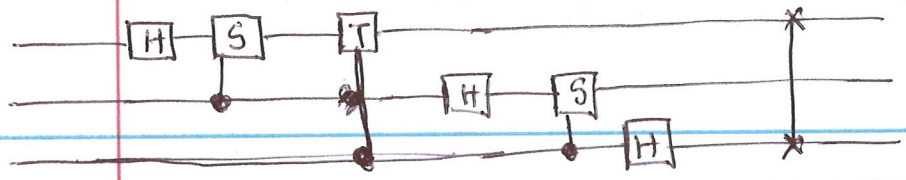
e.g. Circuit for QFT on 3 qubits.



(*)

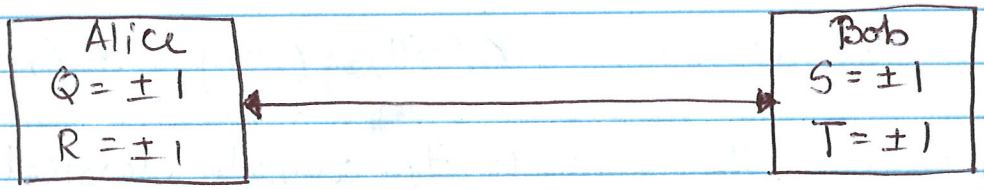
[Ex: Implement controlled S, controlled T using CNOT & single qubit gates].

>>> Di-Vincenzo's Criteria

1. A scalable physical system with well characterized qubit.
2. Ability to initialize the state of the qubits to a simple fiducial state ($|10\cdots0\rangle$).
3. Long relevant decoherence times.
4. A "universal set" of quantum gates.
5. A qubit specific measurement capability.

[Ex: Read about Di-Vincenzo's criteria on wikipedia].

>>> Bell's Inequality



— Charlie prepares two particles, & sends one particle to Alice, & other to Bob. (Charlie should be able to ~~prepare identical copies~~). repeat experimental procedure).

— Alice, after receiving particle, performs measurement on it
- P_Q, P_R are two physical properties
- P_Q has value $Q \in \{1,-1\}$
- P_R has value $R \in \{1,-1\}$
- Alice uses a random method to decide if she will measure P_Q or P_R

Q, R are objective properties which are merely revealed by expt

— Bob similarly measures
- P_S or P_T with values $S, T \in \{1,-1\}$ respectively.

Classical scenario

$$QS + RS + RT - QT = (Q+R)S + (R-Q)T = \pm 2$$

$$\Rightarrow \mathbb{E}(QS) + \mathbb{E}(RS) + \mathbb{E}(RT) - \mathbb{E}(QT) \leq 2. \quad \text{(Bell inequality)}$$

Quantum Mechanical Expt

$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ (Bell state) → prepared by Charlie.

- Qubit 1 → Alice, Qubit 2 → Bob
- $Q = Z_1$, $R = X_1$. Evals are ± 1
- $S = \frac{-Z_2 - X_2}{\sqrt{2}} = -H_2$
- $T = \frac{Z_2 - X_2}{\sqrt{2}}$. Evals are ± 1.

$$S = \frac{-1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = -\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = -H \quad \checkmark$$

$$T = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} - \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix} \quad \checkmark$$

$$\langle QS\rangle = \frac{1}{\sqrt{2}}; \quad \langle RS\rangle = \frac{1}{\sqrt{2}}; \quad \langle RT\rangle = \frac{1}{\sqrt{2}}; \quad \langle QT\rangle = \frac{-1}{\sqrt{2}}$$

So, $\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2}$!! [Nature chooses this!]

