TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 360, Number 4, April 2008, Pages 2007–2019
S 0002-9947(07)04242-0
Article electronically published on October 23, 2007

A NEW CONSTRUCTION OF QUANTUM ERROR-CORRECTING CODES

KEQIN FENG AND CHAOPING XING

Abstract. In this paper, we present a characterization of (binary and non-binary) quantum error-correcting codes. Based on this characterization, we introduce a method to construct p-ary quantum codes using Boolean functions satisfying a system of certain quadratic relations. As a consequence of the construction, we are able to construct quantum codes of minimum distance 2. In particular, we produce a class of binary quantum $((n, 2^{n-2}-\frac{1}{2}\binom{n-1}{(n-1)/2}, 2))$-codes for odd length $n \geq 5$. For $n \geq 11$, this improves the result by Rains in *Quantum codes of minimal distance two*, 1999, showing the existence of binary quantum $((n, 3\cdot 2^{n-4}, 2))$-codes for odd $n \geq 5$. Moreover, our binary quantum $((n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2))$-codes of odd length achieve the Singleton bound asymptotically.

Finally, based on our characterization some propagation rules of quantum codes are proposed and the rules are similar to those in classical coding theory. It turns out that some new quantum codes are found through these propagation rules.

1. Introduction

Quantum information has received much attention for the past few years. Since the pioneering work in [2, 3, 12, 13, 14], the theory of quantum error-correcting codes has developed rapidly.

As in classical coding theory, one of the central tasks in quantum coding theory is to construct good quantum codes. The first systematic mathematical construction is given by Calderbank et al. [2] in the binary case and then generalized by Rains [8], Ashikhmin and Knill [1] and Matsumoto and Uyematsu [7] to the non-binary case. The p-ary quantum codes by this construction are called stabilizer quantum codes and are derived from classical codes over finite fields $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ through various techniques. Another construction is presented by Schlingemann and Werner [11] using combinatorial properties of matrices over finite fields. Many good quantum codes with various parameters have been constructed in these ways, but all p-ary quantum codes produced by these constructions have dimensions being powers of p. On the other hand, quantum codes with general dimensions have been studied by Knill [4, 5] and Rains [9], etc.

One extreme situation is the construction of quantum codes with minimum distance 2. For p-ary quantum codes with $p > 2$, the optimal quantum codes with

Received by the editors June 30, 2005 and, in revised form, November 7, 2005 and December 20, 2005.

2000 *Mathematics Subject Classification.* Primary 11T71, 94B60, 05A18.

This work was supported by the National Scientific Research Project 973 of China.

minimum distance 2, i.e., quantum codes with length n, minimum distance 2 and dimension p^{n-2}, are in fact readily obtained using the stabilizer method [2, 8, 1, 7]. For the binary case, optimal quantum codes with minimum distance 2 and dimension 2^{n-2} have been constructed [2, 9]. However, hardly anything is known about the dimension of optimal binary quantum codes with odd length and minimum distance 2.

In this paper we present a characterization of (binary and non-binary) quantum codes. Based on this characterization, we are able to derive a method to construct pure p-ary quantum codes with dimensions not necessarily equal to powers of p. With this method, the construction of quantum codes is reduced to finding functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ satisfying a system of quadratic relations. As the first consequence of the construction, we are able to construct quantum codes of minimum distance 2. In particular, we produce a class of binary quantum $((n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2))$-codes for odd length $n \geq 5$. By a simple propagation rule, Rains [9] gives a family of binary quantum $((n, 3 \cdot 2^{n-4}, 2))$-codes for odd $n \geq 5$. For $n \geq 11$, our codes are better than those by Rains [9] in the sense that our codes are bigger in size. Moreover, our binary quantum $((n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2))$-codes of odd length achieve the quantum Singleton bound asymptotically.

Other advantages of our characterization of quantum codes include the formulation of propagation rules for quantum codes. Classical coding theory has a much longer history, and various constructions and propagation rules have been proposed. Based on our characterization of quantum codes, we can induce some propagation rules for quantum codes similar to those in classical coding theory. In particular, some new binary quantum codes are found based on our propagation rules.

The paper is organized as follows. We recall the definitions and basic facts on quantum codes in Section 2 and show our characterization of quantum codes in Section 3. Then we present our construction of quantum codes by using quadratic functions and show several consequences in Section 4. Finally in Section 5, some propagation rules are derived based on our characterization in Section 3.

2. Basic facts on quantum codes

Binary quantum codes have been generalized to q-ary quantum codes with q being any prime number [8] and even a power of a prime [1]. In this paper we restrict ourselves to p-ary quantum codes with p being a prime number for simplicity. First we recall the definition of quantum codes.

Let $\mathbb{C}^p$ be a complex vector space of dimension p and let $\{\mid 0 >, \mid 1 >, \cdots, \mid p-1 >\}$ be an orthonormal basis of $\mathbb{C}^p$ with respect to the hermitian inner product, denoted by $\langle \cdot, \cdot \rangle$, or $\langle \cdot | \cdot \rangle$ or $(\cdot, \cdot)$. A *p-ary quantum state* $\mid v >$ is a non-zero vector in $\mathbb{C}^p$:

$$0 \neq \mid v >= \sum_{i=0}^{p-1} \alpha_i \mid i >= \sum_{c \in \mathbb{F}_p} \alpha_c \mid c > \qquad (\alpha_c \in \mathbb{C}),$$

where $\mathbb{F}_p$ denotes the finite field with p elements.

For $n \geq 1$, the *n-th* tensor product $(\mathbb{C}^p)^{\otimes n} = \mathbb{C}^{p^n}$ has a basis

$$\left\{ \mid \mathbf{c} >= \mid c_1 > \otimes \mid c_2 > \otimes \cdots \otimes \mid c_n >: \ \mathbf{c} = (c_1, \cdots, c_n) \in \mathbb{F}_p^n \right\}.$$

A p-ary n-system state $\mid \mathbf{v} >$ is a non-zero vector in $(\mathbb{C}^p)^{\otimes n}$:

$$0 \neq \mid \mathbf{v} >= \sum_{\mathbf{c}\in\mathbb{F}_p^n} \alpha_{\mathbf{c}} \mid \mathbf{c} >,$$

where $\alpha_{\mathbf{c}} \in \mathbb{C}$.

Let ζ be the *p-th* primitive root of unity: $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$. There are three types of *quantum bit errors*: σ_a, τ_b and the composition $\sigma_a\tau_b$, where $a, b \in \mathbb{F}_p$. They act on a quantum state as unitary linear operators on $\mathbb{C}^p$ defined by

$$\sigma_a \mid v >= \mid v + a >, \quad \tau_b|v >= \zeta^{bv}|v > .$$

Thus,

$$\sigma_a\tau_b \mid v >= \zeta^{bv} \mid v + a >= \zeta^{-ab}\zeta^{(a+v)b}|v + a >= \zeta^{-ab}\tau_b\sigma_a|v > .$$

Hence, the set of bit errors

$$\left\{\zeta^\lambda\sigma_a\tau_b :\ 0 \leq \lambda \leq p-1,\ a, b \in \mathbb{F}_p\right\}$$

forms a group under the group law $\sigma_a\tau_b = \zeta^{-ab}\tau_b\sigma_a$, $\sigma_a\sigma_{a'} = \sigma_{a+a'}$ and $\tau_b\tau_{b'} = \tau_{b+b'}$. It is clear that the identity of this group is $\sigma_0 = \tau_0$ and two elements $\zeta^\lambda\sigma_a\tau_b$ and $\zeta^{\lambda'}\sigma_{a'}\tau_{b'}$ are equal if and only if $(\lambda, a, b) = (\lambda', a', b')$.

