Ph/CS 219A
Quantum Computation

Lecture 12. Quantum Circuits (continued)

Last time we discussed quantum circuits, establishing these facts:

(1) We can simulate an ideal quantum circuit with T gates using noisy gates if the error per gate is $\mathrm{O}(1/T)$.
(2) To accurately approximate a typical unitary transformation acting on *n* qubits, a quantum circuit with size exponential in *n* is required.
(3) A quantum circuit with T = poly(*n*) gates can be simulated by a classical computer with memory size poly(*n*), though the classical circuit may need to have exponential size.
(4) Any unitary transformation can be constructed *exactly* as a circuit of two-qubit gates.

Today we will consider further the task of approximating a unitary transformation using a finite universal gate set. We will see that:
(1) A single generic two-qubit gate is universal for quantum computing.
(2) One universal gate set can efficiently simulate any other universal gate set.

See Chapter 5 of the Lecture Notes. Note that Problem Set 3 has been posted, due November 20.

Finite universal gate sets

Universal set of unitary quantum gates $\{U_1, U_2, \ldots, U_{n_G}\}$.

V is target unitary in $SU(2^n)$. $\tilde{V}$ is a circuit. We want: $\| \tilde{V} - e^{i\phi} V \|_{\sup} \leq \epsilon$.

Example: $\{\left(e^{2\pi i \alpha Z}\right)^k, k = 1, 2, 3, \ldots\}$, α irrational. Dense in rotations about the z axis.

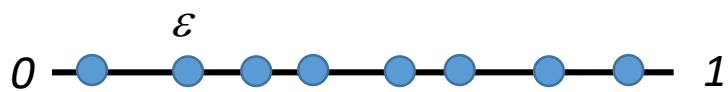
Consider points on the unit interval $[0,1)$, $\{\alpha k \pmod 1, \quad k = 1, 2, 3, \ldots\}$.

All points are distinct. Else $\alpha k = \alpha k' + \text{integer} \Rightarrow \alpha = \text{integer} / (k - k') = \text{rational}$.

If $K\epsilon > 1$, then $\exists \quad k, k' < K$ such that $| k\alpha - k'\alpha \pmod 1 | \leq \epsilon$.

(K points, with neighboring points distance ϵ apart, would not fit in the interval.)

Hence $|(k - k')\alpha \times \text{integer} \pmod 1|$ comes within distance ϵ of each point on the interval.



Generic $N \times N$ unitary: $U = \text{diag}(e^{2\pi i \alpha_1}, e^{2\pi i \alpha_2}, e^{2\pi i \alpha_3}, \ldots, e^{2\pi i \alpha_N})$.

The α_j and the ratios α_j / α_k are irrational.

Powers of U are dense in $U(1)^N$: $\text{diag}(e^{i\theta_1}, e^{i\theta_2}, e^{i\theta_3}, \ldots, e^{i\theta_N})$.

Finite universal gate sets

For generic e^{iA} and e^{iB}, we can "reach" $e^{i\alpha A}$ and $e^{i\beta B}$.

Lie algebra: We can also reach $e^{i(\alpha A+\beta B)}$ and $e^{i\gamma[A,B]}$.

(1) $$\lim_{n\to\infty}(e^{i\alpha A/n}e^{i\beta B/n})^n=\lim_{n\to\infty}\left(1+\frac{i}{n}(\alpha A+\beta B)+O\left(\frac{1}{n^2}\right)\right)^n=e^{i(\alpha A+\beta B)}.$$

(2) $$\lim_{n\to\infty}\left(e^{iA/\sqrt{n}}e^{iB/\sqrt{n}}e^{-iA/\sqrt{n}}e^{-iB/\sqrt{n}}\right)^n=\left(1+\frac{1}{n}\left(-AB+A^2+AB+BA+B^2-AB-\frac{1}{2}\left(A^2+B^2+A^2+B^2\right)\right)+\ldots\right)^n$$

$$=\lim_{n\to\infty}\left(1-\frac{1}{n}\left(AB-BA\right)+O\left(\frac{1}{n^{3/2}}\right)\right)^n=e^{-[A,B]},$$

Two generic noncommuting elements of $\mathrm{SU}(2)$ generate all of $\mathrm{SU}(2)$. Choosing suitable axes on the Bloch sphere, these two elements are exponentials of

$$\alpha Z,\quad \beta Z+\gamma X\quad\Rightarrow\quad[\alpha Z,\beta Z+\gamma X]=i\alpha\gamma Y.$$

Finite universal gate sets

The same ideas apply to two-qubit gates. The group $\mathrm{SU}(4)$ has 15 generators. Two noncommuting elements of the Lie algebra generically "close" on the whole algebra. This fails only if some nested commutators vanish "by accident" --- which is nongeneric.

