CSE491/596 Lecture Friday 12/04: Quantum Computing II---Qubits and Quantum Circuits

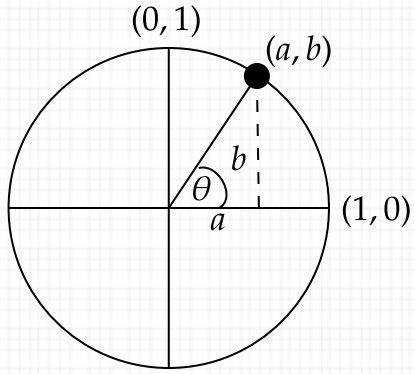
[Based on https://cse.buffalo.edu/~regan/cse491596/CSE596lect112618.pdf but goes further. The break to Monday will be somewhere between the "Two Qubits" and "Three Qubits" sections.]

A **qubit** is a physical system whose **state** ϕ is described by a pair (a, b) of complex numbers such that $|a|^2 + |b|^2 = 1$. The components of the pair *index* the *basic outcomes* 0 and 1. There are two ways we can gain knowledge about the values a and b:

- We can **prepare** the state from the known initial state $e_0 = (1, 0)$ by known quantum operations, which here can be represented by 2×2 matrices.
- We can **measure** the state (with respect to these basic outcomes), in which case:
  - We either **observe** 0, whereupon the state becomes $\mathbf{e}_0$, or we observe 1, in which case the state becomes $\mathbf{e}_1 = (0, 1)$.
  - The probability of observing 0 is $|a|^2$, of getting 1 is $|b|^2$.

If both a and b are real numbers, then we can picture the qubit as a point on the unit circle in $\mathbb{R}^2$:

$$|a|^2 + |b|^2 = 1$$
$$a = \cos\theta$$
$$b = \sin\theta$$



For example, we can have $a = b = 1$. Oops, not quite, because their squares add up to 2, so what we really mean is $a = b = \sqrt{1/2} = 0.70710678...$ If we measure $\pi = \frac{1}{\sqrt{2}}(1, 1)$, then we observe 0 and 1 with equal probability $\frac{1}{2}$. Measuring this π is like flipping a fair coin. Another legal state is $\mu = \frac{1}{\sqrt{2}}(1, -1)$. This gives the same probabilities, because $(-1)^2 = 1$. If all we can do is measure (*in the* 0, 1 *basis*), we can't tell the difference between whether the state is π or μ. Note that we can prepare the π and μ states by applying the Hadamard matrix $\mathbf{H}$ to 0 and 1:

- $\mathbf{H}\mathbf{e}_0 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \pi$
- $\mathbf{H}\mathbf{e}_1 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mu$

Three other operators, named for the physicist Wolfgang Pauli, and their effects on states, are:

- $\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, aka. **NOT**: $\mathbf{X}\mathbf{e}_0 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{e}_1; \mathbf{X}\mathbf{e}_1 = \mathbf{e}_0.$
- $\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}: \mathbf{Z}\pi = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mu; \mathbf{Z}\mu = \pi; \mathbf{Z}\mathbf{e}_0 = \mathbf{e}_0.$
- $\mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}: \mathbf{Y}\mathbf{e}_0 = i\mathbf{e}_1; \mathbf{Y}\mathbf{e}_1 = -i\mathbf{e}_0; \mathbf{Y}\pi = \frac{1}{\sqrt{2}}\begin{pmatrix} -i \\ i \end{pmatrix} = -i\mu; \mathbf{Y}\mu = i\pi.$

What can be confusing in the diagram is that we also habitually use the unit circle in $\mathbb{R}^2$ to illustrate a single unit complex number c, that is, an element of $\mathbb{C}^1$ of magnitude 1. We would then write $c = a + bi$, and then $|c|^2 = 1$ is the same as $a^2 + b^2 = 1$. Our pair (a, b) of complex numbers, however, is an element of $\mathbb{C}^2$, which is 4-dimensional if we tried to view it in real space.

