Multi-Qubit System

State Space of Bits

- The state space of a single bit is $\{0, 1\}$.
- n-bit state space is $\{0, 1\}^n$. These are the vertices of the n-dimensional hypercube.

State Space of Qubits

- The state space of a single qubit is a 2-dimensional vector space over $\mathbb{C}$. It is written as $a\,|0\rangle + b\,|1\rangle$ where $a, b \in \mathbb{C}$, such that $|a|^2 + |b|^2 = 1$ and $\{|0\rangle, |1\rangle\}$ are orthonormal base vectors.
- The state space of n-qubit system is a 2^n-dimensional vector space over $\mathbb{C}$. It is the tensor product of n copies of the single qubit spaces.

State Space Postulate

A closed quantum mechanical system can be modelled as a vector space with inner product - it is a Hilbert Space. Each state of the system is a unit vector of the space.

Tensor Product $\mathbb{R}^2 \otimes \mathbb{R}^3$

We start with an example.

- Consider 2-dimensional and 3-dimensional vector spaces over reals - $\mathbb{R}^2$ and $\mathbb{R}^3$.
- The tensor product of these two spaces is a vector space of dimension $2 \times 3 = 6$.
- It is denoted by $\mathbb{R}^2 \otimes \mathbb{R}^3$.

Tensor Product $\mathbb{R}^2 \otimes \mathbb{R}^3$

- The standard basis for $\mathbb{R}^2$ and $\mathbb{R}^3$ are $B_2 = \{(1,0),(0,1)\}$ and $B_3 = \{(1,0,0),(0,1,0),(0,0,1)\}$ respectively.
- Six elements of $B_2 \otimes B_3$ forms a basis of $\mathbb{R}^2 \otimes \mathbb{R}^3$.
- They are $\{(1,0) \otimes (1,0,0),(1,0) \otimes (0,1,0),(1,0) \otimes (0,0,1),(0,1) \otimes (1,0,0),(0,1) \otimes (0,1,0),(0,1) \otimes (0,0,1)\}$.

Tensor Product $\mathbb{R}^2 \otimes \mathbb{R}^3$

- Let $(a, b) = a(1, 0) + b(0, 1) \in \mathbb{R}^2$ and $(p, q, r) = p(1, 0, 0) + q(0, 1, 0) + r(0, 0, 1) \in \mathbb{R}^3$.
- The tensor product $(a, b) \otimes (p, q, r) = ap(1, 0) \otimes (1, 0, 0) + aq(1, 0) \otimes (0, 1, 0) + ar(1, 0) \otimes (0, 0, 1) + bp(0, 1) \otimes (1, 0, 0) + bq(0, 1) \otimes (0, 1, 0) + br(0, 1) \otimes (0, 0, 1)$.

Tensor Product of $\mathbb{R}^2 \otimes \mathbb{R}^3$

We may view

$$
\begin{aligned}
& B_2 \otimes B_3 \\
= \;& \{(1,0),(0,1)\} \otimes \{(1,0,0),(0,1,0),(0,0,1)\} \\
= \;& \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes [1,0,0], \cdots, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes [0,0,1] \right\} \\
= \;& \left\{ \begin{bmatrix} 1[1,0,0] \\ 0[1,0,0] \end{bmatrix}, \cdots, \begin{bmatrix} 0[0,0,1] \\ 1[0,0,1] \end{bmatrix} \right\} \\
= \;& \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \cdots, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \right\}.
\end{aligned}
$$

It may also be viewed as column vectors.

Tensor Product of $\mathbb{R}^2 \otimes \mathbb{R}^3$

- $B_2 \otimes B_3 = \{(1,0,0,0,0,0),(0,1,0,0,0,0),(0,0,1,0,0,0),(0,0,0,1,0,0),(0,0,0,0,1,0),(0,0,0,0,0,1)\}$.
- So, $(a,b) \otimes (p,q,r) = ap(1,0,0,0,0,0) + aq(0,1,0,0,0,0) + ar(0,0,1,0,0,0) + bp(0,0,0,1,0,0) + bq(0,0,0,0,1,0) + br(0,0,0,0,0,1) = (ap,aq,ar,bp,bq,br)$.