A quantum error $\mathbf{e}$ on an n-system state is a unitary linear operator on $(\mathbb{C}^p)^{\otimes n}$ of the form

$$\mathbf{e} = \zeta^\lambda w_1 \otimes \cdots \otimes w_n \tag{2.1}$$

with $w_i = \sigma_{a_i}\tau_{b_i}$ for some $a_i, b_i, \lambda \in \mathbb{F}_p$, $i = 1, \ldots, n$. It acts on the basis elements $\mid \mathbf{v} >= \mid v_1 > \otimes \cdots \otimes |v_n >$ bit-by-bit:

$$\mathbf{e} \mid \mathbf{v} >= \zeta^\lambda(w_1 \mid v_1 >) \otimes \cdots \otimes (w_n \mid v_n >) = \zeta^{\lambda+\mathbf{b}\cdot\mathbf{v}} \mid \mathbf{v} + \mathbf{a} >, \tag{2.2}$$

where $\mathbf{a} = (a_1, \cdots, a_n), \mathbf{b} = (b_1, \cdots, b_n) \in \mathbb{F}_p^n$ and $\mathbf{b} \cdot \mathbf{v} = \sum_{i=1}^n b_i v_i \in \mathbb{F}_p$ is the usual inner product in $\mathbb{F}_p^n$. Let

$$X(\mathbf{a}) = \sigma_{a_1} \otimes \cdots \otimes \sigma_{a_n}, \quad Z(\mathbf{b}) = \tau_{b_1} \otimes \cdots \otimes \tau_{b_n}.$$

Then the quantum error $\mathbf{e}$ in (2.1) can be denoted by $\mathbf{e} = \zeta^\lambda X(\mathbf{a})Z(\mathbf{b})$ and the set of all quantum errors

$$E_n := \left\{\zeta^\lambda X(\mathbf{a})Z(\mathbf{b}) :\ \mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n,\ \lambda \in \mathbb{F}_p\right\}$$

forms a non-abelian group of order p^{2n+1} under the group law

$$X(\mathbf{a})X(\mathbf{a}') = X(\mathbf{a}+\mathbf{a}'); \quad Z(\mathbf{b})Z(\mathbf{b}') = Z(\mathbf{b}+\mathbf{b}'); \quad X(\mathbf{a})Z(\mathbf{b}) = \zeta^{-\mathbf{a}\cdot\mathbf{b}}Z(\mathbf{b})X(\mathbf{a}).$$

For two error operators $\mathbf{e} = \zeta^\lambda X(\mathbf{a})Z(\mathbf{b})$ and $\mathbf{e}' = \zeta^{\lambda'} X(\mathbf{a}')Z(\mathbf{b}')$, we have the following basic relationships:

$$\mathbf{e}^p = I \text{ (identity)}, \quad \mathbf{e}\mathbf{e}' = \zeta^{\mathbf{a}'\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}'}\mathbf{e}'\mathbf{e}. \tag{2.3}$$

It is easy to verify that the center $C(E_n)$ of E_n is $\left\{\zeta^\lambda I :\ \lambda \in \mathbb{F}_p\right\}$. It follows from (2.3) that the quotient group

$$\overline{E}_n = E_n/C(E_n)$$

is an elementary p-group of order $|\overline{E}_n| = p^{2n}$, hence it is isomorphic to the additive group $\mathbb{F}_p^{2n}$. For simplicity, we denote the canonical image of $\mathbf{e} = \zeta^\lambda X(\mathbf{a})Z(\mathbf{b})$ in $\overline{E}_n$ by $\overline{\mathbf{e}} = (\mathbf{a} \mid \mathbf{b}) \in \mathbb{F}_p^{2n}$; then $(\mathbf{a} \mid \mathbf{b}) \cdot (\mathbf{a}' \mid \mathbf{b}') = (\mathbf{a} + \mathbf{a}' \mid \mathbf{b} + \mathbf{b}')$.

In quantum mechanics, two n-system states $|\ \mathbf{v}>$ and $\alpha\ |\ \mathbf{v}>$ ($\alpha \in \mathbb{C}^*$) represent the same quantum state. Thus, $\mathbf{e}$ and $\zeta^\lambda \mathbf{e}$ are the same error operator on $(\mathbb{C}^p)^{\otimes n}$, so that we can define the action of $\overline{\mathbf{e}} \in \overline{E}_n$ by $\overline{\mathbf{e}}\ |\ \mathbf{v}>=\mathbf{e}\ |\ \mathbf{v}>$.

For $\mathbf{e}=\zeta^\lambda X(\mathbf{a})Z(\mathbf{b}) \in E_n$ and $\overline{\mathbf{e}}=(\mathbf{a}\ |\ \mathbf{b}) \in \overline{E}_n$ with $\mathbf{a}=(a_1,\cdots,a_n),\ \mathbf{b}=(b_1,\cdots,b_n) \in \mathbb{F}_p^n$, we define the *quantum weight* of $\mathbf{e}$ and $\overline{\mathbf{e}}$ by

$$w_Q(\mathbf{e})=w_Q(\overline{\mathbf{e}})=\#\left\{i:\ 1\le i\le n,\ (a_i,b_i)\ne(0,0)\in\mathbb{F}_p^2\right\}.$$

For $0\le l\le n$, we denote by

$$E_n(l)=\{\mathbf{e}\in E_n:\ w_Q(\mathbf{e})\le l\},\quad \overline{E}_n(l)=\{\overline{\mathbf{e}}\in\overline{E}_n:\ w_Q(\overline{\mathbf{e}})\le l\}$$

the subsets E_n and $\overline{E}_n$ of, respectively, weight less than or equal to l. It is easy to see that $|\overline{E}_n(l)|=\sum_{i=0}^{l}(p^2-1)^i\binom{n}{i}$ and $|E_n(l)|=p\cdot|\overline{E}_n(l)|$.

Definition 2.1. Let p be a prime number. A complex linear subspace $Q\ne\{\mathbf{0}\}$ of $\left(\mathbb{C}^p\right)^{\otimes n}=\mathbb{C}^{p^n}$ is called a *quantum code* of *length* n.

We denote by $K=\dim_{\mathbb{C}} Q$ the dimension of Q over $\mathbb{C}$ and put $k=\log_p K$. Then k is a real number and $0\le k\le n$.

The *minimum distance* of a quantum code Q is defined to be the largest positive integer d satisfying the following condition:

> for any $|\ \mathbf{u}>$ and $|\ \mathbf{v}>$ in Q with $\langle \mathbf{u}\ |\ \mathbf{v}\rangle=0$ and $\overline{\mathbf{e}}\in\overline{E}_n(d-1)$, we have $\langle \mathbf{u}\ |\ \overline{\mathbf{e}}\ |\ \mathbf{v}\rangle=0$, where $\langle,\rangle$ denotes the hermitian inner product in $(\mathbb{C}^p)^{\otimes n}$.

