Quantum Computation

(The computational model)

Luís Soares Barbosa

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

UNITED NATIONS UNIVERSITY UNU-EGOV

MFES - Arquitectura e Cálculo

March 2019

Qubits

$$|v\rangle = \alpha|u\rangle + \beta|u'\rangle$$

In a sense $|u\rangle$ can be thought as being simultaneously in both states, but be careful: states that are combinations of basis vectors in similar proportions but with different amplitudes, e.g.

$$\frac{1}{\sqrt{2}}(|u\rangle + |u'\rangle) \quad \text{and} \quad \frac{1}{\sqrt{2}}(|u\rangle - |u'\rangle)$$

are distinct and behave differently in many situations.

Amplitudes are not real (e.g. probabilities) that can only increase when added, but complex so that they can cancel each other or lower their probability

The state space of a qubit

Representation redundancy:

qubit state space $\neq$ complex vector space used for representation

Global phase

Unit vectors equivalent up to multiplication by a complex number of modulus one, i.e. a phase $e^{i\theta}$, represent the same state.

Let

$$|v\rangle = \alpha|u\rangle + \beta|u'\rangle$$

$$|e^{i\theta}\alpha|^2 = (\overline{e^{i\theta}\alpha})(e^{i\theta}\alpha) = (e^{-i\theta}\overline{\alpha})(e^{i\theta}\alpha) = \overline{\alpha}\alpha = |\alpha|^2$$

and similarly for β.

As the probabilities $|\alpha|^2$ and $|\beta|^2$ are the only measurable quantities, the global phase has no physical meaning.

The state space of a qubit

Relative phase

Is a measure of the angle between the two complex numbers α and β, cf

$$\frac{1}{\sqrt{2}}(|u\rangle + |u'\rangle) \quad \frac{1}{\sqrt{2}}(|u\rangle - |u'\rangle) \quad \frac{1}{\sqrt{2}}(e^{i\theta}|u\rangle + |u'\rangle)$$

... cannot be discarded!

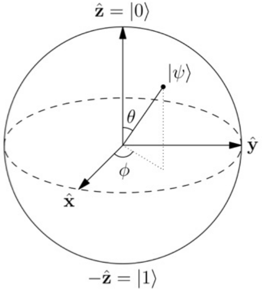
Projective space representation

There is a bijective correspondence between the state space of a qubit and the complex projective space of dimension 1, which can be explored in several ways.

The Bloch sphere

A latitude (ϕ) and longitude (θ) representation

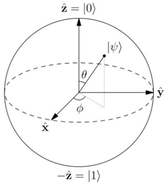
The Bloch sphere



$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

where $0 \leq \theta \leq \pi$, $0 \leq \phi \leq 2\pi$
Numbers θ and ϕ define a point on the surface of the sphere.

The Bloch sphere



- The poles represent the classical bits. In general, orthogonal states correspond to antipodal points and every diameter to a basis for the single-qubit state space.
- Once measured a qubit collapses to one of the two poles. Which pole depends exactly on the arrow direction: The angle θ measures that probability: If the arrow points at the equator, there is 50-50 chance to collapse to any of the two poles.
- Rotating a vector wrt the z-axis results into a *phase change* (ϕ), and does not affect which state the arrow will collapse to, when measured.

The Bloch sphere

Representing $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Express $|\psi\rangle$ in polar form

$$|\psi\rangle = \rho_1 e^{i\phi_1}|0\rangle + \rho_2 e^{i\phi_2}|1\rangle$$

and eliminate one of the four real parameters multiplying by $e^{-i\phi_1}$

$$|\psi\rangle = \rho_1|0\rangle + \rho_2 e^{i(\phi_2-\phi_1)}|1\rangle = \rho_1|0\rangle + \rho_2 e^{i\phi}|1\rangle$$

making $\phi = \phi_2 - \phi_1$.

Switch back the coefficient of $|1\rangle$ to Cartesian coordinates and compute the normalization constraint

$$|\rho_1|^2 + |a+ib|^2 \; = \; |\rho_1|^2 + (a-ib)(a+ib) \; = \; |\rho_1|^2 + a^2 + b^2 \; = \; 1$$

which is the equation of a unit sphere in Real 3-dim space with Cartesian coordinates: (a, b, ρ_1).

