On the Existence of Nonadditive Quantum Codes

Vwani P. Roychowdhury and Farrokh Vatan

Electrical Engineering Department
UCLA
Los Angeles, CA 90095
vwani@ee.ucla.edu and vatan@ee.ucla.edu

Abstract. Most of the quantum error-correcting codes studied so far fall under the category of additive (or stabilizer) quantum codes, which are closely related to classical linear codes. The existence and general constructions of efficient quantum codes that do not have such an underlying structure have remained elusive. Recently, specific examples of nonadditive quantum codes with minimum distance 2 have been presented. We, however, show that there exist infinitely many non-trivial nonadditive codes with different minimum distances, and high rates. In fact, we show that nonadditive codes that correct t errors can reach the asymptotic rate $R = 1 - 2H_2(2t/n)$, where $H_2(x)$ is the binary entropy function. In the process, we also develop a general set of sufficient conditions for a quantum code to be nonadditive. Finally, we introduce the notion of *strongly* nonadditive codes, and provide a construction for an ((11,2,3)) strongly nonadditive code.
key words: quantum code, additive code, Gilbert–Varshamov bound.

1 Introduction

Almost all quantum error–correcting codes known so far are additive (or stabilizer) codes. An additive code can be described as follows. Consider the group $\mathcal{G}$ of unitary operators on the Hilbert space $\mathbb{C}^{2^n}$ defined by the tensor products $\pm M_1 \otimes M_2 \otimes \cdots \otimes M_n$, where each M_i is either the identity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ or one the Pauli matrices σ_x, σ_z, or $\sigma_y = i\sigma_x\sigma_z$. Then an additive code is a subspace $\mathcal{Q}$ of $\mathbb{C}^{2^n}$ for which there is an Abelian subgroup H of $\mathcal{G}$ such that every vector of $\mathcal{Q}$ is a fixed point of every operator in H [3,4,7].[1] This approach leads to a close connection between self–orthogonal (under a specific inner product) linear binary codes and additive codes, such that the minimum distance of the additive code is determined from the binary code.

[1] This is actually the definition of a *real* additive code; i.e., a code which has a basis consisting of vectors from $\mathbb{R}^{2^n}$. In this paper we restrict ourselves to the set of real codes, but this does not restrict our results, since every additive code is equivalent to a real one [11].

C.P. Williams (Ed.): QCQC'98, LNCS 1509, pp. 325–336, 1999.

It is natural to ask whether there is any quantum error–correcting code that cannot be constructed in this way, directly or via some equivalence. We should make here a comment on the correct formulation of this question. Since the dimension of every additive quantum code is a power of 2, any quantum code whose dimension is not a power of 2 is not additive or equivalent to an additive code; especially, any subspace of an additive code with dimension not a power of 2 is a nonadditive code. We call such codes *trivial nonadditive codes*. But we prove a general theorem that shows that infinite families of non-trivial nonadditive codes with different values of d exist. The nonadditiveness of these codes does not follow from their dimensions (the dimensions of these codes are also powers of two), but from their very special structure. Moreover, we show that these nonadditive codes asymptotically reach the same rate as Calderbank–Shor–Steane codes.

We also propose the notion of *strongly nonadditive* codes: a quantum code $\mathcal{Q}$ is strongly nonadditive if the trivial code $\mathbb{C}^{2^n}$ is the only additive code that contains any code equivalent to $\mathcal{Q}$. Now the interesting problem is to find strongly nonadditive quantum codes. Recently in [13] it is shown that a $((5,6,2))$ strongly nonadditive code exists, which is better than any $((5,K,2))$ additive code. Later in [12], Rains showed that there exists a $((2m,4^{m-1},2))$ nonadditive code, for every $m \geq 3$. We present an $((11,2,3))$ strongly nonadditive code.

In Section 3 we first determine a criterion that guarantees additiveness and strongly nonadditiveness of quantum codes, and then we present our examples of additive and strongly nonadditive codes.

2 Preliminaries

Consider the Hilbert space $\mathbb{C}^{2^n}$ with its standard basis $|v_1\rangle, \ldots, |v_{2^n}\rangle$, where $v_1, \ldots, v_{2^n}$ is a list of binary vectors of length n in $\{0,1\}^n$. For every binary vector α of length n, we define the unitary operators X_α and Z_α by the following equations

$$X_\alpha |v_i\rangle = |v_i + \alpha\rangle ,$$
$$Z_\alpha |v_i\rangle = (-1)^{v_i \cdot \alpha} |v_i\rangle .$$

Note that $X_\alpha Z_\beta = (-1)^{\alpha \cdot \beta} Z_\beta X_\alpha$.