A p-ary quantum code Q with length n, dimension K ($k=\log_p K$) and minimum distance d is denoted by $((n,K,d))_p$ or $[[n,k,d]]_p$. A quantum $((n,K,d))_p$-code Q is called *pure* if $\langle \mathbf{u}\ |\ \overline{\mathbf{e}}\ |\ \mathbf{v}\rangle=0$ for all $\overline{\mathbf{e}}\in\overline{E}_n(d-1)\setminus\{\mathbf{0}\}$ and $\mathbf{u},\mathbf{v}\in Q$ (note that we do not require $\langle \mathbf{u}|\mathbf{v}\rangle=0$ here).

As in classical coding theory, we have the following two fundamental bounds.

Lemma 2.2. *Let Q be a quantum $((n,K,d))_p$-code and put $k=\log_p K$.*

(i) (**quantum Hamming bound** [2]) *If Q is pure, then*

$$p^n\ge K\sum_{i=0}^{\lfloor\frac{d-1}{2}\rfloor}(p^2-1)^i\binom{n}{i}.$$

(ii) (**quantum Singleton bound** [8]) *If $K>1$, then*

$$K\le p^{n-2d+2}\qquad (or\ n\ge k+2d-2).$$

3. A characterization of quantum codes

In this section, we present a characterization on quantum $Q=((n,K,d))_p$-codes. It gives an alternative way to construct quantum codes.

An n-system state $|\mathbf{v}>=\sum_{\mathbf{c}\in\mathbb{F}_p^n}\alpha_{\mathbf{c}}|\mathbf{c}>$ can be identified with a mapping φ: $\mathbb{F}_p^n\to\mathbb{C}$ defined by $\varphi(\mathbf{c})=\alpha_{\mathbf{c}}$ for all $\mathbf{c}\in\mathbb{F}_p^n$.

For a map φ: $\mathbb{F}_p^n\to\mathbb{C}$ and a partition $\{1,2,\cdots,n\}=A\cup B$, we denote $\varphi(\mathbf{c})$ by $\varphi(\mathbf{c}_A,\mathbf{c}_B)$, where $\mathbf{c}_A$ and $\mathbf{c}_B$ are the subvectors of $\mathbf{c}$ whose coordinate positions belong to A and B, respectively. For two maps $\varphi,\psi:\mathbb{F}_p^n\to\mathbb{C}$, we define their

hermitian inner product by

$$(\varphi, \psi) = \sum_{\mathbf{c} \in \mathbb{F}_p^n} \overline{\varphi(\mathbf{c})} \psi(\mathbf{c}) \in \mathbb{C},$$

where $\overline{\varphi(\mathbf{c})}$ stands for the conjugate of the complex number $\varphi(\mathbf{c})$.

Now we state and prove our characterization on quantum codes.

Theorem 3.1. (i) *There exists a quantum $((n, K, d))_p$-code with $K \geq 2$ if and only if there exist K non-zero mappings*

$$\varphi_i : \mathbb{F}_p^n \to \mathbb{C} \quad (1 \leq i \leq K) \tag{3.1}$$

satisfying the following condition:

for each partition $\{1, 2, \cdots, n\} = A \cup B$ with $\mid A \mid = d-1$ and $\mid B \mid = n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1}$, $1 \leq i, j \leq n$,

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = \begin{cases} 0 & \text{if } 1 \leq i \neq j \leq K; \\ f & \text{if } 1 \leq i = j \leq K, \end{cases} \tag{3.2}$$

where $f = f(\mathbf{c}_A, \mathbf{c}'_A)$ is independent of i.

(ii) *There exists a pure quantum $((n, K, d))_p$-code with $K \geq 1$ if and only if there exist K mappings $\mathbb{F}_p^n \to \mathbb{C}$ $(1 \leq i \leq K)$ such that*

(I) *the rank of the matrix $(\varphi_i(\mathbf{c}))_{1 \leq i \leq K,\, \mathbf{c} \in \mathbb{F}_p^n}$ is K;*

(II) *for each partition $\{1, 2, \cdots, n\} = A \cup B$ with $\mid A \mid = d-1$ and $\mid B \mid = n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1}$, $1 \leq i, j \leq n$,*

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = \begin{cases} 0 & \text{if } \mathbf{c}_A \neq \mathbf{c}'_A; \\ (\varphi_i, \varphi_j)/p^{d-1} & \text{if } \mathbf{c}_A = \mathbf{c}'_A. \end{cases} \tag{3.3}$$

Proof. (i) Let Q be a K-dimensional subspace of $\mathbb{C}^{p^n}$ with an orthonormal basis:

$$\mid \mathbf{v}_i > = \sum_{\mathbf{c} \in \mathbb{F}_p^n} \varphi_i(\mathbf{c}) \mid \mathbf{c} > \quad (1 \leq i \leq K),$$

i.e.,

$$(\varphi_i, \varphi_j) = \sum_{\mathbf{c} \in \mathbb{F}_p^n} \overline{\varphi_i(\mathbf{c})} \varphi_j(\mathbf{c}) = \langle \mathbf{v}_i \mid \mathbf{v}_j \rangle = \begin{cases} 0 & \text{if } i \neq j; \\ 1 & \text{if } i = j. \end{cases}$$

For two vectors in Q

$$\mid \mathbf{u} > = \sum_{i=1}^{K} \alpha_i \mid \mathbf{v}_i >, \quad \mid \mathbf{u}' > = \sum_{i=1}^{K} \alpha'_i \mid \mathbf{v}_i > \qquad (\alpha_i, \alpha'_i \in \mathbb{C}),$$

we have

$$\langle \mathbf{u} \mid \mathbf{u}' \rangle = \sum_{i,\, j=1}^{K} \overline{\alpha}_i \alpha'_j \langle \mathbf{v}_i \mid \mathbf{v}_j \rangle = \sum_{i=1}^{K} \overline{\alpha}_i \alpha'_i. \tag{3.4}$$

For each $\mathbf{e} = X(\mathbf{a}) Z(\mathbf{b})$ with $w_Q(\mathbf{e}) = l$, let

$$A = \{i \mid 1 \leq i \leq n,\ (a_i, b_i) \neq (0, 0)\}.$$

Then we have a partition $\{1,2,\cdots,n\} = A \cup B$ with $|A| = l,\ |B| = n-l$, and $\mathbf{e} = X(\mathbf{a}_A, \mathbf{0}_B)Z(\mathbf{b}_A, \mathbf{0}_B)$. Thus,

$$\begin{aligned}
\mathbf{e} \mid \mathbf{u}' > &= \sum_{j=1}^{K} \alpha'_j \mathbf{e} \mid \mathbf{v}_j > = \sum_{j=1}^{K} \alpha'_j \sum_{\mathbf{c}\in\mathbb{F}_p^n} \varphi_j(\mathbf{c})\mathbf{e} \mid \mathbf{c} > \\
&= \sum_{j=1}^{K} \alpha'_j \sum_{\mathbf{c}\in\mathbb{F}_p^n} \varphi_j(\mathbf{c})\zeta^{\mathbf{b}\cdot\mathbf{c}} \mid \mathbf{a}+\mathbf{c} > \qquad \text{(by (2.2))} \\
&= \sum_{j=1}^{K} \alpha'_j \sum_{\mathbf{c}_A\in\mathbb{F}_p^l,\, \mathbf{c}_B\in\mathbb{F}_p^{n-l}} \varphi_j(\mathbf{c}_A, \mathbf{c}_B)\zeta^{\mathbf{b}_A\cdot\mathbf{c}_A} \mid \mathbf{a}_A + \mathbf{c}_A,\ \mathbf{c}_B > \\
&= \sum_{j=1}^{K} \alpha'_j \sum_{\mathbf{c}_A,\, \mathbf{c}_B} \zeta^{\mathbf{b}_A\cdot(\mathbf{c}_A-\mathbf{a}_A)}, \varphi_j(\mathbf{c}_A - \mathbf{a}_A,\ \mathbf{c}_B) \mid \mathbf{c}_A, \mathbf{c}_B > .
\end{aligned}$$