Note

1. Every element of $\mathbb{R}^2 \otimes \mathbb{R}^3$ is not a tensor product of the vectors of $\mathbb{R}^2$ and $\mathbb{R}^3$ i.e. not of the the form $(a, b) \otimes (p, q, r)$.
2. An example: $(2, 4, 6, 8, 10, 12) \in \mathbb{R}^2 \otimes \mathbb{R}^3$, but there is no $(a, b) \in \mathbb{R}^2$ and $(p, q, r) \in \mathbb{R}^3$ such that $(a, b) \otimes (p, q, r) = (ap, aq, ar, bp, bq, br) = (2, 4, 6, 8, 10, 12)$.

Note

3. If possible, then $\frac{ap}{aq} = \frac{2}{4} \Rightarrow \frac{p}{q} = \frac{1}{2}$. But $\frac{bp}{bq} = \frac{8}{10} \Rightarrow \frac{p}{q} = \frac{4}{5}$ - a contradiction.
4. Every element of $\mathbb{R}^2 \otimes \mathbb{R}^3$ is a linear combination of vectors of the form $(a, b) \otimes (p, q, r)$.

Definition: Tensor Product

Let A and B be two inner product spaces over a field F with base $E_a = \{|a_1\rangle, \cdots, |a_m\rangle\}$ and $E_b = \{|b_1\rangle, \cdots, |b_n\rangle\}$ respectively.
The tensor product of A and B is an mn-dimensional inner product space with the base
$E_{a\otimes b} = \{|a_i\rangle \otimes |b_j\rangle : 1 \leq i \leq m, 1 \leq j \leq n\}$.

Notation

- If $|a\rangle \in A$ and $|b\rangle \in B$, then $|a\rangle \otimes |b\rangle$ is also written as $|a\rangle\,|b\rangle$, $|a, b\rangle$, or $|ab\rangle$.
- A shorter notation for $|0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle = |0110\rangle$.

Notation

- Let $E_a = \{|a_1\rangle, |a_2\rangle\}$ and $E_b = \{|b_1\rangle, |b_2\rangle\}$.
- Consider two vectors
  $|a\rangle = \alpha_1 |a_1\rangle + \alpha_2 |a_2\rangle \in A$ and
  $|b\rangle = \beta_1 |b_1\rangle + \beta_2 |b_2\rangle$.
- Their tensor product
  $|a\rangle \otimes |b\rangle = |ab\rangle = (\alpha_1 |a_1\rangle + \alpha_2 |a_2\rangle) \otimes (\beta_1 |b_1\rangle + \beta_2 |b_2\rangle) = \alpha_1\beta_1 |a_1 b_1\rangle + \alpha_1\beta_2 |a_1 b_2\rangle + \alpha_2\beta_1 |a_2 b_1\rangle + \alpha_2\beta_2 |a_2 b_2\rangle$.

Notation

- Consider the qubit space $V = \mathbb{C}^2$ with standard pair of base vectors $|0\rangle, |1\rangle$.
- The n-times tensor product of V, $\overbrace{V \otimes \cdots \otimes V}^{n} = V^{\otimes n} = (\mathbb{C}^2)^{\otimes n}$ has 2^n standard base vectors, $|b_1 \cdots b_n\rangle$, where $b_1, \cdots, b_n \in \{0, 1\}$.
- Using the decimal notation the set of basis can be written as $\{|0\rangle, |1\rangle, \cdots, |2^n - 1\rangle\}$.

Properties

Let $\alpha \in F$, $\quad |a\rangle, |a'\rangle \in A$ and $|b\rangle, |b'\rangle \in B$

1. $\alpha(|a\rangle \otimes |b\rangle) = (\alpha |a\rangle) \otimes |b\rangle = |a\rangle \otimes (\alpha |b\rangle)$.
2. $(|a\rangle + |a'\rangle) \otimes |b\rangle = (|a\rangle \otimes |b\rangle) + (|a'\rangle \otimes |b\rangle)$.
3. $|a\rangle \otimes (|b\rangle + |b'\rangle) = (|a\rangle \otimes |b\rangle) + (|a'\rangle \otimes |b'\rangle)$.

