Quantum Error Correction Via Codes Over $GF(4)$

A. R. Calderbank,[1] *E. M. Rains*,[2] *P. W. Shor*,[1] and *N. J. A. Sloane*[1]

[1]AT&T Labs - Research, Florham Park, New Jersey 07932-0971

[2]Institute for Defense Analyses, Princeton, New Jersey 08540

August 27, 1997

ABSTRACT

The problem of finding quantum-error-correcting codes is transformed into the problem of finding additive codes over the field $GF(4)$ which are self-orthogonal with respect to a certain trace inner product. Many new codes and new bounds are presented, as well as a table of upper and lower bounds on such codes of length up to 30 qubits.

Manuscript received _____; revised _____

The authors are with AT&T Labs - Research, Florham Park, NJ 07932-0971, USA. The work of the second author was performed while he was with the Institute for Defense Analyses, Princeton, NJ, USA.

1. Introduction

The relationship between quantum information and classical information is a subject currently receiving much study. While there are many similarities, there are also substantial differences between the two. Classical information cannot travel faster than light, while quantum information appears to in some circumstances (although proper definitions can resolve this apparent paradox). Classical information can be duplicated, while quantum information cannot [29], [72].

It is well known that classical information can be protected from degradation by the use of classical error-correcting codes [52]. Classical error-correcting codes appear to protect classical information by duplicating it, so because of the theorem that a quantum bit cannot be cloned, it was widely believed that these techniques could not be applied to quantum information. That quantum-error-correcting codes could indeed exist was recently shown by one of us [60]. Two of us [17] then showed that a class of good quantum codes could be obtained by using a construction that starts with a binary linear code C containing its dual $C^{\perp}$. Independently, Steane also discovered the existence of quantum codes [68] and the same construction [67]. At around the same time, Bennett et al. [4] discovered that two experimenters each holding one component of many noisy Einstein-Podolsky-Rosen (EPR) pairs could *purify* them using only a classical channel to obtain fewer nearly perfect EPR pairs. The resulting pairs can then be used to teleport quantum information from one experimenter to the other [3]. Although it was not immediately apparent, these two discoveries turned out to be different ways of looking at the same phenomenon. A purification protocol that uses only a one-way classical channel between the experimenters can be converted into a quantum-error-correcting code, and vice versa [5]. After these discoveries, a number of improved quantum codes were soon found by various researchers.

The setting in which quantum-error-correcting codes exist is the quantum state space of n qubits (quantum bits, or two-state quantum systems). This space is $\mathbb{C}^{2^n}$, and it has a natural decomposition as the tensor product of n copies of $\mathbb{C}^2$, where each copy corresponds to one qubit. We noticed that the known quantum codes seemed to have close connections to a finite group of unitary transformations of $\mathbb{C}^{2^n}$, known as a Clifford group, and denoted here by L. This group contains all the transformations necessary for encoding and decoding quantum codes. It is also the group generated by fault-tolerant bitwise operations performed on qubits

that are encoded by certain quantum codes [17], [61], [67]. Investigation of the connection between this group and existing quantum codes has led us to a general construction for such codes which allows us to generate many new examples. The initial results of this study were reported in [16]. However, it is very hard to construct codes using the framework of [16]. In the present paper we develop the theory to the point where it is possible to apply standard techniques from classical coding theory to construct quantum codes. Some of the ideas in [16] (although neither the connections with the Clifford group nor with finite geometries or fields) were discovered independently by Gottesman [35].

The paper is arranged as follows. Section 2 transforms the problem into one of constructing a particular type of binary space (Theorem 1). Section 3 shows that these spaces in turn are equivalent to a certain class of additive codes over $GF(4)$ (Theorem 2). The rest of the paper is then devoted to the study of such codes. Their basic properties are described in the remainder of Section 3, and Section 4 gives a number of general constructions. Sections 5, 6, and 7 then deal with cyclic and related codes, self-dual codes, and bounds. Until now little was known about general bounds for quantum codes. The linear programming bound (Theorems 21 and 22) presented in Section 7 appears to give quite sharp bounds for those codes. This can be seen in the main table of the paper, Table III, given in Section 8, which is based on the results of the earlier sections. Although there are still a large number of gaps in the table, the upper and lower bounds are generally not too far apart and there are a considerable number of entries where the parameters of the best codes are known exactly. Section 9 contains an update on developments that have occurred since the manuscript of this paper was first circulated.

In order to reduce the length of the paper, proofs which either use standard techniques in coding theory or are straightforward will be omitted.

2. From quantum codes to binary spaces

Recall from Section 1 that the quantum state space of n qubits is $\mathbb{C}^{2^n}$. The idea behind quantum error correction is to encode quantum states into qubits so that errors or decoherence in a small number of individual qubits will have little or no effect on the encoded data. More precisely, an encoding of k qubits into n qubits is taken to be a linear mapping of $\mathbb{C}^{2^k}$ onto a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$. Since the error correction properties of this mapping depend only on the subspace rather than on the mapping, the subspace itself will be called the quantum error correcting code.

Correction of arbitrary errors in an arbitrary 2^k-dimensional subspace is in general infeasible, since errors which map states in the subspace to other states in the subspace cannot be corrected (because the latter are also permissible states). To overcome this, we make use of the tensor product decomposition of $\mathbb{C}^{2^n}$ into n copies of $\mathbb{C}^2$. Quantum error correcting codes are subspaces oriented so that any error in a relatively small number of qubits moves the state in a direction perpendicular to the coded subspace, and thus can be corrected.

A bit error in an individual qubit corresponds to applying the Pauli matrix $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to that qubit, and a phase error to the Pauli matrix $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The third Pauli matrix, $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_x\sigma_z$, corresponds to a combination of bit and phase errors. The group E of tensor products $\pm w_1 \otimes \cdots \otimes w_n$ and $\pm iw_1 \otimes \cdots \otimes w_n$, where each w_j is one of I, $\sigma_x, \sigma_y, \sigma_z$, describes the possible errors in n qubits. E is a subgroup of the unitary group $U(2^n)$. In general, there is a continuum of possible errors in qubits, and there are errors in sets of qubits which cannot be described by a product of errors in individual qubits. For the purposes of quantum error correction, however, we need consider only the three types of errors σ_x, σ_y and σ_z, since any error-correcting code which corrects t of these errors will be able to correct arbitrary errors in t qubits [5], [33], [45]. We do not go into the details of this result, but essentially it follows from the fact that the matrices I, σ_x, σ_y and σ_z form a basis for the space of all 2×2 matrices, and so the tensor products of t of these errors form a basis for the space of $2^t \times 2^t$ matrices.

Our codes will thus be tailored for the error model in which each qubit undergoes independent errors, and the three errors σ_x, σ_y and σ_z are all equally likely. The results of [5], [33], [45] show that any code which corrects these types of quantum errors will be able to correct errors in arbitrary error models, assuming the errors are not correlated among large numbers of qubits and that the error rate is small. For other error models it may be possible to find codes which correct errors more efficiently than our codes do; this is not discussed in this paper.

This section and Section 3 show how to convert the problem of finding quantum-error-correcting codes into one of finding certain types of classical error-correcting codes. We do this in two stages. The first stage reduces the problem from a quantum (continuous) one to a classical (discrete) problem in finite geometry. The second stage converts the latter to a coding theory problem.

The finite geometry problem can be summarized as follows. Let $\bar{E}$ denote a $2n$-dimensional binary vector space, whose elements are written $(a|b)$ and which is equipped with the inner

product

$$((a|b),(a'|b')) = a \cdot b' + a' \cdot b \ . \tag{1}$$

This is a symplectic inner product, since it satisfies

$$((a|b),(a|b)) = 0 \ .$$

Define the weight of $(a|b) = (a_1 \cdots a_n|b_1 \cdots b_n)$ to be the number of coordinates i such that at least one of a_i and b_i is 1. The distance between two elements $(a|b)$, $(a'|b') \in \bar{E}$ is defined to be the weight of their difference.

Then we have the following theorem, which is an immediate consequence of Theorem 1 of [16].

Theorem 1. *Suppose $\bar{S}$ is an $(n-k)$-dimensional linear subspace of $\bar{E}$ which is contained in its dual $\bar{S}^{\perp}$ (with respect to the inner product (1)), and is such that there are no vectors of weight $\leq d-1$ in $\bar{S}^{\perp} \setminus \bar{S}$. Then there is a quantum-error-correcting code mapping k qubits to n qubits which can correct $[(d-1)/2]$ errors.*

We will describe such a quantum-error-correcting code by saying it has parameters $[[n,k,d]]$, and call d the *minimal distance* of the code. A code obtained via Theorem 1 will be called an *additive code.* Almost all quantum-error-correcting codes known at the present time are additive. However, we will have occasion to discussion more general codes in this paper, and will use the symbol $((n,K,d))$ to indicate a code with minimal distance d (see [62]) that encodes K states into n qubits. Of course, an $[[n,k,d]]$ code is also an $((n,2^k,d))$ code.

Readers who are most interested in the codes themselves could now proceed directly to Section 3.

To motivate the following discussion we begin by describing classical binary linear codes from a slightly unusual perspective. A linear code C is of course a linear subspace of $\mathbb{Z}_2^n$, where $\mathbb{Z}_2 = \{0,1\}$. But $\mathbb{Z}_2^n$ can also be regarded as the group of possible errors, i.e., C is also a subgroup of the error group. Furthermore, this subgroup C has the following characterization in terms of the error group: an error e is in C precisely when translation by e takes codewords to codewords and thus cannot be detected. C corrects a set of errors if and only if the sum of any two errors can be detected, i.e. lies outside C, except that the sum may be the trivial error $\mathbf{0}$, which, while it cannot be detected, has no effect.

In the quantum setting, it is possible for a nontrivial error to be undetectable and yet have no impact on the encoded state. This suggests that we should attempt to construct a quantum

code from a pair of subgroups of the quantum error group E. One subgroup (which we will call S') specifies the undetectable errors, while the other (called S) is the subgroup of S' consisting of errors that have no effect on the encoded state. S is the analogue of the zero subgroup in the classical coding case.

It will turn out to be important to require that every element of S' commutes with S. This implies in particular that S is abelian. So we are led to consider when elements of E commute.

The group[1] E has order 2^{2n+2} and center $\Xi(E) = \{\pm I, \pm iI\}$. The quotient group $\bar{E} = E/\Xi(E)$ is an elementary abelian group of order 2^{2n}, and hence a binary vector space. Let V denote the vector space $\mathbb{Z}_2^n$, and label the standard basis of $\mathbb{C}^{2^n}$ by $|v\rangle$, $v \in V$. Every element $e \in E$ can be written uniquely in the form

$$e = i^\lambda X(a)Z(b) \tag{2}$$

where $\lambda \in \mathbb{Z}_4$, $X(a) : |v\rangle \to |v+a\rangle$, $Z(b) : |v\rangle \to (-1)^{b\cdot v}|v\rangle$, for $a, b \in V$. The element $X(a)Z(b)$ indicates that there are bit errors in the qubits for which $a_j = 1$ and phase errors in the qubits for which $b_j = 1$.

If $e, e' \in E$ are given by (2) then $ee' = \pm e'e$, where the sign is $(-1)^{a\cdot b' + a'\cdot b}$. This induces the symplectic inner product given in (1):

$$((a|b), (a'|b')) = a \cdot b' + a' \cdot b \ ,$$

where we write $(a|b)$ for the image of $X(a)Z(b)$ in $\bar{E}$. Two elements in E commute if and only if their images in $\bar{E}$ are orthogonal with respect to this inner product.

A subspace $\bar{S}$ of $\bar{E}$ is said to be *totally isotropic* if for all $\bar{s}_1$, $\bar{s}_2 \in \bar{S}$ the symplectic inner product $(\bar{s}_1, \bar{s}_2) = 0$. A subgroup S of E is commutative if and only if its image $\bar{S}$ in $\bar{E}$ is totally isotropic. The dimension of a totally isotropic subspace is at most n. The groups $X = \{X(a) : a \in V\}$ and $Z = \{Z(b) : b \in V\}$ are examples of subgroups of E whose images $\bar{X}$, $\bar{Z}$ have dimension n.

We define $S^\perp$ to be the lift of $(\bar{S})^\perp$ to E; or, in other words, $S^\perp$ is the centralizer of S in E. We will take S' to be $S^\perp$, that is, $S^\perp$ will be group of undetectable errors.

Since S is abelian, its elements can be simultaneously diagonalized. This induces a decomposition of $\mathbb{C}^{2^n}$ into orthogonal eigenspaces. In order for S to act trivially on the code, it is

[1] 'E' stands for 'error group', but also serves as a reminder that E is essentially an extraspecial 2-group. The association of extraspecial 2-groups with finite orthogonal spaces, underlying all of this section, is a standard one in group theory (cf. [1], Theorem 23.10; [39], Theorem 13.8). We have made further use of this theory in [63], [13].

necessary for the code to lie entirely in one of these eigenspaces. Since we also want $S^\perp$ to preserve the code, we take the code to be one of the eigenspaces, to be denoted by Q (say). We call codes obtained in this way *additive* codes.

To each eigenspace of S there corresponds a homomorphism $\chi : S \to \mathbb{C}$, under which each element of S is mapped to the corresponding eigenvalue. Then χ is a character of S, and $\chi(iI) = i$.

Every element $e \in E$ normalizes S, and so conjugation by e induces an action on characters. Since $S^\perp$ commutes with S, elements of $S^\perp$ induce the trivial action on the characters. Any element outside $S^\perp$ negates the value of the character at each element of S with which it anticommutes. In particular, it induces a nontrivial action on the characters, and so $E/S^\perp$ acts faithfully.

