Quantum Information Processing: An Essential Primer

Emina Soljanin, Rutgers

ICASSP 2020, ETON talk

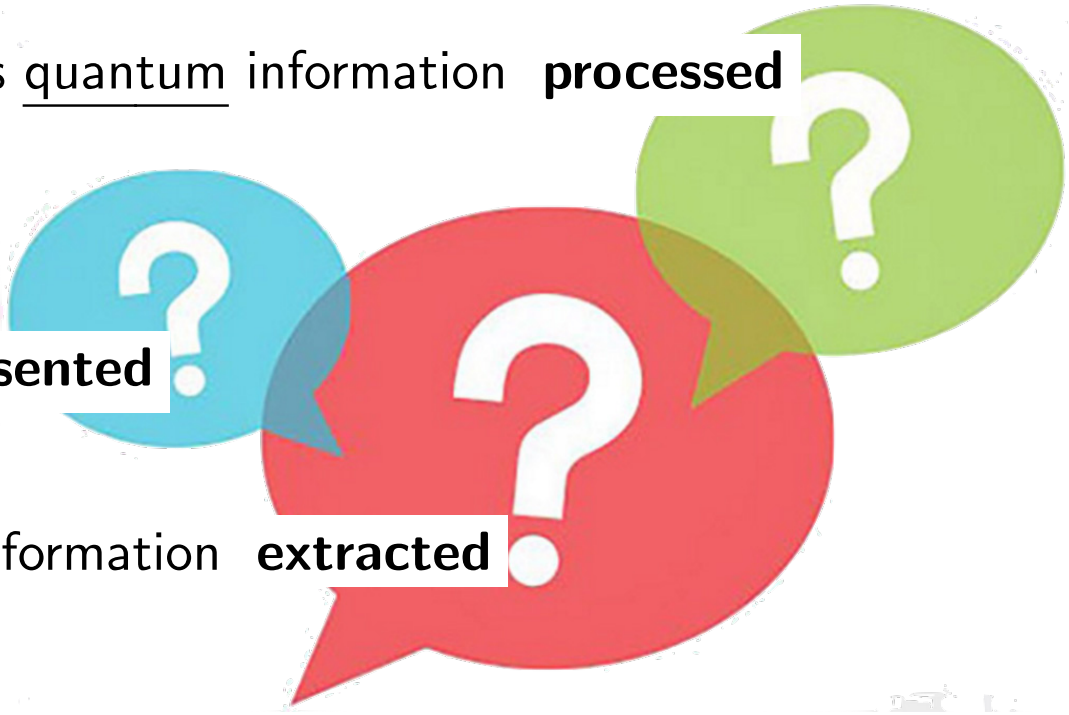
You probably have very many questions about Quantum Information Science ...

... we will start with the essential 3:

How is quantum information **processed**

How is quantum information **represented**

How is classical information **extracted**



... and address a few FAQs afterwards.

Pay special attention to  and  .

How is Quantum information represented?

Classical computers store and operate on **bits**. What about quantum?

What is a Qubit?

A qubit is a quantum computing/information counterpart to a bit.

Physically, a qubit is a two-level quantum system.

Mathematically, a qubit is a unit-norm column vector in $\mathbb{C}^2$.

$|\psi\rangle$ is Dirac's notation that indicates a column vector.

If we denote the basis vectors of $\mathbb{C}^2$ by $|0\rangle = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right]$ and $|1\rangle = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$ then qubit $|\psi\rangle$ is a linear combination

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

How are two qubits represented?