The Bloch sphere

Back to polar,

$$\begin{aligned} x =& \rho \sin\theta \cos\phi \\ y =& \rho \sin\theta \sin\phi \\ z =& \rho \cos\theta \end{aligned}$$

So, recalling that $\rho = 1$,

$$\begin{aligned} |\psi\rangle &= z|0\rangle + (a + ib)|1\rangle \\ &= \cos\theta|0\rangle + \sin\theta(\cos\phi - i\sin\phi)|1\rangle \\ &= \cos\theta|0\rangle + e^{i\phi}\sin\theta|1\rangle \end{aligned}$$

which, with two parameters, defines a point in the sphere's surface.

The Bloch sphere

Actually, one may just focus on the upper hemisphere ($0 \leq \theta' \leq \frac{\pi}{2}$) as opposite points in the lower one differ only by a phase factor of -1:

Let $|\psi'\rangle$ be the opposite point on the sphere with polar coordinates $(1, \pi - \theta', \phi + \pi)$

$$\begin{aligned} |\psi'\rangle &= \cos(\pi - \theta')|0\rangle + e^{i(\phi+\pi)} \sin(\pi - \theta')|1\rangle \\ &= -\cos\theta'|0\rangle + e^{i\phi} e^{i\pi} \sin\theta'|1\rangle \\ &= -\cos\theta'|0\rangle + e^{i\phi} \sin\theta'|1\rangle \\ &= -|\psi\rangle \end{aligned}$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

where $0 \leq \theta \leq \pi$, $0 \leq \phi \leq 2\pi$

The mathematical framework

Complex, inner-product vector space

A set U of vectors generates a complex vector space whose elements can be written as linear combinations of vectors in U:

$$|v\rangle = a_1|u_1\rangle + a_2|u_2\rangle + \cdots + a_n|u_n\rangle$$

i.e.

- Abelian group $(V, +, -^1, 0)$
- with scalar multiplication ($c \cdot |v\rangle$ distributing over $+$, often represented by juxtaposition)

The mathematical framework

- A inner product $\langle - | - \rangle : V \times V \longrightarrow \mathbb{C}$ such that

$$
\begin{array}{ll}
(1) & \langle v | \sum_i \lambda_i \cdot |w_i\rangle\rangle \; = \; \sum_i \lambda_i \langle v | w_i \rangle \\
(2) & \langle v | w \rangle = \overline{\langle w | v \rangle} \\
(3) & \langle v | v \rangle \geq 0 \;\; (\text{with equality iff } |v\rangle = 0)
\end{array}
$$

Note: $\langle - | - \rangle$ is conjugate linear in the first argument:

$$\langle \sum_i \lambda_i \cdot |w_i\rangle | v \rangle \; = \; \sum_i \overline{\lambda_i} \langle w_i | v \rangle$$

Notation: $\langle v | w \rangle \; \equiv \; \langle v, w \rangle \equiv (|v\rangle, |w\rangle)$

The mathematical framework

Old friends

- $|v\rangle$ and $|w\rangle$ are orthogonal if $\langle v|w\rangle = 0$
- norm: $\||v\rangle| = \sqrt{\langle v|v\rangle}$
- normalization: $\frac{|v\rangle}{\||v\rangle|}$
- $|v\rangle$ is a unit vector if $\||v\rangle| = 1$
- A set of vectors $\{|i\rangle, |j\rangle, \cdots,\}$ is orthonormal if each $|i\rangle$ is a unit vector and

$$\langle i|j\rangle \;=\; \delta_{i,j} \;=\; \begin{cases} i = j & \Rightarrow 1 \\ \text{otherwise} & \Rightarrow 0 \end{cases}$$

Note

A basis for V (set of linearly independent elements of V spanning V) will usually be taken as orthonormal.

The mathematical framework

$\mathcal{C}^n$

The inner product in $\mathcal{C}^n$ of two vectors over the same orthonormal basis boils down to vector multiplication:

$$\begin{aligned}
\langle v|w\rangle &= \langle \sum_i v_i \,|i\rangle| \sum_j w_j \,|j\rangle\rangle \\
&= \sum_{i,j} \overline{v_i} w_j \delta_{i,j} \\
&= \sum_i \overline{v_i} w_i \\
&= \begin{bmatrix} \overline{v_1} \cdots \overline{v_n} \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}
\end{aligned}$$

The mathematical framework

Matrices as linear maps

Any $m \times n$ matrix M can be seen as a linear operator mapping vectors in $\mathcal{C}^n$ to vectors in $\mathcal{C}^m$. Linearity means that

$$M\left(\sum_j \alpha_j |v_j\rangle\right) = \sum_j \alpha_j M |v_j\rangle$$

holds, where the action of M in a m-dimensional vector corresponds to multiplication.

