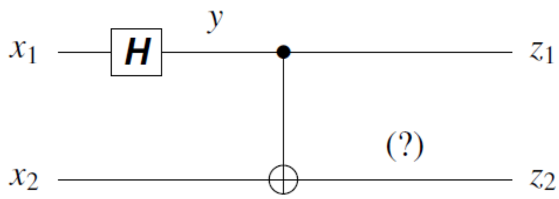
CSE491/596 Lecture Mon. Dec. 7: Large But Feasible Operators, and Measurements

Picking up with the example of a CNOT gate and the basic entangling circuit:



If $x_1 = |0\rangle$, then we can tell exactly what y is: it is the $|+\rangle$ state. And if $x_1 = |1\rangle$, then $y = |-\rangle$. If x_1 is any other qubit state $(a,b) = a|0\rangle + b|1\rangle$, then by linearity we know that $y = a|+\rangle + b|-\rangle$. This expresses y over the transformed basis; in the standard basis it is

$$\frac{1}{\sqrt{2}}(a(1,1)+b(1,-1)) = \frac{1}{\sqrt{2}}(a+b,a-b) .$$

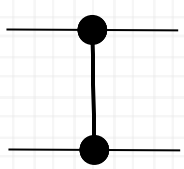
So we can say exactly what the input coming in to the first "wire" of the CNOT gate is. And the input to the second wire is just whatever x_2 is. But because that gate does entanglement, we cannot specify individual values for the wires coming *out*. The state is an inseparable 2-qubit state:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right).$$

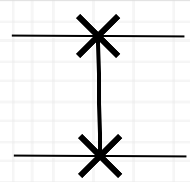
If you measure either qubit individually, you get 0 or 1 with equal probability. This is the same as if you measured the state $|{+}{+}\rangle$. But that state is outwardly as well as inwardly different. When *both* qubits to be measured, it allows 01 and 10 as possible outcomes, whereas measuring the entangled state does not. I've seen papers telling ways to visualize entangled states of 2 or 3 qubits, but none implemented by an applet so far---`quantum-circuit.com` just shows Bloch spheres with the black dot at the center for the "completely mixed state": | ¯_(ツ)_/¯ ⟩.

Two other 2-qubit gates and their matrix and circuit representations are:

$$\mathbf{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$



$$\mathbf{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

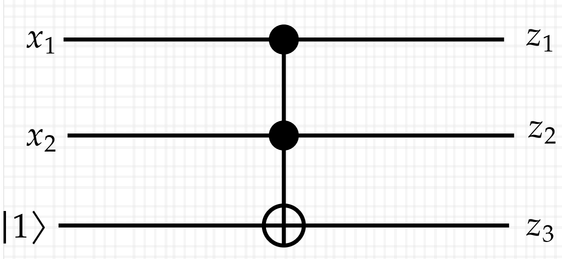


The $\mathbf{CZ}$ gate is symmetric: note that its results on $|01\rangle$ and on $|10\rangle$ are the same. So are the $\mathbf{CS}$ and $\mathbf{CT}$ gates, which have i and $\omega = e^{i\pi/4} = \sqrt{i}$ in place of the -1. For a general $r \times r$ matrix A, $\mathbf{C}A$ is the $2r \times 2r$ matrix given in block form as $\begin{bmatrix} I & 0 \\ 0 & A \end{bmatrix}$. The circuit convention is to put a black dot on the **control** qubit line and a vertical line extending to A in a box the **target** line(s). Most applets make you do that with $\mathbf{CZ}$ as well as $\mathbf{CS}$ and $\mathbf{CT}$, but it is good to remember that these three (and further ones with roots of ω at bottom right) are symmetric.

Three Qubits and More

The **CNOT** gate by itself has the logical description $z_1 = x_1$ and $z_2 = x_1 \oplus x_2$. This means that if $x_1 = 0$ then $z_2 = x_2$, but if $x_1 = 1$ then $z_2 = \neg x_2$. Since this description is complete for all of the standard basis inputs $x = x_1 x_2 = 00, 01, 10, 11$, it extends by linearity to all quantum states. We can use this idea to specify the 3-qubit **Toffoli gate** (**Tof**). It has inputs x_1, x_2, x_3 and symbolic outputs z_1, z_2, z_3 (which, however, might not have individual values in non-basis cases owing to entanglement). Its spec in the basis quantum coordinates is:

$$z_1 = x_1,\ z_2 = x_2, z_3 = x_3 \oplus (x_1 \wedge x_2).$$



$$\begin{array}{c|cccccccc}
 & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline
000 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
001 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
010 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
011 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
100 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
101 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
110 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
111 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{array}$$

Of particular note is that if x_3 is fixed to be a constant-1 input, then

$$z_3 = \neg(x_1 \wedge x_2) = NAND(x_1, x_2).$$

Thus the Toffoli gate subsumes a classical NAND gate, except that you need an extra "helper wire" to put $x_3 = 1$ and you gate two extra output wires z_1, z_2 that only compute the identity on x_1, x_2 (in classical logic, that is---the Toffoli effect of switching the 7th and 8th vector components can have knock-on effects). If you have polynomially many Toffoli gates, then you get only polynomial wastage of wires, and you can use the good ones to simulate any polynomial-size Boolean circuit of NAND gates. The m helper wires are like extra tape cells used by a polynomialt-time Turing machine. They are called *ancilla* qubits, from a Latin word meaning (female) "helper."

Because DTIME$[t(n)]$ has Boolean circuits of size $\widetilde{O}(t(n))$, and because Toffoli gates are deterministic, we can state an immediate consequence:

Theorem: For fully time-constructible $t(n)$ between linear and exponential,

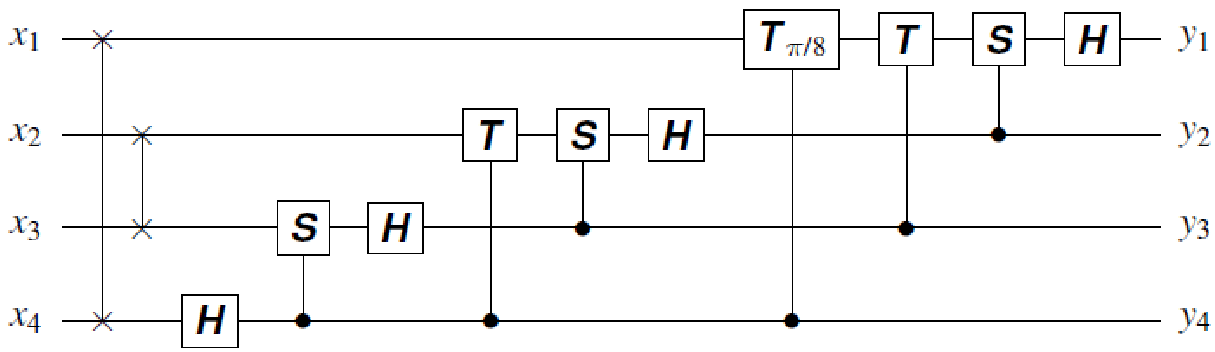
$$\mathrm{DTIME}[t(n)] \subseteq \mathrm{DQ}\left[\widetilde{O}(t(n))\right].$$

In particular, P $\subseteq$ DQP $\subseteq$ BQP, where BQP is to DQP as BPP is to P. (We define BQP formally after saying more about measurements.)

We first need to say more broadly what it means for quantum computations to be (polynomially) **feasible**. The community convention is simply to count up gates of 1, 2, or 3 qubits as constant cost. Gates involving more qubits are OK if they can be built up out of the small gates:

- We have already seen that $H^{\otimes n}$ is just n binary Hadamard gates laid out in parallel.
- The n-qubit **quantum Fourier transform** (QFT) can be built up out of $O(n^2)$ smaller gates---examples for $n = 3$ or 4 are a presentation option.

There is one thing that needs to be said about the QFT. The usual recursive way to build it via $O(n^2)$ unary and binary gates uses controlled rotations by exponentially tiny angles. This is already evident from the four-qubit illustration in the textbook (where the two gates on the left are :

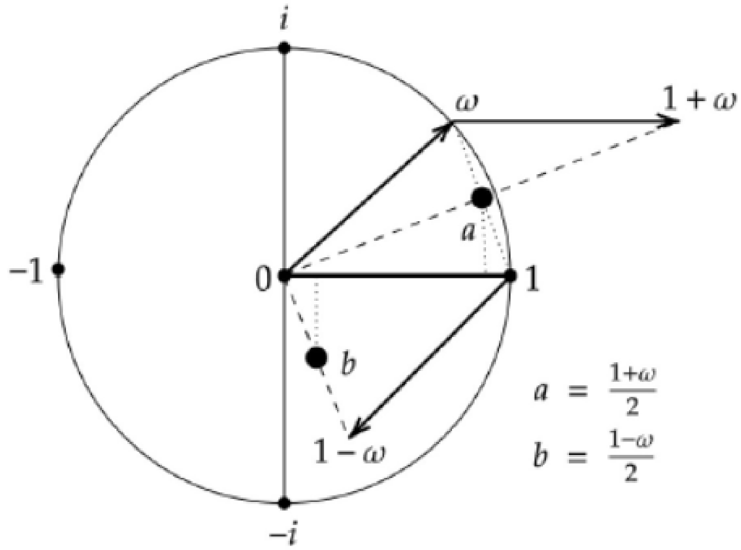


Here $T_{\pi/8} = \begin{bmatrix} 1 & 0 \\ 0 & \omega' \end{bmatrix}$ with $\omega' = e^{i\pi/8}$ not $\omega = e^{i\pi/4}$ as with the T-gate. So ω' has a phase angle one-sixteenth of a circle. For $n = 5$ the next bank uses $1/32$, then $1/64$, and soon the angles would be physically impossible so the gates could never be engineered. Those super-tiny angles are in the definition of the QFT itself. For any n, it takes $\omega_n = e^{2\pi i/N}$ where $N = 2^n$. With $n = 3$, the matrix together with its quantum coordinates is:

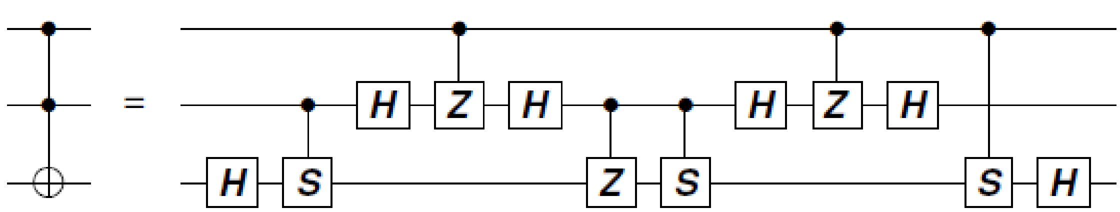
$$\left[\begin{array}{c|cccccccc}
 & 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ \hline
000 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
001 & 1 & \omega & i & i\omega & -1 & -\omega & -i & -i\omega \\
010 & 1 & i & -1 & -i & 1 & i & -1 & -i \\
011 & 1 & i\omega & -i & \omega & -1 & -i\omega & i & -\omega \\
100 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
101 & 1 & -\omega & i & -i\omega & -1 & \omega & -i & i\omega \\
110 & 1 & -i & -1 & i & 1 & -i & -1 & i \\
111 & 1 & -i\omega & -i & -\omega & -1 & i\omega & i & \omega
\end{array}\right]
=
\left[\begin{array}{c|cccccccc}
 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \hline
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & \omega & \omega^2 & \omega^3 & -1 & \omega^5 & \omega^6 & \omega^7 \\
2 & 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\
3 & 1 & \omega^3 & \omega^6 & \omega & -1 & \omega^7 & \omega^2 & \omega^5 \\
4 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
5 & 1 & \omega^5 & \omega^2 & \omega^7 & -1 & \omega & \omega^6 & \omega^3 \\
6 & 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\
7 & 1 & \omega^7 & \omega^6 & \omega^5 & -1 & \omega^3 & \omega^2 & \omega
\end{array}\right]$$

$$\mathbf{QFT}[i,j] = \omega^{ij}$$

For $\mathbf{QFT}_N$ we raise ω_N with its tiny phase to exponentially many different powers. How can this possibly be feasible? Leonid Levin among others raised this objection. Here are several answers:



- Basic gates can fabricate quantum states having finer phases. This is already hinted by the diagram in the case of $\mathbf{HTH}$. Try composing $\mathbf{HTHT^*H}$ and $\mathbf{HTHT^*HTHT^*H}$. The *Solovay-Kitaev theorem* enables approximating operators with exponentially fine angles by polynomially many gates of phases that are multiples of ω (using **CNOT** to extend this to multiple-qubit operators).
- The Toffoli and Hadamard gates by themselves, which have phases only $+1$ and -1, can simulate the real parts and imaginary parts of quantum computations separately via binary code, in a way that allows re-creating all measurement probabilities. (This is undertaken in exercises 7.8--7.14 with a preview in the solved exercise 3.8.)
- The **CNOT** and Hadamard gates do not suffice for this, even when the so-called "phase gate" $\mathbf{S} = \mathbf{T}^2 = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$ is added. The Pauli $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$ gates and also $\mathbf{CZ}$ can be built from these, but quantum circuits of these gates can be simulated in deterministic ("classical") polynomial time. However, $\mathbf{CS}$ suffices to build the Toffoli gate, per the diagram below (which is also a presentation option). So Hadamard + $\mathbf{CS}$ is a universal set using only quarter phases.
- The signature application of the QFT, which is *Shor's algorithm* showing that factoring belongs to BQP, may only require coarsed-grained approximations to $\mathbf{QFT}_N$.



For these reasons, $\mathbf{QFT}_N$ is considered feasible even though $N = 2^n$ is exponential. Not every $N \times N$ unitary matrix U is feasible---the Solovay-Kitaev theorem relies on U having a small exact formulation to begin with. But if we fix a finite **universal gate set** (such as $\mathbf{H+T+CNOT}$, $\mathbf{H+Tof}$, or $\mathbf{H+CS}$ above) and use only matrices that are compositions and tensor products of these gates, then we can use the simple gate-counting metric as the main complexity measure.