>>> Universal Quantum Gates (I)

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

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix},\quad S=\begin{pmatrix}1&0\\0&i\end{pmatrix},\quad T=\begin{pmatrix}1&0\\0&e^{i\pi/4}\end{pmatrix}$$

S: phase gate $=\begin{pmatrix}1&0\\0&e^{i\pi/2}\end{pmatrix}$; T: $\frac{\pi}{8}$-gate $=e^{i\pi/8}\begin{pmatrix}e^{-i\pi/8}&0\\0&e^{i\pi/8}\end{pmatrix}$ (global phase can be ignored)

$H=\frac{X+Z}{\sqrt{2}}$ $\quad H^*=H$

$T^2=S$ $\quad T^*=T^7$, $S^*=S^3$

Rotation Matrices

$$R_n(\theta)=e^{-i\theta X/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}X=\begin{pmatrix}\cos\theta/2&-i\sin\theta/2\\-i\sin\theta/2&\cos\theta/2\end{pmatrix}$$

$$R_y(\theta)=e^{-i\theta Y/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Y=\begin{pmatrix}\cos\theta/2&-\sin\theta/2\\\sin\theta/2&\cos\theta/2\end{pmatrix}$$

$$R_z(\theta)=e^{-i\theta Z/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}Z=\begin{pmatrix}e^{-i\theta/2}&0\\0&e^{i\theta/2}\end{pmatrix}.$$

▶ Rotation about arbitrary axis.

Thm: $R_{\hat{n}}(\theta)=e^{-i\theta\,\hat{n}\cdot\vec{\sigma}/2}=\cos\frac{\theta}{2}I-i\sin\frac{\theta}{2}(n_xX+n_yY+n_zZ)$

where $\hat{n}=(n_x,n_y,n_z)$ unit vector in 3d.

Pf: $\exp(iAx)=(\cos x)I+(i\sin x)A$, if $A^2=I$.

$(\hat{n}\cdot\vec{\sigma})^2=(n_x^2+n_y^2+n_z^2)I=I$. ∎

Thm: If U is unitary, then $U=e^{i\alpha}R_{\hat{n}}(\theta)$, $U\in\mathbb{C}^{2\times2}$

Pf: $U=e^{iK}$, K is Hermitian, so $K=\alpha_0I+\alpha_1\sigma_1+\alpha_2\sigma_2+\alpha_3\sigma_3$

$$=e^{i\alpha_0I}\,e^{i(\alpha_1\sigma_1+\alpha_2\sigma_2+\alpha_3\sigma_3)}$$

$$=e^{i\alpha_0}\,e^{i\sqrt{|\alpha_1|^2+|\alpha_2|^2+|\alpha_3|^2}\;\hat{n}\cdot\vec{\sigma}}$$ ∎

Thm: (Z-Y decomposition for a single qubit). If $U \in \mathbb{C}^{2\times 2}$ is unitary, then $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Pf: Any 2×2 unitary can be expressed as

$$U \overset{(*)}{=} \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)}\sin\gamma/2 \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)}\cos\gamma/2 \end{bmatrix}$$

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

Pf of (*).

$$U = \begin{pmatrix} r_1 e^{i\theta_1} & r_2 e^{i\theta_2} \\ r_3 e^{i\theta_3} & r_4 e^{i\theta_4} \end{pmatrix} \qquad U^* = \begin{pmatrix} r_1 e^{-i\theta_1} & r_3 e^{-i\theta_3} \\ r_2 e^{-i\theta_2} & r_4 e^{i\theta_4} \end{pmatrix}$$

$$U^*U = \begin{pmatrix} r_1^2+r_3^2 & r_1 r_2 e^{i(\theta_2-\theta_1)} + r_3 r_4 e^{i(\theta_4-\theta_3)} \\ r_1 r_2 e^{-i(\theta_2-\theta_1)} + r_3 r_4 e^{-i(\theta_4-\theta_3)} & r_2^2+r_4^2 \end{pmatrix}$$

$$UU^* = \begin{pmatrix} r_1^2+r_2^2 & r_1 r_3 e^{i(\theta_1-\theta_3)} + r_2 r_4 e^{i(\theta_2-\theta_4)} \\ r_1 r_3 e^{-i(\theta_1-\theta_3)} + r_2 r_4 e^{-i(\theta_2-\theta_4)} & r_3^2+r_4^2 \end{pmatrix}$$

$r_1^2+r_3^2 = r_2^2+r_4^2$
$= r_1^2+r_2^2 = r_3^2+r_4^2 = 1$

$r_1 r_2 = r_3 r_4$, $r_1 r_3 = r_2 r_4$

Note:
$r_1 = r_4 = \cos\gamma/2$ satisfies
$r_2 = r_3 = \sin\gamma/2$ all this.