Consider two qubits: $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$.
The state of the pair is the Kronecker product of the individual states:

$$\begin{aligned}|\psi_1\rangle \otimes |\psi_2\rangle &= \big(\alpha_1|0\rangle + \beta_1|1\rangle\big) \otimes \big(\alpha_2|0\rangle + \beta_2|1\rangle\big) \\ &= \alpha_1\alpha_2\,|0\rangle \otimes |0\rangle + \alpha_1\beta_2\,|0\rangle \otimes |1\rangle + \beta_1\alpha_2\,|1\rangle \otimes |0\rangle + \beta_1\beta_2\,|1\rangle \otimes |1\rangle\end{aligned}$$

where

$$\begin{array}{cccc} |0\rangle \otimes |0\rangle & |0\rangle \otimes |1\rangle & |1\rangle \otimes |0\rangle & |1\rangle \otimes |1\rangle \\ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{array}$$

$$(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)/\sqrt{2}$$

In general, a 2-qubit state is any linear combination of the 4 basis states, and thus cannot always be expressed as a product of single qubit states.

How are multiple qubits represented?

- An n-qubit state is is a unit-norm vector in $\mathcal{H}_{2^n}$:

$$\sum_{i=0}^{2^n-1} \alpha_i |i_0 i_1 \dots i_{n-1}\rangle,$$

  where $i_0 i_1 \dots i_{n-1}$ is the binary representation of i and $\mathcal{H}_{2^n} = \underbrace{\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2}_{n}$.

- (Shorthand) notation for $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle$ (the i-th basis vector of $\mathcal{H}_{2^n}$):

$$|i_0\rangle|i_1\rangle \dots |i_{n-1}\rangle \equiv |i_0, i_1, \dots, i_{n-1}\rangle \equiv |i_0 i_1 \dots i_{n-1}\rangle$$

What is entanglement?

A Bell state (aka EPR pair):

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big).$$

EPR stands for Einstein, Podolsky and Rosen, who were the first to point out the "strange" properties of this state: *spooky action at a distance.*

A quantum state is **separable** if it can be expressed as a Kronceker product of single-qubit states. Otherwise, the state is **entangled**.

How is quantum information processed?

Quantum Gates:

Action on an n-qubit state is described by a $2^n \times 2^n$ **unitary matrix** U.

U can be a Kronecker product of matrices of smaller dimensions, or not.

When $U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1}$, then its action on the basis vector $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle \in \mathcal{H}_{2^n}$ is given by

$$U\,|i_0 i_1 \ldots i_{n-1}\rangle = \boxed{U_0|i_0\rangle} \otimes \boxed{U_1|i_1\rangle} \otimes \cdots \otimes \boxed{U_{n-1}|i_{n-1}\rangle}$$

Why is quantum evolution unitary?

In a closed system, $|\psi(t)\rangle$ evolves according to the Schrödinger equation:

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H \cdot |\psi(t)\rangle$$

where H is a fixed Hermitian matrix known as the system's Hamiltonian.

$\Longrightarrow$

When H does not depend on time, the solution of this equation is

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle$$

where $U(t) = \exp\left(-\frac{i}{\hbar} H t\right)$ is a unitary matrix.

Are there some standard gates? 📌

The Hadamard gate:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \begin{array}{l} |0\rangle \;—\boxed{H}—\; (|0\rangle + |1\rangle)/\sqrt{2} \\ |1\rangle \;—\boxed{H}—\; (|0\rangle - |1\rangle)/\sqrt{2} \end{array}$$

The Identity and the Pauli Matrices:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \begin{array}{l} |0\rangle \;—\boxed{I}—\; |0\rangle \\ |1\rangle \;—\boxed{I}—\; |1\rangle \end{array} \qquad \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \begin{array}{l} |0\rangle \;—\boxed{Y}—\; i\,|1\rangle \\ |1\rangle \;—\boxed{Y}—\; -i\,|0\rangle \end{array}$$

$$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \begin{array}{l} |0\rangle \;—\boxed{X}—\; |1\rangle \\ |1\rangle \;—\boxed{X}—\; |0\rangle \end{array} \qquad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \begin{array}{l} |0\rangle \;—\boxed{Z}—\; |0\rangle \\ |1\rangle \;—\boxed{Z}—\; -|1\rangle \end{array}$$

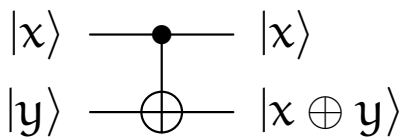
σ_X is often referred to as `NOT` or a bit-flip gate.

