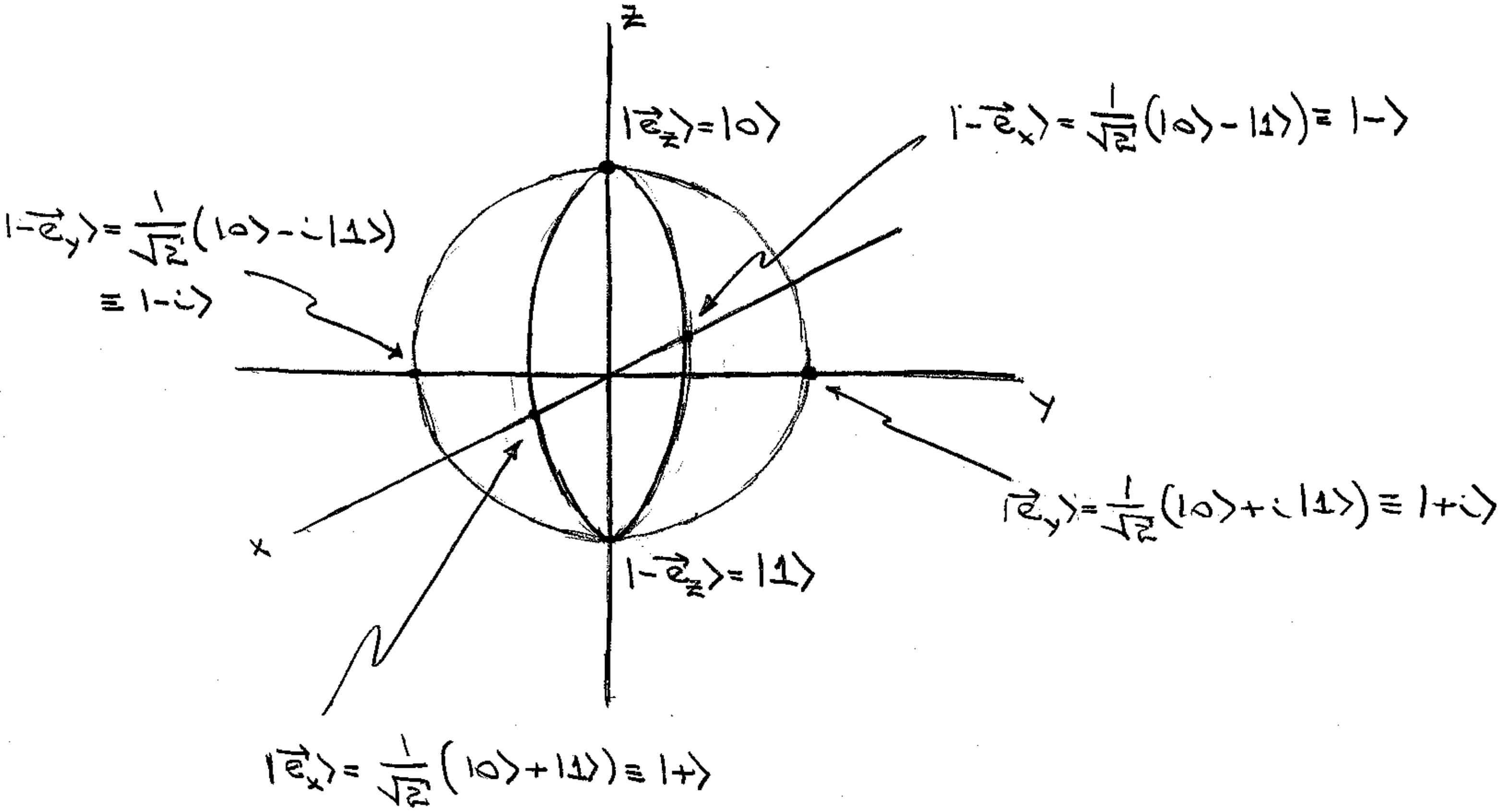
Quantum computation

Lectures 3-5

Quantum gates and controlled operations

Single qubit

States: $|\vec{n}\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle$ $\qquad 0 \le \theta \le \pi$, $\quad 0 \le \phi < 2\pi$



Bloch sphere

Poincare sphere

$Z|\pm\vec{e}_z\rangle = \pm|\pm\vec{e}_z\rangle \qquad Z \leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad Z|a\rangle = (-1)^a|a\rangle$

$X|\pm\vec{e}_x\rangle = \pm|\pm\vec{e}_x\rangle \qquad X \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad X|\pm\rangle = \pm|\pm\rangle$

$Y|\pm\vec{e}_y\rangle = \pm|\pm\vec{e}_y\rangle \qquad Y \leftrightarrow \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Y|\pm i\rangle = \pm|\pm i\rangle$

Pauli operators

$$\vec{\sigma} = \underset{\sigma_x}{\underset{\uparrow}{X}}\vec{e}_x + \underset{\sigma_y}{\underset{\uparrow}{Y}}\vec{e}_y + \underset{\sigma_z}{\underset{\uparrow}{Z}}\vec{e}_z \qquad \vec{\sigma}\cdot\vec{n} = Xn_x + Yn_y + Zn_z$$

$$\vec{\sigma}\cdot\vec{n}\,|\pm\vec{n}\rangle = \pm|\pm\vec{n}\rangle$$

Single qubit

State [illegible] $|1\rangle$

Unitary operators: $\mathcal{U} = e^{i\delta}\, \underbrace{e^{-i\vec{n}\cdot\vec{\sigma}\,\theta/2}}$

$\uparrow$ overall phase $(0 \le \delta < \pi)$

$$\mathcal{U}_R = \mathcal{U}_{\vec{n}}(\theta) = e^{-i\vec{S}\cdot\vec{n}\,\theta/\hbar} = \cos(\theta/2) - i\vec{n}\cdot\vec{\sigma}\sin(\theta/2) = e^{-i\theta/2} \overset{|\vec{n}\rangle\langle\vec{n}|}{P_{\vec{n}}} + e^{+i\theta/2} \overset{|-\vec{n}\rangle\langle-\vec{n}|}{P_{-\vec{n}}}$$

$$\vec{S} = \tfrac{1}{2}\hbar\vec{\sigma} \qquad \longleftrightarrow \qquad \begin{pmatrix} c - in_z s & -(n_y + in_x)s \\ (n_y - in_x)s & c + in_z s \end{pmatrix}$$