- My textbook with Lipton takes the attitude that there is enough similarity between $\mathbb{R}^2$ and $\mathbb{C}^2$ to visualize using the above diagram anyway---provided you handle complex numbers correctly if and when they come up. The similarities go into using the common general term **Hilbert Space** for $\mathbb{R}^n$ and $\mathbb{C}^n$, though quantum physicists use the term most when the dimensionality is infinite.
- The fully correct diagram is being employed more by web tools, however, so we will take an excursion to discuss it. (I added it to Part II, Chapter 14 for the textbook's new 2nd ed.)

The Bloch Sphere

There is a way to cut the dimensions down to 3. The following definition will be useful for quantum states of multiple qubits as well:

Definition: Two quantum states ϕ, ϕ' are **equivalent** if there is a unit complex number c such that $\phi' = c\phi$.

For example, $\frac{1}{\sqrt{2}}(-1, 1)$ is equivalent to $\frac{1}{\sqrt{2}}(1, -1)$, but neither is equivalent to $\frac{1}{\sqrt{2}}(1, 1)$, nor any of these to our basic states $(1, 0)$ and $(0, 1)$. In the line for the matrix $\mathbf{Y}$, $i\mathbf{e}_1$ is simply equivalent to just $\mathbf{e}_1$, $-i\mathbf{e}_0$ to $\mathbf{e}_0$, $-i\mu$ to μ, and $i\pi$. We could also regard $\mathbf{Y}$ as equivalent to

$$i\mathbf{Y} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

which makes clearer that it is a combination of $\mathbf{X}$ and $\mathbf{Z}$ (indeed, $i\mathbf{Y} = \mathbf{Z}\mathbf{X} = -\mathbf{X}\mathbf{Z}$). Finally, to finish the line for $\mathbf{Z}$, $\mathbf{Z}\mathbf{e}_1 = -\mathbf{e}_1 \equiv \mathbf{e}_1$.

Regarding our saying *equivalence*, note that

$$\frac{1}{c} = \frac{1}{a+bi} = \frac{a - bi}{(a+bi)(a-bi)} = \frac{a - bi}{a^2 + b^2} = \frac{a - bi}{1} = a - bi = \overline{c},$$

