Lecture 3 (13/2/24)

Tuesday, 13 February 2024 12:42

Lecture 3: Quantum linear algebra

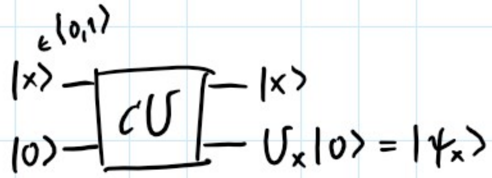
1. QUANTUM SWAP TEST

$\underbrace{U_0|0\rangle = |\psi_0\rangle \quad , \quad U_1|0\rangle = |\psi_1\rangle}$ → (actually, (slightly stronger) $cU_0 = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U_0$

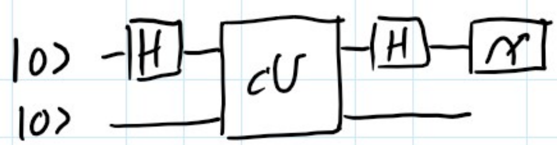
$cU_1 = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U_1$)

? $|\psi_0\rangle = |\psi_1\rangle$ or $|\psi_0\rangle \perp |\psi_1\rangle$

$\rightsquigarrow cU = |0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1$



$\rightsquigarrow$ SWAP test:



? prob. "0" v.s. "1"

Ex.: Show that circuit can distinguish $|\psi_0\rangle = |\psi_1\rangle$ from $|\psi_0\rangle \perp |\psi_1\rangle$.

$$|0\rangle|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle$$

$$\xrightarrow{cU} \frac{1}{\sqrt{2}}|0\rangle U_0|0\rangle + \frac{1}{\sqrt{2}}|1\rangle U_1|0\rangle = \frac{1}{\sqrt{2}}|0\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle|\psi_1\rangle$$

$$\xrightarrow{H} \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|\psi_0\rangle + \frac{1}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|\psi_1\rangle$$

$$= \frac{1}{2}|0\rangle\left(|\psi_0\rangle + |\psi_1\rangle\right) + \frac{1}{2}|1\rangle\left(|\psi_0\rangle - |\psi_1\rangle\right)$$

$$= \frac{1}{2}|0\rangle\big(|\psi_0\rangle + |\psi_1\rangle\big) + \frac{1}{2}|1\rangle\big(|\psi_0\rangle - |\psi_1\rangle\big)$$

$\xrightarrow{\mathcal{M}}$ "0" w. prob. $\left\| \frac{1}{2}|0\rangle(|\psi_0\rangle+|\psi_1\rangle)\right\|^2 = \frac{1}{4}\left\||0\rangle(|\psi_0\rangle+|\psi_1\rangle)\right\|^2$

$$= \frac{1}{4}\left\||\psi_0\rangle+|\psi_1\rangle\right\|^2$$

"1" w. prob. $\frac{1}{4}\left\||\psi_0\rangle-|\psi_1\rangle\right\|^2$

<u>Note</u>: * $|\psi_0\rangle = |\psi_1\rangle$: "0" w. prob. 1

* $|\psi_0\rangle \perp |\psi_1\rangle$: "0" w. prob. $\frac{1}{4}\left\||\psi_0\rangle+|\psi_1\rangle\right\|^2$

$$= \frac{1}{4}\left(\||\psi_0\rangle\|^2 + \||\psi_1\rangle\|^2\right) = \frac{1}{2}$$

"1" w. prob. $\frac{1}{2}$.

! strong contrast with randomized circuits:

$0^n - \boxed{R_0} - p_0$, $\quad 0^n - \boxed{R_1} - p_1 \rightarrow$ prob. distr. over $\{0,1\}^n$ (i.e., returns x w. prob. $p_1(x)$)

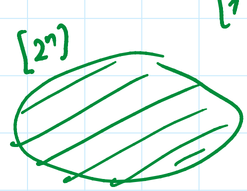
$0^n - \boxed{D_0} - x_0 \in \{0,1\}^n$

$0^n - \boxed{D_1} - x_1 \in \{0,1\}^n$

? $p_0 = p_1$ or $p_0 \perp p_1$ (i.e., p_0, p_1 disjoint support)

(e.g., $p_0 = p_1 = \frac{1}{2^n}\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}$ or $p_0 = \frac{1}{2^{n-1}} 1_S$, $p_1 = \frac{1}{2^{n-1}} 1_{S^c}$)

($S \subseteq [2^n]$, $|S| = 2^{n-1}$



"birthday paradox"

$O(2^{n/2})$ samples suffice (and are necessary!)

