QUANTUM COMPUTING 11.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

November 20, 2002

11. QUANTUM ERROR CORRECTION CODES

Quantum computing based on pure states and unitary evolutions is an idealization that works fine for the so-called closed (idealised) quantum systems.

In any real quantum computing one has to assume an interaction between the quantum system used for computing and its environment. This has deep and negative consequences, for potential to have stable quantum memory and error-free quantum computation, termed as **decoherence**.

Strong scepticism concerning the possibility to have powerful quantum computers has been mainly due to the phenomenon of decoherence.

Quantum error correcting codes and quantum fault-tolerant computation methods represent a powerful way to fight decoherence.

QUANTUM DECOHERENCE

Decoherence is the process of interaction of a quantum system with its environment.

An interaction of a quantum system with its environment causes that some of its states get entangled with the states of the environment and that can destroy supersensitive quantum superpositions.

Quantum system	t_s	τ_{dec}	comput. steps
Mössbauer nucleus	10^{-19}	10^{-10}	10^{9}
GaAs electrons	10^{-13}	10^{-10}	10^{3}
Au 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: Switching time t_s, decoherence τ_{dec}, both in seconds, and the number of computation steps performed before decoherence impacts occur

Moreover, as a quantum system evolves, information about its states leaks into environment, causing the states to loose their purity and, consequently, their ability to interfer.

Decoherence is the main enemy of the potential quantum computers.

A WAY OUT — QUANTUM ERROR-CORRECTING CODES

CLASSICAL LINEAR CODES

The **Hamming distance** of two words u and v, notation $hd(u,v)$, is the number of symbols in which u and v differ.

A **binary code** C is a subset of $\{0,1\}^n$ for some n; its elements are called **codewords**. For error detection and correction the minimal distance $d(C)$ of a code C is of importance.

$$d(C) = \min\{hd(u,v) \,|\, u,v \in C, u \neq v\}.$$

This allows us to formulate one of the most basic results of the error-detecting and -correcting codes.

Theorem 0.1 *(1) A code C can detect up to s errors in any codeword if and only if $d(C) \geq s+1$; (ii) A code C can correct up to t errors if and only if $d(C) \geq 2t+1$.*

Definition 0.2 *An (n,M,d)-**code** is a code of M words of length n and minimal distance d.*

A very important class of codes are so-called linear codes.

Definition 0.3 *A binary code C is linear if for any two codewords $w_1, w_2 \in C$ also $w_1 \oplus w_2$ is in C. A linear code of codewords of length n form a subspace of n-dimensional vector space over $\mathbf{Z_2}$.*

If the dimension *dim*(C) of a linear code C, as that of the subspace C, is k then C is said to be an $[n,k]$-code. In addition if C is of distance d, then it is said to be $[n,k,d]$-**code**.

If C is a linear code, then $C^\perp = \{w \,|\, u \cdot w = 0$ if $u \in C\}$ is called the **dual code** to C. A code C is **self-dual** if $C^\perp = C$.

A matrix G whose rows are all vectors of a basis of a linear code C (as a subspace) is said to be a **generator** of C. A generator matrix H of the dual code $C^\perp$ is called the **parity-check** matrix of C.

EXAMPLES of LINEAR CODES

Code

$$C = \{000, 011, 101, 110\}$$

is linear and his generating matrix has the form

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

Code

$$\begin{aligned} C' \;=\{ \;& 0000000, 1111111, 1000101, 1100010 \\ & 0110001, 1011000, 0101100, 0010110 \\ & 0001011, 01110101, 00111101, 1001110 \\ & 0100111, 1010011, 1101001, 1110100\} \end{aligned}$$

is also linear and its generating matrix has the form

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

CHANNELS, CODES and CORRECTABLE ERRORS

A noisy communication channel changes a message u to u'. The difference $e = u' - u$ is called error (word, vector).

A set $\mathcal{E}$ of errors is said to be correctable by a code C if for $e_i \neq e_j$ or $u \neq v$:

$$u + e_i \neq v + e_j . \forall u, v \in C (u \neq v).$$

Example Let channel errors occur in bursts affecting always pairs, i.e. let error vectors are $\mathcal{E} = \{00, 11\}$. This set of errors is correctable by the code

$$\{00, 01\}.$$

Example Let a channel changes a bit with probability $p < \frac{1}{2}$. Then the code

$$C = \{000, 111\}$$

corrects the set of errors

$$\mathcal{E} = \{000, 100, 010, 001\}.$$

ENCODING and SYNDROME DECODING for LINEAR CODES

Encoding with linear codes.

If C is an linear $[n, k]$-code with a generator matrix G, then C contains 2^k codewords and therefore it can be used to communicate up to 2^k distinct messages.

Let us identify messages with binary words of length k. Encoding of a message u is done by the matrix multiplication uG.

Syndrome decoding with linear codes

is also easy, but several new concepts are needed.

Definition 0.4 *If C is a linear binary $[n, k]$-code and a is any binary vector of length n then the set $a + C = \{a + x \mid x \in C\}$ is called the* **coset** *of C. A vector of a coset with the minimum weight is its* **leader** *(which does not have to be unique).*

Algorithm 0.5 (Syndrome decoding for linear codes) *Given a word y to decode do the following;*
1. compute $S(y) = yH^T$;
2. Decode y as $y - l_y$, where l_y is the coset leader in the coset with the syndrome $S(y)$.

PROBLEMS with QUANTUM ERROR CORRECTING CODES

There seemed to be reasons to believe that powerful quantum error correcting codes are impossible.

1. The variety of possible errors seems to be much larger (even infinite).
2. Faithful copying of quantum information is impossible due to no-cloning theorem.
3. The assumption that encoding and decoding are error free is much less realistic.
4. QECC would need to have potential "to fight exponentially growing decoherence in polynomial time" what seemed to be impossible.

BASIC IDEAS and BASIC EXAMPLES

The very basic idea of quantum computation with quantum error-correcting codes goes as follows:

Quantum evolution is restricted to a subspace of a Hilbert space that is carefully chosen in such a way that if quantum bits are encoded using states of the chosen subspace, then all departures from this subspace, due to errors, lead to mutually orthogonal subspaces.

Code	$\|0_E\rangle$	$\|1_E\rangle$
Shor's 9 qb code	$(X)(X)(X)$ $X = \|000\rangle + \|111\rangle$	$(Y)(Y)(Y)$ $Y = \|000\rangle - \|111\rangle$
Steane's 7 qb code	$\|0000000\rangle + \|1010101\rangle + \|0110011\rangle$ $+\|1100110\rangle + \|0001111\rangle + \|1011010\rangle$ $\|0111100\rangle + \|1101001\rangle$	$\|1111111\rangle + \|0101010\rangle + \|1001100\rangle$ $+\|0011001\rangle + \|1110000\rangle + \|0100101\rangle$ $+\|1000011\rangle + \|0010110\rangle$
LMPZ's 5 qb code	$+\|00000\rangle + \|11100\rangle - \|10011\rangle - \|01111\rangle$ $+\|11010\rangle + \|00110\rangle + \|01001\rangle + \|10101\rangle$	$-\|00011\rangle + \|11111\rangle - \|10000\rangle + \|01100\rangle$ $+\|11001\rangle - \|00101\rangle - \|01010\rangle + \|10110\rangle$
Barenco's 3 qb code	$\|000\rangle + \|011\rangle + \|101\rangle + \|110\rangle$	$\|111\rangle + \|100\rangle + \|010\rangle + \|001\rangle$

Figure 1: Examples of 1-qubit quantum error-correcting codes; all superpositions are equally weighted, but amplitudes are omitted in the table

After a quantum state is entangled with the environment and an "error" occurs , one can determine, by a measurement, but without destroying the "erroneous state", into which of the erroneous subspaces the erroneous state has felt, and an error can be undone using a unitary transformation.

