國立交通大學

應用數學系

碩士論文

量子編碼的數學性質與建構

Mathematical Properties and Construction of Quantum Codes

研 究 生 ：蔡睿翊

指導教授 ：翁志文 教授

中華民國一百零三年七月

量子編碼的數學性質與建構

Mathematical Properties and Construction of Quantum Codes

研究生 ： 蔡睿翊　　Student ： Jui-Yi, Tsai

指導教授 ： 翁志文　　Advisor ： Chih-Wen Weng

國立交通大學

應用數學系

碩士論文

A Thesis
Submitted to Department of Applied Mathematics
College of Science
National Chiao Tung University
in Partial Fulfillment of Requirements
for the Degree of Master
in Applied Mathematics
July 2014
Hsinchu, Taiwan, Republic of China

中華民國一百零三年七月

量子糾錯碼的數學性質與建構

研究生：蔡睿翊　　　　指導教授：翁志文 教授

國立交通大學

應用數學系

摘要

本論文以傳統糾錯碼的觀點來看量子糾錯碼。我們亦將介紹文獻中所提及之量子糾錯碼的構造與刻劃，最後給出一種與圖有關的量子糾錯碼的建構方法，其擴充文獻中排除二元情形的方法，能適用所有情形。

關鍵詞：量子糾錯碼、圖。

Mathematical Properties and Construction of Quantum Codes

Student：Jui-Yi, Tsai Advisor：Dr. Chih-Wen Weng

Department of Applied Mathematics

National Chiao Tung University

Hsinchu 300, Taiwan, R.O.C.

Abstract

This thesis introduces about the quantum error correcting codes in the viewpoint of classical error correcting codes. We also introduce some construction and characterization of quantum error correcting codes. Thereafter, we give a construction of quantum error correcting codes associated with graphs, which generalizes a previous result that excludes the binary case so that it is valid for all cases.

Keywords: quantum error correcting codes, graph.

誌　謝

首先，非常感謝指導教授翁志文老師，對我在學習及研究的方法與態度上有很多指引與指正，這對我在研究上有相當大的幫助。也很感謝家人在這兩年間對我的關懷與督促，讓我即使在外地不致偏離該走的路，遇上困難時也不致感到灰心喪志。

感謝系上師長 (翁志文老師、康明軒老師、楊一帆老師等) 的教導，讓我有機會接觸到更加高深的代數與組合學的知識；感謝系辦職員的協助，讓我們有非常好的學習環境；感謝人社系段馨君老師的鼓勵及分享，使我能找到自己可以努力下去的方向；感謝系上各位同學 (特別是黃于哲、黃建順兩位同研究室的同學的分享與建議、組合數學組的許博喻、林凡軒、楊凱帆、余冠儒等同學們在課業方面及 LaTeX 等方面的協助) 及學長姊 (特別是林易萱、李光祥、鄭硯仁、蔡志奇這四位學長，他們分別在我的課業、研究、助教工作及生活各方面上幫了我很多忙)、學弟妹們還有友聲合唱團團員們的陪伴與扶持，使我這兩年間的學校生活增添了許多色彩；也感謝真耶穌教會新竹教會及關東橋教會的傳道、長執、同靈們及大清交團契、新竹高級班給予我的勉勵及代禱，使我在這兩年間得到心靈上的成長，也使我有堅持下去的動力。

最後，最感謝的，就是主耶穌。若非祢一路帶領，我想就沒有今天的我了。謹此表示對在這兩年間遇到的所有師長，朋友的感謝。願一切榮耀歸於天上的真神！

睿翊　謹誌于新竹交大
2014 年 7 月 24 日

Contents

Chapter 1

Introduction

Quantum communication like quantum coding theory and quantum cryptography has been developed in the recent decades. This is a great improvement in communication theory. Its concepts are based on quantum mechanics, but we will not mention anything about quantum mechanics in this thesis. We will give the strict mathematical definition of quantum error correcting codes based on [3]. The results from [6] and [7] will be introduced. Thereafter, we give a construction of quantum error correcting codes associated with graphs, which generalizes a previous result in [7] that excludes the binary case so that it is valid for all cases.

The thesis is organized as follows: Chapter 2 introduces the notations which will be used in this thesis. To compare the similarities and differences between classical error correcting codes and quantum error correcting codes, chapter 3 recalls the definitions and propositions of classical error correcting codes; those of quantum error correcting codes will also be introduced in parallel. Chapter 4 introduces a method to characterize quantum error correcting codes by logic functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ introduced in [6]. Chapter 5 introduces about the construction of quantum error correcting codes using the graph-theoretical method introduced in [7], in which only non-binary quantum codes are discussed. Thus we will generalize the result in [7].

Chapter 2

Preliminaries

In this section, we will introduce the notations which will be used in this thesis. Throughout the thesis, let $\mathbb{F}_p = \{0, 1, \cdots, p-1\}$ be the finite field of p elements. Sometimes we also treat an element $i \in \mathbb{F}_p$ as its corresponding integer. Let ω be the p-th primitive root of unity. Let $A = (a_{i,j})$ be an $m \times n$ matrix and B an $s \times t$ matrix. Then the **Kronecker tensor product** $A \otimes B$ of A and B is defined by the following $ms \times nt$ matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Note that $(A \otimes B)(C \otimes D) = AC \otimes BD$ for matrices A, B, C, D of suitable sizes. The n-th **Kronecker tensor power** of a vector space V over a field F is defined by

$$V^{\otimes n} := \operatorname{span}\{\mathfrak{v}_1 \otimes \mathfrak{v}_2 \otimes \cdots \otimes \mathfrak{v}_n | \mathfrak{v}_i \in V\}.$$

The **Hermitian inner product** of complex vectors $\mathfrak{u} = (u_1, \cdots, u_n)^T, \mathfrak{v} = (v_1, \cdots, v_n)^T$ is defined by

$$\langle \mathfrak{u}, \mathfrak{v} \rangle := \sum_{i=1}^{n} \overline{u_i} v_i,$$

where $\bar{\ }$ stands for complex conjugation. In the the last two sections, we will frequently use the block notations of matrices. Therefore we should introduce the following notation of a matrix M and a column vector $\mathbf{u}$:

$$M = \begin{array}{c c} & \begin{array}{cc} \Delta_1 & \Delta_2 \end{array} \\ \begin{array}{c} \Delta_1 \\ \Delta_2 \end{array} & \begin{pmatrix} M[\Delta_1|\Delta_1] & M[\Delta_1|\Delta_2] \\ M[\Delta_2|\Delta_1] & M[\Delta_2|\Delta_2] \end{pmatrix} \end{array}, \mathbf{u} = \begin{pmatrix} \mathbf{u}[\Delta_1] \\ \mathbf{u}[\Delta_2] \end{pmatrix},$$

where $M[\Delta_1|\Delta_2]$ means the sub-matrix of M with rows indexed by elements in Δ_1 and the columns by elements in Δ_2, and $\mathbf{u}[\Delta_1]$ means the sub-column vector with entries are indexed by Δ_1.

Chapter 3

Comparison between Classical and Quantum Error Correcting Codes

In this chapter, we are going to recall the definitions and propositions of classical error correcting codes and introduce those of quantum error correcting codes to compare the similarities and differences between them.

3.1 Basic Definitions and Structures of Classical Codes and Quantum Codes

The classical (linear) codes are vector spaces over finite fields; whereas the quantum codes are vector spaces over the complex number field $\mathbb{C}$.

Definition 3.1. A **classical (linear)** $[n,k]_p$**-code** (or a classical $(n,K)_p$**-code**, where $K = p^k = |C|$) is a k-dimensional subspace C of $\mathbb{F}_p^n$.

Definition 3.2. A **quantum** $[[n,k]]_p$**-code** (or a **quantum** $((n,K))_p$**-code**, where $k = log_pK$) is a K-dimensional subspace Q of $(\mathbb{C}^p)^{\otimes n}$.

Remark 3.3. Error-correcting coding theory depends on what basis of a vector space is chosen.

(i) Classical coding theory:

$$\{e_i = (0,\cdots,0,1,0,\cdots,0)^T \in \mathbb{F}_p^n \mid 1 \leq i \leq n\},$$

where 1 appears in the i-th position.

(ii) Quantum coding theory:

$$\{e_{i_1+1} \otimes \cdots \otimes e_{i_n+1} \mid i_j \in \{0, 1, \ldots, p-1\}\}.$$

It is a convention in Quantum coding theory (Dirac notation) to write $|i\rangle$ for e_{i+1} and $|i_1 i_2 \cdots i_n\rangle$ for $e_{i_1+1} \otimes e_{i_2+1} \cdots \otimes e_{i_n+1}$.

3.2 Error Detection and Correction of Classical Codes and Quantum Codes

An error can occur when passing a message, so we have to correct it to the right one. Here we introduce the error detection and correction of classical codes and quantum codes in an algebraic point of view.

An error in classical codes is simply a vector over a finite field, and the codewords is interrupted by an error under addition.

Definition 3.4. An **error** is a nonzero vector $\mathbf{e}$ independent to C.

The quantum codewords may be interrupted by the errors under matrix multiplication. Here is the definition of the errors in quantum codes.

