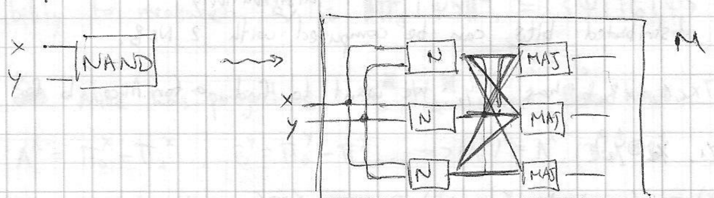
Fault tolerance - Von Neumann ['56]

How to compute reliably with faulty gates?

NAND multiplexing: Assume we have a NAND gate that's faulty with probability p.

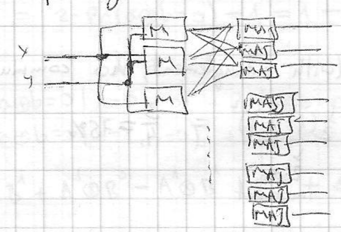


Each of the gates has fault w.p p. The entire new circuit failes w.p bounded by $15p^2$, which is better that p for $p<\frac{1}{15}$

Now assume we have a circuit with N NAND gates.

If we achieve $\frac{0.1}{N}$-error per gate, the final error is 0.1, which is good

We can amplify M by:



The probability 2 units fail is now bounded by $15\cdot(15p^2)^2 = 15^3\cdot p^4$

We can take this circuit and amplify it again and again. After k times we fail with probability bounded by $15^{2^k-1}\cdot p^{2^k}$.

In order to promise: $15^{2^k-1}\cdot p^{2^k} \le \frac{0.1}{N}$, we can take $k=O(\log\log N)$.

This only works for $p<\frac{1}{15}$.

The number of extra gates per NAND (the overhead) is poly log N.

So the total number of gates in the circuit is $N\cdot$poly log N.

Remark: This is called a "concatenated scheme".

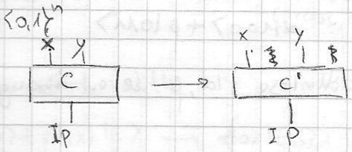
Fault tolerance threshold

This is the highest probability p_{th} with which we can still deal, and build a fault-tolerance scheme.

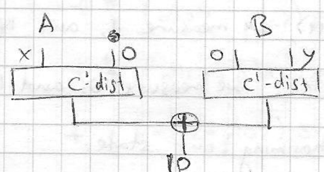
Theorem: For NAND-gate circuits $p_{th} \le \frac{1}{4}$

Proof: Assume (in contradiction) any NAND-circuit C can be simulated by a NAND circuit C', s.t C' is correct w.p 90% even if each NAND fails w.p. $1/4$.

NAND is universal, so we can construct a NAND circuit C to compute $IP(x,y)$, $x,y \in \{0,1\}^n$



Compute C' distributively between Alice & Bob, where A uses input $(x,0)$, B uses input $(0,y)$.



Here we need only one bit of communication, and entanglement (to compute NAND distributively). But the lower bound for communication for IP is $O(n)$. Contradiction

□

Remark: The thershold for NAND can be improved to 8.8%, but not with quantum means.

Quantum Error Correction

(1) In order to perform Shor's algorithm we need to do QFT with high precision, but it is very fragile.

(2) Experimentalists have small precisions. (~10% errors)

(3) Classically the error is between 0 and 1. Quantumly we have a continuum of possible errors.

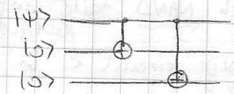
(4) We can't use cloning, so we can't use redundancy for correction.

(5) In order to correct a qubit, it seems we need to measure it first, which ruins the state for us.

Both Shor and Steane found in '95 (independently) schemes for Quantum error correction.

<u>Example</u>: Assume we only have bit flip-error $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and only 1 qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

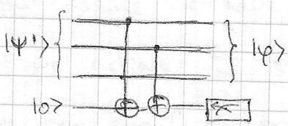
The encoding of $|\psi\rangle$ will be ~~$|\psi\rangle$~~ $\alpha|000\rangle + \beta|111\rangle$. (Note that this is not ~~$|\psi\rangle$~~ $|\psi\rangle|\psi\rangle|\psi\rangle$).



If we have an error on the first qubit: $\alpha|100\rangle + \beta|011\rangle$.

We can't measure in the standard basis → we will lose α, β (even though we will find the error).

The idea is to measure the parity (so not to collapse the state).

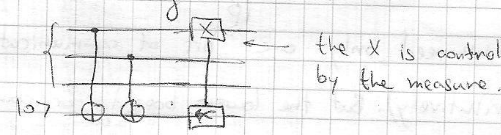
① 

If $|\psi'\rangle = \alpha|100\rangle + \beta|011\rangle$, we measure 1, and $|\varphi\rangle = |\psi'\rangle$

If $|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$, we measure 0, and $|\varphi\rangle = |\psi'\rangle$

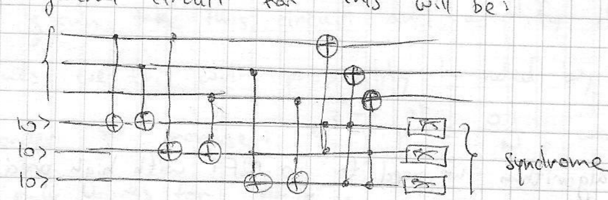
So we can discover that error without harming our state.

