Today's outline - January 17, 2023

- Tensor products of vector spaces
- Multiple qubit systems
- Measurement of n-qubit systems
- Quantum key distribution revisited

Reading Assignment: Reiffel: 4.1-4.2 Wong: 4.2.4

Homework Assignment #01:
due Thursday, January 19, 2023

Homework Assignment #02:
due Thursday, January 26, 2023

Direct sum of vector spaces

Consider two classical state spaces, V and W with bases

$$A = \{|\alpha_1\rangle, |\alpha_1\rangle, \dots, |\alpha_n\rangle\}, \qquad B = \{|\beta_1\rangle, |\beta_1\rangle, \dots, |\beta_m\rangle\}$$

The combined state space of these two state spaces is obtained through a direct sum, $V \oplus W$ with basis

$$A \cup B = \{|\alpha_1\rangle, |\alpha_1\rangle, \dots, |\alpha_n\rangle, |\beta_1\rangle, |\beta_1\rangle, \dots, |\beta_m\rangle\}$$

Every element $|x\rangle \in V \oplus W$ can be written as $|x\rangle = |v\rangle \oplus |w\rangle$, where $|v\rangle \in V$ and $|w\rangle \in W$

Addition and scalar multiplication are done on the component systems separately and then adding results and inner products are performed as

$$(\langle v_2| \oplus \langle w_2|)(|v_1\rangle \oplus |w_1\rangle) = \langle v_2|v_1\rangle + \langle w_2|w_1\rangle$$

Thus, for a system of n two-state objects, the dimension of the state space of the system is $2n$, linear with the number of objects

Tensor product of vector spaces

Quantum systems, such as qubits combine as tensor products so for V and W with bases

$$A = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle\}, \qquad B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_m\rangle\}$$

The tensor product $V \otimes W$ is an $n \times m$-dimensional space consisting of elements $|\alpha_i\rangle \otimes |\beta_j\rangle$

Operations on such a vector space are now:

$$\begin{aligned}
(|v_1\rangle + |v_2\rangle) \otimes |w\rangle &= |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \\
|v\rangle \otimes (|w_1\rangle + |w_2\rangle) &= |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \\
(a|v\rangle) \otimes |w\rangle &= |v\rangle \otimes (a|w\rangle) = a\,(|v\rangle \otimes |w\rangle)
\end{aligned}$$

for $k = \min(n, m)$, all elements of $V \otimes W$ have the form

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle + \cdots + |v_k\rangle \otimes |w_k\rangle, \qquad v_i \in V, w_i \in W$$

The $\otimes$ symbol will often be dropped with the understanding that the tensor product is always implied: $|v\rangle \otimes |w\rangle \to |v\rangle|w\rangle \to |vw\rangle$

More about tensor products

The inner product in $V \otimes W$ space is defined as

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle\langle w_2|w_1\rangle$$

The tensor product of two unit vectors is also a unit vector, and given orthonormal bases $\{|\alpha_i\rangle\}$ and $\{|\beta_j\rangle\}$ for V and W, the basis $\{|\alpha_i\rangle\} \otimes \{|\beta_j\rangle\}$ for $V \otimes W$ is also orthonormal

For quantum computing, the tensor product of n 2-dimensional vector spaces (2^n dimensional) is most relevant

Most vectors $|u\rangle \in V \otimes W$ cannot be written as the tensor product of $|v\rangle \in V$ and $|w\rangle \in W$ these are so-called entangled states and are of fundamental importance to quantum computing

For entangled states, it is meaningless to discuss the state of a single qubit that is part of the system

Standard basis for multiple qubit systems

For a system of n qubits, the standard basis of the combined space $V_{n-1} \otimes \cdots \otimes V_0$ is given by 2^n unit vectors:

$$\{|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0, |0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0, |0\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0, \ldots$$
$$\ldots, \{|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0, |1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0\}$$

which uses the little endian notation

The state of a system with n qubits can be written in the explicit or more compact form

$$|b\rangle_{n-1} \cdots |b\rangle_1 |b\rangle_0 \equiv |b_{n-1} \cdots b_1 b_0\rangle$$

The 2^n standard basis vectors in the compact notation are thus

$$\{|0 \cdots 00\rangle, |0 \cdots 01\rangle, \cdots |1 \cdots 10\rangle, |1 \cdots 11\rangle\}$$

