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

$$(177)\quad \begin{matrix}|0\rangle|E\rangle \\ |1\rangle|E\rangle\end{matrix} \xrightarrow{\quad U(t)\quad} \begin{matrix}|1\rangle|E_{01}\rangle \\ |0\rangle|E_{10}\rangle\end{matrix}$$

spin flip

or

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

dephasing

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

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

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

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

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

(187)

$$\rho_0 = \begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix}$$

spin flip

$$\begin{pmatrix} |\beta|^2 & \alpha^*\beta \underbrace{\langle E_{01}(t)|E_{10}(t)\rangle}_{\hookrightarrow 0} \\ \alpha\beta^* \underbrace{\langle E_{10}(t)|E_{01}(t)\rangle}_{\hookrightarrow 0} & |\alpha|^2 \end{pmatrix}$$

dephasing

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

In both cases the off-diagonal terms decay

"decoherence"

In general

(182)

$$(\alpha|0\rangle + \beta|1\rangle)|E\rangle \longrightarrow$$

$$(\alpha|0\rangle + \beta|1\rangle)|E_0\rangle$$
$$+ (\alpha|1\rangle + \beta|0\rangle)|E_x\rangle$$
$$+ (\alpha|0\rangle - \beta|1\rangle)|E_2\rangle$$
$$+ (-\alpha|1\rangle + \beta|0\rangle)|E_r\rangle$$

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

where

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

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

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

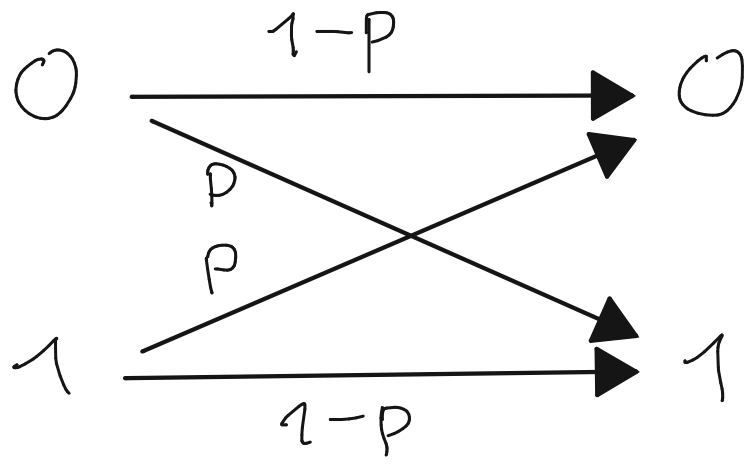
basic idea: encode bit into larger code

(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): $3p(1-p)$

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

correctable ✓

majority vote

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

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

(A) Linear binary codes

binary code — k bits encoded in $n \geq k$ 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 — $\{\underline{v}_1, \underline{v}_2, \ldots \underline{v}_k\}$

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

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

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

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

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

$$\underline{\underline{G}} = \begin{bmatrix} \cdots \underline{v}_1 \cdots \\ \cdots \underline{v}_2 \cdots \\ \\ \cdots \underline{v}_k \cdots \end{bmatrix} \begin{matrix} \} k \\ \\ \\ \\ \end{matrix} \qquad \underbrace{\qquad\qquad}_{n} \tag{186}$$

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

$$\underline{\underline{G}} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \tag{187}$$

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

$$\underline{v} = \underline{\alpha}\,\underline{\underline{G}} \qquad \underline{\alpha} = (\alpha_1, \alpha_2 \ldots \alpha_k) \tag{188}$$

alternative characteristics: parity-check matrix

(189) $$\underline{\underline{H}}\,\underline{v}^T = 0$$ n-k conditions on all codewords

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

proof: $(0,1,1)\cdot(1,1,1) = 0\oplus 1\oplus 1 = 0 \mod 2$
$(1,0,1)\cdot(1,1,1) = 1\oplus 0\oplus 1 = 0 \mod 2$

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) $$\underline{v} \longrightarrow \underline{v}\oplus\underline{e}$$

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

$$\underline{H}(\underline{v} \oplus \underline{e}) = \underline{H}\,\underline{v} \oplus \underline{H}\underline{e} = \underline{H}\underline{e} \tag{192}$$

error syndrome

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

error correction

$$\underbrace{(\underline{v} \oplus \underline{e}_j)}_{\substack{\text{codeword} \\ \text{with error}}} \oplus \underline{e}_j = \underline{v} \tag{193}$$