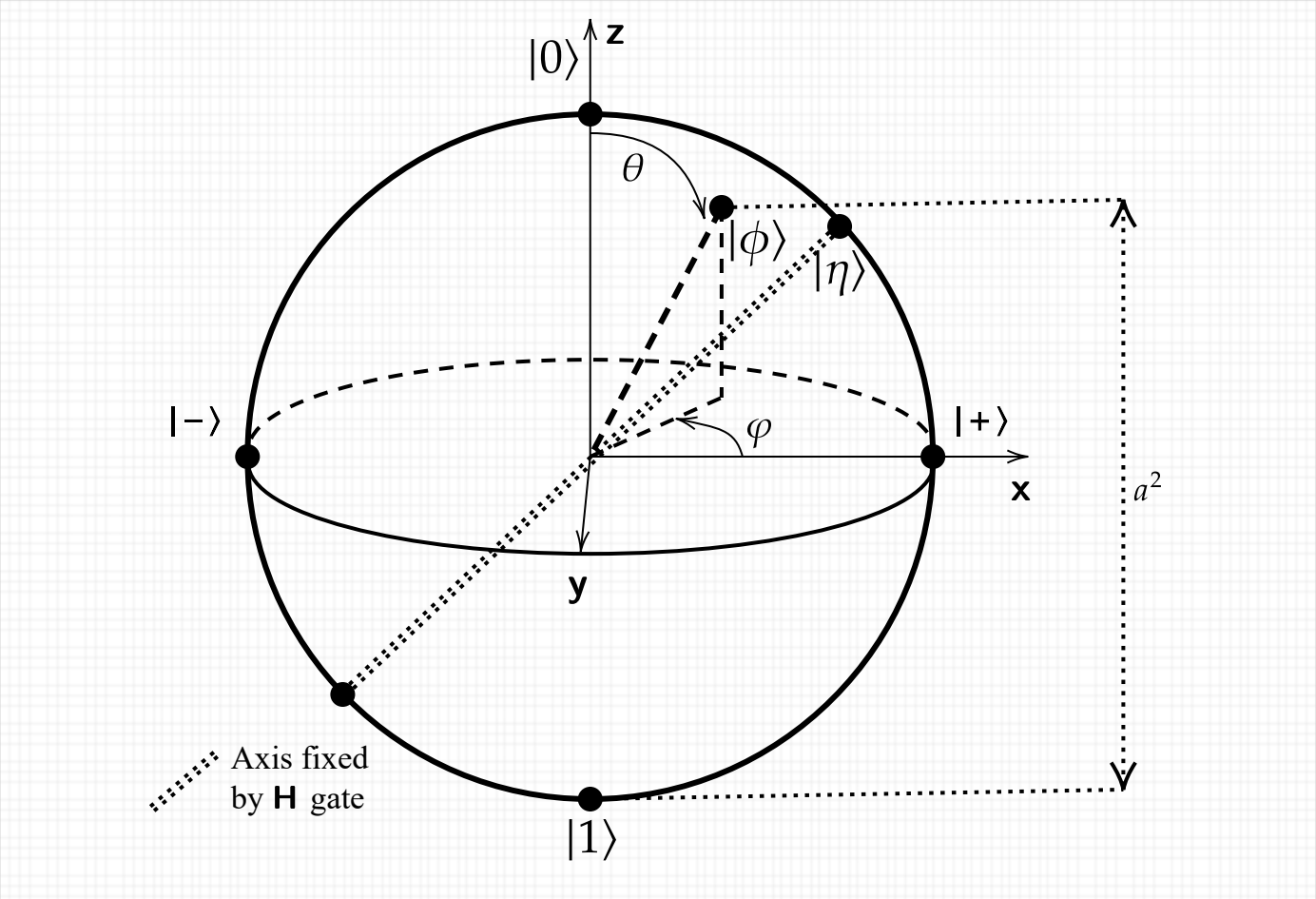
which is the **complex conjugate** of c and is likewise a unit complex number. Since $\phi = \overline{c}\phi'$ the relation is symmetric. That the product of two unit complex numbers is a unit complex number makes it transitive, and being reflexive is immediate with $c = 1$, so this is an equivalence relation.

A unit complex number can be written in polar coordinates as $c = e^{i\gamma}$ for some angle γ, which represents a "global phase." Thus, dividing out by this equivalence relation emphasizes the **relative phase** φ of the two components. So let us write our original quantum state ϕ in polar coordinates as $\left(ae^{i\alpha}, be^{i\beta}\right)$ where now a, b are real numbers between 0 and 1. Choose $\gamma = -\alpha$, then $c\phi = \left(a, be^{i\varphi}\right)$ with $\varphi = \beta - \alpha$. Since $a^2 + b^2 = 1$, the value of b is forced once we specify a. So a and φ are enough to specify the state.

