Quantum Programming Foundations: Linear Algebra

Jens Palsberg

Apr 8, 2019

Outline

Hook: The math that we need for quantum computing is linear algebra. Some of the notation for vectors is from quantum mechanics, which differs a bit from what we are used to in math, yet we can learn it. All the linear algebra that we need for quantum computing fits into a single lecture.

Purpose: Persuade you that the linear algebra is mostly stuff that you know already.

Preview:

1. The basic concept is Hilbert spaces.
2. We can explain qubits, superposition, entanglement, and measurement.
3. The possibly unfamiliar stuff is Dirac notation and tensor products.

Transition to Body: First let me introduce the basic mathematical structure that we will use.

Main Point 1: The basic concept is Hilbert spaces.
[A Hilbert space is a set with some operations]
[The key operations that we need for quantum computing are unitary, linear functions]
[The concept of a basis]

Transition to MP2: The concepts of quantum computing have mathematical counterparts.

Main Point 2: We can explain qubits, superposition, entanglement, and measurement.
[Qubits and superposition]
[Measurement]
[Entanglement]

Transition to MP3: Now have covered the basic stuff and can move on to advanced topics.

Main Point 3: The possibly unfamiliar stuff is Dirac notation and tensor products.
[Dirac notation]
[Tensor products]
[Laws]

Transition to Close: So there you have it.

Review: Based on Hilbert spaces, we can explain all the concepts of quantum computing, and when we use tensor products and Dirac notation, the notation is compact.

Strong finish: Now we are ready for quantum computing and we will get into it next lecture.

Call to action: Brush up on basic linear algebra by doing the first math homework.

Detailed presentation

Hook: The math that we need for quantum computing is linear algebra. Some of the notation for vectors is from quantum mechanics, which differs a bit from what we are used to in math, yet we can learn it. All the linear algebra that we need for quantum computing fits into a single lecture.

Purpose: Persuade you that the linear algebra is mostly stuff that you know already.

Preview:

1. The basic concept is Hilbert spaces.
2. We can explain qubits, superposition, entanglement, and measurement.
3. The possibly unfamiliar stuff is Dirac notation and tensor products.

Transition to Body: First let me introduce the basic mathematical structure that we will use.

Main Point 1: The basic concept is Hilbert spaces.

[A Hilbert space is a set with some operations]

If $z = a+bi$, then the complex *conjugate* of z is $z^* = a-bi$. The length $|z|$ of z is a nonnegative real number given by $|z|^2 = zz^* = (a+bi)(a-bi) = a^2+b^2$. Euler's formula says that $e^{i\theta} = \cos\theta + i\sin\theta$, so we can represent any complex number as $re^{i\theta}$.

In quantum computing, the state of the system is a unit vector in a Hilbert space. A unit vector is a vector of length 1. A Hilbert space is a vector space with an inner product that satisfies some conditions. In our case, the Hilbert space consists of vectors of complex numbers and scalars that are also complex numbers. Vector addition and scalar multiplication work as usual, and for two vectors,

$$\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_{k-1} \end{pmatrix} \quad \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{k-1} \end{pmatrix}$$

the inner product is $\Sigma_i \alpha_i^* \beta_i$. Notation: we write the inner product of $|v\rangle$ and $|w\rangle$ as $\langle v|w\rangle$, which is shorthand for $\langle v||w\rangle$, which itself is the matrix product of a row vector and column vector. Two vectors are orthogonal if their inner product is 0. Examples:

$$\begin{aligned}
|v\rangle &= a_0|0\rangle + a_1|1\rangle \\
|w\rangle &= b_0|0\rangle + b_1|1\rangle \\
\langle v|w\rangle &= (a_0^*\ a_1^*)\begin{pmatrix} b_0 \\ b_1 \end{pmatrix} = a_0^* b_0 + a_1^* b_1 \\
|+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
\langle 0|1\rangle &= (1\ 0)\begin{pmatrix} 0 \\ 1 \end{pmatrix} = 1\times 0 + 0 \times 1 = 0 \\
\langle +|-\rangle &= (\frac{1}{\sqrt{2}}\ \frac{1}{\sqrt{2}})\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{2} - \frac{1}{2} = 0
\end{aligned}$$