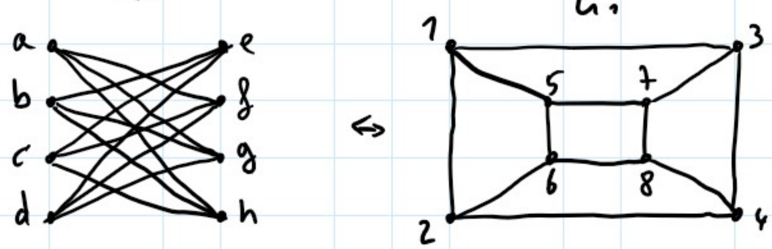
$\mathcal{O}(2^{n/2})$ samples suffice (and are necessary!)

(contrast with quantum: $|\psi_0\rangle = |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum |x\rangle$

v.s. $|\psi_0\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \in S} |x\rangle$, $|\psi_1\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{x \notin S} |x\rangle$)

Application: "graph isomorphism" (between P and NP)

G_0, G_1 isomorphic if $\exists$ bijection $\underset{V_0 \to V_1}{\varphi}$ between vertices that preserves edges $((u,v) \in E_0 \Leftrightarrow (\varphi(u), \varphi(v)) \in E_1)$



isomorphic: $\varphi(a) = 1$, $\varphi(b) = 6$, $\varphi(c) = 4$, $\varphi(d) = 7$
$\varphi(e) = 8$, $\varphi(f) = 3$, $\varphi(g) = 5$, $\varphi(h) = 2$

"adjacency matrix encoding" A_0, A_1

? $\exists$ permutation σ s.t. $A_1 = \sigma(A_0) = P^T A_0 P$

Ex.: Consider unitaries $U_i |0\rangle = |\psi_i\rangle$,

where $|\psi_i\rangle \sim \sum_{\sigma \in S_n} |\sigma(A_i)\rangle$.

Use SWAP test on U_0, U_1 to solve GI.

Use SWAP test on U_0, U_1 to solve GI.

$\rightsquigarrow$ if isomorphic: $A_1 = \tilde{\sigma}(A_0)$

$$|\psi_1\rangle \sim \sum_\sigma |\sigma(A_1)\rangle$$

$$= \sum_\sigma |\underbrace{\sigma(\tilde{\sigma}}_{\hat{\sigma}}(A_0))\rangle$$

$$= \sum_{\hat{\sigma}} |\hat{\sigma}(A_0)\rangle \sim |\psi_0\rangle$$

n^2-bit string
↓
$$\langle \sigma(A_0) | \sigma'(A_1)\rangle = \delta_{\sigma(A_0),\, \sigma'(A_1)}$$

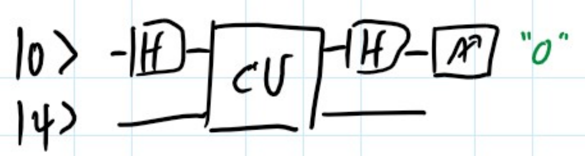
if not: $\langle\psi_0|\psi_1\rangle \neq 0 \Leftrightarrow \exists\, \sigma, \sigma'$ s.t. $\sigma(A_0) = \sigma(A_1)$
$\Leftrightarrow \exists\, \hat{\sigma}$ s.t. $A_0 = \hat{\sigma}(A_1)$ ↯

