$\boxed{\text{Ph 452}}$ Lecture 11

1Q1 Quick review

Approximation error $E(U,V)$. Today: $d(U,V) := E(U,V)$

- Errors add linearly

Universal gate basis examples

An <u>instruction set</u> is a UGB $\mathcal{G}$ s.t. $g \in \mathcal{G} \Rightarrow g^{-1} \in \mathcal{G}$.

<u>Utility:</u> If $d(g_k \cdots g_1, U) < \varepsilon$, then $d(g_1^\dagger \cdots g_k^\dagger, U^\dagger) < \varepsilon$

<u>Proof:</u>
$$\varepsilon > \| g_k \cdots g_1 - U \|$$
$$= \| g_1^\dagger \cdots g_k^\dagger \| \cdot \| g_k \cdots g_1 - U \| \cdot \| U^\dagger \|$$
$$\geq \| U^\dagger - g_1^\dagger \cdots g_k^\dagger \|$$

Is approximation efficiently achievable? Yes!

<u>Solovay-Kitaev Theorem:</u> Let $\mathcal{G}$ be a UGB. Then

$$(\forall \varepsilon > 0)(\exists c > 0)(\forall U \text{ s.t. } U^\dagger U = I)(\exists \text{ gate sequence } G \in \langle \mathcal{G} \rangle)$$
$$\left[d(G,U) < \varepsilon \quad \text{and} \quad |G| = \mathcal{O}(\log^c(1/\varepsilon)) \right]$$

Can efficient approximation be found efficiently? Yes!

<u>Solovay-Kitaev Algorithm:</u>

Finds G in time $\mathcal{O}(\log^{2.71}(1/\varepsilon))$
$|G| = \mathcal{O}(\log^{3.97}(1/\varepsilon))$ — G has redundancies in description

$\Rightarrow$ Algorithm $V_T \cdots V_1$ can be approximated using $\mathcal{G}$ with
$\mathcal{O}(T \log^{3.97}(T/\varepsilon))$ instructions
$\mathcal{O}(T \log^{2.71}(T/\varepsilon))$ compile time
(ea. gate V_i approximated to ε/T)

Ph 452 Lecture 11

NC appendix 3
KSV 8.3
Both inaccessible

Quantum Compiling [Dawson + Nielsen, QIC 6 (1) 81-95 (2006)]

time cost

```
Function Solovay-Kitaev ( Gate U, depth n) {

    if (n==0)
        return  ε0-Approx (U)
    else
        U_{n-1}  := Solovay-Kitaev (U, n-1)                    t_{n-1}
    [V, W]  := Group_Commutator-Approx (U U_{n-1}^†)           const
        V_{n-1}^†  := Solovay-Kitaev (V, n-1)                  t_{n-1}
        W_{n-1}  := Solovay-Kitaev (W, n-1)                    t_{n-1}
        return  V_{n-1} W_{n-1} V_{n-1}^† W_{n-1}^† U_{n-1}    const (use pointers to redundant info)
}
```

The group commutator of A and B is

$$[\![A,B]\!] := A B A^{-1} B^{-1}$$

$$= A B A^{\dagger} B^{\dagger} \quad \text{if } A, B \text{ are unitary}$$

c.f. "Quantum Safecracker"

Basic ideas:

sk is a recursive alg. Let's look @ base case

① ε_0-Approx (U) returns a gate sequence from $\mathcal{G}$ approximating U to within ε_0.

· Found by exhaustive search!

SU(d) has d^2-1 params
$d = 2^k$

If $\mathcal{G}$ has k-qubit gates ($2^k \times 2^k$ unitaries w/ $2^{2k}-1$ params), need $O(1/\varepsilon_0^{2^{2k}-1})$ sequences to find one ε_0-close to U.

answer as to why is subtle!

$\boxed{\text{Ph 452}}$ Lecture 11

There are $\mathcal{O}(|\mathcal{G}|^{\ell})$ length-ℓ sequences.

