

Remarks on Clifford Codes

Andreas Klappenecker*, Martin Rötteler†

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

†Institute for Quantum Computation, University of Waterloo
Waterloo, Ontario, Canada N2L 3G1,
mroetteler@iqc.ca

Abstract

Clifford codes are a class of quantum error control codes that form a natural generalization of stabilizer codes. These codes were introduced in 1996 by Knill, but only a single Clifford code was known, which is not already a stabilizer code. We derive a necessary and sufficient condition that allows to decide when a Clifford code is a stabilizer code, and compile a table of all true Clifford codes for error groups of small order.

Keywords Quantum error correcting codes, stabilizer codes, Clifford codes.

1 Introduction

Storing and manipulating the states of quantum mechanical systems for the purpose of quantum information processing is appealing. One can take advantage of quantum mechanical states to gain considerable computational advantages. However, this kind of information processing is highly sensitive to noise, and protection by some means of quantum error correction is necessary.

The most common construction of quantum error correcting codes is based on binary stabilizer codes, a concept developed by Gottesman [6] and Calderbank, Rains, Shor, and Sloane [4], and others. Subsequently, stabilizer codes were generalized to nonbinary alphabets by Ashikhmin and Knill [1], Bierbrauer and Edel [2], Feng [5], and Matsumoto and Uyematsu [11].

A further generalization of stabilizer codes, the so-called Clifford codes, was introduced by Knill [10]. Knill realized that it is possible to lift the restriction to *abelian* normal subgroups in the definition of stabilizer codes, allowing arbitrary normal subgroups instead.

A fundamental problem is to decide when a Clifford code is not equal to a stabilizer code. So far, this has been demonstrated for just a single example [9]. The construction of this example required an exhaustive search of all codes based on a given error group, because more convenient criteria did not exist at the time. The search for such examples is complicated by the fact that in many error groups there simply do not exist any Clifford codes that are not equal to stabilizer codes.

We further develop the theory of Clifford codes. We derive a necessary and sufficient condition that allows to decide when a Clifford code is equal to a stabilizer code. This condition enables us to compile a table of all Clifford codes that are not stabilizer codes for error groups of order up to 255.

2 Basic Notions

Let G be a finite group having an irreducible, faithful character ϕ of degree $d := \phi(1) = (G:Z(G))^{1/2}$. Denote by ρ a unitary representation of G affording ϕ . The matrices $\mathcal{E} = \{\rho(g) \mid g \in G\}$ represent a discrete set of errors. For instance, in the special case of binary stabilizer codes, the error group G is given by an extraspecial 2-group and the representing matrices $\rho(g)$ by tensor products of Pauli matrices.

Let $N \trianglelefteq G$ be a normal subgroup of G , and let χ an irreducible character of N such that $[\chi, \phi_N] \neq 0$. A **Clifford code** with data (G, ρ, N, χ) is defined to be the image of the orthogonal projector

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

that is, a subspace of dimension $\text{tr } P$ of \mathbf{C}^d . If the normal subgroup N is abelian, then the Clifford code is called a **stabilizer code**.

A fundamental problem is to decide when a Clifford code is a stabilizer code. If N is not abelian, then the image of the projector P might still be a stabilizer code, but with respect to another normal abelian subgroup A of G . We derive necessary and sufficient criteria when a Clifford code is a stabilizer code. Note that we keep the discrete set of errors fixed for this comparison.

3 Clifford Codes versus Stabilizer Codes

Let $Q \subseteq \mathbf{C}^d$ be a Clifford code with data (G, ρ, N, χ) . The inertia subgroup

$$T = \{g \in G \mid \chi(n) = \chi(gng^{-1}) \text{ for all } n \in N\}$$

consists of all elements g of G such that $\rho(g)Q = Q$. Let $\vartheta \in \text{Irr}(T)$ denote the character such that $[\vartheta_N, \chi] \neq 0$ and $[\phi_T, \vartheta] \neq 0$. This is the character afforded by the irreducible \mathbf{CT} -module Q . The quasikernel

$$Z(\vartheta) = \{g \in G \mid \vartheta(1) = |\vartheta(g)|\}$$

consists of the elements g of G that act on the code Q by scalar multiplication. These two groups characterize the errors in G that are detectable by the code. An error $\rho(g)$ is detectable by the code Q if and only if $g \notin T - Z(\vartheta)$, see [10, 8].