$\Rightarrow \langle\psi_0|\psi_1\rangle = 0$

---

2. Linear combination of unitaries (LCU)

SWAP test



$$|0\rangle|\psi\rangle \xrightarrow{H} \dots \xrightarrow{CU} \dots \xrightarrow{H} \tfrac{1}{2}|0\rangle(U_0+U_1)|\psi\rangle + \tfrac{1}{2}|1\rangle(U_0-U_1)|\psi\rangle$$

$\xrightarrow{\nearrow}$ "0" w. prob. $\frac{1}{4}\|(U_0+U_1)|\psi\rangle\|^2 = P_0$, !matrix arithmetic

corresponding state $\boxed{\dfrac{|0\rangle(U_0+U_1)|\psi\rangle}{\|(U_0+U_1)|\psi\rangle\|}}$

$$\| |0\rangle \otimes (U_0+U_1)|\psi\rangle\|^2$$

$$= \left(\langle 0| \otimes \langle\psi|(U_0^\dagger+U_1^\dagger)\right)\left(|0\rangle \otimes (U_0+U_1)|\psi\rangle\right)$$

$$= \underbrace{\langle 0|0\rangle}_{1} \cdot \underbrace{\langle\psi|(U_0^\dagger+U_1^\dagger)(U_0+U_1)|\psi\rangle}_{\|(U_0+U_1)|\psi\rangle\|^2}$$

"1" w. prob. $\frac{1}{4}\|(U_0-U_1)|\psi\rangle\|^2$,

corresp. state $\dfrac{|1\rangle(U_0-U_1)|\psi\rangle}{\|(U_0-U_1)|\psi\rangle\|}$

$\underbrace{\qquad\qquad\qquad}_{\|(U_0+U_1)|\psi\rangle\|^2}$ 1 $\qquad$ corresp. state $\dfrac{|1\rangle(U_0-U_1)|\psi\rangle}{\|(U_0-U_1)|\psi\rangle\|}$

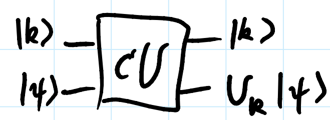
$\rightsquigarrow$ prepare state $\sim (U_0+U_1)|\psi\rangle$

by running circuit $\frac{1}{p_0} = \frac{1}{\|(U_0+U_1)|\psi\rangle\|^2}$ times.

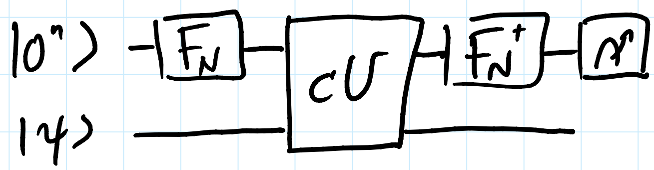
Generalize: more unitaries!

$U_0, U_1, \dots, U_{N-1}, \quad N = 2^n$ $\qquad$ $cU = \sum_{k=0}^{2^n-1} |k\rangle\langle k| \otimes U_k$

$(QPE: U_k = U^k)$



LCU:



?Ex: - outcome if measure "0"

- prob. of measuring "0"

$F_N |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{N-1} e^{i\frac{2\pi}{N}lk} |l\rangle$

$F_N^\dagger |k\rangle = \frac{1}{\sqrt{2^n}} \sum_{l=0}^{N-1} e^{-i\frac{2\pi}{N}lk} |l\rangle$

$$|0^n\rangle|\psi\rangle \xrightarrow{F_N} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} |k\rangle|\psi\rangle$$

$$\xrightarrow{cU} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} |k\rangle U_k|\psi\rangle$$

$$\xrightarrow{F_N^\dagger} \frac{1}{2^n} \sum_{l=0}^{N-1} |l\rangle \Big(\sum_k e^{-i\frac{2\pi}{N}lk} U_k|\psi\rangle \Big)$$

$$\xrightarrow{\mathcal{M}} \text{"}l\text{" w. prob. } \Big\| \frac{1}{2^n} |l\rangle \Big(\sum_k e^{-i\frac{2\pi}{N}lk} U_k|\psi\rangle \Big) \Big\|^2$$

