Introduction to error correction

Desired gate: U

Actual unitary (involving the environment): $\tilde{U}$

Quantum circuits are very sensitive to errors...

Error bound without correction

Let each gate in a quantum circuit be realized with accuracy δ :

$$\| \tilde{U} - U \otimes I_{env} \| \leq \delta$$

Then $\| \tilde{U}_L \cdots \tilde{U}_1 - U_L \cdots U_1 \otimes I_{env} \| \leq L\,\delta$

Classical analogue

If each gate involves a spontaneous bit flip with probability ε, then the overall error probability is $\leq L\varepsilon$

State-of-the-art qubits

$$\delta \sim \underbrace{10}_{\text{single-qubit gates or storage}}^{-3} \div \underbrace{10}_{\text{two-qubit gates}}^{-2}$$

Classical capacitor-based memory cells

$\varepsilon < 10^{-20}$ due to physical protection
(the capacitor charge is made up by ~ 100 electrons)

Goal: Find a way to do arbitrary long computation with arbitrary small overall error probability using imperfect physical elements.

↙ ↘

Task 1: Reliable quantum memory

Task 2: Fault-tolerant computation

Error models (classical)

Probabilistic model: Each bit flips with probability p

Combinatorial model: "Likely" errors: $\le r$ flips; "Unlikely" errors: $> r$ flips (out of n bits) $\left(r < \frac{n}{2}\right)$

$$\text{Prob}\,[\underbrace{\text{unlikely error}}_{\text{a set of } s>r \text{ bits has flipped}}] = \sum_{s>r} \binom{n}{s} p^s (1-p)^{n-s} \le \underbrace{\binom{n}{r+1}}_{\frac{n(n-1)\cdots(n-r)}{(r+1)!}} p^{r+1} \le \frac{(np)^{r+1}}{(r+1)!}$$

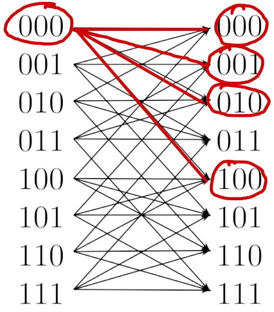
For small p, Prob [unlikely error] $= O\left((np)^{r+1}\right)$

Strategy

Protect data from likely errors.

Make sure that the probability of an "unlikely" error is really small (i.e. much less than L^{-1})

Set of likely errors $E(n,r)$



$$E(\underset{\#\text{ of bits}}{3},\underset{\#\text{ of flips allowed}}{1}) \subseteq \{0,1\}^3 \times \{0,1\}^3$$

Protecting data from likely errors using redundancy

Repetition code:

$$\begin{array}{ccc} 0 & \mapsto & 000 \\ \underbrace{1}_{\text{logical}} & \mapsto & \underbrace{111}_{\text{physical}} \end{array}$$

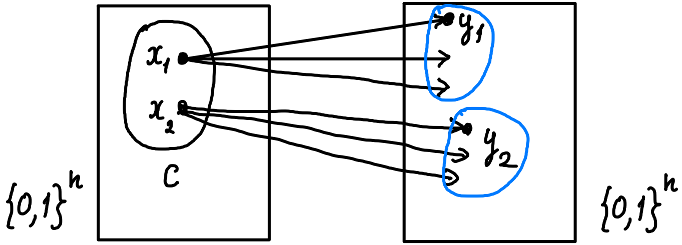
3 physical bits, 1 logical bit

$n = 3, \quad k = 1$

Definition 1. A *classical code of type* $[n, k]$ is a subset $C \subseteq \{0,1\}^n$ of cardinality 2^k. A corresponding *encoding* is a 1-to-1 map $v : \{0,1\}^k \to \{0,1\}^n$ with image C.

