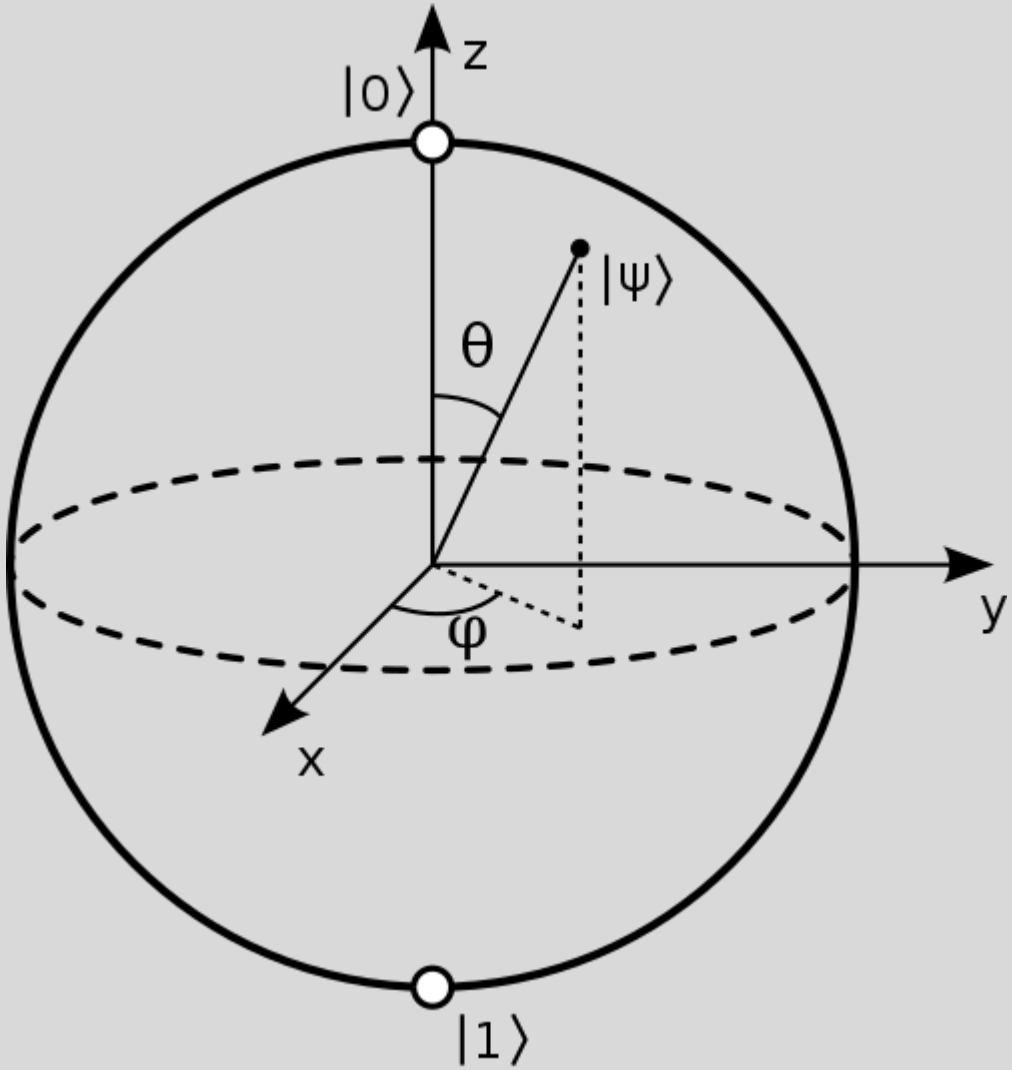
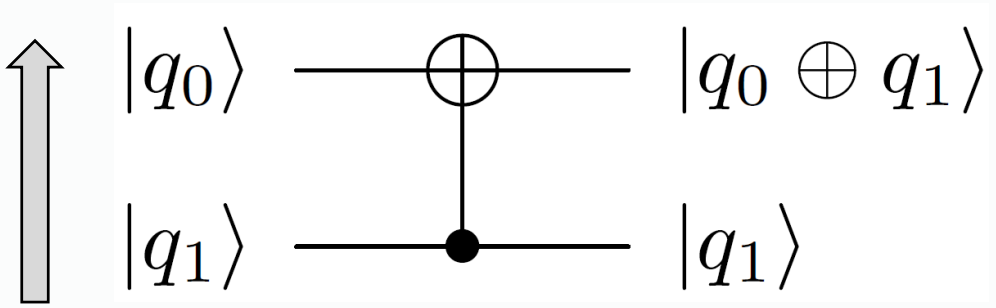