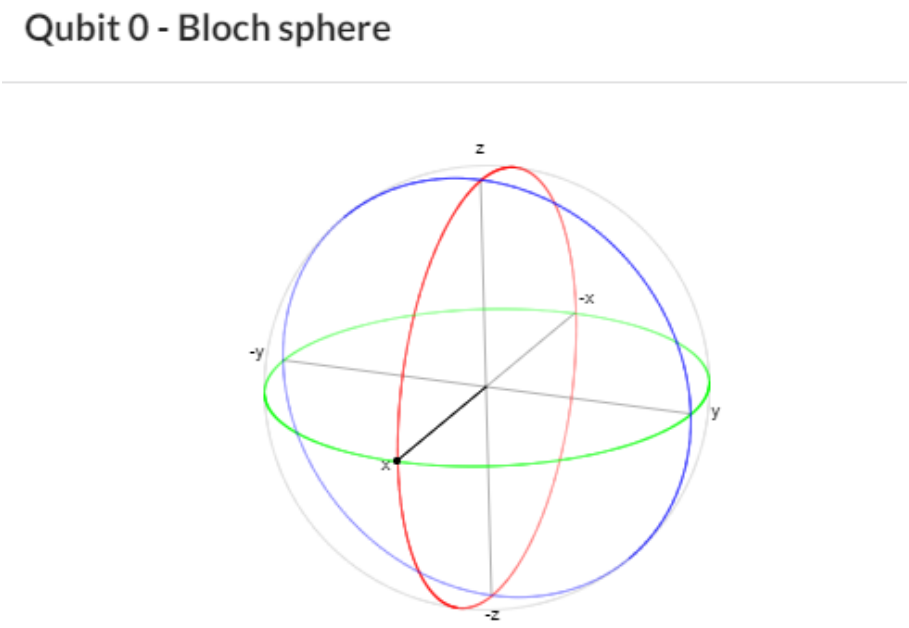
We can uniquely map points (a, φ) to the sphere by treating φ as a longitude and a^2 (rather than a) as a latitude where the north pole is 1, the equator is 0.5, and the south pole is 0. Then the latitude gives the probability of getting the outcome 0. All states like π and μ that give equal probability of 0 and 1 fan out along the equator. The north pole is 0 and the south pole is 1. Well, it's high time we give these states their formal names using **Dirac notation**:

- $e_0 = 0$ is called $|0\rangle$ and $e_1 = 1$ is called $|1\rangle$.
- $\frac{1}{\sqrt{2}}(1, 1) = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ is called $|+\rangle$, the "plus" state.
- $\frac{1}{\sqrt{2}}(1, -1) = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ is called $|-\rangle$, the "minus" state.

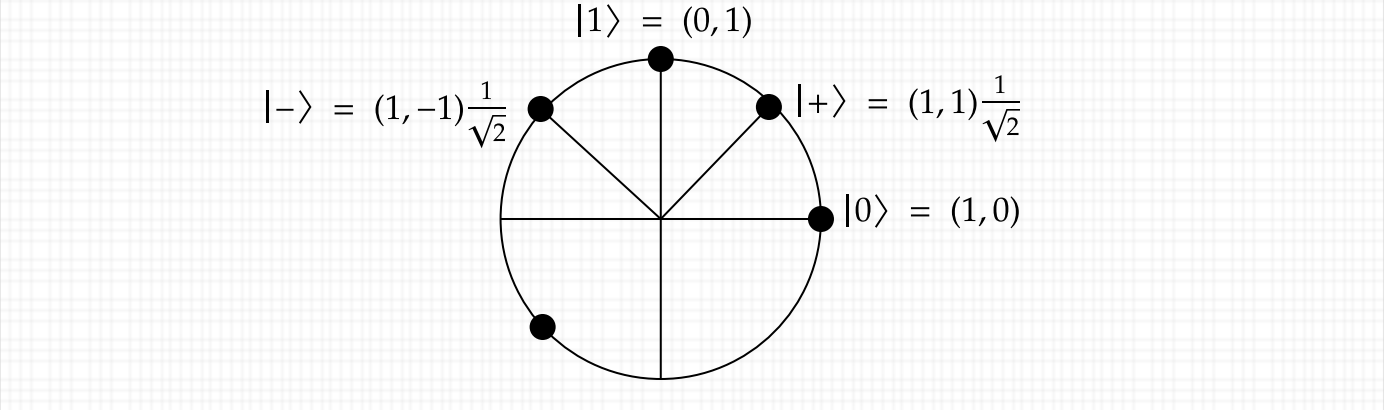
Here they all are, graphed on the **Bloch Sphere**:



Among web applets displaying Bloch spheres for qubits is https://quantum-circuit.com/home (free registration required). Here is its graph for the $|+\rangle$ state. It is more usual to show the $\mathbf{x}$ axis out toward the reader and $\mathbf{y}$ at right, but that is less convenient IMHO for picturing $|+\rangle$ and $|-\rangle$.



