A physics-free introduction to quantum error correcting codes

William J. Martin

Department of Mathematical Sciences
and
Department of Computer Science
Worcester Polytechnic Institute
Worcester, Massachusetts, USA 01609
martin@wpi.edu

Abstract. Research in the field of quantum algorithms and quantum error correction is progressing at an astounding rate. There are many good papers on both subjects, but reading even a few of these may seem a daunting task to the newcomer.
The aim of this paper is to give a leisurely introduction to the basic theory of quantum error correcting codes without appealing to even the most basic notions in physics. Thus the article is not a substitute for important papers such as [12] or [7] but rather an advertisement for them. I would be pleased if, in addition, some readers view this as a useful companion article if and when they go on to read more substantial literature on the subject of quantum error correction.
I present nothing new here. Rather, I give an elementary account of the important theorems and proofs which appear in these fundamental works using only undergraduate algebra and a bit of classical coding theory. In particular, I give a full proof of the Knill/Laflamme theorem as well as an elementary treatment of stabilizer codes. The goal is to make the literature dealing with this exciting new area more accessible to discrete mathematicians.

1 This paper is not about quantum mechanics

What is quantum mechanics? I cannot answer that; the reader should consult an expert. Because this essay is aimed at readers with little physics background — and because I am not an authority on quantum mechanics — I am determined to avoid any discussion of physics in this essay. It is assumed that the reader has been exposed to the concept of quantum computing and can put the abstractions discussed here in a physical context if they so desire.

It is by no means my intent to imply that physics is irrelevant to quantum error correction. It's **all** about physics and the serious researcher needs to read the literature on the subject. Instead, I aim to isolate that fragment of the theory which is both introductory and explainable in purely mathematical terms. Fortunately, we can cover quite a lot using only undergraduate algebra and basic (classical) coding theory. I have chosen the notation of standard linear algebra over the "bra" and "ket" of Dirac. I have avoided the computation of non-zero probabilities, thus eliminating the need for unit vectors. Quantum states are treated as points in complex projective space, although I never make any concrete use of this language. All of this is designed to make the core ideas accessible to an audience more comfortable with discrete mathematics than with physics.

2 Qubits and quantum registers

We will define a *qubit* as a two-dimensional complex vector space with a pre-specified orthonormal basis, which we will denote $\{\underline{0}, \underline{1}\}$. A *qubit in state* x consists of an ordered pair (A, x) where A is a qubit and x is any vector in A. Many authors include the restriction $||x|| = 1$, but we shall not. Every state x is a linear combination of $\underline{0}$ and $\underline{1}$.

Fig. 1. A qubit is a two-dimensional complex vector space.

We are interested in the space of linear operators (i.e., 2×2 matrices) acting on the qubit A. Each such operator can be uniquely expressed as a linear combination of the following four matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Proposition 1. *The set $\mathcal{P} = \{\pm I, \pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}$ forms a group. This group is isomorphic to the dihedral group D_4.*

The matrices in $\mathcal{P}$ are called *Pauli matrices*. (Be warned that some authors extend this term to matrices iP, $P \in \mathcal{P}$.)

Here is the basic idea of this paper. We have a collection of qubits. These are subject to some "noise". For example, the noise might act on each qubit as a linear operator. We must restrict the allowable configurations of qubits so as to be able to detect and remove (invert) any noise which is sufficiently small. We try to do this by expressing the noise on each qubit as a linear combination of Pauli matrices. What I have just said is terribly imprecise. One shortcoming is that the qubits must be allowed to interact, or become "entangled" in some way. So let us first create an algebraic object which accounts for this.

An *n-qubit quantum register* is a 2^n-dimensional complex vector space A together with a distinguished orthonormal basis $\mathcal{B}$. The basis elements — called the "computational basis states" — are indexed by binary n-tuples a:

$$\mathcal{B} = \{\underline{a} : a \in \mathbb{Z}_2^n\}. \tag{1}$$

Obviously, A can be written

$$A \cong \mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2,$$

i.e., as a tensor product of n qubits, In fact, we can assume that this has been done in such a way that

$$\underline{a} = \bigotimes_{i=1}^{n} \underline{a_i}.$$

An *n-qubit quantum register in state x* consists of an ordered pair (A, x) where A is an n-qubit quantum register and x is any vector in A. Of course, x need not be expressible as a tensor product of vectors in $\mathbb{C}^2$. For a function $f : A \to A$, we will freely use terminology such as "f applied to A in state x leaves A in state y" where $y = f(x)$.

3 Very little about quantum computing

It is beyond the scope of our discussion to give a fully accurate treatment of quantum computation. What I give here is a bit of a lie. It is a slightly distorted description of a quantum algorithm which is just enough for our purposes; namely to prove that error-correction algorithms actually exist. There will be two significant omissions in my description of a quantum algorithm. First, I will say that any unitary operator can be applied to a register without regard to the physical task of constructing such operators in polynomial time. Second, I will all but remove the probability issues from my definition of a measurement. Anyone who seeks a more accurate treatment is encouraged to read [13], [5] or any of the other fine references on quantum computation. Fortunately, this muted treatment will suffice for our needs.

A *quantum algorithm* begins with a quantum register A in an unknown state $x \neq 0$ — perhaps together with some classical information such as bases for some special subspaces of A (which do not depend on x) — and consists of a finite sequence of steps, each of which is of one of the following two types:

1. we may apply any unitary operator to A. Such a step returns no information;
2. we may perform a *measurement*, defined as follows:
   - we specify an orthogonal decomposition

     $$A = A_1 \oplus \cdots \oplus A_r$$

     of A. The current state of the register x may be orthogonal to some A_i's and not to others;
   - An oracle chooses a random index i ($1 \leq i \leq r$). All we will say about this probability distribution [1] is that the probability that an index i is chosen is zero if and only if x is orthogonal to A_i;
   - The state changes from x to $P_i x$ where P_i denotes orthogonal projection onto A_i. Note that $P_i x \neq 0$;
   - The only information we glean from this measurement is that we are told the value of i.

   Our notation for such a measurement will be

   $$\mathcal{M} = \{A_1, \ldots, A_r\}.$$

[1] I do not mean to sound mysterious. The probability of choosing i is $\frac{\|x_i\|^2}{\|x\|^2}$. But we will not use this formula.

Many authors are more careful and only allow measurements in which each A_i admits a basis of computational basis states. The equivalence between the two approaches is obtained by applying U, then measuring, then applying $U^\dagger$ for some unitary matrix U. So the issue of efficiently constructing such U arises again here.

Note that branching is permitted. Our choice of what to do in step k can depend not only on the initial information but also on the information obtained in any measurements among steps $1, \ldots, k-1$. But it cannot depend (directly) on those steps in which unitary operators are applied, for in those steps no information is returned.

We now give a very elementary example of a quantum algorithm. Suppose we begin with a register A in an unknown state $x \neq 0$. We wish to apply an algorithm which leaves A in state $\alpha\underline{0}$ for some non-zero scalar α. First, we perform the measurement

$$\mathcal{M} = \{\mathsf{span}(\underline{a}) : a \in \mathbb{Z}_2^n\}$$

consisting of the coordinate axes. This measurement projects x onto one of the coordinate axes. We are guaranteed that the projection, $\alpha\underline{b}$ say, is non-zero and the value of b is returned by the measurement. Next, we apply the unitary transformation

$$U = \bigotimes_{i=1}^{n} \sigma_x^{b_i}$$

which acts on the standard basis as mod-2 addition of the binary vector b:

$$U\underline{c} = \underline{c+b} \qquad (c \in \mathbb{Z}_2^n)\,.$$

This clearly achieves the desired result.