Definition 2. A code $C \subseteq \{0,1\}^n$ *protects from a set of errors* $E \subseteq \{0,1\}^n \times \{0,1\}^n$ if

$$\forall\, x_1, x_2 \in C \quad \forall y_1, y_2 \text{ such that } (x_1, y_1), (x_2, y_2) \in E, \quad x_1 \neq x_2 \Rightarrow y_1 \neq y_2.$$



Example: C is the repetition code,

$$E = E(\underset{\text{3 bits}}{3}, \underset{\text{1 flip allowed}}{1})$$

$x_1 = 000 \longrightarrow y_1 \in \{000, 001, 010, 100\}$

$x_2 = 111 \longrightarrow y_2 \in \{111, 110, 101, 011\}$

A quantum error model (similar to the combinatorial model)

Space of likely errors: $\mathcal{E}(n,r) \subseteq \mathbb{L}(\mathcal{B}^{\otimes n})$

max. allowed # of single-qubit errors

$\mathcal{B} = \mathbb{C}^2$ -- a qubit

$\mathbb{L}(\mathcal{B}^{\otimes n})$ -- space of operators acting on *n* qubits

A basis of $\mathbb{L}(\mathcal{B}^{\otimes n})$ consists of Pauli operators, e.g.

$$I = I\,I\,I$$

$$\sigma_1^x = X\,I\,I$$

$$\sigma_1^y \sigma_3^z = Y\,I\,Z$$

Error types: X -- bit flip

Z -- phase error

Y -- both

$$(\sigma^y = i\,\sigma^x \sigma^z)$$

$\sigma^x|0\rangle = |1\rangle$, $\sigma^x|1\rangle = |0\rangle$

$\sigma^z|0\rangle = |0\rangle$ $\sigma^z|1\rangle = -|1\rangle$

$\mathcal{E}(n,r) =$ linear span of Pauli operators acting on $\leq r$ qubits

For example, $\mathcal{E}(3,1) = \text{lin. span}\left(I, \sigma_j^x, \sigma_j^y, \sigma_j^z\right)$

General error $E \in \mathcal{E}(3,1)$: $E = a_0 I + a_x \sigma_1^x + a_y \sigma_1^y + a_z \sigma^z$ (*E* is not necessarily unitary.)

Physical error models and their connection to this model will be discussed later

Definition of a quantum code

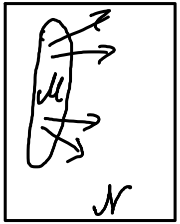
Let $\mathcal{N} = \mathcal{B}^{\otimes n}$ – physical Hilbert space
$\mathcal{L} = \mathcal{B}^{\otimes k}$ – logical Hilbert space
$\mathcal{E} = \mathcal{E}(n, k)$ – space of likely errors

(But we may consider arbitrary $\mathcal{N}, \mathcal{L}, \mathcal{E} \subseteq \mathbb{L}(\mathcal{N})$)

Definition 3. A *quantum code* is a subspace $\mathcal{M} \subseteq \mathcal{N}$. A corresponding *encoding* is an isometric embedding $V : \mathcal{L} \to \mathcal{N}$ with image $\mathcal{M}$.

$\forall |\xi\rangle \in \mathcal{M} \quad \| V|\xi\rangle \| = \| |\xi\rangle \|$

$\boxed{V^{\dagger} V = I_{\mathcal{L}}}$



Definition 4. A code $\mathcal{M} \subseteq \mathcal{N}$ *protects from errors in* $\mathcal{E} \subseteq \mathrm{L}(\mathcal{N})$ if

$$\forall |\xi_1\rangle, |\xi_2\rangle \in \mathcal{M} \quad \forall E_1, E_2 \in \mathcal{E}, \quad |\xi_1\rangle \perp |\xi_2\rangle \Rightarrow E_1|\xi_1\rangle \perp E_2|\xi_2\rangle.$$