$\Rightarrow$ need all sequences of length $\ell_0 = \mathcal{O}\left(\frac{2^{2k}-1}{\log|\mathcal{G}|}\log(1/\varepsilon_0)\right)$

How small should ε_0 be? We'll get to that later

Numerically: $k=1$, $\mathcal{G} = \{H, T, T^{-1}\}$, $\varepsilon_0 = 0.14$ $\ell_0 = 16$ good enough

---

(2) Solovay-Kitaev(U, n) returns an ε_n-approx to U s.t. $\varepsilon_n \to 0$ as $n \to \infty$

(3) Group-Commutator-Approx$(UU_{n-1}^{\dagger})$ returns unitary V, W s.t.

$$d([V,W], UU_{n-1}^{\dagger}) < 4c^3 \varepsilon_{n-1}^{3/2}$$

$$d(I, V) < c\sqrt{\varepsilon_{n-1}}$$

$$d(I, W) < c\sqrt{\varepsilon_{n-1}}$$

$$c := 2^{\frac{k}{4}}\left(\frac{2^k-1}{2}\right)^{1/2} \to \underline{\text{constant}}$$

Great! We have is $UU_{n-1}^{\dagger}$, how do we extract ε_{n-1}? A: using this $\rightarrow$

$$\varepsilon_{n-1} := d(I, UU_{n-1}^{\dagger}) = d(U, U_{n-1})$$

(3) Solovay-Kitaev(U, n) returns an $\varepsilon_n = (4c^3+8c)\varepsilon_{n-1}^{3/2}$ approx to U because

$$d([\underbrace{V_{n-1}}, \underbrace{W_{n-1}}]U_{n-1}, U) \le \underbrace{(4c^3+8c)}_{b}\varepsilon_{n-1}^{3/2}$$

note: Not V & W but V_{n-1} & W_{n-1}

$\boxed{\text{Ph 452}}$ Lecture 11

Runtime:

$\varepsilon_n \le b\, \varepsilon_{n-1}^{3/2}$	$\varepsilon_n = \frac{1}{b^2}\left(\varepsilon_0 b^2\right)^{\left(\frac{3}{2}\right)^n}$ Tricky to solve for
$\ell_n = 5\,\ell_{n-1}$	$\ell_n = O(5^n)$
$t_n \le 3\, t_{n-1} + \text{const}$	$t_n = O(3^n)$

To get accuracy ε, choose n to be

$$n = \left\lceil \frac{\ln\left[\frac{\ln(1/\varepsilon b^2)}{\ln(1/\varepsilon_0 b^2)}\right]}{\ln(3/2)} \right\rceil$$

$$\Rightarrow \quad \ell_\varepsilon = O\left(\ln^{\ln 5/\ln(3/2)}(1/\varepsilon)\right)$$

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

$$\frac{\ln 5}{\ln 3/2} \approx 3.97, \qquad \frac{\ln 3}{\ln 3/2} \approx 2.71$$

$\boxed{\text{Ph 452}}$ Lecture 11

Algorithm analysis

Suppose Group-Commutator-Approx acts as promised.

Must show $d([\![V_{n-1}, W_{n-1}]\!] U_{n-1}, U) \le (4c^3 + 8c)\,\varepsilon_{n-1}^{3/2}$

Proof:

$$\mathcal{T} := d([\![V_{n-1}, W_{n-1}]\!] U_{n-1}, U) = d([\![V_{n-1}, W_{n-1}]\!], U U_{n-1}^\dagger)$$

$$\le d([\![V_{n-1}, W_{n-1}]\!], [\![V, W]\!]) + \underbrace{d([\![V, W]\!], U U_{n-1}^\dagger)}_{\le 4c^3 \varepsilon_{n-1}^{3/2} \text{ by GC-Approx}}$$

But $d(V_{n-1}, V) \le \varepsilon_{n-1} \Rightarrow V_{n-1} = V + \Delta_V \qquad \|\Delta_V\| \le \varepsilon_{n-1}$

$d(W_{n-1}, W) \le \varepsilon_{n-1} \Rightarrow W_{n-1} = W + \Delta_W \qquad \|\Delta_W\| \le \varepsilon_{n-1}$

$d(W, I) \le c\sqrt{\varepsilon_{n-1}} \Rightarrow W = I + \delta_W \qquad \|\delta_W\| \le c\sqrt{\varepsilon_{n-1}}$

$d(V, I) \le c\sqrt{\varepsilon_{n-1}} \Rightarrow V + I + \delta_V \qquad \|\delta_V\| \le c\sqrt{\varepsilon_{n-1}}$