We can also fix the state with:



No we can also find ~~errors on~~ and fix ~~errors~~ similar errors on the 2nd and 3rd qubits.

The general circuit for this will be:



errors	syndrome
1st	110
2nd	101
3rd	011
none	000

<u>Example</u>: A more general error: $|0\rangle|E\rangle \rightarrow \sqrt{1-p}\,|0\rangle\cdot|E_0\rangle + \sqrt{p}\,|1\rangle|E_1\rangle \quad \langle E_0|E_1\rangle = 0$

"Environment" $\quad |1\rangle|E\rangle \rightarrow \sqrt{p}\,|0\rangle|E_1\rangle + \sqrt{1-p}\,|1\rangle|E_0\rangle$

Assume we start with $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, encode it with $|\varphi\rangle = \alpha|000\rangle + \beta|111\rangle$, and assume we have error in the 1st qubit:

$$|\varphi\rangle|E\rangle \xrightarrow{\text{error}} \sqrt{1-p}\,(\alpha|000\rangle + \beta|111\rangle)E_0 + \sqrt{p}\,(\alpha|100\rangle + \beta|011\rangle)E_1$$

Use the detection circuit ① ⇒

$$\xrightarrow{①} \sqrt{1-p}\,|\varphi\rangle\cdot|0\rangle_p|E_0\rangle + \sqrt{p}\,(\alpha|100\rangle + \beta|011\rangle)|1\rangle_p|E_1\rangle \xrightarrow{\text{measure}} \begin{cases} (1-p): & |\varphi\rangle|E_0\rangle \\ (p): & (\alpha|100\rangle + \beta|011\rangle)|E_1\rangle \end{cases}$$

Now, as earlier, we can correct, if needed, and continue with the circuit.

Notice that measurement gave us a discrete error.

An error on one qubit is a unitary process:

the most general error
$$\begin{cases} |0\rangle|E\rangle \xrightarrow{U} |0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle \\ |1\rangle|E\rangle \xrightarrow{U} |0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle \end{cases}$$
$|E_{ij}\rangle$ any state, $\| |E_{ij}\rangle \| \leq 1$

Example: A measurement error can be written as: $|E_{01}\rangle = 0$, $|E_{10}\rangle = 0$, $|E_{00}\rangle = |0\rangle$, $|E_{11}\rangle = |1\rangle$

Notice that we can't control (access, change) the environment register

Say we start with $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. After the error:

$$(\alpha|0\rangle + \beta|1\rangle)|E\rangle \longrightarrow \alpha(|0\rangle|E_{00}\rangle + |1\rangle|E_{01}\rangle) + \beta(|0\rangle|E_{10}\rangle + |1\rangle|E_{11}\rangle) =$$

$$= (\alpha|0\rangle + \beta|1\rangle) \otimes \tfrac{1}{2}(|E_{00}\rangle + |E_{11}\rangle) + \quad \rightarrow \text{identity } \mathbb{1}$$

$$+ (\alpha|0\rangle - \beta|1\rangle) \otimes \tfrac{1}{2}(|E_{00}\rangle - |E_{11}\rangle) + \quad \rightarrow \text{phase-flip } Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$+ (\alpha|1\rangle + \beta|0\rangle) \otimes \tfrac{1}{2}(|E_{01}\rangle + |E_{10}\rangle) + \quad \rightarrow \text{bit-flip } X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$+ (\alpha|1\rangle - \beta|0\rangle) \otimes \tfrac{1}{2}(|E_{01}\rangle - |E_{10}\rangle). \quad \rightarrow \text{both } XZ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

So, as in the bit-flip error, we will add a few ancillary bits, and when we measure them, we will collapse into one of 4 states. Then fix the state.

Shor's 9 qubit gates - Notation: $[[9, 1, 3]]$ - code (9 = # qubits, 1 = # encoded qubits, $3 = 2t+1$, t = # errors it can correct)

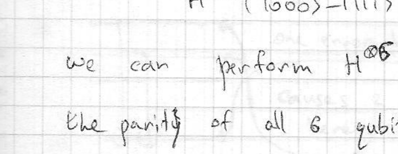
$$|0\rangle \rightarrow \frac{1}{\sqrt{2}^3}(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{2}^3}(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)$$

- Bit flip error can be detected and fixed with 9 extra parity bits.
- Phase flip error is dealt as follows.

Since:
$$H^{\otimes 3}(|000\rangle + |111\rangle) = \tfrac{1}{2}(|000\rangle + |110\rangle + |101\rangle + |011\rangle)$$
$$H^{\otimes 3}(|000\rangle - |111\rangle) = \tfrac{1}{2}(|111\rangle + |001\rangle + |010\rangle + |100\rangle)$$

we can perform $H^{\otimes 6}$ on the first 6 qubits. If there was no error, the parity of all 6 qubits will be 0. If there was an error, the parity of all 6 qubits will be 1. The circuit for detection can be simplified to:



The correction is also similar to bit flip.

