An Introduction to Quantum Computation

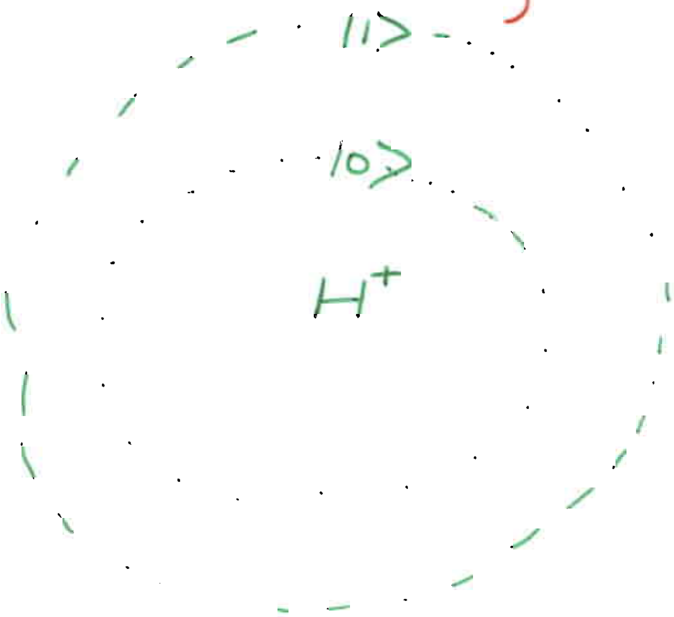
Umesh V. Vazirani

U.C. Berkeley / MSRI

Quantum Physics

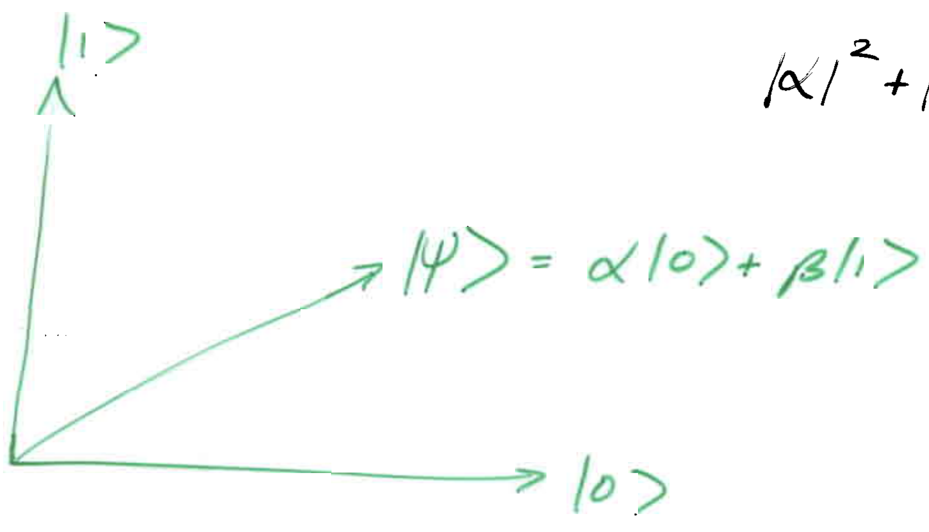
* Entanglement
* Superposition
* Measurement
* Unitary evolution

Qubits



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \in \mathbb{C}^2$$

$$|\alpha|^2 + |\beta|^2 = 1.$$

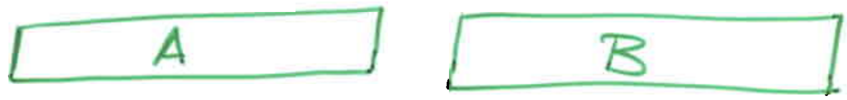


K-State System:

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{K-1}|K-1\rangle \quad \in \mathbb{C}^K$$

$$\sum_{i=0}^{K-1} |\alpha_i|^2 = 1.$$

Tensor Products



$\mathbb{C}^k$ $\qquad$ $\mathbb{C}^l$

State-space(AB) = State-space$(A) \otimes$ state-space(B)

$$\text{State-space}(AB) = \mathbb{C}^{k \cdot l}$$

$$|\psi_A\rangle = \sum_x \alpha_x |x\rangle$$

$$|\psi_B\rangle = \sum_y \beta_y |y\rangle$$

$$|\psi_{AB}\rangle = \sum_{x,y} \gamma_{x,y} |x,y\rangle$$

Entanglement

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$

Bell States:

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

* The Bell state cannot be factored

* State of first qubit?

n qubits

$\boxed{100011101101}$

State-space $= \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}$

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \qquad \sum_x |\alpha_x|^2 = 1$$

* Exponential resources

Measurement

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Measure: See x with probability $|\alpha_x|^2$

$$|\psi'\rangle = |x\rangle$$

* Limited access to quantum state
* State collapse

Partial Measurement

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

Measure first qubit:

See 0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

e.g. Bell State $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Quantum Algorithms & Complexity

Modified Church-Turing Thesis: Any "reasonable" model of computation can be simulated efficiently on a probabilistic Turing machine.

* Quantum computers only known model that violate this thesis.
  e.g. Shor's factoring algorithm.

* Exponential resources
  vs
  limited access.

Quantum Communication

$$A \xleftrightarrow[\text{quantum bits}]{} B$$

* Exponential resources vs limited access.
* Entanglement...

Bell Inequalities:

* A, B share a Bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.

A B

	A	B
Input:	$x_A \in \{0,1\}$	$x_B \in \{0,1\}$
Output	a	b

$$\Pr[x_A \wedge x_B = a \oplus b] \approx .8$$

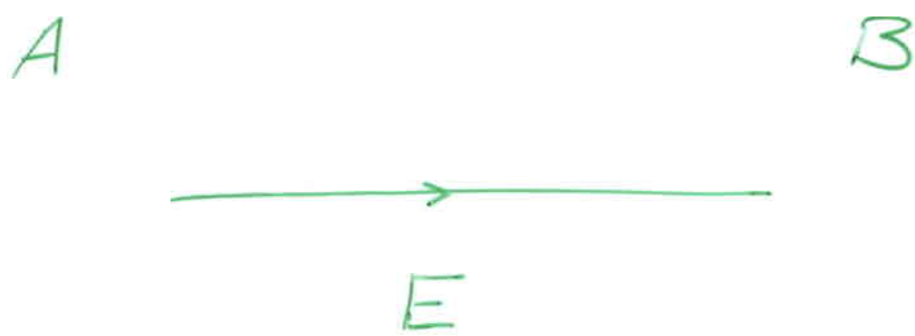
Classically:

r

	A	B
Input	$x_A \in \{0,1\}$	$x_B \in \{0,1\}$
Output	a	b

$$\Pr[x_A \wedge x_B = a \oplus b] \leq 3/4$$

Quantum Cryptography



* Limited access to quantum state

* Measurement modifies state.

Quantum Error-correction

Decoherence — Inadvertent measurement by environment.

$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

Measure first bit:

0 with probability $\frac{1}{2}$. $|\psi'\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{i}{\sqrt{2}}|01\rangle$

1 with probability $\frac{1}{2}$. $|\psi'\rangle = -|11\rangle$

* No cloning theorem $|\psi\rangle \otimes |0\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle$
* Linearity of quantum physics.

* Fault-tolerance: compute on encoded data.

Dirac Bra/Ket Notation:

"kets" $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ $|\phi\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$

"bra" $\langle\psi| = (\bar{a} \ \ \bar{b})$

"bra-ket" $\langle\psi|\phi\rangle = (\bar{a} \ \ \bar{b})\begin{pmatrix} c \\ d \end{pmatrix} = \bar{a}c + \bar{b}d$

= inner-product.

$$P = |\psi\rangle\langle\psi| = \begin{pmatrix} a \\ b \end{pmatrix}(\bar{a} \ \ \bar{b}) = \begin{pmatrix} a\bar{a} & a\bar{b} \\ \bar{a}b & b\bar{b} \end{pmatrix}$$