Quantum Gates, Circuits, and Algorithms

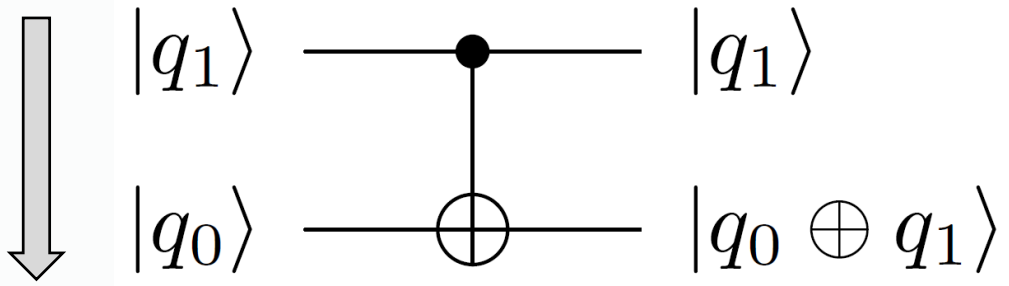
(Part 2)

ECE 592/CSC 591 – Fall 2019



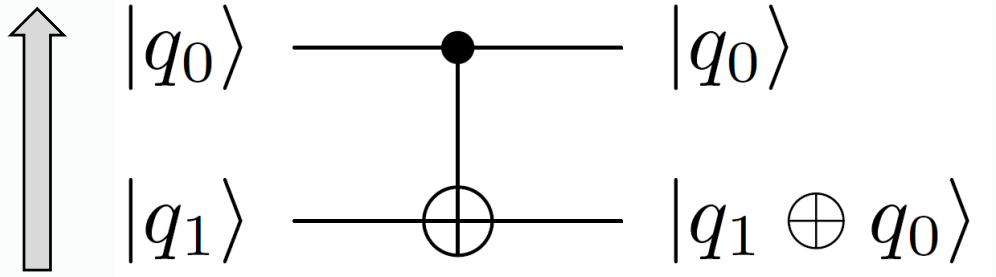
Start	End
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

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



Start	End
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

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



Start	End
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|11\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$\|01\rangle$