Many authors writing about quantum algorithms assume that the initial state of the register is fully controllable, up to multiplication by a non-zero scalar. With a slight modification, the above algorithm justifies this assumption.

Two more remarks are in order before we leave the subject of quantum algorithms. First, at the physical level, the only measurements allowed are those in which each of the subspaces A_i admits a basis of elementary basis vectors: $A_i = \mathsf{span}(\underline{a} : \underline{a} \in S_i \subseteq \mathcal{B})$. Our definition of a measurement (which is taken from [5]) is no more general since any measurement of this type is "conjugate" under the unitary group to one of the restricted type.

Using the language of "superoperators", one can argue that every quantum algorithm is equivalent to a quantum algorithm with essentially one step. Thus one may read that a quantum algorithm amounts to a three-part process: (i) expand the quantum register A by adding ancilla qubits to

obtain $A' = A \otimes A_1$ where A_1 is another quantum register (consequently, so also is A'); (ii) apply a single unitary operator; and (iii) measure all the qubits in A_1 (i.e., the measurement contains one projector for each elementary basis vector in A_1). This is terribly vague, especially since I have not defined a superoperator. We will not use this idea anywhere in this paper. I include this comment mainly to make the reader aware of alternative language that appears in the literature.

4 The error group

Let n be a positive integer. We assume that each error operates linearly on $\mathbb{C}^{2^n}$. That is, an error can be viewed as a $2^n \times 2^n$ matrix with complex entries. We first consider errors of a very special type. Consider the set $\mathcal{E}$ consisting of all tensor products

$$E = s_1 \otimes s_2 \otimes \cdots \otimes s_n \tag{2}$$

where each s_i is a Pauli matrix:

$$s_i \in \mathcal{P} = \{\pm I, \pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}.$$

Recall that tensor products can be multiplied component-by-component:

$$(M \otimes N)(R \otimes S) = (MR) \otimes (NS).$$

Thus, since $\mathcal{P}$ forms a group, so does $\mathcal{E}$. This is called the *error group*. We can collect all powers of -1 at the front of any such product and write

$$\mathcal{E} = \{\pm s_1 \otimes \cdots \otimes s_n : s_i \in \{I, \sigma_x, \sigma_y, \sigma_z\}\}. \tag{3}$$

Clearly, $|\mathcal{E}| = 2 \cdot 4^n = 2^{1+2n}$. Define the *weight* of $E \in \mathcal{E}$ as the number of non-identity components:

$$\mathsf{wt}(E) = |\{j : s_j \neq I\}|.$$

It is easy to see that there are $2\binom{n}{t}3^t$ matrices of weight t in $\mathcal{E}$.

The next step is to index the elements of $\mathcal{E}$ by binary $(2n+1)$-tuples. Since $\sigma_y = \sigma_x\sigma_z$, any matrix of the form (2) where $s_i \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ can be written uniquely as

$$E = \left(\bigotimes_{i=1}^{n} \sigma_x^{a_i}\right) \cdot \left(\bigotimes_{i=1}^{n} \sigma_z^{b_i}\right)$$

where a and b are 01-vectors of length n. We abbreviate this by writing

$$E = X(a)Z(b) \tag{4}$$

where

$$X(a) = \sigma_x^{a_1} \otimes \cdots \otimes \sigma_x^{a_n}$$

and similarly for $Z(b)$. Thus

$$\mathcal{E} = \{\pm X(a)Z(b) : a, b \in \mathbb{Z}_2^n\}$$

where there is a slight abuse of notation in viewing $\mathbb{Z}_2$ as consisting of $\{0, 1\}$. So there is a one-to-one correspondence between matrices $\pm X(a)Z(b)$ in $\mathcal{E}$ and signed binary $2n$-tuples $\pm(a|b)$.

Lemma 1. *Any two elements of $\mathcal{E}$ either commute or anti-commute. More precisely, if $E = \pm X(a)Z(b)$ and $E' = \pm X(a')Z(b')$, then*

$$EE' = \begin{cases} E'E, & \text{if } \langle (a|b), (a'|b') \rangle = 0; \\ -E'E, & \text{if } \langle (a|b), (a'|b') \rangle = 1 \end{cases} \tag{5}$$

where $\langle \cdot, \cdot \rangle$ is the binary inner product

$$\langle (a|b), (a'|b') \rangle = \sum_{i=1}^{n} a_i b_i' + \sum_{i=1}^{n} a_i' b_i \pmod 2. \tag{6}$$

If $\cdot$ denotes the ordinary dot product on $\mathbb{Z}_2^n$, then the inner product $a \cdot b' + a' \cdot b$ is a binary symplectic inner product since it is represented by an anti-symmetric bilinear form over $\mathbb{Z}_2$.

Proof. We have

$$\sigma_x^2 = I, \qquad \sigma_z^2 = I, \qquad \sigma_x \sigma_z = -\sigma_z \sigma_x.$$

Suppose $E = X(a)Z(b)$ and $E' = X(a')Z(b')$. Observe that $Z(b')X(a) = (-1)^{a \cdot b'} X(a)Z(b')$ and $Z(b)X(a') = (-1)^{a' \cdot b} X(a')Z(b)$. Thus

$$\begin{aligned} E'E &= X(a')Z(b')X(a)Z(b) \\ &= (-1)^{a \cdot b'} X(a')X(a)Z(b')Z(b) \\ &= (-1)^{a \cdot b'} X(a)X(a')Z(b)Z(b') \\ &= (-1)^{a \cdot b' + a' \cdot b} X(a)Z(b)X(a')Z(b') \\ &= (-1)^{a \cdot b' + a' \cdot b} EE'. \square \end{aligned}$$

A *binary code* is simply a non-empty subset of $\mathbb{Z}_2^m$ for some m. A binary code C is *additive* if C is a subgroup of $\mathbb{Z}_2^m$. Suppose we are given an inner product $\langle \cdot, \cdot \rangle$ on $\mathbb{Z}_2^m$. If C is a subgroup of this binary space, then C has a *dual code* $C^\perp$ given by

$$C^\perp = \{a \in \mathbb{Z}_2^m : \langle a, c \rangle = 0 \text{ for all } \ c \in C\}.$$

An additive binary code is *self-orthogonal* if $C \subseteq C^{\perp}$.

Now if $\mathcal{G}$ is a subgroup of the error group $\mathcal{E}$, then the set

$$\{(a|b) : X(a)Z(b) \in \mathcal{G} \quad \text{or} \quad -X(a)Z(b) \in \mathcal{G}\}$$

is a binary additive code. Conversely, for any binary additive code C, we obtain a subgroup

$$\{\pm X(a)Z(b) : (a|b) \in C\}\,.$$

Corollary 1. *A subgroup $\mathcal{G}$ of $\mathcal{E}$ is abelian if and only if the corresponding binary code is self-orthogonal under the symplectic inner product.*

We will later be interested in finding abelian subgroups of $\mathcal{E}$. So let us toy with this question before we get deeper into the application. Two obvious abelian subgroups are

$$\{X(a) : a \in \mathbb{Z}_2^n\}$$

and

$$\{Z(b) : b \in \mathbb{Z}_2^n\}.$$

But these are not terribly interesting. Here is a more interesting class of examples. Let C_1 be any additive binary code of length n with generator matrix G_1. Let C_2 be an additive subcode of its dual $C_1^{\perp}$ and suppose G_2 is a generator matrix for C_2. Let C be the rowspace over $\mathbb{Z}_2$ of the matrix

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}.$$

Then it is easy to check that C is self-orthogonal under $\langle \cdot, \cdot \rangle$. Thus the set

$$\mathcal{G} = \{\pm X(a)Z(b) : (a|b) \in C\}$$

is an abelian subgroup of $\mathcal{E}$.

