Introduction to Quantum Computing

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Quantum State Spaces

Direct Sums of Vector Spaces

- Let V be a vector space, with basis $A = \{|\alpha_1\rangle, |\alpha_2\rangle, \ldots, |\alpha_n\rangle\}$.
- Let W be a vector space, with basis $B = \{|\beta_1\rangle, |\beta_2\rangle, \ldots, |\beta_m\rangle\}$.
- The **direct sum** $V \oplus W$ of V and W is the vector space with basis

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

- Every element $|x\rangle \in V \oplus W$ can be written as

$$|x\rangle = |v\rangle \oplus |w\rangle,$$

  for some $|v\rangle \in V$ and $|w\rangle \in W$.
- For V and W of dimension n and m respectively, $V \oplus W$ has dimension $n + m$,

$$\dim(V \oplus W) = \dim(V) + \dim(W).$$

Direct Sums of Vector Spaces (Cont'd)

- Addition and scalar multiplication are defined by:
  - Performing the operation on the two component vector spaces separately;
  - Adding the results.
- Suppose V and W are inner product spaces.
- Then the standard inner product on $V \oplus W$ is given by

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

- The vector spaces V and W embed in $V \oplus W$ in the obvious canonical way.
- The images are orthogonal under the standard inner product.

State Space in the Classical Case

- Suppose that the state of each of three classical objects O_1, O_2 and O_3 is fully described by two parameters,
  - The position x_i;
  - The momentum p_i.
- Then the state of the system can be described by the direct sum of the states of the individual objects:

$$\begin{pmatrix} x_1 \\ p_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ p_2 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ p_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \\ x_3 \\ p_3 \end{pmatrix}.$$

- The state space of n such classical objects has dimension $2n$.
- Thus the size of the state space grows linearly with the number of objects.

Tensor Product of Vector Spaces

- Let V be a vector space, with basis $A = \{|\alpha_1\rangle, |\alpha_2\rangle, \dots, |\alpha_n\rangle\}$.
- Let W be a vector space, with basis $B = \{|\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_m\rangle\}$.
- The **tensor product** $V \otimes W$ of V and W is an nm-dimensional vector space, with a basis consisting of the nm elements of the form

$$|\alpha_i\rangle \otimes |\beta_j\rangle.$$

- Here $\otimes$ is the **tensor product**, a binary operator that satisfies the following relations:
  - $(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$;
  - $|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$;
  - $(a|v\rangle) \otimes |w\rangle = |v\rangle \otimes (a|w\rangle) = a(|v\rangle \otimes |w\rangle)$.

Tensor Product Representations

- Take $k = \min(n, m)$.
- All elements of $V \otimes W$ have the form

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle + \cdots + |v_k\rangle \otimes |w_k\rangle,$$

  for some $v_i \in V$ and $w_i \in W$.
- Due to the relations defining the tensor product, such a representation is not unique.
- All elements of $V \otimes W$ can be written

$$a_1(|\alpha_1\rangle \otimes |\beta_1\rangle) + a_2(|\alpha_2\rangle \otimes |\beta_1\rangle) + \cdots + a_{nm}(|\alpha_n\rangle \otimes |\beta_m\rangle).$$

- However, most elements of $V \otimes W$ cannot be written as $|v\rangle \otimes |w\rangle$, where $v \in V$ and $w \in W$.
- It is common to write $|v\rangle|w\rangle$ for $|v\rangle \otimes |w\rangle$.

Example

- Consider two two-dimensional vector spaces,
  - V, with orthonormal basis $A = \{|\alpha_1\rangle, |\alpha_2\rangle\}$;
  - W, with orthonormal basis $B = \{|\beta_1\rangle, |\beta_2\rangle\}$.

  Let $|v\rangle = a_1|\alpha_1\rangle + a_2|\alpha_2\rangle$ be an element of V.

  Let $|w\rangle = b_1|\beta_1\rangle + b_2|\beta_2\rangle$ be an element of W.