Inner product

The inner product on $A \otimes B$ (if both A and B are inner product spaces) is defined as follows: Inner product of $|a\rangle \otimes |b\rangle$ with $|a'\rangle \otimes |b'\rangle$ is defined as

$$(\langle a'| \otimes \langle b'|) \cdot (|a\rangle \otimes |b\rangle) = (\langle a'|a\rangle)(\langle b'|b\rangle).$$

Orthonormal Basis

We know that the set of basis $\{|a_1\rangle, \cdots .|a_m\rangle\}$ of an inner product space A is orthonormal if $\langle a_i|a_j\rangle = \delta_{ij}$.

Standard Basis

We consider standard basis of a 2-qubit system - $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Inner product of two of them $|b_i b_j\rangle$ and $|b_k b_l\rangle$ is

$$\langle b_k b_l| \cdot |b_i b_j\rangle = \langle b_k|b_i\rangle \langle b_l|b_j\rangle = \begin{cases} 1 & \text{if } b_k = b_i \\ & \quad \text{and } b_l = b_j, \\ 0 & \text{otherwise.} \end{cases}$$

So this is an orthonormal basis.

Hadamard $\otimes$ Standard Basis

- We choose the Hadamard basis for the first first qubit and standard basis for the second qubit.
- So the basis of the 2-qubit system is $B_{HS} = \{|+\rangle, |-\rangle\} \otimes \{|0\rangle, |1\rangle\} = \{|+0\rangle, |+1\rangle, |-0\rangle, |-1\rangle\}$.

Hadamard $\otimes$ Standard Basis

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

Similarly other two base vectors can be constructed.

Hadamard $\otimes$ Standard Basis is Orthonormal

Inner product of $|{+0}\rangle$ with itself is

$$
\begin{aligned}
& \frac{1}{\sqrt{2}}(\langle 00| + \langle 10|) \cdot \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \\
= \; & \frac{1}{2}(\langle 00| \cdot |00\rangle + \langle 00| \cdot |10\rangle + \langle 10| \cdot |00\rangle + \langle 10| \cdot |10\rangle) \\
= \; & \frac{1}{2}(1 + 0 + 0 + 1) \\
= \; & 1
\end{aligned}
$$

Hadamard ⊗ Standard Basis is Orthonormal

Inner product of $|+0\rangle$ with $|+1\rangle$ is

$$\begin{aligned}
& \frac{1}{\sqrt{2}}(\langle 00| + \langle 10|) \cdot \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) \\
= & \frac{1}{2}(\langle 00| \cdot |01\rangle + \langle 00| \cdot |11\rangle + \langle 10| \cdot |01\rangle + \langle 10| \cdot |11\rangle) \\
= & \frac{1}{2}(0 + 0 + 0 + 0) \\
= & 0
\end{aligned}$$

So B_{HS} is orthonormal.

Bell Basis

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

Bell Basis is Orthonormal

Inner product of $|\Phi^+\rangle$ with itself.

$$
\begin{aligned}
&= (\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)) \cdot (\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)) \\
&= \frac{1}{2}(\langle 00|00\rangle + \langle 00|11\rangle + \langle 11|00\rangle + \langle 11|11\rangle) \\
&= \frac{1}{2}(1 + 0 + 0 + 1) \\
&= 1.
\end{aligned}
$$

Bell Basis is Orthonormal

Inner product of $|\Phi^+\rangle$ with $|\Phi^-\rangle$.

$$\begin{aligned}
&= (\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)) \cdot (\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)) \\
&= \frac{1}{2}(\langle 00|00\rangle - \langle 00|11\rangle + \langle 11|00\rangle - \langle 11|11\rangle) \\
&= \frac{1}{2}(1 - 0 + 0 - 1) \\
&= 0.
\end{aligned}$$

Phase Factor

The concept of global phase is similar to the single qubit system with the only difference that the phase factor may be attached to any of the component vectors of the tensor product. So we have

$$(e^{i\phi}|a\rangle) \otimes |b\rangle = e^{i\phi}(|a\rangle \otimes |b\rangle) = |a\rangle) \otimes (e^{i\phi}|b\rangle),$$

representing the same state.

Phase Factor

The concept of relative phase is also similar to the single qubit system. Note that though $e^{i\phi}|a\rangle$ and $|a\rangle$ are equivalent states, $e^{i\phi}|a\rangle + |b\rangle$ and $|a\rangle + |b\rangle$ are not be equivalent.

