

IV. Quantum error correction & fault-tolerant quantum computing

A key problem that needs to be understood and properly addressed if a large-scale quantum computer is going to become reality is how to deal with unavoidable errors resulting from the coupling to environment.

The coupling of a single qubit to the environment will lead to

$$(177) \quad \begin{array}{l} |0\rangle |E\rangle \\ |1\rangle |E\rangle \end{array} \xrightarrow{U(t)} \begin{array}{l} |1\rangle |E_{01}\rangle \\ |0\rangle |E_{10}\rangle \end{array} \quad \begin{array}{l} \text{spin} \\ \text{flip} \end{array}$$

or

$$(178) \quad \begin{array}{l} |0\rangle |E\rangle \\ |1\rangle |E\rangle \end{array} \xrightarrow{U(t)} \begin{array}{l} |0\rangle |E_{00}\rangle \\ |1\rangle |E_{11}\rangle \end{array} \quad \text{dephasing}$$

In the course of time the environment states become more and more orthogonal, i.e.:

$$(179) \quad |\langle E_{01}(t) | E_{10}(t) \rangle| \xrightarrow{t \rightarrow \infty} 0$$

$$(180) \quad |\langle E_{00}(t) | E_{11}(t) \rangle| \xrightarrow{t \rightarrow \infty} 0$$

This leads to the evolution of the reduced density matrix of the qubit

$$t=0 \quad |\psi(t=0)\rangle = [\alpha|0\rangle + \beta|1\rangle] \cdot |E\rangle$$

$$(187) \quad \rho_0 = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \begin{matrix} \nearrow \text{spin flip} \\ \searrow \text{dephasing} \end{matrix} \begin{pmatrix} |\beta|^2 & \alpha^*\beta \underbrace{\langle E_{01}(t) | E_{10}(t) \rangle}_{\hookrightarrow 0} \\ \underbrace{\alpha\beta^* \langle E_{10}(t) | E_{01}(t) \rangle}_{\hookrightarrow 0} & |\alpha|^2 \end{pmatrix}$$

$$\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \underbrace{\langle E_{00}(t) | E_{11}(t) \rangle}_{\hookrightarrow 0} \\ \underbrace{\alpha^*\beta \langle E_{11}(t) | E_{00}(t) \rangle}_{\hookrightarrow 0} & |\beta|^2 \end{pmatrix}$$

In both cases the off-diagonal terms decay
"decoherence"

In general

$$(182) \quad (\alpha|0\rangle + \beta|1\rangle) |E\rangle \rightarrow \begin{aligned} & (\alpha|0\rangle + \beta|1\rangle) |E_0\rangle \\ & + (\alpha|1\rangle + \beta|0\rangle) |E_x\rangle \\ & + (\alpha|0\rangle - \beta|1\rangle) |E_z\rangle \\ & + (-\alpha|1\rangle + \beta|0\rangle) |E_y\rangle \end{aligned}$$

$$= (\hat{I}|\psi_0\rangle)|E_0\rangle + (\hat{X}|\psi_0\rangle)|E_x\rangle + (\hat{Y}|\psi_0\rangle)|E_y\rangle + (\hat{Z}|\psi_0\rangle)|E_z\rangle$$

where

$$(183) \quad \hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

spin flip both dephasing

$$(184) \quad \hat{Y} = \hat{Z} \hat{X}$$

For a single qubit there are 3 different errors. In addition to the spin flip $\hat{X}$ corresponding to a classical bit flip error there is dephasing $\hat{Z}$ and the combination $\hat{Y} = \hat{Z} \hat{X}$

For classical computing a well consolidated theory building of error correction has been established. Many ideas carry over to the quantum case with some modifications

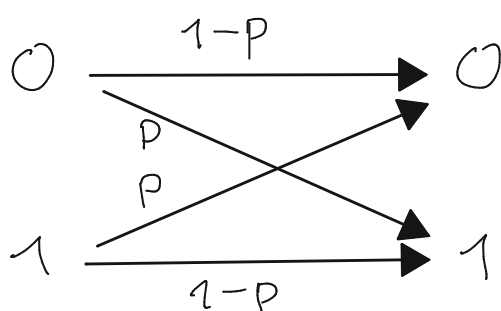
- (i) qubits have more than spin-flip errors
- (ii) state of qubit should not be measured or cloned in error correction procedure
- (iii) there is a new class of codes, known as degenerate codes, which do not exist in classical systems

4.1 Some elements of classical error correction

basic idea: encode bit into larger code

(185) 0 $\longrightarrow$ 000
 1 $\longrightarrow$ 111 3 bit repetition code

if a bit flip error occurs, e.g. in a binary symmetric channel



$0 \leq p \leq 1$ error probability.

- probability of error w/o coding: p
- probability of single error in code (185): $3p(1-p)$

$000 \xrightarrow{1 \text{ error}} 100 \quad 010 \quad 001$
 $111 \longrightarrow 011 \quad 101 \quad 110$

correctable !

$\longrightarrow$ majority vote 000
111

- probability of two or more errors in code (185)

$$P_{\text{error}} = 3p^2(1-p) + p^3 < p \quad \text{if } p < \frac{1}{2}$$

(A) Linear binary codes

binary code k bits encoded in $n > k$ bits

number of code words 2^k
 total number of words 2^n

linear, binary code

set C of code words which form a Galois field
 (endlicher Körper) with respect to bitwise
 addition modulo 2

• example: $C : \underbrace{\{(0,1,1), (1,0,1), (1,1,0), (0,0,0)\}}_{=4=2^2}$

$$(0,1,1) \oplus (0,1,1) = (0,0,0)$$

$$(0,1,1) \oplus (1,0,1) = (1,1,0)$$

$$(0,1,1) \oplus (1,1,0) = (1,0,1)$$

$$(0,1,1) \oplus (0,0,0) = (0,1,1)$$

$$n = 3$$

$$k = 2$$

basis in C $\{\underline{u}_1, \underline{u}_2, \dots, \underline{u}_k\}$

$\exists$ k basis vectors ; u_j code words
 consisting of $n \geq k$ bits

Every code word can be written as linear combination (mod 2) with prefactors

$$(185) \quad \alpha_j \in (0,1) \quad \underline{v} = \bigoplus_{j=1}^k \alpha_j \underline{v}_j$$

► $\underline{v}$ encodes a message $(\alpha_1, \alpha_2, \dots, \alpha_k)$ of k bits.

The basis vectors form a $k \times n$ generating matrix

$$(186) \quad \underline{\underline{G}} = \begin{bmatrix} \dots & \underline{v}_1 & \dots \\ \dots & \underline{v}_2 & \dots \\ \dots & \underline{v}_k & \dots \end{bmatrix} \left. \vphantom{\begin{bmatrix} \dots & \underline{v}_1 & \dots \\ \dots & \underline{v}_2 & \dots \\ \dots & \underline{v}_k & \dots \end{bmatrix}} \right\}^k$$

$\underbrace{\hspace{10em}}_n$

In the above example two basis vectors are e.g. $(0,1,1)$ and $(1,0,1)$. Thus

$$(187) \quad \underline{\underline{G}} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

With $\underline{\underline{G}}$ every codeword $\underline{v}$ can be written as

$$(188) \quad \underline{v} = \underline{\alpha} \underline{\underline{G}} \quad \underline{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_k)$$

alternative characteristics: parity-check matrix

$$(189) \quad \underline{\underline{H}} \underline{c}^T = 0 \quad \begin{array}{l} n-k \text{ conditions} \\ \text{on all codewords} \end{array}$$

$\underline{\underline{H}}$ is $(n-k) \times n$ matrix. Its rows are the $(n-k)$ linear independent vectors which are orthogonal to all code-words. In the example above (eq. 187, 188)

$$(190) \quad \underline{\underline{H}} = (1, 1, 1)$$

proof: $(0, 1, 1) \cdot (1, 1, 1) = 0 \oplus 1 \oplus 1 = 0 \pmod{2}$
 $(1, 0, 1) \cdot (1, 1, 1) = 1 \oplus 0 \oplus 1 = 0 \pmod{2}$

The same holds for all linear combination of basis vectors and thus for all codewords.

In a classical channel the only error is a bit-flip.

(B) Error detection and correction

Bit flip error

$$(191) \quad \underline{c} \longrightarrow \underline{c} \oplus \underline{e}$$

and $\underline{e} = (0, 1, 0)$ etc. with a "1" at the position of the error.

error detection

In a linear, binary code errors can be detected by application of the parity-check matrix

$$(192) \quad \underline{H}(\underline{u} \oplus \underline{e}) = \underline{H}\underline{u} \oplus \underline{H}\underline{e} = \underline{H}\underline{e} \quad \leftarrow \text{error syndrome}$$

The set $\mathcal{E}$ of all errors $\{\underline{e}_j\}$ which have different error syndromes can be detected and corrected

error correction

$$(193) \quad \underbrace{(\underline{u} \oplus \underline{e}_j)}_{\text{codeword with error}} \oplus \underline{e}_j = \underline{u}$$

If however $\underline{H}\underline{e}_1 = \underline{H}\underline{e}_2$ this does not work as

$$(\underline{u} \oplus \underline{e}_1) \oplus \underline{e}_2 \neq \underline{u}$$

$\Rightarrow$ What is the maximum number of errors correctable in a linear code?

(C) Hamming distance

The Hamming distance of a linear, binary code is the minimum number of bits to be flipped to transfer one element of the code into another one

A linear code with Hamming distance $d = 2t + 1$ can correct up to t bit flips

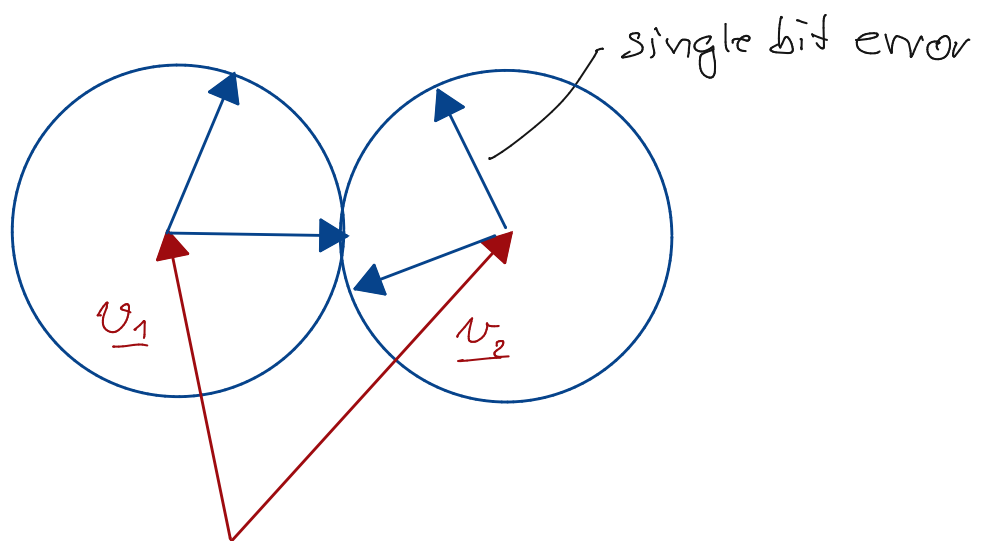
The code used in the above example has $d = 2$ and thus is useless for error correction

$$\underline{v}_1 = (0, 1, 1) \quad \underline{v}_2 = (1, 0, 1)$$

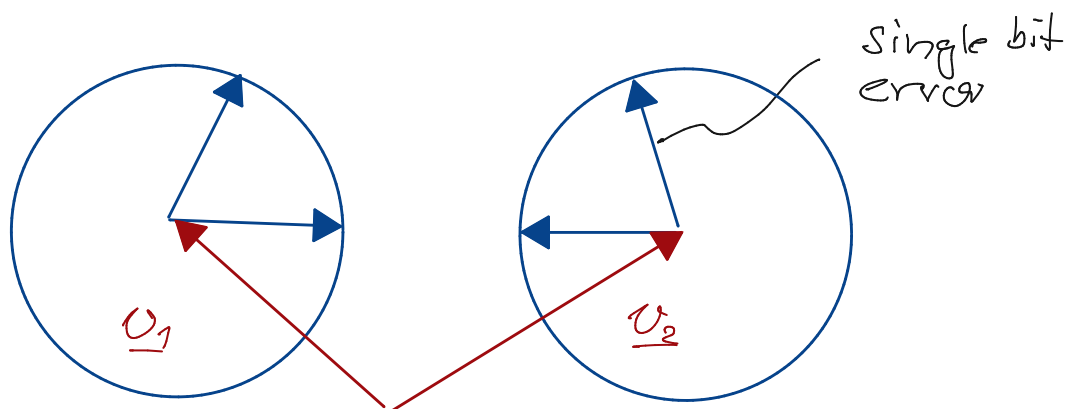
$$\underline{e}_1 = (1, 0, 0) \quad \underline{e}_2 = (0, 1, 0)$$

and $\underline{v}_1 \oplus \underline{e}_1 = \underline{v}_2 \oplus \underline{e}_2$ ☹️