Let $\mathcal{G}$ be the group of all unitary operators of the form $\pm M_1 \otimes \cdots \otimes M_n$, where $M_i \in \{ I, \sigma_x, \sigma_y, \sigma_z \}$. Then every member of $\mathcal{G}$ can be represented uniquely as $(-1)^\lambda X_\alpha Z_\beta$, where $\lambda \in \{0,1\}$ and $\alpha, \beta \in \{0,1\}^n$. For every subgroup $\mathcal{S}$ of $\mathcal{G}$, let $\overline{\mathcal{S}} \subset \{0,1\}^{2n}$ be the set of all vectors $(\alpha|\beta)$ such that either $X_\alpha Z_\beta \in \mathcal{S}$ or $-X_\alpha Z_\beta \in \mathcal{S}$. We say $\overline{\mathcal{S}}$ is *totally singular* if for every $(\alpha|\beta) \in \overline{\mathcal{S}}$ we have $\alpha \cdot \beta = 0$. We also define a special inner product on $\{0,1\}^{2n}$ as

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

where the right–hand side is evaluated in GF(2). For any quantum code $\mathcal{Q}$ in $\mathbb{C}^{2^n}$, we define the *stabilizer* $\mathcal{H}_\mathcal{Q}$ of $\mathcal{Q}$ as

$$\mathcal{H}_\mathcal{Q} = \{ \varphi \in \mathcal{G} : \varphi |x\rangle = |x\rangle \text{ for every } |x\rangle \text{ in } \mathcal{Q} \} .$$

Then it is easy to check that $\mathcal{H}_\mathcal{Q}$ is an Abelian group and every element of $\mathcal{H}_\mathcal{Q}$ squares to the identity operator. So $\overline{\mathcal{H}_\mathcal{Q}}$ is totally singular. It also follows that $\mathcal{H}_\mathcal{Q}$ is isomorphic to a vector space $\mathrm{GF}(2)^m$, for some m. This means that $\mathcal{H}_\mathcal{Q}$ is generated by operators $\varphi_1, \ldots, \varphi_m \in \mathcal{H}_\mathcal{Q}$ and every $\varphi \in \mathcal{H}_\mathcal{Q}$ can be written (uniquely, up to the order of the φ_i's) as $\varphi = {\varphi_1}^{c_1} \cdots {\varphi_m}^{c_m}$, where $c_i \in \{0, 1\}$. In this case the quantum code $\mathcal{Q}$ has dimension 2^{n-m}. Suppose that $\varphi_i = (-1)^{\lambda_i} X_{\alpha_i} Z_{\beta_i}$. So $\overline{\mathcal{H}_\mathcal{Q}}$ can be determined by its $m \times (2n)$ binary generating matrix

$$M = \left(\begin{array}{c|c} \alpha_1 & \beta_1 \\ \vdots & \vdots \\ \alpha_m & \beta_m \end{array}\right). \tag{2}$$

Note that if such a matrix M obtained from a stabilizer, then $\alpha_i \cdot \beta_i = 0$ and $\alpha_i \cdot \beta_j + \alpha_j \cdot \beta_i = 0$, for every i and j. A quantum code $\mathcal{Q}$ is called *additive* (or *stabilizer*) if it is defined by its stabilizer $\mathcal{H}_\mathcal{Q}$, i.e.,

$$\mathcal{Q} = \left\{ |x\rangle \in \mathbb{C}^{2^n} : \varphi\,|x\rangle = |x\rangle \text{ for every } \varphi \in \mathcal{H}_\mathcal{Q} \right\}.$$

The quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ in $\mathbb{C}^{2^n}$ are *locally equivalent* if there is a transversal operator $\mathcal{U} = u_1 \otimes \cdots \otimes u_n$, with $u_i \in \mathrm{SU}(2)$, mapping $\mathcal{Q}_1$ into $\mathcal{Q}_2$. We say these codes are *globally equivalent*, or simply equivalent, if $\mathcal{Q}_1$ is locally equivalent to a code obtained from $\mathcal{Q}_2$ by a permutation on qubits.

A quantum code $\mathcal{Q} \subseteq \mathbb{C}^{2^n}$ is called **nonadditive** if it is not equivalent to any additive code; moreover, $\mathcal{Q}$ is **strongly nonadditive** if the only additive code that contains any code equivalent to $\mathcal{Q}$ is the trivial code $\mathbb{C}^{2^n}$; in other words, if $\pm X_\alpha Z_\beta$ is in the stabilizer of any code equivalent to a supercode of $\mathcal{Q}$ then $\alpha = \beta = \mathbf{0}$.

A K–dimensional subspace of $\mathbb{C}^{2^n}$ that as an error–correcting quantum code can protect against $< d/2$ errors, is called an $((n, K, d))$ code. If this code is additive, then $K = 2^k$, for some k, and is called an $[[n, k, d]]$ code. The following theorem gives a sufficient condition for a subspace of $\mathbb{C}^{2^n}$ to be an $((n, K, d))$ code. Here $\mathrm{wt}(c)$ denotes the Hamming weight of the binary vector c, i.e., the number of 1–components in c, and $\alpha \cup \beta$ is the binary vector resulting from a component-wise OR operation of α and β; for example $(10110) \cup (00101) = (10111)$.

Theorem 1. ([1], [8]) *Let $\mathcal{Q}$ be a K–dimensional subspace of $\mathbb{C}^{2^n}$. Consider an orthonormal basis for $\mathcal{Q}$ of the form $\{\, |c_i\rangle : i = 1, \ldots, K \,\}$. Then $\mathcal{Q}$ is an $((n, K, d))$ code if $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_j \rangle = 0$ for every $1 \le i, j \le K$ and for every $\alpha, \beta \in \{0, 1\}^n$ with $1 \le \mathrm{wt}(\alpha \cup \beta) \le d-1$. In general, a necessary and sufficient condition for $\mathcal{Q}$ to be an $((n, K, d))$ code is that for all $1 \le i, j \le K$ and $\mathrm{wt}(\alpha \cup \beta) \le d-1$ we have $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_i \rangle = \langle c_j \,|\, X_\alpha Z_\beta \,|\, c_j \rangle$ and if $i \ne j$ then $\langle c_i \,|\, X_\alpha Z_\beta \,|\, c_j \rangle = 0$.* □

For an additive code $\mathcal{Q}$ with stabilizer $\mathcal{H}_\mathcal{Q}$ there is a sufficient condition in term of the dual of $\mathcal{H}_\mathcal{Q}$ with respect to the inner product defined by equation (1) for $\mathcal{Q}$ to be a t–error–correcting code.