Also, we have:

$$\theta_2 - \theta_1 = \theta_4 - \theta_3 + \pi \pmod{2\pi}$$

Notice:

$$\text{invertible system} \begin{cases} \theta_1 = \alpha - \beta/2 - \delta/2 \\ \theta_3 = \alpha + \beta/2 - \delta/2 \\ \theta_4 = \alpha + \beta/2 + \delta/2 \end{cases} \Rightarrow \theta_2 = \theta_1 + \theta_4 - \theta_3 + \pi \pmod{2\pi}$$

$$= \alpha - \beta/2 + \delta/2 + \pi \pmod{2\pi}$$

$\blacksquare$

$$\begin{pmatrix} \theta_1 \\ \theta_2 \\ \theta_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta/2 \\ \delta/2 \end{pmatrix}$$

$$\det = 1(1+1) + 1(1+1) - 1(1-1)$$
$$= 4 \neq 0. \quad \checkmark$$

Fact: $XYX = -Y$, $XZX = -Z$

Pf: $XYX = -YXX = -Y$ ∎

Fact: $XR_y(\theta)X = R_y(-\theta)$, $XR_z(\theta)X = R_z(-\theta)$.

Pf: From above. ∎

Corollary: $U \in \mathbb{C}^{2\times 2}$ is unitary. Then $\exists$ unitary A, B, C s.t. $ABC = I$, & $U = e^{i\alpha} AXBXC$.

Pf: Set $A = R_z(\beta) R_y\left(\frac{\gamma}{2}\right)$, $B = R_y\left(\frac{-\gamma}{2}\right) R_z\left(-\left(\frac{\delta+\beta}{2}\right)\right)$

$C = R_z\left(\frac{\delta-\beta}{2}\right)$

Clearly, $ABC = I$.

$XBX = R_y\left(\frac{\gamma}{2}\right) R_z\left(\frac{\delta+\beta}{2}\right)$

$AXBXC = R_z(\beta) R_y(\gamma) R_z(\delta)$ ∎.

More generally if $\hat{m}, \hat{n}$ are orthonormal unit vectors:

Thm: $U \in \mathbb{C}^{2\times 2}$ is unitary $\Rightarrow U = e^{i\alpha} R_{\hat{m}}(\beta) R_{\hat{n}}(\gamma) R_{\hat{m}}(\delta)$.

Pf: [Exercise].

Thm: If $\hat{m}, \hat{n}$ are unit vectors & not parallel. Then if $U \in \mathbb{C}^{2\times 2}$ is unitary $\Rightarrow U = e^{i\alpha} R_{\hat{m}}(\beta_1) R_{\hat{n}}(\gamma_1) R_{\hat{m}}(\beta_2) R_{\hat{n}}(\gamma_2) \cdots$ finitely many terms. The # of terms needed is independent of U (i.e. $\exists$ an upper bound).

Pf: [Exercise].

