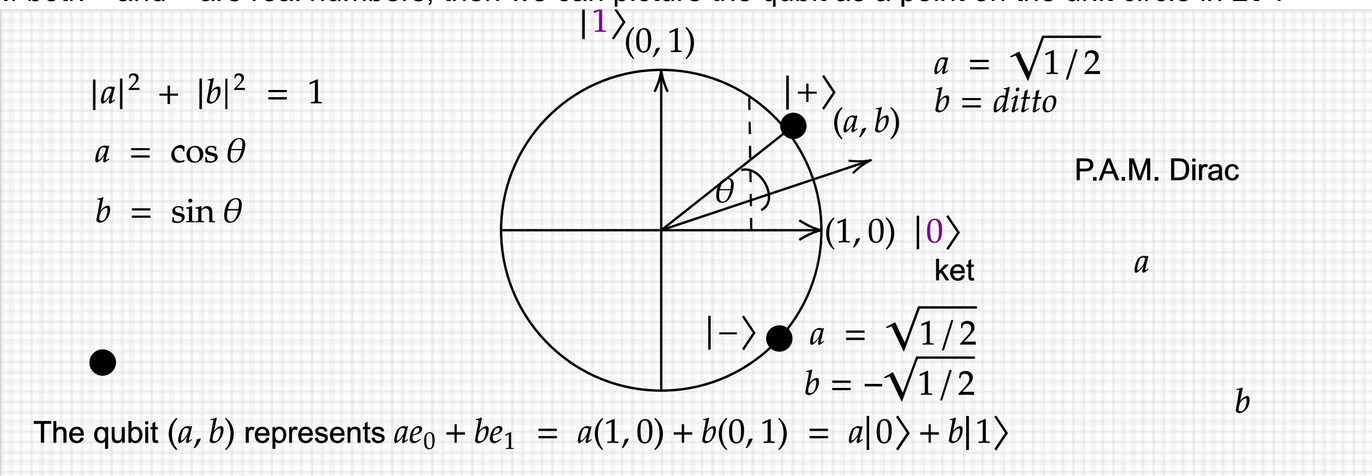
CSE491/596 Lecture 11/15/23: Quantum Computing Basics II

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* $\mathbf{0}$ and $\mathbf{1}$. 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** $\mathbf{0}$, whereupon the state becomes $\mathbf{e_0}$, or we observe $\mathbf{1}$, in which case the state becomes $\mathbf{e_1} = (0, 1)$.
  - The probability of observing $\mathbf{0}$ is $|a|^2$, of getting $\mathbf{1}$ 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 $\mathbb{R}^2$:



Notation: A^* vs. $A^\dagger$ for conjugate transpose. The latter is becoming preferred.

Note: Generally, $\langle\phi| = |\phi\rangle^*$. Thus $\langle\psi|\cdot|\phi\rangle = \langle\psi|\phi\rangle$

The triple product with a matrix is written as e.g. $\langle y|A|x\rangle = y^*Ax$ as ordinary vector-matrix multiplication.

