If $P_j = \mathbb{1} \otimes$ ____, then $H_1 P_j H_1^\dagger = \mathbb{1} \otimes$ ____ $= P_j$.

If $P_j = X \otimes$ ____, then $H_1 P_j H_1^\dagger = Z \otimes$ ____

If $P_j = Z \otimes$ ____, then $H_1 P_j H_1^\dagger = X \otimes$ ____

If $P_j = Y \otimes$ ____, then $H_1 P_j H_1^\dagger = Y \otimes$ ____

Similar rules can be generated for CNOT and S updates.

Gottesman–Knill

Thm given a circuit $g_m \cdots g_1$ with each $g_t \in \{CNOT, S, H\}$, we can efficiently compute a collection of stabilizers for

$g_m \cdots g_1 |0^n\rangle$.

Pf. Starting with $P_j = Z_j$ which stabilize $|0^n\rangle$, we update stabilizers gate by gate. Each update takes $O(n^2)$ time as there are $n$ stabilizers each of $O(n)$ bits. Total time is $O(mn^2)$, space $O(n^2)$. $\square$

What about measurements?

Wlog, we only need to consider measuring the first qubit in standard basis.

Notice if $P|\psi\rangle = P'|\psi\rangle = |\psi\rangle$ for Paulis $P, P'$, then

$PP'|\psi\rangle = P|\psi\rangle = |\psi\rangle$ so $PP'$ stabilizes $|\psi\rangle$ as well.

So if $P_1, \dots, P_n$ stabilize $|\psi\rangle$ then

$\langle P_1, \dots, P_n \rangle$ stabilizes $|\psi\rangle$ where this is the stabilizer

subgroup $\leq \mathcal{P}_n$.

Let $S_\psi = \{ P \in \mathcal{P}_n \mid P|\psi\rangle = |\psi\rangle \}$.

Measuring $|\psi\rangle$:

1. If $Z_1 \in S_\psi$, then measurement outcome is $0$ and state doesn't change. Deterministic measurement.

2. If $-Z_1 \in S_\psi$, then measurement outcome is $1$ and state doesn't change. Deterministic measurement.

3. If $Z_1 \notin S_\psi$, things get more complicated.

$Z_1$ must not commute with all of $S_\psi$.

Find a basis for $S_\psi$ s.t. $S_\psi = \langle b_1, \dots, b_n \rangle$,

and $b_1 Z_1 = -Z_1 b_1$ but $b_j Z_1 = Z_1 b_j$ for $j > 1$.

Flip a coin. Replace $b_1$ with $Z_1$ or $-Z_1$ depending on the coin flip.

<u>Pf of correctness</u>

Since $b_1$ and $Z_1$ anticommute, square to $\mathbb{1}$, by prob 2 problem, there exists a change of basis s.t.

$$\mathcal{U} b_1 \mathcal{U}^\dagger = X_1 \quad \text{and} \quad \mathcal{U} Z_1 \mathcal{U}^\dagger = Z_1, \text{ and } \mathcal{U} b_j \mathcal{U}^\dagger = \mathbb{1} \otimes b_j'.$$

Since $b_1 \in S_\psi$, $\mathcal{U}|\psi\rangle = |+\rangle \otimes$ ____

So measuring, $Z_1$ is a coin-flip resulting in $|0\rangle$ or $|1\rangle$. Doesn't change remainder of state, so new state is stabilized by $Z_1, b_2, \dots, b_n$ or $-Z_1, b_2, \dots, b_n$ depending on outcome. $\square$

Finding a basis $\langle b_1, \dots b_n \rangle$ for $S_\psi$ s.t. only $b_1$ anticommutes:

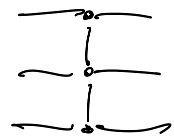
① Renumber bases s.t. $b_1$ anticommutes.

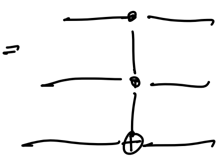
② If $b_k$ anticommutes, replace $b_k$ with $b_1 b_k$.

Next, computation with a few non-Clifford gates.

non-Clifford gate examples:

$$T = \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

CCZ 

CCX = 

(Toffoli)

<u>Theorem</u> (Solovay-Kitaev) Any 2-qubit unitary can be $\epsilon$-approximated using $O(\mathrm{polylog}(1/\epsilon))$ $H, T, CNOT$ gates.

