Investigations on Automorphism Groups of Quantum Stabilizer Codes

Hanson Hao

Stanford University

Introduction

Although quantum computers are thought to be significantly more efficient than classical computers (e.g. Shor's algorithm for integer factorization), they are also inherently more susceptible to noise and breakdown processes. Therefore, a challenge of great practical importance is to replicate the theory of classical error correction in the quantum setting.

The central concept of error correction is *redundancy*. In the classical case, this can be done with bit repetition: suppose we wanted to send a single 0 or 1 bit, but there is a possibility of a bit flip error. We can get around this by the following encoding scheme:

$$0 \mapsto 000$$
$$1 \mapsto 111$$

As long as the probability p of a bit flip error is not too high (i.e. $p < 1/2$), we can use "majority rules" to decode the message with a high probability of success. For example if we received 010, we guess that the intended message was 000.

Quantum Error Correction Basics

Definition: A *qubit* is the basic unit of quantum computation. It is represented as the complex vector space $\mathbb{C}^2$ with basis vectors $\mathbf{0}$ and $\mathbf{1}$. A space of n qubits is represented as the tensor product $\mathbb{C}^{2^n} \cong \underbrace{\mathbb{C}^2 \otimes_{\mathbb{C}} \ldots \otimes_{\mathbb{C}} \mathbb{C}^2}_{n \text{ times}}$. A basis for this space is given by $\{\mathbf{0}\ldots\mathbf{0}, \mathbf{0}\ldots\mathbf{01}, \ldots, \mathbf{1}\ldots\mathbf{1}\}$, the 2^n binary vectors of length n.

In quantum error correction, we want to identify a k-qubit space with some 2^k-dimensional linear subspace, called the *codespace*, of an n-qubit space, called the *ambient space*. We will call states in the ambient 2^n-dimensional space *physical*, and states in the 2^k-dimensional codespace *logical*. Errors are linear operators acting on $\mathbb{C}^{2^n}$.

We also have two extra difficulties not encountered in the classical setting:

- Quantum information cannot be directly copied. This is the *no-cloning theorem* ([6]).
- We have to correct for a continuum of possible errors.

Fortunately, for the second item, the following quantum error-correction conditions ([6]) show that correcting a discrete set of errors allows us to correct any linear combination of such errors:

Quantum error-correction conditions: Let $C \subset \mathbb{C}^{2^n}$ be a quantum code, and let P be the orthogonal projection onto C. Then C can correct a set of errors $\mathcal{E} = \{E_i\}$ if and only if there is a complex Hermitian matrix (α_{ij}) such that

$$PE_i^* E_j P = \alpha_{ij} P, \tag{1}$$

where E_i, E_j run over all operators in $\mathcal{E}$, and * is the conjugate transpose.

Because of this property, it makes sense to define the four Pauli matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad Y = iXZ = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}. \tag{2}$$

These matrices are unitary, Hermitian, pairwise commute or anticommute, and form a basis of the 2×2 complex matrices. In particular, correcting these means we correct all errors on 1 qubit!

Notice that the action of X is to swap $\mathbf{0}$ and $\mathbf{1}$; we call it the *bit flip*. The action of Z is to send $\mathbf{0}$ to $\mathbf{0}$ and $\mathbf{1}$ to $-\mathbf{1}$; we call it the *phase flip*.

Moreover, n-fold tensor products of the Pauli matrices act "qubit-wise" on $\mathbb{C}^{2^n}$. We may collect all such tensor products into a group:

Definition: The n-qubit Pauli group, denoted G_n, is the group of matrices generated by n-fold tensor products of the Pauli matrices. This is a group of order 4^{n+1}: for instance,

$$G_1 = \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}.$$

We also define $P_n \coloneqq G_n / Z(G_n)$, the quotient of G_n by its center $\langle iI \rangle$.

We make one more definition related to G_n, which will be needed later on.