Definition 3.5. (i) For $a, b \in \mathbb{F}_p$, define two linear operators $X(a)$ and $Z(b)$ on $\mathbb{C}^p$ by

$$X(a)|x\rangle = |x + a\rangle, Z(b)|x\rangle = \omega^{b \cdot x}|x\rangle,$$

where $x \in \mathbb{F}_p$. Then $X(a)$ is called a **bit error**; $Z(b)$ is called a **phase error**.

(ii) For $\mathbf{a} = (a_1, \cdots, a_n)^T, \mathbf{b} = (b_1, \cdots, b_n)^T \in \mathbb{F}_p^n$,

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

(iii) $\mathcal{E}_n := \{\omega^t X(\mathbf{a})Z(\mathbf{b}) | 0 \leq t \leq p-1, \mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n\}$ is called the **quantum error group**.

An element of $\mathbf{E} \in \mathcal{E}_n$ is called an **error** of quantum code. Note that $\mathbf{E}|\mathbf{u}\rangle = \omega^{t+\mathbf{b}\cdot\mathbf{u}}|\mathbf{u}+\mathbf{a}\rangle$ for $\mathbf{u} \in \mathbb{F}_p^n$ and $\mathbf{E} = \omega^t X(\mathbf{a})Z(\mathbf{b})$. In fact, from the previous definition, we have the following proposition.

Proposition 3.6. *The following (i)-(ii) holds.*

(i) With respect to the basis $\{|0\rangle, |1\rangle, \cdots, |p-1\rangle\}$, the operator $X(1)$ is a cyclic matrix, and the operator $Z(1)$ is a diagonal matrix as follows.

$$X(1) = \begin{pmatrix} 0 & & & & 1 \\ 1 & 0 & & & \\ & 1 & \ddots & & \\ & & \ddots & 0 & \\ 0 & & & 1 & 0 \end{pmatrix}, \qquad Z(1) = \begin{pmatrix} 1 & & & & 0 \\ & \omega & & & \\ & & \omega^2 & & \\ & & & \ddots & \\ 0 & & & & \omega^{p-1} \end{pmatrix}.$$

(ii) $X(a) = X(1)^a$, $Z(b) = Z(1)^b$, $\overline{X(a)}^T = X(-a) = X(a)^{-1}$, $\overline{Z(b)}^T = Z(-b) = Z(b)^{-1}$, and $Z(b)X(a) = \omega^{-b\cdot a}X(a)Z(b)$ for all $a, b \in \mathbb{F}_p$.

Moreover, $\mathcal{E}_n$ is a group of order p^{2n+1}. □

Here we compare the Hamming weight with the quantum weight.

Definition 3.7. (i) The **Hamming weight** $\mathrm{wt}_H(\mathbf{e})$ of an element $\mathbf{e} \in \mathbb{F}_p^n$ is the number of nonzero entries in $\mathbf{e}$. The **Hamming distance** of $\mathbf{u}, \mathbf{v} \in \mathbb{F}_p^n$ is defined by $d(\mathbf{u}, \mathbf{v}) := \mathrm{wt}_H(\mathbf{u} - \mathbf{v})$. Note that the Hamming distance is a metric (i.e. its value is always nonnegative, and it satisfies the symmetry and the triangle inequality).

(ii) The **quantum weight** $\mathrm{wt}_Q(\mathbf{E})$ of an element $\mathbf{E} = \omega^t X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{E}_n$ is the number of nonzero pairs (a_i, b_i) in the two vectors $\mathbf{a}$, $\mathbf{b} \in \mathbb{F}_p^n$.

For classical codes, the Hamming distance is used to describe the ability of error detection and correction. As for quantum codes, we use the Hermitian inner products of quantum codewords in a quantum code Q. The orthogonality is usually used to describe the ability of error detection and correction.

Definition 3.8. For two quantum codewords $\mathfrak{u}, \mathfrak{v} \in Q$. Then

(i) If $\mathfrak{u} = \gamma\mathfrak{v}$ for some nonzero $\gamma \in \mathbb{C}$, then we say $\mathfrak{u}, \mathfrak{v}$ are **totally indistinguishable**.

(ii) If $\langle \mathfrak{u}, \mathfrak{v} \rangle = 0$, then we say $\mathfrak{u}, \mathfrak{v}$ are **totally distinguishable** in Q.

Here is the comparison between the definitions of error detection of classical codes and of quantum codes.

Definition 3.9. C can **detect** an error $\mathbf{e}$ if $d(\mathbf{u}, \mathbf{v} + \mathbf{e}) > 0$ for distinct $\mathbf{u}, \mathbf{v} \in C$.

Definition 3.10. For a quantum $((n, K))_p$-code Q with $K \geq 2$ and an error $\mathbf{E} \in \mathcal{E}_n$, Q can **detect** an error $\mathbf{E}$ if $\mathfrak{u}, \mathfrak{v}$ are totally distinguishable implies that $\mathfrak{u}, \mathbf{E}\mathfrak{v}$ are totally distinguishable.

Note that 3.10 is equivalent to $\langle \mathfrak{u}, \mathbf{E}\mathfrak{v} \rangle = \lambda_{\mathbf{E}} \langle \mathfrak{u}, \mathfrak{v} \rangle$, where $\lambda_{\mathbf{E}} \in \mathbb{C}$ depends only on $\mathbf{E}$ but is independent of $\mathfrak{u}, \mathfrak{v}$.

Here is the comparison between the definitions of error correction of classical codes and of quantum codes.

Definition 3.11. C can **correct** an error $\mathbf{e}$ if $d(\mathbf{v}, \mathbf{v} + \mathbf{e}) < d(\mathbf{w}, \mathbf{v} + \mathbf{e})$ for all distinct $\mathbf{v}, \mathbf{w} \in C$.

Definition 3.12. For a quantum $((n, K))_p$-code Q, where $K \geq 2$. Q can **correct** errors of weight at most t if, for any totally distinguishable $\mathfrak{u}, \mathfrak{v} \in Q$ and any errors $\mathbf{E}_1, \mathbf{E}_2 \in \mathcal{E}_n$ with $\mathrm{wt}_Q(\mathbf{E}_1), \mathrm{wt}_Q(\mathbf{E}_2) \leq t$, $\mathbf{E}_1\mathfrak{u}, \mathbf{E}_2\mathfrak{v}$ are totally distinguishable; in other words, $\langle \mathbf{E}_1\mathfrak{u}, \mathbf{E}_2\mathfrak{v} \rangle = 0$.

Here is the comparison between the definitions of minimum distance of classical codes and of quantum codes.

Definition 3.13. The **minimum distance** of C with $|C| \geq 2$ is at least d if C can detect errors of Hamming weight at most $d - 1$; in other words, $0 < \mathrm{wt}_H(\mathbf{e}) < d$ implies that $d(\mathbf{u}, \mathbf{e} + \mathbf{v}) > 0$ for distinct $\mathbf{u}, \mathbf{v} \in C$.

Note that the previous definition is equivalent to the common one; that is,

$$d = \min\{d(\mathbf{u}, \mathbf{v}) | \mathbf{u}, \mathbf{v} \in C \text{ are distinct.}\}.$$

This can be verified by the triangle inequality of Hamming distance.

Definition 3.14. A quantum $((n, K))_p$-code Q with $K \geq 2$ has **minimum distance** at least d if Q can detect errors of quantum weight at most $d-1$; in other words, $\langle \mathfrak{u}, \mathfrak{v} \rangle = 0$ implies $\langle \mathfrak{u}, \mathbf{E}\mathfrak{v} \rangle = 0$ for any error $\mathbf{E} \in \mathcal{E}_n$ with $\mathrm{wt}_Q(\mathbf{E}) \leq d-1$.

Note that the definitions of the minimum distance of classical codes and quantum codes are similar because the minimum distance d is given by the detection of classical errors of Hamming weight $d-1$ in classical case and the detection of quantum errors of quantum weight $d-1$ in the quantum case.

Here is a special property often used in quantum codes.

Definition 3.15. A quantum code Q is a d**-pure** code if for any $\mathfrak{u}, \mathfrak{v} \in Q$ and any errors $\mathbf{E} \in \mathcal{E}_n$ with $0 < \mathrm{wt}_Q(\mathbf{E}) < d$, $\mathfrak{u}, \mathbf{E}\mathfrak{v}$ are totally distinguishable; in other words, $\langle \mathfrak{u}, \mathbf{E}\mathfrak{v} \rangle = 0$.

This property can help us to distinguish a codeword from another one interrupted by an error of quantum weight less than d.

Remark 3.16. (i) A (quantum or classical) code has **minimum distance** exactly d if it has minimum distance at least d, but does not have minimum distance at least $d+1$.

(ii) From definition 3.14, a quantum $((n, K))_p$-code Q (or a quantum $[[n, k]]_p$-code) is an $((n, K, \geq d))_p$-quantum code (or an $[[n, k, \geq d]]_p$-quantum code) for some $d \geq 1$ means a p^k-dimensional (or K-dimensional) quantum code in $(\mathbb{C}^p)^{\otimes n}$ with minimum distance at least d; if Q has minimum distance exactly d, then Q is a quantum $((n, K, d))_p$-code (or a quantum $[[n, k, d]]_p$-code).