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

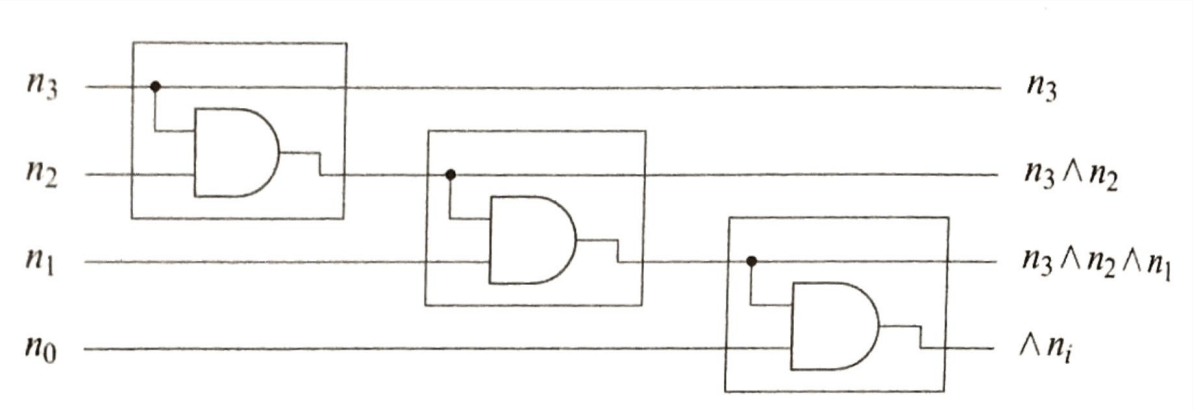
Next Steps

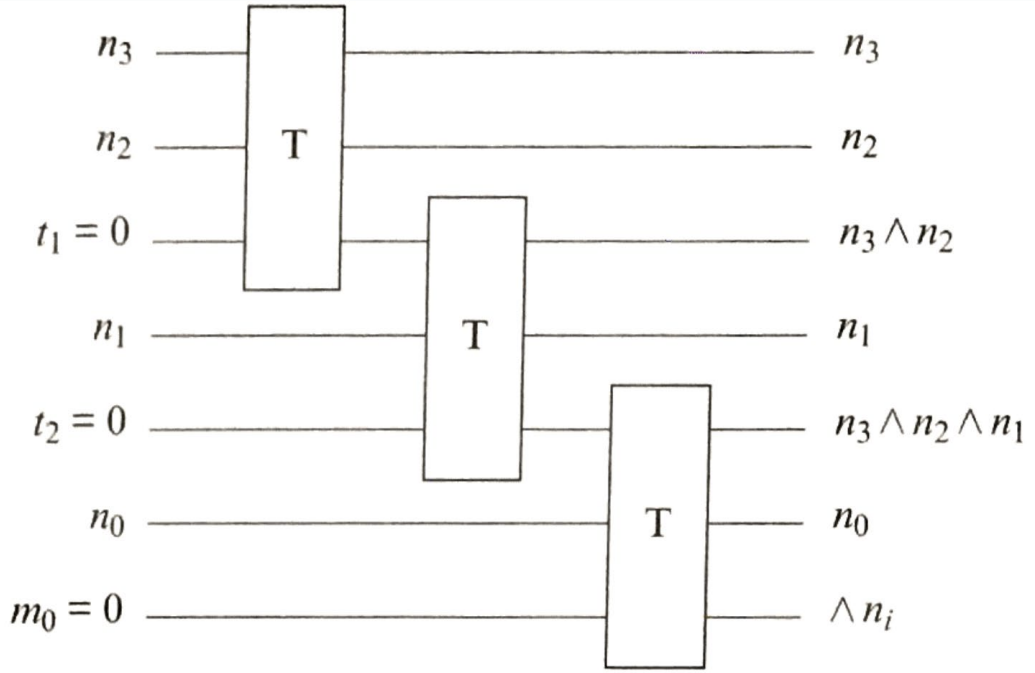
- Efficient quantum implementations of classical functions
  - Create reversible classical circuits
  - Convert to quantum
  - Undo entanglement

- Quantum algorithms

Classical (Boolean) Circuits

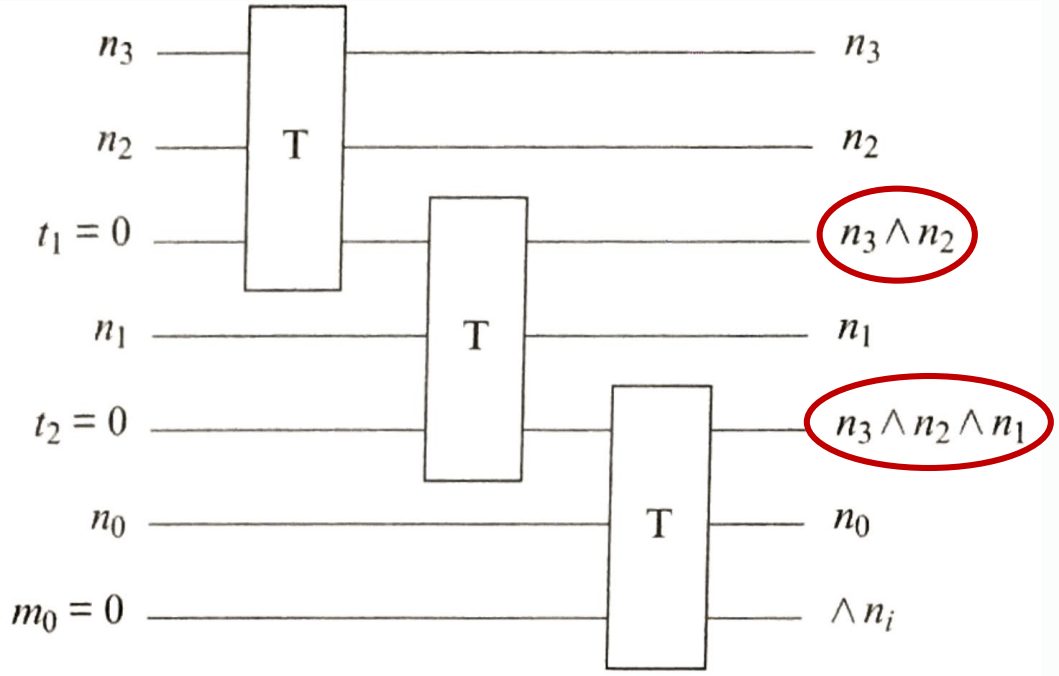
In general, classical circuits are not reversible. Consider this circuit for a 4-way AND.