For such a partitioned binary vector $(a|b)$, let $wt(a|b)$ denote the number of indices i for which $a_i \neq 0$ or $b_i \neq 0$. Steane observes that this is the Hamming weight of the bitwise OR of a and b. For our purposes, this number $wt(a|b)$ will be called the *weight* of $(a|b)$. We will see later that the parameter

$$\min\{wt(a|b) : (a|b) \in C^{\perp} - C\}$$

for binary codes $C \leq \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ self-orthogonal under $\langle \cdot, \cdot \rangle$ corresponds to the error detection abilities of a quantum code associated to C. This beautiful connection between symplectic geometry and subgroups of the unitary group is explored in [7] (in the context of quantum error correction) and in [6] (in relation to codes over $\mathbb{Z}_4$). These are recommended reading.

Let me finish this section with one concrete example of an abelian subgroup of $\mathcal{E}$ which is not of the above type. Let $n = 2$ and consider $C = \{(00|00), (10|10), (01|01), (11|11)\}$. This is a self-orthogonal code with respect to the symplectic inner product and the corresponding abelian subgroup of $\mathcal{E}$ is

$$\mathcal{G} = \left\{ \pm \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \right.$$

$$\left. \pm \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}.$$

5 Error models

We have a quantum register A and a state vector $x \in A$ which we wish to protect against errors. An error is any linear operator on A. Fortunately, physicists assure us that some errors are more likely to occur than others. In fact, we can assume that many $2^n \times 2^n$ matrices M **never** occur as errors. In the next section, I will explain why mathematicians working on quantum error correction can usually work under the following absurd error model:

- any error acts on each qubit as a Pauli matrix. Hence the error operator belongs to the error group $\mathcal{E}$;
- there is some integer t such that errors having weight exceeding t do not occur.

A more reasonable error model is the following:

- errors occur independently on different qubits;
- the probability of experiencing any error occurring on a given qubit is bounded above by $\epsilon \approx 0$;
- the error acts on any given qubit as a 2×2 matrix over $\mathbb{C}$.

The first two conditions guarantee that the probability of an error occurring which simultaneously affects k qubits decays as $O(\epsilon^k)$. Thus, given some tolerance for undetected/uncorrected error, we may ignore all errors

$$E = s_1 \otimes \cdots \otimes s_n, \qquad (s_i \in \mathsf{Mat}_2(\mathbb{C}))$$

having weight greater than t for some integer t. The independence assumption allows to concern ourselves only with errors which can be expressed as tensor products. But this is not realistic.

Let us say that an error $E \in \mathsf{Mat}_{2^n}(\mathbb{C})$ *does not affect* the first qubit if E can be expressed as a tensor product $E = I_2 \otimes E'$ where E' is a $2^{n-1} \times 2^{n-1}$ complex matrix. Otherwise E *affects* the first qubit. With simple relabeling, this definition extends to any qubit. Here is my final attempt at a reasonable, but physics-free error model:

- any error acts as a linear operator on $\mathbb{C}^{2^n}$;
- there is some $\epsilon > 0$ such that the probability of seeing an error affecting k qubits diminishes as $O(\epsilon^k)$.

This model allows for correlated errors provided the probability of occurrence of errors affecting large numbers of qubits is negligible. In the next section, we will state and prove the Knill/Laflamme theorem. An important consequence of this theorem is the fact that a code which corrects errors under the first error model also works well under this error model.

6 Detecting and correcting errors

A *quantum code* is simply a non-trivial subspace Q of some quantum register. We are interested in finding such Q which allow us (via the use of quantum algorithms) to detect and correct certain types of errors. We begin by defining a detectable error.

Two vectors $x, y \in \mathbb{C}^m$ are distinguishable — with certainty — by a measurement if and only if they are orthogonal. Alexei Ashikhmin once lectured on quantum codes using this as an axiom thus eliminating the need to define "measurement". Ashikhmin also showed me the following idea.

Definition 1. *Let A denote a quantum register. Let Q be a subspace of A and let E be a $2^n \times 2^n$ matrix. We say E is* **detectable** *(relative to Q) provided, for all $x, y \in Q$, if $x \perp y$, then $x \perp Ey$.*

Let me briefly explain why this definition is justified and why it is not a theorem. If the register is in initial state $y \in Q$ and matrix E is applied to arrive at the state Ey, we may apply the measurement $\{Q, Q^\perp\}$. If the measurement leaves the register in some state in $Q^\perp$, then we know $Ey \notin Q$ and we have detected an error. Otherwise, we know that the measurement has projected the vector Ey — via the matrix Π_Q which denotes orthogonal projection onto Q — back into Q (or it has left $Ey \in Q$ fixed). The hypothesis $Ey \perp x$ for all $x \in Q$ with $x \perp y$ now guarantees that $\Pi_Q Ey$ is a non-zero multiple of y. In summary, an error is detectable in this sense if there exists a measurement which either restores the initial state (up to multiplication by a scalar) or tells us that some error has occurred.

Let me remark that I allow the state to vary over all of the ambient space. Many papers on quantum computing insist that — at all times — the state is a unit vector. (This is useful for probability calculations.) However, the physicist really works in complex projective space when she does quantum mechanics. So any non-zero multiple of $y \in Q$ is just as good as y itself.

We now explain what we mean by error correction. By definition, we say that *the all-zero matrix is a correctable error.* (This definition is due to Emmanuel Knill who assures me that the zero matrix will never arise as an error in practical systems.) Let Q be a non-trivial subspace of A and let $\mathcal{T}$ be any set of $2^n \times 2^n$ matrices. We say that Q *allows correction* of all errors in $\mathcal{T}$ provided there is a quantum algorithm which — when applied to A in state Ex where E is any non-zero matrix in $\mathcal{T}$ and x is any vector in Q — will leave the quantum register in state αx for some non-zero complex number α. Note that neither E nor x is known, nor will we expect the algorithm to determine either of them.

7 The error correction algorithm

In this section, we present the most important theorem in quantum error correction. The theorem characterizes correctable sets of errors. As sometimes happens with important results, attribution is a tricky business. In 1995, Peter Shor [17] demsonstrated that quantum error correction is possible. Essentially the same result was obtained by Bennett, *et al.* [4], but in a very different language. Meanwhile, Ekert and Macchiavello [9] independently made fundamental discoveries as well. Yet it was not immediately clear what kind of error sets could be handled by an error correction algorithm. In 1995, Manny Knill and Raymond Laflamme [12] gave a simple characterization of sets $\mathcal{T}$ of correctable errors. Our treatment is based on their paper. The proof necessarily includes a quantum algorithm. We begin with a simple but beautiful lemma from geometry.