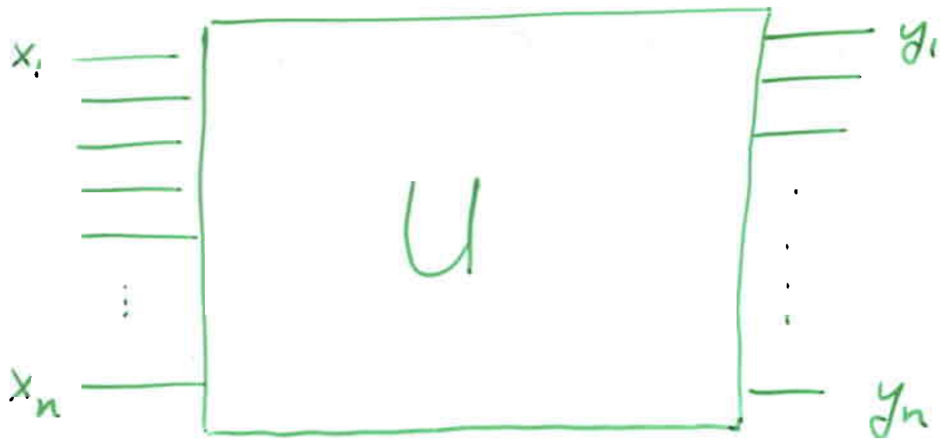
= Projection onto $|\psi\rangle$.

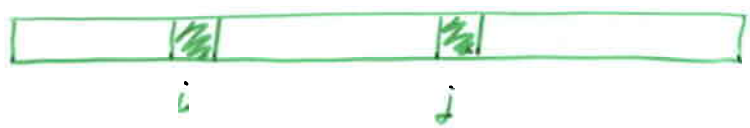
$$P^2 = |\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{\overset{\shortparallel}{1}}\langle\psi| = |\psi\rangle\langle\psi| = P$$

$$P|\phi\rangle = |\psi\rangle\underbrace{\langle\psi|\phi\rangle}_{\text{inner-product.}}$$

* In quantum computation: represent both that state is a vector, and is data.

Unitary Evolution.





U_k is <u>simple</u> if $U_k = V_{ij} \otimes I$

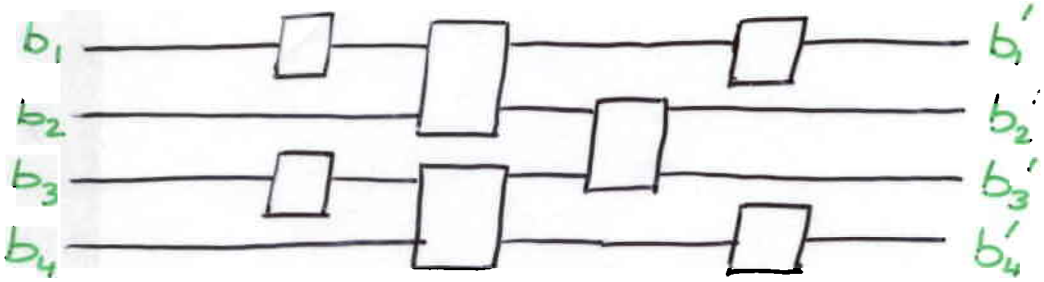
want:

$$U = U_1 \cdot U_2 \cdots U_M \quad \text{for} \quad M = poly(n).$$

Theorem: $\forall\, U, \varepsilon \;\exists$ simple $U_1, \ldots, U_M$:

$$\| U - U_1 \cdot U_2 \cdots U_M \| \leq \varepsilon \quad \text{and} \quad M = 2^{poly(n)}.$$

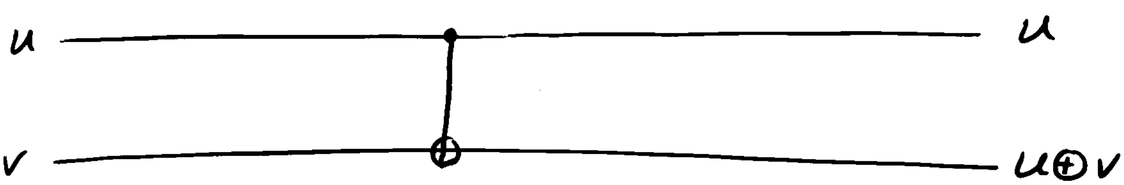
Quantum Circuits



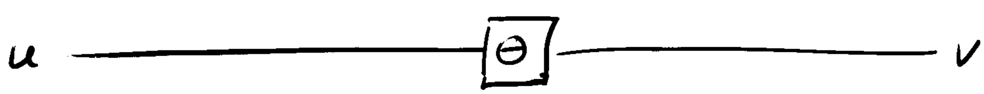
* Each wire carries a qubit

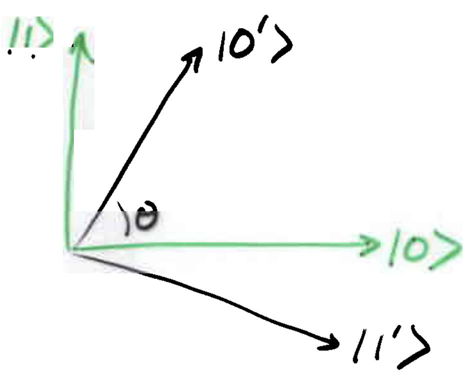
$$|u\rangle = \alpha|0\rangle + \beta|1\rangle$$

* Controlled-NOT or XOR gate



* Rotation Gate





$$|0\rangle \longrightarrow \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$

$$|1\rangle \longrightarrow \sin\theta\,|0\rangle - \cos\theta\,|1\rangle.$$

Complexity Classes

Does $x \in$ Primes?

P = Polynomial time (in length of x)

BPP = Bounded-error probabilistic polynomial time.

$x \in L \Rightarrow A(x)$ accepts with probability $\geq 2/3$

$x \notin L \Rightarrow A(x)$ rejects with probability $\geq 2/3$.

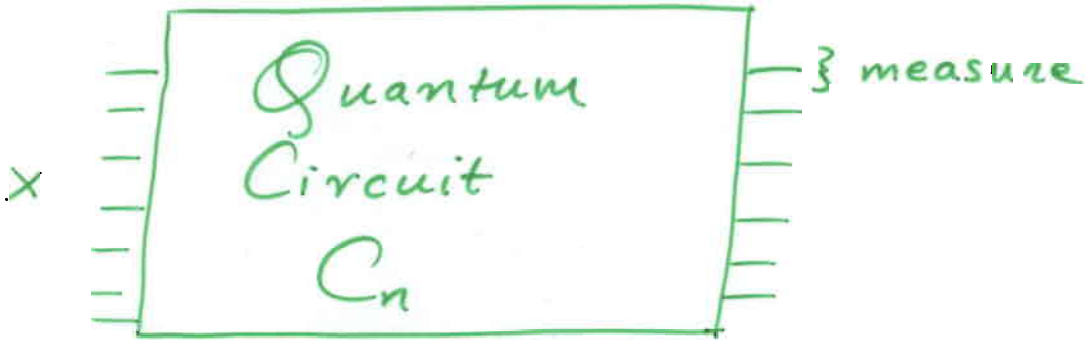
Can increase $2/3$ to $1 - \frac{1}{2^k}$ by taking majority of $O(k)$ runs.

NP = non-deterministic polynomial time.

Polynomial time verifiable proof that $x \in L$.

BQP

Bounded-error quantum polynomial time.

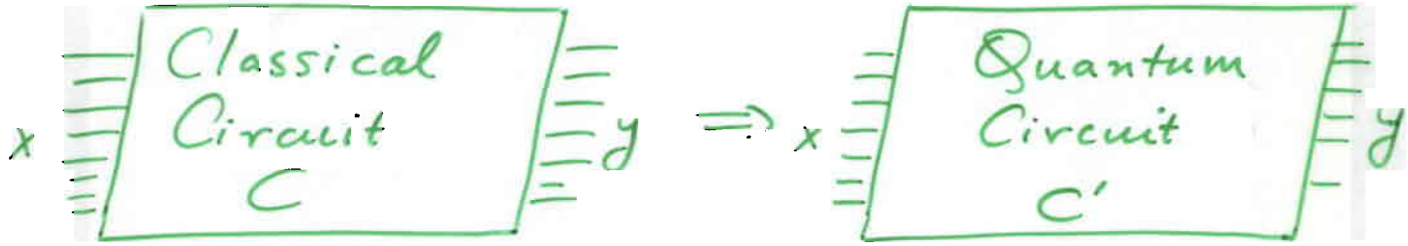


$x \in L \Rightarrow C_n(x)$ accepts with probability $\geq 2/3$

$x \notin L \Rightarrow C_n(x)$ rejects with probability $\geq 2/3$

* $|C_n| = O(poly(n))$
* C_n is poly-uniform
* Can increase $2/3$ to $1 - \frac{1}{2^k}$ at $O(k)$ cost.

$P \subseteq BQP$



* Unitary evolution +

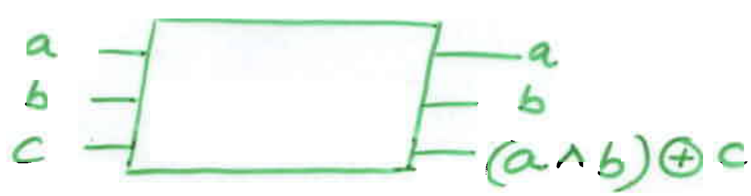
  basis states $\longrightarrow$ basis states

  $\Longrightarrow$ permutation of basis states.

* i.e. cannot erase.

* AND, NOT gates universal for classical ckts.

Tofolli gate

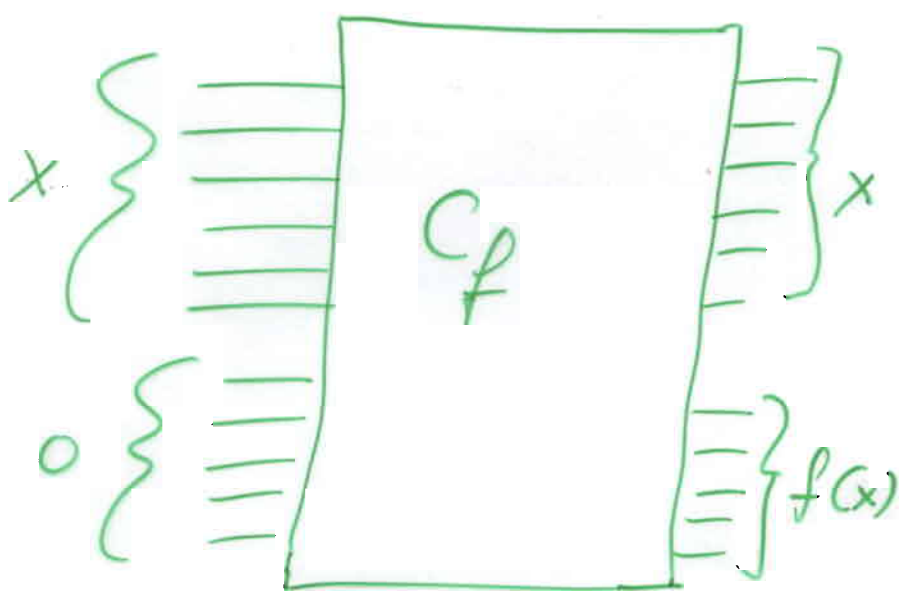


* Set $c=0$ to get AND gate
* Set $a=b=1$ to get NOT gate.
* Cannot erase. $\therefore$ $|x\rangle|0\rangle \longrightarrow |x\rangle|f(x)\rangle$

f efficiently computible classically

$$\Downarrow$$

$$\sum_x \alpha_x |x\rangle|0\rangle \longrightarrow \sum_x \alpha_x |x\rangle|f(x)\rangle$$

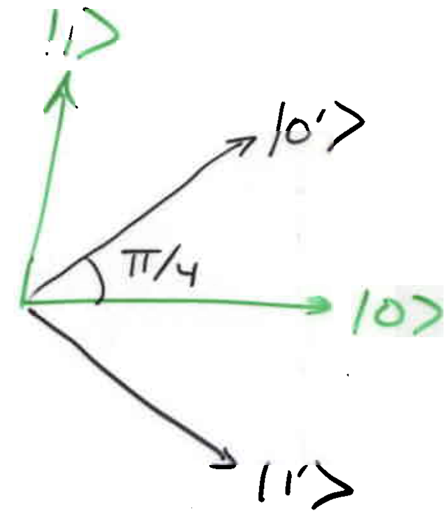


$BPP \subseteq BQP$

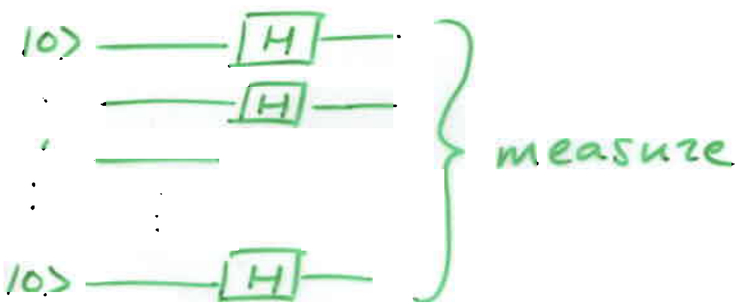
Hadamard Gate = $\pi/4$ rotation.

$|0\rangle \to \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

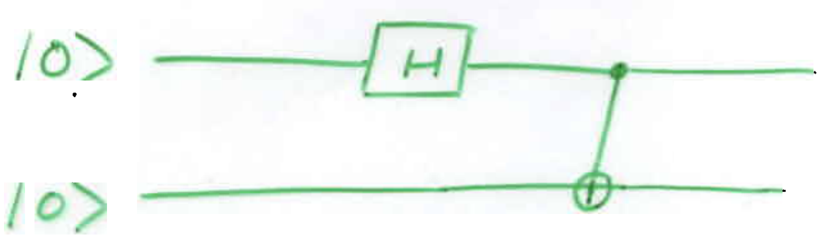
$|1\rangle \to \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$



To obtain m random bits:



Principle of deferred measurement:

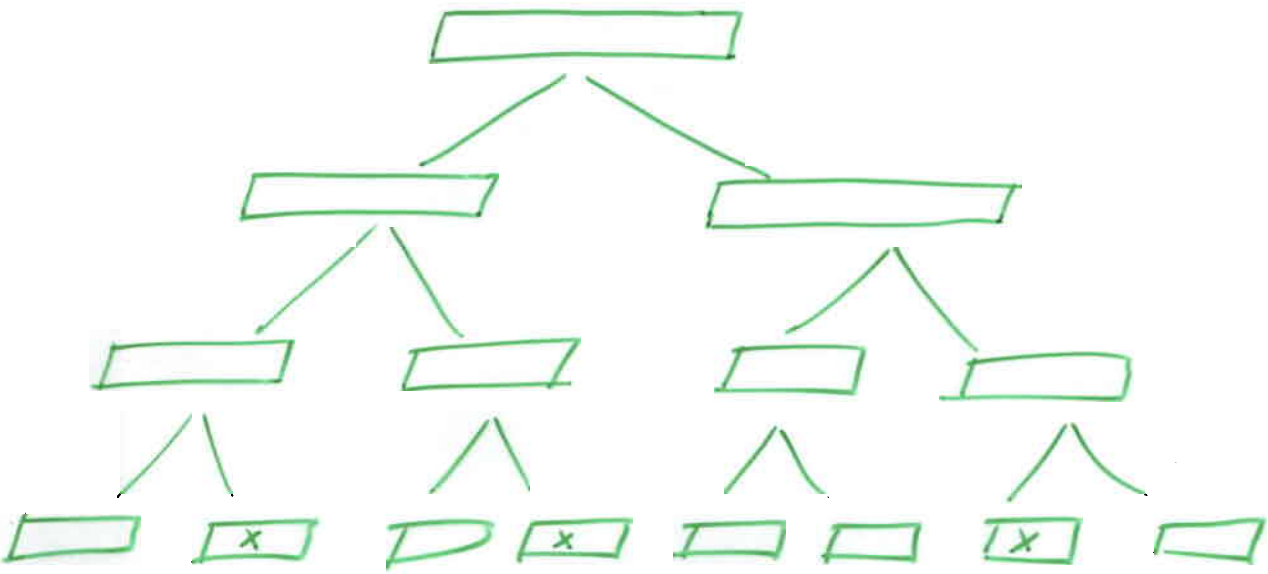


$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

* Measuring a qubit after the last gate has been applied to it does not change outcome of quantum computation.

BQP ⊆ PSPACE

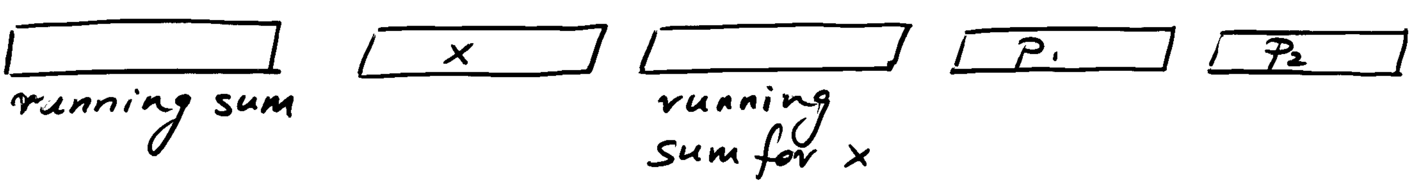
Quantum Computation:



* Wlog all amplitudes are real.

* $$\Pr[x] = \Big|\sum_{\substack{\text{paths } p \\ \text{ending in } x}} \alpha_p \Big|^2$$

$$= \sum_{\substack{p_1, p_2 \\ \text{ending in } x}} \alpha_{p_1} \cdot \alpha_{p_2}$$



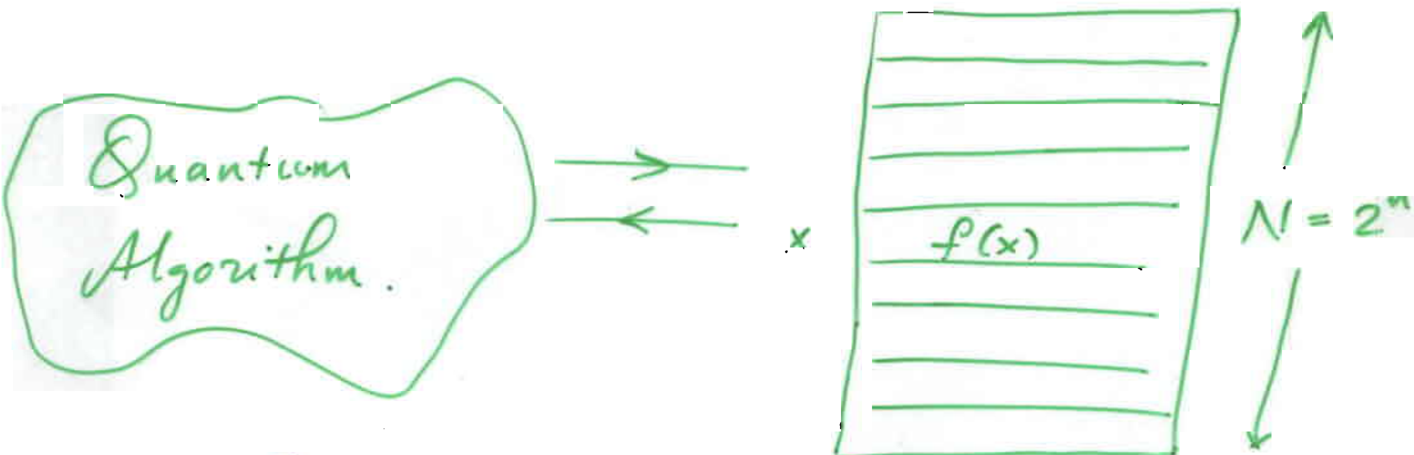
$P \subseteq BPP \subseteq BQP \subseteq PSPACE$.

* $P \neq PSPACE$? is a major open question in computational complexity theory.

$NP \subseteq BQP$?

SAT: $f : \{0,1\}^n \to \{0,1\}$ boolean formula.

$\exists\, x_1, \ldots, x_n : f(x_1, \ldots, x_n) = 1$?



$$\sum_x \alpha_x |x\rangle|0\rangle \longrightarrow \sum_x \alpha_x |x\rangle|f(x)\rangle$$

Theorem: Any quantum algorithm must make $\Omega(\sqrt{N}) = \Omega(2^{n/2})$ queries.

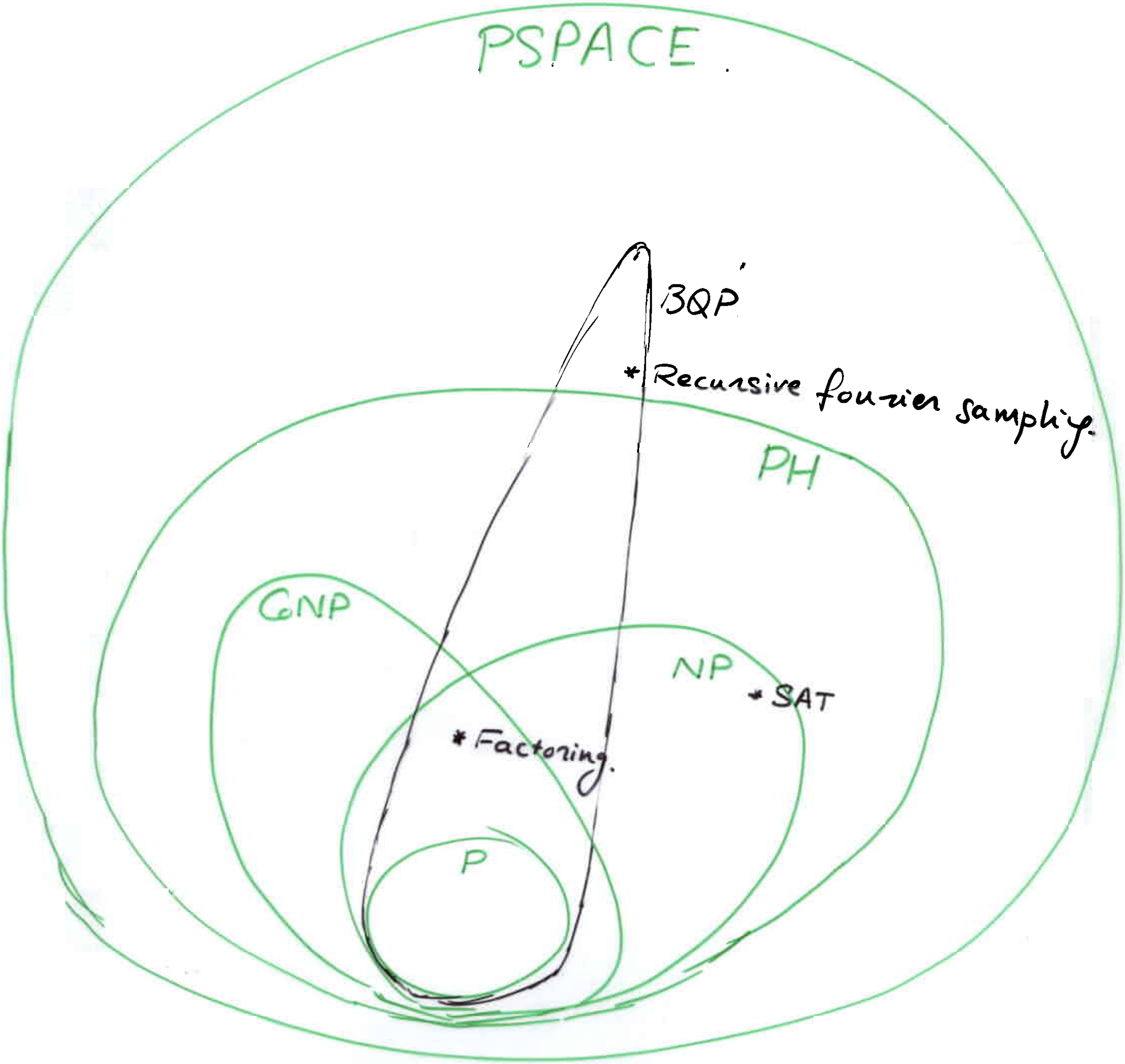
$NP \cap CoNP \subseteq BQP$?

$f : \{0,1\}^n \to \{0,1\}^n$ permutation.

On input y, decide whether $x : f(x) = y$ has $x_1 = 1$.

Theorem: $\Omega(\sqrt{N}) = \Omega(2^{n/2})$ queries necessary.

Corollary: $\exists A : (NP \cap CoNP)^A \not\subseteq BQP^A$.



Conjecture: Recursive fourier sampling $\notin$ PH.

$\exists A : BQP^A \not\subseteq MA^A$.