Definition: The (one-qubit) *Clifford group* L_1 is the matrix group generated by G_1, $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, and $S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ ([1]). The n-qubit *diagonal Clifford group* L_n is defined as $L_n \coloneqq \{A_1 \otimes \ldots \otimes A_n : A_i \in L_1\}$. Note that G_1, H, and S all normalize G_1, so L_n has a natural conjugation action on G_n.

In the terminology of quantum logic gates, H is the *Hadamard gate*, and S is the *phase shift gate* where the shift is by $\frac{\pi}{4}$. The conjugation actions of H and S on X, Y, and Z are as follows:

$HXH^{-1} = Z$	$SXS^{-1} = Y$
$HZH^{-1} = X$	$SZS^{-1} = Z$
$HYH^{-1} = -Y$	$SYS^{-1} = -X$

Therefore, up to sign, H and S generate the action of S_3 on X, Y, and Z. This is an important property that was exploited in our hand calculations.

Stabilizer Codes

An important idea of Gottesman ([3]) was to try to define quantum codes via suitable subgroups of G_n. The key construction is the following:

Definition: Let S be an *abelian* subgroup of G_n *not containing* $-I$ (in particular, S is be an elementary abelian 2-group). Then

$$C(S) = \{v \in \mathbb{C}^{2^n} : sv = v \text{ for all } s \in S\} \tag{3}$$

is the *stabilizer code* corresponding to S. We call S the *stabilizing subgroup* corresponding to $C(S)$.

The conditions on S are meant to ensure that $C(S)$ is not 0-dimensional. In fact, if $S = 2^m$, then $\dim(C) = 2^{n-m}$; that is, it encodes $k \coloneqq n - m$ logical qubits. Here, we call C an $[[n, k]]$ code.

It is also much simpler to deduce the error-correcting properties of C than if we applied the quantum error-correction conditions on some arbitrary code.

Definition: Let $N(S)$ be the normalizer of S in G_n. We say that $p \in P_n$ is in $N(S) - S$ if there is some lift $g \in G_n$ of p in $N(S) - S$. Also, let the *weight* of an element $p \in P_n$ be the number of non-identity tensor factors in p.
Now let C be an $[[n, k]]$ stabilizer code corresponding to a subgroup $S \subset G_n$, where $k \geq 1$. Then the *distance* d of C is defined as

$$d = \min\{\text{weight}(p) : p \in P_n, p \in N(S) - S\}. \tag{4}$$

In this case, we call C a $[[n, k, d]]$ code. In the degenerate case $k = 0$, $N(S) - S$ is empty, so the above definition does not make sense. We follow the convention of [2] and say that the distance is

$$d = \min\{\text{weight}(p) : p \in S, p \neq I\}. \tag{5}$$

Using the quantum error-correction conditions, one can prove that:

Proposition: Any code with distance greater than $2w$ can correct arbitrary errors (independently) affecting any w qubits.

Example: Consider a subgroup $S \subset G_5$ generated by $\{XZZXI, IXZZX, XIXZZ, ZXIXZ\}$. These elements all pairwise commute, and S does not contain $-I$, so the stabilizer code C corresponding to S encodes $5 - 4 = 1$ logical qubit. One can directly verify that the distance of S is 3. This shows that C can correct any error affecting one qubit, since $3 > 2 \cdot 1$. In fact C is the smallest code (in terms of n) able to correct an arbitrary error on any one qubit.

Automorphism Groups

We wanted to investigate automorphism groups of quantum codes, since this theory has been less developed than the theory of automorphism groups of classical codes. Our motivation was to try to connect quantum codes to "moonshine" theory, as in [5] and known results about the classical Golay code.

