Foundations of Quantum Error Correction

Alexei Ashikhmin

Simon Litsyn

Author address:

Communications and Statistics Research Department, Bell Labs, Lucent Technologies, 600 Mountain Ave., #2C-355, Murray Hill, NJ 07974

E-mail address: aea@research.bell-labs.com

Department of Electrical Engineering-Systems, Tel Aviv University, Ramat Aviv 69978, Israel

E-mail address: litsyn@eng.tau.ac.il

1991 *Mathematics Subject Classification.* Primary 1; Secondary 2.

Abstract. This tutorial gives an introduction into the theory of quantum error correcting codes for researchers with background in mathematics and the combinatorial coding theory. We first give a short introduction into main notions of quantum computations such as qubits, measurement, and quantum gates. Next, we give a formal definition of unrestricted quantum error correcting codes and the quantum completely depolarizing channel. Further, we consider generalization of fundamental notions and results of the classical coding theory for the quantum case. In particular, we consider quantum stabilizer codes, which can be considered as analogs of classical linear codes, define and study properties of quantum weight enumerators, and derive upper and lower bounds on the quantum minimum distance.

Contents

Chapter 1. Introduction 1

Chapter 2. Basic Notions of Quantum Computations 3
2.1. Qubits 3
2.2. Linear Algebra Notation versus Dirac Notation 4
2.3. Unitary Transformation and von Neumann Measurement 5
2.4. Quantum Circuits 6
2.5. Non Cloning Theorem 8

Chapter 3. Introduction to the Theory of Quantum Error Correcting Codes 9
3.1. Completely Depolarizing Channel 9
3.2. Quantum Repetition Code 10
3.3. Formal Definition of Quantum Codes 13

Chapter 4. Quantum Stabilizer Codes 17
4.1. Construction and Parameters 17
4.2. Encoding of Quantum Codes 21
4.3. Decoding of Quantum Stabilizer Codes 22

Chapter 5. Bounds on Minimum Distance of Quantum Codes 25
5.1. Quantum MacWilliams Identities 25
5.2. Upper Bounds on Minimum Distance of Quantum Codes 30
5.3. Lower Bound on the Minimum Distance 34

Bibliography 39

CHAPTER 1

Introduction

In the beginning of the 1980s Richard Feynman conjectured that a quantum computer might be radically more powerful than any classical computational device. The first spectacular confirmation of this conjecture was Peter Shor's discovery in 1995 of a quantum algorithm for factoring numbers in polynomial time. Other impressive potential applications of the quantum computer include Grover's algorithm, which allows one to find a single object among unsorted N objects in O(sqrt(N)) time, efficient simulation of quantum mechanical systems, quantum cryptographical systems, which can not be compromised by a classical computer.

In order to exploit the advantages of a quantum computational device it should be constructed. There are a number of proposals for the physical realization of basic quantum devices with the help of various media that possess quantum properties. Examples include electron spins, collective states of superconductors, nuclear spins in electrons, and photons. All these proposals are based on well investigated physical models, that, under ideal conditions, allow manipulation and extraction of quantum information. Unfortunately, any real physical system can not be completely isolated from its environment and the parameters of the system are not known exactly. This causes unavoidable environmental and control errors in basic quantum devices and during quantum information transmission through quantum channels.

An efficient way for fighting quantum errors is the application of quantum error correcting codes. Unlike the classical case the very existence of quantum error correcting codes is far from being obvious. Indeed, according to the no-cloning theorem one can not produce a copy of a quantum bit. This means that even the classical repetition code, the simplest classical code, does not have a quantum analog. Fortunately, with the help of proper understanding of nature of quantum information, quantum error correcting codes can be well defined and used for fighting different types of quantum errors.

In these lecture notes we give basic properties of quantum bits (qubits) and elementary quantum operations. Next we give a formal definition of unrestricted quantum error correcting codes and the quantum completely depolarizing channel. Then we proceed with the theory of quantum stabilizer (additive) codes, which establish the most important class of quantum error correcting codes. We consider connections between quantum stabilizer codes and classical codes, and use this connection to construct a large class of powerful quantum codes. Next we consider the Shor-Laflamme quantum enumerators and establish a quantum analog of the classical MacWilliams identities. With the help of the quantum MacWilliams identities we derive lower and upper bounds on the minimum distance of quantum codes.

CHAPTER 2

Basic Notions of Quantum Computations

2.1. Qubits

One of the basic concepts of classical computations, theory of error correcting codes and other related disciplines, is *bit*. An analog of this notion in quantum computations is *quantum bit* or *qubit*. Qubits are defined as physical systems exhibiting quantum properties. Examples of such systems are photons, electron spins, ions, collective states of superconductors and many others.

As a typical example let us consider an ion, fig.1. The ion consists of a nuclear and an electron. The electron can orbit around the nuclear either on a low energy orbit or a high energy orbit. If in a particular moment the electron is on the low energy orbit, then sending a laser beam of an appropriate frequency we can force the electron to absorb a photon and move to the high energy orbit. Similarly, sending a beam of a different frequency forces the electron to emit a photon and move to the low energy orbit. Obviously we can use these two levels of energy for encoding logical 0 and 1 of a classical bit. Much more surprising fact is that by sending two laser beams simultaneously, we can force the electron to behave such as if it was on both orbits simultaneously. For instance, we can force the electron to spend 30% of its time on the low energy orbit and 70% of its time on the opposite orbit. Note that the given description is a very simplified, and even not correct, interpretation of a real ion. A physicist probably would not agree with this description. We still believe that it gives a good inside in the behavior of a qubit.

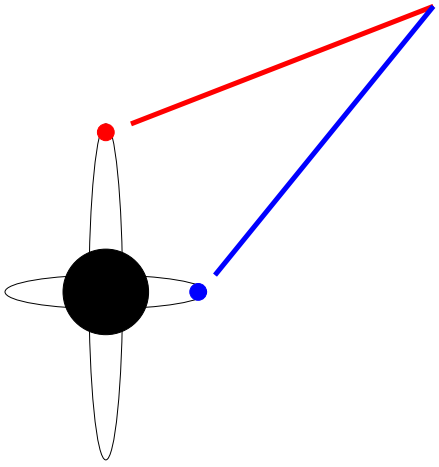


FIGURE 1. Realization of qubit with the help of an ion

This phenomenon does not have a classical analog - indeed a classical bit is always either 0 or 1. In quantum physics the low and high energy states of the ion are described with the help of two orthogonal vectors $\mathbf{v}_0$ and $\mathbf{v}_1$ from $\mathbb{C}^2$ respectively. As we already said, an arbitrary state of the ion is a superposition of the low and high energy states. Thus, we come to the following formal definition of the *state of a qubit.*

DEFINITION 2.1. A (pure) state of a qubit is a norm one complex vector

$$\mathbf{v} \in \mathbb{C}^2, \ ||\mathbf{v}|| = 1.$$

REMARK 2.2. We would like to note that beyond pure states there is also a very important notation of *mixed states.* However, in this tutorial we confine ourselves by working only with pure states. Almost all theorems and properties of quantum error correcting codes described in this text are also valid in the case of mixed states.

Similar to the notion of the pure state of one qubit we define the state of n qubits.

DEFINITION 2.3. A pure state of n qubits is a norm one vector

$$\mathbf{v} \in \mathbb{C}^{2^n}, \ ||\mathbf{v}|| = 1.$$

REMARK 2.4. It follows from the definition of the von Neumann measurement (see Section 2.3) that there is no way to learn whether qubits are in the state $\mathbf{v}$ or in the state $\mathbf{w} = \alpha\mathbf{v}, \alpha \in \mathbb{C}, \mathbf{v} \in \mathbb{C}^{2^n}$. For this reason vectors $\mathbf{v}$ and $\mathbf{w}$ define one and the same quantum state. Thus all possible pure quantum states of n qubits define the projective space $\mathbb{C}P^{2^n}$.

REMARK 2.5. As one can see from this definition, for describing a quantum state of n qubits we need $2^n - 1$ complex numbers. For this reason the complexity of simulation of a quantum system on a classical computer has exponential complexity.

Unlike the classical case, in which it is usually not a problem to read off the values (the states) of classical bits, we can not determine the quantum state of qubits. As it is explained in Section 2.3, one can learn only some partial information about a quantum state with the help of a quantum measurement.

2.2. Linear Algebra Notation versus Dirac Notation

In quantum physics it is customary to use the Dirac notation, which replace the standard linear algebra notation.

Let vectors $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{2^n-1}$ form an orthonormal basis of the space $\mathbb{C}^{2^n}$ (when we say vectors we always assume column vectors). Let $(a_0, a_1 \ldots, a_{n-1})$ be the binary representation of an integer $i, 0 \leq i \leq 2^n - 1$. Then the linear algebra notation $\mathbf{v}_i$ corresponds to the Dirac notation

$$|i\rangle \text{ or } |a_0, a_1, \ldots, a_{n-1}\rangle. \tag{2.1}$$

The linear algebra notation $\mathbf{v} = \alpha_0\mathbf{v}_0 + \alpha_1\mathbf{v}_1 + \ldots + \alpha_{2^n-1}\mathbf{v}_{2^n-1}$ corresponds to

$$|\mathbf{v}\rangle = \alpha_0|0\ldots00\rangle + \alpha_1|0\ldots01\rangle + \ldots + \alpha_{2^n-1}|1\ldots11\rangle$$

or

$$|\mathbf{v}\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \ldots + \alpha_{2^n-1}|(2^n-1)\rangle$$

The Hermitian transposition $\mathbf{v}_i^\dagger$ corresponds to

$$\langle i| \text{ or } \langle a_0, a_1, \ldots, a_{n-1}|.$$

Finally, if A is a linear operator and $b_0, b_1, \ldots, b_{n-1}$ is the binary representation of j than the linear algebra notation $\mathbf{v}_j^\dagger A \mathbf{v}_i$ corresponds to

$$\langle j|A|i\rangle \text{ or } \langle b_0, b_1 \ldots, b_{n-1}|A|a_0, a_1, \ldots, a_{n-1}\rangle.$$

In this tutorial we mostly use the standard linear algebra notation. We still apply the Dirac notation in several places where it makes notation much shorter and easier to understand.

Before continuing, we would like to recall here some well known facts from linear algebra (see for example [**L**]), which we often use in the next sections.

- Any subspace Q of the complex space $\mathbb{C}^N$ has the orthogonal projection operator P_Q.
- If $\mathbf{v} \in Q$ then $P_Q \mathbf{v} = \mathbf{v}$.
- If $\mathbf{w}$ belongs to the orthogonal complement of Q in $\mathbb{C}^N$ then $P_Q \mathbf{w} = 0$.
- The dimension of Q can be found via P_Q as

$$\dim Q = \mathrm{Tr}\,(P_Q). \tag{2.2}$$

- If $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_M$ is an orthonormal basis of Q then

$$P_Q = \sum_{i=1}^{M} \mathbf{v}_i \mathbf{v}_i^\dagger. \tag{2.3}$$

- A linear operator P is an orthogonal projector iff

$$P^\dagger = P \text{ and } PP = P.$$

2.3. Unitary Transformation and von Neumann Measurement

Generally speaking a quantum computer can make two types of transformations over qubits - unitary rotation and measurement. Below we give definitions of these transformations.

If we have n qubits in a state $\mathbf{v} \in \mathbb{C}^{2^n}$ then a quantum computer can rotate the state $\mathbf{v}$ by any unitary operator U. After this rotation the new state of the qubits is $U\mathbf{v}$. Design of a low complexity quantum circuit for implementation of a unitary rotation U is a separate problem, which will not be covered in this tutorial.

Unlike the unitary transformation the von Neumann Measurement is a probabilistic procedure. A measurement has several possible outcomes and each outcome can happen with a certain probability. We define a measurement with respect to a partition of the space $\mathbb{C}^{2^n}$ into a set of orthogonal subspaces. Let $P_1, P_2, \ldots, P_t$ be a set of orthogonal projection operators such that

$$P_i P_j = \delta_{ij} P_i, \tag{2.4}$$

$$P_1 + P_2 + \ldots + P_t = I_{2^n}. \tag{2.5}$$

Obviously the subspaces corresponding to $P_i, i = 1, \ldots, t$, are mutually orthogonal and span $\mathbb{C}^{2^n}$. We will say that they form a partition of $\mathbb{C}^{2^n}$. If we measure n qubits in a state $\mathbf{v} \in \mathbb{C}^{2^n}$ with respect to $P_1, P_2, \ldots, P_t$ then with the probability

$$p_i = \mathbf{v}^\dagger P_i \mathbf{v}$$

the new state of the qubits is

$$\mathbf{z} = \frac{P_i \mathbf{v}}{\sqrt{\mathbf{v}^\dagger P_i \mathbf{v}}}.$$

From (2.4) and (2.5) it follows that $p_1 + p_2 + \ldots + p_t = 1$. In other words during the measurement the original state $\mathbf{v}$ is projected to one of the subspaces defined by $P_1, P_2, \ldots, P_t$. The index i of the subspace, to which the projection was done, is available to us after the measurement. This is the only information that we can learn about the quantum state $\mathbf{v}$ with the help of the measurement. The process of measurement of one qubit is illustrated in fig.2. As we discussed above the measuring device has two outputs - the quantum output $P_i\mathbf{v}$ and the classical output i.

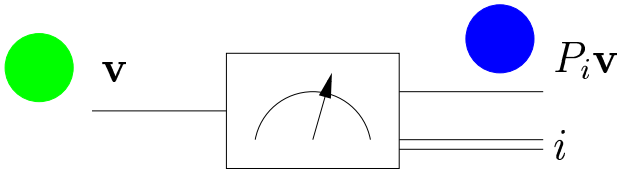


FIGURE 2. von Neumann Measurement device

Sometimes we would like to measure only a subset of a set of qubits. For example, let us say that we have n qubits and would like to measure the first m of them with respect to projector operators $P_1, \ldots, P_t$, which act on $\mathbb{C}^{2^m}, m \leq n$, and satisfy properties (2.4) and (2.5). From the definition of the measurement it is not difficult to see that such measurement is equivalent to the measurement of the all n qubits with respect to $P_1 \otimes I_{n-m}, \ldots, P_t \otimes I_{n-m}$. For example if we have the state

$$\alpha|01\rangle + \beta|10\rangle$$

and measure the first qubit with respect to the subspaces generated by $|0\rangle$ and $|1\rangle$ then with probability α^2 we obtain $|01\rangle$ and with probability β^2 we obtain $|10\rangle$.