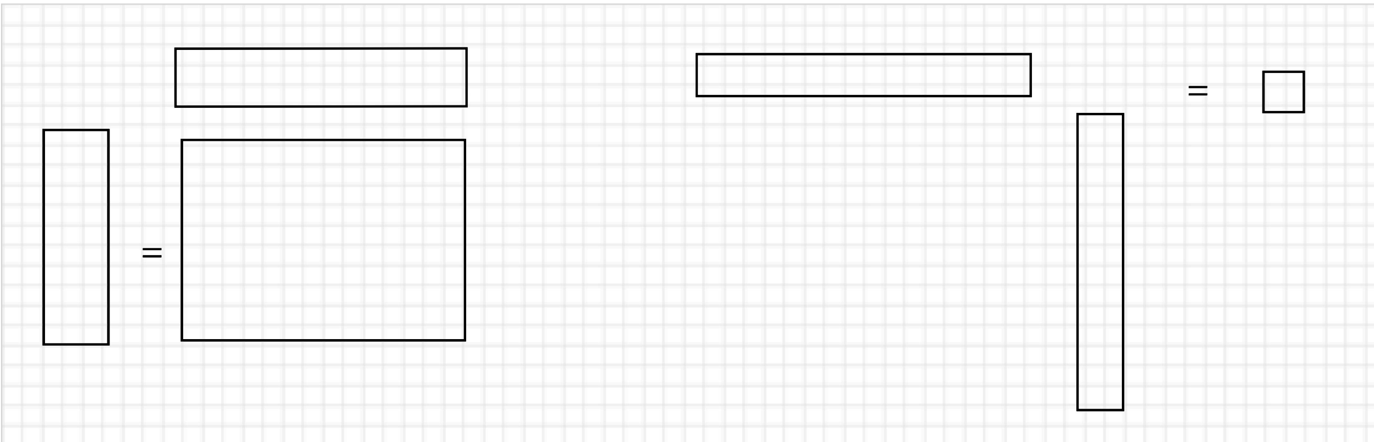
If instead we do $|\phi\rangle\cdot\langle\psi|$, then we have a column vector multiplying a conjugated row vector. As an operator, $|\psi\rangle\cdot\langle\psi|$ is a matrix that when multiplying a vector $|\phi\rangle$ gives $|\psi\rangle\cdot\langle\psi| \cdot |\phi\rangle = |\psi\rangle\cdot\langle\psi|\phi\rangle = |\psi\rangle$ multiplied by the scalar inner product of ψ and ϕ.

Finally, $|\psi\rangle\cdot|\phi\rangle$ is the tensor product of $|\psi\rangle$ *and* $|\phi\rangle$. E.g. $|0\rangle|1\rangle = |01\rangle = |0\rangle\otimes|1\rangle$.

$$A \otimes B = \begin{bmatrix} a_{1,1}B & a_{1,2}B & a_{1,3}B & a_{1,4}B \\ a_{2,1}B & a_{2,2}B & a_{2,3}B & a_{2,4}B \end{bmatrix}$$ if A is 2×4 and B is arbitrary. Then

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ 0 \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = e_{01}, = |0\rangle|1\rangle = |01\rangle,$$

which comes second in the standard basis $\{e_0, e_1, e_2, e_3\} = \{e_{00}, e_{01}, e_{10}, e_{11}\}$ of the 4-dimensional vector space over $\mathbb{C}$.



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 $\pi = |+\rangle = \frac{1}{\sqrt{2}}(1, 1)$, 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 $\mu = |-\rangle = \frac{1}{\sqrt{2}}(1, -1)$. 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:

$$\mathbf{HH^*} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \mathbf{I}.$$

- $\mathbf{He_0} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \pi = |+\rangle = \frac{1}{\sqrt{2}}(\mathbf{e_0} + \mathbf{e_1})$
- $\mathbf{He_1} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mu = |-\rangle = \frac{1}{\sqrt{2}}(\mathbf{e_0} - \mathbf{e_1})$

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**: $\mathbf{Xe_0} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \mathbf{e_1}$; $\mathbf{Xe_1} = \mathbf{e_0}$. $\mathbf{X}|0\rangle = |1\rangle$
- $\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$: $\mathbf{Z}\pi = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \mu$; $\mathbf{Z}\mu = \pi$; $\mathbf{Ze_0} = \mathbf{e_0}$.
- $\mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$: $\mathbf{Ye_0} = i\mathbf{e_1}$; $\mathbf{Ye_1} = -i\mathbf{e_0}$; $\mathbf{Y}\pi = \frac{1}{\sqrt{2}}\begin{pmatrix} -i \\ i \end{pmatrix} = -i\mu$; $\mathbf{Y}\mu = i\pi$.

The rule for a matrix A to be usable in a quantum circuit is that A be **unitary**, meaning that $AA^* =$ the identity matrix. Let's try:

$\mathbf{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$: $\mathbf{X}^* = \mathbf{X}$ because $\mathbf{X}$ is real and symmetric. And $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}$

$\mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$: $\mathbf{Y}^T = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$ but, Y-transpose-conjugate = $\mathbf{Y}^* = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = \mathbf{Y}$ again.