ERROR CORRECTION SETTING

Alice encodes a to-be-sent quantum state into a new quantum state which is then sent through a noisy channel on which an error operator operates (changes the state).

Encoding has to be such that even if the error operator changes the state being transmitted, it cannot entangle it with the environment.

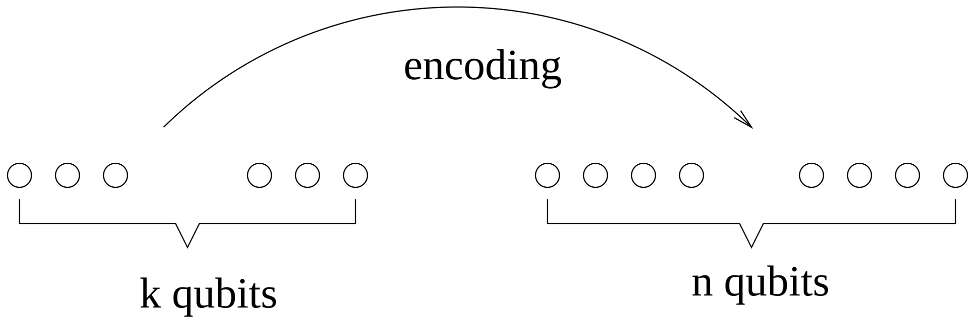
Consequently, Bob, who can act on the state he receives, but not on the environment, is then able to determine which error was made, and then Bob can undo its effect and to receive the original state.

For Bob to be able to undo the error effect, no information about the state Alice sends should leak into the environment.

ENCODING IDEA

The idea is to use such encodings that encoded

quantum information of k qubits is spread out over n qubits



in a non-local way, through an entangled state in such a way that environment which can access only a small number of qubits can gain no information about the overall state being transmitted and this way the transmitted quantum state is protected.

ERROR MODELS

Noise and decoherence can be described in terms of the most general quantum operators — superoperators — in terms of unitary operators on the system and its environment.

A large variety of quantum errors is possible. However, successful QECC can be developed under the assumption that errors are:

- **Locally independent** (that is errors in different qubits or gates are not correlated).
- **Sequentially independent** (That is subsequent errors on the same qubit are not correlated).

No knowledge about the physical nature of errors will be assumed.

As a consequence, an error on n qubits can be written at each time step as a tensor product of errors on particular qubits.

If the above conditions are satisfied, then it is believed that errors are correctable provided that error rate is below 10^{-5} per qubit and clock cycle.

ERROR DECOMPOSITION

Any interaction between a qubit

$$\alpha|0\rangle + \beta|1\rangle$$

and environment has the form

$$\begin{aligned} |e\rangle(\alpha|0\rangle + \beta|1\rangle) &\rightarrow \alpha(|e_{00}\rangle|0\rangle + |e_{01}\rangle|1\rangle) + \beta(|e_{11}\rangle|1\rangle + |e_{10}\rangle|0\rangle) \\ &= (|e_{0+}\rangle I + |e_{0-}\rangle\sigma_z + |e_{1+}\rangle\sigma_x - |e_{1-}\rangle i\sigma_y)(\alpha|0\rangle + \beta|1\rangle), \end{aligned}$$

where $|e\rangle, \{|e_{ij}\rangle, | \, i, j \in \{0,1\}\}$ are states of the environment, $\sigma_x, \sigma_y, \sigma_z$ are Pauli matrices, and

$$|e_{0+}\rangle = \frac{1}{2}(|e_{00}\rangle + |e_{10}\rangle) \qquad |e_{0-}\rangle = \frac{1}{2}(|e_{00}\rangle - |e_{10}\rangle)$$

$$|e_{1+}\rangle = \frac{1}{2}(|e_{01}\rangle + |e_{11}\rangle) \qquad |e_{1-}\rangle = \frac{1}{2}(|e_{01}\rangle - |e_{11}\rangle)$$

CONSEQUENCES

- Any quantum error can be seen as being composed of four basic errors and therefore if we are able to correct any of these four types of errors we can correct any error.
- Error model resembles more a discrete one than a continuous one.
- The resulting state of the environment is independent of the state on which an error process acts and depends only on the type of error operators being applied.

BASIC ERROR TYPES

Three Pauli matrices represents three basic types of errors:

- σ_x — **bit error**
- σ_z — **sign error**
- σ_y — **bit-sign error**

This is due to the following impacts Pauli matrices have on a qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$\begin{aligned}
\sigma_x(\alpha|0\rangle + \beta|1\rangle) &: \alpha|1\rangle + \beta|0\rangle; \\
\sigma_z(\alpha|0\rangle + \beta|1\rangle) &: \alpha|0\rangle - \beta|1\rangle; \\
\sigma_x\sigma_z(\alpha|0\rangle + \beta|1\rangle) &: \alpha|1\rangle - \beta|0\rangle; \\
-i\sigma_y|\phi\rangle(\alpha|0\rangle + \beta|1\rangle) &: \alpha|1\rangle - \beta|0\rangle.
\end{aligned}$$

General type of errors:

$$M = \bigotimes_{i=1}^{n} M_i,$$

where

$$M_i \in \{X, Y, Z, I\}, X = \sigma_x, Z = \sigma_z, Y = \sigma_x\sigma_z.$$

For the case all $M_i \in \{X, I\}$ $(M_i \in \{I, Z\})$ error operators are usually written as

$$X_u \quad (Z_u)$$

where $u \in \{0,1\}^n$ and $M_i = X$ $(M_i = Z)$ if and only if $u_i = 1$.