From definitions 3.14 and 3.15, we have the following propositions:

Proposition 3.17. *A d-pure quantum $((n, K))_p$-code Q with $K \geq 2$ has minimum distance $\geq d$.*

Proof. Suppose $\mathbf{E} \in \mathcal{E}_n$ with $\mathrm{wt}_Q(\mathbf{E}) \leq d-1$. Let $\mathfrak{c}_1, \mathfrak{c}_2 \in Q$ be codewords with $\langle \mathfrak{c}_1, \mathfrak{c}_2 \rangle = 0$. Now if $\mathbf{E} = \omega^k I$, then $\mathrm{wt}_Q(e) = 0$. Thus $\langle \mathfrak{c}_1, \mathbf{E}\mathfrak{c}_2 \rangle = \omega^k \langle \mathfrak{c}_1, \mathfrak{c}_2 \rangle = 0$. If $\mathrm{wt}_Q(\mathbf{E}) \neq 0$, then $1 \leq \mathrm{wt}_Q(\mathbf{E}) \leq d-1$, and so $\langle \mathfrak{c}_1, \mathbf{E}\mathfrak{c}_2 \rangle = 0$ by definition 3.14. □

Note that, by definition 3.15, for $K = 1$ (i.e. $k = 0$), Q is a d-pure quantum $((n, 1, d))_p$-code (or a d-pure quantum $[[n, 0, d]]_p$-code) since any two vectors in $\{\mathbf{E}\mathfrak{c} | \mathbf{E} \in \mathcal{E}_n, 0 \leq \mathrm{wt}_Q(\mathbf{E}) \leq d-1\}$ are orthogonal, where $\mathfrak{c}$ is the non-zero vector that spans Q.

Here is the comparison between the abilities of error correction of classical codes and of quantum codes.

Theorem 3.18. *An $[n, k, d]_p$-code C can correct errors of weight at most $\lfloor \frac{d-1}{2} \rfloor$.*

Proof. Let $\mathbf{e}$ be an error of weight at most $\lfloor \frac{d-1}{2} \rfloor$. From the triangle inequality, we have

$$d(\mathbf{w}, \mathbf{v}+\mathbf{e}) \geq d(\mathbf{w}, \mathbf{v}) - d(\mathbf{v}, \mathbf{v}+\mathbf{e}) \geq d - \left\lfloor \frac{d-1}{2} \right\rfloor \geq \left\lceil \frac{d-1}{2} \right\rceil > d(\mathbf{v}, \mathbf{v}+\mathbf{e}).$$

(The inequality $d(\mathbf{w}, \mathbf{v}) \geq d$ comes from the definition of minimum distance; the other one $\mathrm{wt}_H(\mathbf{e}) = d(\mathbf{v}, \mathbf{v}+\mathbf{e}) \leq \lfloor \frac{d-1}{2} \rfloor$ is from the hypothesis.) □

Theorem 3.19. *If Q is an quantum $((n, K, d))_p$-code with $K \geq 2$, then Q can correct errors of weight at most $\lfloor \frac{d-1}{2} \rfloor$.*

Proof. Let $\mathbf{E}_1, \mathbf{E}_2 \in \mathcal{E}_n$ with $\mathrm{wt}_Q(\mathbf{E}_1), \mathrm{wt}_Q(\mathbf{E}_2) \leq \lfloor \frac{d-1}{2} \rfloor$. It is clear that $\mathrm{wt}_Q(\mathbf{E}_1\mathbf{E}_2) \leq \mathrm{wt}_Q(\mathbf{E}_1) + \mathrm{wt}_Q(\mathbf{E}_2) \leq d-1$. Since Q has minimum distance d, Q can detect $\mathbf{E}_1\mathbf{E}_2$; that is, for any totally distinguishable $\mathfrak{c}_1, \mathfrak{c}_2 \in Q$, we have $\langle \mathfrak{c}_1, \mathbf{E}_1\mathbf{E}_2\mathfrak{c}_2 \rangle = 0$, completing the proof. □

3.3 Bounds in Classical Codes and Quantum codes

In classical and quantum coding theory, the parameters (n, K, d) or (n, k, d) determine the efficiency of communication (k/n) and the ability of error correction(d), but there are some restrictions called the **Hamming bound** and the **Singleton bound**, causing that we can not obtain both high efficiency of communication and good ability of error correction. For the proofs, please see [3] in detail.

Theorem 3.20. *(classical Hamming bound) If C is an $(n, K, d)_p$ code, then*

$$p^n \geq K \cdot \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} (p-1)^i \binom{n}{i}. \tag{3.1}$$

Theorem 3.21. *(classical Singleton bound) If C is an $(n, K, d)_p$ code, then*

$$K \leq p^{n-d+1}. \tag{3.2}$$

Theorem 3.22. *(quantum Hamming bound) If Q is a d-pure quantum $((n, K, d))_p$-code, then*

$$p^n \geq K \cdot \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} (p^2-1)^i \binom{n}{i}. \tag{3.3}$$

Theorem 3.23. *(quantum Singleton bound) If Q is a quantum $((n, K, d))_p$-code, then*

$$K \leq p^{n-2d+2}. \tag{3.4}$$

3.4 Some Simple Lemmas

In this section, we provide some simple lemmas, which will be used many times in the thesis.

Lemma 3.24. *Let p be a prime and ω the p-th root of unity. Then $\sum_{\mathbf{u} \in \mathbb{F}_p^n} \omega^{\mathbf{u} \cdot \mathbf{v}} = 0$ for all non-zero vectors $\mathbf{v} \in \mathbb{F}_p^n$.*

Proof. For $\mathbf{u} = (u_1, \cdots, u_n) \in \mathbb{F}_p^n$ and $\mathbf{v} = (v_1, \cdots, v_n) \in \mathbb{F}_p^n \setminus \{\mathbf{0}\}$, we have

$$\sum_{\mathbf{u}\in\mathbb{F}_p^n} \omega^{\mathbf{u}\cdot\mathbf{v}} = \sum_{(u_1,\cdots,u_n)\in\mathbb{F}_p^n} \omega^{u_1v_1+\cdots+u_nv_n} = \sum_{(u_1,\cdots,u_n)\in\mathbb{F}_p^n} \omega^{u_1v_1}\cdots\omega^{u_nv_n}$$

$$= \left(\sum_{u_1\in\mathbb{F}_p} \omega^{u_1v_1}\right)\cdots\left(\sum_{u_n\in\mathbb{F}_p} \omega^{u_nv_n}\right)$$

For $\mathbf{v} \neq 0$, there is some $v_i \neq 0$, which is certainly an inverse of some other element in $\mathbb{F}_p$. Thus $v_i\mathbb{F}_p = \mathbb{F}_p$, and so $\sum_{u_i\in\mathbb{F}_p} \omega^{u_iv_i} = 0$ (because $1+\omega+\cdots+\omega^{p-1} = 0$). □

Lemma 3.25. *Let p be a prime, ω a p-th primitive root of unity and $V_p = (\omega^{ij})_{i,j\in\mathbb{F}_p}$ a $p \times p$ Vandermonde matrix of the form*

$$V_p = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{p-1} & \cdots & \omega^{(p-1)^2} \end{pmatrix}.$$

Then V_p is invertible with $V_p^{-1} = (1/p)\overline{V_p}$, and so the Kronecker tensor product $V_p \otimes V_p \otimes \cdots \otimes V_p$ of m V_p's is invertible.

Proof. (i) By lemma 3.24, we have

$$(V_p\overline{V_p})_{i,j} = \sum_{k=0}^{p-1} \omega^{ik}\omega^{-kj} = \sum_{k=0}^{p-1} \omega^{k(i-j)} = \begin{cases} 0, & \text{if } i \neq j \\ p, & \text{if } i = j. \end{cases}$$

Thus V_p is invertible with $V_p^{-1} = (1/p)\overline{V_p}$.

(ii) By the multiplication rule of the Kronecker tensor product, we have

$$\begin{aligned} &(V_p \otimes V_p \otimes \cdots \otimes V_p)(V_p^{-1} \otimes V_p^{-1} \otimes \cdots \otimes V_p^{-1}) \\ =&(V_pV_p^{-1}) \otimes (V_pV_p^{-1}) \otimes \cdots \otimes (V_pV_p^{-1}) \\ =&I_p \otimes I_p \otimes \cdots \otimes I_p = I_{p^m}, \end{aligned}$$

and so $(V_p \otimes V_p \otimes \cdots \otimes V_p)^{-1} = V_p^{-1} \otimes V_p^{-1} \otimes \cdots \otimes V_p^{-1}$, completing the proof.

□

Chapter 4

The Characterization of Quantum Codes Using Logic Functions

In this chapter, we introduce a characterization of quantum codes using logic functions introduced in [5] and [6] (for logic functions, see [1] and [2]).

Throughout this section, let Q be a K-dimensional quantum code of $(\mathbb{C}^p)^{\otimes n}$ with an orthonormal basis $\{\mathfrak{v}_i = \sum_{\mathbf{u}\in\mathbb{F}_p^n} v_i(\mathbf{u})|\mathbf{u}\rangle | 1 \leq i \leq K\}$, where $v_i : \mathbb{F}_p^n \to \mathbb{C}, 1 \leq i \leq K$ are functions.