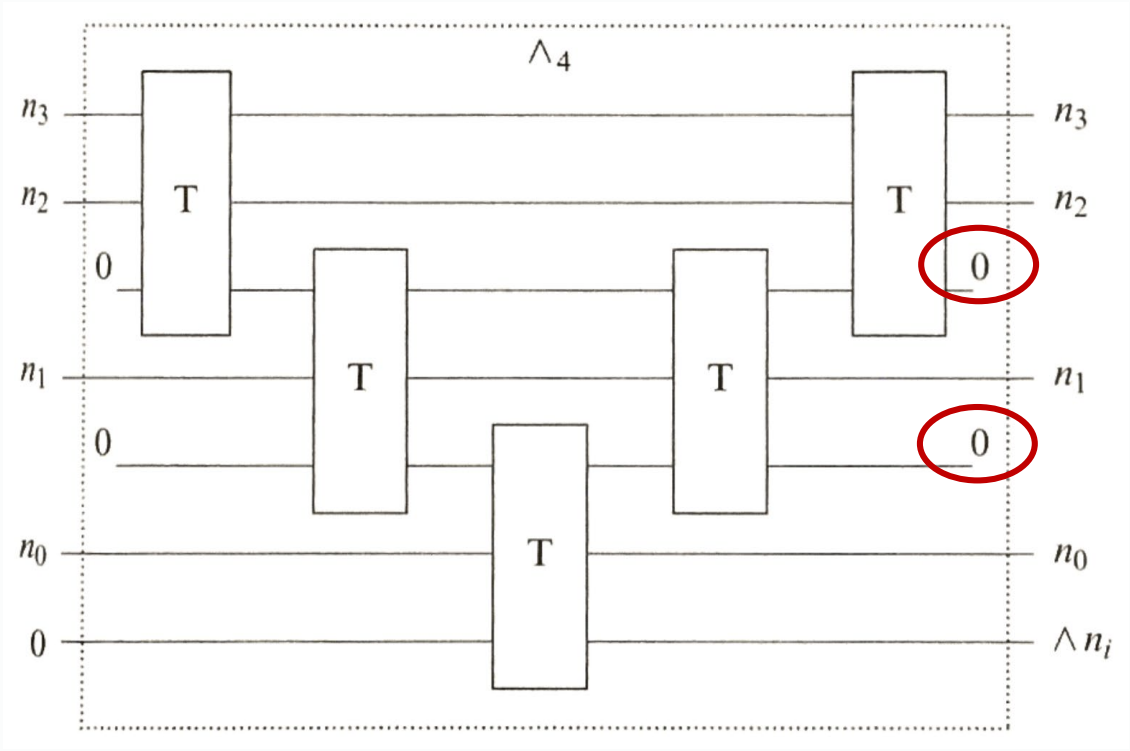


By using (classical) Toffoli gate, we can construct a reversible circuit. Requires one additional bit per AND gate, and of course a Toffoli gate is more complex than an AND gate.

Reusing Temporary Bits



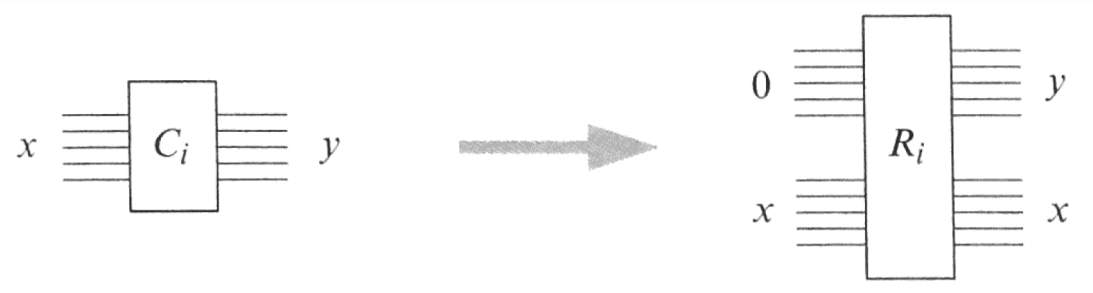
These bits are no longer zero, and can't be reused if this feeds into additional computation. Can't just "reset" them, because that's not reversible. Need to uncompute to reclaim them.

