determines the error correcting properties of the quantum code Q. We show in this section how the inertia groups can be calculated for abstract error groups with abelian index groups.

Let us first recall a few standard notations from group theory. If E is a finite group, then E' denotes the commutator subgroup,

$$E' = \langle [g,h] = g^{-1}h^{-1}gh \,|\, g, h \in E \rangle.$$

The center $Z(E)$ of E is given by the group

$$Z(E) = \{z \in E \,|\, zg = gz \text{ for all } g \in E\}.$$

An abstract error group E has an abelian index group $G \cong E/Z(E)$ if and only if its commutator subgroup E' is contained in $Z(E)$. For that reason, it is of interest to study the inertia groups in such groups E. We will see that the inertia group of a character χ of N defining a Clifford code is simply given by the centralizer of $Z(N)$ in E.

Let G be a finite group. We denote by $\mathrm{Irr}(G)$ the set of irreducible characters of G. We say that a character $\chi \in \mathrm{Irr}(G)$ is faithful on $H \subseteq G$ if and only if the intersection of H with the kernel of χ is trivial

$$H \cap \ker(\chi) = H \cap \{g \in G \,|\, \chi(1) = \chi(g)\} = \{1\}.$$

We need to establish a few simple properties of characters. We will see that a character defining a Clifford code will satisfy the assumption of the following lemma, which gives some information about character values.

Lemma 2: Let E be a finite group, $N \trianglelefteq E$. Let χ be an irreducible character of N that is faithful on $Z = Z(E) \cap N$. If $z \in Z$, $z \neq 1$, and $n \in N$, then $\chi(zn) = \omega\chi(n)$ for some $\omega \neq 1$.

Proof: Denote by ϱ a representation affording χ. Since ϱ is irreducible, $\varrho(z)$ is a scalar multiple of the identity matrix I for all $z \in Z$ by Schur's lemma. If $z \neq 1$, then $\varrho(z) = \omega I$ with $\omega \neq 1$, since χ is faithful on Z. Hence $\chi(zn) = \operatorname{tr}(\varrho(zn)) = \operatorname{tr}(\omega\varrho(n)) = \omega \operatorname{tr} \varrho(n) = \omega\chi(n)$ as claimed. □

In the next step we want to show that the character χ defining a Clifford code is indeed faithful on the central elements of E contained in N. We exploit the fact that χ is a constituent of a faithful character $\phi \in \operatorname{Irr}(E)$ of the abstract error group satisfying $\phi(1)^2 = (E : Z(E))$. Recall that a scalar product of two characters $\chi, \vartheta \in \operatorname{Irr}(N)$ is defined by

$$\langle \chi, \vartheta \rangle = \frac{1}{|N|} \sum_{n \in N} \chi(n)\vartheta(n^{-1}).$$

This allows to define the set of irreducible components of the restriction of $\phi \in \operatorname{Irr}(E)$ to N by

$$\operatorname{Irr}(\phi \,|\, N) = \{\chi \in \operatorname{Irr}(N) \,|\, \langle \chi, \phi{\downarrow}N \rangle \neq 0\},$$

where $\phi{\downarrow}N$ denotes the restriction of ϕ to N. Using this notation, we can now formulate

Lemma 3: Let E be a finite group, $N \trianglelefteq E$, $\phi \in \operatorname{Irr}(E)$, and $\chi \in \operatorname{Irr}(\phi \,|\, N)$. If ϕ is faithful on $Z(E)$, then χ is faithful on $Z = Z(E) \cap N$.

Proof: By Clifford's theorem, the restriction of ϕ to N can be expressed as a sum of characters $\chi^g(x) = \chi(gxg^{-1})$ conjugated to χ:

$$(\phi \downarrow N)(x) = m \sum_{g \in R} \chi^g(x),$$

for some subset R of E. The conjugated characters satisfy $\chi^g(z) = \chi(gzg^{-1}) = \chi(z)$ for all central elements $z \in Z$. Hence

$$(\phi \downarrow N)(z) = |R| m \chi(z)$$

for all $z \in Z$, which proves the claim. □

Recall that the support $\operatorname{supp}(\chi)$ of a function $\chi : E \to \mathbf{C}$ is given by the set $\operatorname{supp}(\chi) = \{g \in E \,|\, \chi(g) \neq 0\}$. We use our knowledge of character values to determine the support of the character χ:

Lemma 4: Let E be a finite group satisfying $E' \subseteq Z(E)$, and $N \trianglelefteq E$. If $\chi \in \mathrm{Irr}(N)$ is faithful on $Z = N \cap Z(E)$, then $\mathrm{supp}(\chi) = Z(N)$.