Lemma 2. *Suppose* $\{y_i : i \in I\}$ *and* $\{z_i : i \in I\}$ *are sets of vectors in* $\mathbb{C}^m$ *such that for all* $i, j \in I$*,*

$$\langle y_i, y_j \rangle = \langle z_i, z_j \rangle.$$

Then there exists a unitary matrix M *such that* $My_i = z_i$ *for all* $i \in I$*.*

In the statement and proof of the next theorem, we will find it convenient to define

$$\mathcal{T}^\dagger \mathcal{T} = \{E^\dagger E' : E, E' \in \mathcal{T}\}.$$

I should warn the reader that the proof consumes the next five pages.

Theorem 1 (Knill and Laflamme [12]; compare Bennett, *et al.* [4]). *Let Q be a subspace of an n-qubit quantum register A having dimension at least three and let $\mathcal{T}$ be any set of $2^n \times 2^n$ matrices. Then the following are equivalent:*

(i) *Q allows correction of all errors in $\mathcal{T}$;*
(ii) *all errors in $\mathcal{T}^\dagger\mathcal{T}$ are detectable relative to Q;*
(iii) *for all E and E' in $\mathcal{T}$, for all x, y in Q, if x is orthogonal to y, then Ex is orthogonal to $E'y$;*
(iv) *for all E and E' in $\mathcal{T}$, there exists a constant $\lambda_{(E,E')}$ such that, for all $x \in Q$,*

$$\langle Ex, E'x\rangle = \lambda_{(E,E')}||x||^2; \tag{7}$$

(v) *for each E in $\mathcal{T}^\dagger\mathcal{T}$, there exists a constant λ_E such that*

$$\Pi_Q E \Pi_Q = \lambda_E \Pi_Q$$

where Π_Q denotes orthogonal projection of A onto Q.

Proof. The equivalence of **(ii)** and **(iii)** follows immediately from our definition of detectable. The proof will proceed by showing the equivalence of **(iii)** and each of the remaining statements.

Let us first establish the equivalence of **(iii)** and **(iv)**. Suppose first that **(iii)** holds. Consider matrices $E, E' \in \mathcal{T}$ and two orthogonal unit vectors x and y in Q. Then $x + y$ is orthogonal to $x - y$ and **(iii)** gives $E(x+y) \perp E'(x-y)$. We have

$$0 = (x+y)^\dagger E^\dagger E'(x-y) = x^\dagger E^\dagger E'x - x^\dagger E^\dagger E'y + y^\dagger E^\dagger E'x - y^\dagger E^\dagger E'y.$$

Now since $x \perp y$, we have $Ex \perp E'y$ and $Ey \perp E'x$ and the middle terms vanish giving

$$x^\dagger E^\dagger E'x = y^\dagger E^\dagger E'y.$$

Now since $\dim Q \geq 3$, the orthogonality relation is a connected relation on Q. Thus, for fixed E and E', the product $\langle Ex, E'x\rangle$ is constant over all unit vectors $x \in Q$.

Next, assume that **(iv)** holds. Then, for $E \in \mathcal{T}^\dagger\mathcal{T}$, there exists a scalar λ_E such that $x^\dagger Ex = \lambda_E$ for all unit vectors $x \in Q$. Thus $x^\dagger \Pi_Q E x = \lambda_E$ as well. As $\Pi_Q E$ is a normal matrix, it is unitarily similar to a diagonal matrix. So we may extend an orthonormal basis $\{x_{k+1}, x_{k+2}, \ldots, x_{2^n}\}$ for $Q^\perp$ to an orthonormal basis $\{x_1, \ldots, x_{2^n}\}$ for A consisting of eigenvectors of $\Pi_Q E$. Since $\langle x_i, \Pi_Q E x_i\rangle = \lambda_E$ for all $i = 1, \ldots, k$, we see that $\Pi_Q E$ acts as $\lambda_E I$ on Q. This immediately implies $\langle x, Ey\rangle = 0$ for $x \perp y$ in Q.

(iii) implies **(v)**: Since **(iii)** implies **(iv)**, we can assume that both **(iii)** and **(iv)** hold. Let $\{x_1, \ldots, x_k\}$ be an orthonormal basis for Q. Then

$$\Pi_Q = \sum_{i=1}^{k} x_i x_i^\dagger.$$

Let $E \in \mathcal{T}^\dagger \mathcal{T}$. From **(iii)** and **(iv)**, there exists a constant λ_E such that

$$x_i^\dagger E x_j = \delta_{i,j} \lambda_E.$$

So we have

$$\begin{aligned}
\Pi_Q E \Pi_Q &= \sum_{i=1}^{k} \sum_{j=1}^{k} x_i x_i^\dagger E x_j x_j^\dagger \\
&= \sum_{i=1}^{k} \sum_{j=1}^{k} \delta_{i,j} \lambda_E x_i x_j^\dagger \\
&= \lambda_E \sum_{i=1}^{k} x_i x_i^\dagger \\
&= \lambda_E \Pi_Q
\end{aligned}$$

(v) implies **(ii)**: Suppose $x \perp y$ in Q and $E \in \mathcal{T}^\dagger \mathcal{T}$. Then

$$\Pi_Q E y = \Pi_Q E \Pi_Q y = \lambda_E \Pi_Q y = \lambda_E y.$$

So $\Pi_Q E y$ is orthogonal to x which implies that $Ey \perp x$ as $x \in Q$.

(i) implies **(iii)**: Using the language of superoperators, a physicist will prove this statement in one sentence. But I want to avoid discussion of superoperators and give proofs that are convincing to discrete mathematicians. So here is a simpler, if more tedious, argument. Suppose there exists an algorithm which, with certainty, will restore Ex to x and $E'y$ to y. Define a *trajectory* of Ex under this algorithm as a sequence of the form

$$x_0 = Ex, x_1, x_2, \ldots, x_s = \alpha x \qquad (\alpha \neq 0)$$

where the algorithm, applied to the register in state Ex, uses s steps and x_i is the state of the system after the i^{th} step. (Since measurements potentially involve random selections, there can be many such trajectories.) Similarly, let

$$y_0 = E'y, y_1, y_2, \ldots, y_t = \beta y \qquad (\beta \neq 0)$$

be a trajectory of $E'y$ under the algorithm applied to A in state Ey. Note that since Ex is non-orthogonal to $E'y$, neither x nor y is zero, so none of the x_i or y_i can be the zero vector either.

In each step of the algorithm either a unitary operator or a projection operator is applied to the current state. First, consider the case where $s = t$ and the sequence of operators applied in the two scenarios are identical. Since unitary operators preserve inner products and a projection operator cannot map two non-orthogonal vectors to orthogonal vectors unless it maps one to zero, we see that x_i is non-orthogonal to y_i for all i giving the contradiction $x \not\perp y$.

Otherwise, there exists a step k with the following properties: in all steps $1, \ldots, k-1$, the same exact operators were applied in both scenarios, but in step k the operators differ. Thus the k^{th} step must have been a measurement and different projections were applied to x_{k-1} and y_{k-1}. The same argument as above guarantees that x_{k-1} is not orthogonal to y_{k-1}. So the measurement applied in step k contains a subspace, B say, to which neither x_{k-1} nor y_{k-1} is orthogonal. Hence there is a nonzero probability that this measurement will map both x_{k-1} and y_{k-1} into subspace B. Note that the images under this map cannot be orthogonal. This shows that there exist trajectories of Ex and $E'y$ under the algorithm which apply the same operators in steps $1, \ldots, k$. Continuing in this manner and using finiteness of the algorithm, we see that, with non-zero probability, there exist trajectories which involve the same operators at every step. Thus the argument of the previous paragraph shows that there is a non-zero probability that the terminal vectors x_s and y_t will be non-orthogonal. Thus the algorithm has a non-zero probability of failure.