An even more compact form is to use the decimal value of the binary representation

$$\{|0\rangle, |1\rangle, \cdots, |2^n - 2\rangle, |2^n - 1\rangle\}$$

Multiple qubit examples

Given a 2 qubit state it is possible to represent it in the full, compact, or vector notations

$$\frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle + \frac{1}{\sqrt{2}}|3\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{i}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{aligned} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) &= \frac{1}{2}\left[\left(|0\rangle + |1\rangle\right) \otimes \left(|0\rangle + |1\rangle\right)\right] \\ &= \frac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right] \end{aligned}$$

$$\begin{aligned} \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right) &= \frac{1}{2}\left(|0\rangle + \sqrt{3}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + i|1\rangle\right) \\ &= \frac{1}{2\sqrt{2}}\left(|00\rangle + i|01\rangle + \sqrt{3}|10\rangle + i\sqrt{3}|11\rangle\right) \end{aligned}$$

Conventional representation

Just as for a single qubit, the global phase is indeterminate and by convention, a quantum superposition is written

$$a_0|0\cdots 00\rangle + a_1|0\cdots 01\rangle + \cdots + a_{2^n-1}|1\cdots 11\rangle$$

with the first non-zero coefficient being real and non-negative to ensure a unique representation for each state

For an n-qubit system there are $2^n - 1$ unique complex coefficients for each vector

The space in which vectors which are multiples of each other are considered equivalent is called the complex projective space of dimension $2^n - 1$

The expression $|v\rangle \sim |w\rangle$ means that the two vectors represent the same quantum state because they differ only by a global phase

A change in relative phase represents a different state

$$\frac{1}{\sqrt{2}}(e^{i\phi}|00\rangle + |11\rangle) \nsim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$\frac{1}{\sqrt{2}}(e^{i\phi}|00\rangle + e^{i\phi}|11\rangle) \sim \frac{1}{\sqrt{2}}e^{i\phi}(|00\rangle + |11\rangle) \sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alternate bases

Generally, the standard basis is used for multiple qubit systems but occasionally an alternate basis is useful

One of the more common bases for a 2-qubit system is the Bell basis: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Just as for a single qubit, there is redundance in the 2^n-dimensional space generated by n qubits since global phase factors distribute over tensor products

$$|v\rangle \otimes \left(e^{i\phi}|w\rangle\right) = e^{i\phi}\left(|v\rangle \otimes |w\rangle\right) = \left(e^{i\phi}|v\rangle\right) \otimes |w\rangle$$

A state might look different when it is represented in a different basis

$$\begin{aligned}\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) &= \frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|+\rangle + |-\rangle\right) + \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|+\rangle - |-\rangle\right)\right] \\ &= \frac{1}{\sqrt{2}}\left(|+\rangle|+\rangle + |-\rangle|-\rangle\right)\end{aligned}$$

Entanglement

For an n qubit system, only a few of the 2^n possible states can be described as product states of individual qubit states

Therefore the vast majority of states in the system are so-called entangled states

The Bell states are an example of entangled states of a 2-qubit system

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

For example, the $|\Phi^+\rangle$ Bell state cannot be described by the product below

$$(a_1|0\rangle_1 + b_1|1\rangle_1) \otimes (a_2|0\rangle_2 + b_2|1\rangle_2) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

if $a_1b_2 = 0$, then either $a_1a_2 = 0$ or $b_1b_2 = 0$ and the same if $b_1a_2 = 0$

The two particles in a Bell state are said to be maximally entangled and are called an EPR pair

More about entanglement

Entanglement is determined with respect to a specific decomposition of the state space, if

$$|\psi\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \cdots \otimes |v_n\rangle \in V, \qquad V = V_1 \otimes V_2 \otimes \cdots \otimes V_n$$

Then $|\psi\rangle$ is separable (or unentangled) with respect to the specific decomposition defined by V_i

The default decomposition for an n-qubit system is the tensor product of the n two-dimensional vector spaces corresponding to the individual qubits: $V_{n-1}, \ldots, V_0$

Entanglement is not, however, dependent on basis, for example the Bell state is entangled in any of the three common 2-qubit bases

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \tfrac{1}{\sqrt{2}}(|++\rangle + |--\rangle) = \tfrac{1}{\sqrt{2}}(|i\,\bar{i}\rangle + |\bar{i}\,i\rangle)$$

$$|\Phi^+\rangle = \tfrac{1}{\sqrt{2}}\left[\tfrac{1}{\sqrt{2}}\tfrac{1}{\sqrt{2}}(|i\rangle + |\bar{i}\rangle)(|i\rangle + |\bar{i}\rangle) + \tfrac{-i}{\sqrt{2}}\tfrac{-i}{\sqrt{2}}(|i\rangle - |\bar{i}\rangle)(|i\rangle - |\bar{i}\rangle)\right]$$

$$= \tfrac{1}{\sqrt{8}}\left[\cancel{|i\rangle|i\rangle} + |i\rangle|\bar{i}\rangle + |\bar{i}\rangle|i\rangle + \cancel{|\bar{i}\rangle|\bar{i}\rangle} - \cancel{|i\rangle|i\rangle} + |i\rangle|\bar{i}\rangle + |\bar{i}\rangle|i\rangle - \cancel{|\bar{i}\rangle|\bar{i}\rangle}\right]$$

Multiple meanings of entanglement

Since entanglement is not an intrinsic property of the state but depends on the particular decomposition, it is often convenient to use a decomposition into subsystems where the state is separable, Consider the 4-qubit state

$$|\psi\rangle = \tfrac{1}{2}\left(|00\rangle + |11\rangle + |22\rangle + |33\rangle\right) = \tfrac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right)$$

$$= \tfrac{1}{2}\left(|0\rangle_3|0\rangle_2|0\rangle_1|0\rangle_0 + |0\rangle_3|1\rangle_2|0\rangle_1|1\rangle_0 + |1\rangle_3|0\rangle_2|1\rangle_1|0\rangle_0 + |1\rangle_3|1\rangle_2|1\rangle_1|1\rangle_0\right)$$
$$= \tfrac{1}{\sqrt{2}}\left(|0\rangle_3|0\rangle_1 + |1\rangle_3|1\rangle_1\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle_2|0\rangle_0 + |1\rangle_2|1\rangle_0\right)$$

Thus $|\psi\rangle$ is not entangled with respect to the system decomposition into a subsystem of qubits 1 & 3 and qubits 0 & 2 However, it can be shown that any other subsystem decomposition leaves $|\psi\rangle$ entangled

$$|\psi\rangle \neq \tfrac{1}{\sqrt{2}}\left(|0\rangle_3|0\rangle_2 + |1\rangle_3|1\rangle_2\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_0 + |1\rangle_1|1\rangle_0\right)$$
$$= \tfrac{1}{2}\left(|0\rangle_3|0\rangle_2|0\rangle_1|0\rangle_0 + |0\rangle_3|0\rangle_2|1\rangle_1|1\rangle_0 + |1\rangle_3|1\rangle_2|0\rangle_1|0\rangle_0 + |1\rangle_3|1\rangle_2|1\rangle_1|1\rangle_0\right)$$
$$= \tfrac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) = \tfrac{1}{2}\left(|00\rangle + |03\rangle + |30\rangle + |33\rangle\right)$$

Measuring multiple qubits

Suppose we have an n-qubit system with vector space V of dimensionality $N = 2^n$

A device that takes measurements on this system will have an associated direct sum decomposition into orthogonal subspaces given by $V = S_1 \oplus \cdots \oplus S_k$, $k \leq N$

where k is the maximum number of possible outcomes of the measurement of a state with this device

The polarization of a photon is a trivial example of this where the system is defined as $n = 1$, $N = 2$, and $k = 2$, and the detector has an orthonormal basis $\{|v_1\rangle, |v_2\rangle\}$

Each of the orthonormal basis vectors, $|v_i\rangle$ generates a one-dimensional subspace, S_i consisting of $a|v_i\rangle$ and $V = S_1 \oplus S_2$

When a measurement is made with the polarization detector, the qubit state will then lie entirely in one of the two subspaces, S_1 or S_2

Measurement formalism

Similarly, with an n-qubit system, when the device with the decomposition $V = S_1 \oplus \cdots \oplus S_k$, the state $|\psi\rangle$ is

$$|\psi\rangle = a_1|\psi_1\rangle \oplus \cdots \oplus a_i|\psi_i\rangle \oplus \cdots \oplus a_k|\psi_k\rangle, \qquad |\psi_i\rangle \in S_i, a_1 \geq 0, Im\{a_1\} \equiv 0$$

When the device interacts with the state $|\psi\rangle$, the state will end up in state $|\psi_i\rangle \in S_i$ with a probability of $|a_i|^2$

Suppose a device measured a single qubit in the Hadamard basis

$$\left\{|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), |-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right\}$$

$|+\rangle$ and $|-\rangle$ generate S_+ and S_- respectively

$$|\psi\rangle = a|0\rangle + b|1\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle$$

$|\psi\rangle$ is then measured as $|+\rangle$ with probability $\left|\frac{a+b}{\sqrt{2}}\right|^2$ and $|-\rangle$ with probability $\left|\frac{a-b}{\sqrt{2}}\right|^2$

Measurement in a 2-qubit system

Consider a 2-qubit system with a measuring device that uses the standard basis and associated decomposition $V = S_1 \oplus S_2$ such that

$$S_1 = |0\rangle_1 \otimes V_2, \quad \text{span}(S_1) = \{|00\rangle, |01\rangle\} \qquad S_2 = |1\rangle_1 \otimes V_2, \quad \text{span}(S_2) = \{|10\rangle, |11\rangle\}$$

This device is used to measure an arbitrary 2-qubit state $|\psi\rangle$ with normalization factors

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = c_1|\psi_1\rangle + c_2|\psi_1\rangle$$

$$|\psi_1\rangle = \frac{1}{c_1}\left(a_{00}|00\rangle + a_{01}|01\rangle\right) \in S_1 \qquad |\psi_2\rangle = \frac{1}{c_2}\left(a_{10}|10\rangle + a_{11}|11\rangle\right) \in S_2$$

$$c_1 = \sqrt{|a_{00}|^2 + |a_{01}|^2}, \qquad c_2 = \sqrt{|a_{10}|^2 + |a_{11}|^2}$$

Measurement with this device will give $|\psi_1\rangle$ with probability

$$|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$$

and $|\psi_2\rangle$ with probability

$$|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$$

Measurement in the Hadamard basis

A device that measured the first qubit of a 2-qubit system with respect to the Hadamard basis $\{|+\rangle, |-\rangle\}$ has an associated decomposition $V = S_1' \oplus S_2'$ such that

$$S_1' = |+\rangle \otimes V_2, \quad \text{span}(S_1') = \{|+\rangle|0\rangle, |+\rangle|1\rangle\} \qquad S_2' = |-\rangle \otimes V_2, \quad \text{span}(S_2') = \{|-\rangle|0\rangle, |-\rangle|1\rangle\}$$

This device is used to measure an arbitrary 2-qubit state $|\psi\rangle$ with normalization factors

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = c_1'|\psi_1'\rangle + c_2'|\psi_1'\rangle$$

$$|\psi_1'\rangle = \frac{1}{c_1'}\left(\frac{a_{00}+a_{10}}{\sqrt{2}}|+\rangle|0\rangle + \frac{a_{01}+a_{11}}{\sqrt{2}}|+\rangle|1\rangle\right) \qquad |\psi_2'\rangle = \frac{1}{c_2'}\left(\frac{a_{00}-a_{10}}{\sqrt{2}}|-\rangle|0\rangle + \frac{a_{01}-a_{11}}{\sqrt{2}}|-\rangle|1\rangle\right)$$

$$c_1' = c_2' = \sqrt{|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2}/2$$

Measurement with this device will give $|\psi_1'\rangle$ and $|\psi_2'\rangle$ with equal probabilities

A special case is $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with $a_{00} = a_{11} = \frac{1}{\sqrt{2}}$ and $a_{10} = a_{01} = 0$

Quantum key distribution with entangled states

The Ekert91 protocol uses entangled states to transmit keys

A series of qubits are created in the entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice gets the first qubit of the pair and Bob gets the second

Each of them measures their qubit using either the standard basis, $\{|0\rangle, |1\rangle\}$, or the Hadamard basis, $\{|+\rangle, |-\rangle\}$, chosen randomly and independently

They compare their bases and discard those bits where they differ. Why?

If Alice obtains $|0\rangle$ using the standard basis, then they know the entire entangled state becomes $|00\rangle$ and Bob will also measure $|0\rangle$ in the standard basis

If Bob uses the Hadamard basis, he will get $|0\rangle$ and $|1\rangle$ with equal probability so the differing bases must be discarded

Since there is no exchange of quantum states in this protocol Eve has a much harder time gathering any information about the key