Single qubit operations

a) Pauli matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

b) Other matrices

Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Phase gate $S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\quad Z = S^2$

$\pi/8$ gate $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$ $\quad S = T^2$

c) Rotation operation

$$R_n(\theta) = e^{-i\theta n \cdot \sigma/2}$$

Decomposing single qubit unitaries

Any $U \in U(\mathbb{C}^2)$ can be written as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Proof

$$U = e^{i\alpha} \underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\text{determinant} = 1} \qquad e^{i\alpha} = \det U.$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\dagger} = \begin{pmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{pmatrix}$$

$$\Rightarrow \quad d = \bar{a} \;\&\; b = -\bar{c}$$

$$U = e^{i\alpha} \underbrace{\begin{pmatrix} a & -\bar{c} \\ c & \bar{a} \end{pmatrix}}_{\det = 1 \Rightarrow |a|^2 + |c|^2 = 1}$$

so $|a| = \cos \gamma/2$ & $|c| = \sin \gamma/2$

$$U = e^{i\alpha} \begin{pmatrix} e^{i\theta} \cos \gamma/2 & -e^{-i\psi} \sin \gamma/2 \\ e^{i\psi} \sin \gamma/2 & e^{-i\theta} \cos \gamma/2 \end{pmatrix}$$

letting $\theta = -(\beta + \delta)/2 \qquad \psi = (\beta - \delta)/2$

$$U = e^{i\alpha} \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix} \begin{pmatrix} \cos \frac{\gamma}{2} & -\sin \frac{\gamma}{2} \\ \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{pmatrix} \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}$$

∎

Cor $U = e^{i\alpha} A \otimes B \otimes C$ where

$A, B, C \in U(\mathbb{C}^2)$ s.t. $ABC = I_{\mathbb{C}^2}$.

proof: Let

$$\begin{cases} A = R_z(\beta) R_y(\gamma/2) \\ B = R_y(-\gamma/2) R_z(-(\delta+\beta)/2) \\ C = R_z((\delta-\beta)/2) \end{cases}$$

a) $ABC = I_{\mathbb{C}^2}$ easy to verify.

b) Observe that $\boxed{XYX = -Y}$.

Therefore

$$X R_y(\theta) X = X\left(\cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y\right) X$$

$$= \cos\frac{\theta}{2} I + i \sin\frac{\theta}{2} Y$$

$$= R_y(-\theta)$$

Similarly $X R_z(\theta) X = R_z(-\theta)$

c) Using (b) we obtain

$$AXBXC = A\left(X R_y(-\gamma/2) \overset{XX}{} R_z(-(\delta+\beta)/2) X\right) C$$

$$= A R_y(\gamma/2) R_z((\delta+\beta)/2) C$$

$$= R_z(\rho)\, \underbrace{R_y(\gamma/2)\, R_y(\gamma/2)}_{R_y(\gamma)}\, \underbrace{R_z((\delta+\rho)/2)\, R_z((\delta-\rho)/2)}_{R_z(\delta)}$$

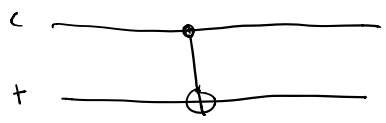
$$= R_z(\rho)\, R_y(\gamma)\, R_z(\delta) \qquad \blacksquare$$

Controlled operations

CNOT-gate

$$\text{CNOT}: \mathbb{C}^2 \otimes \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$$

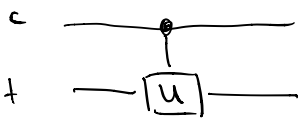
$$|c\rangle|t\rangle \longmapsto |c\rangle|t \oplus c\rangle$$



This is a special case of controlled-U gate

$$C(U): (\mathbb{C}^2)^{\otimes 2} \longrightarrow (\mathbb{C}^2)^{\otimes 2}$$

$$|c\rangle|t\rangle \longmapsto |c\rangle U^c |t\rangle$$

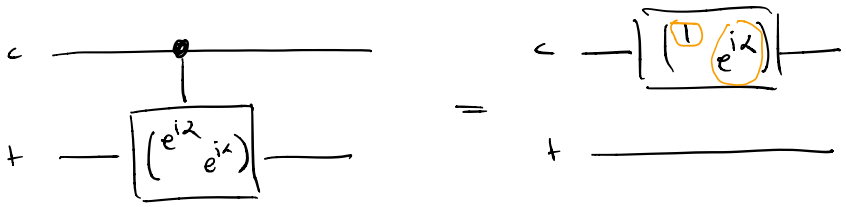


So $\text{CNOT} = C(X)$

Implementation of C(U)

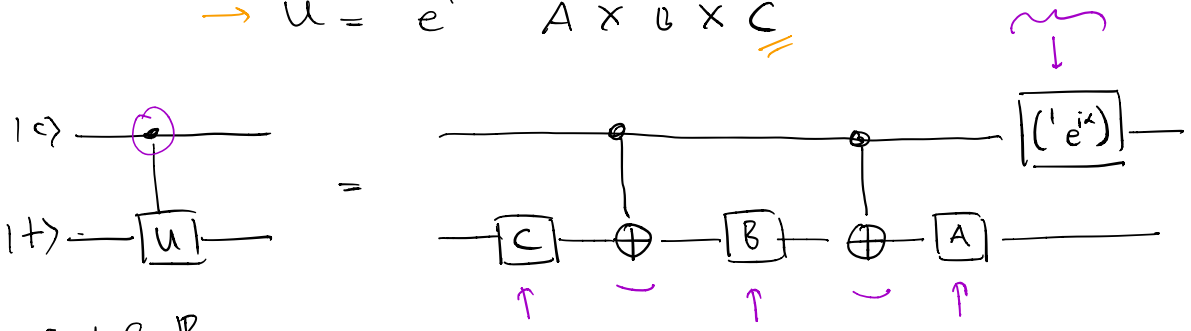
a) Implementing $C(e^{i\alpha} I_{\mathbb{C}^2})$ ← U

$$|c\,t\rangle \mapsto |c\rangle\, e^{i\alpha c}\, |t\rangle$$



b) Implementing C(U) where (Corollary above)

$\rightarrow U = e^{i\alpha} A \times B \times C$



$$e^{i\alpha} A^{c} B^{c} C = \begin{cases} e^{i\alpha} ABC = e^{i\alpha} I_{\mathbb{C}^2} & c = 0 \\ U & c = 1 \end{cases}$$