Separable and Entangled States

- We have already shown that every vector of $\mathbb{R}^2 \bigotimes \mathbb{R}^3$ cannot be expressed as a tensor product of vectors of $\mathbb{R}^2$ and $\mathbb{R}^3$.
- This is true for tensor product of qubit spaces. We consider two 2-qubit states, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ and $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Separable and Entangled States

The state $|\psi\rangle$ can be decomposed into the tensor product of two 1-qubit state - $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle$. These types of states are known as separable.

Separable and Entangled States

- But $|\Phi^+\rangle$ cannot be decomposed in that way. If possible, let $|\Phi^+\rangle = (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle$.
- But $ad = 0$ implies that $a = 0$ or $d = 0$. That makes either $ac = 0$ or $bd = 0$ - a contradiction. These types of states are known as entangled stater.

Separable and Entangled States

If we perform a measurement in standard computational basis, on the second qubit of $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$, we get a $|0\rangle$ with probability 1 and the state remains unchanged.

Separable and Entangled States

If we perform a similar measurement on the second qubit of $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, we get $|0\rangle$ or $|1\rangle$ with equal probability $\frac{1}{2}$. But the outcome of this experiment also determines the first qubit with certainty - so the 2-qubit state changes.

If two qubits in entangled state are separated out, taken far apart and one of them is measured, the outcome of the measurement on the other qubit is known.

Entanglement and Decomposition

- Consider the decomposition of 4-qubit state $|u\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$ to $\bigotimes_{i=1}^{4}(a_i\,|0\rangle + b_i\,|1\rangle)$.
- Such a decomposition must satisfy, $a_1a_2a_3a_4 = a_1a_2b_3b_4 = b_1b_1a_3a_4 = b_1b_2b_3b_4 = 1/2$ and $a_1a_2a_3b_4 = 0$ - which is impossible.
- So $|u\rangle$ is an entangled state with respect to 1-qubit decomposition.

Entanglement and Decomposition

But $|u\rangle = \frac{1}{2}(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle)$ is equal to $|\Phi^+\rangle \otimes |\Phi^+\rangle$.
So $|u\rangle$ is separable in 2-qubit decomposition.

Direct Sum of Vector Spaces

Consider the m and n-dimensional vector spaces A and B over a field F, with the corresponding bases E_a and E_b respectively. The direct sum of A and B is an $(m+n)$-dimensional vector space with the base $E_a \cup E_b$. The space is written as $A \oplus B$.

Any vector $|x\rangle \in A \oplus B$ can be written as $|x\rangle = |a\rangle \oplus |b\rangle$, where $|a\rangle \in A$ and $|b\rangle \in B$.

Direct Sum $\mathbb{R}^2 \oplus \mathbb{R}^3$

The basis of $\mathbb{R}^2 \oplus \mathbb{R}^3$ is $B_2 \cup B_3 = \{(1,0),(0,1),(1,0,0),(0,1,0),(0,0,1)\}$. Each of these base vectors is viewed as 5-dimensional vector i.e $\{(1,0,0,0,0),(0,1,0,0,0),$
$(0,0,1,0,0),(0,0,0,1,0),(0,0,0,0,1)\}$
where the first two components are for $\mathbb{R}^2$ and the last three components are for $\mathbb{R}^3$.
Addition and scalar multiplications are defined in a natural way.

Measurement Postulate

Let $B = \{|b_i\rangle\}_{i \in I}$ is orthonormal basis for the state space V_A of a system A.

A von Neumann measurement on a state $|x\rangle = \sum_{i \in I} a_i |b_i\rangle$ will output a real value v_i with the the probability $|a_i|^2$. The system will be in the state $|b_i\rangle$ after the measurement.

Measurement Postulate

Let the state space $V_A \otimes V_C$ be a tensor product of V_A with basis $B = \{|b_i\rangle\}_{i \in I}$ (orthonormal) and V_C with basis $D = \{|d_j\rangle\}_{j \in J}$ (with unit norm).

A von Neumann measurement of a state $|x\rangle = \sum_{i,j} a_{ij} |b_i\rangle |d_j\rangle$ on the space V_A will give a value v_{ij} with the probability $|a_{ij}|^2$. The system will be in the state $|b_i\rangle |d_j\rangle$ after the measurement.