Interlude: Likewise $H = H^*$ and $Z = Z^*$, which defines that these matrices are **Hermitian**. But that does not necessarily imply unitary: only if the square of a Hermitian matrix is the identity.

$$Y^2 = YY^* = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix} = \begin{bmatrix} +1 & 0 \\ 0 & +1 \end{bmatrix} = I.$$

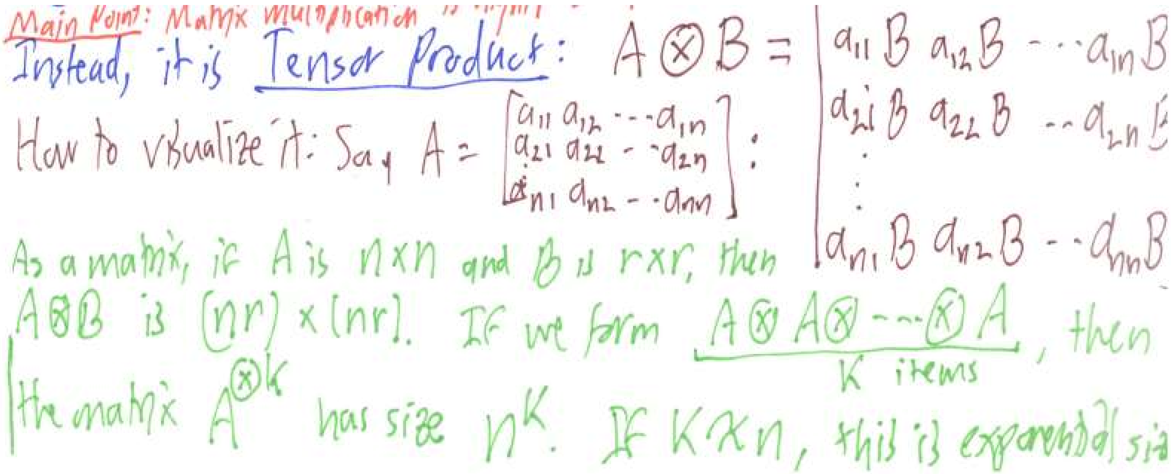
$$H^2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I$$

Note: $X \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$, so $|+\rangle$ is preserved by X, so is the eigenvector with eigenvalue 1.

