

CSE439/510 Week 3: Operations on Quantum States and Computations (chs. 3 into 4)

The first part has been seen before. In Fall 2025 I zipped over it but reminded how we showed $\mathbf{H}e_0 = \frac{1}{\sqrt{2}}[1, 1]^T$, which we called $|+\rangle$, and $\mathbf{H}e_1 = \frac{1}{\sqrt{2}}[1, -1]^T$, which we called $|-\rangle$ because of the $-$ sign. The Hadamard matrix thus does a change of basis operation---from the standard basis to the $|+\rangle, |-\rangle$ basis, which is also an **orthonormal** basis. Also, I did parts on the blackboard that are reviewed in the section of "reversals and..." below.

Fall 26: I will preface this with a discussion related to Assignment 1 about the **types** involved: **scalar**, **vector**, **matrix**, and higher-dimensional **tensors**. NB: The word "dimension" is used in two senses. E.g., a 3×4 matrix is a 2D grid, but its column dimension is 4, so it multiplies 4-dimensional vectors, which by themselves are "1D". Tensors are "3D" and higher; the "D" is more formally called their **rank**, but that usage is equally confusing.

Unit Vectors

Back on ground level, note that for a complex scalar c , c^*c and cc^* both equal its squared magnitude $|c|^2$. To wit, if we write $c = a + bi$ with a and b real, then $c^* = a - bi$, and we get

$$cc^* = (a + bi)(a - bi) = a^2 - abi + abi + b^2 = a^2 + b^2 = |c|^2.$$

And for a vector $\mathbf{a}$,

$$\langle \mathbf{a} | \mathbf{a} \rangle = \sum_{i=1}^n a_i^* a_i = \sum_{i=1}^n |a_i|^2$$

is its **squared magnitude**. The **norm** of the vector is the positive square root of this:

$$|\mathbf{a}| = \sqrt{\langle \mathbf{a} | \mathbf{a} \rangle}.$$

Definition: A **unit vector** has norm 1, equivalently, has squared magnitude 1. Any unit vector $\mathbf{v}$ in a Hilbert space gives rise to a "**legal quantum state**", which we can write as $|\mathbf{v}\rangle$ for pretentious emphasis (or decide not to do so).

In the two-dimensional real space $\mathbb{R}^2$, the unit vectors (x, y) correspond to the points on the unit circle in the plane, as defined by $x^2 + y^2 = 1$. The simplest quantum states are unit vectors of two **complex** numbers, i.e., members of $\mathbb{C}^2$. But in many cases we can ignore the distinction between complex and real entries and pretend-visualize them as points on the unit circle in the plane anyway. (There is a non-fudged, non-lossy visualization in 3D called the **Bloch Sphere**---we will come to it later.)

Now for operations, we begin by extending some notation we just used for vectors:

Definition. The **conjugate transpose** of an $m \times n$ matrix A is obtained by first transposing A to make the $n \times m$ matrix A^T , and then taking the complex conjugate of every element. We write A^* for the resulting $n \times m$ matrix. (Many other sources write $A^\dagger$ instead.)

Examples:

- If $A = \begin{bmatrix} 1+i & 1-i \\ 2 & 0 \end{bmatrix}$, then $A^T = \begin{bmatrix} 1+i & 2 \\ 1-i & 0 \end{bmatrix}$ and $A^* = \begin{bmatrix} 1-i & 2 \\ 1+i & 0 \end{bmatrix}$.
- If $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, then $Y^T = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}$, and weirdly, $Y^* = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = Y$ back again.
- For our old friend the Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $H^T = H^* = H$ because H is symmetric and has all-real entries.

Note that

$$He_0 = H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{e_0 + e_1}{\sqrt{2}},$$

a vector we saw in the previous lecture, and ditto for

$$He_1 = H|1\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{e_0 - e_1}{\sqrt{2}}.$$

The two resulting vectors are also unit vectors, and they are linearly independent. Indeed, they are **orthogonal**, because

$$\langle [1, 1], [1, -1] \rangle = 1 \cdot 1 + 1 \cdot (-1) = 0.$$

Thus, like e_0 and e_1 , they form an **orthonormal basis** for $\mathbb{C}^2$ (not to mention also for $\mathbb{R}^2$). Focusing on the plus and minus sign between e_0 and e_1 , the "Dirac names" for these states are $|+\rangle$ and $|-\rangle$, respectively.