Multi-Qubit Measurement

We have already stated that for a single-qubit system the every measuring device has an orthonormal basis $B = \{|b_1\rangle, |b_2\rangle\}$ for the associated vector space V of 1-qubit states.

Each element of B generates an 1-dimensional subspace, $V_1 = a_1 |b_1\rangle$ and $V_2 = a_2 |b_2\rangle$, where $a_1, a_2 \in \mathbb{C}$, such that $V = V_1 \bigoplus V_2$.

Multi-Qubit Measurement

The 2^n-dimensional vector space V corresponding to an n-qubit system is decomposed by a measuring device into $k \leq n$ orthogonal subspaces $V_1, \cdots, V_k$ so that $V = V_1 \oplus \cdots \oplus V_k$.

Multi-Qubit Measurement

Any n-qubit state $|x\rangle \in V$ on measurement on this device chooses a subspaces V_i with a probability $p_i = |a_i|^2$, where a_i is the amplitude of $|x\rangle$ in V_i. So we have $|x\rangle = a_1 |x_1\rangle + \cdots + a_k |x_k\rangle$, where x_i is the unit vector in the subspace V_i.

Example 1

The device measures the first qubit state of a 2-qubit system in standard basis. Let V the state space of the 2-qubit system.

- We decompose $V = V_1 \oplus V_2$ where V_1 is the space spanned by $\{|00\rangle, |01\rangle\}$ and V_2 is the space spanned by $\{|10\rangle, |11\rangle\}$. In other words $V_1 = |0\rangle \otimes W$ and $V_2 = |1\rangle \otimes W$, where W is 1-qubit state space.

Example 1

- The state of a 2-qubit system is $|\psi\rangle = a_0 |00\rangle + a_1 |01\rangle + a_2 |10\rangle + a_3 |11\rangle$ where $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1$.
- We rewrite the state as $|\psi\rangle = b_1 |\psi_1\rangle + b_2 |\psi_2\rangle$, where $|\psi_1\rangle \in V_1$ and $|\psi_2\rangle \in V_2$, $b_1 = \sqrt{|a_0|^2 + |a_1|^2}$ and $b_2 = \sqrt{|a_2|^2 + |a_3|^2}$.

Example 1

- So, $|\psi_1\rangle = \frac{1}{b_1}(a_0 |00\rangle + a_1 |01\rangle)$ and $|\psi_2\rangle = \frac{1}{b_2}(a_2 |10\rangle + a_3 |11\rangle)$.
- When the first qubit is measured, the probability that the resulting state is ψ_1 is $|a_0|^2 + |a_1|^2 = b_1^2$, and the probability that the resulting state is ψ_2 is $|a_2|^2 + |a_3|^2 = b_2^2$

Example 2

The device measures the first qubit state of a 2-qubit system in Hadamard basis. The state space V of the 2-qubit system is expressed as

- $V = V_1 \oplus V_2$ where V_1 is the space spanned by $\{|+0\rangle, |+1\rangle\}$ and V_2 is the space spanned by $\{|-0\rangle, |-1\rangle\}$. In other words $V_1 = |+\rangle \otimes W$ and $V_2 = |-\rangle \otimes W$, where W is 1-qubit state space.

Example 2

- The state of a 2-qubit system is $|\psi\rangle = a_0\,|00\rangle + a_1\,|01\rangle + a_2\,|10\rangle + a_3\,|11\rangle$ where $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1$.
- We rewrite $|\psi\rangle$ as

$$\frac{a_0}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |0\rangle + \frac{a_1}{\sqrt{2}}(|+\rangle + |-\rangle) \otimes |1\rangle +$$
$$\frac{a_2}{\sqrt{2}}(|+\rangle - |-\rangle) \otimes |0\rangle + \frac{a_3}{\sqrt{2}}(|+\rangle - |-\rangle) \otimes |1\rangle$$