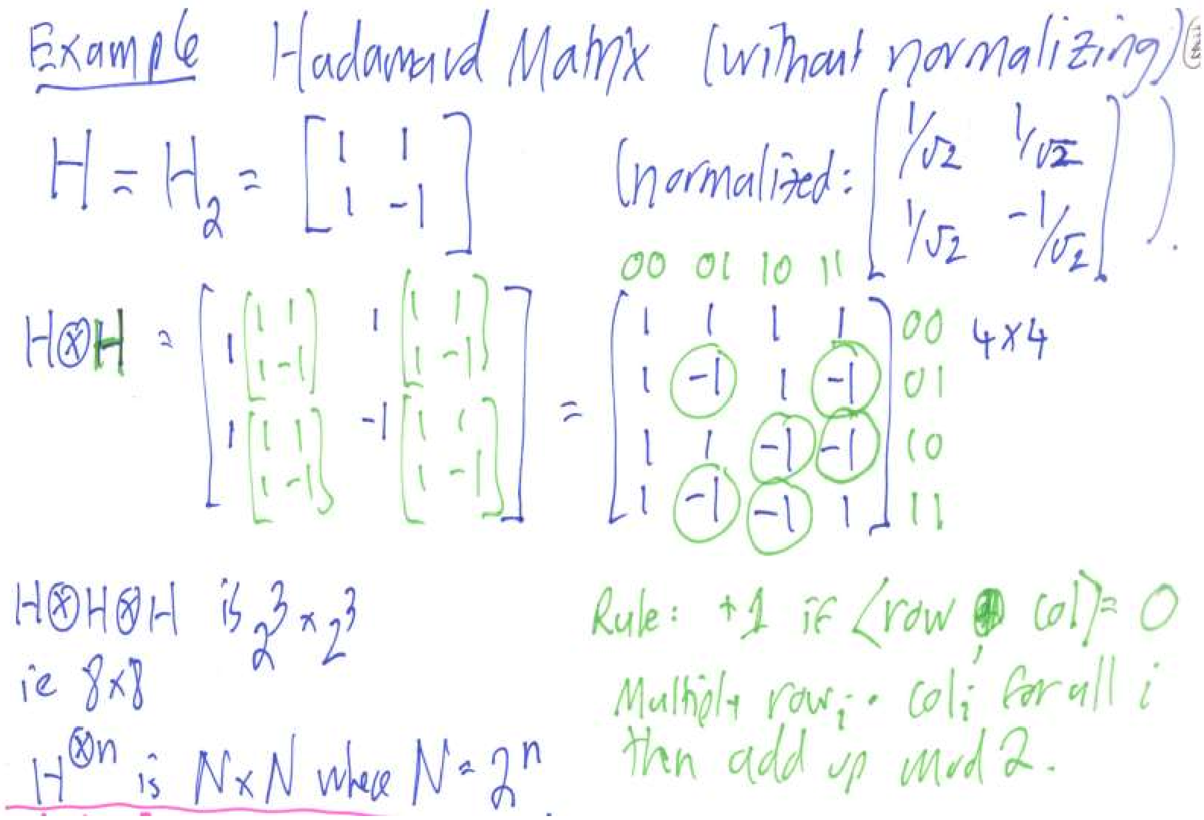
Note: $\mathbf{HZH}^{-1} = \mathbf{HZH} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 & 2 \\ 2 & 0 \end{bmatrix} = \mathbf{X}$

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.)



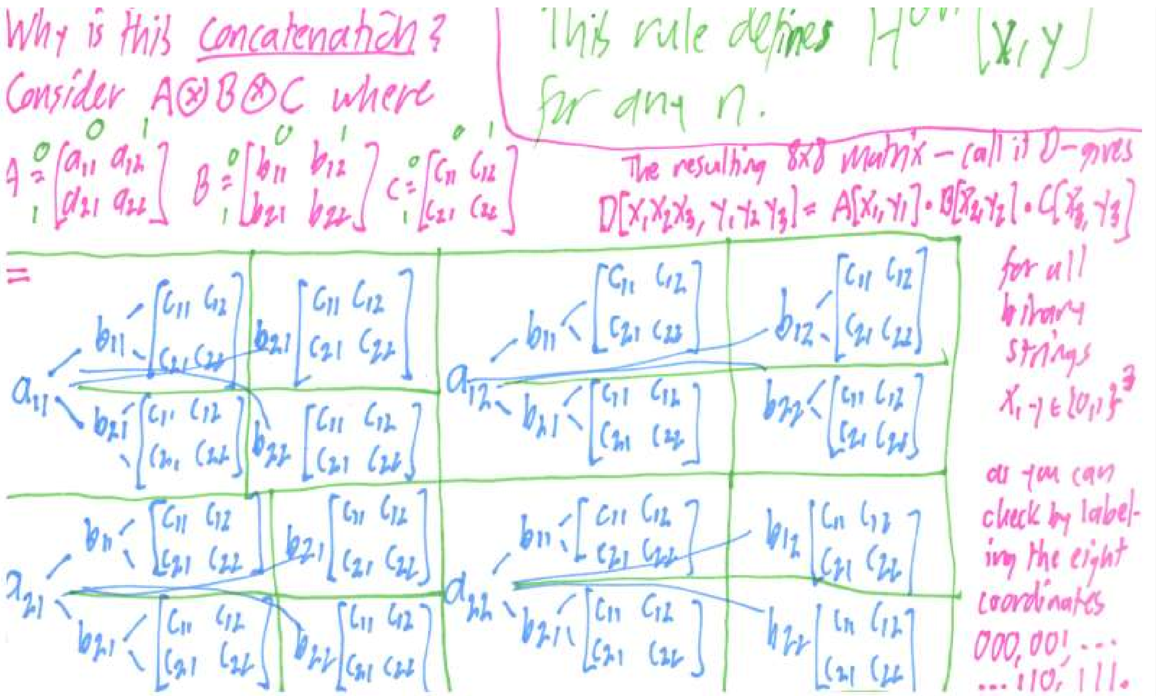
If A is $\ell \times m$ and B is $n \times r$ then $A \otimes B$ is $\ell n \times mr$, so the dimensions can be anything. In particular, A and B can both be column vectors with $m = r = 1$, whereupon $A \otimes B$ is a column vector of length ℓn.



