Quantum error correction

Mika Hirvensalo

Turku Centre for Computer Science
TUCS Technical Report No 178
May 1998
ISBN 952-12-0217-3
ISSN 1239-1891

Abstract

An introduction to formalism of quantum computation and to the theory of quantum error-correcting codes is presented. Error-correction schemes due to Shor and Calderbank are also represented.

TUCS Research Group
Theory Group: Mathematical Methods in Computer Science

1 Introduction

Quantum computers may have more computational power than the ordinary ones [7]. But in order to actually build a quantum computer, one has to solve many technical problems. The quantum system used in computation should be carefully isolated from the environment in order to shield against destructive interaction. On the other hand, it cannot be completely isolated since the computation should carry on and supervised somehow. It seems to be inevitable that a quantum system will eventually become entangled with the environment and therefore decay. This procedure is referred as *decoherence*. The goal of quantum error correction is to provide methods to restore the quantum state after destructive decoherence.

The purpose of this report is to provide an introduction to formalism of quantum computation and to the theory of quantum error-correction. Error-correction schemes due to Shor [6] and Calderbank, Shor [2] are represented.

2 A Model of quantum computation

2.1 Quantum states as vectors

We shall first introduce the formalism of quantum physics in the simple form, based on *state vectors*. However, this set-up will not fully describe the behavior of compound quantum systems which is needed to understand the error processes in quantum computations. Therefore we shall generalize the formalism into the one based on *self-adjoint operators*. Throughout this paper we handle *finite-dimensional* quantum systems.

The basic information unit in quantum computation is *quantum bit*, *qubit*, for short. Qubits could be implemented in principle by using any two-state microsystem. The table 2.1 (extracted from [7]) lists some physical systems that have been investigated as potential qubits.

Definition 2.1.1. The *basis states* of a qubit are represented as orthonormal basis vectors in two-dimensional complex vector space. Using the notations of P. Dirac, we denote these basis vectors by $|\,0\rangle$ and $|\,1\rangle$ and assign logical 0 and 1 to these vectors. □

Equipped with standard inner product $\langle\psi \mid \varphi\rangle$ this vector space becomes two-dimensional Hilbert space $\mathcal{H}_2$. Conventionally, in the literature of physics, the inner product is assumed to be linear with respect to the second

Quantum System	Time per Gate Operation (sec)	Coherence Duration (sec)	Maximum No. Coherent Steps
Mössbauer nucleus	10^{-19}	10^{-10}	10^{9}
GaAs electrons	10^{-13}	10^{-10}	10^{3}
Gold electrons	10^{-14}	10^{-8}	10^{6}
Trapped indium ions	10^{-14}	10^{-1}	10^{13}
Optical microcavity	10^{-14}	10^{-5}	10^{9}
Electron spin	10^{-7}	10^{-3}	10^{4}
Electron quantum dot	10^{-6}	10^{-3}	10^{3}
Nuclear spin	10^{-3}	10^{4}	10^{7}

Table 1: The maximum number of computational steps that can be accomplished without losing coherence for various quantum systems.

argument:

$$\langle \psi \,|\, c_1\varphi_1 + c_2\varphi_2 \rangle = c_1\langle \psi \,|\, \varphi_1 \rangle + c_2\langle \psi \,|\, \varphi_2 \rangle. \tag{2.1.1}$$

Recall that $\langle \psi \,|\, \varphi \rangle = \overline{\langle \varphi \,|\, \psi \rangle}$, where $\overline{c}$ means the complex conjugate of c.

The *states* of a quantum bit are given by equivalence classes of unit-length vectors in $\mathcal{H}_2$. Two vectors φ_1 and φ_2 on the unit sphere are equivalent, if they are linearly dependent. This is equivalent to relation $\varphi_1 = e^{i\theta}\varphi_2$ for some $\theta \in \mathbb{R}$. We will however identify the equivalence class with a representative.

Principle 1. The states of a quantum bit are of form

$$c_0 \,|\, 0 \rangle + c_1 \,|\, 1 \rangle, \text{ where } |c_0|^2 + |c_1|^2 = 1.$$

Space $\mathcal{H}_2$ is called the *state space* of a quantum bit. If $c_0c_1 \neq 0$, then the state is called a *superposition* of $|\, 0 \rangle$ and $|\, 1 \rangle$. □

The compound state space of two quantum systems can be represented, under some physical assumptions, as the *tensor product* of the original state spaces. Thus, if we have two quantum bits in states $a_0 \,|\, 0 \rangle + a_1 \,|\, 1 \rangle$ (bit number 1) and $b_0 \,|\, 0 \rangle + b_1 \,|\, 1 \rangle$ (bit number 2), the state of bit system 1, 2 (from left to right) is given by

$$\begin{aligned} & (a_0 \,|0\rangle + a_1 \,|1\rangle) \otimes (b_0 \,|0\rangle + b_1 \,|1\rangle) && (2.1.2) \\ = \;& a_0 b_0 \,|0\rangle \otimes |0\rangle + a_0 b_1 \,|0\rangle \otimes |1\rangle + a_1 b_0 \,|1\rangle \otimes |0\rangle + a_1 b_1 \,|1\rangle \otimes |1\rangle . \end{aligned}$$

This state in $\mathcal{H}_2 \otimes \mathcal{H}_2 \simeq \mathcal{H}_4$ is an example of a *decomposable* state: It can be represented as a tensor product of states in $\mathcal{H}_2$, but this is not always the case. Consider, for instance, a unit-length vector in $\mathcal{H}_2 \otimes \mathcal{H}_2$ (the tensor space inherits the inner product in the most obvious way) like

$$\frac{1}{\sqrt{2}}\Big(\,|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \Big). \tag{2.1.3}$$

The assumption that state (2.1.3) would be of form (2.1.2) would lead to equations $a_0 b_1 = a_1 b_0 = 0$, which is impossible since neither a_0 nor b_1 could be zero. A state that is not decomposable is *entangled.*

Taking more quantum bits, we get the analogue of *register* of n bits in quantum computation, which is (binary) *quantum register* of length n.

Principle 2. The states of a quantum register of length n are given by unit-length vectors in n-fold tensor product of $\mathcal{H}_2$, which is isomorphic to 2^n-dimensional Hilbert space $\mathcal{H}_{2^n}$. We use notations

$$\begin{aligned} & |x_0\rangle \otimes |x_1\rangle \otimes \ldots \otimes |x_{n-1}\rangle \\ = \;& |x_0\rangle \,|x_1\rangle \ldots |x_{n-1}\rangle \\ = \;& |x_0 x_1 \ldots x_{n-1}\rangle \\ = \;& |x_0 2^{n-1} + x_1 2^{n-2} + \ldots + x_{n-2}2 + x_{n-1}\rangle . \end{aligned}$$

□

Using the latest notation, space $\mathcal{H}_{2^n}$ has orthonormal basis $|0\rangle$, $|1\rangle$, $|2\rangle$, $\ldots$, $|2^n - 1\rangle$ and a general state of quantum register of length n is

$$c_0 \,|0\rangle + c_1 \,|1\rangle + c_2 \,|2\rangle + \ldots + c_{2^n-1} \,|2^n - 1\rangle, \tag{2.1.4}$$

where $|c_0|^2 + |c_1|^2 + \ldots + |c_{2^n-1}|^2 = 1$.

2.2 Boolean circuits

We shall introduce a model for polynomial time quantum computation similar to a well-known computation model for polynomial time classical computation:

Definition 2.2.1. A *Boolean circuit* is a finite, directed, acyclic graph whose vertices are labeled using set $\{\text{AND}, \text{NOT}, \text{OR}, \text{OUTPUT}, x_1, x_2, x_3, \dots\}$. All AND and OR-vertices have indegree 2, NOT and OUTPUT-vertices have indegree 1, and x_i-vertices have indegree 0. There is exactly one OUTPUT-vertex and it has outdegree 0. Vertices with label x_i are referred as *input variables* or *input wires*. Vertices with label AND, OR, NOT are called *gates*. □

The input wires of a Boolean circuit can be given a value 0 or 1. Then the function computed by the circuit is interpreted in the obvious way.

Definition 2.2.2. The *size* of a circuit is the number of gates in it. A *family of circuits* is a sequence $\mathcal{C} = (C_0, C_1, \dots)$ of Boolean circuits, where C_n has n input variables. We say that a language $L \subseteq \{0,1\}^*$ *has polynomial circuits* if there is a family of circuits $\mathcal{C}$ and a number k such that

- The size of C_n is at most n^k.
- $x \in L$ if and only if $C_{|x|}$ on input x outputs 1.

We also say that family $\mathcal{C} = (C_0, C_1, \dots)$ *decides* L. □

In order to obtain a good model for computation, we have to strengthen the notion of circuits:

Definition 2.2.3. The family $\mathcal{C} = (C_0, C_1, \dots)$ of polynomial circuits is *uniform* if there is a number l and a Turing machine that on input 1^n outputs C_n using no more than n^l computational steps. We also say that a language L has *uniformly polynomial circuits* if there is a uniform family $\mathcal{C} = (C_0, C_1, \dots)$ that decides L. □

See [4] for the proof of the following theorem

Theorem 2.2.4. *A language L has uniformly polynomial circuits if and only if $L \in \mathbf{P}$.*

2.3 Quantum circuits

Representing a linear mapping by a matrix, we will use coordinate representation $|\,k\rangle = e_k = (0, \dots, 1, \dots, 0)^T$, where the kth component is the only nonzero one.

To introduce the notion of quantum gates, we begin with

Principle 3. Quantum states evolve via unitary transformations:

$$\varphi \mapsto U\varphi, \tag{2.3.1}$$

where U is a unitary mapping on the state space of φ.

Recall that unitarity on the finite dimensional spaces mean that the complex conjugate of the transpose of the matrix (i.e. the adjoint matrix) is the inverse of the original one.

Definition 2.3.1. A *quantum gate* on $\mathcal{H}_{2^n}$ is a unitary mapping such that if

$$\mathcal{H}_{2^n} = \mathcal{H}_2^{(0)} \otimes \mathcal{H}_2^{(1)} \otimes \ldots \otimes \mathcal{H}_2^{(n-1)}, \tag{2.3.2}$$

then there are subspaces $\mathcal{H}_2^{(i)}$, $\mathcal{H}_2^{(j)}$ and $\mathcal{H}_2^{(k)}$ such that U restricted on

$$\bigotimes_{\substack{k=1 \\ k\neq i,j,k}}^{n} \mathcal{H}_2^{(k)} \tag{2.3.3}$$

is identity. In other words, U operates only on at most three qubits. □

Definition 2.3.2. A *quantum circuit* is finite, directed acyclic graph, where each vertex is labeled by a quantum gate, or by an element of set

$$\{\text{OUTPUT}, q_1, q_2, q_3, \ldots, d_2, d_3, d_4, \ldots\}.$$

Vertices OUTPUT and d_i have indegree 1 and outdegree 0, vertices q_i have indegree 0 and outdegree 1. Any other vertex has the same in- and outdegree, 1, 2 or 3. There is exactly one OUTPUT-vertex. The number of d_i-vertices is the number of q_i-vertices minus one. Nodes labeled by q_i are referred as *input* vertices and those ones having labels d_i as *futile outputs.* □

The value computed by a quantum circuit is interpreted according to definition 2.3.1.

To show that quantum circuits have at least the same power as classical ones, we consider matrices $M_\neg$, $M_\wedge$ and $M_\vee$ given by

$$M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$M_\wedge = \begin{pmatrix} I_2 & & & 0 \\ & I_2 & & \\ 0 & & I_2 & \\ & & & M_\neg \end{pmatrix} \quad M_\vee = \begin{pmatrix} I_2 & & & 0 \\ & M_\neg & & \\ 0 & & M_\neg & \\ & & & M_\neg \end{pmatrix},$$

where I_2 is the 2×2 identity matrix. These matrices induce permutations and thus unitary mappings. They operate as

$$\begin{array}{rcl} M_\neg\,|0\rangle &=& |1\rangle \\ M_\neg\,|1\rangle &=& |0\rangle \end{array}, \quad \begin{array}{rcl} M_\wedge\,|000\rangle &=& |000\rangle \\ M_\wedge\,|010\rangle &=& |010\rangle \\ M_\wedge\,|100\rangle &=& |100\rangle \\ M_\wedge\,|110\rangle &=& |111\rangle \end{array}, \quad \begin{array}{rcl} M_\vee\,|000\rangle &=& |000\rangle \\ M_\vee\,|010\rangle &=& |011\rangle \\ M_\vee\,|100\rangle &=& |101\rangle \\ M_\vee\,|110\rangle &=& |111\rangle \end{array}$$

So $M_\neg$, $M_\wedge$ and $M_\vee$ essentially compute logical NOT, AND and OR respectively. It should be noticed that they require some *dummy qubits* that must initially be set zero. If we finally introduce a unitary matrix (actually this is not necessary, $M_\wedge$ could replace this)

$$M_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I_2 & 0 \\ 0 & M_\neg \end{pmatrix} \tag{2.3.4}$$

that shall do the work of copymachine: $M_c\,|00\rangle = |00\rangle$ and $M_c\,|10\rangle = |11\rangle$, it is clear that whatever computation can be done with a classical circuit, there is a quantum circuit of (essentially) same size, equipped with some ancillary input wires, doing the same computation.

2.4 Quantum parallelism

Consider a family of Boolean circuits computing a function $f : \{0,1\}^* \to \{0,1\}$. Denote the restriction of f onto $\{0,1\}^n$ by f_n. Now, for each n, there is a quantum circuit U_n with n inputs and some dummy input wires that computes the function f_n:

$$U_n\,|k\rangle\,|0\rangle = |k\rangle\,|f_n(k)\rangle, \tag{2.4.1}$$

where ancillary qubits are not written explicitly.

We define the *Hadamard transformation* to be a unary quantum gate given by matrix

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}. \tag{2.4.2}$$

Then $H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

If we add, on each input wire of U_n a Hadamard transform, the modified circuit will on input $|00\ldots 0\rangle\,|0\rangle$ compute

$$\begin{aligned}
& U_n\big(H \otimes H \otimes \ldots \otimes H \otimes I\big)(|0\rangle\,|0\rangle \ldots |0\rangle\,|0\rangle) \\
= \;& U_n\Big(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \ldots \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle\Big) \\
= \;& U_n\Big(\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\,|0\rangle\Big) \\
= \;& \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} |j\rangle\,|f_n(j)\rangle, \qquad (2.4.3)
\end{aligned}$$

so actually *all* 2^n values were computed simultaneously. This is called *quantum parallelism.*

2.5 Observation

Principle 4. An *observation* of the last qubit of quantum register at state

$$\sum_{j=0}^{2^n-1} c_j\,|j\rangle\,|b_j\rangle, \quad b_j \in \{0,1\} \qquad (2.5.1)$$

will yield 0 with probability $P(0) = \sum_{b_j=0} |c_j|^2$ and 1 with probability $P(1) = \sum_{b_j=1} |c_j|^2$. The post-observation state will be

$$\begin{aligned}
&\frac{1}{\sqrt{P(0)}} \sum_{b_j=0} c_j\,|j\rangle\,|0\rangle \text{ or} \\
&\frac{1}{\sqrt{P(1)}} \sum_{b_j=1} c_j\,|j\rangle\,|1\rangle
\end{aligned}$$

depending on which one of values 0 or 1 was seen. □

This "collapse" of the state in the observation procedure is usually called the *projection postulate.*

2.6 Quantum states as operators

When we think about superposition (2.1.3), it would be convenient to say that both qubits still have a state of their own, as a subsystems of the compound system. Heuristically we would require a state representation for both qubits that is somehow between $|\,0\rangle$ and $|\,1\rangle$, but a superposition will not do, as we have seen. In this section we will generalize the concept of a state and the generalization will be used in the sequel. In fact, the error processes in quantum systems are due to the fact that eventually the system will become entangled with the environment and therefore change.

An *operator* means a linear mapping $A : \mathcal{H}_m \to \mathcal{H}_m$. Operators on $\mathcal{H} = \mathcal{H}_m$ can be represented as $m \times m$-matrices.

For a state vector $|\,\psi\rangle = (a_0, a_1, \dots, a_{m-1})^T$ we define the *dual vector* $\langle\psi\,| = (\overline{a}_0, \overline{a}_1, \dots, \overline{a}_{m-1})$. Vectors $\langle\psi\,|$ and $|\,\psi\rangle$ are referred as *bra*-vectors and *ket*-vectors respectively (from word *bracket*). A bra-vector $\langle\psi\,|$ can be identified with a functional $\in \mathcal{H}^*$ (the dual space of $\mathcal{H}$) by

$$\langle\psi\,|\,(|\,\varphi\rangle) = \langle\psi\,||\,\varphi\rangle = \langle\psi\,|\,\varphi\rangle.$$

On the other hand, Fréchet-Riesz' theorem says that for each functional $f \in \mathcal{H}^*$ there exists unique vector ψ_f such that

$$f(\varphi) = \langle\psi_f\,|\,\varphi\rangle \text{ for each } \varphi \in \mathcal{H}.$$

For a state vector $|\,\varphi\rangle = (\omega_0, \omega_1, \dots, \omega_{m-1})^T$ we will define the *density matrix* belonging to $|\,\varphi\rangle$ by

$$\begin{aligned}
|\,\varphi\rangle \otimes \langle\varphi\,| &= \begin{pmatrix} \omega_0 \\ \omega_1 \\ \vdots \\ \omega_{m-1} \end{pmatrix} \otimes (\overline{\omega}_0, \overline{\omega}_1, \dots, \overline{\omega}_{m-1}) \\
&= \begin{pmatrix} |\omega_0|^2 & \omega_0\overline{\omega}_1 & \dots & \omega_0\overline{\omega}_{m-1} \\ \omega_1\overline{\omega}_0 & |\omega_1|^2 & \dots & \omega_1\overline{\omega}_{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{m-1}\overline{\omega}_0 & \omega_{m-1}\overline{\omega}_1 & \dots & |\omega_{m-1}|^2 \end{pmatrix}.
\end{aligned}$$

Notice that if $|\,\varphi_1\rangle = e^{i\theta}\,|\,\varphi\rangle$, then $|\,\varphi_1\rangle \otimes \langle\varphi_1\,| = |\,\varphi\rangle \otimes \langle\varphi\,|$. We use also notation $|\,\varphi\rangle \otimes \langle\varphi\,| = |\,\varphi\rangle\langle\varphi\,|$.

For each φ, η the equation

$$|\,\varphi\rangle\langle\varphi\,|\,\eta = \langle\varphi\,|\,\eta\rangle\varphi \tag{2.6.1}$$

holds, but this is to say that each mapping induced by a matrix $|\varphi\rangle\langle\varphi|$ is a projection onto the subspace generated by unit vector φ.

There are three important properties of density matrices: Firstly,

$$\operatorname{Tr} |\varphi\rangle\langle\varphi| = \sum_{i=0}^{m-1} |\omega_i|^2 = 1,$$

so density matrices have unit trace. Secondly,

$$\begin{aligned}
\big\langle \eta \,\big|\, |\varphi\rangle\langle\varphi| \xi \big\rangle &= \langle \varphi \,|\, \xi\rangle\langle \eta \,|\, \varphi\rangle \\
\big\langle\, |\varphi\rangle\langle\varphi|\eta \;\big|\, \xi \big\rangle &= \overline{\langle \varphi \,|\, \eta\rangle}\langle \varphi \,|\, \xi\rangle = \langle \varphi \,|\, \xi\rangle\langle \eta \,|\, \varphi\rangle.
\end{aligned}$$

This property says that density matrices induce *self-adjoint* operators. Operator A is *self-adjoint* if $\langle \eta \,|\, A\xi\rangle = \langle A\eta \,|\, \xi\rangle$ for any η, $\xi \in \mathcal{H}$. More generally, for each operator A there is an *adjoint operator* A^* which is defined by $\langle \eta \,|\, A\xi\rangle = \langle A^*\eta \,|\, \xi\rangle$ for all η, $\xi \in \mathcal{H}$.

The third property is obtained from the second one by letting $\xi = \eta$:

$$\big\langle \eta \,\big|\, |\varphi\rangle\langle\varphi|\eta \big\rangle \geq 0 \text{ for each } \eta \in \mathcal{H}. \tag{2.6.2}$$

This is the definition of a *positive* operator. It turns out that positivity implies self-adjointness.

Definition 2.6.1. A *state* of a quantum system is a positive, unit-trace operator on $\mathcal{H}$. The set of states is denoted by $\mathcal{S}(\mathcal{H})$ □

All matrices representing states will be called density matrices as well. A density matrix associated to a state vector is nothing but another representation of an equivalence class of state vectors (i. e. a state), but how is the general notion of state related to the simple density matrices belonging to state vectors? We begin the analysis by observing that if λ is a eigenvalue of a state A and φ and eigenvector belonging to λ, then

$$\begin{aligned}
\lambda\langle \varphi \,|\, \varphi\rangle &= \langle \varphi \,|\, \lambda\varphi\rangle = \langle \varphi \,|\, A\varphi\rangle = \langle A\varphi \,|\, \varphi\rangle, \\
\overline{\lambda}\langle \varphi \,|\, \varphi\rangle &= \langle \lambda\varphi \,|\, \varphi\rangle = \langle A\varphi \,|\, \varphi\rangle,
\end{aligned}$$

and it follows that the eigenvalues must be real. Moreover, eigenvectors belonging to disjoint eigenvalues are orthogonal: If $\lambda_1 \neq \lambda_2$ and $A\varphi_1 = \lambda_1\varphi_1$, $A\varphi_2 = \lambda_2\varphi_2$, then

$$\begin{aligned}
\langle \varphi_2 \,|\, A\varphi_1\rangle &= \lambda_1\langle \varphi_2 \,|\, \varphi_1\rangle, \\
\langle \varphi_2 \,|\, A\varphi_1\rangle &= \langle A\varphi_2 \,|\, \varphi_1\rangle = \lambda_2\langle \varphi_2 \,|\, \varphi_1\rangle.
\end{aligned}$$

The claim follows, since $\lambda_1 \neq \lambda_2$.

If $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_m$ are the eigenvalues of A (not necessarily disjoint) and $\varphi_1, \varphi_2, \ldots, \varphi_m$ an orthonormal set of eigenvectors (there exists such a set, since A is self-adjoint) such that $A\varphi_i = \lambda_i \varphi_i$, we have a *spectral representation* of A:

$$A = \lambda_1 \,|\,\varphi_1\rangle\langle\varphi_1\,| + \lambda_2 \,|\,\varphi_2\rangle\langle\varphi_2\,| + \ldots + \lambda_m \,|\,\varphi_m\rangle\langle\varphi_m\,| \,. \tag{2.6.3}$$

If the eigenvalues are all disjoint, this representation is unique by construction. If, on the other hand, there is some *degeneration* (i. e. multiple eigenvalues), then (2.6.3) can never be unique, since

$$|\,\varphi_1\rangle\langle\varphi_1\,| + |\,\varphi_2\rangle\langle\varphi_2\,| \quad = \quad |\,\varphi_1'\rangle\langle\varphi_1'\,| + |\,\varphi_2'\rangle\langle\varphi_2'\,| \tag{2.6.4}$$

whenever

$$\begin{pmatrix} \varphi_1' \\ \varphi_2' \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \begin{pmatrix} \varphi_1 \\ \varphi_2 \end{pmatrix}.$$

Even in this case, we can collect together the projections in (2.6.3) belonging to the same eigenvalue resulting

$$A = \lambda_1' P_1 + \lambda_2' P_2 + \ldots + \lambda_k' P_k, \tag{2.6.5}$$

where $\lambda_1' < \lambda_2' < \ldots < \lambda_k'$ are disjoint eigenvalues and P_i the projection onto the eigenspace of λ_i'. Now representation (2.6.5) is unique, called the *spectral representation* of A (Notice that here also $P_i P_j = 0$ if $i \neq j$).

So, any state (with respect to the new notion) is some kind of combination of states with respect to old notion. But we can say more: Firstly,

$$1 = \operatorname{Tr} A = \sum_{i=1}^{m} \langle\varphi_i\,|\,A\varphi_i\rangle = \sum_{i=1}^{m} \langle\varphi_i\,|\,\lambda_i\varphi_i\rangle = \sum_{i=1}^{m} \lambda_i. \tag{2.6.6}$$

Secondly,

$$\lambda_i = \langle\varphi_i\,|\,A\varphi_i\rangle \geq 0, \tag{2.6.7}$$

since states are positive operators. This is to say that *each state can be represented as a convex combination of one-dimensional projections.* Representation is unique if and only if the state has disjoint eigenvalues. One-dimensional projections $|\,\varphi\rangle\langle\varphi\,|$ are extreme elements of the state set. They are called *pure states* and often identified with vector states. The states that are not pure, are *mixed.*

It still remains to describe the time evolution of the states in this new formalism. We would like to preserve the time evolution of pure states, so

$$|\varphi\rangle\langle\varphi| \mapsto |U\varphi\rangle\langle U\varphi| = U\,|\varphi\rangle\langle\varphi|\,U^*. \tag{2.6.8}$$

This generalizes straightforwardly: State T evolves via unitary mapping U:

$$T \mapsto UTU^* \tag{2.6.9}$$

2.7 Observables

An *observable* takes its values in $\mathbb{R}$. Let E be an observable having possible values $\{\theta_1, \theta_2, \dots, \theta_n\}$. For each vector state φ there should be a probability $p(\{\theta_i\} \mid \varphi)$ having θ_i as outcome, if E is measured when system is prepared in state φ.

In quantum physics this is organized as follows: For each θ_i there is a projection $E(\{\theta_i\}) = E(\theta_i)$ such that

$$p(\{\theta_i\} \mid \varphi) = \langle\varphi \,|\, E(\theta_i)\varphi\rangle. \tag{2.7.1}$$

We should also have

$$p(\{\theta_i, \theta_j\} \mid \varphi) = \langle\varphi \,|\, E(\theta_i)\varphi\rangle + \langle\varphi \,|\, E(\theta_j)\varphi\rangle = \langle\varphi \,|\, E(\{\theta_i, \theta_j\})\varphi\rangle \tag{2.7.2}$$

and

$$1 = p(\bigcup_{i=1}^{n}\{\theta_i\} \mid \varphi) = \sum_{i=1}^{n}\langle\varphi \,|\, E(\theta_i)\varphi\rangle = \langle\varphi \,|\, E(\bigcup_{i=1}^{n}\{\theta_i\})\varphi\rangle. \tag{2.7.3}$$

Therefore, we identify an observable with a *projection-valued measure* E that maps (Borel) subsets of $\mathbb{R}$ to projections on the state space. Measure E satisfies

1) $E(X)$ is a projection for each Borel set X,

2) $E(\mathbb{R}) = I$,

3) $E(\cup X_i) = \sum E(X_i)$ for disjoint sequence (X_i) of Borel sets.

From condition 3) it follows that $E(X)$ and $E(Y)$ are orthogonal projections whenever X and Y are disjoint sets. Therefore, an observable E defines a self-adjoint mapping A_E by spectral representation

$$A_E = \theta_1 E(\theta_1) + \theta_2 E(\theta_2) + \ldots + \theta_n E(\theta_n). \tag{2.7.4}$$

The *expected value* of E at state φ is given by

$$\begin{aligned} & \theta_1 p(\theta_1 \mid \varphi) + \theta_2 p(\theta_2 \mid \varphi) + \ldots + \theta_n p(\theta_n \mid \varphi) \\ = \; & \theta_1 \langle \varphi \,|\, E(\theta_1)\varphi \rangle + \theta_2 \langle \varphi \,|\, E(\theta_2)\varphi \rangle + \ldots + \theta_n \langle \varphi \,|\, E(\theta_n)\varphi \rangle \\ = \; & \langle \varphi \,|\, \sum_{i=1}^{n} \theta_i E(\theta_i)\varphi \rangle \\ = \; & \langle \varphi \,|\, A_E \varphi \rangle, \end{aligned}$$

which is also called the expected value of the operator A_E at state φ.

Here $\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ is again an orthonormal basis of $\mathcal{H}$. Consider now a state vector

$$\varphi = c_1\varphi_1 + c_2\varphi_2 + \ldots + c_m\varphi_m$$

and an observable E with value range $\{1, 2, \ldots, m\}$, projections determined by $E(\{i\}) = |\,\varphi_i\rangle\langle\varphi_i\,|$. The probability of seeing i is

$$p(\{i\} \mid \varphi) = \langle \varphi \,||\, \varphi_i \rangle \langle \varphi_i \,| \varphi \rangle = |\langle \varphi_i \,|\, \varphi \rangle|^2 = |c_i|^2 .$$

We conclude that the observation procedure described in section 2.5 can be realized by observables of this form.

To generalize the probabilities into other than vector states, we write

$$\begin{aligned} P(\theta_i \mid \varphi) &= \langle \varphi \,|\, E(\theta_i)\varphi \rangle \\ &= \langle \sum_{j=1}^{m} \langle \varphi_j \,|\, \varphi \rangle \varphi_j \,|\, E(\theta_i)\varphi \rangle \\ &= \sum_{j=1}^{m} \langle \varphi_j \,|\, E(\theta_i) \langle \varphi \,|\, \varphi_j \rangle \varphi \rangle \\ &= \sum_{j=1} \langle \varphi_j \,|\, E(\theta_i) \; |\, \varphi \rangle \langle \varphi \,| \varphi_j \rangle \\ &= \mathrm{Tr}(E(\theta_i) \,|\, \varphi \rangle \langle \varphi \,|) \\ &= \mathrm{Tr}(|\, \varphi \rangle \langle \varphi \,|\, E(\theta_i)). \end{aligned}$$

Any observable E and any state T together induce a probability measure

$$X \mapsto \mathrm{Tr}(TE(X)), \tag{2.7.5}$$

and we interpret this in

Principle 5. Given a state T and observable E, the value

$$\mathrm{Tr}(TE(X))$$

is the probability that measurement of E while system is in state T, gives a result in set X. $\square$

There is also an inverse result on probability measures of form (2.7.5), see [5] for proof. For the statement, we define the set $\mathcal{P}(\mathcal{H})$ to be the projections on $\mathcal{H}$.

Theorem 2.7.1 (A. Gleason, 1957). *If* $\dim \mathcal{H} \geq 3$*, then each probability measure* $\mu : \mathcal{P}(\mathcal{H}) \to [0,1]$ *having properties*

1) $\mu(0) = 0$, $\mu(I) = 1$

2) $\mu(\sum P_i) = \sum \mu(P_i)$ *for each orthogonal sequence* (P_i) *in* $\mathcal{P}(\mathcal{H})$

is generated via a state T *by*

$$\mu_T(P) = \mathrm{Tr}(TP). \tag{2.7.6}$$

Let $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$ be the state spaces of two quantum systems and tensor product $\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)}$ the state space of the compound system. If $T_1 \in \mathcal{S}(\mathcal{H}^{(1)})$, and $T_2 \in \mathcal{S}(\mathcal{H}^{(2)})$, then $T_1 \otimes T_2 \in \mathcal{S}(\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)})$ and

$$\mathrm{Tr}\left((T_1 \otimes T_2)(P_1 \otimes I)\right) = \mathrm{Tr}(T_1 P_1 \otimes T_2) = \mathrm{Tr}(T_1 P_1) \tag{2.7.7}$$

for any projection P_1 on $\mathcal{H}^{(1)}$. This gives idea to

Principle 6. Let $T \in \mathcal{S}(\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)})$ be any state of the compound system. The states of the subsystems $\Pi_1(T)$ and $\Pi_2(T)$ are determined by requirements

$$\begin{aligned} \mathrm{Tr}(\Pi_1(T)P_1) &= \mathrm{Tr}(T(P_1 \otimes I)) \text{ for each } P_1 \in \mathcal{P}(\mathcal{H}^{(1)}) && (2.7.8) \\ \mathrm{Tr}(\Pi_2(T)P_2) &= \mathrm{Tr}(T(I \otimes P_2)) \text{ for each } P_2 \in \mathcal{P}(\mathcal{H}^{(2)}). && (2.7.9) \end{aligned}$$

We say that $\Pi_1(T)$ is obtained by *tracing over* $\mathcal{H}^{(2)}$ and vice versa. $\square$

See [1] for the proof of the following theorem.

Theorem 2.7.2. *For any state $T \in \mathcal{S}(\mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)})$ there are unique states $\Pi_1(T) \in \mathcal{S}(\mathcal{H}^{(1)})$ and $\Pi_2(T) \in \mathcal{S}(\mathcal{H}^{(2)})$ that satisfy (2.7.8) and (2.7.9). If $\{\varphi_1, \dots, \varphi_r\}$ and $\{\psi_1, \dots, \psi_s\}$ are orthonormal bases of $\mathcal{H}^{(1)}$ and $\mathcal{H}^{(2)}$, then*

$$\Pi_1(T) = \sum_{i,j,k} \langle \varphi_i \otimes \psi_k \,|\, T(\varphi_j \otimes \psi_k) \rangle \; |\,\varphi_i\rangle\langle\varphi_j\,| \,. \tag{2.7.10}$$

An analogous representation can be found for $\Pi_2(T)$.

Notice that from (2.7.10) it evident that $\Pi_1(aT+bS) = a\Pi_1(T) + b\Pi_1(S)$.

For future use, we will compute the state of the first subsystem, when the compound system is in a pure state $T = |\,\eta\rangle\langle\eta\,|$ and

$$\eta = \sum_{l=1}^{t} c_l \varphi_l \otimes \xi_l. \tag{2.7.11}$$

Using the notations above, a straightforward calculation gives

$$\begin{aligned} T(\varphi_j \otimes \psi_k) &= |\,\eta\rangle\langle\eta\,| \; (\varphi_j \otimes \psi_k) \\ &= \sum_{l=1}^{t} \langle c_l \varphi_l \otimes \xi_l \,|\, \varphi_j \otimes \psi_k \rangle \eta \\ &= \sum_{l=1}^{t} \overline{c}_l \langle \varphi_l \,|\, \varphi_j \rangle \langle \xi_l \,|\, \psi_k \rangle \eta = \overline{c}_j \langle \xi_j \,|\, \psi_k \rangle \eta \end{aligned}$$

and

$$\begin{aligned} &\langle \varphi_i \otimes \psi_k \,|\, T(\varphi_j \otimes \psi_k) \rangle \\ = \; &\overline{c}_j \langle \xi_j \,|\, \psi_k \rangle \sum_{l=1}^{t} \langle \varphi_i \otimes \psi_k \,|\, c_l \varphi_l \otimes \xi_l \rangle \\ = \; &\overline{c}_j \langle \xi_j \,|\, \psi_k \rangle \sum_{l=1}^{t} c_l \langle \varphi_i \,|\, \varphi_l \rangle \langle \psi_k \,|\, \xi_l \rangle \\ = \; &\overline{c}_j c_i \langle \xi_j \,|\, \psi_k \rangle \langle \psi_k \,|\, \xi_i \rangle. \end{aligned}$$

Finally,

$$\Pi_1(T) = \sum_{i,j,k} \overline{c}_j c_i \langle \xi_j \,|\, \psi_k \rangle \langle \psi_k \,|\, \xi_i \rangle \; |\,\varphi_i\rangle\langle\varphi_j\,| \tag{2.7.12}$$

$$= \sum_{i,j} \overline{c}_j c_i \langle \xi_j \,|\, \xi_i \rangle \; |\,\varphi_i\rangle\langle\varphi_j\,| \,. \tag{2.7.13}$$

If vectors $\xi_1, \xi_2, \ldots, \xi_t$ are orthonormal, then the latest expression becomes

$$\sum_i |c_i|^2 \, |\varphi_i\rangle\langle\varphi_i| \; .$$

This is how measurement procedure is usually described: A vector state

$$\varphi = c_1\varphi_1 + c_2\varphi_2 + \ldots + c_r\varphi_r \tag{2.7.14}$$

of the system and the initial state of the measuring apparatus ψ_1 form a joint state $\varphi \otimes \psi_1$ that evolves like $\varphi_i \otimes \psi_1 \mapsto \varphi_i \otimes \psi_i$. The resulting state of the first system will be

$$|c_1|^2 \, |\varphi_1\rangle\langle\varphi_1| + |c_2|^2 \, |\varphi_2\rangle\langle\varphi_2| + \ldots + |c_r|^2 \, |\varphi_r\rangle\langle\varphi_r|, \tag{2.7.15}$$

the state of measuring apparatus is

$$|c_1|^2 \, |\psi_1\rangle\langle\psi_1| + |c_2|^2 \, |\psi_2\rangle\langle\psi_2| + \ldots + |c_r|^2 \, |\psi_r\rangle\langle\psi_r|, \tag{2.7.16}$$

and the outcome will be read from the measuring device, leading to a *realization* of a outcome.

The following ad hoc-postulate (projection postulate) is due to von Neumann: If measurement leads to realization of ψ_i, then the state of first system is $|\varphi_i\rangle\langle\varphi_i|$ (c. f. the measurement paradox of quantum physics).

3 Errors and correction

3.1 Decoherence

In the ordinary model, the errors during quantum computation are caused by unwanted interaction between the environment and the quantum system where computation goes on. Consider a n-qubit system on $\mathcal{H}_2^n = \mathcal{H}_{2^n}$, and its t-qubit subsystem $\mathcal{H}_2^t$. Without loss of generality, we can write now $\mathcal{H}_2^n = \mathcal{H}_2^{n-t} \otimes \mathcal{H}_2^t$.

Definition 3.1.1. *Decoherence* on t qubits means that that there is a Hilbert space $\mathcal{H}_{env}$ describing the environment, and a unitary mapping U

$$U : \mathcal{H}_2^t \otimes \mathcal{H}_{env} \to \mathcal{H}_2^t \otimes \mathcal{H}_{env}. \tag{3.1.1}$$

The state of $\mathcal{H}_2^n$ after decoherence is obtained using formula for Π_1 in (2.7.10) for $\mathcal{H}_2^{n-t} \otimes \mathcal{H}_2^t \otimes \mathcal{H}_{env}$, where $\mathcal{H}^{(1)} = \mathcal{H}_2^{n-t} \otimes \mathcal{H}_2^t$ (tracing over environment). □

3.2 Shor's error-correcting scheme

Because of *quantum no-cloning theorem* [8] it was widely believed that error correction in quantum computation is impossible, because no redundancy could be obtained by duplicating qubits. If this assumption were correct, it would mean that it would be practically impossible to build a quantum computer that could work arbitrarily long.

In this section we represent the first quantum error correcting scheme introduced by Peter W. Shor [6]. This error correcting procedure can correct the decoherence of one single qubit. Shor encoded one qubit into nine qubits by the following rule:

$$\begin{aligned} |0\rangle &\mapsto \frac{1}{2\sqrt{2}}\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big)\big(|000\rangle + |111\rangle\big), \\ |1\rangle &\mapsto \frac{1}{2\sqrt{2}}\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big)\big(|000\rangle - |111\rangle\big). \end{aligned}$$

Expanding these triplets we get

$$\begin{aligned} |0\rangle \mapsto \tfrac{1}{2\sqrt{2}} & (|000\,000\,000\rangle + |000\,000\,111\rangle \\ + & \ |000\,111\,000\rangle + |000\,111\,111\rangle \\ + & \ |111\,000\,000\rangle + |111\,000\,111\rangle \\ + & \ |111\,111\,000\rangle + |111\,111\,111\rangle), \end{aligned} \tag{3.2.1}$$

$$\begin{aligned} |1\rangle \mapsto \tfrac{1}{2\sqrt{2}} & (|000\,000\,000\rangle - |000\,000\,111\rangle \\ - & \ |000\,111\,000\rangle + |000\,111\,111\rangle \\ - & \ |111\,000\,000\rangle + |111\,000\,111\rangle \\ + & \ |111\,111\,000\rangle - |111\,111\,111\rangle). \end{aligned} \tag{3.2.2}$$

We consider then a decoherence process for one qubit:

$$\begin{aligned} |e_0\rangle\,|0\rangle &\mapsto |a_0\rangle\,|0\rangle + |a_1\rangle\,|1\rangle, \\ |e_0\rangle\,|1\rangle &\mapsto |a_2\rangle\,|0\rangle + |a_3\rangle\,|1\rangle, \end{aligned} \tag{3.2.3}$$

where $|a_0\rangle$, $|a_1\rangle$, $|a_2\rangle$ and $|a_3\rangle$ are orthogonal environment states. We check what happens when the first qubit of first triplet $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ goes through this decoherence procedure, but this will generalize to the case where any other of these nine qubits goes through decoherence procedure.

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}\,|\,e_0\rangle(|\,000\rangle + |\,111\rangle) \\
\mapsto\ & \frac{1}{\sqrt{2}}\big((|\,a_0\rangle\ |\,0\rangle + |\,a_1\rangle\ |\,1\rangle)\ |\,00\rangle + (|\,a_2\rangle\ |\,0\rangle + |\,a_3\rangle\ |\,1\rangle)\ |\,11\rangle\big) \\
=\ & \frac{1}{2\sqrt{2}}(|\,a_0\rangle + |\,a_3\rangle)(|\,000\rangle + |\,111\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_0\rangle - |\,a_3\rangle)(|\,000\rangle - |\,111\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_1\rangle + |\,a_2\rangle)(|\,100\rangle + |\,011\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_1\rangle - |\,a_2\rangle)(|\,100\rangle - |\,011\rangle).
\end{aligned}
$$

In the same way,

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}\,|\,e_0\rangle(|\,000\rangle - |\,111\rangle) \\
\mapsto\ & \frac{1}{2\sqrt{2}}(|\,a_0\rangle + |\,a_3\rangle)(|\,000\rangle - |\,111\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_0\rangle - |\,a_3\rangle)(|\,000\rangle + |\,111\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_1\rangle + |\,a_2\rangle)(|\,100\rangle - |\,011\rangle) \\
+\ & \frac{1}{2\sqrt{2}}(|\,a_1\rangle - |\,a_2\rangle)(|\,100\rangle + |\,011\rangle).
\end{aligned}
$$

Notice that the states of the environment coincide, and the states of original systems are mixtures of density matrices belonging to state vectors (the normalization factor omitted)

$$|\,000\rangle + |\,111\rangle,\ |\,000\rangle - |\,111\rangle,\ |\,100\rangle + |\,011\rangle,\ |\,100\rangle - |\,011\rangle \tag{3.2.4}$$

(decoherence of encoding of $|\,0\rangle$) and

$$|\,000\rangle - |\,111\rangle,\ |\,000\rangle + |\,111\rangle,\ |\,100\rangle - |\,011\rangle,\ |\,100\rangle + |\,011\rangle \tag{3.2.5}$$

(decoherence of encoding of $|\,1\rangle$).

These can be interpreted that the effect of decoherence of encoding of $|\,0\rangle$ is one of following:

$$|\,000\rangle + |\,111\rangle \mapsto |\,000\rangle + |\,111\rangle \text{ (no errors)} \tag{3.2.6}$$
$$|\,000\rangle + |\,111\rangle \mapsto |\,000\rangle - |\,111\rangle \text{ (sign error)} \tag{3.2.7}$$
$$|\,000\rangle + |\,111\rangle \mapsto |\,100\rangle + |\,011\rangle \text{ (bit error)} \tag{3.2.8}$$
$$|\,000\rangle + |\,111\rangle \mapsto |\,100\rangle - |\,011\rangle \text{ (sign error \textit{and} bit error).} \tag{3.2.9}$$

Similarly for encoding of $|\,1\rangle$. To conclude: Decoherence process (3.2.3) turns (3.2.1) into a mixed state of four pure states, where (3.2.6) corresponds to the original one, (3.2.7) is like the original one (3.2.1), but signs changed in the two last lines, (3.2.8) corresponds to

$$\begin{aligned}
\tfrac{1}{2\sqrt{2}} & \ (|\,100\,000\,000\rangle + |\,100\,000\,111\rangle \\
+ & \ |\,100\,111\,000\rangle + |\,100\,111\,111\rangle \\
+ & \ |\,011\,000\,000\rangle + |\,011\,000\,111\rangle \\
+ & \ |\,011\,111\,000\rangle + |\,011\,111\,111\rangle),
\end{aligned} \tag{3.2.10}$$

and finally (3.2.9) corresponds to a state similar to (3.2.10), but signs at last two lines flipped.

A *bit error* like in (3.2.10) can be corrected by majority vote (using repetition code): Quantum circuit checks the three triplets, and corrects the error according to rules

$$\begin{array}{ll}
|\,000\rangle \mapsto |\,000\rangle, & |\,001\rangle \mapsto |\,000\rangle, \\
|\,010\rangle \mapsto |\,000\rangle, & |\,011\rangle \mapsto |\,111\rangle, \\
|\,100\rangle \mapsto |\,000\rangle, & |\,101\rangle \mapsto |\,111\rangle, \\
|\,110\rangle \mapsto |\,111\rangle, & |\,111\rangle \mapsto |\,111\rangle.
\end{array}$$

This can be done with Boolean circuits, so it can be done with quantum circuits as well, using some ancillary qubits.

Assume now that bit errors have been corrected and a sign error still remains, so the state is of form

$$\frac{1}{2\sqrt{2}}\big(\,|\,000\rangle - |\,111\rangle\big)\big(\,|\,000\rangle + |\,111\rangle\big)\big(\,|\,000\rangle + |\,111\rangle\big). \tag{3.2.11}$$

Applying *enlarged Hadamard transform*

$$\begin{aligned}
|\,000\rangle & \mapsto \frac{1}{\sqrt{2}}\,|\,000\rangle + \frac{1}{\sqrt{2}}\,|\,111\rangle \\
|\,111\rangle & \mapsto \frac{1}{\sqrt{2}}\,|\,000\rangle - \frac{1}{\sqrt{2}}\,|\,111\rangle
\end{aligned}$$

to each triplet, (3.2.11) turns into

$$|111\rangle\ |000\rangle\ |000\rangle, \tag{3.2.12}$$

and now comparing the *triplets*, using repetition coding, we learn which one had the wrong sign. We can thus correct (3.2.12) into

$$|000\rangle\ |000\rangle\ |000\rangle,$$

and reverse the enlarged Hadamard transform to restore the original state.

3.3 A construction of quantum codes

See [3] for the coding-theoretical concepts in this section.

Definition 3.3.1. Quantum error correcting code $\mathcal{Q}$ with rate $\frac{k}{n}$ is unitary mapping of H_2^k into a 2^k-dimensional subspace $\mathcal{H}_2^n$. To be more precise, we can view a quantum code as a unitary mapping

$$U : \mathcal{H}_2^k \otimes |\underbrace{0\dots 0}_{n-k}\rangle \otimes \mathcal{H}_{anc} \to \mathcal{H}_2^n \otimes \mathcal{H}_{anc},$$

where $\mathcal{H}_{anc}$ stands for ancillary qubits, as usually. □

Definition 3.3.2. Let $|y\rangle \in \mathcal{H}_2^n$ be a vector state. Then $D\,|y\rangle$ means any pure state in a mixture recovered after decoherence process (3.1.1). In (3.1.1) $\mathcal{H}_2^t$ means now any t qubits of state vector in $\mathcal{H}_2^n$. □

Definition 3.3.3. Quantum code $\mathcal{Q}$ corrects t errors, if the original state $|x\rangle$ can be recovered from decohered state $D\mathcal{Q}\,|x\rangle$ using a unitary transformation in space $\mathcal{H}_2^n \otimes \mathcal{H}_{anc}$, where $\mathcal{H}_{anc}$ is again a supplementary system. □

The construction represented in this section was introduced in [2]. Let $\mathcal{C}_1 \subseteq \mathbb{F}_2^n$ be a linear code with a generator matrix M and $k_1 = \dim \mathcal{C}_1$. Let also $\mathcal{H}_{\mathcal{C}_1}$ to be the 2^{k_1}-dimensional subspace of $\mathcal{H}_2^n$ generated by orthonormal vectors $\{|c\rangle \mid c \in \mathcal{C}_1\}$. We shall find another orthonormal basis for $\mathcal{H}_{\mathcal{C}_1}$: For each $w \in \mathbb{F}_2^n$ we define

$$|c_w\rangle = \frac{1}{\sqrt{2^{k_1}}} \sum_{v \in \mathbb{F}_2^{k_1}} (-1)^{vMw^T}\ |vM\rangle. \tag{3.3.1}$$

If $w_1 - w_2 \in \mathcal{C}_1^\perp$, then $0 = vM(w_1 - w_2)^T = vMw_1^T - vMw_2^T$, hence $|\, c_{w_1}\rangle = |\, c_{w_2}\rangle$. On the other hand, if w is not in the dual $\mathcal{C}_1^\perp$, then there is a $v_1 \in \mathbb{F}_2^{k_1}$ such that $v_1 M w^T \neq 0$ and

$$S = \sum_{v \in \mathbb{F}_2^{k_1}} (-1)^{vMw^T} = \sum_{v \in \mathbb{F}_2^{k_1}} (-1)^{(v+v_1)Mw^T} = (-1)^{v_1 M w^T} S,$$

so $S = 0$ if and only if $w \notin \mathcal{C}^\perp$. It follows that if $w_1 - w_2 \notin \mathcal{C}_1^\perp$, then

$$\begin{aligned}
\langle c_{w_1} \,|\, c_{w_2}\rangle &= \frac{1}{2^{k_1}} \sum_{v \in \mathbb{F}_2^{k_1}} \sum_{u \in \mathbb{F}_2^{k_1}} (-1)^{vMw_1^T} (-1)^{vMw_2^T} \langle vM \,|\, uM\rangle \\
&= \frac{1}{2^{k_1}} \sum_{v \in \mathbb{F}_2^{k_1}} (-1)^{vM(w_1-w_2)^T} \\
&= \begin{cases} 1, & \text{if } w_1 - w_2 \in \mathcal{C}_1^\perp, \\ 0, & \text{if } w_1 - w_2 \notin \mathcal{C}_1^\perp. \end{cases}
\end{aligned}$$

This means that $2^{n-(n-k_1)} = 2^{k_1}$ representatives of $\mathbb{F}_2^n/\mathcal{C}_1^\perp$ form an orthonormal basis for $\mathcal{H}_{\mathcal{C}_1}$.

Let $\mathcal{C}_2$ be another linear code, having dimension k_2, such that

$$\{0\} \subset \mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathbb{F}_2^n. \tag{3.3.2}$$

Definition 3.3.4. The codewords (i.e. the images under unitary mapping $\mathcal{H}_2^k \to \mathcal{H}_2^n$) of quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ are $\{|\, c_w\rangle \mid w \in \mathcal{C}_2^\perp\}$. There are $2^{n-k_2-(n-k_1)} = 2^{k_1-k_2}$ codewords, and a natural indexing is a set of representatives of $\mathcal{C}_2^\perp/\mathcal{C}_1^\perp$. Quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ has rate $\frac{k_1-k_2}{n}$. □

Example 3.3.5. Let $\mathcal{C}_1$ be $[7,4,3]$-Hamming code with generator matrix

$$G = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{3.3.3}$$

and $\mathcal{C}_2 = \mathcal{C}_1^\perp$ with generator matrix

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \tag{3.3.4}$$

Now $\dim \mathcal{C}_1 = 4$ and $\dim \mathcal{C}_2 = 3$, so quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ contains 2 codewords and the rate is $\frac{1}{7}$. This code maps one qubit to seven qubits. Representatives set can be chosen, for example, as $\mathbf{0} = 0000000 \in \mathcal{C}_2^{\perp} = \mathcal{C}_1$ and $\mathbf{1} = 1111111 \in \mathcal{C}_2^{\perp}$. Then

$$\begin{aligned}
|c_{\mathbf{0}}\rangle = & \ \tfrac{1}{4}\ (|0000000\rangle + |1110001\rangle + |1100010\rangle + |0010011\rangle \\
+ & \ |1010100\rangle + |0100101\rangle + |0110110\rangle + |1000111\rangle \\
+ & \ |0111000\rangle + |1001001\rangle + |1011010\rangle + |0101011\rangle \\
+ & \ |1101100\rangle + |0011101\rangle + |0001110\rangle + |1111111\rangle)
\end{aligned}$$

and

$$\begin{aligned}
|c_{\mathbf{1}}\rangle = & \ \tfrac{1}{4}\ (|0000000\rangle + |1110001\rangle - |1100010\rangle - |0010011\rangle \\
- & \ |1010100\rangle - |0100101\rangle + |0110110\rangle + |1000111\rangle \\
- & \ |0111000\rangle - |1001001\rangle + |1011010\rangle + |0101011\rangle \\
+ & \ |1101100\rangle + |0011101\rangle - |0001110\rangle - |1111111\rangle).
\end{aligned}$$

How can this coding correct errors? We consider two error types: The first taking $|0\rangle \mapsto |1\rangle$ and $|1\rangle \mapsto |0\rangle$ (bit error), the second one mapping $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto -|1\rangle$ (phase error). If one of qubits in $|c_{\mathbf{0}}\rangle$ or $|c_{\mathbf{1}}\rangle$ goes only through first error type, then the error can surely be corrected, since both $|c_{\mathbf{0}}\rangle$ and $|c_{\mathbf{1}}\rangle$ are superpositions of qubit strings and these strings are exactly the codewords of $[7,4,3]$-Hamming code, which can correct one error.

For the second type of errors, we operate the Hadamard transform on each qubit of $|c_{\mathbf{0}}\rangle$ and $|c_{\mathbf{1}}\rangle$. The influence of this transform on a vector $|c\rangle = |c_1\rangle\,|c_2\rangle \ldots |c_n\rangle$ in a basis state ($c_i \in \{0,1\}$) is

$$\begin{aligned}
|c\rangle &= |c_1\rangle\,|c_2\rangle \ldots |c_n\rangle \\
&\mapsto \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{c_1}\,|1\rangle)\tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{c_2}\,|1\rangle)\ldots\tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^{c_n}\,|1\rangle) \\
&= \frac{1}{\sqrt{2^n}}\sum_{u\in\mathbb{F}_2^n}(-1)^{cu^T}\,|u\rangle, \qquad (3.3.5)
\end{aligned}$$

so $|\,c_w\rangle$ transforms into $|\,s_w\rangle$, where

$$
\begin{aligned}
|\,s_w\rangle &= \frac{1}{\sqrt{2^{k_1}}}\sum_{v\in\mathbb{F}_2^{k_1}}(-1)^{vMw^T}\frac{1}{\sqrt{2^n}}\sum_{u\in\mathbb{F}_2^n}(-1)^{vMu^T}\,|\,u\rangle \\
&= \frac{1}{\sqrt{2^{k_1}}}\frac{1}{\sqrt{2^n}}\sum_{u\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^{k_1}}(-1)^{vM(u-w)^T}\,|\,u\rangle \\
&= \frac{1}{\sqrt{2^{k_1}}}\frac{1}{\sqrt{2^n}}\sum_{u\in\mathbb{F}_2^n}\underbrace{\sum_{v\in\mathbb{F}_2^{k_1}}(-1)^{vMu^T}}_{\substack{0, \quad \text{if } u\notin\mathcal{C}_1^\perp \\ 2^{k_1}, \quad \text{if } u\in\mathcal{C}_1^\perp}}\,|\,u+w\rangle \\
&= \frac{1}{\sqrt{2^{n-k_1}}}\sum_{u\in\mathcal{C}_1^\perp}|\,u+w\rangle.
\end{aligned}
$$

In our example,

$$
\begin{aligned}
|\,s_{\mathbf{0}}\rangle = {} & \tfrac{1}{2\sqrt{2}}\;(|\,0000000\rangle + |\,0011101\rangle + |\,0101011\rangle + |\,0110110\rangle \\
+ {} & \;|\,1000111\rangle + |\,1011010\rangle + |\,1101100\rangle + |\,1110001\rangle)
\end{aligned}
$$

and

$$
\begin{aligned}
|\,s_{\mathbf{1}}\rangle = {} & \tfrac{1}{2\sqrt{2}}\;(|\,1111111\rangle + |\,1100010\rangle + |\,1010100\rangle + |\,1001001\rangle \\
+ {} & \;|\,0111000\rangle + |\,0100101\rangle + |\,0010011\rangle + |\,0001110\rangle).
\end{aligned}
$$

We get superpositions formed of translations of words in *dual* of $\mathcal{C}_1$. Because the word w causing the translation was supposed to be in $\mathcal{C}_2^\perp$ and $\mathcal{C}_1^\perp \subseteq \mathcal{C}_2^\perp$, we actually have superpositions of words in $\mathcal{C}_2^\perp$.

In general, a phase error on jth bit of (3.3.1) causes $|\,c_w\rangle$ transform into

$$
\begin{aligned}
|\,c_w\rangle &\mapsto \frac{1}{\sqrt{2^k}}\sum_{v\in\mathbb{F}_2^k}(-1)^{vMw^T}(-1)^{vMe_j^T}\,|\,vM\rangle \\
&= \frac{1}{\sqrt{2^k}}\sum_{v\in\mathbb{F}_2^k}(-1)^{vM(w+e_j)^T}\,|\,vM\rangle.
\end{aligned}
$$

Applying Hadamard transformation on each qubit this turns into

$$
\frac{1}{\sqrt{2^{n-k}}}\sum_{u\in\mathcal{C}_1^\perp}|\,u+e_j+w\rangle,
$$

which means that phase errors turn into bit errors. Since each $u + w$ is a word in $\mathcal{C}_2^\perp$, we can correct these errors if the minimum distance of $\mathcal{C}_2^\perp$ is large enough.

See [2] for the proof of the following theorem:

Theorem 3.3.6. *If $\mathcal{C}_1$ and $\mathcal{C}_2^\perp$ are linear codes with parameters $[n, n-k, d]$ and $\{0\} \subset \mathcal{C}_2 \subset \mathcal{C}_1 \subset \mathbb{F}_2^n$, then the quantum code $\mathcal{Q}_{\mathcal{C}_1,\mathcal{C}_2}$ has rate $1 - \frac{2k}{n}$ and it can correct $t = \lfloor \frac{d-1}{2} \rfloor$ errors.*

References

[1] P. Busch, P. J. Lahti, P. Mittelstaedt: *The Quantum Theory of Measurement*, Springer-Verlag, 1991.

[2] A. R. Calderbank, Peter W. Shor: *Good quantum error-correcting codes exist*, Physical Review A, Vol 54, no. 2, 1996.

[3] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, Third printing 1981.

[4] Christos H. Papadimitriou: *Computational Complexity*, Addison-Wesley Publishing Company, Inc., 1994.

[5] K. R. Parthasarathy: *An Introduction to Quantum Stochastic Calculus*, Birkhäuser Verlag Basel, 1992.

[6] Peter W. Shor: *Scheme for reducing decoherence in quantum computer memory*, Physical Review A, Vol. 52, no. 4, 1995.

[7] Colin P. Williams, Scott H. Clearwater: *Explorations in Quantum Computing*, Springer-Verlag, New York Inc., 1998.

[8] W. K. Wooters, W. H. Zurek, *A Single Quantum Cannot be Cloned*, Nature Vol 299, 802, 1982.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**