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

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

⇒ 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

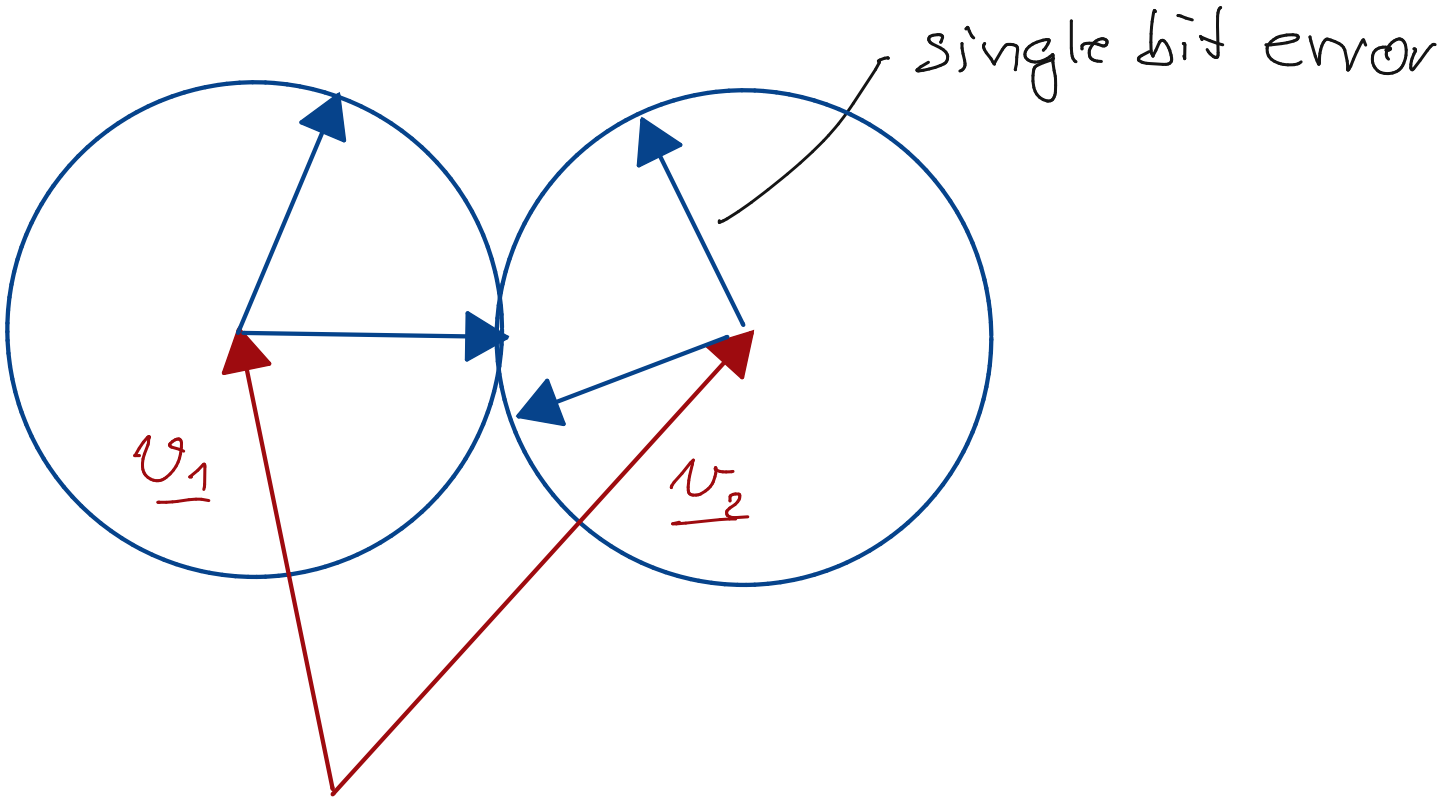
The code used in the above example has $d=2$ and thus is useless for error correction