X : Pauli X-matrix

Multiqubit controlled operations

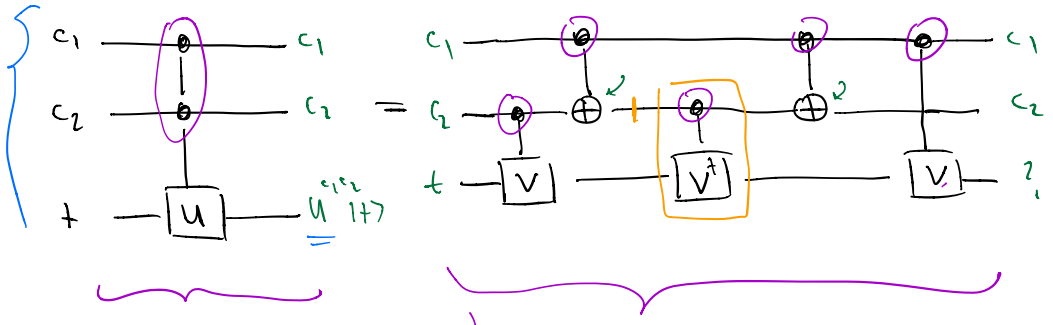
$$C^n(U) : (\mathbb{C}^2)^{\otimes n} \otimes \mathbb{C}^2 \longrightarrow (\mathbb{C}^2)^{\otimes (n+1)}$$

prod. c_i's

$$|c_1 \cdots c_n\rangle |t\rangle \longmapsto |c_1 \cdots c_n\rangle U^{c_1 \cdots c_n} |t\rangle$$

a) Implementing $C^2(U)$

Let $V \in U(\mathbb{C}^2)$ s.t. $V^2 = U$.



$C^2(U)$

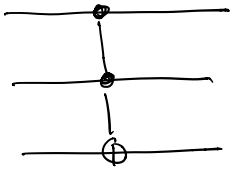
$$|t\rangle \longmapsto V^{c_1} (V^\dagger)^{(c_1 \oplus c_2)} V^{c_2} |t\rangle$$

$$V^{c_1 + c_2 - (c_1 \oplus c_2)}$$

$U^{c_1 c_2}$	$c_1 c_2$	$c_1 + c_2 - (c_1 \oplus c_2)$	$V^{c_1 + c_2 - (c_1 \oplus c_2)}$
I	00	0	I
I	01	$0 + 1 - (0 \oplus 1) = 0$	I
I	10	$1 + 0 - (1 \oplus 0) = 0$	I
U	11	$1 + 1 - (1 \oplus 1) = 2$	$V^2 = U$

(2 under $1+1$, 0 under $1 \oplus 1$)

Ex: Toffoli gate

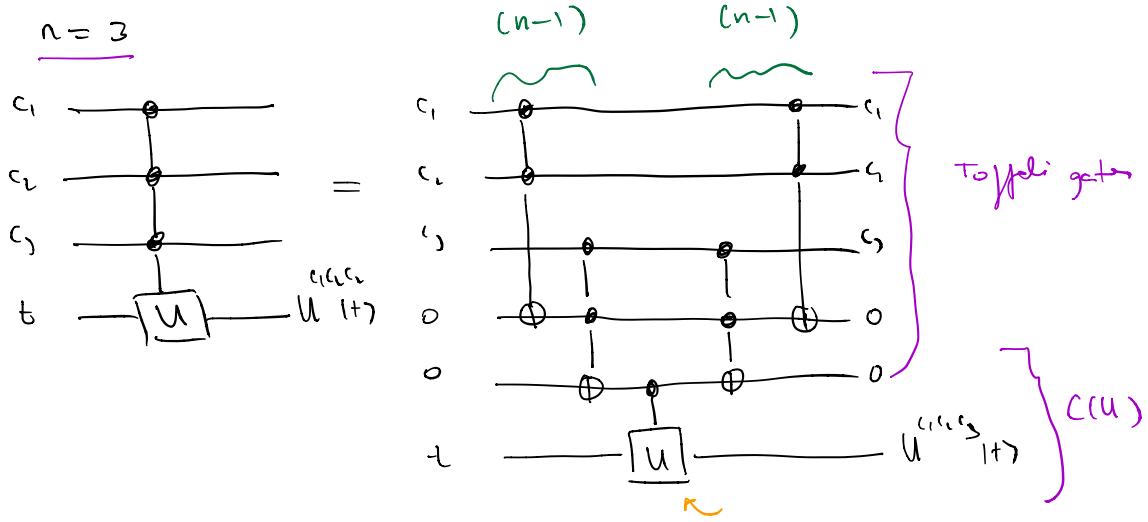


$$V = (1-i)\frac{I + iX}{2}$$

$$V^2 = \frac{-2i}{4}(I + 2iX - I) = X$$

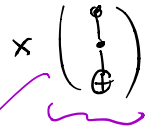
Rem $\{$TOFFOLI$\}$ is universal in classical computation. We see that $\{$single qubit, CNOT$\}$ can be used to implement any classical circuit.

b) Implementing $C^n(U)$



Total number of gates $C^n(U)$

$U(\mathbb{C}^2)$

$2(n-1) \times$  $+ 1 \times$  $= O(n) \times$ CNOTs

$+$

$O(n) \times$ Single Qubits

$= O(n) \times \{$ Single Qubits, CNOT $\}$

12 × Single Qubits + 8 CNOTs

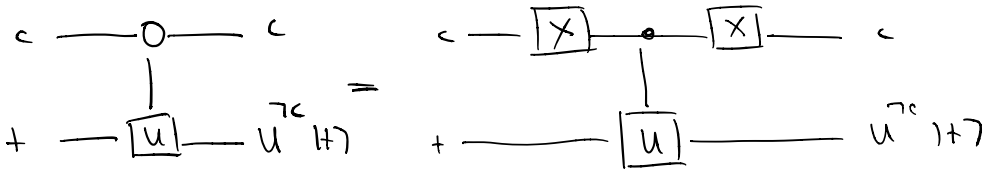
4 × Single Q + 2 CNOTs

2 × CNOT

3 × C(U)

} 12 × Single Q + 6 × CNOTs

Rem



Measurements in circuits

Measurements in the computational basis will be denoted by

a) Other measurements can be obtained by introducing ancilla qubits & applying a unitary:

Let $|\psi\rangle \in V$ & consider $\{M_i\}_{i=1}^m$ arbitrary meas.

1) Introduce $W = \mathbb{C}^m$ & consider $V \otimes W$

2) Define $U : V \otimes W \longrightarrow V \otimes W$ $\quad U(|\psi\rangle|0\rangle)$

by extending

$$|\psi\rangle|0\rangle \longmapsto \sum_{i=1}^{m} M_i|\psi\rangle|0\rangle$$

unit vector since $\sum_{i=1}^{m} M_i^\dagger M_i = I_V$

3) Define projective meas. $\left\{ P_i = I_V \otimes |i\rangle\langle i| \right\}_{i=1}^m$

Then

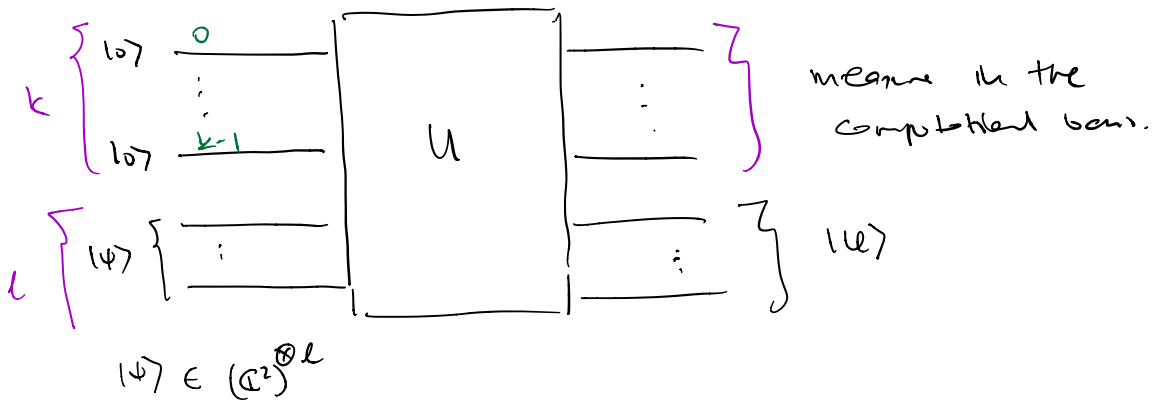
$$p(i) = (\langle\psi|\langle 0|) U^\dagger P_i \otimes I \, U (|0\rangle|\psi\rangle)$$

$$= \langle\psi| M_i^\dagger M_i |\psi\rangle$$

We can construct a circuit:

let $m = \sum_{j=0}^{k-1} b_j 2^j$

$i = \sum_{j=0}^{k-1} d_j 2^j$



$$|\psi\rangle = \frac{M_i|\psi\rangle}{\sqrt{\langle\psi|M_i^\dagger M_i|\psi\rangle}}$$

projector corresponding to $|d_0 d_1 \cdots d_{k-1}\rangle\langle d_0 d_1 \cdots d_{k-1}|$

b) Principle of implicit meas.

Qubits at the end of the circuit can be assumed to be meas.

1) Suppose $\rho \in \mathrm{Den}(V \otimes W)$

2) Consider $\{I_V \otimes P_i\}_{i=1}^m$ where $P_i \in \mathrm{Proj}(W)$

3) If ρ' is the density operator after

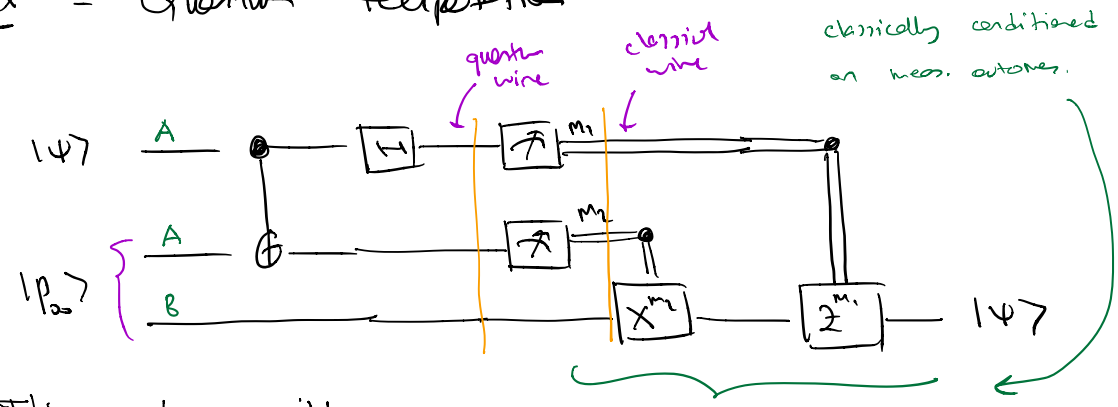
the measurement.

Then $Tr_W(\rho) = Tr_W(\rho')$.

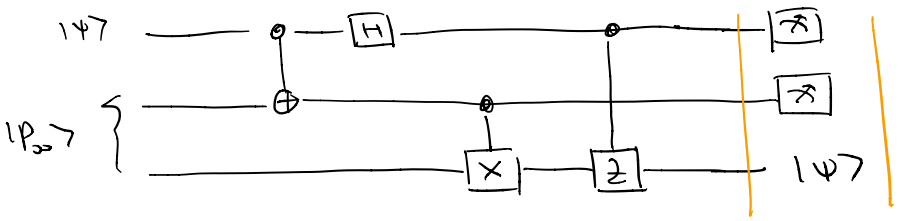
c) Principle of deferred meas.

Measurements can be moved from an intermediate stage to the end of the circuit.

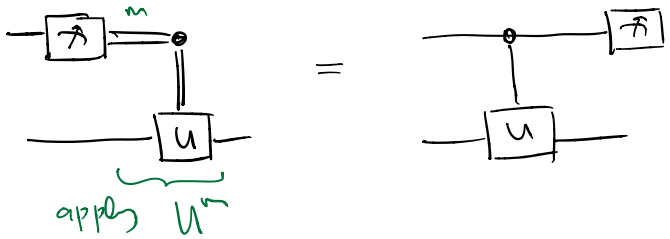
Ex - Quantum teleportation



This can be rewritten as



So the idea is that



Universal quantum gates

A set $\mathcal{A}_Q$ of gates is universal for quantum computation if any unitary operator can be approximated to arbitrary accuracy by a quantum circuit built from $\mathcal{A}_Q$.

Thm: $\mathcal{A}_Q = \{ H, T, CNOT \}$ is universal for quantum computation.

to be more precise.

Lem 1 (Two level unitary gates are universal)

Let $U \in U(V)$ where $V = \mathbb{C}^d$.

There exists a sequence $\{|e_j\rangle\}$

$$\{ U_i \in U(V) \}_{i=1}^{n}$$

such that

1) $\{ 1 \le j \le d \mid U_i |e_j\rangle = |e_j\rangle \}$ has size $\geq d-2$ ← U_i acts on at most two basis vectors non-trivially.