The outer product of two vectors is defined as follows:

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}(\alpha_2^*\ \beta_2^*) \;=\; \begin{pmatrix}\alpha_1\alpha_2^* & \alpha_1\beta_2^*\\ \beta_1\alpha_2^* & \beta_1\beta_2^*\end{pmatrix}$$

The outer product is the matrix product of a column vector and a row vector; the result is a matrix.

[The key operations that we need for quantum computing are unitary, linear functions]
A linear operation U is unitary iff $UU^\dagger = U^\dagger U = I$. Here $U^\dagger$ is the conjugate transpose of U. We have $U^{-1} = U^\dagger$. Examples:

$$H = \tfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad U = \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix} \qquad S = \begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$$
$$NOT = X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \qquad Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

The matrices X, Y, Z, are called the Pauli gates. Note that $H^\dagger = H$ and $H^2 = I$. Note that $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. Here are detailed calculations:

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = |+\rangle$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = |-\rangle$$

Note that $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

Here is how to decompose H into a sum of outer products:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix}(1\ 0) + \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix}(0\ 1) = (|+\rangle\ \langle 0|) + (|-\rangle\ \langle 1|)$$

Let us check that NOT works like a classical Boolean negation operator.

$$NOT|0\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \begin{pmatrix}0\\ 1\end{pmatrix} = |1\rangle$$
$$NOT|1\rangle = |0\rangle$$
$$NOT(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix} = \beta|0\rangle + \alpha|1\rangle$$

[The concept of a basis]
A generating set for a vector space is a finite set of vectors such that every vector in this space can be written as a linear combination of these vectors, that is, if $\{|e_i\rangle\}$ is a generating set for a vector space, then every element of the vector space can be expressed as $\Sigma_i\ v_i|e_i\rangle$. A set of vectors $\{|e_i\rangle\}$ is linearly independent if $\Sigma_i\ v_i|e_i\rangle = 0$ if and only if $v_i = 0$ for all i. A basis is a generating set of vectors that are all linearly independent. An orthonormal basis is a basis for which the basis vectors are unit vectors and are orthogonal to each other.

Note that $\{|0\rangle, |1\rangle\}$ forms an orthonormal basis. Note that $\{|+\rangle, |-\rangle\}$ forms an orthonormal basis. The Hadamard gate goes back and forth between the $\{|0\rangle, |1\rangle\}$ basis and the $\{|+\rangle, |-\rangle\}$-basis.

Transition to MP2: The concepts of quantum computing have mathematical counterparts.

Main Point 2: We can explain qubits, superposition, entanglement, and measurement.

[Qubits and superposition]

A qubit is a vector $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$, where α, β are complex numbers that satisfy $|\alpha|^2 + |\beta|^2 = 1$. Here, α, β are amplitudes (probabilities as complex numbers). Quantum mechanics people prefer to write $\alpha|0\rangle + \beta|1\rangle$. Here we see a linear combination, also known as a superposition: the qubit is 0 and 1 at the same time, with some amplitudes.

[Measurement]

We cannot measure the amplitudes in a qubit; this is enshrined in the measurement postulate of quantum mechanics. What we can do is to choose an orthonormal basis $\{|v\rangle, |w\rangle\}$ and measure the qubit in that basis. For example, when we measure the qubit $\alpha|0\rangle + \beta|1\rangle$ in the basis $\{|0\rangle, |1\rangle\}$, we use the Born rule and get:

$$\begin{cases} |0\rangle & \text{with probability } |\alpha|^2 \\ |1\rangle & \text{with probability } |\beta|^2 \end{cases}$$

More generally, we can choose the orthonormal basis $\{|v\rangle, |w\rangle\}$, rewrite the qubit in that basis: $\alpha|0\rangle + \beta|1\rangle = \alpha'|v\rangle + \beta'|w\rangle$, and now the outcome of the measurement is v with probability $|\alpha'|^2$, and w with probability $|\beta'|^2$. The outcome of the measurement is also the new state of the qubit. We can wonder why measurement alters the state; researchers have proposed three interpretations.