Strong, Weak, Clifford Automorphisms

There is a natural action of S_n on the n-qubit ambient space $\mathbb{C}^{2^n}$. Hence a reasonable first definition of an automorphism group is

$$\text{Aut}_{\text{strong}}(C) = \{\sigma \in S_n : \sigma(C) = C\} \tag{6}$$

for a stabilizer code C corresponding to stabilizing subgroup $S \subset G_n$. We call this the *strong automorphism group* to distinguish it from later generalizations of this concept.

Noting that S_n also acts on G_n in a natural way, we can show that such strong automorphisms also act on S in a reasonable manner:

Proposition: Let C be a nontrivial (i.e. nonzero) stabilizer code corresponding to a subgroup $S \subset G_n$. Then $\sigma \in \text{Aut}_{\text{strong}}(C)$ if and only if $\sigma(S) = S$.

This proposition makes it easier to calculate automorphism groups by hand or by computer.

Example: Let $S = \{III, XZZ, ZXZ, YYI\} \subset G_3$. Then C is a $[[3, 1]]$ code spanned by $\mathbf{0}_L = \frac{1}{2}(\mathbf{000} + \mathbf{010} + \mathbf{100} - \mathbf{110})$ and $\mathbf{1}_L = \frac{1}{2}(\mathbf{001} - \mathbf{011} - \mathbf{101} - \mathbf{111})$. Checking each of the permutations in S_3, we obtain $\text{Aut}_{\text{strong}}(C) = \{(1), (12)\}$. Indeed, these are also all the permutations σ that satisfy $\sigma(S) = S$.

We may also ask what extra "automorphisms" we get if we are allowed to "twist" by an element that normalizes G_n. We make the following definitions:

Definition/Proposition: The *weak automorphism group* of C is

$$\text{Aut}_{\text{weak}}(C) = \{\sigma \in S_n : \sigma(C) = \gamma_\sigma \cdot C \text{ for some } \gamma_\sigma \in G_n\}. \tag{7}$$

It turns out that we get a result analogous to the above proposition: $\sigma \in \text{Aut}_{\text{weak}}(C)$ if and only if $\sigma(S) \subset S \cup -S$, where $-S = \{-s : s \in S\}$. So the adjective "weak" is somewhat deserved.

Definition: Recall the n-qubit Clifford group L_n, which acts on G_n by "componentwise" conjugation. We define the *Clifford-twisted automorphism group* of C as

$$\text{Aut}_{\text{Clif}}(C) = \{\sigma \in S_n : \sigma(S) = \lambda_\sigma S \lambda_\sigma^{-1} \text{ for some } \lambda_\sigma \in L_n\}. \tag{8}$$

Examples and Results

From the definitions, is immediate that $\text{Aut}_{\text{strong}}(C) \subseteq \text{Aut}_{\text{weak}}(C) \subseteq \text{Aut}_{\text{Clif}}(C)$. Here is a list of some interesting automorphism groups that we found:

$[[n, k, d]]$	$\text{Aut}_{\text{strong}}$	Aut_{weak}	Aut_{Clif}
$[[6, 0, 4]]$	D_{10}	$\text{PSL}(2, 5) \cong A_5$	S_6
$[[7, 1, 3]]$	$\text{PGL}(3, 2)$	$\text{PGL}(3, 2)$	$\text{PGL}(3, 2)$
$[[8, 3, 3]]$	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	$\text{AGL}(1, 8)$	$\text{AGL}(1, 8) \rtimes \text{Aut}(\mathbb{F}_8)$
$[[10, 0, 4]]$	D_{20}	D_{20}	$M_{10}.2 \cong \text{P}\Gamma\text{L}(2, 9)$