Examples: The Pauli matrices

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

The mathematical framework

Linear maps as matrices

Let V and W be vector spaces with basis, respectively,

$$B_V = \{|v_1\rangle, \cdots, |v_n\rangle\} \quad \text{and} \quad B_W = \{|w_1\rangle, \cdots, |w_m\rangle\}$$

A linear operator, i.e. a map $M : V \longrightarrow W$ st

$$M\left(\sum_j \alpha_j \, |v_j\rangle\right) = \sum_j \alpha_j \, M(|v_j\rangle)$$

can be represented by a $m \times n$ matrix st, for each $j \in 1..n$,

$$M(|v_j\rangle) = \sum_i M_{i,j} \, |w_i\rangle$$

Composition of linear operators amounts to multiplication of the corresponding matrices.
This representation is, of course, basis dependent.

The mathematical framework

Hilbert spaces

Complete, complex, inner-product vector space, complete meaning that any Cauchy sequence

$$|v_1\rangle, |v_2\rangle, \cdots$$

converges

$$\forall_{\epsilon>0}\ \exists_N\ \forall_{m,n>0}\ \ \| v_m\rangle, |v_n\rangle| \leq \epsilon$$

This completeness condition is trivial in finite dimensional vector spaces

Classical systems

State spaces in a classical system combine through direct sum:

$\boxed{n \text{ 2-dimensional vector} \quad \rightsquigarrow \quad \text{a vector in } 2n\text{-dimensional vector space}}$

Direct sum $V \oplus W$

- $B_{V \oplus W} = B_V \cup B_W$ and $\dim(V \oplus W) = \dim(V) + \dim(W)$
- Vector addition and scalar multiplication are performed in each component and the results added
- $\langle (|u_2\rangle \oplus |z_2\rangle) | (|u_1\rangle \oplus |z_1\rangle) \rangle \;=\; \langle u_2|u_1\rangle + \langle z_2|z_1\rangle$
- V and W embed canonically in $V \oplus W$ and the images are orthogonal under the standard inner product

Example

$$\begin{bmatrix} a \\ b \end{bmatrix} \oplus \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

Quantum systems

State spaces in a classical system combine through tensor:

$$\boxed{n \text{ 2-dimensional vector} \quad \rightsquigarrow \quad \text{a vector in } 2^n\text{-dimensional vector space}}$$

i.e. the state space of a quantum system grows exponentially with the number of particles: Feyman's original motivation

Tensor $V \otimes W$

- $B_{V \otimes W}$ is a set of elements of the form $|v_i\rangle \otimes |w_j\rangle$, for each $|v_i\rangle \in B_V$, $|w_i\rangle \in B_W$ and $\dim(\mathrm{V} \otimes \mathrm{W}) = \dim(\mathrm{V}) \times \dim(\mathrm{W})$
- $(|u_1\rangle + |u_2\rangle) \otimes |z\rangle \;=\; |u_1\rangle \otimes |z\rangle + |u_2\rangle \otimes |z\rangle$
- $|z\rangle \otimes (|u_1\rangle + |u_2\rangle) \;=\; |z\rangle \otimes |u_1\rangle + |z\rangle \otimes |u_2\rangle$
- $(\alpha|u\rangle) \otimes |z\rangle \;=\; |u\rangle \otimes (\alpha|z\rangle) \;=\; \alpha(|u\rangle \otimes |z\rangle)$
- $\langle(|u_2\rangle \otimes |z_2\rangle)|(|u_1\rangle \otimes |z_1\rangle)\rangle \;=\; \langle u_2|u_1\rangle\langle z_2|z_1\rangle$

Assembling through $\otimes$

Clearly, every element of $V \otimes W$ can be written as

$$\alpha_1(|v_1\rangle \otimes |w_1\rangle) + \alpha_2(|v_2\rangle \otimes |w_1\rangle) + \cdots + \alpha_{nm}(|v_n\rangle \otimes |w_m\rangle)$$

Example

The basis of $V \otimes W$, for V, W qubits with the standard basis is

$$\{|0\rangle \otimes |1\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$$

Thus, the tensor of $\alpha_1|0\rangle + \beta_1|1\rangle$ and $\alpha_2|0\rangle + \beta_2|1\rangle$

$$\alpha_1\alpha_2|0\rangle \otimes |0\rangle \ + \ \alpha_1\beta_2|0\rangle \otimes |1\rangle \ + \ \alpha_2\beta_1|1\rangle \otimes |0\rangle \ + \ \alpha_2\beta_2|1\rangle \otimes |1\rangle$$