It follows that the orbit of any given character must have size $|E/S^\perp|$. If $\bar{S}$ has dimension $n-k$, $|E/S^\perp| = 2^{n-k}$. On the other hand there are 2^{n-k} characters of S such that $\chi(iI) = i$, since the quotient of any two such characters is a character of $\bar{S}$. Thus $E/S^\perp$ acts transitively. It follows that each eigenspace must have the same dimension, namely 2^k.

It remains to determine the error-correcting properties of the code Q. In the classical setting, we can correct a set of errors when the quotient (really, difference) of any pair of the errors lies outside the set $C \setminus \{0\}$, that is, can either be detected or acts trivially. Analogously, we have the following lemma.

Lemma 1. *An additive quantum-error-correcting code Q with associated space $\bar{S}$ can correct a set of errors $\Sigma \subseteq E$ precisely when $\bar{e}_1^{-1}\bar{e}_2 \notin \bar{S}^\perp \setminus \bar{S}$ for all $e_1, e_2 \in \Sigma$.*

Proof. Suppose an error $e \in E$ has occurred. In order to correct e we must find some error $e_1 \in E$ such that $e_1^{-1}e$ acts trivially on Q, i.e., $e_1^{-1}e \in S$. In other words, we must determine the coset eS. The hypothesis implies that every coset of $S^\perp$ contains at most one coset of S intersecting Σ. It therefore suffices to determine the coset $eS^\perp$. Recall that $E/S^\perp$ permutes the eigenspaces of S regularly. If we measure in which eigenspace we now lie (which we can do because distinct eigenspaces are orthogonal) we can immediately read off $eS^\perp$. This measurement has no effect on the state, since the state lies inside one of the eigenspaces.

On the other hand, suppose e_1 and e_2 are two errors such that $\bar{e}_1^{-1}\bar{e}_2 \in \bar{S}^\perp \setminus \bar{S}$. Any correction procedure must take any state $e_1(v) \in e_1(Q)$ to v. Since $e_1^{-1}e_2 \in S^\perp$, $e_2(v) \in e_1(Q)$, so $e_2(v)$ is corrected to $e_1^{-1}e_2(v)$. However, since $e_1^{-1}e_2 \notin S$, there is a state $v \in Q$ such that

$e_1^{-1}e_2(v)$ is not proportional to v, and we have failed to correct e_2. □

It follows from the Lemma that if we let d be the minimal weight of $\bar{S}^\perp \setminus \bar{S}$, the code can correct the set of all errors of weight at most $[(d-1)/2]$. We have now completed the proof of Theorem 1: Q maps k qubits into n qubits and can correct $[(d-1)/2]$ errors.

Recall that the eigenspaces of S are in one-to-one correspondence with characters of S satisfying $\chi(iI) = i$. To determine which eigenspace contains a given state it is therefore enough to compute this character. Moreover, since χ is a homomorphism, it suffices to compute the character on a basis for $\bar{S}$. Each element of the basis thus provides one bit of information; the collection of these bits is the *syndrome* of the error. Of course, as in classical coding theory, identifying the most likely error given the syndrome can be a difficult problem. (There is no theoretical difficulty, since in principle an exhaustive search can always be used.)

The Clifford groups. Encoding is carried out with the help of a family of groups called Clifford groups.[2] There are both complex (denoted by L) and real (denoted by L_R) versions of these groups.

The *complex Clifford group* L is defined to be the subgroup of the normalizer of E in $U(2^n)$ that contains entries from $\mathbb{Q}[\eta]$, $\eta = (1+i)/\sqrt{2}$. The full normalizer of E in $U(2^n)$ has an infinite center consisting of the elements $e^{2\pi i\theta}I$, $\theta \in \mathbb{R}$. Although these central elements have no effect quantum-mechanically, we wish to work with a finite group. The smallest coefficient ring we can use is $\mathbb{Q}[\eta]$, since

$$\left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \right\}^3 = \begin{pmatrix} \eta & 0 \\ 0 & \eta \end{pmatrix} .$$

The *real Clifford group* L_R is the real subgroup of L, or equivalently the subgroup of L with entries from $\mathbb{Q}[\sqrt{2}]$. If we define E_R to the real subgroup of E, then L_R is the normalizer of E_R in the orthogonal group $O(2^n)$. The group E_R consists of the tensor products $\pm w_1 \otimes \cdots \otimes w_n$, where each w_j is one of I, σ_x, σ_z, $\sigma_x\sigma_z$. E_R is an extraspecial 2-group with order 2^{2n+1} and center $\{\pm I\}$, and $E_R/\{\pm I\} = E/\Xi(E) = \bar{E}$. For many applications it is simpler to work with the real groups E_R and L_R rather than E and L.

The following are explicit generators for these groups. First, L is generated by E, all matrices of the form

$$I_2 \otimes \cdots \otimes I_2 \otimes H_2 \otimes I_2 \otimes \cdots \otimes I_2 \ , \tag{3}$$

[2] We follow Bolt et al. ([6], [7]) in calling these Clifford groups. The same name is used for a different family of groups by Chevalley [19] and Jacobson [40].

where $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and all matrices $\mathrm{diag}(i^{\phi(v)})_{v \in V}$, where ϕ is any $\mathbb{Z}_4$-valued quadratic form on V. Similarly, L_R is generated by E_R, (3) and all matrices $\mathrm{diag}((-1)^{\phi(v)})_{v \in V}$, where ϕ is now any $\mathbb{Z}_2$-valued quadratic form on V.

We also record some further properties of L and L_R:

- $L/\langle E, \eta I \rangle$ is isomorphic to the symplectic group $Sp_{2n}(2)$ (the group of $2n \times 2n$ matrices over $\mathbb{Z}_2$ preserving the inner product (1) [23]).
- L has order $8|Sp_{2n}(2)|2^{2n}$
$$= 2^{n^2+2n+3} \prod_{j=1}^{n} (4^j - 1) \ .$$
- L_R/E_R is isomorphic to the orthogonal group $O^+_{2n}(2)$ [23].
- L_R has order $2|O^+_{2n}(2)|2^{2n}$
$$= 2^{n^2+n+2}(2^n - 1) \prod_{j=1}^{n-1} (4^j - 1) \ .$$
- L acts on $\bar{E}$ as the symplectic group $Sp_{2n}(2)$; L_R acts on $\bar{E}$ as the orthogonal group $O^+_{2n}(2)$.

The groups L and L_R have arisen in several different contexts, and provide a link between quantum codes, the Barnes-Wall lattices [6], [7], [71], the construction of orthogonal spreads and Kerdock sets [12], the construction of spherical codes [41], [64], [65], and the construction of Grassmannian packings [63], [13]. They have also occurred in several purely group-theoretic contexts — see [12] for references. These groups are discussed further in the final paragraphs of the present paper.

Encoding an additive code Q. Since $Sp_{2n}(2)$ acts transitively on isotropic subspaces, and E acts transitively on eigenspaces for a given subspace, the Clifford group L acts transitively on additive codes. One such code is the trivial code corresponding to the subspace $\bar{S}$ with generators $(0|e_i)$, $i = k+1, \ldots, n$. By transitivity we can find an element $\lambda \in L$ which takes the trivial code to Q. Of course λ is not unique. Cleve and Gottesman [21] have given explicit gate descriptions to doing this.

Pure vs. degenerate. In the quantum coding literature there is an important distinction made between degenerate and nondegenerate codes. A *nondegenerate* code is one for which different elements of E produce linearly independent results when applied to elements of the

code. We will find it convenient to introduce a second dichotomy, between pure and impure codes. We will say that a code is *pure* if distinct elements of E produce orthogonal results.

It is straightforward to verify that, for additive codes, 'pure' and 'nondegenerate' coincide. In general, however, a pure code is nondegenerate but the converse need not be true.

For many purposes the pure/impure distinction is the correct one to use for generalizing results from additive to nonadditive codes, and we will therefore use this terminology throughout the paper.

Bases. To find an explicit basis for Q we may proceed as follows. Choose a maximal isotropic subspace $\bar{T}$ containing $\bar{S}$, and consider the 1-dimensional eigenspaces of T. We obtain a basis for Q by selecting those eigenspaces for which the corresponding character agrees with the given character on S. (Equivalently, we may take all the eigenspaces lying inside Q.) The choice of T is of course not unique, and we have the same freedom in choosing a basis as we did earlier when choosing the element λ of the Clifford group.

We conclude this section by restating Theorem 1 in more detail.

Theorem 1. *Suppose $\bar{S}$ is an $n-k$-dimensional linear subspace of $\bar{E}$ which is contained in its dual $\bar{S}^{\perp}$ (with respect to the inner product (1)), and is such that there are no vectors of weight $\leq d-1$ in $\bar{S}^{\perp} \setminus \bar{S}$. Then by taking an eigenspace (for any chosen linear character) of $\bar{S}$, we obtain a quantum-error-correcting code mapping k qubits to n qubits which can correct $[(d-1)/2]$ errors.*

3. From binary spaces to codes over $GF(4)$

As is customary (cf. [52]) we take the Galois field $GF(4)$ to consist of the elements $\{0, 1, \omega, \bar{\omega}\}$, with $\omega^2 = \omega + 1$, $\omega^3 = 1$, and conjugation defined by $\bar{x} = x^2$; the trace map $\mathrm{Tr} : GF(4) \to \mathbb{Z}_2$ takes x to $x + \bar{x}$. The *Hamming weight* of a vector $u \in GF(4)^n$, written $\mathrm{wt}(u)$, is the number of nonzero components, and the *Hamming distance* between $u, u' \in GF(4)^n$ is $\mathrm{dist}(u, u') = \mathrm{wt}(u - u')$. The minimal Hamming distance between the members of a subset C of $GF(4)^n$ will be denoted by $\mathrm{dist}(C)$.

To each vector $v = (a|b) \in \bar{E}$ we associate the vector $\phi(v) = \omega a + \bar{\omega} b \in GF(4)^n$. It is immediate that the weight of v is equal to the Hamming weight of $\phi(v)$, and the distance between vectors $v = (a|b)$, $v' = (a'|b') \in \bar{E}$ is equal to $\mathrm{dist}(\phi(v), \phi(v'))$. The symplectic inner product of v and v' (see (1)) is equal to $\mathrm{Tr}(\phi(v) \cdot \overline{\phi(v')})$, where the bar denotes conjugation in

$GF(4)$, since

$$\begin{aligned}\mathrm{Tr}(\phi(v)\cdot\overline{\phi(v')}) &= \mathrm{Tr}((\omega a+\bar{\omega}b)\cdot(\bar{\omega}a'+\omega b'))\\ &= (a\cdot a')\mathrm{Tr}(1)+(a\cdot b')\mathrm{Tr}(\bar{\omega})+(a'\cdot b)\mathrm{Tr}(\omega)+(b\cdot b')\mathrm{Tr}(1)\\ &= a\cdot b'+a'\cdot b\ .\end{aligned}$$

If $\bar{S}$ is a linear subspace of $\bar{E}$ then $C=\phi(\bar{S})$ is a subset of $GF(4)^n$ which is closed under addition. We shall refer to C as an *additive* code over $GF(4)$, and refer to it as an $(n,2^k)$ code if it contains 2^k vectors. If C is also closed under multiplication by ω, we say it is *linear*.

The *trace inner product* of vectors $u,v\in GF(4)^n$ will be denoted by

$$u*v=\mathrm{Tr}\,u\cdot\bar{v}=\sum_{j=1}^{n}(u_j\bar{v}_j+\bar{u}_jv_j)\ . \tag{4}$$

If C is an $(n,2^k)$ additive code, its dual is defined to be

$$C^{\perp}=\{u\in GF(4)^n : u*v=0 \ \text{ for all } \ v\in C\}\ . \tag{5}$$

Then $C^{\perp}$ is an $(n,2^{2n-k})$ code. If $C\subseteq C^{\perp}$ we say C is *self-orthogonal*, and if $C=C^{\perp}$ then C is *self-dual*.

Theorem 1 can now be reformulated.

Theorem 2. *Suppose C is an additive self-orthogonal subcode of $GF(4)^n$, containing 2^k vectors, such that there are no vectors of weight $\le d-1$ in $C^{\perp}\setminus C$. Then any eigenspace of $\phi^{-1}(C)$ is a quantum-error-correcting code with parameters $[[n,n-k,d]]$.*

We say that C is *pure* if there are no nonzero vectors of weight $<d$ in $C^{\perp}$; otherwise we call C *impure*. Note that the associated quantum-error-correcting code is pure in the sense of Section 2 if and only if C is pure. We also say that a quantum-error-correcting code is *linear* if the associated additive code C is linear.

When studying $[[n,k,d]]$ codes we allow $k=0$, adopting the convention that this corresponds to a self-dual $(n,2^n)$ code C in which the minimal nonzero weight is d. In other words, an $[[n,0,d]]$ code is "pure" by convention. An $[[n,0,d]]$ code is then a quantum state such that, when subjected to a decoherence of $[(d-1)/2]$ coordinates, it is possible to determine exactly which coordinates were decohered. Such a code might be useful for example in testing whether certain storage locations for qubits are decohering faster than they should. These codes are the subject of Section 6.

Most codes over $GF(4)$ that have been studied before this have been linear and duality has been defined with respect to the hermitian inner product $u \cdot \bar{v}$. We shall refer to such codes as *classical.*

Theorem 3. *A linear code C is self-orthogonal (with respect to the trace inner product (4)) if and only if it is classically self-orthogonal with respect to the hermitian inner product.*

Proof. The condition is clearly sufficient. Suppose C is self-orthogonal. For $u, v \in C$ let $u \cdot \bar{v} = \alpha + \beta\omega$, $\alpha, \beta \in \mathbb{Z}_2$. Then $\mathrm{Tr}(u \cdot \bar{v}) = 0$ implies $\beta = 0$, and $\mathrm{Tr}(u \cdot \bar{\omega}\bar{v}) = 0$ implies $\alpha = 0$, so $u \cdot \bar{v} = 0$. □

The following terminology applies generally to additive codes over $GF(4)$. We specify an $(n, 2^k)$ additive code by giving either a $k \times n$ *generator matrix* whose rows span the code additively, or by listing the generators inside diamond brackets $\langle \ \rangle$. If the code is linear a $k/2 \times n$ generator matrix will suffice, whose rows are a $GF(4)$-basis for the code.

