Ph/CS 219A
Quantum Computation

Lecture 11. Quantum Circuits

Last time we discussed randomized and reversible classical circuits, leading into the formulation of the quantum circuit model.

Today we develop the quantum circuit model further, addressing several key questions:

(1) How accurate should quantum gates be, in order to be computationally useful?
(2) How large a quantum circuit is needed to accurately approximate a typical unitary transformation?
(3) What resources suffice for a classical computer to simulate a quantum computer?
(4) How do we construct universal quantum gates?

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

Quantum Circuits

A more powerful computational model (or so we believe).

1) Qubits $\mathcal{H}_n = \left(\mathcal{H}_2\right)^{\otimes n} = \text{span}\{|x\rangle, \quad x = 0,1,2,\ldots,2^n - 1\}$.

Preferred decomposition into small subsystems, because "physics is local."

2) Initialization $|000\ldots0\rangle$. We can cool a register close to absolute zero, relatively easily.

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

Finite instruction set. Each acts on a constant number of qubits (e.g. two). *Universal* means we can approximate any *n*-qubit unitary to high accuracy.

4) Classical control. A classical computer builds a circuit and directs its execution.

5) Readout of one or more qubits in the standard basis $\{|0\rangle, |1\rangle\}$. Hence the quantum model is a randomized computational model. (Measurements can be delayed until the end of the computation.)

This model (1)--(5) can be simulated by a randomized classical computer, but not *efficiently.* Reversible classical computation is a special case, because permutations of basis states are unitary. Randomized computation is a special case, because we can flip a coin by measuring an *X* eigenstate in the *Z* basis.

There is a quantum analog of BPP: BQP = bounded-error quantum polynomial time.

$$\text{BQP} = \{\text{languages decided by polynomial-size uniform quantum circuit families}\}$$

Accuracy

Ideal quantum circuit: $|\varphi_T\rangle = U_T U_{T-1} \ldots U_2 U_1 |\varphi_0\rangle.$

Noisy quantum circuit: $|\tilde{\varphi}_T\rangle = \tilde{U}_T \tilde{U}_{T-1} \ldots \tilde{U}_2 \tilde{U}_1 |\tilde{\varphi}_0\rangle.$ Acts on data *and* environment.

$\tilde{U}_t = U_t + E_t.$ Suppose $\| E_t \|_{\sup} \le \epsilon.$ How small does this error need to be?

Suppose the final measurement projects onto a complete basis. (If complete probability distributions are close, then so are marginal distributions.) Recall from homework …

$$p(x) = |\langle x|\varphi_T\rangle|^2, \quad \tilde{p}(x) = |\langle x|\tilde{\varphi}_T\rangle|^2 \quad \Rightarrow \quad \frac{1}{2}\|\tilde{p} - p\|_1 = \frac{1}{2}\sum_x |\tilde{p}(x) - p(x)| \le \| |\tilde{\varphi}_T\rangle - |\varphi_T\rangle \| .$$

Error needs to a sufficiently small constant δ. How does the error accumulate as the circuit is executed?

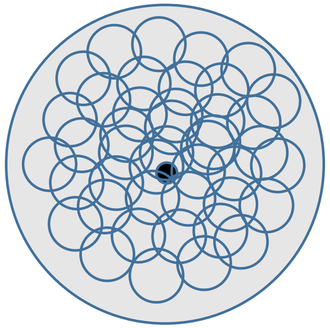
$$\tilde{U} = U_T U_{T-1} \ldots U_2 U_1 + \tilde{U}_T \tilde{U}_{T-1} \ldots \tilde{U}_2 E_1 + \tilde{U}_T \tilde{U}_{T-1} \ldots \tilde{U}_3 E_2 U_1 + \tilde{U}_T \tilde{U}_{T-1} \ldots \tilde{U}_4 E_3 U_2 U_1 + \ldots + E_T U_{T-1} \ldots U_2 U_1$$

$$\Rightarrow \quad \|\tilde{U} - U\|_{\sup} = \| T \text{ terms} \|_{\sup} \le T\epsilon \quad \Rightarrow \quad \text{suffices if} \quad \epsilon < \delta / T.$$

That is not so bad, but not so good either. Fortunately, the theory of quantum error correction and fault-tolerant quantum computing shows that actually it suffices for the error per gate to be less than a sufficiently small constant, at the cost of a polylog(T) increase in circuit size.

Most unitary transformations require large quantum circuits

$$N_{\text{balls}} \ge \frac{\text{Vol}(U(N))}{\text{Vol}(\delta\text{-ball})}, \quad N = 2^n, \quad \Rightarrow \quad N_{\text{balls}} \ge \left(\frac{C}{\delta}\right)^{N^2} = \left(\frac{C}{\delta}\right)^{2^{2n}}.$$



Number of constant radius balls needed to cover all *n*-qubit unitaries is *doubly exponential* in *n*.