Theorem 4.1. *Assume $K \geq 2$. Then Q is a quantum $((n, K, \geq d))_p$-code if and only if for any subset $E \subseteq \{1, 2, \cdots, n\}$ with $|E| = d - 1, d \geq 2, E^c = \{1, 2, \cdots, n\} \setminus E, |E^c| = n - d + 1$ and $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_p^{d-1}, 1 \leq i, j \leq K$, we have*

$$\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = \begin{cases} 0, & \text{if } i \neq j \\ \eta(\mathbf{w}, \mathbf{w}'), & \text{if } i = j, \end{cases} \tag{4.1}$$

where the sum is indeed over $\mathbf{u}, \mathbf{u}' \in \mathbb{F}_p^n$ with $\mathbf{u}[E^c] = \mathbf{u}'[E^c]$ and $\mathbf{u}[E] = \mathbf{w}, \mathbf{u}'[E] = \mathbf{w}'$, and $\eta(\mathbf{w}, \mathbf{w}') \in \mathbb{C}$ is a constant independent of i (depends on $\mathbf{w}, \mathbf{w}'$).

Proof. " $\Rightarrow$ " : Let $\mathbf{E} = X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{E}_n$ be an error of quantum weight at most $d - 1$, where $\mathbf{a}$ satisfies $\mathbf{a}[E] = \mathbf{w} - \mathbf{w}'$, $\mathbf{a}[E^c] = 0$, and $\mathbf{b} \in \mathbb{F}_p^n$ is a vector of $d - 1$ variables satisfying $\mathbf{b}[E^c] = 0$. Then by definition 3.10,

$$\lambda_{\mathbf{E}} \delta_{ij} = \langle \mathfrak{v}_i, \mathbf{E}\mathfrak{v}_j \rangle = \sum_{\mathbf{x}\in\mathbb{F}_p^{d-1}} \omega^{\mathbf{b}[E]\cdot\mathbf{x}'} \sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}'), \tag{4.2}$$

where $\delta_{ij} = 0$ if $i \neq j$; $\delta_{ij} = 1$ otherwise, $\lambda_{\mathbf{E}}$ depends only on $\mathbf{E}$ and is independent of i, j, and the second sum is indeed over $\mathbf{u}, \mathbf{u}' \in \mathbb{F}_p^n$ with $\mathbf{u}[E^c] = \mathbf{u}'[E^c]$ and $\mathbf{u}[E] = \mathbf{x}, \mathbf{u}'[E] = \mathbf{x} - \mathbf{a}[E]$. In matrix form, (4.2) becomes

$$\Omega \mathbf{y} = \begin{cases} \mathbf{0}, & \text{if } i \neq j \\ \lambda_{\mathbf{E}}(1, 1, \cdots, 1)^T, & \text{if } i = j, \end{cases},$$

where Ω is an $p^{d-1} \times p^{d-1}$ matrix indexed by $\mathbb{F}_p^{d-1}$ with $\mathbf{b}[E], \mathbf{x}'$-entry $\omega^{\mathbf{b}[E] \cdot \mathbf{x}'}$, and

$$\mathbf{y} = \sum_{\mathbf{u}[E^c] = \mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') \qquad \text{(being indexed depending on } \mathbf{x}')$$

is a $(d-1)$-dimensional column vector over $\mathbb{F}_p$. Since the matrix Ω is invertible by lemma 3.25, we find the column vector

$$\mathbf{y} = \begin{cases} \mathbf{0}, & \text{if } i \neq j \\ \lambda_{\mathbf{E}} \Omega^{-1}(1, 1, \cdots, 1)^T, & \text{if } i = j, \end{cases}.$$

Hence the result follows by considering the $\mathbf{x} = \mathbf{w}$ entry of vector $\mathbf{y}$.

" $\Leftarrow$ " : To show that Q has minimum distance at least d, let $\mathbf{E} = \omega^t X(\mathbf{a}) Z(\mathbf{b}) \in \mathcal{E}_n$ be an error of quantum weight at most $d - 1$. Without loss of generality, we can assume $t = 0$. Choose E such that $|E| = d - 1$ and $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n$ satisfy $(\mathbf{a}[E^c], \mathbf{b}[E^c]) = (\mathbf{0}, \mathbf{0})$. Pick two totally distinguishable codewords $\mathfrak{v} = \sum_{i=1}^K \alpha_i \mathfrak{v}_i, \mathfrak{w} = \sum_{j=1}^K \beta_j \mathfrak{v}_j \in Q$. Note that

$$\mathbf{E}\mathfrak{w} = \sum_{j=1}^K \beta_j e \mathfrak{v}_j = \sum_{j=1}^K \beta_j \sum_{\mathbf{u}' \in \mathbb{F}_p^n} v_j(\mathbf{u}') e |\mathbf{u}'\rangle = \sum_{j=1}^K \beta_j \sum_{\mathbf{u}' \in \mathbb{F}_p^n} v_j(\mathbf{u}') \omega^{\mathbf{b} \cdot \mathbf{u}'} |\mathbf{u}' + \mathbf{a}\rangle.$$

Thus for $\mathbf{u}[E] = \mathbf{x}, \mathbf{u}'[E] = \mathbf{x} - \mathbf{a}[E]$, we have

$$\begin{aligned} \langle \mathfrak{v}, \mathbf{E}\mathfrak{w} \rangle &= \sum_{i,j=1}^K \overline{\alpha_i} \beta_j \sum_{\mathbf{u} = \mathbf{u}' + \mathbf{a}} \omega^{\mathbf{b} \cdot \mathbf{u}'} v_i(\mathbf{u}) v_j(\mathbf{u}') \\ &= \sum_{i,j=1}^K \overline{\alpha_i} \beta_j \sum_{\mathbf{x} \in \mathbb{F}_p^{d-1}} \omega^{\mathbf{b}[E] \cdot (\mathbf{x} - \mathbf{a}[E])} \sum_{\mathbf{u}[E^c] = \mathbf{u}'[E^c]} v_i(\mathbf{u}) v_j(\mathbf{u}') \\ &= \sum_{i=1}^K \overline{\alpha_i} \beta_i \sum_{\mathbf{x} \in \mathbb{F}_p^{d-1}} \omega^{\mathbf{b}[E] \cdot (\mathbf{x} - \mathbf{a}[E])} \sum_{\mathbf{u}[E^c] = \mathbf{u}'[E^c]} v_i(\mathbf{u}) v_i(\mathbf{u}') \\ &= \sum_{\mathbf{x} \in \mathbb{F}_p^{d-1}} \eta(\mathbf{x}, \mathbf{x} - \mathbf{a}[E]) \omega^{\mathbf{b}[E] \cdot (\mathbf{x} - \mathbf{a}[E])} \langle \mathfrak{v}, \mathfrak{w} \rangle = 0 \end{aligned}$$

(The last equality is obtained by the condition: when $i \neq j$, $\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = 0$; when $i = j$, $\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_i(\mathbf{u}') = \eta(\mathbf{x}, \mathbf{x} - \mathbf{a}[E])$, which is independent to i), completing the proof. □

Theorem 4.2. *Let $K \geq 1$. Then Q is a pure quantum $((n, K, \geq d))_p$-code if and only if for any subset $E \subseteq \{1, 2, \cdots, n\}$ with $|E| = d - 1, d \geq 2, E^c = \{1, 2, \cdots, n\} \setminus E, |E^c| = n - d + 1$ and $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_p^{d-1}$, we have*

$$\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = \begin{cases} 0, & \textit{if } \mathbf{w} \neq \mathbf{w}' \\ \delta_{i,j} p^{1-d}, & \textit{if } \mathbf{w} = \mathbf{w}', \end{cases} \tag{4.3}$$

where the sum is indeed over $\mathbf{u}, \mathbf{u}' \in \mathbb{F}_p^n$ with $\mathbf{u}[E^c] = \mathbf{u}'[E^c]$, and $\mathbf{u}[E] = \mathbf{w}, \mathbf{u}'[E] = \mathbf{w}' \in \mathbb{F}_p^{d-1}$.