2) $U = U_1 U_2 \cdots U_n$

→ such a unitary is called a two-level unitary.

Proof. Induction on d.

For $d \leq 2$ nothing to prove.

Let $d > 2$.

$$U = \begin{pmatrix} a_{11} & \cdots & a_{1d} \\ \vdots & & \vdots \\ a_{d1} & \cdots & a_{dd} \end{pmatrix}$$

1) Claim: There exists unitaries $U_1, \ldots, U_{d-1}$ such that

$$(U_{d-1} \cdots U_1)U = \begin{pmatrix} a'_{11} & a'_{12} & \cdots & a'_{1d} \\ 0 & a'_{12} & \cdots & \vdots \\ \vdots & \vdots & & \vdots \\ 0 & a'_{d2} & \cdots & a'_{dd} \end{pmatrix}$$

Let $c_1, \ldots, c_d$ denote the colums in

$(U_{d-1} \cdots U_1) U$.

Since this is a unitary

$$\langle c_1 | c_i \rangle = \delta_{1i} \quad \forall\, i = 1, \ldots, d$$

Therefore

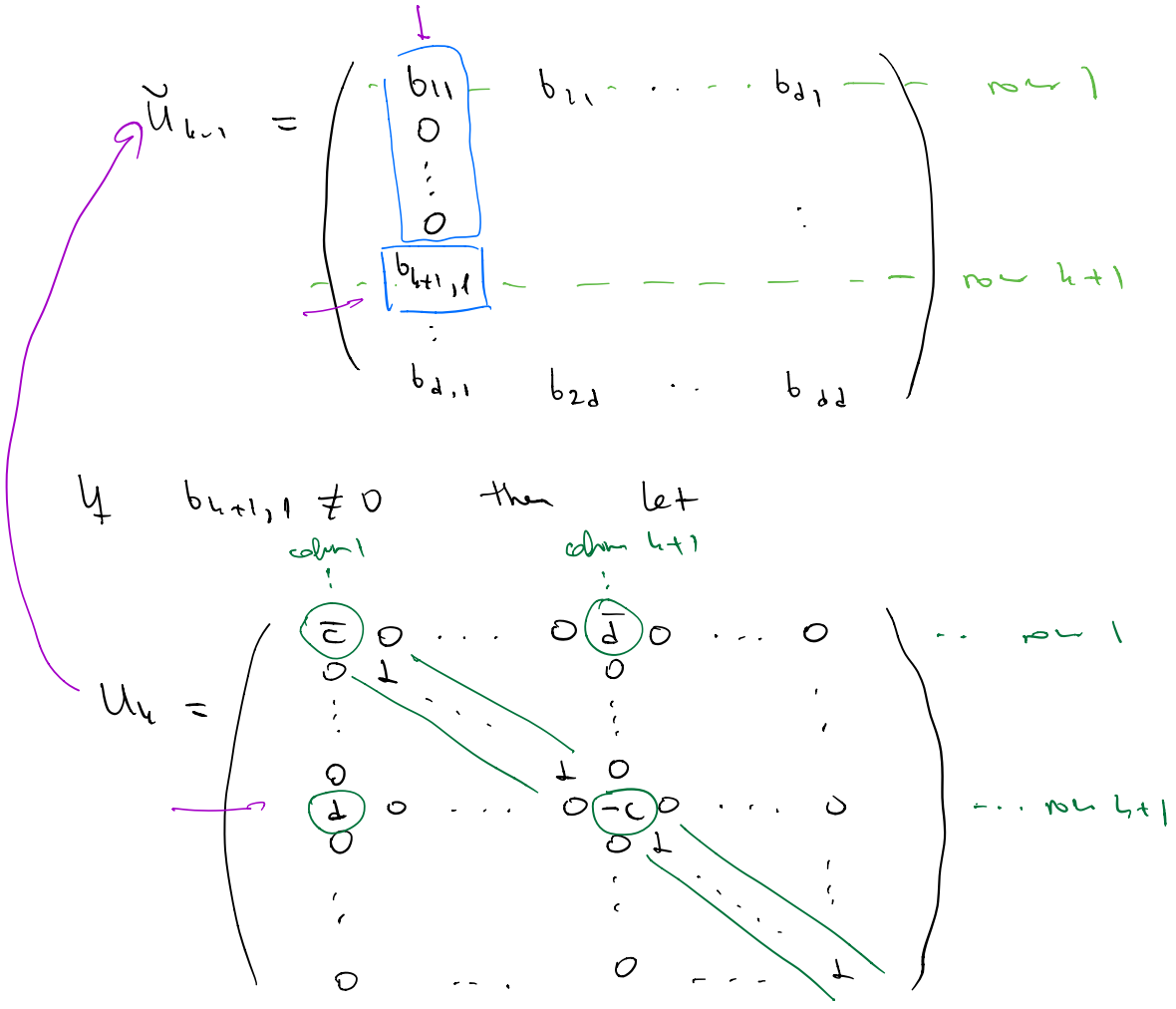
$$a'_{11} = 1 \quad \& \quad a'_{12} = \cdots = a'_{1d} = 0.$$

$$\underbrace{(U_{d-1} \cdots U_1)\, U}_{d-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & \boxed{\text{unitary } \mathbb{C}^{d-1}} & \\ 0 & & & \end{pmatrix}$$

↳ by induction we are done.

2) Proof of the claim in (1).

$$\tilde{U}_{k-1} = (U_{k-1} \cdots U_1)\, U$$



$$c = \frac{b_{11}}{\sqrt{|b_{11}|^2 + |b_{k+1,1}|^2}} \qquad d = \frac{b_{k+1,1}}{\sqrt{|b_{11}|^2 + |b_{k+1,1}|^2}}$$

$\tilde{U}_k = U_k \tilde{U}_{k-1}$ will have

$$(\tilde{U}_k)_{k+1,1} = d\, b_{11} - c\, b_{k+1,1} = 0$$

3) Therefore

$$(U_1^{(d-1)}) \cdots (U_{d-2}^{(2)} \cdots U_1^{(2)})(U_{d-1}^{(1)} \cdots U_1^{(1)})U = I_{C^d}$$

$$U = (U_1^{(d-1)})^\dagger \cdots (U_1^{(2)})^\dagger \cdots U_{d-2}^{(2)\dagger})(U_1^{(1)\dagger} \cdots U_{d-1}^{(1)\dagger})$$

two-level

#two-level unitaries $\leq (d-1) + (d-2) + \cdots + 1$

$= d(d-1)/2$

Implementing two-level unitaries

Let $U \in U((\mathbb{C}^2)^{\otimes n})$ be a two-level unitary matrix acting trivially on the basis vectors except

(computational) $|s_1 \cdots s_n\rangle$ & $|t_1 \cdots t_n\rangle$

where $s_i, t_i \in \mathbb{B}$.