The group $Z(\vartheta)$ will allow us to decide whether or not the Clifford code Q is a stabilizer code. Denote by $\mathcal{A} = \{A \leq Z(\vartheta) \mid A \trianglelefteq G, A \text{ abelian}\}$ the set of all normal abelian subgroups A of G that are contained in $Z(\vartheta)$. We will show that in case Q is a stabilizer code, then its stabilizer can be defined in terms of a maximal group of \mathcal{A} .

Lemma 1. *If $A \in \mathcal{A}$, then there exists a linear character θ of A such that the image of the orthogonal projector*

$$P_A = \frac{1}{|A|} \sum_{a \in A} \theta(a^{-1}) \rho(a) \tag{2}$$

contains Q , meaning that $P_A v = v$ holds for all $v \in Q$.

Proof. The condition $A \leq Z(\vartheta)$ ensures that each matrix $\rho(a)$, $a \in A$, acts by multiplication with a scalar $\theta(a)$ on the code space Q . The eigenvalues $\theta(a)$ form a linear character of A . Choosing this character in (2) yields $P_A v = v$ because $\theta(a^{-1})\theta(a) = 1$. \square

Lemma 2. *Let A be an abelian normal subgroup of G with linear character θ . If the image of the projector (2) contains the Clifford code Q , then $A \leq Z(\vartheta)$.*

Proof. Direct calculation shows that $\rho(a)P_A = \theta(a)P_A$ for all $a \in A$. Thus, $\rho(a)$ acts by multiplication with a scalar $\theta(a)$ on the code space Q . It follows that $A \leq Z(\vartheta)$. \square

Theorem 3. *Let Q be a Clifford code with data (G, ρ, N, χ) , and denote by ϕ the irreducible character of G afforded by the representation ρ . Keeping the above notations, we can conclude that Q is a stabilizer code if and only if $\dim Q = |A \cap Z(G)|\phi(1)/|A|$ holds for some $A \in \mathcal{A}$.*

Proof. By the previous two lemmas, the image of the projector (2) contains Q if and only if $A \in \mathcal{A}$. It follows that $\text{im } P_A = Q$ if and only if $\dim(\text{im } P_A) = \text{tr } P_A = |A \cap Z(G)|\phi(1)/|A|$ coincides with $\dim Q$. \square

We can strengthen this result by observing that we can assume without loss of generality that the elements of the center $Z(G) = \{z \mid zg = gz \text{ for all } G\}$ of G are contained in the normal subgroup N .

Lemma 4. *Let Q be a Clifford code with data (G, ρ, N, χ) . It is possible to define Q over the normal subgroup $N_Z = NZ(G)$ of G that is obtained by extending N by central elements of G .*

Proof. Let σ denote a unitary representation of N with character χ . We can extend this representation to a representation σ_Z of N_Z by defining $\sigma_Z(zn) = \alpha(z)\sigma(n)$, where $\alpha(z)$ is the scalar $\rho(z) = \alpha(z)\mathbf{1}$, $z \in Z(G)$. It is easy to check that this is well-defined, because σ is a constituent of the restriction of the representation ρ to N . Denote by χ_Z the character $\chi_Z = \text{tr } \sigma_Z$. Let Z be a transversal of N_Z/N such that $Z \subseteq Z(G)$. Then the definition of the character χ_Z ensures that

$$\frac{\chi_Z(1)}{|N_Z|} \sum_{z \in Z} \sum_{n \in N_Z} \chi(n^{-1}z^{-1})\rho(zn) = \frac{\chi_Z(1)}{|N_Z|} \sum_{z \in Z} \sum_{n \in N_Z} \chi(n^{-1})\rho(n)$$

coincides with the projector onto the Clifford code Q given by (1); therefore (G, ρ, N_Z, χ_Z) defines the Clifford code Q . \square

From now on, we will assume without loss of generality that the center $Z(G)$ of G is contained in N . If Q is not a stabilizer code, then we can prove this by looking at just one group in \mathcal{A} that is of maximal order:

Corollary 5. *A Clifford code Q is a stabilizer code if and only if $\dim Q = |Z(G)|\phi(1)/|A|$ holds for a group $A \in \mathcal{A}$ that has maximal order among the groups in \mathcal{A} .*