(iii) implies **(i)**: Since **(iii)** implies **(iv)**, we can assume that both **(iii)** and **(iv)** hold.

Fix an orthonormal basis $\mathcal{B} = \{x_1, \ldots, x_k\}$ for Q. For each i $(1 \leq i \leq k)$, define a subspace

$$\mathcal{V}_i = \mathsf{span}\{Ex_i : E \in \mathcal{T}\}.$$

CLAIM: For $i \neq j$, $\mathcal{V}_i \perp \mathcal{V}_j$.

For the proof of this claim, it will be convenient to be able to express each Ex_i where $E \in \mathcal{T}$ as a linear combination of some fixed *finite* subset of such vectors. Since the space of all linear operators on $A \cong \mathbb{C}^{2^n}$ is finite-dimensional, we can find a finite subset $T = \{E_1, \ldots, E_m\}$ of $\mathcal{T}$ such that every matrix $E \in \mathcal{T}$ is a linear combination of matrices in T.
Proof: Let $a \in \mathcal{V}_i$ and $b \in \mathcal{V}_j$. Write

$$a = \sum_{h=1}^{m} a_h E_h x_i, \qquad b = \sum_{h'=1}^{m} b_{h'} E_{h'} x_j.$$

Then the inner product

$$\langle a, b\rangle = \sum_h \sum_{h'} a_h b_{h'} \langle E_h x_i, E_{h'} x_j\rangle = 0$$

since, by **(iii)**, $E_h x_i$ is orthogonal to $E_{h'} x_j$. This proves the claim.

CLAIM: There exists an integer ℓ such that $\dim \mathcal{V}_i = \ell$ for all $i = 1, \ldots, k$.
Proof: From **(iii)**, we see that the spanning configuration

$$\{Ex_i : E \in \mathcal{T}\}$$

satisfies

$$\langle Ex_i, E'x_i\rangle = \lambda_{(E,E')}$$

independent of the choice of i. So the corresponding configuration

$$\{Ex_j : E \in \mathcal{T}\}$$

has the same set of angles. Consequently, we may appeal to Lemma 2 to find a unitary transformation $\mathcal{U}_{ij}$ acting on A and mapping $\mathcal{V}_i$ to $\mathcal{V}_j$ in such a way that $\mathcal{U}_{ij}(Ex_i) = Ex_j$ for all $E \in \mathcal{T}$. In fact, if we define $U_j = \mathcal{U}_{1j}$, then we can choose $\mathcal{U}_{ij} = U_j U_i^{-1}$. By the way, this proves the claim.

Now, choose an orthonormal basis for $\mathcal{V}_1$, say

$$\{v_{1,r} : r = 1, \ldots, \ell\}$$

starting with $v_{1,1} = x_1$. Then we obtain an orthonormal basis $\{v_{i,r} : r = 1, \ldots, \ell\}$ for each $\mathcal{V}_i$ by

$$v_{i,r} = U_i v_{1,r}.$$

Note that, by choice of U_i, $v_{i,1} = x_i$ for all i.

Next, define spaces $\mathcal{W}_1, \ldots, \mathcal{W}_\ell$ by

$$\mathcal{W}_r = \mathsf{span}\{v_{i,r} : i = 1, \ldots, k\}. \tag{8}$$

Now

$$v_{i,r} \perp v_{j,s}$$

unless both $i = j$ and $r = s$. Thus the spaces $\mathcal{W}_r$ each have dimension k and are pairwise orthogonal. These will give us our measurement. Clearly, the $k\ell$ vectors $v_{i,r}$ span a subspace of A of dimension $k\ell$ which contains our entire problem. More precisely, assuming $E \in \mathcal{T}$ and $x \in Q$, Ex lies in this subspace and our error correction algorithm need deal only with this subspace.

The matrix representing orthogonal projection onto $\mathcal{W}_r$ is

$$P_r = \sum_{i=1}^{k} v_{i,r} v_{i,r}^\dagger. \tag{9}$$

Fig. 2. The pairwise orthogonal vectors $v_{i,r}$ from the spaces $\mathcal{V}_i$ give us, in turn, the new spaces $\mathcal{W}_r$.

Since the $v_{i,r}$ form an orthonormal basis for $\mathcal{W}_r$, there exist unitary matrices R_r satisfying

$$R_r v_{i,r} = x_i \qquad \text{for all } i = 1, \ldots, k. \tag{10}$$

These are the error recovery operators.

Now we are ready to give our error recovery algorithm. It will consist of two steps. The first is a measurement which projects the damaged state onto some $\mathcal{W}_s$. From this measurement, we obtain the index s. The second step of the algorithm is then to simply apply the recovery operator R_s. Now let us go through this rigorously.

Let $\mathcal{O}$ denote the orthogonal complement of our $k\ell$-dimensional working space $\mathcal{W}_1 \oplus \cdots \oplus \mathcal{W}_\ell$. We first perform the measurement

$$\mathcal{M} = \{\mathcal{W}_1, \ldots, \mathcal{W}_\ell, \mathcal{O}\}.$$

CLAIM: For any non-zero $x \in Q$ and for any $E \in \mathcal{T}$, the measurement will return $\mathcal{W}_r$ for some r.
Proof: We know that x is a linear combination of the x_i and Ex_i lies in $\mathcal{V}_i$ for each i. So each Ex_i is orthogonal to $\mathcal{O}$, hence Ex is orthogonal to $\mathcal{O}$.

Consequently, the measurement returns some integer r $(1 \leq r \leq \ell)$ and as a result of the measurement, the vector Ex has been mapped to $y = P_r Ex$ which is guaranteed to be nonzero. The second step of our quantum algorithm is to apply the recovery operator R_r.

CLAIM: $R_r y$ is a non-zero multiple of x.
Proof: As y is non-zero and R_r is unitary, it is clear that the resulting vector is not zero.

As a preliminary step, we choose a basis vector $x_i \in \mathcal{B}$ and any $E \in \mathcal{T}$ and express $Ex_i \in \mathcal{V}_i$ as a linear combination of the basis vectors $v_{i,s}$:

$$Ex_i = \sum_{s=1}^{\ell} \tau_{E,i,s} v_{i,s}. \tag{11}$$

Note that $\tau_{E,i,s}$ is determined by the inner product of Ex_i with each $v_{i,s}$. By construction of the basis $\{v_{i,s}\}$ for $\mathcal{V}_i$, these inner products do not depend on i. So $\tau_{E,i,s} = \tau_{E,j,s}$ for any i, j $(1 \leq i, j \leq k)$ and we are permitted to suppress the subscript i.