$\xrightarrow{\ }$ "ℓ" w. prob. $\left\| \frac{1}{2^n} |\ell\rangle \left(\sum_k e^{-i\frac{2\pi}{N}\ell k} U_k |\psi\rangle \right) \right\|$

$$= \frac{1}{2^{2n}} \left\| \sum_k e^{-i\frac{2\pi}{N}\ell k} U_k |\psi\rangle \right\|^2$$

Hence, returns "0" w. prob. $\frac{1}{2^{2n}} \left\| \left(\sum_k U_k \right) |\psi\rangle \right\|^2$,

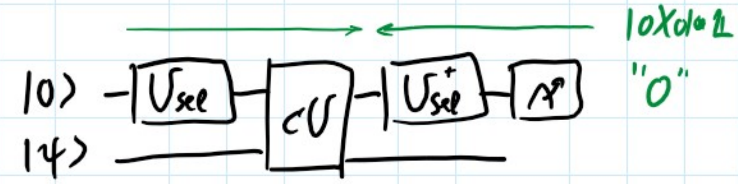
corresp. state $\sim |0\rangle \otimes \left(\sum_k U_k \right) |\psi\rangle$.

Further generalization: "LCU" $\sum_k c_k U_k$

↳ coefficients $c_0, c_1, \ldots, c_{N-1} \geq 0$ and $\sum c_k = 1$

"select" unitary $U_{sel} |0\rangle = \sum_{k=0}^{N-1} \sqrt{c_k} |k\rangle$

LCU circuit:



$(|0\rangle\langle 0| \otimes \mathbb{1}) U_{sel}^\dagger \, cU \, U_{sel} |0\rangle |\psi\rangle$

Ex.: – outcome if postselect on "0"? $\sim |0\rangle \otimes \left(\sum c_k U_k \right) |\psi\rangle$

– success probability? $p_0 = \left\| \sum c_k U_k |\psi\rangle \right\|^2$

$$|0\rangle |\psi\rangle \xrightarrow{U_{sel}} \sum \sqrt{c_k} |k\rangle |\psi\rangle$$

$$\xrightarrow{cU} \sum \sqrt{c_k} |k\rangle U_k |\psi\rangle$$

$$\xrightarrow{U_{sel}^\dagger} \underbrace{|0\rangle \otimes \_\_\_}_{} + \overbrace{|1\rangle \otimes \_\_\_ + |2\rangle \otimes \_\_\_ + \ldots}^{\text{don't care!}}$$

$\dagger$ ($U_{sel} |0\rangle = \sum \sqrt{c_k} |k\rangle$

$\langle 0| U_{sel}^\dagger = \sum \sqrt{c_k} \langle k|$

$$(|0\rangle\langle 0| \otimes \mathbb{1}) U_{sel}^\dagger \sum \sqrt{c_k} |k\rangle U_k |\psi\rangle$$

$$= (|0\rangle \underline{\langle 0| U_{sel}^\dagger} \otimes \mathbb{1}) \left(\sum \sqrt{c_k} |k\rangle U_k |\psi\rangle \right)$$

$$= \left(|0\rangle \left(\sum \sqrt{c_k} \langle k| \right) \otimes \mathbb{1} \right) (\text{"}) = \sum \left(\sqrt{c_k} |0\rangle\langle k| \otimes \mathbb{1} \right) \left(\sum \sqrt{c_{k'}} |k'\rangle U_{k'} |\psi\rangle \right)$$

$$= \left(|0\rangle \left(\sum \sqrt{c_k}\langle k|\right) \otimes \mathbb{1}\right) \left(\;"\; \right) = \sum_k \underbrace{\left(\sqrt{c_k}\,|0\rangle\langle k| \otimes \mathbb{1}\right)\left(\sum \sqrt{c_{k'}}\,|k'\rangle U_{k'}|\psi\rangle\right)}_{c_k |0\rangle U_k |\psi\rangle}$$

$$= |0\rangle \otimes \sum c_k U_k |\psi\rangle .$$

$\llcorner$ success prob. $p_0 = \left\| \sum c_k U_k |\psi\rangle \right\|^2$ $\square$