Theorem 2. ([3], [7]) *Let $\mathcal{Q}$ be an additive code with stabilizer $\mathcal{H}_\mathcal{Q}$. Let $\overline{\mathcal{H}_\mathcal{Q}}^\perp$ be the space orthogonal to $\overline{\mathcal{H}_\mathcal{Q}}$ with respect to the inner product* (1)*. If for every pair of binary vectors $\alpha, \beta \in \{0,1\}^n$ with $\mathrm{wt}(\alpha \cup \beta) \leq d-1$ we have $(\alpha|\beta) \notin \overline{\mathcal{H}_\mathcal{Q}}^\perp \backslash \overline{\mathcal{H}_\mathcal{Q}}$ then $\mathcal{Q}$ is an $[[n,k,d]]$ additive code.* □

3 Existence of Nonadditive Codes

3.1 Quantum Codes Equivalent to Additive Codes

We study the quantum codes equivalent to additive codes. For such code $\mathcal{Q}$, we find a sufficient condition that guarantees that the stabilizer of $\mathcal{Q}$ contains a nontrivial operator.

We begin with some useful notions and notations. Let $|c_1\rangle, \ldots, |c_{2^n}\rangle$ be the standard orthonormal basis of $\mathbb{C}^{2^n}$, where each c_i is a binary vector of length n. For the vector $|x\rangle = \sum_{i=1}^{2^n} \lambda_i |c_i\rangle$, we define the *support* of $|x\rangle$ as

$$\mathrm{supp}(|x\rangle) = \{\, c_i \in \{0,1\}^n : \lambda_i \neq 0 \,\}.$$

Let $\mathcal{C} \subseteq \{0,1\}^n$ be a set of binary vectors. Define the vector $|\mathcal{C}\rangle$ in $\mathbb{C}^{2^n}$ as

$$|\mathcal{C}\rangle = \frac{1}{|\mathcal{C}|^{1/2}} \sum_{c \in \mathcal{C}} |c\rangle .$$

(If $\mathcal{C}$ is empty then $|\mathcal{C}\rangle$ is the zero vector.) For any binary vector α of length $m < n$, define

$$\mathcal{C}_\alpha = \left\{\, x \in \{0,1\}^{n-m} : (\alpha, x) \in \mathcal{C} \,\right\}. \tag{3}$$

So to construct $\mathcal{C}_\alpha$, consider all vectors in $\mathcal{C}$ starting with α (if there is any), then delete α from these vectors. Note that $\mathcal{C}_\alpha$ may be empty.

For a quantum code $\mathcal{Q}$, let us define *the generalized stabilizer* of $\mathcal{Q}$ as the set $GS(\mathcal{Q})$ of all unitary operators $\mathcal{V}$ on $\mathbb{C}^{2^n}$ such that $\mathcal{V}|x\rangle = |x\rangle$ for every $|x\rangle \in \mathcal{Q}$. Then the *stabilizer* of $\mathcal{Q}$ is $\mathrm{St}(\mathcal{Q}) = \mathcal{G} \cap GS(\mathcal{Q})$.

Lemma 1. *Suppose that the quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are locally equivalent via the transversal unitary operator $\mathcal{U}$. Then for every $M \in GS(\mathcal{Q}_1)$ the operator $\mathcal{U}M\mathcal{U}^\dagger$ is in $GS(\mathcal{Q}_2)$.*

Proof. Let $|x\rangle \in \mathcal{Q}_2$. Now, we know that there exists a code word $|y\rangle \in \mathcal{Q}_1$ such that $|x\rangle = \mathcal{U}|y\rangle$. Since $M|y\rangle = |y\rangle$, so $(M\mathcal{U}^\dagger)\mathcal{U}|y\rangle = |y\rangle$, and therefore $(\mathcal{U}M\mathcal{U}^\dagger)\mathcal{U}|y\rangle = \mathcal{U}|y\rangle$. This implies $(\mathcal{U}M\mathcal{U}^\dagger)|x\rangle = |x\rangle$. □

We are interested in the case of $M \in \mathcal{G}$, i.e., $M = M_1 \otimes \cdots \otimes M_n$, where $M_j \in \{I, \sigma_x, \sigma_y, \sigma_z\}$. We define $\mathrm{wt}(M)$ the *weight* of any $M \in \mathcal{G}$ as the number of

j's such that $M_j \neq I$. In this case $\mathcal{U}M\mathcal{U}^\dagger = v_1 \otimes \cdots \otimes v_n$ such that $\det(v_j) = \pm 1$ and if $M_j = I$ then $v_j = I$, otherwise

$$v_j = \eta_j \begin{pmatrix} a_j & b_j \\ \pm b_j{}^* & -a_j \end{pmatrix}, \qquad \eta_j \in \{1, i\},\ a_j \in \mathbb{R} \text{ and } b_j \in \mathbb{C}. \tag{4}$$

