Quantum computation

Lecture 6

Universal quantum gates

<u>Universality</u> N qubits $D=2^N$ Establish universality in 3 steps.

① Any $D\times D$ unitary matrix $\mathcal{U}$ can be written as a product of at most $D(D-1)/2$ <u>two-level</u> (unitary) <u>transition</u> matrices.

relation to Lie group $U(D)$

not efficient

Brief discussion of making an arbitrary state using 2-level transitions (Law-Eberly protocol).

Let T^{JK} denote a transition matrix between levels $|J\rangle$ and $|K\rangle$.

$$T^{JK}=\begin{array}{c} \\ J \\ \\ K \\ \\ \end{array}\begin{array}{c}\begin{array}{cc} \quad\quad J & \quad K \end{array}\\ \begin{pmatrix} 1 & & & & & & & & & & \\ & 1 & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & \alpha & & & & \beta & & & \\ & & & & 1 & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & 1 & & & & \\ & & & \gamma & & & & \delta & & & \\ & & & & & & & & 1 & & \\ & & & & & & & & & 1 & \\ & & & & & & & & & & 1 \end{pmatrix}\end{array}$$

$\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}\equiv\tilde{T}$ is a 2×2 unitary.

$$T^{JK}_{jk}=\begin{cases}\delta_{jk}, & j\neq J,K \text{ and } k\neq J,K\\ \alpha, & j=J,\ k=J\\ \beta, & j=J,\ k=K\\ \gamma, & j=K,\ k=J\\ \delta, & j=K,\ k=K\end{cases}$$

Suppose $\mathcal{U}'=\mathcal{U}T^{JK}$. All matrix elements of $\mathcal{U}'$ are the same as those in $\mathcal{U}$, <u>except</u> those in columns J and K, for which we have

$$\mathcal{U}'_{jJ}=\mathcal{U}_{jk}T^{JK}_{kJ}=\alpha\,\mathcal{U}_{jJ}+\gamma\,\mathcal{U}_{jK},$$

$$\mathcal{U}'_{jK}=\mathcal{U}_{jk}T^{JK}_{kK}=\beta\,\mathcal{U}_{jJ}+\delta\,\mathcal{U}_{jK}.$$

In each row, T^{JK} mixes the elements in columns J and K to get new elements for columns J and K.

Now suppose U has the following structure of 1's and 0's:

$$U = \begin{array}{cc} & \begin{array}{cc} \quad & J \qquad K \end{array} \\ \begin{array}{c} \\ J \\ K \end{array} & \left(\begin{array}{c|c} I & 0 \\ \hline & x000xxx \\ 0 & X \end{array}\right) \end{array}$$

x, means an arbitrary entry

What we want to show is that there is a transition matrix T^{JK} such that $U' = UT^{JK}$ has the same structure as U, but with, in addition, $U'_{JK} = 0$ and U'_{JJ} real and nonnegative. It is clear from the way T^{JK} acts that it doesn't disturb the existing structure of 1's and 0's in U.

$$U'_{JK} = \beta U_{JJ} + \delta U_{JK}, \quad U'_{JJ} = \alpha U_{JJ} + \gamma U_{JK}$$

If $U_{JJ} = U_{JK} = 0$, any unitary choice for T will do, including the unit matrix. If not, then choose

$$\beta = \frac{U_{JK}}{\sqrt{|U_{JJ}|^2 + |U_{JK}|^2}} = \gamma^*, \quad , \quad \delta = -\frac{U_{JJ}}{\sqrt{|U_{JJ}|^2 + |U_{JK}|^2}} = -\alpha^*,$$

which makes T^{JK} unitary and makes $U'_{JK} = 0$ and $U'_{JJ} = \sqrt{|U_{JJ}|^2 + |U_{JK}|^2}$.