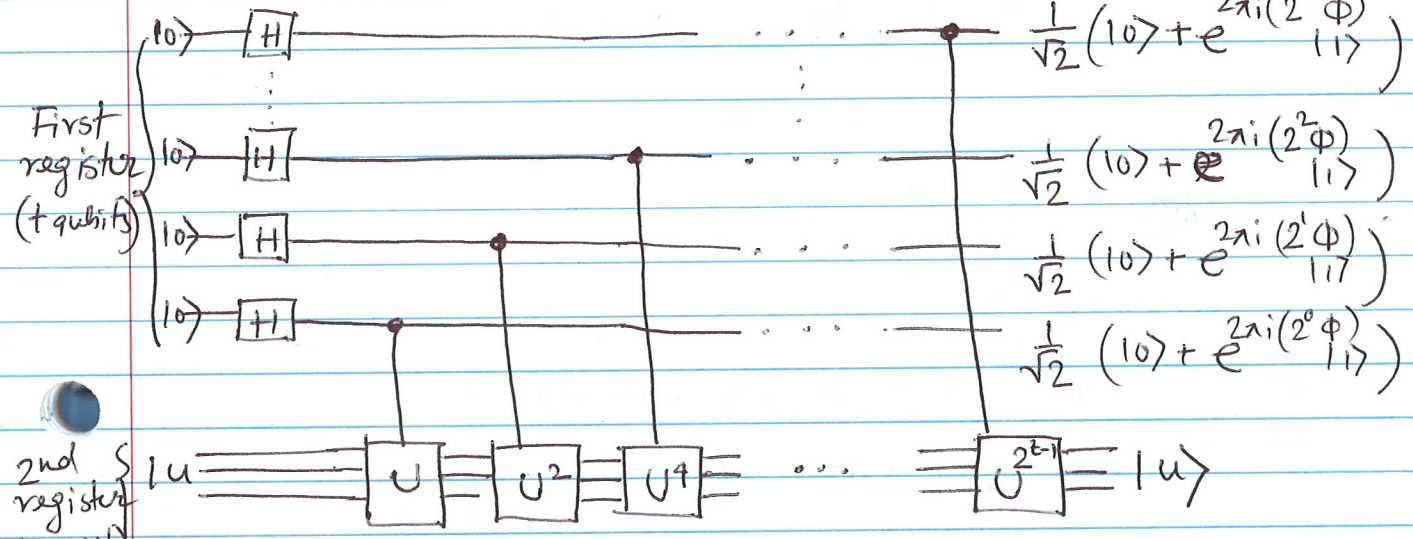
Quantum Phase Estimation

- Suppose there is an unitary op. U has an eigenvector $|u\rangle$ with eigenval $e^{2\pi i\phi}$.

$$U|u\rangle = e^{2\pi i\phi}|u\rangle, \quad 0 \le \phi < 1.$$

- Classically estimating ϕ is $O(\text{poly}(2^n))$.
- Can we do better with quantum computing?

Stage 1.



Thm.

$$|0\rangle^{\otimes t}|u\rangle \to \frac{1}{\sqrt{2^t}}\left(|0\rangle + e^{2\pi i(2^{t-1}\phi)}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i(2^0\phi)}|1\rangle\right)|u\rangle$$

$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\phi k}|k\rangle|u\rangle \quad \text{where}$$

Pf.

Calculation as QFT.

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i\phi k}|u\rangle = \frac{1}{2^{t/2}}\sum_{k_1,\ldots,k_t=0}^{1} e^{2\pi i\phi\sum_{l=1}^{t}k_l 2^{l-1}}|k_1\ldots k_n\rangle$$

$$= \frac{1}{2^{t/2}}\sum_{k_1,\ldots,k_t=0}^{1}\bigotimes_{l=1}^{t} e^{2\pi i\phi k_l 2^{l-1}}|k_l\rangle$$

$$= \frac{1}{2^{t/2}}\bigotimes_{l=1}^{t}\sum_{k_l=0}^{1} e^{2\pi i k_l\phi 2^{l-1}}|k_l\rangle \quad \blacksquare.$$

Suppose ϕ has an exact t-bit representation.

$$\phi = 0.\phi_1 \cdots \phi_t$$

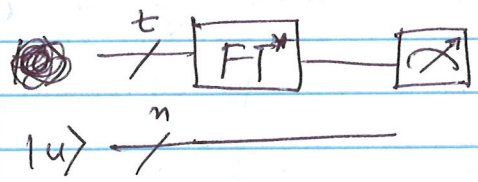
Then state after 1st stage:

$$\frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.\phi_{t-1}\phi_t}|1\rangle\right) \otimes \cdots$$

$$\cdots \otimes \left(|0\rangle + e^{2\pi i 0.\phi_1 \cdots \phi_t}|1\rangle\right) |u\rangle.$$

↑ This is exactly the state after QFT.