Let us write the error as a linear combination of the matrices in our chosen spanning set T:

$$E = \sum_{h=1}^{m} \gamma_h E_h. \tag{12}$$

Denote the damaged state by $z = Ex$ where $x \in Q$ is the initial state. We have

$$\begin{aligned} z &= \sum_{h=1}^{m} \gamma_h E_h x \\ R_r P_r z &= \sum_{h=1}^{m} \gamma_h R_r P_r E_h x \\ &= \sum_{h=1}^{m} \sum_{i=1}^{k} \gamma_h \beta_i R_r P_r E_h x_i \end{aligned}$$

where we have expressed $x = \sum \beta_i x_i$ in Q. Now we use Equation (11) together with the observation that $\tau_{E_h,i,s}$ is independent of i and can hence be written $\tau_{h,s}$.

$$\begin{aligned} R_r P_r z &= \sum_{h=1}^{m} \sum_{i=1}^{k} \sum_{s=1}^{\ell} \gamma_h \beta_i \tau_{h,s} R_r P_r v_{i,s} \\ &= \sum_{h=1}^{m} \sum_{i=1}^{k} \gamma_h \beta_i \tau_{h,r} R_r v_{i,r} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{h=1}^{m} \sum_{i=1}^{k} \gamma_h \beta_i \tau_{h,r} x_i \\
&= \sum_{h=1}^{m} \gamma_h \tau_{h,r} \sum_{i=1}^{k} \beta_i x_i \\
&= \left(\sum_{h=1}^{m} \gamma_h \tau_{h,r} \right) x
\end{aligned}
$$

Thus the recovered state is a multiple of the initial state x and this multiple is non-zero. □

Early on, it was thought that the spaces $E(Q)$ ($E \in \mathcal{T}$) had to be pairwise orthogonal. There are examples of such codes and their discovery by Shor was a significant breakthrough. However, one important aspect of the Knill/Laflamme theorem is the relaxation of this condition. The existence of the spaces $\mathcal{W}_r$ constructed in the proof allow for this extension. Observe that there is no guarantee that any $\mathcal{W}_r$ other than $\mathcal{W}_1 = Q$ coincides with $E(Q)$ for any $E \in \mathcal{T}$. It is also curious that the error correction algorithm potentially introduces additional error to the system by projecting onto one of the spaces $\mathcal{W}_r$.

Corollary 2. *For any subspace Q of the n-qubit quantum register A, if Q allows correction of all errors in some set $\mathcal{T}$ of $2^n \times 2^n$ matrices, then Q allows correction of all errors in the linear span of $\mathcal{T}$.*

Proof. This follows from the above proof. For each i, the space $\mathcal{V}_i$ contains all vectors of the form Ex_i where E lies in the span of $\mathcal{T}$. The error correction algorithm given never assumes that the error actually lies in $\mathcal{T}$, but rather that it can be expressed as a linear combination of elements of a finite spanning set T for $\mathcal{T}$. □

These results have important implications for our error models. For example, if we find a code Q which allows correction of all errors of weight at most one in $\mathcal{E}$, then Q corrects any 2×2 matrix whatsoever acting on any single qubit. (More precisely, the error is the tensor product of this matrix with $n - 1$ copies of the identity.)

More generally, we may design a code which allows correction of some nice subset of $\mathcal{E}$ and find that it in fact corrects a much wider variety of errors. For example, we may be lucky enough to correct an inadvertent measurement of the n-qubit register provided the acting projection matrix lies in the span of $\mathcal{T}$. One can verify, however, that any correctable error acts in a one-to-one fashion on the code Q. This follows from statement (iv) of the Knill/Laflamme theorem.

Henceforth, we only concern ourselves with errors belonging to the group $\mathcal{E}$.

8 Stabilizer codes

The stabilizer code formalism was introduced by Gottesman in [10]. The approach of Calderbank, *et al.* [7], on which this section is based, is essentially equivalent and was developed independently.

Let A be an n-qubit quantum register and let $\mathcal{G}$ be an abelian subgroup of the corresponding error group $\mathcal{E}$. Some authors define a stabilizer code as follows:

$$Q = \{x \in A : Ex = x \text{ for all } E \in \mathcal{G}\}.$$

Unfortunately, Q is the zero space when $-I \in \mathcal{G}$; this is a nuisance. We can avoid this restriction by extending the definition of our code. For an abelian subgroup $\mathcal{G}$ of $\mathcal{E}$, let Q be any common eigenspace of the matrices in $\mathcal{G}$. Thus

$$Q = \{x \in A : Ex = \theta_E x \text{ for all } E \in \mathcal{G}\} \tag{13}$$

where θ_E is some pre-specified function from $\mathcal{G}$ to $\mathbb{C}$. A code which can be described in this way is called a *stabilizer code*. Note that, since we are ignoring multiplication of states by non-zero scalars, this terminology is still valid (just view Q as a subspace of a projective space). Since $E^2 = \pm I$ for all $E \in \mathcal{E}$, we may restrict to $\theta_E \in \{\pm 1, \pm i\}$. Of course, not all such selections give rise to non-trivial subspaces Q.

Proposition 1 tells us how to locate abelian subgroups of $\mathcal{E}$ by working in a binary space with a symplectic inner product. The goal now is to find abelian subgroups $\mathcal{G}$ which give rise to codes correcting many low-weight errors.

While Q consists of all vectors (projectively) stabilized by $\mathcal{G}$, it may not hold that $\mathcal{G}$ consists of all group elements which stabilize every line in Q. We will see in a moment that the full stabilizer of Q is the subgroup generated by $\mathcal{G}$ and $-I$.

Proposition 2. *Let $E' \in \mathcal{E}$ and let Q be a stabilizer code determined by the abelian subgroup $\mathcal{G}$. If there exists a matrix $E \in \mathcal{G}$ which anti-commutes with E', then E' is a detectable error relative to Q.*

Proof. For every $x \in Q$, we have $Ex = \theta_E x$. So Q is a subspace of the eigenspace of E corresponding to the eigenvalue $\theta_E \neq 0$. Now, let y be any vector in Q. We have

$$\begin{aligned} E(E'y) &= (EE')y \\ &= (-E'E)y \end{aligned}$$

$$= -E'(Ey)$$
$$= -\theta_E(E'y)$$

Thus $E'y$ is an eigenvector for E with eigenvalue $-\theta_E$. Since eigenvectors in distinct eigenspaces are orthogonal, we have $E'y \perp Q$. □

On the other hand, if E' commutes with every $E \in \mathcal{G}$, we can easily see that E' fixes each eigenspace of each matrix in $\mathcal{G}$. Hence, E' maps each $x \in Q$ to some vector in Q. This shows that Q is stabilized *as a subspace* by $\mathcal{Z}(\mathcal{G})$, the centralizer of $\mathcal{G}$ in $\mathcal{E}$. However, if $-I \in \mathcal{G}$, no element of $\mathcal{Z}(\mathcal{G}) \setminus \mathcal{G}$ stabilizes every $x \in Q$ projectively.

Since σ_x does not commute with σ_z, the center of the error group $\mathcal{E}$ is $\{I, -I\}$. The factor group

$$\bar{\mathcal{E}} = \mathcal{E}/\{\pm I\}$$

is an elementary abelian 2-group with 2^{2n} elements. Multiplication of cosets is in exact correspondence with vector addition over $\mathbb{Z}_2$: if $e = \{\pm X(a)Z(b)\}$ and $e' = \{\pm X(a')Z(b')\}$, then

$$e \odot e' = \{\pm X(a + a')Z(b + b')\}.$$

We will use the notation $\mathcal{K}$ and $\bar{\mathcal{K}}$ to denote the relationship between a subset of $\mathcal{E}$ closed under multiplication by -1 and the partition of it into cosets in $\bar{\mathcal{E}}$.

