Quantum Computation- Quantum Circuits- Universal quantum gates

- A small set of gates (e.g. AND , OR , NOT) can be used to compute an arbitrary classical function. We say that such a set of gates is *universal* for classical computation.
- Any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase,CNOT , and $\pi/8$ gates. You may wonder why the phase gate appears in this list, since it can be constructed from two $\pi/8$ gates; it is included because of its natural role in the fault-tolerant constructions

Quantum Computation- Quantum Circuits- Universal quantum gates

- The first construction shows that an arbitrary unitary operator may be expressed exactly as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states.
- The second construction combines the first construction with the results of the previous section to show that an arbitrary unitary operator may be expressed exactly using single qubit and CNOT gates.
- The third construction combines the second construction with a proof that single qubit operation may be approximated to arbitrary accuracy using the Hadamard, phase, and $\pi/8$ gates. This in turn implies that any unitary operation can be approximated to arbitrary accuracy using Hadamard, phase, CNOT, and $\pi/8$ gates.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Two-level unitary gates are universal.
- Consider a unitary matrix U which acts on a d-dimensional Hilbert space.
- We explain how U may be decomposed into a product of two-level unitary matrices.
- That is, unitary matrices which act non-trivially only on two-or-fewer vector components.
- The essential idea behind this decomposition may be understood by considering the case when U is 3×3, so suppose that U has the form.

Quantum Computation- Quantum Circuits- Universal quantum gates

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}$$

- We will find two-level unitary matrices $U_1, \ldots, U_3$ such that

$$U_3 U_2 U_1 U = I \, .$$

- It follows that

$$U = U_1^\dagger U_2^\dagger U_3^\dagger \, .$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- U1, U2 and U3 are all two-level unitary matrices, and it is easy to see that their inverses, $U^{\dagger}_1$, $U^{\dagger}_2$ and $U^{\dagger}_3$ are also two-level unitary matrices.
- Use the following procedure to construct U_1: if b = 0 then set

$$U_1 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- If b ≠ 0 then set

$$U_1 \equiv \begin{bmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

- Note that in either case U_1 *is a two-level unitary matrix, and when we multiply the* matrices out we get

$$U_1U = \begin{bmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & j' \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- The key point to note is that the middle entry in the left hand column is zero. We denote the other entries in the matrix with a generic prime ‘ ; their actual values do not matter. Now apply a similar procedure to find a two-level matrix U_2 such that U_2U_1U has no entry in the bottom left corner. That is, if c’ = 0 we set

$$U_2 \equiv \begin{bmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- while if $c' \neq 0$ then we set

$$U_2 \equiv \begin{bmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- In either case, when we carry out the matrix multiplication we find that

$$U_2U_1U = \begin{bmatrix} 1 & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{bmatrix}$$

- Since *U, U_1 and U_2 are unitary, it follows that U_2U_1U is unitary, and thus $d'' = g'' = 0$,* since the first row of *U_2U_1U must have norm 1.*

Quantum Computation- Quantum Circuits- Universal quantum gates

- Finally, set

$$U_3 \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & e^{''*} & f^{''*} \\ 0 & h^{''*} & j^{''*} \end{bmatrix}$$

- It is now easy to verify that $U_3U_2U_1U = I$, *and thus* $U = U^\dagger_1\, U^\dagger_2\, U^\dagger_3$, which is a decomposition of *U into two-level unitaries.*

Quantum Computation- Quantum Circuits- Universal quantum gates

- More generally, suppose U acts on a d-dimensional space. Then, in a similar fashion to the 3×3 case, we can find two-level unitary matrices $U_1, \ldots, U_{d-1}$ such that the matrix $U_{d-1}U_{d-2} \ldots U_1 U$ has a one in the top left hand corner, and all zeroes elsewhere in the first row and column. We then repeat this procedure for the $d - 1$ by $d - 1$ unitary submatrix in the lower right hand corner of $U_{d-1}U_{d-2} \ldots U_1 U$, and so on, with the end result that an arbitrary $d\times d$ unitary matrix may be written