$\det \mathcal{U}_R = 1 \qquad \mathcal{U}_R \in SU(2)$

$\det \mathcal{U} = e^{2i\delta} \qquad \mathcal{U} \in U(2)$

$\downarrow$

rotation by θ about $\vec{n}$

$$\mathcal{U}_R^\dagger \vec{\sigma}\, \mathcal{U}_R = R_{\vec{n}}(\theta)\vec{\sigma} = \vec{\sigma}\cdot\vec{n} + \underbrace{(\vec{\sigma} - \vec{n}(\vec{n}\cdot\vec{\sigma}))}_{-\vec{n}\times(\vec{n}\times\vec{\sigma})}\cos\theta + \vec{n}\times\vec{\sigma}\sin\theta$$

$$\mathcal{U}_R^\dagger \vec{\sigma}\cdot\vec{m}\, \mathcal{U}_R = R\vec{\sigma}\cdot\vec{m} = \vec{\sigma}\cdot R^T\vec{m}$$

$$\mathcal{U}_R^\dagger \sigma_j \mathcal{U}_R = \mathcal{U}_R^\dagger \vec{\sigma}\cdot\vec{e}_j\, \mathcal{U}_R = R\vec{\sigma}\cdot\vec{e}_j = \sum_k \sigma_k \underbrace{\vec{e}_j\cdot R\vec{e}_k}_{R_{jk}} = \sum_k R_{jk}\sigma_k$$

rotation of states:

$$\vec{\sigma}\cdot R\vec{m}\; \mathcal{U}_R|\vec{m}\rangle = \mathcal{U}_R \underbrace{\mathcal{U}_R^\dagger \vec{\sigma}\, \mathcal{U}_R \cdot R\vec{m}}_{R\vec{\sigma}\cdot R\vec{m} = \vec{\sigma}\cdot\vec{m}} |\vec{m}\rangle = \mathcal{U}_R|\vec{m}\rangle$$

$$\Longrightarrow \quad \mathcal{U}_R|\vec{m}\rangle = e^{i\phi(R,\vec{m})}|R\vec{m}\rangle$$

$\boxed{\text{Review: see link on web page}}$

Special single qubit gates:

These phases give $H^2 = I$ instead of the -1 associated with a 2π rotation

Hadamard $H = \frac{1}{\sqrt{2}}(X+Z) \longleftrightarrow \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad H^2 = I \quad H = i\exp\left(-i\frac{X+Z}{\sqrt{2}}\frac{\pi}{2}\right)$

$H_{ab} = \frac{1}{\sqrt{2}}(-1)^{ab}, \quad H|b\rangle = \sum_a (-1)^{ab}|a\rangle$ $\quad \uparrow$ 180° rotation about $(\vec{e}_x + \vec{e}_z)/\sqrt{2}$

$X \longleftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad X^2 = I \quad X = i\,e^{-iX\pi/2}$

$X|a\rangle = |\bar{a}\rangle = |1 \oplus a\rangle$ $\quad \uparrow$ 180° rotation about $\vec{e}_x$

$Y \longleftrightarrow \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Y^2 = I \quad Y = i\,e^{-iY\pi/2}$

$\uparrow$ 180° rotation about $\vec{e}_y$

$Z \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad Z^2 = I \quad Z = i\,e^{-iZ\pi/2}$

$Z|a\rangle = (-1)^a|a\rangle$ $\quad \uparrow$ 180° rotation about $\vec{e}_z$

$S \longleftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad S^2 = Z \quad S = e^{i\pi/4}e^{-iZ\pi/4} = \frac{e^{i\pi/4}}{\sqrt{2}}(1 - iZ)$

$\uparrow$ 90° rotation about $\vec{e}_z$

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

$\uparrow$ 45° rotation about $\vec{e}_z$

The overall phase cancels out of the action on operators.

① Action of H: $H\vec{\sigma}H = X\vec{e}_z + Y(-\vec{e}_y) + Z\vec{e}_x$

$$\underset{R\vec{e}_x}{\uparrow} \quad \underset{R\vec{e}_y}{\uparrow} \quad \underset{R\vec{e}_z}{\uparrow}$$

$HXH = Z$

$HYH = -Y$

$HZH = X$

② Action of X: $X\vec{\sigma}X = X\vec{e}_x + Y\vec{e}_y - Z\vec{e}_z$

$XXX = X$

$XYX = -Y$

$XZX = -Z$

$\boxed{\text{Action of } Y, Z}$

Why these phases? What we have done is to redefine a rotation by θ about $\vec{n}$ as $e^{i\theta/2}e^{-i\vec{n}\cdot\vec{\sigma}\theta/2}$, so that $U_{\vec{n}}(2\pi) = +1$, instead of -1.

Are these phases important? Not in single-qubit operations. But they are physical in controlled operations, where this phase is a relative phase determined by physical considerations.

③ Action of S: $S^\dagger \vec{\sigma} S = \underset{\uparrow\, R\vec{e}_x}{X\vec{e}_y} + \underset{\uparrow\, R\vec{e}_y}{Y(-\vec{e}_x)} + Z\vec{e}_z$ $\quad R = R_{\vec{e}_z}(\pi/2)$

$$S^\dagger X S = -Y \qquad\qquad S X S^\dagger = Y \qquad\qquad S^\dagger = S^3$$
$$S^\dagger Y S = X \quad \Longleftrightarrow \quad S Y S^\dagger = -X$$
$$S^\dagger Z S = Z \qquad\qquad S Z S^\dagger = Z$$

For any but 180° rotations, we have to distinguish U and $U^\dagger$.