Stage 2.



On measuring first t-qubits we get:

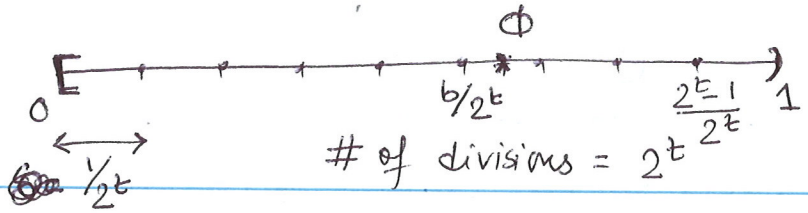
$|\phi_1 \cdots \phi_t\rangle$ exactly! (So we know ϕ exactly).

What happens when ϕ does not have an exact t-bit representation?

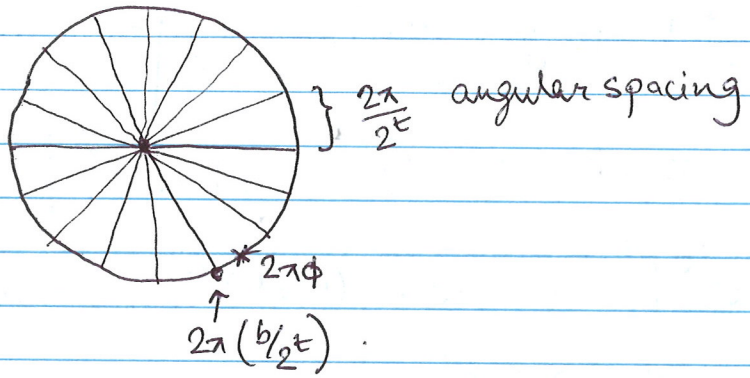
- By increasing t, we can get more & more accurate estimate of ϕ with high probability.

Analysis of general case

- Let b be an integer $0 \leq b \leq 2^t - 1$, s.t $b/2^t \leq \phi$ is the best t-bit approx to ϕ.



# of divisions = 2^t



$$0 \le \delta = \Phi - b/2^t \le 2^{-t} \quad \Rightarrow 0 \le 2^t\delta = 2^t\Phi - b \le 1$$

Apply FT* to state after Phase 1 gives following state.

$$\left(\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{2\pi i \Phi k}\, e^{-2\pi i kl/2^t}\,|l\rangle\right)|u\rangle.$$

so on First register we have:

$$\frac{1}{2^t}\sum_{k,l=0}^{2^t-1} e^{2\pi i(\Phi - l/2^t)k}\,|l\rangle$$

$$= \frac{1}{2^t}\sum_{l=0}^{2^t-1}\left(\sum_{k=0}^{2^t-1} e^{2\pi i(\Phi - l/2^t)k}\right)|l\rangle$$

$$= \frac{1}{2^t}\sum_{l=0}^{2^t-1}\left(\frac{1-e^{2\pi i(2^t\Phi - l)}}{1-e^{2\pi i(\Phi - l/2^t)}}\right)|l\rangle.$$

Let α_l be amplitude of $|(b+l) \pmod{2^t}\rangle$.

$$\alpha_l = \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\Phi - (b+l))}}{1-e^{2\pi i(\Phi - \frac{b+l}{2^t})}}\right).$$

$$= \frac{1}{2^t}\left(\frac{1-e^{2\pi i(2^t\delta - l)}}{1-e^{2\pi i(\delta - l/2^t)}}\right).$$

Observe:

$$|\alpha_\ell| = \frac{1}{2^t} \left| \frac{1 - e^{2\pi i (\frac{t}{2}\delta - \ell)}}{1 - e^{2\pi i (\delta - \ell/2t)}} \right|$$

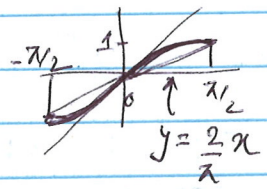
$$\leq \frac{1}{2^{t-1}} \cdot \frac{1}{\left| 1 - e^{2\pi i (\delta - \ell/2t)} \right|}$$

Fact: if $-\pi \leq \theta \leq \pi$, then $|1 - e^{i\theta}| \geq \frac{2|\theta|}{\pi}$.

