Lecture 12

Universal quantum gates

Single qubit + CNOT gates

Single qubit and CNOT gates together can be used to implement an arbitrary two-level unitary operation on the state space of n qubits.

Suppose U is a two-level unitary matrix which acts non-trivially on the space spanned by the computational basis states |s> and |t>, where $s = s_1 \ldots s_n$ and $t = t_1 \ldots t_n$. Let $\widetilde{U}$ be non-trivial 2 x 2 unitary submatrix of U.

$$U = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & b \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ c & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix} \qquad \widetilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Goal: to construct a circuit implementing U from single qubit and CNOT gates.

Use Gray codes: A Gray code connecting binary numbers 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 one bit.

Example: s=101001, t=110011.

Gray code $g_1 \ldots g_m$, $g_1 = s$, $g_m = t$:

g_1	1	0	1	0	0	1
g_2	1	0	1	0	1	1
g_3	1	0	0	0	1	1
g_4	1	1	0	0	1	1

<u>Basic idea of the quantum circuit implementing U</u>

- Swap the states $|g_1\rangle$ and $|g_2\rangle$.
- Swap the states $|g_2\rangle$ and $|g_3\rangle$ and continue until we swap $|g_{m-2}\rangle$ and $|g_{m-1}\rangle$.
- Apply a controlled-$\widetilde{U}$ operation, with the target qubit located at the single bit where g_{m-1} and g_m differ.
- Undo the swap operations: swap $|g_{m-2}\rangle$ and $|g_{m-1}\rangle$, and so on until $|g_2\rangle$ and $|g_1\rangle$ are swapped.

Example: consider the U gate on the previous page.

Question for the class: what logical operation does gate U perform?

U
|000> $\rightarrow$
|001> $\rightarrow$
|010> $\rightarrow$
|011> $\rightarrow$
|100> $\rightarrow$
|101> $\rightarrow$
|110> $\rightarrow$
|111> $\rightarrow$

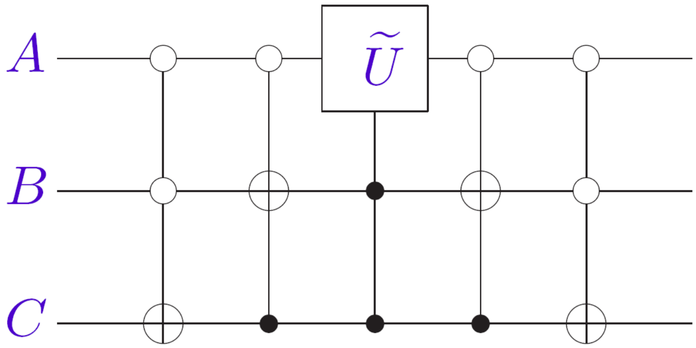
?

U
|000> $\rightarrow$ a|000>+c|111>
|001> $\rightarrow$ |001>
|010> $\rightarrow$ |010>
|011> $\rightarrow$ |011>
|100> $\rightarrow$ |100>
|101> $\rightarrow$ |101>
|110> $\rightarrow$ |110>
|111> $\rightarrow$ b|000>+d|111>

Since the U acts non-trivially only on states |000> and |111>, the Gray codes is

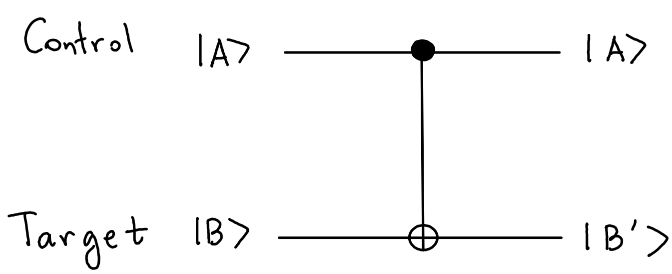
A	B	C
0	0	0
0	0	1
0	1	1
1	1	1

The circuit to implement the gate U is:



REVIEW: Controlled operations: "If A is true, then do B"

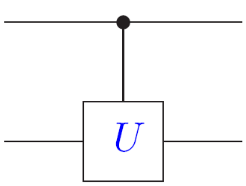
Controlled-NOT (CNOT) gate



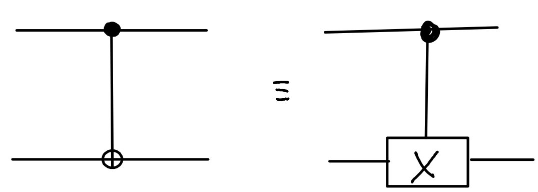
$\|AB\rangle$	$\|AB'\rangle$
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

More on controlled operations

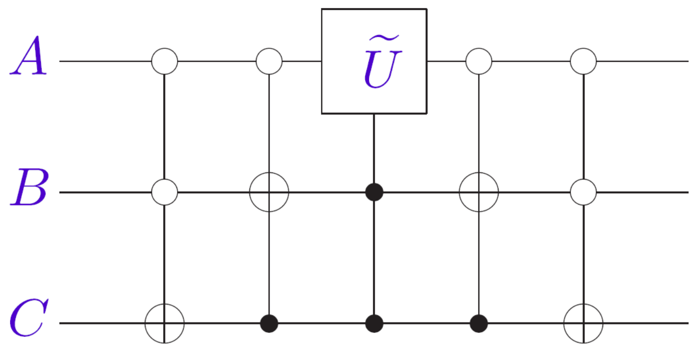
Suppose U is an arbitrary single qubit unitary operation. A controlled-U operation is a two-qubit operation with a control qubit and a target qubit. If control qubit is set, then U is applied to the target qubit.



Example: controlled-NOT gate is controlled-X gate.



The circuit to implement the gate U is:



Class exercise: work out what this circuit does gate by gate.

Hint: you only need to keep track on four states listed in the Gray code as the remaining four states are not affected at all.

ABC	1	2	3
$\vert 000\rangle$	$\vert 001\rangle$	$\vert 011\rangle$	$a\vert 011\rangle + c\vert 111\rangle$
$\vert 001\rangle$	$\vert 000\rangle$	$\vert 000\rangle$	$\vert 000\rangle$
$\vert 011\rangle$	$\vert 011\rangle$	$\vert 001\rangle$	$\vert 001\rangle$
$\vert 111\rangle$	$\vert 111\rangle$	$\vert 111\rangle$	$b\vert 011\rangle + d\vert 111\rangle$

↑ swap $|000\rangle$ and $|001\rangle$ (column 1)

↑ swap $|001\rangle$ and $|011\rangle$ (column 2)

↑ apply $\tilde{U}$ if both B & A are $|1\rangle$ (column 3)

4	5
$a\vert 001\rangle + c\vert 111\rangle$	$a\vert 000\rangle + c\vert 111\rangle$
$\vert 000\rangle$	$\vert 001\rangle$
$\vert 011\rangle$	$\vert 011\rangle$
$b\vert 001\rangle + d\vert 111\rangle$	$b\vert 000\rangle + d\vert 111\rangle$

unswap the states back

Measurement

Principle of deferred measurement: Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit.

Principle of implicit measurement: Without loss of generality, any unterminated quantum wires (qubits which are not yet measured) at the end of the quantum circuit may be assumed to be measured.

In order for a measurement to be reversible, it must reveal no information about the quantum system being measured!

Summary of the quantum circuit model of computation

- **Classical resources.** For example, many schemes for quantum error-correction involve classical computations to maximize efficiency.

- **A suitable state space.** For a quantum circuit operating on n qubits the state space is 2^n dimensional Hilbert space. Computational basis: $|x_1 \ldots x_n>$, where $x_i = 0, 1$.

- **Ability to prepare states in the computational basis.** (Any computational basis state can be prepared in at most n steps.)

- **Ability to perform quantum gates.** The set of Hadamard + phase + CNOT $+\pi/8$ gates is universal.

- **Ability to perform measurements in the computational basis.**