In a simplified notation

$$\alpha_1\alpha_2|00\rangle \ + \ \alpha_1\beta_2|01\rangle \ + \ \alpha_2\beta_1|10\rangle \ + \ \alpha_2\beta_2|11\rangle$$

Assembling through $\otimes$

Notation

Writing in a more familiar matrix notation requires fixing an ordering for the basis of the tensor product space; typically the lexicographic ordering

Example

Let $|u\rangle = \frac{1}{\sqrt{5}}\left[1, -2\right]^T$ and $|z\rangle = \frac{1}{\sqrt{10}}\left[-1, 3\right]^T$. Then

$$|u\rangle \otimes |z\rangle \ = \ \frac{1}{5\sqrt{2}}\left[-1, 3, 2, -6\right]^T$$

Assembling through $\otimes$

Other basis

... besides the standard one:

Bell basis

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

Assembling through $\otimes$

Representation

- As before, vectors that differ only in a global phase represent the same quantum state
- but also the same phase factor in different qubits of a tensor product represent the same state:

$$|u\rangle \otimes (e^{i\Phi}|z\rangle) \ = \ e^{i\Phi}(|u\rangle \otimes |z\rangle) \ = \ (e^{i\Phi}|u\rangle) \otimes |z\rangle$$

Actually, phase factors in qubits of a single term of a superposition can always be factored out into a coefficient for that term, i.e. phase factors distribute over tensors.

Assembling through $\otimes$

Representation

- Relative phases still matter (of course!)

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad \text{differs from} \quad \frac{1}{\sqrt{2}}(e^{i\Phi}|00\rangle + |11\rangle)$$

  even if

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

- Redundancy: the quantum state space of a n-qubit system has 2^{n-1} complex dimensions
- The complex projective space of dimension 1 (depicted in the Block sphere) generalises to higher dimensions, although in practice linearity makes vector spaces easier to use.

Entanglement

Most states in $V \otimes W$ cannot be written as $|u\rangle \otimes |z\rangle$

- A single-qubit state can be specified by a single complex number so any tensor product of n qubit states can be specified by n complex numbers. But it takes $2^n - 1$ complex numbers to describe states of an n qubit system.
- Since $2^n \gg n$, the vast majority of n-qubit states cannot be described in terms of the state of n separate qubits.
- Such states, that cannot be written as the tensor product of n single-qubit states, are entangled states.

Entanglement

Example

The Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled

Actually, to make $|\Phi^+\rangle$ equal to

$$(\alpha_1|0\rangle+\beta_1|1\rangle)\otimes(\alpha_2|0\rangle+\beta_2|1\rangle) \;=\; \alpha_1\alpha_2|00\rangle+\alpha_1\beta_2|01\rangle+\beta_1\alpha_2|10\rangle+\beta_1\beta_2|11\rangle$$

would require that $\alpha_1\beta_2 = \beta_1\alpha_2 = 0$ which implies that either $\alpha_1\alpha_2 = 0$ or $\beta_1\beta_2 = 0$.

Note

Entanglement can also be observed in simpler structures, e.g. relations:

$$\{(a,a),(b,b)\} \subseteq A \times A$$

cannot be separated, i.e. written as a Cartesian product of subsets of A.

Entanglement

The notion of entanglement

- is not basis dependent
- but depends on the tensor decomposition used

Example.

$$u = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)$$

is entangled wrt the decomposition into single qubits, since it cannot be expressed as the tensor product of four single-qubit states, but it is not for a decomposition consisting of a subsystem of the first and third qubit and another with the second and fourth qubit:

$$u = \frac{1}{\sqrt{2}}(|0_1 0_3\rangle + |1_1 1_3\rangle) \otimes \frac{1}{\sqrt{2}}(|0_2 0_4\rangle + |1_2 1_4\rangle)$$

Measuring composed states

Recalling the single-qubit case

Every measuring tool has an associated orthonormal basis $\{|v_1\rangle, |v_2\rangle\}$ for the vector space V associated with the single-qubit system.

Each basis vector $|v_i\rangle$ generates a one-dimensional subspace S_i consisting of all multiples $\alpha|v_i\rangle$, where α is a complex number, and $V = S_1 \oplus S_2$, the direct sum decomposition of V.