Quantum Computation- Quantum Circuits- Universal quantum gates

$$U = V_1 \dots V_k,$$

- where the matrices V_i are two-level unitary matrices, and $k \leq (d-1)+(d-2)+\cdot\cdot\cdot+1 = d(d-1)/2$.
- Exercise: Provide a decomposition of the transform

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

- into a product of two-level unitaries. This is a special case of the quantum Fourier transform, which we study in more detail later.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Single qubit and CNOT gates are universal
- We show that single qubit and CNOT gates together can be used to implement an arbitrary two-level unitary operation on the state space of *n qubits.*
- Combining these results we see that single qubit and CNOT gates can be used to implement an arbitrary unitary operation on *n qubits,* and therefore are universal for quantum computation.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Suppose U is a two-level unitary matrix on an n qubit quantum computer. Suppose in particular that U acts non-trivially on the space spanned by the computational basis states |s> and |t>, where $s = s_1 \ldots s_n$ and $t = t_1 \ldots t_n$ are the binary expansions for s and t.
- Let *U˜ be the non-trivial 2×2 unitary submatrix of U; U˜ can be thought of as a* unitary operator on a single qubit.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Our immediate goal is to construct a circuit implementing U, built from single qubit and CNOT gates.
- To do this, we need to make use of Gray codes. Suppose we have distinct binary numbers, s and t.
- A Gray code connecting s and t is a sequence of binary numbers, starting with s and concluding with t, such that adjacent members of the list differ in exactly one bit.

Quantum Computation- Quantum Circuits- Universal quantum gates

- For instance, with s = 101001 and t = 110011 we have the Gray code

$$\begin{matrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{matrix}$$

- Let g_1 through g_m be the elements of a Gray code connecting s and t, with $g_1 = s$ and $g_m = t$.
- Note that we can always find a Gray code such that $m \leq n+1$ since s and t can differ in at most n locations.

Quantum Computation- Quantum Circuits- Universal quantum gates

- The basic idea of the quantum circuit implementing U is to perform a sequence of gates effecting the state changes $|g_1\rangle \rightarrow |g_2\rangle \rightarrow \ldots \rightarrow |g_{m-1}\rangle$, then to perform a controlled-$\tilde{U}$ operation, with the target qubit located at the single bit where g_{m-1} and g_m differ, and then to undo the first stage, transforming $|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \rightarrow \ldots \rightarrow |g_1\rangle$.
- Each of these steps can be easily implemented using operations developed earlier in this chapter, and the final result is an implementation of *U.*

Quantum Computation- Quantum Circuits- Universal quantum gates

- A more precise description of the implementation is as follows.
- The first step is to swap the states $|g_1>$ and $|g_2>$. Suppose g_1 and g_2 differ at the i^{th} digit.
- Then we accomplish the swap by performing a controlled bit flip on the i^{th} qubit, conditional on the values of the other qubits being identical to those in both g_1 and g_2.
- Next we use a controlled operation to swap $|g_2>$ and $|g_3>$.
- We continue in this fashion until we swap $|g_{m-2}>$ with $|g_{m-1}>$

Quantum Computation- Quantum Circuits- Universal quantum gates

- The effect of this sequence of *m – 2 operations is to achieve the operation*

$$
\begin{aligned}
|g_1\rangle &\rightarrow |g_{m-1}\rangle \\
|g_2\rangle &\rightarrow |g_1\rangle \\
|g_3\rangle &\rightarrow |g_2\rangle \\
&\cdots\cdots\cdots \\
|g_{m-1}\rangle &\rightarrow |g_{m-2}\rangle
\end{aligned}
$$

- All other computational basis states are left unchanged by this sequence of operations.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Next, suppose g_{m-1} and g_m differ in the j^{th} bit. We apply a controlled-$\tilde{U}$ operation with the j^{th} qubit as target, conditional on the other qubits having the same values as appear in both g_m and g_{m-1}.
- Finally, we complete the U operation by undoing the swap operations: we swap $|g_{m-1}>$ with $|g_{m-2}>$, then $|g_{m-2}>$ with $|g_{m-3}>$ and so on, until we swap $|g_2>$ with $|g_1>$.

