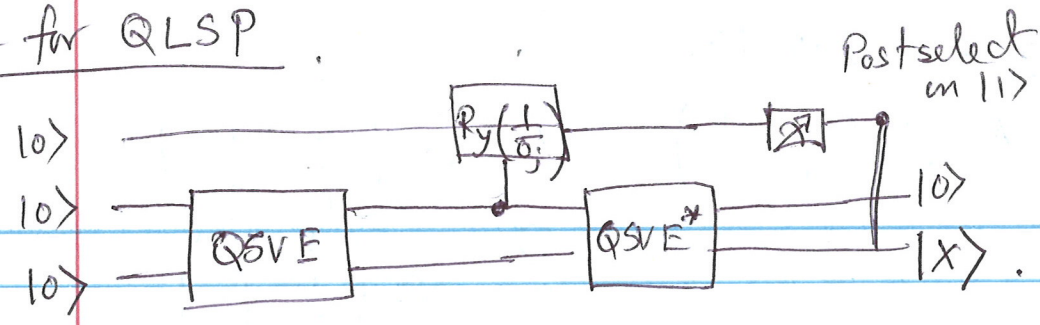
Use for QLSP.



$O\left(\text{poly}\log(N)\,\kappa^2\,\|A\|_F/\varepsilon\right)$ complexity for QLSP.

Lec 9.

>>> Optimality of quantum search.

$M=1$, N items, $N=2^n$ (assume).

We showed that to have a success prob $> \varepsilon$, Grover's search needs to perform $O\left(\sqrt{\frac{N}{M}}\right)$ calls to the oracle.

Here we show # calls needed $= \Omega\left(\sqrt{\frac{N}{M}}\right)$.

We prove for the case $M=1$, $\varepsilon = 1/2$ (for simplicity).

Let $|\psi_0\rangle$ be starting state in Grover.

$O_x = I - 2|x\rangle\langle x|$. ← oracle.

Define: $|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi_0\rangle$

$$|\psi_k^x\rangle = U_k O_x U_{k-1} O_x \cdots U_1 O_x |\psi_0\rangle$$

$$D_k = \sum_x \|\psi_k^x - \psi_k\|^2$$

$$E_k = \sum_x \|\psi_k^x - x\|^2$$

$$F_k = \sum_x \|\psi_k - x\|^2$$

Claim 1. $D_k \le 4k^2$

Pf: (By induction)

$D_0 = 0$ (true), Let $D_k \le 4k^2$.

for $k+1$.

$$D_{k+1} = \sum_x \| \psi_{k+1}^x - \psi_{k+1} \|^2 = \sum_x \| U_{k+1} O_x \psi_k^x - U_{k+1} \psi_k \|^2$$

$$= \sum_x \| O_x \psi_k^x - \psi_k \|^2 = \sum_x \| O_x (\psi_k^x - \psi_k) + (O_x - I)\psi_k \|^2$$

$\| b+c \|^2 \le \|b\|^2 + \|c\|^2 + 2\|b\|\|c\|$

$b = O_x(\psi_k^x - \psi_k) \Rightarrow \|b\| = \|\psi_k^x - \psi_k\|$

$c = (O_x - I)\psi_k = -2\langle x|\psi_k\rangle |x\rangle \Rightarrow \|c\| = 2|\langle x|\psi_k\rangle|$

$$D_{k+1} \le \sum_x \|\psi_k^x - \psi_k\|^2 + 4 \underbrace{\sum_x |\langle x|\psi_k\rangle|^2}_{1} + 4 \sum_x \|\psi_k^x - \psi_k\| |\langle x|\psi_k\rangle|$$

$$\le D_k + 4 + 4 \left(\sum_x \|\psi_k^x - \psi_k\|^2 \right)^{1/2} \underbrace{\left(\sum_x |\langle x|\psi_k\rangle|^2 \right)^{1/2}}_{1}$$

$$= D_k + 4 + 4\sqrt{D_k}$$

$$\le 4k^2 + 4 + 4 \cdot 2k = 4(k+1)^2. \qquad \blacksquare$$

Fact: If $|\psi_k\rangle$ is normalized, and $\{|x\rangle\}$ are orthonormal basis states, then $\sum_x \|\psi_k - x\|^2 \ge 2N - 2\sqrt{N}$.