Let $\mathcal{G}_n$ denote the group of order $6^n n!$ generated by permutations of the n coordinates, multiplication of any coordinates by ω, and conjugation of any coordinates. Equivalently, $\mathcal{G}_n$ is the wreath product of S_3 by S_n generated by permutations of the coordinates and arbitrary permutations of the nonzero elements of $GF(4)$ in each coordinate. $\mathcal{G}_n$ preserves weights and trace inner products. Two additive codes over $GF(4)$ of length n are said to be *equivalent* if one can be obtained from the other by applying an element of $\mathcal{G}_n$. The subgroup of $\mathcal{G}_n$ fixing a code C is its *automorphism group* $Aut(C)$. The number of codes equivalent to C is then equal to

$$\frac{6^n n!}{Aut(C)} \ . \tag{6}$$

We determine the automorphism group of an $(n, 2^k)$ additive code C by the following artifice. We map C to a $[3n, k]$ binary linear code $\beta(C)$ by applying the map $0 \to 000$, $1 \to 011$, $\omega \to 101$, $\bar{\omega} \to 110$ to each generator of C. Let Ω denote the $(n, 2^{2n})$ code containing all vectors, and form $\beta(\Omega)$. Using a program such as MAGMA [8], [9], [10] we compute the automorphism groups of the binary linear code $\beta(C)$ and $\beta(\Omega)$; their intersection is $Aut(C)$.

Any $(n, 2^k)$ additive code is equivalent to one with generator matrix of the form

$$\begin{bmatrix} I_{k_0} & \omega B_1 & A_1 \\ \omega I_{k_0} & \omega B_2 & A_2 \\ 0 & I_{k_1} & B_3 \end{bmatrix} \ ,$$

where I_r denotes an identity matrix of order r, A_j is an arbitrary matrix, B_j is a binary matrix, and $k = 2k_0 + k_1$. An $(n, 2^k)$ code is called *even* if the weight of every codeword is even, and otherwise *odd*.

Theorem 4. *An even additive code is self-orthogonal. A self-orthogonal linear code is even.*

Proof. The first assertion holds because

$$\mathrm{wt}(u+v) \equiv \mathrm{wt}(u) + \mathrm{wt}(v) + u * v \pmod 2 \tag{7}$$

for all $u, v \in GF(4)^n$, and the second because

$$u * (\omega u) \equiv \mathrm{wt}(u) \pmod 2 \ . \tag{8}$$

□

The *weight distribution* of an $(n, 2^k)$ additive code C is the sequence $A_0, \ldots, A_n$, where A_j is the number of vectors in C of weight j. It is easy to see that the weight distribution of any translate $u+C$, for $u \in C$, is the same as that of C, and so the minimal distance between vectors of C is equal to the minimal nonzero weight in C. The polynomial $W(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j$ is the *weight enumerator* of C (cf. [52]).

Theorem 5. *If C is an $(n, 2^k)$ additive code with weight enumerator $W(x, y)$, the weight enumerator of the dual code $C^\perp$ is given by $2^{-k} W(x + 3y, x - y)$.*

Proof. This result, analogous to the MacWilliams identity for linear codes, follows from the general theory of additive codes developed by Delsarte [28], since our trace inner product is a special case of the symmetric inner products used in [28]. □

4. General constructions

In this section we describe some general methods for modifying and combining additive codes over $GF(4)$.

The *direct sum* of two additive codes is defined in the natural way: $C \oplus C' = \{uv : u \in C, v \in C'\}$. In this way we can form the direct sum of two quantum-error-correcting codes, combining $[[n, k, d]]$ and $[[n', k', d']]$ codes to produce an $[[n + n', k + k', d'']]$ code, where $d'' = \min\{d, d'\}$. An additive code which is not a direct sum is called *indecomposable*.

Theorem 6. *Suppose an* $[[n, k, d]]$ *code exists. (a) If* $k > 0$ *then an* $[[n+1, k, d]]$ *code exists. (b) If the code is pure and* $n \geq 2$ *then an* $[[n-1, k+1, d-1]]$ *code exists. (c) If* $k > 1$ *or if* $k = 1$ *and the code is pure, then an* $[[n, k-1, d]]$ *code exists. (d) If* $n \geq 2$ *then an* $[[n-1, k, d-1]]$ *code exists. (e) If* $n \geq 2$ *and the associated code* C *contains a vector of weight 1 then an* $[[n-1, k, d]]$ *code exists.*

Proof. Let C and $C^\perp$ be the associated $(n, 2^{n-k})$ and $(n, 2^{n+k})$ additive codes, respectively, with $C \subset C^\perp$. (a) Form the direct sum of C with $c_1 = \{0, 1\}$. The resulting $[[n+1, k, d]]$ code is impure (which is why the construction fails for $k = 0$). (b) Puncture $C^\perp$ (cf. [52]) by deleting the first coordinate, obtaining an $(n-1, 2^{n+k})$ code $B^\perp$ (say) with minimal distance at least $d-1$. The dual of $B^\perp$ consists of the vectors u such that $0u \in C$, and so is contained in $B^\perp$. (c) There are $(n, 2^{n-k+1})$ and $(n, 2^{n+k-1})$ additive codes B and $B^\perp$ with $C \subset B \subset B^\perp \subset C^\perp$. (d) Take $B = \{u : 0u \text{ or } 1u \in C\}$, so that $B^\perp = \{v : 0v \text{ or } 1v \in C^\perp\}$. The words in $B^\perp \setminus B$ arise from truncation of words in $C^\perp \setminus C$. Any words in $C^\perp \setminus C$ of weight less than d either begin with ω or $\bar{\omega}$, and so are not in $B^\perp$, or begin with a 0 or 1, and so (after truncation) are in $B^\perp \setminus B$. Words of weight d in $C^\perp$ beginning with 1 become words of weight $d-1$, so the minimal distance in general is reduced by 1. The proof of (e) is left to the reader. □

To illustrate Part (a) of the theorem, from the $[[5, 1, 3]]$ Hamming code (see Section 5) we obtain an impure $[[6, 1, 3]]$ code. On the other hand exhaustive search (or integer programming, see Section 7) shows that no pure $[[6, 1, 3]]$ exists. This is the first occasion when an impure code exists but a pure one does not.

A second $[[6, 1, 3]]$ code, also impure not equivalent to the first, is generated by 000011, 011110, $0\omega\omega\omega\omega\omega$, $101\omega\bar{\omega}\omega$, $\omega 0\omega\bar{\omega}10$. Up to equivalence, there are no other $[[6, 1, 3]]$ codes.

If we have additional information about C then there is a more powerful technique (than that in Theorem 6(d)) for shortening a code.

Lemma 2. *Let* C *be a linear self-orthogonal code over* $GF(4)$*. Suppose* S *is a set of coordinates of* C *such that every codeword of* C *meets* S *in a vector of even weight. Then the code obtained from* C *by deleting the coordinates in* S *is also self-orthogonal.*

Proof. Follows from Theorem 4. □

Theorem 7. *Suppose we have a linear* $[[n, k, d]]$ *code with associated* $(n, 2^{n-k})$ *code* C*. Then there exists a linear* $[[n-m, k', d']]$ *code with* $k' \geq k-m$ *and* $d' \geq d$*, for any* m *such that there*

exists a codeword of weight m in the dual of the binary code generated by the supports of the codewords of C.

Proof. Let S be the support of such a word of weight m. Then S satisfies the conditions of the Lemma, and deleting these coordinates gives the desired code. □

For example, consider the $[[85, 77, 3]]$ Hamming code given in the following section. The code C is an $(85, 2^4)$ code, and the supports of the codewords in C generate a binary code with weight enumerator

$$x^{85} + 3570x^{53}y^{32} + 38080x^{45}y^{40} + 23800x^{37}y^{48} + 85x^{21}y^{64} \ .$$

The MacWilliams transform of this ([52], Theorem 1, p. 127) shows that the dual binary code contains vectors of weights 0, 5 through 80, and 85. From Theorem 7 we may deduce the existence of $[[9, 1, 3]]$, $[[10, 2, 3]], \ldots, [[80, 72, 3]]$ codes (see the entries labeled S in the main table in Section 8).

There is an analogue of Theorem 7 for additive codes, but the construction of the corresponding binary code is somewhat more complicated.

The direct sum construction used inTheorem 6(a) can be generalized.

Theorem 8. *Given two codes $[[n_1, k_1, d_1]]$ and $[[n_2, k_2, d_2]]$ with $k_2 \leq n_1$ we can construct an $[[n_1 + n_2 - k_2, k_1, d]]$ code, where $d \geq \min\{d_1, d_1 + d_2 - k_2\}$.*

Proof. Consider the associated codes C_1, $C_1^\perp$ with parameters $(n_1, 2^{n_1-k_1})$, $(n_1, 2^{n_1+k_1})$ and C_2, $C_2^\perp$ with parameters $(n_2, 2^{n_2-k_2})$, $(n_2, 2^{n_2+k_2})$. Let ρ be the composition of the natural map from $C_2^\perp$ to $C_2^\perp/C_2$ with any inner-product preserving map from $C_2^\perp/C_2$ to $GF(4)^{k_2}$. Then we form a new code $C = \{uv : v \in C_2^\perp, u\rho(v) \in C_1\}$, with $C^\perp = \{uv : v \in C_2^\perp, u\rho(v) \in C_1^\perp\}$. If $\rho(v) \neq 0$, v contributes at least d_2 to the weight of uv, but u need have weight only $d_1 - k_2$. If $\rho(v) = 0$, and $uv \neq 0$, $\mathrm{wt}(u) \geq d_1$. □

Different choices for ρ may produce inequivalent codes. Choosing ρ corresponds to choosing an encoding method for C_2.

For example, if the second code is the $[[1, 0, 1]]$ code with generator matrix [1], the new code has parameters $[[n_1 + 1, k_1, d_1]]$, as in Theorem 6(a). A different $[[n_1 + 1, k, d_1]]$ code is obtained if we take the second code to be the $[[2, 1, 1]]$ code with generator matrix [11]. In particular, the second $[[6, 1, 3]]$ code mentioned above may be obtained in this manner.

Theorem 8 can be used to produce an analogue of concatenated codes in the quantum setting. If Q_1 is an $[[nm, k]]$ code such that the associated $(nm, 2^{nm+k})$ code has minimal nonzero weight d in each m-bit block, and Q_2 is an $[[n_2, m, d_2]]$ code, then encoding each block of Q_1 using Q_2 (as in Theorem 8) produces an $[[nn_2, k, dd_2]]$ *concatenated* code.

A particularly interesting example is obtained by concatenating the $[[5, 1, 3]]$ Hamming code (see Section 5) with itself. We take $Q_1 = Q_2$, and let the associated linear $(5, 2^4)$ code have generator matrix $\begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & \omega & \bar{\omega} \end{bmatrix}$. Then we obtain a $[[25, 1, 9]]$ code for which the associated $(25, 2^{24})$ and $(25, 2^{26})$ linear codes have the generator matrices shown in Fig. 1. Although the Hamming code is pure, the concatenated code is not.

Figure 1: Generator matrices for a $(25, 2^{24})$ linear code (above the line) and its dual, a $(25, 2^{26})$ linear code (all rows), corresponding to a $[[25, 1, 9]]$ quantum code.

$$\left[\begin{array}{c}
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,\omega\,\bar{\omega} \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,\omega\,\bar{\omega}\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,1\,\omega\,\bar{\omega}\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,1\,0\,1\,\omega\,\bar{\omega}\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
1\,0\,1\,\omega\,\bar{\omega}\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,0\,0\,0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,1\,\bar{\omega}\,\omega \\
0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,0\,0\,0\,0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,\omega\,1\,\bar{\omega}\,0\,0\,\bar{\omega}\,\omega\,1 \\
\hline
0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,\bar{\omega}\,\omega\,0\,0\,\bar{\omega}\,\omega\,1\,0\,0\,\omega\,1\,\bar{\omega}
\end{array}\right]$$

The construction of quantum codes used in [17] can be restated in the present terminology (and slightly generalized):

Theorem 9. *Let $C_1 \subseteq C_2$ be binary linear codes. By taking $C = \omega C_1 + \bar{\omega} C_2^{\perp}$ in Theorem 2 we obtain an $[[n, k_2 - k_1, d]]$ code, where $d = \min\{\mathrm{dist}(C_2 \setminus C_1), \mathrm{dist}(C_1^{\perp} \setminus C_2^{\perp})\}$.*

Proof. It is easily verified that C is additive and that $C \subseteq C^{\perp} = \bar{\omega} C_1^{\perp} + \omega C_2$. □

Another construction based on binary codes due to Gottesman [35] can be generalized as follows.

Theorem 10. *Let $\mathcal{S}_m$ be the classical binary simplex code of length $n = 2^m - 1$, dimension m and minimal distance 2^{m-1} (Chapter 14 of [52]). Let f be any fixed-point-free automorphism*

of $\mathcal{S}_m$ and let $\mathcal{G}_m$ be the $(2^m, 2^{m+2})$ additive code generated by the vectors $u + \omega f(u)$, $u \in \mathcal{S}_m$, with a 0 appended, together with the vectors $11\ldots1$, $\omega\omega\ldots\omega$ of length 2^m. This yields a $[[2^m, 2^m - m - 2, 3]]$ quantum code.

We omit the proof.

We can show that $\mathcal{G}_m$ has the following properties (again, to save space, the proofs are omitted).