The following is an entirely standard observation from coding theory. Let C be an additive binary code of length $2n$, self-orthogonal under the symplectic inner product. If $C \neq C^\perp$, we can extend C to a larger code with the same properties by inserting a tuple $(a|b) \in C^\perp \setminus C$ and taking the span of $C \cup \{(a|b)\}$. Thus every self-orthogonal code is contained in a self-dual code. We now translate this information into a statement about the error group.

Proposition 3. *If $\mathcal{G}$ is an abelian subgroup of $\mathcal{E}$, then there exists an abelian subgroup $\mathcal{H}$ of $\mathcal{E}$ containing $\mathcal{G}$ having cardinality 2^{n+1}. In other words, every maximal abelian subgroup of $\mathcal{E}$ consists of 2^{n+1} elements.*

A maximal abelian subgroup $\mathcal{H}$ has 2^{n+1} distinct linear characters. The corresponding group $\bar{\mathcal{H}}$ has 2^n linear characters and each of these extends to a character of $\mathcal{H}$: they are precisely the characters χ satisfying $\chi(-I) = 1$. Since the matrices in $\mathcal{H}$ commute, they may be simultaneously diagonalised. Suppose U is a matrix such that $U^\dagger EU$ is diagonal for every $E \in \mathcal{H}$. Then the map

$$\chi_j : \mathcal{H} \to \mathbb{C}$$

mapping $E \in \mathcal{H}$ to the row j, column j entry of $U^\dagger EU$ is a linear character of $\mathcal{H}$. In this way, we obtain 2^n characters all satisfying $\chi(-I) = -1$. Since these are all distinct (exercise), they yield precisely the non-identity coset of the subgroup consisting of characters of $\bar{\mathcal{H}}$.

Now $\mathcal{G}$ is a subgroup of $\mathcal{H}$ and Q is a common eigenspace of the matrices in $\mathcal{G}$. Since the characters of $\bar{\mathcal{H}}$ give a complete basis of eigenvectors for the matrices in $\mathcal{H}$, Q admits a basis $\mathcal{B}$ of characters. As each $E \in \mathcal{G}$ has the same eigenvalue independent of the character chosen in $\mathcal{B}$, these characters form a full coset of the dual subgroup of $\bar{\mathcal{G}}$ in the character group $\bar{\mathcal{H}}^*$. If $\bar{\mathcal{G}}$ has size 2^k, then its dual subgroup $\bar{\mathcal{G}}^*$ has size 2^{n-k}. Thus the coset giving a basis for Q has this size and, as any set of distinct characters is linearly independent, we have:

Theorem 2. *Let Q be the stabilizer code constructed as in (13) from the abelian subgroup $\mathcal{G}$ of $\mathcal{E}$ containing $-I$. If $\mathcal{G}$ contains 2^{k+1} elements, then Q has dimension 2^{n-k}.*

Now if C is a self-orthogonal code and $\mathcal{G} = \{\pm X(a)Z(b) : (a|b) \in C\}$, then the subgroup of $\mathcal{E}$ constructed in the same way from the dual code $C^\perp$ is precisely the centralizer $\mathcal{Z}(\mathcal{G})$. This follows directly from Lemma 1.

In view of the Knill/Laflamme theorem, it is natural to define the *minimum distance* of a quantum code Q as the minimum weight of any non-detectable error in $\mathcal{E}$.

Theorem 3 (Calderbank/Rains/Shor/Sloane). *Let A be a quantum register with error group $\mathcal{E}$. Let $\mathcal{G}$ be an abelian subgroup of $\mathcal{E}$ containing $-I$ and arising from the binary code C which is self-orthogonal under the symplectic inner product. Let Q be constructed as in (13). Then the minimum distance of the quantum code Q is equal to the smallest weight of any binary $2n$-tuple in $C^\perp \setminus C$.*

Proof. let $E \in \mathcal{E}$. If $E \notin \mathcal{Z}(\mathcal{G})$, then $EE' = -E'E$ for some $E' \in \mathcal{G}$. So E is detectable by Proposition 2. On the other hand, if $E \in \mathcal{G}$, then $Ex = \theta_E x$ for all $x \in Q$. Such an error is also detectable by definition. □

We now have a concrete target. If we can find a binary additive code C of length $2n$ which is self-orthogonal under the symplectic inner product such that the dual code $C^\perp$ contains no words of weight less than d aside from those in C, then the stabilizer construction yields a quantum code Q having minimum distance d and dimension equal to 2^{n-k}. Thus, by the Knill/Laflamme theorem, Q will encode $n-k$ qubits into n qubits and will correct any error $E \in \mathcal{E}$ of weight at most $\lfloor (d-1)/2 \rfloor$.

9 Some examples

We have easy access to a large number of interesting abelian subgroups which, in turn, give us non-trivial quantum codes. The groups themselves were introduced in Section 4, but I'll repeat the construction here.

Let C_1 be an additive binary code of length n. Suppose G_1 is a generator matrix for this code. Let C_2 be an additive subcode of the dual code $C_1^\perp$ and let G_2 be a generator matrix for C_2. Now consider the binary code of length $2n$ whose generator matrix is

$$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}.$$

The codewords in C are precisely the $2n$-tuples $(a|b)$ for which $a \in C_1$ and $b \in C_2$. Thus, if $(a|b)$ and $(a'|b')$ both belong to C, we have

$$\langle (a|b), (a'|b') \rangle = a \cdot b' + a' \cdot b = 0 + 0 = 0.$$

So C is self-orthogonal. Hence the group

$$\mathcal{G} = \{\pm X(a)Z(b) : a \in C_1,\ b \in C_2\}$$

is abelian. The stabilizer construction (13) thus gives us a quantum code of dimension $2^{n-k_1-k_2}$ where k_1 denotes the dimension of C_1 and k_2 that of C_2. This construction is due to Steane and, independently, Calderbank and Shor.

The dual code of C under the symplectic product has a similar description:

$$C^\perp = \left\{(a'|b') : a' \in C_1^\perp,\ b' \in C_2^\perp\right\}.$$

Now $C_2 \subseteq C_1^\perp$ and $C_1 \subseteq C_2^\perp$. So the minimum weight of a tuple in $C^\perp$ not in C is the smaller of the two values

$$\min\{wt_H(a') : a' \in C_1^\perp,\ a' \notin C_1\}, \qquad \min\{wt_H(b') : b' \in C_2^\perp,\ b' \notin C_2\}$$

where $wt_H(a) = |\{i : a_i \neq 0\}|$ denotes the ordinary Hamming weight of a binary tuple. This gives us the minimum distance of the corresponding stabilizer code.

10 The $GF(4)$ trick

If $E = \pm \otimes s_i$ is a matrix in the error group, then there are four choices for each s_i. So far, we have used the correspondence $E \leftrightarrow \pm(a|b)$ where $b_i = 0$ if $s_i = \sigma_x$, and so on. Since there are four choices for s_i, it is natural to replace $\mathbb{Z}_2 \times \mathbb{Z}_2$ by an alphabet of size four in such a way that the symplectic inner

product on $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ is replaced by a natural inner product. This approach was successfully taken up in [8].