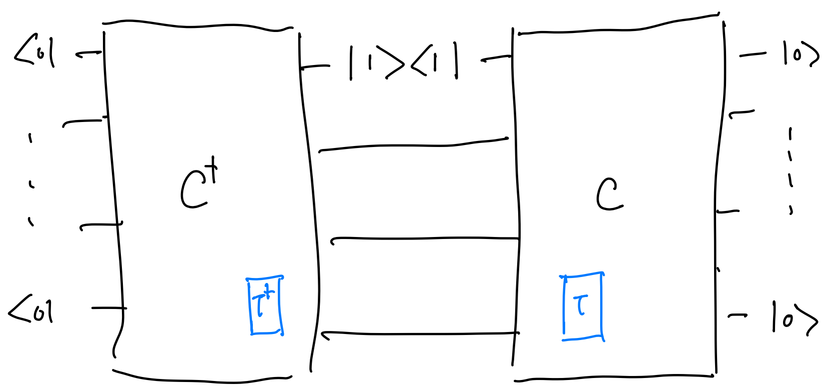
Solovay-Kitaev + Clifford simulation suggests that the number of $T$ gates in a $H, T, CNOT$ circuit should be a measure of the circuits complexity.

**Thm** $\exists$ a constant $\alpha > 0$, s.t. computing the output probability of a quantum circuit consisting of $m$ - Clifford gates, $t$ T-gates on $n$ qubits can be classically computed in time $O(2^{\alpha t} \cdot \mathrm{poly}(n,m))$.

Best: $\alpha < 0.4$ (Qassim-Pashayan-Gosset)

Today $2^{\alpha} = 3$, $\alpha < 1.6$.

Model of such a computation:




↑ one big matrix multiplication:

Replacement :

$$T^\dagger \otimes T = a\, \mathbb{1} \otimes \mathbb{1} + b\, S^\dagger \otimes S + c\, Z^\dagger \otimes Z.$$

$$\begin{pmatrix} 1 & & & \\ & e^{i\pi/4} & & \\ & & e^{-i\pi/4} & \\ & & & 1 \end{pmatrix} = \begin{pmatrix} a & & & \\ & a & & \\ & & a & \\ & & & a \end{pmatrix} + \begin{pmatrix} b & & & \\ & bi & & \\ & & -bi & \\ & & & b \end{pmatrix} + \begin{pmatrix} c & & & \\ & -c & & \\ & & -c & \\ & & & c \end{pmatrix}$$

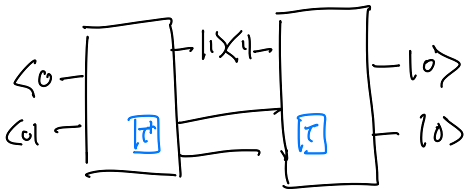
Solve

$$a + b + c = 1 \qquad a = 1/2$$

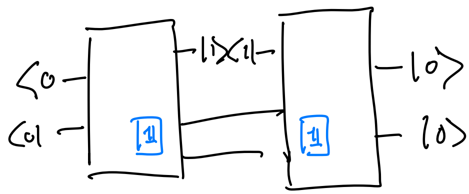
$$a + bi - c = e^{i\pi/4} \qquad b = 1/\sqrt{2}$$

$$a - bi - c = e^{-i\pi/4}. \qquad c = \frac{1}{2} - \frac{1}{\sqrt{2}}.$$

By linearity,

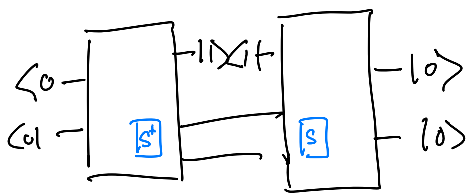



$= a$



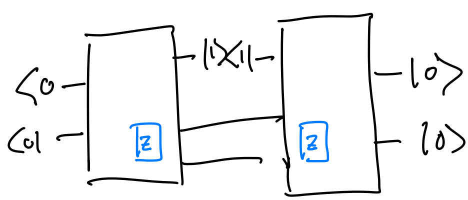

$+$

$b$




$+$

$c$



Apply this replacement recursively for every pair of T gates.

Yields $3^t$ calculations each of which was a only Clifford computation. So previous, subroutine gives an efficient poly$(n, m)$ algorithm.

# Quantum Complexity Theory

In a previous lecture, we defined BQP – the class of decision problems decidable in poly-time by a family of uniform quantum circuits.

Other complexity classes.