How about 2-qubit gates?

The two-qubit quantum gate known as XOR or CNOT:

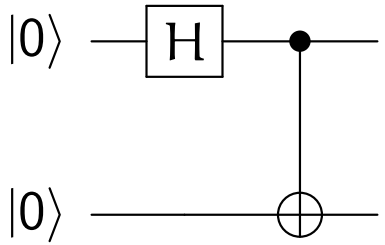
$$\texttt{CNOT} : |x, y\rangle \to |x, x \oplus y\rangle$$

$$x, y \in \{0, 1\}$$



$$U_{\texttt{CNOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

We use the Hadamard and the CNOT gate to create entanglement:



$$\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

Is there something we cannot do?

The No-Cloning Principle:

There is no physical process that leads to an evolution

$$|\phi\rangle \otimes |s\rangle \rightarrow |\phi\rangle \otimes |\phi\rangle$$

where $|\phi\rangle$ is an arbitrary state and $|s\rangle$ is a fixed state.

This is an easy to prove theorem that simply says that there is no unitary matrix U_c, s.t. for all $|\psi\rangle$, we have

$$U_c(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

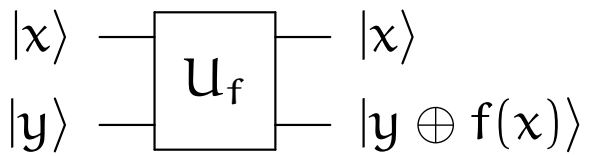
That is all, but it is often misunderstood.

What is quantum parallelism?

Evaluation gate for a function $f : \{0,1\}^n \to \{0,1\}^m$:

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$$

$$x \in \{0,1\}^n,\ y \in \{0,1\}^m$$



(Note that U_f operates on $\mathbb{C}^{\otimes n} \otimes \mathbb{C}^{\otimes m}$.)

Quantum Parallelism:

1. Apply $H^{\otimes n}$ gate to $|0\rangle^{\otimes n}$ to create <u>uniform superposition</u> of the basis states: $|0\rangle^{\otimes n} \;—\boxed{H^{\otimes n}}—\; \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$

2. Apply the U_f gate, to <u>simultaneously evaluate f</u> on its entire domain:

$$U_f \left(H^{\otimes n} \otimes I_m\right) \left(|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m}\right) = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$$

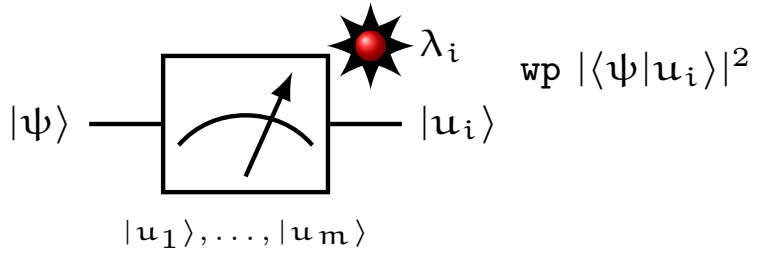
But can we read all out? Is there quantum speedup?

How can classical information be extracted?

To every physical observable, there corresponds a Hermitian matrix H.

Let $|u_i\rangle$ & λ_i be the eigenvectors and eigenvalues of H.

- The only possible results of "measuring H" are λ_i.
- The only possible states after "measuring H" are $|u_i\rangle$.



If we me measure $|\psi\rangle$, the result will be λ_i with probability $|\langle\psi|u_i\rangle|^2$.

When we "see" λ_i, we know that state $|\psi\rangle$ has collapsed to $|u_i\rangle$.