Proof. " $\Rightarrow$ " : Let a set E of cardinality $d - 1$ and $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_p^{d-1}$ be given. Choose $\mathbf{E} = X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{E}_n$ be an error of quantum weight at most $d - 1$, where $\mathbf{a}$ satisfies $\mathbf{a}[E] = \mathbf{w} - \mathbf{w}'$, $\mathbf{a}[E^c] = 0$, and $\mathbf{b} \in \mathbb{F}_p^n$ is any vector satisfying $\mathbf{b}[E^c] = 0$. Since Q is a pure $((n, K, d))_p$-quantum code, for all $1 \leq i, j \leq K$,

$$\delta_{\mathrm{wt}_Q(\mathbf{E}),0} = \langle \mathfrak{v}_i, e\mathfrak{v}_j \rangle = \sum_{\mathbf{x}'=\mathbf{x}-\mathbf{a}[E]} \omega^{\mathbf{b}[E]\cdot\mathbf{x}'} \sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}'). \tag{4.4}$$

Note that

$$\sum_{\mathbf{x}\in\mathbb{F}_p^{d-1}} \sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = \sum_{\mathbf{u}\in\mathbb{F}_p^n} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}) = \delta_{i,j}.$$

In matrix form, (4.4) becomes

$$\Omega\mathbf{y} = \begin{cases} (\delta_{i,j}, 0, 0, \cdots, 0)^T, & \text{if } \mathbf{w} = \mathbf{w}'(\mathbf{a}[E] = \mathbf{0}); \\ (0, 0, 0, \cdots, 0)^T, & \text{if } \mathbf{w} \neq \mathbf{w}'(\mathbf{a}[E] \neq \mathbf{0}), \end{cases}$$

where Ω and $\mathbf{y}$ are as described in the proof of theorem 4.1. Note that the first column of Ω^{-1} is $p^{1-d}(1, 1, \cdots, 1)^T$. Thus

$$\mathbf{y} = \begin{cases} \delta_{i,j} p^{1-d}(1, 1, \cdots, 1)^T, & \text{if } \mathbf{w} = \mathbf{w}'(\mathbf{a}[E] = \mathbf{0}); \\ (0, 0, 0, \cdots, 0)^T, & \text{if } \mathbf{w} \neq \mathbf{w}'(\mathbf{a}[E] \neq \mathbf{0}), \end{cases}$$

proving the necessary condition.

" $\Leftarrow$ " : To show that Q is d-pure, let $\mathbf{E} = \omega^t X(\mathbf{a})Z(\mathbf{b}) \in \mathcal{E}_n$ with $1 \leq \mathrm{wt}_Q(\mathbb{E}) \leq d-1$. Without loss of generality, we can assume $t = 0$. Choose $E = \{i | 1 \leq i \leq n, (a_i, b_i) \neq (0,0)\}$ so that $|E| = d-1$, $(\mathbf{a}[E], \mathbf{b}[E]) \neq (\mathbf{0}, \mathbf{0})$ and $(\mathbf{a}[E^c], \mathbf{b}[E]^c) = (\mathbf{0}, \mathbf{0})$ for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_p^n$. Pick two codewords $\mathfrak{v} = \sum_{i=1}^K \alpha_i \mathfrak{v}_i, \mathfrak{w} = \sum_{j=1}^K \beta_j \mathfrak{v}_j \in Q$. Then for $\mathbf{u}[E] = \mathbf{x}, \mathbf{u}'[E] = \mathbf{x} - \mathbf{a}[E]$, we have

$$\begin{aligned}
\langle \mathfrak{v}, \mathbf{E}\mathfrak{w} \rangle &= \sum_{i,j=1}^{K} \overline{\alpha_i}\beta_j \sum_{\mathbf{u}=\mathbf{u}'+\mathbf{a}} \omega^{\mathbf{b}\cdot\mathbf{u}'} v_i(\mathbf{u}) v_j(\mathbf{u}') \\
&= \sum_{i,j=1}^{K} \overline{\alpha_i}\beta_j \sum_{\mathbf{x}\in\mathbb{F}_p^{d-1}} \omega^{\mathbf{b}[E]\cdot(\mathbf{x}-\mathbf{a}[E])} \sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} v_i(\mathbf{u}) v_j(\mathbf{u}') \\
&= \begin{cases} \sum_{i,j=1}^{K} \delta_{i,j} p^{1-d} \overline{\alpha_i}\beta_j \sum_{\mathbf{x}\in\mathbb{F}_p^{d-1}} \omega^{\mathbf{b}[E]\cdot\mathbf{x}} = 0, & \text{if } \mathbf{a}[E] = \mathbf{0} \\ 0, & \text{if } \mathbf{a}[E] \neq \mathbf{0} \end{cases}
\end{aligned}$$

(The last equality is obtained by the second condition: when $\mathbf{a}[E] \neq \mathbf{0}$,

$$\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = 0;$$

when $\mathbf{a}[E] = \mathbf{0}$, $\mathbf{b}[E] \neq \mathbf{0}$ and

$$\sum_{\mathbf{u}[E^c]=\mathbf{u}'[E^c]} \overline{v_i(\mathbf{u})} v_j(\mathbf{u}') = \delta_{i,j} p^{1-d}),$$

completing the proof. □

In fact, the functions $v_i : \mathbb{F}_p^n \to \mathbb{C}$ can be obtained simply by $v_i(\mathbf{u}) = \omega^{f_i(\mathbf{u})}$, where $1 \leq i \leq K$ and $\mathbf{u} \in \mathbb{F}_p^n$ and f_i are functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ so that the functions $v_i(\mathbf{u}) = \omega^{f_i(\mathbf{u})}$ satisfy the conditions (4.1) and (4.3) in the previous theorems (see [6]). Hence these functions can be used to construct (pure) quantum codes. Such function is called a **logic function** (for $p = 2$, a **Boolean function**).

Chapter 5

Graph-theoretical Method

In this chapter, we will discuss about a method to construct quantum error correcting codes introduced by Schlingemann and Werner in [7], in which only the case for the odd primes is discussed, therefore we are going to improve the method by applying $v_i(\mathbf{u}) = \omega^{\mathbf{u}_i^T B\mathbf{w}+\mathbf{w}^T A\mathbf{w}}$ for $\mathbf{u}_i \in \mathbb{F}_p^k$ $(1 \leq i \leq K)$ to theorem 4.2 so that it is valid for all primes.

Throughout this section, we assume the following hypotheses: Let p be a prime and ω the p-th primitive root of unity. Let X, Y be sets with cardinality $|X| = k$ and $|Y| = n$. Let $d \geq 2$ and (n, k, d) satisfy the quantum Singleton bound $n \geq k + 2(d-1)$. Let A be an $n \times n$ matrix with rows and columns indexed by Y, B an $k \times n$ matrix with rows indexed by X and columns indexed by Y. Define a linear function $f : (\mathbb{C}^p)^{\otimes k} \to (\mathbb{C}^p)^{\otimes n}$ by

$$f(|\mathbf{u}\rangle) = \sum_{\mathbf{w} \in \mathbb{F}_p^n} \omega^{\mathbf{u}^T B\mathbf{w}+\mathbf{w}^T A\mathbf{w}} |\mathbf{w}\rangle \tag{5.1}$$

for $\mathbf{u} = (x_1, x_2, \cdots, x_k)^T \in \mathbb{F}_p^k$. Let $Q = f((\mathbb{C}^p)^{\otimes k})$, the image of f. Here we will use the function (5.1)to reprove the result in [7] in three steps.

In step 1, we shall give a definition and prove two lemmas, which give a necessary condition and a sufficient condition of quantum pairs, respectively:

Definition 5.1. The pair (A, B) is an $[[n, k, d]]_p$-**quantum pair** if for any $E \subseteq Y$

with $|E| = d-1$, $\mathbf{u} \in \mathbb{F}_p^k$ and $\mathbf{e} \in \mathbb{F}_p^{d-1}$, the following implication holds:

$$\mathbf{u}^T B[X|E^c] - \mathbf{e}^T (A + A^T)[E|E^c] = \mathbf{0} \Rightarrow \mathbf{u} = \mathbf{0} \text{ and } B[X|E]\mathbf{e} = \mathbf{0}, \tag{5.2}$$

where $E^c = Y \setminus E$.

First we prove the necessary condition:

Lemma 5.2. *If (A, B) is an $[[n, k, d]]_p$-quantum pair, then the sub-matrix $B[X|E^c]$ of B has rank k over $\mathbb{F}_p$, and the intersection of row space of $B[X|E^c]$ and $(A + A^T)[E|E^c]$ is the zero space for any $(d-1)$-subset E of Y.*

Proof. Taking $\mathbf{e} = 0$ in (5.2), we find that $B[X|E^c]$ has rank k. Suppose $\mathbf{u}^T B[X|E^c] = \mathbf{e}^T (A + A^T)[E|E^c]$ is a vector in the intersection of row spaces of $B[X|E^c]$ and $(A + A^T)[E|E^c]$. Then $\mathbf{u} = \mathbf{0}$ by (5.2). Hence the vector $\mathbf{u}^T B[X|E^c] = \mathbf{0}$. □

Now we prove the sufficient condition:

Lemma 5.3. *If the sub-matrix $B[X|E^c]$ of B has rank k over $\mathbb{F}_p$, the sub-matrix $(A + A^T)[E|E^c]$ of $A + A^T$ has rank $d-1$ over $\mathbb{F}_p$ and the intersection of row spaces of $B[X|E^c]$ and $(A + A^T)[E|E^c]$ is the zero space for any $(d-1)$-subset E of Y, then (A, B) is an $[[n, k, d]]_p$-quantum pair.*

Proof. Suppose that $\mathbf{u}^T B[X|E^c] - \mathbf{e}^T (A + A^T)[E|E^c] = \mathbf{0}$. Then $\mathbf{u}^T B[X|E^c] = \mathbf{e}^T (A + A^T)[E|E^c] = \mathbf{0}$ since it is in the intersection of row spaces of $B[X|E^c]$ and $(A + A^T)[E|E^c]$. Since $\operatorname{rank}(B[X|E^c]) = k$, the row vectors of $B[X|E^c]$ are linearly independent, thus $\mathbf{u} = \mathbf{0}$. And $\operatorname{rank}((A + A^T)[E|E^c]) = d-1$ implies that $\mathbf{e} = \mathbf{0}$ by similar argument. □

