QUANTUM COMPUTING 10.

Jozef Gruska

Faculty of Informatics
Brno
Czech Republic

December 3, 2018

10. QUANTUM ERROR CORRECTION CODES

Quantum computing based on pure states and unitary evolutions is an idealization that works fine for 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 interfere.

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.

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

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 $C^\perp = \{w \mid u \cdot w = 0 \text{ if } u \in C\}$ 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 matrix** 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 $a + C = \{a + x \,|\, x \in C\}$ 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 $S(y)$.

SOME ADVANCES of CLASSICAL ERROR-CORRECTING CODES

In general to represent a code C with 2^{200} codewords we wcould need to represent

$$2^{200}$$

codewords what would need more space than universe has particles.

To represent a linear code C with of dimenion 200 with 2^{200} codewords we need to present

$$200$$

codewords (of some basis) of C.

To reperesent a so-called cyclic codes with 2^{200} codewords one needs to present only

$$1$$

codeword.

CYCLIC CODES

A code C of codewords of length n is cyclic if it is linear and with each codeword $a_1a_2\ldots a_n$ contains also codeword $a_2a_3\ldots a_na_1$.

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 quantum "errors" seems to be much larger (even infinite) than in the classical case.
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	$(1/\sqrt{8})(X)(X)(X)$ $X = \|000\rangle + \|111\rangle$	$(1/\sqrt{8}(Y)(Y)(Y)$ $Y = \|000\rangle - \|111\rangle$
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.

SHOR CODE

For $i \in \{0, 1\}$

$$|i\rangle \rightarrow \frac{1}{\sqrt{8}} \otimes_{i=1}^{3} \left(|000\rangle + (-1)^{i}|111\rangle\right)$$

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.

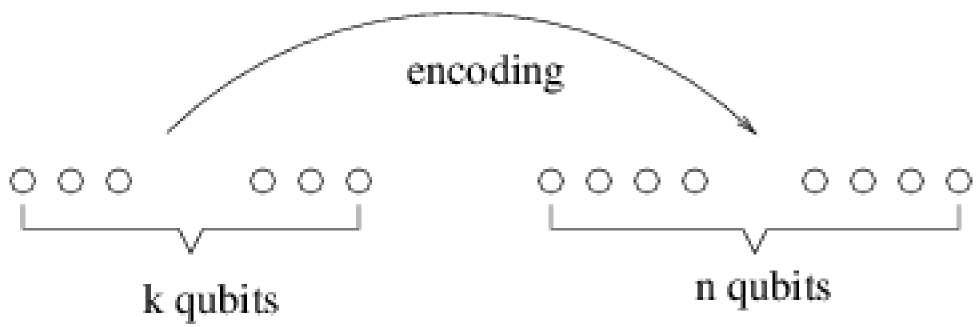
Consequently, Bob, who can act on the state he receives, but not on the environment, is then able to determine which error was made, and then undo its effect and to receive the original state.

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 in a quantum states composd of n qubits.

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

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 $u_i = 1$.

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:

resulting state	its 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

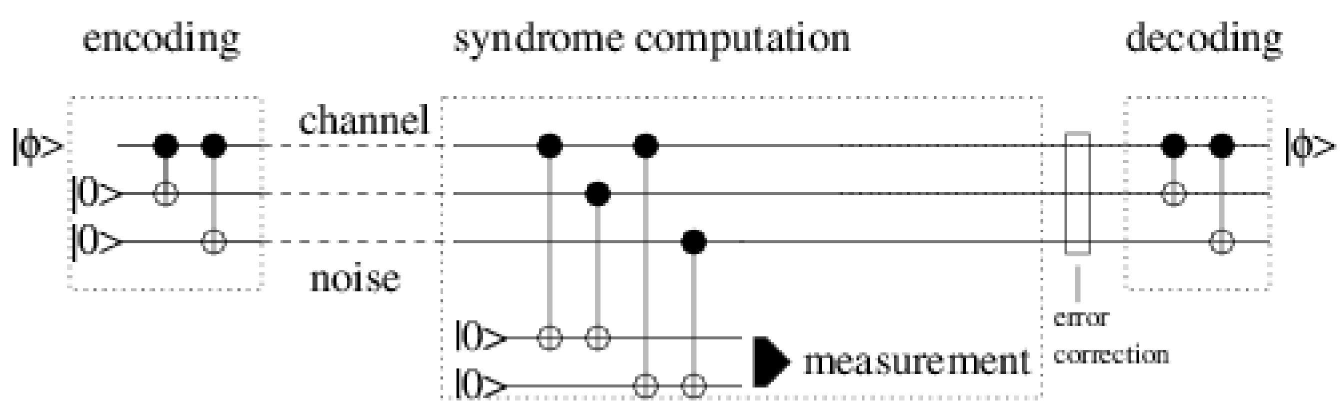
BOB: Syndrome computation process. By using two additional ancilla qubits in state $|00\rangle$ and four XOR operations syndromes of errors can be computed as shown in the following table

resulting state	its 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 $\beta|0\rangle + |1\rangle$.


encoding
syndrome computation
decoding
|φ>
|0>
|0>
channel
noise
|0>
|0>
measurement
error
correction
|φ>

VARIATIONS on SYNDROME COMPUTATIONS

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

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

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 without error correction 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 after error-correction 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 a 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

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

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}.

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

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

$$|\phi_E\rangle \xrightarrow{\mathcal{E}} |\mathcal{E}\phi_E\rangle.$$

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:

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

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

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

where each M_s is a tensor product of n error matrices from the set $\{X, Y, Z, I\}$ and $|\psi^s_{env}\rangle$ 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

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

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:

$$|\psi^{s_0}_{env}\rangle(M_{s_0}|\phi_E\rangle|s_0\rangle)$$

for a single, randomly chosen, s_0.

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

Instead of a complicated erroneous state (??) 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 perfectly 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 the codeword $|\psi_i\rangle$ of a basis vector from the case E_b is acting on any codeword $|\phi_j\rangle, i \neq j$ of another basis vector.

Hence it has to hold

$$\langle\psi_i|E_a^* E_b|\psi_j\rangle = 0 \qquad (3)$$

In other words

errors on codewords of different basis vectors 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 (??)

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

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

No, the condition (??) is too strong.

Second main idea.

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

How we learn information about an erroneous codeword? By computing

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

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 (??) and (??) 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.

In general any physically realisable operation can be an error.

WHAT ARE QUANTUM OPERATIONS?

Informally, there are four basic quantum operations: additions of ancillas, unitary operations, quantum measurements and discarding quantum subsystems.

Formally, as discussed later, there are several equivalent mathematical concepts that are very useful when quantum operations are considered.

Let us now discuss in more details what are all physically realizable operations (superoperators) one can perform (at least theoretically) on (mixed) states (to get again (mixed) states)?

In closed quantum systems unitary operations are actually the only quantum operations that are available. Measurements are actually outside of the closed system framework, an interface from quantum to classical world, but surely they are operations we consider as physically realizable.

It is perhaps a bit surprising, but actually nice, useful and natural, that we can actually study and consider open quantum systems in the framework of closed quantum systems. We can consider as the basic setting that our (principal) quantum system and its environment form a closed quantum system in which we operate.

The requirement to consider only physically realizable (at least theoretically) operation is, of course, logical. As we shall see this question has, in a sense and at least theoretically, clear and simple answer. They are, as discussed later, *trace preserving completely positive linear maps*.

THREE APPROACHES

There are basically three main approaches to define what are "physically realizable quantum operations" (superoperators) $\mathcal{E}$.

A physically motivated axiomatic approach says that for a Hilbert space $\mathcal{H}$ we should consider as physically realizable operations maps $\mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$ which are *consistent with the (statistical) interpretation of quantum theory*. That is map that are linear (to preserve superpositions), *positive* and *trace preserving* (to map density operators to density operators) and actually completely positive (to be sure that if a superoperator is applied to a subsystem, then the whole system is again in a quantum state).

A pragmatic approach says that superoperators are those operations that can be combined from unitary operations, adding ancillas, performing (non-selective) projective measurement and discarding subsystems (ancillas), by performing a tracing out operation.

A mathematical approach says that all basic quantum operations: adding and discardi ng quantum subsystems, unitary operations and non-selective projective measurements have **Kraus operator-sum representation**

$$\rho \to \sum_{i=1}^{k} E_i \rho E_i^{\dagger},$$

where so called *Kraus operators* $E_i : \mathcal{H} \to \mathcal{H}$ are not necessarily Hermitian operators, but they should be positive and should form a "decomposition of the identity operator", that is, $\Sigma_{i=1}^{k} E_i^{\dagger} E_i = I_{\mathcal{H}}$ – so called **completeness condition.**

It is a consequence of the completeness condition, and a property of trace operation, that for an y superoperator $\mathcal{E}$ holds

$$Tr(\mathcal{E}(\rho)) = Tr(\sum_i E_i \rho E_i^{\dagger}) = Tr(\sum_i E_i^{\dagger} E_i \rho) = Tr((\sum_i E_i^{\dagger} E_i)\rho) = Tr(\rho) = 1.$$

In general Kraus operators $E_i^{\dagger}$ and E_i do not commute. Condition $\Sigma_{i=1}^{k} E_i E_i^{\dagger} = I$ is therefore different from the condition $\Sigma_{i=1}^{k} E_i^{\dagger} E_i = I$.

STINESPRING DILATION THEOREM

So called *Stinespring dilation theorem*, discussed below, says, that each superoperator can be realized in "one big three-stage-step" : adding an ancilla, performing a unitary operation on a composed quantum system and, finally, discarding the ancilla, see Figure ??, or other subsystems.

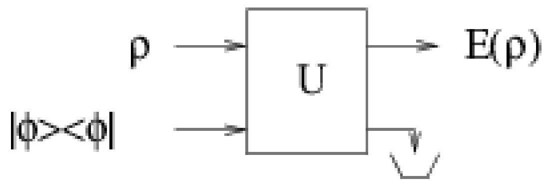


Figure 2: A Stinespring realization of a superoperator. In this view a superoperator $\mathcal{E}$ performs the mapping $\mathcal{E}(\rho) = Tr_a(U(\rho \times \rho_a)U^\dagger)$, where ρ_a is the "initial state", for example $|\phi\rangle\langle\phi|$ of an ancilla subsystem, U is a unitary operation on composed system and, finally, a tracing out operation is performed.

ANALYSIS of THREE APPROACHES

Each of the above three approaches to the definition of quantum operations has its strong and week points.

- Pragmatic approach is easy to justify, but hard to deal with mathematically.
- Axiomatic approach is easy to justify, but neither easy to transfer to practical actions nor to handle mathematically.
- Kraus' approach is mathematically easy to handle, but less easy "to see into" and to justify. However, it has one very important advantage – it actually says that when thinking about operations in a quantum system $\mathcal{S}$ we can actually ignore ancillas and express all operations on $\mathcal{S}$ in terms of operators in $\mathcal{S}$ (and that way to ignore "unessential" developments, from the system $\mathcal{S}$ point of view, going on in ancillas, no matter how they are chosen).

Observe that unitary transformations $\rho \rightarrow U\rho U^\dagger$ and measurement operators $\mathcal{E}_m(\rho) = \sqrt{\mathbf{F}_m}\rho\sqrt{\mathbf{F}_m}$ are actually also of the above Kraus form.
In general, Kraus operators $E_i^\dagger$ and E_i do not commute. Condition $\sum_{i=1}^k E_i E_i^\dagger = I$ is therefore different from the condition $\sum_{i=1}^k E_i^\dagger E_i = I$.

EXAMPLE – XOR

Example 0.6 *In the case of a two-qubit circuit for XOR operation, see Figure ??, it is straightforward to calculate that after discarding the ancilla (in the state $|0\rangle$), the resulting state is*

$$\mathcal{E}(\rho) = P_0\rho P_0 + P_1\rho P_1,$$

where

$$P_0 = |0\rangle\langle 0|$$

and

$$P_1 = |1\rangle\langle 1|.$$

Observe that

$$XOR = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|.$$

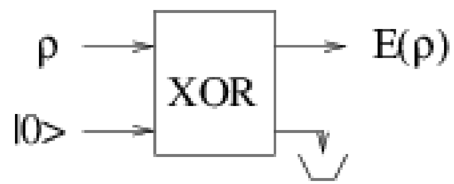


Figure 3: A realization of XOR operation where $\mathcal{E}(\rho) = P_0\rho P_0 + P_1\rho P_1$, where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$

EXAMPLE

Shor's code has encodings:

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

After the bit error on the first qubit we get the states

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

In the encoding using **Shor's code**

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

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

we get after the 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 the bit-and-sign error on the first qubit we get:

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

QUANTUM ERROR CORRECTION CODES - GENERAL CASE

Let $\{\beta_i\}_{i=1}^{2^k}$ be an orthonormal basis of $\mathcal{H}_{2^k}$ and let U a unitary transformation on $\mathcal{H}_{2^n}$, $k < n$. A quantum $[n, k]$ code is a subspace of $\mathcal{H}_{2^n}$ of the dimension 2^k generated by the orthonormal vectors $\{U(\beta_i \otimes 0^{n-k})\}_{i=1}^{2^k}$

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,

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

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

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

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

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

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

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

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

and for LMPZ's code

$$|0\rangle \to \frac{1}{\sqrt{8}}(|00000\rangle + |11100\rangle - |10011\rangle - |01111\rangle + |11010\rangle + |00110\rangle + |01001\rangle + |10101\rangle)$$

$$|1\rangle \to \frac{1}{\sqrt{8}}(-|00011\rangle + |11111\rangle - |10000\rangle + |01100\rangle + |11001\rangle - |00101\rangle - |01010\rangle + |10110\rangle)$$

are shown in Figures ??a,b.

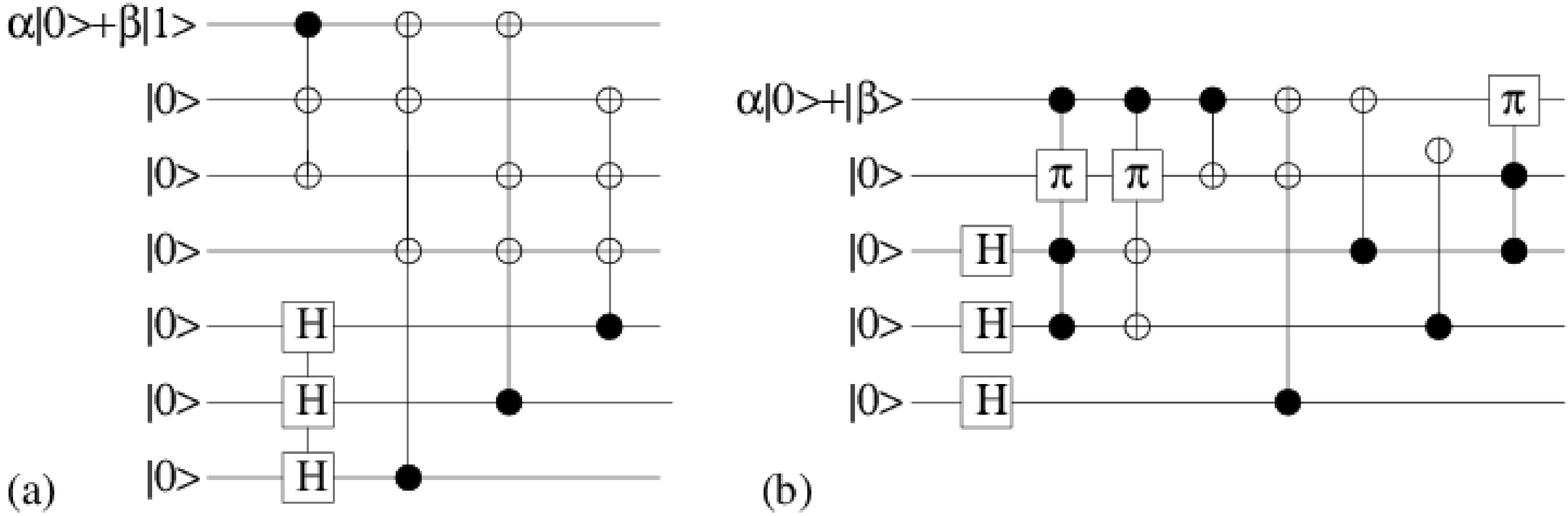


Figure 4: Encoding circuits for the Steane's and LMPZ's codes; π-gate realizes π-rotation

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

HAMMING CODES I

An important family of simple error-correcting linear codes which are easy to encode and decode are the so-called Hamming codes.

Definition 0.7 *Let r be an integer and H be an $r \times (2^r - 1)$ matrix columns of which are non-zero distinct words from $V(r,2)$. The code having H as its parity-check matrix is called* **binary Hamming code** *and denoted by $Ham(r,2)$.*

$$\text{Ham}(2,2) = H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \Rightarrow G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

$$\text{Ham}(3,2) = H = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \Rightarrow G = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{vmatrix}$$

Theorem 0.8 *Hamming code $Ham(r,2)$*

- *is $[2^r - 1, 2^r - 1 - r]$-code,*
- *has minimum distance 3,*
- *is a perfect code.*

HAMMING CODE II

Theorem 0.9 *Coset leaders for the Hamming code are precisely words of weight* ≤ 1*. The syndrome of the word* $0\ldots010\ldots0$*, with 1 in* j*-th position and* 0 *otherwise, is the transpose of the* j*-th column of* H*.*

Decoding algorithm for the case the columns of H are arranged in the order of increasing binary numbers the columns represent.

- **Step 1** Given y compute syndrome $S(y) = yH^{\top}$.
- **Step 2** If $S(y) = 0$, then y is assumed to be the codeword sent.
- **Step 3** If $S(y) \neq 0$, then assuming a single error, $S(y)$ gives the binary position of the error.

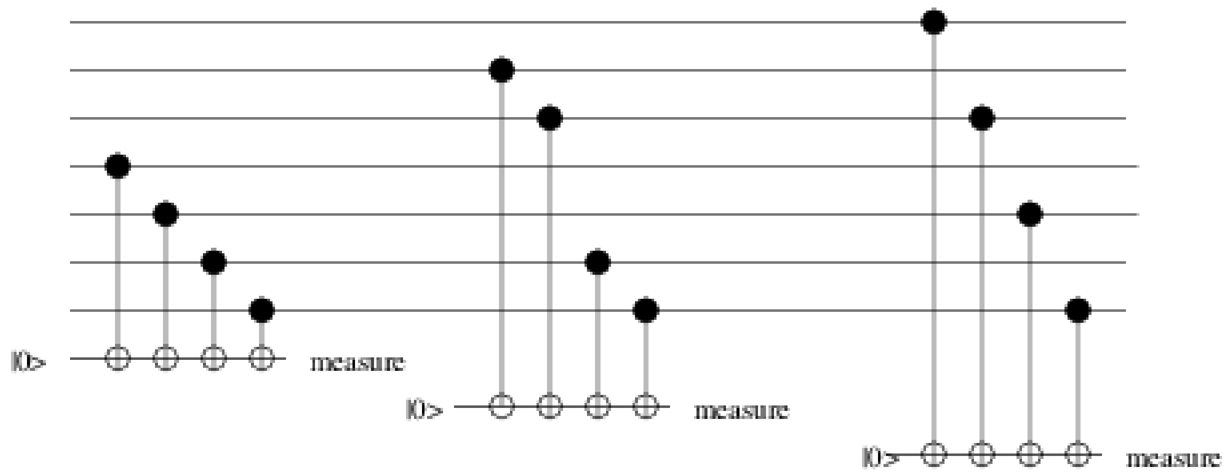
SYNDROME COMPUTATION for STEANE's CODE

For Steane's code

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

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

the syndrome 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 ??a.

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	
S5	0011	
BS2	1010	
B5	1100	$-\alpha\|0\rangle - \beta\|1\rangle$
S1	0001	
S2	0010	
S4	0100	
B1	0110	$-\alpha\|1\rangle + \beta\|0\rangle$
B3	1110	
B4	1101	
BS1	1110	
BS4	1001	

Figure 5: 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 linear 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 $hd(e) \leq t, e \in \{0,1\}^n$ 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 by XOR_C the unitary operator such that

$$\text{XOR}_C|u+e\rangle|0^{(k)}\rangle = |u+e\rangle|P_C e^T\rangle, \tag{7}$$

where P_C is the parity-check matrix for C. XOR_C can be implemented by a circuit consisting of k XOR gates that have their control bits on qubits of $|u+e\rangle$ and their target bits are from the ancilla $|0^{(k)}\rangle$. Each row of P_C define a parity check and consequently a sequence of XOR's has to be used.

Relation ?? describes the syndrome extraction operation for the code B_C.

Syndrome extraction for the code S_C has the form

$$(H_n \text{XOR}_C H_n) H_n|u+e\rangle = |P_C e^T\rangle H_n|u+e\rangle.$$

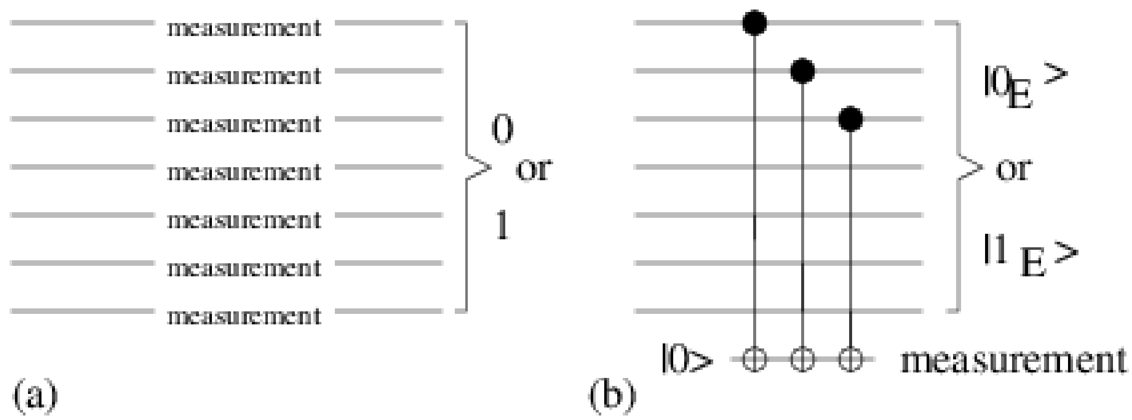
DESTRUCTIVE and NONDESTRUCTIVE MEASUREMENT

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

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

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

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

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

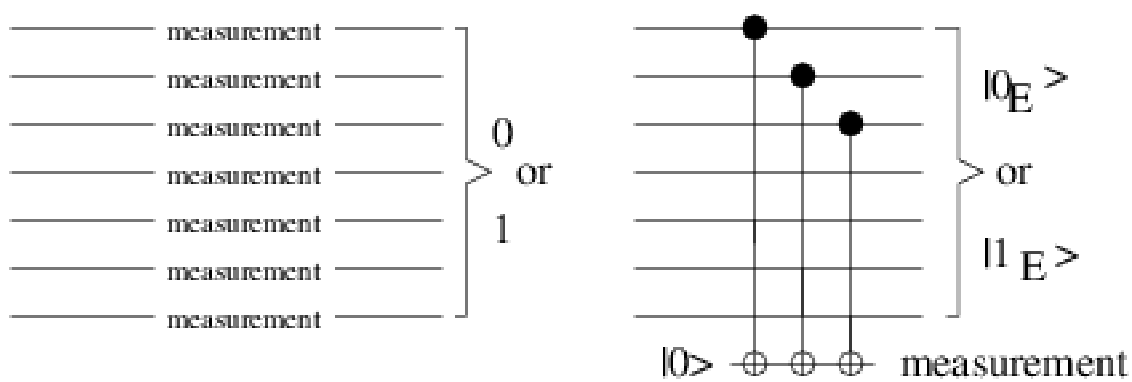
what equals

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

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$|1_E\rangle$



(a) (b)

MOTIVATION for STABILIZER CODES

Binary stabilizer codes represent a very important family of quantum codes for the following reasons:

- Stabilizer codes have similar advantages as classical linear codes, with stabilizer and check matrices playing a similar role as syndromes and parity check matrices for linear codes;
- Stabilizer codes have very concise description, straightforward encoding, decoding, syndrome computation and error-correction. Moreover, very important CSS codes, discussed later and constructed easily from two classical linear codes, are a special class of binary stabilizer codes.

STABILIZERS

Stabilizers, especially Pauli stabilizers, represent special ways to specify efficiently and elegantly certain quantum states and operations.

So called quantum stabilizer circuits are a powerful class of circuits that can be efficiently simulated on classical computers and that play the key role in various areas of QIP, especially in quantum error correction and fault-tolerant processes.

The basic point is that some quantum states and subspaces have a very concise and handy description in terms of fix-points of certain operators. For example:

- The state $|\phi\rangle = \frac{1}{\sqrt{2^n}}\Sigma_{x\in\{0,1\}^n}|x\rangle$, that plays so important role in the design of efficient quantum algorithms, is the fixpoint of the operator $\mathcal{O} = \otimes_{i=1}^n \sigma_x$, that is $\mathcal{O}|\phi\rangle = |\phi\rangle$.
- The state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is fully specified/defined as the only fix point of operators $\sigma_x \times \sigma_x$ and $\sigma_z \times \sigma_z$.
- The subspace generated by Bell states $|\Phi^+\rangle$ and $|\Psi^+\rangle$ is the subspace of states that are fix-points of the operator $\sigma_x \otimes \sigma_x$.
- The subspace generated by states $|000\rangle$ and $111\rangle$, that was used for a single bit error correction, is the fixed point of the operators $I\otimes\sigma_z\otimes\sigma_z$, $\sigma_z\otimes I\otimes\sigma_z$ and $\sigma_z\otimes\sigma_z\otimes I$.

STABILIZERS II

It is easy to observe that the set of operators that stabilizes a state is a group and that the set of states stabilized by an operator is a subspace.

In case a state $|\phi\rangle$ is a fix-point of an operator O, that is $|\phi\rangle$ is the eigenvector of O corresponding to its eigenvalue $+1$, it got common to say that the *operator O stabilizes $|\phi\rangle$* and/or that *O is a stabilizer of $|\phi\rangle$*.

In terms of stabilizers one can also characterize some unitary operators, and thereby certain quantum dynamics, in a concise and useful way.

Indeed, if a state $|\phi\rangle$ is stabilized by an operator O, that is $O|\phi\rangle = |\phi\rangle$, and U is any unitary operator. then the state $U|\phi\rangle$ is stabilized by the operator $UOU^\dagger$.

An operator U can therefore be seen as mapping stabilizers of some states into stabilizers of other states. For example, since $H\sigma_x H^\dagger = \sigma_z$, the Hadamard transform maps the σ_x stabilizer, that stabilizes (and specifies) the state $|0'\rangle$, to the σ_z stabilizer, that stabilizes (and specifies) the state $|0\rangle$.

Important operations that maps Pauli stabilizers to Pauli stabilizers are CNOT, Hadamard and Phase operators. Circuits composed of these operators form a very important class of circuits that can be efficiently simulated on classical computers and that produce so called stabilizer states that have very concise specification.

SUBSPACES STABILIZED BY PAULI STABILIZERS

In all examples above, the stabilizers were Pauli operators σ_x, or σ_z, or their tensor products.

This has not been by a chance. Exactly such stabilizers will play a crucial role in the following and also later when they will be used to define the most important class of quantum error-correcting codes.

Since $O^\dagger = O$ for all such operators, and any product of two stabilizers of a state or subspace is again its stabilizer, a set of Pauli stabilizers of a state, or of a set of states, forms an Abelian group. The existence of such a nice group-structure plays then an important role in all major applications of the stabilizer concept.

Observe that the following states are stabilized by Pauli operators

$$\sigma_x : \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \quad -\sigma_x : \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle \tag{8}$$

$$\sigma_y : \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle \quad -\sigma_y : \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle \tag{9}$$

$$\sigma_z : |0\rangle \qquad -\sigma_z : |1\rangle \tag{10}$$

$$I : \text{all states} \qquad -I : \text{no states} \tag{11}$$

PAULI GROUP

It is the group $\mathcal{P}_n$ generated by Pauli operators

$$M = E_1 \otimes E_2 \otimes \ldots \otimes E_n, \tag{12}$$

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

A Pauli operator (??) is said to have **weight** t if it has t Pauli matrices different from I.

Group $\mathcal{P}_n$ has 4^{n+1} elements – there are 4 Pauli matrices for each E_i and four phase factors ± 1 and $\pm i$ (that are needed to have really a group). According to the Lagrange theorem, each subgroup of $\mathcal{P}_n$ has 2^i elements for some integer i.

All elements M_1 and M_2 of $\mathcal{P}_n$ square to one, have eigenvalues ± 1 and either commute (notation $[M_1, M_2] = 0$), or anticommute, (notation $\{M_1, M_2\} = 0$).

STABILIZER GROUPS and THEIR REPRESENTATIONS

To each subgroup G of the Pauli group $\mathcal{P}_n$ we can associate the subspace S_G of $\mathcal{H}_{2^n}$ of all those states in $\mathcal{H}_{2^n}$ that are common fix-points of all operators from G.

It is easy to see that if $-I$ is an element of G, or G is not Abelian, then the subspace S_G is trivial.

Indeed, there is no state $|\phi\rangle$ such that $-I|\phi\rangle = |\phi\rangle$.

Moreover, if G is non-Abelian, then it has to have two elements g_1, g_2 such that $g_1 g_2 = -g_2 g_1$ and therefore if $|\phi\rangle \in S_G$, then
$|\phi\rangle = g_1(g_2(|\phi\rangle)) = -g_2(g_1(|\phi\rangle)) = -|\phi\rangle$. That is, S_G is empty – or trivial.

In the following we will therefore consider only Abelian subgroups of $\mathcal{P}_n$ that do not contain $-I$.

Each Abelian subgroup G of $\mathcal{P}_n$ with 2^k elements can be specified by an independent set of k generators $\{g_1, \ldots, g_k\}$.

That is by such a set of its elements that each element of the group can be expressed as a product of the generators and that is no longer true if any of the generators of the set is omitted.

It turned out useful to associate to each generator g a $2n$-dimensional binary row vector $v(g)$ that has, for $1 \leq i \leq n$, in the ith position ($(n+i)$th position) 1 if and only if g has in the ith position X or Y (Y or Z).

By putting all such row vectors together we can represent a set of generators by so called *stabilizer check matrix of the dimension* $k \times (2n)$ that is usually drawn as two matrices separated by a vertical line (as a "double-matrix").

For example, the set of generators

$$\begin{array}{c|ccccccc} M_1 & \mathsf{I} & \mathsf{I} & \mathsf{I} & \mathsf{X} & \mathsf{X} & \mathsf{X} & \mathsf{X} \\ M_2 & \mathsf{I} & \mathsf{X} & \mathsf{X} & \mathsf{I} & \mathsf{I} & \mathsf{X} & \mathsf{X} \\ M_3 & \mathsf{X} & \mathsf{I} & \mathsf{X} & \mathsf{I} & \mathsf{X} & \mathsf{I} & \mathsf{X} \\ M_4 & \mathsf{I} & \mathsf{I} & \mathsf{I} & \mathsf{Z} & \mathsf{Z} & \mathsf{Z} & \mathsf{Z} \\ M_5 & \mathsf{I} & \mathsf{Z} & \mathsf{Z} & \mathsf{I} & \mathsf{I} & \mathsf{Z} & \mathsf{Z} \\ M_6 & \mathsf{Z} & \mathsf{I} & \mathsf{Z} & \mathsf{I} & \mathsf{Z} & \mathsf{I} & \mathsf{Z} \end{array}$$

has the check matrix.

$$\left(\begin{array}{ccccccc|ccccccc} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

The following result is the first demonstration of the usefulness of the concept of the stabilizer check matrix.

Theorem 0.10 *Rows of a* stabilizer check matrix *are independent if and only if they correspond to an independent set of generators.*

In connection with *stabilizer check matrices* of importance is so called symplectic inner product $\cdot_s$ of row vectors

$$v(g_1) = (a_1, \ldots, a_{2n}) \text{ and } v(g_2) = (b_1, \ldots, b_{2n})$$

defined by

$$v(g_1) \cdot_s v(g_2) = \sum_{i=1}^{n} a_i b_{n+i} + b_i a_{n+i}.$$

One reason why simpletic product is considered as important is the following result.

Theorem 0.11 *Two generators commute if and only if the symplectic inner product of their row vectors is* 0.

MEASURING EIGENVALUES of OPERATORS

In the following we will deal with so-called *measurement of operators* or, in other terminology, with *measurement of eigenvalues*. This concerns the case that operators are at the same time observables and their eigenvalues are $+1$ or -1.

In such a case there is a trick how to "measure eigenvalues" corresponding to given eigenvectors, that is demonstrated in Figure ??, where we assume that U is an one-qubit operator whose eigenvalues are ± 1 – an important example are Pauli operators. It is easy to determine that after the last Hadamard transformation the overall state is

$$\frac{1}{2}(|\phi\rangle + U|\phi\rangle)|0\rangle + \frac{1}{2}(|\phi\rangle - U|\phi\rangle)|1\rangle.$$

This means that if the input eigenvector corresponds to the eigenvalue 1, then a measurement of second qubit gives 0 and if the input eigenvector corresponds to the eigenvalue -1, then measurement of the second qubit gives 1.

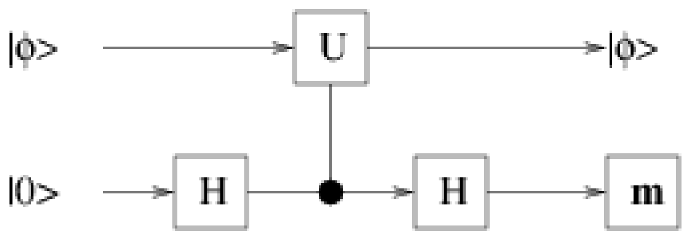


Figure 6: A circuit to measure eigenvalues of operators/observable

STABILIZER CIRCUITS AND STATES

If a subgroup G of the Pauli group $\mathcal{P}_n$, with a set of generators $\{g_1, \ldots, g_k\}$, stabilizes a subspace S_G and U is a unitary operation, then the subgroup denoted $UGU^\dagger$, and generated by generators $\{Ug_1U^\dagger, \ldots, Ug_kU^\dagger\}$, stabilizes the subspace $US_GU^\dagger$.

This implies that in order to understand an impact of a unitary transformation on a set (infinite in general) S_G of states stabilized by G, we only need to understand impact of U on a finite set of generators of G.

This is already "a big deal". The advantage of this approach is then much amplified by the fact that for some especially important unitary transformations such a transformations of Pauli generators have especially simple form and result again in easy to determine Pauli generators.

It is straightforward to see the impact of Pauli operators on themselves because

$$XXX = X, \quad XZX = -Z, \quad XYX = -Y$$

$$YXY = -X, \quad YYY = Y, \quad YZY = -Z$$

$$ZXZ = -X, \quad ZYZ = -Y, \quad ZZZ = Z$$

and also for the CNOT, Hadamard and Phase shift operations as depicted in the following table that shows how the above operation map possible Pauli generators.

Operation U	stabilizer g	$UgU^\dagger$
CNOT	$X \otimes I$	$X \otimes X$
	$I \otimes X$	$I \otimes X$
	$Z \otimes I$	$Z \otimes I$
	$I \otimes Z$	$Z \otimes Z$
H	X	Z
	Z	X
P	X	Y
	Z	Z

It has not been by chance that we have considered CNOT, H and P operations/gates. As the following theorem demonstrates, these gates play the crucial role concerning Pauli stabilizers and in the understanding of a certain class of quantum dynamics in terms of stabilizers.

Theorem 0.12 *If U is a unitary operation such that $UgU^\dagger \in \mathcal{P}_n$ for any $g \in \mathcal{P}_n$, then, up to a global phase, U can be implemented by a circuit consisting of n^2 gates CNOT, H and P.*

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 $\mathcal{P}_n$ can be seen as acting on states of C.

A **stabilizer** $\mathcal{S}_C$ of the error-correcting code C is the set

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

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

If $M \in \mathcal{P}_n$ and $S \in S_C$ are such that $\{M, S\} = 0$ (that is $MS = -SM$), 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

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

for some constant $c_{a,b}$, whenever errors M_a and M_b are such that ${M_a}^* M_b$ anticommute with some element of S_C.

This implies that if for all errors M_a, M_b of some set $\mathcal{E}$ of errors $M_a^* M_b$ anticomutes with some element of S_C, 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	Z	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 7: Stabilizers

Figures ??a,b,c show 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 Shor's code. Error vectors in Figure ??a 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. Indeed, 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.

BASICS of (binary) STABILIZERS CODES

The very basic concept is very simple. An $[n,k]$ *stabilizer code* C_G is the subspace of $\mathcal{H}_{2^n}$ stabilized by a an Abelian subgroup G of $\mathcal{P}_n$, such that $-I \notin G$, and generated by an independent set of $n-k$ generators (say $G = \langle g_1, \ldots, g_{n-k} \rangle$).

Error-correction potential of an $[n,k]$ stabilizer code C_G is characterized by the following theorem.

Theorem 0.13 *Let C_G be an $[n,k]$ stabilizer code with a stabilizer group G. Any set of Pauli error operators $\{E_i\}$ from $\mathcal{P}_n$ such that $E_j^\dagger E_i \notin Z(G) - G$, for all j and i, where $Z(G)$ is the centralizer[1] of G, is correctable by C_G.*

Proof Let $\{g_1, \ldots, g_{n-k}\}$ be a set of generators of G. In the proof we will make an essential use of the fact that the projector P_G into the code C_G has the form $P_G = 2^{k-n}\Pi_{i=1}^{n-k}(I+g_i)$.

For two error operators E_i and E_j there are two possibilities.

1. $E_i^\dagger E_j \in G$. Since the projector P_G is invariant under multiplication by elements of G we get $P_G E_i^\dagger E_j P_G = P_G^2 = P_G$.

[1] A centralize $Z(G)$ of G is the set of all elements of $\mathcal{P}_n$ that commute with all elements of G. An equivalent concept is that of a normalizer of G as the set of all those elements E of $\mathcal{P}_n$ such that $EgE^\dagger \in G$ for all $g \in G$.

2. $E_i^\dagger E_j \in \mathcal{P}_n - N(G)$. Then $E_i^\dagger E_j$ has to anticomute with some element of G and without loss of generality we can assume that anticomutes with g_1. This implies

$$P_G E_i^\dagger E_j P_G = \frac{\Pi_{l=2}^{n-k}(I+g_l)}{2^{n-k}}(I+g_1)(I-g_1)E_i^\dagger E_j \frac{\Pi_{l=2}^{n-k}(I+g_l)}{2^{n-k}} = 0$$

because $(I+g_1)(I-g_1)=0$ and, due to anticomutativity, $(1-g_1)E_i^\dagger E_j = E_i^\dagger E_j(1+g_1)$.

In both cases therefore the error correction conditions ?? are satisfied, what was to show.

The above theorem has implications that have a form similar to that for classical linear codes.

Let us say that a stabilizer $[n,k]$ code with generator group G has a distance d, or that it is an $[n,k,d]$ code, if d is the smallest weight of operators in $Z(G)-G$ (that is number of elements of the tensor products forming the operator that are not the identity).

By Theorem ??, a code with distance at least $2t+1$ is capable to correct Pauli errors on t qubits.

DESIGN of LOGICAL X and Z OPERATORS

and computational basis states

Given a stabilizer code C_G with $G = \langle g_1, \ldots, g_{n-k} \rangle$ we can choose as codes of the computational basis states any orthonormal set of 2^k vectors in C_G.

There is, however, a better (more elegant/straightforward/systematic) way of doing that.

The basic task is to define logical operators x and z acting on particular qubits.

1. First, we choose, somehow, operators $z_1, \ldots z_k$ of $\mathcal{P}_n$ such that the set of operators $g_1, \ldots, g_{n-k}, z_1, \ldots, z_k$ forms an independent and commuting set. z_j will play the role of a logical Pauli σ_z-operator acting on the jth logical qubit. Once this is done, the logical computational basis state $|a_1 \ldots a_k\rangle$ is then the fix-point of the stabilizer

$$\langle g_1, \ldots, g_{n-k}, z_1, \ldots, z_k \rangle.$$

In order to define the logical x_j operator acting as NOT on the jth logical qubit, we take as x_j such a product of Pauli matrices that maps z_j into $-z_j$ under conjugation and maps all other z_j and generators g_i into themselves.

Clearly, such x_j commutes with all z_i except z_j, with which it anticomutes.

ENCODINGS and DECODINGS of STABILIZER CODES

We again assume that an $[n, k]$ stabilizer code C_G is given by a set of independent generators $G = \langle g_1, \ldots, g_{n-k}\rangle$ and a set $z_1, \ldots, z_k$ of logical Z-operators.

There are several ways to encode using stabilizer codes. A simple to explain, though non-unitary, is the following approach to encoding of an known quantum state:

The starting point is the state $|0\rangle^{\oplus n}$ which is first measured by observables $g_1, \ldots, g_{n-k}, z_1, \ldots, z_k$ and then the resulting state will have stabilizer $\langle \pm g_1, \ldots, \pm g_{n-k}, \pm z_1, \ldots, \pm z_k\rangle$, where signs depend on the results of the measurement.

As the next step we can obtain a state with the stabilizer $g_1, \ldots, g_{n-k}, z_1, \ldots, z_k$ by changing necessary signs of stabilizers using the technique presented in the proof of Theorem ??.

The resulting state encodes $|0\rangle^{\oplus k}$. Using the corresponding operators from the set $x_1, \ldots, x_k$ we can obtain then encoding of the computational basis states $|a_1 \ldots a_k\rangle$.

Cleve and Gottesman (????) have shown how to design systematically a unitary stabilizer circuit with $\mathcal{O}(n(n-k))$ gates for encoding of an arbitrary (unknown) state in a given stabilizer $[n, k]$ code, using the above standard form of the check matrix. This circuit can be used also for decoding once applied in the reverse way.

However, such decoding is mostly not needed because once computation is realized in a fault-tolerant manner, gates are performed by circuits on encoded qubits and also the outcome of computations can be obtained by measuring logical Z operators.

SYNDROME COMPUTATION by STABILIZER CODES

Syndrome computation and subsequent error-correction is also very simple for stabilizer $[n, k]$ codes with a generator group $G = \langle g_1, \ldots, g_{n-k} \rangle$ and a set $\{E_i\}$ of correctable errors.

To compute the error syndrome of an erroneous state the state is measured with respect to the observables $g_1, \ldots, g_{n-k}$ to obtain, as the syndromes, classical outcomes $m_1, \ldots, m_{n-k}$ of the measurements.

In the case the syndrome uniquely determines (up to a phase factor) the error E_j, what is always true for non-degenerate codes, then the application of the operator $E_j^\dagger$ makes needed error correction.

For degenerate codes it may happen that syndromes for two errors, say E_i and E_j are the same. In such a case $E_i P E_i^\dagger = E_j P E_j^\dagger$, where P is the projector into C_G code, and therefore $E_i^\dagger E_j P E_j^\dagger E_i = P$ what implies that $E_i^\dagger E_j \in G$. Hence an application of the operator $E_j^\dagger$ again performs desired error correction.

In other words, if an error E_i is detected, using a syndrome computation, then an application of the operator $E_j^\dagger$ performs error correction and it does not matter whether error is uniquely determined by a syndrome.

CSS codes

A very important class of stabilizer quantum codes are so called CSS-codes, or Calderbank-Shor-Steane codes, as named by their inventors.

CSS quantum codes make, in a very simple and direct way, an elegant use of the bit correction potential of certain pairs of the classical linear codes.

If C_1 and C_2 are classical $[n, k_1]$ and $[n, k_2]$ linear codes such that $C_2 \subseteq C_1$ and both C_1 and $C_2^{\perp}$ can correct up to t errors, then these codes can be used to construct an $[n, k_1 - k_2]$ quantum CSS code, of C_1 over C_2, denoted as CSS(C_1, C_2), capable of correcting errors on t qubits, as follows:

C_1 is partitioned by C_2 on cosets $u + C_2$ for $u \in C_1$ in such a way that for different $u, v \in C_1$ cosets $u + C_2$ and $v + C_2$ are either identical or disjoint. Number of different cosets is therefore $\frac{|C_1|}{|C_2|} = 2^{k_1 - k_2}$.

The quantum code CSS(C_1, C_2) is now defined as the vector space (of dimension $2^{k_1-k_2}$) spanned by the states

$$|u + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} |u + w\rangle = \frac{1}{\sqrt{|C_2^{\dagger}|}} \sum_{w \in C_1^{\perp}} |u + w\rangle.$$

If u_1 and u_2 are elements of the same (or different) cosets of C_1 with respect to C_2, then the states $|u_1 + C_2\rangle$ and $|u_2 + C_2\rangle$ are identical (are orthogonal) as it follows from the definition of cosets.

It is easy to verify that each CSS(C_1, C_2) code is a stabilizer code with generators having the following check matrix

$$\left[\begin{array}{c|c} H_{C_2^{\perp}} & 0 \\ 0 & H_{C_1} \end{array}\right].$$

An important special case of CSS-codes is if $C_1 = C_2 = C$ and $C^{\perp} \subseteq C$, that is if C is self-dual.

Example Let us now illustrate in details how to detect and correct errors in the case a codeword

$$|\phi\rangle = \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{w \in C_2^{\perp}} |u + w\rangle$$

of the code CSS(C_1, C_2), associated to an $u \in C_1$, is corrupted by bit errors represented by a bit-vector x and by sign errors represented by a bit-vector z to get a state $|\phi_1\rangle$.

Let us now denote briefly by $H_i, i = 1, 2$ the parity check matrices for codes C_1 and C_2. By using an ancilla and a syndrome computation circuit to map

$$|v\rangle|0\rangle \text{ to } |v\rangle|H_1 v\rangle,$$

we can transform

$$|\phi_1\rangle|0\rangle \rightarrow |\phi_1\rangle|H_1 x\rangle$$

and that allows to detect and to correct bit errors x. After the correction, the resulting state is

$$|\phi_2\rangle = \frac{1}{\sqrt{|C_2^{\perp}|}} \sum_{w \in C_2^{\perp}} (-1)^{(u+w) \cdot z} |u + w\rangle.$$

Next task is to detect and correct z-errors. This can be done at first by multiplying $|\phi_2\rangle$ with the Hadamard transform to get

$$|\phi_3\rangle = H|\phi_2\rangle = \frac{1}{\sqrt{|C_2^\perp|2^n}} \sum_{v\in C_2} \sum_{w\in C_2^\perp} (-1)^{(u+w)\cdot(v+z)}|v\rangle$$

and then by "removing" z from the exponent in the phase of the basis states using at first the substitution $z+v \rightarrow v'$ and then replacing v' with v. Hence

$$|\phi_4\rangle = \frac{1}{\sqrt{|C_2^\perp|2^n}} \sum_{v\in C_2} \sum_{w\in C_2^\perp} (-1)^{(u+w)\cdot v}|v+z\rangle.$$

The above sum can be simplified using the following identities

$$\sum_{w\in C_2^\perp} (-1)^{w\cdot v} = \begin{cases} |C_2^\perp|, & \text{if } v \notin C_2, \\ 0, & \text{otherwise;} \end{cases}$$

to yield

$$|\phi_4\rangle = \sqrt{\frac{|C_2^\perp|}{2^n}} \sum_{v\in C_2} (-1)^{u\cdot v}|v+z\rangle.$$

The rest of the error detection and correction process is then straightforward. At first, using the parity check matrix for C_2, the error z is detected and then corrected to get the state

$$|\phi_5\rangle = \sqrt{\frac{|C_2^\perp|}{2^n}} \sum_{v\in C_2} (-1)^{u\cdot v}|v\rangle = H|\phi\rangle$$

Since the Hadamard transform is self-inverse, one application on the Hadamard transform on the state $|\phi_5\rangle$ provides the original state $|\phi\rangle$.