What is quantum measurement?

Von Neumann Measurement:

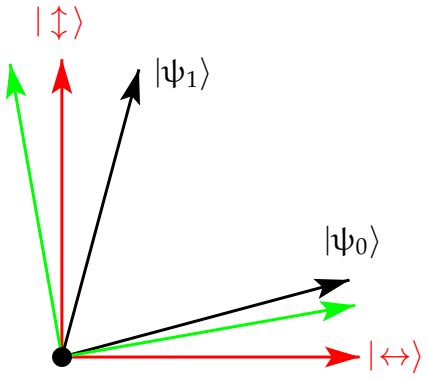
- A set of pairwise orthogonal projection operators $\{\Pi_i\}$ that form a complete resolution of the identity: $\sum_i \Pi_i = I$.
- For input $|\psi\rangle$, output $\Pi_i |\psi\rangle$ happens with probability $\langle\psi| \Pi_i |\psi\rangle$.

Positive Operator-Valued Measure (POVM):

- Any set of positive-semidefinite operators $\{E_i\}$ that form a complete resolution of the identity: $\sum_i E_i = I$.
- For input $|\psi\rangle$, output $E_i |\psi\rangle$ happens with probability $\langle\psi| E_i |\psi\rangle$.

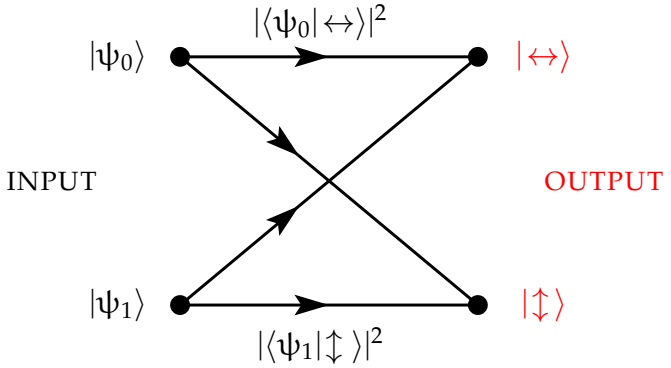
Examples of Quantum Measurement

Von Neumann Measurement:

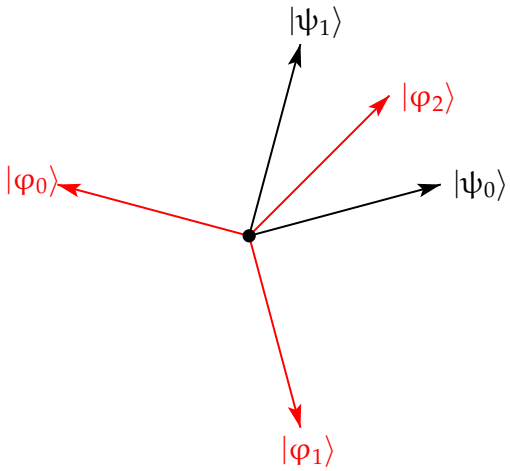


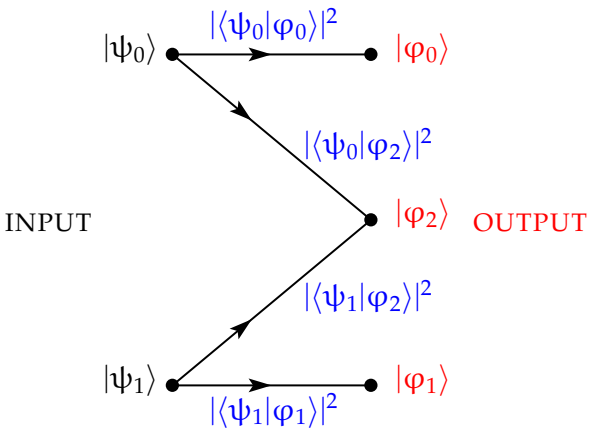
$\Pi_0 = |\leftrightarrow\rangle\langle\leftrightarrow|$