Proof. If Q is a stabilizer code, then there exists some $A \in \mathcal{A}$ such that Q is the image of the projector (2). By the previous lemma, we can assume without loss of generality that $Z(G)$ is contained in A , hence the dimension of the code is $\text{tr } P_A = |Z(G)|\phi(1)/|A| = \dim Q$. Seeking a contradiction, we assume that this group A is not a group of maximal order in \mathcal{A} . This would imply that \mathcal{A} contains a group $A_* \geq Z(G)$ with $|A_*| > |A|$. By definition of \mathcal{A} , the image of the projector P_{A_*} contains Q , hence

$$\dim Q < |Z(G)|\phi(1)/|A_*| < |Z(G)|\phi(1)/|A| = \dim Q,$$

yields the desired contradiction

Conversely, if A is a group of maximal order in \mathcal{A} , then $Z(G)$ is contained in A . Therefore, $|Z(G)|\phi(1)/|A| = \dim Q$ is the dimension of its stabilizer, and since the image of P_A contains Q , it follows that $\text{im } P_A = Q$; hence, Q is a stabilizer code. \square

If we want to show that Q is a stabilizer code, then the following condition is convenient.

Corollary 6. *Suppose that $Z(G) \leq N$. A Clifford code (G, ρ, N, χ) is a stabilizer code if and only if $\chi^2(1) = |N|/|A|$ for some $A \in \mathcal{A}$ with $Z(G) \leq A$.*

Proof. Compare $\text{tr } P = \chi(1)^2 \phi(1) |Z(G)|/|N|$ and $\text{tr } P_A = \phi(1) |Z(G)|/|A|$ and apply Theorem 3. \square

4 Examples

We give two examples to illustrate the method. In the first example, we construct a Clifford code for the data (G, ρ, N, χ) which turns out to be equal to a stabilizer code for an abelian normal subgroup $A \triangleleft G$. In the second example, we construct a true Clifford code, that is, we rule out that this code is equal to a stabilizer code by Corollary 6. This shows that the class of Clifford codes is strictly bigger than the class of stabilizer codes.

Example 7. Let G be a group. Recall that the commutator of the elements $g, h \in G$ is defined by $[g, h] := g^{-1}h^{-1}gh$. Now, consider the group G given by the power-commutator presentation

$$G = \langle a, b, c, d, e \mid a^2 = d, b^2 = c^2, d^2 = e^2, [b, a] = c, [c, a] = e, [d, a], [e, a], [c, b], [d, b] = e, [e, b], [d, c], [e, c], [e, d] \rangle.$$

We find that G is a finite group of size 32. The group G has an irreducible four-dimensional representation ρ . Since the order of the centre is $|Z(G)| = 2$ we have that $[G : Z(G)] = \text{deg}(\rho)^2$, i. e., G is an error group. Actually, G is isomorphic to the group `SmallGroup(32,6)` which is contained in the catalog of error groups of small order [7]. Also note that the set $\{a, b, c, d, e\}$ is not a minimal generating set of G . In fact, we have that $G = \langle a, ab \rangle$. We find that ρ is the irreducible four-dimensional representation given by

$$\rho(a) = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad \rho(ab) = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$

In search for suitable Clifford codes we choose the normal subgroup $N = \langle b, c, d, e \rangle$ of order 16. Then N has ten conjugacy classes with representatives

$$(), e, d, c, ce, cd, b, bd, bc, bcd.$$

We define the irreducible character χ with respect to this ordering of the conjugacy classes. Then χ is given by the values

$$2, -2, 0, 2, -2, 0, 0, 0, 0, 0.$$

Next, we construct the corresponding projector $P = \frac{\chi(1)}{|N|} \sum_{n \in N} \chi(n^{-1})\rho(n)$, which turns out to be

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

The corresponding Clifford code Q is equal to a stabilizer code. In order to see this, we have to compute the inertia group $T(\chi)$ first. It turns out to be no larger than the normal subgroup, i. e., we have $T(\chi) = N$. Hence the representation ϑ of the inertia group coincides with χ in this case. The quasikernel $Z(\chi)$ is a group of order four given by $Z(\vartheta) = \langle c, e \rangle$. Note that $Z(\vartheta) \cong Z_2 \times Z_2$, i. e., the quasikernel is not cyclic.

We obtain that $\deg(\chi)^2 = 4 = \frac{|N|}{|Z(\vartheta)|}$, i. e., by the criterion given in Corollary 6 the code is a stabilizer code.