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

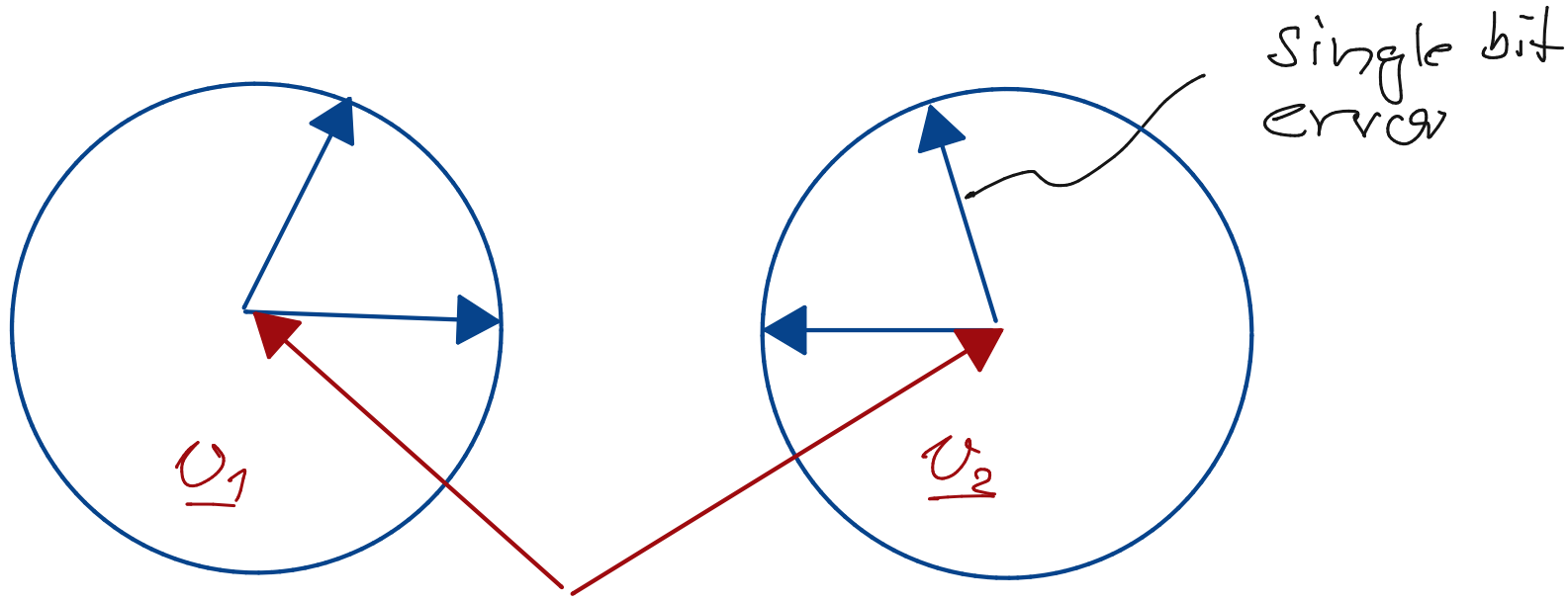
$$\underline{e}_1 = (1,0,0) \qquad \underline{e}_2 = (0,1,0)$$

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

$d=2$



$d=3$



notation $[n, k, d]$ code

- n: number of bit in code
- k: number of encodable bits
- d: Hamming distance

example: $[7,4,3]$ Hamming code

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

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

j

if $\underline{e}_j$ is bit flip error at jth bit : error syndrom

$$\underline{\underline{H}}\underline{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad \underline{\underline{H}}\underline{e}_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \underline{\underline{H}}\underline{e}_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \quad \underline{\underline{H}}\underline{e}_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$\underline{\underline{H}}\underline{e}_5 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \quad \underline{\underline{H}}\underline{e}_6 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \quad \underline{\underline{H}}\underline{e}_7 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

Gilbert-Varshanov bound

For large n there exisb 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.

