Lec 9, 1 Oct 2020

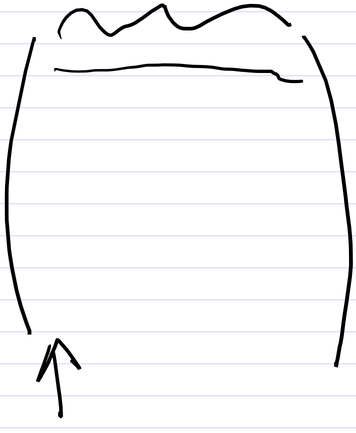
$a = (0\ 0\ 1)$

$$y = \left.\begin{matrix} (0,0,0) \\ (0\ 1\ 0) \\ (1\ 0\ 0) \\ (1\ 1\ 0) \end{matrix}\right\}$$

Appendix G for details of argument for why $n+\alpha$:

$n-1$ columns = basis for $(n-1)$-dim orthog space

$n+\alpha$ rows



a value of y in each row

probability they're not linearly dependent

$$\left(1 - \frac{1}{2^{n+\alpha}}\right)$$

← probability that 1st column not all zero

$$\cdot \left(1 - \frac{1}{2^{n+\alpha+1}}\right)$$

← probability that 2nd column $\neq 0$ and also not first column

$$\vdots$$

$$\left(1 - \frac{1}{2^{\alpha+2}}\right)$$

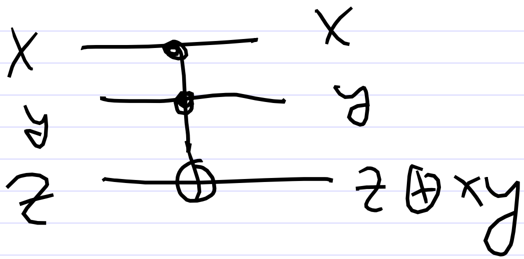
← also not lin. comb. of first $n+\alpha-1$ columns

$$\text{product} > 1 - \frac{1}{2^{\alpha+1}}$$

$$\alpha = 20 \qquad > 1 - 10^{-6}$$

i.e. high probability of enough linearly independent y values to determine a

Toffoli



Classically can't create from 1,2 Cbit gates since

$(110) \leftrightarrow (111)$

is an odd permutation

QM. Two ways to be given here:

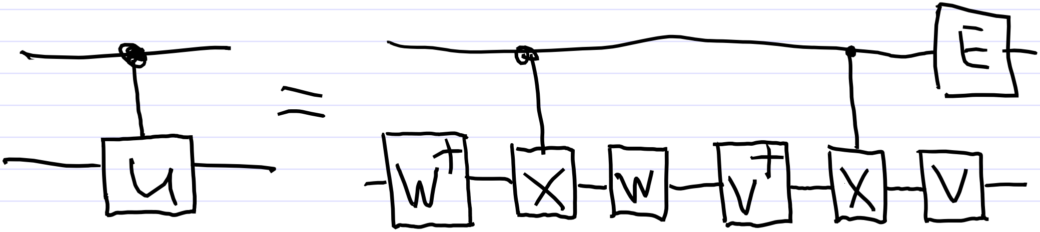
I. first method

needs a) C^{U} (uses 2 CNOTs)

and then b) $C^{U^2}|x_2\, x_1\, x_0\rangle$

$$= U_0^{2x_1x_2}|x_2\, x_1\, x_0\rangle$$

a)



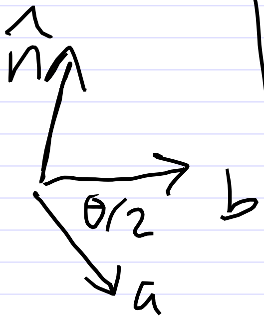
$$U = VXV^\dagger WXW^\dagger$$

$$VXV^\dagger = \vec{a}\cdot\vec{\sigma} \qquad WXW^\dagger = \vec{b}\cdot\vec{\sigma}$$

$$X = \hat{x}\cdot\vec{\sigma}$$

$$U = (\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = \vec{a}\cdot\vec{b}\,\mathbb{1} + i(\vec{a}\times\vec{b})\cdot\vec{\sigma}$$

can always pick a, b:



$$= e^{i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}}$$

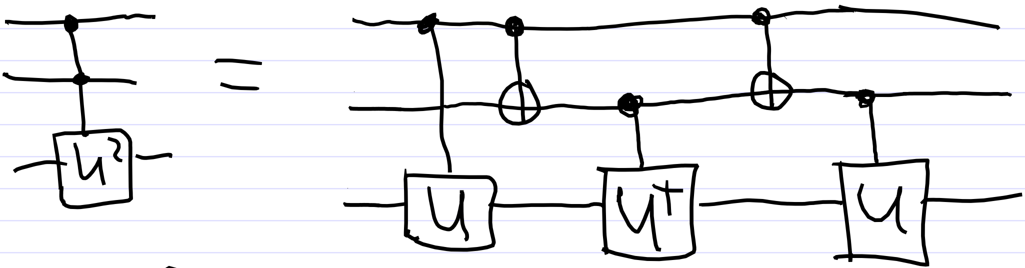
$$= \cos\frac{\theta}{2}\mathbb{1} + i\hat{n}\cdot\vec{\sigma}\sin\frac{\theta}{2}$$

to produce desired $\hat{n}, \theta$, hence U.

then $E = \begin{pmatrix} 1 & \\ & e^{i\alpha} \end{pmatrix}$ adjusts phase b)