$\Pi_1 = |\updownarrow\rangle\langle\updownarrow|$



Positive Operator-Valued Measure (POVM):





Pauli Matrices as Gates and Observables

matrix	action	eigenvalue/eigenvector
$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\lvert 0\rangle$ —$\boxed{X}$— $\lvert 1\rangle$	$+1/(\lvert 0\rangle + \lvert 1\rangle)$
	$\lvert 1\rangle$ —$\boxed{X}$— $\lvert 0\rangle$	$-1/(\lvert 0\rangle - \lvert 1\rangle)$
$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\lvert 0\rangle$ —$\boxed{Y}$— $i\lvert 1\rangle$	$+1/(\lvert 0\rangle + i\lvert 1\rangle)$
	$\lvert 1\rangle$ —$\boxed{Y}$— $-i\lvert 0\rangle$	$-1/(\lvert 0\rangle - i\lvert 1\rangle)$
$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\lvert 0\rangle$ —$\boxed{Z}$— $\lvert 0\rangle$	$+1/\lvert 0\rangle$
	$\lvert 1\rangle$ —$\boxed{Z}$— $-\lvert 1\rangle$	$-1/\lvert 1\rangle$

How can such measurements be useful?

Recall that quantum parallelism allows us to evaluate $f : \{0,1\}^n \to \{0,1\}^m$ on its entire domain: $|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m} \longrightarrow \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$

But we cannot simultaneously extract all the values by a measurement!

Quantum Algorithms (many of them)

prescribe further processing of the state $\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x, f(x)\rangle$ so that, when a measurement is eventually performed, the probability of getting the answer to the question we posed is (close to) 1.

How can we correct errors?

... well, we'll just use error correction codes.

Encoding Doubts

We protect classical information by making it redundant, but how can we introduce redundancy when "there is no cloning"?

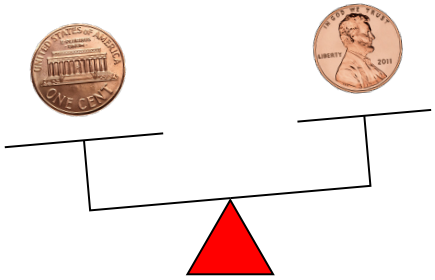
Decoding Doubts

We diagnose errors by looking into and using what we received, but how can we use the received qubits without using them up?

How do we find a fake penny?

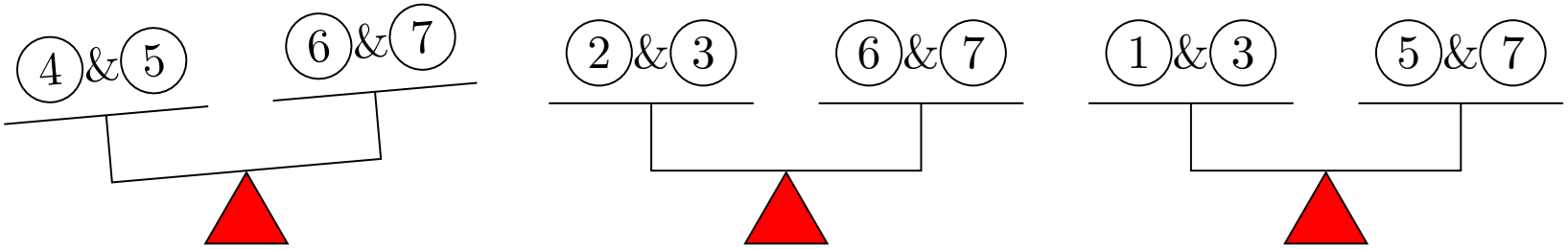
Classical Penny Weighing

- You are given 8 pennies, and told that one has a different weight.
  - You only have a balance scale.
  - How many measurements are required to tell which penny is different?
  - How will you perform the measurements?