  Then

$$\begin{array}{rcl} |v\rangle \otimes |w\rangle & = & (a_1|\alpha_1\rangle + a_2|\alpha_2\rangle) \otimes (b_1|\beta_1\rangle + b_2|\beta_2\rangle) \\ & = & a_1|\alpha_1\rangle \otimes (b_1|\beta_1\rangle + b_2|\beta_2\rangle) + a_2|\alpha_2\rangle \otimes (b_1|\beta_1\rangle + b_2|\beta_2\rangle) \\ & = & a_1 b_1|\alpha_1\rangle \otimes |\beta_1\rangle + a_1 b_2|\alpha_1\rangle \otimes |\beta_2\rangle \\ & & \quad + a_2 b_1|\alpha_2\rangle \otimes |\beta_1\rangle + a_2 b_2|\alpha_2\rangle \otimes |\beta_2\rangle. \end{array}$$

Example (Cont'd)

- Suppose V and W are vector spaces corresponding to a qubit, each with standard basis
$$\{|0\rangle, |1\rangle\}.$$
Then $V \otimes W$ has basis
$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}.$$
Consider two single-qubit states
$$a_1|0\rangle + b_1|1\rangle \quad \text{and} \quad a_2|0\rangle + b_2|1\rangle.$$
Their tensor product is
$$a_1a_2|0\rangle \otimes |0\rangle + a_1b_2|0\rangle \otimes |1\rangle + a_2b_1|1\rangle \otimes |0\rangle + a_2b_2|1\rangle \otimes |1\rangle.$$

Using Matrices

- To write examples in the more familiar matrix notation for vectors, we must choose an ordering for the basis of the tensor product space.
- For example, we can choose the dictionary ordering

$$\{|\alpha_1\rangle|\beta_1\rangle, |\alpha_1\rangle|\beta_2\rangle, |\alpha_2\rangle|\beta_1\rangle, |\alpha_2\rangle|\beta_2\rangle\}.$$

Example: Consider the tensor product space.

Order the basis using the dictionary ordering.

Consider the tensor product of the unit vectors with matrix representation $|v\rangle = \frac{1}{\sqrt{5}}(1, -2)^\dagger$ and $|w\rangle = \frac{1}{\sqrt{10}}(-1, 3)^\dagger$.

It is the unit vector

$$|v\rangle \otimes |w\rangle = \frac{1}{5\sqrt{2}}(-1, 3, 2, -6)^\dagger.$$

Inner Product and Dimensions

- Suppose V and W are inner product spaces.
- Then $V \otimes W$ can be given an inner product by taking the product of the inner products on V and W.
- The inner product of $|v_1\rangle \otimes |w_1\rangle$ and $|v_2\rangle \otimes |w_2\rangle$ is given by

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

- The tensor product of two unit vectors is a unit vector.
- Given orthonormal bases $\{|\alpha_i\rangle\}$ for V and $\{|\beta_i\rangle\}$ for W, the basis $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ for $V \otimes W$ is also orthonormal.
- The tensor product $V \otimes W$ has dimension $\dim(V) \times \dim(W)$.
- So the tensor product of n two-dimensional vector spaces has 2^n dimensions.

Entangled States

- Most elements $|w\rangle \in V \otimes W$ cannot be written as the tensor product of a vector in V and a vector in W (even though they are all linear combinations of such elements).
- This observation is of crucial importance to quantum computation.
- States of $V \otimes W$ that cannot be written as the tensor product of a vector in V and a vector in W are called **entangled states**.
- We will see, for most quantum states of an n-qubit system, in particular for all entangled states, it is not meaningful to talk about the state of a single qubit of the system.