Pf: $\sum_x \|\psi_k - x\|^2 = 2N - \sum_x \left(\langle \psi_k | x \rangle + \langle x | \psi_k \rangle \right)$

$$= 2N - \langle \psi_k | \sum_x x \rangle - \langle \sum_x x | \psi_k \rangle$$

$$\ge 2N - 2 |\langle \psi_k | \sum_x x \rangle| \ge 2N - 2 \|\psi_k\| \left\| \sum_x |x\rangle \right\| = 2N - 2\sqrt{N}$$

Now follows a calculation.

Claim 2: $D_k \geq \left(\sqrt{F_k} - \sqrt{E_k}\right)^2$

Pf:

$$D_k = \sum_x \|\psi_k^x - x + x - \psi_k\|^2$$

$$\geq \sum_x \|\psi_k^x - x\|^2 + \sum_x \|x - \psi_k\|^2 - 2\sum_x \|\psi_k^x - x\| \, \|x - \psi_k\|$$

Demonstrate in class why this is true

$$= E_k + F_k - 2\sum_x \|\psi_k^x - x\| \, \|x - \psi_k\|$$

$$\geq E_k + F_k - 2\left(\sum_x \|\psi_k^x - x\|^2\right)^{1/2} \left(\sum_x \|x - \psi_k\|^2\right)^{1/2}$$

$$= E_k + F_k - 2\sqrt{E_k}\sqrt{F_k} = \left(\sqrt{F_k} - \sqrt{E_k}\right)^2. \quad \blacksquare$$

Claim 3: $E_k \leq (2-\sqrt{2})N$, assuming $|\langle x | \psi_k^x \rangle|^2 \geq 1/2 \ \forall x$.

(Ex).

Claim 2 + Claim 3 + Fact

$$\sqrt{F_k} - \sqrt{E_k} \geq \sqrt{2N - 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N}$$

$$\sqrt{2N - 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N} = \sqrt{N}\left(\sqrt{2 - 2/\sqrt{N}} - \sqrt{2-\sqrt{2}}\right) \geq 0 \text{ for } N \geq 2$$

$$\Rightarrow \left(\sqrt{F_k} - \sqrt{E_k}\right)^2 \geq 2N - 2\sqrt{N} + 2N - \sqrt{2}N - 2\sqrt{2N - 2\sqrt{N}}\sqrt{(2-\sqrt{2})N}$$

Asymptotically

$D_k \geq \left(\sqrt{F_k} - \sqrt{E_k}\right)^2 \geq cN$, c is const indep of N.

$cN \leq D_n \leq 4k^2$

$\Rightarrow k = \Omega(\sqrt{N})$. ∎

Solovay-Kitaev Algorithm / Theorem

- Suppose you have a topologically dense subgroup G of $SU(2)$, where G is generated by a finite set $\mathcal{G}$. So $G = \langle \mathcal{G} \rangle$.
- Assumptions.
  - $\mathcal{G} \in SU(2)$, i.e. $\det(P) = 1$ if $P \in \mathcal{G}$.
  - $\mathcal{G}$ is closed under inverse (Solovay-Kitaev like theorem is still open w/o this).
  - $\langle \mathcal{G} \rangle$ is dense in $SU(2)$ meaning for any $U \in SU(2)$ and ε, $\exists$ a sequence $g_1 \cdots g_m$ s.t $d(U, g_1 \cdots g_m) \leq \varepsilon$, each $g_i \in \mathcal{G}$.
- We will use: $d(U,V) = \|U - V\|_2$ (other choices possible).