Quantum Computation- Quantum Circuits- Universal quantum gates

- A simple example illuminates the procedure further. Suppose we wish to implement the two-level unitary transformation

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

Quantum Computation- Quantum Circuits- Universal quantum gates

- Here, *a, b, c and d are any complex numbers such that*

$$\tilde{U} \equiv \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

- is a unitary matrix.
- Notice that U acts non-trivially only on the states |000> and |111>. We write a Gray code connecting 000 and 111:

A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

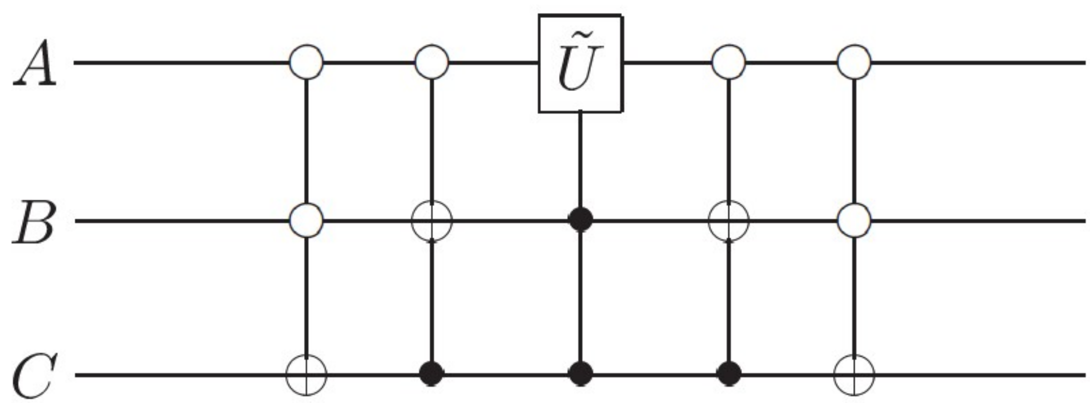
Quantum Computation- Quantum Circuits- Universal quantum gates

- From this we read off the required circuit
- The first two gates shuffle the states so that |000> gets swapped with |011>.
- Next, the operation U˜ is applied to the first qubit of the states |011> and |111>, conditional on the second and third qubits being in the state |11>.
- Finally, we unshuffle the states, ensuring that |011> gets swapped back with the state |000>.

Quantum Computation- Quantum Circuits- Universal quantum gates

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

A	B	C
0	0	0
0	0	1
0	1	1
1	1	1



Quantum Computation- Quantum Circuits- Universal quantum gates

- Returning to the general case, we see that implementing the two-level unitary operation U requires at most $2(n-1)$ controlled operations to swap $|g_1>$ with $|g_{m-1}>$ and then back again.
- Each of these controlled operations can be realized using O(n) single qubit and CNOT gates; the controlled-$\tilde{U}$ operation also requires O(n) gates. Thus, implementing U requires $O(n^2)$ single qubit and CNOT gates.

Quantum Computation- Quantum Circuits- Universal quantum gates

- We saw in the previous section that an arbitrary unitary matrix on the 2^n-dimensional state space of n qubits may be written as a product of $O(2^{2n}) = O(4^n)$ two-level unitary operations.
- Combining these results, we see that an arbitrary unitary operation on n qubits can be implemented using a circuit containing $O(n^2 4^n)$ single qubit and gates.

Quantum Computation- Quantum Circuits- Universal quantum gates

- Exercise: Find a quantum circuit using single qubit operations and CNOTs to implement the transformation

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

- Where $\tilde{U} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$

Quantum Computation- Quantum Circuits- Universal quantum gates

- Please read the following sections from the book:
  - A discrete set of universal operations
  - Approximating arbitrary unitary gates is generically hard
  - Quantum computational complexity
  - Summary of the quantum circuit model of computation
  - Simulation of quantum systems
  - History and further reading