Pf. $|1 - e^{i\theta}|^2 = (1-\cos\theta)^2 + (\sin\theta)^2 = 2 - 2\cos\theta = 4\sin^2\theta/2$

$\Rightarrow |1 - e^{i\theta}| = 2|\sin\theta/2|$

$\geq 2\frac{|\theta|}{\pi}$



Fact: Let $-2^{t-1} < \ell \leq 2^{t-1}$, $\ell \in \mathbb{Z}$ (Notice by varying ℓ we get all states $|\ell\rangle$).

Then $|\alpha_\ell| \leq \frac{1}{2^{t+1}} \frac{1}{(\delta - \ell/2t)}$.

Pf. $-\frac{1}{2} + \frac{1}{2^t} \leq \ell/2^t \leq 1/2 \Rightarrow \frac{1}{2} - \frac{1}{2^t} \geq -\ell/2^t \geq -\frac{1}{2}$

$\Rightarrow \frac{1}{2} + \delta - \frac{1}{2^t} \geq \delta - \ell/2^t \geq \delta - 1/2$

$2\pi(\delta - 1/2) \leq 2\pi(\delta - \ell/2^t) \leq 2\pi\left(\frac{1}{2} + \delta - \frac{1}{2^t}\right)$

$-\pi + 2\pi\delta \leq 2\pi(\delta - \ell/2^t) \leq \pi$

$\Rightarrow -\pi \leq 2\pi(\delta - \ell/2^t) \leq \pi.$

So, $|\alpha_l| \le \frac{1}{2^{t-1}} \cdot \frac{1}{|1 - e^{2\pi i(\delta - l/2^t)}|}$

$\le \frac{1}{2^{t-1}} \cdot \frac{\pi}{2} \cdot \frac{1}{2\pi(\delta - l/2^t)}$

$= \frac{1}{2^{t+1}} \cdot \frac{1}{\delta - l/2^t}$ ∎

Let $-2^{t-1} < m \le 2^{t-1}$, $m \in \mathbb{Z}$.

We measure one of these m's.

$$P(m) = |\alpha_m|^2 \le \left(\frac{1}{2^{t+1}(\delta - l/2^t)}\right)^2 = \frac{1}{4} \cdot \frac{1}{(2^t\delta - l)^2}$$

If we want accuracy e, i.e, $-e \le m \le e$, then

$$P(|m| > e) = \sum_{l=e+1}^{2^{t-1}} |\alpha_l|^2 + \sum_{l=-(e+1)}^{-2^{t-1}+1} |\alpha_l|^2$$

$$\le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{(2^t\delta - l)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(2^t\delta - l)^2}\right]$$

Notice, $0 \le 2^t\delta \le 1$.

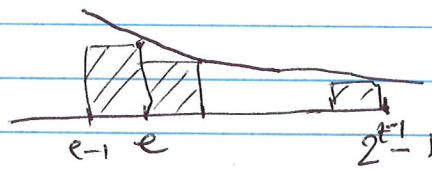
$$l \ge l - 2^t\delta \ge l - 1$$

$\le \frac{1}{(l-1)^2}$

$\le \frac{1}{l^2}$

$$\le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{l^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right] = \frac{1}{2}\sum_{l=e}^{2^{t-1}-1} \frac{1}{l^2}$$

$$\le \frac{1}{2}\int_{e-1}^{2^{t-1}-1} \frac{1}{l^2}\,dl$$



$$= \frac{1}{2}\left(\frac{1}{e-1} - \frac{1}{2^{t-1}-1}\right) \le \frac{1}{2(e-1)}.$$

Suppose you want to estimate ϕ to an accuracy $2^{-\tilde{n}}$.