GENERAL ERROR CORRECTION

Let an extra ancilla qubit, initially in state $|0\rangle$, records what type of errors occurs.

$$\sigma_z(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle_{an} \rightarrow (\alpha|0\rangle - \beta|1\rangle) \otimes |\sigma_z\rangle_{an}$$
$$I(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle_{an} \rightarrow (\alpha|0\rangle + \beta|1\rangle) \otimes |no - error\rangle_{an}$$

If the actual error is

$$R_{\theta/2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta/2} \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} = (\cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}\sigma_z)e^{i\theta/2},$$

then recording the error in the ancilla gives us a superposition

$$e^{i\theta/2}(\cos\frac{\theta}{2}I(\alpha|0\rangle + \beta|1\rangle) \otimes I_{an} - i\sin\frac{\theta}{2}(\alpha|0\rangle - \beta|1\rangle) \otimes |\sigma_z\rangle_{an})$$

If we now measure the ancilla we get with probability $\sin^2\theta/2$

$$(\alpha|0\rangle - \beta|1\rangle) \otimes |\sigma_z\rangle_{an}$$

and with probability $\cos^2\theta/2$ we get

$$I(\alpha|0\rangle + \beta|1\rangle) \otimes I_{an}.$$

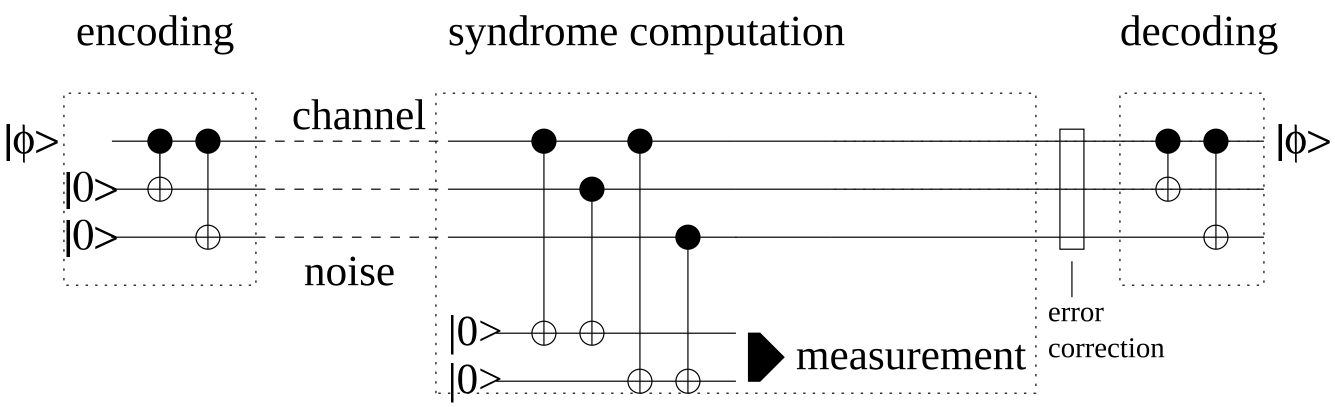
In each case, inverting the error indicated in the ancilla restores the original state.

The above arguments work for any linear combination of errors.
Theorem If a quantum code corrects errors E_a and E_b, it also corrects any linear combination of E_a and E_b. In particular, if it corrects all weight t Pauli errors, then the code corrects all t-qubit errors.

QECC — EXAMPLE

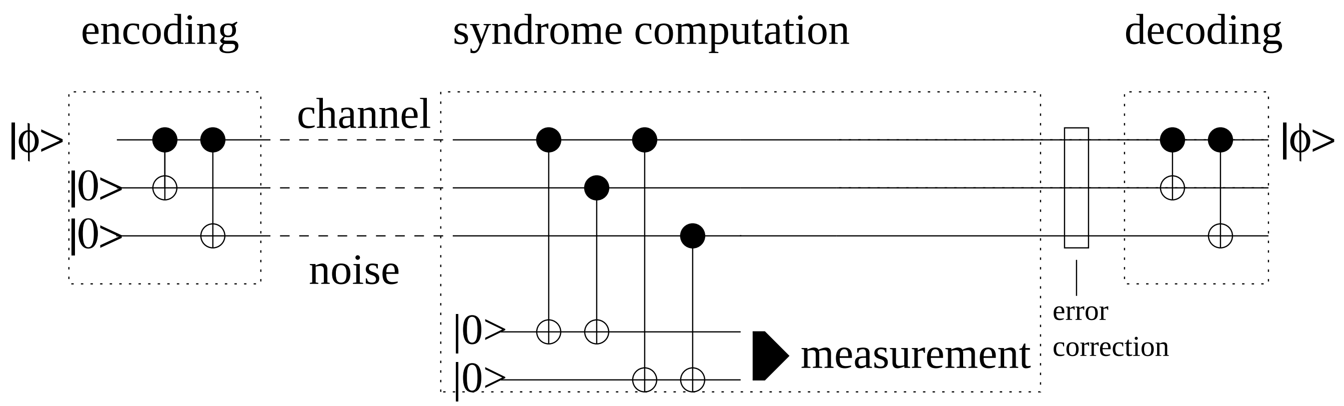
Example of a qubit communication process through a noisy channel using a 3-qubit bit-error correction code.

Alice: encoding. Alice encodes the qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ by a network of two XOR gates and two additional qubits in the ancilla state $|00\rangle$ into the entangled state $\alpha|000\rangle + \beta|111\rangle$, see Figure.



Noisy channel. A bit error is assumed to occur with probability $p > \frac{1}{2}$ on any qubit and results in one of the states shown bellow:

state	probability
$\alpha\|000\rangle + \beta\|111\rangle$	$(1-p)^3$
$\alpha\|100\rangle + \beta\|011\rangle$	$p(1-p)^2$
$\alpha\|010\rangle + \beta\|101\rangle$	$p(1-p)^2$
$\alpha\|001\rangle + \beta\|110\rangle$	$p(1-p)^2$
$\alpha\|110\rangle + \beta\|001\rangle$	$p^2(1-p)$
$\alpha\|101\rangle + \beta\|010\rangle$	$p^2(1-p)$
$\alpha\|011\rangle + \beta\|100\rangle$	$p^2(1-p)$
$\alpha\|111\rangle + \beta\|000\rangle$	p^3



BOB: Syndrome computation process: By using two additional ancilla qubits in state $|00\rangle$ and four XOR operations syndromes of errors can be computed as shown in the following table

state	probability
$(\alpha\|000\rangle + \beta\|111\rangle)\|00\rangle$	$(1-p)^3$
$(\alpha\|100\rangle + \beta\|011\rangle)\|11\rangle$	$p(1-p)^2$
$(\alpha\|010\rangle + \beta\|101\rangle)\|10\rangle$	$p(1-p)^2$
$(\alpha\|001\rangle + \beta\|110\rangle)\|01\rangle$	$p(1-p)^2$
$(\alpha\|110\rangle + \beta\|001\rangle)\|01\rangle$	$p^2(1-p)$
$(\alpha\|101\rangle + \beta\|010\rangle)\|10\rangle$	$p^2(1-p)$
$(\alpha\|011\rangle + \beta\|100\rangle)\|11\rangle$	$p^2(1-p)$
$(\alpha\|111\rangle + \beta\|000\rangle)\|00\rangle$	p^3

Error correction. Bob does nothing if syndrome is 00 and performs σ_x operation

on third qubit if syndrome is 01
on second qubit if syndrome is 10
on first qubit if syndrome is 11

Resulting state is either $\alpha|000\rangle + \beta|111\rangle$ or $\beta|000\rangle + \alpha|111\rangle$.
Final decoding provides either the state $\alpha|0\rangle + \beta|1\rangle$ or the state $\beta|0\rangle + |1\rangle$.

VARIATIONS on SYNDROME COMPUTATIONS

Syndrome computation can be seen in the above example as a measurement with the following four projection operators

$$
\begin{array}{lcll}
P_0 & \equiv & |000\rangle\langle 000| + |111\rangle\langle 111| & \text{no error} \\
P_1 & \equiv & |100\rangle\langle 100| + |011\rangle\langle 011| & \text{bit flip on first qubit} \\
P_2 & \equiv & |010\rangle\langle 010| + |101\rangle\langle 101| & \text{bit flip on second qubit} \\
P_3 & \equiv & |001\rangle\langle 001| + |110\rangle\langle 110| & \text{bit flip on third qubit}
\end{array}
$$

Observe that our error correction procedure works perfectly if there is at most one bit error, that is with probability

$$(1-p)^3 + 3p(1-p)^2 = 1 - 3p^2 + 2p^3.$$

IMPROVED ERROR ANALYSIS

If a bit error occurs with probability p, then without error-correction the resulting state, after the transmission through the noisy channel of the qubit $|\phi\rangle = a|0\rangle + b|1\rangle$, is

$$\rho = (1-p)|\phi\rangle\langle\phi| + p\sigma_X|\phi\rangle\langle\phi|\sigma_x.$$

The fidelity is given by

$$F = \sqrt{\langle\phi|\rho|\phi\rangle} = \sqrt{(1-p) + p\langle\phi|\sigma_x|\phi\rangle\langle\phi|\sigma_x|\phi\rangle}.$$

Minimum fidelity is $F = \sqrt{1-p}$ if $|\phi\rangle = |0\rangle$.

On the other hand, the resulting mixed state after both the noise and error correction is

$$\rho = [(1-p)^3 + 3p(1-p)^2]\phi\rangle\langle\phi| + \dots$$

and the fidelity is

$$F = \sqrt{\langle\phi|\rho|\phi\rangle} \geq \sqrt{(1-p)^3 + 3p(1-p)^2}.$$

Hence, the fidelity is improved provided $p < \frac{1}{2}$.

SIGN-ERROR CASE

Let us now assume that instead of a bit-error channel we have sign error channel that with probability p changes the state $|\phi\rangle = a|0\rangle + b|1\rangle$ into the state $a|0\rangle - b|1\rangle$.

Observe

$$\begin{aligned}
\sigma_x|0\rangle &= |1\rangle, \quad \sigma_x|1\rangle = |0\rangle; \\
\sigma_x|0'\rangle &= |0'\rangle, \quad \sigma_x|1'\rangle = -|1'\rangle; \\
\sigma_z|0\rangle &= |0\rangle, \quad \sigma_z|1\rangle = -|1\rangle; \\
\sigma_z|0'\rangle &= |1'\rangle, \quad \sigma_z|1'\rangle = |0'\rangle.
\end{aligned}$$

Hence, sign error in the standard basis $\{|0\rangle, |1\rangle\}$ is the bit error in the dual basis $\{|0'\rangle, |1'\rangle\}$.

The corresponding encoding is then

$$|0\rangle = |0'0'0'\rangle \quad |1\rangle = |1'1'1'\rangle$$

and hence the corresponding encoding circuit is then obtained by adding one Hadamard transformation gate on each qubit after encoding circuit for bit error.

QUANTUM ERROR CORRECTION PROCESS I

ENCODING PROCESS

Encoding of k qubits into $n > k$ qubits is done by first introducing $n - k$ new, auxiliary, qubits (an **ancilla**), in a special state, say $|0^{(n-k)}\rangle$, and then

> any k qubit state $|\phi\rangle$ is mapped using a (unitary) **encoding** transformation E

as follows

$$E(|\phi\rangle|0^{(n-k)}\rangle \rightarrow |\phi_E\rangle$$

and $|\phi_E\rangle$ is said to be **quantum code (codeword)** of $|\phi\rangle$ determined by E.

> Encodings of the basis states of k qubits form an orthonormal basis of a 2^k-dimensional subspace of H_{2^n}.

$$E|0\rangle \rightarrow |0_E\rangle,$$
$$E|1\rangle \rightarrow |1_E\rangle,$$

QUANTUM ERROR CORRECTION PROCESS II

ERRORS

If an error occurs in a state $|\phi_E\rangle$, then $|\phi_E\rangle$ is altered by some superoperator $\mathcal{E}$ to have

$$|\phi_E\rangle \stackrel{\mathcal{E}}{\to} |\mathcal{E}\phi_E\rangle.$$

ERROR CORRECTION PROCESS

An error-correction process (ECP) can now be modeled by unitary transformations that first entangle the erroneous state $|\mathcal{E}\phi_E\rangle$ with a new **ancilla** (an auxiliary state of auxiliary qubits), and then transform the resulting entangled state into a tensor product of the state $|\mathcal{E}\phi_E\rangle$ and a new state $|A_{\mathcal{E}}\rangle$ of the ancilla:

$$|\mathcal{E}\phi_E\rangle|A\rangle \stackrel{ECP}{\to} |\mathcal{E}\phi_E\rangle|A_{\mathcal{E}}\rangle.$$

Since the state $|\mathcal{E}\phi_E\rangle|A_{\mathcal{E}}\rangle$ is not entangled we can measure $|A_{\mathcal{E}}\rangle$ without disturbing $M_s|\mathcal{E}\phi_E\rangle$ and this way we can determine a transformation which has to be applied to $|\mathcal{E}\phi_E\rangle$ to get $|\phi_E\rangle$.

ERROR CREATION and CORRECTION — DETAILS

Consider the important case where erroneous states have the form

$$\sum_{s=1}^{l} M_s|\phi_E\rangle \quad \text{or} \quad \sum_{s=1}^{l} |\psi_{env}^s\rangle M_s|\phi_E\rangle, \tag{1}$$

where each M_s is a tensor product of n error matrices from the set $\{X, Y, Z, I\}$ and $|\psi_{env}^s\rangle$ are states of the environment.

The basic task is to determine, without disturbing $M_S|\phi_E\rangle$ in an irreversible way, an operation to be performed to get $|\phi_E\rangle$ out of $M_s|\phi_E\rangle$.

The basic idea is to compute, as in the case of linear codes, syndromes of errors without disturbing $M_S|\phi_E\rangle$. This is done by introducing an ancilla in the state $|0^{(n-k)}\rangle$ and then a carefully chosen syndrome-extraction operator S is applied to get the state

$$\sum_{s=1}^{l} |\psi_{env}^s\rangle(M_s|\phi_E\rangle|s\rangle). \tag{2}$$

where the states $|s\rangle$ are mutually orthogonal and specify different syndromes. Since the states $|s\rangle$ are orthogonal we can measure the ancilla qubits in the basis $\{|s\rangle\}$ to get:

$$|\psi_{env}^{s_0}\rangle(M_{s_0}|\phi_e\rangle|s_0\rangle)$$

for a single, randomly chosen, s_0.

SUPER!!!!!!!!!!!!

Instead of a complicated erroneous state (2) we have now only one error operator M_{s_0} and by applying $M_{s_0}^{-1}$ we get as the result the state

$$|\psi_{env}^{s_0}\rangle|\phi_E\rangle|s_0\rangle.$$

Therefore, the state $|\phi_E\rangle$ has been reconstructed—it is no longer entangled.

QECC — NECESSARY AND SUFFICIENT CONDITIONS I

A necessary and sufficient condition will be derived for a QECC to correct any error from a given set $S_{\mathcal{E}}$ of errors.

First basic idea.

In order to be able to correct any two error E_a and E_b from $S_{\mathcal{E}}$, one has to be able to distinguish the case E_a is acting on a basis codeword $|\psi_i\rangle$ from the case E_b is acting on a different basis codeword $|\phi_j\rangle, i \neq j$.

Hence it has to hold

$$\langle\psi_i|E_a^* E_b|\psi_j\rangle = 0 \tag{3}$$

In other words

> errors on different basis codewords have to result in orthogonal states.

QECC — NECESSARY and SUFFICIENT CONDITIONS II

How about different errors on a same basis codeword? Should we require again that the condition (3)

$$\langle\psi_i|E_a^* E_b|\psi_j\rangle = 0 \tag{4}$$

holds? Namely, that (4) holds also for $i = j$ and all E_a, E_b from $\mathcal{S}_\mathcal{E}$?

No, the condition (4) is too strong.

Second main idea.

What is needed for a QECC is that when we make a measurement to find out about an error, we must learn nothing about the actual state of the coding space on which the error was made.

How we learn information about a codeword? By measuring

$$\langle\psi_i|E_a^* E_b|\psi_i\rangle.$$

This value has therefore to be the same for all basis codewords. Therefore for any correctable errors (i.e. from $\mathcal{S}_\mathcal{E}$) E_a and E_b and any $i \neq j$ it has to hold:

$$\langle\psi_i|E_a^* E_b|\psi_i\rangle = \langle\psi_j|E_a^* E_b|\psi_j\rangle. \tag{5}$$

It can be shown that conditions (3) and (5) are necessary and sufficient for a code to be able to correct a given set $\mathcal{S}_\mathcal{E}$ of errors.

Notation A code is called **orthogonal** or **non-degenerate** if for all errors E_a and E_b and any basis states $|\psi_i\rangle$ and $|\psi_j\rangle$

$$\langle\psi_i|E_a^* E_b|\psi_j\rangle = 0.$$

Such codes are more easy to deal with.

EXAMPLE

In the case of Shor's code , we cannot distinguish between errors σ_{z1} and σ_{z2}, but that is O.K. since we can correct either one with a single operation.

To understand the necessary condition for the existence of quantum codes, it is helpful to look at the operators

$$F_1 = (\sigma_{z1} + \sigma_{z2})/2, F_2(\sigma_{z1} - \sigma_{z2})$$

instead of σ_{z1} and σ_{z2}.
F_1 and F_2 spans the same space as σ_{z1} and σ_{z2} does, so Shor's code certainly corrects them.

Indeed, if we use F's as the basis errors the equation

$$\langle 0_E | F_1^* F_2 | 0_E \rangle = \langle 1_E | F_1^* F_2 | 1 \rangle$$

is satisfied.

That is we can make measurement and learn what error is.

We have also invert the error, and this is a potential problem, since F_1 and F_2 are not unitary.

However, F_1 acts the same way as σ_{z1} on the coding space, so σ_{z1}^* suffices to invert F_1 on the state of interest.

F_2 acts the same way as the 0 operator on the coding space. We can't invert this, but we don't need to — since F_2 annihilates codewords, it can never contribute a componenet to the actual state of the system.

EXAMPLE

Shor's code

$$|0\rangle \to |0_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} |xxxyyyzzz\rangle$$

$$|1\rangle \to |1_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} (-1)^{x+y+z}|xxxyyyzzz\rangle$$

After bit error on the first qubit

$$\sigma_x|0_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} |\bar{x}xxyyyzzz\rangle$$

$$\sigma_x|1_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} (-1)^{x+y+z}|\bar{x}xxyyyzzz\rangle$$

After sign error on the first qubit

$$\sigma_z|0_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} (-1)^{x}|xxxyyyzzz\rangle$$

$$\sigma_z|1_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} (-1)^{\bar{x}+y+z}|xxxyyyzzz\rangle$$

After bit and sign error on the first qubit

$$\sigma_y|0_E\rangle = \frac{1}{\sqrt{8}} \sum_{x,y,z\in\{0,1\}} (-1)^{\bar{x}}|\bar{x}xxyyyzzz\rangle \qquad \sigma_y|1_E\rangle = ???$$

BOUNDS on QECC

A bound on parameters k, n, t of QECC mapping k qubits into n and correcting t errors can be developed.

There are 2^k basis states of k qubits.

Since there are three possible errors (X, Y or Z) on each qubit. The number of possibilities for having i errors on a codeword of n qubits is $3^i\binom{n}{i}$ and for $i \in \{0, \ldots, t\}$ there are

$$2^k \sum_{i=0}^{t} 3^i \binom{n}{i}$$

possible error states.

If the code is non-degenerate, all error states obtained from the original basis state have to be orthogonal. Hence

$$2^k \sum_{i=0}^{t} 3^i \binom{n}{i} \leq 2^n.$$

In the case $k = 1 = t$ the bound is

$$2(3n + 1) \leq 2^n$$

and

$$n = 5$$

is the minimal n satisfying the bound $2(3n + 1) \leq 2^n$.

BIT versus SIGN ERRORS

There is a simple relation between bit errors, represented by the matrix $X = \sigma_x$ and the phase error, represented by the matrix $Z = \sigma_z$. Namely,

$$Z = HXH \qquad \text{and} \qquad X = HZH \tag{6}$$

where H is the Hadamard matrix, an application of which transforms the states expressed in the standard basis to the dual basis and vice versa.

In other words a sign error in the standard basis is the bit error in the dual basis and vice versa.

There are several other important identities concerning Hadamard transformation in the area of quantum error-correcting codes:

1. For any $u, e \in \{0,1\}^n$

$$Z_e H_n |u\rangle = H_n X_e |u\rangle = H_n |u + e\rangle.$$

2. (Dual code theorems.) For any linear $[n,k]$-code C

$$H_n \sum_{u \in C} |u\rangle = \sum_{v \in C^\perp} |v\rangle$$

and

$$H_n \sum_{v \in C^\perp} |u + v\rangle = \sum_{v \in C} (-1)^{u \cdot v} |v\rangle.$$

ENCODERS — ENCODING CIRCUITS

To use a quantum code with mappings $|0\rangle \to |0_E\rangle$, $|1\rangle \to |1_E\rangle$, a quantum circuit is needed to transform an arbitrary quantum state $\alpha|0\rangle + \beta|1\rangle$ into the state $\alpha|0_E\rangle + \beta|1_E\rangle$.
Encoding circuits for Steane's code

$$\begin{aligned} |0\rangle \;\to\; & |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ & +|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \end{aligned}$$

$$\begin{aligned} |1\rangle \;\to\; & |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ & +|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \end{aligned}$$

and for LMPZ's code

$$|0\rangle \to |00000\rangle + |11100\rangle - |10011\rangle - |01111\rangle + |11010\rangle + |00110\rangle + |01001\rangle + |10101\rangle$$

$$|1\rangle \to -|00011\rangle + |11111\rangle - |10000\rangle + |01100\rangle + |11001\rangle - |00101\rangle - |01010\rangle + |10110\rangle$$

are shown in Figures 2a,b.

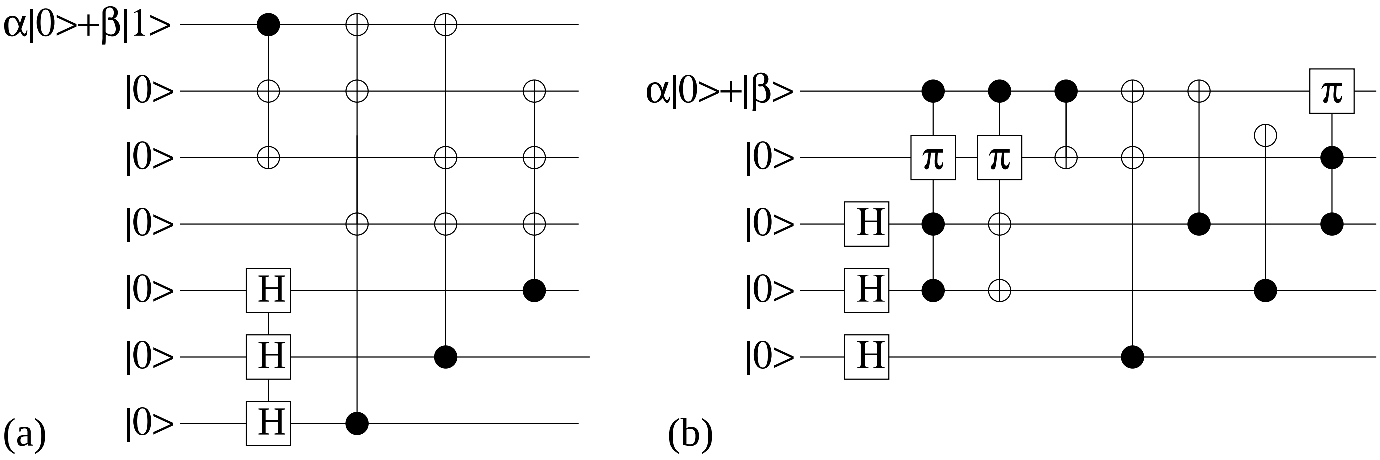


Figure 2: Encoding circuits for the Steane's and LMPZ's codes; π-gate realizes π-rotation

ERROR CORRECTION — SHOR's CODE

In the case of Shor's code the impact of the decoherence process

$$|e_0\rangle|0\rangle \rightarrow |a_0\rangle|0\rangle + |a_1\rangle|1\rangle, \qquad |e_1\rangle|1\rangle \rightarrow |b_0\rangle|0\rangle + |b_1\rangle|1\rangle,$$

where $|a_0\rangle$. $|a_1\rangle$, $|b_0\rangle$, $|b_1\rangle$ are states of the environment, on the first qubit of the states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$ results in the states

$$\begin{array}{ll} \frac{1}{\sqrt{8}}(|a_0\rangle + |b_1\rangle)(|000\rangle + |111\rangle) & \frac{1}{\sqrt{8}}(|a_0\rangle + |b_1\rangle)(|000\rangle - |111\rangle) \\ +\frac{1}{\sqrt{8}}(|a_0\rangle - |b_1\rangle)(|000\rangle - |111\rangle) & +\frac{1}{\sqrt{8}}(|a_0\rangle - |b_1\rangle)(|000\rangle + |111\rangle) \\ +\frac{1}{\sqrt{8}}(|a_1\rangle + |b_0\rangle)(|100\rangle + |011\rangle) & +\frac{1}{\sqrt{8}}(|a_1\rangle + |b_0\rangle)(|100\rangle - |011\rangle) \\ +\frac{1}{\sqrt{8}}(|a_1\rangle - |b_0\rangle)(|100\rangle - |011\rangle) & +\frac{1}{\sqrt{8}}(|a_1\rangle - |b_0\rangle)(|100\rangle + |011\rangle) \end{array}$$

At the measurement during the syndrome computation, with respect to Bell basis, the erroneous state, obtained from the state $\alpha|0_E\rangle + \beta|1_E\rangle$, collapses into one of the states

$$\begin{array}{c} (|a_0\rangle + |b_1\rangle)((\alpha+\beta)|000\rangle + (\alpha-\beta)|111\rangle), \\ (|a_0\rangle - |b_1\rangle)((\alpha+\beta)|000\rangle - (\alpha-\beta)|111\rangle), \\ (|a_1\rangle + |b_0\rangle)((\alpha+\beta)|100\rangle + (\alpha-\beta)|011\rangle), \\ (|a_1\rangle - |b_0\rangle)((\alpha+\beta)|100\rangle - (\alpha-\beta)|011\rangle), \end{array} \tag{7}$$

In order to make the correction to each of such resulting states a unitary transformation has to be applied that produces the original state

$$\alpha(|000\rangle + |111\rangle) + \beta(|000\rangle - |111\rangle).$$

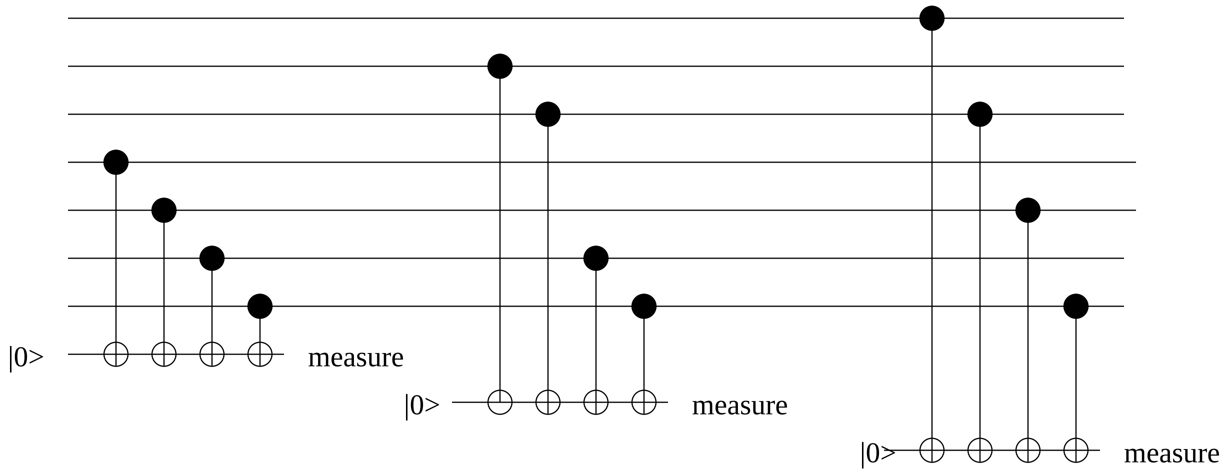
SYNDROM COMPUTATION for STEANE's CODE

For Steane's code

$$\begin{aligned}
|0\rangle &\rightarrow \frac{1}{\sqrt{8}}(\sum_{even\ v\in Hamming} |v\rangle \\
&= |0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\
&\quad +|0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle
\end{aligned}$$

$$\begin{aligned}
|1\rangle &\rightarrow \frac{1}{\sqrt{8}}(\sum_{odd\ v\in Hamming} |v\rangle \\
&= |1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\
&\quad +|1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle
\end{aligned}$$

the syndrom computation circuit has the form



because parity check matrix for Hamming code is

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

ERROR SYNDROME COMPUTATION — LMPZ-CODE

Efficient syndrome computation is the key problem in using quantum error-correcting codes.

Syndromes for LMPZ's code can be computed with the same circuit as for code generation; it is only necessary to run this circuit backward. A relation between syndromes and errors is shown in Figure 3a.

error type	syndrome s_1, s_2, s_3, s_4	resulting state
no	0000	$\alpha\|0\rangle + \beta\|1\rangle$
BS3	1011	$-\alpha\|1\rangle + \beta\|0\rangle$
BS5	1111	$-\alpha\|0\rangle + \beta\|1\rangle$
B2	1000	$\alpha\|0\rangle - \beta 11\rangle$
S3	0101	$\alpha\|0\rangle - \beta 11\rangle$
S5	0011	$\alpha\|0\rangle - \beta 11\rangle$
BS2	1010	$\alpha\|0\rangle - \beta 11\rangle$
B5	1100	$-\alpha\|0\rangle - \beta\|1\rangle$
S1	0001	$-\alpha\|0\rangle - \beta\|1\rangle$
S2	0010	$-\alpha\|0\rangle - \beta\|1\rangle$
S4	0100	$-\alpha\|0\rangle - \beta\|1\rangle$
B1	0110	$-\alpha\|1\rangle + \beta\|0\rangle$
B3	1110	$-\alpha\|1\rangle + \beta\|0\rangle$
B4	1101	$-\alpha\|1\rangle + \beta\|0\rangle$
BS1	1110	$-\alpha\|1\rangle + \beta\|0\rangle$
BS4	1001	$-\alpha\|1\rangle + \beta\|0\rangle$

Figure 3: Syndrome tables for the LMPZ's code. (B (S) stands for bit (sign) error and the number specifies the qubit.

QUASI-CLASSICAL QUANTUM CODES

With each $[n,k]$ classical binary code C which can correct up to t errors, two quantum codes can be assigned

$$B_C = \{|u\rangle \mid u \in C\} \qquad S_C = \{H_n|u\rangle \mid u \in C\}$$

Code B_C (S_C) can correct t bit (sign) errors, X_e (Z_e), where $hw(e) \leq t, e \in \{0,1\}^n$ and

$$X_e|u\rangle = |u+e\rangle \qquad Z_e H_n|u\rangle = H_n X_e|u\rangle = H_n|u+e\rangle.$$

Denote XOR_C the unitary operator such that

$$XOR_C|u+e\rangle|0^{(n-k)}\rangle = |u+e\rangle|P_C e^T\rangle, \tag{8}$$

where P_C is the parity-check matrix for C. XOR_C can be implemented by a circuit consisting of XOR gates only that have their control bits on qubits of $|u+e\rangle$ and their target bits are from ancilla. Each row of P_C define a parity check and consequently a sequence o XOR's has to be used.

Relation 8 describes syndrom extraction operation for the code B_C.

Syndrom extraction for the code S_C has the form

$$(H_n XOR_C H_n)H_n|u+e\rangle = |P_C e^T\rangle H_n|u+e\rangle.$$

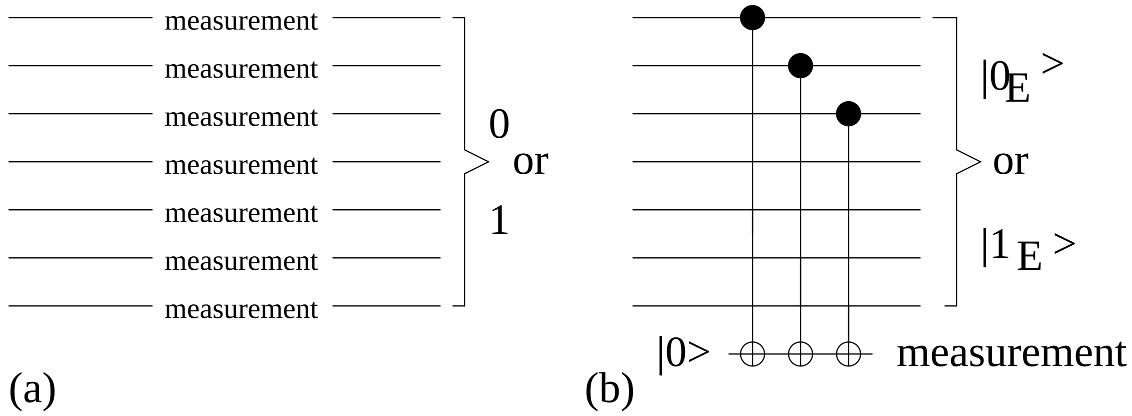
DESTRUCTIVE and NONDESTRUCTIVE MEASUREMENT

Encoded qubits can be measured in a destructive or nondestructive way. In the case of Steane's code

$$\begin{aligned}|0\rangle \;\rightarrow\; |0_E\rangle &= \frac{1}{\sqrt{8}}(|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \\ &+ |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle)\end{aligned}$$

$$\begin{aligned}|1\rangle \;\rightarrow\; |1_E\rangle &= \frac{1}{\sqrt{8}}(|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \\ &+ |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle)\end{aligned}$$

by the measurement of encoded qubits in the standard basis (Figure a) we get a codeword and its parity is the value of the logical qubit. This is a **destructive** measurement – it does not preserve the code subspace.



Nondestructive measurement is shown in Figure b with outcome

$$XOR_{18}XOR_{28}XOR_{38}(\alpha|0_E\rangle + \beta|1_E\rangle)|0\rangle$$

what equals

$$\alpha|0_E\rangle|0\rangle + \beta|1_E\rangle|1\rangle$$

and the measurement of the ancilla provides the answer

0 with probability $|\alpha|^2$ and the state collapses into the state$|0_E\rangle$

1 with probability $|\beta|^2$ and the state collapses into the state$|1_E\rangle$

CSS -CODES

A simple and powerful method of designing one QECC, so-called CSS-code, out of two, or out of one (dual), classical error-correcting linear codes, was developed by Calderbank Shor and Steane.

Let C_1 be an $[n,k]$ linear binary code with the generator matrix G. Denote by H_{C_1} the subspace of H_{2^n} spanned by the set of vectors $\{|c\rangle \mid c \in C_1\}$.

If to each $w \in \{0,1\}^n$ we associate a quantum state:

$$|c_w\rangle = \frac{1}{\sqrt{2^k}} \sum_{v\in\{0,1\}^k} (-1)^{vG\cdot w}|vG\rangle \quad (9)$$

$$= \frac{1}{\sqrt{2^{n-k}}} \sum_{u\in C^\perp} (-1)^{u\cdot w}|v+w\rangle. \quad (10)$$

then the set $\{|c_w\rangle \mid w \in \{0,1\}^*\}$ contains exactly 2^k different states that form an orthogonal basis in H_{C_1}.

If $C_2 \subseteq C_1$ is another code, then we define a quantum code

$$Q_{C_1,C_2} = \{|c_w\rangle \mid w \in C_2^\perp\}.$$

Clearly,

$$\mathit{dim}(Q_{C_1,C_2}) = \mathit{dim}(C_1) - \mathit{dim}(C_2).$$

If C is a self-dual (n,k,d) code, then

$$Q_C = Q_{C,C^\perp} = \{|c_w\rangle \mid w \in C^\perp\}$$

and $\mathit{dim}(Q_C) = k-(n-k) = 2k-n$.

The following theorem (see Calderbank and Shor, 1996), provides a justification of the codes Q_{C_1,C_2}.

Theorem 0.6 (Quantum Correction Theorem) *If C_1, C_2 are linear $[n,k,d]$-codes and $C_2^\perp \subset C_1$, then $Q_{C_1,C_2^\perp}$ is a t error-correcting quantum code for $t = \lceil (d-1)/2 \rceil$.*

STABILIZER CODES - BASICS I

A general class of quantum error-correcting codes, the so called **stabilizer codes**, were introduced by Gottesman (1996) and Calderbank and Shor (1997) and included all QECC known till that time.

The basic elements to work with at this approach are error operators

$$M = E_1 \otimes E_2 \otimes \ldots \otimes E_n, \tag{11}$$

where each $E_i \in \{I, X, Y, Z\}$ and $X = \sigma_x$, $Z = \sigma_z$ and $Y = XZ = i\sigma_y$, where σ_x, σ_y and σ_z are Pauli matrices.

An error operator (11) is said to have **weight** t if it has t component matrices different from I.

Denote by X_i, Y_i and Z_i operator/matrices X, Y and Z acting on the ith qubit and let $\mathcal{G}_n$ be the group generated by $3n$ of such matrices.

Properties of $\mathcal{G}_n$:

$$X_i^2 = Z_i^2 = I = -Y_i^2 \text{ and } Y_i = -X_iZ_i = Z_iX_i, \quad \text{for } 1 \leq i \leq n.$$

$\mathcal{G}_n$ has order $2 \cdot 4^n = 2^{2n+1}$ (there are four possible elements for each i and the sign). In addition, each element of $\mathcal{G}_n$ squares to ± 1 and if $A, B \in \mathcal{G}_n$, then A and B either commute or anticommute, i.e., either $[A, B] = 0$ or $\{A, M\} = 0$.

STABILIZER CODES - STABILIZERS

Let C be a quantum error-correcting code of H_{2^n}. C spans a subspace of H_{2^n}. The group $\mathcal{G}_n$ can be seen as acting on states of C.

A **stabilizer** $\mathcal{S}_C$ of C is the set

$$\mathcal{S}_C = \{M \in \mathcal{G}_n \mid M|\phi\rangle = |\phi\rangle \text{ if } |\phi\rangle \in C\}.$$

The following property is of crucial importance for the "stabilizer codes" to be defined later:

If $M \in \mathcal{G}_n$ and $S \in S_C$ are such that $\{M, S\} = 0$, then for any $|\phi\rangle$, $|\psi\rangle \in C$,

$$\langle\phi|M|\psi\rangle = \langle\phi|MS|\psi\rangle = -\langle\phi|SM|\psi\rangle = -\langle\phi|M|\psi\rangle$$

and therefore $\langle\phi|M|\psi\rangle = 0$.

The code C therefore satisfies the condition

$$\langle\psi_i|M_a^*M_b|\psi_j\rangle = c_{a,b}\delta_{ij},$$

whenever errors M_a and M_b are such that ${M_a}^*M_b$ anticommute with some element of S.

This implies that if $M_a^*M_b$ anticomutes with some element of S_C for all errors M_a, M_b of some set $\mathcal{E}$ of errors, then the code C corrects the set $\mathcal{E}$ of errors.

Comment However, it is unlikely that $M_a^*M_b$ anticomutes with some element of S_C for all errors M_a, M_b that need to be corrected. A trivial example is the "error" I which commutes with all elements of S_C. In addition, I is in S_C because S_C is a group. However, this actually does not matter because for all $S \in S_C$ it holds $\langle\psi_i|S|\psi_j\rangle = \langle\psi_i|\psi_j\rangle = \delta_{ij}$.

STABILIZER CODES – EXAMPLE

M_1	Z	Z	I	I	I	I	I	I	I
M_2	Z	I	Z	I	I	I	I	I	I
M_3	I	I	I	Z	Z	I	I	I	I
M_4	I	I	I	Z	I	Z	I	I	I
M_5	I	I	I	I	I	I	Z	Z	I
M_6	I	I	I	I	I	I	Z	I	Z
M_7	X	X	X	X	X	X	I	I	I
M_8	X	X	X	I	I	I	X	X	X

(a)

M_1	I	I	I	X	X	X	X
M_2	I	X	X	I	I	X	X
M_3	X	I	X	I	X	I	X
M_4	I	I	I	Z	Z	Z	Z
M_5	I	Z	X	I	I	Z	Z
M_6	Z	I	Z	I	Z	I	Z

(b)

M_1	X	Z	Z	X	I
M_2	I	X	Z	Z	X
M_3	X	I	X	Z	Z
M_4	Z	X	I	X	Z

(c)

M_1	X	X	X	X	X	X	X	X
M_2	Z	Z	Z	Z	Z	Z	Z	Z
M_3	I	X	I	X	Y	Z	Y	Z
M_4	I	X	Z	Y	I	X	Z	Y
M_5	I	Y	X	Z	X	Z	I	Y

(d)

Figure 4: Stabilizers

Figures 4a,b,c generators of the stabilizers for Shor's code, Steane's code and LMPZ's code.

Let us discuss design and use of the stabilizer for Steane's code. Error vectors in Figure 4b can be discovered in a straightforward way from how one detects a single bit or sign error for this code. Indeed, to detect a bit error in a state $|\psi\rangle$ on one of the first three qubits it is sufficient to compare the first qubit with second and then the first qubit with the third in $|\psi\rangle$.

One way of doing that is to measure $|\psi\rangle$ with respect to M_1 and M_2 as observables. Indeeed, in the case of the bit error on the first or the second (on the second or on the third) qubit we have $M_1|\psi\rangle = -|\psi\rangle$ ($M_2|\psi\rangle = -|\psi\rangle$). A similar role play the generators M_3 to M_6. M_3 and M_4 (M_5 and M_6) are used to detect bit errors in the second (third) triplet of qubits. M_7 and M_8 can be used to detect sign errors.

In general, in order to perform error detection for a stabilizer code all one needs to do is to measure eigenvalues of each generator of the stabilizer.

MEASURING of STABILIZERS

The stabilizer codes are chosen so that every error operator (a tensor product of error operators I, X, Y, Z) as well as a product of any two such operators anticomute with at least one of the generators (and therefore every error changes the eigenvalues of some generators) and two independent errors always change eigenvalues of generators in distict way.

Measuring eigenvalue of a stabilizer generator M is not difficult.

First we perform an appropriate unitary change of basis on each qubit so that M in the rotated baais is the product of only I's and Z's.

In case of the operator X (Y) rotation is done using Hadamard operator (using the operator $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$).

The eigenvalue is then just parity of the bits for which Z appears in M.

This parity we can measure by performing an XOR to the ancilla from each qubit in the block for which Z appears in M.

Finally, we invert the changes of bases.