(i) For any choice of f, $\mathcal{G}_m$ has weight enumerator

$$x^{2^m} + 4(2^m - 1)x^{2^{m-2}}y^{3.2^{m-2}} + 3y^{2^m} \ .$$

(ii) The vectors of weight 2^m generate a subcode of dimension 2.

(iii) Suppose $\mathcal{G}_m$ is constructed using the automorphism f, and $\mathcal{G}'_m$ using f'. Then $\mathcal{G}'_m$ is equivalent to $\mathcal{G}_m$ if and only if f' is conjugate under $Aut(\mathcal{S}_m)$ to one of

$$\{f, 1-f, 1/f, 1-1/f, 1/(1-f), f/(1-f)\} \ . \tag{9}$$

(iv) The automorphism group of $\mathcal{G}_m$ has a normal subgroup H which is a semidirect product of the centralizer of f in $Aut(\mathcal{S}_m)$ with $\mathcal{S}_m$, the index $[Aut(\mathcal{G}_m) : H]$ being the number of elements of (9) that are conjugate to f.

(v) $\mathcal{G}_m$ is linear precisely when f satisfies $f^2 + f + 1 = 0$.

Before giving some examples, we remark that $Aut(\mathcal{S}_m)$ is isomorphic to the general linear group $GL_m(2)$, and conjugacy classes of $GL_m(2)$ are determined by their elementary divisors. So the most convenient way to specify f is by listing its elementary divisors.

For $m = 3$, there is a unique choice for f, with elementary divisor $x^3 + x + 1$, and so there is a unique $\mathcal{G}_3$, with parameters $[[8, 3, 3]]$. Then $Aut(\mathcal{G}_3)$ has order 168, and is a semidirect product of a cyclic group C_3 with the general affine group $GA_1(8)$.

For $m = 4$ there are three distinct codes $\mathcal{G}_4$, with parameters $[[16, 10, 3]]$. The corresponding elementary divisors for f are:

(a) $x^2 + x + 1$ (twice). This produces a linear code, with $|Aut(\mathcal{G}_4)| = 17280$. (In general the code is linear precisely when all the elementary divisors are equal to $x^2 + x + 1$.)

(b) $(x^2 + x + 1)^2$, with $|Aut(\mathcal{G}_4)| = 1152$.

(c) $x^4 + x + 1$, with $|Aut(\mathcal{G}_4)| = 480$.

For $m = 5$ there are two distinct $\mathcal{G}_5$ codes, with parameters $[[32, 25, 3]]$. The corresponding elementary divisors are

(a) $x^3 + x + 1$ and $x^2 + x + 1$, with $|Aut(\mathcal{G}_5)| = 2016$.

(b) $x^5 + x^2 + 1$, with $|Aut(\mathcal{G}_5)| = 992$.

Gottesman [37] used just a single f, which he took to be (if m is even)

$$\begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ & \cdot & \cdot & \cdot & \cdots & \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix}$$

while if m is odd the first row is complemented. Gottesman's codes correspond to those labeled (c) (for $m = 4$) and (b) (for $m = 5$).

The codes in Theorem 10 can be extended.

Theorem 11. *For $m \geq 2$, there exists an $[[n, n - m - 2, 3]]$ code, where n is*

$$\sum_{i=0}^{m/2} 2^{2i} \quad (m \text{ even}), \qquad \sum_{i=1}^{(m-1)/2} 2^{2i+1} \quad (m \text{ odd}) \ .$$

Sketch of proof. The corresponding $(n, 2^{m+2})$ additive code C (say) has weight enumerator

$$x^n + (2^{m+2} - 1)x^{n-2^m} y^{2^m} \quad (m \text{ even})$$

or

$$x^n + (2^{m+2} - 2^m)x^{n-2^m+2} y^{2^m-2} + (2^m - 1)x^{n-2^m} y^{2^m} \quad (m \text{ odd}) \ .$$

We take C_2 and C_3 to be the additive codes corresponding to the $[[5, 1, 3]]$ and $[[8, 3, 3]]$ codes already mentioned. For $m > 3$, let $\mathcal{G}_m$ be as in Theorem 10, and let $\mathcal{G}'_m$ be the subcode consisting of the weight 2^m codewords in $\mathcal{G}_m$. Finally, let ϕ be any isomorphism between C_{m-2} and $\mathcal{G}_m/\mathcal{G}'_m$ (note that both are spaces of dimension m). Define a new code C_m to consist of all vectors $v_1 v_2$, where $v_1 \in C_{m-2}$ and $\phi(v_1) = v_2 + \mathcal{G}'_m$. A simple counting argument verifies that C_m has the claimed weight distribution. By applying Theorem 5 we find that $C_m^\perp$ has minimal distance 3. □

Theorem 11 was independently discovered by Gottesman [37].

The resulting codes, like those constructed in Theorem 10, are pure and additive but in general are not linear. For even m we obtain the Hamming codes of Section 5 as well as nonlinear codes with the same parameters. For odd m we obtain $[[8, 3, 3]]$, $[[40, 33, 3]]$,

$[[168, 159, 3]]$, ... codes. A generator matrix for the $(40, 2^7)$ additive code corresponding to a $[[40, 33, 3]]$ code is shown in Fig. 2.

Figure 2: Generator matrix for $(40, 2^7)$ additive code, producing a $[[40, 33, 3]]$ quantum code.

$$\begin{bmatrix}
0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,0\,0\,\omega \\
0\,0\,1\,\bar{\omega}\omega\omega\bar{\omega}\,1\omega\,0\,1\,0\,1\,\bar{\omega}\omega\omega\bar{\omega}\,1\,0\,1\,0\,\omega\bar{\omega}\,1\,0\,\omega\bar{\omega}\omega\bar{\omega}\,1\,0\,0\,1\,\bar{\omega}\omega\bar{\omega}\omega\,0\,1\,\bar{\omega} \\
0\,1\,\omega\omega\,1\,0\,\bar{\omega}\bar{\omega}\,0\omega\,0\,0\omega\,0\omega\bar{\omega}\,1\bar{\omega}\,1\,1\bar{\omega}\,1\bar{\omega}\bar{\omega}\,1\bar{\omega}\,1\,1\bar{\omega}\,1\bar{\omega}\omega\,0\omega\,0\,0\omega\,0\omega\omega \\
0\omega\,0\bar{\omega}\,1\bar{\omega}\,1\omega\,0\,1\,1\,0\,0\,1\,1\omega\omega\bar{\omega}\bar{\omega}\omega\omega\bar{\omega}\bar{\omega}\,0\,0\,1\,1\,0\,0\,1\,1\omega\omega\bar{\omega}\bar{\omega}\omega\omega\bar{\omega}\bar{\omega}\,0 \\
1\,0\omega\,0\omega\bar{\omega}\,1\bar{\omega}\,0\,0\,0\omega\omega\omega\,1\,1\,1\,1\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\,0\,0\,0\,0\omega\omega\omega\,1\,1\,1\,1\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\,0 \\
\omega\,0\omega\,1\bar{\omega}\,1\bar{\omega}\,0\,0\,0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1\omega\omega\omega\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\omega\omega\omega\bar{\omega}\bar{\omega}\bar{\omega}\bar{\omega}\,0
\end{bmatrix}$$

The "$u|u+v$" construction for binary codes ([52], page 76) has an analogue for quantum codes.

Theorem 12. *Suppose there is a pure $[[n, k_1, d_1]]$ code with associated $(n, 2^{n-k_1})$ additive code C_1, and a pure $[[n, k_2, d_2]]$ code with associated code C_2, such that $C_1 \subseteq C_2$. Then there exists a pure $[[2n, k_1 - k_2, d]]$ code, where $d = \min\{2d_1, \delta\}$, $\delta = \mathrm{dist}(C_2)$.*

Proof. Take C to be the $(2n, 2^{2n-k_1+k_2})$ additive code consisting of the vectors $u|u+v$, $u \in C_2^{\perp}$, $v \in C_1$, where the bar denotes concatenation. Then $C^{\perp} = \{u|u+v : u \in C_1^{\perp},\ v \in C_2\}$ has minimal distance $\min\{2d_1, \delta\}$, by Theorem 33 of [52], Chapter 1. □

For example, by combining the $[[14, 8, 3]]$ and $[[14, 0, 6]]$ codes shown in Table II of the next section we obtain a $[[28, 8, 6]]$ code.

Concerning the structure of additive but nonlinear codes, it is pointless to simply add one generator to a linear code. For if D is an $(n, 2^{n+k})$ linear code, and $D' = \langle D, v\rangle$ is an $(n, 2^{n+k+1})$ additive code with minimal distance d, then it is easy to show that the linear code $D'' = \langle D, v, \omega v\rangle$ also has minimal distance d.

We end this section by listing some trivial codes. An $[[n, k, 1]]$ code exists for all $0 \le k \le n$, $n \ge 1$. An $[[n, k, 2]]$ code exists provided $0 \le k \le n-2$, if $n \ge 2$ is even, or provided $0 \le k \le n-3$ if $n \ge 3$ is odd.

5. Cyclic and related codes

An $(n, 2^k)$ additive code C is *constacyclic* if there is a constant κ (which in our case will be $1, \omega$ or $\bar{\omega}$) such that $(u_0, u_1, \ldots, u_{n-1}) \in C$ implies $(\kappa u_{n-1}, u_0, u_1, \ldots, u_{n-2}) \in C$. If $\kappa = 1$

the code is *cyclic*. Besides these standard terms from the classical theory, we also need a new concept: if $(u_0, u_1, \ldots, u_{n-1}) \in C$ implies $(\bar{u}_{n-1}, u_0, u_1, \ldots, u_{n-2}) \in C$, the code will be called *conjucyclic*.

We begin with linear codes. If vectors are represented by polynomials in the natural way, a *linear* constacyclic code is represented by an ideal in the ring of polynomials modulo $x^n - \kappa$ ([52], [47]). The latter is a principal ideal ring, so the code consists simply of all multiples of a single generator polynomial $g(x)$, which must divide $x^n - \kappa$. We assume n is odd.

Theorem 13. *A linear cyclic or constacyclic code with generator polynomial $g(x)$ is self-orthogonal if and only if*

$$g(x)g^\dagger(x) \equiv 0 \pmod{x^n - \kappa} ,$$

where if $g(x) = \sum_{j=0}^{n-1} g_j x^j$,

$$g^\dagger(x) = \kappa \bar{g}_0 + \sum_{j=1}^{n-1} \bar{g}_{n-j} x^j . \tag{10}$$

We omit the elementary proof (cf. [15]). Note that

$$g^\dagger(x) \equiv \overline{g(x^{-1})} \pmod{x^n - \kappa} .$$

The † operation induces an involution on factors of $x^n - \kappa$, so we can write

$$x^n - \kappa = \prod_i p_i(x) \prod_j (q_j(x) q_j^\dagger(x)) , \tag{11}$$

where the p_i, q_j and $q_j^\dagger$ are all distinct and $p_i^\dagger = p_i$. Then a divisor $g(x)$ of $x^n - \kappa$ generates a self-orthogonal linear constacyclic code if and only if $g(x)$ is divisible by each of the p_i's and by at least one from each q_j, $q_j^\dagger$ pair.

Example. The classical *Hamming code* H over $GF(4)$ has length $n = (4^m - 1)/3$, contains 4^{n-m} codewords and has minimal distance 3, for $m \geq 1$ [52], [50]. The dual code $C = H^\perp$ is a self-orthogonal linear code, and the corresponding quantum code has parameters $[[n, n-2m, 3]]$, where $n = (4^m - 1)/3$. C and H are cyclic if m is even, constacyclic if m is odd. For example when $m = 2$ we can take H to have generator polynomial $g(x) = x^2 + \omega x + 1$, a divisor of $x^5 - 1$, and when $m = 3$ we take $g(x) = x^3 + x^2 + x + \omega$, a divisor of $x^{21} - \omega$. These codes meet the sphere-packing bound (14) (see Section 7) with equality. The smallest Hamming code, a $[[5, 1, 3]]$ code, was independently discovered in the present context by [5] and [48]. See also [16].

Hamming codes correct single errors. In the classical theory the generalizations of Hamming codes that correct multiple errors are known as BCH codes [52]. A similar generalization yields multiple-error correcting quantum codes.

Rather than giving a complete analysis of these codes, which involves a number of messy details, we simply outline the construction and give some examples. These *quantum BCH codes* may be cyclic or constacyclic.

In the cyclic case we let ξ be a primitive n-th root of unity in some extension field of $GF(4)$, and write each factor q_j in (11) as $q_j(x) = \prod_{s\in S_j}(x-\xi^s)$, the *zero set* S_j being a cyclotomic coset modulo n under multiplication by 4 (see [52], Chap. 7). The zero set associated with $q_j^\dagger$ is then $-2S_j$. We choose a minimal subset of the q_j's subject to the conditions that (a) there is an arithmetic progression of length $d-1$ in the union of its zero sets, for which the step size is relatively prime to n, and (b) if q_j is chosen, $q_j^\dagger$ is not. Let B be the cyclic code whose generator polynomial is the product of the q_j's. Then (a) guarantees that B has minimal distance at least d and (b) guarantees that $B \supset B^\perp$. In this way we obtain a quantum error-correcting code with parameters $[[n,k,d]]$, where $k = n - 2\deg g$.

A similar construction works in the constacyclic case, only now we choose ξ to be a primitive $(3n)$-th root of unity.

In the special case when $n = (4^m-1)/3$, most of the q_j have degree m, and we obtain a sequence of cyclic or constacyclic codes which provided m is at least 4, begins

$$[[n, n-2m, 3]], [[n, n-4m, 4]], [[n, n-6m, 5]], [[n, n-8m, 7]], \ldots \ .$$

For example when $m=4$ we obtain $[[85,77,3]]$, $[[85,69,4]]$, $[[85,61,5]]$ and $[[85,53,7]]$ codes.