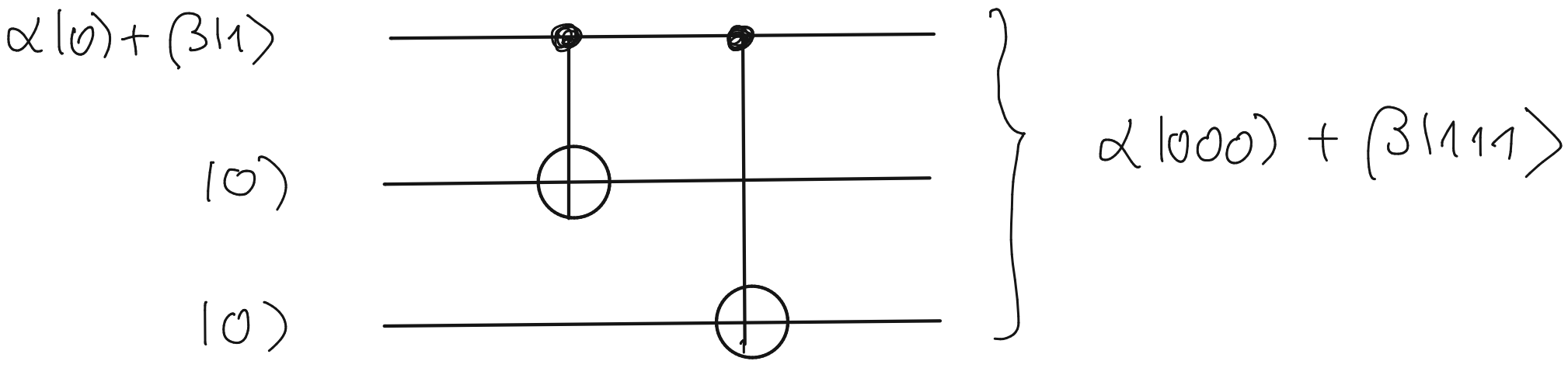
4.3 linear qubit codes

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

(A) The 3qubit spin flip code

(i) encode qubit

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



(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	$O(p^2)$	small

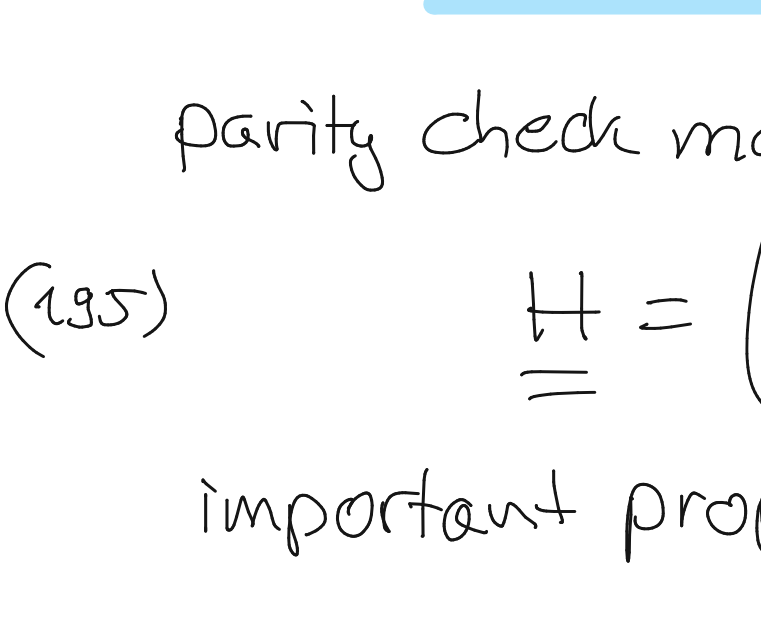
(iii) error detection $\quad k=1, n=3, d=3$

parity check matrix

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

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

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



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

measurement of error syndrom

$\hat{X}$ 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

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

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

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

(196)

$$\begin{array}{ll} & (\alpha|000\rangle + \beta|111\rangle) \quad |00\rangle \quad \leftarrow \text{no error} \\ \Rightarrow & (\alpha|100\rangle + \beta|011\rangle) \quad |11\rangle \\ & (\alpha|010\rangle + \beta|101\rangle) \quad |10\rangle \\ & (\alpha|001\rangle + \beta|110\rangle) \quad |01\rangle \end{array} \Big\} \text{error syndrom}$$

(iv) error correction

application of $\hat{X}_j$

(197)

$$\begin{aligned} \text{if } |10\rangle &\Rightarrow \hat{I}_1 \hat{X}_2 \hat{I}_3 \\ |01\rangle &\Rightarrow \hat{I}_1 \hat{I}_2 \hat{X}_3 \\ |11\rangle &\Rightarrow \hat{X}_1 \hat{I}_1 \hat{I}_3 \end{aligned}$$

remark:

The extraction of the error syndrom through the implementation of $\underline{\underline{H}}^T$ can also be interpreted in a different way. The measurement scheme actually projects on the four eigenstates of

(198)
$$Z_1 Z_2 \quad \text{and} \quad Z_2 Z_3$$
$$\lambda = \pm 1 \qquad \lambda = \pm 1$$