$d=2$



$$d=3$$



notation

$[n, k, d]$ code

number of
bits in code

number
of encodable
bits

Hamming
distance

example:

$[7, 4, 3]$

Hamming code

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

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

if e_j is bit flip error at j th bit : error syndrome

$$He_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad He_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad He_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad He_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$He_5 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad He_6 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad He_7 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Gilbert-Varshamov bound

For large n there exist an $[n, k, 2t+1]$ codes that protect against t bits for some k such that

$$\frac{k}{n} \geq 1 - H\left(\frac{2t}{n}\right)$$

where $H(x) = -x \log x - (1-x) \log(1-x)$ is the binary Shannon entropy.

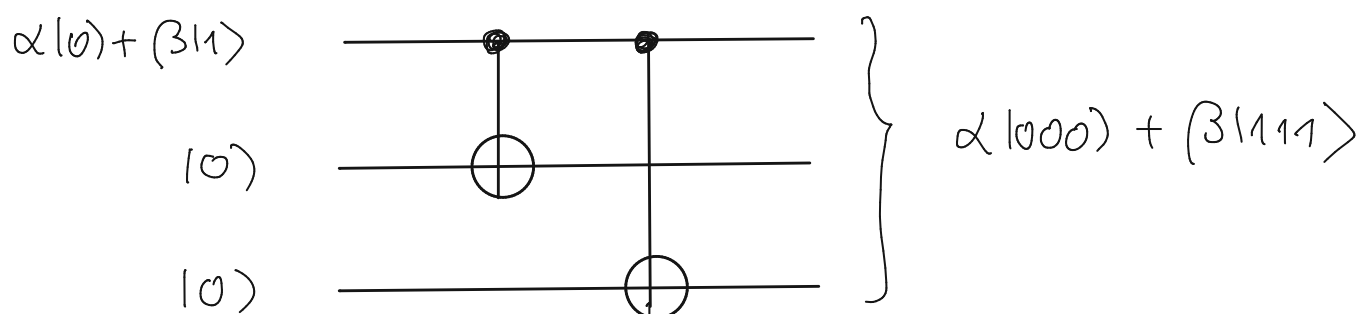
4.3 linear qubit codes

Surprisingly much of the ideas of classical error correction can be translated to qubits.

(A) The 3 qubit spin flip code

(i) encode qubit

$$(194) \quad \alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|000\rangle + \beta|111\rangle$$



(ii) interaction with environment
spin flip only; probability $p \ll 1/2$

$$\alpha|000\rangle + \beta|111\rangle$$

probability

$$\alpha|000\rangle + \beta|111\rangle$$

$$(1-p)^3 \approx 1-3p$$

$$\alpha|100\rangle + \beta|011\rangle$$

$$p(1-p)^2 \approx p$$

$$\alpha|010\rangle + \beta|101\rangle$$

$$p(1-p)^2 \approx p$$

$$\alpha|001\rangle + \beta|110\rangle$$

$$p(1-p)^2 \approx p$$

other

$$O(p^2) \text{ small}$$

(iii) error detection

$$k=1, n=3, d=3$$

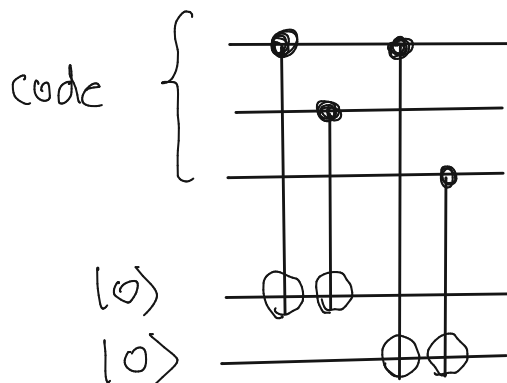
parity check matrix

$$(135) \quad \underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

important property

$$\underline{\underline{H}} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \underline{\underline{H}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 0$$

can be used to detect errors by entanglement with ancillas and detection of ancillas



$$\hat{=} \underline{\underline{H}}^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$$

} measurement of error syndrome

$\hat{X}$ error on $j = 1, 2, 3$ qubit: $\hat{X}_j$

e.g. $\hat{X}_2 |x, 0, z\rangle = |x, 1, z\rangle = |x, 0 \oplus 1, z\rangle$

in general

$\hat{=}$ classical error

$$\hat{X}_2 |x, y, z\rangle = |x, y \oplus 1, z\rangle = |x, y, z\rangle + \underbrace{|0, 1, 0\rangle}$$

$$\underline{\underline{H}} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \underline{\underline{H}} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \underline{\underline{H}} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

all $\hat{X}$ errors in the code (194) can be detected up to one spin flip

$$\begin{aligned} & (\alpha |1000\rangle + \beta |1111\rangle) \\ \Rightarrow & \begin{pmatrix} \alpha |100\rangle + \beta |011\rangle \\ \alpha |010\rangle + \beta |101\rangle \\ \alpha |001\rangle + \beta |110\rangle \end{pmatrix} \end{aligned}$$

$\begin{matrix} |00\rangle \\ |11\rangle \\ |10\rangle \\ |01\rangle \end{matrix}$

$\leftarrow$ no error
 $\left. \begin{matrix} |11\rangle \\ |10\rangle \\ |01\rangle \end{matrix} \right\}$ error syndrome

(iv) error correction

application of $\hat{X}_j$

if $|10\rangle \Rightarrow \hat{I}_1 \hat{X}_2 \hat{I}_3$

(197) $|01\rangle \Rightarrow \hat{I}_1 \hat{I}_2 \hat{X}_3$

$|11\rangle \Rightarrow \hat{X}_1 \hat{I}_2 \hat{I}_3$

remark:

The extraction of the error syndrome through the implementation of H^T can also be interpreted in a different way. The measurement scheme actually projects on the four eigenstates of

$$(198) \quad \begin{array}{cc} Z_1 Z_2 & \text{and} \quad Z_2 Z_3 \\ \lambda = \pm 1 & \quad \lambda = \pm 1 \end{array}$$

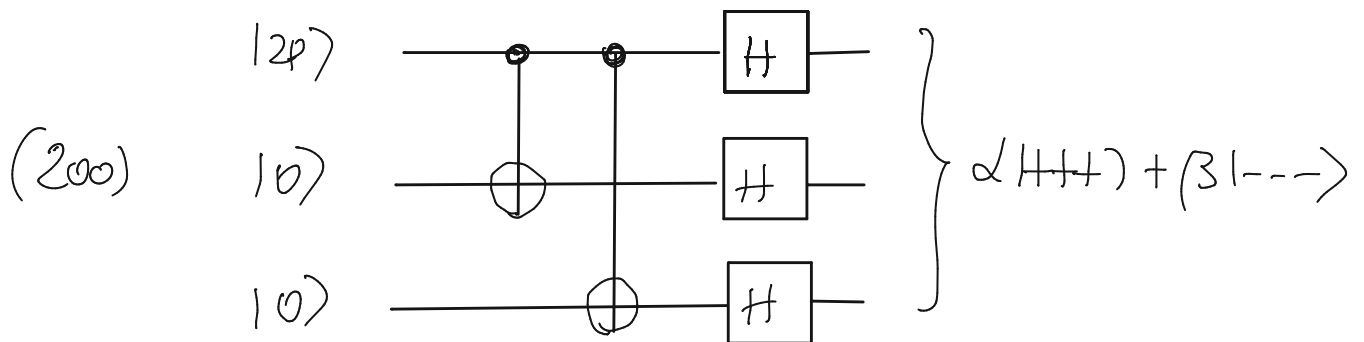
importantly the measurement of $Z_1 Z_2$ and $Z_2 Z_3$ leaves the states $|000\rangle$ and $|111\rangle$ invariant so their measurement does not kill coherences or entanglement

(B) The 3 qubit phase flip code

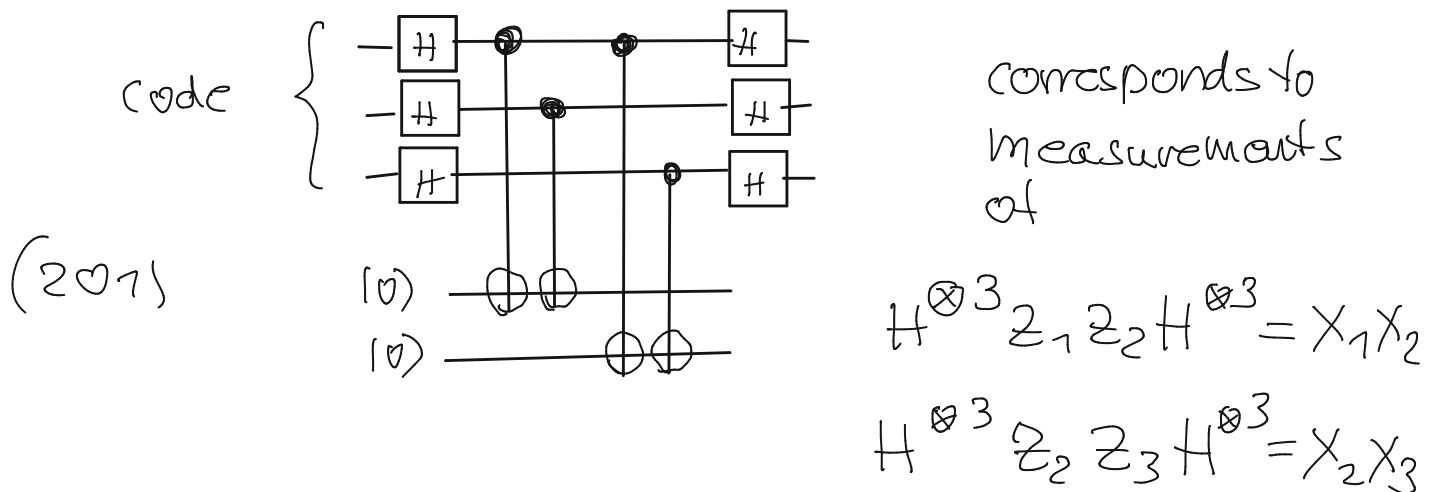
Much more relevant in quantum channels are phase flips rather than spin flips. Then we can use the 3 qubit phase flip code