The first is the Copenhagen interpretation (Niels Bohr), which says that nature operates in a quantum world, but we live in a classical world. The idea that we get information from the quantum world via measurement is an axiom. Intuitively, asking in quantum mechanics "what is a measurement?" is equivalent to asking the axioms of euclidean geometry "what is a point?".

The second is the many-world interpretation (Hugh Everett), which says that every time one measures a quantum object, the universe branches into two equally real universes.

The third is the non-local hidden variables interpretation (David Bohm), which says that both of the previous answers are unacceptable and that quantum mechanics is an incomplete theory. Non-local hidden variables is one among several proposals to fill the gap.

In general, for an orthogonal basis $\{|v\rangle, |w\rangle\}$, measurement of $|\psi\rangle$ gives $|v\rangle$ with probability $|\langle v|\psi\rangle|^2$, and gives $|w\rangle$ with probability $|\langle w|\psi\rangle|^2$.

For example, let us measure $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$ in the basis $\{|+\rangle, |-\rangle\}$. Notice

$$\begin{aligned}
|0\rangle &= \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \\
|1\rangle &= \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \\
|\psi\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle \\
&= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) + \frac{e^{i\theta}}{\sqrt{2}}\frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \\
&= \frac{1}{2}(|+\rangle + |-\rangle) + \frac{e^{i\theta}}{2}(|+\rangle - |-\rangle) \\
&= \frac{1+e^{i\theta}}{2}|+\rangle + \frac{1-e^{i\theta}}{2}|-\rangle
\end{aligned}$$

What is the probability of getting $|+\rangle$? We have $|\frac{1+e^{i\theta}}{2}|^2 = cos^2(\frac{\theta}{2})$.

Suppose we have two qubits:

$$|\psi\rangle \quad = \quad \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \qquad \text{where } \Sigma_{ij}\ |\alpha_{ij}|^2 = 1$$

The probability that we measure $|x\rangle$, where $x \in \{0,1\}^2$ is $|\alpha_x|^2$. Additionally, after the measurement, the state of the two qubits is $|x\rangle$.

Suppose Alice measures the first qubit in the standard basis and observes $|0\rangle$, which she will do with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$. After the measurement, the state of the two qubits is:

$$\frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}} \quad = \quad |0\rangle \otimes \frac{\alpha_{00}|0\rangle + \alpha_{01}|1\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

The probability rule for measuring the second qubit is now given by the rules of conditional probability. Now a measurement of the second qubit in the standard basis will give:

$$\begin{cases} |0\rangle & \text{with probability } \frac{|\alpha_{00}|^2}{|\alpha_{00}|^2+|\alpha_{01}|^2} \\ |1\rangle & \text{with probability } \frac{|\alpha_{01}|^2}{|\alpha_{00}|^2+|\alpha_{01}|^2} \end{cases}$$

Notice that once Alice made her first measurement, the probability of observing each of $|10\rangle$ and $|11\rangle$ becomes zero.

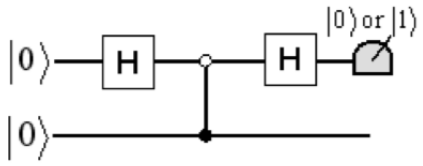
Notice that measuring the first qubit and then measuring the second qubit gives the same result as measuring both qubits at once.

