OLLSCOIL NA GAILLIMHE
UNIVERSITY OF GALWAY

Automorphisms of Finite Groups and Logical Operations in Quantum Error Correcting Codes

School of Mathematical and Statistical Sciences - Summer Studentship

Author: *Paul Cassidy*
Supervisor: *Dr Mark Howard*

Abstract
This paper defines logical operations and finite automorphism groups in the context of stabiliser quantum error correcting codes (QECC). The two concepts are compared and a connection is established. The comparison of these concepts reveals a significant relationship, enabling the examination of fundamental properties of stabiliser codes through their automorphism groups. These groups can be easier to understand and allow one to use pre-existing methodologies from group theory.

Contents

1 Introduction

Quantum circuits are noisy, necessitating the development of a fault-tolerant framework for effective real-world application. Massive strides in the area of quantum error correction (QEC) have been made over the past 25 years. In 1998, Gottesman introduced his stabiliser formalism which has emerged as the predominant form of QEC. Chapter 2 explores this formalism and some concepts related to logical operations.

The logical operations allowed in a QEC can be identified and understood through the analysis of the QEC's automorphism groups. Two useful automorphism groups are defined in Chapter 3 and a connection to logical operations is established. Examples of QECCs are provided throughout.

For an introduction to the stabiliser formalism and the requisite group theory, I recommend [1] and [2] respectively.

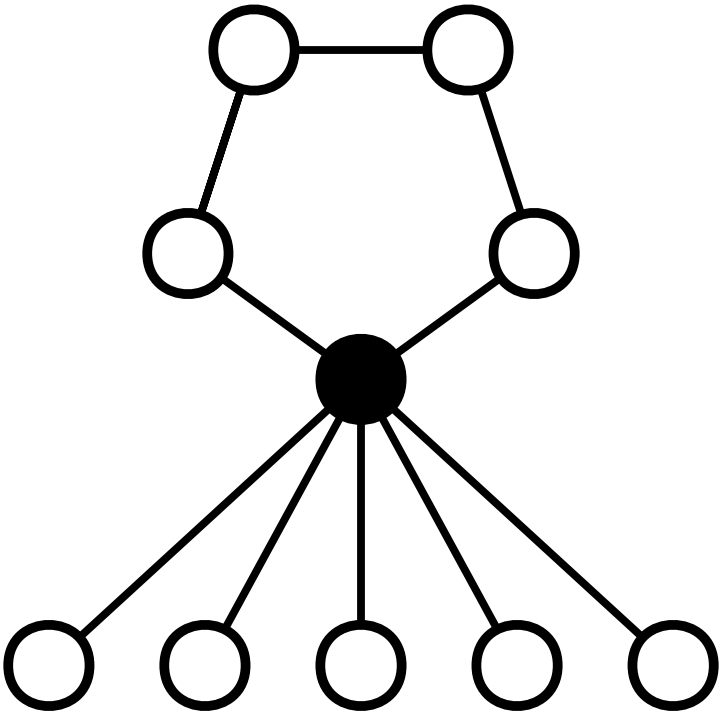

Figure 1.1: The cycle graph of D_{10}, the dihedral group of order 10 (sometimes known as D_5 as it is the symmetry group of a regular 5-gon), is presented. In Chapter 3, it is shown that this serves as both the strong and weak automorphism group of the [5,1,3] QECC.

2 Logical Operations in QECC

Definition 1. A *logical operation* is an operation that acts on the encoded qubits of a QECC.

Example 1. In the [7,1,3] Steane code, the logical Hadamard operation H_L is defined as applying the physical Hadamard on each of the 7 physical qubits:

$$H_L \equiv H^{\otimes 7}$$

Definition 2. The *stabiliser*, S, is an abelian subgroup of G_n (the n qubit Pauli group) which does not contain $-I$ and whose elements "fix" the *codewords* corresponding to S, $C(S) \in \mathbb{C}^{2^n}$:

$$S := \{s \in S, |\psi\rangle \in C(S) \mid s|\psi\rangle = |\psi\rangle\}.$$

One can choose to define the stabilising subgroup in terms of the corresponding codewords or vice versa.

Definition 3. The *normaliser* of S is the set of elements in the group X which commute with all of the elements in S:

$$N_X(S) := \{x \in X, x^{-1}Sx = S\}$$

Elements of the normaliser transform codewords to codewords and thus are useful for QEC.

Definition 4. *Logical operations* are unitary operations which commute with the stabiliser but lie outside of it [3].

$$N_G(S)/S$$

Note that this implies that logical operations do not form a group as S necessarily contains the identity element. These logical operations preserve the codespace but act non-trivially on it. The most general single qubit operation in $N_G(S)$ can be viewed as a rotation of the Bloch sphere permuting the three coordinate axes [1].

3 Automorphism Groups

3.1 Definitions

Definition 5. An *automorphism* is an isomorphism between a mathematical object O and itself. $\phi : O \mapsto O$.

Definition 6. The automorphisms of a group G form a group themselves, known as the *automorphism group* $\mathrm{Aut}(G)$.

In the context of QECC one can define some interesting automorphism groups known as the strong and weak automorphism groups [4].

Definition 7. The *strong automorphism group* of a quantum code C:

$$\mathrm{Aut}_{\mathrm{strong}}(C) := \{\phi \in S_n \mid \phi(C) = C\}$$

where S_n is a symmetric group of order n and acts as a permutation of the Pauli operators in the code.

Definition 8. The *weak automorphism group* of a quantum code C:

$$\mathrm{Aut}_{\mathrm{weak}}(C) := \{\phi \in S_n, g_\phi \in G_n \mid \phi(C) = g_\phi \cdot C\}$$

Example 2. Both the strong and weak automorphism groups of the [5,1,3] code (the smallest code with a single logical qubit where any single physical qubit error can be detected and corrected [5]) are D_{10}, the dihedral group of order 10. The equality of the two automorphism groups implies that there are no single qubit errors that can occur which could change the logical state without it being detected.

3.2 Connection to Logical Operations

3.2.1 The stabiliser and strong automorphism groups

It is clear that the strong automorphisms of a quantum code are those that correspond to unitary operations that leave the code space invariant. They act trivially on the logical state of the code. These are the automorphisms that are generated by elements of the stabiliser.

$$\mathrm{Aut}_{\mathrm{strong}}(C) : |\psi\rangle \overset{\phi}{\mapsto} |\psi\rangle$$
$$\implies \phi(S) = S \implies \phi \in S$$

ϕ must be in S as it maps elements of S to S implying that it is itself in the group.

3.2.2 The normaliser and the weak automorphism groups

On the other hand, the weak automorphism group appears to correspond to the normaliser of S in G_n. It twists the vectors in C by an element of G_n. As G_n contains I it forms a supergroup of the strong automorphism group. The additional elements of the group are those that are correctable by QECC but change the logical state. There is an obvious comparison to the normaliser and the rotations of the Bloch sphere discussed in Chapter 2.

One must find the set of elements $\phi(S)$ which stabilise $\phi(C)$.

$$S|\psi\rangle = |\psi\rangle \text{ and } |\psi\rangle \overset{\phi}{\mapsto} g_\phi \cdot |\psi\rangle$$

$$\implies \phi(S) = g_\phi S g_\phi^{-1} \equiv N_G(S)$$

Giving a direct equivalence between the normaliser of S in G_n and the weak automorphism group of C corresponding to S.

Definition 9. The set of fault tolerant *logical operations* in a QECC is given by the quotient of the weak automorphism group by the strong automorphism group:

$$\{\textit{logical operations}\} \equiv N_G(S)/S \equiv \mathrm{Aut}_{\mathrm{weak}}(C)/\mathrm{Aut}_{\mathrm{strong}}(C)$$

4 Conclusion

In this short report the definitions of the strong and weak automorphisms were juxtaposed with the stabiliser and normaliser of a class of QECC. Through this comparison a new interpretation of a logical operation in stabiliser QECC was found.

In recent times the many results in physics and mathematics have stemmed from dualities between two distinct systems or objects. These dualities have allowed for easier problem solving, exemplified by the likes of ADS/CFT or the Langlands programme. While this connection is more modest in its scope, it can still yield valuable insights for both sides. Hopefully, centuries of group theory research can help quantum computing researchers in their young field and vice versa.

References

[1] Daniel Gottesman. "Theory of fault-tolerant quantum computation". In: *Phys. Rev. A* 57 (1 Jan. 1998), pp. 127–137. DOI: 10.1103/PhysRevA.57.127. URL: https://link.aps.org/doi/10.1103/PhysRevA.57.127.

[2] D. A. R. Wallace. *Groups, Rings and Fields*. Springer London, 1998. DOI: https://doi.org/10.1007/978-1-4471-0425-4.

[3] John Preskill. "Chapter 7: Quantum Error Correction". In: *PH219 - California Institute of Technology*. 1999.

[4] Hanson Hao. *Investigations on Automorphism Groups of Quantum Stabilizer Codes*. 2021. arXiv: 2109.12735 [cs.IT].

[5] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.