We can use coding theory or compressed sensing to solve this problem.

There are multiple solutions, but the following is of interest to us:



How do we protect bit x from errors?

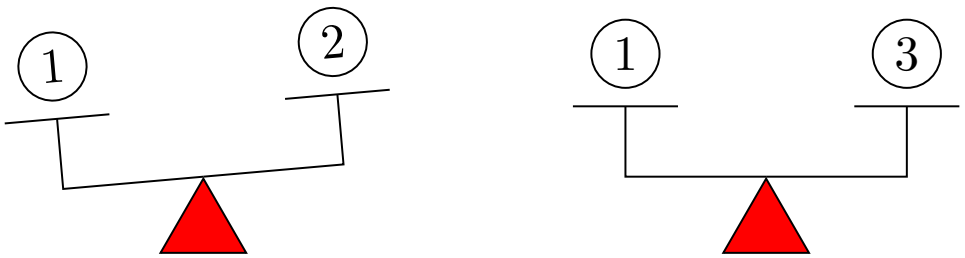
We introduce redundancy: $x \to x\,x\,x$ ($0 \to 000$ and $1 \to 111$)

This is a rate 1/3 code that can correct a single bit flips:

Let $y_0\,y_1\,y_2$ be a corrupted version of $x\,x\,x$ with at most one bit flip:

additive error	y_0	y_1	y_2
000	x	x	x
100	$x \oplus 1$	x	x
010	x	$x \oplus 1$	x
001	x	x	$x \oplus 1$

Compare with the 3-penny weighing problem.



A 1 bit to 3 bits Repetition Code – Decoder

Measurement is non-adaptive, and gives us the error syndrome:

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} y_0 \oplus y_1 \\ y_0 \oplus y_2 \end{bmatrix}$$

Error Correction: The syndrome instructs us how to correct errors:

y_0	y_1	y_2	$y_0 \oplus y_1$	$y_0 \oplus y_2$	add
x	x	x	0	0	000
$x \oplus 1$	x	x	1	1	100
x	$x \oplus 1$	x	1	0	010
x	x	$x \oplus 1$	0	1	001

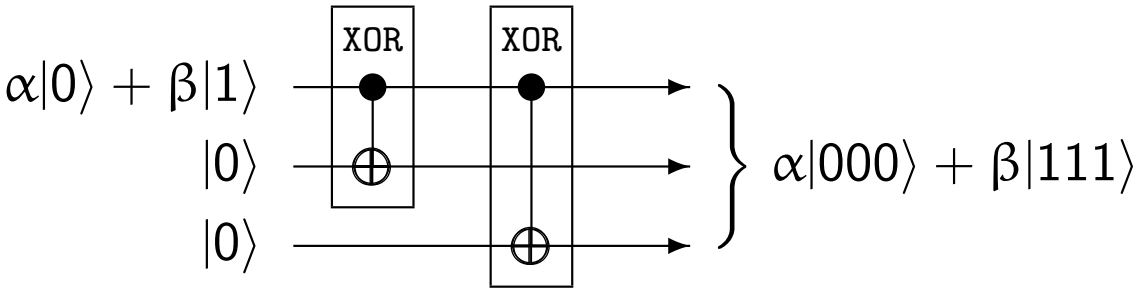
How can we protect a qubit from errors?