P – decision problems solvable by deterministic classical polynomial time computation

BPP – decision problems solvable by randomized classical polynomial time computation

NP – decision problems solvable by non-deterministic classical polynomial time computation

also known as efficiently verifiable decision problems.

interaction-perspective:

Prover

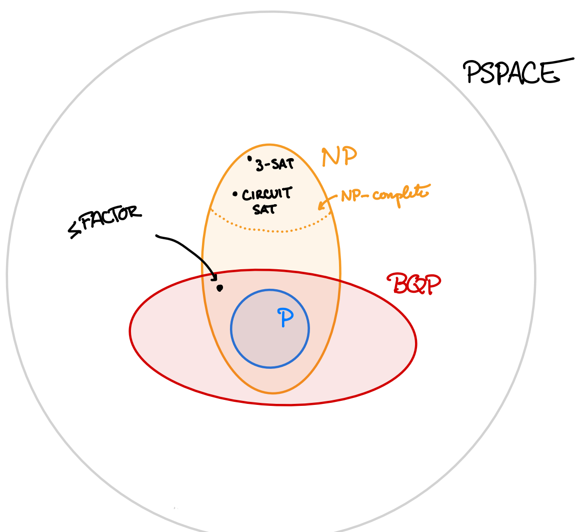
$\downarrow \pi \in \{0,1\}^{poly(n)}$

Verifier

$V(x,\pi)$ poly-time computation.

$x \in \mathcal{L}$ if $\exists\, \pi$ s.t. $V(x,\pi)$ accepts

$x \notin \mathcal{L}$ if $\forall\, \pi$, $V(x,\pi)$ rejects.



$\leq$FACTOR $= \{ \underbrace{(N, K)}_{\text{as binary numbers}} : N$ has a factor $\leq K \}$.

Useful to understand the notion of reductions.

<u>Def</u>. Promise Lang $\mathcal{L}$ poly-time reduces to $\mathcal{L}'$ if

$\exists$ a poly-time algorithm $f : \{0,1\}^* \longrightarrow \{0,1\}^*$ s.t.

(1) $x \in \mathcal{L}_{yes}$ iff $f(x) \in \mathcal{L}'_{yes}$

(2) $x \in \mathcal{L}_{no}$ iff $f(x) \in \mathcal{L}'_{no}$.

<u>Not</u>. $\mathcal{L} \leq \mathcal{L}'$.

"if we can solve $\mathcal{L}'$, then we can solve $\mathcal{L}$". $\mathcal{L}'$ is as hard as $\mathcal{L}$.

<u>Not</u>. A lang $\mathcal{L}'$ is hard for a comp. class $C$ if

$\forall \mathcal{L} \in C$, $\mathcal{L} \leq \mathcal{L}'$.

$\mathcal{L}'$ is $C$-complete if $\mathcal{L}' \in C$ and $\mathcal{L}'$ is $C$-hard.

<u>Ex</u>. 3-SAT is NP-complete

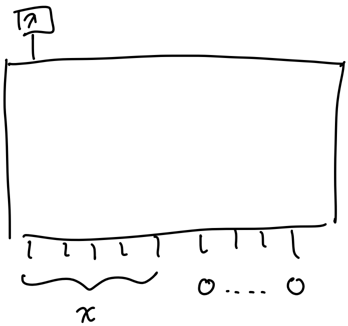
Traveling Salesman is NP-complete.

Ex. $(\leq \text{FACTOR}) \leq (\leq \text{ORDER-FINDING})$

Circuit-sat is NP-complete.

Input: $\langle C \rangle \leftarrow$ classical boolean reversible circuit with some free wires and some fixed ancilla.

Decide if $\exists\, x$ s.t. $C(x)$ accepts.



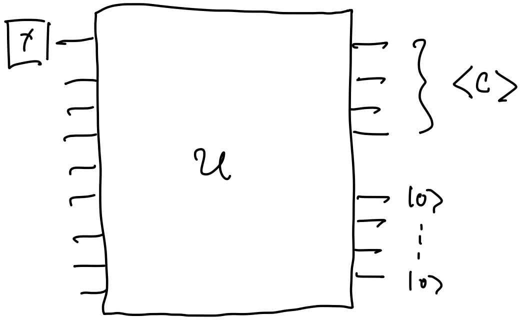

BQP-complete: Input $\langle C \rangle \leftarrow$ quantum circuit

Decide if ① yes: $\| \langle 1 | \otimes \mathbb{1} \, | C | 0^n \rangle \|^2 \geq \frac{2}{3}$

② no: ______ $\leq 1/3$.