~~The notati~~

Observe: (1) codes = (small) sub-spaces $\mathcal{C} \subseteq \mathbb{C}^2$

(2) We have a descrete set $\{E_\alpha\}_\alpha$ of errors.

(3) Each E_α maps $\mathcal{C}$ to a space orthogonal to $\mathcal{C}$.

Notice that errors Z_1, Z_2 on Shor's code $\mathcal{C}$ give the same subspace (where Z_i is the error of phase flip on the i^{th} bit of the code).

QECC conditions (Knill-Laflamme '97)

conditions for a code $\mathcal{C} = \{|\psi_i\rangle \mid 1 \le i \le k\}$ to be against a set of errors $\{E_\alpha\}$:

(iff) $\langle \psi_j | E_\beta^\dagger E_\alpha | \psi_i \rangle = \begin{cases} 0 & \text{if } i \neq j \\ c_{\alpha\beta} & \text{if } i = j \end{cases}$ [Doesn't depend on i!]

Classical ECC

ECC: $\{0,1\}^n \to \{0,1\}^m$.

$d(x,y) =$ # bits where x & y are different (Hamming distance).

We can correct if there are at most $t = \frac{d-1}{2}$ errors.

$\mathcal{C}$ is a linear code if $v \in \mathcal{C} \iff H v = \vec{0}$
($\mathcal{C} \subseteq \{0,1\}^m$; H matrix)

H is called parity check matrix.

Say there was an error of bit flip on the i^{th} bit.

So the new vector is $E(x) \oplus e_i$. $\Rightarrow H(E(x) \oplus e_i) = H E(x) + H e_i = H e_i$

Hence we can find what's the error by multiplying by H, and then correct!

$d_{\mathcal{C}} = \min_{\substack{v \in \mathcal{C} \\ v \neq 0}} wt(v) \longrightarrow$ Hamming weight.

Example: Hamming code, $d_{\mathcal{C}} = 3$, $[7,4,3]$, $|\mathcal{C}_{HAM}| = 2^4$

$$H_{HAM} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Steane-code [[7,1,3]]

$$|0\rangle \longrightarrow |0\rangle_{code} = \frac{1}{\sqrt{8}} \sum_{\substack{v \in \mathcal{C}_{HAM} \\ wt(v) \equiv 0 \pmod 2}} |v\rangle = \frac{1}{\sqrt{8}} \cdot \big(|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle + |1010101\rangle + |1011010\rangle + |1101001\rangle + |1100110\rangle \big)$$

$$|1\rangle \longrightarrow |1\rangle_{code} = \frac{1}{\sqrt{8}} \cdot \sum_{\substack{v \in \mathcal{C}_{HAM} \\ wt(v) \equiv 1 \pmod 2}} |v\rangle = \frac{1}{\sqrt{8}} \big(|1111111\rangle + |1110000\rangle + |1000011\rangle + |1001100\rangle + |0101010\rangle + |0100101\rangle + |0010110\rangle + |0011001\rangle \big)$$

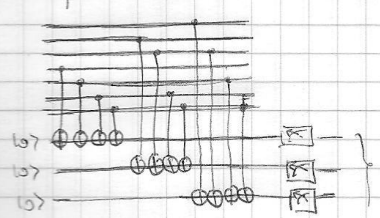
Bit flip error is corrected as in the classical case – "apply" H_{HAM} (using CNOTs) to the register. If we get result $\begin{pmatrix}0\\0\\0\end{pmatrix}$ – there was no error. If we get $\begin{pmatrix}0\\0\\1\end{pmatrix}$ – the error is in 1st qubit, $\begin{pmatrix}0\\1\\0\end{pmatrix}$ – 2nd qubit, etc.

Phase flip error is corrected in the same way, but applying $H^{\otimes 7}$ before and after the circuit, because

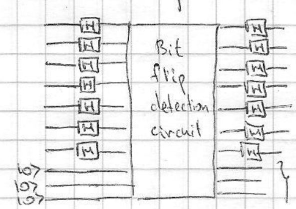
$$H^{\otimes 7} |0\rangle_{code} = \frac{1}{\sqrt{2}} \left(|0\rangle_{code} + |1\rangle_{code} \right)$$

$$H^{\otimes 7} |1\rangle_{code} = \frac{1}{\sqrt{2}} \left(|0\rangle_{code} - |1\rangle_{code} \right)$$

Bit flip detection circuit.



Phase flip detection circuit

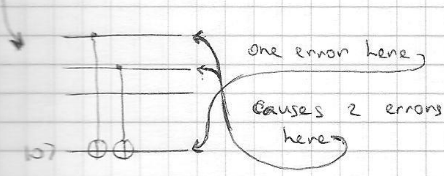


Fault-tolerant designs

(1) Encoding / decoding / state preparation does not introduce more errors than code can correct.

(2) Correction doesn't propagate errors

(3) Gates / measurement done without decoding.



(Error detection for our first example code)

$\longrightarrow$