Encoding map:

$$\underbrace{\alpha|0\rangle + \beta|1\rangle}_{\in \mathcal{H}_2} \quad \rightarrow \quad \underbrace{\alpha|000\rangle + \beta|111\rangle}_{\in \mathcal{H}_{2^3}}$$

$$\boxed{\begin{array}{ccc} |0\rangle & \rightarrow & |000\rangle \\ |1\rangle & \rightarrow & |111\rangle \end{array}}$$

Encoding circuit:



$$\texttt{XOR} : |x, y\rangle \rightarrow |x, x \oplus y\rangle \quad U_{\texttt{XOR}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

A 1 Qubit to 3 Qubits Code – Decoder

Error model:

error operators	resulting state
$I \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
$\sigma_X \otimes I \otimes I$	$\alpha\|100\rangle + \beta\|011\rangle$
$I \otimes \sigma_X \otimes I$	$\alpha\|010\rangle + \beta\|101\rangle$
$I \otimes I \otimes \sigma_X$	$\alpha\|001\rangle + \beta\|110\rangle$

Measurements & Correction:

corrupted state	$\sigma_Z \otimes \sigma_Z \otimes I$	$\sigma_Z \otimes I \otimes \sigma_Z$	apply
$\alpha\|000\rangle + \beta\|111\rangle$	$+1$	$+1$	$I \otimes I \otimes I$
$\alpha\|100\rangle + \beta\|011\rangle$	-1	-1	$\sigma_X \otimes I \otimes I$
$\alpha\|010\rangle + \beta\|101\rangle$	-1	$+1$	$I \otimes \sigma_X \otimes I$
$\alpha\|001\rangle + \beta\|110\rangle$	$+1$	-1	$I \otimes I \otimes \sigma_X$

What can we read/understand after this talk?

Many topics should be accessible, e.g.,

- Quantum teleportation
- Dense coding
- Quantum key distribution
- Deutsch-Jozsa Problem
- Gover's search algorithm
- Shor's factoring algorithm

A little more is needed for quantum Information/Communications Theory.

A lot more is necessary for some other topics.

What is quantum computing "state of the art"?

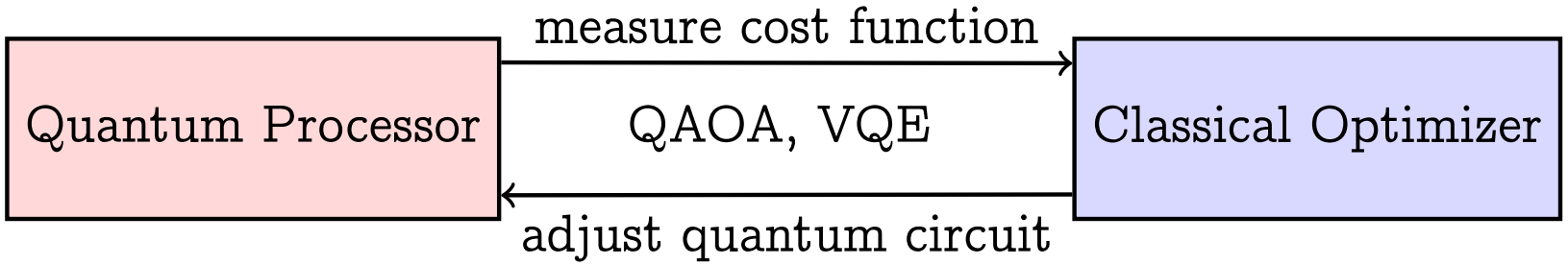
Ware currently in the NISQ computing era:

- NISQ stands for Noisy Intermediate-Scale Quantum.
- NISQ devices operate on 50-100 qubits,
  too few to spare for error-correction.
- NISQ systems may be able to perform tasks that exceed
  the capabilities of today's classical digital computers

What is NISQ computing good for?

Algorithms that are appropriate for (NISQ) systems

- should not need extensive error correction (can tolerate noise), and
- should not need very large numbers of qubits (intermediate scale),
- but should exhibit quantum speedup and solve useful problems.



Is there funding for research in quantum computing?

Yes, very much so in the US ...

Quantum Leap is one of the NSF's 10 big ideas for future investments.

