1 Unitary Operators and Quantum Gates

1.1 Unitary Operators

A postulate of quantum physics is that quantum evolution is unitary. That is, if we have some arbitrary quantum system U that takes as input a state $|\phi\rangle$ and outputs a different state $U|\phi\rangle$, then we can describe U as a *unitary linear transformation*, defined as follows.

If U is any linear transformation, the *adjoint* of U, denoted $U^\dagger$, is defined by $(U\vec{v},\vec{w}) = (\vec{v},U^\dagger\vec{w})$. In a basis, $U^\dagger$ is the conjugate transpose of U; for example, for an operator on $\mathscr{C}^2$,

$$U = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \Rightarrow U^\dagger = \left(\begin{smallmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{smallmatrix}\right) \quad .$$

We say that U is *unitary* if $U^\dagger = U^{-1}$. For example, rotations and reflections are unitary. Also, the composition of two unitary transformations is also unitary (Proof: U,V unitary, then $(UV)^\dagger = V^\dagger U^\dagger = V^{-1}U^{-1} = (UV)^{-1}$).

Some properies of a unitary transformation U:

- The rows of U form an orthonormal basis.
- The colums of U form an orthonormal basis.
- U preserves inner products, i.e. $(\vec{v},\vec{w}) = (U\vec{v},U\vec{w})$. Indeed, $(U\vec{v},U\vec{w}) = (U\big|v\big\rangle)^\dagger U\big|w\big\rangle = \big\langle v\big|U^\dagger U\big|w\big\rangle = \big\langle v\big|w\big\rangle$. Therefore, U preserves norms and angles (up to sign).
- The eigenvalues of U are all of the form $e^{i\theta}$ (since U is length-preserving, i.e., $(\vec{v},\vec{v}) = (U\vec{v},U\vec{v})$).
- U can be diagonalized into the form

$$\begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & e^{i\theta_d} \end{pmatrix}$$

1.2 Quantum Gates

We give some examples of simple unitary transforms, or "quantum gates."

Some quantum gates with one qubit:

- Hadamard Gate. Can be viewed as a reflection around $\pi/8$, or a rotation around $\pi/4$ followed by a reflection.

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

The Hadamard Gate is one of the most important gates. Note that $H^\dagger = H$ – since H is real and symmetric – and $H^2 = I$.

- Rotation Gate. This rotates the plane by θ.

$$U = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

- NOT Gate. This flips a bit from 0 to 1 and vice versa.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Phase Flip.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The phase flip is a NOT gate acting in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis. Indeed, $Z|+\rangle = |-\rangle$ and $Z|-\rangle = |+\rangle$.

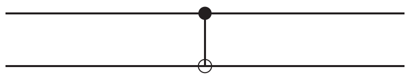
And a two-qubit quantum gate:

- Controlled Not (CNOT).

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The first bit of a CNOT gate is the "control bit;" the second is the "target bit." The control bit never changes, while the target bit flips if and only if the control bit is 1.

The CNOT gate is usually drawn as follows, with the control bit on top and the target bit on the bottom:



1.3 Tensor product of operators

Suppose $|v\rangle$ and $|w\rangle$ are unentangled states on $\mathscr{C}^m$ and $\mathscr{C}^n$, respectively. The state of the combined system is $|v\rangle \otimes |w\rangle$ on $\mathscr{C}^{mn}$. If the unitary operator A is applied to the first subsystem, and B to the second subsystem, the combined state becomes $A|v\rangle \otimes B|w\rangle$.

In general, the two subsystems will be entangled with each other, so the combined state is not a tensor-product state. We can still apply A to the first subsystem and B to the second subsystem. This gives the operator $A \otimes B$ on the combined system, defined on entangled states by linearly extending its action on unentangled states.

(For example, $(A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle$. $(A \otimes B)(|1\rangle \otimes |1\rangle) = A|1\rangle \otimes B|1\rangle$. Therefore, we define $(A \otimes B)(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle)$ to be $\frac{1}{\sqrt{2}}(A \otimes B)|00\rangle + \frac{1}{\sqrt{2}}(A \otimes B)|11\rangle = \frac{1}{\sqrt{2}}\left(A|0\rangle \otimes B|0\rangle + A|1\rangle \otimes B|1\rangle\right)$.)

Let $|e_1\rangle, \ldots, |e_m\rangle$ be a basis for the first subsystem, and write $A = \sum_{i,j=1}^{m} a_{ij} |e_i\rangle\langle e_j|$ (the i,jth element of A is a_{ij}). Let $|f_1\rangle, \ldots, |f_n\rangle$ be a basis for the second subsystem, and write $B = \sum_{k,l=1}^{n} b_{kl} |f_k\rangle\langle f_l|$. Then a basis for the combined system is $|e_i\rangle \otimes |f_j\rangle$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. The operator $A \otimes B$ is

$$\begin{aligned} A \otimes B &= \left(\sum_{ij} a_{ij} |e_i\rangle\langle e_j|\right) \otimes \left(\sum_{kl} b_{kl} |f_k\rangle\langle f_l|\right) \\ &= \sum_{ijkl} a_{ij} b_{kl} |e_i\rangle\langle e_j| \otimes |f_k\rangle\langle f_l| \\ &= \sum_{ijkl} a_{ij} b_{kl} (|e_i\rangle \otimes |f_k\rangle)(\langle e_j| \otimes \langle f_l|) \ . \end{aligned}$$

Therefore the $(i,k),(j,l)$th element of $A \otimes B$ is $a_{ij}b_{kl}$. If we order the basis $|e_i\rangle \otimes |f_j\rangle$ lexicographically, then the matrix for $A \otimes B$ is

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots \\ a_{21}B & a_{22}B & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} ;$$

in the i,jth subblock, we multiply a_{ij} by the matrix for B.

2 No cloning theorem

A quantum operation which copied states would be very useful. For example, we considered the following problem in Homework 1: Given an unknown quantum state, either $|\phi\rangle$ or $|\psi\rangle$, use a measurement to guess which one. If $|\phi\rangle$ and $|\psi\rangle$ are not orthogonal, then no measurement perfectly distinguishes them, and we always have some constant probability of error. However, if we could make many copies of the unknown state, then we could repeat the optimal measurement many times, and make the probability of error arbitrarily small. The no cloning theorem says that this isn't physically possible. Only sets of mutually orthogonal states can be copied by a single unitary operator.

No Cloning Theorem. *Assume we have a unitary operator U and two quantum states $|\phi\rangle$ and $|\psi\rangle$ which U copies, i.e.,*

$$\begin{aligned} |\phi\rangle \otimes |0\rangle &\xrightarrow{U} |\phi\rangle \otimes |\phi\rangle \\ |\psi\rangle \otimes |0\rangle &\xrightarrow{U} |\psi\rangle \otimes |\psi\rangle \ . \end{aligned}$$

Then $\langle\phi|\psi\rangle$ is 0 or 1.

Proof: $\langle\phi|\psi\rangle = (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) = (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle^2$. In the second equality we used the fact that U, being unitary, preserves inner products. $\square$

3 Superdense Coding

Suppose Alice and Bob have a *quantum* communications channel, over which Alice can send qubits to Bob. However, Alice just wants to send a regular classical letter (sequence of bits). One way to send her message is to encode a 0 as $|0\rangle$ and a 1 as $|1\rangle$. But can she do better than sending as many qubits as bits in her message?

Intuitively, since quantum systems are more complex than classical systems, they can hold information – so maybe Alice can do better. But quantum information is hard to access; when you measure a quantum state, it looks classical – so maybe she can't.

In fact, if Alice and Bob share a Bell state, then she can send two classical bits of information using only one qubit.

Say Alice and Bob share $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Depending on the message Alice wants to send, she applies a gate to her qubit, then sends it to Bob. If Alice wants to send 00, then she does nothing to her qubit, just sends it to Bob. If Alice wants to send 01, she applies the phase flip Z to her qubit, changing the quantum state to $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$. To send 10, she applies the NOT gate, giving $\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\Psi^+\rangle$. To send 11, she applies both NOT and Z, giving $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$.

After receiving the qubit from Alice, Bob has one of the four mutually orthogonal Bell states. He can therefore apply a measurement to distinguish between them with certainty, and determine Alice's message. In practice, the way he'll make this measurement is by running the circuit we saw in Lecture 2 backwards (i.e., applying $(H \otimes I) \circ CNOT$), then measuring in the standard basis.

Note that Alice really did use two qubits total to send the two classical bits. After all, Alice and Bob somehow had to start with a shared Bell state. However, the first qubit – Bob's half of the Bell state – could have been sent well before Alice had decided what message she wanted to send. Perhaps only much later did she decide on her message and send over the second qubit.

One can show that it is not possible to do any better. Two qubits are necessary to send two classical bits. Superdense coding allows half the qubits to be sent before the message has been chosen.