"Canonical BQP-complete problem".

Containment $\in$ BQP is because of the notion of a universal quantum circuit.




s.t. pr measurement = 1 is equal to success prob. of C.

$\Rightarrow$ BQP $\subseteq$ PSPACE as we gave a PSPACE alg for this problem.

$$\mathcal{L}_{a,b} = \left\{ \langle C \rangle \text{ s.t. } \begin{array}{ll} p_C \geq a & (\text{yes}) \\ \text{or } p_C \leq b & (\text{no}) \end{array} \right\}$$

where $\| \langle 1 | C | 0^n \rangle \|^2 =: p_c$.

Claim $\mathcal{L}_{a,b} \in$ BQP for $\epsilon := a - b \geq$

Pf. Use Universal q.c. to run Circuit C T times getting outcomes $X_1, \dots, X_T$. wlog assume $a \geq \frac{1}{2}$.

if $\langle C \rangle \in \mathcal{L}_{yes}$ (i.e. $p_c \geq a$), then

$\mathbb{E} X_t \geq a$. So $X = \sum X_t$.

$$\Pr[\mathbb{E}X \le b] = \Pr[X \le (aT) - (\epsilon T)]$$

$$= \Pr[aT - X \ge \epsilon T]$$

$$\le \Pr[aT - X \ge \epsilon a T]$$

$$\le \exp\left(-\frac{\epsilon^2 a T}{3}\right) \le \exp\left(-\frac{\epsilon^2 T}{6}\right)$$

only need error bound of $\le \frac{1}{3}$.

So $T \ge \Omega\left(\frac{1}{\epsilon^2}\right)$.

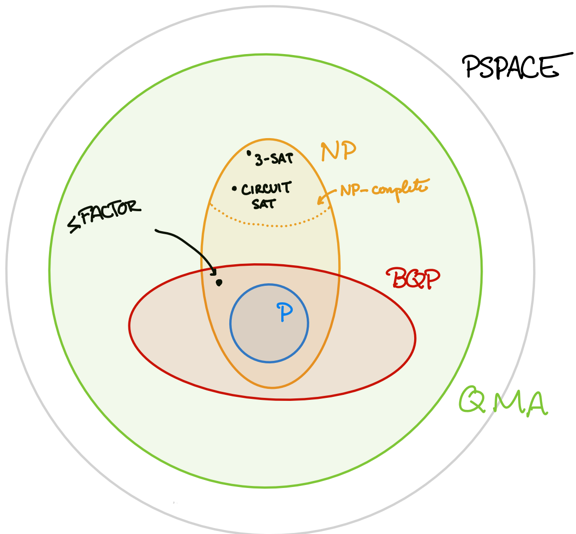
BQP can estimate $p_C$ to accuracy $1/\text{poly}(n)$.

We can also boost success probability to $2^{-p(n)}$ of outputting correct answer by choosing $T \ge \Omega\left(\frac{p(n)}{\epsilon^2}\right)$.

Next: QMA "Quantum Merlin-Arthur"

Easiest to define by complete problem:

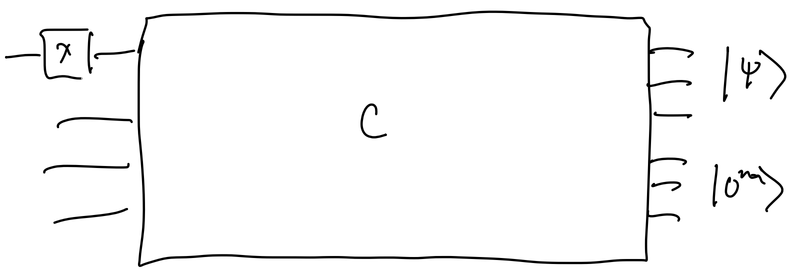
QCIRCUIT-SAT




QCIRCUIT-SAT : $\langle C \rangle$ - q circuit with some inputs fixed to 0.

Decide: if ① $\exists |\psi\rangle$ s.t. $\| \langle 1 | C | \psi, 0^m \rangle \|^2 \geq \frac{2}{3}$

② $\underbrace{\forall |\psi\rangle}_{\text{witness}}$ $\| \langle 1 | C | \psi, 0^m \rangle \|^2 \leq \frac{1}{3}$.




Generalizes circuit-sat & canonical BQP-complete problem.