Example of how measuring along way changes the computation. Consider the matrix:

$$U \quad = \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

Now, $UU|0\rangle = |1\rangle$. In contrast, if we do $U|0\rangle$, then measure, then apply U again, then half of the time we get $|0\rangle$ and half of the time we get $|1\rangle$.

Principle of deferred measurement: if we want to measure qubit x, we can introduce a second qubit y and do $CNOT(x, y)$. We say that "y measures x", which we justify as follows.



In the above circuit, the qubits go through the following states:

$$|00\rangle \quad \rightarrow \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}}\ |0\rangle \quad \rightarrow \quad \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad \rightarrow \quad \frac{|00\rangle + |10\rangle + |01\rangle - |11\rangle}{2}$$

Now if we measure the first qubit after the first H, we have an equal chance of getting 0 or 1. Notice that the second qubit holds the result of the measurement; this is because of the entanglement created by the use of $CNOT$. Thus, we can encode any intermediate measurement by use of a $CNOT$ and thereby save all measurement until the end. In summary, a $CNOT$ with another qubit acts the same as measurement.

[Entanglement]
If we have two qubits, their quantum state can be expressed as:

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

where $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. One of the possibilities here is a so-called Bell pair, which is an entangled state:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Notice that if we measure one of the qubits as zero, the other qubit has to measure zero as well. In general, we say that if a state can be expressed as a tensor product, then it is separable, and otherwise it is entangled.

Here is an example. Assume there are three characters, Alice, Bob and Charlie. Charlie has two pairs of gloves. Charlie decides based on a random coin flip whether to pick the left-hand gloves or the right-hand gloves. Then Charlie gives each of Alice and Bob a box with one of the picked gloves. Charlie keeps all this secret from Alice and Bob. Afterwards, Alice goes to Mars, while Bob stays on Earth. When Alice opens her box, she finds out she has a left glove, which means that she knows immediately that Bob has a left glove. Since Alice and Bob don't communicate and thus information does not travel between them, this does not violate relativity theory.

Transition to MP3: Now have covered the basic stuff and can move on to advanced topics.

Main Point 3: The possibly unfamiliar stuff is Dirac notation and tensor products.

[Dirac notation]
We will use Dirac's ket notation, which is a compact way to write a column vector:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Those vectors are pairwise orthogonal unit vectors so they form an orthonormal basis for the vector space; we call it the *standard basis*. Notice that:

$$\langle i|j\rangle \quad = \quad \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}$$

The advantage of the ket notation is that the it labels the basis vectors explicitly.

Dirac's word "ket" is part of the word *bracket*; he also has a "bra" notation for row vectors.

$$\langle 0| = (1\ 0) \quad \text{and} \quad \langle 1| = (0\ 1)$$

Technically, $\langle i|$ is the conjugate transpose of $|i\rangle$, so $\langle\psi| = |\psi\rangle^\dagger$.

Examples:

$$\begin{array}{rclcrcl} |\psi\rangle & = & \begin{pmatrix} \frac{1+i}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix} & & \langle\psi| & = & (\frac{1-i}{2} \quad \frac{1}{\sqrt{2}}) \\ |\phi\rangle & = & \frac{i}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle & & \langle\phi| & = & \frac{-i}{\sqrt{2}}\langle 0| + \frac{1-i}{2}\langle 1| \end{array}$$

In ket notation, the outer product looks like $|\Psi_1\rangle\ \langle\Psi_2|$. The matrix $|\Psi\rangle\ \langle\Psi|$ is called the density matrix of the quantum state Ψ.