In fact, as we've seen, powers of a generic element of $\mathrm{SU}(4)$ are dense in $\mathrm{U}(1)^3$, and there is no subgroup of $\mathrm{SU}(4)$ that contains two noncommuting subgroups. So circuits built from two generic elements of $\mathrm{SU}(4)$ are dense in $\mathrm{SU}(4)$.

Furthermore, U and $V = (\mathrm{SWAP})\ U\ (\mathrm{SWAP})$ are generically noncommuting. So just one generic two-qubit gate is sufficient, if we can choose the "order" of the two qubits when the gate is applied.

Since two-qubit gates are exactly universal, circuits constructed using one generic two-qubit gate already suffice to approximate any unitary.

Nongeneric gates might, of course, fail to be universal. For example, Hadamard H and S (90 degree rotation about *z* axis) generate the symmetry group of a square, a finite subgroup of $\mathrm{SU}(2)$.

But circuits built from H and T (45 degree rotation about the *z* axis) are dense in $\mathrm{SU}(2)$.

Solovay-Kitaev approximation

So far our focus has been on *reachability*, but what about *complexity*? How large a circuit suffices to provide a good approximation to a target unitary?

Suppose a finite repertoire $\mathcal{R}$ of elements of $\mathrm{U}(N)$ ("gates") provides an ε-net: every element of $\mathrm{U}(N)$ is within distance ε (in the sum norm) of an element of $\mathcal{R}$. Suppose also that the repertoire is "closed under inverse": For each unitary $V \in \mathcal{R}$, V^{-1} is also in $\mathcal{R}$.

Claim: Circuits of size 5, constructed from these gates, provide a repertoire $\mathcal{R}'$, also closed under inverse, which is an ε'-net, where $\varepsilon' = C\varepsilon^{3/2}, \quad C = \text{constant}.$

What this implies: Start with repertoire $\mathcal{R}_0$, an ε_0-net, where $\varepsilon_0 < 1/C^2$. According to the claim, circuits of 5 gates from $\mathcal{R}_0$ provide an ε_1-net $\mathcal{R}_1$, where $\varepsilon_1 = C\varepsilon_0^{3/2} = \left(C^2\varepsilon_0\right)^{1/2}\varepsilon_0 < \varepsilon_0,$ a finer net.

Iterate this k times:

$$C^2\varepsilon_k = \left(C^2\varepsilon_{k-1}\right)^{3/2} \quad \Rightarrow \quad C^2\varepsilon_k = \left(C^2\varepsilon_0\right)^{(3/2)^k} \quad \Rightarrow \quad \left(\frac{3}{2}\right)^k = \frac{\log\left(1/C^2\varepsilon_k\right)}{\log\left(1/C^2\varepsilon_0\right)}$$

achieved with circuit size L_k, where:

$$L_k / L_0 = 5^k = \left(\left(\frac{3}{2}\right)^k\right)^{\log 5/\log(3/2)} = \left(\frac{\log\left(1/C^2\varepsilon_k\right)}{\log\left(1/C^2\varepsilon_0\right)}\right)^{\log 5/\log(3/2)} \quad \Rightarrow$$

We can approximate any unitary to accuracy ε using a circuit with polylog($1/\varepsilon$) gates

Solovay-Kitaev approximation

Claim: Circuits of size 5, constructed from these gates, provide a repertoire $\mathcal{R}'$, also closed under inverse, which is an ε'-net, where

$$\varepsilon' = C\varepsilon^{3/2}, \quad C = \text{constant}.$$

To prove the claim:

For $U \in \mathrm{U}(N)$, there is $\tilde{U} \in \mathcal{R}$ such that $\|U - \tilde{U}\|_{\sup} \le \varepsilon \quad \Rightarrow \quad \|U\tilde{U}^{-1} - I\|_{\sup} \le \varepsilon.$

We are to construct W as a circuit of four elements of $\mathcal{R}$ such that $\|U\tilde{U}^{-1} - W\|_{\sup} \le \varepsilon'.$

Then $\|U - W\tilde{U}\|_{\sup} \le \varepsilon'$, where $W\tilde{U}$ is a circuit of five elements of $\mathcal{R}$.

To find W : $U\tilde{U}^{-1} = e^{iA}$, where $A = O(\varepsilon) \Rightarrow \exists$ Hermitian $B, C = O(\varepsilon^{1/2})$ such that $[B, C] = -iA$.

Furthermore, $\exists\, e^{i\tilde{B}}, e^{i\tilde{C}} \in \mathcal{R}$, which are ε-close to $e^{iB}, e^{iC} \quad \Rightarrow \quad B - \tilde{B} = O(\varepsilon)$ and $C - \tilde{C} = O(\varepsilon)$.

Recalling $\mathcal{R}$ closed under inverse, construct : $W = e^{i\tilde{B}} e^{i\tilde{C}} e^{-i\tilde{B}} e^{-i\tilde{C}} = I - [\tilde{B}, \tilde{C}] + O(\varepsilon^{3/2})$

$$\Rightarrow \quad W = I - [B + O(\varepsilon), C + O(\varepsilon)] + O(\varepsilon^{3/2}) = I + iA + O(\varepsilon^{3/2}) = e^{iA} + O(\varepsilon^{3/2}).$$

That shows $\mathcal{R}'$ is an ε'-net where $\varepsilon' = O(\varepsilon^{3/2})$; we also see that inverse of W is in $\mathcal{R}'$.

Solovay-Kitaev approximation

Claim: Circuits of size 5, constructed from these gates, provide a repertoire $\mathcal{R}'$, also closed under inverse, which is an ε'-net, where $\varepsilon' = C\varepsilon^{3/2}, \quad C = \text{constant}.$

The Solovay-Kitaev algorithm provides a method for constructing a circuit of size polylog($1/\varepsilon$) that approximates any target unitary, to error ε. The classical cost of finding this circuit is also polylog($1/\varepsilon$), because each step of the recursive procedure increases the classical cost by a constant factor.

What makes it possible to build a circuit of gates, all with error O(ε), such that the error of the circuit is smaller: O($\varepsilon^{3/2}$)? It works because we have carefully arranged for the leading O(ε) error to cancel. For this it was important that the gate set is closed under inverse.

Suppose we have compiled an algorithm as a size-T circuit of two-qubit gates, but these gates are not in our hard-wired universal set? We approximate each gate in that ideal circuit to accuracy O($1/T$). According to Solovay-Kitaev, this blows up the size of the circuit by only a polylog(T) factor.

For some gate sets, we can improve the Solovay-Kitaev estimate from O($\log^{3.97}(1/\varepsilon)$) to O($\log(1/\varepsilon)$). We can't do better than that, because we've seen that an ε-net requires circuit size

$T \geq 2^{2n} \frac{\log(C/\varepsilon)}{\log(\text{poly}(n))}$, that is, $\Omega(\log(1/\varepsilon))$, for fixed n.

Coming next: The power of quantum computing

The rest of this course concerns the power and potential applications of quantum computing.

We don't know how to prove from first principles that quantum computers are more powerful than classical computers (BQP strictly larger than BPP), but we believe it is true.

We'll discuss:

-- Efficient quantum algorithms that solve problems we don't know how to solve efficiently with a classical computer, e.g., factoring and simulation of quantum systems.

-- "Relativized speedups": The "black box model" = "oracle model" = "query model" in which we can prove a separation between classical and quantum computing (though the practical implications of these results are not entirely clear).

-- Polynomial speedups, such as $T_{quantum} \sim (T_{classical})^{1/2}$. Not relevant to BQP $\neq$ BPP, but nonetheless interesting.