$$(199) \quad \begin{array}{ccc} |2\rangle = \alpha|0\rangle + \beta|1\rangle & & |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \\ \downarrow & & \\ \alpha|+++ \rangle + \beta|--- \rangle & & \end{array}$$

implementation of encoding



error detection



error correction

analogously to spin-flip code

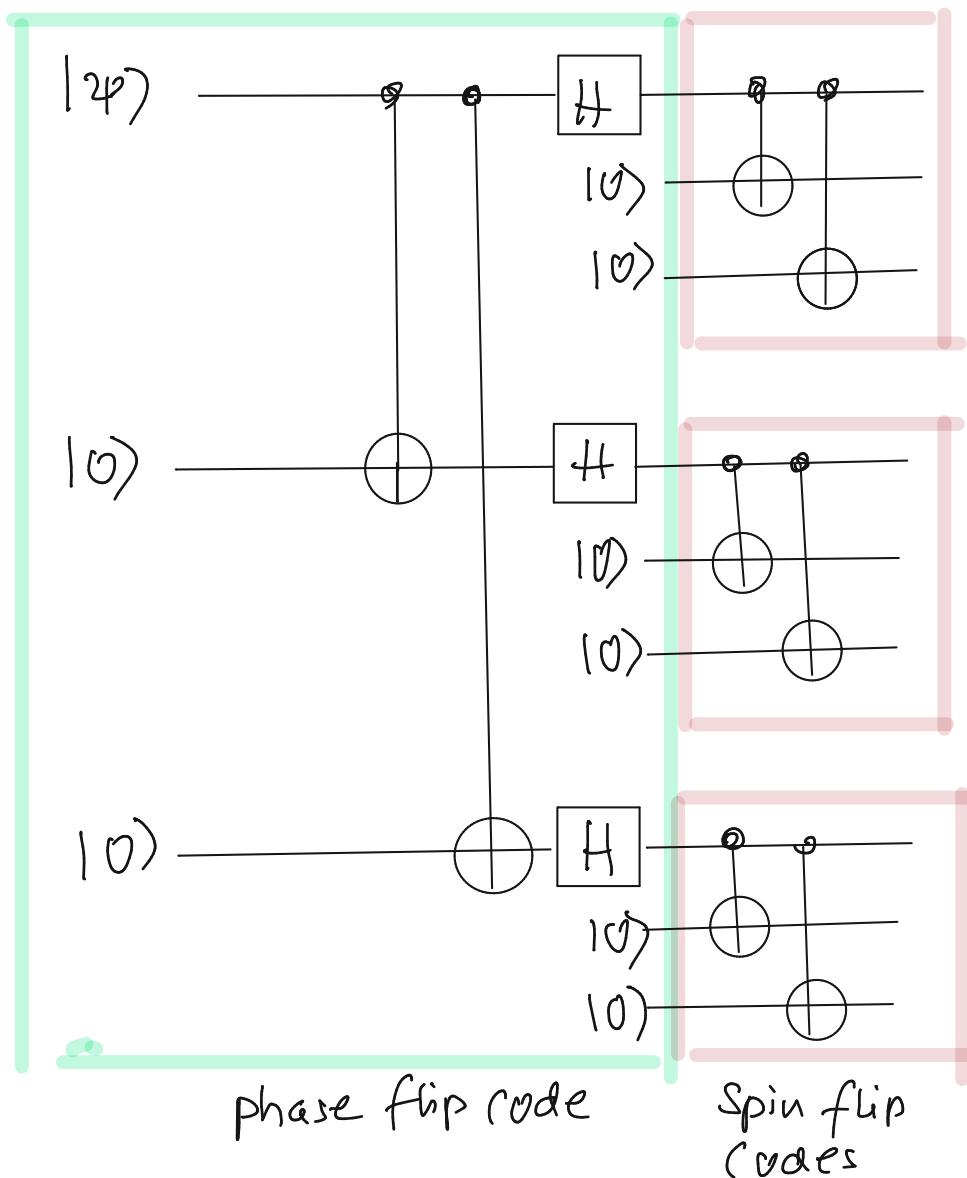
(C) Shor 9 qubit code

A linear quantum code that can correct arbitrary qubit errors on a single qubit is the Shor code. It is a combination of the spin-flip

and phase-flip code using a scheme known as concatenation of simple codes

$$\begin{aligned} (202) \quad |0\rangle &\rightarrow \frac{(|1000\rangle + |1111\rangle)(|1000\rangle + |1111\rangle)(|1000\rangle + |1111\rangle)}{2\sqrt{2}} \\ |1\rangle &\rightarrow \frac{(|1000\rangle - |1111\rangle)(|1000\rangle - |1111\rangle)(|1000\rangle - |1111\rangle)}{2\sqrt{2}} \end{aligned}$$

implementation:



for more details
see e.g.
Nielsen & Chuang

detection of error syndromes and correction

► spin flip e.g. in first block 1, 2, 3:

detect $z_1 z_2$ and $z_2 z_3$

+	+	no error
-	+	1st qubit
-	-	2nd qubit
+	-	3rd qubit

analogously for other blocks

correct apply X_1 or X_2 or X_3

► phase flip e.g. on first block

⇒ changes sign on first qubit block

$$(|000\rangle + |111\rangle)(\dots)(\dots)$$



$$(|000\rangle - |111\rangle)(\dots)(\dots)$$

detect

$X_1 X_2 X_3 X_4 X_5 X_6$ and $X_4 X_5 X_6 X_7 X_8 X_9$

+

-

-

-

+

+

-

+

no error

phase in 1st block

phase in 2nd block

phase in 3rd block

correct

apply

$Z_1 Z_2 Z_3$ or $Z_4 Z_5 Z_6$
or $Z_7 Z_8 Z_9$

(D) Conditions for Error correction

The reason why classical error correction in digital information processing is so powerful is that classical bit errors are discrete!

In analog systems this is not the case!

⇒ How about quantum errors? They are not discrete but can be arbitrary superpositions of X , Z and $Y = XZ$

The continuum of errors that can happen to a qubit can all be corrected by correcting only a discrete subset of errors.

consider single qubit e.g. in Shor code $(|0\rangle_L, |1\rangle_L)$

$$|\psi\rangle = \alpha|0\rangle_L + \beta|1\rangle_L$$

error

$$(203) \quad \mathcal{E}(|\psi\rangle\langle\psi|) = \sum_j \hat{E}_j |\psi\rangle\langle\psi| \hat{E}_j^\dagger$$

where $\hat{E}_j$ are Krauss operators of error
arbitrary error on first qubit of the code

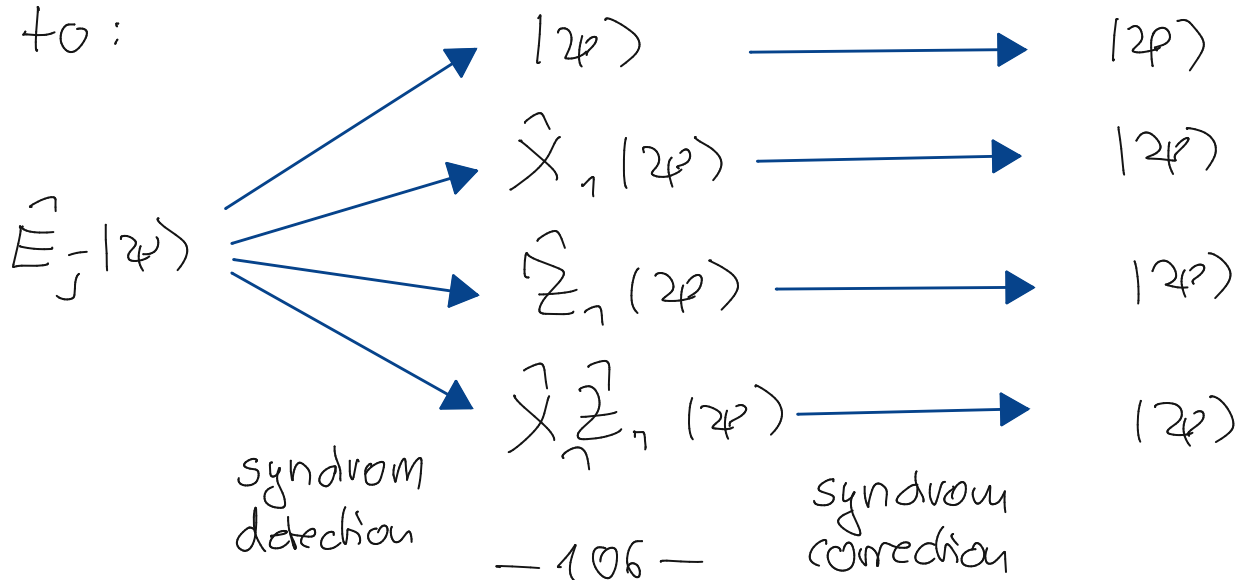
$$(204) \quad \hat{E}_j = \varepsilon_{j0} \hat{I} + \varepsilon_{j1} \hat{X}_1 + \varepsilon_{j2} \hat{Z}_1 + \varepsilon_{j3} \hat{X}_1 \hat{Z}_1$$

so

$$\begin{aligned} \hat{E}_j |\psi\rangle &= \varepsilon_{j0} |\psi\rangle + \varepsilon_{j1} \hat{X}_1 |\psi\rangle \\ &\quad + \varepsilon_{j2} \hat{Z}_1 |\psi\rangle + \varepsilon_{j3} \hat{X}_1 \hat{Z}_1 |\psi\rangle \end{aligned}$$

measuring error syndrome collapses this state

to:



Quantum error-correction condition

Let C be a quantum code and P the projector on the code (subspace). Suppose $\mathcal{E}$ is a quantum error with Krauss operators $\hat{E}_j$. A necessary and sufficient condition for the existence of an error-correcting operation R on C which corrects $\mathcal{E}$ is

$$(205) \quad P \hat{E}_m \hat{E}_j^\dagger P = \alpha_{mj} P$$

with some hermitian matrix α . The set of errors $\mathcal{E}$ is called correctable set of errors.

4.4 Stabilizer codes

We have seen in specific examples that error correction can be applied to quantum systems. Can we systematically understand

- how to construct quantum codes?
- how to construct error syndrome detection?

- What are correctable errors?

An important class of quantum codes are the so called stabilizer codes, which we will now discuss.

(A) Stabilizer formalism

To discuss stabilizer codes it is useful to first introduce the stabilizer formalism. The latter can be illustrated with the following simple example

EPR state of two qubits

$$(206) \quad |2\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

It is easy to see that $|2\rangle$ is an eigenstate of

$$(207) \quad \hat{X}_1 \hat{X}_2 |2\rangle = |2\rangle \quad \text{and} \quad \hat{Z}_1 \hat{Z}_2 |2\rangle = |2\rangle$$

We say $|2\rangle$ is stabilized by the operators $\hat{X}_1 \hat{X}_2$ and $\hat{Z}_1 \hat{Z}_2$. One can show that $|2\rangle$ is the only state which fulfills eq. (207).