Note that the automorphism groups of a stabilizer code cannot be completely determined by the parameters $[[n, k, d]]$, so these examples should be taken as interesting specific cases rather than showcasing a general phenomenon (all examples except the last were taken from the database [4]). For instance, let $S = \{IIII, XXXX, ZZZZ, YYYY\}$ and $S' = \{IIII, XXZZ, YYXX, ZZYY\}$ be subgroups of G_4. Then the corresponding stabilizer codes C and C' both have parameters $[[4, 2, 2]]$. But $\text{Aut}_{\text{strong}}(C) = S_4$, while $\text{Aut}_{\text{strong}}(C') = \{(1), (12), (34), (12)(34)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Important Example: The last code from the table is particularly interesting; it has stabilizing subgroup $S \subset G_{10}$ generated by

$$XIIZXZXZII$$
$$IXIIZXZXZI$$
$$IIXIIZXZXZ$$
$$ZIIXIIZXZX$$
$$XZIIXIIZXZ$$
$$ZXZIIXIIZX$$
$$XZXZIIXIIZ$$
$$ZXZXZIIXII$$
$$IZXZXZIIXI$$
$$IIZXZXZIIX$$

These ten elements are cyclic permutations of each other, and they pairwise commute. It can be checked that S determines a degenerate $[[10, 0, 4]]$ code C, and from [4] we see that 4 is the best possible distance for a $[[10, 0]]$ code. Note that this is not the same $[[10, 0, 4]]$ code given at [4]. Our construction provides a possible connection to the *Mathieu moonshine* phenomenon mentioned previously (see [5]): we have

$$\text{Aut}_{\text{Clif}}(C) = \langle (1\,2\,3\,4\,5\,6\,7\,8\,9\,10), (8\,9)(4\,10)(5\,6) \rangle \cong M_{10}.2,$$

a 3-transitive group of order 1440 related to the simple Mathieu groups.

Given enough examples as above, one might ask whether a "good" stabilizer code (with large distance d) can have highly transitive strong or weak automorphism group. We can show that in certain cases, this is impossible.

Theorem A: Let C be an $[[n, k, d]]$ stabilizer code. Then if C has S_n or A_n as its strong or weak automorphism group, then $d \leq 2$.
Theorem B: There is no $k \geq 1$ stabilizer code with ambient space $\mathbb{C}^{2^{12}}$ (resp. $\mathbb{C}^{2^{11}}$) that has strong or weak automorphism group M_{12} (resp. M_{11}).

The proofs of both theorems rely on counting arguments, as well as the high degree of transitivity of the groups involved. The main idea is to use the high degree of transitivity of the automorphism group to produce an element of small weight, and from there derive some sort of contradiction.

Remark: Note that the Classification of Finite Simple Groups shows that the only t-transitive groups for $t \geq 4$ are S_n, A_n, M_{24}, M_{23}, M_{12}, and M_{11}. Then the previous two theorems show that a "good" code won't have a highly transitive group as its strong or weak automorphism group. This suggests that the Clifford-twisted automorphism group may be the "right" notion to work with if we want to find more examples of interesting automorphism groups, such as the larger Mathieu groups. The aforementioned $[[10, 0, 4]]$ code that we found is evidence towards this heuristic.

Acknowledgements

This research was supported by the Stanford Undergraduate Research Institute in Mathematics (SURIM) program during the summer of 2021. The presenter would like to thank Dr. Pawel Grzegrzolka for coordinating the program. The presenter also thanks his mentor, Dr. Daniel Bump, for introducing him to the area of quantum error correction, and also for many helpful conversations and insightful suggestions.

References

[1] Beverley Bolt, T. G. Room, and G. E. Wall. On the clifford collineation, transform and similarity groups. i-ii. *J. Aust. Math. Soc.*, 2(1):60–96, 1961.
[2] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane. Quantum error correction via codes over GF(4). pages 292–, 1997.
[3] Daniel Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, May 1997.
[4] Markus Grassl. Quantum error-correcting code tables. `http://codetables.de`, 2019. Accessed: 2021-08-08.
[5] Jeffrey A. Harvey and Gregory W. Moore. Moonshine, superconformal symmetry, and quantum error correction. *Journal of High Energy Physics*, 2020(5), May 2020.
[6] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, USA, 10th edition, 2011.