Therefore,

$$\langle \mathbf{u} \mid \mathbf{e} \mid \mathbf{u}' \rangle = \zeta^{-\mathbf{b}_A\cdot\mathbf{a}_A} \sum_{i,\, j=1} \overline{\alpha}_i \alpha'_j \sum_{\mathbf{c}_A,\, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A - \mathbf{a}_A, \mathbf{c}_B)\zeta^{\mathbf{b}_A\cdot\mathbf{c}_A}. \tag{3.5}$$

By Definition 2.1, Q is a quantum code with minimum distance d if and only if $\langle \mathbf{u} \mid \mathbf{e} \mid \mathbf{u}' \rangle = 0$ for any orthogonal $\mid \mathbf{u} >$ and $\mid \mathbf{u}' >$ in Q and $\mathbf{e} \in E_n(d-1)$. It follows from (3.4) and (3.5) that this is equivalent to the following:

> for each partition $\{1,2,\cdots,n\} = A \cup B$ with $|A| = d-1,\ |B| = n-d+1$ and $\mathbf{a}_A, \mathbf{b}_A \in \mathbb{F}_p^{d-1}$ with $(\mathbf{a}_A, \mathbf{b}_A) \neq (\mathbf{0}, \mathbf{0})$, $\sum_{i=1}^{K} \overline{\alpha}_i \alpha'_j = 0$ implies that

$$\sum_{i,\, j=1}^{K} \overline{\alpha}_i \alpha'_j \sum_{\mathbf{c}_A,\, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A - \mathbf{a}_A, \mathbf{c}_B)\zeta^{\mathbf{b}_A\cdot\mathbf{c}_A} = 0. \tag{3.6}$$

By the Fourier transform, the condition (3.6) is equivalent to

$$\sum_{i,\, j=1}^{K} \overline{\alpha}_i \alpha'_j \sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = 0 \tag{3.7}$$

for each partition $\{1,2,\cdots,n\} = A \cup B$ with $|A| = d-1,\ |B| = n-d+1$ and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1}$. Let

$$M = (m_{ij})_{1\le i,j\le K}, \quad m_{ij} = \sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}'_A, \mathbf{c}_B) \in \mathbb{C}.$$

The above condition becomes that for any $\mathbf{a}$=$(a_1,\cdots,a_K), \mathbf{a}' = (a'_1,\cdots,a'_K) \in \mathbb{C}^K$, $\langle \mathbf{a},\ \mathbf{a}' \rangle = 0$ implies that $\overline{\mathbf{a}} M {\mathbf{a}'}^T = 0$. It is easy to see that under the assumption $K \ge 2$, the condition is equivalent to the equality $M{\mathbf{a}'}^T = f{\mathbf{a}'}^T$ for any $\mathbf{a}' \in \mathbb{C}^K$, where $f \in \mathbb{C}$ is independent of $\mathbf{a}'$. Thus, $M = fI_K$. This implies that our condition is equivalent to the condition (3.2).

(ii) Let $\mid \mathbf{v}_i > = \sum_{\mathbf{c}\in\mathbb{F}_p^n} \varphi_i(\mathbf{c}) \mid \mathbf{c} >\ \ (1 \le i \le K)$. Let Q be the subspace of $\mathbb{C}^{p^n}$ with the basis $\mid \mathbf{v}_i >\ \ (1 \le i \le K)$. By definition, Q is a pure quantum $((n,K,d))_p$-code if and only if $\langle \mathbf{v}_i \mid \mathbf{e} \mid \mathbf{v}_j \rangle = 0$ for $1 \le i,j \le K$ and each $\mathbf{e} \in E_n$

with $1 \le w_Q(\mathbf{e}) \le d-1$. By arguments similar to those in (i), this requirement can be transformed into

$$\sum_{\mathbf{c}_A,\, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A - \mathbf{a}_A, \mathbf{c}_B)\zeta^{\mathbf{b}_A \cdot \mathbf{c}_A} = 0 \tag{3.8}$$

for each partition $\{1, 2, \cdots, n\} = A \cup B$ with $|A| = d-1,\ |B| = n-d+1$ and any $\mathbf{a}_A, \mathbf{b}_A \in \mathbb{F}_p^{d-1}$ such that $(\mathbf{a}_A, \mathbf{b}_A) \ne (\mathbf{0}, \mathbf{0})$.

If $\mathbf{a}_A \ne \mathbf{0}$, then (3.8) is satisfied for all $\mathbf{b}_A \in \mathbb{F}_p^{d-1}$. This implies the first equality of condition (II).

If $\mathbf{a}_A = \mathbf{0}$, then for all $\mathbf{0} \ne \mathbf{b}_A \in \mathbb{F}_p^{d-1}$,

$$\sum_{\mathbf{c}_A,\, \mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A, \mathbf{c}_B)\zeta^{\mathbf{b}_A \cdot \mathbf{c}_A} = 0.$$

By the Fourier transform, this is equivalent to

$$\sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A, \mathbf{c}_B) = f_{ij},$$

where $f_{ij} \in \mathbb{C}$ is independent of $\mathbf{c}_A$. Then we have

$$(\varphi_i, \varphi_j) = \sum_{\mathbf{c}_A,\, c_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)}\varphi_j(\mathbf{c}_A, \mathbf{c}_B) = \sum_{\mathbf{c}_A \in \mathbb{F}_p^{d-1}} f_{ij} = f_{ij}p^{d-1},$$

i.e., $f_{ij} = (\varphi_i, \varphi_j)/p^{d-1}$. This completes the proof. □

For stabilizer quantum codes (see [2] for $p = 2$, and [1] for $p \ge 3$), φ_i are simply maps from $\mathbb{F}_p^n$ to the set $\{\zeta^i :\ i = 0, 1, \cdots, p-1\} \cup \{0\}$.

Now we consider even simpler maps φ from $\mathbb{F}_p^n$ to $\{\zeta^i :\ i = 0, 1, \cdots, p-1\}$. It is clear that φ is determined by a function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ through the relationship

$$\varphi(\mathbf{c}) = \zeta^{f(\mathbf{c})} \qquad (\mathbf{c} \in \mathbb{F}_p^n).$$

As a direct consequence of Theorem 3.1, we obtain the following construction of quantum codes.