Some algorithms, however, are IMHO easier to picture using the original planar diagram:



For one thing, this makes it easier to tell that $|0\rangle$ and $|1\rangle$ are orthogonal vectors, that $|+\rangle$ and $|-\rangle$ are likewise orthogonal vectors, and that the orthonormal basis $\{|+\rangle, |-\rangle\}$ is obtained by a linear transformation (indeed, a simple rotation) of the standard basis $\{|0\rangle, |1\rangle\}$.

A downside, however, is that this diagram gives extra points for equivalent space, whereas the Bloch sphere is completely non-redundant. The Bloch sphere is also "more real" than the way we usually graph complex numbers via Cartesian coordinates. In fact, *every unitary* 2×2 *matrix* U *induces a rotation of the Bloch sphere and hence fixes an axis, so the axes of the sphere are in 1-to-1 correspondence with lossless quantum operations on a single qubit.* Whereas, the planar diagram gives a cut-down picture of how $\mathbf{H}$ acts as a rotation without fully showing you its axis.

[There is optional reading for Dirac Notation and the Bloch Sphere, which I have posted to the non-public link https://cse.buffalo.edu/~regan/cse491596/LRQmitbook2pp131-147.pdf I worry it is overkill, and its illustration of "quarts" might confuse with what follows; I regard the above notes as enough. The following section returns to chapters 3--4 of the text.]

Two Qubits [Based on https://cse.buffalo.edu/~regan/cse491596/CSE596lect112818.pdf]

An n-qubit quantum state is denoted by a unit vector in $\mathbb{C}^N$ where $N = 2^n$. Thus, a 2-qubit state is represented by a unit vector in $\mathbb{C}^4$. That takes up 8 real dimensions, and even trying tricks as for the Bloch Sphere would bring that down only to a 6-dimensional hypersurface in $\mathbb{R}^7$. Until we have a Hyper-Zoom able to help us visualize 7-dimensional space, we have to rely on linear algebra and some general ideas shared by Hilbert Spaces whether real or complex.

One of those ideas is the **standard basis**. In 4-space, this is given by the vectors:

$$e_1 = (1,0,0,0),\ e_2 = (0,1,0,0),\ e_3 = (0,0,1,0),\ e_4 = (0,0,0,1)\ .$$

The indexing scheme for **quantum coordinates** changes the labels to come from $\{0,1\}^2$ instead of from $\{1,2,3,4\}$, using the canonical binary order $00, 01, 10, 11$. Then we have:

$$e_{00} = (1,0,0,0),\ e_{01} = (0,1,0,0),\ e_{10} = (0,0,1,0),\ e_{11} = (0,0,0,1)\ .$$

The big advantage is that these basis elements are all separable and the labels respect the tensor products involved:

$$\begin{aligned}
|00\rangle &= e_{00} = (1,0,0,0) = (1,0)\otimes(1,0) = e_0 \otimes e_0 = |0\rangle\otimes|0\rangle = |0\rangle|0\rangle\\
|01\rangle &= e_{01} = (0,1,0,0) = (1,0)\otimes(0,1) = e_0 \otimes e_1 = |0\rangle\otimes|1\rangle = |0\rangle|1\rangle\\
|10\rangle &= e_{00} = (0,0,1,0) = (0,1)\otimes(1,0) = e_1 \otimes e_0 = |1\rangle\otimes|0\rangle = |1\rangle|0\rangle\\
|11\rangle &= e_{11} = (0,0,0,1) = (0,1)\otimes(0,1) = e_1 \otimes e_1 = |1\rangle\otimes|1\rangle = |1\rangle|1\rangle
\end{aligned}$$

It is OK to picture the tensoring with row vectors, but because humanity chose to write matrix-vector products as Mv rather than vM, they need to be treated as column vectors. This will lead to cognitive dissonance when we read quantum circuits left-to-right but have to compose matrices right-to-left. Lipton and I are curious whether a "non-handed" description of nature can work.