④ Action of T: $T^\dagger \vec{\sigma} T = X \underbrace{\frac{1}{\sqrt{2}}(\vec{e}_x + \vec{e}_y)}_{R\vec{e}_x} + Y \underbrace{\frac{1}{\sqrt{2}}(-\vec{e}_x + \vec{e}_y)}_{R\vec{e}_y} + \underset{\uparrow\, R\vec{e}_z}{Z\vec{e}_z}$

$R = R_{\vec{e}_z}(\pi/4)$

$$= \frac{1}{\sqrt{2}}(X - Y)\vec{e}_x + \frac{1}{\sqrt{2}}(X + Y)\vec{e}_y + Z\vec{e}_z$$

$$T^\dagger X T = \frac{1}{\sqrt{2}}(X - Y) \qquad\qquad T X T^\dagger = \frac{1}{\sqrt{2}}(+X + Y)$$
$$T^\dagger Y T = \frac{1}{\sqrt{2}}(X + Y) \qquad\qquad T Y T^\dagger = \frac{1}{\sqrt{2}}(-X + Y)$$
$$T^\dagger Z T = Z \qquad\qquad T Z T^\dagger = Z$$

<u>Z-Y decomposition:</u>

$R_\theta(\vec{n}) = R_z(\beta) R_y(\gamma) R_z(\delta)$ for some β, γ, δ

$\uparrow\ \uparrow\ \uparrow$ Euler angles $\longleftarrow$ the standard Euler angles are associated with the Z-X decomposition

$\Updownarrow$

$U_\theta(\vec{n}) = U_z(\beta)\, U_y(\gamma)\, U_z(\delta)$

OR

$U = e^{i\alpha}\, U_z(\beta)\, U_y(\gamma)\, U_z(\delta)$ for some $\alpha, \beta, \gamma, \delta$

Using the $SU(2)$ rep of $SO(3)$ is the easy way to get the Euler angles. The angles in $SU(2)$ were called the Cayley-Klein parameters in the 19th Century.

It is easy to check that the general 2×2 unitary matrix is

$$U = e^{i\alpha} \underbrace{\begin{pmatrix} e^{-i(\beta+\delta)/2}\cos(\gamma/2) & -e^{-i(\beta-\delta)/2}\sin(\gamma/2) \\ e^{+i(\beta-\delta)/2}\sin(\gamma/2) & e^{+i(\beta+\delta)/2}\cos(\gamma/2) \end{pmatrix}}_{\underbrace{\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}}_{U_z(\beta)} \underbrace{\begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix}}_{U_y(\gamma)} \underbrace{\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}}_{U_z(\delta)}}$$

(the $\vec{m}$-$\vec{n}$ decomposition)

There is a comparable decomposition for any orthogonal vectors $\vec{n}$ and $\vec{m}$ (but not for nonorthogonal vectors):

Let R rotate $\vec{e}_z$ to $\vec{n}$ and $\vec{e}_y$ to $\vec{m}$. Then

$$V\vec{\sigma}V^\dagger = R^T\vec{\sigma} \implies \begin{aligned} VZV^\dagger &= R^T\vec{\sigma}\cdot\vec{e}_z = \vec{\sigma}\cdot R\vec{e}_z = \vec{\sigma}\cdot\vec{n} \\ VYV^\dagger &= R^T\vec{\sigma}\cdot\vec{e}_y = \vec{\sigma}\cdot R\vec{e}_y = \vec{\sigma}\cdot\vec{m} \end{aligned}$$

So
$$V\,U_z(\theta)V^\dagger = V e^{-iZ\theta/2}V^\dagger = e^{-i\vec{\sigma}\cdot\vec{n}\,\theta/2} = U_{\vec{n}}(\theta)$$
$$V\,U_y(\phi)V^\dagger = V e^{-iY\phi/2}V^\dagger = e^{-i\vec{\sigma}\cdot\vec{m}\,\phi/2} = U_{\vec{m}}(\phi)$$

Now let

$$V^\dagger U V = e^{i\alpha}U_z(\beta)\,U_y(\gamma)\,U_z(\delta)$$

$$\implies U = e^{i\alpha}U_{\vec{n}}(\beta)\,U_{\vec{m}}(\gamma)\,U_{\vec{n}}(\delta) \quad \text{for some } \alpha, \beta, \gamma, \delta$$

Key result (to be used in breaking down any controlled-U gate into CNOT's and single-qubit operations)

For any qubit unitary U, there exist unitaries U_1, U_2, and U_3, and a phase α such that $U_3 U_2 U_1 = I$ and

$$U = e^{i\alpha} U_3 X U_2 X U_1.$$

Proof: Use the Z-Y decomposition $U = e^{i\alpha} U_z(\beta) U_y(\gamma) U_z(\delta)$, and define

$$U_3 = U_z(\beta)\, U_y(\gamma/2)$$

$$U_2 = U_y(-\gamma/2)\, U_z(-(\delta+\beta)/2) \Rightarrow U_3 U_2 U_1 = I$$

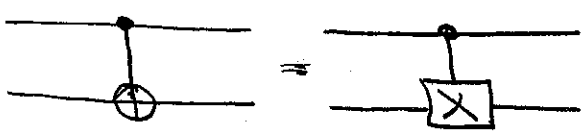
$$U_1 = U_z((\delta-\beta)/2)$$

$$\underset{\substack{\uparrow \\ \text{reverses sign of } Y \text{ and } Z}}{X U_2 X} = U_y(\gamma/2)\, U_z((\delta+\beta)/2) \Rightarrow U_3 X U_2 X U_1 = U_z(\beta) U_y(\gamma) U_z(\delta)$$

$$\Rightarrow U = e^{i\alpha} U_3 X U_2 X U_1$$

Controlled operations: the IFs of the quantum circuit model.