1) Choose a sequence $g_1, \ldots, g_m \in \mathbb{B}^n$ s.t. g_i differs from g_{i-1} by exactly one bit and $g_1 = s_1 \cdots s_n$ and $g_m = t_1 \cdots t_n$

Such a sequence is called a Gray code.

Ex

$g_1 =$ 0 0 0 $(s_1 s_2 s_3)$

$g_2 =$ 0 0 1

$g_3 =$ 0 1 1

$g_4 =$ 1 1 1 $(t_1 t_2 t_3)$

2) Consider the unitary operator $V(G)$

$$|g_1\rangle \mapsto |g_2\rangle \mapsto \cdots \mapsto |g_{m-1}\rangle \mapsto |g_m\rangle$$

and other basis vectors are fixed.

Rem a) This is a permutation $(g_1 g_2) \cdots (g_{m-2} g_{m-1})$

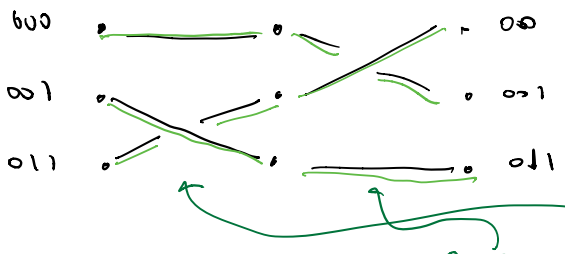
$$\sigma = (g_1 g_2 \cdots g_{m-1})$$

Ex $000 \to 001 \to 011 \to 000$

$$\sigma = (g_1 g_2 g_3)$$

Swap 1) $000 \overset{G_1}{\longleftrightarrow} 001$

2) $001 \overset{G_2}{\longleftrightarrow} 011$



$$(g_1 g_2 g_3) = (g_1 g_2)(g_2 g_3)$$

In general

transposition.

$$(g_1 g_2 \cdots g_{m-1}) = (g_1 g_2)(g_1 g_3) \cdots (g_{m-2} g_{m-1})$$

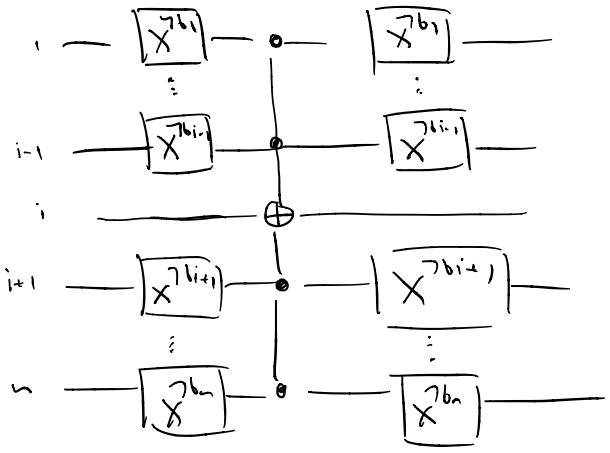
b) For a permutation $\sigma = (g_1 \cdots g_{m-1})$

$$V(g_1 \cdots g_{m-1}) = V(g_1 g_2) V(g_2 g_3) \cdots V(g_{m-2} g_{m-1})$$

We can implement $V(gh)$ when g & h only differs at the i-th location

$g = b_1 \cdots b_i \cdots b_n$ & $h = b_1 \cdots (\neg b_i) \cdots b_n$

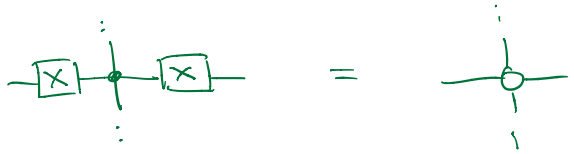
as follows

$C(b_1 \cdots b_n ; i)$ = 

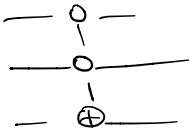
↑ target

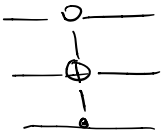
$C^{n-1}(X)$

but target is the i-th qubit

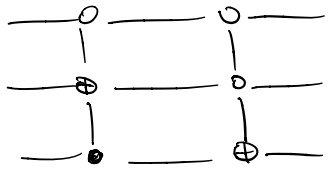
Recall 

Ex $G_1 = (g_1, g_2)$ $G_2 = (g_2, g_3)$

$V(G_1) = C(00; 3) =$ 

$V(G_2) = C(01; 2) =$ 

Let $g = (g_1 g_2 g_3) = \underbrace{(g_1 g_2)}_{G_1} \underbrace{(g_2 g_3)}_{G_2}$

$V(G) = V(G_1) V(G_2) =$ 

3) Recall g_{m-1} & g_m differ at the ith bit:

$$g_{m-1} = b_1 \cdots b_{i-1} \, b_i \, b_{i+1} \cdots b_n$$
$$g_m = b_1 \cdots b_{i-1} \, (\neg b_i) \, b_{i+1} \cdots b_n$$

We have

$$U|s_1 \cdots s_n\rangle = a|s_1 \cdots s_n\rangle + c|t_1 \cdots t_n\rangle$$

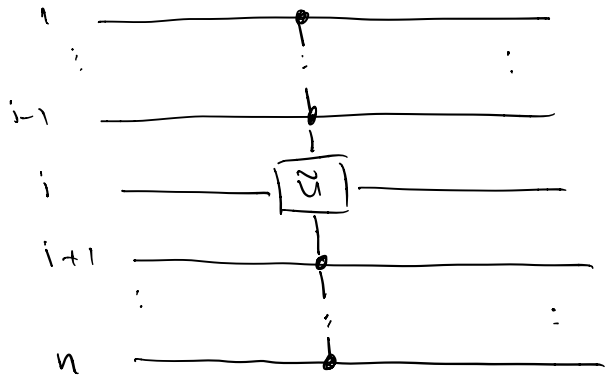
$$U|t_1 \cdots t_n\rangle = b|s_1 \cdots s_n\rangle + d|t_1 \cdots t_n\rangle$$

Let $\tilde{U}$ be the 2×2 unitary defined by

$$\tilde{U}|b_i\rangle = a|b_i\rangle + c|\neg b_i\rangle$$
$$\tilde{U}|\neg b_i\rangle = b|b_i\rangle + d|\neg b_i\rangle$$

and $C_i(\tilde{U})$ denote the controlled operation
(i ← target qubit)

other notation $C^{n-1}_{(i)}(\tilde{U})$



Finally

$$U = V^{\dagger}(G)\; C_i(\tilde{U})\; V(G). \qquad \text{(pg 192 NC)}$$

(elementary)

Total number of gates for two level U

a) $V(G)$ is a product of $n-1$ many operations of the form $C(b_1 \cdots b_n; i)$

\# gates in $C(b_1 \cdots b_n; i)$

$$\underbrace{O(n-1)}_{C^{n-1}_{i(X)}} + \underbrace{2(n-1)}_{\times} = O(n)$$

single Qubit + CNOT

(elementary gates)

\# $V(G)$ requires

$$(n-1)\,O(n) = O(n^2)$$

b) $U = \underbrace{V(G)^{\dagger}}_{O(n^2)}\; \underbrace{C_i(\tilde{U})}_{O(n-1)}\; \underbrace{V(G)}_{O(n^2)}$ requires $O(n^2)$ gates.

Total # of gates for an arbitrary $U \in U((\mathbb{C}^2)^{\otimes n})$

Recall $U = U_k \cdots U_1$ where

U_i two-level & $k \leq \frac{2^n(2^n-1)}{2}$

U requires

$O(4^n) \cdot O(n^2) = O(n^2 4^n)$ gates

Single Qubit + CNOT

We have proved

Thm 2: $\mathcal{A}_Q' = \{ \text{CNOT}, \underbrace{\text{Sig Qubit Gates}}_{U(\mathbb{C}^2)} \}$ is universal for quantum computation

Approximating $U(\mathbb{C}^2)$

For $U, V \in U(\mathbb{C}^2)$ define

$$\underbrace{E(U,V)}_{\text{error}} = \max_{|\psi\rangle} \| (U-V)|\psi\rangle \|$$

U: original unitary; V: implemented unitary

Properties of this quantity

1) Let $\{P_i\}_i$ denote a POVM

$$|p^u(i) - p^v(i)| = |\langle\psi|U^\dagger P_i U|\psi\rangle - \langle\psi|V^\dagger P_i V|\psi\rangle|$$

$$= |\langle\psi|U^\dagger P_i|\varphi\rangle + \langle\varphi|P_i V|\psi\rangle|$$

let $|\varphi\rangle = (U-V)|\psi\rangle$

$$\leq \underbrace{|\langle\psi|U^\dagger P_i|\varphi\rangle|}_{\text{triangle ineq.}} + \underbrace{|\langle\varphi|P_i V|\psi\rangle|}_{\text{similar}} \leq \|\varphi\|$$

$$\leq \underbrace{\|P_i U|\psi\rangle\|}_{\text{CS ineq}} \|\varphi\|$$

≤ 1 since $\sum_i P_i = I_{\mathbb{C}^2}$

$$\leq \|\varphi\| + \|\varphi\| = 2\|\varphi\| \leq 2E(U,V)$$

2) Suppose U_i is implemented by V_i, $i = 1, \ldots, m$.

Then

$$E(U_m \cdots U_1, V_m \cdots V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$$

To see this $(m=2)$

exists by compactness $P(\mathbb{C}^2) = S^2$

$$E(U_2U_1, V_2V_1) = \|(U_2U_1 - V_2V_1)|\psi\rangle\|$$

$$= \|(U_2 - V_2)U_1|\psi\rangle + V_2(U_1 - V_1)|\psi\rangle\|$$

$$\leq \|(U_2 - V_2)U_1|\psi\rangle\| + \|V_2(U_1 - V_1)|\psi\rangle\|$$

triangle ineq

$$\leq E(U_2, V_2) + E(U_1, V_1)$$

Lem 3. Any $U \in U(\mathbb{C}^2)$ can be approximated (to arbitrary accuracy) by $\{H, T\}$.

Proof: 1) Recall that (Correct version of Ex 4.11)

$$U = e^{i\alpha} R_n(\beta_1) R_m(\gamma_1) \cdots R_n(\beta_c) R_m(\gamma_c) \quad (*)$$

for some c (independent of U).

2) Approximating rotations $R_n(\theta) = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}\, n\cdot\sigma$

$$T = e^{i\pi/8} R_z(\pi/4)$$

$$HTH = e^{i\pi/8} R_x(\pi/4)$$

a) Consider

$$T(HTH) = e^{i\pi/4} \left(\cos\tfrac{\pi}{8} I - i \sin\tfrac{\pi}{8} Z\right)\left(\cos\tfrac{\pi}{8} I - i \sin\tfrac{\pi}{8} X\right)$$

$$= e^{i\pi/4} \left(\underbrace{\cos^2\tfrac{\pi}{8}}_{\cos\frac{\theta}{2}} I - i \Big[\underbrace{\cos\tfrac{\pi}{8}(X+Z) + \sin\tfrac{\pi}{8}\, Y}_{(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})\cdot(X,Y,Z)}\Big] \sin\tfrac{\pi}{8}\right)$$

$$V = |v| n$$

$$|v| = \sqrt{\cos^2\tfrac{\pi}{8} + \sin^2\tfrac{\pi}{8} + \cos^2\tfrac{\pi}{8}} = \sqrt{1 + \cos^2\tfrac{\pi}{8}} = \sqrt{\frac{3\sqrt{2}+1}{2\sqrt{2}}}$$

$$\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8} = \frac{1+\cos\pi/4}{2} = \frac{1+1/\sqrt{2}}{2} = \frac{\sqrt{2}+1}{2\sqrt{2}}$$

$$\sin\frac{\theta}{2} = \sqrt{1-\cos^2\frac{\theta}{2}} = \sqrt{1-\frac{3+2\sqrt{2}}{8}} = \sqrt{\frac{5-2\sqrt{2}}{8}} = \frac{\sqrt{5-2\sqrt{2}}}{2\sqrt{2}}$$

↳ same as $\left(\sin\frac{\pi}{8}\right)|v| = \sqrt{\frac{4-2\sqrt{2}}{8}}\sqrt{\frac{2\sqrt{2}+1}{2\sqrt{2}}}$

$$= \frac{1}{2\sqrt{2}}\sqrt{\frac{10\sqrt{2}-8}{2\sqrt{2}}}$$

equal

$= e^{i\pi/4}\boxed{R_n(\theta)}$ where (θ is an irrational multiple of 2π)

1) θ satisfies $\cos\frac{\theta}{2} = \frac{\sqrt{2}+1}{2\sqrt{2}}$

2) $n = \left(\frac{3\sqrt{2}+1}{2\sqrt{2}}\right)^{-1/2}$ $\left(\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8}\right)$

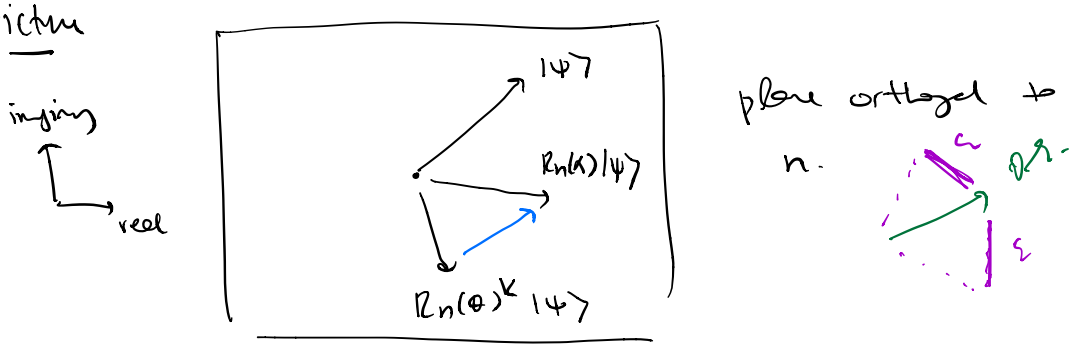
↳ $\cos\frac{\theta}{2} = \cos\frac{\pi}{8} = \frac{1+\cos\pi/4}{2} = \frac{\sqrt{2}+1}{2\sqrt{2}}$

$\sin\frac{\theta}{2} = \frac{\sqrt{5-2\sqrt{2}}}{2\sqrt{2}} = \sin\frac{\pi}{8}\,|v|$

b) Given $R_n(\alpha)$ for some $0 \le \alpha < 2\pi$ and $\varepsilon > 0$ there exists an integer $K > 0$ such that

$$E\left(\underbrace{R_n(\alpha)}_{\text{original}}, \underbrace{R_n(\theta)^K}_{\text{implemented}}\right) < \varepsilon/2c$$

picture



We can think of this plane as $\mathbb{C}$ and rotations both like $e^{i\alpha} \times e^{i K\theta}$

$$E(R_n(\alpha), R_n(\theta)^K) = \underbrace{(R_n(\alpha) - R_n(\theta)^K)}_{e^{i\alpha} - e^{iK\theta}} |\psi\rangle$$

We can make this arbitrarily small when the subgroup $\underbrace{\langle e^{i\theta} \rangle}_{\text{become } \theta \text{ irrational multiple of } 2\pi.}$ in $\underbrace{U(1)}_{\text{subgroups of } U(1) \text{ are either finite or dense in } U(1).}$ is $\underbrace{\text{dense}}_{\text{we can make this arbitrarily small.}}$.

Let $R_n(\alpha) = H R_n(\alpha) H$

Then similarly

$$E(R_n(\alpha), R_n(\theta)^{k'}) < \varepsilon/2c.$$

c) Since U expressed as in $(*)$

$$E(R_n(\beta_1)R_n(\gamma_1)\cdots R_n(\beta_c)R_n(\gamma_c), R_n(\theta)^{k_1} R_n(\theta)^{k_1'} \cdots R_n(\theta)^{k_c} R_n(\theta)^{k_c'})$$

$$\leq \sum_i \underbrace{E(R_n(\beta_i), R_n(\theta)^{k_i})}_{< \varepsilon/2c} + \sum_i \underbrace{E(R_n(\gamma_i), R_n(\theta)^{k_i'})}_{< \varepsilon/2c} < \varepsilon.$$

∎

Combining Lem 1, 2, 3 gives the proof of the universality theorem:

Thm $A_Q = \{H, T, CNOT\}$ is universal for quantum computation

Thm [Solovay–Kitaev] Let $G \subseteq U(2)$ be a finite set of elements (of determinant 1) containing the inverse of each element.

Let

$$G_\ell = \{ g_1 \cdots g_n \mid g_i \in G \text{ & } n \leq \ell \}$$

Given $\varepsilon > 0$ taking $\ell = O(\log^c(1/\varepsilon))$ (where $c \approx 4$) satisfies the property that

for any $U \in U(2)$ there exists $g \in G_\ell$

such that

$$E(U, g) < \varepsilon.$$

We will apply SK thm to $G = \{H, T, H^\dagger, T^\dagger\}$

Consider a circuit C consists of m single qubit & CNOT gates.

Using the additivity of $E(-,-)$ we can see that approximating the circuit C to a precision ε would require

$$O(m \log^c(m/\varepsilon)) \text{ gates from } G.$$

polylogarithmic increase in size of C.

Quantum computational complexity

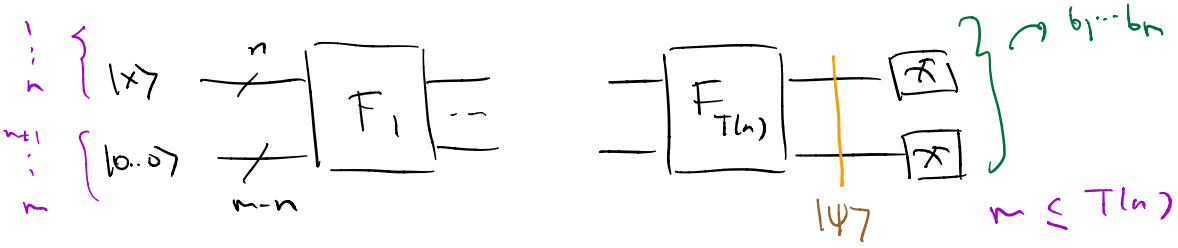
The complexity class BQP

1) Let $T : \mathbb{N} \to \mathbb{N}$ be a function.

A predicate $f : \mathbb{B}^* \to \mathbb{B}$ is computable in quantum $T(n)$-time if there is a (classical det.) TM that outputs a description of the gates

$$F_1, \ldots, F_{T(n)} \in \mathcal{A}_Q = \{H, T, \text{CNOT}\}$$

such that the quantum circuit



outputs $(-1)^{f(x)}$ on the first qubit with probability $\geq 1-\varepsilon$ where $\varepsilon = 1/3$.

Note that identifying $(-1)^b$ with $b \in \mathbb{B}$

$$p(b) = \sum_{b_2, \ldots, b_m} \underbrace{p(b\, b_2 \cdots b_m)}_{|\langle b\, b_2 \cdots b_m | \psi \rangle|^2}$$

The language $L = f^{-1}(1)$ is decidable in quantum $T(n)$-time if f is computable in quantum $T(n)$-time.