Theorem 3.2. (i) *Suppose that $n \ge 2,\ 1 \le d \le n$ and $2 \le K \le p^n$. If there exist K functions $f_i : \mathbb{F}_p^n \to \mathbb{F}_p$ $(1 \le i \le K)$ such that for any partition $\{1, 2, \cdots, n\} = A \cup B$ with $|A| = d-1,\ |B| = n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1}$,*

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \zeta^{f_i(\mathbf{c}_A,\, \mathbf{c}_B) - f_j(\mathbf{c}'_A,\, \mathbf{c}_B)} = \begin{cases} 0 & \text{if } 1 \le i \ne j \le K; \\ f & \text{if } 1 \le i = j \le K, \end{cases} \tag{3.9}$$

where $f = f(\mathbf{c}_A, \mathbf{c}'_A) \in \mathbb{C}$ is independent of i, then there exists a quantum $((n, K, d))_p$-code.

(ii) *Suppose that $n \ge 2,\ 1 \le d \le n$ and $1 \le K \le p^n$. If there exist K functions $f_i : \mathbb{F}_p^n \to \mathbb{F}_p$ $(1 \le i \le K)$ such that*

(I) *the rank of the matrix $(\zeta^{f_i(\mathbf{c})})_{1 \le i \le K,\, \mathbf{c} \in \mathbb{F}_p^n}$ is K;*

(II) *for each partition $\{1, 2, \cdots, n\} = A \cup B$ with $|A| = d-1$ $|B| = n-d+1$, and any $\mathbf{c}_A, \mathbf{c}'_A \in \mathbb{F}_p^{d-1},\ 1 \le i, j \le K$,*

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \zeta^{f_i(\mathbf{c}_A,\, \mathbf{c}_B) - f_j(\mathbf{c}'_A,\, \mathbf{c}_B)} = \begin{cases} 0 & \text{if } \mathbf{c}_A \ne \mathbf{c}'_A; \\ f_{ij} & \text{if } \mathbf{c}_A = \mathbf{c}'_A, \end{cases} \tag{3.10}$$

where f_{ij} is independent of $\mathbf{c}_A$ (so that $f_{ij}=p^{-(d-1)}\sum_{\mathbf{c}\in\mathbb{F}_p^n}\zeta^{f_i(\mathbf{c})-f_j(\mathbf{c})}$), then there exists a pure quantum $((n,K,d))_p$-code.

Remark 3.3. (i) If f_{ij} in condition (I) of Theorem 3.2(ii) are equal to 0 for all $1\le i\ne j\le K$, then all rows in the matrix $(\zeta^{f_i(\mathbf{c})})_{1\le i\le K,\,\mathbf{c}\in\mathbb{F}_p^n}$ are orthogonal to each other. Hence, condition (I) is satisfied automatically.

(ii) All p-ary quantum codes previously constructed in [1, 2, 11] have dimensions K being powers of p (note that quantum codes with general dimensions have been considered by Knill [4, 5] and Rains [9], etc.). Theorems 3.1 and 3.2 in this paper make it possible to construct good quantum codes with arbitrary dimension. In the next section, we try to construct quadratic functions satisfying condition (3.10) in Theorem 3.2. We will show that, even in this simple case, several new quantum codes can be obtained and some previous results are improved.

4. Quantum codes from quadratic functions

For a matrix $H=(h_{ij})_{1\le i\le m,\,1\le j\le n}$ over $\mathbb{F}_p$ and a partition $\{1,2,\cdots,n\}=A\cup B$, we denote by H_A and H_B the submatrices

$$H_A=(h_{ij})_{1\le i\le m;\,j\in A},\quad H_B=(h_{ij})_{1\le i\le m;\,j\in B}.$$

However, if H is a square matrix, i.e., $m=n$, we have a different way to define four submatrices H_{AA}, H_{AB}, H_{BA} and H_{BB}, where, for example, $H_{AB}=(h_{ij})_{i\in A,\,j\in B}$.

Theorem 4.1. *Suppose that $d\ge 2$, $1\le k\le n$ and $1\le K\le p^k$. Let $N_{k\times n}$ and $M_{n\times n}$ be two matrices, and let $\{\mathbf{v}_1,\cdots,\mathbf{v}_K\}$ be K distinct vectors in $\mathbb{F}_p^k$. Suppose $M=(m_{ij})$ is a zero-diagonal symmetric matrix (i.e., $m_{ii}=0$ and $m_{ij}=m_{ji}$ for $1\le i,j\le n$) and the following condition is satisfied:*

for each partition $\{1,2,\cdots,n\}=A\cup B$ with $|A|=d-1$, $|B|=n-d+1$, any $\mathbf{c}\in\mathbb{F}_p^{d-1}$ and $1\le i,j\le K$, the equality

$$(\mathbf{v}_i-\mathbf{v}_j)N_B=\mathbf{c}M_{AB} \tag{4.1}$$

implies that $\mathbf{c}=0$ and $\mathbf{v}_i=\mathbf{v}_j$.

Then there exists a pure quantum $((n,K,d))_p$-code. In particular, if the rank of $\begin{pmatrix} N_B \\ M_{AB}\end{pmatrix}$ is $k+d-1$ for each partition $\{1,2,\cdots,n\}=A\cup B$ with $|A|=d-1$, $|B|=n-d+1$, then there exists a pure quantum $[[n,k,d]]_p$-code.

Proof. For a square matrix $H=(h_{ij})_{1\le i,\,j\le t}$, we denote it by $\widetilde{H}=(\widetilde{h}_{ij})_{1\le i,\,j\le t}$, where

$$\widetilde{h}_{ij}=\begin{cases} h_{ij} & \text{if } i<j;\\ 0 & \text{otherwise.}\end{cases}$$

Consider quadratic functions $f_i:\mathbb{F}_p^n\to\mathbb{F}_p$ $(1\le i\le K)$ are defined by

$$f_i(\mathbf{x})=\mathbf{v}_iN\mathbf{x}^T+\mathbf{x}\widetilde{M}\mathbf{x}^T,$$

where $\mathbf{x}^T$ stands for the transpose of $\mathbf{x}=(x_1,\cdots,x_n)$.

Then for each partition

$$\{1,2,\cdots,n\}=A\cup B,\quad |A|=d-1,\quad |B|=n-d+1, \tag{4.2}$$

we have

$$f_i(\mathbf{c}_A,\mathbf{x}_B)=\mathbf{v}_iN_A\mathbf{c}_A^T+\mathbf{v}_iN_B\mathbf{x}_B^T+\mathbf{c}_AM_{AB}\mathbf{x}_B^T+\mathbf{c}_A\widetilde{M}_{AA}\mathbf{c}_A^T+\mathbf{x}_B\widetilde{M}_{BB}\mathbf{x}_B^T.$$

Therefore,

$$\begin{aligned} f_i(\mathbf{c}_A, \mathbf{x}_B) - f_j(\mathbf{c'}_A, \mathbf{x}_B) &= \mathbf{v}_i N_A \mathbf{c}_A^T - \mathbf{v}_j N_A \mathbf{c'}_A^T + (\mathbf{v}_i - \mathbf{v}_j) N_B \mathbf{x}_B^T \\ &\quad + (\mathbf{c}_A - \mathbf{c'}_A) M_{AB} \mathbf{x}_B^T + \mathbf{c}_A \widetilde{M}_{AA} \mathbf{c}_A^T - \mathbf{c'}_A \widetilde{M}_{AA} \mathbf{c'}_A^T \\ &= g(\mathbf{c}_A, \mathbf{c'}_A, \mathbf{v}_i, \mathbf{v}_j) + (\mathbf{v}_i - \mathbf{v}_j, \mathbf{c}_A - \mathbf{c'}_A) \begin{pmatrix} N_B \\ M_{AB} \end{pmatrix} \mathbf{x}_B^T, \end{aligned}$$

where

$$g := g(\mathbf{c}_A, \mathbf{c'}_A, \mathbf{v}_i, \mathbf{v}_j) := \mathbf{v}_i N_A \mathbf{c}_A^T - \mathbf{v}_j N_A \mathbf{c'}_A^T + \mathbf{c}_A \widetilde{M}_{AA} \mathbf{c}_A^T - \mathbf{c'}_A \widetilde{M}_{AA} \mathbf{c'}_A^T.$$

If $i = j$ and $\mathbf{c}_A = \mathbf{c'}_A$, then

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \zeta^{f_i(\mathbf{c}_A, \mathbf{c}_B) - f_j(\mathbf{c'}_A, \mathbf{c}_B)} = \sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} 1 = p^{n-d+1}.$$

Otherwise, $\mathbf{u} := (\mathbf{v}_i - \mathbf{v}_j, \mathbf{c}_A - \mathbf{c'}_A) \begin{pmatrix} N_B \\ M_{AB} \end{pmatrix} \neq \mathbf{0} \in \mathbb{F}_p^{n-d+1}$ by assumption. Hence,

$$\sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \zeta^{f_i(\mathbf{c}_A, \mathbf{c}_B) - f_j(\mathbf{c'}_A, \mathbf{c}_B)} = \zeta^g \sum_{\mathbf{c}_B \in \mathbb{F}_p^{n-d+1}} \zeta^{\mathbf{u} \cdot \mathbf{c}_B} = 0.$$

By Theorem 3.2, it follows that there exists a pure quantum $((n, K, d))_p$-code.

If the rank of $\begin{pmatrix} N_B \\ M_{AB} \end{pmatrix}$ is $k + d - 1$ over $\mathbb{F}_p$ for each partition (4.2), then (4.1) implies that $(\mathbf{v}_i - \mathbf{v}_j, \mathbf{c}) = (\mathbf{0}, \mathbf{0})$. Therefore, we can choose $\{\mathbf{v}_1, \cdots, \mathbf{v}_K\} = \mathbb{F}_p^k$ and hence $K = p^k$. This completes the proof of Theorem 4.1. □

Remark 4.2. The last statement in Theorem 4.1 was essentially proved in [11] where quantum $[[5, 1, 3]]_p$-codes for all prime number p were obtained in this way.

At the end of this paper we show two applications of Theorem 4.1.

Theorem 4.3. (i) *If $p > 2$ is a prime, then there exist pure quantum $((n, p^{n-2}, 2))_p$-codes for all $n \geq 2$.*

(ii) *If $p = 2$, then there exist binary pure quantum $((n, K_n, 2))_p$-codes for all $n \geq 4$, where*

$$K_n = \begin{cases} 2^{n-2} & \text{if } n \text{ is even;} \\ 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Proof. Let $k = n-1$. Let $M = (m_{ij})_{1 \leq i,j \leq n}$ be the symmetric matrix with $m_{ij} = 1$ for all $i \neq j$ and $m_{ii} = 0$ for all $i = 1, 2, \cdots, n$ and choose

$$N = \begin{pmatrix} & & 1 \\ & I_{n-1} & \vdots \\ & & 1 \end{pmatrix}.$$

For a partition $\{1, 2, \cdots, n\} = A \cup B$ with $|A| = 1$, $|B| = n - 1$, let $A = \{\lambda\}$ $(1 \leq \lambda \leq n)$. We have

$$M_{AB} = (1, \cdots, 1) \in \mathbb{F}_p^{n-1}$$

and N_λ is the sub-matrix of N obtained by deleting the λ-th column of N, i.e.,

$$N_1 = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ & & & \vdots \\ & I_{n-2} & & 1 \end{pmatrix}, \cdots, N_{n-1} = \begin{pmatrix} & & & 1 \\ & I_{n-2} & & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}, \quad N_n = I_{n-1}. \tag{4.3}$$

It is easy to see that $\det(N_\lambda) = \pm 1$, and hence all matrices N_λ are invertible. In this case, the equality (4.1) of Theorem 4.1 becomes

$$(\mathbf{v}_i - \mathbf{v}_j)N_\lambda = c(1, 1, \cdots, 1) \in \mathbb{F}_p^{n-1}. \tag{4.4}$$

If $c = 0$, then $\mathbf{v}_i = \mathbf{v}_j$ since each N_λ is invertible.

From now on, we assume $0 \neq c \in \mathbb{F}_p$. By combining (4.3) with (4.4), we have that $\mathbf{v}_i - \mathbf{v}_j = c\mathbf{a}_\lambda$ $(1 \leq \lambda \leq n)$, where

$$\mathbf{a}_1 = (3-n, 1, \cdots, 1),\ \mathbf{a}_2 = (1, 3-n, 1, \cdots, 1), \cdots,$$
$$\mathbf{a}_{n-1} = (1, \cdots, 1, 3-n), \mathbf{a}_n = (1, 1, \cdots, 1).$$

In order to get a pure quantum $((n, K, 2))_p$-code from Theorem 4.1, we have to find a subset $S = \{\mathbf{v}_1, \cdots, \mathbf{v}_K\}$ of $\mathbb{F}_p^{n-1}$ satisfying the following condition:

$$(*) \qquad \mathbf{v}_i - \mathbf{v}_j \text{ are not equal to } c\mathbf{a}_\lambda \quad \text{for all } 1 \leq i \neq j \leq K,\ 1 \leq \lambda \leq n.$$

If $n \equiv 2 \pmod{p}$, then $\mathbf{a}_1 = \mathbf{a}_2 = \cdots = \mathbf{a}_n = (1, \cdots, 1) \in \mathbb{F}_p^{n-1}$. Let S be the dual subspace of the 1-dimensional subspace spanned by $\mathbf{1} = (1, \cdots, 1)$ in $\mathbb{F}_p^{n-1}$, i.e.,

$$S = \{\mathbf{c} = (c_1, \cdots, c_{n-1}) \in \mathbb{F}_p^{n-1} :\ \mathbf{c} \cdot \mathbf{1} = c_1 + \cdots + c_{n-1} = 0\}.$$

Since S is a linear subspace of $\mathbb{F}_p^{n-1}$, any difference of two distinct vectors in S belongs to S. However, $\mathbf{a}_\lambda \notin S$ since $\mathbf{a}_\lambda \cdot \mathbf{1} = 1$ $(1 \leq \lambda \leq n)$. Therefore, the set S satisfies the condition $(*)$ and $K = |S| = p^{n-2}$.