Basis of the Tensor Product

- Suppose we are given two quantum systems.
  - The states of the first are represented by unit vectors in V;
  - The states of the first are represented by unit vectors in W.
- Then the possible states of the joint quantum system are represented by unit vectors in the vector space $V \otimes W$.
- For $0 \leq i < n$, let V_i be the vector space, with basis $\{|0\rangle_i, |1\rangle_i\}$, corresponding to a single qubit.
- The standard basis for the vector space $V_{n-1} \otimes \cdots \otimes V_1 \otimes V_0$ for an n-qubit system consists of the 2^n vectors

$$\begin{aligned}\{ \quad & |0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0, \\ & |0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0, \\ & |0\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0, \\ & \vdots \\ & |1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0 \}.\end{aligned}$$

Simplifying the Notation

- The subscripts are often dropped, since the corresponding qubit is clear from position.
- Recall that adjacency of kets means the tensor product.
- This enables us to write this basis more compactly.

$$\{|0\rangle \cdots |0\rangle|0\rangle, |0\rangle \cdots |0\rangle|1\rangle, |0\rangle \cdots |1\rangle|0\rangle, \ldots, |1\rangle \cdots |1\rangle|1\rangle\}.$$

- The tensor product space corresponding to an n-qubit system occurs so frequently throughout quantum information processing.
- So an even more compact and readable notation uses $|b_{n-1} \ldots b_0\rangle$ to represent $|b_{n-1}\rangle \otimes \cdots \otimes |b_0\rangle$.
- In this notation the standard basis for an n-qubit system can be written

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

Decimal Representation of Bases

- Decimal notation is more compact than binary notation.
- Consider a state
$$|b_{n-1}\cdots b_1 b_0\rangle.$$
- Let x be the decimal number whose binary representation is
$$b_{n-1}\cdots b_1 b_0.$$
- Then the state $|b_{n-1}\cdots b_1 b_0\rangle$ will be represented more compactly as
$$|x\rangle.$$
- In this notation, the standard basis for an n-qubit system is written
$$\{|0\rangle, |1\rangle, |2\rangle, \ldots, |2^{n-1}\rangle\}.$$

Decimal Representation and Number of Qubits

- The standard basis for a two-qubit system can be written as

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}.$$

- The standard basis for a three-qubit system can be written as

$$\begin{aligned} &\{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\} \\ &\quad = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle\}. \end{aligned}$$

- Note that the notation $|3\rangle$ corresponds to two different quantum states in these two bases.
- So in order for such notation to be unambiguous, the number of qubits must be clear from context.

Specialized Notation

- The following reasons may entice a less compact notation.
  - Setting apart certain sets of qubits;
  - Indicating separate registers of a quantum computer;
  - Indicating qubits controlled by different people.

  Example: Consider a scenario in which:
  - Alice controls the first two qubits;
  - Bob the last three qubits.

  We may write a state as

$$\frac{1}{\sqrt{2}}(|00\rangle|101\rangle + |10\rangle|011\rangle).$$

  Sometimes, for added clarity, we may even write

$$\frac{1}{\sqrt{2}}(|00\rangle_A|101\rangle_B + |10\rangle_A|011\rangle_B),$$

  where the subscripts indicate the qubits controlled by each party.

Example

- Consider a three-qubit system.

  The following superpositions represent possible states of the system.

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|7\rangle = \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{\sqrt{2}}|111\rangle,$$

$$\frac{1}{2}(|1\rangle + |2\rangle + |4\rangle + |7\rangle) = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle).$$

Matrix Representation

- To use matrix notation for state vectors of an n-qubit system, the order of basis vectors must be established.
- Unless specified otherwise, basis vectors labeled with numbers are assumed to be sorted numerically.

  Example: Consider the two qubit state

  $$\frac{1}{2}|00\rangle + \frac{\boldsymbol{i}}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|0\rangle + \frac{\boldsymbol{i}}{2}|1\rangle + \frac{1}{\sqrt{2}}|3\rangle.$$

  Suppose basis vectors are sorted numerically.

  Then the given state has matrix representation $\begin{pmatrix} \frac{1}{2} \\ \frac{\boldsymbol{i}}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$.

Choice of Basis

- We use the standard basis predominantly.
- But, occasionally, we also use other bases.

  Example: The **Bell basis** for a two-qubit system is

  $$\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\},$$

  where

  $$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
  $$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

  The Bell basis is important for various applications of quantum information.

Superpositions for Multiple Qubits

- As in the single-qubit case, a state $|v\rangle$ is a **superposition** with respect to a set of orthonormal states

$$\{|\beta_1\rangle, \ldots, |\beta_i\rangle\}$$

  if:
  - It is a linear combination of these states,

$$|v\rangle = a_1|\beta_1\rangle + \cdots + a_i|\beta_i\rangle;$$

  - At least two of the a_i are non-zero.
- When no set of orthonormal states is specified, we will mean that the superposition is with respect to the standard basis.

Redundancies

- Any unit vector of the 2^n-dimensional state space represents a possible state of an n-qubit system.
- Just as in the single-qubit case there is redundancy.
- Of course, vectors that are multiples of each other refer to the same quantum state.
- Additionally, in the multiple-qubit case, properties of the tensor product mean that phase factors distribute over tensor products.
- So the same phase factor in different qubits of a tensor product represent the same state:

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

Examples

- Phase factors in individual qubits of a single term of a superposition can always be factored out into a single coefficient for that term.

  Example:

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

  Example:

$$\begin{aligned}(\tfrac{1}{2}|0\rangle + \tfrac{\sqrt{3}}{2}|1\rangle) \otimes (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{\boldsymbol{i}}{\sqrt{2}}|1\rangle) \\ = \tfrac{1}{2\sqrt{2}}|00\rangle + \tfrac{\boldsymbol{i}}{2\sqrt{2}}|01\rangle + \tfrac{\sqrt{3}}{2\sqrt{2}}|10\rangle + \tfrac{\boldsymbol{i}\sqrt{3}}{2\sqrt{2}}|11\rangle.\end{aligned}$$

Complex Projective Space

- Just as in the single-qubit case, vectors that differ only in a global phase represent the same quantum state.
- Write every quantum state as
$$a_0|0\dots00\rangle + a_1|0\dots01\rangle + \cdots + a_{2^n-1}|1\dots11\rangle.$$
- If we require the first non-zero a_i to be real and non-negative, then every quantum state has a unique representation.
- Consequently, the quantum state space of an n-qubit system has $2^n - 1$ complex dimensions.
- For any complex vector space of dimension N, the space in which vectors that are multiples of each other are considered equivalent is called **complex projective space** of dimension $N - 1$.
- So the space of distinct quantum states of an n-qubit system is a complex projective space of dimension $2^n - 1$.

Sources of Potential Confusion

- As in the single-qubit case, we should not confuse the vector space in which we write our computations with the quantum state space itself.
- We should also avoid confusion between the relative phases between terms in the superposition, of critical importance in quantum mechanics, and the global phase which has no physical meaning.
- We write
  $$|v\rangle \sim |w\rangle$$
  when two vectors $|v\rangle$ and $|w\rangle$ differ only by a global phase.
- Such vectors represent the same quantum state.

Example

- By construction, we have

$$|00\rangle \sim e^{\boldsymbol{i}\phi}|00\rangle.$$

On the other hand, the vectors

$$|v\rangle = \frac{1}{\sqrt{2}}(e^{\boldsymbol{i}\phi}|00\rangle + |11\rangle) \quad \text{and} \quad |w\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

represent different quantum states.

We have

$$\frac{1}{\sqrt{2}}(e^{\boldsymbol{i}\phi}|00\rangle + |11\rangle) \not\sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

However,

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

Vector Space versus State Space

- Quantum mechanical calculations are usually performed in the vector space rather than in the projective space because linearity makes vector spaces easier to work with.
- But we must always be aware of the $\sim$ equivalence when we interpret the results of our calculations as quantum states.

Writing in Terms of Different Bases

- Further confusion may arise when states are written in different bases.

  Example: Recall that

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad \text{and} \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

  The expression $\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ is a different way of writing $|0\rangle$.

  Moreover, we have

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

Subsection 2

Entangled States

Entangled States

- We saw that a single-qubit state can be specified by a single complex number.
- So any tensor product of n individual single-qubit states can be specified by n complex numbers.
- We also saw that it takes $2^n - 1$ complex numbers to describe states of an n-qubit system.
- Since $2^n \gg n$, the vast majority of n-qubit states cannot be described in terms of the state of n separate single-qubit systems.
- States that cannot be written as the tensor product of n single-qubit states are called **entangled states**.
- Thus, the vast majority of quantum states are entangled.

Example

- The elements of the Bell basis are entangled.

  Consider the Bell state

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

  $|\Phi^+\rangle$ cannot be described in terms of the state of each of its component qubits separately.

  It cannot be decomposed, because it is impossible to find a_1, a_2, b_1, b_2, such that

  $$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Example (Cont'd)

- To see this, note that
$$\begin{aligned}(a_1|0\rangle + b_1|1\rangle) \oplus (a_2|0\rangle + b_2|1\rangle) \\ = a_1 a_2|00\rangle + a_1 b_2|01\rangle + b_1 a_2|10\rangle + b_1 b_2|11\rangle.\end{aligned}$$
  Suppose $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

  Then $a_1 b_2 = 0$.

  Hence, $a_1 = 0$ or $b_2 = 0$.

  Therefore, $a_1 a_2 = 0$ or $b_1 b_2 = 0$.

  This contradicts the equation above.
- Two particles in the Bell state $|\Phi^+\rangle$ are called an **EPR pair** (for reasons to be explained later).

Example

- Other examples of two-qubit entangled states include

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

$$\frac{1}{\sqrt{2}}(|00\rangle - \boldsymbol{i}|11\rangle),$$

$$\frac{\boldsymbol{i}}{10}|00\rangle + \frac{\sqrt{99}}{10}|11\rangle$$

and

$$\frac{7}{10}|00\rangle + \frac{1}{10}|01\rangle + \frac{1}{10}|10\rangle + \frac{7}{10}|11\rangle.$$

Bell States

- Consider the four entangled states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

- They are called **Bell states**.
- Bell states are of fundamental importance to quantum information processing.

Entanglement and Decompositions

- Strictly speaking, entanglement is always with respect to a specified tensor product decomposition of the state space.
- Consider a quantum system, with associated vector space V.
- Suppose V has a tensor decomposition

$$V = V_1 \otimes \cdots \otimes V_n.$$

- Let $|\psi\rangle$ be a state of the quantum system.
- $|\psi\rangle$ is **separable**, or **unentangled**, *with respect to the given decomposition* if it can be written as

$$|\psi\rangle = |v_1\rangle \otimes \cdots \otimes |v_n\rangle,$$

  where $|v_i\rangle$ is contained in V_i.
- Otherwise, $|\psi\rangle$ is **entangled** with respect to this decomposition.

Convention

- Unless we specify a different decomposition, when we say an n-qubit state is entangled, we mean it is entangled with respect to the tensor product decomposition of the vector space V, associated to the n-qubit system, into the n two-dimensional vector spaces $V_{n-1}, \ldots, V_0$ associated with each of the individual qubits.
- For such statements to have meaning, it must be specified or clear from context which of the many possible tensor decompositions of V into two-dimensional spaces corresponds with the set of qubits under consideration.

Entanglement: Dependence on Decomposition

- It is vital to remember that entanglement:
  - Is not an absolute property of a quantum state;
  - Depends on the particular decomposition of the system into subsystems under consideration.
- States entangled with respect to the single-qubit decomposition may be unentangled with respect to other decompositions into subsystems.
- In particular, when discussing entanglement in quantum computation, we will be interested in entanglement with respect to:
  - A decomposition into registers;
  - A decomposition into subsystems consisting of multiple qubits;
  - The decomposition into individual qubits.

Example: Multiple Meanings of Entanglement

- Consider the four-qubit state

$$\begin{aligned} |\psi\rangle &= \tfrac{1}{2}(|00\rangle + |11\rangle + |22\rangle + |33\rangle) \\ &= \tfrac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle). \end{aligned}$$

- It is entangled, since it cannot be expressed as the tensor product of four single-qubit states.
- It is implicit in this statement that the entanglement is with respect to the decomposition into single qubits.
- There are other decompositions with respect to which this state is unentangled.

Example: Multiple Meanings of Entanglement (Cont'd)

- E.g., $|\psi\rangle$ can be expressed as the product of two two-qubit states.

$$\begin{aligned} |\psi\rangle &= \tfrac{1}{2}(|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4 + |0\rangle_1|1\rangle_2|0\rangle_3|1\rangle_4 \\ &\qquad + |1\rangle_1|0\rangle_2|1\rangle_3|0\rangle_4 + |1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4) \\ &= \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_3 + |1\rangle_1|1\rangle_3) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2|0\rangle_4 + |1\rangle_2|1\rangle_4). \end{aligned}$$

- The subscripts indicate which qubit we are talking about.
- So $|\psi\rangle$ is not entangled with respect to the system decomposition consisting of:
  - A subsystem of the first and third qubit;
  - A subsystem consisting of the second and fourth qubit.
- But, we can check that $|\psi\rangle$ is entangled with respect to the decomposition into the two two-qubit systems consisting of:
  - The first and second qubits;
  - The third and fourth qubits.

Entanglement: Independence from Basis

- Entanglement depends on the tensor decomposition.
- However, entanglement is not basis dependent.
- There is no reference, explicit or implicit, to a basis in the definition of entanglement.
- Certain bases may be more or less convenient to work with, depending, for instance, on how much they reflect the tensor decomposition under consideration.
- However, the choice does not affect what states are considered entangled.

On Quantum Superpositions

- As in the single-qubit case, most n-qubit states are superpositions, i.e., nontrivial linear combinations of basis vectors.
- As always, the notion of superposition is basis-dependent.
- All states are superpositions with respect to some bases, and not superpositions with respect to other bases.
- For multiple qubits, the answer to the question of what superpositions mean is more involved than in the single-qubit case.

Untenability of "Two States at the Same Time"

- The common way of talking about superpositions in terms of the system being in two states "at the same time" is even more suspect in the multiple-qubit case.
- This way of thinking fails to distinguish between states like $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|00\rangle + \boldsymbol{i}|11\rangle)$ that differ only by a relative phase and behave differently under a variety of circumstances.
- Furthermore, which states a system is viewed as "being in at the same time" is basis-dependent.
- The expressions $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$ represent the same state but have different interpretations.
  - One as being in the states $|00\rangle$ and $|11\rangle$ at the same time;
  - The other as being in the states $|++\rangle$ and $|--\rangle$ at the same time.
- This is absurd since they denote the same state and, thus, behave in precisely the same way under all circumstances.
- So quantum superpositions are not probabilistic mixtures.

Subsection 3

Basics of Multi-Qubit Measurement

Measuring Devices and Direct Sum Decomposition

- Let V be the $N = 2^n$ dimensional vector space associated with an n-qubit system.
- Any device that measures this system has an associated direct sum decomposition into orthogonal subspaces
$$V = S_1 \oplus \cdots \oplus S_k,$$
for some $k \leq N$.
- The number k corresponds to the maximum number of possible measurement outcomes for a state measured with that particular device.
- This number varies from device to device, even between devices measuring the same system.

Measuring Devices Generalized

- That any device has an associated direct sum decomposition is a direct generalization of the single-qubit case.
- Every device measuring a single-qubit system has an associated orthonormal basis
$$\{|v_1\rangle, |v_2\rangle\}$$
for the vector space V associated with the single-qubit system.
- The vectors $|v_i\rangle$ each generate a one-dimensional subspace S_i (consisting of all multiples $a|v_i\rangle$ where a is a complex number).
- Moreover, $V = S_1 \oplus S_2$.
- The only nontrivial decompositions of the vector space V are into two one-dimensional subspaces.
- Any choice of unit length vectors, one from each of the subspaces, yields an orthonormal basis.

Measurement

- Let a measuring device have associated direct sum decomposition

$$V = S_1 \oplus \cdots \oplus S_k.$$

- Consider an n-qubit system in state $|\psi\rangle$.
- Suppose the measuring device interacts with the n-qubit system.
- Then the interaction:
  - Changes the state to one entirely contained within one of the subspaces;
  - Chooses the subspace with probability equal to the square of the absolute value of the amplitude of the component of $|\psi\rangle$ in that subspace.
- More formally, the state $|\psi\rangle$ has a unique direct sum decomposition

$$|\psi\rangle = a_1|\psi_1\rangle \oplus \cdots \oplus a_k|\psi_k\rangle,$$

where $|\psi_i\rangle$ is a unit vector in S_i and a_i is real and non-negative.
- When $|\psi\rangle$ is measured, the state $|\psi_i\rangle$ is obtained with probability $|a_i|^2$.

Measurement and Quantum Mechanics

- The following are *axioms* of quantum mechanics.
  - Any measuring device has an associated direct sum decomposition;
  - The interaction between the device and a qubit ystem can be modeled in this way.
- It is not possible to prove that every device behaves in this way.
- However, so far it has provided an excellent model that predicts the outcome of experiments with high accuracy.

Single-Qubit Measurement in Standard Basis

- Let V be the vector space associated with a single-qubit system.
- A device that measures a qubit in the standard basis has, by definition, the associated direct sum decomposition

$$V = S_1 \oplus S_2,$$

  where:
  - S_1 is generated by $|0\rangle$;
  - S_2 is generated by $|1\rangle$.
- An arbitrary state

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

  measured by such a device will be:
  - $|0\rangle$ with probability $|a|^2$, the amplitude of $|\psi\rangle$ in the subspace S_1;
  - $|1\rangle$ with probability $|b|^2$, the amplitude of $|\psi\rangle$ in the subspace S_2.

Single-Qubit Measurement in Hadamard Basis

- Suppose a device measures a single qubit in the Hadamard basis
$$\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$$
- It has associated subspace decomposition
$$V = S_+ \oplus S_-,$$
where:
    - S_+ is generated by $|+\rangle$;
    - S_- is generated by $|-\rangle$.
- A state $|\psi\rangle = a|0\rangle + b|1\rangle$ can be rewritten as
$$|\psi\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle.$$
    - The probability that $|\psi\rangle$ is measured as $|+\rangle$ is $\left|\frac{a+b}{\sqrt{2}}\right|^2$.
    - The probability that $|\psi\rangle$ is measured as $|-\rangle$ is $\left|\frac{a-b}{\sqrt{2}}\right|^2$.

Measuring of First Qubit in Standard Basis

- Let V be the vector space associated with a two-qubit system.
- A device that measures the first qubit in the standard basis has associated subspace decomposition

$$V = S_1 \oplus S_2,$$

  where:
  - $S_1 = |0\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|00\rangle, |01\rangle\}$;
  - $S_2 = |1\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|10\rangle, |11\rangle\}$.
- We explore what happens when such a device measures an arbitrary two-qubit state

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

Measuring of First Qubit in Standard Basis (Cont'd)

- We write
$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle,$$
where:
    - $|\psi_1\rangle = \frac{1}{c_1}(a_{00}|00\rangle + a_{01}|01\rangle) \in S_1$;
    - $|\psi_2\rangle = \frac{1}{c_2}(a_{10}|10\rangle + a_{11}|11\rangle) \in S_2$.
- c_1 and c_2 are normalization factors,
$$c_1 = \sqrt{|a_{00}|^2 + |a_{01}|^2} \quad \text{and} \quad c_2 = \sqrt{|a_{10}|^2 + |a_{11}|^2}.$$
- Measurement of $|\psi\rangle$ with this device results in:
    - The state $|\psi_1\rangle$ with probability $|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$;
    - The state $|\psi_2\rangle$ with probability $|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$.
- In particular, when the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is measured, we obtain $|00\rangle$ and $|11\rangle$ with equal probability.

Measuring of First Qubit in Hadamard Basis

- A device that measures the first qubit of a two-qubit system with respect to the Hadamard basis $\{|+\rangle, |-\rangle\}$ has an associated direct sum decomposition
$$V = S_1' \oplus S_2',$$
where:
  - $S_1' = |+\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|+\rangle|0\rangle, |+\rangle|1\rangle\}$;
  - $S_2' = |-\rangle \otimes V_2$, the two-dimensional subspace spanned by $\{|-\rangle|0\rangle, |-\rangle|1\rangle\}$
- We explore what happens when such a device measures an arbitrary two-qubit state
$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle.$$

Measuring of First Qubit in Hadamard Basis (Cont'd)

- We write $|\psi\rangle$ as
$$|\psi\rangle = a_1'|\psi_1'\rangle + a_2'|\psi_2'\rangle,$$
where:
$$\begin{aligned} |\psi_1'\rangle &= c_1'\left(\frac{a_{00}+a_{10}}{\sqrt{2}}|+\rangle|0\rangle + \frac{a_{01}+a_{11}}{\sqrt{2}}|+\rangle|1\rangle\right), \\ |\psi_2'\rangle &= c_2'\left(\frac{a_{00}-a_{10}}{\sqrt{2}}|-\rangle|0\rangle + \frac{a_{01}-a_{11}}{\sqrt{2}}|-\rangle|1\rangle\right). \end{aligned}$$
- We may calculate the normalization factors c_1' and c_2'.
- These yield the probabilities for the two outcomes.
- This measurement on the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ yields $|+\rangle|+\rangle$ and $|-\rangle|-\rangle$ with equal probability.

Subsection 4

Quantum Key Distribution Using Entangled States

The Ekert 91 Protocol

- Alice and Bob wish to create a secret key.
- The protocol begins with the creation of a sequence of pairs of qubits, all in the entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice receives the first qubit of each pair.
- Bob receives the second qubit of each pair.
- For each qubit, they both independently and randomly choose one of the following in which to measure.
  - The standard basis $\{|0\rangle, |1\rangle\}$;
  - The Hadamard basis $\{|+\rangle, |-\rangle\}$.
- After they have made their measurements, they compare bases and discard those bits for which their bases differ.

The Ekert 91 Protocol (Cont'd)

- If Alice measures the first qubit in the standard basis and obtains $|0\rangle$, then the entire state becomes $|00\rangle$.
- If Bob now measures in the standard basis, he obtains the result $|0\rangle$ with certainty.
- If, instead, he measures in the Hadamard basis $\{|+\rangle, |-\rangle\}$, he obtains $|+\rangle$ and $|-\rangle$ with equal probability, since $|00\rangle = |0\rangle \left(\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \right)$.
- He interprets the states $|+\rangle$ and $|-\rangle$ as corresponding to the classical bit values 0 and 1, respectively.
- Thus when he measures in the basis $\{|+\rangle, |-\rangle\}$ and Alice measures in the standard basis, he obtains the same bit value as Alice only half the time.
- The behavior is similar when Alice's measurement indicates her qubit is in state $|1\rangle$.

The Ekert 91 Protocol (Cont'd)

- If instead Alice measures in the Hadamard basis and obtains the result that her qubit is in the state $|+\rangle$, the whole state becomes $|+\rangle|+\rangle$.
- If Bob now measures in the Hadamard basis, he obtains $|+\rangle$ with certainty.
- If he measures in the standard basis he obtains $|0\rangle$ and $|1\rangle$ with equal probability.
- Since Alice and Bob always get the same bit value if they measure in the same basis, the protocol results in a shared random key, as long as the initial pairs were EPR pairs.

The Ekert 91 Protocol (Cont'd)

- The security of the scheme relies on adding steps to the protocol we have just described that enable Alice and Bob to test the fidelity of their EPR pairs.
- The tests Ekert suggested are based on Bell's inequalities.
- This protocol has the intriguing property that in theory Alice and Bob can prepare shared keys as they need them, never needing to store keys for any length of time.
- In practice, to prepare keys on an as-needed basis in this way, Alice and Bob would need to be able to store their EPR pairs so that they are not corrupted during that time.
- The capability of long-term reliable storage of entangled states does not exist at present.