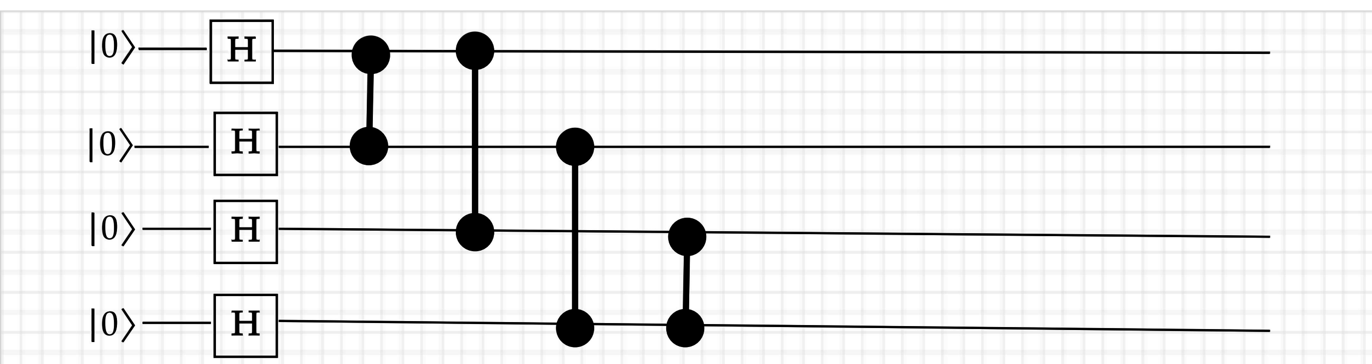
CSE491/596 Lecture Mon. 11/20/23: General Quantum Circuits and Computations

If there are n qubits, then the underlying matrices we get are $N \times N$ with $N = 2^n$. It is much harder to handle 2^n-sized stuff than n-sized stuff. Happily, we can always break the basic gates down to constant size---3 at most with the Toffoli gate in practice---and there are theorems that guarantee constant size gates working in general. One important case of using n single-qubit gates is the **Hadamard transform** $\mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H}$ (n times), which can be abbreviated $\mathbf{H}^{\otimes n}$:

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \quad H^{\otimes 3} = \frac{1}{2\sqrt{2}}\left[\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]$$

We always have $H^{\otimes n}|0^n\rangle = |+\rangle^{\otimes n} = |+^n\rangle =$ the all-1 vector of length $N = 2^n$ divided by $\sqrt{N} = \sqrt{2^n} = 2^{n/2}$. Often this is the first step of a quantum circuit, for example:



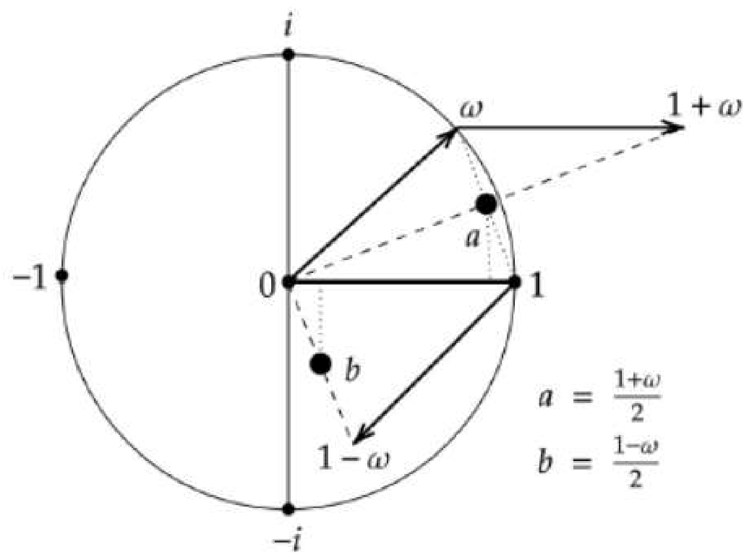
Putting the same Hadamard transform also at the end creates what is called a **graph state circuit**; we will analyze them later.

We will call an $N \times N$ matrix that arises from a single small gate---or a tensor product of small gates---a **succinct** matrix. Thus a **quantum computation** of **length** s is formally a composition of s succinct matrices applied to some input vector. The text draws allusion to a classical computation on a binary string x of length n, such as $x = 10100010$, say. The quantum circuit starts with input the basis state $|x\rangle = |10100010\rangle$. We could actually start with $|0^8\rangle$ but then **prepare** the state $|x\rangle$ by making the first column of the circuit be the tensor product

$$\mathbf{X} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{I} \otimes \mathbf{X} \otimes \mathbf{I},$$

which has a NOT gate where x has a 1. This is why we often suppose ("without loss of generality") that the circuit starts with the all-zero basis vector.