We now discuss additive (but not necessarily linear) codes. Note that an additive constacyclic code (with $\kappa = \omega$ or $\bar\omega$) is necessarily linear.

Theorem 14. *(a) Any $(n, 2^k)$ additive cyclic code C has two generators, and can be represented as $\langle \omega p(x) + q(x), r(x)\rangle$, where $p(x)$, $q(x)$, $r(x)$ are binary polynomials, $p(x)$ and $r(x)$ divide $x^n - 1 \pmod 2$, $r(x)$ divides $q(x)(x^n-1)/p(x) \pmod 2$, and $k = 2n - \deg p - \deg r$. (b) If $\langle \omega p'(x) + q'(x), r'(x)\rangle$ is another such representation, then $p'(x) = p(x)$, $r'(x) = r(x)$ and $q'(x) \equiv q(x) \pmod{r(x)}$. (c) C is self-orthogonal if and only if*

$$\begin{aligned} p(x)r(x^{n-1}) &\equiv p(x^{n-1})r(x) \equiv 0 \pmod{x^n-1}\ , \\ p(x)q(x^{n-1}) &\equiv p(x^{n-1})q(x) \pmod{x^n-1}\ . \end{aligned}$$

Proof. (a) Consider the map Tr : $C \to \mathbb{Z}_2[x]/(x^n-1)$ obtained by taking traces componentwise. The kernel of this map is a binary cyclic code, so can be represented uniquely as $\langle r(x)\rangle$, where $r(x)$ divides x^n-1. The image of the map is similarly a binary cyclic code $\langle p(x)\rangle$. The original code is generated by $r(x)$ and some inverse image of $p(x)$, say $\omega p(x)+q(x)$. Finally, if $r(x)$ did not divide $q(x)(x^n-1)/p(x)$, then $((x^n-1)/p(x))(\omega p(x)+q(x))$ would be a binary vector of C not in $\langle r(x)\rangle$, a contradiction. We omit the proof of (b). (c) One readily verifies that the inner product of the vectors corresponding to $\omega f(x)+g(x)$ and $\omega h(x)+i(x)$ is given by the constant coefficient of

$$f(x)i(x^{n-1})+g(x)h(x^{n-1}) \pmod{x^n-1} .$$

But then the inner product of the vectors corresponding to $\omega f(x)+g(x)$ and $x^m(\omega h(x)+i(x))$ is given by the coefficient of x^m in $f(x)i(x^{n-1})+g(x)h(x^{n-1})$. The result follows immediately. □

We remark without giving a proof that if C is self-orthogonal we may assume that $q(x)$ satisfies

$$q(x^{n-1}) = \frac{\pi(x)}{p(x)} + \frac{\sigma(x)(x^n-1)}{p(x)} , \tag{12}$$

and $r(x)$ divides $q(x)(x^n-1)/p(x)$, where $\pi(x) \equiv \pi(x^{n-1}) \pmod{x^n-1}$, $\pi(x) \equiv 0 \pmod{p(x)}$, and $\deg\sigma < \deg r + \deg p - n$. This makes it possible to search through all self-orthogonal additive cyclic codes of a given dimension: $r(x)$ ranges over all divisors of x^n-1, $p(x)$ ranges over all divisors of $(x^n-1)/gcd\{r(x^{n-1}), x^n-1\}$ of the appropriate degree, and finally all choices for $\pi(x)$ and $\sigma(x)$ must be considered.

Table I lists some additive cyclic codes that were found in this way.

Table I: Cyclic codes.

Parameters	Generators for additive code
$[[15,0,6]]$	$\omega 1\,1\,0\,1\,0\,1\,0\,0\,1\,0\,1\,0\,1\,1$
$[[21,0,8]]$	$\bar{\omega}\bar{\omega}1\omega 0\,0\,1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,1\,1\,0\,0\,0$, $1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,0\,1\,1\,1\,0\,0\,1\,0\,1\,1\,0\,0$
$[[23,0,8]]$	$\omega 0\,1\,0\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,0\,1\,0$
$[[23,12,4]]$	$\bar{\omega}\bar{\omega}\omega\bar{\omega}\omega 1\,1\,\bar{\omega}\,1\,1\,\omega\,1\,\omega\,1\,0\,1\,1\,0\,0\,0\,0\,0$
$[[25,0,8]]$	$1\,1\,1\,0\,1\,0\,\omega\,0\,1\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0$

Theorem 15. *Let C be an $(n, 2^k)$ additive conjucyclic code, and form the binary code*

$$C' = \{\mathrm{Tr}(\omega u)|\mathrm{Tr}(\bar{\omega}u) : u \in C\} \ ,$$

when the trace is applied componentwise and the bar denotes concatenation. Then C' is a binary cyclic code of length $2n$, which is self-orthogonal if and only if C is self-orthogonal.

We omit the proof. Note that C' determines C, since

$$\omega\mathrm{Tr}(\omega u) + \bar{\omega}\mathrm{Tr}(\omega u) = u \ .$$

Theorem 15 makes it possible to search for codes of this type. So far no record codes have been found.

We now return to linear codes. A *quasicyclic* code is a code of length $n = ab$ on which the group acts as a cycles of length b. T. A. Gulliver of Carleton University (Canada) and the University of Canterbury (New Zealand) has extensively studied quasicyclic codes over small fields [38]. The last five examples in Table II were found by him. Double parentheses indicate the permutation to be applied.

Table II: Linear quasicyclic codes.

Parameters	Generator
$[[14, 0, 6]]$	$((1000000))\ ((\bar{\omega}1\bar{\omega}\omega00\omega))$
$[[14, 8, 3]]$	$((1011100))\ ((1\bar{\omega}\omega\omega10\bar{\omega}))$
$[[15, 5, 4]]$	$((10000))\ ((11\bar{\omega}00))\ ((11\omega\omega0))$
$[[18, 6, 5]]$	$((110000))\ ((101\bar{\omega}00))\ ((11\omega1\omega0))$
$[[20, 10, 4]]$	$((10000))\ ((1\bar{\omega}100))\ ((1111\omega))\ ((11\bar{\omega}\omega\bar{\omega}))$
$[[25, 15, 4]]$	$((10000))\ ((1\omega1\omega0))\ (0101\bar{\omega}))\ ((1\omega\bar{\omega}\omega1))\ ((10\omega\omega0))$
$[[28, 14, 5]]$	$((\omega\omega\bar{\omega}1000))\ ((\bar{\omega}0\bar{\omega}1000))\ ((1\bar{\omega}\bar{\omega}1\omega\bar{\omega}0))\ ((\bar{\omega}\omega\bar{\omega}\omega\omega00))$
$[[30, 20, 4]]$	$((11100))\ ((10\omega00))\ ((11\bar{\omega}\omega0))\ ((1\omega1\omega\bar{\omega}))\ ((10\omega10))\ ((1\omega100))$
$[[40, 30, 4]]$	$((001\omega\omega))\ ((011\omega1))\ ((0010\bar{\omega}))\ ((001\omega1))\ (00101)\ ((1\omega1\omega\bar{\omega}))\ ((111\bar{\omega}\omega))\ ((01\omega1\bar{\omega}))$

6. Self-dual codes

In this section we study $[[n, 0, d]]$ quantum-error-correcting codes and their associated $(n, 2^n)$ self-dual codes C. These codes are of interest in their own right — for instance, the

unique $[[2,0,2]]$ code corresponds to the quantum state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, that is, an EPR pair. They are also important for constructing $[[n,k,d]]$ codes with $k > 0$, as we will see in Section 8.

We begin with some properties of weight enumerators of self-dual codes.

Theorem 16. *(a) The weight enumerator of a self-dual code is fixed under the transformation*

$$\text{replace } \begin{pmatrix} x \\ y \end{pmatrix} \text{ by } \frac{1}{2}\begin{pmatrix} 1 & 3 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}, \tag{13}$$

and is therefore a polynomial in $x+y$ and x^2+3y^2. (b) The minimal distance of a self-dual code of length n is $\leq [n/2]+1$.

Proof. (a) (13) follows from Theorem 5, and the proof of the second assertion is parallel to that of Theorem 13 of [51]. (b) Parallel to the proof of Corollary 3 of [53]. □

(The result in (b) has since been improved — see Section 9.)

Theorem 17. *(a) The weight enumerator of an even self-dual code is a polynomial in x^2+3y^2 and $y^2(x^2-y^2)^2$. (b) The minimal distance of an even self-dual code of length n is $\leq 2[n/6]+2$.*

Proof. (a) This is an immediate consequence of Theorem 13 of [51]. (b) From Corollary 15 of [51]. □

In view of the importance of *doubly-even* self-dual codes in binary coding theory, we also note the following result.

Theorem 18. *If there is an integer constant $c > 1$ such that the weight of every vector in a self-dual code is divisible by c, then $c = 2$.*

Proof. The proof of the Gleason-Prange theorem for classical self-dual codes as given in [66] applies unchanged. □

It is possible to give a complete enumeration of all self-dual codes of modest length, following the methods of [51] and [24].

Theorem 19. *(a) The total number of self-dual codes of length n is $\prod_{j=1}^{n}(2^j+1)$.*

(b)
$$\sum \frac{1}{|Aut(C)|} = \frac{\prod_{j=1}^{n}(2^j+1)}{6^n n!},$$

where the sum is over all inequivalent self-dual codes C of length n.

Proof. (a) Parallel to that of Theorem 19 of [51]. (b) From (a) and (6). □

Let d_n be the $(n, 2^{n-1})$ code spanned by all even-weight binary vectors of length n, $n \geq 2$, and let $d_n^+ = \langle d_n, \omega\omega \ldots \omega \rangle$.

Theorem 20. *Suppose C is a self-orthogonal additive code, in which no coordinate is identically zero, and which is generated by words of weight 2. Then C is equivalent to a direct sum $d_2^+ \oplus \ldots \oplus d_2^+ \oplus d_i \oplus d_j \oplus d_k \oplus \ldots$, i, j, $k \geq 2$.*

Proof. Analogous to that of Theorem 4 of [24]. □

With the help of Theorems 19 and 20 we find that the numbers t_n (respectively i_n) of inequivalent (respectively inequivalent indecomposable) self-dual codes of length n for $n \leq 5$ are

n	1	2	3	4	5
t_n	1	2	3	6	11
i_n	1	1	1	2	4

This enumeration could be extended to larger values of n without too much difficulty.

The indecomposable codes mentioned in the above table are the trivial code c_1, the codes d_n^+ for $n \geq 2$, the length 4 code $\langle 1100, 0011, \omega\omega\omega\omega, 01\omega\bar{\omega} \rangle$, the length 5 codes

$$\langle 11000, 00110, 00101, 01\omega\omega\omega, \omega\omega 001 \rangle$$

and

$$\langle 11000, 00110, 10101, \omega\omega 00\omega, 00\omega\omega\omega \rangle \ ,$$

and a $(5, 2^5)$ $d = 3$ code obtained from the hexacode (see Section 8) using Theorem 6.

We have also investigated the highest achievable minimal distance of any self-dual code of length n, or equivalently of any $[[n, 0, d]]$ quantum-error-correcting code. The results are shown in the $k = 0$ column of the main table (Section 8). Of course in view of Theorem 6(c) this also gives bounds on the minimal distance of any pure $[[n, k, d]]$ code.

We see from that table that the bound in Theorem 17 for even self-dual codes is met with equality at lengths $2, 4, \ldots, 22, 28$ and 30. In all but one of those cases the code can be taken to be a classical self-dual linear code over $GF(4)$. The exception is at length 12, where although no classical self-dual codes exists with minimal distance 6 [24], there is an additive code. This

is the $(12, 2^{12})$ $d = 6$ additive code having generator matrix

$$\begin{bmatrix}
0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 \\
0\,0\,0\,0\,0\,0\,\omega\omega\omega\omega\omega\omega \\
1\,1\,1\,1\,1\,1\,0\,0\,0\,0\,0\,0 \\
\omega\omega\omega\omega\omega\omega\,0\,0\,0\,0\,0\,0 \\
0\,0\,0\,1\,\omega\bar{\omega}\,0\,0\,0\,1\,\omega\bar{\omega} \\
0\,0\,0\,\omega\bar{\omega}\,1\,0\,0\,0\,\omega\bar{\omega}\,1 \\
1\,\bar{\omega}\omega\,0\,0\,0\,1\,\bar{\omega}\omega\,0\,0\,0 \\
\omega\,1\,\bar{\omega}\,0\,0\,0\,\omega\,1\,\bar{\omega}\,0\,0\,0 \\
0\,0\,0\,1\,\bar{\omega}\omega\omega\bar{\omega}\,1\,0\,0\,0 \\
0\,0\,0\,\omega\,1\,\bar{\omega}\,1\,\omega\bar{\omega}\,0\,0\,0 \\
1\,\omega\bar{\omega}\,0\,0\,0\,0\,0\,0\,\bar{\omega}\omega\,1 \\
\bar{\omega}\,1\,\omega\,0\,0\,0\,0\,0\,0\,1\,\bar{\omega}\omega
\end{bmatrix},$$

which we will call the *dodecacode*. This code is equivalent to the cyclic code with generator $\omega 10100100101$. It has weight distribution $A_0 = 1$, $A_6 = 396$, $A_8 = 1485$, $A_{10} = 1980$, $A_{12} = 234$, and its automorphism group has order 648 and acts transitively on the coordinates.

There is an interesting open question concerning length 24. There exists a $(24, 2^{24})$ $d = 8$ classical code over $GF(2)$, the Golay code, and at least two $(24, 3^{12})$ $d = 9$ classical codes over $GF(3)$, all meeting the analogous bounds to Theorem 17(b) [52]. It is known [49] that there is no $(24, 4^{12})$ $d = 10$ classical code over $GF(4)$, but the possibility of a $(24, 2^{24})$ $d = 10$ *additive* self-dual code remains open. Linear programming shows that if such a code exists then it must be even. However, all our attempts so far to construct this code have failed, so it may not exist.

