Today's outline - January 18, 2022

Today's outline - January 18, 2022

- Multiple qubit systems

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement
- Measurement of *n*-qubit systems

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement
- Measurement of n-qubit systems
- Quantum key distribution revisited

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement
- Measurement of n-qubit systems
- Quantum key distribution revisited

Reading Assignment: Chapter 4.1-4.2

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement
- Measurement of *n*-qubit systems
- Quantum key distribution revisited

Reading Assignment: Chapter 4.1-4.2

Homework Assignment #01:
Chapter 2:1,2,3,5,6,11
due Thursday, January 20, 2022

Today's outline - January 18, 2022

- Multiple qubit systems
- Entanglement
- Measurement of *n*-qubit systems
- Quantum key distribution revisited

Reading Assignment: Chapter 4.1-4.2

Homework Assignment #01:
Chapter 2:1,2,3,5,6,11
due Thursday, January 20, 2022

Homework Assignment #02:
Chapter 3:1,4,8,10,14,15
due Thursday, January 27, 2022

Tensor product review

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

Tensor product review

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

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

Tensor product review

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

Tensor product review

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

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

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

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

Tensor product review

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

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

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

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

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

Tensor product review

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

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

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

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

Tensor product review

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

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

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

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

the tensor product of n 2-dimensional vector spaces has dimension 2^n

Tensor product review

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

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

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

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

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

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

the tensor product of n 2-dimensional vector spaces has dimension 2^n

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

Tensor product review

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

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

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

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

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

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

the tensor product of n 2-dimensional vector spaces has dimension 2^n

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

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

the state of a system with n qubits can be written in the explicit

$$|b\rangle_{n-1} \cdots |b\rangle_1 |b\rangle_0$$

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

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

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

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

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

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

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

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

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: $\{|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_0\}, \dots, \{|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_0\}$

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

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

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

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

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

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

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

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

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

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

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

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

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

given a 2 qubit state it is possible to represent it in the full, compact

$$\frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

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

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

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

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

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

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

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

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: $\{|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_0\}, \dots, \{|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_0\}$

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

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

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

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

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

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

Alternate bases

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

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: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

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: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

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

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: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

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

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

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: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

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

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

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

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: $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$

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

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

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

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

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

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

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

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

$$\left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle\right)$$

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

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

phase factors in individual qubits of a single term in a superposition can be factored out

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

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

Conventional representation

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

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

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

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

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

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 $2^n - 1$

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

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

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

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

Conventional representation

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

$$a_0|0\cdots00\rangle + a_1|0\cdots01\rangle + \cdots + a_{2^n-1}|1\cdots11\rangle$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$(a_1|0\rangle_1 + b_1|1\rangle_1) \otimes (a_2|0\rangle_2 + b_2|1\rangle_2)$$

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

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

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

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

if $a_1 b_2 = 0$, then either $a_1 a_2 = 0$ or $b_1 b_2 = 0$ and the same if $b_1 a_2 = 0$

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

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

if $a_1 b_2 = 0$, then either $a_1 a_2 = 0$ or $b_1 b_2 = 0$ and the same if $b_1 a_2 = 0$

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

More about entanglement

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

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

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

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: $V_{n-1}, \ldots, V_0$

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

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

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

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

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

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: $V_{n-1}, \dots, V_0$

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

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

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,

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

$$|\psi\rangle = \frac{1}{2}\left(|00\rangle + |11\rangle + |22\rangle + |33\rangle\right)$$

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

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

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

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

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

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

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

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

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

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

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

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

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

thus $|\psi\rangle$ is not entangled with respect to the system decomposition into a subsystem of qubits 1 & 3 and qubits 0 & 2

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$= \tfrac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)$$

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

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

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

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

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

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

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

$$= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right) = \frac{1}{2}\left(|00\rangle + |03\rangle + |30\rangle + |33\rangle\right)$$

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

$$
\begin{aligned}
|\psi\rangle &= \tfrac{1}{2}\left(|00\rangle + |11\rangle + |22\rangle + |33\rangle\right) = \tfrac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right) \\
&= \tfrac{1}{2}\left(|0\rangle_3|0\rangle_2|0\rangle_1|0\rangle_0 + |0\rangle_3|1\rangle_2|0\rangle_1|1\rangle_0 + |1\rangle_3|0\rangle_2|1\rangle_1|0\rangle_0 + |1\rangle_3|1\rangle_2|1\rangle_1|1\rangle_0\right) \\
&= \tfrac{1}{\sqrt{2}}\left(|0\rangle_3|0\rangle_1 + |1\rangle_3|1\rangle_1\right) \otimes \tfrac{1}{\sqrt{2}}\left(|0\rangle_2|0\rangle_0 + |1\rangle_2|1\rangle_0\right)
\end{aligned}
$$

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

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

Measuring multiple qubits

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

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 $V = S_1 \oplus \cdots \oplus S_k$, $k \leq N$

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

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 $k = 2$,

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 $\{|v_1\rangle, |v_2\rangle\}$

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 $V = S_1 \oplus S_2$

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

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

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

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 $|a_i|^2$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $|\psi\rangle$

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 $|\psi\rangle$

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

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 $|\psi\rangle$

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

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 $|\psi\rangle$

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

$$|\psi_1\rangle = \frac{1}{c_1}\left(a_{00}|00\rangle + a_{01}|01\rangle\right) \in S_1$$

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 $|\psi\rangle$

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

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

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

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

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

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 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

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

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

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

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

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

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

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

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

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

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

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

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

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 $|\psi\rangle$

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 $|\psi\rangle$

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

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

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

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

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

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

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

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

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

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

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 $|\psi\rangle$

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

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

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

$S'_1 = |+\rangle \otimes V_2, \ \ \text{span}(S'_1) = \{|+\rangle|0\rangle, |+\rangle|1\rangle\}$ $\quad S'_2 = |-\rangle \otimes V_2, \ \ \text{span}(S'_2) = \{|-\rangle|0\rangle, |-\rangle|1\rangle\}$

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

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle = c'_1|\psi'_1\rangle + c'_2|\psi'_1\rangle$$

$$|\psi'_1\rangle = \frac{1}{c'_1}\left(\frac{a_{00}+a_{10}}{\sqrt{2}}|+\rangle|0\rangle + \frac{a_{01}+a_{11}}{\sqrt{2}}|+\rangle|1\rangle\right) \qquad |\psi'_2\rangle = \frac{1}{c'_2}\left(\frac{a_{00}-a_{10}}{\sqrt{2}}|-\rangle|0\rangle + \frac{a_{01}-a_{11}}{\sqrt{2}}|-\rangle|1\rangle\right)$$

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 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

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

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

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

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

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?

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

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

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