So

$$[\![V_{n-1}, W_{n-1}]\!] = \overbrace{V W V^\dagger W^\dagger}^{[\![V,W]\!]} + \Delta_V W V^\dagger W^\dagger + V \Delta_W V^\dagger W^\dagger$$

$$+ V W \Delta_V^\dagger W^\dagger + V W V^\dagger \Delta_W^\dagger + O(\Delta^2)$$

$$d([\![V_{n-1}, W_{n-1}]\!], [\![V, W]\!]) \le \|\Delta_V V^\dagger + V \Delta_V^\dagger\| + \|\Delta_W W^\dagger + W \Delta_W^\dagger\|$$

$$+ 8\|\Delta\|\cdot\|\delta\| + O(\Delta\delta^2) + O(\Delta^2)$$

But $(V + \Delta_V)^\dagger (V + \Delta_V) = I = \overset{I}{\cancel{V^\dagger V}} + \Delta_V^\dagger V + V \Delta_V^\dagger + \Delta_V^\dagger \Delta_V$

So $\|\Delta_V V^\dagger + V \Delta_V^\dagger\| = \|-\Delta_V^\dagger \Delta_V\| = O(\Delta^2)$

$\boxed{\text{Ph 452}}$ Lecture 11

Hence

$$d([\![V_{n-1}, W_{n-1}]\!], [\![V,W]\!]) \le 8c\,\varepsilon_{n-1}^{3/2}$$

Got this far $\Rightarrow \Upsilon \le (8c + 4c^3)\,\varepsilon_{n-1}^{3/2} = b\,\varepsilon_{n-1}^{3/2}$ $\square$

How does Group-Commutator-Approx(UU_{n-1}) work?

We know $d(I, UU_{n-1}) \le \varepsilon_{n-1}$

(Gell-Mann matrices or FT of diag. basis of H)

① Find $H = H^\dagger$, $\operatorname{tr} H = 0$ s.t. $UU_{n-1} = e^{iH}$. [Must show how]

Then $d(I, UU_{n-1}) = \|H\| + O(\|H\|^3)$

② Find F, G satisfying [Must show how]

$F = F^\dagger, \quad G = G^\dagger$

$FG - GF = iH$

$\|F\|, \|G\| \le c\sqrt{\|H\|} \le c\sqrt{\varepsilon_{n-1}}$

✓ ③ Let $V := e^{iF}$, $W := e^{iG}$

Then $d(I, V) = \|F\| + O(\|F\|^3) \le c\sqrt{\varepsilon_{n-1}}$

$d(I, W) = \|G\| + O(\|G\|^3) \le c\sqrt{\varepsilon_{n-1}}$

$d([\![V,W]\!], U) < 4\left(\max(\|F\|, \|G\|)^3\right)$ [To Show]

$\le 4c^3\,\varepsilon_{n-1}^{3/2}$

$\boxed{\text{Ph 450}}$ Lecture 11

"Almost finished! Let's address the open points ①, ②, ③ in reverse order."

③ <u>Lemma 1</u>: Let $F = F^\dagger$, $G = G^\dagger$, $\|F\| < \delta$, $\|G\| < \delta$. Then

$$d\left(e^{iF} e^{iG} e^{-iF} e^{-iG},\ e^{GF-FG}\right) \le 4\delta^3$$

<u>Proof</u>: Taylor expand each term, use triangle inequality w/ abandon

② Let $H = H^\dagger$, $\operatorname{tr} H = 0$, $\dim H = 2^k$, $H \circ I = 0$ (H is 0 on diagonals) ← subtle point see paper.

Define $J := \frac{H}{\|H\|}$, $G' := \operatorname{diag}\left(\frac{-(2^k-1)}{2}, -\frac{(2^k-1)}{2}+1, \dots, \frac{2^k-1}{2}\right)$

$$F'_{jk} := \begin{cases} \dfrac{iJ_{jk}}{G'_{kk} - G'_{jj}} & \text{if } j \neq k \\ 0 & \text{if } j = k \end{cases}$$

Then $[F', G'] = iJ$, $F' = F'^\dagger$, and $G' = G'^\dagger$ by construction.

