Lecture 7

14 FEB 2014

Last time, we proved that CNOT gates & single-qubit unitaries suffice to realize an arbitrary unitary <u>exactly</u>. However, there are many reasons for why we would want to restrict the gate set to be chosen as a discrete set (for simplicity & fault-tolerant applications). For this purpose, we need a notion of approximation. A natural measure is given by the operator norm:

$$\|A\|_\infty = \max_{\substack{|\psi\rangle : \\ \| |\psi\rangle \|_2 = 1}} \| A|\psi\rangle \|_2$$

Observe that $\|A\|_\infty^2$ is equal to the largest eigenvalue of $A^\dagger A$

It is a norm, so that

$$\|A\|_\infty = 0 \iff A = 0$$

$$\|A_1 + A_2\|_\infty \leq \|A_1\|_\infty + \|A_2\|_\infty$$

$$+ \quad \|cA\|_\infty = |c| \, \|A\|_\infty$$

+ in addition,

$$\|XY\|_\infty \leq \|X\|_\infty \|Y\|_\infty$$

$$\|X \otimes Y\|_\infty = \|X\|_\infty \|Y\|_\infty$$

$$\|U\|_\infty = 1 \qquad \text{for } U \text{ unitary}$$

We say that $\tilde{U}$ δ-approximates U if

$$\| U - \tilde{U} \|_\infty \le \delta$$

Furthermore, errors accumulate only linearly, i.e., if

$$\| U_i - \tilde{U}_i \|_\infty \le \delta_i \quad \forall i \in \{1, \dots, L\}$$

then

$$\| U_L \cdots U_2 U_1 - \tilde{U}_L \cdots \tilde{U}_2 \tilde{U}_1 \|_\infty \le \sum_i \delta_i$$

To prove this, just analyze case where $L = 2$

$$\| U_2 U_1 - \tilde{U}_2 \tilde{U}_1 \|_\infty =$$

$$\| U_2 U_1 - U_2 \tilde{U}_1 + U_2 \tilde{U}_1 - \tilde{U}_2 \tilde{U}_1 \|_\infty$$

$$\le \| U_2 U_1 - U_2 \tilde{U}_1 \|_\infty + \| U_2 \tilde{U}_1 - \tilde{U}_2 \tilde{U}_1 \|_\infty$$

$$= \|U_2(U_1 - \tilde{U}_1)\|_\infty + \|(U_2 - \tilde{U}_2)U_1\|_\infty$$

$$= \|U_1 - \tilde{U}_1\|_\infty + \|U_2 - \tilde{U}_2\|_\infty$$

$$= \delta_1 + \delta_2$$

for general case, proceed in a similar way by induction

Proceeding, we define an instruction set G for a qubit to be a finite set of gates such that

1) $g \in G \Rightarrow g \in SU(2)$ (unitary w/ determinant 1)
2) For $g \in G$, $g^{-1} \in G$
3) G is universal for $SU(2)$. That is, $\forall\, U \in SU(2)$ & $\varepsilon > 0$ $\exists\, g_1, \ldots, g_L$ such that

$$\|g_L \cdots g_1 - U\|_\infty \le \varepsilon$$

To illustrate the importance of the approximation, suppose that someone has an implementation of a q. algorithm using gates $U_1, \ldots, U_m$. However, not all of these will be in the instruction set, so that it will be necessary to compile each gate U_i using our instruction set. If overall accuracy should be ε, then each unitary U_j will require accuracy ε/m. Now suppose that an accuracy $\delta > 0$ requires length $O(\frac{1}{\delta})$, then each unitary U_j requires a sequence of length $O(\frac{m}{\varepsilon})$ so that overall the number of gates needed will be $O(m^2/\varepsilon)$. This blowup will remove quantum speedups for Grover's alg.

We now go through a proof of the Solovay-Kitaev theorem.

Begin w/ the "workhorse lemma" behind ~~the~~ an algorithms that proves the theorem

Lemma: Let V, W, $\underbrace{\tilde{V}, \& \tilde{W}}_{\text{approximations of } V \& W}$ be unitaries such that

$$\|I - V\|, \|I - W\| \leq \delta$$

$$\|\tilde{V} - V\|, \|\tilde{W} - W\| \leq \Delta$$

$$\Rightarrow \|\tilde{V}\tilde{W}\tilde{V}^\dagger\tilde{W}^\dagger - VWV^\dagger W^\dagger\| = O(\Delta^2 + \delta\Delta)$$

"group commutator of $V \& W$ is well approximated by group commutator of $\tilde{V} \& \tilde{W}$"

Proof: Let $\Delta_V = \tilde{V} - V$

$$\Delta_W = \tilde{W} - W$$

group commutator quantifies the degree to which ~~two~~ operators fail to be commutative for example, where the gain is only quadratic. So we will need something better than this...