With the "plus" and "minus" states, we also have (note $\frac{1}{\sqrt{2}}(1,1)\otimes\frac{1}{\sqrt{2}}(1,1) = \frac{1}{2}(1,1)\otimes(1,1)$):

$$\begin{aligned}
|{+}{+}\rangle &= |+\rangle\otimes|+\rangle = \tfrac{1}{2}(1,\ 1)\otimes(1,\ 1) = \tfrac{1}{2}(1,\ 1,\ 1,\ 1) = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}\\
|{+}{-}\rangle &= |+\rangle\otimes|-\rangle = \tfrac{1}{2}(1,\ 1)\otimes(1,-1) = \tfrac{1}{2}(1,-1,\ 1,-1) = \frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}
\end{aligned}$$

$$|-+\rangle = |-\rangle\otimes|+\rangle = \tfrac{1}{2}(1,-1)\otimes(1,\ 1) = \tfrac{1}{2}(1,\ 1,-1,-1) = \frac{|00\rangle+|01\rangle-|10\rangle-|11\rangle}{2}$$
$$|--\rangle = |-\rangle\otimes|-\rangle = \tfrac{1}{2}(1,-1)\otimes(1,-1) = \tfrac{1}{2}(1,-1,-1,\ 1) = \frac{|00\rangle-|01\rangle-|10\rangle+|11\rangle}{2}$$

These four vectors are linearly independent and mutually orthogonal, so they form an orthonormal basis. We can map the standard 4-dimensional basis to this one by forming the target vectors into a matrix---happily the matrix is symmetric and real so "handedness" does not come into play:

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\otimes\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \mathbf{H}\otimes\mathbf{H} = \mathbf{H}^{\otimes 2}.$$

Well, this is the case $m = 2$ of the Hadamard transform $\mathbf{H}^{\otimes m}$, about which more on Monday. Also note the following tensor products of 2×2 matrices:

$$\mathbf{H}\otimes\mathbf{I} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\otimes\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{array}\right],$$

$$\mathbf{I}\otimes\mathbf{H} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\otimes\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left[\begin{array}{cc|cc} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{array}\right].$$

Some examples of states you can produce with these matrices are:

$$|+0\rangle = |+\rangle\otimes|0\rangle = \frac{1}{\sqrt{2}}(1,1)\otimes(1,0) = \frac{1}{\sqrt{2}}(1,0,1,0) = \frac{|00\rangle+|10\rangle}{\sqrt{2}}$$
$$|0+\rangle = |0\rangle\otimes|+\rangle = \frac{1}{\sqrt{2}}(1,0)\otimes(1,1) = \frac{1}{\sqrt{2}}(1,1,0,0) = \frac{|00\rangle+|01\rangle}{\sqrt{2}}$$