Unitary Operations

Getting just a little bit ahead for visualizing qubits, here is a diagram:

This also works vice-versa: if $AA^* = \mathbf{I}$, then $A^*A = \mathbf{I}$. So an equivalent definition of unitary is that $AA^* = \mathbf{I}$.

$$A^*A = (A^{-1}A)A^*A = A^{-1}(AA^*)A = A^{-1}(\mathbf{I})A = \mathbf{I}$$

Definition: A matrix A is **Hermitian** if $A^* = A$.

The Pauli matrices are all both Hermitian and unitary. So is the Hadamard matrix.

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

If we took away the factor $\frac{1}{\sqrt{2}}$, the resulting matrix $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is Hermitian but not unitary. The matrix

$$\mathbf{S} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \text{ is unitary but not Hermitian.}$$

In Part I of the text we toe the line of identifying unitary matrices with "legal quantum operations." When we dabble into Chapter 14, we will encounter the view that Hermitian operators are the "physically actual" ones. Most in particular:

Proposition: For any unit vector $\mathbf{c}$, the outer product $C = |\mathbf{c}\rangle\langle\mathbf{c}|$ is a Hermitian matrix.

Proof: It is a general fact that if $C = AB$, then $C^* = (AB)^* = B^*A^*$. So

$$C^* = (|\mathbf{c}\rangle\langle\mathbf{c}|)^* = (\langle\mathbf{c}|)^* \cdot (|\mathbf{c}\rangle)^* = |\mathbf{c}\rangle \cdot \langle\mathbf{c}| = C$$

back again. ☒

Now we can use the reversal rule for adjoints to give a shorter and snappier proof of Lemma 3.1 than what the text gives:

Lemma 3.1: If $\mathbf{U}$ is a unitary matrix and $\mathbf{a}$ is a vector then $\|\mathbf{Ua}\| = \|\mathbf{a}\|$.

$$\textbf{Proof: } \|\mathbf{Ua}\| = \sqrt{\|\mathbf{Ua}\|^2} = \sqrt{(\mathbf{Ua})^*(\mathbf{Ua})} = \sqrt{(\mathbf{a}^*\mathbf{U}^*)(\mathbf{Ua})} = \sqrt{\mathbf{a}^*(\mathbf{U}^*\mathbf{U})\mathbf{a}} = \sqrt{\mathbf{a}^*\mathbf{a}} = \|\mathbf{a}\|. \text{ ☒}$$

The proof became a one-liner. Thus a unitary matrix always preserves the lengths of vectors, and in particular, it always maps a unit vector to a unit vector. This is what makes it "legal" from the quantum probability point of view.

Conversely (later): if a matrix $\mathbf{U}$ always preserves the lengths of vectors, then it must be unitary.

Reversal, Adjoint, and Duality.

The reversal x^R of a string x just means writing it "backwards": $01001^R = 10010$, $FACED^R = DECAF$, and so on. A string x is a palindrome if $x^R = x$, for instance 1001. The empty string ϵ counts as a palindrome since $\epsilon^R = \epsilon$. The rule for reversal and concatenation is that for any strings x and y ,

$$(xy)^R = y^R x^R.$$

For example,

$$(\text{PUCK-FACED})^R = (\text{FACED})^R (\text{PUCK-})^R = \text{DECAF-KCUP}.$$

Actually, if the minus sign is a -1 factor which could go anywhere, this would be equivalent to say "DECAF K-CUP" meaning a certain pod for a Keurig coffee-maker.

This gives intuition for how matrix transpose, matrix adjoint, and matrix inverse all work like reversal with regard to matrix product. The rules for any (invertible) matrices A and B are:

1. $(AB)^T = B^T A^T$
2. $(AB)^* = B^* A^*$
3. $(AB)^{-1} = B^{-1} A^{-1}$.

Rule 2 follows from rule 1 because the only difference with $*$ is doing complex conjugates of individual entries. Rule 3 follows since $(AB)(B^{-1}A^{-1}) = ABB^{-1}A^{-1} = AA^{-1} = \mathbf{I}$. So why does rule 1 hold? Here our functional view might help: The transpose A^T is the function with the two index arguments reversed: $A^T(j, i) = A(i, j)$. So:

$$(AB)^T(i, j) = (AB)(j, i) = \sum_k A(j, k)B(k, i) = \sum_k B(k, i)A(j, k) = \sum_k B^T(i, k)A^T(k, j) = B^T A^T(i, j)$$

for all arguments (i.e., indices) i and j , so $(AB)^T = B^T A^T$. (Note that the switch $A(j, k)B(k, i) = B(k, i)A(j, k)$ in the middle step was just ordinary multiplication of numbers.)

Also note that transpose, reversal, inverse, and adjoint all have the "self-dual" property that applying them twice gives the original back again: $(x^R)^R = x$, $(A^T)^T = A$, $(A^{-1})^{-1} = A$, and $(A^*)^* = A$.

Now we can review some other basic useful rules, with-and-without Dirac notation:

1. Dot product **is** commutative: $x \cdot y = y \cdot x$. This is implicit in the step in red above.
2. Complex inner product is "not quite" commutative:
 $\langle y|x \rangle = \langle y| \cdot |x \rangle = |y\rangle^* \cdot \langle x| = (\langle x| \cdot |y \rangle)^* = \langle x|y \rangle^*$ by the reversal rule. So the flipped-around inner product $\langle y|x \rangle$ is just the complex conjugate of the scalar $\langle x|y \rangle$. But often the difference caused by the conjugate is minimal.
3. Outer product is not commutative. But: $(|y\rangle\langle x|)^* = \langle x|^*|y\rangle^*$ by the reversal rule, and by the definitions of "ket" and "bra" that becomes $|x\rangle\langle y|$. So flipping the outer product around creates the adjoint of the matrix. This is another reason why taking the outer product of a vector with itself always creates a self-adjoint (i.e., **Hermitian**) matrix.
4. Tensor product is not commutative: generally $A \otimes B \neq B \otimes A$. But here's a real curveball: $(A \otimes B)^*$ is **NOT** the same as $(B^* \otimes A^*)$. Instead, it equals $(A^* \otimes B^*)$. The intuitive reason, which we'll picture soon when we visualize quantum circuits, is that elements of tensor products "stay in their lane" when it comes to the indexing scheme.

Tensor Product and Qubit "Lines in Lanes" (Thu. 9/10 lecture began here)

Two basic facts:

- The tensor product of two unit vectors is always a unit vector.
- The tensor product of two unitary matrices is always a unitary matrix.

For the second one, suppose $A \cdot B$ and $C \cdot D$ are compatible matrix products. We can give A indices i, j , give B indices j, k , give C indices ℓ, m , and give D indices m, n . Then $A \otimes C$ has indices $i\ell, jm$ and $B \otimes D$ has indices jm, kn . Therefore $E = (A \otimes C) \cdot (B \otimes D)$ is a compatible matrix product, and it comes out with indices $i\ell, kn$. The value of any particular entry is

$$E[i\ell, kn] = \sum_{jm} (A \otimes C)[i\ell, jm] (B \otimes D)[jm, kn].$$

By definition of tensor product, $(A \otimes C)[i\ell, jm] = A[i, j]C[\ell, m]$ and similarly for $B \otimes D$. So we get

$$E[i\ell, kn] = \sum_{jm} A[i, j]C[\ell, m]B[j, k]D[m, n] = \sum_{jm} A[i, j]B[j, k]C[\ell, m]D[m, n].$$

This in turn equals $\left(\sum_j A[i, j]B[j, k]\right)\left(\sum_m C[\ell, m]D[m, n]\right) = (AB)[i, k](CD)[\ell, n]$. Again by definition of tensor product, this is the same as $(AB \otimes CD)[i\ell, kn]$. So $E = (AB) \otimes (CD)$. (Note the distinction between the use of the comma for array rows-versus-columns versus not using a comma when tensored coordinates are "rammed together.")

In Fall 2026, the above example was elaborated more fully on the whiteboard, using general indices a running $1 \dots i$, b running $1 \dots j$, c running $1 \dots k$, d running $1 \dots \ell$, e running $1 \dots m$, and f running $1 \dots n$. See the four "Week 3 Thu." whiteboard photos on the course webpage. This was painful but important to get the feel of jockeying tensor product indices at least once.

The second fact then follows because if A and C are unitary, then

$$(A \otimes C)^*(A \otimes C) = (A^* \otimes C^*)(A \otimes C) = (A^*A \otimes C^*C) = (I \otimes I) = I.$$

We will often use this silently when C itself is just the identity---a "non-gate" on one or more qubit "wires" running underneath the action of A on "upper" wires---and vice-versa when A is the identity. Despite all the fuss in our notation, for Nature this just means running things side-by-side. Here is a statement that uses a lot of notational fuss to express the simplest of ideas:

Proposition: For any $m \times n$ matrix A , $p \times q$ matrix B , n -vector $\mathbf{x}$ and q -vector $\mathbf{y}$,

$$(A\mathbf{x}) \otimes (B\mathbf{y}) = (A \otimes B) \cdot (\mathbf{x} \otimes \mathbf{y}).$$

Proof. The dimensions are consistent: both sides give a column vector of mp entries. Showing equality is where our effort to interpret vectors $\mathbf{x}$ as functions $\mathbf{x}(u)$ of their indices in binary notation may help. Under this view, $\mathbf{z} = \mathbf{x} \otimes \mathbf{y}$ gives the function $\mathbf{z}(uv) = \mathbf{x}(u)\mathbf{y}(v)$, where uv means concatenation of binary strings, while the right-hand side is an ordinary numeric product. And a matrix A gives the two-argument function $A(u, w) = a_{u,w}$.

$$[0.5, 0.5, -0.5, 0.5] \otimes [0.6, 0.8] = [0.3, 0.4, 0.3, 0.4, -0.3, -0.4, 0.3, 0.4]$$

Indices: $[000, 001, 010, 011, 100, 101, 110, 111]$ $100 = 10 \cdot 0: -0.3 = (-0.5)(0.6).$

Style note: When vector and matrix indices are regarded as binary strings rather than numbers, we will write things like $\mathbf{A}[u, w]$ and $\mathbf{C}[uv, wt]$ below, where $\mathbf{C} = \mathbf{A} \otimes \mathbf{B}$.

The vector $\mathbf{x}' = A\mathbf{x}$ becomes the function mapping a row-index u to $\mathbf{x}'(u) = \sum_w A(u, w)\mathbf{x}(w)$. Thus, putting $\mathbf{z}' = (A\mathbf{x}) \otimes (B\mathbf{y})$, the right-hand side is the function

$$\mathbf{z}'(uv) = \mathbf{x}'(u)\mathbf{y}'(v) = \left(\sum_w A(u, w)\mathbf{x}(w) \right) \cdot \left(\sum_t B(v, t)\mathbf{y}(t) \right)$$

Now by usual rules of re-ordering summations, the right-hand side of this can be rearranged as

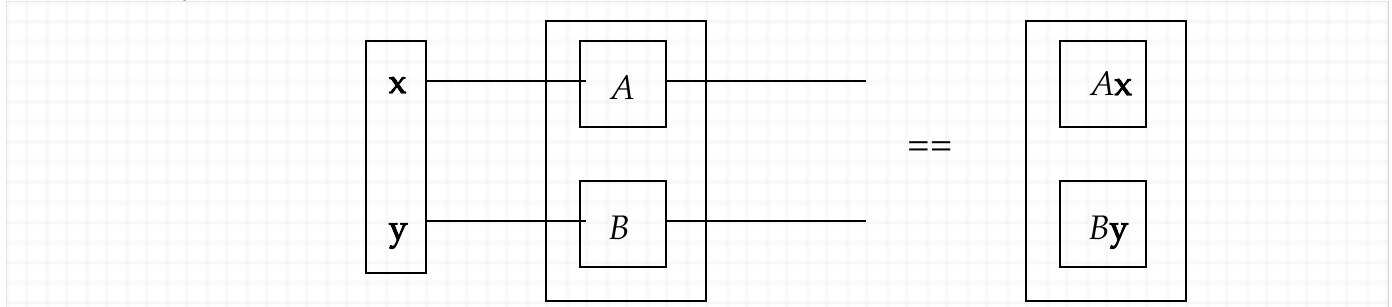
$$\sum_w \sum_t A(u, w)B(v, t)\mathbf{x}(w)\mathbf{y}(t)$$

With $\mathbf{z} = \mathbf{x} \otimes \mathbf{y}$, we can already recognize that the $\mathbf{x}(w)\mathbf{y}(t)$ part is the same as $\mathbf{z}(wt)$. And $A(u, w)B(v, t)$ is the same as $(A \otimes B)(uv, wt)$. So the whole thing becomes

$$\sum_{w,t} (A \otimes B)(uv, wt) \cdot (\mathbf{x} \otimes \mathbf{y})(wt),$$

which is exactly the meaning of $(A \otimes B) \cdot (\mathbf{x} \otimes \mathbf{y})$. So the two sides are equal. ☒

The simple idea is that $(A \otimes B) \cdot (\mathbf{x} \otimes \mathbf{y})$ does the A operation on x side-by-side with B doing its operation on y , but with no connection at all between them. We will soon have diagrams like this---



---note that we picture the inputs coming in from the left but when writing them as matrix arguments they will swing around to the right. As a tandem, this is formally the tensor product $\mathbf{x} \otimes \mathbf{y}$ coming in to $(A \otimes B)$. But really---and **locally**---it is just $A\mathbf{x}$ happening in one place and $B\mathbf{y}$ happening independently in another place. The upshot is this:

When we have entanglement, not independence, between the x part and the y part, then the notation will stay the same but the interpretation will change a whole lot.

Linearity

All of these products are, however, *linear on both sides*. That is, they obey the distributive law for addition on either side, and (hence) constant multiples also can "come out" or "go inside". Here are the cases for linearity on the right-hand side, assuming the vectors and matrices being added have compatible dimensions and a is a (possibly complex) scalar:

- $u \cdot (av + w) = a(u \cdot v) + u \cdot w$.
- $\langle u | av + w \rangle = a\langle u | v \rangle + \langle u | w \rangle$.
- But note on the left: $\langle au + v | w \rangle = a^* \langle u | w \rangle + \langle v | w \rangle$, because a is implicitly conjugated "inside the bra".
- And furthermore, this time on the right: $|u\rangle \langle av + w| = a^* |u\rangle \langle v| + |u\rangle \langle w|$. Same reason coming from inside the "bra". This is a common cause of typos.
- $A \cdot (aB + C) = aA \cdot B + A \cdot C$.
- $A \otimes (aB + C) = a(A \otimes B) + (A \otimes C)$.

- $(aC)^* = C^*a^* = a^*C^*$ because scalars commute with matrices. Ditto with vectors. Using bar instead of star: if $\mathbf{z} = a\mathbf{x}$ where $\mathbf{x}$ and $\mathbf{z}$ are numeric vectors and a is a (possibly complex) scalar, then we have the rule $\mathbf{z}^* = \bar{a}\mathbf{x}^*$. We have to remember to conjugate any factor we pull out of the adjoint.

Super-weeny point: A Khan Faculty video writes the rules $|a\psi\rangle = a|\psi\rangle$ and $\langle a\psi| = a^*\langle\psi|$, but you have to be careful that ψ stands for a numeric vector here. It makes no sense to say e.g. that $3|1\rangle = |3\rangle$ when the $|1\rangle$ is the binary-bit attribute, nor that $3|7\rangle = |21\rangle$ if the "7" is the rank of a playing card. This is one reason I used card-suit symbols and "honor/spot-card", to get away from the temptation of treating the insides of $|0\rangle$ and $|1\rangle$ as if they were numbers rather than attributes.

Two consecutive kets as in $|x\rangle|y\rangle$ is a gray area. Equating it to $|x\rangle \otimes |y\rangle$ is AOK when manipulating standard basis vectors, e.g. $|1\rangle|0\rangle|0\rangle|1\rangle|0\rangle = |10010\rangle$. Likewise,

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}[1, 1] \otimes \frac{1}{\sqrt{2}}[1, 1] = \frac{1}{2}[1, 1, 1, 1]^T = |++\rangle$$

is kosher as nomenclature, likewise writing $|+\rangle|-\rangle$ as $|+-\rangle$ and so on. But the product of two column vectors is not really defined, and in general cases of $|x\rangle|y\rangle$ where "x" and "y" are *not* what I have been calling "attributes", combo-ing it as " $|xy\rangle$ " may not make sense. What might bail you out of doubt is if you have a bra $\langle w|$ before $|x\rangle|y\rangle$. Then it becomes $\langle w|x\rangle \cdot |y\rangle$, where the $\cdot$ is now the same as ordinary multiplication. But $\langle w| \cdot |xy\rangle$ may not make sense off the top---because inner product wants the dimensions to agree. (??)

[The Fall 2026 week 3 Thursday lecture ended here.]