Application: quantum linear system solving [HHL'06]

$$A x = b, \quad \text{Hermitian, invertible } A \in \mathbb{C}^{N \times N}$$

given A, b — find $x = A^{-1} b$ (classical: "matrix mlp. time" N^{ω}, $\omega < 2.37\ldots$)

Quantum: HHL algorithm = Hamiltonian simulation + LCU

(given $\cancel{H}$ A, apply e^{iHt})

$e^{iA} = U$

$|\psi\rangle - \boxed{e^{iA}} - e^{iA}|\psi\rangle$

$\downarrow$

LCU, $U_k = e^{iAk}$

need: c_k's such that $\boxed{\sum c_k U_k = \sum c_k e^{iAk} \approx A^{-1}}$

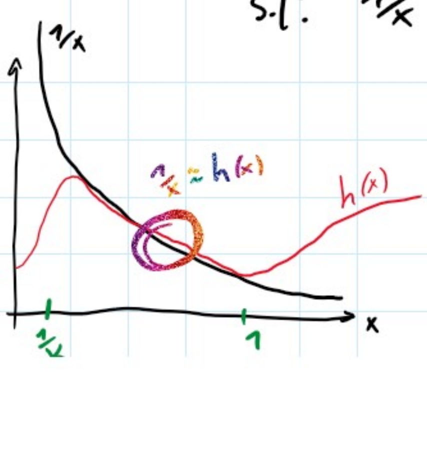
about functions

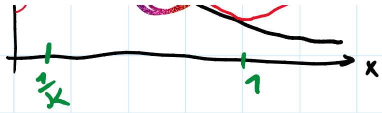
! lemma: $\exists\, c_0, c_1, \ldots, c_L \geq 0$, $\sum c_k = 1$

(not 100% true)

s.t. $\displaystyle \tfrac{1}{x} \simeq \kappa \underbrace{\sum_{k=0}^{L} c_k e^{ikx}}_{\substack{\text{Fourier series} \\ h(x)}}$ for $\frac{1}{\kappa} \leq |x| \leq 1$

$L \in O(\kappa)$.





$\hookrightarrow$ Assume $\lambda_{max}(A) \leq 1$, $\lambda_{min}(A) \geq \frac{1}{\kappa} > 0$, $(\Leftrightarrow \frac{1}{\kappa} \leq \lambda_j \leq 1)$

then $A^{-1} \approx \underline{\kappa} \sum c_k e^{iAk}$.

$$\left.\begin{cases} A = \sum \lambda_j |v_j\rangle\langle v_j| \\ A^{-1} = \sum \frac{1}{\lambda_j} |v_j\rangle\langle v_j| \\ e^{iAk} = \sum e^{i\lambda_j k} |v_j\rangle\langle v_j| \end{cases}\right\} \quad \begin{aligned} A^{-1} &= \sum_j \frac{1}{\lambda_j} |v_j\rangle\langle v_j| \\ &\approx \sum_j \Big(\kappa \sum_k c_k e^{i\lambda_j k}\Big) |v_j\rangle\langle v_j| \\ &= \kappa \sum c_k e^{iA_k} \end{aligned}$$

HHL algorithm: c_k's from lemma, $U_k = e^{iAk}$

LCU outputs $|0\rangle \left(\sum c_k e^{ikA}\right)|\psi\rangle \approx \frac{1}{\kappa}|0\rangle A^{-1}|\psi\rangle$ $\sim |0\rangle|x\rangle$ if $|\psi\rangle = |b\rangle$

w. prob. $\|\frac{1}{\kappa} A^{-1}|\psi\rangle\|^2 \geq \frac{1}{\kappa^2}$

$\hookrightarrow$ Complexity: # tries $\sim \kappa^2$
per try: Ham. sim. for time κ $\rightarrow$ cost $\sim \kappa$

Total cost $\sim \kappa^3$ ($\times$ polylog(N))

$\ll$ poly(N) (if well-conditioned!)