Fact 1: $d\left(I, e^{iH}\right) = \max_{\lambda} 2\left|\sin\frac{\lambda}{2}\right|$, λ are evals of H. where H Hermitian.

Pf: Do in class. (easy computation). if needed.

Fact 2: $d(I, e^{iH}) \leq \|H\|$

Pf: $d(I, e^{iH}) = \max_{\lambda} 2\left|\sin\frac{\lambda}{2}\right|$

But $\left|\sin\frac{\lambda}{2}\right| \leq \left|\frac{\lambda}{2}\right| = \frac{1}{2}|\lambda|$

$\Rightarrow 2\left|\sin\frac{\lambda}{2}\right| \leq |\lambda| \leq |\lambda_{max}|$ ∎.

Fact 3: if $|\lambda_{max}| \leq \pi$, $d(I, e^{iH}) = \|H\| + O(\|H\|)^3$.

Pf: Sin is increasing in $[-\pi/2, \pi/2]$.

So $d(I, e^{iH}) = 2\left|\sin\frac{\lambda_{max}}{2}\right|$, $\|H\| = |\lambda_{max}|$

$= 2\sin\frac{|\lambda_{max}|}{2}$

Then use Taylor's theorem. ∎.

Soloray - Kitaev Algorithm

function SK(U, depth n)

if (n==0)

Return Basic Approximation to U

else

$U_{n-1} = SK(U, \text{depth } n-1)$

$V, W = GC\text{-Decompose}(UU_{n-1}^*)$

$V_{n-1} = SK(V, \text{depth } n-1)$

$W_{n-1} = SK(W, \text{depth } n-1)$

$U_n = V_{n-1} W_{n-1} V_{n-1}^* W_{n-1}^* U_{n-1}$

Basic Approx. step.

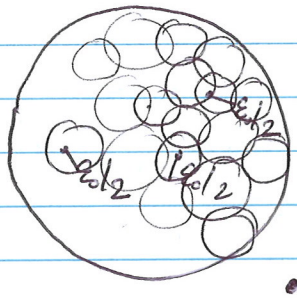
- $SU(2)$ is ~~isomor~~ diffeomorphic to $\mathbb{S}^3$.

$$\phi: \mathbb{C}^2 \to M(2, \mathbb{C})$$

$$\phi(\alpha, \beta) = \begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} \to$$ injective real linear map from $\mathbb{R}^4 \to \mathbb{R}^8$.

($\Rightarrow$ differential $d\phi$ also injective
$\Rightarrow \phi$ is an embedding)

$\Rightarrow$ $\mathbb{S}^3 \mapsto \phi(\mathbb{S}^3)$ is a compact connected submanifold of $\mathbb{R}^8$.



$\varepsilon/2$ net on $\mathbb{S}^3$

- Precompute a point in each ball of radius $\varepsilon/2$ (can be done as $\langle g \rangle$ is dense in $SU(2)$).
- Then these points form an ε-net on $SU(2) \sim \mathbb{S}^3$.

- Call this point set $\{p\}$, which is finite cardinality.
- each $p = g_1 \cdots g_\ell$, let $\ell_0 = \max_p \{\text{len}(p)\}$, and append I to each element in $\{p\}$, so all have length ℓ_0.

→ In basic approx step, given U, search $\{p\}$ for an ε_0 approx gate sequence

- done in constant time $O(1)$, as ~~$\{p\}$~~ $\{p\}$ is finite.

- Basic idea: Take a sequence monotonically strictly decreasing and going to 0 as a functi in of n.

  $\varepsilon_0 > \varepsilon_1 > \varepsilon_2 \cdots > \varepsilon_n \to 0.$

- SK (U, n) guaranteed to return ε_n approx to U.

- Claim: $\|U - U_{n-1}\| \leq \varepsilon_{n-1} \Rightarrow \|I - UU_{n-1}^*\| \leq \varepsilon_{n-1}$

  Pf: By unitary invariance of 2-norm.

  Let $\Delta = UU_{n-1}^*$.