Also,

$$\|G'\| = \sqrt{\lambda_{max}(G'^\dagger G')} = \frac{2^k-1}{2}$$

$$\begin{aligned}
\|F'\| &= \sqrt{\lambda_{max}(F'^\dagger F')} \\
&\le \sqrt{\textstyle\sum \lambda_i (F'^\dagger F')} \\
&= \sqrt{\operatorname{tr}(U F'^\dagger F' U^\dagger)} \\
&= \sqrt{\operatorname{tr} F'^2} \\
&\le \sqrt{\operatorname{tr} J^2} \qquad (|f_{jk}| \le |J_{jk}|) \\
&= \sqrt{\textstyle\sum \lambda_i (J^\dagger J)} \\
&\le \sqrt{2^k \lambda_{max}(J^\dagger J)} \\
&= \sqrt{2^k \cancel{\|J\|}^{\,1}} \\
&= \sqrt{2^k}
\end{aligned}$$

$\boxed{\text{Ph 453}}$ Lecture 11

Define $F := F' \sqrt{\|H\|} \left(\frac{1}{\sqrt{2^k}}\right) 2^{k/4} \left(\frac{2^k-1}{2}\right)^{1/2}$

$$G := G' \sqrt{\|H\|} \left(\frac{2}{2^k-1}\right) 2^{k/4} \left(\frac{2^k-1}{2}\right)^{1/2}$$

Then

$[F, G] = iH$, $F = F^\dagger$, $G = G^\dagger$, and

$$\|F\| \leq \sqrt{\|H\|} \sqrt{2^k} \left(\frac{1}{\sqrt{2^k}}\right) 2^{k/4} \left(\frac{2^k-1}{2}\right)^{1/2} = c\sqrt{\|H\|}$$

$$\|G\| \leq \sqrt{\|H\|} \left(\frac{2^k-1}{2}\right)\left(\frac{2}{2^k-1}\right) 2^{k/4} \left(\frac{2^k-1}{2}\right)^{1/2} = c\sqrt{\|H\|}$$

Last step: Finding H

① Given unitary U, spse we could find H s.t.

$$U = e^{iH}, \quad H = H^\dagger, \quad \operatorname{tr} H = 0, \quad \lambda_i(H) \in [-\pi, \pi]$$

Then $d(I, U) = \|H\| + O(\|H\|^2)$

<u>Proof:</u> $\|I - e^{iH}\| = \|I - I - iH + \frac{(iH)^2}{2!} + \frac{(iH)^3}{3!} + \cdots\|$

$$\leq \|H\| + \frac{1}{2}\|H\|^2 + O(\|H\|^3)$$

How to find such an H? $H_0 = -i \ln U$, $H = H_0 - H_0 \circ I$

Diagonalize - take ln - "undiagonalize"

$\boxed{\text{Ph 452}}$ Lecture 11

How small does ε_0 have to be for $\mathcal{G}$ over k-bit gates?

$$c := 2^{\frac{k}{4}} \left(\frac{2^k - 1}{2} \right)^{1/2}$$

$$b := 8c + 4c^3 = 4(2c + c^3)$$

$\varepsilon_0 < 1/b$ for Solovay-Kitaev algorithm to work.

<u>k = 1:</u>

$$c = 2^{\frac{1}{4}} 2^{-1/2} = 2^{-1/4}$$

$$b = 4(2^{3/4} + 2^{-3/4}) \cong 9.1$$

$$\varepsilon_0 \leq 1/b < \frac{1}{9}$$

<u>k = 2:</u>

$$c = 2^{\frac{1}{2}} \left(\frac{3}{2} \right)^{1/2} = \sqrt{3}$$

$$b = 4(2\sqrt{3} + 3^{3/2}) = 34.6$$

$$\varepsilon_0 < 1/b < 1/34$$

<u>k = 3:</u>

$$c = 2^{\frac{3}{4}} \left(\frac{7}{2} \right)^{1/2} = 2^{\frac{1}{4}} 7^{1/2} = \sqrt{7\sqrt{2}}$$

$$b = 4(2\sqrt{7\sqrt{2}} + 2^{3/4} 7^{3/2}) = 149.7$$

$$\varepsilon_0 < 1/b < \frac{1}{149}$$