Number of quantum circuits of size T: $\quad N_T \le \left(\text{poly}(n)\right)^T \quad \Rightarrow \quad T \ge 2^{2n}\frac{\log(C/\delta)}{\log(\text{poly}(n))}.$

With quantum circuits of polynomial size we can "reach" (approximately with constant error) only an exponentially small portion of the unitary group acting on *n* qubits.

This also applies to the unitaries we can reach by evolving for time poly(*n*) according to a Schroedinger equation governed by any physically reasonable Hamiltonian.

Not only that, but reaching a typical quantum state starting from any initial state (such as a product state) also requires an exponentially large quantum circuit. Hilbert space is *BIG*. For quantum states, unlike for classical bit strings, it makes sense to speak of the complexity of a *state*, as well as of a computation.

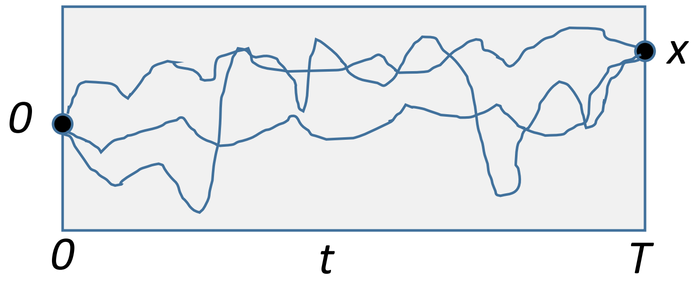
Classical simulation of quantum circuits

We can simulate a quantum circuit using a classical computer by evaluating a product of $2^n \times 2^n$ matrices. That simulation would require an exponentially large classical memory. Can we do the simulation using only a memory of poly(n) size? In fact we can: BQP $\subseteq$ PSPACE.

We want to calculate $\mathrm{Prob}(x) = |\langle x | U | 0 \rangle|^2$ where U is a circuit constructed from T gates.

$$\langle x | U | 0 \rangle = \sum_{\{x_t\}} \langle x | U_T | x_{T-1} \rangle \langle x_{T-1} | U_{T-1} | x_{T-2} \rangle \ldots \langle x_2 | U_2 | x_1 \rangle \langle x_1 | U_1 | 0 \rangle.$$

Repeatedly sum over a complete basis ("Feynman path integral").



We sum up $2^{n(T-1)}$ complex numbers, one for each computational path. Each of these numbers is obtained by multiplying together T numbers. However, most of these numbers are zero.

A classical circuit computes each $\langle z | U_t | y \rangle$.

This is easy because each gate acts on a constant number of qubits (*e.g.* 2 qubits). The matrix element vanishes unless all other computational basis states match between left and right.

Each matrix element is estimated to accuracy scaling like $\frac{1}{T} 2^{-n(T-1)}$.

Storing matrix elements of quantum gates to $nT \log T$ bits of precision is sufficient.

Universal quantum gates

Finite instruction set: $\mathcal{G} = \{U_1, U_2, \ldots, U_m\}$, U_j acts on $k_j \le k$ qubits (any k_j out of n).

Universality means that circuits constructed from can come arbitrarily close (*e.g.* in the sup norm) to any specified unitary acting on *n* qubits. We may also consider *encoded universality*, meaning circuits are dense in some exponentially large subgroup of $U(2^n)$.

(1) *Exact universality* (uncountable instruction set). Two-qubit gates are exactly universal. So are single-qubit gates together with *any* entangling two-qubit gate.

(2) *Generic universality*. *Almost any* two-qubit gate is universal, if it can be applied to any pair among the *n* qubits.

(3) *Particular finite universal gate sets* (Problem set 3). $\mathcal{G} = \{H, \Lambda(S)\}, \quad \{H, T, \Lambda(X)\}, \quad \{H, S, \Lambda^2(X)\}$

$$\Lambda(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U, \quad \Lambda^2(U) = \left(I - |11\rangle\langle 11|\right) \otimes I + |11\rangle\langle 11| \otimes U.$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad S = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}, \quad T = \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}.$$

Exact universality of two-qubit gates

Two steps: (1) Every unitary is a product of "2×2 unitaries". (2) Every 2×2 unitary can be constructed as a circuit of two-qubit unitaries.

A 2×2 unitary acting on an *N*-dimensional vector space has only two nonzero off-diagonal entries. It is a *direct sum* of a unitary acting on two basis states, and the identity acting on the remaining *N* -2 basis states.

A two-qubit unitary acting on an *n*-qubit space is a *direct product* of a unitary acting on 2 qubits and the identity acting on the remaining *n*-2 qubits.