Indeed, we can construct this stabilizer code as follows: the characters $\epsilon_1, \dots, \epsilon_4$ of $Z(\vartheta)$ are given by the rows of the Hadamard matrix

$$H_2 \otimes H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

We find that the Clifford code corresponding to $(G, \rho, Z(\vartheta), \epsilon_3)$ is equal to Q .

The preceding example shows that there are Clifford codes (G, ρ, N, χ) for which the corresponding projector is equal to a stabilizer code (G, ρ, A, χ') , where $A \triangleleft G$ is an *abelian* subgroup of G . In [9] it has been shown that there is an error group of size 32 (namely, the group `SmallGroup(32,5)`) which gives rise to a true Clifford code. The dimension of the corresponding ambient space in this example was four and the dimension of the code, i. e., the rank of the projector, was two. In the following example we exhibit a true Clifford code for a six-dimensional system.

Example 8. Let G be the group generated by the matrices $A, B, C \in \mathbf{C}^{6 \times 6}$ which

are defined as follows:

$$A := \begin{pmatrix} \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot \end{pmatrix}, \quad B := \begin{pmatrix} \omega^3 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \omega^7 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \omega^{11} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -\omega^3 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & -\omega^{11} & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & -\omega^7 \end{pmatrix},$$

and $C := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \otimes \mathbf{1}_3$. Here $\omega := \exp(2\pi i/12)$ is a primitive 12th root of unity and we have replaced entries equal to 0 with a dot. Then G is isomorphic to the group `SmallGroup(216,66)` and is an abstract error group, i. e., $[G : Z(G)] = \deg(\phi)^2$, where ϕ is the character of degree 6 corresponding to the natural matrix representation of G .

As normal subgroup N we choose the group generated by $N = \langle A, C, D \rangle$, where $D = \text{diag}(1, \omega_3, \omega_3^2, 1, \omega_3^2, \omega_3)$. Here $\omega_3 := \exp(2\pi i/3)$. We find that N has order 108 and that N has a character χ leading to the projector

$$P = \frac{1}{2} \begin{pmatrix} 1 & \cdot & \cdot & i & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & i \\ \cdot & \cdot & 1 & \cdot & i & \cdot \\ -i & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & -i & \cdot & 1 & \cdot \\ \cdot & -i & \cdot & \cdot & \cdot & 1 \end{pmatrix}$$

of rank 3. Like in the previous example we find that the inertia group $T(\chi)$ coincides with N .

We find that the quasikernel $Z(\vartheta)$ has order 6. Hence we obtain that the possible quotients $\frac{|N|}{|A|}$, where A is a subgroup of $Z(\vartheta)$ are given by 216, 108, 72, and 36, i. e., none of them equals $\deg(\chi)^2 = 9$. This shows that the Clifford code Q defined by the projector P is not equal to a stabilizer code for the group G .

5 Nonstabilizer Clifford Codes of Small Order

We have compiled a table containing information about Clifford codes for error groups of small order to illustrate the above theory. We have carried out a search over all error groups up to size 255, where we made use of the fact that information about these groups is available in [7]. We maintain a catalog of error groups of small order at

<http://faculty.cs.tamu.edu/klappi/ueb/ueb.html>

from which the relevant information about error groups can be extracted.

For each error group G , we constructed Clifford codes for all possible data (G, ρ, N, χ) . This includes a computation of the lattice of normal subgroups of G and a search for all suitable characters χ . Using the criterion given in Corollary 6, we have filtered all those Clifford codes which are not equivalent to a stabilizer code. In Table 1, we give condensed information about the result of this search. The catalog number refers to the number in the Neubüser catalog used in MAGMA and GAP, cf. [3, 12], which can be accessed via the command `SmallGroup(<size>, <no>)`. The character ϕ is the character of G corresponding to ρ which defines the error basis. The normal subgroup N together with its character χ defines the Clifford code. In the last column we give the dimension of the resulting Clifford code. For instance the row

216	66, 68, 72	6	108	3	3
-----	------------	---	-----	---	---

shows that there are three different abstract error groups of size 216 which give rise to nonstabilizer Clifford codes. These groups can be constructed using the commands

`SmallGroup(216,66)`, `SmallGroup(216,68)`, and `SmallGroup(216,72)`

in GAP. The third column shows that all these error groups give rise to six-dimensional error groups. Furthermore, in each of these groups exists a normal subgroup N of order 108 having an irreducible character χ of degree 3. This in turn gives rise to a projector onto a Clifford code of dimension 3, which is not equal to a stabilizer code.