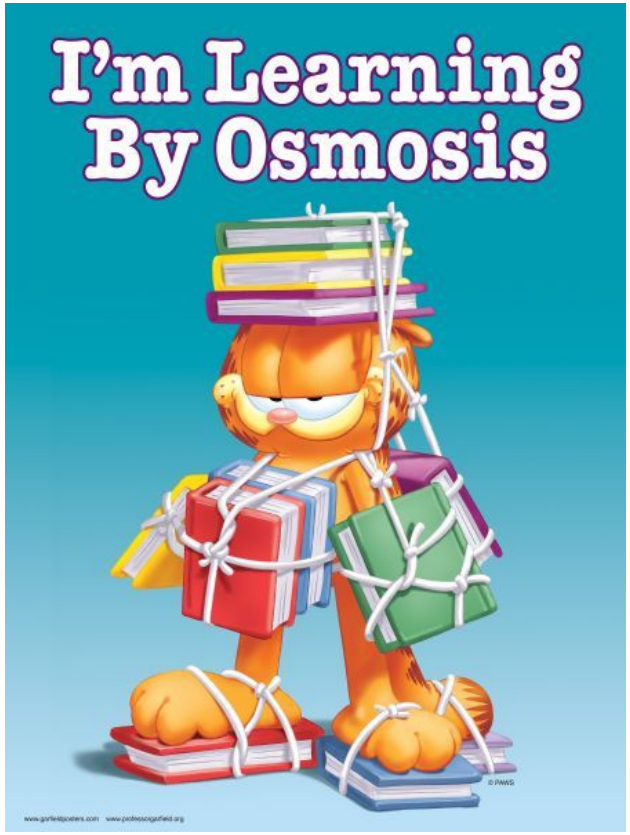
National Quantum Initiative approved by the science committee of the US House of Representatives in 2018 to create a 10-year federal effort.

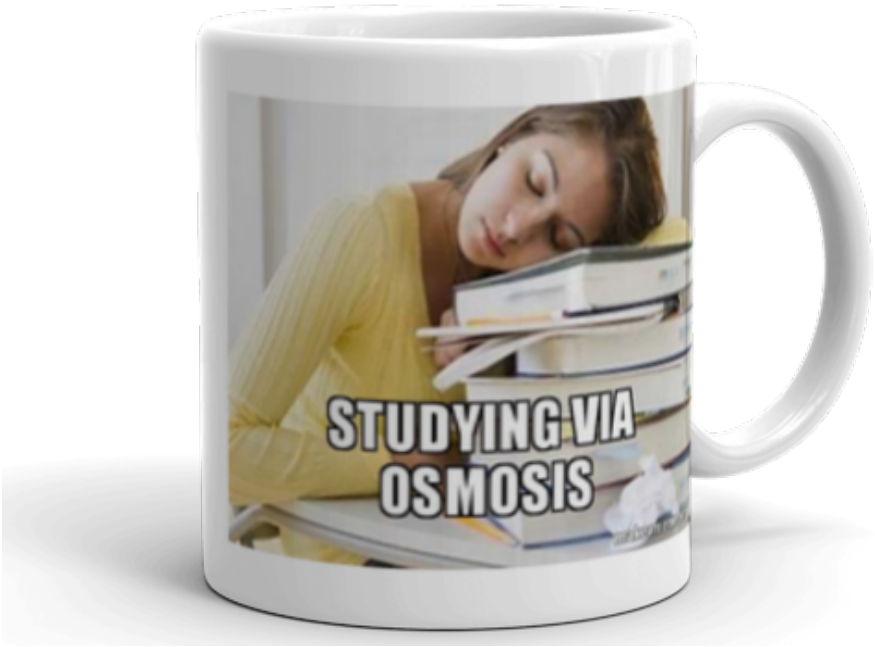
The Trump administration's 2021 budget requests $237 million in funding to support **quantum information research**.

... and elsewhere.

How hard is it to enter the field?

The mathematics is easy but the concepts are abstract, and thus ...





... certain learning methods will not work!


I wish we could be there ...