① Two-qubit control:

CNOT 

$P_0 \otimes I + P_1 \otimes X$

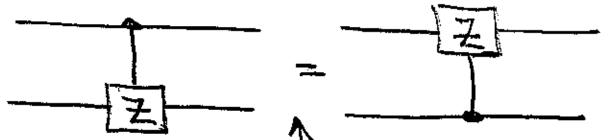
$|00\rangle \rightarrow |00\rangle$
$|01\rangle \rightarrow |01\rangle$
$|10\rangle \rightarrow |11\rangle$
$|11\rangle \rightarrow |10\rangle$

$$|a\rangle \otimes |b\rangle \xrightarrow[\text{CNOT}]{} |a\rangle \otimes \underbrace{|a \oplus b\rangle}_{X^a|b\rangle}$$

XOR stored in target

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

CSIGN:



↑ symmetric in control and target

$P_0 \otimes I + P_1 \otimes Z = I \otimes P_0 + Z \otimes P_1$

$|00\rangle \longrightarrow |00\rangle$
$|01\rangle \longrightarrow |01\rangle$
$|10\rangle \longrightarrow |10\rangle$
$|11\rangle \longrightarrow -|11\rangle$

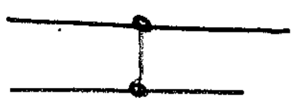
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$|a\rangle \otimes |b\rangle \xrightarrow[\text{CPHASE}]{} |a\rangle \otimes \underbrace{(-1)^{ab}|b\rangle}_{Z^a|b\rangle}$$

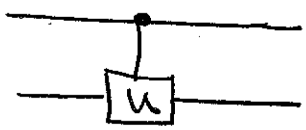
AND stored in phase

This nonclassical operation can store AND in a phase. This is why 2-qubit controls are sufficient for qc, but not for reversible computation.

To recognize its symmetry in control and target, we often write CSIGN as



$C\text{-}U = C^{(1)}(U)$



$P_0 \otimes I + P_1 \otimes U$

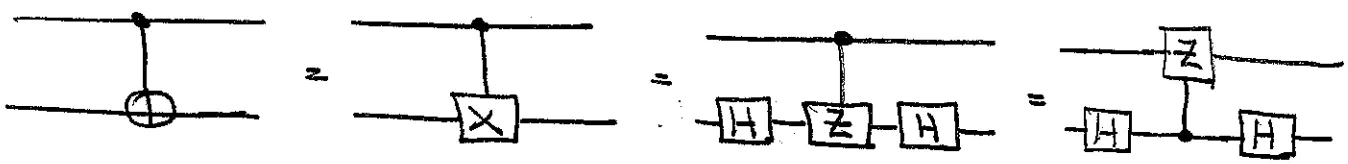
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \multicolumn{2}{c}{\boxed{U}} \\ 0 & 0 & & \end{pmatrix}$$

$$|a\rangle \otimes |b\rangle \xrightarrow[C\text{-}U]{} |a\rangle \otimes U^a|b\rangle$$

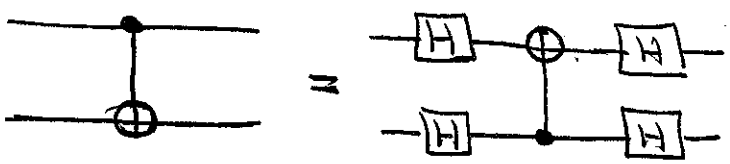
Two applications: $|a\rangle \otimes |b\rangle \longrightarrow |a\rangle \otimes U^{2a}|b\rangle$

↑ not binary arithmetic

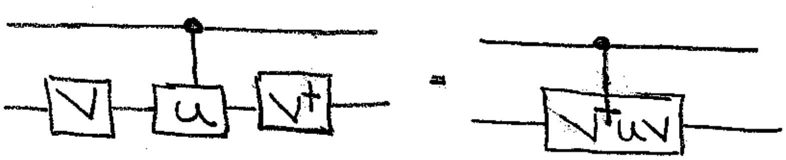
Manipulation:



$$P_0\otimes I + P_1\otimes X = P_0\otimes(P_x+P_{-x}) + P_1\otimes(P_x-P_{-x})$$
$$= (P_0+P_1)\otimes P_x + (P_0-P_1)\otimes P_{-x}$$
$$= I\otimes P_x + Z\otimes P_{-x}$$
$$= (I\otimes H)(I\otimes P_0 + Z\otimes P_1)(I\otimes H)$$

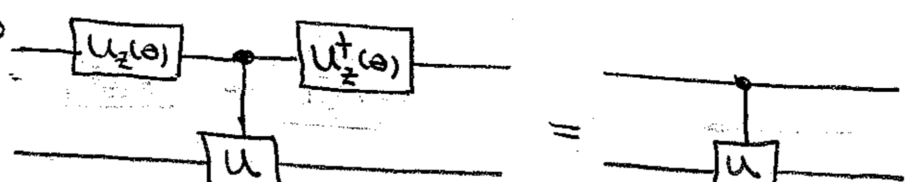


(1)



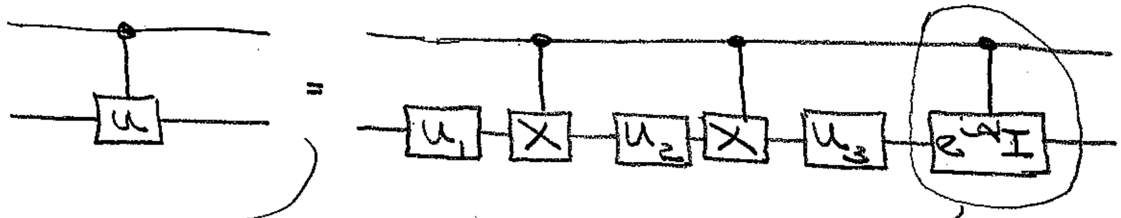
$$(I\otimes V^\dagger)(P_0\otimes I + P_1\otimes U)(I\otimes V) = P_0\otimes I + P_1\otimes V^\dagger U V$$

(2)

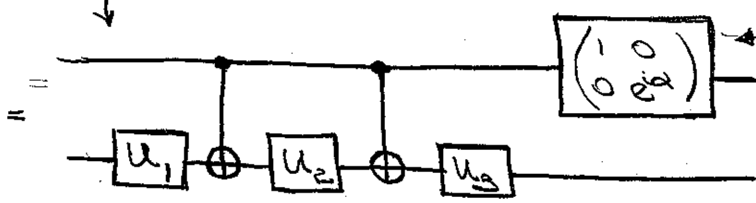


$$(U_z^\dagger(\theta)\otimes I)(P_0\otimes I + P_1\otimes U)(U_z(\theta)\otimes I) = P_0\otimes I + P_1\otimes U$$

2 Generalization of 1 gives us a way to reduce any C-U to CNOTs and single-qubit unitaries:



$U_3 U_2 U_1 = 1$



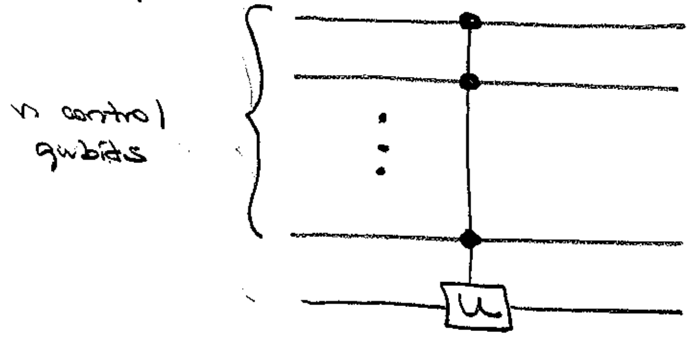
$$P_0 \otimes I + P_1 \otimes e^{i\alpha} I$$
$$= (P_0 + e^{i\alpha} P_1) \otimes I$$
$$= e^{i\alpha/2} e^{-iZ\alpha/2} \otimes I$$

6 gates per C-U.

This isn't a controlled operation at all, but rather a rotation of the control by α about $\vec{e}_z$. The $e^{i\alpha/2}$ is an overall phase that could be removed.

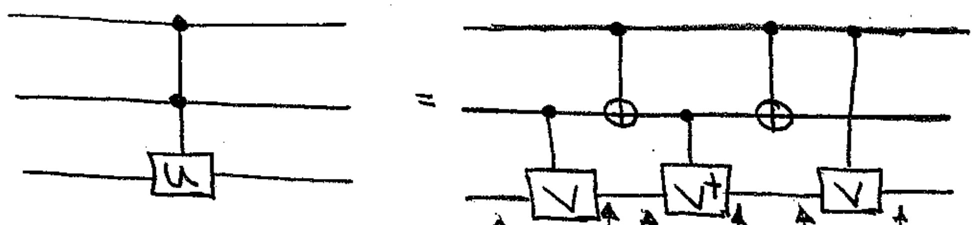
② Multiqubit control

$C^{(n)}(U)$



$$|a_1,\dots,a_n\rangle\otimes|\psi\rangle \longrightarrow |a_1,\dots,a_n\rangle \otimes U^{a_1\cdots a_n}|\psi\rangle$$

Implementing $C^{(2)}(U)$



relies on the identity

$$2ab = a + b - (a\oplus b)$$

AND

quantum mechanics allows square roots of unitaries

Let $U = V^2$

$|a_1,a_2\rangle\otimes|\psi\rangle$

$|a_1,a_2\rangle\otimes V^{a_2}|\psi\rangle$

$|a_1,a_1\oplus a_2\rangle\otimes V^{a_2}|\psi\rangle$

$|a_1,a_1\oplus a_2\rangle\otimes V^{a_2-(a_1\oplus a_2)}|\psi\rangle$

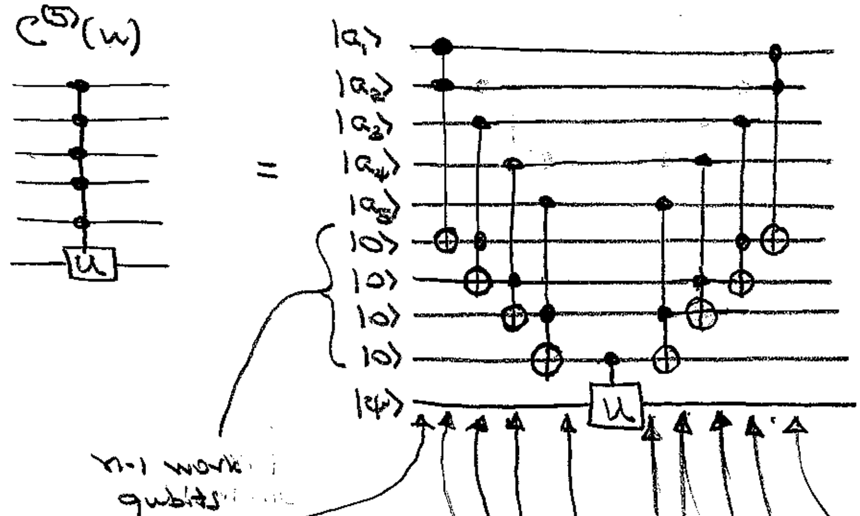
$|a_1,a_2\rangle\otimes V^{a_2-(a_1\oplus a_2)}|\psi\rangle$

$|a_1,a_2\rangle\otimes \underbrace{V^{a_1+a_2-(a_1\oplus a_2)}|\psi\rangle}_{V^{2ab}=U^{ab}}$

$3\times 6 + 2 = \underline{20 \text{ gates}}$ for $C^{(2)}(U)$

This means that the Toffoli gate, $C^{(2)}(X)$, can be reduced to CNOTs and single-bit rotations [$U = X = i e^{-iX\pi/2}$, $V = e^{i\pi/4} e^{-iX\pi/4} = HSH$], so all of reversible classical computation is available to us.

Can we go on to $C^{(n)}(U)$: textbook has a nice example of how to do $C^{(n)}(U)$ efficiently using Toffoli gates, with $C^{(5)}(U)$ as an example:



$|a_1,\dots,a_5\rangle|0\rangle|0\rangle|0\rangle|0\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

$|a_1,\dots,a_5\rangle|0\rangle|0\rangle|0\rangle|0\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

$|a_1,\dots,a_5\rangle|0\rangle|0\rangle|0\rangle|0\rangle|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|0\rangle|0\rangle|0\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|0\rangle|0\rangle|0\rangle|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|0\rangle|0\rangle|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|0\rangle|0\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

$$\begin{pmatrix}\#\text{ of}\\ \text{gates}\end{pmatrix} = \underbrace{2(n-1)}_{\#\text{ of Toffoli's}}\,20 + 6$$

gates per Toffoli

$C^{(1)}(U)$

$= 40n - 34$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|a_1a_2a_3a_4\rangle|0\rangle|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|a_1a_2a_3a_4\rangle|a_1a_2a_3a_4a_5\rangle|\psi\rangle$

There is a more efficient way to do this, in $O(\log n)$ gates, by dividing the product successively into two parts.

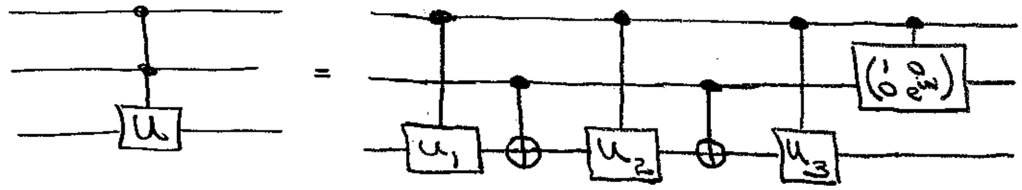
$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|a_1a_2a_3a_4\rangle|0\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

$|a_1,\dots,a_5\rangle|a_1a_2\rangle|a_1a_2a_3\rangle|a_1a_2a_3a_4\rangle|a_1a_2a_3a_4a_5\rangle U^{a_1a_2a_3a_4a_5}|\psi\rangle$

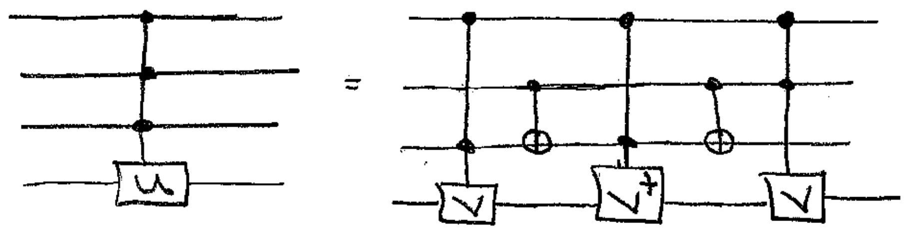
We're really finished at this point. The remaining Toffoli's simply return the work bits to their initial state.

Notice that another way to make higher-order controlled gates is simply to add controls to lower-order gates:

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



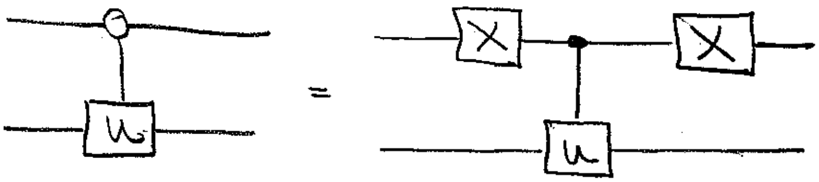
$C^{(3)}(U)$



But it is not hard to convince oneself that when the new controlled gates are reduced by this method to CNOTs and single-bit rotations, the total number of gates is exponential in n. Thus, although this is a quick-and-dirty way to get higher-order controlled gates, it is not efficient.

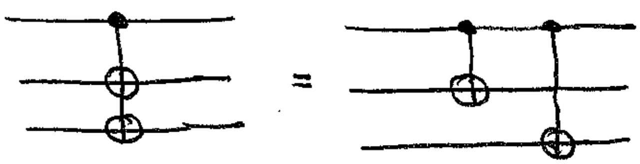
We now have an efficient $[O(\log n)]$ way to break down $C^{(n)}(U)$ into CNOTs and single-qubit rotations.

Control on 0, instead of 1:



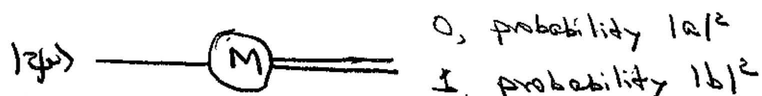
$$P_0 \otimes U + P_1 \otimes I = (X \otimes I)(P_0 \otimes I + P_1 \otimes U)(X \otimes I)$$

Multiple targets:



$$P_0 \otimes I \otimes I + P_1 \otimes X \otimes X = (P_0 \otimes I \otimes I + P_1 \otimes I \otimes X)(P_0 \otimes I \otimes I + P_1 \otimes X \otimes I)$$

Measurement:



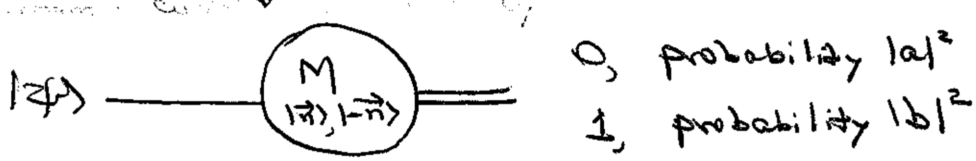
$|\psi\rangle = a|0\rangle + b|1\rangle$

① Measurement in another basis $U|a\rangle$, $U|0\rangle = |\vec{n}\rangle$, $U|1\rangle = |-\vec{n}\rangle$

$|\psi\rangle = a|\vec{n}\rangle + b|-\vec{n}\rangle$

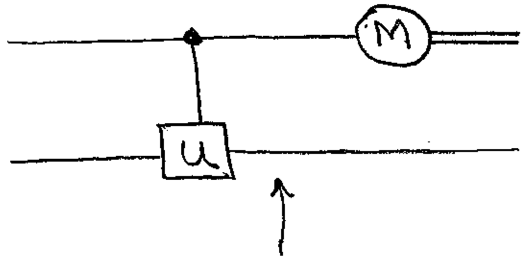
$aU^\dagger|\vec{n}\rangle + bU^\dagger|-\vec{n}\rangle = a|0\rangle + b|1\rangle$

$\Updownarrow$



② Quantum control followed by measurement is equivalent to measurement followed by classical control.

$$|\Psi\rangle = \sum_{a,b} c_{ab}|a,b\rangle$$



a, probability $p_a = \sum_b |c_{ab}|^2$

$a=0$: $p_0 = |c_{00}|^2 + |c_{01}|^2$

$|\psi_0\rangle = (c_{00}|0\rangle + c_{01}|1\rangle)/\sqrt{p_0}$

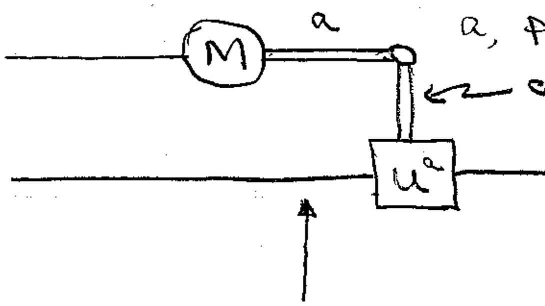
$a=1$: $p_1 = |c_{10}|^2 + |c_{11}|^2$

$|\psi_1\rangle = U(c_{10}|0\rangle + c_{11}|1\rangle)/\sqrt{p_1}$

$$\sum_{a,b} c_{ab}|a\rangle \otimes U^a|b\rangle$$

$$\Updownarrow$$

$$|\Psi\rangle = \sum_{a,b} c_{ab}|a,b\rangle$$



a, probability $p_a = \sum_b |c_{ab}|^2$

classical control

$a=0$: $|\psi_0\rangle = (c_{00}|0\rangle + c_{01}|1\rangle)/\sqrt{p_0}$

$a=1$: $|\psi_1\rangle = U(c_{10}|0\rangle + c_{11}|1\rangle)/\sqrt{p_1}$

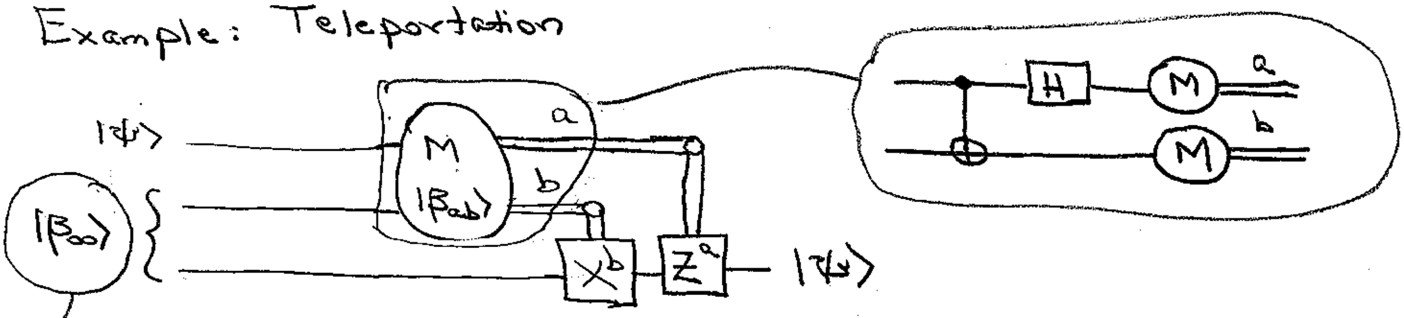
$a=0$: $p_0 = |c_{00}|^2 + |c_{11}|^2$

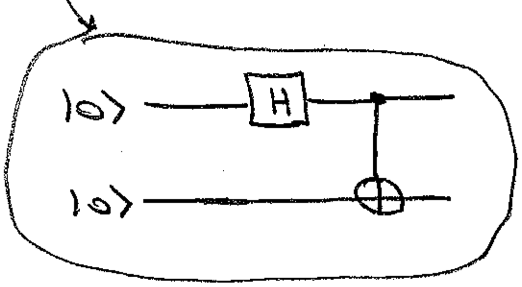
$|\psi_0\rangle = (c_{00}|0\rangle + c_{01}|1\rangle)/\sqrt{p_0}$

$a=1$: $p_1 = |c_{10}|^2 + |c_{11}|^2$

$|\psi_1\rangle = (c_{10}|0\rangle + c_{11}|1\rangle)/\sqrt{p_1}$

Example: Teleportation

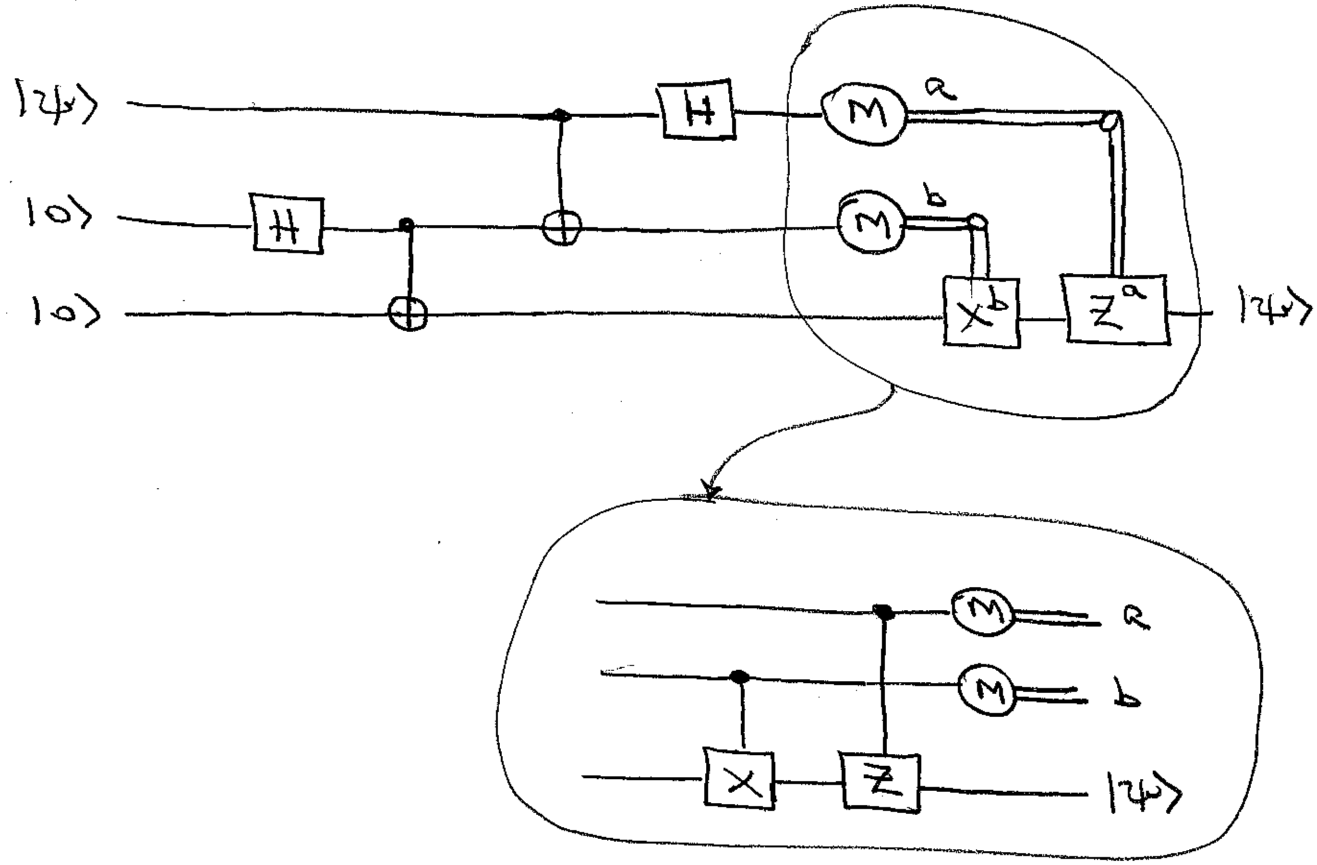




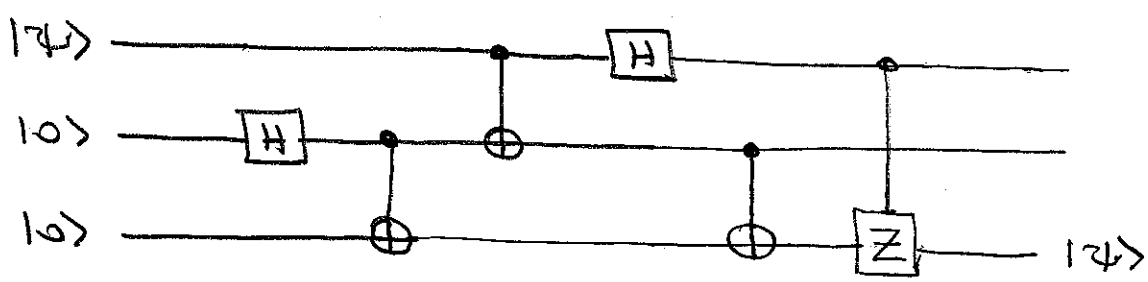
$$|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}\left(|0b\rangle + (-1)^a|1\bar{b}\rangle\right)$$

phase bit

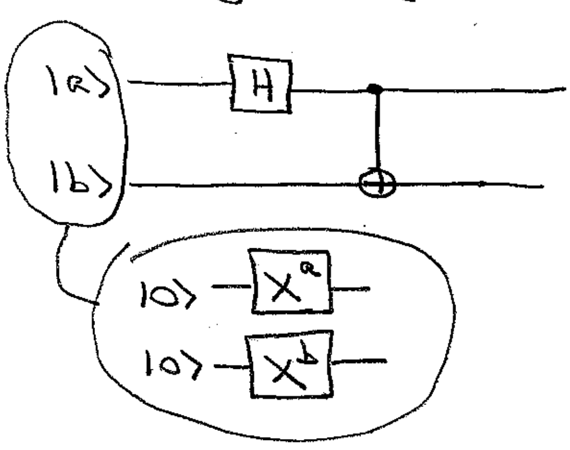
parity bit



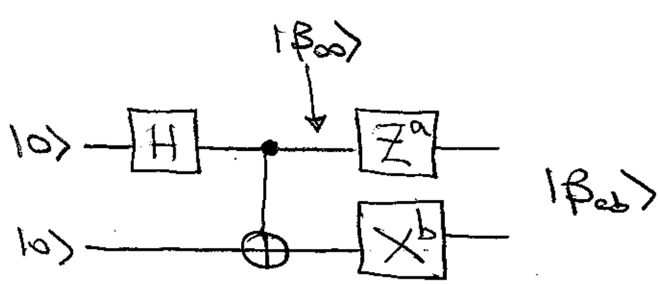
We can now omit the measurements, leaving us with the reversible teleportation circuit:



② Making entanglement

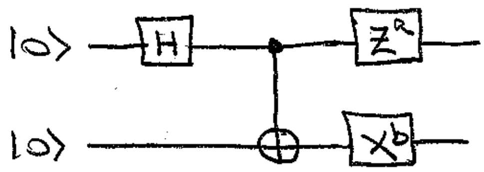


$|\beta_{ab}\rangle =$

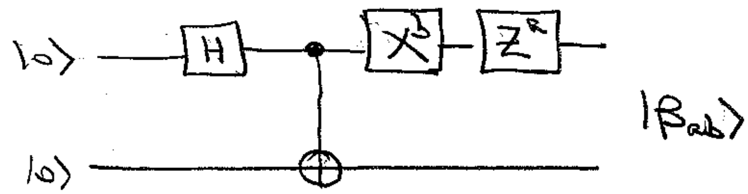


Use $1 \otimes A|\beta_{00}\rangle = A^T \otimes 1\,|\beta_{00}\rangle$ to move the Z^a or X^b.

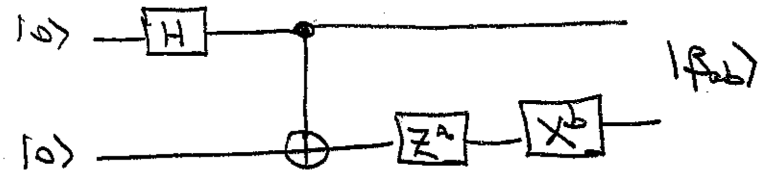
Superdense coding



$|\beta_{ab}\rangle =$



$=$



$|\beta_{ab}\rangle = (\mathbb{1} \otimes Z^a)(\mathbb{1} \otimes X^b)|\beta_{00}\rangle$

$= Z^a X^b \otimes \mathbb{1} \, |\beta_{00}\rangle$

$= \mathbb{1} \otimes X^b Z^a \, |\beta_{00}\rangle$

Summary:

① Any $C^{(1)}(U)$ can be reduced to CNOTs and single-qubit rotations, requiring $O(1)$ elementary gates.

② Any $C^{(2)}(U)$, including $C^{(2)}(X)$ (Toffoli), can be reduced to CNOTs and single-qubit rotations, requiring $O(1)$ elementary gates. (This gives all of reversible classical computation.)

③ Any $C^{(n)}(U)$ can be reduced to CNOTs and single-qubit rotations, requiring $O(\log n)$ elementary gates.