Proof: Let $n \in \mathrm{supp}(\chi)$. Seeking a contradiction, we assume that $n \notin Z(N)$. Since $E' \subseteq Z(E)$, this means that there exists an element $g \in N$ such that $gng^{-1} = zn$ for some $z \in Z(E)$, $z \neq 1$. Note that zn, hence z, is an element of N since N is a normal subgroup of E. Thus,

$$\chi(n) = \chi(gng^{-1}) = \chi(zn) = \omega\chi(n)$$

with $\omega \neq 1$, by Lemma 2. This contradicts the fact that $\chi(n) \neq 0$, hence $\mathrm{supp}(\chi) = Z(N)$ as claimed. $\square$

Recall that the centralizer $C_E(H)$ of a subgroup H in E is given by the group

$$C_E(H) = \{g \in E \,|\, ghg^{-1} = h \text{ for all } h \in H\}.$$

Using this notation, we are able to explicitly determine the inertia subgroup $T(\chi)$:

Lemma 5 ("Tacheles" Lemma) Let E be a finite group satisfying $E' \subseteq Z(E)$, and $N \trianglelefteq E$. Let $\phi \in \mathrm{Irr}(E)$ be faithful on $Z(E)$, and $\chi \in \mathrm{Irr}(\phi \,|\, N)$. Then the inertia group of χ in E is given by $T(\chi) = C_E(Z(N))$.

Proof: The character χ is faithful on $Z(E) \cap N$ by Lemma 3. Thus $\mathrm{supp}(\chi) = Z(N)$ by Lemma 4. It follows that $C_E(Z(N)) \leq T(\chi)$. Conversely, suppose that $g \notin C_E(Z(N))$. We want to show that g cannot be an element of the inertia group. Since $E' \subseteq Z(E)$, the condition $g \notin C_E(Z(N))$ implies that there exists an element $n \in Z(N)$ such that $gng^{-1} = zn$ for some $z \in Z(E)$, $z \neq 1$. Since N is a normal subgroup of E, we also obtain that $zn \in N$. Together with $n \in N$ this shows that $z \in N$. By Lemma 2, $\chi^g(n) = \chi(gng^{-1}) = \chi(zn) = \omega\chi(n)$ with $\omega \neq 1$. Since $n \in Z(N) \subseteq \mathrm{supp}(\chi)$, $\chi(n) \neq 0$, whence $g \notin T(\chi)$. $\square$

IV. Abelian Index Groups

Suppose that we fix a normal subgroup N of an abstract error group E and define a Clifford code Q using a character $\chi \in \mathrm{Irr}(\phi \,|\, N)$. If the index group of E is abelian, then the next theorem shows that Q could have been derived from an abelian group, namely from the center $Z(N)$ of N.

Theorem 6: Let E be an abstract error group with abelian index group. Let N be a normal subgroup of E. Suppose that Q is a Clifford code with respect to N, then Q is also a Clifford code with respect to $Z(N)$.

Proof: We divide the proof into several steps.

Step 1. The Clifford code Q is defined by the following data. There exists a faithful irreducible character ϕ of E that corresponds to a unitary representation ϱ of degree $(E\colon Z(E))^{1/2}$ and $\chi \in \mathrm{Irr}(\phi \,|\, N)$ such that

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

is an orthogonal projector onto Q.

Step 2. Recall that E satisfies $E' \subseteq Z(E)$, since the index group $E/Z(E)$ is abelian. We want to show that $N \trianglelefteq E$ implies that $Z(N) \trianglelefteq E$. Indeed, take $n \in Z(N)$ and $g \in E$. We have $gng^{-1} = zn$ for some $z \in Z(E)$, since $E' \subseteq Z(E)$. Now $zn \in N$, since $N \trianglelefteq E$, and thus $z \in N$. On the other hand, an element $z \in Z(E) \cap N$ is an element of $Z(N)$. This shows that all conjugates of an element $n \in Z(N)$ are again elements of $Z(N)$, whence $Z(N) \trianglelefteq E$.