Example: quantum repetition code

$\mathcal{L} = \mathcal{B} = \mathbb{C}^2, \quad \mathcal{N} = \mathcal{B}^{\otimes 3}, \quad \mathcal{M} = \text{lin. span}(|000\rangle, |111\rangle)$

$$V_{rep} : \begin{array}{l} |0\rangle \mapsto |000\rangle \\ |1\rangle \mapsto |111\rangle \end{array}$$

$$V_{rep}(c_0|0\rangle + c_1|1\rangle) = c_0|000\rangle + c_1|111\rangle$$

Protects from a single bit flip:

$$\mathcal{E} = \text{lin. span}\left(\underset{III}{I}, \underset{XII}{\sigma_1^x}, \underset{IXI}{\sigma_2^x}, \underset{IIX}{\sigma_3^x}\right)$$

Does not protect from phase errors

The quantum repetition code does not protect from phase errors

Let $E_1 = I$, $E_2 = \sigma_1^z$

If we take $|\xi_1\rangle = |000\rangle$, $|\xi_2\rangle = |111\rangle$, then $E_1|\xi_1\rangle = |\xi_1\rangle$, $E_2|\xi_2\rangle = -|\xi_2\rangle$

So far so good, but consider

$$|\eta_1\rangle = |000\rangle + |111\rangle \qquad E_1|\eta_1\rangle = |\eta_1\rangle$$

$$|\eta_2\rangle = |000\rangle - |111\rangle \qquad E_2|\eta_2\rangle = |\eta_1\rangle$$

$|\eta_1\rangle \perp |\eta_2\rangle$ but $\underline{E_1|\eta_1\rangle \not\perp E_2|\eta_2\rangle}$

Dual repetition code (protects from phase errors but not bit flips)

$$V_{drep} : \begin{cases} |+\rangle \mapsto |+\rangle \otimes |+\rangle \otimes |+\rangle = 2^{-\frac{3}{2}} \sum\limits_{x_1, x_2, x_3} |x_1, x_2, x_3\rangle \\ |-\rangle \mapsto |-\rangle \otimes |-\rangle \otimes |-\rangle = 2^{-\frac{3}{2}} \sum\limits_{x_1, x_2, x_3} (-1)^{x_1 + x_2 + x_3} |x_1, x_2, x_3\rangle \end{cases}$$

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \mapsto \sum_{even}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \mapsto \sum_{odd}$$

$$V_{drep}|x\rangle = \frac{1}{2} \sum_{x_1 \oplus x_2 \oplus x_3 = x} |x_1, x_2, x_3\rangle$$

Characterizing the code vectors and errors (for the repetition code) in terms of stabilizer operators

The code is defined by these *stabilizer operators:* $S_1 = ZZI, \quad S_2 = IZZ$

Defining property: $\boxed{\forall |\xi\rangle \in \mathcal{M} \qquad S_j|\xi\rangle = |\xi\rangle}$ e.g. $S_1|111\rangle = |111\rangle$

Consider an error $E \in \mathcal{E}, \quad E = \sigma^x(f)$ for $f = (f_1, f_2, f_3)$ $\left(\text{e.g. } \sigma^x(100) = XII\right)$

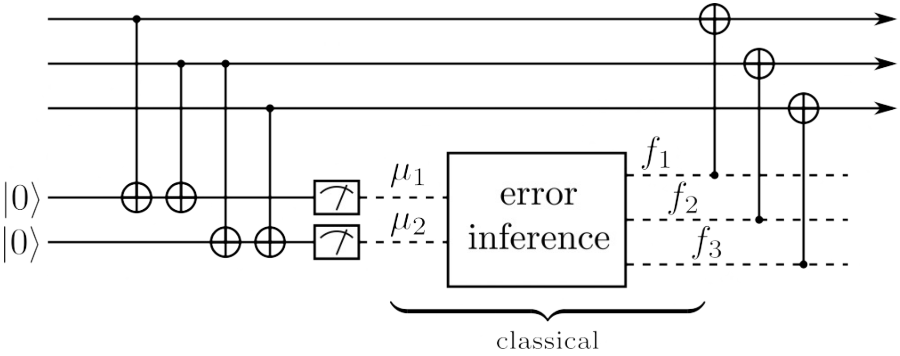
Then $\boxed{S_j E = (-1)^{\mu_j} E S_j}$ $\quad \mu_j = \mu_j(f)$ $\quad \underline{(\mu_1, \mu_2)}$ -- *error syndrome*