Let $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ denote the finite field of order four and replace the correspondence (4) by the following:

$$I_2 \mapsto 0, \qquad \sigma_x \mapsto 1, \qquad \sigma_y \mapsto \omega, \qquad \sigma_z \mapsto \bar{\omega}.$$

Under this group isomorphism $\bar{\mathcal{E}} \to \mathbb{F}_4^n$, an error E of weight k is mapped to a quaternary n-tuple of Hamming weight k. But the multiplicative structure of $\mathbb{F}_4$ has no obvious counterpart in $\bar{\mathcal{E}}$. Of course, the ordinary inner product on $\mathbb{F}$ yields values in $\mathbb{F}$. We now show that a slight modification gives us an inner product useful for our purposes. Recall the *trace* takes on a simple form

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^2$$

in this small field. We now define the *trace inner product*

$$a * b = \mathrm{Tr}(a \cdot b)$$

where $a \cdot b = \sum \bar{a}_i b_i$ denotes the ordinary Hermitian inner product.

Proposition 4. *Let E and F be elements of $\mathcal{E}$ and let a and b be the corresponding tuples in $\mathbb{F}_4^n$. Then EF is equal to FE or $-FE$ depending as $\mathrm{Tr}(a \cdot b)$ is equal to 0 or 1. Thus a subgroup of $\mathcal{E}$ is abelian if and only if the corresponding code is additive and self-orthogonal under the trace inner product.*

Proof. If $E = \otimes s_i$ and $F = \otimes t_i$, then $EF = \otimes s_i t_i$ and $FE = \otimes t_i s_i$. Observe that $s_i t_i$ and $t_i s_i$ anticommute if and only if $s_i \neq t_i$ and neither is equal to the identity. Consider the table

$\bar{\alpha}\beta$	0	1	ω	$\bar{\omega}$
0	0	0	0	0
1	0	1	ω	$\bar{\omega}$
ω	0	$\bar{\omega}$	1	ω
$\bar{\omega}$	0	ω	$\bar{\omega}$	1

Clearly, the term $\mathrm{Tr}(\bar{a}_i b_i)$ contributes one to the sum $\mathrm{Tr}(\bar{a} \cdot b)$ if and only if the corresponding Pauli matrices anti-commute. □

Of course, much more is known about codes which are self-orthogonal under the ordinary Hermitian inner product. Fortunately, for codes linear over $\mathbb{F}_4$, the two concepts of self-orthogonality coincide.

Theorem 4. *Let C be a linear code over $\mathbb{F}_4$. Then C is self-orthognal under the trace inner product $*$ if and only if C is self-orthogonal under the Hermitian inner product.*

Proof. For $a, b \in C$. If $a \cdot b = 0$, then clearly $a * b$ is zero. Conversely, suppose C is self-orthogonal under the trace inner product and let $a, b \in C$. Then both $a * b = 0$ and $(\omega a) * b = 0$ so that $a \cdot b$ must equal zero. □

11 Further reading

The theory of quantum computation and quantum information is already quite substantial. Two good starting points for the reader who wants to investigate this are are the book [13] by Neilsen and Chuang and the survey article [5] by Berthiaume. Some readers will wish to see quantum coding theory from a physical perspective. For this, I recommend the paper of Knill and Laflamme [12], but there is also an extensive discussion of quantum codes in [13].

In many ways, quantum coding theory parallels classical coding theory, particularly with an alphabet of size four. MacWilliams identities for quantum stabilizer codes were first found by Shor and Laflamme in [18]. Since then, Rains has led the way in the study of weight enumerators of quantum codes. (See [15] and the references therein.)

Only a few quantum codes are known which are not stabilizer codes. In [14], Rains, *et al.* describe a 5-qubit quantum code of dimension 6 and minimum distance 2 which does not arise from the stabilizer construction. This was found with the aid of a computer. Yet this code has larger dimension than any stabilizer code of length five having minimum distance two or more. It would be interesting to identify further non-stabilizer codes. In particular, the Knill-Laflamme theorem allows for the image of Q under a detectable error to be isoclinic to Q ($\Pi_Q E \Pi_Q = \lambda_E \Pi_Q$) and not simply orthogonal to Q. The non-stabilizer code just described has $\Pi_Q E \Pi_Q = 0$ just as all stabilizer codes do. I know no non-trivial examples of codes with some $\lambda_E \neq 0$ ($E \neq \alpha I$).

Another direction one might consider is the study of non-binary quantum codes. If we replace our most basic structure, the qubit, by a 3-, 4- or higher-dimensional complex vector space, then we will need ternary, quaternary or q-ary quantum codes. These structures are investigated in [16] and [3].

Acknowledgments

I have benefited greatly from conversations with Alexei Ashikhmin, Chris Godsil, and Manny Knill. It seems unlikely that I could have absorbed all of this material had it not been for their generous help. Yet any errors or inaccuracies you find here are due to me alone.

This paper was written while I was visiting the Department of Combinatorics and Optimization at the University of Waterloo. I wish to thank the department for its hospitality and accommodation during this visit. My research is supported by the Canadian government through NSERC grant number OGP0155422. Additional support was provided by MITACS and CITO through the Centre for Applied Cryptographic Research. Current support provided through NSF-ITR grant number 0112889.

References

1. A. E. Ashikhmin, A. M. Barg, E. Knill, S. N. Litsyn. Quantum error detection I: statement of the problem. *IEEE Trans. Inform. Theory*, **46** (no. 3) (2000), 778–788.
2. A. E. Ashikhmin, A. M. Barg, E. Knill, S. N. Litsyn. Quantum error detection II: bounds. *IEEE Trans. Inform. Theory*, **46** (no. 3) (2000), 789–800.
3. A. E. Ashikhmin and E. Knill. Nonbinary quantum stabilizer codes. *IEEE Trans. Inform. Theory*, **47** (no. 7) (2001), 3065–3072.
4. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, **54** (no. 5) (1996), 3824–3851.
5. A. Berthiaume. Quantum computation. in: *Complexity theory retrospective, II*, 23–51, Springer, New York, 1997.
6. A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc.* **75** (no. 2) (1997), 436–480.
7. A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.* **78** (no. 3) (1997), 405–408.
8. A. R. Calderbank, E. M. Rains, P. W. Shor, N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inform. Theory* **44** (no. 4) (1998), 1369–1387.
9. A. Ekert and C. Macchiavello. Quantum error correction for communication. *Phys. Rev. Lett.*, **77** (1996), 2585–2588.
10. D. Gottesman. Class of quantum error correcting codes saturating the quantum Hamming bound. *Phys. Rev. A*, **54** (1996), 1862–1868.
11. M. Grassl and T. Beth. A note on non-additive quantum codes. Los Alamos preprint server `arXiv:quant-ph/9703016 v1 Mar 1997`
12. E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Physical Review A* **55** (1997), 900-911.
13. M. A. Nielsen and I. L. Chuang. Quantum Computation and Quantum Information Cambridge University Press, Cambridge, 2000.
14. E. M. Rains, R. H. Hardin, P. W. Shor, N. J. A. Sloane. A Nonadditive Quantum Code. *Phys. Rev. Lett.*, **79** (1997), 953–954.
15. E. M. Rains. Quantum weight enumerators. *IEEE Trans. Inform. Theory*, **44** (no. 4) (1998), 1388–1394.

16. E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inform. Theory*, **45** (no. 6) (1999), 1827–1832.
17. P. W. Shor. Scheme for reducing decoherence in quantum memory. *Phys. Rev. A*, **52** (1995), 2493.
18. P. Shor and R. Laflamme. Quantum Analog of the MacWilliams Identities for Classical Coding Theory. *Phys. Rev. Lett.* **78** (1997), 1600–1602.