REMARK 2.6. There is an important generalization of the von Neumann measurement - the Positive Operator-Valued Measurement (POVM). For our purposes it will be enough to use only the von Neumann measurement. Thus we omit the definition of POVM.

2.4. Quantum Circuits

Similar to the classical case it is convenient to introduce the notation of elementary quantum gates. The elementary quantum gates are analogs of classical gates, such as NOT, XOR, OR, and so on.

Let first consider some single qubit gates presented in figure 3. Each of this gates implements some unitary rotation. For example the X gate is equivalent to the unitary rotation

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.6}$$

The quantum state $\alpha|0\rangle + \beta|1\rangle$ in the Dirac notation corresponds to the vector $(\alpha, \beta)^\top$ in the linear algebra notation. Thus at the output of the gate we have

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}, \tag{2.7}$$

which is $\beta|1\rangle + \alpha|0\rangle$ in the Dirac notation. Similarly, one can check that the Z, H, and S gates correspond to the following unitary rotation operators

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \; H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \; S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}.$$

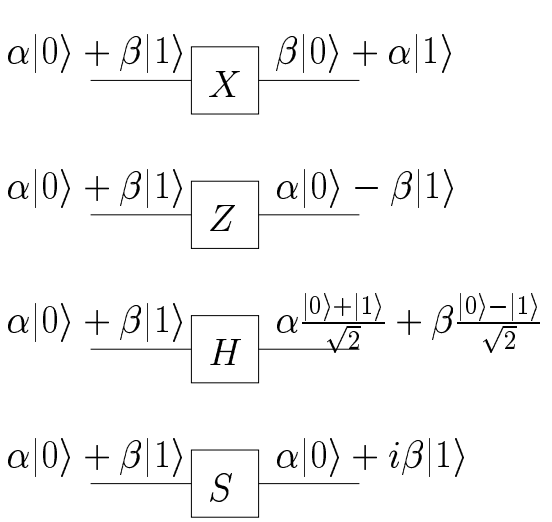


FIGURE 3. elementary quantum gates

In figure 4 we present the very important quantum Control-Not gate, which acts on two qubits. The effect of this gate is equivalent to the rotation of a state of two qubits by the unitary operator

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

The joint state at the input of the gate is

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \mu|1\rangle) = \alpha\gamma|00\rangle + \alpha\mu|01\rangle + \beta\gamma|10\rangle + \beta\mu|11\rangle.$$

One can check that by multiplying this state by U_{CNOT}, we obtain

$$\alpha\gamma|00\rangle + \alpha\mu|01\rangle + \beta\gamma|11\rangle + \beta\mu|10\rangle.$$

On figure 5 we present the *Toffoli* gate. The input state

$$\alpha_{000}|000\rangle+\alpha_{001}|001\rangle+\alpha_{010}|010\rangle+\alpha_{011}|011\rangle+\alpha_{100}|100\rangle+\alpha_{101}|101\rangle+\alpha_{110}|110\rangle+\alpha_{111}|111\rangle$$

is moved by the Toffoli gate into the state

$$\alpha_{000}|000\rangle+\alpha_{001}|001\rangle+\alpha_{010}|010\rangle+\alpha_{011}|011\rangle+\alpha_{100}|100\rangle+\alpha_{101}|101\rangle+\alpha_{110}|111\rangle+\alpha_{111}|110\rangle.$$

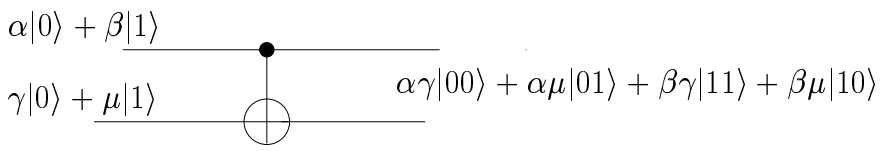


FIGURE 4. CNOT gate

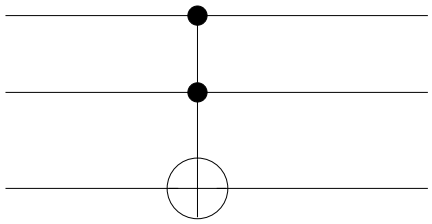


FIGURE 5. Toffoli Gate

It is well known that classical AND and NOT gates allow one to implement an arbitrary boolean function. Similarly some sets of quantum gates allow approximation of any unitary rotation with arbitrary accuracy. Such sets of quantum gates are called *universal quantum gates*. For example, the gates $H, S, CNOT$, $Toffoli$ form a set of universal quantum gates.

2.5. Non Cloning Theorem

When we start to think about protecting classical information perhaps the first thing that comes to our mind is the repetition of the information. In other words if we would like to transmit one bit of information, say a, through a noisy channel, we send several, say 3, copies of it - a, a, a. Then in the case of flipping any of these three bits we still can reconstruct the original bit using the majority rule. It is natural to ask the question whether we can copy quantum states. The answer is NO [**WOOT**].

Indeed, let us assume that there exists a map such that

$$\mathbf{v} \to \mathbf{v} \otimes \mathbf{v} \tag{2.8}$$

Then

$$\mathbf{v} + \mathbf{w} \to (\mathbf{v} + \mathbf{w}) \oplus (\mathbf{v} + \mathbf{w}). \tag{2.9}$$

According to the quantum mechanics postulates this map must be linear. Therefore

$$\mathbf{v} + \mathbf{w} \to \mathbf{v} \otimes \mathbf{v} + \mathbf{w} \otimes \mathbf{w},$$

which contradicts to (2.9).

CHAPTER 3

Introduction to the Theory of Quantum Error Correcting Codes

3.1. Completely Depolarizing Channel

Similar to the classical case there is an infinite variety of quantum channels. In this notes we will consider only the quantum channel that can be considered as a quantum analog of the classical memoryless binary symmetric channel - the quantum *completely depolarizing channel*.

In the completely depolarizing channel there are only three types of errors that can effect a qubit - the flip error, phase error, and flip-phase error.

The flip error is equivalent to the quantum gate X (2.6) and its effect on a quantum state (α, β) is described by equation (2.7). Similar, the phase error is equivalent to the quantum gate Z. The flip-phase error, also called Y error, is defined by the unitary operator

$$Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}.$$

REMARK 3.1. One of the reasons why we confine ourselves by this set of errors is that the operators I_2, X, Z, and Y form an orthonormal basis of the linear space of linear operators acting on $\mathbb{C}^2$ and any other error that act on $\mathbb{C}^2$ can be represented as a linear combination of I_2, X, Z, and Y.

Error operators that effect n qubits have the form

$$E = e_1 \otimes e_2 \otimes \ldots \otimes e_n, \tag{3.1}$$

where $e_i \in \{I_2, X, Z, Y\}$. Thus if we send through the completely depolarizing channel n qubits with a state $\mathbf{v}$ we receive on the other end of the channel the same n qubits whose state is $E\mathbf{v}$. If $e_i = I_2$ we will say that the i-th qubit is not effected by an error. If e_i is equal to X, Z, or Y we will say that the i-th qubit is effected by the flip, phase, or flip-phase error respectively.

We will assume that the probability of an error is p, that is

$$\Pr(e_i = I_2) = 1 - p \text{ and } \Pr(e_i = X) = \Pr(e_i = Y) = \Pr(e_i = Z) = \frac{p}{3}.$$

Similar to the classical case, we define the weight $\mathrm{wt}\,(E)$ of an error operator E acting on n qubits as the number of corrupted qubits.

DEFINITION 3.2. $\mathrm{wt}\,(E) = |\{e_i \neq I_2, i = 1, \ldots, n\}|$.

Obviously the probability of a particular error operator is the following function of its weight:

$$\Pr(E) = \left(\frac{p}{3}\right)^{\mathrm{wt}\,(E)} (1-p)^{n-\mathrm{wt}\,(E)}.$$

From the last equation it follows that if $p < \frac{1}{4}$, which we always assume is the case, error operators of small weights have dominating probabilities. For this reason we would like to construct quantum codes so that they could correct all, or almost all, error operators up to a certain weight.

3.2. Quantum Repetition Code

Based on the non cloning theorem one can make a wrong conclusion that quantum states can not be protected from channel errors. Fortunately, to protect quantum information we do not have to clone it. Instead we are going to use a linear map of original quantum state $\mathbf{v} \in \mathbb{C}^{2^m}$ into a state $\mathbf{w}$ from a 2^m dimensional subspace Q of the space $\mathbb{C}^{2^n}$. If an error moves $\mathbf{w}$ out of Q we will detect this fact with the help of a von Neumann measurement and further reconstruct the original state $\mathbf{v}$ by applying an appropriate unitary rotation. We will call Q a *quantum code*.

The first quantum error correcting codes were discovered independently by P.Shor [**SH95**] and A.M.Steane [**Ste96a**]. In this section we first consider linear maps that allow us to construct quantum analogs of classical repetition codes that can correct either flip or phase errors. Next we present the first Shor nine qubits code that can correct any flip, phase, or flip-phase error. In the next section we will give a formal definition of quantum error correcting codes.

Let us start with the code that is capable of correcting one flip error. We will define the code with the help of the following linear map

$$\alpha|0\rangle + \beta|1\rangle \to \alpha|000\rangle + \beta|111\rangle.$$

A quantum circuit for implementing this linear map is shown in figure 1. The state $\alpha|000\rangle + \beta|111\rangle$ is the codeword corresponding to the uncoded (information) vector $\alpha|0\rangle + \beta|1\rangle$.

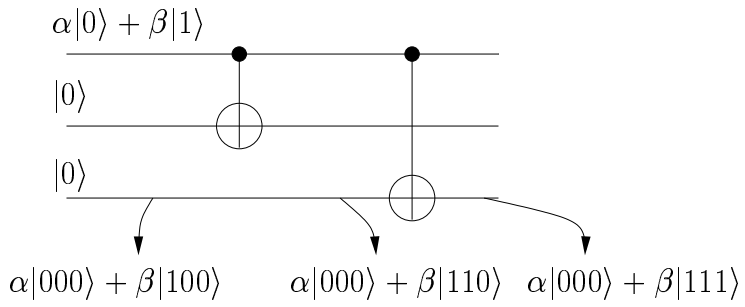


FIGURE 1. Encoding

Now let us assume that the first bit of the codeword is flipped, so we have the state $\alpha|100\rangle + \beta|011\rangle$. The quantum circuit in fig. 2 can be used for decoding. As one can see the decoder correctly reconstructs the original state $\alpha|0\rangle + \beta|1\rangle$. It is easy to check that this decoder can correct flipping of any single qubit.

It is interesting to note that unlike the classical case the probability of decoding error can be different for different code states.

Let the probability of a flip error be equal to $p_{fl} = 0.25$. The probabilities of the all possible states after transmission the state $|0\rangle$ through the channel and after

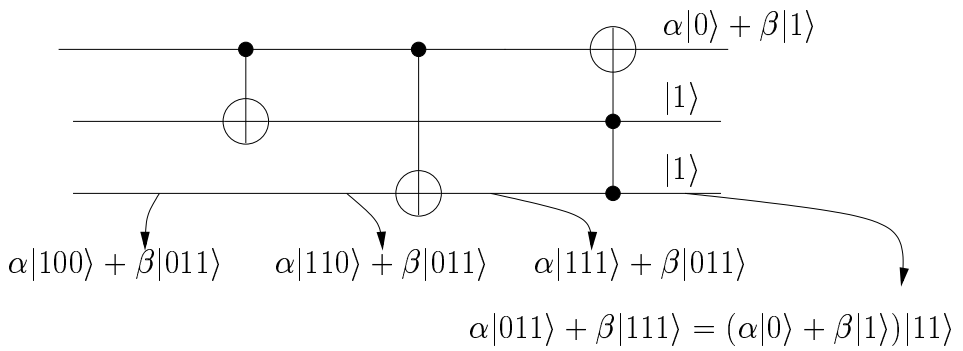


FIGURE 2. Decoding

decoding are presented at the following picture

$$|0\rangle \overset{\text{encode}}{\longrightarrow} |000\rangle \overset{\text{channel}}{\longrightarrow} \begin{cases} 0.75^3: & |000\rangle \\ 0.25\cdot 0.75^2: & |100\rangle \\ \vdots & \vdots \\ 0.25^3: & |111\rangle \end{cases} \overset{\text{decode}}{\longrightarrow} \begin{cases} 0.4219: & |0\rangle|00\rangle \\ 0.1406: & |0\rangle|11\rangle \\ \vdots & \vdots \\ 0.0156: & |1\rangle|00\rangle \end{cases}$$

One can see that the probability of decoding error equals $P_{de} = 0.1563 < p_{fl} = 0.25$. The same probabilities for the state $|0\rangle + |1\rangle$ are

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \overset{\text{encode}}{\longrightarrow} \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

$$\rightarrow \begin{cases} 0.75^3: & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ 0.25\cdot 0.75^2: & \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle) \\ \vdots & \vdots \\ 0.25^3: & \frac{1}{\sqrt{2}}(|111\rangle + |000\rangle) \end{cases} \begin{cases} 0.4219: & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ 0.1406: & \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \\ \vdots & \vdots \\ 0.0156: & \frac{1}{\sqrt{2}}(|111\rangle + |000\rangle) \end{cases}$$

We observe that after decoding we always have one and the state $|000\rangle + |111\rangle$. Thus the probability of decoding error equals zero, $P_{de} = 0$.

Now let us consider a code that can correct any single phase error. The code is defined with the help of the following map

$$\begin{aligned} |0\rangle &\rightarrow (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle), \\ |1\rangle &\rightarrow (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle). \end{aligned}$$

Encoding and decoding of the code can be implemented with the help of the circuits shown in fig.3 and fig.4 respectively. In fig.3 we show the encoding of the state $|1\rangle$ and in fig.4 we show the process of decoding assuming that the first bit suffered the phase error.