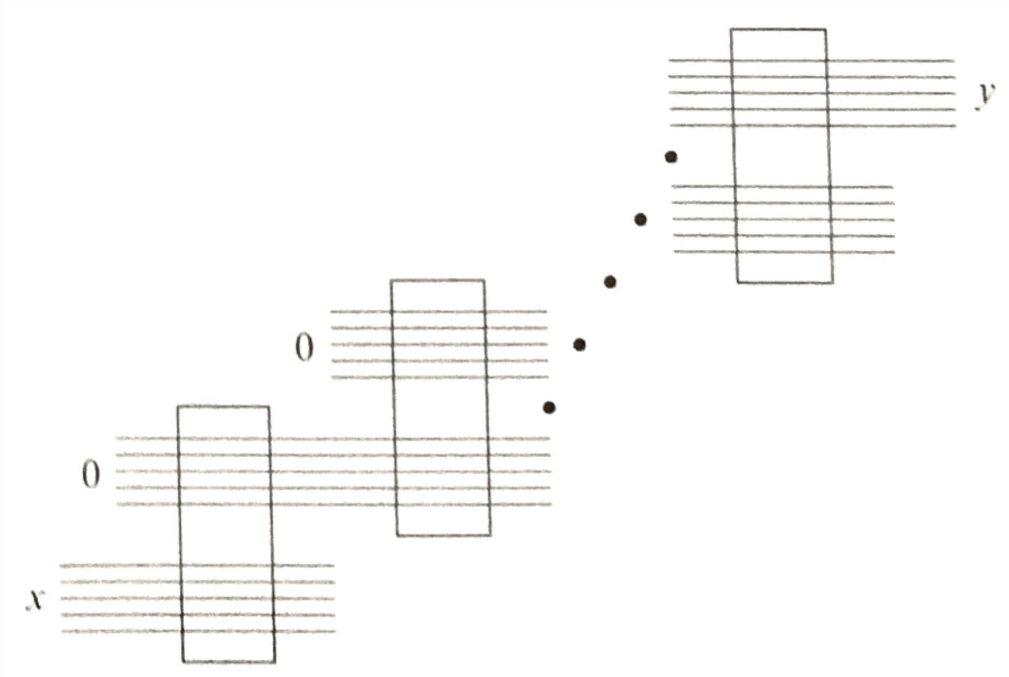


Tradeoff: Uncomputing requires extra gates, so when is it better to reclaim vs. retain for potential later use?

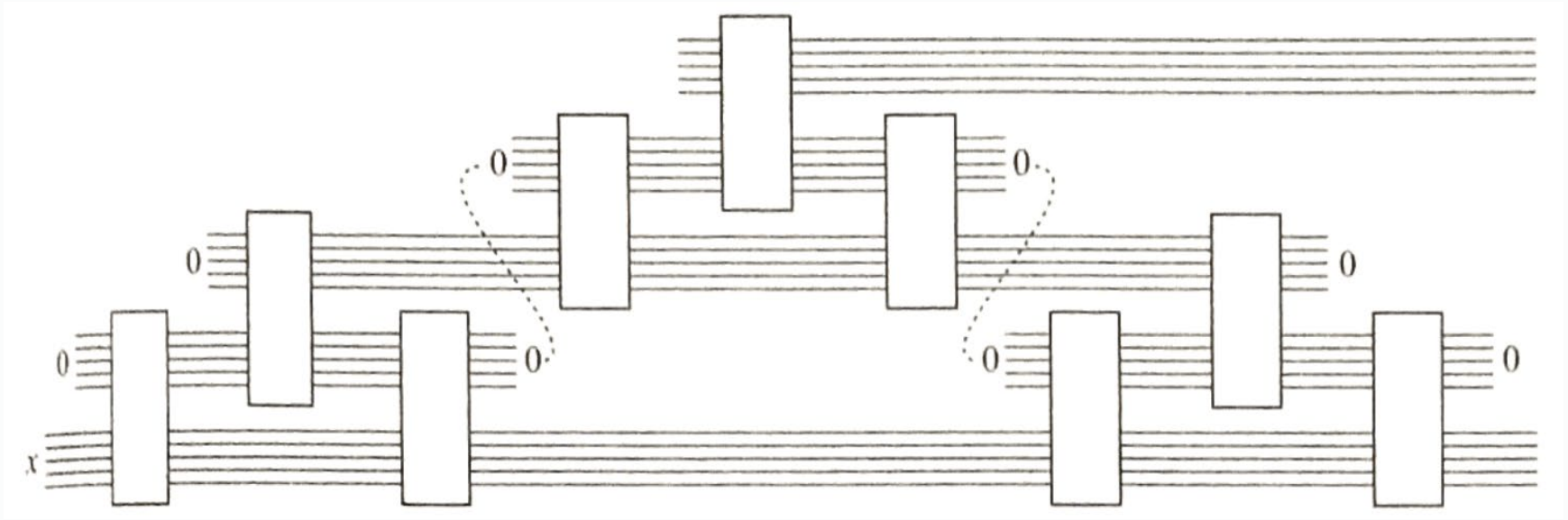
General Scheme

Assume a classical circuit C can be decomposed into subcircuits C_i, convert each to reversible R_i.





General Scheme



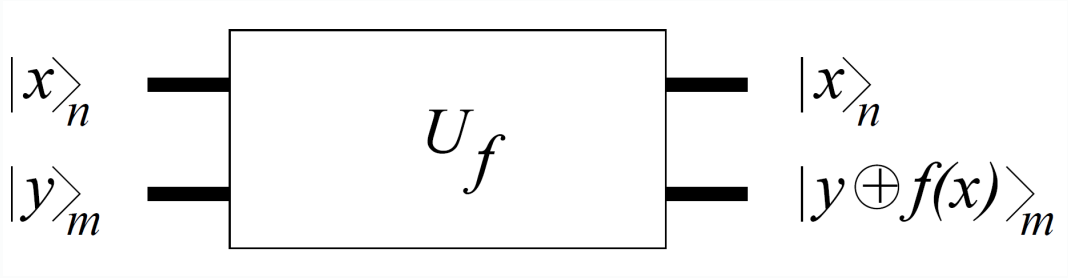
Using this general scheme, any classical circuit with t steps and s bits can be done reversibly in $O(t^{1+\varepsilon})$ steps and $O(s \log t)$ bits. There may be more efficient implementations for a specific circuit.

Uncomputing temporary qubits is more important in the quantum realm, because:

- Qubits are more precious than bits. Reducing storage is more important (for now) than reducing gates.
- Temporary bits may be **entangled** with output bits.
  Measuring them to reset, for use in later computation, can disturb the output bits.

Summary

- Any computation with an efficient classical circuit has an equivalent efficient quantum circuit.



- Use reverse computation to unentangle and reuse tmp qubits.

Further reading:

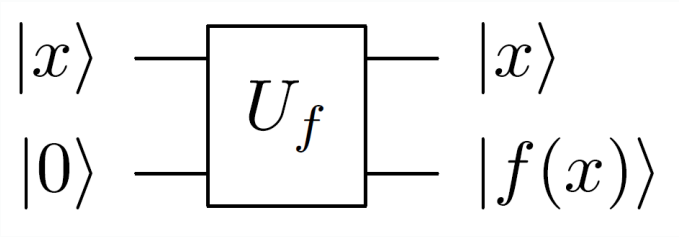
- John Preskill notes, Chapter 6
- Vedral, Barenco, and Ekert, **Quantum Networks for Elementary Arithmetic Operations**, *Physical Review A*, 54(1):147-153, 1996.
- Barenco, et al., **Elementary Gates for Quantum Computation**, *Physical Review A*, 52(5):3457-3467, 1995.

Simple Quantum Algorithms

- Deutsch
- Phase Change for a Subset of Basis Vectors
- Deutsch-Josza
- Simon

Deutsch Algorithm

Problem: Given a Boolean function $f: \mathbb{Z}_2 \to \mathbb{Z}_2$, determine whether f is constant.



Apply U_f to the input state $|+\rangle|-\rangle$.

If $f(x)$ is constant, then output is $|+\rangle|-\rangle$.
If not, output is $|-\rangle|-\rangle$.

Apply Hadamard to first qubit and measure: 1 if constant, 0 if not.

(Details on next slides.)

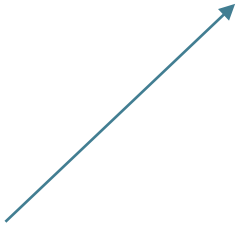
Requires only a single call to black box U_f, while classical algorithm requires two calls.

$$U_f \left|+\right\rangle \left|-\right\rangle = U_f(\frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle))$$

$$
\begin{aligned}
U_f \left|+\right\rangle \left|-\right\rangle &= U_f(\frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)) \\
&= \frac{1}{2}(\left|0\right\rangle \left(\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle\right) + \left|1\right\rangle \left(\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle\right))
\end{aligned}
$$

$$
\begin{aligned}
U_f \left|+\right\rangle \left|-\right\rangle &= U_f(\frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)) \\
&= \frac{1}{2}(\left|0\right\rangle \left(\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle\right) + \left|1\right\rangle \left(\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle\right)) \\
&= \frac{1}{2}\sum_{x=0}^{1} \left|x\right\rangle \left(\left|0 \oplus f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle\right)
\end{aligned}
$$

$$
\begin{aligned}
U_f \left|+\right\rangle \left|-\right\rangle &= U_f(\frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)) \\
&= \frac{1}{2}(\left|0\right\rangle \left(\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle\right) + \left|1\right\rangle \left(\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle\right)) \\
&= \frac{1}{2}\sum_{x=0}^{1} \left|x\right\rangle \left(\left|0 \oplus f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle\right)
\end{aligned}
$$



When $f(x) = 0$, this becomes $\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) = \left|-\right\rangle$.
When $f(x) = 1$, this becomes $\frac{1}{\sqrt{2}}(\left|1\right\rangle - \left|0\right\rangle) = -\left|-\right\rangle$.