This is given by the Solovay-Kitaev theorem: (interesting history)

(SK): Let G be an instruction set for $SU(2)$ & let $\varepsilon > 0$. Then $\exists$ $c > 0$ such that $\forall U \in SU(2)$ $\exists$ a finite sequence S of gates from G of length $O(\log^c(1/\varepsilon))$ & such that

$$\|S - U\|_\infty \leq \varepsilon$$

Going back to the example, for overall accuracy $\varepsilon > 0$, each gate needs accuracy ε/m so that length is $O(\log^c(m/\varepsilon))$ & overall length is $O(m \log^c(m/\varepsilon))$. good for applications...

$$\tilde{V}\tilde{W}\tilde{V}^{+}\tilde{W}^{+} = (V+\Delta_V)(W+\Delta_W)(V^{+}+\Delta_V^{+})(W^{+}+\Delta_W^{+})$$

$$= VWV^{+}W^{+} \quad +$$

1st order terms

$$\Delta_V W V^{+} W^{+} + V\Delta_W V^{+} W^{+} +$$

$$V W \Delta_V^{+} W^{+} + V W V^{+} \Delta_W^{+} +$$

$$O(\Delta^2)$$

Focus on bounding

$$\Delta_V W V^{+} W^{+} + V W \Delta_V^{+} W^{+}$$

Let $\delta_W = W - I$, Then

$$= \Delta_V (I+\delta_W) V^{+}(I+\delta_W^{+}) +$$

$$V(I+\delta_W)\Delta_V^{+}(I+\delta_W^{+})$$

$$= \Delta_V V^{+} + V\Delta_V^{+} + O(\delta\Delta)$$

Since $\tilde{V} = V + \Delta_V$ is unitary

$$I = \tilde{V}\tilde{V}^{+} = (V+\Delta_V)(V^{+}+\Delta_V^{+})$$

$$= I + \Delta_V V^{+} + V\Delta_V^{+} + O(\Delta^2)$$

$$\Rightarrow \Delta_V V^\dagger + V\Delta_V^\dagger = O(\Delta^2)$$

$$\Rightarrow \tilde{V}\tilde{W}\tilde{V}^\dagger\tilde{W}^\dagger = VWV^\dagger W^\dagger + O(\delta\Delta) + O(\Delta^2)$$

$\square$

"Magical part" is that by starting w/ some approximation of V & W, we get a better approximation to the group commutator of V & W.

We can now present the recursive Solovay-Kitaev algorithm:

```
SK (unitary U, recursion depth n)
    If (n=0)
        return basic approximation
            to U w/ accuracy ≤ ε₀ = 1/1000
    If (n>0)
        U_{n-1} = SK(U, n-1)
        Find operators V & W such
         that 1) U U_{n-1}^† = V W V^† W^†
              2) ||I-V||, ||I-W|| = O(√ε_{n-1})
        Ṽ = SK(V, n-1), W̃ = SK(W, n-1)
        return Ṽ W̃ Ṽ^† W̃^† U_{n-1}
```

Explanation

Line 1: SK accepts two arguments:

a) the unitary we want to approximate

b) & a recursion depth (this will be a function of desired accuracy ε)

It returns an ε_n - approximation of U. Idea is that each level of recursion reduces error, so that

$$\varepsilon_n < \varepsilon_{n-1} < \dots < \varepsilon_1 < \varepsilon_0$$

We will see that

$$\varepsilon_n = O\left(\varepsilon_{n-1}^{3/2}\right),$$ so that

error decreases doubly exponentially fast w/ recursion depth n.

Lines 2-3:

$n=0$ is the lowest level of the recursion tree.

Here we simply tabulate by brute force an ε_0-net for all unitaries $U \in SU(2)$. I.e., we make a table of U_i such that

$$\forall U \in SU(2) \quad \| U_i - U \|_\infty \leq \varepsilon_0$$

where $U_i = g_{i,1} \cdots g_{i,m_i}$

w/ $g_{i,j} \in G$

The cost associated w/ this level is considered to be constant as a function of ε_0.

can do this w/ H + T gate b/c they ~~are~~ form a dense subgroup of $SU(2)$.