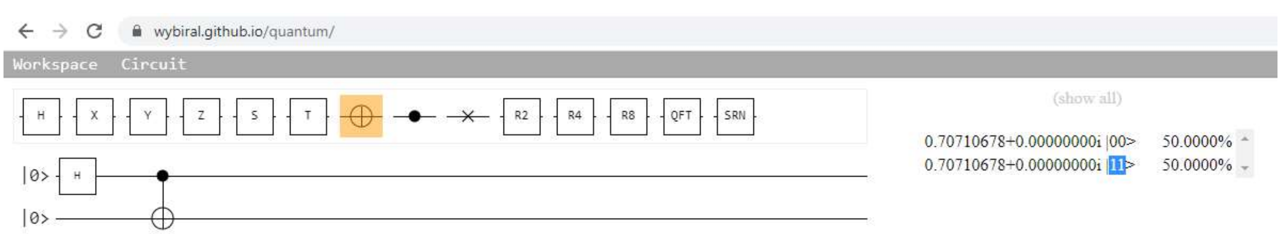
The entries of $H^{\otimes n}$ are indexed by binary strings x, y of length n. Take the Boolean inner product mod 2 of x and y. If it is 0, then $H^{\otimes n}[x, y] = 1$, but if it is 1, then $H^{\otimes n}[x, y] = -1$.

E.g. $\langle 00, y \rangle = 0$ for any y, so the row for 00 is all 1s. But $\langle 01, 01 \rangle = 1$, so the entry $H^{\otimes 2}[01, 01] = -1$. And $\langle 11, 11 \rangle = 2 = 0 \ (mod\ 2)$, so $H^{\otimes 2}[11, 11] = +1$ back again.

This rule defines $H^{\otimes n}$ for any n as an $N \times N$ matrix. On paper that is exponential size, but in a **quantum circuit diagram** on n qubits, it is $O(n)$ gates. Is it linear effort for Nature to compute? Because the computation is unitary, hence **reversible** and ideally accompanied by zero entropy, it might be zero effort. Or, because it represents splitting beams of particles, possibly serially, it might be exponential effort after all.



At the end I showed the [applet for quantum circuits by Davy Wybiral](wybiral.github.io/quantum/):



There is also Craig Gidney's Quirk simulator. This has a graphical feature referenced in the pysics-based chapter 14.

The Bloch Sphere **[This was skimmed---just the diagramwith the H-gate action was shown.]**

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, $i\mathbf{Y} = \mathbf{ZX} = -\mathbf{XZ}$). 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