[Tensor products]
The tensor product is also known as the Kronecker product; it is defined for two vectors as follows:

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} \;=\; \begin{pmatrix}\alpha_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\\ \beta_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\end{pmatrix} \;=\; \begin{pmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{pmatrix}$$

We can show that

$$|\alpha_1|^2 + |\beta_1|^2 = 1 \text{ and } |\alpha_2|^2 + |\beta_2|^2 = 1 \iff |\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 = 1$$

The above definition generalizes to a tensor product of two matrices.

$$A \otimes B \;=\; \begin{pmatrix}A_{11}B & A_{12}B & \dots & A_{1m}B\\ A_{21}B & A_{22}B & \dots & A_{2m}B\\ \vdots & \vdots & \vdots & \vdots\\ A_{n1}B & A_{n2}B & \dots & A_{nm}B\end{pmatrix}$$

We will write $|\psi\rangle|\phi\rangle$ as an abbreviation for $|\psi\rangle \otimes |\phi\rangle$. Additionally, we will often eliminate internal brackets. Thus, $0\rangle \otimes |1\rangle \otimes |1\rangle$ and $0\rangle|1\rangle|1\rangle$ and $|011\rangle$ all denote the same vector. If $s \in \{0,1\}^n$, then $|s\rangle$ denotes a column vector with 2^n entries. If we think of s as a number in binary notation, then $|s\rangle$ is a column vector that is 0 everywhere except that it is 1 in the position indexed by the number denoted by s.

Examples:

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \;=\; \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$$NOT \otimes H \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\\ 1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\end{pmatrix}$$

$$|00\rangle \;=\; |0\rangle|0\rangle \;=\; |0\rangle \otimes |0\rangle \;=\; \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \;=\; \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

$$|01\rangle \;=\; |0\rangle|1\rangle \;=\; |0\rangle \otimes |1\rangle \;=\; \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \;=\; \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

$$|10\rangle \;=\; |1\rangle|0\rangle \;=\; |1\rangle \otimes |0\rangle \;=\; \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} \;=\; \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

$$|11\rangle \;=\; |1\rangle|1\rangle \;=\; |1\rangle \otimes |1\rangle \;=\; \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} \;=\; \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

$$\frac{1}{\sqrt{2}}|000000\rangle + \frac{1}{\sqrt{2}}|111111\rangle \quad = \quad \ldots \quad = \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \vdots \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} \qquad \text{here we have 62 zeroes!}$$

Example:

$$H \otimes I \quad = \quad \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \qquad \phi \quad = \quad \tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad (H \otimes I)\phi \quad = \quad \tfrac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

Or, in Dirac notation:

$$(H \otimes I)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle) \quad = \quad \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$$

Now let us use properties of the tensor product to do the calculation.

$$\begin{aligned}
\phi \quad &= \quad \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \quad = \quad \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle \quad = \quad \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \\
(H \otimes I)(\phi) \quad &= \quad (H \otimes I)(\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)) \\
&= \quad \frac{1}{\sqrt{2}}((H|0\rangle \otimes I|0\rangle) + (H|1\rangle \otimes I|1\rangle)) \\
&= \quad \frac{1}{\sqrt{2}}(((\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle) \otimes |0\rangle) + ((\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle) \otimes |1\rangle)) \\
&= \quad ((\frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle) \otimes |0\rangle) + ((\frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle) \otimes |1\rangle) \\
&= \quad \frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|11\rangle
\end{aligned}$$

Example:

$$\begin{aligned}
& H \text{ applied to the second qubit of } \frac{1}{2}|00\rangle - \frac{i}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
= \quad & \frac{1}{2}|0+\rangle - \frac{i}{\sqrt{2}}|0-\rangle + \frac{1}{\sqrt{2}}|1-\rangle \\
= \quad & (\frac{1}{2}\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{2}\frac{1}{\sqrt{2}}|01\rangle) - (\frac{i}{\sqrt{2}}\frac{1}{\sqrt{2}}|00\rangle - \frac{i}{\sqrt{2}}\frac{1}{\sqrt{2}}|01\rangle) + (\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}|11\rangle) \\
= \quad & (\frac{1}{2\sqrt{2}}|00\rangle + \frac{1}{2\sqrt{2}}|01\rangle) - (\frac{i}{2}|00\rangle - \frac{i}{2}|01\rangle) + (\frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle) \\
= \quad & (\frac{1}{2\sqrt{2}} - \frac{i}{2})|00\rangle + (\frac{1}{2\sqrt{2}} + \frac{i}{2})|01\rangle) + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle
\end{aligned}$$

In the above example we use notation like $|0+\rangle$ that goes beyond putting only 0 and 1 between $|$ and $\rangle$.

[Laws]
The tensor product of two unitary matrices is unitary. Tensor product is associative, distributes over matrix addition, can be applied to a tensor product, and satisfies a "floating scalars" law:

$$\begin{aligned}(A \otimes B) \otimes C &= A \otimes (B \otimes C) \\ A \otimes (B + C) &= (A \otimes B) + (A \otimes C) \\ (A + B) \otimes C &= (A \otimes C) + (B \otimes C) \\ (A \otimes B)(C \otimes D) &= (AC) \otimes (BD) \\ (\alpha A) \otimes B &= A \otimes (\alpha B) = \alpha(A \otimes B)\end{aligned}$$

In particular, if $|a\rangle = \Sigma_j\ \alpha_j|a_j\rangle$ and $|b\rangle = \Sigma_k\ \beta_k|b_k\rangle$, then

$$|a\rangle \otimes |b\rangle = \Sigma_j\ \Sigma_k\ \alpha_j\beta_k(|a_j\rangle \otimes |b_k\rangle) = \Sigma_j\ \Sigma_k\ \alpha_j\beta_k|a_jb_k\rangle$$

In general, the tensor product fails to be commutative: $|0\rangle \otimes |1\rangle = |01\rangle \neq |10\rangle = |1\rangle \otimes |0\rangle$.

Laws about outer product:

$$\begin{aligned}|\psi\rangle\ \langle\phi|\ |\gamma\rangle &= |\psi\rangle\ \langle\phi|\gamma\rangle = \langle\phi|\gamma\rangle\ |\psi\rangle \\ (\alpha|v\rangle\langle w|M)^\dagger &= M^\dagger(\langle w|)^\dagger(|v\rangle)^\dagger(\alpha)^\dagger = M^\dagger|w\rangle\langle v|\alpha^* = \alpha^*M^\dagger|w\rangle\langle v|\end{aligned}$$

We can express any matrix M as a sum of outer product terms:

$$\begin{aligned}M &= \Sigma_{i,j}\ M_{ij}|i\rangle\langle j| \\ M^\dagger &= \Sigma_{i,j}\ M^*_{ji}|i\rangle\langle j| \\ I &= \Sigma_i\ |i\rangle\langle i| \\ |v\rangle &= \Sigma_k\ v_k|k\rangle \\ M|v\rangle &= \Sigma_{i,j}\ M_{ij}|i\rangle\langle j|\ \Sigma_k\ v_k|k\rangle = \Sigma_{i,j,k}\ M_{ij}v_k|i\rangle\langle j|\ |k\rangle = \Sigma_{i,j,k}\ M_{ij}v_k|i\rangle\langle j|k\rangle \\ &= \Sigma_{i,j}\ M_{ij}v_j|i\rangle\end{aligned}$$

If $\{w_i\}$ and $\{v_i\}$ are two bases, we can express any unitary operation as

$$U = \Sigma_i\ |w_i\rangle\ \langle v_i|$$

An application of U changes the basis from $\{v_i\}$ to $\{w_i\}$:

$$U|v_j\rangle = \Sigma_i\ |w_i\rangle\ \langle v_i|\ |v_j\rangle = |w_j\rangle$$

Transition to Close: So there you have it.

Review: Based on Hilbert spaces, we can explain all the concepts of quantum computing, and when we use tensor products and Dirac notation, the notation is compact.

Strong finish: Now we are ready for quantum computing and we will get into it next lecture.

Call to action: Brush up on basic linear algebra by doing the first math homework.