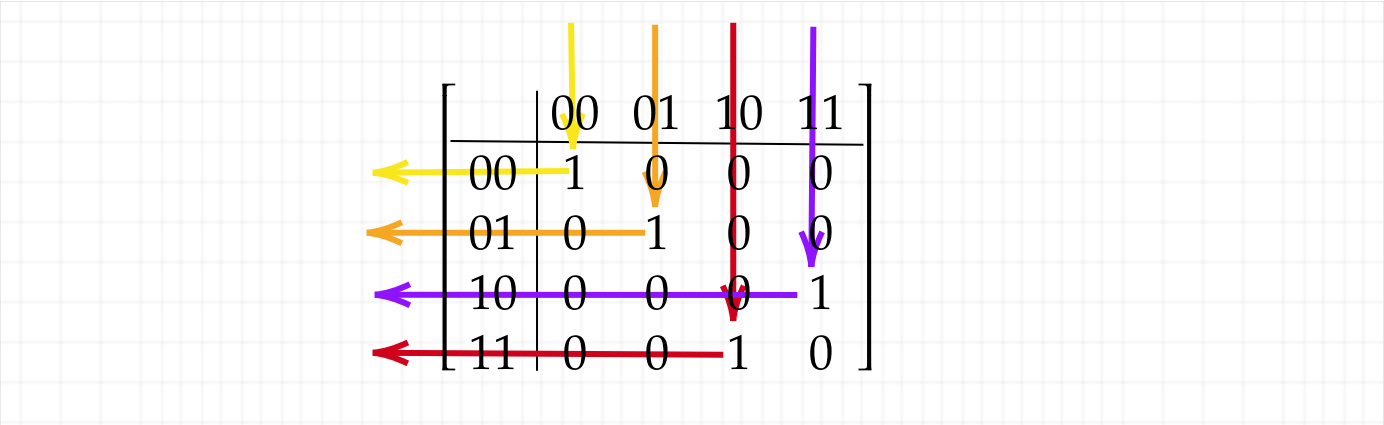
Meanwhile,

$$|+1\rangle = |+\rangle\otimes|1\rangle = \frac{1}{\sqrt{2}}(1,1)\otimes(0,1) = \frac{1}{\sqrt{2}}(0,1,0,1) = \frac{|01\rangle+|11\rangle}{\sqrt{2}}$$

can be gotten as $\mathbf{H}\otimes\mathbf{I}$ applied to the column vector $(0,1,0,0)^T = |01\rangle$. However, the state $\frac{1}{\sqrt{2}}(1,0,0,1) = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, which we saw in the last lecture is entangled, cannot be gotten this way. Instead, it needs the help of a 4×4 unitary matrix that is not a tensor product of two smaller matrices. The most omnipresent one of these is:

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

Any linear operator is uniquely defined by its values on a particular basis, and on the standard basis, the values are: $\mathbf{CNOT}e_{00} = \mathbf{CNOT}|00\rangle = |00\rangle$, $\mathbf{CNOT}e_{01} = \mathbf{CNOT}|01\rangle = |01\rangle$, $\mathbf{CNOT}e_{10} = \mathbf{CNOT}|10\rangle = |11\rangle$, and $\mathbf{CNOT}e_{11} = \mathbf{CNOT}|11\rangle = |10\rangle$. We can get these from the respective columns of the $\mathbf{CNOT}$ matrix, and we can also label the quantum coordinates right on it:



Because we multiply column vectors, the co-ordinates of the argument vector come in the top and go out to the left. If the first qubit is 0, then the whole gate acts as the identity. But if the first qubit is 1, then the basis value of the second qubit gets flipped---the same action as the **NOT** gate $\mathbf{X}$. Hence the name Controlled-NOT, abbreviated $\mathbf{CNOT}$: the **NOT** action is controlled by the first qubit. The action on a general 2-qubit quantum state $\phi = (a, b, c, d)$ is even easier to picture:

$$\mathbf{CNOT}\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}.$$

All it does is switch the third and fourth components---of any 4-dim. state vector. Hence, $\mathbf{CNOT}$ is a **permutation gate** and is entirely deterministic. Permuting these two indices is exactly what we need to transform the separable state $\frac{1}{\sqrt{2}}(1, 0, 1, 0)$ into the entangled state $\frac{1}{\sqrt{2}}(1, 0, 0, 1)$. Since we got the former state from $\mathbf{H} \otimes \mathbf{I}$ applied to $\mathbf{e}_{00}$, the matris we want is

$$\mathbf{CNOT} \cdot (\mathbf{H} \otimes \mathbf{I}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left[\begin{array}{c|ccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{array}\right].$$

We can see the result coming from the first column. When we do a quantum circuit left-to-right, however, the $(\mathrm{H} \otimes \mathrm{I})$ part comes first on the left. The symbol for a **CNOT** gate is to use a black dot to represent the control on the *source qubit* and $\oplus$ (which I have used as a symbol for XOR) on the *target qubit*. This is more easily pictured by a quantum circuit diagram: