Relations between Classical and Quantum Error–Correcting Codes*

Markus Grassl and Thomas Beth

Institut für Algorithmen und Kognitive Systeme (IAKS)
Professor Dr. Th. Beth, Arbeitsgruppe *Quantum Computing*
Universität Karlsruhe, Am Fasanengarten 5, D-76 128 Karlsruhe, Germany
e–mail: grassl@ira.uka.de, EISS_Office@ira.uka.de

Abstract. In this survey we describe relations between classical and quantum error–correcting codes. After a brief introduction to both quantum computation and classical linear error–correcting codes, we show how to construct quantum error–correcting codes based on classical ones. Furthermore, quantum circuits for encoding and syndrome computation are presented.

Keywords: quantum computation, error–correcting codes

1 Introduction

The foundations for the field of quantum computation were laid by Richard Feynman and Paul Benioff in the early 80s by studying the relationship of physical and computational processes. From the observation that quantum mechanical processes are hard to be simulated on classical computers, they concluded that quantum mechanics might help to speed–up computations. After some results of mainly theoretical nature, it was Peter Shor who presented an algorithm of practical interest for a computer based on the principles of quantum mechanics (cf. [22]). His algorithm for factoring integers is exponentially faster than any classical algorithm known so far. The algorithm renders a lot of currently used crypto systems insecure since they rely on the fact that factoring (very) large numbers is infeasible on a classical computer.

But quantum computation would still have been only of theoretical interest if there had not been suggestions for the physical realization of quantum computers (cf. [7, 10, 12, 20]). Nevertheless, another difficulty appeared on the way to the realization of quantum computers. The physical system of a quantum computer is modelled as a closed system that is isolated from its environment. But compared to classical systems, quantum mechanical systems are much more sensitive to any

* Presented at the Workshop on Physics and Computer Science (Physik Informatik Informationstechnik), DPG–Frühjahrstagung, Heidelberg, March 15–16, 1999.

disturbance, e. g., by single photons. And it was believed that there is no way to circumvent this problem by methods of error correction since arbitrary quantum states cannot be replicated (see [26]). It was again SHOR who showed that even in the quantum case error correction is possible (see [23]).

His work initiated a lot of research establishing a theory of quantum error correction. Independently, STEANE [24,25] and CALDERBANK and SHOR [6] came up with methods to construct quantum error–correcting codes from classical linear binary codes. Then, GOTTESMAN [13] and CALDERBANK et al. [5] presented different approaches to generalize the construction of quantum error–correcting codes, but yielding the very same codes. The general conditions for quantum error–correcting codes have been studied by EKERT and MACCHIAVELLO [11], being extended by KNILL and LAFLAMME [18].

The paper is organized as follows: In section 2, we give a short introduction to both the field of quantum computation and the theory of classical error–correcting codes. Then we describe the basic ideas of quantum error correction. The main results about the relations between classical and binary codes are presented in section 4. We conclude with briefly mentioning other relations between classical and quantum codes.

2 Background

2.1 Quantum Registers

Classically, information is often represented by bits. A single bit takes either the value 0 or 1. In physical systems, 0 and 1 are represented by two different states of the system. These could be two different voltages, signals with two different frequencies, but also states on the quantum mechanical level, e. g., ground state and excited state of an electron of an atom or ion, the spin of a nucleus, or the polarization of photons. In Dirac notation, the two states are written as

$$\text{“0”} \mathrel{\hat{=}} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2 \qquad \text{and} \qquad \text{“1”} \mathrel{\hat{=}} |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2 .$$

In quantum mechanics, the principle of superposition allows a system to be simultaneously in different states. Mathematically, the state of the basic unit of quantum information, a *quantum bit* (or short *qubit*), is represented by the normalized linear combination

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{where } \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

The normalization condition stems from the fact that when extracting classical information from the quantum system by a measurement, the values 0 and 1 occur with probability $|\alpha|^2$ and $|\beta|^2$, resp.

Similar to classical registers, a quantum register is built by combining several qubits. Mathematically, this corresponds to the tensor product of two–dimensional vector spaces. Hence the state of a quantum register of length n could be any normalized complex linear combination of the 2^n mutually orthogonal basis states

$$|b_1\rangle \otimes \ldots \otimes |b_n\rangle =: |b_1 \ldots b_n\rangle = |\boldsymbol{b}\rangle \qquad \text{where } b_i \in \{0,1\}.$$

2.2 Quantum Gates

The laws of quantum mechanics say that any transformation on quantum systems is linear. Furthermore, in order to preserve the normalization any operation has to be unitary. Let us first consider operations involving only one qubit, i.e., one subsystem. Similar to the classical NOT gate, there is a quantum operation exchanging the states $|0\rangle$ and $|1\rangle$ given by the matrix

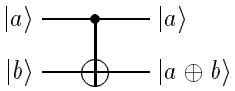
$$NOT := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

But on a single qubit, there is not only this "classical" operation. Examples for non–classical operations on single qubits are given by

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{and} \qquad \theta := \frac{1}{2} \begin{pmatrix} i-1 & i-1 \\ i+1 & -(i+1) \end{pmatrix}. \tag{1}$$

Besides single qubit operations, the so–called controlled NOT gate ($CNOT$) plays an important rôle since any unitary operation on a 2^n dimensional space can be implemented using only single qubit operations and $CNOT$ gates (see [1]). As a classical gate, the $CNOT$ gate corresponds to a gate with two inputs and two outputs. One of the inputs is copied to the first output, the second output is the XOR of the inputs. The transformation matrix of the $CNOT$ gate is given by:

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \tag{2}$$



On the right hand side, the notation for the $CNOT$ gate as a quantum circuit is given. Each of the horizontal lines (*wires*) corresponds to a qubit of the whole quantum register. The dot on the upper wire indicates that the transformation on the lower qubit (the target)—a NOT gate—is only applied when the state of the upper qubit (the control) is $|1\rangle$.

In Fig. 1 a simple quantum circuit is shown. Starting from the state $|000\rangle$, a Hadamard transformation H (see equation (1)) is applied to the first qubit resulting in the state $1/\sqrt{2}\,|000\rangle + 1/\sqrt{2}\,|100\rangle$. Next, a $CNOT$ gate with control

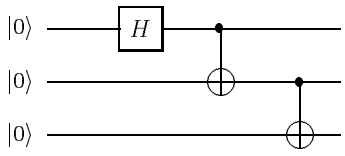


Fig. 1. A quantum circuit to prepare a GHZ state (see [17])

1 and target 2 is applied yielding $1/\sqrt{2}\,|0\rangle\,|0\oplus 0\rangle\,|0\rangle + 1/\sqrt{2}\,|1\rangle\,|0\oplus 1\rangle\,|0\rangle = 1/\sqrt{2}\,|000\rangle + 1/\sqrt{2}\,|110\rangle$. The state obtained after the final $CNOT$ gate with control 2 and target 3 is $1/\sqrt{2}\,|000\rangle + 1/\sqrt{2}\,|111\rangle$.

In matrix notation, the transformation is given by

$$\begin{array}{ccccc} & (I_2 \otimes CNOT) & \cdot & (CNOT \otimes I_2) & \cdot & (H \otimes I_4) \\ = & \begin{pmatrix} 1 & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . & . \\ . & . & . & . & . & . & . & 1 \\ . & . & . & . & . & . & 1 & . \end{pmatrix} & \cdot & \begin{pmatrix} 1 & . & . & . & . & . & . & . \\ . & 1 & . & . & . & . & . & . \\ . & . & 1 & . & . & . & . & . \\ . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & . & 1 & . \\ . & . & . & . & . & . & . & 1 \\ . & . & . & . & 1 & . & . & . \\ . & . & . & . & . & 1 & . & . \end{pmatrix} & \cdot \frac{1}{\sqrt{2}} & \begin{pmatrix} 1 & . & . & . & 1 & . & . & . \\ . & 1 & . & . & . & 1 & . & . \\ . & . & 1 & . & . & . & 1 & . \\ . & . & . & 1 & . & . & . & 1 \\ 1 & . & . & . & -1 & . & . & . \\ . & 1 & . & . & . & -1 & . & . \\ . & . & 1 & . & . & . & -1 & . \\ . & . & . & 1 & . & . & . & -1 \end{pmatrix} \end{array}$$

where I_n denotes an $n \times n$ identity matrix, and zeros are replaced by dots.

2.3 Classical Error–Correcting Codes

In this section we recall some basic definitions and results for classical error–correcting codes (for a more comprehensive treatment see, e. g., [19]).

A *linear block code* $C = [n,k]_q$ of length n is a k–dimensional subspace of the n–dimensional vector space $\mathbb{F}_q^n$ over the finite field $\mathbb{F}_q$ with q elements (for $q = 2$, the notation $C = [n,k]$ is used). Fixing a basis $\{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_k\}$ of C, an information vector $\boldsymbol{i} = (i_1, \ldots, i_k) \in \mathbb{F}_q^k$ is mapped to the code word $\boldsymbol{c}$ where

$$\boldsymbol{c} = \sum_{j=1}^{k} i_j \boldsymbol{g}_j = \boldsymbol{i}G. \tag{3}$$

The $n \times k$ matrix formed by the row vectors $\boldsymbol{g}_j$ is called the *generator matrix* G of the code.

The *dual code* $C^\perp$ of C is the set of vectors that are orthogonal to all vectors of the code with respect to the inner product $\boldsymbol{x} \cdot \boldsymbol{y} = \sum_j x_j y_j$, i.e.,

$$C^\perp := \{\boldsymbol{x} \in \mathbb{F}_q^n \mid \forall \boldsymbol{c} \in C\colon \boldsymbol{x} \cdot \boldsymbol{c} = 0\}.$$

The dual code is again a linear vector space of dimension $n-k$, i.e., $C^{\perp} = [n, n-k]_q$ with a generator matrix H. By definition, $GH^{\mathrm{t}} = 0$ and thus

$$\forall \boldsymbol{c} \in C\colon \boldsymbol{c}H^{\mathrm{t}} = 0. \tag{4}$$

The matrix H can be used to check whether a given vector lies in the code C and is called *parity check matrix* of C. But H can also be used in the process of error correction. Assume that a code word $\boldsymbol{c}$ was sent through a channel that added an error $\boldsymbol{e}$, i.e., the received vector is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$. Now H can be used to compute the *error syndrome*

$$\boldsymbol{s} = \boldsymbol{r}H^{\mathrm{t}} = \boldsymbol{c}H^{\mathrm{t}} + \boldsymbol{e}H^{\mathrm{t}} = \boldsymbol{e}H^{\mathrm{t}} \tag{5}$$

which depends only on the error $\boldsymbol{e}$, i.e., the syndrome is constant on the coset $C+\boldsymbol{e}$. The difficult task is then to deduce the most likely error from the syndrome (which is known to be NP–hard for certain channels [2]).

Nevertheless, there are some results about the error–correcting capabilities of linear codes. The *minimum (Hamming) distance* of a code C is defined by

$$\mathrm{d}_{\min}(C) := \min_{\substack{\boldsymbol{c},\boldsymbol{c}' \in C \\ \boldsymbol{c} \neq \boldsymbol{c}'}} \mathrm{d}_H(\boldsymbol{c}, \boldsymbol{c}') \qquad \text{where } \mathrm{d}_H(\boldsymbol{c}, \boldsymbol{c}') := |\{j\colon c_j \neq c'_j\}|.$$

For linear codes, the minimum distance equals the minimum weight since

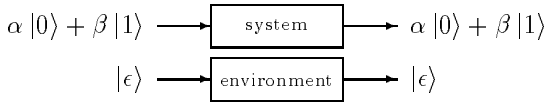
$$\mathrm{d}_H(\boldsymbol{c}, \boldsymbol{c}') = \mathrm{d}_H(\boldsymbol{c} - \boldsymbol{c}', \boldsymbol{0}) =: \mathrm{wgt}_H(\boldsymbol{c} - \boldsymbol{c}').$$

It is easy to show that a code with minimum distance d can detect any error $\boldsymbol{e}$ of weight $\mathrm{wgt}_H(\boldsymbol{e}) \leq d-1$ and correct any error of weight $\mathrm{wgt}_H(\boldsymbol{e}) \leq (d-1)/2$. When the minimum distance of a code is known it is added to the notation as $C = [n, k, \mathrm{d}_{\min}]_q$.

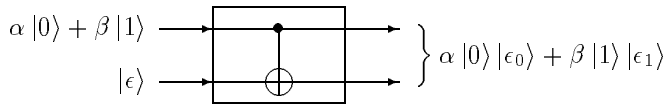
3 Quantum Error–Correcting Codes

3.1 The Error Model

The error free transmission (or storage) of a single qubit $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ without any interaction with the environment in the state $|\epsilon\rangle$ is depicted by:



The system and the environment remain uncorrelated which is reflected by the fact that the output state is still a tensor product. But if there is some interaction between the system and the environment (e.g., by photon absorption/emission), the situation changes:



Now the output states of the system and the environment might be entangled. This entanglement destroys interference as shown by the following calculation:

after error free transmission:

$$\begin{aligned}(H \otimes I_2)\left(\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|\epsilon\rangle\right) &= \tfrac{1}{2}(|0\rangle + |1\rangle)\,|\epsilon\rangle + \tfrac{1}{2}(|0\rangle - |1\rangle)\,|\epsilon\rangle \\ &= |0\rangle\,|\epsilon\rangle\end{aligned}$$

after interaction:

$$\begin{aligned}(H \otimes I_2)\left(\tfrac{1}{\sqrt{2}}(|0\rangle\,|\epsilon_0\rangle + |1\rangle\,|\epsilon_1\rangle)\right) &= \tfrac{1}{2}(|0\rangle + |1\rangle)\,|\epsilon_0\rangle + \tfrac{1}{2}(|0\rangle - |1\rangle)\,|\epsilon_1\rangle \\ &= \tfrac{1}{2}\,|0\rangle\,(|\epsilon_0\rangle + |\epsilon_1\rangle) + \underbrace{\tfrac{1}{2}\,|1\rangle\,(|\epsilon_0\rangle - |\epsilon_1\rangle)}_{\text{error term}}\end{aligned}$$

Similar to the classical case, for quantum registers the assumption is made that errors are restricted to a small number of qubits. In general, an error is modelled by linear, not necessarily unitary transformations. It has been shown (cf. [18]) that it is nevertheless sufficient to be able to correct so–called bit–flip errors, phase–flip errors, and their combination. A bit–flip error resembles the classical inversion of bit, whereas the phase–flip error has no classical equivalent. Here the relative phase between the state $|0\rangle$ and $|1\rangle$ is changed by π, i. e., the coefficient of the state $|1\rangle$ is multiplied by -1.

These elementary errors are modelled by the identity and the Pauli matrices

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \text{and} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (i^2 = -1).$$

The bit–flip error and the phase–flip error correspond to σ_x and σ_z, resp. An error on a quantum register of length n is represented by the tensor product of single qubit errors. Similar to the classical case, the weight of an error is defined to be the number of tensor factors different from identity.

3.2 Basic Principle

As discussed in section 2.3, for classical linear block codes the correctable errors and the error syndromes are in one–to–one correspondence. The set of all vectors of length n is partitioned into cosets of the code $C = [n, k]_q$, i. e.,

$$\mathbb{F}_q^n = C \,\dot\cup\, (C + \boldsymbol{e}_1) \,\dot\cup\, \ldots \,\dot\cup\, \left(C + \boldsymbol{e}_{q^{n-k}-1}\right). \tag{6}$$

This idea is adapted for quantum error–correcting codes. The code itself is a subspace of the whole space. Errors act now by multiplication with a unitary

matrix (cf. section 3.1). The set partitioning of equation (6) translates into an orthogonal decomposition of the whole vector space, i.e.,

$$\mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2 = \mathcal{C} \oplus (U_1\,\mathcal{C}) \oplus \ldots \oplus (U_{2^{n-k}-1}\,\mathcal{C})\,. \tag{7}$$

Instead of the computation of the syndrome, a partial (non–demolition) measurement is used to project onto one of this error spaces. In a final step, the error is corrected applying the inverse transformation U_i^{-1} (see Fig. 2).

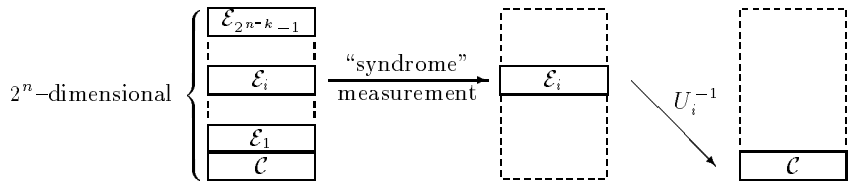


Fig. 2. Orthogonal decomposition of the 2^n–dimensional space into the 2^k–dimensional code space $\mathcal{C}$ and the error spaces $\mathcal{E}_i = U_i\,\mathcal{C}$

Unfortunately, the situation is a little bit more complicated than described above. It is not sufficient to construct an orthogonal decomposition into the code space and the error spaces. The information to be protected is represented by a linear combination of the basis states of the code space. Additionally, it has to be ensured that for all errors to be corrected the angles between the basis states of the code space are preserved.

In the following section we will show how classical linear block codes can be used to construct quantum error–correcting codes and how quantum circuits for encoding and syndrome computation/measurement can be derived from the generator matrix of the classical codes.

4 Binary Codes and Quantum Codes

4.1 Construction

The partitioning of the set of binary vectors into cosets of a linear binary block code $C = [n, k]$ (see equation (6)) can be directly translated into an orthogonal decomposition of $\mathbb{C}^{2^n}$ (see equation (7)) as shown in the following example. The cosets of the code $C = \{000, 111\}$ are given by:

C	$C + 001$	$C + 010$	$C + 100$
000	001	010	100
111	110	101	011

The orthogonal decomposition is obtained by replacing the binary vectors by the corresponding quantum states and the addition of the error vectors by multiplication with a tensor product of σ_x and id:

	$\mathcal{C}$	$(id \otimes id \otimes \sigma_x)\mathcal{C}$	$(id \otimes \sigma_x \otimes id)\mathcal{C}$	$(\sigma_x \otimes id \otimes id)\mathcal{C}$
basis	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|100\rangle$
	$\|111\rangle$	$\|110\rangle$	$\|101\rangle$	$\|011\rangle$

This yields a two–dimensional code which is able to correct one bit–flip error σ_x at any position. But the code cannot cope with arbitrary single qubit errors since it cannot correct phase–flip errors.

Using the Hadamard transformation H, phase–flip errors can be changed into bit–flip errors and vice versa since

$$H\sigma_x H^{-1} = \sigma_z \qquad \text{and} \qquad H\sigma_z H^{-1} = \sigma_x.$$

Furthermore, the Hadamard transformation $H^{\otimes n}$ relates a linear binary code $C = [n, k]$ and its dual $C^\perp$ in the following manner: Let χ_C be the characteristic function of the code, i.e., $\chi_C(\boldsymbol{c}) = 1$ if $\boldsymbol{c} \in C$ and $\chi_C(\boldsymbol{c}) = 0$ else. Then the characteristic function $\chi_{C^\perp}$ of the dual code is proportional to the Hadamard transformation $\widehat{\chi}_C$ of χ_C, i.e.,

$$|C| \cdot \chi_{C^\perp}(\boldsymbol{u}) = \widehat{\chi}_C(\boldsymbol{u}) := \sum_{\boldsymbol{v} \in \mathbb{F}_2^n} (-1)^{\boldsymbol{u}\cdot\boldsymbol{v}} \chi_C(\boldsymbol{v}).$$

These are the main results used in the proof of the following theorem.

Theorem 1. *Let $C_1 = [n, k_1, d_1]$ and $C_2 = [n, k_2, d_2]$ be linear binary block codes with $C_2^\perp \leq C_1$. Furthermore, let $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_K\}$ be a set of coset representatives of $C_1/C_2^\perp$.*

Then the $K = 2^{k_1-(n-k_2)}$ mutually orthogonal states

$$|\underline{i}\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{c} \in C_2^\perp} |\boldsymbol{c} + \boldsymbol{w}_i\rangle \tag{8}$$

span a quantum error correcting code $\mathcal{C} = [[n, k]]$ of length n and dimension 2^k where $k = k_1 - (n - k_2)$. (The notation is similar to that for classical linear block codes.) The code is able to correct up to $(d_1 - 1)/2$ bit–flip errors and up to $(d_2 - 1)/2$ phase–flip errors.

Proof. (Sketch)
A general state in the code space can be written as

$$|\psi\rangle = \sum_{\boldsymbol{i}} \alpha_i |\underline{i}\rangle = \sum_{\boldsymbol{i}} \alpha_i' \sum_{\boldsymbol{c} \in C_2^\perp} |\boldsymbol{c} + \boldsymbol{w}_i\rangle = \sum_{\boldsymbol{c} \in C_1} \beta_{\boldsymbol{c}} |\boldsymbol{c}\rangle . \tag{9}$$

Since this is a superposition of states corresponding to the (classical) linear code C_1, up to $(d_1 - 1)/2$ bit–flips can be corrected.

Hadamard transforming the state $|\underline{\boldsymbol{i}}\rangle$ (see equation (8)) results in

$$H^{\otimes n} |\underline{\boldsymbol{i}}\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{\boldsymbol{c} \in C_2} (-1)^{\boldsymbol{c} \cdot \boldsymbol{w}_i} |\boldsymbol{c}\rangle .$$

Hence the Hadamard transform of $|\psi\rangle$ (see equations (9)) can be written as

$$H^{\otimes n} |\psi\rangle = \sum_{\boldsymbol{c} \in C_2} \gamma_{\boldsymbol{c}} |\boldsymbol{c}\rangle . \tag{10}$$

As this is a superposition of states corresponding to C_2, up to $(d_2 - 1)/2$ bit–flip errors with respect to the Hadamard transformed basis can be corrected, i.e., up to $(d_2 - 1)/2$ phase–flip errors in the original basis can be corrected.

Corollary 1. *Theorem 1 applies particularly to weakly self dual codes C, i.e., $C \leq C^{\perp}$ (setting $C_1 = C_2 = C^{\perp}$).*

Next we will show how a quantum circuit for the encoding process can be constructed.

4.2 Encoding

As an example, we consider the linear binary Hamming code $C = [7, 4, 3]$ that is the linear row–span of the matrix G_1. The dual code $C^{\perp} = [7, 3, 4]$ is generated by G_2, where

$$G_1 = \begin{pmatrix} 1\,0\,0\,0\,1\,1\,0 \\ 0\,1\,0\,0\,0\,1\,1 \\ 0\,0\,1\,0\,1\,1\,1 \\ 0\,0\,0\,1\,1\,0\,1 \end{pmatrix} \qquad \text{and} \qquad G_2 = \begin{pmatrix} 1\,0\,0\,1\,0\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1\,1 \end{pmatrix} .$$

Since the Hamming code contains its dual, we can construct a quantum error–correcting code using Theorem 1 with $C_1 = C_2 = C$. The last three rows of the matrix

$$G = \left(\begin{array}{c} 0\,0\,0\,1\,1\,0\,1 \\ \hline 0\,0\,1\,0\,1\,1\,1 \\ 0\,1\,0\,1\,1\,1\,0 \\ 1\,0\,0\,1\,0\,1\,1 \end{array}\right) = \left(\begin{array}{c} \boldsymbol{g}_4 \\ \hline \boldsymbol{g}_3 \\ \boldsymbol{g}_2 \\ \boldsymbol{g}_1 \end{array}\right) \tag{11}$$

generate $C^{\perp}$, and $\boldsymbol{w}_0 = (0, 0, 0, 0, 0, 0, 0)$ and $\boldsymbol{w}_1 = \boldsymbol{g}_4$ are representatives of the cosets $C/C^{\perp}$. The states of the quantum code (cf. equation (8)) can be written

as

$$|\underline{\mathbf{0}}\rangle = \frac{1}{\sqrt{8}} \sum_{i_1,i_2,i_3 \in \{0,1\}} |0\boldsymbol{g}_4 + i_3\boldsymbol{g}_3 + i_2\boldsymbol{g}_2 + i_1\boldsymbol{g}_1\rangle$$
$$\text{and} \quad |\underline{\mathbf{1}}\rangle = \frac{1}{\sqrt{8}} \sum_{i_1,i_2,i_3 \in \{0,1\}} |1\boldsymbol{g}_4 + i_3\boldsymbol{g}_3 + i_2\boldsymbol{g}_2 + i_1\boldsymbol{g}_1\rangle\,. \tag{12}$$

(Note the similarity to the classical encoding in equation (3).)

Based on the fact that the matrix G in equation (11) is in lower triangular form, a quantum circuit for the encoding $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \mapsto \alpha\,|\underline{\mathbf{0}}\rangle + \beta\,|\underline{\mathbf{1}}\rangle = |\psi\rangle$ can be deduced directly from G (see Fig. 3).

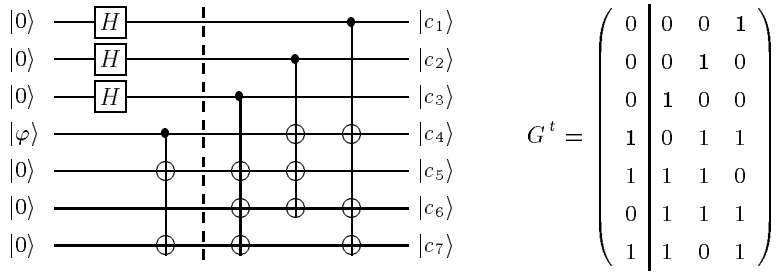


Fig. 3. Encoding "binary" quantum codes

The upper three lines correspond to i_1, i_2, and i_3 in (12). The Hadamard gates H produce a superposition of $|0\rangle$ and $|1\rangle$ corresponding to the summation indices. The next four rows of $CNOT$ gates correspond to the summands $i_j\,\boldsymbol{g}_j$ in (12). Whenever the control qubit corresponding to i_j is one, the qubits corresponding to positions of $\boldsymbol{g}_j$ being one are inverted.

4.3 Syndrome Computation

The next task in the process of error correction is to perform the "syndrome" measurement (cf. section 3.2). As shown in the proof of Theorem 1, bit–flip errors and phase–flip errors can be treated separately. A bit–flip error on n qubits can be written as

$$E_{\text{bit}}(\boldsymbol{e}) = {\sigma_x}^{e_1} \otimes {\sigma_x}^{e_2} \otimes \ldots \otimes {\sigma_x}^{e_n},$$

where $\boldsymbol{e} = (e_1, e_2, \ldots, e_n) \in \mathbb{F}_2^n$. This error operator changes a general state of the code (9) to

$$E_{\text{bit}}(\boldsymbol{e}) \left(\sum_{\boldsymbol{c} \in C_1} \beta_{\boldsymbol{c}}\,|\boldsymbol{c}\rangle \right) = \sum_{\boldsymbol{c} \in C_1} \beta_{\boldsymbol{c}}\,|\boldsymbol{c} + \boldsymbol{e}\rangle\,.$$

Now we compute the error syndrome of the vector $\boldsymbol{c}+\boldsymbol{e}$ with respect to a parity check matrix H_1 of the code C_1 using auxiliary qubits as syndrome register. This results in the state

$$\sum_{\boldsymbol{c}\in C_1} \beta_{\boldsymbol{c}} \Big(|\boldsymbol{c}+\boldsymbol{e}\rangle \otimes |(\boldsymbol{c}+\boldsymbol{e})H_1^{\mathrm{t}}\rangle \Big) = \left(\sum_{\boldsymbol{c}\in C_1} \beta_{\boldsymbol{c}} \, |\boldsymbol{c}+\boldsymbol{e}\rangle \right) \otimes |\boldsymbol{e}H_1^{\mathrm{t}}\rangle \, . \qquad (13)$$

As the error syndrome $\boldsymbol{s} = \boldsymbol{e}H_1^{\mathrm{t}}$ is independent of $\boldsymbol{c}$, the state (13) is a tensor product and measuring the syndrome register does not disturb the state of the code register. The measurement reveals the classical syndrome $\boldsymbol{s}$ from which it is possible to derive the (classical) error vector $\boldsymbol{e}$. This allows to correct the (quantum mechanical) bit–flip errors.

The treatment of the phase–flip errors is very similar to that of the bit–flip errors due to their duality using Hadamard transformation. A phase–flip error of the form

$$E_{\mathrm{phase}}(\boldsymbol{e}) = {\sigma_z}^{e_1} \otimes {\sigma_z}^{e_2} \otimes \ldots \otimes {\sigma_z}^{e_n}$$

acts on the state (9) as

$$E_{\mathrm{phase}}(\boldsymbol{e}) \left(\sum_{\boldsymbol{c}\in C_1} \beta_{\boldsymbol{c}} \, |\boldsymbol{c}\rangle \right) = \sum_{\boldsymbol{c}\in C_1} \beta_{\boldsymbol{c}} (-1)^{\boldsymbol{e}\cdot\boldsymbol{c}} \, |\boldsymbol{c}\rangle \, .$$

After Hadamard transformation the state is of the form (cf. equation (10))

$$\sum_{\boldsymbol{c}\in C_2} \gamma_{\boldsymbol{c}} \, |\boldsymbol{c}+\boldsymbol{e}\rangle$$

since the phase–errors are changed into bit–flip errors. Using the same technique as described above, the syndrome with respect to a parity check matrix H_2 of the code C_2 can be measured. After another Hadamard transformation we return to the original basis.

Again, we use the example of the Hamming code $C = [7, 4, 3]$ to illustrate the preceding. As $C_1 = C_2 = C$ in the construction of the quantum code using Theorem 1, the syndromes for both the bit–flip errors and the phase–flip errors are computed using a parity check matrix for C. For this, we can use the generator matrix

$$G_2^{\mathrm{t}} = H^{\mathrm{t}} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

of the dual $C^{\perp}$ of the Hamming code. The quantum circuit for the computation of the whole "quantum syndrome" is shown in Fig. 4.

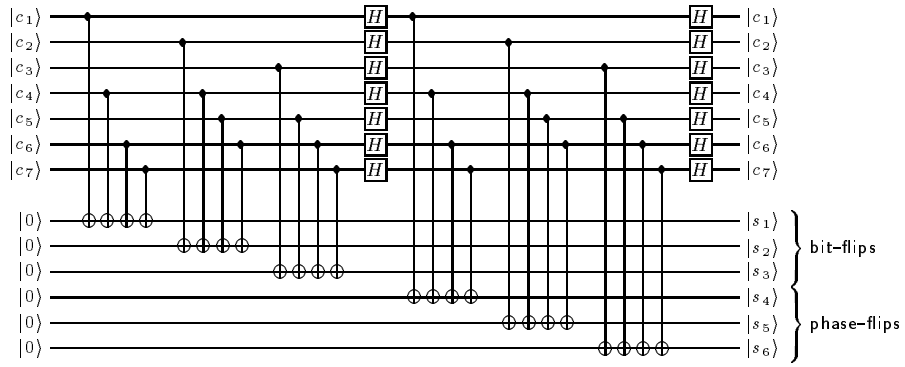


Fig. 4. Syndrome computation for "binary" quantum codes

The first group of four $CNOT$ gates corresponds to the computation of the inner product of the vector $\boldsymbol{c} = (c_1, c_2, \ldots, c_7)$ with the first column of the parity check matrix H^{t}. (Recall from equation (2) that a $CNOT$ gate maps the state $|a\rangle\,|b\rangle$ to $|a\rangle\,|a \oplus b\rangle$.) The next two groups of $CNOT$ gates serve to compute the inner products of $\boldsymbol{c}$ with the second and third column of H^{t}. After the Hadamard transform, the syndrome corresponding to phase–flip errors is computed in the same manner.

5 More Relations between Classical and Quantum Codes

Quantum error–correcting codes can not only be constructed from classical linear binary codes, but also from quaternary codes (cf. [4]). Again, quantum circuits for encoding and syndrome computation can be directly derived from certain generator and parity check matrices of the classical codes (see [9, 15]). Another class of quantum error–codes, the class of non–binary codes, parallels classical non–linear codes (cf. [14]).

It is also possible to construct classical error–correcting codes from some quantum error–correcting codes (see [8]). Although the codes obtained are not of great interest to be used in their original context, namely for error correction, the construction allows the translation of bounds for classical codes into bounds for quantum error–correcting codes. Such bounds are also obtained via a quantum version of the famous MacWilliams identities (see [19] and [21]).

In this paper, we have not addressed one of the major problems of coding theory, the question of how to determine the most likely error given the error syndrome. This is subject of ongoing research (see, e. g., [3, 15, 16]).

References

1. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, *Elementary gates for quantum computation*, Physical Review A, 52 (1995), pp. 3457–3467. See also LANL preprint quant–ph/9503016.
2. E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems*, IEEE Transactions on Information Theory, IT–24 (1978), pp. 384–386.
3. T. Beth and M. Grassl, *Improved Decoding of Quantum Error Correcting Codes from Classical Codes*, in PhysComp96, T. Toffoli, M. Biafore, and J. Leão, eds., Boston, Nov. 1996, pp. 28–31.
4. ———, *The Quantum Hamming and Hexacodes*, Fortschritte der Physik, 46 (1998), pp. 459–491.
5. A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum Error Correction Via Codes over GF(4)*, IEEE Transactions on Information Theory, IT–44 (1998), pp. 1369–1387. See also LANL preprint quant–ph/9608006.
6. A. R. Calderbank and P. W. Shor, *Good quantum error–correcting codes exist.*, Physical Review A, 54 (1996), pp. 1098–1105. See also LANL preprint quant–ph/9512032.
7. J. I. Cirac and P. Zoller, *Quantum Computation with Cold Trapped Ions*, Physical Review Letters, 74 (1995), pp. 4091–4094.
8. R. Cleve, *Quantum Stabilizer Codes and Classical Linear Codes*, Physical Review A, 55 (1997), pp. 4054–4059.
9. R. Cleve and D. Gottesman, *Efficient computations of encodings for quantum error correction*, Physical Review A, 56 (1997), pp. 76–82.
10. D. G. Cory, A. F. Fahmy, and T. F. Havel, *Ensemble Quantum Computing by Nuclear Resonance Spectroscopy*, Tech. Rep. TR–10–96, B. C. M. P., Harvard Medical Medical School, Boston, Dec. 1996.
11. A. Ekert and C. Macchiavello, *Quantum Error Correction for Communication*, Physical Review Letters, 77 (1996), pp. 2585–2588.
12. N. A. Gershenfeld and I. L. Chuang, *Bulk Spin–Resonance Quantum Computation*, Science, 275 (1997), pp. 350–356.
13. D. Gottesman, *A Class of Quantum Error–Correcting Codes Saturating the Quantum Hamming Bound*, Physical Review A, 54 (1996), pp. 1862–1868. See also LANL preprint quant–ph/9604038.
14. M. Grassl and T. Beth, *A Note on Non–Additive Quantum Codes*, Tech. Rep. quant–ph/9703016, Los Alamos National Laboratory, 1997.
15. ———, *Codierung und Decodierung zyklischer Quantencodes*, in Fachtagung Informations– und Mikrosystemtechnik, B. Michaelis and H. Holub, eds., Magdeburg, 25.–27. Mar. 1998, Otto–von–Guericke–Universität Magdeburg, Fakultät für Elektrotechnik, Institut für Prozeßmeßtechnik und Elektronik (IPE), LOGISCH GmbH, pp. 137–144.
16. M. Grassl, T. Beth, and T. Pellizzari, *Codes for the Quantum Erasure Channel*, Physical Review A, 56 (1997), pp. 33–38. See also LANL preprint quant–ph/9610042.
17. D. M. Greenberger, M. Horne, and A. Zeilinger, *Going beyond Bell's Theorem*, in Bell's Theorem, Quantum Theory, and Conceptions of the Universe, M. Kafatos, ed., Kluwer, Dordrecht, 1989, pp. 73–77.

18. E. Knill and R. Laflamme, *Theory of quantum error–correcting codes*, Physical Review A, 55 (1997), pp. 900–911. See also LANL preprint quant–ph/9604034.
19. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*, North–Holland, Amsterdam, 1977.
20. T. Pellizzari, S. A. Gardiner, J. I. Cirac, and P. Zoller, *Decoherence, Continuous Observation, and Quantum Computing: A Cavity QED Model*, Physical Review Letters, 75 (1995), pp. 3788–3791.
21. P. Shor and R. Laflamme, *Quantum Analog of the MacWilliams Identities for Classical Coding Theory*, Physical Review Letters, 78 (1997), pp. 1600–1602. See also LANL preprint quant–ph/9610040.
22. P. W. Shor, *Algorithms for Quantum Computation: Discrete Logarithm and Factoring*, in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, IEEE Computer Society Press, Nov. 1994, pp. 124–134. See also LANL preprint quant-ph/9508027.
23. ———, *Scheme for reducing decoherence in quantum computer memory*, Physical Review A, 52 (1995), pp. R2493–R2496.
24. A. Steane, *Error Correcting Codes in Quantum Theory*, Physical Review Letters, 77 (1996), pp. 793–797.
25. ———, *Multiple Particle Interference and Quantum Error Correction*, Proceedings of the Royal Society London Series A, 452 (1996), pp. 2551–2577. See also LANL preprint quant–ph/9601029.
26. W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature, 299 (1982), pp. 802–803.

Some of the papers are also available at the LANL archive (`http://xxx.lanl.gov`)