Example

A measuring tool for a qubit in the standard basis has $V = S_1 \oplus S_2$ as the associated direct sum decomposition, where S_1 is generated by $|0\rangle$ and S_2 by $|1\rangle$.
State $|u\rangle = \alpha|0\rangle + \beta|1\rangle$ will be $|0\rangle$ with probability $|\alpha|^2$, the amplitude of $|u\rangle$ in the subspace S_1, and $|1\rangle$ with probability $|\beta|^2$.

Measuring composed states

The n-qubit case

To every measuring tool corresponds a direct sum decomposition

$$V = S_1 \oplus S_2 \oplus \cdots \oplus S_k$$

of the 2^n dimensional vector space V, for some $k \leq 2^n$ standing for the maximum number of outcomes for a states measured with that toll

Measuring composed states

Example: First qubit of a 2-qubit system with SB

$$V = S_1 \oplus S_2$$

- $S_1 = |0\rangle \otimes V_2$, the 2-dim subspace spanned by $\{|00\rangle, |01\rangle\}$
- $S_2 = |1\rangle \otimes V_2$, the 2-dim subspace spanned by $\{|10\rangle, |11\rangle\}$

To measure

$$|u\rangle \; = \; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

$$|u\rangle \; = \; \gamma_1|s_1\rangle + \gamma_2|s_2\rangle$$

$$\gamma_1 = \sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2} \qquad |s_1\rangle = \frac{1}{\gamma_1}(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle)$$

$$\gamma_2 = \sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2} \qquad |s_1\rangle = \frac{1}{\gamma_2}(\alpha_{10}|10\rangle + \alpha_{11}|11\rangle)$$

Dirac's notation

Dirac's bra/ket notation is a handy way to represent elements and constructions on an Hilbert space, amenable to calculations and with direct correspondence to diagrammatic (categorial) representations of process theories

$|u\rangle$ A ket stands for a vector in an Hilbert space V. In $\mathcal{C}^n$, a column vector of complex entries. The identity for $+$ (the zero vector) is just written 0.

$\langle u|$ A bra is a vector in the dual space $V^\dagger$, i.e. scalar-valued linear maps in V — a row vector in $\mathcal{C}^n$.

There is a bijective correspondence between $|u\rangle$ and $\langle u|$

$$|u\rangle = \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \Leftrightarrow \begin{bmatrix} \overline{u}_1 \cdots \overline{u}_n \end{bmatrix} = \langle u|$$

A tradition going back to Penrose in the 1970's.

Dirac's notation

Dirac's bra/ket notation provides a convenient way of specifying linear transformations on quantum states:

outer product

$$|w\rangle\langle u|\,(|z\rangle) \;\widehat{=}\; |w\rangle\langle u||z\rangle \;=\; |w\rangle\,\langle u|z\rangle \;=\; \langle u|z\rangle\,|w\rangle$$

- matrix multiplication (composition of linear maps) is associative and scalars (zero objects in the corresponding universe) commute with everything

Dirac's notation

Example: $|0\rangle\langle 1|$

$|0\rangle\langle 1|$ maps $|1\rangle \mapsto |0\rangle$ and $|0\rangle \mapsto 0$

$$\begin{aligned} |0\rangle\langle 1|\,|1\rangle &= |0\rangle\,\langle 1|1\rangle = |0\rangle\,1 = |0\rangle \\ |0\rangle\langle 1|\,|0\rangle &= |0\rangle\,\langle 1|0\rangle = |0\rangle\,0 = 0 \end{aligned}$$

Using matrices:

$$|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

Dirac's notation

Example: $X = |0\rangle\langle 1| + |1\rangle\langle 0|$

$$|0\rangle\langle 1| + |1\rangle\langle 0| \left(|0\rangle\right) = |0\rangle\langle 1| \left(|0\rangle\right) + |1\rangle\langle 0| \left(|0\rangle\right) = 0 + |1\rangle = |1\rangle$$
$$|0\rangle\langle 1| + |1\rangle\langle 0| \left(|1\rangle\right) = |0\rangle\langle 1| \left(|1\rangle\right) + |1\rangle\langle 0| \left(|1\rangle\right) = |0\rangle + 0 = |0\rangle$$

represented by the following matrix in the standard basis:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Example: $|10\rangle\langle 00| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01|$
Maps $|00\rangle \mapsto |01\rangle$ and $|01\rangle \mapsto |00\rangle$
Clearly,

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Dirac's notation

An operator on an n-qubit system that maps the basis vector $|j\rangle$ to $|i\rangle$ and all other standard basis elements to 0 can be expressed in the standard basis as

$$O = |i\rangle\langle j|$$

Matrix for O has a single non-zero entry 1 in the i, j place.