  Claim: If $\|\tilde{\Delta} - \Delta\| \leq \varepsilon_n \Rightarrow \|\tilde{\Delta} U_{n-1} - U\| \leq \varepsilon_n$.

  Pf: By unitary invariance of 2 norm.

- Key fact that make S-K possible:
  - if Δ is close to identity, then one can find an improved approx to Δ quickly (using the exponential map).
  - this is done using the balanced group commutator.

- Balanced group commutator

  Thm: $U \in SU(2)$, and let $\|I - U\| < \varepsilon$. Then $\exists$ $V, W \in SU(2)$ s.t $VWV^*W^* = U$ and $\|I - V\|, \|I - W\| < c_{gc}\sqrt{\varepsilon}$, where c_{gc} is a const.

Pf (Sketch).

Key idea, Take V, W to be rotations about X, Y by same angle ϕ.

i.e. $V = R_x(\phi)$, $W = R_y(\phi)$.

Then $R_x(\phi) R_y(\phi) R_x(-\phi) R_y(-\phi) = R_{\hat{n}}(\theta)$.

where, $\sin\frac{\theta}{2} = 2\sin^2(\phi/2)\sqrt{1-\sin^4(\phi/2)}$.

Facts: (i) $U R_{\hat{n}}(\delta) U^* = R_{\hat{m}}(\delta)$, if U is unitary, and for some $\hat{m}$, $\hat{n}$ fixed.

(Ex). { (i) easy; (ii) slightly hard. } (ii) $\exists$ unitary U s.t $U R_{\hat{n}}(\delta) U^* = R_{\hat{m}}(\delta)$ for fixed $\hat{n}$, $\forall \hat{m}$.

Using these facts any $U \in SU(2)$, $U = R_{\hat{n}}(\theta)$ can be expressed as $U = \tilde{V}\tilde{W}\tilde{V}^*\tilde{W}^*$, where V, W are X, Y rotations as above, and $\tilde{V} = SVS^*$, $\tilde{W} = SWS^*$ for some unitary S.

Then simple computations give:

$d(I, \tilde{V}) < \sqrt{\frac{\varepsilon}{2}}$, $d(I, \tilde{W}) < \sqrt{\frac{\varepsilon}{2}}$, i.e. $\varepsilon_{gc} = \frac{1}{\sqrt{2}}$. ∎

This computation is $O(1)$ operation for any U.

— At the end of this you obtain V, W that satisfies the Thm.

Next goal: Approximate VWV^*W^*.

Claim: $V, W, \tilde{V}, \tilde{W}$ are unitaries, s.t $d(V,\tilde{V}) < \mu$, $d(W,\tilde{W}) < \mu$, $d(I,V) < \delta$, $d(I,W) < \delta$. Then:

$$d(VWV^*W^*, \tilde{V}\tilde{W}\tilde{V}^*\tilde{W}^*) < 8\mu\delta + 4\mu\delta^2 + 8\mu^2 + 4\mu^3 + \mu^4.$$

$\tilde{V} = V + \Delta V$, $\tilde{W} = W + \Delta W$.

Pf:

$$d(VWV^*W^*, \tilde{V}\tilde{W}\tilde{V}^*\tilde{W}^*)$$

$$< \| \Delta V W V^* W^* + V \Delta W V^* W^* + VW \Delta V^* W^* + VW V^* \Delta W^* \| + 6\mu^2 + 4\mu^3 + \mu^4.$$

$$< \| \Delta V W V^* W^* + VW \Delta V^* W^* \| + \| V \Delta W V^* W^* + VW V^* \Delta W^* \| + 6\mu^2 + 4\mu^3 + \mu^4.$$

~~Each term.~~

$$\| \Delta V W V^* W^* + VW \Delta V^* W^* \| < \| \Delta V V^* + V \Delta V^* \| + 4\mu\delta + 2\mu\delta^2.$$

by writing $W = I + \delta W$.

$$(V+\Delta V)(V+\Delta V)^* = I \Rightarrow \Delta V V^* + \Delta V V^* = -\Delta V \Delta V^*$$

$$\| \Delta V V^* + V \Delta V^* \| \leq \mu^2$$

Similarly other term.

Combine everything to get the result. ∎.

Corollary: Set $\Delta = \varepsilon_{n-1}$, $\delta = c_{gc}\sqrt{\varepsilon_{n-1}}$, then $d(VWV^*W^*, \tilde{V}\tilde{W}\tilde{V}^*\tilde{W}^*) < c_{approx}\,\varepsilon_{n-1}^{3/2}$ for ε_0 sufficiently small (but fixed).

c_{approx}: another fixed const. $\sim 8c_{gc} = 4\sqrt{2}$

▶ Set $\varepsilon_n = c_{approx}\,\varepsilon_{n-1}^{3/2}$

$\Rightarrow \dfrac{\varepsilon_n}{\varepsilon_{n-1}} = c_{approx}\sqrt{\varepsilon_{n-1}}$

if $\varepsilon_{n-1} < \dfrac{1}{c_{approx}^2} \Rightarrow \varepsilon_n < \varepsilon_{n-1}$

To have a guarantee $\varepsilon_0 > \varepsilon_1 > \varepsilon_2 \cdots > \varepsilon_n$, we need $\varepsilon_0 < \dfrac{1}{c_{approx}^2}$. (so choose smaller of the constants that make the statements true).

$\sim \dfrac{1}{32}$.

▶ Analysis.

$\varepsilon_n = c_{approx}\,\varepsilon_{n-1}^{3/2}$

$l_n = 5 l_{n-1}$

$t_n = 3 t_{n-1} + \text{const}$

const requires some discussion
— use of pointers
— do not output redundant sequences V^*, W^*.

$l_n = 5^n l_0$

$\varepsilon_n = \dfrac{1}{c_{approx}^2}\left(\varepsilon_0 c_{approx}^2\right)^{\left(\frac{3}{2}\right)^n}$

$t_n = O(3^n)$.

$\therefore \varepsilon_n \to 0.$

To obtain accuracy ε, we thus need

$$n = \left\lceil \frac{\ln\left(\frac{\ln(\varepsilon\, c_{approx}^2)}{\ln(\varepsilon_0\, c_{approx}^2)}\right)}{\ln(3/2)} \right\rceil .$$

$$l_\varepsilon = O\left(\ln^{\ln 5/\ln(3/2)}(1/\varepsilon)\right) \approx O\left(\ln^{3.97}(1/\varepsilon)\right)$$

$$t_\varepsilon = O\left(\ln^{\ln 3/\ln(3/2)}(1/\varepsilon)\right) \approx O\left(\ln^{2.71}(1/\varepsilon)\right).$$

$\gg$ $H + \pi/8$ universal (read from book).

$\gg$ Some open problems

1. Mutually unbiased bases. (MUB)

$\mathbb{C}^d$, $\{|e_1\rangle, \ldots, |e_d\rangle\}$, $\{|f_1\rangle, \ldots, |f_d\rangle\}$ are two orthonormal basis. They are called mutually unbiased iff.

$$|\langle e_j | f_k \rangle|^2 = 1/d \quad \forall\, j,k \in \{1, \ldots, d\}.$$

Q: How many mutually unbiased bases can you find for given d? $N(d)$.

What is known?

Let $d = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ is prime factorization.

where $p_1^{n_1} < p_2^{n_2} \ldots < p_k^{n_k}$

** Open quantum problems

oqp.iqoqi.univie.ac.at/open-quantum-problems

---

then $p_1^{n_1} + 1 \leq M(d) \leq d + 1$

so, if $d = p_1^{n_1}$, then $M(d)$ is completely known.

Open problem

$d = 6 = 2^1 \cdot 3^1$, $\quad 3 \leq M(6) \leq 7$

▸ Widely believed $M(6) = 3$, computer simulations have failed to locate otherwise.