We shall call such a pair (A, B) in lemma 5.3 a **pure $[[n, k, d]]_p$-quantum pair**. In step 2, we shall prove

Theorem 5.4. *For any $\mathfrak{v}, \mathfrak{v}' \in \mathbb{C}^{\otimes k}$, if (A, B) is an $[[n, k, d]]_p$-quantum pair, then $\langle f(\mathfrak{v}')|f(\mathfrak{v})\rangle = p^n \langle \mathfrak{v}'|\mathfrak{v}\rangle$. In other words, f preserves orthogonality. In particular, $Q = f((\mathbb{C}^p)^{\otimes k})$ has dimension p^k.*

Proof. Let

$$\begin{aligned}\mathfrak{v} &= \sum_{\mathbf{u}\in\mathbb{F}_p^k} v(\mathbf{u})|\mathbf{u}]\rangle \in \mathbb{C}^{|\otimes k},\\ \mathfrak{v}' &= \sum_{\mathbf{u}'\in\mathbb{F}_p^k} v'(\mathbf{u}')|\mathbf{u}'\rangle \in \mathbb{C}^{|\otimes k},\end{aligned}$$

where $v(\mathbf{u}), v'(\mathbf{u}') \in \mathbb{C}$. Then

$$\begin{aligned}\mathfrak{w} =& f(\mathfrak{v}) = \sum_{\mathbf{u}\in\mathbb{F}_p^k}\sum_{\mathbf{w}\in\mathbb{F}_p^n} v(\mathbf{u})\omega^{\mathbf{u}^T B\mathbf{w}+\mathbf{w}^T A\mathbf{w}}|\mathbf{w}\rangle,\\ \mathfrak{w}' =& f(\mathfrak{v}') = \sum_{\mathbf{u}'\in\mathbb{F}_p^k}\sum_{\mathbf{w}\in\mathbb{F}_p^n} v'(\mathbf{u}')\omega^{\mathbf{u}'^T B\mathbf{w}'+\mathbf{w}'^T A\mathbf{w}'}|\mathbf{w}'\rangle.\end{aligned}$$

Now, we can compute the Hermitian inner product:

$$\langle\mathfrak{w}', \mathfrak{w}\rangle = \sum_{\mathbf{u},\mathbf{u}'}\left[\overline{v'(\mathbf{u}')}v(\mathbf{u})\left(\sum_{\mathbf{w}=\mathbf{w}'}\omega^t\right)\right],$$

where

$$t = (\mathbf{u}-\mathbf{u}')^T B\mathbf{w}.$$

Since (A, B) is an $[[n, k, d]]_p$-quantum pair, $\mathrm{rank} B[X|E^c] = k$. Hence, by lemma 3.24, we have

$$\sum_{\mathbf{w}}\omega^{(\mathbf{u}-\mathbf{u}')^T B\mathbf{w}} = \begin{cases} p^n, & \text{if } \mathbf{u}=\mathbf{u}',\\ 0, & \text{otherwise.}\end{cases}$$

This follows that

$$\langle\mathfrak{w}', \mathfrak{w}\rangle = p^n\sum_{\mathbf{u}=\mathbf{u}'}\overline{v'(\mathbf{u}')}v(\mathbf{u}) = p^n\langle\mathfrak{v}', \mathfrak{v}\rangle.$$

Hence f preserves the orthogonality, and so f maps the basis of $(\mathbb{C}^p)^{\otimes k}$ to that of $(\mathbb{C}^p)^{\otimes n}$. Hence f is 1-1, which means the image of f has dimension p^k. □

In step 3, we shall prove

Theorem 5.5. *If (A, B) is an $[[n, k, d]]_p$-quantum pair, then $Q = f((\mathbb{C}^p)^{\otimes k})$ has minimum distance at least d.*

Proof. Let

$$\begin{aligned}\mathfrak{w} =& f(\mathfrak{v}) = \sum_{\mathbf{u}\in\mathbb{F}_p^k}\sum_{\mathbf{w}\in\mathbb{F}_p^n} v(\mathbf{u})\omega^{\mathbf{u}^TB\mathbf{w}+\mathbf{w}^TA\mathbf{w}}|\mathbf{w}\rangle \in Q,\\ \mathfrak{w}' =& f(\mathfrak{v}') = \sum_{\mathbf{u}'\in\mathbb{F}_p^k}\sum_{\mathbf{w}'\in\mathbb{F}_p^n} v'(\mathbf{u}')\omega^{\mathbf{u}'^TB\mathbf{w}'+\mathbf{w}'^TA\mathbf{w}'}|\mathbf{w}'\rangle \in Q.\end{aligned}$$

be totally distinguishable (hence $\mathfrak{v}', \mathfrak{v}$ are totally distinguishable). For any $\mathbf{E} = X(\mathbf{l})Z(\mathbf{s}) \in \mathcal{E}_n$ with $\mathrm{wt}_Q(\mathbf{E}) \leq d-1$, we have $\mathbf{E}|\mathbf{w}[E], \mathbf{w}[E^c]\rangle = \omega^{\mathbf{s}[E]\cdot\mathbf{w}[E]}|\mathbf{w}[E] + \mathbf{l}[E], \mathbf{w}[E^c]\rangle$ for all $(d-1)$-subset E of Y and $\mathbf{s}, \mathbf{l} \in \mathbb{F}_p^n$ with $\mathbf{s}[E^c] = \mathbf{l}[E^c] = \mathbf{0}$. It follows that

$$\begin{aligned}\mathbf{E}\mathfrak{w} &= \sum_{\mathbf{u}\in\mathbb{F}_p^k}\sum_{\mathbf{w}\in\mathbb{F}_p^n} v(\mathbf{u})\omega^{\mathbf{u}^TB\mathbf{w}+\mathbf{w}^TA\mathbf{w}}e|\mathbf{w}\rangle\\ &= \sum_{\mathbf{u}\in\mathbb{F}_p^k}\sum_{\mathbf{w}[E],\mathbf{w}[E^c]} v(\mathbf{u})\omega^{\mathbf{s}[E]\cdot\mathbf{w}[E]+\mathbf{u}^TB(\mathbf{w},\mathbf{w}[E^c])+(\mathbf{w}[E],\mathbf{w}[E^c])^TA(\mathbf{w}[E],\mathbf{w}[E^c])}|\mathbf{w}[E]+\mathbf{l}[E],\mathbf{w}[E^c]\rangle,\end{aligned}$$

and so

$$\langle\mathfrak{w}', \mathbf{E}\mathfrak{w}\rangle = \sum_{\mathbf{u},\mathbf{u}'\in\mathbb{F}_p^k}\sum_{\mathbf{w}'=\mathbf{w}+\mathbf{l}} \omega^r\overline{v'(\mathbf{u}')}v(\mathbf{u}),$$

where

$$\begin{aligned}
r =& \mathbf{s}[E]\cdot\mathbf{w}[E] + \mathbf{u}^T B[X|E]\mathbf{w}[E] - \mathbf{u}^T B[X|E]\mathbf{l}[E] + \mathbf{u}^T B[X|E^c]\mathbf{w}[E^c] \\
& + \mathbf{w}[E]^T A[E|E]\mathbf{w}[E] - \mathbf{l}[E]^T A[E|E]\mathbf{w}[E] - \mathbf{w}[E]^T A[E|E]\mathbf{l}[E] - \mathbf{l}[E]^T A[E|E]\mathbf{l}[E] \\
& + \mathbf{w}[E^c]^T A[E^c|E]\mathbf{w}[E] - \mathbf{w}[E^c]^T A[E^c|E]\mathbf{l}[E] \\
& + \mathbf{w}[E]^T A[E|E^c]\mathbf{w}[E^c] - \mathbf{l}[E]^T A[E|E^c]\mathbf{w}[E^c] \\
& + \mathbf{w}[E^c]^T A[E^c|E^c]\mathbf{w}[E^c] - \mathbf{u}'^T B[X|E]\mathbf{w}'[E] - \mathbf{u}'^T B[X|E^c]\mathbf{w}'[E^c] \\
& - \mathbf{w}'[E]^T A[E|E]\mathbf{w}'[E] - \mathbf{w}'[E]^T A[E|E^c]\mathbf{w}'[E^c] \\
& - \mathbf{w}'[E^c]^T A[E^c|E]\mathbf{w}'[E] - \mathbf{w}'[E^c]^T A[E^c|E^c]\mathbf{w}'[E^c] \\
=& \mathbf{s}[E]\cdot\mathbf{w}[E] + (\mathbf{u}-\mathbf{u}')^T B[X|E]\mathbf{w}[E] + (\mathbf{u}-\mathbf{u}')^T B[X|E^c]\mathbf{w}[E^c] \\
& - \mathbf{u}^T B[X|E]\mathbf{l}[E] - \mathbf{l}[E]^T A[E|E]\mathbf{l}[E] - \mathbf{l}[E]^T A[E|E]\mathbf{w}[E] - \mathbf{w}[E]^T A[E|E]\mathbf{l}[E] \\
& - \mathbf{l}[E]^T A[E|E^c]\mathbf{w}[E^c] - \mathbf{w}[E^c]^T A[E^c|E]\mathbf{l}[E] \\
=& \mathbf{s}[E]\cdot\mathbf{w}[E] + (\mathbf{u}-\mathbf{u}')^T B[X|E]\mathbf{w}[E] + (\mathbf{u}-\mathbf{u}')^T B[X|E^c]\mathbf{w}[E^c] \\
& - \mathbf{u}^T B[X|E]\mathbf{l}[E] - \mathbf{l}[E]^T A[E|E]\mathbf{l}[E] \\
& - \mathbf{l}[E]^T (A + A^T)[E|E]\mathbf{w}[E] - \mathbf{l}[E]^T (A + A^T)[E|E^c]\mathbf{w}[E^c]
\end{aligned}$$