The $\mathbf{Z}$ and $\mathbf{CZ}$ gates are the heads of an important family of basic gates having to do with rotations of **phase**, which is a curious but definitely physical property. When a complex number $x + iy$ is rewritten in polar form as $re^{i\theta}$, the angle θ is the phase. The magnitude is r, so when $r = 1$ we have a unit complex number. Note that i itself is the same as $e^{i\pi/2}$ since $\frac{\pi}{2}$ means 90° phase. Then $i^2 = e^{i\pi} = -1$ and if we put $\omega = e^{i\pi/4}$ then $\omega^2 = i$. In Cartesian coordinates, $\omega = \frac{1+i}{\sqrt{2}}$. Here is some more geometry:



The vector $\mathbf{u} = [a, b]^T$ is a funky unit vector. To see that it is a unit vector, note that

$$||\mathbf{u}||^2 = \langle \mathbf{u}, \mathbf{u} \rangle = \mathbf{u}^* \mathbf{u} = a^* a + b^* b = \left(\frac{1+\overline{\omega}}{2}\right)\left(\frac{1+\omega}{2}\right) + \left(\frac{1-\overline{\omega}}{2}\right)\left(\frac{1-\omega}{2}\right).$$

In polar form, the complex conjugate of $e^{i\theta}$ is always $e^{-i\theta} = e^{i(2\pi-\theta)}$, so $\overline{\omega} = e^{i7\pi/4} = \omega^7$. In Cartesian coordinates,

$$\frac{1+\omega}{2} = \frac{1}{2}\left(1 + \frac{1+i}{\sqrt{2}}\right) = \frac{\sqrt{2}+1+i}{2\sqrt{2}} \quad \text{and} \quad \frac{1-\omega}{2} = \frac{1}{2}\left(1 - \frac{1+i}{\sqrt{2}}\right) = \frac{\sqrt{2}-1-i}{2\sqrt{2}}$$

So

$$\frac{1+\overline{\omega}}{2} = \frac{1}{2}\left(1 + \frac{1-i}{\sqrt{2}}\right) = \frac{\sqrt{2}+1-i}{2\sqrt{2}} \quad \text{and} \quad \frac{1-\overline{\omega}}{2} = \frac{1}{2}\left(1 - \frac{1-i}{\sqrt{2}}\right) = \frac{\sqrt{2}-1+i}{2\sqrt{2}}.$$

Then

$$\left(\frac{1+\overline{\omega}}{2}\right)\left(\frac{1+\omega}{2}\right) = \frac{1}{8}\left(\sqrt{2}+1+i\right)\left(\sqrt{2}+1-i\right) = \frac{1}{8}\left[\left(\sqrt{2}+1\right)^2+1\right] = \frac{1}{8}\left(2+1+2\sqrt{2}+1\right) = \frac{2+\sqrt{2}}{4}$$

and

$$\left(\frac{1-\overline{\omega}}{2}\right)\left(\frac{1-\omega}{2}\right) = \frac{1}{8}\left(\sqrt{2}-1-i\right)\left(\sqrt{2}-1+i\right) = \frac{1}{8}\left[\left(\sqrt{2}-1\right)^2+1\right] = \frac{1}{8}\left(2+1-2\sqrt{2}+1\right) = \frac{2-\sqrt{2}}{4}.$$

These squared values add to 1 as promised, so $\mathbf{u} = [a, b]^T$ is a unit vector. How do we get it? Here is the start of an infinite family of gates:

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \ \mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \ \mathbf{T} = \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}, \ \mathbf{T}_{\pi/8} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}.$$

The controlled versions to go with $\mathbf{CZ}$ are $\mathbf{CS}$, $\mathbf{CT}$, etc. They, too, are symmetric---indeed, all of these gates are controlled phase shifts conditioned on the basis-state 1 of all of the (one or two) qubits involved. (Here I must note global inconsistency and confusion in notation, especially about rotations, which we will try to resolve when we cover the **Bloch Sphere** next week.)

Now we have all the background we need to read **quantum circuits**. Lecture will go on to illustrate them, both out of section 4.5 and (the same examples) on QC web applets.