11	=		-	U^2
01		-	=	1
10	-	-		1
00				1

need



total of $3 \cdot 2 + 2 = 8$ CNOTs

$U^2 = X \qquad U = \sqrt{X}$

$\sqrt{Z} = \begin{pmatrix} 1 & \\ & i \end{pmatrix} \qquad H\sqrt{Z}H = \sqrt{X}$

$(H\sqrt{Z}H)^2 = H\sqrt{Z}H^2\sqrt{Z}H$

$= HZH = X$

multiply

$H\sqrt{Z}H = e^{i\pi/4}(1 - iX)/\sqrt{2}$

in 1^{st} probset, we saw:

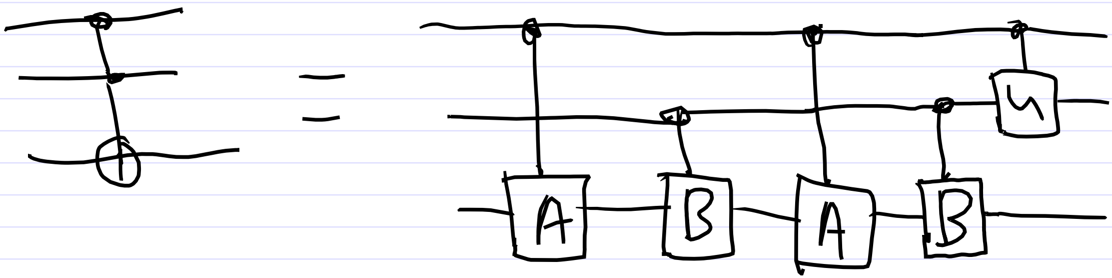
$$u(\vec{x}, \pi/2) = \frac{1}{\sqrt{2}}(1 + iX)/\sqrt{2}$$

$$(\quad)^2 = \frac{1}{2}(1 + 2iX - 1) = iX$$
$$= u(\vec{x}, \pi)$$

Here, with the phase have

$$\left(\sqrt{X}\right)^2 = \left(e^{i\pi/4}\frac{(1 - iX)}{\sqrt{2}}\right)^2 = i(-iX)$$
$$= X$$

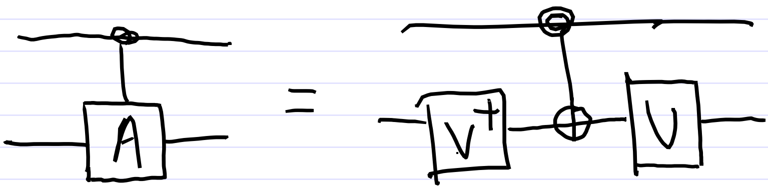
II. second method (6 CNOT)



$\begin{smallmatrix}1\\0\end{smallmatrix}$ gives $A^2 = 1$

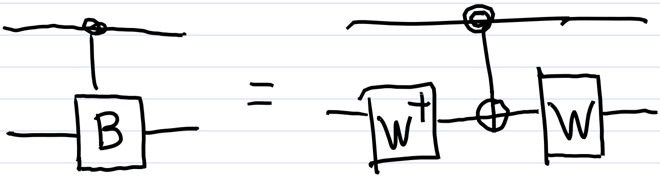
$\begin{smallmatrix}0\\1\end{smallmatrix}$ gives $B^2 = 1$

$\begin{smallmatrix}1\\1\end{smallmatrix}$ $u(BA)^2 = X$



$A = VXV^\dagger$, $A^2 = VX(V^\dagger V)XV^\dagger = VX^2V^\dagger$

$= VV^\dagger = 1$



$B = WXW^\dagger$ $B^2 = 1$

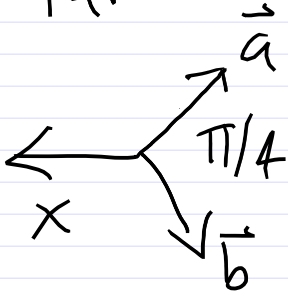
$$(BA)^2 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}\,\vec{x}\cdot\vec{\sigma} = iX$$

$$BA = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\,\sigma_x$$

$$= \frac{1}{\sqrt{2}}\left(1 + i\sigma_x\right)$$

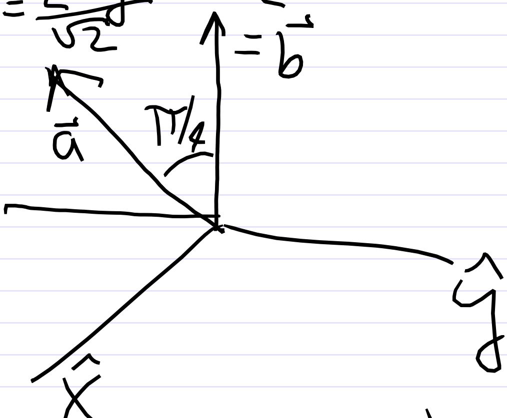
$$BA = (\vec{b}\cdot\vec{\sigma})(\vec{a}\cdot\vec{\sigma}) = \vec{a}\cdot\vec{b}\,\mathbb{1} + i(\vec{b}\times\vec{a})\cdot\vec{\sigma}$$

take



e.g.

$\vec{a} = \frac{\hat{z}-\hat{y}}{\sqrt{2}}$



$$U = \begin{pmatrix} 1 & \\ & e^{-i\pi/2} \end{pmatrix} \qquad (-i)(iX) = X$$

"double-controlled $-i$" corrects this