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

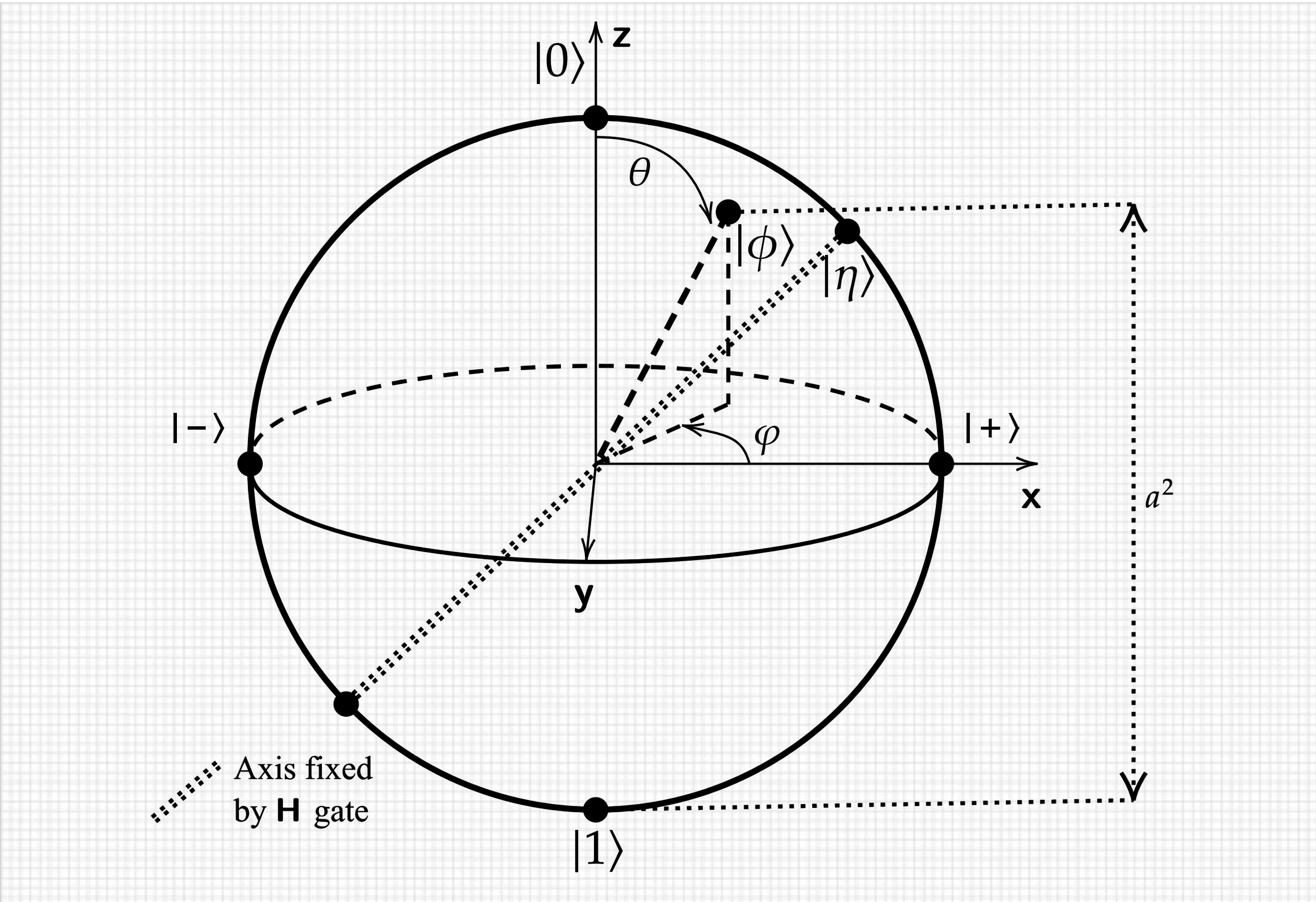
which is the **complex conjugate** of c and is likewise a unit complex number. Since $\phi = \bar{c}\phi'$ the relation is symmetric. That the product of two unit complex numbers is a unit complex number makes it transitive, and being reflexive is immediate with $c = 1$, so this is an equivalence relation.

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 $(ae^{i\alpha}, be^{i\beta})$ where now a, b are real numbers between 0 and 1. Choose $\gamma = -\alpha$, then $c\phi = (a, be^{i\varphi})$ 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.