7. Linear programming and other bounds

Gottesman [35] showed that any nondegenerate $[[n, k, 2t+1]]$ code must satisfy the sphere-packing bound

$$\sum_{j=0}^{t} 3^j \binom{n}{j} \leq 2^{n-k} \ . \tag{14}$$

Knill and Laflamme [45] have shown that any (pure or impure) code must satisfy the following version of the Singleton bound (cf. [52]):

$$n \geq 4e + k, \tag{15}$$

where $e = \lfloor (d-1)/2 \rfloor$ is the number of errors correctable by the code. In this section we first establish a linear programming bound which applies to all $[[n, k, d]]$ codes, and then give a slightly stronger version of the Singleton bound for pure codes.

Suppose an $[[n,k,d]]$ code exists, let C be the corresponding $(n,2^{n-k})$ code over $GF(4)$ and let $C^\perp$, an $(n,2^{n+k})$ code, be its dual (see Theorem 2). Let $A_0,\ldots,A_n$ and $A'_0,\ldots,A'_n$ be the weight distributions of C and $C^\perp$ respectively.

In view of Theorem 6(e), we may assume that $A_1 = 0$. (Only minor modifications to Theorem 21 are required if this assumption is not made.)

The Krawtchouk polynomials appropriate for studying a code of length n over $GF(4)$ will be denoted by

$$P_j(x,n) = \sum_{s=0}^{j} (-1)^s 3^{j-s} \binom{x}{s}\binom{n-x}{j-s} ,$$

for $j = 0,\ldots,n$ (see Chapter 6 of [52]).

Theorem 21. *If an $[[n,k,d]]$ quantum-error-correcting code exists such that the associated $(n,2^{n-k})$ code C contains no vectors of weight 1, then there is a solution to the following set of linear equations and inequalities:*

$$A_0 = 1, A_1 = 0, A_j \geq 0 \ (2 \leq j \leq n) , \tag{16}$$

$$A_0 + A_1 + \cdots + A_n = 2^{n-k} , \tag{17}$$

$$A'_j = \frac{1}{2^{n-k}} \sum_{r=0}^{n} P_j(r,n) A_r \quad (0 \leq j \leq n) , \tag{18}$$

$$A_j = A'_j \ (0 \leq j \leq d-1), \ A_j \leq A'_j \ (d \leq j \leq n) , \tag{19}$$

$$\sum_{j \geq 0} A_{2j} = 2^{n-k-1} \quad \textit{or} \quad 2^{n-k} , \tag{20}$$

$$\frac{1}{2^{n-k-1}} \sum_{r=0}^{n} P_j(2r,n) A_{2r} \geq A'_j \ (0 \leq j \leq n) . \tag{21}$$

(If the second possibility obtains in (20), (21) just says that $2A'_j \geq A'_j$ and can be omitted.)

Proof. (18) is a consequence of Theorem 5, and (19) follows from the facts that $C \subset C^\perp$ and any vectors in $C^\perp$ of weights between 1 and $d-1$ inclusive must also be in C. From (7), the even weight vectors in C form an additive subcode C', which is either half or all of C; (20) then follows. If C' is half of C, then $C' \subset C \subset C^\perp \subset (C')^\perp$, which yields (21). The other constraints are clear. □

A more compact statement of the linear programming bound may be obtained by rephrasing Theorem 21 in terms of weight enumerators.

Theorem 22. *If an $[[n,k,d]]$ quantum-error-correcting code exists then there are homogeneous polynomials $W(x,y)$, $W^\perp(x,y)$ and $S(x,y)$ of degree n such that the following conditions hold:*

$$W(1,0) = W^\perp(1,0) = 1 \ , \tag{22}$$

$$W^\perp(x,y) = 2^k W\left(\frac{x+3y}{2}, \frac{x-y}{2}\right) \ , \tag{23}$$

$$S(x,y) = 2^k W\left(\frac{x+3y}{2}, \frac{y-x}{2}\right) \ , \tag{24}$$

$$W^\perp(1,y) - W(1,y) = O(y^d) \ , \tag{25}$$

and

$$W(x,y), W^\perp(x,y) - W(x,y), S(x,y) \geq 0 \ , \tag{26}$$

where $P(x,y) \geq 0$ indicates that the coefficients of $P(x,y)$ are nonnegative.

Proof. Take $W(x,y)$ to be the weight enumerator of C and $W^\perp(x,y)$ to be the weight enumerator of $C^\perp$. $S(x,y)$ is the *shadow enumerator* (by analogy with [25]) and is nonnegative by Eq. (21). □

We have implemented Theorems 21 and 22 on the computer in two different ways.

(i) We attempt to minimize $A_1 + \cdots + A_{d-1}$ subject to (16)–(21) using an optimization program such as CPLEX [27] or CONOPT [32]. The AMPL language [34] makes it easy to formulate such problems and to switch from one package to another.

If all goes well, the program either finds a solution (which may lead to additional discoveries about the code, such as that there must exist a vector of a particular weight), or else reports that no feasible solution exists, in which case we can conclude that no $[[n,k,d]]$ code exists.

Unfortunately, for values of n around 30, the coefficients may grow too large for the problems to be handled using double precision arithmetic, and the results cannot be trusted.[3]

(ii) Alternatively, using a symbolic manipulation program such as MAPLE [18], we may ask directly if there is a feasible solution to (16)–(21) or to (22)–(26) (the latter being easier to implement). Since the calculations are performed in exact arithmetic, the answers are (presumably) completely reliable. On the other hand the calculations are much slower than when floating point arithmetic is used.

Most of the upper bounds in the main table were independently calculated using both methods.

[3]It is hoped that the multiple precision linear programming package being developed by David Applegate of Rice University will soon remove this difficulty.

When investigating the possible existence of a pure $[[n,k,d]]$ code, we may set A_2 through A_{d-1} equal to 0. In all cases within the range of table III below, this had no effect; that is, the LP bound for pure codes was the same as that for impure codes. We handle (20) by running the problem twice, once for each choice of the right-hand side.

For example, using Theorem 21 we find that there are no $[[n,1,5]]$ codes of length $n \le 10$ for which C has $A_1 = 0$. From Theorem 6 we conclude that no $[[n,1,5]]$ code of any type exists with $n \le 10$. On the other hand an $[[11,1,5]]$ code does exist — see the following section.

Additional constraints can be included in Theorem 21 to reflect special knowledge about particular codes, or to attempt to narrow the range of a particular A_i. Many variations are the basic argument are possible, as illustrated in the following examples.

(i) No $[[13,0,6]]$ code exists. Let C be a $(13, 2^{13})$ additive code with $d \ge 5$, and let C' be its even subcode. The linear constraints in Theorem 21 enable us to express all the unknowns in terms of A_5 and A_6. The condition that the weight distribution of $(C')^\perp$ be integral implies certain congruence conditions on A_5 and A_6, from which it is possible to eliminate A_6. The resulting congruence implies $A_5 \equiv 1 \pmod 2$. In particular $A_5 \neq 0$, and so $d = 5$.

(ii) No $[[18,12,3]]$ code exists. Consider the $(18, 2^6)$ additive code C. Linear programming shows that C must contain a vector of weight 12, which without loss of generality we may take to be $u_0 = 0^6 1^{12}$. We define the refined weight enumerator of C with respect to u_0 to be

$$R_C(x_0, x_1, y_0, y_1, y_2) = \sum_{u \in C} x_0^{6-a(u)} x_1^{a(u)} y_0^{12-b(u)-c(u)} y_1^{b(u)} y_2^{c(u)} \ ,$$

where $a(u)$ is the weight of u in the first 6 coordinates, and $b(u)$ (resp. $c(u)$) is the number of 1's (resp. ω's or $\bar{\omega}$'s) in u in the last 12 coordinates. The conditions on C imply that $c(u) \equiv 0 \pmod 2$,

$$(a(u+u_0), b(u+u_0), c(u+u_0)) = (a(u), 12 - b(u) - c(u), c(u)) \ ,$$

and

$$R_{C^\perp} = \frac{1}{|C|} R_C(x_0 + 3x_1, x_0 - x_1, y_0 + y_1 + 2y_2, y_0 + y_1 - 2y_2, y_0 - y_1) \ .$$

By applying linear programming, we find that the weight distribution of C must be either $A_0 = 1$, $A_{12} = 9$, $A_{14} = 54$ or $A_0 = 1$, $A_{12} = 1$, $A_{13} = 24$, $A_{14} = 30$, $A_{15} = 8$. In either case, adding these constraints to the refined weight enumerator produces a linear program with no feasible solution.

(iii) Similar arguments eliminate the parameters $[[7,0,4]]$, $[[15,4,5]]$, $[[15,7,4]]$, $[[16,8,4]]$, $[[19,3,3]]$, $[[22,14,4]]$ and $[[25,0,10]]$.

In the remainder of this section we briefly discuss another version of the Singleton bound (cf. (15)):

Theorem 23. *If a pure* $[[n, k, d]]$ *code exists then* $k \leq n - 2d + 2$.

Proof. The associated code $C^{\perp}$ is then an additive $(n, 2^{n+k})$ code with minimal distance d. From Theorem 15 of [28], we have

$$2^{n+k} \leq 4^{n-d+1} \ ,$$

which implies $k \leq n - 2d + 2$. □

If d is odd this coincides with the Knill and Laflamme bound (15), but is slightly stronger if d is even.

We have determined all codes that meet this bound — these are analogues of the classical MDS codes (cf. Chapter 11 of [52]). Since the results are somewhat disappointing we simply state the answer and omit the rather lengthy proof.

Theorem 24. *A pure* $[[n, n - 2d + 2, d]]$ *code has parameters* $[[n, n, 1]]$ $(n \geq 1)$, $[[n, n - 2, 2]]$ $(n$ *even* $\geq 2)$, $[[5, 1, 3]]$ *or* $[[6, 0, 4]]$. *Up to equivalence there is a unique code in each case.*

Even allowing $k = n - 2d + 1$ does not appear to lead to any new codes. Further analysis shows that any pure $[[n, n - 2d + 1, d]]$ code has parameters $[[n, n - 1, 1]]$ $(n \geq 1)$, $[[n, n - 3, 2]]$ $(n \geq 3)$, $[[5, 0, 3]]$ or $[[8, 3, 3]]$.

8. A table of quantum-error-correcting codes

Table III, obtained by combining the best upper and lower bounds given in the previous sections, shows our present state of knowledge about the highest minimal distance d in any $[[n, k, d]]$ code of length $n \leq 30$.

Table III about here

Notes on Table III

When the exact value of d is not known, the lower and upper bounds are separated by a dash.

All unmarked upper bounds in the table come from the linear programming bound of Theorem 21. (A few of these bounds can also be obtained from Eq. (14) or from Theorem 16.)

Unmarked lower bounds are from Theorem 6. Note in particular that, except in the $k = 0$ column, once a particular value of d has been achieved, the same value holds for all lower entries in the same column using Theorem 6(a).

α. A code meeting this upper bound must be impure (this follows from integer programming by an argument similar to that used in Section 7 to show that no $[[13, 0, 6]]$ code exists).

β. A special upper bound given in Section 7. These bounds do not apply to nonadditive codes, for which the upper bound must be increased by 1.

γ. This is the unique other entry in the table (besides those marked 'β') where the known upper bound for nonadditive codes is different from the bound for additive codes: if we omit (21) (which says that the code is either odd or even) from the linear program, the bound increases by 1. In all other entries in the table, condition (21) is superfluous. However, we will be surprised if a $((19, 2^8, 5))$ nonadditive code exists.

Most of the following lower bounds are specified by giving the associated $(n, 2^{n-k})$ additive code.

a. The *hexacode*, a $(6, 2^6)$ $d = 4$ classical code that can be taken to be the $GF(4)$ span of $\langle 001111, 0101\omega\bar{\omega}, 1001\bar{\omega}\omega\rangle$ (see Chapter 3 of [26]). $Aut(h_6) = 3.S_6$, of order 2160.

b. A classical self-dual code over $GF(4)$ — see [51], [24].

c. A cyclic code, see Table I.

d. A $[[25, 1, 9]]$ code obtained by concatenating the $[[5, 1, 3]]$ Hamming code with itself (Fig. 1 of Section 4).

e. The dodecacode defined in Section 6.

f. An $[[8, 3, 3]]$ code, discovered independently in [16], [35] and [68]. The $(8, 2^5)$ additive code may be generated by vectors $((01\omega\omega\bar{\omega}1\bar{\omega}))0$, 11111111, $\omega\omega\omega\omega\omega\omega\omega\omega$ (where the double parentheses mean that all cyclic shifts of the enclosed string are to be used). Exhaustive search shows that this code is unique. Another version is obtained from Theorem 10. The automorphism group has order 168, and is the semidirect product of a cyclic group of order 3 and the general affine group $\{x \to ax + b : a, b, x \in GF(8), a \neq 0\}$.

g. A quasicyclic code found by T. A. Gulliver — see Table II of Section 5.

h. A Hamming code, see Section 5.

i. Use the $(12, 2^8)$ and $(14, 2^8)$ linear codes with generator matrices

$$\begin{bmatrix} 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,0\,0\,1\,1\,\omega\,\omega \\ 0\,1\,0\,1\,\omega\,\bar{\omega}\,0\,1\,0\,\omega\,1\,\omega \\ 1\,0\,0\,1\,\bar{\omega}\,\omega\,0\,1\,\omega\,0\,\omega\,1 \end{bmatrix}$$

and

$$\begin{bmatrix} 0\,0\,0\,0\,0\,0\,1\,1\,1\,1\,1\,1\,1\,1 \\ 0\,0\,1\,1\,1\,1\,0\,0\,0\,0\,1\,1\,1\,1 \\ 0\,1\,0\,1\,\omega\,\bar{\omega}\,0\,1\,\omega\,\bar{\omega}\,0\,1\,\omega\,\bar{\omega} \\ 1\,0\,0\,1\,\bar{\omega}\,\omega\,0\,1\,\bar{\omega}\,\omega\,1\,0\,\omega\,\bar{\omega} \end{bmatrix}$$

respectively. Their automorphism groups have orders 720 and 8064, and both act transitively on the coordinates. The first of these can be obtained from the $u|u+v$ construction (c.f. Theorem 12) applied to the unique $[[6, 4, 2]]$ and $[[6, 0, 4]]$ codes.

j. A $[[17, 9, 4]]$ code, for which the corresponding $(17, 2^8)$ $d = 12$ code C is a well-known linear code, a two-weight code of class TF3 [14]. The columns of the generator matrix of C represent the 17 points of an ovoid in $PG(3, 4)$. Both C and $C^{\perp}$ are cyclic, a generator for $C^{\perp}$ being $1\omega 1\omega 10^{12}$. The weight distribution of C is $A_0 = 1$, $A_{12} = 204$, $A_{16} = 51$, and its automorphism group has order 48960.

s. By shortening one of the following codes using Theorem 7 or its additive analogue: the $[[21, 15, 3]]$ or $[[85, 77, 3]]$ Hamming codes (see Section 5), the $[[32, 25, 3]]$ Gottesman code (Theorem 10), the $[[40, 30, 4]]$ code given in Table II or $[[40, 33, 3]]$ code shown in Fig. 2.

u. From the $u|u + v$ construction (see Theorem 12).

v. The following $(17, 2^6)$ code with trivial automorphism group found by random search:

$$\begin{bmatrix} 0\,0\,1\,0\,\omega\bar{\omega}\omega\bar{\omega}\,1\,1\,\omega\bar{\omega}\,0\,0\,1\,1\,\bar{\omega} \\ 0\,0\,\omega\,1\,0\,\omega\,0\,\bar{\omega}\bar{\omega}\bar{\omega}\,1\,1\,\omega\bar{\omega}\bar{\omega}\,1\,1 \\ 0\,1\,0\,0\,1\,\omega\,1\,\omega\bar{\omega}\bar{\omega}\bar{\omega}\,0\,\bar{\omega}\,1\,\omega\,0\bar{\omega} \\ 0\,\omega\,0\,\omega\omega\,0\,\bar{\omega}\,1\,\bar{\omega}\,1\,\omega\bar{\omega}\omega\,1\,\omega\omega\,1 \\ 1\,0\,0\,\omega\bar{\omega}\,0\,0\,1\,\omega\omega\bar{\omega}\,1\,\bar{\omega}\omega\,0\,\bar{\omega}\,1 \\ \omega\,0\,0\,1\,\bar{\omega}\bar{\omega}\bar{\omega}\,0\,\bar{\omega}\,0\,\bar{\omega}\,1\,0\,1\,1\,\omega\bar{\omega} \end{bmatrix}$$

Comparison of the table with the existing tables [11] of classical codes over $GF(4)$ reveals a number of entries where it may be possible to improve the lower bound by the use of linear codes. For example, classical linear $[30, 18, 8]$ codes over $GF(4)$ certainly exist. If such a code can be found which contains its dual, we would obtain a $[[30, 6, 8]]$ quantum code.

Table III: Highest achievable minimal distance d in any $[[n, k, d]]$ quantum-error-correcting code. The symbols are explained in the text.

$n \setminus k$	0	1	2	3	4	5	6	7
3	2	1	1	1				
4	2	2	2	1	1			
5	3	$^{h}3$	2	1	1	1		
6	$^{a}4$	3^{α}	2	2	2	1	1	
7	3^{β}	$^{s}3$	2	2	2	1	1	1
8	$^{b}4$	$^{s}3$	$^{s}3$	$^{f}3$	2	2	2	1
9	4	$^{s}3$	$^{s}3$	$^{s}3$	2	2	2	1
10	$^{b}4$	4	4	$^{s}3$	$^{s}3$	2	2	2
11	5	5	4	$^{s}3$	$^{s}3$	$^{s}3$	2	2
12	$^{e}6$	5^{α}	4	4	$^{i}4$	$^{s}3$	$^{s}3$	2
13	5^{β}	5	4	4	4	$3-4$	$^{s}3$	$^{s}3$
14	$^{b}6$	5	$4-5$	$4-5$	4	4	$^{i}4$	$^{s}3$
15	$^{c}6$	5	5	5	$^{g}4^{\beta}$	4	4	$^{s}3^{\beta}$
16	$^{b}6$	6	6	5	$4-5$	$4-5$	4	$3-4$
17	7	7	6	$5-6$	$4-5$	$4-5$	$4-5$	4
18	$^{b}8$	7	6	$5-6$	$5-6$	5	$^{g}5$	4
19	$7-8$	7	6	$5-6$	$5-6$	$5-6$	5	$4-5$
20	$^{b}8$	7	$6-7$	$5-7$	$5-6$	$5-6$	$5-6$	$4-5$
21	$^{c}8$	7	$6-7$	$5-7$	$5-7$	$5-6$	$5-6$	$4-6^{\alpha}$
22	$^{b}8$	$7-8$	$6-8$	$5-7$	$5-7$	$5-7$	$5-6$	$4-6$
23	$^{c}8-9$	$7-9$	$6-8$	$5-8$	$5-7$	$5-7$	$5-7$	$5-6$
24	$^{b}8-10$	$8-9^{\alpha}$	$6-8$	$6-8$	$6-8$	$6-7$	$6-7$	$5-7$
25	$^{c}8-9^{\beta}$	$^{d}9$	$7-8$	$7-8$	$7-8$	$7-8$	$6-7$	$5-7$
26	$8-10$	9	$8-9$	$8-9$	8	$7-8$	$6-8$	$5-8$
27	$9-10$	9	9	9	$8-9$	$7-8$	$6-8$	$5-8$
28	10	10	10	9	$8-9$	$7-9$	$6-8$	$6-8$
29	11	11	10	$9-10$	$8-9$	$7-9$	$6-9$	$6-8$
30	$^{b}12$	11^{α}	10	$9-10$	$8-10$	$7-9$	$6-9$	$6-9$

Table III cont.

$n \setminus k$	8	9	10	11	12	13	14	15
3								
4								
5								
6								
7								
8	1							
9	1	1						
10	2	1	1					
11	2	1	1	1				
12	2	2	2	1	1			
13	2	2	2	1	1	1		
14	${}^{s}3$	2	2	2	2	1	1	
15	${}^{s}3$	${}^{s}3$	2	2	2	1	1	1
16	${}^{s}3^{\beta}$	${}^{s}3$	${}^{s}3$	2	2	2	2	1
17	4	${}^{j}4$	${}^{s}3$	${}^{v}3$	2	2	2	1
18	4	4	${}^{s}3$	${}^{s}3$	2^{β}	2	2	2
19	4^{γ}	4	$3-4$	${}^{s}3$	${}^{s}3$	2^{β}	2	2
20	$4-5$	4	${}^{g}4$	$3-4$	${}^{s}3$	${}^{s}3$	2	2
21	$4-5$	$4-5$	4	${}^{s}4$	$3-4$	${}^{s}3$	${}^{s}3$	${}^{h}3$
22	$4-6$	$4-5$	$4-5$	4	${}^{s}4$	$3-4$	${}^{s}3^{\beta}$	${}^{s}3$
23	$4-6$	$4-6$	$4-5$	$4-5$	${}^{c}4$	${}^{s}4$	$3-4$	${}^{s}3$
24	$4-6$	$4-6$	$4-6$	$4-5$	$4-5$	4	${}^{s}4$	$3-4$
25	$4-7$	$4-6$	$4-6$	$4-6$	$4-5$	$4-5$	4	${}^{g}4$
26	$4-7$	$4-7$	$4-6$	$4-6$	$4-6$	$4-5$	$4-5$	4
27	$4-8$	$5-7$	$4-7$	$4-6$	$4-6$	$4-5$	$4-5$	$4-5$
28	${}^{u}6-8$	$5-8$	$5-7$	$5-7$	$5-6$	$5-6$	${}^{g}5-6$	$4-5$
29	$6-8$	$5-8$	$5-7$	$5-7$	$5-6$	$5-6$	$5-6$	$4-5$
30	$6-8$	$5-8$	$5-8$	$5-7$	$5-7$	$5-6$	$5-6$	$4-6$

Table III cont.

$n \setminus k$	16	17	18	19	20	21	22	23
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
15								
16	1							
17	1	1						
18	2	1	1					
19	2	1	1	1				
20	2	2	2	1	1			
21	2	2	2	1	1	1		
22	2	2	2	2	2	1	1	
23	$^s3$	2	2	2	2	1	1	1
24	$^s3$	$^s3$	2	2	2	2	2	1
25	$3-4$	$^s3$	$^s3$	2	2	2	2	1
26	$^s4$	$3-4$	$^s3$	$^s3$	2	2	2	2
27	4	$^s4$	$3-4$	$^s3$	$^s3$	2	2	2
28	4	4	$^s4$	$3-4$	$^s3$	$^s3$	2	2
29	$4-5$	4	4	$3-4$	$3-4$	$^s3$	$^s3$	2
30	$4-5$	$4-5$	4	4	$^g4$	$3-4$	$^s3$	$^s3$

9. Subsequent developments

In the year and a half since the manuscripts of [16] and the present paper were first circulated there have been a number of further developments.

(i) While we showed in Section 2 that the Clifford group L suffices to encode additive codes, we did not give explicit recipes for doing so. Such recipes can now be found in Cleve and Gottesman [21].

(ii) The Cleve and Gottesman technique applies only to real (not complex) codes. However, it can be shown [57] that any additive code is equivalent to a real additive code (and any linear code is equivalent to a real linear code), so this is not a severe restriction.

(iii) DiVincenzo and Shor [30] have shown how to correct errors in additive codes even when using imperfect computational gates. The techniques of Shor [61] for performing computations on encoded qubits using imperfect gates have been extended to general additive codes by Gottesman [36].

However, the most efficient methods currently known for fault-tolerant computation [2], [42], [46], [70] use only Calderbank-Shor-Steane codes (cf. Theorem 9).

(iv) It turns out that the proofs of the lower bounds on the capacity of quantum channels given in Bennett et al. [4], [5] and DiVincenzo, Shor and Smolin [31] can be restated in terms of additive codes. In particular, this implies that these bounds can be attained using additive codes.

(v) Cleve [20] has found a way to apply asymptotic upper bounds for classical binary codes to additive codes.

(vi) Steane [69] has extended Gottesman's [35] construction (compare Theorem 10) to obtain quantum analogues of Reed-Muller codes. The smallest of these new codes has parameters $[[32, 10, 6]]$.

(vii) The upper bounds in the column headed '$k = 0$' in Table III (with the exception of the entries marked 'β') have an obvious pattern with period 6. Further investigation of this pattern has led to an $n/3$ bound for quantum codes (cf. Theorem 17) [57] and an analogous $n/6$ bound for classical singly-even binary self-dual codes [55].

(viii) The main construction in this paper (described in Section 2) can be generalized to primes greater than 2. Some preliminary work along these lines has been done in [2], [43], [44], [54].

(ix) There are analogues of parts (a)–(c) of Theorem 6 for nonadditive codes. Parts (a) and (c) are trivial, while (b) now asserts that if a pure $((n, K, d))$ codes exists with $n \geq 2$ then an $((n-1, 2K, d-1))$ code exists [58].

(x) How much of a restriction is it to use only additive quantum-error-correcting codes? We conjecture: Not much! So far essentially only one good nonadditive code has been found. This is the $((5, 6, 2))$ code described in [59]. The best comparable additive code is a $((5, 4, 2))$ code. The $((5, 6, 2))$ code can be used to construct a family of nonadditive codes with parameters $((2m+1, 3.2^{2m-3}, 2))$ for all $m \geq 2$ [56]. The $((5, 6, 2))$ code is optimal in that there exists no $((5, 7, 2))$ code. It is not known if this is true for other codes in the family. The next candidate for a good nonadditive code is at length 7, where we have unsuccessfully tried to find a $((7, 1, 4))$ code.

(xi) Most of the upper bounds in this paper have only been proved to hold for additive codes. It turns out however that our strongest technique, the linear programming bound of Theorem 22, applies even to nonadditive codes with the appropriate definitions of W, $W^{\perp}$ (see [62]) and S (see [57]). The sole change needed in the statement of Theorem 22 is that 2^k must be replaced by K.

As a consequence, all but ten of the upper bounds in Table III (those marked 'β' or 'γ') apply equally to nonadditive codes.

(xii) The purity conjecture. As we have already remarked, in the range of Table III the linear programming bound for pure codes is no stronger than that for impure codes. Moreover, for several entries in the table a code meeting the linear programming bound must be pure. This suggests the following conjecture.

Conjecture. Let K be the largest number (not necessarily an integer) greater than 1 such that there exist polynomials W, $W^{\perp}$, S as in the nonadditive version of Theorem 22. Then for any such solution,

$$W(1, y) = 1 + O(y^d) \ ,$$

or in other words the weight enumerator is pure.

This conjecture, together with some sort of monotonicity result about solutions to Theorem 22, would imply the equivalence of the pure and impure linear programming bounds for general (additive or nonadditive) codes.

We have verified the conjecture for all $n \leq 50$.

(xiii) Referring to the above conjecture, cases in which the extremal K are powers of 2 are of particular interest. In the range $n \leq 45$ these are listed in the following table.

Table IV: Putative extremal quantum-error-correcting codes $((n, K, d))$ in which K is a power of 2.