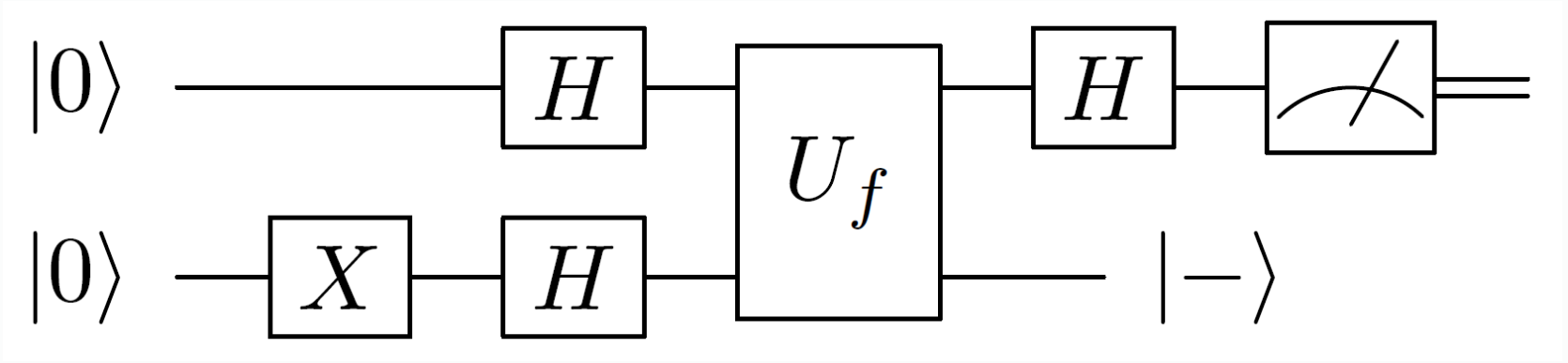
$$
\begin{aligned}
U_f \left|+\right\rangle \left|-\right\rangle &= U_f(\frac{1}{2}(\left|0\right\rangle + \left|1\right\rangle)(\left|0\right\rangle - \left|1\right\rangle)) \\
&= \frac{1}{2}(\left|0\right\rangle \left(\left|0 \oplus f(0)\right\rangle - \left|1 \oplus f(0)\right\rangle\right) + \left|1\right\rangle \left(\left|0 \oplus f(1)\right\rangle - \left|1 \oplus f(1)\right\rangle\right)) \\
&= \frac{1}{2}\sum_{x=0}^{1} \left|x\right\rangle \left(\left|0 \oplus f(x)\right\rangle - \left|1 \oplus f(x)\right\rangle\right)
\end{aligned}
$$

When $f(x) = 0$, this becomes $\frac{1}{\sqrt{2}}(\left|0\right\rangle - \left|1\right\rangle) = \left|-\right\rangle$.
When $f(x) = 1$, this becomes $\frac{1}{\sqrt{2}}(\left|1\right\rangle - \left|0\right\rangle) = -\left|-\right\rangle$.

$$
U_f \left|+\right\rangle \left|-\right\rangle = U_f\left(\frac{1}{\sqrt{2}}\sum_{x=0}^{1} \left|x\right\rangle \left|-\right\rangle\right) = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle
$$

$$U_f |+\rangle |-\rangle = U_f\left(\frac{1}{\sqrt{2}}\sum_{x=0}^{1} |x\rangle |-\rangle\right) = \frac{1}{\sqrt{2}}\sum_{x=0}^{1}(-1)^{f(x)} |x\rangle |-\rangle$$

When $f(x)$ is constant, $(-1)^{f(x)}$ is a meaningless global phase, and the output is $|+\rangle |-\rangle$.
When $f(x)$ is not constant, then $(-1)^{f(x)}$ negates exactly one of the terms, so the output is $|-\rangle |-\rangle$.
By applying a Hadamard gate and measuring the first bit, we get 0 if constant and 1 if not constant.



Dangers of Entangled Ancilla

In the previous section, we said that it's important to uncompute ancilla qubits used to implement quantum functions, in order to un-entangle them from the output bits.

We'll use Deutsch's algorithm to illustrate why.