With this result, we see that we can start with a unitary matrix of the form

$$U^J = \begin{array}{cc} & \begin{array}{cc} \quad & J \end{array} \\ \begin{array}{c} \\ J \end{array} & \left(\begin{array}{c|c} I & 0 \\ \hline 0 & X \end{array}\right) \end{array}$$

and convert it, by application of transition matrices, to one where the Jth row has all zeroes except a real, nonnegative entry on the diagonal.

$$\begin{array}{c c} & \begin{array}{ccc} & J & \end{array} \\ J & \left(\begin{array}{c|c|c} I & 0 & O \\ \hline & A & 0 \\ \hline O & x & X \end{array}\right) \end{array}$$

$A \geq 0$
$A = 1$ by normalization of this row.

The x's in this column must be zero by normalization of this column.

So we end up with a matrix U_{J+1}:

$$U^{J+1} = U^{J} T^{J,J+1} T^{J,J+2} \ldots T^{JD}.$$

Overall, we have

$$I = U T^{12} \ldots T^{1D} T^{23} \ldots T^{2D} \ldots T^{D-2,D-1} T^{D-2,D} T^{D-1,D}$$

$$\Rightarrow \quad U = \underbrace{(T^{D-1,D})^{\dagger} (T^{D-2,D})^{\dagger} (T^{D-2,D-1})^{\dagger} \ldots (T^{2D})^{\dagger} \ldots (T^{23})^{\dagger} \times (T^{1D})^{\dagger} (T^{12})^{\dagger}}_{D(D-1)/2 \text{ transition matrices}}.$$

What we've established is that the two-level transitions are universal.

---

② Any two-level transition can be reduced to CNOTs and single-bit rotations.

<u>Strategy</u>: Show that any two-level transition T^{JK} on N qubits can be converted to a controlled unitary $C^{(N-1)}(\tilde{T})$, which can be reduced to CNOTs and single-bit rotations.

$$C^{(N-1)}(U) \longleftrightarrow \begin{pmatrix} 1 & & & & & & & \\ & 1 & & & & & 0 & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & 0 & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & \boxed{U} \end{pmatrix}$$

This <u>is</u> a 2-level transition; to convert an arbitrary two-level transition to this, we shuffle levels till the 2 important levels are $|1\rangle^{\otimes(N-1)}|0\rangle$ and $|1\rangle^{\otimes(N-1)}|1\rangle$, do a $C^{(N-1)}(\tilde{T})$, and then shuffle the levels back.

$$T^{JK}: \quad |J\rangle = |s\rangle = |s_1,\ldots,s_N\rangle \equiv |g_0\rangle$$
$$|K\rangle = |t\rangle = |t_1,\ldots,t_N\rangle \equiv |g_m\rangle$$

m: number of bits where s and t differ

$$\tilde{T} \longleftrightarrow \begin{pmatrix} \langle s|T|s\rangle & \langle s|T|t\rangle \\ \langle t|T|s\rangle & \langle t|T|t\rangle \end{pmatrix}$$

2x2 unitary

Convert s to t through a sequence of strings

$$s = g_0, g_1, \ldots, g_{m-1}, g_m;$$

at each step the last differing bit is switched.

Example: $N = 3$ $\quad |s\rangle = |000\rangle$ $\quad |t\rangle = |111\rangle$

$s = g_0 = 000$
$g_1 = 001$
$g_2 = 011$
$t = g_3 = 111$

Circuit:

(i)
① $|g_0\rangle \longleftrightarrow |g_1\rangle$
② $|g_1\rangle \longleftrightarrow |g_2\rangle$
⋮
(m-1) $|g_{m-2}\rangle \longleftrightarrow |g_{m-1}\rangle$

Each of these is a controlled operation with N-1 controls (the shared bits) and 1 target (the differing bit): bit flip on the target conditioned on the shared bits. Each is a 2-level transition that shuffles the levels

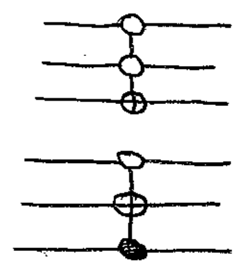
$\Longleftrightarrow$

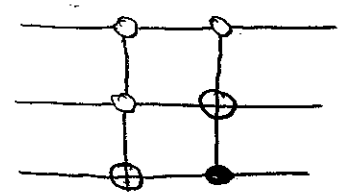
Overall transformation in ①

$$\boxed{\begin{aligned} |g_0\rangle &\rightarrow |g_{m-1}\rangle \\ |g_1\rangle &\rightarrow |g_0\rangle \\ |g_2\rangle &\rightarrow |g_1\rangle \\ &\vdots \\ |g_{m-1}\rangle &\rightarrow |g_{m-2}\rangle \end{aligned}}$$

$|000\rangle \longleftrightarrow |001\rangle$

$|001\rangle \longleftrightarrow |011\rangle$





(ii)

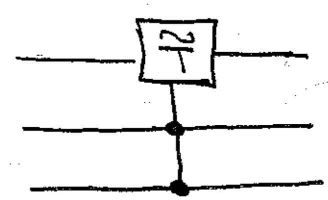
$|g_{m-1}\rangle \longrightarrow |g_{m-1}\rangle T_{ss} + |g_m\rangle T_{ts}$

$|g_m\rangle \longrightarrow |g_{m-1}\rangle T_{st} + |g_m\rangle T_{tt}$

Controlled-$\tilde{T}$ with N-1 controls (N-1 shared bits of g_{m-1} and g_m) and 1 target (bit that differs between g_{m-1} and g_m)

$|011\rangle \rightarrow |011\rangle T_{ss} + |111\rangle T_{ts}$

$|111\rangle \longrightarrow |011\rangle T_{st} + |111\rangle T_{tt}$



(iii) Reverse (i)

1. $|g_{m-1}\rangle \longleftrightarrow |g_{m-2}\rangle$
2. $|g_{m-2}\rangle \longleftrightarrow |g_{m-3}\rangle$

$\vdots$

$m-2$. $|g_2\rangle \longleftrightarrow |g_1\rangle$

$m-1$. $|g_1\rangle \longleftrightarrow |g_0\rangle$

$\Longleftrightarrow$

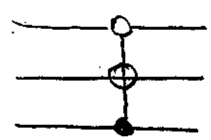
Overall transformation in (iii)

$$\boxed{\begin{array}{l} |g_0\rangle \longrightarrow |g_1\rangle \\ |g_1\rangle \longrightarrow |g_2\rangle \\ \\ |g_{m-2}\rangle \longrightarrow |g_{m-1}\rangle \\ |g_{m-1}\rangle \longrightarrow |g_0\rangle \end{array}}$$

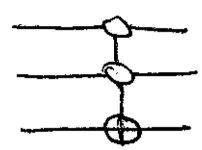
Any 2-level transition can be broken up into $\underbrace{2(m-1)+1}_{O(N)}$ $C^{(N-1)}$ gates, each of which can be reduced to $O(\log N)$ CNOTs and single-bit rotations.

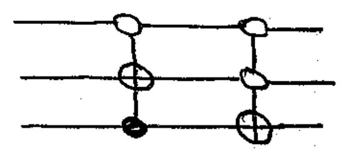
Resources: $O(N\log N)$

$|011\rangle \longleftrightarrow |001\rangle$



$|001\rangle \longleftrightarrow |000\rangle$



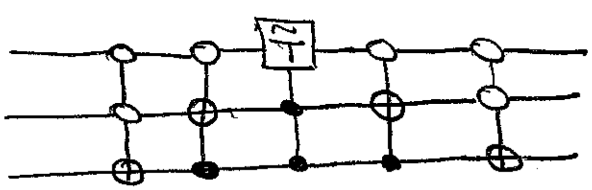


Put it all together:

$$|s\rangle = |g_0\rangle \longrightarrow |g_0\rangle T_{ss} + |g_m\rangle T_{ts} = |s\rangle T_{ss} + |t\rangle T_{ts} = T\,|s\rangle$$

$$|t\rangle = |g_m\rangle \longrightarrow |g_0\rangle T_{st} + |g_m\rangle T_{tt} = |s\rangle T_{st} + |t\rangle T_{tt} = T\,|t\rangle$$

Other levels unchanged.



Any unitary operator on N qubits can be decomposed into $O(D^2) = O(2^{2N})$ two-level transitions, each of which can be decomposed into $O(N \log N)$ CNOTs and single-bit rotations.

CNOT and single-bit rotations are a universal set for quantum computation. The resource requirement of $O(N 4^N \log N)$ gates turns out to be nearly optimal for a generic unitary.

---

③ Any single-qubit rotation can be approximated by a sequence of rotations drawn from a finite set, e.g., H and T. Moreover, the approximation can be efficient in the sense that in a circuit with M gates (CNOTs or single-bit rotations), the approximation can be performed with a number of gates $O(M \log(M/\epsilon))$, where ϵ is the desired overall accuracy of the approximation.

See textbook for details.

CNOT, H, and T are a universal gate set.

Generic unitaries:

Any two-level transition can be efficiently implemented using $O(N^2)$ CNOTs and single-bit rotations, but a a single-bit rotation U cannot be efficiently implemented using two-level transitions.

$$\begin{pmatrix} \boxed{U} & & & \\ & \boxed{U} & & \\ & & \boxed{U} & \\ & & & \boxed{U} \end{pmatrix}$$

3 qubits:
U on last

It takes 2^{N-1} two-level transitions to implement a single-bit rotation U, as compared to $O(2^{2N})$ for a generic unitary.

Although two-level transitions are universal, they are less powerful than CNOTs and single-bit rotations. Nonetheless, the $O(N 4^N \log N)$ gates we got by detouring through two-level unitaries is nearly optimal for a generic unitary.

N qubits

g gates to choose from, each acting on

$f \leq N/2$ qubits

$$\begin{pmatrix} \text{\# of different gates} \\ \text{available at each} \\ \text{step in circuit} \end{pmatrix} \leq g\binom{N}{f} \sim g\left(\frac{N}{f}\right)^f \sim g N^f$$

$$\begin{pmatrix}\text{\# of different} \\ \text{unitaries after} \\ M \text{ steps}\end{pmatrix} \lesssim \left(g \left(\frac{N}{f}\right)^{f} \right)^{M} = g^{M} \left(\frac{N}{f}\right)^{Mf}$$

$$\begin{pmatrix}\text{\# of real parameters} \\ \text{to specify } N\text{-qubit unitary}\end{pmatrix} = 2D^2 - \overbrace{D}^{\text{\# of real normalization conditions}} - 2\underbrace{\tfrac{1}{2}D(D-1)}_{\text{\# of orthogonality relations}}$$

complex numbers

\# of matrix element

Complex numbers

$$= D^2$$

$$\begin{pmatrix}\text{\# of bits to specify} \\ N\text{-qubit unitary}\end{pmatrix} \sim D^2 \overbrace{\log(1/\epsilon)}^{(\text{\# of bits})/\text{parameter}}$$

resolution

$$\begin{pmatrix}\text{\# of unitaries} \\ \text{at resolution } \epsilon\end{pmatrix} \sim \left(\frac{1}{\epsilon}\right)^{D^2} = \left(\frac{1}{\epsilon}\right)^{4^N}$$

$\boxed{\text{\# of unitaries to simulate is doubly exponentially large.}}$

$$M\left(\log g + f \log N\right) \sim 4^N \log(1/\epsilon)$$

\# of gates to implement a generic unitary at resolution ϵ

$$\boxed{M \sim \frac{4^N \log(1/\epsilon)}{f \log N}}$$

A generic unitary is exponentially hard.

What if we allowed all two-level transitions at resolution ϵ at each step?

$$\begin{pmatrix}\text{\# of different}\\ \text{gates at each step}\end{pmatrix} \sim \frac{1}{2}D(D-1)\left(\frac{1}{\epsilon}\right)^4 \sim 4^N\left(\frac{1}{\epsilon}\right)^4$$

$$\begin{pmatrix}\text{\# of different}\\ \text{unitaries after}\\ M \text{ steps}\end{pmatrix} \lesssim \left(4^N\left(\frac{1}{\epsilon}\right)^4\right)^M$$

$$M\left(2N + 4\log\left(\frac{1}{\epsilon}\right)\right) \sim 4^N \log\left(\frac{1}{\epsilon}\right)$$

$$M \sim \frac{4^N \log(1/\epsilon)}{2N + 4\log(1/\epsilon)}$$