- Choose $e = 2^{t-\tilde{n}} - 1$

$$\frac{e}{2^t} = 2^{-\tilde{n}} - \frac{1}{2^t} \Rightarrow \phi - \frac{e}{2^t} = \phi - 2^{-\tilde{n}} + \frac{1}{2^t}$$

if $e/2^t \geq \phi \Rightarrow \frac{e}{2^t} - \phi = 2^{-\tilde{n}} - \phi - \frac{1}{2^t} \leq 2^{-\tilde{n}} - \phi$

- Choose $t = \tilde{n} + p \Rightarrow t - \tilde{n} = p \Rightarrow e = 2^p - 1$.

Then $P(|m| \leq e) = 1 - \frac{1}{2(2^p - 1)}$

Suppose want to make $P(|m| \leq e) \geq 1 - \varepsilon \Rightarrow 1 - \frac{1}{2(2^p-1)} \geq 1 - \varepsilon$

$$\Rightarrow \frac{1}{2(2^p-1)} \leq \varepsilon \Rightarrow 2^p - 1 \geq \frac{1}{2\varepsilon}$$

$$\Rightarrow 2^p \geq 1 + \frac{1}{2\varepsilon} \Rightarrow p \geq \log_2\left(1 + \frac{1}{2\varepsilon}\right).$$

Accuracy: $\frac{e}{2^{\tilde{n}+p}} = \frac{2^p - 1}{2^{\tilde{n}+p}} = 2^{-\tilde{n}} - \frac{1}{2^{\tilde{n}+p}} \leq 2^{-\tilde{n}}$.

>>> Universal quantum gates (II)

Thm: $U \in \mathbb{C}^{2\times 2}$ unitary $\Rightarrow U = e^{i\alpha} R_{\hat{m}}(\beta) R_{\hat{n}}(\gamma) R_{\hat{m}}(\delta)$
where $\hat{m}, \hat{n}$ unit vectors in $\mathbb{R}^3$ & orthogonal.

Pf $R_{\hat{m}}(\beta) R_{\hat{n}}(\gamma) R_{\hat{m}}(\delta)$

$$= \cos\frac{\gamma}{2}\cos\left(\frac{\beta+\delta}{2}\right) I - i\cos\frac{\gamma}{2}\sin\left(\frac{\beta+\delta}{2}\right)(\hat{m}\cdot\vec{\sigma})$$

$$- i\sin\frac{\gamma}{2}\cos\left(\frac{\beta-\delta}{2}\right)(\hat{n}\cdot\vec{\sigma}) - i\sin\frac{\gamma}{2}\sin\left(\frac{\beta-\delta}{2}\right)(\hat{m}\times\hat{n})\cdot\vec{\sigma} \quad (**)$$

Notice, $\{ I, (\hat{m}\cdot\vec{\sigma}), (\hat{n}\cdot\vec{\sigma}), \bullet(\hat{m}\times\hat{n})\cdot\vec{\sigma} \}$ is an orthonormal basis for Hermitian matrices in $\mathbb{C}^{2\times 2}$, w.r.t. H-S inner prod.

Note: $(\hat{m}\cdot\vec{\sigma})(\hat{n}\cdot\vec{\sigma}) = i(\hat{m}\times\hat{n})\cdot\vec{\sigma}$ → [Ex].

$(\hat{m}\cdot\vec{\sigma})^2 = I$. → [Do in class].

$\tilde{X} = \hat{m}\cdot\vec{\sigma}$, $\tilde{Y} = \hat{n}\cdot\vec{\sigma}$, $\tilde{Z} = \bullet(\hat{m}\times\hat{n})\cdot\vec{\sigma} = (\hat{n}\times\hat{m})\cdot\vec{\sigma}$

$$\boxed{\tilde{X}^2 = \tilde{Y}^2 = \tilde{Z}^2 = -i\tilde{X}\tilde{Y}\tilde{Z} = I}$$ → just like Pauli algebra.