It turns out that the discussion of many codes, their manipulation, description of errors and measurements can conveniently be discussed in terms of the stabilizers rather than the states.

stabilizer formalism $\hat{=}$ clever use of group theory

Pauli group of one qubit

$$(208) \quad G_1 \equiv \{ \pm \hat{I}, \pm i \hat{I}, \pm \hat{X}, \pm i \hat{X}, \pm \hat{Y}, \pm i \hat{Y}, \pm \hat{Z}, \pm i \hat{Z} \}$$

is a group under matrix multiplication

Pauli group of n qubits G_n : all tensor products

Def: Consider a subgroup S of G_n .
Let V_S be the set of n -qubit states that are stabilized by the elements of S . Then S is called stabilizer of the space V_S

- linear combination of two elements of V_S is in V_S

example: $n=3$

$$(209) \quad S = \{ \hat{I}, \hat{z}_1 \hat{z}_2, \hat{z}_2 \hat{z}_3, \hat{z}_1 \hat{z}_3 \}$$

$\hat{I}$: all 3 qubit states

$$\begin{aligned} z_1 z_2 &: |000\rangle, |001\rangle, |110\rangle, |111\rangle \\ z_2 z_3 &: |000\rangle, |100\rangle, |011\rangle, |111\rangle \\ z_1 z_3 &: |000\rangle, |010\rangle, |101\rangle, |111\rangle \end{aligned}$$

$$(210) \quad V_S : |000\rangle, |111\rangle$$

here looking at elements $z_1 z_2$ and $z_2 z_3$ is sufficient $\Rightarrow$

Def: A subset of elements $\{g_1, g_2, \dots, g_e\}$ of a group G is called generator of G if all elements of G can be written as products of the g_j

notation

$$(211) \quad G = \langle g_1, \dots, g_e \rangle$$

in our example:

$$(212) \quad S = \langle z_1 z_2, z_2 z_3 \rangle$$

proof: $z_1 z_2 \cdot z_2 z_3 = z_1 z_3$

$$(z_1 z_2)^2 = \hat{I} \quad \square$$

Def: The elements of a generator are called independent if removing one generator makes the stabilizer smaller

- how to see if $S = \langle g_1, g_2, \dots, g_l \rangle$ is an independent set of generators?

check matrix

g_j : n -qubit operator eg. $\hat{X}_1 \hat{Z}_2 \hat{I}_3 \hat{X}_4 \hat{Y}_5 \dots$
consisting of $\hat{X}, \hat{Y}, \hat{Z}, \hat{I}$

$$\begin{array}{c}
 l \\
 \left\{ \begin{array}{c} \left(\begin{array}{c} \text{--- } g_1 \text{ ---} \\ \text{--- } g_2 \text{ ---} \\ \vdots \\ \text{--- } g_l \text{ ---} \end{array} \right) \end{array} \right.
 \end{array}$$

$\underbrace{\hspace{10em}}_n$

$\underbrace{\hspace{10em}}_n$

(213)

$$\left(\begin{array}{c|c}
 \begin{array}{cccccc} 0 & 0 & 1 & 0 & 0 & 0 & 1 & \dots \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & \dots \end{array} &
 \begin{array}{c} \text{--- } g_1 \text{ ---} \\ \text{--- } g_2 \text{ ---} \\ \vdots \\ \text{--- } g_l \text{ ---} \end{array} \\
 \begin{array}{c} \uparrow \\ \text{"1" at position} \\ \text{of } \boxed{X} \end{array} &
 \begin{array}{c} \uparrow \\ \text{"1" at position} \\ \text{of } \boxed{Z} \end{array}
 \end{array} \right)$$

- for a $\hat{Y}$ at some position j put a 1 in the left (X) side and a 1 in the right (Z) side

The elements of a generator of a stabilizer $S = \langle g_1, g_2, \dots, g_e \rangle$ are independent if the $2n$ dimensional row vectors of the check matrix are linear independent and S does not contain $-I$

lets denote the $2n$ -dimensional row vectors $r(g)$

Two elements g_1 and g_2 commute if

$$r(g_1) \wedge r(g_2)^T = 0$$

where

$$\wedge = \begin{pmatrix} 0 & I_n \\ I_n & 0 \end{pmatrix}$$

- Why condition of $-I$ not being an element of S ?

Note that not every subgroup S of the Pauli group is a useful stabilizer, e.g. $G_1 = \{\pm I, \pm X\}$ has only the trivial vector as space V_S since

$$-I |\varphi\rangle = |\varphi\rangle \Rightarrow |\varphi\rangle = 0$$

condition for non-trivial stabilizer $S \subset G_n$

(i) all elements commute

(ii) $-I$ is not an element of S

to emphasize the compactness of the stabilizer formalism let's consider the 7-qubit Steane code

$$(213) \quad |0\rangle_L = \frac{1}{\sqrt{8}} \left[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \right. \\ \left. + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \right]$$

$$|1\rangle_L = \frac{1}{\sqrt{8}} \left[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \right. \\ \left. + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \right]$$

stabilizers of Steane code

$$(214) \quad \begin{array}{l} g_1 \\ g_2 \\ g_3 \\ g_4 \\ g_5 \\ g_6 \end{array} \quad \begin{array}{cccccc} 1 & 1 & 1 & X & X & X & X \\ 1 & X & X & 1 & 1 & X & X \\ X & 1 & X & 1 & X & 1 & X \\ 1 & 1 & 1 & Z & Z & Z & Z \\ 1 & Z & Z & 1 & 1 & Z & Z \\ Z & 1 & Z & 1 & Z & 1 & Z \end{array}$$

- What is the dimension of the Hilbert space V_S of code states stabilized by S ?

Let $S = \langle g_1, g_2, \dots, g_{n-k} \rangle$ be a stabilizer for n qubits, such that $-I$ is not element. If all $n-k$ generators are independent and commute then the vector space of code states V_S is 2^k dimensional

(B) Unitary operations in stabilizer formalism

We will now see that all unitary operations i.e. gate operations but also errors due to interaction with environments can conveniently be described in the stabilizer formalism

Let $|\psi\rangle \in V_S$ and $g \in S$, i.e.

$$g|\psi\rangle = |\psi\rangle$$

$$\Rightarrow U|\psi\rangle = U g |\psi\rangle = U g U^{-1} U |\psi\rangle$$

$\Rightarrow$ vector space UV_S is stabilized by the group of all $\{U g U^{-1}\} = U S U^{-1}$

i.e. to compute effect of U it is sufficient to know its action on the independent generators

$$Ug_1U^{-1} \quad Ug_2U^{-1} \quad \dots \quad Ug_eU^{-1}$$

- for particular unitaries U this takes a very simple form:

$$\boxed{U = H} \quad \text{single qubit Hadamard} \quad H^+ = H^{-1}$$

$$(215) \quad \begin{aligned} HXH^+ &= Z & HZH^+ &= X \\ \Rightarrow H\gamma H^+ &= -\gamma \end{aligned}$$

$$\boxed{U = X, Y, Z}$$

$$(216) \quad \begin{aligned} XXX^+ &= X & XZX^+ &= -Z \end{aligned}$$

$$(217) \quad \begin{aligned} ZXZ^+ &= -X & ZZZ^+ &= Z \end{aligned}$$

$$\boxed{U = S} \quad \text{phase gate } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$(218) \quad \begin{aligned} SX S^+ &= Y & SZ S^+ &= Z \end{aligned}$$

This allows for every compact description of states that are stabilized (in the stabilizer space), e.g.

$$S = \langle Z_1, Z_2, \dots, Z_n \rangle \rightarrow |0\rangle^{\otimes n}$$

$$S = \langle X_1, X_2, \dots, X_n \rangle = \langle H Z_1 H^\dagger, H Z_2 H^\dagger, \dots \rangle$$

$$\rightarrow \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle)^{\otimes n} \text{ has } 2^n \text{ coefficients}$$

O.k., but may be not so impressive since stabilized states are not entangled!

• but consider two qubit operation CNOT

$$\boxed{U = \text{CNOT}}$$

(219)

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

one finds:

$$U X_1 U^\dagger = X_1 X_2$$

$$U Z_1 U^\dagger = Z_1$$

(220)

$$U X_2 U^\dagger = X_2$$

$$U Z_2 U^\dagger = Z_1 Z_2$$

- 117 -

closed!

$\Rightarrow$ Gottesman-Knill theorem

Def: n -qubit Clifford group W_n

group of unitary operators U which map all elements of the Pauli group to elements of the Pauli group

$$(221) \quad U G_n U^\dagger \in G_n^* \quad (* \text{ w/o } \pm 1)$$

The n -qubit Clifford group is generated by the Hadamard gate, the phase gate and the CNOT gate

$$(222) \quad W_n = \langle \{H, S, \text{CNOT}\} \rangle$$

rem: • Pauli X, Y, Z are elements of W_n

• the $\pi/8$ gate T is not element of the Clifford group

$$(223) \quad T X T^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\pi/4} \end{pmatrix} \\ = \begin{bmatrix} 0 & e^{-i\pi/4} \\ e^{i\pi/4} & 0 \end{bmatrix} = \underbrace{\frac{1}{\sqrt{2}} X + \frac{1}{\sqrt{2}} Y}_{\neq G_n}$$

number of Pauli's increases by factor 2 in each step

The action of a quantum algorithm that only contains operators from the Clifford group on a suitable initial n -qubit state can efficiently be described classically (e.g. by keeping track of the action of the Clifford gates on the stabilizers of the state).

$\Rightarrow$ Gottesman - Knill theorem

rem: • also measurements in the computational basis can easily be described in the stabilizer formalism

(c) Constructing a stabilizer code, error detection, and correction

- $[n, k]$ stabilizer code: constructed of the 2^k orthonormal vectors $|\psi\rangle \in V$ of n qubits ($n > k$) stabilized by subgroup $S \subset G_n$

$$S = \langle g_1, g_2, \dots, g_{n-k} \rangle$$

and g_i independent and mutually commuting

$$g_j |\psi\rangle = |\psi\rangle \quad j=1,2,\dots,n-k$$

• error detection

Any error happening on a state $|\psi\rangle$ is an element (or superposition of elements) of G_n

$$(224) \quad E \in G_n$$

So E either commutes or anticommutes with the generators g_j .

$$\boxed{\text{I}} \quad \exists \{E, g_e\} = 0 \quad \text{i.e. it anticommutes with some } g_e$$

$$(225) \quad g_e E |\psi\rangle = -E g_e |\psi\rangle = -E |\psi\rangle$$

$$\text{while } g_e |\psi\rangle = |\psi\rangle$$

$\Rightarrow$ action of error easily detectable!

$$\boxed{\text{II}} \quad E \text{ commutes with all } g_j \\ \text{and, } E \in S$$

$\Rightarrow$ does not corrupt the code

$$\boxed{\text{III}} \quad E \text{ commutes with all } g_j \\ \text{but } E \notin S \quad \text{not detectable}$$

Def: The set of all operators $E \in G_n$ which commute with all generators of stabilizer S i.e.

$$Eg_j = g_j E$$

(225) is called centralizer $Z(S)$.

Def: The set of all operators $E \in G_n$ for which holds

$$Eg_j E^\dagger \in S$$

(226) for all generators of stabilizer S are called normalizer $N(S)$

If S does not contain $-I$ then $N(S) = Z(S)$.

Error correction condition for stabilizer codes

Let S be the stabilizer of a stabilizer code $C(S)$. Suppose $\{E_j\}$ is a set of operators in G_n . If

$$(227) \quad E_j^\dagger E_k \notin N(S) - S \quad \forall j, k$$

then $\{E_j\}$ is a correctable set of errors for the code $C(S)$

Can we define something analogous to the Hamming distance?