6 Conclusions

We have further developed the theory of Clifford codes by giving a necessary and sufficient condition that allows to decide when a Clifford code is equal to a stabilizer code. This condition allowed us to compile a table of all Clifford codes that are not stabilizer codes for error groups of order up to 255.

One of the main open problems in the theory of Clifford codes is whether there exists a true Clifford code which is better than any stabilizer code. We expect the characterization shown in this paper to be useful in the study of Clifford codes for composite systems, where the error basis is given by the tensor product of several copies of a fixed basis. In this case, the group is a central product of the individual components and the challenging task is to identify suitable normal subgroups of this central product such that the corresponding Clifford code outperforms any stabilizer code.

#G	Catalog Number	$\phi(1)$	#N	$\chi(1)$	dim(Q)
32	43, 44	4	16	2	2
64	102, 111, 125, 256	4	32	2	2
96	183, 184	4	48	2	2
128	71, 72, 73, 74, 87, 88, 138, 139, 634, 635, 636, 637, 641, 642, 643, 644, 645, 646, 647, 853, 854, 855, 859, 860, 861, 865, 866, 867, 912, 913, 922, 923, 931, 932, 933, 934, 935, 970, 971, 1751, 1752, 1753, 1754, 1758, 1759, 1760, 1800, 1801, 2020, 2021, 2317, 2318	8	32	2	2
128	138, 139, 144, 145, 853, 854, 855, 859, 860, 861, 865, 866, 867, 912, 913, 922, 923, 931, 932, 933, 934, 935, 970, 971, 1751, 1752, 1753, 1754, 1758, 1759, 1760, 1800, 1801, 2020, 2021, 2317, 2318	8	64	4	4
128	912, 913, 922, 2020, 2021, 2317, 2318	8	16	2	4
128	849, 885, 903, 1687	4	64	2	2
160	197, 198	4	80	2	2
192	854, 863, 877, 1464	4	96	2	2
216	39, 41, 42	6	72	2	2
216	66, 68, 72	6	108	3	3
224	171, 172	4	112	2	2
243	28, 29, 30, 56, 57, 58, 59, 60	9	81	3	3

Table 1: Error groups of size up to 255 giving rise to Clifford codes which are not equivalent to stabilizer codes. Note that some groups be listed in several rows of this table since. This is due to the fact that Clifford codes for various normal subgroups N and characters χ might exist.

Acknowledgments. This research was supported by NSF grant EIA 0218582 and Texas A&M TITF. M. R. acknowledges support by CFI, ORDFC, and MITACS.

References

- [1] A. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, 47(7):3065–3072, 2001.
- [2] J. Bierbrauer and Y. Edel. Quantum twisted codes. *J. Comb. Designs*, 8:174–188, 2000.
- [3] W. Bosma, J.J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24:235–266, 1997.
- [4] 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.
- [5] K. Feng. Quantum error-correcting codes. In *Coding Theory and Cryptology*, pages 91–142. World Scientific, 2002.
- [6] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, 54:1862–1868, 1996.
- [7] A. Klappenecker and M. Rötteler. Beyond stabilizer codes I: Nice error bases. *IEEE Transaction on Information Theory*, 48(8):2392–2395, 2002.
- [8] A. Klappenecker and M. Rötteler. Beyond stabilizer codes II: Clifford codes. *IEEE Transaction on Information Theory*, 48(8):2396–2399, 2002.
- [9] A. Klappenecker and M. Rötteler. Clifford codes. In R. Brylinski and G. Chen, editors, *Mathematics of Quantum Computing*, pages 253–273. Chapman & Hall/CRC Press, 2002.
- [10] E. Knill. Group representations, error bases and quantum codes. Los Alamos National Laboratory Report LAUR-96-2807, 1996.
- [11] R. Matsumoto and T. Uyematsu. Constructing quantum error correcting codes for p^m -state systems from classical error correcting codes. *IEICE Trans. Fundamentals*, E83-A(10):1878–1883, 2000.
- [12] The GAP Team. GAP – Groups, Algorithms, and Programming. Lehrstuhl D für Mathematik, RWTH Aachen and School of Mathematical and Computational Sciences, Univ. St. Andrews, Scotland, 1997.