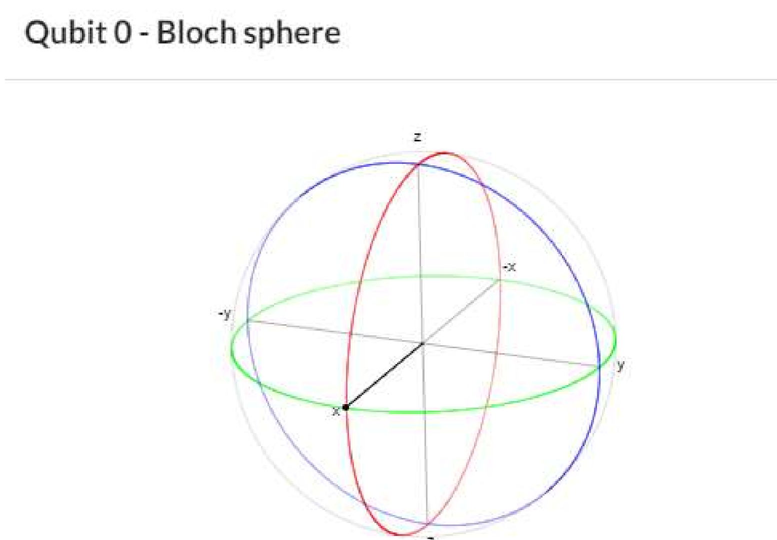
We can uniquely map points (a, φ) to the sphere by treating φ as a longitude and a^2 (rather than a) as a latitude where the north pole is 1, the equator is 0.5, and the south pole is 0. Then the latitude gives the probability of getting the outcome $\mathbf{0}$. All states like π and μ that give equal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

- $\mathbf{e}_0 = \mathbf{0}$ is called $|0\rangle$ and $\mathbf{e}_1 = \mathbf{1}$ is called $|1\rangle$.
- $\frac{1}{\sqrt{2}}(1, 1) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ is called $|+\rangle$, the "plus" state.
- $\frac{1}{\sqrt{2}}(1, -1) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ is called $|-\rangle$, the "minus" state.

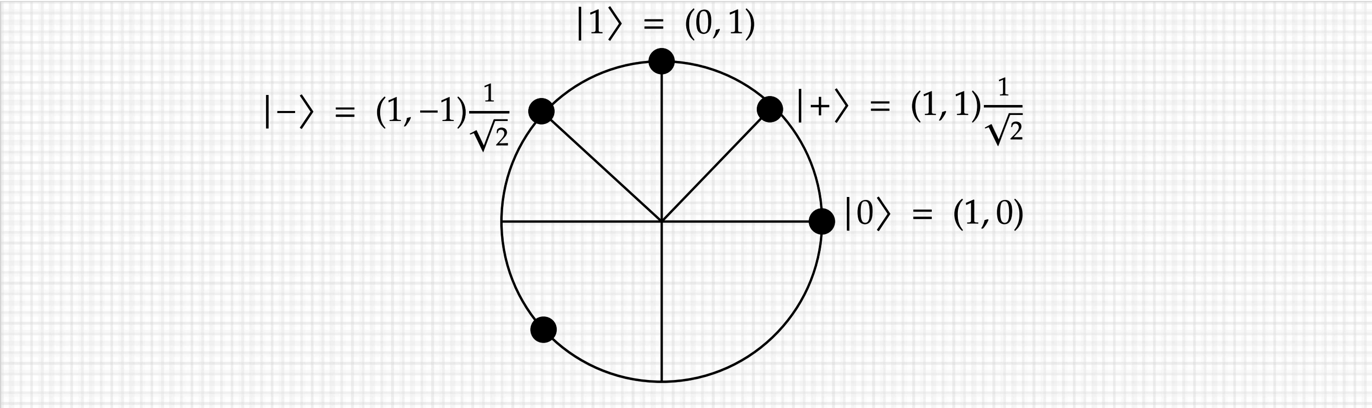
Here they all are, graphed on the **Bloch Sphere**:



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 **x** axis out toward the reader and **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 lecture will return to chapters 3--4 of the text.]