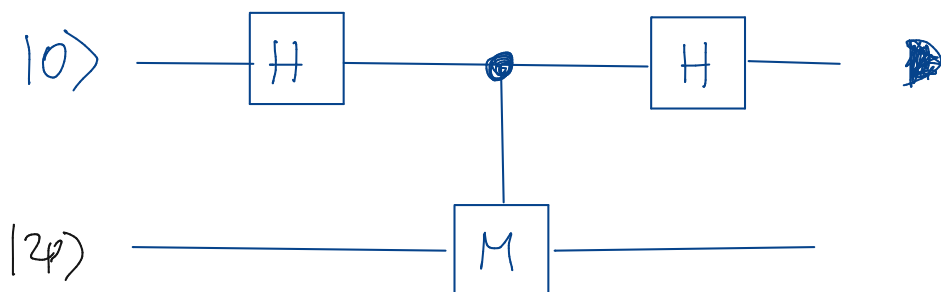
Def: The distance d of a stabilizer code $C(S)$ is the minimum number of single qubit operators different from the identity in $N(S) - S$.

An $[[n, k, d=2t+1]]$ stabilizer code can correct arbitrary qubit errors on any t qubits.

e.g. $E = I_1 I_2 \underline{X}_3 I_4 \underline{Z}_5 I_6 I_7 \underline{Y}_8$ has 3 operators

• Quantum circuits for error detection

Quantum circuit for measuring single-qubit operator M with eigenvalues ± 1



$$|\psi\rangle = \alpha |M=+1\rangle + \beta |M=-1\rangle = \alpha |+\rangle + \beta |-\rangle$$

$$|0\rangle|2\rangle \xrightarrow{H} \frac{(|0\rangle + |1\rangle)}{\sqrt{2}}|2\rangle \xrightarrow{M} \frac{(|0\rangle|2\rangle + |1\rangle M|2\rangle)}{\sqrt{2}}$$

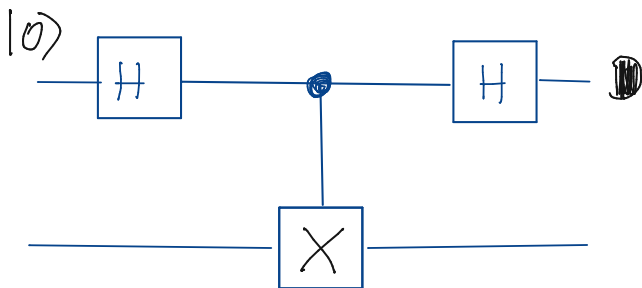
$$= \frac{|0\rangle(\alpha|+\rangle + \beta|-\rangle) + |1\rangle(\alpha|+\rangle - \beta|-\rangle)}{\sqrt{2}}$$

$$= \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}}|+\rangle + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}|-\rangle$$

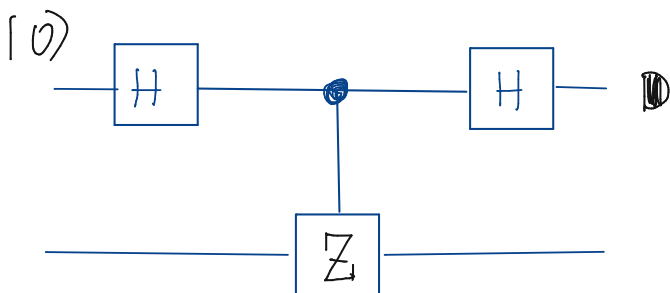
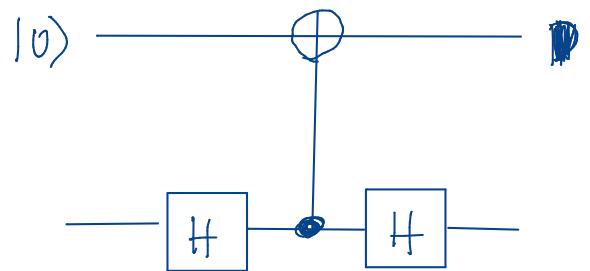
$$\xrightarrow{H} \alpha|1\rangle|+\rangle + \beta|0\rangle|-\rangle$$

$\swarrow$
 $p(1) = |\alpha|^2$
 $\searrow$
 $p(0) = |\beta|^2$

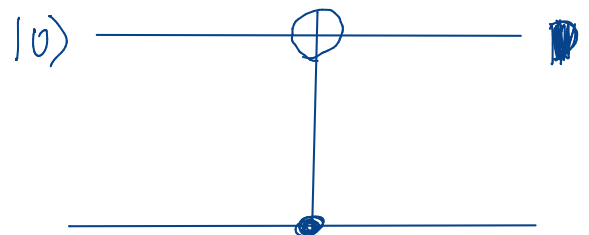
equivalent circuit



$\equiv$



$\equiv$



How to construct circuit for detecting error syndromes?
 Starting point is the check matrix eq. (213).

$$(228) \quad G = \left[\underbrace{G_x}_{2n} \mid \underbrace{G_z}_{2n} \right] \}^{n-k}$$

First we bring this matrix into a standard form by

- Swapping rows (re-label generators)
- Swapping columns simultaneously on the left and right submatrix (re-label qubits)
- adding two rows (multiplying generators)

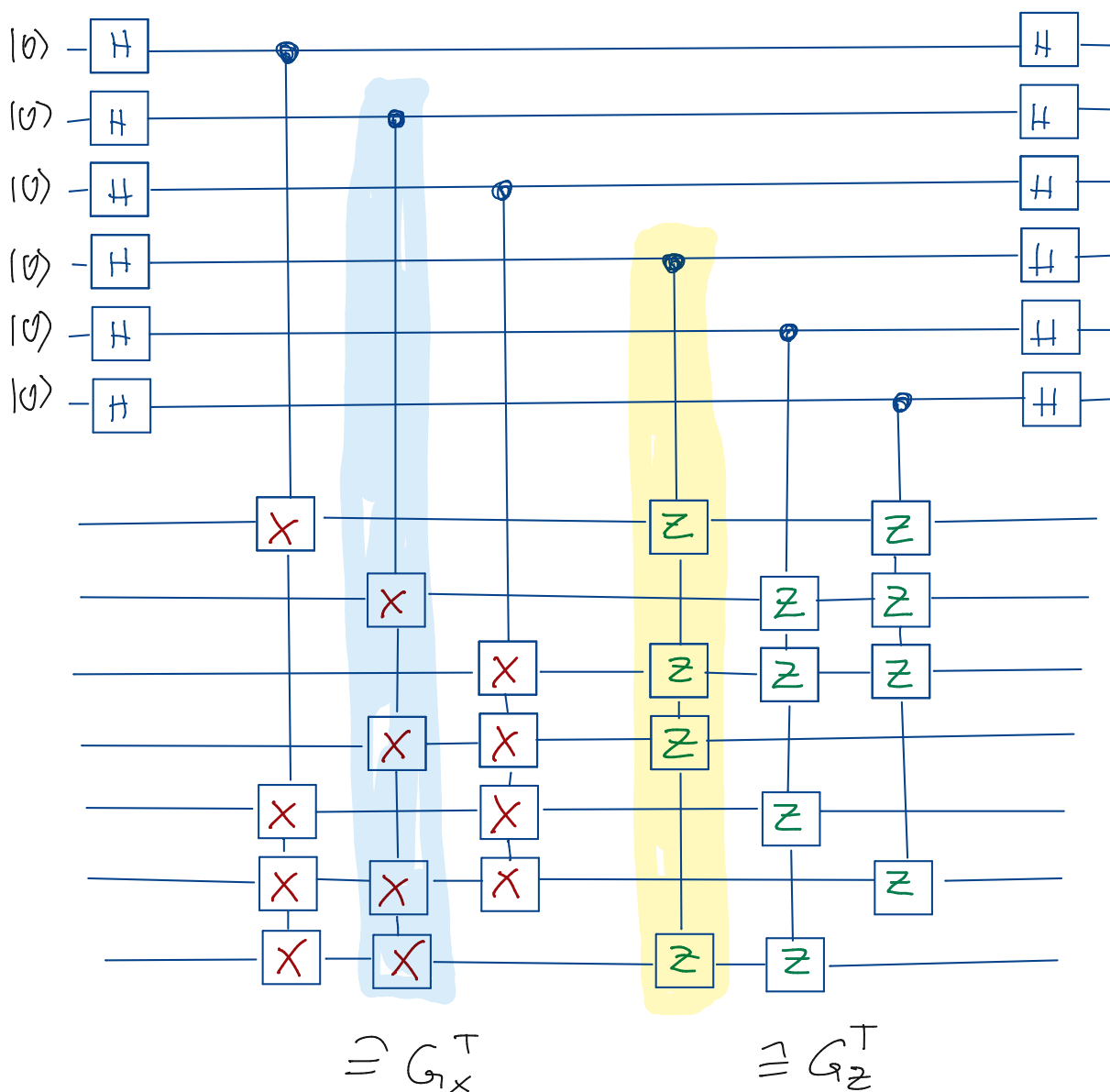
If r is the rank of G , then we can bring G to a standard form (not completely unique)

$$\begin{array}{l} r \{ \\ n-k-r \{ \end{array} \left[\begin{array}{ccc|ccc} \overbrace{\quad}^r & \overbrace{\quad}^{n-k-r} & \overbrace{\quad}^k & \overbrace{\quad}^r & \overbrace{\quad}^{n-k-r} & \overbrace{\quad}^k \\ \hline \mathbb{1} & A_1 & A_2 & B & 0 & C \\ 0 & 0 & 0 & D & \mathbb{1} & E \end{array} \right]$$

(229)

e.g. standard form of check matrix of 7-qubit Steane code

$$\left[\begin{array}{cccccc|cccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{array} \right]$$



4.5 Fault tolerant q-computing

(A) Goal and principle

Goal: Protection of quantum information during computation dynamics

remember: error correction idea

$$|0\rangle \longrightarrow |000\rangle = |0\rangle_L$$

$$|1\rangle \longrightarrow |111\rangle = |1\rangle_L$$

physical qubit
error probability

$$p$$

qubit code
error probability

$$O(p^2)$$

• how about gate operations?

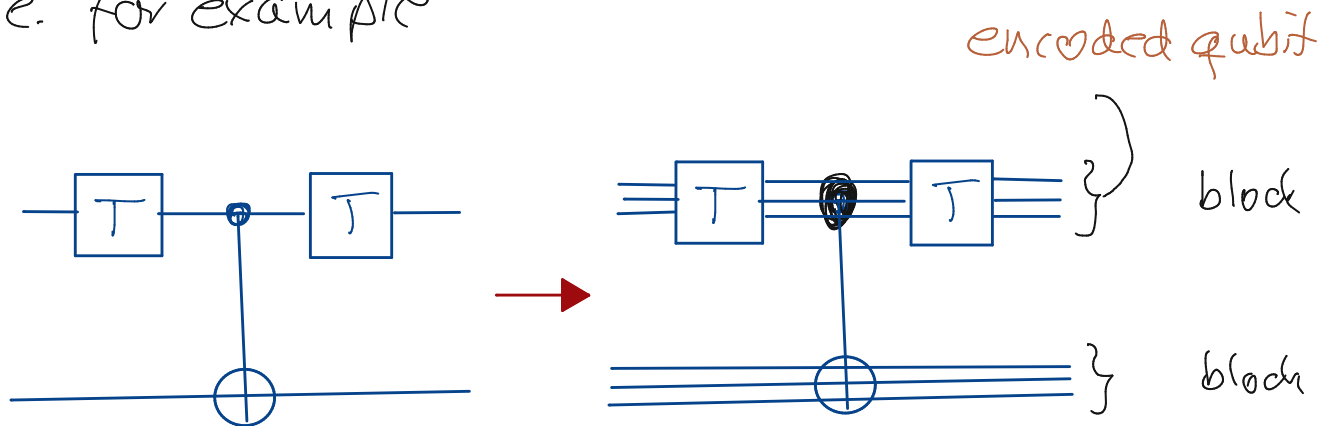
naive (and stupid) approach:

- (i) decoding of logical qubits
- (ii) gate operations
- (iii) coding of results ?

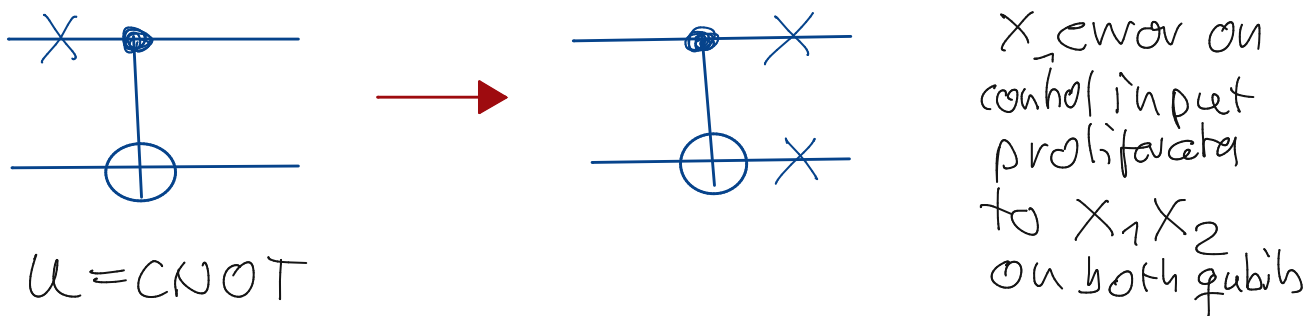
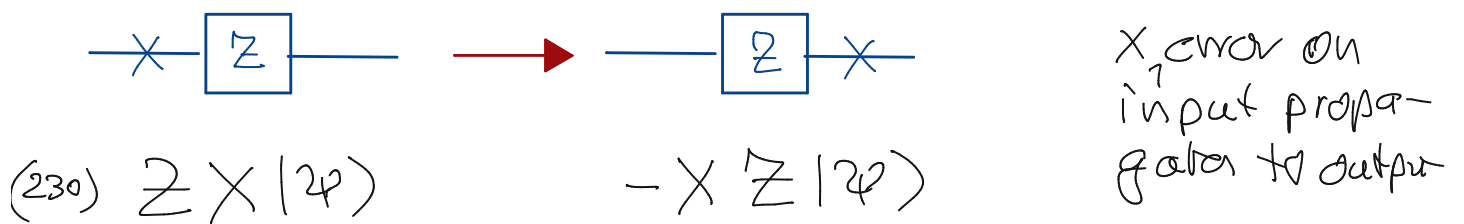
If during operation a single error on a physical qubit happens with probability p the whole gate operation has an error probability of p ! 😞

(i) need circuits for computation to operate on encoded data.

i.e. for example



This is however not sufficient as quantum gates can cause errors to propagate and proliferate. E.g.: error X_1

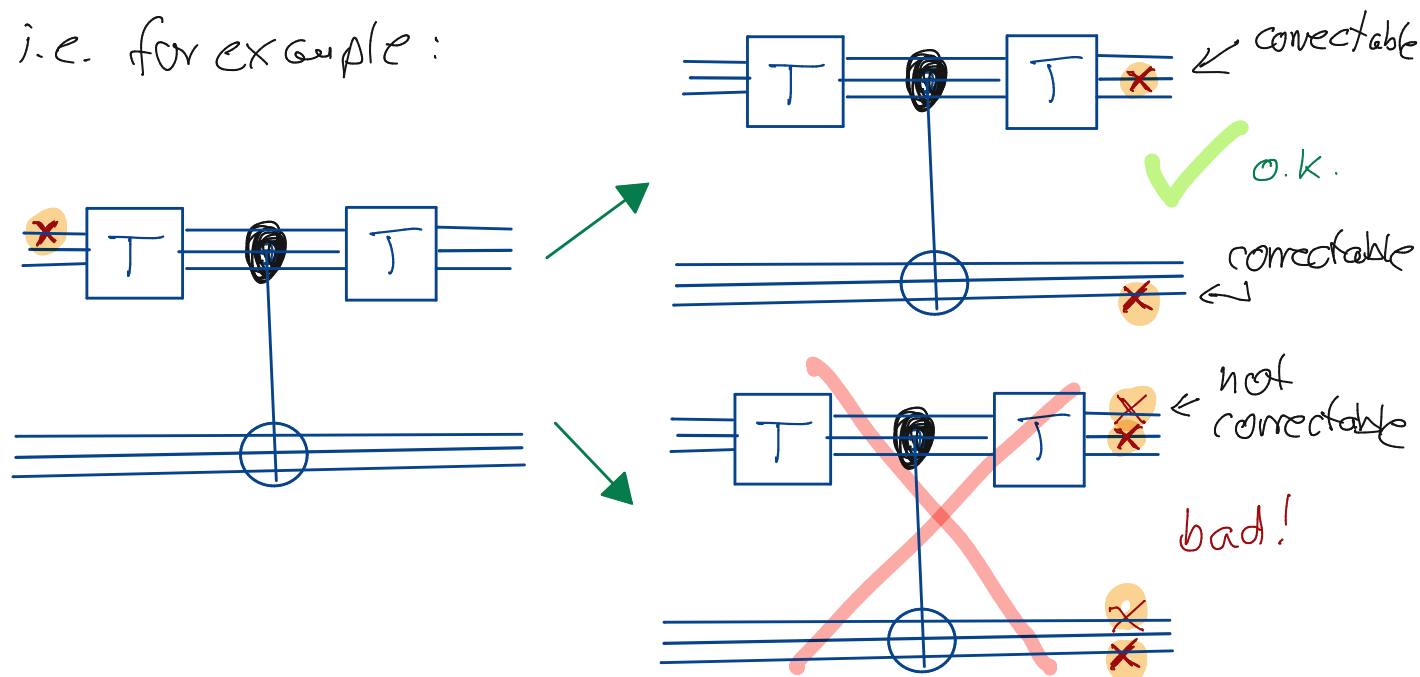


$$U X_1 | \psi \rangle = U X_1 U^{-1} U | \psi \rangle = X_1 X_2 U | \psi \rangle$$

(231)

(ii) need to construct circuits such that error on one physical qubit of input leads to an error in at most one physical qubit per output block

i.e. for example:



Finally the gate operation (measurement) itself may be faulty, e.g. a noisy CNOT gate

$$\Sigma = \Sigma_0 U^{-1} U \quad U = \text{CNOT}$$

$\Rightarrow$ CNOT + subsequent error " $\Sigma_0 U^{-1}$ "

$\Sigma_0 U^{-1}$ is an error such as X, Z in the tensor space affecting both (logical, i.e. encoded) qubits.

Finally we need fault tolerant preparation of states and measurements which can be defined in an analogous way.

(B) Concatenating codes and threshold condition

Let us assume that the fault tolerant gate architecture discussed in section (A) can be realized with d being the number of operations needed in one gate operation. How many gates do we need in total if the algorithm altogether shall have an error probability

$$\leq \epsilon \quad ?$$

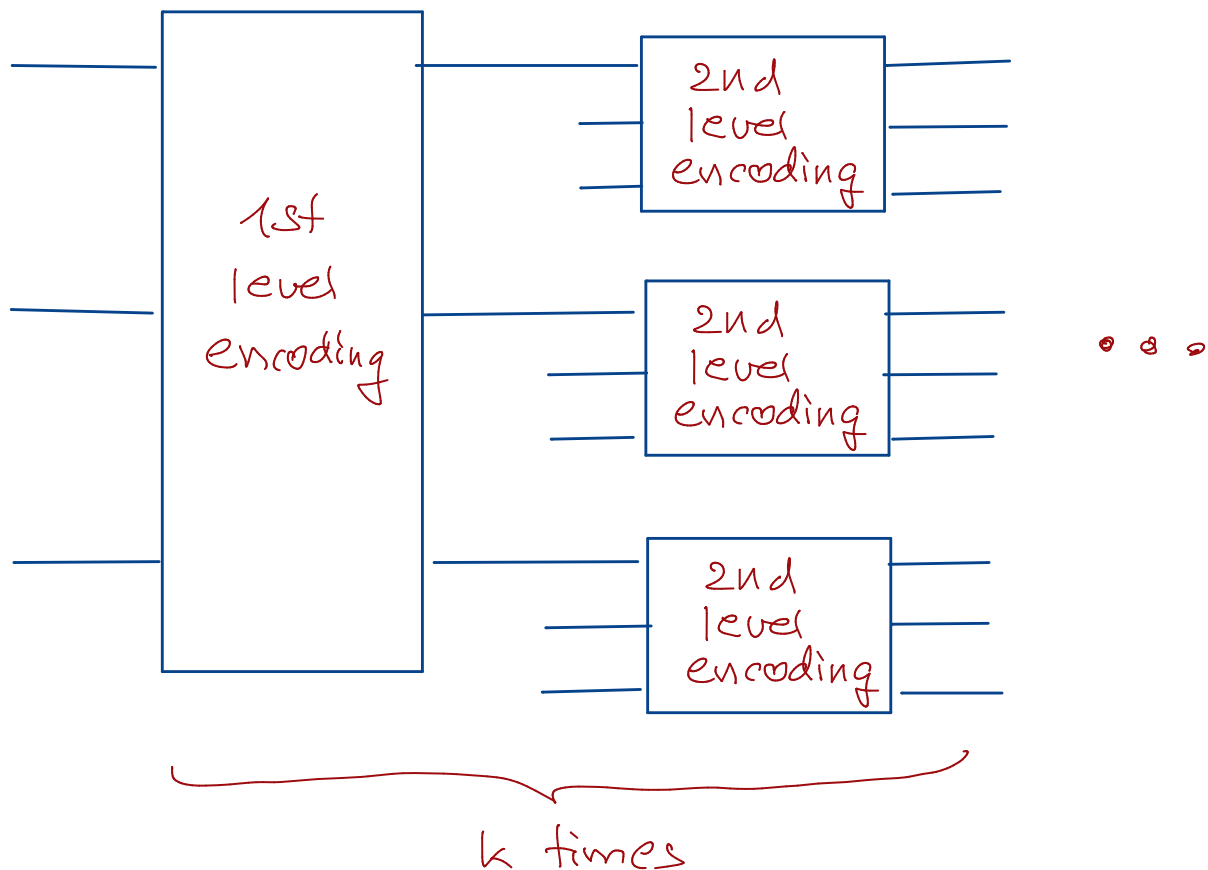
Let n describe the size of the problem (e.g. # of input bits). Suppose we want to implement a circuit with

$$(232) \quad N(n) = \text{poly}(n)$$

gates. Then the allowed error probability per fault-tolerant gate must be less than

$$(233) \quad p_{\text{gate}} \leq \epsilon / N(n)$$

This is demanding! However we can use a clever trick: concatinating codes for fault tolerant gates, e.g.



(i) probability of physical qubit error in one fault tolerant gate p

(ii) error probability of fault tolerant gate (1st level)
 cp^2

(iii) error probability of fault tolerant gate (2nd level)
 $c(cp^2)^2 = \frac{(cp)^4}{c}$

(iv) after k levels of concatenating this reduces to

$$(234) \quad \frac{(cp)^{2^k}}{c}$$

(235) if $p < p_{th} = \frac{1}{c}$ exponential decrease!

From the requirement (233), i.e.

$$(236) \quad \frac{(cp)^{2^k}}{c} < \frac{\varepsilon}{N(n)}$$

We can determine the minimum value of concatenating steps k . This gives the total number of elementary gate operations required

$$(237) \quad d^k = \mathcal{O}\left(\text{poly}\left(\log \frac{N(n)}{\varepsilon}\right) N(n)\right)$$

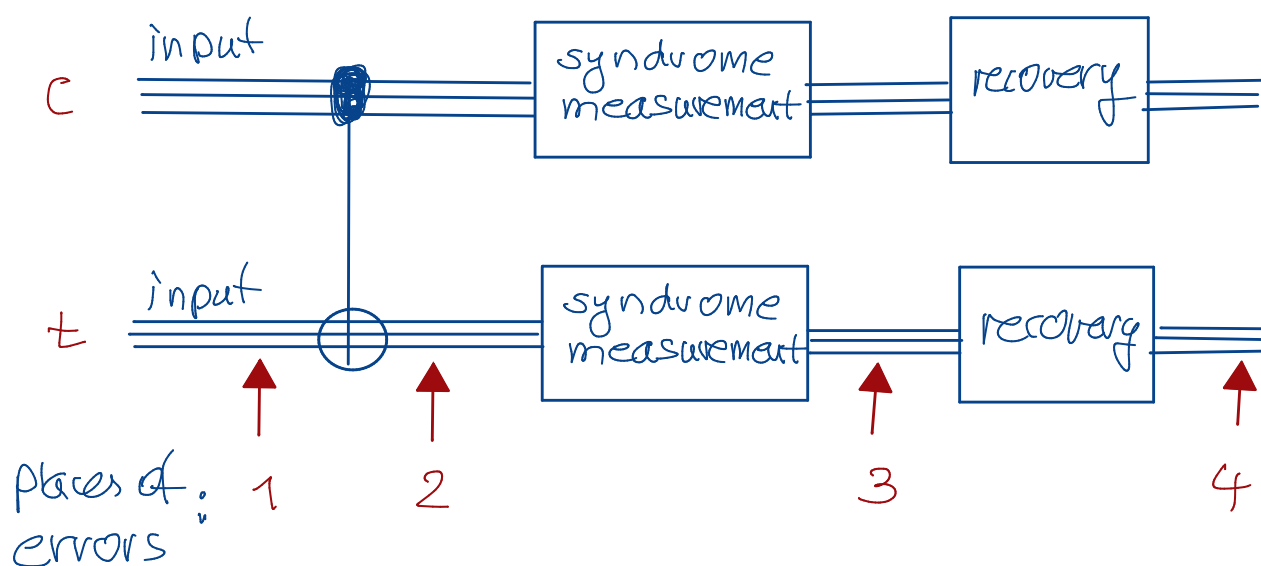
threshold theorem of quantum computation

A quantum circuit containing $N(n)$ logical gate operations may be simulated with error probability less than ε using

$$\mathcal{O}\left(\text{poly}\left(\log \frac{N(n)}{\varepsilon}\right) N(n)\right)$$

gates if the failure of each component happens with probability $p < p_{th} = 1/c$

- What is P_{th} ? This depends very much on the code that is used. Let's discuss this for the 7 qubit Steane code and a fault tolerant CNOT



Two errors per encoded block cannot be corrected, so let's estimate the probability of such an event if the probability of a single error on a physical qubit is p .

- (1) preexisting errors enter on both inputs (c and t) at step 1 and propagate via CNOT to one of the two outputs.

probability of preexisting error in one block

$$C_0 p$$

C_0 : total number of places during syndrome measurement and recovery of previous

stage of circuit. For Steane code $C_0 \approx 60+7$
 ≈ 70

Probability of two errors in output

$$(238) \leq C_0^2 p^2 \quad C_0^2 \approx 5 \cdot 10^3$$

(2) preexisting error enters in step 1 and error in CNOT operation happens

$$\leq 2 \times C_0 p \times n p = C_1 p^2$$

n : number of places in the CNOT circuit where an error can happen. For Steane $n \approx 7$
i.e. $C_1 = 2 \cdot 70 \cdot 7 \approx 10^3$

(3) two failures during CNOT circuit

$$\leq \frac{1}{2} n(n-1) p^2 = C_2 p^2$$

For Steane $C_2 \approx 20$

(4) failure during CNOT circuit and syndrome measurement (60 places)

$$\leq n \cdot 60 \cdot p^2 = C_3 p^2$$

For Steane $C_3 \approx 10^2$

(5) Two failures occur during syndrome measurement

$$\leq C_4 p^2 \quad \text{Steane } C_4 \approx 60^2 \approx 5 \cdot 10^3$$

(6) A failure during syndrome measurement and a failure in recovery

$$\leq C_5 p^2 \quad \text{Steane } C_5 \approx 60 \times 7 \approx 500$$

(7) two failures during recovery

$$\leq C_6 p^2 \quad \text{Steane } C_6 \approx 7^2 \approx 50$$

Total probability to have two or more errors in one of the two output blocks of the fault tolerant CNOT circuit

$$C p^2 \quad C = C_0^2 + C_7 + C_2 + C_3 + C_4 + C_5 + C_6$$

For the Steane code the threshold probability for an error to occur to any physical qubit is

(238)

$$C \approx 10^4 \Rightarrow p_{th}^{\text{steane}} = 10^{-4}$$

(C) Fault-tolerant operations of Clifford gates

A universal set of elementary gates is e.g.

$$(239) \quad \{H, S, CNOT, T\}$$

The first three are Clifford gates, the last one not. It turns out that the property (221) of the Clifford gates to map elements of the Pauli group back to elements of the Pauli group makes their fault tolerant construction relatively easy.

For the Steane code (7 qubit of CSS type) eqs. (213) :

$$|0\rangle_L = \frac{1}{\sqrt{8}} \left[|0000000\rangle + |1010101\rangle + |0110011\rangle + |1100110\rangle \right. \\ \left. + |0001111\rangle + |1011010\rangle + |0111100\rangle + |1101001\rangle \right]$$

$$|1\rangle_L = \frac{1}{\sqrt{8}} \left[|1111111\rangle + |0101010\rangle + |1001100\rangle + |0011001\rangle \right. \\ \left. + |1110000\rangle + |0100101\rangle + |1000011\rangle + |0010110\rangle \right]$$

it is easy to see that the logical Z and X operations read

$$(240) \quad \bar{Z} = Z_1 Z_2 Z_3 Z_4 Z_5 Z_6 Z_7$$
$$(241) \quad \bar{X} = X_1 X_2 X_3 X_4 X_5 X_6 X_7$$

$$\begin{aligned} \text{as } \bar{Z} |0\rangle_L &= |0\rangle_L & \bar{Z} |1\rangle_L &= -|1\rangle_L \\ \bar{X} |0\rangle_L &= |1\rangle_L & \bar{X} |1\rangle_L &= |0\rangle_L \end{aligned}$$

Since

$$(242) \quad HZ = HZH^\dagger H = XH \quad H = H^\dagger$$

and

$$(243) \quad HX = HXH^\dagger H = ZH$$

it is immediately obvious that

$$(244) \quad \bar{H} = H_1 H_2 H_3 H_4 H_5 H_6 H_7$$

This is fault tolerant because a failure in any component Hadamard will not propagate to other components. Property (244) is called transversality.

In a similar way we find that the logical Phase gate $\bar{S}$ can be written as

$$(245) \quad \begin{aligned} \bar{S} &= \bar{Z} \cdot S_1 S_2 S_3 S_4 S_5 S_6 S_7 \\ &= \underline{Z_1 S_1} \underline{Z_2 S_2} \underline{Z_3 S_3} \dots \underline{Z_7 S_7} \end{aligned}$$

and is also transversal and thus fault tolerant.

Remember

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

so

$$(246) \quad \bar{S} |0\rangle_L = \bar{Z} |0\rangle_L = |0\rangle_L$$

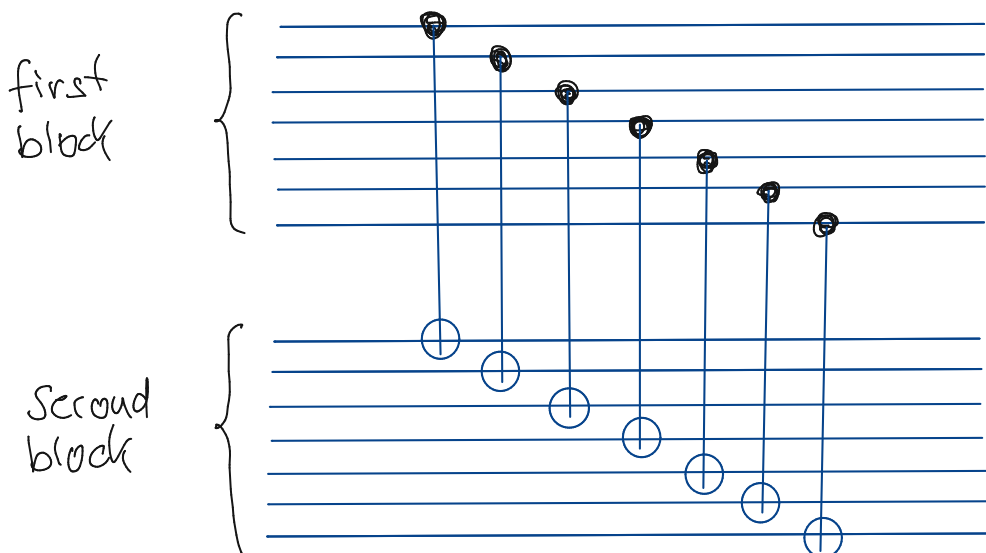
since always $(i)^4 = 1$. Furthermore

$$(247) \quad \bar{S} |1\rangle_L = \bar{Z} (-i) |1\rangle_L = i |1\rangle_L$$

since either $i^3 = -i$ or $i^7 = -i$.

Also the logical CNOT gate is transversal

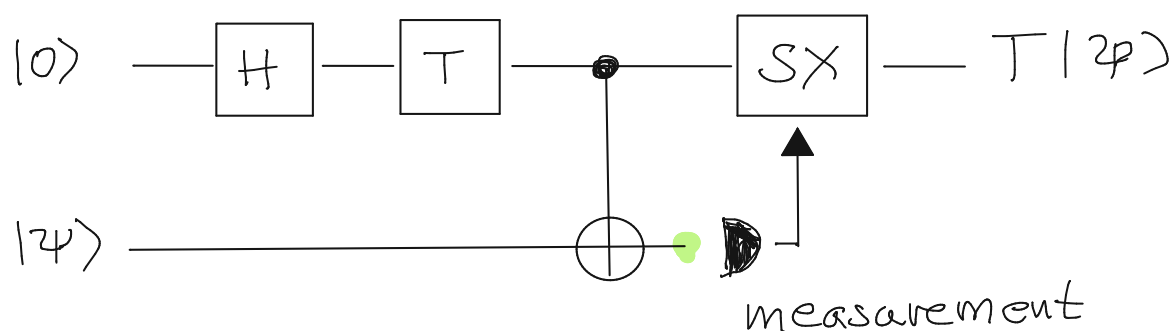
$$(248) \quad \overline{\text{CNOT}} = \text{CNOT}_{11} \text{CNOT}_{22} \cdots \text{CNOT}_{77}$$



The fault-tolerant implementation of the $\pi/8$ gate is a bit more involved but possible as we will see now.