The effect of E on $|\xi\rangle \in \mathcal{M}$: Let $|\psi\rangle = E|\xi\rangle$. Then $S_j \underbrace{|\psi\rangle}_{\text{eigenvector}} = S_j E|\xi\rangle = (-1)^{\mu_j} E S_j |\xi\rangle = \underbrace{(-1)^{\mu_j}}_{\text{eigenvalue}} |\psi\rangle$

Quantum correction of bit flips

error	μ_1, μ_2
III	$0, 0$
XII	$1, 0$
IXI	$1, 1$
IIX	$0, 1$

The syndrome measurement allows to infer and undo the error *without breaking quantum coherence because we don't measure the encoded state*



Shor's 9-qubit code (concatenation of the repetition and dual repetition codes)

$$S_1|\xi\rangle = |\xi\rangle, \quad S_2|\xi\rangle = |\xi\rangle \;\Rightarrow\; S_1 S_2|\xi\rangle = |\xi\rangle$$

$$\text{1 logical qubit} \xrightarrow{V_{drep}} \text{3 intermediate qubits} \xrightarrow{V_{rep}^{\otimes 3}} \text{9 physical qubits}$$

$$V_{shor} = V_{rep}^{\otimes 3} V_{drep} : \quad \boxed{|x\rangle \mapsto \frac{1}{2} \sum_{x_1 \oplus x_2 \oplus x_3 = x} |x_1 x_1 x_1, x_2 x_2 x_2, x_3 x_3 x_3\rangle}$$

Stabilizer operators:

$$S_1 = ZZI\ III\ III, \quad S_3 = III\ ZZI\ III, \quad S_5 = III\ III\ ZZI,$$
$$S_2 = IZZ\ III\ III, \quad S_4 = III\ IZZ\ III, \quad S_6 = III\ III\ IZZ,$$

$$S_7 = XXX\ XXX\ III \qquad S_8 = III\ XXX\ XXX$$

$$\boxed{ZIZ\ IIIIII = S_1 S_2}$$

Shor's code protects from all single-qubit errors

W.l.o.g. we may consider Pauli errors:

$$E = \underbrace{\sigma^x(f_x)}_{\text{bit flip}} \underbrace{\sigma^z(f_z)}_{\text{phase error}} \qquad S_j E = (-1)^{\mu_j} E S_j$$

The action of phase errors is degenerate: it is not possible to uniquely *identify* the error by its syndrome. Nonetheless, we can *correct* the error.

Example:

$$E_1 = ZII\ III\ III, \qquad E_2 = IZI\ III\ III$$

Both errors are characterized by

$$\mu_1 = \cdots = \mu_6 = 0, \quad \mu_7 = 1, \quad \mu_8 = 0$$

$$|\xi\rangle \in \mathcal{M} \;\Rightarrow\; E_1|\xi\rangle = E_2|\xi\rangle$$

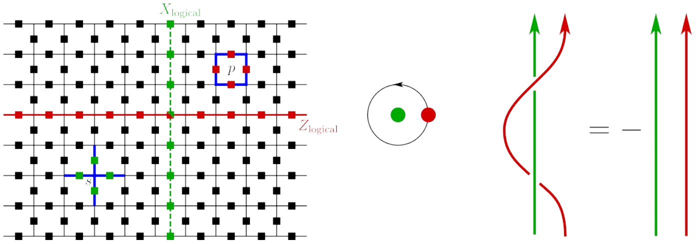
Applying E_1 will correct either error

Path to fault-tolerant computation

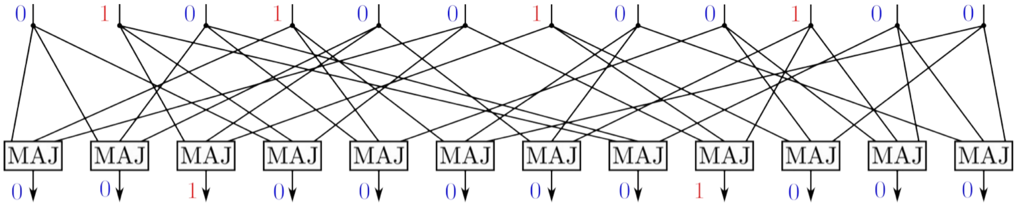
Classical status

1) Error model V
2) Suitable codes V
3) Fault-tolerant error correction procedure
4) Logical gates

We will also discuss protection from errors and quantum fault-tolerance at the *physical* level using topology



Fault-tolerant error correction procedure for the classical *n*-bit repetition code



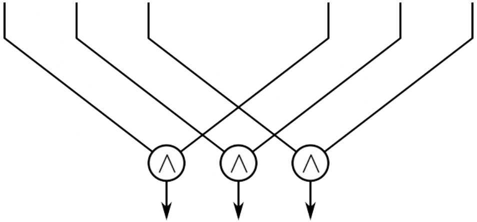
MAJ is the majority function

e.g. $MAJ(0,1,0)=0$

$MAJ(0,1,1)=1$

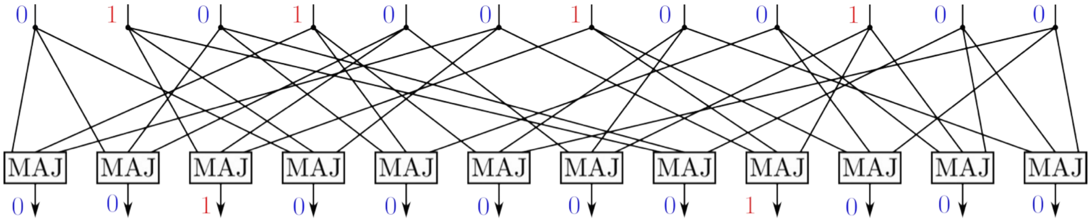
Logical gates for the classical repetition code

AND gate for two encoded bits:



Consider the *n*-bit repetition code.
Suppose each set of input physical bits has r errors, and in addition, q physical AND gates are faulty. In the worst case, there are $l=2r+q$ errors in the output bits. If we can reduce this number back to r, then our computer will work.

Fault-tolerant error correction procedure for the classical *n*-bit repetition code



Here *s*=3

An *s-voting circuit based on a* bipartite graph with *n* input and *n* output vertices such that each output vertex has in-degree *s*. (*s* is a small odd number, e.g. 3 or 5.)

Proposition. *There exist some constants* $0 < a < 1$ *and* $0 < b < 1$ *with the following property. For sufficiently large* n*, there is a* 5*-voting circuit such that if the input has* $l \leqslant an$ *errors, then the output has at most* bl *errors.*

(This gives room for $(1-b)l = (1-b)an$ faults.)

Proof sketch:

1. Suppose that the 5-voting circuit is chosen at random.
2. Let $l \leqslant an$ and $r = \lfloor bl \rfloor$. Consider arbitrary subsets $A, B \subseteq \{1, \ldots, n\}$ such that $|A| = l$ and $|B| = r + 1$. Estimate the probability of the event failure(A, B) defined as follows: *With the input chosen to be the characteristic function of* A*, the voting results in all bits in* B *are equal to* 1.
3. Sum over l, A, B and show that the total failure probability is less than 1.