(because $\mathbf{w}' = \mathbf{w} + \mathbf{l}$ in the summation.). Then by the definition of quantum pairs and the previous lemmas, we can simplify the inner product $\langle \mathfrak{w}', \mathbf{E}\mathfrak{w} \rangle$ as follows:

$$\begin{aligned}
\langle \mathfrak{w}', \mathbf{E}\mathfrak{w} \rangle &= \sum_{\mathbf{u},\mathbf{u}' \in \mathbb{F}_p^k} \sum_{\mathbf{w}=\mathbf{w}'} \omega^r \overline{v'(\mathbf{u}')} v(\mathbf{u}) \\
&= \omega^{-\mathbf{l}[E]^T A[E|E]\mathbf{l}[E]} \sum_{\mathbf{u},\mathbf{u}'} \overline{v'(\mathbf{u}')} v(\mathbf{u}) \\
&\cdot \left[\sum_{\mathbf{w}[E]} \omega^{\mathbf{s}[E]\cdot\mathbf{w}[E] + (\mathbf{u}-\mathbf{u}')^T B[X|E]\mathbf{w}[E] - \mathbf{l}[E]^T (A+A^T)[E|E]\mathbf{w}[E] - \mathbf{u}^T B[X|E]\mathbf{l}[E]} \right] \\
&\cdot \left[\sum_{\mathbf{w}[E^c]} \omega^{(\mathbf{u}-\mathbf{u}')^T B[X|E^c]\mathbf{w}[E^c] - \mathbf{l}[E]^T (A+A^T)[E|E^c]\mathbf{w}[E^c]} \right] \\
&= p^{n-d+1} \omega^{-\mathbf{l}[E]^T A[E|E]\mathbf{l}[E]} \sum_{\mathbf{u},\mathbf{u}'} \overline{v'(\mathbf{u}')} v(\mathbf{u}) \cdot \left[\sum_{\mathbf{w}[E]} \omega^{(\mathbf{s}[\mathbf{E}] - \mathbf{l}[E]^T (A+A^T)[E|E])\mathbf{w}[E]} \right] \\
&= p^{n-d+1} \omega^{-\mathbf{l}[E]^T A[E|E]\mathbf{l}[E]} \left[\sum_{\mathbf{w}[E]} \omega^{(\mathbf{s}[E] - \mathbf{l}[E]^T (A+A^T)[E|E])\mathbf{w}[E]} \right] \langle \mathfrak{v}', \mathfrak{v} \rangle = 0.
\end{aligned}$$

□

The result of theorems 5.4 and 5.5 shows that if (A, B) is an $[[n, k, d]]_p$-quantum pair, then Q is a quantum $[[n, k, d]]_p$-code. Below we quote Theorem 4.1 and 4.2 to prove a stronger result, which was given in [6].

Theorem 5.6. *If (A, B) is a pure $[[n, k, d]]_p$-quantum pair, then Q is a pure quantum $[[n, k, \geq d]]_p$-code.*

Proof. Order the vectors in $\mathbb{F}_p^k$ as $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{p^k}$, and define functions $v_i : \mathbb{F}_p^n \to \mathbb{C}$ by

$$v_i(\mathbf{w}) = \frac{1}{\sqrt{p^n}} \omega^{\mathbf{u}_i^T B\mathbf{w} + \mathbf{w}^T A\mathbf{w}}$$

for $\mathbf{w} \in \mathbb{F}_p^n$. Then by Theorem 5.4, Q has the following orthonormal basis

$$\left\{ \mathfrak{v}_i = \sum_{\mathbf{w} \in \mathbb{F}_p^n} v_i(\mathbf{w}) |\mathbf{w}\rangle | 1 \leq i \leq p^k \right\}.$$

By theorem 4.2, it suffices to show that

$$\frac{1}{p^n} \sum_{\mathbf{w}[E^c]=\mathbf{w}'[E^c]} \overline{\omega^{\mathbf{u}_i^T B\mathbf{w} + \mathbf{w}^T A\mathbf{w}}} \omega^{\mathbf{u_j}^T B\mathbf{w}' + \mathbf{w}'^T A\mathbf{w}'} = \begin{cases} 0, & \mathbf{w}'[E] \neq \mathbf{w}[E] \\ \delta_{i,j} p^{1-d}, & \mathbf{w}'[E] = \mathbf{w}[E], \end{cases}$$

where the sum is over $\mathbf{w}, \mathbf{w}' \in \mathbb{F}_p^n$ such that with $\mathbf{w}[E^c] = \mathbf{w}'[E^c]$, and the two prefixed parts $\mathbf{w}[E]$ and $\mathbf{w}'[E]$ of E. This follows by the following computation

$$
\begin{aligned}
&\overline{v_i(\mathbf{w})}v_j(\mathbf{w}') \\
=&\omega^{\mathbf{u_j}^T B\mathbf{w}' + \mathbf{w}'^T A\mathbf{w}' - (\mathbf{u_i}^T B\mathbf{w} + \mathbf{w}^T A\mathbf{w})} \\
=&\omega^{\mathbf{u}_j^T B(\mathbf{w}'[E],\mathbf{w}[E^c]) - \mathbf{u}_i^T B(\mathbf{w}[E],\mathbf{w}[E^c]) + (\mathbf{w}'[E],\mathbf{w}[E^c])^T A(\mathbf{w}'[E],\mathbf{w}[E^c]) - (\mathbf{w}[E],\mathbf{w}[E^c])^T A(\mathbf{w}[E],\mathbf{w}[E^c])} \\
=&\omega^{\mathbf{u}_j^T B[X|E]\mathbf{w}'[E] - \mathbf{u}_i^T B[X|E]\mathbf{w}[E] + \mathbf{w}'[E]^T A[E|E]\mathbf{w}'[E] - \mathbf{w}[E]^T A[E|E]\mathbf{w}[E]} \\
&\cdot \omega^{\{(\mathbf{u}_j - \mathbf{u}_i)^T B[X|E^c] + (\mathbf{w}'[E] - \mathbf{w}[E])^T (A + A^T)[E|E^c]\}\mathbf{w}[E^c]}.
\end{aligned}
$$

Now we take the part related to E^c, and we have

$$\sum_{\mathbf{w}[E^c]} \omega^{\{(\mathbf{u}_j - \mathbf{u}_i)^T B[X|E^c] + (\mathbf{w}'[E] - \mathbf{w}[E])^T (A + A^T)[E|E^c]\}\mathbf{w}[E^c]}.$$

Since (A, B) is a pure $[[n, k, d]]_p$-quantum pair, then (5.2) implies that $\mathbf{u}_i = \mathbf{u}_j$, $\mathbf{w}'[E] = \mathbf{w}[E]$ and the summation becomes p^{n-d+1}. Otherwise, the summation becomes 0 by lemma 3.24 again, completing the proof. □

Actually, the previous result also shows that, by defining $f_i : \mathbb{F}_p^n \to \mathbb{F}_p$ by $f_i(\mathbf{x}) = \mathbf{u}_i^T B\mathbf{x} + \mathbf{x}^T A\mathbf{x}$ for $\mathbf{u}_i \in \mathbb{F}_p^k (1 \leq i \leq p^k)$, we can obtain an $[[n, k, d]]_p$-quantum code $Q = \text{span}\{\sum_{\mathbf{x}\in\mathbb{F}_p^n} \omega^{f_i(\mathbf{x})}|\mathbf{x}\rangle | 1 \leq i \leq p^k\}$ (see [6]). Now, let R be the $(k + n) \times (k + n)$ matrix with rows and columns indexed by $(X \cup Y)$ of the form

$$R = \begin{pmatrix} 0 & B \\ B^T & A + A^T \end{pmatrix}. \tag{5.3}$$

Then lemma 5.3 is equivalent to that the sub-matrix

$$R[X \cup E|E^c] = \begin{pmatrix} B[X|E^c] \\ (A + A^T)[E|E^c] \end{pmatrix}$$

of R has rank $k + d - 1$ for any $E \subseteq Y$ with $|E| = d - 1$. Hence we have the following corollaries from the previous theorem. The corollaries are used for MDS quantum codes (i.e. the codes reaching Singleton bound).