If $\mathcal{U} \in \mathrm{SU}(2)^{\otimes n}$ then $\mathcal{U}$ is of the form $u_1 \otimes \cdots \otimes u_n$, where each u_j is defined by a matrix of the form

$$\begin{pmatrix} e^{i\alpha}\cos\theta & e^{i\beta}\sin\theta \\ -e^{-i\beta}\sin\theta & e^{-i\alpha}\cos\theta \end{pmatrix}. \tag{5}$$

If $M_j = \sigma_x$, σ_z or σ_y, then the corresponding v_j, respectively, is

$$\left.\begin{array}{c} \begin{pmatrix} \sin 2\theta\cos(\alpha-\beta) & \cos^2\theta e^{i2\alpha} - \sin^2\theta e^{i2\beta} \\ \cos^2\theta e^{-i2\alpha} - \sin^2\theta e^{-i2\beta} & -\sin 2\theta\cos(\alpha-\beta) \end{pmatrix}, \\ \\ \begin{pmatrix} \cos 2\theta & -\sin 2\theta e^{i(\alpha+\beta)} \\ -\sin 2\theta e^{-i(\alpha+\beta)} & -\cos 2\theta \end{pmatrix}, \\ \\ \text{or } \begin{pmatrix} -i\sin 2\theta\sin(\alpha-\beta) & -\cos^2\theta e^{i2\alpha} - \sin^2\theta e^{i2\beta} \\ \cos^2\theta e^{-i2\alpha} + \sin^2\theta e^{-i2\beta} & i\sin 2\theta\sin(\alpha-\beta) \end{pmatrix}. \end{array}\right\} \tag{6}$$

We call a matrix v_i as (4) *full* if $a_i \cdot b_i \neq 0$; and we say the unitary operator $\mathcal{V} = v_1 \otimes \cdots \otimes v_n$ is *thin* if none of v_i's is full. In the next proof we will use this property that if $\mathcal{V}$ is thin then $|\mathrm{supp}(\mathcal{V}|x\rangle)| = |\mathrm{supp}(|x\rangle)|$, for every $|x\rangle$.

A quantum code $\mathcal{Q}$ is called *real* if $\mathcal{Q}$ has a basis consisting of real vectors; i.e., if $|x\rangle = \sum_{i=1}^{2^n} \lambda_i |c_i\rangle$ is any vector in the basis, then $\lambda_i \in \mathbb{R}$, for every i.

An (n, K, d) binary code is a set $\mathcal{C} \subseteq \{0,1\}^n$ of size K such that any two vectors in $\mathcal{C}$ differ in at least d places, and d is the largest number with this property. Note that an $[n, k, d]$ binary linear code is an $(n, 2^k, d)$ binary code.

Theorem 3. *Suppose that the quantum codes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are locally equivalent via the transversal operator $\mathcal{U}$, $\mathcal{Q}_2$ is real and $\mathcal{Q}_2$ contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is an (n, K, d) binary code with $d > k = \lceil \log_2 K \rceil$. Then the following claims hold.*

(i) The image of $\mathrm{St}(\mathcal{Q}_1)$ under the mapping $M \mapsto \mathcal{U}M\mathcal{U}^\dagger$, which we call Γ, consists only of unitary operators of the form $\pm X_\alpha T$, where T is a Z–type unitary operator of the form

$$T = \bigotimes_{j=1}^{n} \begin{pmatrix} e^{i\theta_j} & 0 \\ 0 & \pm e^{-i\theta_j} \end{pmatrix}. \tag{7}$$

(ii) Let $\Delta = \{\, \alpha \in \{0,1\}^n : \pm X_\alpha T \in \Gamma$ for some T of the form (7)$\,\}$. Suppose that $\mathrm{St}(\mathcal{Q}_2)$ does not contain any operator of the form $\pm X_{\mathbf{0}} Z_\beta$, with $\beta \neq \mathbf{0}$. Then $|\mathrm{St}(\mathcal{Q}_1)| \leq |\Delta|$. □

The proof of this theorem can be found in [14].

We now present a criterion for nonadditiveness of quantum codes. First a useful notation. For a subset $\mathcal{C}$ of $\{0,1\}^n$ let

$$\mathcal{T}(\mathcal{C}) = \{\, x \in \{0,1\}^n : x + \mathcal{C} \subseteq \mathcal{C} \,\}.$$

If $\mathcal{C}$ is a binary *linear* code then $\mathcal{T}(\mathcal{C}) = \mathcal{C}$.

Theorem 4. *Suppose that the quantum code $\mathcal{Q}$ of dimension 2^ℓ is real and contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is an (n, K, d) binary code with $d > \lceil \log_2 K \rceil$. If the identity operator is the only unitary operator in the stabilizer of $\mathcal{Q}$ and $2^{n-\ell} > |\mathcal{T}(\mathcal{C})|$ then $\mathcal{Q}$ is nonadditive.*

Proof. Suppose, by contradiction, that $\mathcal{Q}$ is equivalent to additive code $\mathcal{Q}'$ via the transversal unitary operator $\mathcal{U}$ which maps $\mathcal{Q}'$ on $\mathcal{Q}$. Let Γ be the image of $\mathrm{St}(\mathcal{Q}')$ under $\mathcal{U}$. Define $\Delta \subseteq \{0,1\}^n$ as in (ii) of Theorem 3. Then $\Delta \subseteq \mathcal{T}(\mathcal{C})$. Thus

$$2^{n-\ell} = |\mathrm{St}(\mathcal{Q}')| \leq |\Delta| \leq |\mathcal{T}(\mathcal{C})|,$$

which contradicts the assumption of the theorem. □

When the binary code $\mathcal{C}$ in the above theorem is linear we can formulate the theorem as follows.

Corollary 1. *Suppose that the quantum code $\mathcal{Q}$ of dimension 2^ℓ is real and contains $|\mathcal{C}\rangle$, where $\mathcal{C}$ is a linear $[n, k, d]$ code with $d > k$. If $\mathrm{St}(\mathcal{Q}) = \{I\}$ and $n > k + \ell$ then $\mathcal{Q}$ is nonadditive.* □

Finally, we formulate a criterion that guarantees strongly nonadditiveness of quantum codes.

Theorem 5. *Suppose that the quantum code $\mathcal{Q}$ is real and it contains $|\mathcal{C}\rangle$ where $\mathcal{C}$ is an (n, K, d) binary code with $d > \lceil \log_2 K \rceil$. If $\mathrm{St}(\mathcal{Q}) = \{I\}$ and $GS(\mathcal{Q})$ does not contain any operator of the form $X_\alpha T$, where $\alpha \neq \mathbf{0}$ and T is of the form (7), then $\mathcal{Q}$ is strongly nonadditive.*

Proof. Suppose, by contradiction, that $\mathcal{Q} \subseteq \mathcal{Q}_1$ and $\mathcal{Q}_1 \neq \mathbb{C}^{2^n}$ is equivalent to an additive code $\mathcal{Q}'$ with $\mathrm{St}(\mathcal{Q}') \neq \{I\}$. Then, by Theorem 3, any nontrivial stabilizer φ of $\mathcal{Q}'$ defines an operator $\mathcal{V} = v_1 \otimes \cdots \otimes v_n$ in $GS(\mathcal{Q}_1) \subseteq GS(\mathcal{Q})$, where $v_j = I$ or it is of the form (4) or (6). If all v_j have real matrices, then $\mathcal{V} \neq I$ and $\mathcal{V} \in \mathrm{St}(\mathcal{Q})$, which is impossible. If at least one of v_j has a complex matrix, then $\mathcal{V}$ is of the form $X_\alpha T$ with $\alpha \neq \mathbf{0}$, which is again impossible. □

3.2 Construction of Nonadditive Codes

Examples of Nonadditive Codes. Now we show that there is an infinite family of nonadditive quantum error–correcting codes. These codes are constructed

following the scheme similar to the one described in Theorem 2.4 of [16]. Consider an $[n, k]$ binary code $\mathcal{C}$ such that $\mathrm{dist}(\mathcal{C})$ and $\mathrm{dist}(\mathcal{C}^\perp)$ are both at least d_0 ($\mathcal{C}$ needs not to be a weakly self–dual code).

First we define a function $\tau : \mathcal{C} \longrightarrow \{0,1\}^n$ such that for $c, c' \in \mathcal{C}$ and $c \neq c'$ we have $\tau(c)+\tau(c') \notin \mathcal{C}^\perp$. This means $\tau(c)$ and $\tau(c')$ are in different cosets of $\mathcal{C}^\perp$ in $\{0,1\}^n$, for $c \neq c'$. Since there are 2^k different cosets, such mapping τ always can be defined.

Fix $d \leq d_0$, and let $\mathcal{E}$ be the set of binary vectors of length n with weight $\leq d-1$. Consider a subset $R = \{\, a_0, a_1, \ldots, a_m \,\}$ of $\{0,1\}^n$ such that $a_0 = \mathbf{0}$ and a_j is not of the form $c + a_i + e$, for $c \in \mathcal{C}$, $1 \leq i \leq j-1$, and $e \in \mathcal{E}$. Then the vectors

$$|x_i\rangle = \sum_{c \in \mathcal{C}} (-1)^{\tau(c)\cdot a_i} |c + a_i\rangle \tag{8}$$

form a basis for a quantum code with distance d. To prove this, we show that $\langle x_i \mid X_\alpha Z_\beta \mid x_j \rangle = 0$, for $0 < \mathrm{wt}(\alpha \cup \beta) < d$. The case $\alpha \neq \mathbf{0}$ or $i \neq j$ is straightforward. So we only consider the case $\alpha = \mathbf{0}$ and $i = j$. Then for $0 < \mathrm{wt}(\beta) < d$ we have

$$\begin{aligned}
\langle x_i \mid Z_\beta \mid x_i \rangle &= \left\langle \sum_{c \in \mathcal{C}} (-1)^{\tau(c)\cdot a_i} |c + a_i\rangle \,\middle|\, \sum_{c \in \mathcal{C}} (-1)^{\tau(c)\cdot a_i + (c+a_i)\cdot\beta} |c + a_i\rangle \right\rangle \\
&= (-1)^{a_i \cdot \beta} \sum_{c \in \mathcal{C}} (-1)^{c\cdot\beta} \\
&= 0.
\end{aligned}$$

The last equality follows from the fact that $\mathrm{dist}(\mathcal{C}^\perp) \geq d$, so $\beta \notin \mathcal{C}^\perp$.

Lemma 2. *In the above construction, suppose that*

$$(n-1)2^k \sum_{i=0}^{d-1} \binom{n}{i} < 2^{n-1}. \tag{9}$$

Then it is possible to choose n linearly independent vectors $a_1, a_2, \ldots, a_n$ so that the $((\, n, n+1, d \,))$ quantum code $\mathcal{Q}$ with the basis $|x_0\rangle, |x_1\rangle, \ldots, |x_n\rangle$ (each $|x_i\rangle$ is defined by (8)) has trivial stabilizer, i.e., $\mathrm{St}(\mathcal{Q}) = \{I\}$.

Proof. Suppose that the vectors $a_0, a_1, \ldots, a_m$ with the desired properties are chosen. Then it is possible to choose a vector a_{m+1} such that $a_1, \ldots, a_m, a_{m+1}$ are independent and a_{m+1} is not of the form $c + a_i + e$ (for $c \in \mathcal{C}$, $1 \leq i \leq m$, and $e \in \mathcal{E}$) if $2^m + m \cdot 2^k \cdot \sum_{i=0}^{d-1} \binom{n}{i} < 2^n$. This shows that it is possible to choose n vector $a_1, \ldots, a_n$ with the desired properties.

Now we show that the identity operator is the only member of the stabilizer of $\mathcal{Q}$. Suppose that $X_\alpha Z_\beta$ is in the stabilizer of $\mathcal{Q}$. Since

$$X_\alpha Z_\beta |x_0\rangle = \sum_{c \in \mathcal{C}} (-1)^{c\cdot\beta} |c + \alpha\rangle$$

should be equal to $|x_0\rangle = \sum_{c\in\mathcal{C}} |c\rangle$ it follows that $\alpha \in \mathcal{C}$ and $\beta \in \mathcal{C}^\perp$. Similarly, for every $1 \le i \le n$ since

$$\begin{aligned} X_\alpha Z_\beta |x_i\rangle &= \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i + (c+a_i)\cdot\beta} |c + a_i + \alpha\rangle \\ &= \sum_{c\in\mathcal{C}} (-1)^{\tau(c+\alpha)\cdot a_i + (c+a_i+\alpha)\cdot\beta} |c + a_i\rangle \\ &= \sum_{c\in\mathcal{C}} (-1)^{(\tau(c+\alpha)+\beta)\cdot a_i} |c + a_i\rangle \end{aligned}$$

should be equal to

$$|x_i\rangle = \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a_i} |c + a_i\rangle ,$$

it follows that $a_i \cdot (\tau(c) + \tau(c+\alpha) + \beta) = 0$, for every $1 \le i \le n$. Since a_i's are independent, therefore $\tau(c) + \tau(c+\alpha) = \beta \in \mathcal{C}^\perp$, hence $\alpha = \mathbf{0}$. Now the conditions $a_i \cdot \beta = 0$ (for $1 \le i \le n$) imply $\beta = \mathbf{0}$. □

Theorem 6. *Suppose that $\mathcal{C}$ is an $[n, k, d_0]$ binary linear code such that $d_0 > k$ and dist($\mathcal{C}$) and dist($\mathcal{C}^\perp$) are at least d. Moreover, suppose that n, k and d satisfy* (9). *Let ℓ be the greatest integer such that $2^\ell \le 2^{n-k} / \sum_{i=0}^{d-1} \binom{n}{i}$. Suppose that $k + \ell < n$. Then there is a an $((n, 2^\ell, d))$ nonadditive code.*

Proof. Consider the $((n, n+1, d))$ code $\mathcal{Q}_0$ constructed in the previous lemma. Then by Theorem 4.2 of [16] it is possible to add at least $2^\ell - (n+1)$ more vectors to $\mathcal{Q}_0$ to build an $((n, 2^\ell, d))$ code $\mathcal{Q}$, which is, by Corollary 1, nonadditive. □

As an application we show that there are $((n, \lfloor 2^{n-1}/(n+1) \rfloor, 2))$ nonadditive codes, for every $n \ge 8$. Consider the $[n, 1, n]$ binary code $\mathcal{C} = \{\mathbf{0}, \mathbf{1}\}$. Then $\mathcal{C}^\perp$ is consists of all even weight vectors in $\{0,1\}^n$, so it is an $[n, n-1, 2]$ code. The condition (9) satisfies if $n \ge 8$. Then by applying the above theorem (for $k = 1$ and $\ell = \lceil n - 1 - \log_2(n+1) \rceil$) we get the desired code. Other classes of binary codes for which the minimum distance of the code and its dual are known (such as Hamming codes and Reed–Muller codes) can be used to get nonadditive codes with different parameters.

Finally, we show that the nonadditive codes are almost as good as Calderbank–Shor–Steane (CSS) codes, at least in the case that the dimension of code is large enough.

To utilize the CSS codes for constructing nonadditive codes, we must modify them such that the new codes have trivial stabilizers. Let $\mathcal{Q}$ be an $[[n, n-2k, d]]$ CCS code based on the weakly self–dual $[n, k]$ code $\mathcal{C}$ with dist($\mathcal{C}^\perp$) $\ge d$. Consider the basis for $\mathcal{Q}$ consisting of vectors of the form $|x_a\rangle = \sum_{c\in\mathcal{C}} |c + a\rangle$, for $a \in \mathcal{C}^\perp/\mathcal{C}$.

Also consider the function $\tau\colon \mathcal{C} \longrightarrow \{0,1\}^n$ defined at the beginning of this section. We define the quantum code $\widehat{\mathcal{Q}}$ with basis

$$|y_a\rangle = \sum_{c\in\mathcal{C}} (-1)^{\tau(c)\cdot a} |c+a\rangle\,, \tag{10}$$

for $a \in \mathcal{C}^\perp/\mathcal{C}$. Then it is easy to check that $\widehat{\mathcal{Q}}$ is also an $[[n, n-2k, d]]$ code.

Theorem 7. *Suppose that $\mathcal{C}$ is an $[n,k,d_0]$ weakly self–dual binary code, and $\mathcal{C}^\perp$ is an $[n,n-k,d_1]$ code. Assume $d_0 \geq k$ and $2^{n-2k-1} > n-k-1$ (for example it is enough to have $k < (n-\log_2 n)/2$). For any $d \leq d_1$ that staisfies*

$$\left(2^{n-k} + (k-1)2^k\right) \sum_{i=0}^{d-1} \binom{n}{i} < 2^{n-1}, \tag{11}$$

we have an $((n, 2^{n-2k}, d))$ nonadditive code.

Proof. Let $\mathcal{Q}_0$ be the $[[n, n-2k, d]]$ CSS code based on $\mathcal{C}$, and let $\widehat{\mathcal{Q}_0}$ be the quantum code obtained from $\mathcal{Q}_0$ as described in the preceding procedure. We can choose independent vectors $a_1, \ldots, a_{n-k}$ in $\mathcal{C}^\perp$ such that a_i's belong to different cosets of $\mathcal{C}$ in $\mathcal{C}^\perp$. This is possible because $2^{n-2k-1} > n-k-1$. We consider $|y_{a_1}\rangle, \ldots, |y_{a_{n-k}}\rangle$ (defined by (10)) as vectors in $\widehat{\mathcal{Q}_0}$. Then we choose vectors $a_{n-k+1}, \ldots, a_n$ such that $a_1, \ldots, a_n$ are n independent vectors, and $\mathcal{Q}' = \widehat{\mathcal{Q}_0} \cup \{|x_{a_{n-k+1}}\rangle, \ldots, |x_{a_n}\rangle\}$, is an $((n, 2^{n-2k}+k, d))$ code. The inequality (11) implies that it is possible to choose $a_{n-k+1}, \ldots, a_n$ with the desired properties. Then the proof of Lemma 2 shows that $\mathrm{St}(\mathcal{Q}') = \{I\}$

Let $\mathcal{Q}$ be the quantum code obtained from $\mathcal{Q}'$ by removing any k vectors except $|y_{a_i}\rangle$, $i = 1, \ldots, n$. Then $\mathrm{St}(\mathcal{Q}) = \{I\}$ (because $\mathcal{Q}$ contains the $|y_{a_i}\rangle$, $i = 1, \ldots, n$). So, by Corollary 1 with $\ell = n-2k$, $\mathcal{Q}$ is nonadditive. □

To show that there are weakly self–dual codes $\mathcal{C}$ that satisfy the requirements of the above theorem, it is possible to apply the greedy method used in classical coding theory (see [10], Chap. 17). The same method is used in [5] to prove the existence of CSS codes meeting the Gilbert–Varshamov bound. This method gives the following bound.

Theorem 8. *For $d < \lambda n$, where $\lambda = H_2^{-1}(H_2^{-1}(1/2))$, there are nonadditive $((n, 2^k, d))$ quantum codes with rate $k/n \geq 1 - 2H_2(d/n)$.* □

A Strongly Nonadditive Code. In this section we provide an example of a strongly nonadditive quantum error–correcting code. This is an $((11, 2, 3))$ strongly nonadditive code.

Consider the (Paley type) Hadamard matrix of order 12 (see, e.g., [10], p. 48). Delete the all–1 column and replace -1 by 1 and $+1$ by 0. The result is the following matrix

$$H = \begin{bmatrix} 0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0 \\ 1\,0\,1\,0\,0\,0\,1\,1\,1\,0\,1 \\ 1\,1\,0\,1\,0\,0\,0\,1\,1\,1\,0 \\ 0\,1\,1\,0\,1\,0\,0\,0\,1\,1\,1 \\ 1\,0\,1\,1\,0\,1\,0\,0\,0\,1\,1 \\ 1\,1\,0\,1\,1\,0\,1\,0\,0\,0\,1 \\ 1\,1\,1\,0\,1\,1\,0\,1\,0\,0\,0 \\ 0\,1\,1\,1\,0\,1\,1\,0\,1\,0\,0 \\ 0\,0\,1\,1\,1\,0\,1\,1\,0\,1\,0 \\ 0\,0\,0\,1\,1\,1\,0\,1\,1\,0\,1 \\ 1\,0\,0\,0\,1\,1\,1\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,1\,1\,1\,0\,1\,1 \end{bmatrix}.$$

We denote the i^{th} row of H by r_i. The set $\mathcal{C} = \{\, r_i : 1 \le i \le 12 \,\}$ is an $(11, 12, 6)$ code. Then a basis for the desired quantum code consists of the following two vectors:

$$|0_L\rangle = \sum_{i=1}^{12} |r_i\rangle\,,$$
$$|1_L\rangle = \sum_{i=1}^{12} |\mathbf{1} + r_i\rangle\,,$$

where $\mathbf{1}$ is the all–1 vector of length 11. We claim these vectors are basis for an $((11, 2, 3))$ quantum code. We have to show that

$$\langle 0_L \mid X_\alpha Z_\beta \mid 0_L\rangle = 0, \tag{12}$$
$$\langle 1_L \mid X_\alpha Z_\beta \mid 1_L\rangle = 0, \tag{13}$$
$$\langle 0_L \mid X_\alpha Z_\beta \mid 1_L\rangle = 0, \tag{14}$$

for every $\alpha, \beta \in \{0,1\}^{11}$ such that $1 \le \mathrm{wt}(\alpha \cup \beta) \le 2$. First note that that the distance of any two distinct vectors in the set

$$\{\, r_i : 1 \le i \le 12 \,\} \cup \{\, \mathbf{1} + r_i : 1 \le i \le 12 \,\}$$

is at least 5. Thus if $1 \le \mathrm{wt}(\alpha) \le 4$ then all conditions (12)–(14) hold. Now suppose that $\alpha = \mathbf{0}$. Then (14) trivially holds. To see that (12) and (13) hold it is enough to note that if $1 \le \mathrm{wt}(\beta) \le 2$ then $r_i \cdot \beta = 1$ for exactly 6 values of i. This completes the proof that $\{\, |0_L\rangle\,, |1_L\rangle \,\}$ is a basis for an $((11, 2, 3))$ quantum error–correcting code.

To show that this code is nonadditive, let $\varphi = (-1)^\lambda X_\alpha Z_\beta$ be any operator in the stabilizer of this code. Since $\varphi\,|0_L\rangle = |0_L\rangle$ and $\varphi\,|r_1\rangle = |\alpha\rangle$, hence $\lambda = 0$ and α should be one of r_i's. Then we should have $\alpha = r_1 = \mathbf{0}$, because for every r_i, $i \ne 1$, there is some j such that $r_i + r_j$ is not equal to any r_k. Therefore, $\varphi = Z_\beta$. Then

$$Z_\beta\,|1_L\rangle = \sum_{i=1}^{12} (-1)^{(\mathbf{1}+r_i)\cdot\beta}\,|\mathbf{1} + r_i\rangle = \sum_{i=1}^{12} |\mathbf{1} + r_i\rangle$$

implies that $(\mathbf{1} + r_i) \cdot \beta = 0$, for every i. But the set $\{ \mathbf{1} + r_i : 1 \leq i \leq 12 \}$ has rank 11, so $\beta = \mathbf{0}$. This shows that the identity operator is the only operator in the stabilizer of this code. Finally, suppose that $X_\alpha T$ is in the generalized stabilizer of this code, where the operator T is of the form (7). Note that the operator T only affects the phases of the states, so the above argument also implies $\alpha = \mathbf{0}$. Now Theorem 5 implies that this code is strongly nonadditive.

4 Concluding Remarks

We showed that there are nonadditive codes with different minimum distances. We also showed that nonadditive codes that correct t errors can reach the asymptotic rate $R \geq 1 - 2H_2(2t/n)$. We introduced the notion of strongly nonadditive codes, and gave an example of such codes. It would be interesting to find more examples of such codes. We conjecture that the nonadditive codes constructed in Section 3.2 are also strongly nonadditive codes.

Recently we have improved the construction method for nonadditive qunatum codes. With this new scheme, we are now able to give explicit constructions of nonadditive $((2m, \frac{1}{4}2^{2m}, 2))$ and strongly nonadditive $((2m+1, \frac{1}{8}(1 - \frac{1}{2m})2^{2m+1}, 2))$ codes. Also we have improved the asymptotic Gilbert–Varshamov bound for the rate of nonadditive codes. The new bound, which is for *strongly* nonadditive codes, is the same as the bound for additive codes [4], i.e., $R \geq 1 - H_2(2t/n) - (2t/n)\log_2 3$. All these results will appear in the final version of this paper [14].

References

1. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters, "Mixed state entanglement and quantum error correction," *Phys. Rev. A*, Vol. 54, No. 5, pp. 3824–3851 (1996).
2. M. Grassl and Th. Beth, "A note on non–additive quantum codes," LANL e–print quant–ph/97030126.
3. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, Vol. 78, pp. 405–408 (1997).
4. A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," LANL e–print quant–ph/9608006.
5. A. R. Calderbank and P. W. Shor, "Good quantum error–correcting codes exit," *Phys. Rev. A*, Vol. 54, No. 2, pp. 1098–1105 (1996).
6. R. Cleve, "Quantum stabilizer codes and classical linear codes," LANL e–print quant–ph/9612048.
7. D. Gottesman, "A class of quantum error–correcting codes saturating the quantum Hamming bound," *Phys. Rev. A*, Vol. 54, No. 3, pp. 1862–8168 (1996).
8. E. Knill and R. Laflamme, "A theory of quantum error–correcting codes," LANL e–print quant–ph/9604034.
9. F. J. MacWilliams, N. J. Sloane and J. P. Thompson, "Good self dual codes exist," *Discrete Math.*, vol. 3, pp. 153–162 (1972).
10. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North–Holland, New York, 1977.

11. E. M. Rains, "Quantum shadow enumerators," LANL e–print quant–ph/9611001.
12. E. M. Rains, "Quantum codes of minimum distance two," LANL e–print quant–ph/9704043.
13. E. M. Rains, R. H. Hardin, P. Shor and N. J. A. Sloane, "A nonadditive quantum code," *Phys. Rev. Lett.*, Vol. 79, pp. 953–954 (1997).
14. V. Roychowdhury and F. Vatan, "On the structure of additive codes and the existence of nonadditive codes," LANL e–print quant–ph/9710031.
15. A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, Vol. 77, No. 5, pp. 793–797 (1996).
16. F. Vatan, V. P. Roychowdhury and M. P. Anantram, "Spatially correlated qubit errors and burst–correcting quantum codes," LANL e–print quant–ph/9704019. To appear in *IEEE Transactions on Information Theory*.