2) Bounded-error quantum polynomial time (BQP)

$BQP = \{ L \mid L$ is decided in quantum $q(n)$-time for some polynomial $q \}$

a) Alternate def. for BPP.

$BPP = \{ L \mid \exists$ $q(n)$-time TM V (deterministic) for some polynomial q such that

$$V : \mathbb{B}^* \times \mathbb{B}^m \longrightarrow \mathbb{B} \qquad (m \le q(n))$$

$V(x, w) = f_L(x)$ with probability $\geq 1 - \varepsilon$ when $\varepsilon = 1/3 \}$

(w: witness; f_L: predicate such that $f_L^{-1}(1) = L$)

$$p(b) = \frac{|\{ w \in \mathbb{B}^m \mid V(x, w) = b \}|}{2^m}$$

b) Recall that if $L \in Time(t(n))$ then L has (classical) circuit complexity $O(t(n)^2)$

V can be replaced by a classical circuit of polynomial complexity

Since we can efficiently simulate a classical circuit using a quantum circuit (a) & (b) gives

$$NP \supseteq P \subseteq BPP \subseteq BQP$$

not known how to compare with NP

$BPP \subsetneq BQP$ means quantum computing is more powerful than classical computation.
Shor's algorithm is in favor of $\subsetneq$.
But this challenges the strong CT thesis

$\{L \mid$ decidable by any "algorithmic process"$\}$ $=$ (strong CT) BPP

this includes quantum algorithm too. $\Rightarrow BPP = BQP$ ↑ contradicts to this.

But FACTORING $\in BQP$ (Shor) & FACTORING $\notin BPP$. (belief)

Comparison to classical complexity classes

1) Space complexity

The space complexity of TM M is the function $f: \mathbb{N} \to \mathbb{N}$ defined by

$f(n)$ = maximum # of tape cells M scans on any input of length n.

$SPACE(f(n)) = \{ L \mid$ decided by $O(f(n))$ space det. TM $\}$

There is a non-det. version

$NSPACE(f(n)) = \{ L \mid$ decided by $O(f(n))$ space non-det. TM $\}$

Savitch's thm

$$NSPACE(f(n)) \subseteq SPACE(f(n)^2)$$

We define

$$PSPACE = \bigcup_k SPACE(n^k)$$

$$NPSPACE = \bigcup_k NSPACE(n^k)$$

We have $PSPACE = NPSACE$.

Then

$$P \subseteq NP \subseteq PSPACE = NPSPACE \subseteq EXPTIME$$

$$EXPTIME = \bigcup_k TIME(2^{n^k})$$

2) Comparing to BQP

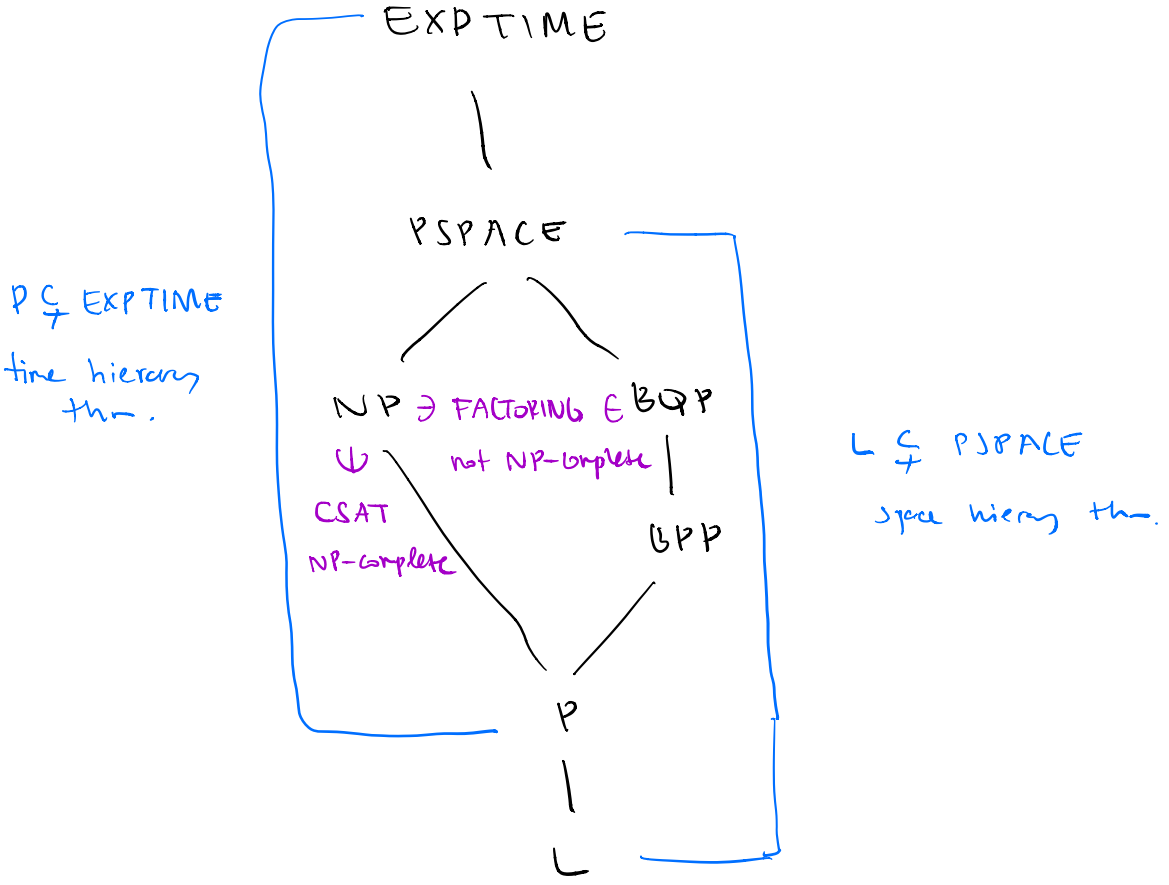
Thm [Bernstein – Vazirani] $BQP \subseteq PSPACE$.

So we have $P \subseteq BPP \subseteq BQP \subseteq PSPACE$.

Therefore if $BPP \subsetneq BQP$ then $BPP \subsetneq PSPACE$.

major open problem in classical cx. theory.

200 of Cx classes



$P \subsetneq EXPTIME$

time hierarchy thm.

$L \subsetneq PSPACE$

space hierarchy thm.

$L = SPACE(\log(n))$