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

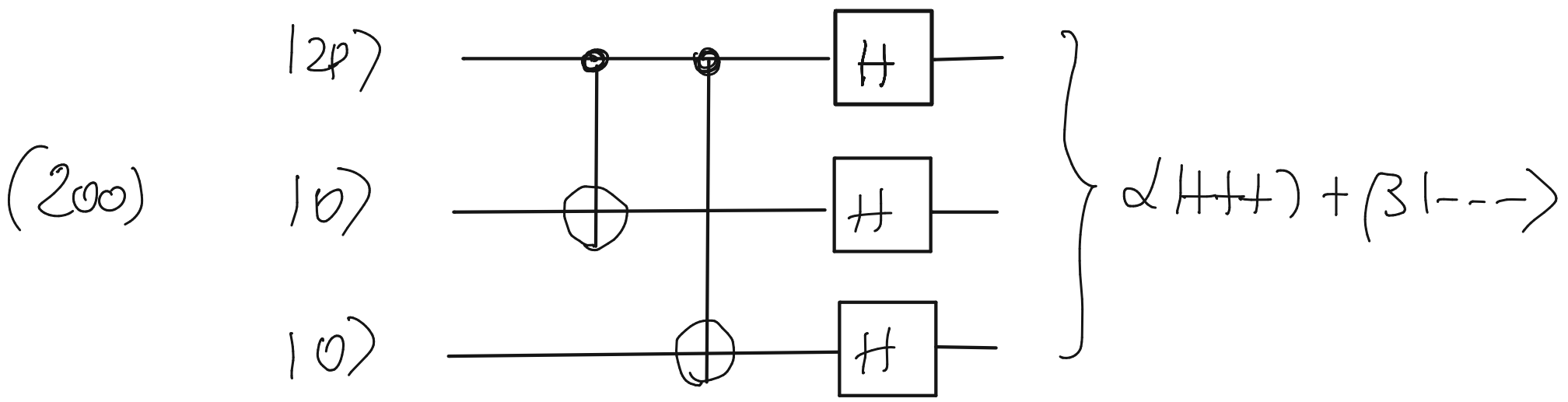
(B) The 3 qubit phase flip code

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

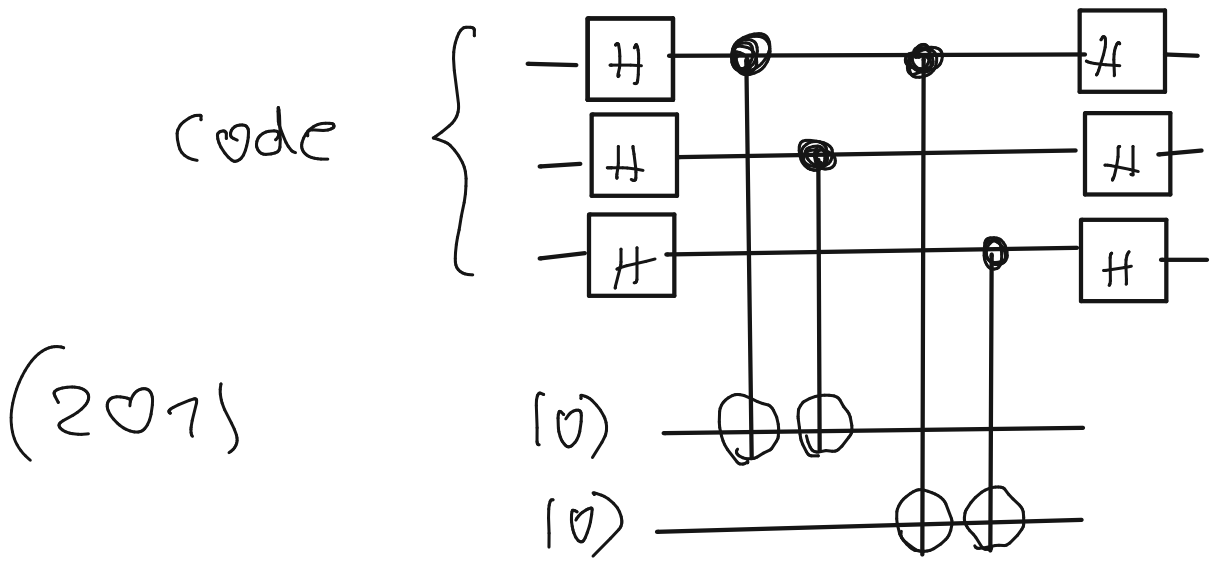
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$$