Example 2

So

$$
\begin{aligned}
|\psi\rangle &= \frac{a_0 + a_2}{\sqrt{2}} \left|+0\right\rangle + \frac{a_1 + a_3}{\sqrt{2}} \left|+1\right\rangle + \\
&\quad \frac{a_0 - a_2}{\sqrt{2}} \left|-0\right\rangle + \frac{a_1 - a_3}{\sqrt{2}} \left|-1\right\rangle \\
&= c_1 \left|\psi_1\right\rangle + c_2 \left|\psi_2\right\rangle,
\end{aligned}
$$

Example 2

where

$$
\begin{aligned}
|\psi_1\rangle &= \frac{1}{c_1}\left(\frac{a_0+a_2}{\sqrt{2}}|{+0}\rangle + \frac{a_1+a_3}{\sqrt{2}}|{+1}\rangle\right) \\
|\psi_2\rangle &= \frac{1}{c_2}\left(\frac{a_0-a_2}{\sqrt{2}}|{-0}\rangle + \frac{a_1-a_3}{\sqrt{2}}|{-1}\rangle\right) \\
c_1 &= \frac{1}{\sqrt{2}}\sqrt{|a_0+a_2|^2+|a_1+a_3|^2} \\
c_2 &= \frac{1}{\sqrt{2}}\sqrt{|a_0-a_2|^2+|a_1-a_3|^2}
\end{aligned}
$$

Example 2

If we consider the Bell Basis state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, then $a_0 = \frac{1}{\sqrt{2}} = a_3$ and $a_1 = 0 = a_2$. So we have $c_1 = \frac{1}{\sqrt{2}} = c_2$ and

$$\begin{aligned} |\psi_1\rangle &= \frac{1}{\sqrt{2}}(|+0\rangle + |+1\rangle) \\ |\psi_2\rangle &= \frac{1}{\sqrt{2}}(|-0\rangle - |-1\rangle) \\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}}|\psi_1\rangle + \frac{1}{\sqrt{2}}|\psi_2\rangle \end{aligned}$$

Example 2

The result of the measurement on first qubit of the Bell basis $|\Phi^+\rangle$ is

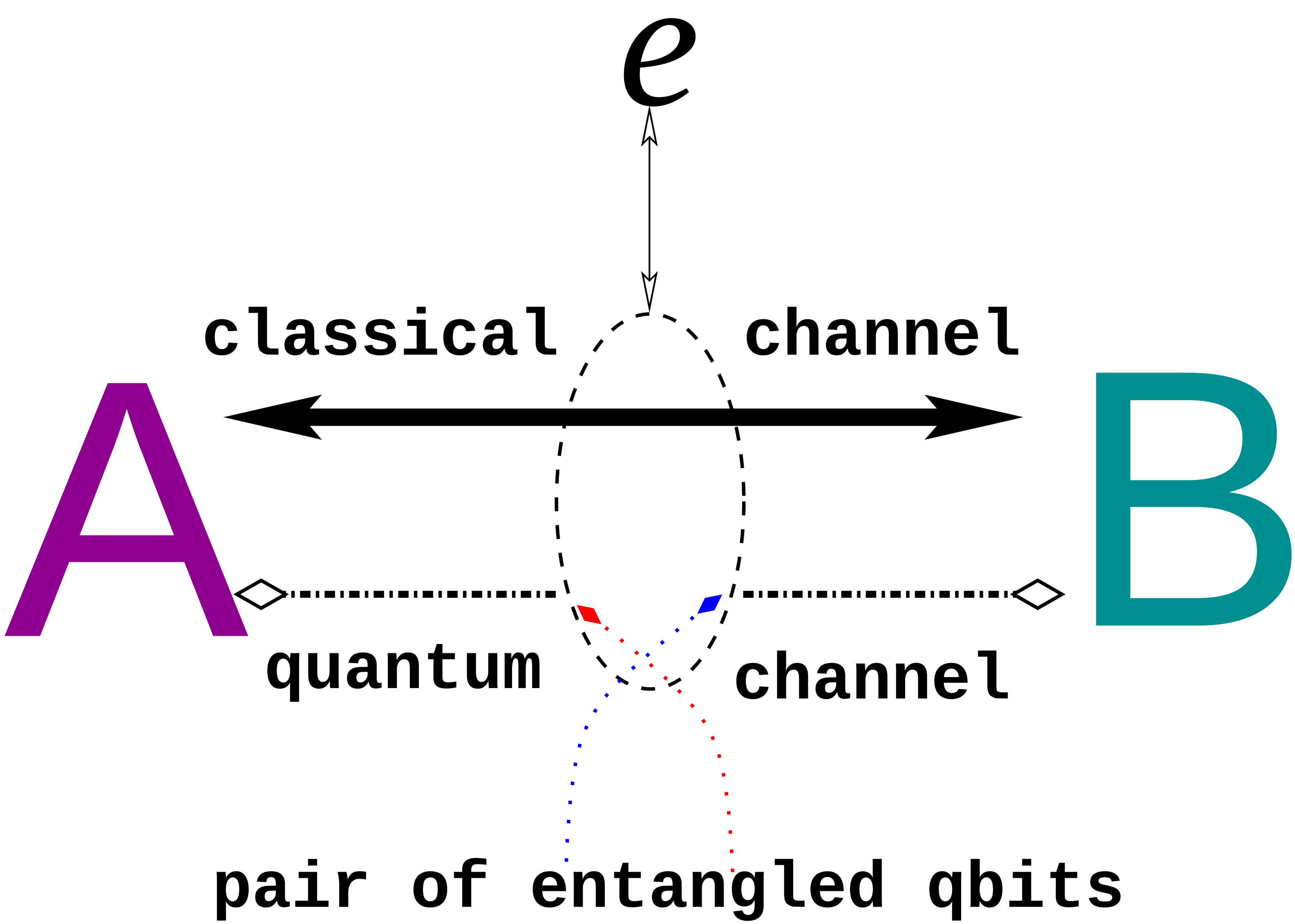
$$
\begin{aligned}
&= \frac{1}{2}(|{+0}\rangle + |{+1}\rangle + |{-0}\rangle - |{-1}\rangle) \\
&= \frac{1}{2\sqrt{2}}[|+\rangle \otimes (|+\rangle + |-\rangle) + |+\rangle \otimes (|+\rangle - |-\rangle) + \\
&\quad |-\rangle \otimes (|+\rangle + |-\rangle) - |-\rangle \otimes (|+\rangle - |-\rangle)]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