(a) $K = 2$:	
$((5, 2, 3))$	(exists: Hamming code)
$((11, 2, 5))$	(exists from dodecacode)
$((17, 2, 7))$	(exists)
$((23, 2, 9))$	(?)
$((29, 2, 11))$	(exists: quadratic residue code)
$((35, 2, 13))$	(?)
$((41, 2, 15))$	(?)
(b) Two infinite families:	
$((2m, 2^{2m-2}, 2)), m \geq 1$	(exist)
$((n, 2^{n-2m}, 3)), n = (4^m - 1)/3, m \geq 2$	(exist: Hamming codes)
(c) Some apparently sporadic possibilities:	
$((18, 4096, 3))$	(?, must be nonadditive)
$((16, 256, 4))$	(?, must be nonadditive)
$((17, 512, 4))$	(exists)
$((22, 2^{14}, 4))$	(?, must be nonadditive)
$((27, 2^{15}, 5))$	(?)
$((28, 2^{14}, 6))$	(?)
$((40, 64, 13))$	(?)

There are also some candidates for which K is not a power of 2. The first of these is $((5, 6, 2))$, and as mentioned above we were able to find such a code. There is an infinite family of other candidates with $d = 2$, none of which can exist [56]. The remaining possibilities for $n \leq 45$ are:

$((10, 24, 3))$
$((13, 40, 4))$
$((21, 7168, 4))$
$((24, 49152, 4))$
$((22, 384, 6))$
$((22, 56, 7))$
$((24, 24, 8))$
$((39, 24, 13))$

It would be very interesting to have an elegant combinatorial construction for any of these codes.

(xiv) In Theorem 24 we listed all sets of parameters of the form $[[n, n-2d+2, d]]$ for which

an additive code exists, and remarked that in each case the code is unique. In [56] this result is extended to nonadditive codes. In particular, any

$$((2,1,2)),((4,4,2)),((5,2,3)),((6,1,4))$$

code is equivalent to the unique

$$[[2,0,2]],[[4,2,2]],[[5,1,3]],[[6,0,4]]$$

additive code, respectively. On the other hand, for all $n > 2$, there exists a nonadditive $((2n, 2^{2n-2}, 2))$ code.

(xv) There is a remarkable story behind this paper. About a year and a half ago one of us (P.W.S.) was studying fault-tolerant quantum computation, and was led to investigate a certain group of 8×8 orthogonal matrices. P.W.S. asked another of us (N.J.A.S.) for the best method of computing the order of this group. N.J.A.S. replied by citing the computer algebra system MAGMA [8], [9], [10], and gave as an illustration the MAGMA commands needed to specify a certain matrix group that had recently arisen in connection with packings in Grassmannian spaces. This group was the symmetry group of a packing of 70 4-dimensional subspaces of $\mathbb{R}^8$ that had been discovered by computer search [22]. It too was an 8-dimensional group, of order 5160960. To our astonishment the two groups turned out to be identical (not just isomorphic)! We then discovered that this group was a member of an infinite family of groups that played a central role in a joint paper [12] of another of the authors (A.R.C.). This is the family of real Clifford groups L_R, described in Section 2 (for $n = 3$, L_R has order 5160960).

This coincidence led us to make connections which further advanced both areas of research (fault-tolerant quantum computing [61] and Grassmannian packings [63]).

While these three authors were pursuing these investigations, the fourth author (E.M.R.) happened to be present for a job interview and was able to make further contributions to the Grassmannian packing problem [13]. As the latter involved packings of 2^k-dimensional subspaces in 2^n-dimensional space, it was natural to ask if the same techniques could be used for constructing quantum-error-correcting codes, which are also subspaces of 2^n-dimensional space. This question led directly to [16] and the present paper. (Incidentally, he got the job.)

A final postscript: At the 1997 IEEE International Symposium on Information Theory, V. I. Sidelnikov presented a paper "On a finite group of matrices generating orbit codes on the

Euclidean sphere" [65] (based on [64], [41]). It was no surprise to discover that — although Sidelnikov did not identify them in this way — these were the Clifford groups appearing in yet another guise.

Acknowledgements

We thank Aaron Gulliver for finding the quasi-cyclic codes mentioned in Section 5, and our colleague Ronald H. Hardin for his contributions to our search for interesting nonadditive codes.

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge Univ. Press, 1986.

[2] D. Aharonov and M. Ben-Or, "Fault-tolerant quantum computation with constant error," *Proceedings of the 29th Annual ACM Symposium on Theory of Computing,* ACM Press, 1997, 176–188; also LANL e-print quant-ph/9611025.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and EPR channels," *Phys. Rev. Lett.*, **70**, pp. 1895–1898 (1993).

[4] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Phys. Rev. Lett.*, **76**, pp. 722–725 (1996).

[5] C. H. Bennett, D. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A*, **54** (1996) pp. 3824–3851; also LANL e-print quant-ph/9604024.

[6] B. Bolt, T. G. Room and G. E. Wall, On Clifford collineation, transform and similarity groups I, *J. Australian Math. Soc.*, **2** (1961), 60–79.

[7] B. Bolt, T. G. Room and G. E. Wall, On Clifford collineation, transform and similarity groups I, *J. Australian Math. Soc.*, **2** (1961), 80–96.

[8] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Sydney, May 22, 1995.

[9] W. Bosma, J. J Cannon and G. Mathews, Programming with algebraic structures: Design of the Magma language, In: M. Giesbrecht (ed.), *Proceedings of the 1994 International Symposium on Symbolic and Algebraic Computation*, Oxford, July 20–22, 1994. Association for Computing Machinery, 1994, 52–57.

[10] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symb. Comp.*, to appear, 1996.

[11] A. E. Brouwer and N. J. A. Sloane, Tables of codes over $GF(3)$ and $GF(4)$, in *Handbook of Coding Theory*, ed. V. Pless et al., in preparation, 1998.

[12] A. R. Calderbank, P. J. Cameron, W. M. Kantor and J. J. Seidel, "$\mathbb{Z}_4$ Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets," *Proc. London Math. Soc.* (to appear).

[13] A. R. Calderbank, R. H. Hardin, E. M. Rains, P. W. Shor and N. J. A. Sloane, "A group-theoretic framework for the construction of packings in Grassmannian spaces," *J. Algebraic Combinatorics*, 1997 (submitted).

[14] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," *Bull. London Math. Soc.*, **118**, pp. 97–122 (1986).

[15] A. R. Calderbank, W.-C. W. Li and B. Poonen, "A 2-adic approach to the analysis of cyclic codes," *IEEE Trans. Inform. Theory*, **43**, pp. 977–986 (1997).

[16] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, **78**, pp. 405–409 (1997).

[17] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, **54**, pp. 1098–1105 (1996); also LANL e-print quant-ph/9512032.

[18] B. W. Char et al., *Maple V Library Reference Manual* Springer-Verlag, NY, 1991.

[19] C. Chevalley, *The Construction and Study of Certain Important Algebras*, Math. Soc. Japan, 1955. Reprinted with corrections in C. Chevalley, *Collected Works*, Springer-Verlag, Vol. 2, 1997.

[20] R. Cleve, "Quantum stabilizer codes and classical linear codes," LANL e-print quant-ph/9612048.

[21] R. Cleve and D. Gottesman, "Efficient computations of encodings for quantum error correction," *Phys. Rev. A.*, **56**, pp. 76–82 (1997). Also LANL e-print quant-ph/9607030.

[22] J. H. Conway, R. H. Hardin, and N. J. A. Sloane, "Packing lines, planes, etc.: packings in Grassmannian space," *Experimental Math.*, Vol. 5, 1996, pp. 139–159.

[23] J. H. Conway, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, 1985.

[24] J. H. Conway, V. Pless, and N. J. A. Sloane, "Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16," *IEEE Trans. Information Theory*, **25**, pp. 312–322 (1979).

[25] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Information Theory*, Vol. 36, 1990, pp. 1319–1333.

[26] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 2nd. ed., 1993.

[27] *CPLEX Manual*, CPLEX Organization Inc., Incline Village, Nevada, 1991.

[28] P. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Res. Reports*, **27**, pp. 272–289 (1972).

[29] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, **92**, p. 271 (1982).

[30] D. P. DiVincenzo and P. W. Shor, "Fault-tolerant error correction with efficient quantum codes," *Phys. Rev. Lett.*, **77** (1996), pp. 3260–3263; also LANL e-print quant-ph/9605031.

[31] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum channel capacity of very noisy channels," LANL e-print quant-ph/9706061.

[32] A. S. Drud, "CONOPT — A large scale GRG code," *ORSA J. Computing*, **6**, pp. 207–218 (1994).

[33] A. Ekert and C. Macchiavello, "Error correction in quantum communication," *Phys. Rev. Lett.*, **77** (1996) pp. 2585–2588; also LANL e-print quant-ph/9602022.

[34] R. Fourer, D. M. Gay and B. W. Kernighan, *AMPL: A Modeling Language for Mathematical Programming*, Scientific Press, San Francisco, 1993.

[35] D. Gottesman, "A class of quantum error-correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, **54** (1996), pp. 1862–1868; also LANL e-print quant-ph/9604038.

[36] D. Gottesman, "A theory of fault-tolerant quantum computation," LANL e-print quant-ph/9702029.

[37] D. Gottesman, "Pasting quantum codes," LANL e-print quant-ph/9607027.

[38] T. A. Gulliver and V. K. Bhargava, "Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over $GF(3)$ and $GF(4)$," *IEEE Trans. Information Theory*, **38**, pp. 1369–1374 (1992).

[39] B. Huppert, *Endliche Gruppen*, Springer-Verlag, Berlin, 1967.

[40] N. Jacobson, *Basic Algebra II*, Freeman, San Francisco, 1980.

[41] L. S. Kazarin, "On the Sidelnikov group" (in Russian), preprint, 1997.

[42] A. Kitaev, personal communication, 1997.

[43] E. Knill, "Non-binary unitary error bases and quantum codes," LANL e-print quant-ph/9608037.

[44] E. Knill, "Group representations, error bases and quantum codes," LANL e-print quant-ph/9608048.

[45] E. Knill and R. Laflamme, "A Theory of Quantum Error-Correcting Codes," LANL e-print quant-ph/9604034.

[46] E. Knill, R. Laflamme and W. Zurek, "Threshold accuracy for quantum computation," LANL e-print quant-ph/9610011.

[47] F. R. Kschischang and S. Pasupathy, "Some ternary and quaternary codes and associated sphere packings," *IEEE Trans. Information Theory*, **38**, pp. 227–246 (1992).

[48] R. Laflamme, C. Miquel, J. P. Paz and W. H. Zurek, "Perfect quantum error correction code," *Phys. Rev. Lett.* **77** (1996) pp. 198–201; also LANL e-print quant-ph/9602019.

[49] C. W. H. Lam and V. Pless, "There is no $(24, 12, 10)$ self-dual quaternary code," *IEEE Trans. Information Theory*, **36**, pp. 1153–1156 (1990).

[50] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, NY, 1982.

[51] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, "Self-dual codes over $GF(4)$," *J. Combinatorial Theory, Series A*, **25**, pp. 288–318 (1978).

[52] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[53] C. L. Mallows and N. J. A. Sloane, "An upper bound for self-dual codes," *Information and Control*, **22**, pp. 188–200 (1973)

[54] E. M. Rains, "Nonbinary quantum codes," LANL e-print quant-ph/9703048

[55] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Trans. Inform. Theory*, to appear.

[56] E. M. Rains, "Quantum codes of minimum distance two," LANL e-print quant-ph/9704043

[57] E. M. Rains, "Quantum shadow enumerators," LANL e-print quant-ph/9611001.

[58] E. M. Rains, "Quantum weight enumerators," LANL e-print quant-ph/9612015.

[59] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane, "A nonadditive quantum code," *Phys. Rev. Lett.* **79** pp. 953-954 (1997).

[60] P. W. Shor, "Scheme for reducing decoherence in quantum memory," *Phys. Rev. A*, **52**, p. 2493 (1995).

[61] P. W. Shor, "Fault-tolerant quantum computation," *Proc. 37th Sympos. Foundations of Computer Science*, IEEE Computer Society Press, 1996, pp. 56–65.

[62] P. W. Shor and R. Laflamme, "Quantum analog of the MacWilliams identities in classical coding theory," *Phys. Rev. Lett.* **78**, pp. 1600-1602 (1997).

[63] P. W. Shor and N. J. A. Sloane, "A family of optimal packings in Grassmannian manifolds," *J. Algebraic Combinatorics*, 1997 (to appear).

[64] V. M. Sidelnikov, "On a finite group of matrices and codes on the Euclidean sphere" (in Russian), *Probl. Peredach. Inform.*, **33**, pp. 35–54 (1997).

[65] V. M. Sidelnikov, "On a finite group of matrices generating orbit codes on the Euclidean sphere," in *Proceedings 1997 IEEE Internat. Sympos. Inform. Theory* (Ulm, 1997), IEEE Press, 1997, p. 436.

[66] N. J. A. Sloane, "Self-dual codes and lattices," in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math., Vol. 34, American Mathematical Society, Providence, RI, 1979, pp. 273–308.

[67] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. Roy. Soc. London A*, submitted; LANL e-print quant-ph/9601029.

[68] A. M. Steane, "Simple quantum error correcting codes," *Phys. Rev. Lett.*, **77**, pp. 793–797 (1996).

[69] A. M. Steane, "Quantum Reed-Muller codes," LANL e-print quant-ph/9608026.

[70] A. M. Steane, "Space, time, parallelism and noise requirements for reliable quantum computing," LANL e-print quant-ph/9708021.

[71] G. E. Wall, On Clifford collineation, transform and similarity groups IV, *Nagoya Math. J.*, **21**, pp. 199–222 (1962).

[72] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, **299**, p. 802 (1982).