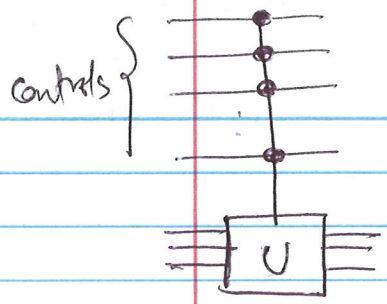
$U = e^{iK}$, K is Hermitian

$$= e^{i(aI + b\tilde{X} + c\tilde{Y} + d\tilde{Z})} = e^{ia} e^{i(b\tilde{X} + c\tilde{Y} + d\tilde{Z})}$$

$$= e^{ia} e^{i\sqrt{b^2+c^2+d^2}\left(\frac{b}{\sqrt{b^2+c^2+d^2}}\tilde{X} + \frac{c}{\sqrt{b^2+c^2+d^2}}\tilde{Y} + \frac{d}{\sqrt{b^2+c^2+d^2}}\tilde{Z}\right)}$$

$= (**)$ for appropriate choices of variables. ∎

Controlled operations

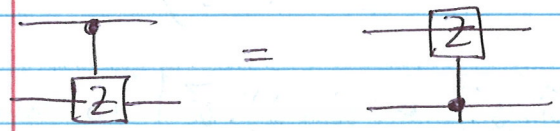


← Prototype operation $(C^n(U))$

[How to design quantum circuits to do this?].

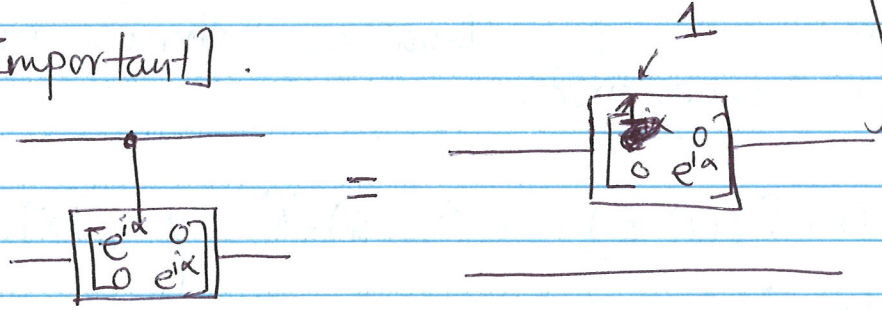
Ex.

Ex.



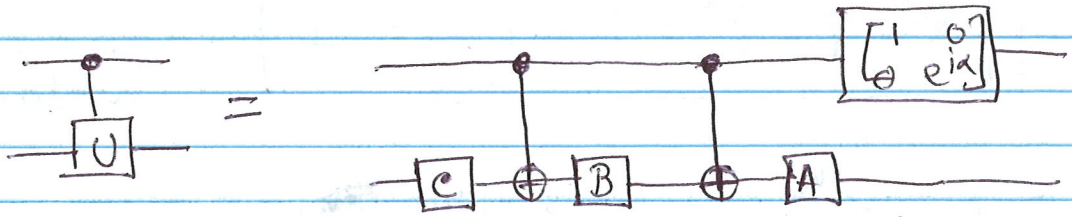
Do in class.

Ex: [Important].



Recall: $U = e^{i\alpha} AXBXC$ for some unitary A, B, C s.t $ABC = I$.

Thm.



Pf: Check basis states.

$|0\rangle|n\rangle \to |0\rangle(ABC|n\rangle) = |0\rangle|n\rangle$

$|1\rangle|n\rangle \to (e^{i\alpha}|1\rangle)(AXBXC|n\rangle) = e^{i\alpha}|1\rangle(U|n\rangle)$.

□