To prove step (1): $U|0\rangle = \sum_{i=0}^{N-1} a_i |i\rangle \quad \Rightarrow \quad \exists$ product of $(N\text{-}1)$ 2×2 unitaries W_0 such that $U|0\rangle = W_0|0\rangle$.

$$|0\rangle \mapsto a_0|0\rangle + b_0|1\rangle, \quad b_0|1\rangle \mapsto a_1|1\rangle + b_1|2\rangle, \quad b_1|2\rangle \mapsto a_2|2\rangle + b_2|3\rangle,$$
$$\ldots \quad , \quad b_{N-2}|N-2\rangle \mapsto a_{N-2}|N-2\rangle + a_{N-1}|N-1\rangle.$$

Next, let $U_1 = W_0^{-1}U$. Then $U_1|0\rangle = |0\rangle$. That is, U_1 is $(N-1)\times(N-1)$ unitary.

$\Rightarrow \quad \exists$ product of $(N\text{-}2)$ 2×2 unitaries W_1 such that $U_1|1\rangle = W_1|1\rangle$, and $U_1|0\rangle = W_1|0\rangle$.

Next, let $U_2 = W_1^{-1}U_1 = W_1^{-1}W_0^{-1}U$. Then U_2 is $(N-2)\times(N-2)$ unitary, etc.

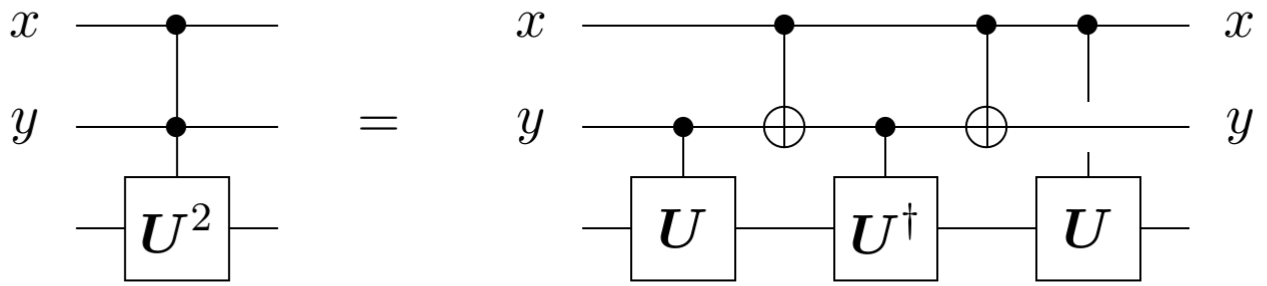
Eventually, find: $W_{N-2}^{-1}W_{N-3}^{-1}\ldots W_1^{-1}W_0^{-1}U = I$.

$U = W_0W_1\ldots W_{N-3}W_{N-2}$,
a product of
$(N\text{-}1)+(N\text{-}2)+\ldots 2+1$
$= \frac{1}{2}N(N-1)$ 2×2 unitaries.

Exact universality of two-qubit gates

Two steps: (1) Every unitary is a product of "2×2 unitaries". (2) Every 2×2 unitary can be constructed as a circuit of two-qubit unitaries.

To prove step (2), this circuit identity:



Number of times U applied to the 3rd qubit: $y-(x \oplus y)+x = y-(x+y-2xy)+x = 2xy$

Generalize: Construct $\Lambda^m(U^2)$ using $\Lambda^{m-1}(U)$, $\Lambda^{m-1}(X)$, $\Lambda(U)$, and $\Lambda(U^\dagger)$ gates.

Replace the $\Lambda(X)$ gates by $\Lambda^{m-1}(X)$ gates, replace the last $\Lambda(U)$ gate by $\Lambda^{m-1}(U)$:

$$x_m + x_1x_2x_3\ldots x_{m-1} - (x_m \oplus x_1x_2x_3\ldots x_{m-1}) = x_m + x_1x_2x_3\ldots x_{m-1} - (x_m + x_1x_2x_3\ldots x_{m-1} - 2x_1x_2x_3\ldots x_{m-1}x_m) = 2x_1x_2x_3\ldots x_{m-1}x_m.$$

Every unitary has a square root, so by a recursive construction we see that any $\Lambda^m(V)$ can be constructed as a circuit of two-qubit gates. In particular we can construct a Toffoli gate, and Toffoli gates, being universal for classical reversible computation, suffice for achieving any permutation of n-bit strings (computational basis states). See notes for details.

Exact universality of two-qubit gates

$\Lambda^{n-1}(V)$ acting on n qubits is a 2×2 unitary. It acts nontrivially only on the span of

$$\{|11111\ldots1110\rangle, \quad |11111\ldots1111\rangle\}$$

To construct a 2×2 unitary acting on the computational basis states $|x\rangle$, $|y\rangle$, use a permutation Σ.

$$\Sigma: \quad |x\rangle \mapsto |11111\ldots1110\rangle, \quad |y\rangle \mapsto |11111\ldots1111\rangle$$

Then: $\Sigma^{-1}\Lambda^{n-1}(V)\Sigma$ is the desired 2×2 unitary.

This completes the argument that two-qubit quantum gates are exactly universal.

Next time we'll discuss universality of finite, rather than uncountable, gate sets.