Step 3. The restriction of χ to the center $Z = Z(N)$ is given by $(\chi \downarrow Z)(x) = \chi(1)\,\varphi(x)$ for some irreducible character φ of Z, cf. Prop. 6.3.5 in [12]. We claim that

$$e_\varphi = \frac{1}{|Z|} \sum_{z \in Z} \varphi(z^{-1}) \varrho(z)$$

is also an orthogonal projector onto Q. It is clear that $\dim_{\mathbf{C}} \mathrm{im}(e_\chi) = \dim_{\mathbf{C}} \mathrm{im}(e_\varphi)$, since the "Tacheles" Lemma shows that the inertia groups of χ and φ are given by $T(\chi) = C_E(Z) = T(\varphi)$. Thus, it suffices to show that the dimension of $\mathrm{im}(e_\varphi e_\chi)$ is not smaller than the dimension of $\mathrm{im}(e_\chi)$.

Step 4. Recall that $\phi(g) = \mathrm{tr}\, \varrho(g)$ is zero for all $g \in E$ not in the center $Z(E)$. Moreover, $(\phi \downarrow Z)(z) = \phi(1)\varphi(z)$ holds for all $z \in Y = Z(E) \cap N$, cf. Lemma 3. Keeping this in mind, it is easy to calculate the dimension of $\mathrm{im}(e_\chi)$ by

$$\dim_{\mathbf{C}} \mathrm{im}(e_\chi) = \mathrm{tr}\, e_\chi = \frac{|Y|\,\phi(1)\chi(1)^2}{|N|}.$$

On the other hand, we find that

$$\begin{aligned} \dim_{\mathbf{C}} \mathrm{im}(e_\varphi e_\chi) &= \mathrm{tr}(e_\varphi e_\chi) \\ &= \frac{\chi(1)}{|N|\,|Z|} \sum_{\substack{n \in N, z \in Z \\ nz \in Y}} \varphi(z^{-1}) \chi(n^{-1})\, \mathrm{tr}\, \varrho(nz). \end{aligned}$$

Since $\chi(z) = \chi(1)\varphi(z)$ holds for $z \in Z$, and the conditions $z \in Z$ and $nz \in Y$ imply that $n \in Z$, we

can further simplify this expression to

$$\begin{aligned} \operatorname{tr}(e_\varphi e_\chi) &= \frac{\chi(1)^2}{|N|\,|Z|} \sum_{\substack{n,z\in Z\\ nz\in Y}} \varphi(z^{-1}n^{-1}) \operatorname{tr} \varrho(nz) \\ &= \frac{|Y||Z|\phi(1)\chi(1)^2}{|N||Z|}. \end{aligned}$$

This shows that $\dim_{\mathbf{C}} \operatorname{im}(e_\chi) = \dim_{\mathbf{C}} \operatorname{im}(e_\varphi e_\chi)$, whence e_χ and e_φ project both onto Q. □

V. Conclusions

We have shown some basic properties of Clifford codes, which are a natural generalization of stabilizer codes. The main result of this note shows that there is no loss in assuming that the normal subgroup defining a Clifford code is abelian provided that the abstract error group is a nilpotent group of class at most 2. An analogue of Theorem 6 does not hold for general index groups. In fact, we have recently shown that there exist Clifford codes which are not stabilizer codes [13]. This result indicates that abstract error groups with nonabelian index groups might provide a new angle to the theory of quantum error correcting codes. Moreover, this shows that the theory of Clifford codes – after all – extends the concept of stabilizer codes.

References

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

[2] 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*, vol. 44, pp. 1369–1387, 1998.

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

[4] E.M. Rains, "Nonbinary quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1827–1832, 1999.

[5] A. Klappenecker and M. Rötteler, "Beyond stabilizer codes I: Nice error bases," this volume.

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

[7] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, 2nd edition, 1983.

[8] C.W. Curtis and I. Reiner, *Methods of Representation Theory*, vol. I, John Wiley & Sons, New York, 1981.

[9] J.-P. Serre, *Linear Representation of Finite Groups*, Springer-Verlag, New York, 1977.

[10] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, and W.K. Wootters, "Mixed State Entanglement and Quantum Error Correction," *Physical Review A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[11] E. Knill and R. Laflamme, "A theory of quantum error–correcting codes," *Physical Review A*, vol. 55, no. 2, pp. 900–911, 1997.

[12] L.C. Grove, *Groups and Characters*, John Wiley, New York, 1997.

[13] A. Klappenecker and M. Rötteler, "Clifford codes," in *The Mathematics of Quantum Computing*, R. Brylinski and G. Chen, Eds. 2002, CRC-Press, to appear.