If $n \not\equiv 2 \pmod{p}$, then $\mathbf{a}_1, \cdots, \mathbf{a}_{n-1}$ are linearly independent as

$$\det \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_2 \\ \vdots \\ \mathbf{a}_{n-1} \end{pmatrix} = \det \begin{pmatrix} 3-n & & & 1 \\ & & \ddots & \\ & 1 & & 3-n \end{pmatrix} = (2-n)^{n-2} \neq 0 \in \mathbb{F}_p.$$

Therefore, we have an invertible $(n-1) \times (n-1)$ matrix L over $\mathbb{F}_p$ such that $\mathbf{a}_\lambda L = \mathbf{a}'_\lambda$ $(1 \leq \lambda \leq n-1)$, where

$$\mathbf{a}'_1 = (1, 0, \cdots, 0),\ \mathbf{a}'_2 = (0, 1, 0, \cdots, 0), \cdots,\ \mathbf{a}'_{n-1} = (0, \cdots, 0, 1).$$

Hence,

$$\mathbf{a}'_n = \mathbf{a}_n L = (\mathbf{a}_1 + \cdots + \mathbf{a}_{n-1})L = \mathbf{a}'_1 + \cdots + \mathbf{a}'_{n-1} = (1, \cdots, 1).$$

Let $S' = \{\mathbf{v}'_1, \cdots, \mathbf{v}'_K\}$, where $\mathbf{v}'_\lambda = \mathbf{v}_\lambda L$ $(1 \leq \lambda \leq K)$. In order for $\mathbf{v}_i$ to satisfy $(*)$, we have to find S' satisfying the following condition:

$$(*') \qquad \mathbf{v}'_i - \mathbf{v}'_j \text{ are not equal to } c\mathbf{a}'_\lambda \quad \text{for all } 1 \leq i \neq j \leq K,\ 1 \leq \lambda \leq n.$$

For $p \geq 3$, we are able to find $\alpha \in \mathbb{F}_p$ such that $\alpha \neq 0, 2-n$. Let S' be the dual subspace of the 1-dimensional subspace spanned by $\mathbf{b} = (1, \cdots, 1, \alpha)$ in $\mathbb{F}_p^{n-1}$:

$$S' = \{\mathbf{c} = (c_1, \cdots, c_{n-1}) \in \mathbb{F}_p^{n-1} \mid \mathbf{c} \cdot \mathbf{b} = c_1 + \cdots + c_{n-2} + \alpha c_{n-1} = 0 \in \mathbb{F}_p\}.$$

It is easy to check that $\mathbf{a}'_\lambda \notin S'$ $(1 \leq \lambda \leq n)$. This implies that the set S' satisfies the condition $(*)'$. Therefore, the set $S = \{\mathbf{v}L^{-1} \mid \mathbf{v} \in S'\}$ satisfies the condition $(*)$ and $K = |S| = |S'| = p^{n-2}$.

Next we consider the case of $p = 2$ and odd n. In this case,

$$\mathbf{a}_1 = (0, 1, \cdots, 1),\ \mathbf{a}_2 = (1, 0, 1, \cdots, 1),$$
$$\mathbf{a}_{n-1} = (1, 1, \cdots, 1, 0),\ \mathbf{a}_n = (1, 1, \cdots, 1) \in \mathbb{F}_2^{n-1}.$$

As the Hamming weight of $\mathbf{a}_\lambda$ is at least $n-2$ for all $1 \le \lambda \le n$, we want to find a subset S of $\mathbb{F}_2^{n-1}$ such that the Hamming weight $d_H(\mathbf{v}_i - \mathbf{v}_j) \le n-3$ for all distinct vectors $\mathbf{v}_i$ and $\mathbf{v}_j$ in S. Let $0 \le i \le n$ and let S_i be the set of the vectors in $\mathbb{F}_2^{n-1}$ with Hamming weight i. It is easy to see that the set $S = \bigcup_{i=0}^{\frac{n-3}{2}} S_i$ satisfies $(*)$ and

$$K = |S| = \sum_{i=0}^{\frac{n-3}{2}} \binom{n-1}{i} = 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}.$$

This completes the proof. □

Remark 4.4. (i) For even $n \ge 4$, binary quantum $((n, 2^{n-2}, 2))$-codes have been constructed in [2, 9]. For odd length n, a pure binary quantum $((5, 6, 2))$-code was obtained in [10]. This code is optimal in the sense that binary quantum $((5, K, 2))$-codes do not exist for $K \ge 7$. By a simple propagation rule, Rains [9] obtains a family of binary quantum $((n, 3 \cdot 2^{n-4}, 2))$-codes for all odd $n \ge 5$. Our binary quantum $((n, 2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}, 2))$-codes obtained in Theorem 4.3 are better than Rains' result for $2 \nmid n \ge 11$. For instance, we have the binary quantum codes $((11, 386, 2))$ and $((13, 1586, 2))$, while the previous result only indicates the existence of $((11, 384, 2))$ and $((13, 1536, 2))$.

(ii) If $p > 2$, Theorem 4.3 shows that we have pure $((n, p^{n-2}, 2))_p$-codes for all $n \ge 2$. This class of codes achieve the Singleton bound, and hence they are optimal.

(iii) Rains [9] defines an asymptotic quantity

$$K_2 = \lim_{m \to \infty} K_0(2m+1)/2^{2m-2},$$

where $K_0(2m+1)$ denotes the maximal dimension K of binary pure quantum $((2m+1, K, 2))$-codes. By the quantum Singleton bound we know that $K_2 \le 2$. Rains' result gives only $K_2 \ge 3/2$. Now we are able to prove that $K_2 = 2$.

Corollary 4.5. $K_2 = 2$.

Proof. It is sufficient to show that $K_2 \ge 2$. By Theorem 4.3 and Stirling's formula we have

$$\begin{aligned} K_2 &\ge \lim_{2 \nmid n \to 0} 2^{3-n}\left(2^{n-2} - \frac{1}{2}\binom{n-1}{(n-1)/2}\right) = 2 - \lim_{2 \nmid n \to \infty} \binom{n-1}{(n-1)/2}/2^{n-2} \\ &\ge 2 - \lim_{2 \nmid n \to \infty} \frac{2^n}{2^{n-2}\sqrt{\pi n/2}} = 2. \end{aligned}$$

This completes the proof. □

5. Propagation rules

In classical coding theory, through the last few decades many propagation rules, such as direct sum, lengthening, shortening, deleting, subcodes, and $(u|u+v)$-construction, have been proposed. Some of these propagation rules have been realized in quantum coding theory in one way or another (see [2, 9]). It is natural to ask whether these propagation rules in classical coding theory have analogs in quantum coding theory. In this section, we derive some analogous propagation rules for quantum codes based on the characterization of quantum codes in Section

3. Some propagation rules in this section are obvious, while others are not. For instance, some new binary quantum codes and many other best known quantum codes can be obtained from these new propagation rules in this section.

Theorem 5.1. *Suppose there is a p-ary $((n, K, d))$-quantum code Q. Then*

(i) **(subcode)** *there exists a p-ary $((n, K-1, \geq d))$-quantum code Q_1;*
(ii) **(puncturing)** *there exists a p-ary $((n-1, K, \geq d-1))$-quantum code Q_2.*

Furthermore, if Q is pure, then Q_i are pure as well for all $1 \leq i \leq 2$.