Selective Phase Change

Problem: Change the phase of terms in a superposition $|\psi\rangle = \sum a_i |i\rangle$, depending on whether i is in a subset X of $\{0,1,\ldots,N-1\}$ or not. More specifically, find an efficient implementation of the following transform:

$$S_X^{\phi}: \sum_{x=0}^{N-1} a_x|x\rangle \rightarrow \sum_{x\in X} a_x e^{i\phi}|x\rangle + \sum_{x\notin X} a_x|x\rangle$$

Requires an efficient implementation of U_f for the function $f(x)$ that tests for membership in X:

$$f(x) = \begin{cases} 1 & \text{if } x \in X \\ 0 & \text{otherwise} \end{cases}$$

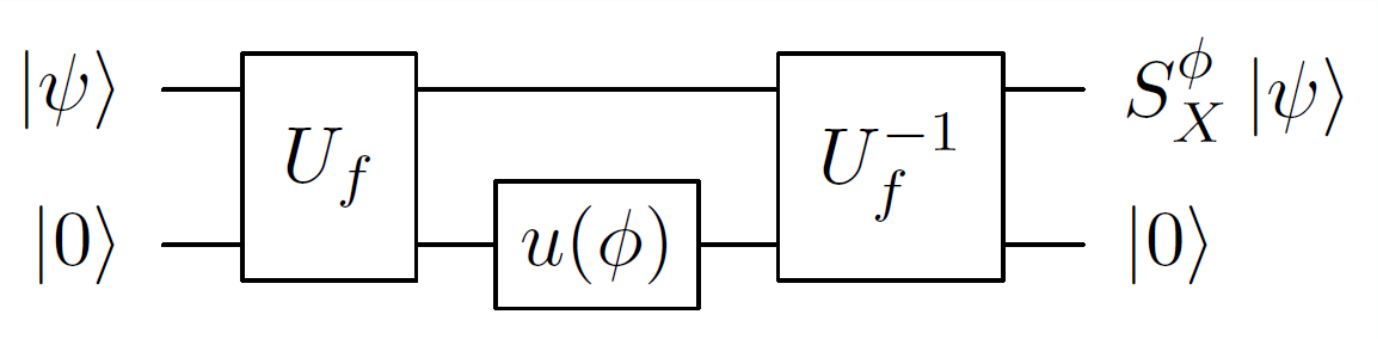
First, apply U_f to $|\psi\rangle|0\rangle$.

$$|\gamma\rangle = U_f|\psi\rangle|0\rangle = \sum_x a_x|x, f(x)\rangle$$
$$= \sum_{x\in X} a_x|x\rangle|1\rangle + \sum_{x\notin X} a_x|x\rangle|0\rangle$$

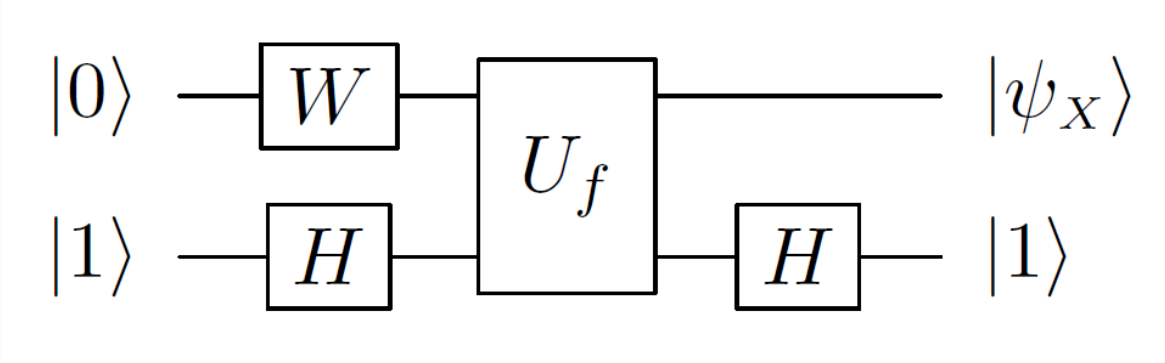
Finally, uncompute using U_f^{-1} to remove any entanglement with the output bit.

Now, apply the phase change gate $u(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$ to the output qubit. This has no effect on $|0\rangle$ and shifts the phase on $|1\rangle$.

$$(I^{\otimes n} \otimes u(\phi))|\gamma\rangle = \sum_{x\in X} a_x|x\rangle e^{i\phi}|1\rangle + \sum_{x\notin X} a_x|x\rangle|0\rangle$$
$$= \sum_{x\in X} a_x e^{i\phi}|x\rangle|1\rangle + \sum_{x\notin X} a_x|x\rangle|0\rangle$$
$$= \left(\sum_{x\in X} a_x e^{i\phi}|x\rangle + \sum_{x\notin X} a_x|x\rangle\right)|f(x)\rangle$$
$$= (S_X^\phi|\psi\rangle)|f(x)\rangle$$



Special case of π:



$$|\psi_X\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle$$