Line 5: Call SK recursively to find U_{n-1} which is an ε_{n-1} approximation of U

(where $\varepsilon_{n-1} > \varepsilon_n$)

$$\|U - U_{n-1}\| \leq \varepsilon_{n-1}$$

$$\Rightarrow \|U U_{n-1}^{\dagger} - I\| \leq \varepsilon_{n-1} \quad \text{(unitary invariance)}$$

Suppose line 6 is possible (for now, but justify later)

Then in Line 7:

$\tilde{V}$ is an ε_{n-1}-approx. to V &

$\tilde{W}$ " " " " " W

By the lemma + assumption that Line 6 works correctly, since we have

$$\|I-V\|, \|I-W\| \leq O(\sqrt{\varepsilon_{n-1}}) \ \&$$

$$\|\tilde{V}-V\|, \|\tilde{W}-W\| \leq \varepsilon_{n-1}$$

we can conclude that

$$\|\tilde{V}\tilde{W}\tilde{V}^{+}\tilde{W}^{+} - VWV^{+}W^{+}\| \leq O(\varepsilon_{n-1}^{2} + \sqrt{\varepsilon_{n-1}}\cdot\varepsilon_{n-1})$$

$$\| \qquad\qquad = O(\varepsilon_{n-1}^{3/2})$$

$$\|\tilde{V}\tilde{W}\tilde{V}^{+}\tilde{W}^{+} - UU_{n-1}^{+}\| = O(\varepsilon_{n-1}^{3/2})$$

$$\Rightarrow \|\tilde{V}\tilde{W}\tilde{V}^{+}\tilde{W}^{+}U_{n-1} - U\| = O(\varepsilon_{n-1}^{3/2})$$

so last step is to return

$\tilde{V}\tilde{W}\tilde{V}^{+}\tilde{W}^{+}U_{n-1}$ as an

$\varepsilon_n = O(\varepsilon_{n-1}^{3/2})$ approximation of U

Analysis of the Algorithm:

n	ε_n	# gates
		$l_n = 5\, l_{n-1}$ (5 calls to SK in algorithm at R.D. n)
0	ε_0	$l_0 = O(1)$
1	$\varepsilon_0^{3/2}$	$5\, l_0$
2	$\left((\varepsilon_0)^{3/2}\right)^{3/2} = \left(\varepsilon_0^{3/2}\right)^2$	$5^2\, l_0$
⋮		
n	$(\varepsilon_0)^{(3/2)^n}$	$5^n\, l_0$

For accuracy ε we want

$$(\varepsilon_0)^{(3/2)^n} < \varepsilon \Rightarrow n = O\left(\log \log \tfrac{1}{\varepsilon}\right)$$

16

$\Rightarrow l_n = \left(\log\left(\frac{1}{\varepsilon}\right)\right)^c$

Need to explain line 6

Given U such that

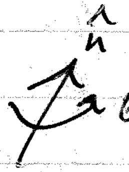
$\|U - I\| \leq \varepsilon$ Find V & W such that

$U = VWV^\dagger W^\dagger$

$\|V - I\|, \|W - I\| \leq O(\sqrt{\varepsilon})$

for qubits, unitaries $\leftrightarrow$ 3D rotations

U can be written as



$$R(\hat{n}, \theta) = \exp\left(i \frac{\theta}{2} \hat{n} \cdot (X, Y, Z)\right)$$

Observation:

$$R(\hat{x}, \theta) R(\hat{y}, \theta) R(\hat{x}, -\theta) R(\hat{y}, -\theta) = R(\hat{z}, O(\theta^2))$$

17

can see geometrically or

can see mathematically

~~dr~~ expand exponential & drop quadratic or higher terms

$$\left(I+i\frac{\theta}{2}X\right)\left(I+i\frac{\theta}{2}Y\right)\left(I-i\frac{\theta}{2}X\right)\left(I-i\frac{\theta}{2}Y\right)$$
$$= I + O(\theta^2)$$

suffices to prove claim

$\theta^2 = \varepsilon$ & $\theta = \sqrt{\varepsilon}$

almost done, but just need to rotate coordinate system so that $\hat{n} = \hat{z}$ & this proves the claim.