In 1995 Peter Shor [**SH95**] discovered the very first quantum code. This code encodes 1 qubit into 9 qubits and is capable of correction of any flip, or any phase Z, or any flip-phase error, and in fact any linear combination of these errors. Shor's code can be viewed as a smart concatenation of the repetition codes that we considered above. It is defined with the help of the following linear map

$$\begin{aligned} |0\rangle &\rightarrow (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle), \\ |1\rangle &\rightarrow (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle). \end{aligned}$$

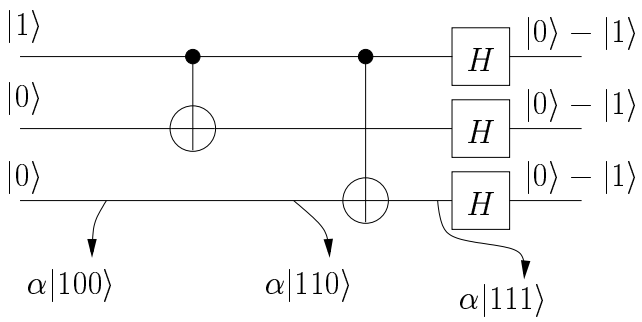


FIGURE 3. Encoding

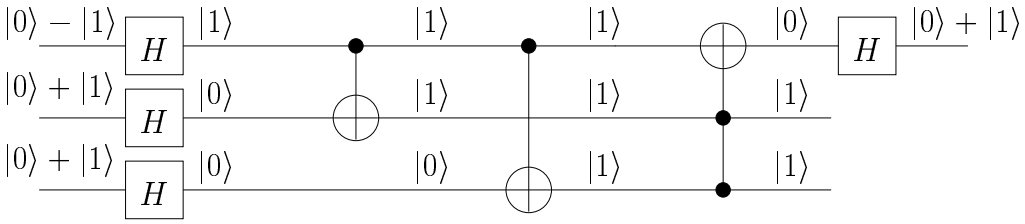


FIGURE 4. Decoding

One can check that encoding can be implemented with the help of the circuit in fig.5.

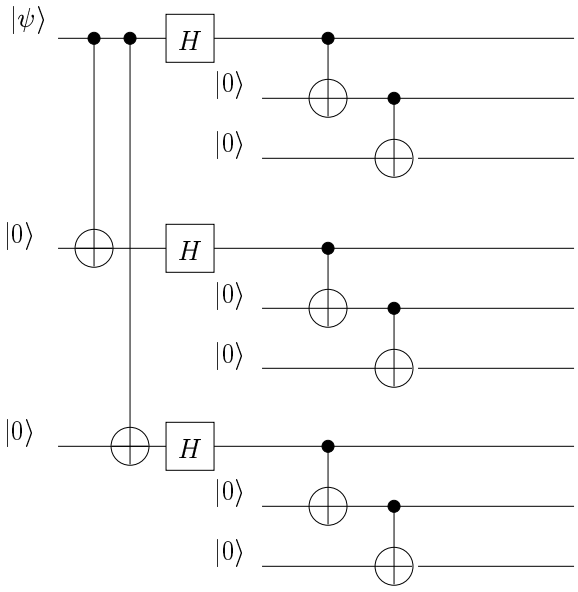


FIGURE 5. Decoding

We leave as an exercise construction of a quantum circuit for decoding the Shor code.

3.3. Formal Definition of Quantum Codes

A classical (n, M) binary code is a set of M binary n-tuples. n is called the code length and M is called the code size. A classical $[n, k]$ binary linear code is a k-dimensional linear subspace of $\mathbb{F}_2^n$; its code size is $M = 2^k$.

Trying to keep the same notation for the quantum case, we define a quantum code as follows.

DEFINITION 3.3. A quantum $((n, K))$ code is a K-dimensional subspace of $\mathbb{C}^{2^n}$.

We will say that n is the code length. Though K is the dimension of the code subspace we prefer to call K the size of the code, not its dimension. The reason is that the number of classical messages that can be transmitted with the help of this code is exactly K, i.e. K plays a role of M, the number of code words, in a classical code. The reason why we can not encode more than K classical messages is that the number of orthogonal subspaces in the finest partition of $\mathbb{C}^K$ is exactly K. Thus if we encode $K + 1$ classical messages we will not be able to figure out which message is encoded with the help of any von Neumann measurement (in fact we will not be able to do it with any POVM measurement as well).

REMARK 3.4. We said that a quantum code Q is a linear subspace of $\mathbb{C}^{2^n}$. There is a subtle point about this definition. Proportional vectors represent one and the same quantum state. Therefore we have to say that Q is the projective space $\mathbb{C}P^{K-1}$. Defining a quantum code as a projective space poses problems with tensoring, which is a very needed operation. We continue to say that Q is a linear subspace, but when we integrate over Q we will take only vectors of unit norm.

Unlike the classical case, the definition of the minimum distance of a quantum code is not so obvious. To give this definition let us first recall ourselves that the minimum distance of classical codes can be defined as the minimum weight among the weights of the undetectable errors. For example, let us consider the classical nonlinear code

$$C = \{(0, 0, 0), (0, 1, 1), (1, 1, 1)\}.$$

The error $(1, 0, 0)$ is not detectable since it moves the code word $(0, 1, 1)$ into the different code word $(1, 1, 1)$. Obviously the weight of any error is greater than or equal to 1. Thus the minimum distance of C is 1. While these arguments are trivial in the classical case, they happened to be useful for defining the minimum distance of quantum codes.

Let Q be a quantum code and P be the orthogonal projector on Q.

DEFINITION 3.5. An error operator E is called detectable iff

$$PEP = c_E P,$$

where c_E is a constant that depends only on E.

Now we are in position to define the minimum distance of a quantum code.

DEFINITION 3.6. The minimum distance of Q is the maximum integer d such that any error $E, \mathrm{wt}(E) \leq d - 1$, is detectable.

Similar to the classical case the minimum distance of a quantum code tells how many errors the code can correct.

THEOREM 3.7. [**KL97**]*(see also* [**BDSW**]*) A code Q with minimum distance d can correct all error operators E with* $\mathrm{wt}(E) \leq \lfloor (d-1)/2 \rfloor$.

We will prove Theorem 3.7 in Section 4.3 for the special class of quantum codes - the quantum stabilizer codes. Below we give two observations that motivate Definition 3.5 of detectable errors.

The first observation is that in the classical case an error $\mathbf{e}$ is detectable iff $\mathbf{e} + \mathbf{c} \notin C$ for any $\mathbf{c} \in C$.

The second observation is that according to the definition of the von Neumann measurements two quantum states, say $\mathbf{v}$ and $\mathbf{w}$, are distinguishable iff they are orthogonal. Indeed, if we know that the state of some qubits is either $\mathbf{v}$ or $\mathbf{w}$ then measuring these qubits with respect to the subspace generated by $\mathbf{v}$ and its orthogonal complement, to which the vector $\mathbf{w}$ obviously belongs, we will learn with probability 1 the state of the qubits.

Taking into account these two observations it is naturally to give the following definition for detectable errors.

DEFINITION 3.8. E is detectable iff

$$\mathbf{v}^\dagger E \mathbf{w} = 0$$

for any orthogonal vectors $\mathbf{v}$ and $\mathbf{w}$ from Q.

In other words any two distinguishable quantum states stay distinguishable if one of them is effected by a detectable error E. Unfortunately, it is quite difficult to use this definition, since there are infinitely many orthogonal (distinguishable) states in Q. For this reason we prefer to use the definition 3.5. The following theorem shows that in fact these two definitions are equivalent.

THEOREM 3.9. *Definitions (3.8) and (3.5) are equivalent.*

PROOF. Let E be detectable according to definition 3.8 and

$$\mathbf{v}_1, \mathbf{v}_2 \in Q,\ \mathbf{v}_1^\dagger \mathbf{v}_2 = 0,\ ||\mathbf{v}_1|| = ||\mathbf{v}_2|| = 1.$$

Let us define vectors $\mathbf{w}_1$ and $\mathbf{w}_2$ as follows

$$\mathbf{w}_1 = \mathbf{v}_1 + \mathbf{v}_2 \text{ and } \mathbf{w}_2 = \mathbf{v}_1 - \mathbf{v}_2.$$

Clearly $\mathbf{w}_1, \mathbf{w}_2 \in Q$ and $\mathbf{w}_1^\dagger \mathbf{w}_2 = 0$. Hence

$$\mathbf{w}_1^\dagger E \mathbf{w}_2 = \mathbf{v}_1^\dagger E \mathbf{v}_1 + \mathbf{v}_2^\dagger E \mathbf{v}_1 - \mathbf{v}_1^\dagger E \mathbf{v}_2 - \mathbf{v}_2^\dagger E \mathbf{v}_2 = 0$$

and therefore

$$\mathbf{v}_1^\dagger E \mathbf{v}_1 = \mathbf{v}_2^\dagger E \mathbf{v}_2 = c_E.$$

Let now vectors $\mathbf{v}_1, \ldots, \mathbf{v}_K$ form an orthonormal basis of Q. Then $P = \sum_{i=1}^K \mathbf{v}_i \mathbf{v}_i^\dagger$ is the orthogonal projection operator on Q by (2.3). and we have

$$PEP = \left(\sum_{i=1}^K \mathbf{v}_i \mathbf{v}_i^\dagger \right) E \left(\sum_{i=1}^K \mathbf{v}_i \mathbf{v}_i^\dagger \right) = \sum_{i,j} \mathbf{v}_i \mathbf{v}_i^\dagger E \mathbf{v}_j \mathbf{v}_j^\dagger = c_E P.$$

Thus definition 3.5 follows from definition 3.8.

In other direction. Let $\mathbf{v}, \mathbf{w} \in Q,\ \mathbf{v}^\dagger \mathbf{w} = 0$. Then we have

$$\begin{aligned} PEP &= c_E P, \\ \mathbf{v}^\dagger PEP\mathbf{w} &= c_E \mathbf{v}^\dagger P\mathbf{w}, \\ \mathbf{v}^\dagger E\mathbf{w} &= c_E \mathbf{v}^\dagger \mathbf{w}, \\ \mathbf{v}^\dagger E\mathbf{w} &= 0. \end{aligned}$$

□

CHAPTER 4

Quantum Stabilizer Codes

4.1. Construction and Parameters

The quantum stabilizer codes were invented independently in [**GOT**] and in [**CRSS97**], [**CRSS98**]. The generalization of these codes for the nonbinary case was suggested in [**AK**]. These codes can be considered as an analog to classical linear codes and have simple encoding and decoding algorithms. They are strongly related to classical self-orthogonal codes and find numerous applications in quantum error correction, fault tolerant quantum computations, quantum secret sharing and other related areas. In this text we mostly follow the description from [**AK**].

The stabilizer codes are defined with the help of the extraspecial group. Let Es be the error operators that we used in the definition of the quantum completely Depolarizing channel, i.e.

$$E = \alpha e_1 \otimes e_2 \otimes \ldots \otimes e_n,\ \alpha = \pm 1, \pm\sqrt{-1}$$

where $e_i \in \{I_2, X, Z, Y\}$. The operators E form the extraspecial group $\mathcal{E}_n, |\mathcal{E}_n| = 4^{n+1}$. (For a detailed description of the extra-special group and its use for construction of quantum codes see [**CRSS97**],[**CRSS98**], [**AK**].)

The extraspecial group is isomorphic to the vector space $\mathbb{F}_2^{2^n}$ and has the center

$$\mathcal{Z}(\mathcal{E}_{2^n}) = \{I_{2^n}, -I_{2^n}, iI_{2^n}, -iI_{2^n}\}.$$

Recall that the center of a group G is

$$\mathcal{Z}(G) = \{g \in G : gg' = g'g \text{ for all } g' \in G\}.$$

Let us take an Abelian subgroup S of $\mathcal{E}_{2^n}$ such that $S \cap \mathcal{Z}(\mathcal{E}_{2^n}) = I_{2^n}$. Let also $\lambda(E), E \in S$, be a linear character of S. We define the quantum stabilizer code $Q_{S,\lambda}$ associated with the subgroup S and the character λ as follows.

DEFINITION 4.1.

$$Q_{S,\lambda} = \{\mathbf{v} \in \mathbb{C}^{2^n} : E\mathbf{v} = \lambda(E)\mathbf{v} \text{ for all } E \in S\}.$$

The set $Q_{S,\lambda}$ is obviously a linear subspace of $\mathbb{C}^{2^n}$. In oder to find the size and the minimum distance of $Q_{S,\lambda}$ we need the following theorem.

THEOREM 4.2. *The operator*

$$P = \frac{1}{|S|}\sum_{E\in S} \bar{\lambda}(E)E$$

is the orthogonal projection on $Q_{S,\lambda}$.

PROOF. Let $E' \in S$. Then

$$E'P = \frac{1}{|S|}\sum_{E\in S} \bar{\lambda}(E)E'E = \frac{1}{|S|}\sum_{E\in S} \bar{\lambda}((E')^\dagger E)E = \lambda(E')P, \tag{4.1}$$

where the last equality uses linearity of λ. From (4.1) it follows that $E'(P\mathbf{v}) = \lambda(E')(P\mathbf{v})$ and therefore the range of P is contained in $Q_{S,\lambda}$.

At the same time for any $\mathbf{v} \in Q$ we have

$$P\mathbf{v} = \frac{1}{|S|}\sum_{E\in S}\bar{\lambda}(E)E\mathbf{v} = \frac{1}{|S|}\sum_{E\in S}\bar{\lambda}(E)\lambda(E)\mathbf{v} = \mathbf{v}.$$

□

THEOREM 4.3. *Let* $|S| = 2^{n-k}$ *then* $K = \dim Q_{S,\lambda} = 2^k$.

PROOF. From the facts that

$$\mathrm{Tr}\,(X) = \mathrm{Tr}\,(Z) = \mathrm{Tr}\,(Y) = 0$$

and the identity

$$\mathrm{Tr}\,(A\otimes B) = \mathrm{Tr}\,(A)\mathrm{Tr}\,(B)$$

we have that

$$\mathrm{Tr}\,(E) = \begin{cases} 2^n, & E = I_{2^n} \\ 0, & E \neq I_{2^n} \end{cases}$$

Hence, using (2.2), we have

$$\dim(Q_{S,\lambda}) = \mathrm{Tr}\,(P) = \frac{1}{|S|}\sum_{E\in S}\lambda(E)\mathrm{Tr}\,(E) = \frac{\mathrm{Tr}\,(I_{2^n})}{|S|} = \frac{2^n}{2^{n-k}} = 2^k.$$

□

If a linear binary code has length n and size 2^k we say that it is an $[n,k]$ linear code. Similarly, we will say that $Q_{S,\lambda}$ is an $[[n,k]]$ quantum stabilizer code.

For studying action of error operators E on code vectors of $Q_{S,\lambda}$ and for estimation the minimum distance of $Q_{S,\lambda}$ it is convenient to introduce the dual subgroup $S^\perp$ of S by

$$S^\perp = \{E \in \mathcal{E}_{2^n} : EE' = E'E \text{ for all } E' \in S\}. \tag{4.2}$$

In other words $S^\perp$ consists of all error operators from $\mathcal{E}_n$ that commute with all operators from S. The error operators of the completely depolarizing channel can be partitioned into three sets according to their effect on $Q_{S,\lambda}$. (In this analysis when we say E we actually assume $\alpha E, \alpha = \pm 1, \pm i$.)

1. $E \in S$. In this case using (4.1) from Theorem 4.2 we have

   $$PEP = \lambda(E)P$$

   Therefore E according to Definition 3.5 is detectable. Moreover $E\mathbf{v} = \lambda(E)\mathbf{v},\ \mathbf{v} \in Q_{S,\lambda}$, i.e. E acts on $Q_{S,\lambda}$ as the identity operator.
2. $E \notin S^\perp$. It is not difficult to show that in this case E commutes with half operators from S, that form a subgroup S_0, and anticommutes with another half of S, which we will denote by $S_1 = S\setminus S_0$. Hence, using (4.1), we obtain

   $$\begin{aligned} |S|PEP &= \sum_{E'\in S}\bar{\lambda}(E)E'EP = E\sum_{E'\in S_0}\bar{\lambda}(E')E'P - E\sum_{E'\in S_1}\bar{\lambda}(E')E'P \\ &= |S_0|EP - |S_1|EP = 0. \end{aligned} \tag{4.3}$$

   Therefore E is again detectable.

3. $E \in S^{\perp} \setminus S$. Let us define the Abelian group $T =< S, E >$. T defines the quantum stabilizer code Q'. From Theorem 4.3 we have that $\dim(Q') = \dim(Q)/2$ and therefore there exists $\mathbf{v} \in Q_{S,\lambda}$ such that $E\mathbf{v} \not\propto \lambda(E)\mathbf{v}$. Hence

$$PEP\mathbf{v} = EPP\mathbf{v} = EP\mathbf{v} = E\mathbf{v} \not\propto \lambda(E)\mathbf{v}.$$

Hence $PEP \not\propto P$ and E is not detectable. It is also important to note that $PE\mathbf{v} = EP\mathbf{v} = E\mathbf{v}$ and therefore $E\mathbf{v} \in Q$. In other words E non-trivially rotates the code space Q.

We proved the following theorem.

THEOREM 4.4. *The minimum distance of $Q_{S,\lambda}$ equals*

$$d(Q_{S,\lambda}) = \min\{\mathrm{wt}\,(E) : E \in S^{\perp} \setminus S\}.$$

From the above arguments one can see that the minimum distance of $Q_{S,\lambda}$ depends only on the choice of the group S and does not depend on the choice of λ. For this reason usually we assume that λ is the trivial character, i.e. $\lambda(E) = 1$ for all $E \in S$, and denote the code by Q_S.

4.1.1. Connection with Classical Codes. It is easy to check that the factor group $\bar{\mathcal{E}}_2 = \mathcal{E}/\mathcal{Z}(\mathcal{E})$ is isomorphic to $\mathbb{F}_2^2$. The isomorphism is defined by the map

$$\alpha I_2 \Leftrightarrow (0,0); \alpha X \Leftrightarrow (1,0); \alpha Z \Leftrightarrow (0,1); \alpha Y \Leftrightarrow (1,1), \alpha \in \{\pm 1, \pm i\} \tag{4.4}$$

For instance

$$XY = iZ \Leftrightarrow (1,0) \oplus (1,1) = (0,1),$$

where $\oplus$ denotes summation by $\mod 2$. Using (4.4) we can establish a correspondence between $\mathbf{c} \in \mathbb{F}_2^{2n}$ and operators $E \in \mathcal{E}_{2^n}$, for instance

$$\mathbf{c} = (0,1,1|0,1,0) \Leftrightarrow E_{\mathbf{c}} = \alpha I_2 \otimes Y \otimes X, \alpha \in \{\pm 1, \pm i\}. \tag{4.5}$$

Let us assume that in (4.5) $\alpha = 1$. Then it is straightforward to check that

$$E_{(\mathbf{a},\mathbf{b})}E_{(\mathbf{a}',\mathbf{b}')} = (-1)^{\mathbf{b}\mathbf{a}'} i^{\mathbf{a}\mathbf{b}'+\mathbf{a}'\mathbf{b}} E_{(\mathbf{a}\oplus\mathbf{a}',\mathbf{b}\oplus\mathbf{b}')}, \tag{4.6}$$

$$E_{\mathbf{a},\mathbf{b}}E_{\mathbf{a}',\mathbf{b}'} = (-1)^{\mathbf{a}\mathbf{b}'-\mathbf{b}\mathbf{a}'} E_{\mathbf{a}',\mathbf{b}'}E_{\mathbf{a},\mathbf{b}}, \tag{4.7}$$

where $\mathbf{a}\mathbf{b} = \sum_i a_i b_i$. The product

$$(\mathbf{a},\mathbf{b}) * (\mathbf{a}',\mathbf{b}') = \mathbf{a}\mathbf{b}' \oplus \mathbf{b}\mathbf{a}' \tag{4.8}$$

is called the symplectic inner product. From (4.7) it follows that operators $E_{\mathbf{a},\mathbf{b}}$ and $E_{\mathbf{a}',\mathbf{b}'}$ commute iff

$$(\mathbf{a},\mathbf{b}) * (\mathbf{a}',\mathbf{b}') = 0.$$

Let us associate the group S with the code C according to (4.4).

EXAMPLE 4.5.

$$S = \{I_4, X \otimes X\} \Leftrightarrow C = \{(0,0|0,0), (1,0|1,0)\}$$

Let us define the dual code of C with respect to the symplectic inner product:

$$C^{\perp} = \{\mathbf{c} \in \mathbb{F}_2^n : \mathbf{c} * \mathbf{c}' = 0 \text{ for all } \mathbf{c}' \in C\}. \tag{4.9}$$

From (4.7) and from the definition (4.2) of $S^{\perp}$ it follows that $C^{\perp}$ is associated with $S^{\perp}$ with respect to (4.4). Therefore we conclude that codes C and $C^{\perp}$ are additive (in fact since they are binary they are linear of $\mathbb{F}_2$) and that $C \subseteq C^{\perp}$.

DEFINITION 4.6. A code C such that $C \subseteq C^{\perp}$ is called selforthogonal.

If we have a classical $[2n, k]$ code C, such that $C \subseteq C^{\perp}$, we can use it for construction of an Abelian group S and further a quantum stabilizer code Q_S. Let vectors $\mathbf{c}_1, \ldots, \mathbf{c}_k$ form a basis of C. Then we can construct an Abelian subgroup S associated with C as follows

$$S =< E_{\mathbf{c}_1}, \ldots, E_{\mathbf{c}_k} > .$$

The subgroup S consists of operators of the form $\beta_{\mathbf{c}} E_{\mathbf{c}}, \mathbf{c} \in C, \beta_{\mathbf{c}} = \pm 1$. If $\mathbf{c} = \mathbf{c}_{i_1} + \mathbf{c}_{i_2} + \ldots + \mathbf{c}_{i_t}, \mathbf{c} \in C$, then $\beta_{\mathbf{c}}$ should be chosen so that $\beta_{\mathbf{c}} E_{\mathbf{c}} = E_{\mathbf{c}_{i_1}} \cdot \ldots \cdot E_{\mathbf{c}_{i_2}}$.

EXAMPLE 4.7. The following vectors form a selforthogonal code C

$$\mathbf{c}_0 = (0,0,0,0,0,0), \mathbf{c}_1 = (0,0,0,0,1,1),$$
$$\mathbf{c}_2 = (1,1,1,1,0,0), \mathbf{c}_3 = (1,1,1,1,1,1).$$

Since $\mathbf{c}_1$ and $\mathbf{c}_2$ form a basis of C we can construct S as $S =< E_{\mathbf{c}_1}, E_{\mathbf{c}_2} >$. In this case, with the help of (4.6), we obtain

$$S = \{E_{\mathbf{c}_0} = I_8, E_{\mathbf{c}_1}, E_{\mathbf{c}_2}, -E_{\mathbf{c}_3}\}.$$

If we use vectors $\mathbf{v}_2, \mathbf{v}_3$ to form a basis of C then as a result we obtain that

$$S = \{E_{\mathbf{c}_0} = I_8, -E_{\mathbf{c}_1}, E_{\mathbf{c}_2}, E_{\mathbf{c}_3}\}.$$

Now using for instance the trivial character of S we can construct an $[[n, n-k]]$ quantum stabilizer code Q_S. Different choices of bases of C lead to Abelian subgroups that differ only by constant factors in front of their operators (see the above example) and do not influence the size and the minimum distance of corresponding quantum codes. Hence different bases of C define equivalent quantum codes. Assuming some particular choice of a basis of C we will denote the corresponding quantum code by Q_C. Thus we established a connection between $[[n, k]]$ quantum stabilizer codes and $[2n, n-k]$ classical binary selforthogonal codes.

For defining the minimum distance of Q_C it is convenient to consider binary codes C and $C^{\perp}$ as codes over $\mathbb{F}_4$. To do this we use the isomorphism between $\mathbb{F}_2^2$ and $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$:

$$(0,0) \Leftrightarrow 0, (1,0) \Leftrightarrow 1, (0,1) \Leftrightarrow \omega, (1,1) \Leftrightarrow \omega^2. \tag{4.10}$$

Let

$$\mathbf{c} = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^{2n}.$$

Using the isomorphism we replace pairs of bits a_i, b_i by elements of $\mathbb{F}_4$ and obtain a vector of length n over $\mathbb{F}_4$. For instance

$$(0,1,0,1,1,1,0,0) \Leftrightarrow (\omega, \omega^2, 0, 1).$$

Let us denote by $\bar{\alpha}$ the conjugated element of $\alpha \in \mathbb{F}_4$, where conjugation is made according to the rule

$$0 \Leftrightarrow 0, 1 \Leftrightarrow 1, \omega \Leftrightarrow \omega^2.$$

For vectors over $\mathbb{F}_4$ we define the trace inner product by

$$\mathbf{a} * \mathbf{b} = \mathrm{tr}_{\mathbb{F}_2}^{\mathbb{F}_4}(\mathbf{a}\bar{\mathbf{b}}) = \mathrm{tr}_{\mathbb{F}_2}^{\mathbb{F}_4}\left(\sum_i a_i \bar{b}_i\right), \ \mathbf{a}, \mathbf{b} \in \mathbb{F}_4^n. \tag{4.11}$$

It is not difficult to check that the trace inner product of vectors over $\mathbb{F}_4$ is equivalent to the symplectic inner product of corresponding binary vectors obtained with the help of (4.10).

Let C be an $[2n, k]$ binary linear code and $\mathcal{C}$ be the code over $\mathbb{F}_4$ obtained from C according to (4.10). Obviously $\mathcal{C}$ is an additive code, i.e. $\mathbf{v} + \mathbf{w} \in \mathcal{C}$ for any $\mathbf{v}, \mathbf{w} \in \mathcal{C}$. If C is selforthogonal with respect to the symplectic inner product (4.8) then $\mathcal{C}$ is selforthogonal with respect to the trace inner product (4.11). Let $\mathcal{C}^{\perp}$ be the dual of $\mathcal{C}$ with respect to (4.11). We can use the code $\mathcal{C}$ for construction of an Abelian group S, similar to how we made it with the help of the code C, and further for construction the quantum code $Q_{\mathcal{C}}$. In this case each codeword $\mathbf{v} \in \mathcal{C}$ will correspond to an operator $E_{\mathbf{v}} \in S$ and each codeword $\mathbf{w} \in \mathcal{C}^{\perp}$ will correspond to an operator $E_{\mathbf{w}} \in S^{\perp}$. Obviously $\mathrm{wt}(\mathbf{v}) = \mathrm{wt}(E_{\mathbf{v}})$ and $\mathrm{wt}(\mathbf{w}) = \mathrm{wt}(E_{\mathbf{w}})$. Thus we have

$$d(Q_{\mathcal{C}}) = \min\{\mathrm{wt}(E) : E \in S^{\perp} \setminus S\} = \min\{\mathrm{wt}(\mathbf{v}) : \mathbf{v} \in \mathcal{C}^{\perp} \setminus \mathcal{C}\}. \tag{4.12}$$

Thus we established a connection between $[[n, k]]$ quantum stabilizer codes and classical codes additive codes over $\mathbb{F}_4$ of length n and size 2^{n-k}.

The connection between quantum stabilizer codes and classical codes allow us to use powerful methods of the classical theory of error correcting codes for construction of quantum codes. Here we consider only one example.

EXAMPLE 4.8. Let us take an $[5, 2]$ MDS code $\mathcal{C}$ over $\mathbb{F}_4$ with the generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

It is easy to check that $\mathcal{C} \subset \mathcal{C}^{\perp}$. Thus we constructed a $[[5, 1, 3]]$ quantum code. This code is optimal since its minimum distance achieves the Singleton bound, which will be derived in Section 5.

4.2. Encoding of Quantum Codes

Let us assume that we have k qubits in a state $\mathbf{u} \in \mathbb{C}^{2^k}$. We can encode $\mathbf{v}$ into a code vector of an $((n, 2^k))$ code Q with the help of the following simple procedure. First we take $n - k$ ancilla qubits each in the ground state $(1, 0)$. The joint state of the ancilla qubits is

$$(1, 0) \otimes (1, 0) \otimes \ldots \otimes (1, 0) = (1, 0, \ldots, 0)$$

and the joint state of all n qubits is

$$\mathbf{u} \otimes (1, 0, \ldots, 0).$$

Vectors $\mathbf{u} \otimes (1, 0, \ldots, 0)$, $\mathbf{u} \in \mathbb{C}^{2^k}$, form a 2^k-dimensional subspace of $\mathbb{C}^{2^n}$. Therefore there exists a unitary transformation U that linearly maps this subspace into the code subspace Q. Since we assume that any unitary rotation can be implemented by a quantum computer the described procedure of encoding is implementable. This procedure is shown in fig.1.

We would like to note that for a generic quantum code this encoding procedure can have very large complexity. Fortunately, in the case of quantum stabilizer code, the encoding can be done with the help of a generator matrix of $\mathcal{C}$. In this case the complexity of encoding is polynomial in the code length. For details see [**CG**].

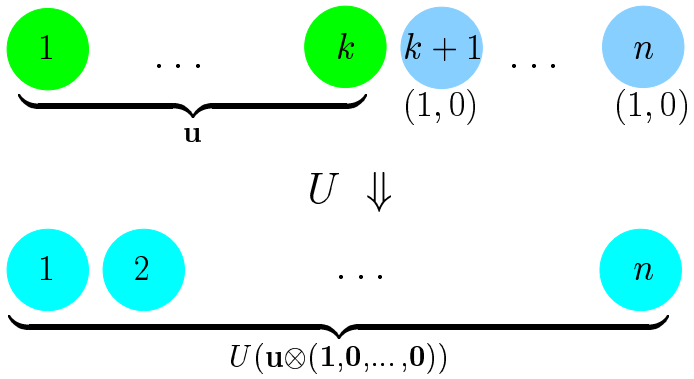


FIGURE 1. Encoding

4.3. Decoding of Quantum Stabilizer Codes

The ML decoding of quantum stabilizer codes resembles the ML decoding of classical linear codes with the help of the standard arrays.

Let $\mathcal{A}$ be the array of cosets of the group $S^\perp$ in $\overline{\mathcal{E}}_n = \mathcal{E}/\mathcal{Z}(\mathcal{E}_n)$. Let us enumerate operators from $\mathcal{E}/\mathcal{Z}(\mathcal{E}_n)$ such that operators $E_0, E_1, \dots, E_{2^{n-k}-1}$ form the group S, operators $E_0, E_1, \dots, E_{2^{n+k}-1}$ form the group $S^\perp$ and the i-th row of $\mathcal{A}$ consists of the operators $E^{(i)}E_j, j = 0, \dots, 2^{n+k}-1$. Clearly, since $S \subseteq S^\perp$, each row of $\mathcal{A}$ consists of 2^{2k} cosets of S. We will denote the i-th coset of $S^\perp$ by $S_i^\perp$, and the j-th coset of S in $S_i^\perp$ by $S_j^{(i)}$. To make notation shorter we denote $r = 2^{n-k}$. The array $\mathcal{A}$ can be visualized with the help of the following picture.

FIGURE 2. The standard array $\mathcal{A}$

$$
\begin{array}{lcccccc}
 & \overbrace{}^{S} & & & & \overbrace{}^{\text{coset } S_{2^{2k}-1}^{(0)} \text{ of } S} & \\
S^\perp: & E_0 & \dots & E_{2^{n-k}-1} & \dots & E_{2^{n+k}-2^{n-k}} & \dots & E_{2^{n+k}-1} \\
 & E^{(1)}E_0 & \dots & E^{(1)}E_{2^{n-k}-1} & \dots & E^{(1)}E_{2^{n+k}-2^{n-k}} & \dots & E^{(1)}E_{2^{n+k}-1} \\
 & E^{(2)}E_0 & \dots & E^{(2)}E_{2^{n-k}-1} & \dots & E^{(2)}E_{2^{n+k}-2^{n-k}} & \dots & E^{(2)}E_{2^{n+k}-1} \\
 & \vdots & & \vdots & & \vdots & & \\
 & \overbrace{}^{\text{coset } S_0^{(i)} \text{ of } S} & & & & \overbrace{}^{\text{coset } S_{2^{2k}-1}^{(i)} \text{ of } S} & \\
\text{coset of } S^\perp: & E^{(i)}E_0 & \dots & E^{(i)}E_{2^{n-k}-1} & \dots & E^{(i)}E_{2^{n+k}-2^{n-k}} & \dots & E^{(i)}E_{2^{n+k}-1} \\
 & \vdots & & \vdots & & \vdots & & \\
 & E^{(r)}E_0 & \dots & E^{(r)}E_{2^{n-k}-1} & \dots & E^{(r)}E_{2^{n+k}-2^{n-k}} & \dots & E^{(1)}E_{2^{n+k}-1}
\end{array}
$$

We still had not defined how to choose leaders $E^{(i)}$ of the cosets of $S^\perp$ in $\mathcal{A}$. Before doing this let us consider how errors from different cosets effect code vectors.

Let us assume that a code vector $\mathbf{v} \in Q$ is corrupted by E' and we receive $\mathbf{w} = E'\mathbf{v}$. We first notice that by (4.6) the operator $E'PE'$ is Hermitian and

idempotent

$$E'PE'E'PE' = E'PPE' = E'PE',$$

and therefore $E'PE'$ is the projection operator on a subspace of dimension

$$\mathrm{Tr}\,(E'PE') = \mathrm{Tr}\,(P) = 2^k.$$

Next we notice that

$$E'PE'E'\mathbf{v} = E'P\mathbf{v} = E'\mathbf{v}$$

and conclude that the vector $E'\mathbf{v}$ belongs to the subspace defined by $E'PE'$. Let E'' be an error operator from the same coset as E'. In this case

$$E'PE'E''\mathbf{v} = E'E'E''P\mathbf{v} = E''\mathbf{v}$$

where the fist equality follows from the fact that $E'E'' \in S^{\perp}$. Thus E'' projects $\mathbf{v}$ to the same subspace as E'. Moreover, if E' and E'' belong to one and the same coset of S, then their action on $\mathbf{v}$ is identical. Indeed, let $E' = EE_i$ and $E'' = EE_j$ for some $E_i, E_j \in S$. Then

$$E'\mathbf{v} = EE_i\mathbf{v} = E\mathbf{v} \text{ and } E''\mathbf{v} = EE_j\mathbf{v} = E\mathbf{v}.$$

Let now E' and E'' be from two different cosets. Then

$$E''PE''E'\mathbf{v} = E''PE''E'P\mathbf{v} = 0.$$

Here the last equality follows from the fact that $E''E' \notin S^{\perp}$ and (4.3).

From these observations it follows that error operators from different cosets of $S^{\perp}$ move code vectors to different orthogonal subspaces, say Q_0, $Q_1, \ldots, Q_{2^{n-k}-1}$, of dimension 2^k. Since the total number of cosets is 2^{n-k} we conclude that these subspaces form a partition of $\mathbb{C}^{2^n}$ and therefore can be used for a von Neumann measurement. The subspace Q_0 obviously coincides with the code space Q.

Now we are in the position to choose coset leaders $E^{(i)}$. As we noticed above error operators from one and the same coset of S have an identical effect on code vectors. Thus in fact we have to choose not individual $E^{(i)}$ among error operators in the i-th coset of $S^{\perp}$, but a leading coset of S among $S_j^{(i)}, j = 0, \ldots, 2^{2k} - 1$. To make this choice we compute

$$p_j = \sum_{E \in S_j^{(i)}} \Pr(E), j = 0, \ldots, 2^{2k} - 1,$$

where $\Pr(E) = (1-p)^{n - \mathrm{wt}\,(E)} p^{\mathrm{wt}\,(E)}$ and p is the error probability of a given completely depolarizing channel. As a leading coset we pick up the coset with the largest p_j. It becomes clear from the following decoding algorithm that this is the optimal choice.

REMARK 4.9. As one can see the choice of a leading coset of S depends on the channel. In fact it is possible to find an example of a quantum stabilizer code so that for different values of p the optimal choices of a leading coset will be different.

An ML decoding for stabilizer codes can be formulated as follows.

Decoding:

1. Make the measurement of $\mathbf{w}$ with respect to the subspaces $Q_0, Q_1, \ldots, Q_{2^{n-k}-1}$. The result of the measurement is the index i of a subspace Q_i to which $\mathbf{w}$ belongs.
2. Take any E from $S_0^{(i)}$.
3. Compute $E\mathbf{w}$.

It is important to note that the measurement that we make on step 1 does not disturb the quantum state $\mathbf{w}$ that we received from the channel, since it is a priory known that $\mathbf{w}$ belongs to one of Q_is and we learn with probability 1 the index of this subspace.

The complexity of this ML decoding algorithm is proportional to 2^{n+k}.

Now we are in position to prove Theorem 3.7 for the case of stabilizer codes.

PROOF. (Theorem 3.7) We first modify the choice of leading cosets of S in $\mathcal{A}$. Namely, we choose $E^{(i)}$ as

$$E^{(i)} = \arg \min_{E \in S_i^{\perp}} \mathrm{wt}\,(E),$$

that is as the minimum weight operator E from $S_i^{\perp}$. We use the same decoding algorithm with this new $\mathcal{A}$.

While this choice of $E^{(i)}$ is not optimal from the point of view of minimization of the probability of decoding error, it helps to prove the theorem. Let us assume that a code vector $\mathbf{v}$ was corrupted by an error operator E with weight $\mathrm{wt}\,(E) \leq \lfloor (d-1)/2 \rfloor$. By the construction of $\mathcal{A}$ it is clear that a decoding error can happen only if $E \in S_j^{(i)}, j > 0$. Again by the construction of $\mathcal{A}$ we have that $S_0^{(i)}$ contains an operator $E', \mathrm{wt}\,(E') \leq \mathrm{wt}\,(E)$. Obviously

$$EE' \in S^{\perp},\ EE' \notin S, \text{ and } \mathrm{wt}\,(E) + \mathrm{wt}\,(E') = \mathrm{wt}\,(EE') < d.$$

Thus we obtain a contradiction with the definition 3.6 of the minimum distance of quantum codes. □

In conclusion of this section we note that the measurement at step 1 of the above decoding algorithm can be efficiently organized with the help of the parity check matrix of code $C^{\perp}$. For details see for example [**NC**, Chapter 10.5.8].

CHAPTER 5

Bounds on Minimum Distance of Quantum Codes

One of the central problems of the classical coding theory is bounding the code minimum distance as a function of the code length and size. Similar questions arise in the quantum case - what is the largest possible d of an $((n, K))$ quantum code and what is the maximum d such that an $((n, K, d))$ code provably exists. This question is not easy to answer even for the case of quantum stabilizer codes. Indeed, thought quantum stabilizer codes are strongly connected to classical codes, we can not just use known bounds on the minimum distance from the classical coding theory. The reason is that the minimum distance of a quantum stabilizer code $Q_{\mathcal{C}}$ according to (4.12) is in fact not a distance, but the minimum weight of the set $\{\mathrm{wt}\,(\mathbf{c}) : \mathbf{c} \in \mathcal{C}^{\perp} \setminus \mathcal{C}\}$. Obviously, the problem becomes even harder in the case of general quantum codes.

The most powerful technique for deriving bounds on minimum distance, covering radius, distance distributions and other parameters of classical codes, is so-called the linear programming, or polynomial method (see [**AB99, AB02, ABL, ABKL, ACKL, AL**] and references over there). In the next sections we will present a generalization of this method for the quantum case.

5.1. Quantum MacWilliams Identities

Let C be a classical linear code over $\mathbb{F}_q$ and A_i be its weight distribution

$$A_i = |\{\mathbf{c} \in C : \mathrm{wt}\,\mathbf{c} = i\}|.$$

Let $C^{\perp}$ be the dual code with weight distribution $A_i^{\perp}$. Let us form polynomials $A(x, y)$ and $A^{\perp}(x, y)$ as follows

$$A(x, y) = \sum_i A_i x^{n-i} y^i \text{ and } A^{\perp}(x, y) = \sum_i A_i^{\perp} x^{n-i} y^i.$$

THEOREM 5.1. *(MacWilliams, 1962)*

$$A^{\perp}(x, y) = \frac{1}{|C|} A(x + (q-1), x - y)$$

COROLLARY 5.2.

$$A_t^{\perp} = \frac{1}{|C|} \sum_{i=0}^{n} A_i \mathcal{K}_t(i), t = 0, \ldots n. \tag{5.1}$$

Here

$$\mathcal{K}_t(i) = \sum_{j=0}^{t} (-q)^j (q-1)^{t-j} \binom{n-j}{t-j} \binom{i}{j}$$

are Krawtchouk polynomials.

Since $A_i^{\perp} \geq 0$, it follows from (5.1) that

$$\frac{1}{|C|}\sum_{i=0}^{n} A_i \mathcal{K}_t(i) \geq 0, t = 0, \ldots n. \tag{5.2}$$

This set of linear inequalities, called the Delsarte inequalities, gives us a powerful method for estimating different combinatorial and probabilistic parameters of classical codes.

It looks far-away nontrivial to generalize this method for quantum codes. Indeed, it is not easy to define even the notion of weight distribution in the quantum case. The breakthrough in this direction was made by P. Shor and R. Laflamme [**SL**].

Let Q be a quantum code defined by an orthogonal projection P. P. Shor and R. Laflamme suggested to define two weight enumerators for Q.

DEFINITION 5.3.

$$B_i(Q) := \frac{1}{K^2}\sum_{\mathrm{wt}\,(E)=i} \mathrm{Tr}\,(EP)^2;\ B_i^{\perp}(Q) := \frac{1}{K}\sum_{\mathrm{wt}\,(E)=i} \mathrm{Tr}\,(EPEP)$$

Similar to the classical case we can define two polynomials

$$B(x,y) = \sum_t B_i x^{n-t} y^t \text{ and } B^{\perp}(x,y) = \sum_t B_i^{\perp} x^{n-t} y^t.$$

The following theorems prove several important properties of the quantum enumerators B_i and $B_i^{\perp}$. These theorems are due to [**SL**]. In the presented proofs we follow mostly to [**K**].

THEOREM 5.4.

B_i and $B_i^{\perp}$ are real

PROOF. E are Hermitian and P is also Hermitian. Hence

$$(PEP)^{\dagger} = P^{\dagger}E^{\dagger}P^{\dagger} = PEP$$

is also Hermitian. Eigenvalues of Hermitian operators are real. Hence

$$\mathrm{Tr}\,(EP) = \mathrm{Tr}\,(EPP) = \mathrm{Tr}\,(PEP)$$

are real. Similarly $(PEP)(PEP)$ is Hermitian and therefore

$$\mathrm{Tr}\,(E(PEP)) = \mathrm{Tr}\,((PEP)(PEP))$$

are real. □

THEOREM 5.5. *(Quantum MacWilliams Identities)*

$$B(x,y) = \frac{1}{2^n K} B^{\perp}(x+3y, x-y). \tag{5.3}$$

PROOF.

$$B(x,y) = \frac{1}{K^2}\sum_t x^{n-t}y^t B_t = \frac{1}{K^2}\sum_t x^{n-t}y^t \sum_{\mathrm{wt}\,(E)=t} \mathrm{Tr}\,(EP)^2$$

$$= \frac{1}{K^2}\sum_{t=0}^{n} x^{n-t}y^t \sum_{\mathrm{wt}\,(E)=t}\sum_{i,j,k,l} p_{j,i}p_{l,k}e_{i,j}e_{k,l}$$

$$= \frac{1}{K^2}\sum_E x^{n-\mathrm{wt}\,(E)}y^{\mathrm{wt}\,(E)}\sum_{i,j,k,l} p_{j,i}p_{l,k}e_{i,j}e_{k,l}$$

$$= \frac{1}{K^2}\sum_{i,j,k,l} p_{j,i}p_{l,k}\sum_E e_{i,j}e_{k,l}x^{n-\mathrm{wt}\,(E)}y^{\mathrm{wt}\,(E)}.$$

We will need the following well known facts

$$E = e^{(n-1)}\otimes e^{(n-2)}\otimes\ldots\otimes e^{(0)}$$

$$i = i_0 + 2i_1 + \ldots + 2^{n-1}i_{n-1};\ j = j_0 + 2j_1 + \ldots + 2^{n-1}j_{n-1}$$

$$e_{i,j} = e^{(0)}_{i_0,j_0}e^{(1)}_{i_1,j_1}\ldots e^{(n-1)}_{i_{n-1},j_{n-1}} \tag{5.4}$$

$$\begin{aligned} & a_0b_0c_0 + a_0b_0c_1 + a_0b_1c_0 + a_0b_1c_1 + a_1b_0c_0 + a_1b_0c_1 + a_1b_1c_0 + a_1b_1c_1 \\ = \ & (a_0+a_1)(b_0+a_1)(b_0+b_1) \end{aligned} \tag{5.5}$$

$$\begin{aligned} B(x,y) \ = \ & \frac{1}{K^2}\sum_{i,j,k,l} p_{j,i}p_{l,k}\prod_{t=0}^{n-1}\{x(I_2)_{i_t,j_t}(I_2)_{k_t,l_t} \\ & + y\left[(\sigma_x)_{i_t,j_t}(\sigma_x)_{k_t,l_t} + (\sigma_y)_{i_t,j_t}(\sigma_y)_{k_t,l_t} + (\sigma_z)_{i_t,j_t}(\sigma_z)_{k_t,l_t}\right]\}. \end{aligned}$$

By the same method, we have

$$\begin{aligned} B^{\perp}(x,y) \ = \ & \frac{1}{K}\sum_{i,j,k,l} p_{j,i}p_{l,k}\prod_{t=0}^{n-1}\{x(I_2)_{i_t,l_t}(I_2)_{k_t,j_t} \\ & + y\left[(\sigma_x)_{i_t,l_t}(\sigma_x)_{k_t,j_t} + (\sigma_y)_{i_t,l_t}(\sigma_y)_{k_t,j_t} + (\sigma_z)_{i_t,l_t}(\sigma_z)_{k_t,j_t}\right]\}. \end{aligned}$$

Denote

$$\begin{aligned} & b_{i_t,j_t,k_t,l_t}(x,y) = x(I_2)_{i_t,j_t}(I_2)_{k_t,l_t} \\ + \ & y\left[(\sigma_x)_{i_t,j_t}(\sigma_x)_{k_t,l_t} + (\sigma_y)_{i_t,j_t}(\sigma_y)_{k_t,l_t} + (\sigma_z)_{i_t,j_t}(\sigma_z)_{k_t,l_t}\right] \end{aligned}$$

and

$$\begin{aligned} & b^{\perp}_{i_t,j_t,k_t,l_t}(x,y) = x(I_2)_{i_t,l_t}(I_2)_{k_t,j_t} \\ + \ & y\left[(\sigma_x)_{i_t,l_t}(\sigma_x)_{k_t,j_t} + (\sigma_y)_{i_t,l_t}(\sigma_y)_{k_t,j_t} + (\sigma_z)_{i_t,l_t}(\sigma_z)_{k_t,j_t}\right]. \end{aligned}$$

To see that

$$b_{i_t,j_t,k_t,l_t}(x,y) = b^{\perp}_{i_t,j_t,k_t,l_t}\left(\frac{x+3y}{2},\frac{x-y}{2}\right). \tag{5.6}$$

one can check all 16 possibilities for binary i_t, j_t, k_t, l_t For instance if $i_t = 0, j_t = 0, k_t = 1$, and $l_t = 1$, we have

$$b_{i_t,j_t,k_t,l_t}(x,y) = x - y,$$

$$b^{\perp}_{i_t,j_t,k_t,l_t}(x,y) = 2y,$$

in compliance with (5.6). □

$$B_i(Q) := \frac{1}{K^2} \sum_{\text{wt }(E)=i} \text{Tr}\,(EP)^2;\ B_i^{\perp}(Q) := \frac{1}{K} \sum_{\text{wt }(E)=i} \text{Tr}\,(EPEP)$$

THEOREM 5.6. *Let Q be a quantum code with enumerators B_i and $B_i^{\perp}$. Then*

i) $B_i^{\perp} \geq B_i \geq 0$, for $i = 0, 1, \ldots, n$, and $B_0 = B_0^{\perp} = 1$,

ii) if t is the largest integer such that $B_i = B_i^{\perp}, i \leq t$, then the minimum distance of Q equals $t + 1$.

PROOF. From $P^2 = P$ and $\text{Tr}(P) = K$, it follows that $B_0 = B_0^{\perp} = 1$. B_i are sums of squares and hence they are nonnegative. Using the matrix form of the Schwartz inequality,

$$\text{Tr}^2(A^{\dagger}B) \leq \text{Tr}(A^{\dagger}A)\text{Tr}(B^{\dagger}B),$$

we get

$$\text{Tr}^2(EP) = \text{Tr}^2((PEP)P) \leq \text{Tr}((PEP)(PEP))\text{Tr}(PP) \tag{5.7}$$

$$= \text{Tr}(PEPE)\text{Tr}(P) = K\text{Tr}(PEPE).$$

This yields $B_i^{\perp} \geq B_i$. The equality holds in (5.7) iff $PEP = c_E P$, for some c_E, or equivalently iff E is detectable. Hence

$$B_i = B_i^{\perp} \ \Leftrightarrow \ \text{all errors of weight } i \text{ are detectable.}$$

□

Note that substituting $x = 1, y = 0$ into

$$B(x,y) = \frac{1}{2^n K} B^{\perp}(x + 3y, x - y)$$

we obtain

$$B(1,0) = \sum_{i=0}^{n} B_i 1^{n-i} 0^i = \frac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} 1^{n-i} 1^i$$

$$B_0 = \frac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp}$$

$$1 = \frac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp}$$

Thus

$$K = \frac{1}{2^n} \sum_{i=0}^{n} B_i^{\perp}. \tag{5.8}$$

5.1.1. Properties of Krawtchouk Polynomials. Before proceeding with deriving bounds on the minimum distance of quantum codes will overview main properties of Quaternary Krawtchouk Polynomials. The Krawtchouk polynomials have the following generating function

$$\sum_{i=0}^{n} \mathcal{K}_i(x) z^i = (1+3z)^{n-x}(1-z)^x \quad (x \text{ integer}) \tag{5.9}$$

The Krawtchouk polynomials are orthogonal

$$\sum_{i=0}^{n} \mathcal{K}_r(i)\mathcal{K}_i(s) = 4^n \delta_{r,s}. \tag{5.10}$$

A symmetry relation is satisfied by the polynomials

$$3^i \binom{n}{i} \mathcal{K}_s(i) = 3^s \binom{n}{s} \mathcal{K}_i(s). \tag{5.11}$$

Every polynomial of degree at most n has the unique expansion in the basis of Krawtchouk polynomials. If a polynomial $f(x)$ has the expansion

$$f(x) = \sum_{i=0}^{t} f_i \mathcal{K}_i(x),$$

then

$$f_i = 4^{-n} \sum_{j=0}^{n} f(j)\mathcal{K}_j(i).$$

The following property holds:

$$\sum_{i=0}^{n} \binom{n-i}{n-j} \mathcal{K}_i(x) = 4^j \binom{n-x}{j}. \tag{5.12}$$

The Christoffel-Darboux formula is of importance:

$$\mathcal{K}_{t+1}(x)\mathcal{K}_t(a) - \mathcal{K}_t(x)\mathcal{K}_{t+1}(a) = \frac{4(a-x)}{t+1} 3^t \binom{n}{t} \sum_{i=0}^{t} \frac{\mathcal{K}_i(x)\mathcal{K}_i(a)}{3^i \binom{n}{i}}. \tag{5.13}$$

The Krawtchouk polynomials satisfy a recurrence relation,

$$(i+1)\mathcal{K}_{i+1}(x) = (3n - 2i - 4x)\mathcal{K}_i(x) - 3(n-i+1)\mathcal{K}_{i-1}(x). \tag{5.14}$$

Some useful values of the Krawtchouk polynomials:

$$\mathcal{K}_0(x) = 1,\ \mathcal{K}_1(x) = 3n - 4x,\ 2\mathcal{K}_2(x) = 16x^2 - 8x(3n-1) + 9n(n-1),$$

$$\mathcal{K}_i(0) = 3^i \binom{n}{i}.$$

We will also need a result on asymptotic behavior of the smallest root r_t of $\mathcal{K}_t(j)$. For t growing linearly in n and $\tau = t/n$

$$\xi_t = \frac{r_t}{n} = \frac{3}{4} - \frac{1}{2}\tau - \frac{1}{2}\sqrt{3\tau(1-\tau)} + o(1). \tag{5.15}$$

Remark All over the paper $o(1)$ tends to 0 as n grows.

5.2. Upper Bounds on Minimum Distance of Quantum Codes

In this section we follow results obtained in [**AL**].

The following key theorem gives a general method for deriving bounds on the quantum minimum distance.

THEOREM 5.7. *Let Q be an $((n, K))$ quantum code of minimum distance d. Let*

$$f(x) = \sum_{i=0}^{n} f_i \mathcal{K}_i(x)$$

be a polynomial satisfying the conditions

i) $f_i \geq 0$,
ii) $f(x) > 0$ *for* $x = 0, \ldots, d-1$, *and*
iii) $f(x) \leq 0$ *for* $x = w, \ldots, n$.

Then

$$K \leq \frac{1}{2^n} \max_{j=0,\ldots,d-1} \frac{f(j)}{f_j}.$$

We can reformulate Theorem 5.5 as follows.

COROLLARY 5.8. *For* $t = 0, \ldots, n$,

$$B_t = \frac{1}{2^n K} \sum_{i=0}^{n} B_i^{\perp} \mathcal{K}_t(i).$$

PROOF. (Theorem 5.7) Let Q be an $((n, K, d))$ quantum code with enumerators B_i and $B_i^{\perp}$. Denote $S = 2^n K$. Then using Corollary 5.8 and Theorem 5.6, we get

$$\begin{aligned} S\sum_{i=0}^{d-1} f_i B_i &\leq S\sum_{i=0}^{n} f_i B_i \\ &= S\sum_{i=0}^{n} \frac{1}{S} f_i \sum_{j=0}^{n} B_j^{\perp} \mathcal{K}_i(j) = \sum_{j=0}^{n} B_j^{\perp} \sum_{i=0}^{n} f_i \mathcal{K}_i(j) \\ &= \sum_{j=0}^{n} f(j) B_j^{\perp} \leq \sum_{j=0}^{d-1} f(j) B_j^{\perp} = \sum_{j=0}^{d-1} f(j) B_j. \end{aligned}$$

Thus,

$$S \leq \frac{\sum_{j=0}^{d-1} f(j) B_j}{\sum_{j=0}^{d-1} f_j B_j} \leq \max_{j=0,\ldots,d-1} \frac{f(j)}{f_j}.$$

□

Now choosing polynomials $f(x)$ that satisfy conditions of Theorem 5.7, we can derive bounds on the quantum minimum distance. Below present some useful choices of $f(x)$.

We start with choosing the polynomial $f(x)$ that gives the Singleton bound on the minimum distance of classical codes. For this reason we will call the corresponding quantum bound the Singleton type bound.

THEOREM 5.9. *(Singleton type bound) In every $((n, K))$ quantum code of minimum distance d,*

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

PROOF. Choose

$$f(x) = 4^{n-d+1} \prod_{j=d}^{n} \left(1 - \frac{x}{j}\right) = 4^{n-d+1} \frac{\binom{n-x}{n-d+1}}{\binom{n}{d-1}}.$$

Then using (5.12), we get

$$f_x = 4^{-n} \sum_{j=0}^{n} f(j)\mathcal{K}_j(x) = 4^{-d+1} \sum_{j=0}^{n} \frac{\binom{n-j}{n-d+1}}{\binom{n}{d-1}} \mathcal{K}_j(x) = \frac{\binom{n-x}{d-1}}{\binom{n}{d-1}}.$$

Now,

$$r(x) = \frac{f(x)}{f_x} = 4^{n-d+1} \frac{\binom{n-x}{n-d+1}}{\binom{n-x}{d-1}}.$$

Considering the ratio

$$\begin{aligned} \frac{r(x)}{r(x+1)} &= \frac{\binom{n-x}{n-d+1}}{\binom{n-x}{d-1}} \times \frac{\binom{n-x-1}{d-1}}{\binom{n-x-1}{n-d+1}} \\ &= \frac{n-x-d+1}{d-x-1}, \end{aligned}$$

we find that it is greater than 1 if $d \leq (n+2)/2$. Note that it is enough for our purposes, since for $d = (n+2)/2$ we have

$$K \leq \frac{f(0)}{f_0} = 1.$$

□

Our next choice is the polynomial $f(x)$ that gives the classical Hamming (or Spherical Packing) bound. Let $e = \lfloor \frac{d-1}{2} \rfloor$. Define

$$f_i = (\mathcal{K}_e(i))^2 \text{ and } f(x) = \sum_{i=0}^{n} f_i \mathcal{K}_i(x).$$

It is well known [**MRRW**, eq. A.19] that product of binary Krawtchouk polynomial $\mathcal{K}_i(x)\mathcal{K}_j(x)$ can be represented as a linear combination of the binary Krawtchouk polynomial $\mathcal{K}_k(x)$. It is not difficult to derive the generalization of this result for the quaternary case.

LEMMA 5.10.

$$\mathcal{K}_i(x)\mathcal{K}_j(x)$$

$$= \sum_{k=0}^{n} \mathcal{K}_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-i-j} \binom{n-k}{s} \binom{2k+2s-i-j}{k+s-j} 2^{i+j-2s-k} 3^s.$$

Using the lemma, we obtain

$$f_x = \sum_{k=0}^{n} \mathcal{K}_k(x) \sum_{s=0}^{n-k} \binom{k}{2k+2s-2e} \binom{n-k}{s} \binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s.$$

This yields

$$\begin{aligned} f(x) &= \sum_{j=0}^{n} f_j \mathcal{K}_j(x) \\ &= \sum_{j=0}^{n}\sum_{k=0}^{n}\sum_{s=0}^{n-k} \binom{k}{2k+2s-2e}\binom{n-k}{s}\binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s \mathcal{K}_k(j)\mathcal{K}_j(x) \\ &= \sum_{k=0}^{n}\sum_{s=0}^{n-k} \binom{k}{2k+2s-2e}\binom{n-k}{s}\binom{2k+2s-2e}{k+s-e} 2^{2e-2s-k} 3^s \sum_{j=0}^{n} \mathcal{K}_k(j)\mathcal{K}_j(x) \\ &= 4^n \sum_{s=\max\{0,e-x\}}^{e-x/2} \binom{x}{2x+2s-2e}\binom{n-x}{s}\binom{2x+2s-2e}{x+s-e} 2^{2e-2s-x} 3^s, \end{aligned}$$

where on the last step we use (5.10). Taking into account that

$$\frac{1}{n}\log\binom{n}{k} = H\left(\frac{k}{n}\right) + O\left(\frac{1}{n}\right),$$

and denoting $\xi = x/n, \nu = s/n$, and $\tau = e/n$, we get

$$\frac{1}{n}\log\left[\binom{x}{2x+2s-2e}\binom{n-x}{s}\binom{2x+2s-2e}{x+s-e} 2^{2e-2s-x} 3^s\right]$$

$$= \xi H\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) + (1-\xi)H\left(\frac{\nu}{1-\xi}\right) + \nu\log 3 + \xi + O\left(\frac{1}{n}\right).$$

Taking derivative in ν of the last expression, we get

$$\begin{aligned} &2\log\left(1-\frac{2\xi+2\nu-2\tau}{\xi}\right) - 2\log\left(\frac{2\xi+2\nu-2\tau}{\xi}\right) \\ &\quad + \log\left(1-\frac{\nu}{1-\xi}\right) - \log\left(\frac{\nu}{1-\xi}\right) + \log 3. \end{aligned} \tag{5.16}$$

This function has only one root on the interval that we are interested. Denoting the root by $\alpha(\tau,\xi)$, we obtain

$$\begin{aligned} \frac{1}{n}\log f(x) &= 2 + \xi + \xi H\left(\frac{2\xi+2\alpha(\tau,\xi)-2\tau}{\xi}\right) \\ &\quad + (1-\xi)H\left(\frac{\alpha(\tau,\xi)}{1-\xi}\right) + \alpha(\tau,\xi)\log 3 + O\left(\frac{1}{n}\right). \end{aligned} \tag{5.17}$$

In a similar way we can find an asymptotic expression for $\frac{1}{n}\log f_j$. Finally we obtain

$$\begin{aligned}
\frac{\log K}{n} &\leq \max_{0\leq\xi\leq 2\tau}\left\{\frac{1}{n}\log f(\xi n) - \frac{1}{n}\log f_{\xi n}\right\} \\
&= \max_{0\leq\xi\leq 2\tau}\left\{1+\xi+\xi H\left(\frac{2\xi+2\alpha(\tau,\xi)-2\tau}{\xi}\right)\right. \\
&+ (1-\xi)H\left(\frac{\alpha(\tau,\xi)}{1-\xi}\right) + \alpha(\tau,\xi)\log 3 - 2\tau\log 3 - 2H(\tau) \\
&- \left. 2\int_0^{\xi}\log\left(\frac{3-2z-4\tau+\sqrt{(3-2z-4\tau)^2-12z(1-z)}}{6-6z}\right)dz\right\} + o(1).
\end{aligned}$$

Computations with Maple show that this function achieves its maximum at $\xi = 0$ for any $\delta \leq \xi_e$.

If $0 \leq \delta \leq (9-3\sqrt{2})/14$ then $\delta \leq \xi_e$. E. Rains showed that $\delta \leq 1/3$ when $\log(K)/n \geq 0$. Since $(9-3\sqrt{2})/14 > 1/3$, the conventional Hamming bound is valid in the interval $0 \leq \delta \leq 1/3$.

COROLLARY 5.11. *The conventional Hamming (Spherical Packing) bound is valid for quantum codes, i.e. if Q is an $((n,K))$ quantum code then*

$$\frac{\log K}{n} \leq 1 - \frac{\delta}{2}\log 3 - H\left(\frac{\delta}{2}\right) + o(1).$$

The Hamming type bound can be improved for low rate $R = \log_2 K/n$ quantum $((n,K))$ codes. Define

$$f(x) = \frac{1}{a-x}\left\{\mathcal{K}_{t+1}(x)\mathcal{K}_t(a) - \mathcal{K}_t(x)\mathcal{K}_{t+1}(a)\right\}^2.$$

This polynomial yields the linear programming bound of the first form (LP1) for classical codes [**MRRW**]. Omitting computations we obtain the theorem.

THEOREM 5.12. *If $0 \leq \delta \leq 0.3152$ then the conventional first linear programming bound is valid for quantum codes, i.e. if Q is an $((n,K))$ quantum code then*

$$\frac{\log K}{n} \leq H\left(\frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}\right) + \left(\frac{3}{4} - \frac{1}{2}\delta - \frac{1}{2}\sqrt{3\delta(1-\delta)}\right)\log 3 - 1 + o(1).$$

5.2.1. Strengthening in the linear case. As we showed in the previous sections a quantum $[[n,k]]$ stabilizer code $Q_{\mathcal{C}}$ is associated with classical additive codes $\mathcal{C}$ and $\mathcal{C}^{\perp}$ over $\mathbb{F}_4$. If the code $\mathcal{C}$ is linear, i.e.

$$\alpha\mathbf{v}_1 + \beta\mathbf{v}_2 \in \mathcal{C}, \text{ for any } \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{C} \text{ and } \alpha, \beta \in \mathbb{F}_4,$$

then we will say that $Q_{\mathcal{C}}$ is linear. As the following theorem shows we can further improve linear programming bounds on some interval for linear quantum codes.

LEMMA 5.13. *Let Q be an $[[n,k]]$ liner quantum code. Then the minimum distance of Q is at most the minimum distance of an $[(n+k)/2,k]$ classical linear code over $GF(4)$.*

Proof Let

$$G_C = \left[\begin{array}{cc} I_{\frac{n-k}{2}} & A \end{array}\right]$$

be a generator matrix of the code C. Since $C \subseteq C^{\perp}$ a generator matrix of $C^{\perp}$ can put into the following form

$$G_{C^{\perp}} = \begin{bmatrix} G_C \\ G' \end{bmatrix} = \begin{bmatrix} I_{\frac{n-k}{2}} & A \\ G'_1 & G'_2 \end{bmatrix}$$

Let C' be the code generated by the matrix G'. It is clear that the minimum distance of C' satisfies

$$d(C') \geq \min\{\mathrm{wt}(\mathbf{c}) : \mathbf{c} \in C^{\perp} \setminus C\} = d(Q).$$

$$G_{C^{\perp}} = \begin{bmatrix} G_C \\ G' \end{bmatrix} = \begin{bmatrix} I_{\frac{n-k}{2}} & A \\ G'_1 & G'_2 \end{bmatrix}$$

Using Gaussian elimination, we can force the elements of G' in the first $\frac{n-k}{2}$ positions to be 0. In this case C' is an $[(n+k)/2, k]$ linear code over GF(4). □

Applying any classical bound for the minimum distance of C' we obtain a bound on the quantum code.

On fig.1 we present several upper and a lower bound on the relative minimum distance of quantum codes as functions of the code rate $R = \log_2(K)/n$ as n tends to infinity.

The bound LP2 is is a bound that would correspond to the so-called classical linear programming bound of the second form. It is still not proven for quantum codes, though we conjecture that it is a valid bound. Being proven the LP2 bound would make improvement over all currently known upper bounds. The Rains Threshold bound is a bound for the case when the code rate R tends to zero. It says that any quantum code can not correct more than $1/6n$ errors. The existence bound will be considered in the next section.

5.3. Lower Bound on the Minimum Distance

The classical Gilbert-Varshamov bound claims that there exists an $[n, k]$ linear code over $\mathbb{F}_q$ whose minimum distance is the largest integer d that satisfies

$$1 + (q-1)\binom{n-1}{1} + \ldots + (q-1)^{d-2}\binom{n-1}{d-2} < q^{n-k}.$$

In asymptotics, as n tends to infinity, we obtain that there exists a linear code with the code rate

$$R \geq 1 - H_q(\delta), \tag{5.18}$$

where $\delta = d/n$ and

$$H_q(x) = -x\log_q(x) - (1-x)\log_q(1-x) + x\log_q(q-1) \tag{5.19}$$

is the q-ary entropy function. In this section we are going to prove a similar result for quantum stabilizer codes.

The minimum distance of a quantum stabilizer code $Q_{\mathcal{C}}$ is greater than or equal to the minimum distance of the associated code $\mathcal{C}^{\perp}$ over $\mathbb{F}_4$. Below we prove that there exists a linear code $\mathcal{C}^{\perp}$ over $\mathbb{F}_4$ such that it meets the Gilbert-Varshamov bound (5.18) and has the property that $\mathcal{C} \subseteq \mathcal{C}^{\perp}$. In fact we will prove an even stronger result - we will derive upper bounds on the quantum weight enumerators B_i and $B_i^{\perp}$. In this section we follow results from [**ABKL**].

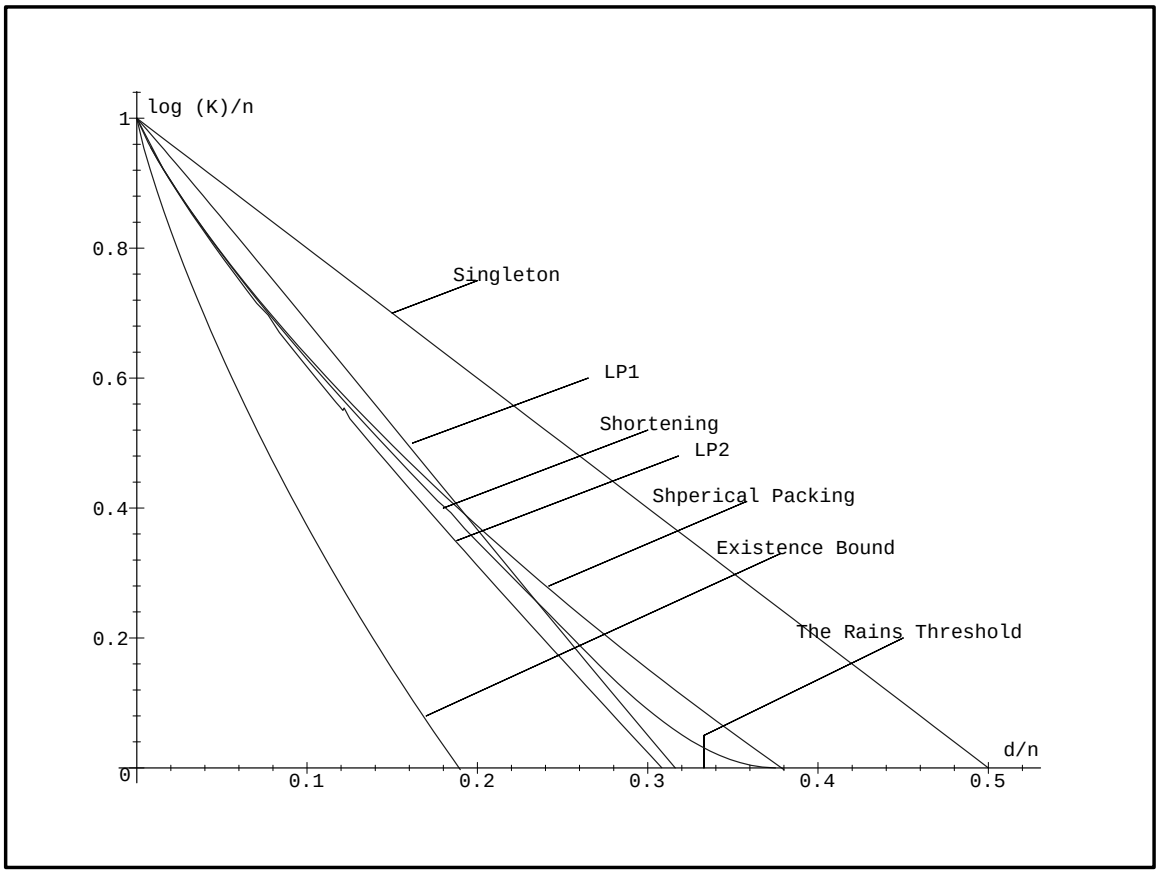


FIGURE 1. Upper and Lower Bounds on Quantum Minimum Distance

A classical code is called even if all its code vectors have even weights. It is proven in [**MOS**] that any $[n,k], k \leq n/2$, even code $\mathcal{C}$ over $\mathbb{F}_4$ is selforthogonal and therefore can be used for construction of a quantum stabilizer code.

Let

$$\mathcal{S}_{n,k} = \{\mathcal{C} \subset \mathbb{F}_4^n \mid \mathcal{C} \text{ even linear code}, \dim \mathcal{C} = k\}$$
$$\mathcal{S}_{n,k}^{\perp} = \{\mathcal{C} \subset \mathbb{F}_4^n \mid \mathcal{C}^{\perp} \in \mathcal{S}_{n,k}\},$$

where $k \leq n/2$. .