The state is still entangled.

Eckert 91

A symmetric key distribution protocol using entangled pair of qubits was proposed by A K Eckert in 1991.

Quantum cryptography based on Bell's theorem, Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661 - 663


e
classical
channel
A
B
quantum
channel
pair of entangled qbits

Eckert 91

1. A sequence of qubit pairs are generated. Each pair is at the state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
2. The first qubit is sent to Alice and the second qubit is sent to Bob on quantum channels.
3. For each qubit they choose randomly either the standard basis or the Hadamard basis for measurement.

Eckert 91

4. After the measurement, they compare the bases. If the bases are not identical, the bit is discarded.

Eckert 91

- If they use the standard base and Alice gets $|0\rangle$ then the state of the entangled pair is $|00\rangle$. So Bob also gets $|0\rangle$ and both of them interpret this as bit 0.
- If they use the Hadamard base and Alice gets $|+\rangle$, the state of the pair is $|++\rangle$. So Bob also gets $|+\rangle$ and both interpret it as bit 0.

Eckert 91

Alice and Bob need to ensure that the qubit pairs are indeed in the state $|\Phi^+\rangle$. That test uses Bell's inequalities.

References

[ERWP] *Quantum Computing: A Gentle Introduction* by Eleanor Rieffel & Wolfgang Polak, Pub. MIT Press, 2011, ISBN 978-0-262-52667-8.

[MNIC] *Quantum Computation and Quantum Information* by Michael A Nielsen & Isaac L Chuang, Pub. Cambridge University Press, 2002, ISBN 81-7596-092-2.

[SA] *Quantum Computing Since Democritus* by Scott Aaronson, Pub. Cambridge University Press, 2013, ISBN 978-0-521-19956-8.

[AAM] *Classical and Quantum Computation* by A Yu Kitaev, A H Shen & M N Vyalyi, Pub. American Mathematical Society (GSM vol 47) 2002, ISBN 978-1-4704-0927-2.

References

[PRM] *An Introduction to Quantum Computing* by Phillip Kaye, Raymond Laflamme & Michele Mosca, Pub. Oxford University Press, 2007, ISBN 978-0-19-923677-0.