Proof. By Theorem 3.1, a p-ary $((n, K-1, d))$-quantum code can be identified with a set $\{\varphi_i\}_{i=1}^{K}$ of non-zero mappings from $\mathbb{F}_p^n$ to $\mathbb{C}$ satisfying condition (3.2).

(i) If we throw φ_K away, then it is easy to verify that the set $\{\varphi_i\}_{i=1}^{K-1}$ gives a p-ary $((n, K-1, \geq d))$-quantum code.

(ii) As φ_i is not identical to zero, there exists an element $\mathbf{a}_i = (a_1^{(i)}, \cdots, a_n^{(i)}) \in \mathbb{F}_p^n$ such that $\varphi_i(\mathbf{a}_i) \neq 0$. Define a new mapping

$$\phi_i : \quad \mathbb{F}_p^{n-1} \to \mathbb{C}; \qquad (x_1, \cdots, x_{n-1}) \mapsto \varphi_i(x_1, \cdots, x_{n-1}, a_n^{(i)})$$

for all $1 \leq i \leq K$. It is clear that every ϕ_i is not identical to zero for all $1 \leq i \leq K$.

Now we have to show that condition (3.2) is satisfied for the set $\{\phi_i\}_{i=1}^{K}$.

For any partition $A_1 \cup B = \{1, \ldots, n-1\}$ with $|A_1| = d-2$, put $A = A_1 \cup \{n\}$. Then we get a partition $A \cup B = \{1, \ldots, n\}$ with $|A| = d-1$. For any $\mathbf{c}_{A_1}, \mathbf{c}'_{A_1} \in \mathbb{F}_p^{d-2}$, let $\mathbf{c}_A = (\mathbf{c}_{A_1}, a_n^{(i)})$ and $\mathbf{c}'_A = (\mathbf{c}'_{A_1}, a_n^{(j)})$. Then by (3.2) we have

(5.1)

$$\sum_{\mathbf{c}_B} \overline{\phi_i(\mathbf{c}_{A_1}, \mathbf{c}_B)} \phi_j(\mathbf{c}_{A_1}, \mathbf{c}_B) = \sum_{\mathbf{c}_B} \overline{\varphi_i(\mathbf{c}_A, \mathbf{c}_B)} \varphi_j(\mathbf{c}'_A, \mathbf{c}_B) = \begin{cases} 0 & i \neq j; \\ f(\mathbf{c}_A, \mathbf{c}'_A) & i = j. \end{cases}$$

If Q is pure, i.e., the set $\{\varphi_i\}_{i=1}^{K}$ satisfies conditions (I) and (II) in Theorem 3.1(ii), then it is easy to check that the sets $\{\varphi_i\}_{i=1}^{K-1}$ and $\{\phi_i\}_{i=1}^{K}$ satisfy conditions (I) and (II) in Theorem 3.1(ii) as well, that is, Q_i are pure for all $1 \leq i \leq 2$. □

Example 5.2. In this example, we can see that some good quantum codes can be obtained by applying the first propagation rule in Theorem 5.1, while the second propagation rule provides some new codes.

(i) By Table III of [2], we know the existence of a binary $((12, 16, 4))$-quantum code. Hence, from the first propagation rule in Theorem 5.1, we get binary $((12, K, 4))$-quantum codes for all $K \leq 16$. By Table III of [2], we know that the $((12, 8, 4))$ and $((12, 4, 4))$-quantum codes are the best in the sense that, given length n and dimension K, the minimum distance is the best among the known ones. One can find many such examples in this way by using Table III of [2].
(ii) By Table III of [2], we know the existence of a binary $((28, 2^8, 6))$-quantum code. Hence, from the second propagation rule in Theorem 5.1, we obtain a binary $((27, 2^8, 5))$-quantum code. This is a new code compared with Table III of [2] as the code of length 27 and dimension 2^8 in Table III of [2] has minimum distance only equal to 4. Furthermore, we can get many best known codes by applying this propagation rule. For instance, a binary $((16, 4, 6))$-quantum code gives rise to a binary $((15, 4, 5))$-quantum code.

Theorem 5.3 (direct sum). *One has a p-ary $((n_1 + n_2, K_1K_2, \min\{d_1, d_2\}))$-quantum code Q if there exist p-ary $((n_i, K_i, d_i))$-quantum codes for $i = 1, 2$. Furthermore, Q is pure if both Q_1 and Q_2 are pure.*

Proof. By Theorem 3.1, assume that $\{\varphi_i\}_{i=1}^{K_1}$ and $\{\phi_i\}_{i=1}^{K_2}$ give p-ary $((n_1, K_1, d_1))$ and $((n_2, K_2, d_2))$-quantum codes, respectively. For each pair (i, j) with $1 \le i \le K_1$ and $1 \le j \le K_2$, define a function

$$\sigma_{ij} : \mathbb{F}_p^{n_1+n_2} \to \mathbb{C}; \qquad (x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2}) \mapsto \varphi_i(x_1, \ldots, x_{n_1})\phi_j(y_1, \ldots, y_{n_2}).$$

Then the set $\{\sigma_{ij}\}_{1\le i\le K_1, 1\le j\le K_2}$ gives rise to the desired quantum code. The details of the proof are omitted here. □

Acknowledgement

The authors are very grateful to the anonymous referee for his/her invaluable suggestions and comments which greatly improved the paper.

References

[1] A. Ashikhmin and E. Knill, Non-binary quantum stabilizer codes, IEEE Trans. IT-47 (2001), 3065-3072. MR1872869 (2003a:94045)
[2] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. IT-44 (1998), 1369-1387. MR1665774 (99m:94063)
[3] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A, 54 (1996), 1098-1105.
[4] E. Knill, Non-binary unitary error bases and quantum codes, Aug., 1996, quant-ph/9608048.
[5] E. Knill, Group representations, error bases and quantum codes, Aug., 1996, quant-ph/9608049.
[6] E. Knill and R. Laflamme, A theory of quantum error correcting codes, Phys. Rev. A, 55 (1997), 900-911. MR1455854 (98j:81039)
[7] R. Matsumoto and T. Uyematsu, Constructing quantum error-correcting codes for p^m-state systems from classical error-correcting codes, IEICE Trans. Fundamentals, E83-A(10) (2000), 1878-1883.
[8] E. M. Rains, Non-binary quantum codes, IEEE Trans. IT-45 (1999), 1827-1832. MR1720636 (2000h:94044)
[9] E. M. Rains, Quantum codes of minimal distance two, IEEE Trans. IT-45 (1999), 266-271. MR1677865 (2000e:94071)
[10] E. M. Rains, R. H. Hardin, P. W. Shor and N. J. A. Sloane, A nonadditive quantum code, Phys. Rev. Lett., 79 (1997), 953-954.
[11] D. Schlingemann and R. F. Werner, Quantum error-correcting codes associated with graphs, Phys. Rev. A, 65 (2002).
[12] P. W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A, 52 (1995).
[13] A. M. Steane, Simple quantum error correcting codes, Phys. Rev. Lett., 77 (1996), 793-797. MR1398854 (97d:81030)
[14] A. M. Steane, Multiple particle interference and quantum error correction, Proc. Roy. Soc. London A, 452 (1996), 2551-2577. MR1421749 (98h:81016)

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, People's Republic of China

E-mail address: kfeng@math.tsinghua.edu.cn

Division of Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore