Establishing the number of distinct stabilizer bases for a quantum qudit error-correcting code

C M Wilmott

Department of Mathematics and Physics, Nottingham Trent University, Nottingham NG11 8NS, UK

E-mail: colin.wilmott@ntu.ac.uk

Abstract. The class of quantum codes called stabilizer codes is increasingly well-understood. The premise of the stabilizer formalism is that a quantum code can be efficiently described by a subgroup of its error group, and, interestingly, the stabilizer formalism permits correspondences with classical linear codes. In this paper, we examine one such correspondence, and we shall use this to establish the number of distinct stabilizer codes that exist for a fixed parametrisation.

1. Introduction

Coding theory is a branch of mathematics which seeks optimal solutions to problems concerning the safe and accurate transfer of information. Shannon (1948) established the topic of coding theory with his seminal paper on the mathematics of communication. Hamming (1950) then introduced the concept of an error-correcting codes with his work on the correction of errors on magnetic storage media. In the intervening decades, our society has become phenomenally technology-orientated and coding theory has played a prominent role in this change.

In recent years, coding theory has evolved beyond its original classical setting and is considered within a quantum theoretical perspective. Quantum stabilizer codes were introduced independently by Gottesman (1997) and Calderbank *et al* (1998), and rank among the most widely studied of all quantum error-correcting codes. The premise of the stabilizer formalism is that a quantum code can be described by a subgroup of its error group, and it is this subgroup which we refer to as the stabilizer of a quantum code. In this paper, we shall provide a brief overview of the stabilizer formalism before establishing the number of distinct stabilizer codes for a fixed parametrisation.

2. Preliminaries

Consider a d-dimensional Hilbert space $\mathbb{C}^d$ and fix each orthonormal basis state of the space to correspond to an element of ring $\mathbb{Z}_d$ of integers modulo d. As such, we have the basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \subset \mathbb{C}^d$ which we call the computational basis whose elements correspond to the column vectors of the identity matrix $\mathbb{I}_d$. A qudit is a d-dimensional quantum state $|\psi\rangle \in \mathbb{C}^d$ which can be written as $|\psi\rangle = \sum_{i=0}^{d-1} \alpha_i |i\rangle$, where $\alpha_i \in \mathbb{C}$ and $\sum_{i=0}^{d-1} |\alpha_i|^2 = 1$. The state space of an n-qudit is formed by taking the n-fold tensor product of the principal space $\mathbb{C}^d$, $(\mathbb{C}^d)^{\otimes n}$, which, correspondingly, possesses a set of orthonormal basis states that can given by $|i_1\rangle \otimes |i_2\rangle \otimes \cdots \otimes |i_n\rangle = |i_1 i_2 \ldots i_n\rangle$ for $i_j \in \mathbb{Z}_d$. The general state of a qudit in the n-fold space $\mathbb{C}^{d^n}$ is

$$|\psi\rangle = \sum_{(i_1 i_2 \ldots i_n) \in \mathbb{Z}_d^n} \alpha_{(i_1 i_2 \ldots i_n)} |i_1 i_2 \ldots i_n\rangle , \tag{1}$$

where $\alpha_{(i_1 i_2 \ldots i_n)} \in \mathbb{C}$ and $\sum |\alpha_{(i_1 i_2 \ldots i_n)}|^2 = 1$.

A basis for the set of bounded operators acting on $\mathbb{C}^d$ is given by the set of well-known generalised Pauli matrices $\mathcal{E} = \{X_i Z_j \mid (i,j) \in \mathbb{Z}_d \times \mathbb{Z}_d\}$. Any error E acting on a qudit state can be written as a linear combination of the generalised Pauli matrices. The generalised Pauli group, or error group, $\mathcal{G}$ is a group of order d^4 generated by $\mathcal{E}$ and τI with center $\zeta(\mathcal{G}) = \langle \tau I \rangle$. For an n-qudit system, any element $E_{i,j}$ of $\mathcal{G}^n$ may be written as $E_{i,j} = \tau^{\alpha}(X_{i_1} Z_{j_1}) \otimes (X_{i_2} Z_{j_2}) \otimes \cdots \otimes (X_{i_n} Z_{j_n})$ where $\alpha \in \mathbb{Z}_d$ and $((i_1, j_1), (i_2, j_2), \ldots, (i_n, j_n)) \in \mathbb{Z}_d^n \times \mathbb{Z}_d^n$. Since the group $\mathcal{G}^n / \langle \tau I \rangle$ is isomorphic to vector space $\mathbb{F}_d^{2n}$ with order d^{2n}, this allows us to write a correspondence between $\mathcal{G}^n / \langle \tau I \rangle$ and $\mathbb{F}_d^{2n}$ as

$$\begin{aligned} E_{ij} &= \otimes_{z=1}^n X_{i_z} \cdot \otimes_{z=1}^n Z_{j_z} \\ &\equiv (i_1, i_2, \ldots, i_n | j_1, j_2, \cdots, j_n) = (i|j). \end{aligned} \tag{2}$$

A quantum code consists of an encoding function e from the Hilbert space $(\mathbb{C}^d)^{\otimes k}$ to the Hilbert space $(\mathbb{C}^d)^{\otimes n} \equiv \mathbb{C}^{d^n}$, e: $\mathbb{C}^{d^k} \to \mathbb{C}^{d^n}$ where k and n are integers and $k < n$. In a manner similar to the classical case, we define the codewords of a quantum code to be those states contained in the image of e, Im(e). The length of the code is given by n while k denotes the number of encoded message qudits of the code. The extra $n - k$ qudits introduce additional information that allows the encoded qudits to be stored in a redundant manner which can then be later used to detect transmission errors. A code $\mathcal{Q}$ is a quantum $[\![n, k]\!]_d$ code over $\mathbb{C}^d$ if it is a subspace of dimension d^k in $\mathbb{C}^{d^n}$. For our purposes, it is not necessary to introduce minimum distance.

3. Stabilizer Codes

Let $\mathcal{Q}$ be a quantum error correcting code. The stabilizer $\mathcal{S}$ of $\mathcal{Q}$ is a formalism that describes a quantum code in terms of error operators acting on $\mathcal{G}^n$. More precisely, the stabilizer of $\mathcal{Q}$ is defined to be a set of operators $\mathcal{M} \in \mathcal{S}$ of $\mathcal{G}^n$ for which the condition

$$\mathcal{M} |\psi\rangle = |\psi\rangle \tag{3}$$

is satisfied for all codewords $|\psi\rangle$ (Gottesman 1997). Thus, the stabilizer maintains a common +1-eigenspace of codespace $\mathcal{Q}$. Stabilizer codes themselves were originally considered over dimension two, and in this situation, errors are said to either commute or anti-commute with a codeword. It is exactly this property that helps stabilizer codes elicit a relatively straight-forward error detection procedure. In particular, the set of all operators that commute with the stabilizer is called the centralizer. Error detection is then explained by the fact that any error which lies outside of the centralizer necessarily anti-commutes with some elements of the stabilizer. Note that since stabilizer codes were initially based on qubit systems, the stabilizer is necessarily an Abelian subgroup while the centralizer is referred to as the normalizer of the group. We shall however be considering more general systems based on qudits.

Definition 1 *A stabilizer code $\mathcal{Q}$ is a subspace of $\mathbb{C}^{d^n}$ that satisfies the relation*

$$\mathcal{Q} = \bigcap_{\mathcal{M} \in \mathcal{S}} \{|\psi\rangle \in \mathbb{C}^{d^n} \mid \mathcal{M} |\psi\rangle = |\psi\rangle\} \tag{4}$$

for some subgroup $\mathcal{S}$ of $\mathcal{G}^n$.

The above definition is a generalisation of the usual definition of stabilizer codes based on qubits. Since $\mathcal{S}$ describes the set of operators that leave each state in the quantum code invariant, $\mathcal{S}$ is therefore said to stabilize the code $\mathcal{Q}$.

4. Stabilizer Equivalence

4.1. A classical coding problem

In classical coding theory, an interesting problem is to determine the number of different generator bases that can be constructed for a linear code for fixed parameters. We will concern ourselves with this problem before asking if a comparable statement can be made for stabilizer codes — these being quantum analogue of linear classical codes.

Let F be a field. A classical code $\mathcal{C}$ of length n is a linear code if and only if $\mathcal{C}$ is a subspace of the vector space F^n. If $\mathcal{C}$ has dimension k over F, then we say that $\mathcal{C}$ is an $[n,k]$ linear code over F. Therefore, $\mathcal{C}$ can be specified by a basis consisting of a minimal set of vectors $v_1, v_2, \ldots, v_k$ such that $\mathcal{C} = \{\sum_{i=1}^{k} \alpha_i v_i \mid \alpha_i \in F\}$. Setting $F = \mathbb{F}_2$, we have the following.

Theorem 1 *(Hoffman et al 1991) A binary linear code of dimension k has precisely*

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i)$$

different generator bases.

4.2. A quantum coding problem

Motivated by theorem 1, let us now consider the problem of determining the number distinct $[\![n,k]\!]_d$ stabilizer codes for fixed n, k and d. We have the following.

Theorem 2 *The number of stabilizer sets in the Hilbert space $\mathbb{C}^{d^n}$ that maintain a +1-eigenspace of dimension d^k is given by*

$$d^{\frac{n-k-1(n-k)}{2}}\prod_{i=0}^{n-k-1}\Big(d^{2(n-i)}-1\Big).$$

Proof. The error group associated with an n-qudit system is the n-fold product $\mathcal{G}^n = \{E_{ij} \mid (i,j) \in \mathbb{Z}_d^n \times \mathbb{Z}_d^n\}$. To count the number of elements within $\mathcal{G}^n$ that maintain a +1-eigenspace, note that the first such element $\mathcal{M}'_1$ can be chosen in $d^{2n}-1$ ways. Let $\mathcal{M}'_2$ be another element of $\mathcal{G}^n$ that commutes with $\mathcal{M}'_1$ but is independent from $\mathcal{M}'_1$. Then it can be shown that there exists an $N'_2 \in \mathcal{G}^n$ that commutes with $\mathcal{M}'_1$ but fails to commute with $\mathcal{M}'_2$ (Gottesman 1997). Hence, M'_2 maintains the +1-eigenspace of $\mathcal{M}'_1$. Thus, the number of choices for $\mathcal{M}'_2$ that maintain a +1-eigenspace with $\mathcal{M}'_1$ is $\frac{d^{2n}}{d} - d$. In a similar fashion, we note that for $\mathcal{M}'_l \neq \{\mathcal{M}'_1, \mathcal{M}'_2, \ldots, \mathcal{M}'_{l-1}\}$, a suitable N'_l can be found such that N'_l commutes with $\mathcal{M}'_1, \mathcal{M}'_2, \ldots, \mathcal{M}'_{l-1}$ but does not commute with $\mathcal{M}'_l$. Hence, the number of choices for $\mathcal{M}'_l$ that preserve the +1-eigenspace of the set $\{\mathcal{M}'_i\}$, $i = 1, \ldots, l-1$, is $\frac{d^{2n}}{d^{l-1}} - d^{l-1}$. Therefore, the total number of ways of choosing $n-k$ stabilizers $\mathcal{M}'_i$ for a code $\mathcal{Q}$ is given as

$$\begin{aligned}\prod_{i=0}^{n-k-1}\left(\frac{d^{2n}}{d^i} - d^i\right) &= d^{\sum_{i=0}^{n-k-1} i}\prod_{i=0}^{n-k-1}\Big(d^{2(n-i)}-1\Big) \\ &= d^{\frac{n-k-1(n-k)}{2}}\prod_{i=0}^{n-k-1}\Big(d^{2(n-i)}-1\Big). \qquad (5)\end{aligned}$$

Theorem 3 *An $[\![n,k]\!]_d$ stabilizer code $\mathcal{Q}$ has precisely*

$$d^{\frac{(n-k-1)(n-k)}{2}}\prod_{i=0}^{n-k-1}(d^{(n-i)}-1) \qquad (6)$$

possible choices for stabilizer sets which maintain its +1-eigenspace.

Proof. The codewords associated with a stabilizer code $\mathcal{Q}$ are given by

$$|\overline{c_1 \dots c_k}\rangle = \overline{X}_1^{c_1} \dots \overline{X}_k^{c_k} \frac{1}{|\mathcal{S}|} \sum_{\mathcal{M} \in \mathcal{S}} \mathcal{M} \, |00 \dots 0\rangle \tag{7}$$

(Gottesman 1997). As the stabilizer code of dimension d^k is defined in terms of a +1-eigenspace $\mathcal{S}$, there are d^{n-k} stabilizer elements that satisfy this definition in a non-trivial manner. There are a further d^k elements associated with the logical encoding process $\bar{X}$ and, thus, there are a total of d^n elements to choose from in order to maintain the code's +1-eigenspace. Counting the numbers of ways that the stabilizer elements $\mathcal{M}_i, i = 1, \dots, n-k$, can be chosen for a particular stabilizer code, we note there are $d^n - 1$ non-trivial choices that can be made for the first stabilizer $\mathcal{M}_1$. $\mathcal{M}_2$ can then chosen independently in $d^n - d$ ways, followed by $d^n - d^2$ choices for $\mathcal{M}_3$. In particular, $\mathcal{M}_l$ can be chosen to preserve the +1-eigenspace of $\mathcal{Q}$ in $d^n - d^{l-1}$ ways. Since we require $n-k$ stabilizers in total, there are

$$\begin{aligned} \prod_{i=0}^{n-k-1} \left(d^n - d^i\right) &= d^{\sum_{i=0}^{n-k-1} i} \prod_{i=0}^{n-k-1} \left(d^{(n-i)} - 1\right) \\ &= d^{\frac{(n-k-1)(n-k)}{2}} \prod_{i=0}^{n-k-1} \left(d^{(n-i)} - 1\right) \end{aligned} \tag{8}$$

choices for elements $\mathcal{M}_i \in \mathcal{S}$ that maintain the +1-eigenspace of $\mathcal{Q}$.

For fixed parameters n and k and d, we can now establish the number of distinct $[\![n,k]\!]_d$ stabilizer codes within $\mathbb{C}^{d^n}$.

Theorem 4 *The number of distinct $[\![n,k]\!]_d$ stabilizer codes over $\mathbb{C}^{d^n}$ is*

$$\prod_{i=0}^{n-k-1} (d^{(n-i)} + 1).$$

Proof. The quotient obtained from equations (5) and (8) is given by

$$\prod_{i=0}^{n-k-1} \left(\frac{d^{\frac{n-k-1(n-k)}{2}} d^{2(n-i)} - 1}{d^{\frac{n-k-1(n-k)}{2}} d^{(n-i)} - 1} \right) = \prod_{i=0}^{n-k-1} \left(d^{(n-i)} + 1\right) \tag{9}$$

and the result now follows.

References

Calderbank A R, Rains E M, Shor P W and Sloane N J A 1998 Quantum Error Correction via Codes over GF(4) *IEEE Trans. Inform. Theory* **44** pp 1369-87

Gottesman D 1997 Stabilizer Codes and Quantum Error Correction *Ph.D. Thesis Calif. Inst. Tech. Pasadena CA*

Hamming R W 1950 Error Detecting and Error Correcting Codes *Bell System Technical Journal* **29** pp 147-60

Hoffman D G, Leonard D A, Lidner C C, Phelps A T, Rodger C A and Wall J R 1991 *Coding Theory: The Essentials* (Marcel Dekker) p X

Shannon C E 1948 A Mathematical Theory of Communication *Bell System Technical Journal* **27** pp 379-423