(D) Fault-tolerant implementation of $\pi/8$ gate

In order to implement a T gate ($\pi/8$ gate) in a fault-tolerant way we first convince ourselves that the T gate on an arbitrary state can be performed by a T gate on an ancilla state combined with a measurement



operation of H and T

$$(249) \quad |0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow |\theta\rangle = \frac{|0\rangle + e^{i\pi/4}|1\rangle}{\sqrt{2}}$$

CNOT with $|\psi\rangle = a|0\rangle + b|1\rangle$

$$|\theta\rangle|\psi\rangle \xrightarrow{\text{CNOT}} \frac{1}{\sqrt{2}} \left[|0\rangle (a|0\rangle + b|1\rangle) + e^{i\pi/4} |1\rangle (a|1\rangle + b|0\rangle) \right]$$

$$(250) \quad = \frac{1}{\sqrt{2}} \left[(a|0\rangle + b e^{i\pi/4} |1\rangle) \underline{|0\rangle} + (b|0\rangle + a e^{i\pi/4} |1\rangle) \underline{|1\rangle} \right]$$

Measurement of second qubit projects the first to

$$(251) \quad \begin{aligned} "0" &\longrightarrow a|0\rangle + b e^{i\frac{\pi}{4}} |1\rangle \\ "1" &\longrightarrow b|0\rangle + a e^{i\frac{\pi}{4}} |1\rangle \end{aligned}$$

In the case of a measurement outcome of "1" we have to apply

$$(252) \quad \begin{aligned} SX [b|0\rangle + a e^{i\frac{\pi}{4}} |1\rangle] &= i b |1\rangle + a e^{i\frac{\pi}{4}} |0\rangle \\ &= e^{i\frac{\pi}{4}} [a|0\rangle + e^{i\frac{\pi}{4}} |1\rangle] \\ &= e^{i\frac{\pi}{4}} T|\psi\rangle \quad \square \end{aligned}$$

In order to translate this into a fault tolerant operation on encoded logical qubits we have to discuss how the measurement and how the preparation of the state $|\theta\rangle$ can be performed in a fault tolerant way. The preparation can be done using again measurements whose fault tolerant implementation will be discussed in the next subsection.

$|\theta\rangle$ is an eigenstate of

$$(253) \quad \hat{\Theta} = e^{-i\pi/4} SX$$

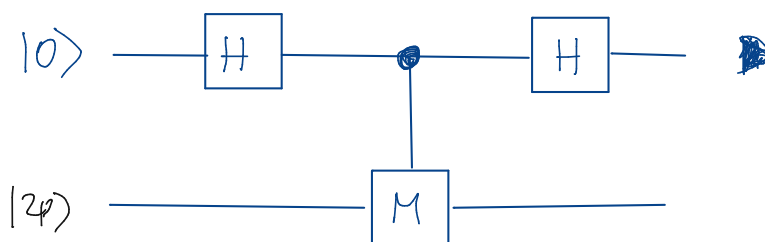
with eigenvalue $+1$. Note that $\hat{\Theta}^+ = \hat{\Theta}$.

So measuring $\hat{\Theta}$ fault-tolerantly with result $+1$ prepares the state $|0\rangle$. If we obtain the result -1 we just have to apply a Z flip

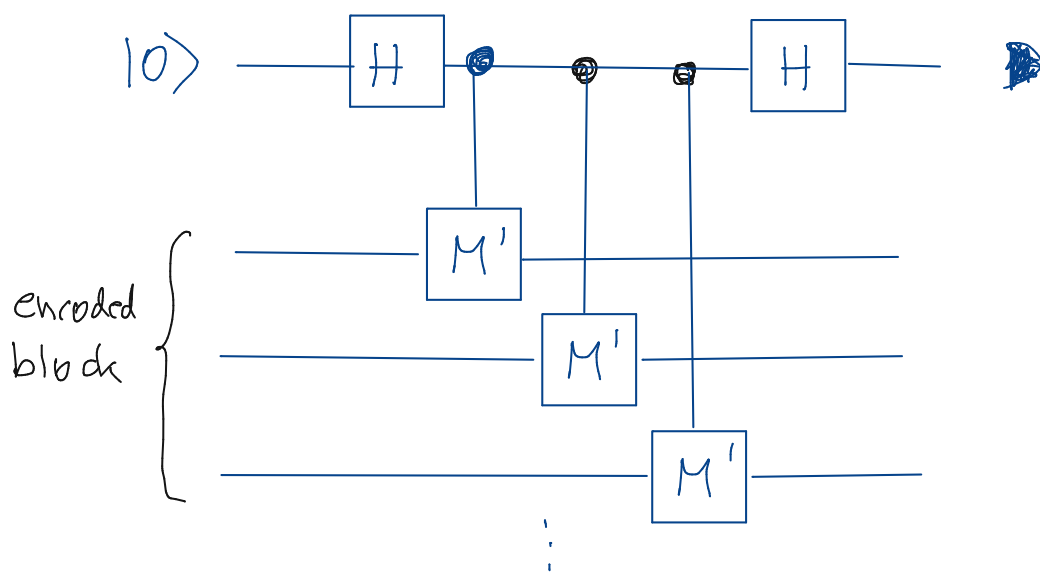
$$(254) \quad Z S X Z^\dagger = -S X$$

(E) Fault tolerant measurements

We have already seen that the measurement of a single qubit operator $\hat{M}$ with eigenvalues ± 1 can be performed via the gate



This can easily be generalized to a transversal operator $\hat{M} = M'_1 M'_2 M'_3 \cdots M'_n$ on n qubits



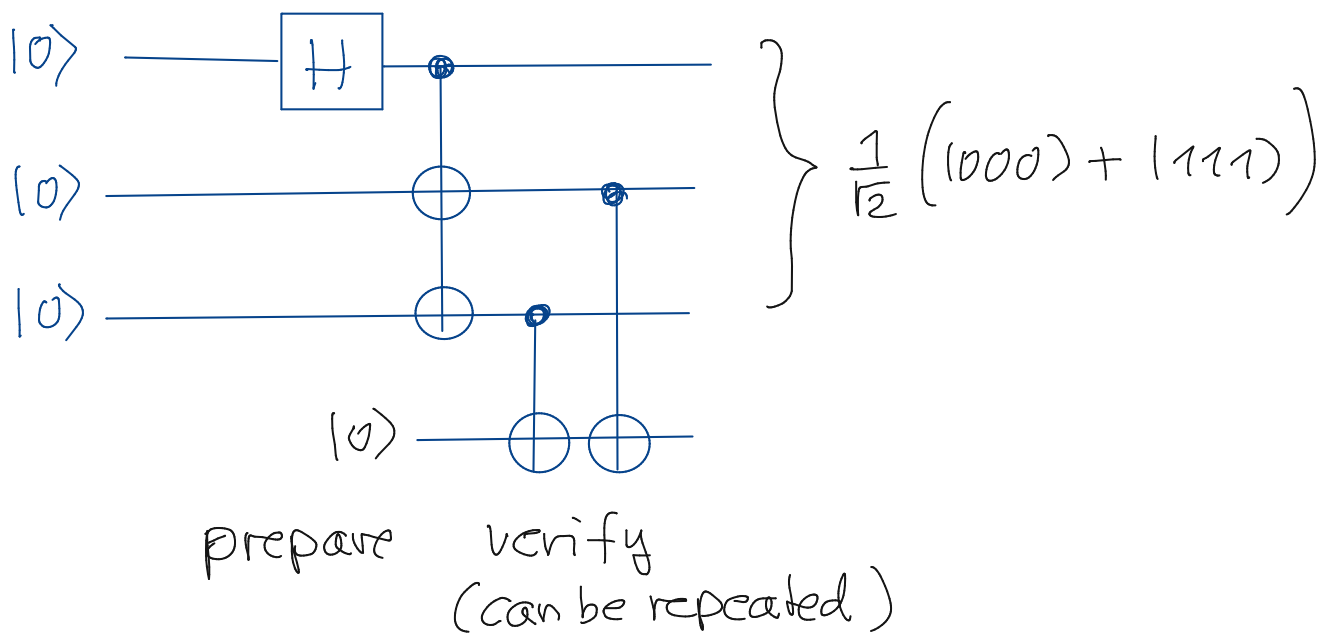
This is not yet fault tolerant since the first line operates on a single qubit. Note that the ancilla after the first Hadamard is

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

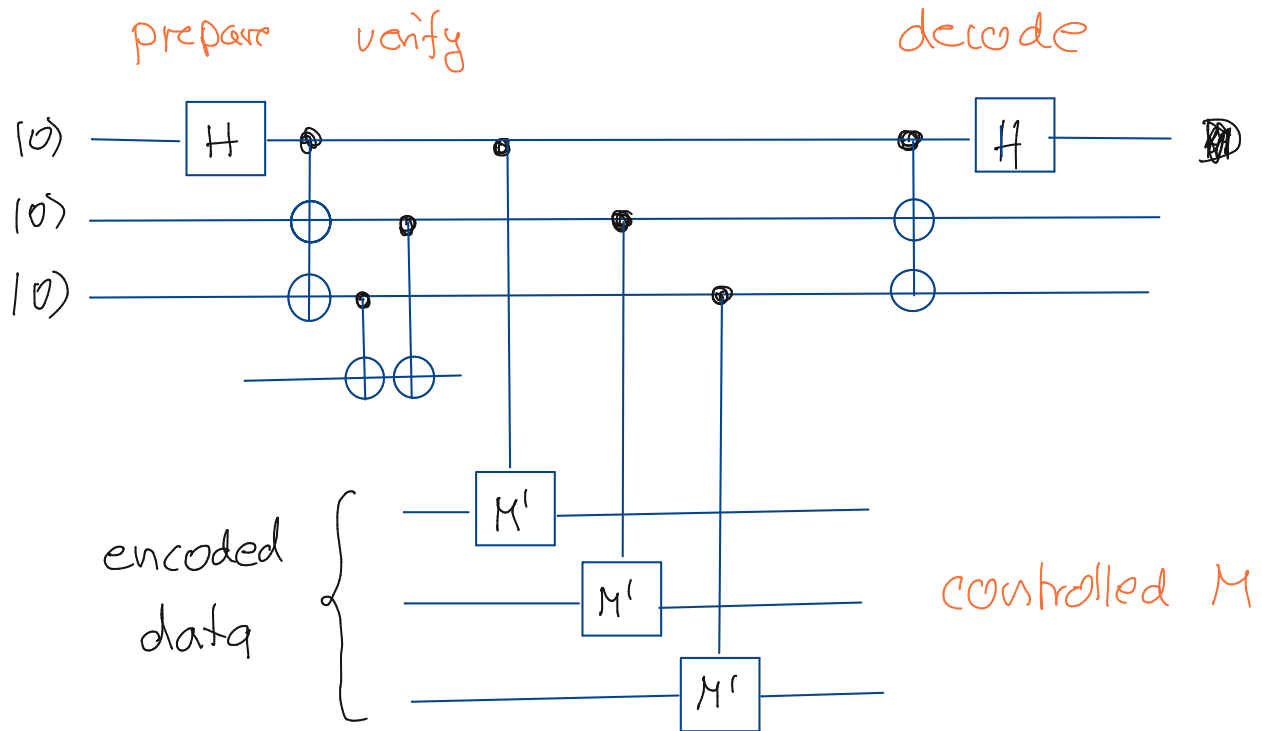
So we prepare the "encoded" state (cat state)

$$(255) \quad \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle)$$

We note that the cat state is not in a code state and a circuit preparing this state is by itself not fault tolerant. Its preparation can however be amended with (several) verification steps



With this we can make the whole measurement circuit fault tolerant



V. Quantum communication

5.1 Classical information transfer, Shannon's theorems

We have already discussed that information is a measure of the a-priori ignorance about an event. A quantitative measure of information about a complete set of events A_i , $i=1,2,\dots,n$ which occur with