Below we use the following three results from [**MOS**].

LEMMA 5.14. *Let $\mathcal{C} \subset \mathbb{F}_4^n$ be an even linear code and $\mathcal{C}^{\perp}$ be its dual. Then the number of even-weight code vectors in $\mathcal{C}^{\perp}$ equals $\frac{1}{2}(4^{n-k} + (-2)^n)$.*

LEMMA 5.15. *Let $\mathcal{C} \subset \mathbb{F}_4^n$ be an even linear code and $\mathcal{C}^{\perp}$ be its dual. If $\mathbf{a} \in \mathcal{C}^{\perp}$ has even (odd) weight then the coset $\mathcal{C} + \mathbf{a}$ is formed by vectors of even (odd) weight.*

Existence of codes with bounded distance distribution will follow from the following lemma, based on Lemmas 5.14-5.15.

LEMMA 5.16. *Let $\mathbf{v} \in \mathbb{F}_4^n$ be any even-weight vector. The number of codes from $\mathcal{S}$ containing $\mathbf{v}$ does not depend on $\mathbf{v}$.*

PROOF. Let us count the number of linear $[n,k]$ codes containing $\mathbf{v}$. Let $\mathcal{C}_1 = \langle \mathbf{v} \rangle$ be the $[n,1]$ code and $\mathbf{w}$ an even-weight vector distinct from $\mathbf{v}$ such that $(\mathbf{w},\mathbf{v}) = 0$. By Lemma 5.15 all the cosets $\mathcal{C}_1 + \alpha\mathbf{w}, \alpha \in F$, are even; so by adjoining $\mathbf{w}$ we obtain an even $[n,2]$ code $\mathcal{C}_2$. By Lemma 5.14 this can be done in

$$\frac{1}{4}\Big[\frac{1}{2}\Big(4^{n-1} + (-2)^n\Big) - 1\Big]$$

ways independent of $\mathbf{v}$. Similarly $\mathcal{C}_2$ can be extended to an even $[n,3]$ code in

$$\frac{1}{16}\Big[\frac{1}{2}\Big(4^{n-2} + (-2)^n\Big) - 1\Big]$$

ways. Continuing in this manner, we obtain all even $[n,k]$ codes that contain $\mathbf{v}$. It is obvious that their number does not depend on a particular choice of $\mathbf{v}$. □

THEOREM 5.17. *The family $\mathcal{S}_{n,k}$ of even $[n,k]$ codes contains a code $\mathcal{C}$ with weight distribution $B_i(\mathcal{C}) \leq n^2 \tilde{B}_i$, $1 \leq i \leq n$, where*

$$\tilde{B}_i = \frac{4^k - 1}{\frac{1}{2}\Big(4^{n-1} + (-2)^n\Big) - 1}\binom{n}{i}3^i$$

is the average weight distribution of codes in $\mathcal{S}_{n,k}$.

PROOF. Let $N = |\mathcal{S}_{n,k}|$. By Lemma 5.16 every even vector $\mathbf{v}$ is contained in one and the same number, say L, of codes from $\mathcal{S}_{n,k}$. So computing the total number of all vectors in codes from $\mathcal{S}_{n,k}$ in two ways, we get

$$N + \Big(\frac{1}{2}\Big(4^{n-1} + (-2)^n\Big) - 1\Big)L = 4^k N,$$

or

$$N = L\frac{\frac{1}{2}\Big(4^{n-1} + (-2)^n\Big) - 1}{4^k - 1}.$$

Let $B_i(\mathcal{C}_j)$ be the number of code vectors of weight i in the j-th code from $\mathcal{S}_{n,k}$. Then we have

$$\sum_{j=1}^{N} B_i(j) = \binom{n}{i}3^i L.$$

Hence the average over $\mathcal{S}_{n,k}$ number of codewords of weight i is $\frac{L}{N}\binom{n}{i}3^i = \tilde{B}_i$, as claimed. The number of codes $\mathcal{C} \in \mathcal{S}_{n,k}$ such that $B_i(\mathcal{C}) \geq n^2\tilde{B}_i$ for a given i is not greater than

$$\frac{\sum_{j=1}^{N} B_i(\mathcal{C}_j)}{n^2\tilde{B}_i} = \frac{L}{n^2}\frac{\frac{1}{2}\Big(4^{n-1} + (-2)^n\Big) - 1}{4^k - 1} = \frac{1}{n^2}N.$$

Hence the number of codes $\mathcal{C}$ such that $B_i(\mathcal{C}) \leq n^2\tilde{B}_i$ for all $1 \leq i \leq n$ is at least

$$N - \frac{N}{n} = N\Big(1 - \frac{1}{n}\Big).$$

To finish the proof we note that

$$\frac{1}{n}\log n^2\tilde{B}_i = R - 1 + H_4\Big(\frac{i}{n}\Big) + o(1).$$

□

Now let us use this result to prove that the family $\mathcal{S}_{n,k}^{\perp}$ also contains codes whose weight distribution is bounded above by a polynomial factor times the average weight distribution in $\mathcal{S}_{n,k}^{\perp}$. In this part we rely on the MacWilliams identities. We will need the following lemma.

LEMMA 5.18. *Let n be an even integer. Then*

$$\sum_{i=0}^{n/2}\binom{n}{2i}3^{2i}K_t(4;2i) = 2^{n-1}\binom{n}{t}(-3)^t.$$

PROOF. By (5.9), the sum $\sum_{i=0}^{n/2}\binom{n}{2i}3^{2i}K_r(4;2i)K_s(4;2i)$ is the coefficient of $y^r z^s$ in

$$\begin{aligned}
&\sum_{i=0}^{n/2}\binom{n}{2i}3^{2i}(1+3y)^{n-2i}(1-y)^{2i}(1+3z)^{n-2i}(1-z)^{2i} \\
&\qquad = \frac{1}{2}\Big([(1+3y)(1+3z)+3(1-y)(1-z)]^n \\
&\qquad\qquad + [(1+3y)(1+3z)-3(1-y)(1-z)]^n\Big) \\
&\qquad = \frac{1}{2}\Big([4+12yz]^n + 2^n[-1+3(y+z)+3yz]^n\Big). \qquad (5.20)
\end{aligned}$$

It is clear that the first term in (5.20) contributes only to coefficients of $y^r z^r$. Consider the second term:

$$2^n[-1+3(y+z)+3yz]^n = 2^n\sum_{i=0}^{n}\binom{n}{i}3^{n-i}y^{n-i}z^{n-i}(3(y+z)-1)^i \qquad (5.21)$$

Since we are interested only in the coefficient $y^0 z^t$, in the sum (5.21) we put $i = n$. This gives

$$\begin{aligned}
2^n(3(y+z)-1)^n &= 2^n\sum_{i=0}^{n}\binom{n}{i}(-3)^i\sum_{j=0}^{i}\binom{i}{j}y^j z^{i-j} \\
&= 2^n\sum_{j=0}^{n}y^j\sum_{i=0}^{n}\binom{n}{i}\binom{i}{j}(-3)^i z^{i-j}
\end{aligned}$$

The coefficient of $y^0 z^t$ in this sum equals $2^n\binom{n}{t}(-3)^t$. □

THEOREM 5.19. *In $\mathcal{S}_{n,k}^{\perp}$ there exists a code $\mathcal{C}$ with $B_i^{\perp} \leq n^2 \tilde{B}_i^{\perp}$, $1 \leq i \leq n$, where*

$$\tilde{B}_i^{\perp} = \frac{1}{4^k}\binom{n}{i}3^i\Big(1 + \frac{((-1)^i 2^{n-1} - 1)(4^k - 1)}{\frac{1}{2}(4^{n-1} + (-2)^n) - 1}\Big) \tag{5.22}$$

is the average weight distribution of codes in $\mathcal{S}_{n,k}^{\perp}$.

PROOF. As in Theorem 5.17, it suffices to compute the average. Using the MacWilliams identities and the fact that $|\mathcal{S}_{n,k}^{\perp}| = |\mathcal{S}_{n,k}|$, we have, for a given t,

$$\begin{aligned}
\sum_{j=1}^{N} B_t^{\perp}(\mathcal{C}_j^{\perp}) &= \frac{1}{4^k}\sum_{j=1}^{N}\sum_{i=0}^{n} B_i(j)K_t(4;i) \\
&= \frac{1}{4^k}\sum_{i=0}^{n}\Big(\sum_{j=1}^{N} B_i(j)\Big)K_t(4;i) \\
&= \frac{1}{4^k}\Big(NK_t(4;0) + L\sum_{i=0}^{n/2}\binom{n}{2i}3^{2i}K_t(4;2i) - LK_t(4;0)\Big).
\end{aligned}$$

From Lemma 5.18 it follows that for $t > 0$

$$\begin{aligned}
vv\sum_{j=1}^{N} B_t^{\perp}(\mathcal{C}_j) &= \frac{1}{4^k}\Big(N\binom{n}{t}3^t + L2^{n-1}(-3)^t\binom{n}{t} - L\binom{n}{t}3^t\Big) \\
&= \frac{1}{4^k}N\binom{n}{t}3^t\Big[1 + ((-1)^t 2^{n-1} - 1)\frac{4^k - 1}{\frac{1}{2}(4^{n-1} + (-2)^n) - 1}\Big].
\end{aligned}$$

Hence

$$\tilde{B}_t^{\perp} = \frac{1}{N}\sum_{j=1}^{N} B_t^{\perp}(\mathcal{C}_j).$$

The proof is completed as in Theorem 5.17. □

THEOREM 5.20. *(Quantum Gilbert-Varshamov Bound)*
There exists quantum stabilizer code with

$$R \geq 1 - H_2(\delta) - \delta\log_2(3),$$

where $\delta = d/n$ is the relative quantum minimum distance.

PROOF. First we notice that the second term of the last factor in the expression (5.22) vanishes as n grows. Thus, using the Chebyshev inequality we obtain that starting with some value of n

$$B_i^{\perp} \leq 2n^2\frac{1}{4^k}\binom{n}{i}3^i. \tag{5.23}$$

The code $\mathcal{C}$ is linear and therefore any $B_i(\mathcal{C}^{\perp})$ is integer. Hence, taking the binary logarithm and dividing by n the right part of (5.23), we obtain that for sufficiently large n,

$$B_i(C^{\perp}) = 0, \text{ if } H_2\left(\frac{i}{n}\right) + \frac{i}{n}\log_2 3 + 2\frac{k}{n} \leq 0.$$

Now taking into account that the dimension of the quantum stabilizer code that corresponds to $\mathcal{C}^{\perp}$ equals $k_Q = n - k$ we finish the proof. □

Bibliography

[AB99] A. Ashikhmin and A. Barg, Binomial Moments: Bounds and Applications, *IEEE Trans. on Inf. Theory,* **45**, (1999), 438–453, 1999.

[AB02] A. Ashikhmin, A. Barg, Bounds on the Covering Radius of Linear Codes, *Designs, Codes and Cryptography,* **27**, (2002), 261–269.

[ABL] A. Ashikhmin, A. Barg, S. Litsyn, S A new upper bound on the reliability function of the Gaussian channel *IEEE Transactions on Information Theory,* **46**, (2000), 1945 – 1961.

[ABKL] A. Ashikhmin, A. Barg, E. Knill, S. Litsyn, Quantum error detection .II. Bounds *IEEE Transactions on Information Theory,* **46**, (2000), 789 – 800.

[ACKL] A. Ashikhmin, G. Cohen, M. Krivelevich, S. Litsyn, Bounds on distance distributions in codes of known size Ashikhmin, A., Cohen, G.D.; Krivelevich, M.; Litsyn, S.N.; *IEEE Transactions on Information Theory,* **51**, (2005), 250 – 258.

[AHLL] A. Ashikhmin, I. Honkala, T. Laihonen, S. Litsyn, On relations between covering radius and dual distance *IEEE Transactions on Information Theory,* **45**, (1999), 1808 – 1816.

[AL] A. Ashikhmin, S. Litsyn, Upper bounds on the size of quantum codes *IEEE Transactions on Information Theory,* **45**, 1999 1206 – 1215.

[AK] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Information Theory,* **47**, (2001), 3065–3072.

[BDSW] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wooters, Mixed state entanglement and quantum error correction, *Phys. Rev. A*, **54**, (1996), 3824–??.

[CRSS97] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, **78**, (1997), 405–409.

[CRSS98] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, "Quantum errors correction via codes over $GF(4)$," *IEEE Trans. Info. Theory*, vol. 44, pp.1369 –1387, 1998.

[CG] R. Cleve and D. Gottesman, Efficient computations of encodings for quantum error correction, *Physical Review A*, **56**, (1997) Number 1, 76–82. quant-ph/9607030: PS

[GOT] D. Gottesman, A class of quantum error-correcting codes saturating the quantum Hamming bound, *Phys. Rev. A*, textbf54, (1996), 1862–1868.

[K] A. Kitaev, private communication, 1997.

[KL97] E. Knill and R. Laflamme *A theory of quantum error-correcting codes*, Phys. Rev. A, **55** (1997), 900.

[L] P. Lancaster, *Theory of Matrices*, Academic Press, Inc., 1969.

[MRRW] R. J. McEliece, E. R. Rodemich,H. C. Rumsey, Jr. and L. R. Welch, New Upper Bounds on the Rate of a Code via the Delsarte-MacWilliams Inequalities, *IEEE Trans. Inform. Theory*, **23**, (1977), 157–166.

[MOS] F. J. MacWilliams, A. M. Odlyzko, and N. J. A. Sloane, Self-dual codes over $GF(4)$, *J. of Combin. Theory*, Ser. A. **25**, (1978), 288–318.

[NC] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge, University Press, 2000.

[SH95] P. Shor *Scheme for reducing decoherence in quantum memory*, Phys. Rev. A, **52** (1995), 2493–2496.

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

[Ste96a] A. M. Steane, Simple quantum error correcting codes, *Phys. Rev. Lett.*, **77**, (1996), 793–797.

[Ste96a] A. M. Steane, Multiple particle interference and quantum error correction, *Proc. R. Soc. London A*, **452**, (1996), 2551–2576.

[WOOT] W. K. Wooters and W. H. Zurek, *A single quantum cannot be cloned*, Nature, **299** (1982), 802.