Corollary 5.7. *Suppose $n = k + 2(d - 1)$, and the square $(k + d - 1) \times (k + d - 1)$ sub-matrix $R[X \cup E|E^c]$ is invertible for any $E \subseteq Y$ with $|E| = d - 1$. Then Q is a pure quantum $[[n, k, d]]_p$-code.*

Proof. By Lemma 5.3 and Theorem 5.6, Q is a pure quantum $[[n,k,t]]_p$-code for some $t \geq d$. By using quantum Singleton bound and the assumption, we have $n-2d+2=k \leq n-2t+2$, so $t=d$. $\square$

Here we give examples for the applications of theorems 5.4 and 5.5 and corollary 5.7.

Example 5.8. Let $X=\{x_0\}, Y=\{y_0,y_1,y_2,y_3,y_4\}$ and E a 2-subset of Y. Consider the graph G_1 with vertex set $V(G_1)=X\cup Y$ as below:

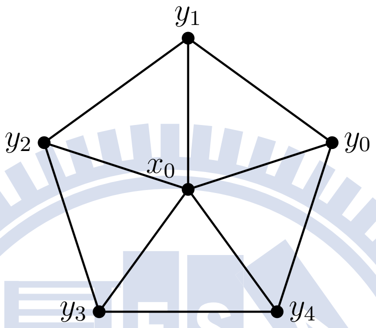

Figure 1. G_1

Then its adjacency matrix is

$$R = \begin{array}{c} \\ x_0 \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array} \begin{array}{c} \begin{array}{cccccc} x_0 & y_0 & y_1 & y_2 & y_3 & y_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} \end{array},$$

which is of the form (5.3) with

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Then we can check that

$$f(|a\rangle) = \sum_{\mathbf{w}\in\mathbb{F}_p^5} \omega^{a(1,1,1,1,1)\cdot\mathbf{w}+\mathbf{w}^TA\mathbf{w}}|\mathbf{w}\rangle = \sum_{\mathbf{w}\in\mathbb{F}_p^5} \omega^{a\sum_{i=1}^5 u_i+\prod_{i(\mathrm{mod}\ 5)} u_iu_{i+1}}|\mathbf{w}\rangle,$$

where $a = 0, 1, 2, \cdots, p-1$, form a basis of $Q = f((\mathbb{C}^p)^{\otimes 1})$, and $\dim Q = p$ by the orthogonality. Also, we check that for any subset E of Y with $|E| = 2$ and $|E^c| = 3$ the sub-matrix $R[X \cup E|E^c]$ is invertible. According the the edge relation between $X \cup E$ and E^c, there are only two situations of $R[X \cup E|E^c]$:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

both of which have determinant 1. Hence we can construct a pure quantum $[[5,1,3]]_p$-code $Q = \mathrm{span}\{\sum_{\mathbf{x}\in\mathbb{F}_p^5} \omega^{(i,i,i,i,i)\cdot\mathbf{x}+\mathbf{x}^TA\mathbf{x}}|\mathbf{x}\rangle | 0 \le i \le 4, i \in \mathbb{F}_p\}$ explicitly.

Here is an example from [1]. We interpret it with the graph-theoretical method.

Example 5.9. Let $X = \phi, Y = \{y_0, y_1, y_2, y_3, y_4, y_5\}$ and G'_1 be the graph with vertex set $V(G'_1) = Y$ as below.

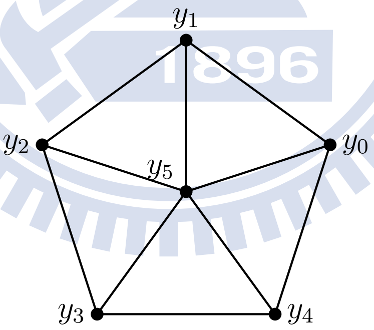

Figure 2. G'_1

Then consider its adjacency matrix

$$R = A + A^T = \begin{array}{c} \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{array} \begin{array}{c} \begin{array}{cccccc} y_0 & y_1 & y_2 & y_3 & y_4 & y_5 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array},$$

with

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

For any $E \subseteq Y$ with $|E| = 3$, we have $\operatorname{rank}(R[E|E^c]) = 3$ since the row vectors of $R[E|E^c]$ are never linearly dependent for any choice of E. Hence we can construct a pure quantum $[[6, 0, 4]]_2$-code

$$Q = \operatorname{span}\{\sum_{\mathbf{x} \in \mathbb{F}_2^6} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle\},$$

where

$$f(\mathbf{x}) = \mathbf{x}^T A \mathbf{x} = x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_0 + x_5(x_0 + x_1 + x_2 + x_3 + x_4).$$

Example 5.10. [4] For $(n, k, d) = (6, 2, 3)$, we can not construct binary($p = 2$) quantum code this way, because these parameters violates Hamming bound when $p = 2$. However, we can use this method to construct non-binary quantum codes with these parameters as follows: Let $(n, k, d) = (6, 2, 3), p = 3$ and consider the graph G_2 with vertex set $V(G_2) = X \cup Y$, where $X = \{x_0, x_1\}, Y = \{y_0, y_1, y_2, y_3, y_4, y_5\}$ and the solid edge has weight 1 and the dashed ones has weight -1 as below:

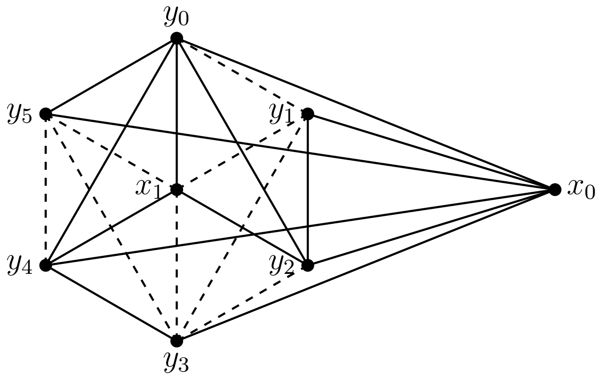

Figure 3. G_2

Then its weighted adjacency matrix is

$$R = \begin{pmatrix} 0 & B \\ B^T & A+A^T \end{pmatrix} = \begin{array}{c} \\ x_0 \\ x_1 \\ y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \end{array} \!\!\begin{array}{c} \begin{array}{cccccccc} x_0 & x_1 & y_0 & y_1 & y_2 & y_3 & y_4 & y_5 \end{array} \\ \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 0 & -1 & 1 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & 1 & -1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & -1 & 0 \\ 1 & -1 & 0 & -1 & 1 & 0 & -1 & -1 \\ 1 & 1 & 1 & 0 & -1 & -1 & 0 & -1 \\ 1 & -1 & 1 & 0 & 0 & -1 & -1 & 0 \end{pmatrix} \end{array},$$

which is in the form (5.3) with

$$A = \begin{pmatrix} 0 & -1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 \end{pmatrix}.$$

For any $E = \{y_i, y_j\}(0 \le i \ne j \le 5)$, it is clear that $\operatorname{rank}(B[X|E^c]) = 2$. The column space of $(A+A^T)[E|E^c]$ is spanned by $\{(1,0)^T, (0,1)^T\}$. So $\operatorname{rank}((A+A^T)[E|E^c]) = 2$. In addition, the intersection of their row spaces contains only the zero vector, we can conclude that (A, B) is a pure $[[6,2,3]]_p$-quantum pair for $p = 3$. Hence

$Q = \mathrm{span}\{\sum_{\mathbf{x}\in\mathbb{F}_3^6} \omega^{\mathbf{u}_i^T B\mathbf{x}+\mathbf{x}^T A\mathbf{x}}|\mathbf{x}\rangle | 1 \leq i \leq 9, \mathbf{u}_i \in \mathbb{F}_3^2\}$ is a pure quantum $[[6,2,3]]_3$-code. As for the verification of the case $p \geq 5$, please see [4].

Bibliography

[1] Zhong Shu-Qin, Ma Zhi, Xu Ya-Jie. Constructing Quantum Error Correcting Code via Logic Function. *Sci China Inf Sci*, 2010, 53: 515-523, doi: 10.1007/s11432-010-0060-6

[2] Xu Ya-Jie, Ma Zhi, Zhang Chun-Yuan, Lu Xin. Logic Functions and Quantum Error Correcting Codes, preprint, 2007.

[3] Ke-Qin, Feng. *Quantum Error Correcting Codes* // Coding Theory and Cryptography. edited by Niederreiter H. Lecture Notes Series. Institute for Mathematical Sciences. National University of Singapore. Singapore: World Scientific, 2002: 91-142.

[4] Ke-Qin, Feng. Quantum Codes $[[6,2,3]]_p$ and $[[7,3,3]]_p$ $(p \geq 3)$ exist. *IEEE Trans.*, 2002, IT-48: 2384-2391.

[5] Ke-Qin, Feng, S. Ling and C. Xing. Asymptotic bounds on quantum error-correcting codes from algebraic geometry codes. *IEEE Trans.*, 2006, IT-52: 986-991.

[6] Ke-Qin, Feng and C. Xing. A new construction of quantum error-correcting codes. *Amer. Math. Soc.*, 2008,360: 2007-2019

[7] D. Schlingemann and R. F. Werner. Quantum error-correcting codes associated with graphs. *Phys. Rev. A*, 2002, 65: 012308.