(199)
$$\alpha|+++\rangle + \beta|---\rangle$$

implementation of encoding



error detection



corresponds to measurements of

$$H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$$

$$H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$$

error correction

analogously to spin-flip code

(C) Shore 9 qubit code

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

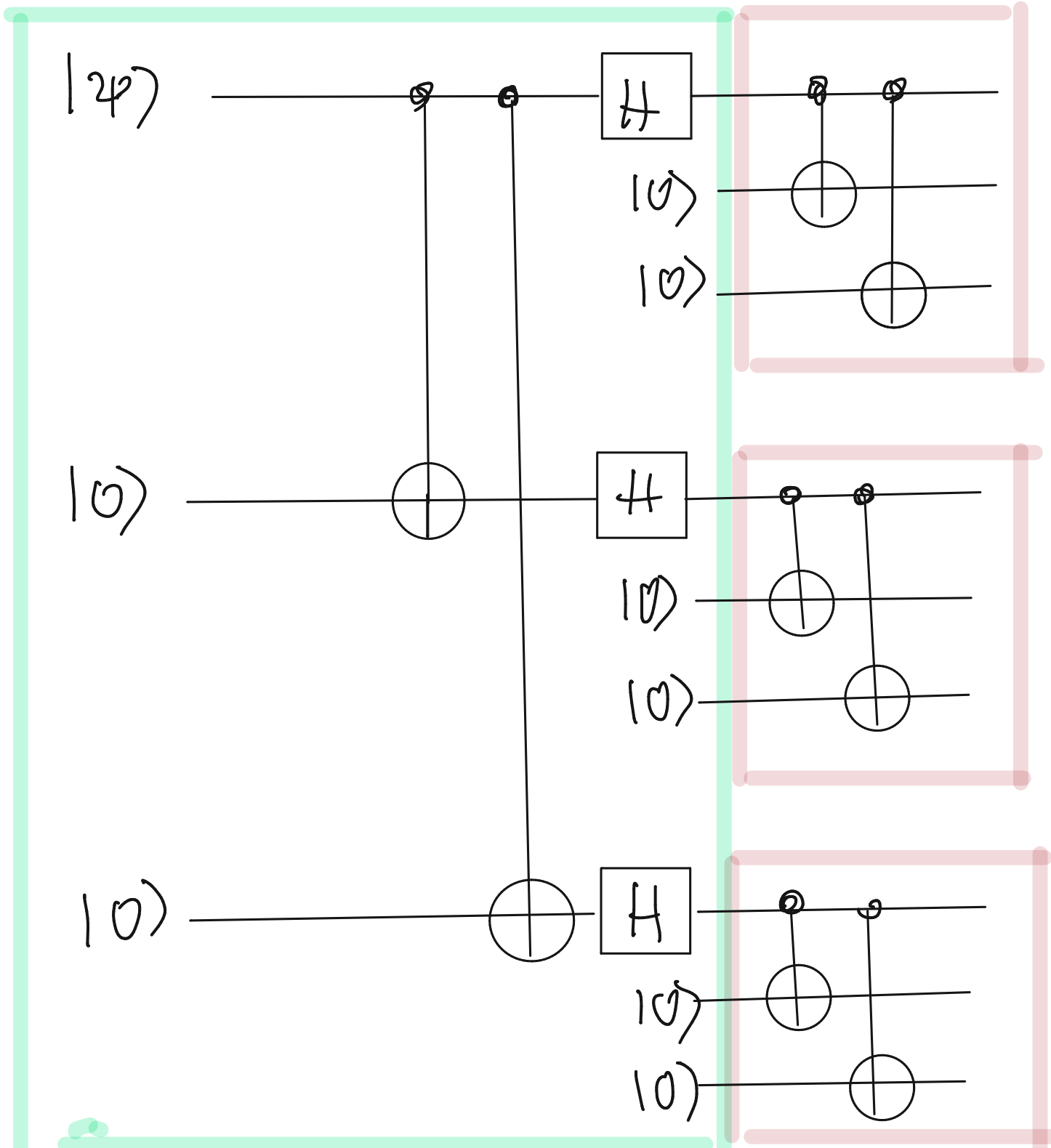
and phase-flip code using a scheme known as concatenation of simple codes

(202)

$$|0\rangle \rightarrow \frac{(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)}{2\sqrt{2}}$$

$$|1\rangle \rightarrow \frac{(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)}{2\sqrt{2}}$$

implementation:



for more details see e.g. Nielsen & Chuang