Quantum computation

Lecture 6.1

Universal quantum gates
Universal.

\[ D = 2^N \]

Any \( D \times D \) unitary matrix \( U \) can be written as a product of at most \( D(D-1)/2 \) two-level (unitary) transition matrices.

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

Let \( T_{JK} \) denote a transition matrix between levels \( 1J \) and \( 1K \).

\[
T_{JK} = \begin{pmatrix}
1 & 1 \\
1 & 1 \\
1 & 1 \\
1 & 1
\end{pmatrix}
\]

\[
(\begin{pmatrix}
\alpha \\
\beta
\end{pmatrix}) \rightarrow T_{JK} \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix} = \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix}
\]

is a \( 2 \times 2 \) unitary.

Suppose \( U' = U T_{JK} \). All matrix elements of \( U' \) are the same as those in \( U \), except those in columns \( J \) and \( K \), for which we have

\[
U'_{jJ} = U_{jJ} T_{JK} - \alpha U_{jJ} + \beta U_{jK},
\]

\[
U'_{jK} = U_{jK} T_{JK} - \beta U_{jJ} + \gamma U_{jK}.
\]

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:

$$U = \begin{pmatrix} I & 0 \\ x & 0 \end{pmatrix}$$

$x_i$ 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 $U$.

$$U'_{JK} = 
\begin{cases} \beta U_{JJ} + \delta U_{JK}, & \quad U_{JJ} = \alpha U_{JJ} + \delta U_{JK} \\
\end{cases}$$

If $U_{JJ} = U_{JK} = 0$, any unitary choice for $T$ will do.

If not, then choose

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

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

$$U = \begin{pmatrix} I & 0 \\ x & 0 \end{pmatrix}$$
and convert it, by application of transition matrices, to one where the $J$th row has all zeroes except a real, nonnegative entry on the diagonal.

$$
\begin{pmatrix}
I & 0 & 0 \\
\hline
A & 0 \\
0 & X & \end{pmatrix}
$$

Azo $Ae_1$ 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 $U_{J+1}$:

$$
U_{J+1} = U_{J+1}^T J_{J+1}^T J_{J+2}^T \ldots J_{J+1}^T
$$

Overall, we have

$$
I = U_{J+1}^T 12 \ldots J^T 12 \ldots J^T 2D \ldots J^T D-1 J^T D J^T D-2 J^T D-1 \ldots J^T 2D
\Rightarrow U = (T_{D-1,D})^T (T_{D-2,D})^T (T_{D-3,D})^T \ldots (T_{2D})^T (T_{2D+1})^T
\times (T_{I1})^T (T_{I2})^T$

$$
\underbrace{D(D-1)/2 \text{ transition matrices}}$

What we've established is that the two-level transitions are universal.
Any two-level transition can be reduced to CNOTs and single-bit rotations.

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

This is 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 $\sim C^{N-1}(U)$, and then shuffle the levels back.

\[ T^{JK} : |1\rangle = |s\rangle = |s_1, ..., s_N\rangle \equiv |g_s\rangle \]
\[ |1\rangle = |t\rangle = |t_1, ..., t_N\rangle \equiv |g_t\rangle \]

Convert $s$ to $t$ through a sequence of strings $s = g_0, g_1, ..., g_{n-1}, g_n$; at each step the last differing bit is switched.
Circuit:

\[ 1 \rightarrow 1 \]
\[ 1 \rightarrow 0 \]
\[ 0 \rightarrow 1 \]
\[ 0 \rightarrow 0 \]

Example: \( N = 2 \)

\[ 1 \rightarrow 11 \]
\[ 1 \rightarrow 10 \]
\[ 0 \rightarrow 10 \]
\[ 0 \rightarrow 11 \]

\[ 1 \rightarrow 1 \]
\[ 0 \rightarrow 0 \]
Result: $O(n \log n)$

and single-bit rotations (see 7.4.2). 

The key observation is that each of which can be broken up into \text{CNOT}s, $2^{(m-1)} \text{(CN-1) gates}$.

Any 2-level transition can be broken down into $2^{(m-1)} \text{(CN-1) gates}$.

Overall transformation in 7.4.2.
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 $O(N^2 N/\log N)$ 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 $O(M \log(M/e))$, where E 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 single-bit rotation $U$ cannot be efficiently implemented using two-level transitions.

\[
\begin{pmatrix}
U & U \\
U & U \\
U & U
\end{pmatrix}
\]

3 qubits: $U$ on last

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

Although two-level transitions are universal, they are less powerful than CNOTs and single-bit rotations. Nonetheless, the $o(N^4 \log N)$ gates we get 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

\[
\left( \text{\# of different gates available at each step in circuit} \right) \leq g\left( \frac{N}{f} \right) \sim g\left( \frac{N^2}{f^2} \right)^f \sim gN^f
\]
\[(\text{\# of different unitaries after M steps}) \sim (g(N/f))^M = g^M(N/f)^M\]

\[\text{\# of real normalization conditions}\]

\[\text{\# of real parameters to specify N-qubit unitary} = eD^2 - D = 2\frac{1}{2}D(D-1)\]

\[\text{\# of matrix elements}\]

\[\text{Complex numbers}\]

\[\text{\# of orthogonality relations}\]

\[= D^2\]

\[\text{\# of bits to specify N-qubit unitary} \sim \frac{D^2}{\log(1/e)}\]

\[\text{\# of basis parameters}\]

\[\text{Resolution}\]

\[\text{\# of unitaries at resolution \(\varepsilon\)} \sim \left(\frac{1}{\varepsilon}\right)^D = \left(\frac{1}{\varepsilon}\right)^{4^N}\]

\[\text{\# of unitaries to simulate is doubly exponentially large}\]

\[M \left(\log g + \frac{1}{f} \log N\right) \sim 4^N \log(1/e)\]

\[\text{\# of gates to implement a generic unitary at resolution \(\varepsilon\)}\]

\[M \sim \frac{4^N \log(1/e)}{f + \frac{1}{f} \log N} \approx \frac{4^N \log(1/e)}{f} \approx 1\]

\[\text{A generic unitary is exponentially hard.}\]
What if we allowed all two-level transitions at resolution $\varepsilon$ at each step?

\[
\left( \text{\# of different gates at each step} \right) \sim \frac{1}{\varepsilon} D(D - 1) \left( \frac{1}{\varepsilon} \right)^4 \sim 4^N \left( \frac{1}{\varepsilon} \right)^4
\]

\[
\left( \text{\# of different unitaries after } M \text{ steps} \right) \leq \left( 4^N \left( \frac{1}{\varepsilon} \right)^4 \right)^M
\]

\[
M \left( 2N + 4 \log \left( \frac{1}{\varepsilon} \right) \right) \sim 4^N \log \left( \frac{1}{\varepsilon} \right)
\]

\[
M \sim \frac{4^N \log \left( \frac{1}{\varepsilon} \right)}{2N + 4 \log \left( \frac{1}{\varepsilon} \right)}
\]