A general operator A with entries a_{ij} in the standard basis can be written

$$A = \sum_i \sum_j a_{ij} |i\rangle\langle j|$$

Conversely, the i, j entry of the matrix for A in the standard basis is given by

$$\langle i|A|j\rangle$$

Dirac's notation

Example

Let $|s\rangle = \sum_k \beta_k |k\rangle$.

$$
\begin{aligned}
A|s\rangle &= \left(\sum_i \sum_j a_{ij} \, |i\rangle\langle j| \right) \left(\sum_k \beta_k |k\rangle \right) \\
&= \sum_i \sum_j \sum_k a_{ij} \, \beta_k \, |i\rangle\langle j| \, |k\rangle \\
&= \sum_i \sum_j a_{ij} \, \beta_j \, |i\rangle
\end{aligned}
$$

Dirac's notation

In general, given a basis $B_V = \{|\beta_i\rangle\}$ for a N-dimensional Hilbert space V, an operator

$$A : V \longrightarrow V$$

can be written as

$$\sum_i \sum_j b_{ij} \, |\beta_i\rangle\langle\beta_j|$$

wrt this basis. The matrix entries are b_{ij}, as expected.

The Dirac's notation is

- independent of the basis and the order of the basis elements
- more compact
- and builds up intuitions ...

Projectors

$$V = S \oplus S^{\dagger}$$

Any vector $|v\rangle$ can be written uniquely as the sum of a vector $\vec{s_1}$ from S_1 and $\vec{s_2}$ from S_2 (not unit vectors in the general case)

Projector

$$\mathrm{P}_S : V \longrightarrow S \quad \text{st} \quad |v\rangle = \vec{s_1} + \vec{s_2} \;\mapsto\; \vec{s_1}$$

Example $|u\rangle\langle u|$ is the projector onto the subspace spanned by $|u\rangle$.

A measuring tool with associated decomposition

$$V = \bigoplus_i S_i$$

into ortogonal subspaces S_i, acting over a state $|v\rangle$ produces, with probability $|\mathrm{P}_i|v\rangle|^2$, a state

$$\frac{\mathrm{P}_i|v\rangle}{|\mathrm{P}_i|v\rangle|}$$

Projectors

Example Let $|v\rangle = \alpha|0\rangle + \beta|1\rangle$. Projector $|0\rangle\langle 0|$ obtains its component in the subspace generated by $|0\rangle$, i.e.

$$|0\rangle\langle 0|\,(|v\rangle) \;=\; \alpha|0\rangle\langle 0||0\rangle + \beta|0\rangle\langle 0||1\rangle \;=\; \alpha|0\rangle$$

Similarly, projector $|10\rangle\langle 10|$ acts on a two-qubit state

$$v \;=\; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

yielding

$$|10\rangle\langle 10|\,(|v\rangle) \;=\; \alpha_{10}|10\rangle$$

and

$$|00\rangle\langle 00| + |10\rangle\langle 10|(|v\rangle) \;=\; \alpha_{00}|00\rangle + \alpha_{10}|10\rangle$$

Projectors are self-adjoint

Adjoint operator

Operator $O^\dagger : U \longrightarrow V$ is adjoint to $O : V \longrightarrow U$ if, for any vectors from V and U, the inner product between $O^\dagger(\vec{u})$ and $\vec{v}$ coincides with the inner product between $\vec{u}$ and $O(\vec{v})$. In Dirac's notation,

$$(\langle u|O)\,|v\rangle \;=\; \langle u|\,(O|v\rangle) \;=\; \langle u|O|v\rangle$$

recalling that $(O|v\rangle)^\dagger = \langle v|\,O^\dagger$.

Clearly, the matrix representation of $O^\dagger$ is the conjugate transpose of that of O

Clearly, $\mathsf{P}\mathsf{P} = \mathsf{P}$ (why?), which combined with $\mathsf{P}^\dagger = \mathsf{P}$, yields

$$|\mathsf{P}|v\rangle|^2 \;=\; (\langle v|\mathsf{P}^\dagger)(\mathsf{P}|v\rangle) \;=\; \langle v|P|v\rangle$$

Projectors

Example

Let $|v\rangle = \alpha|0\rangle + \beta|1\rangle$.
Applying projector $P_0 = |0\rangle\langle 0|$ to $|v\rangle$ results in the state

$$\frac{P_0|v\rangle}{|P_0|v\rangle|^2} = \frac{\alpha|0\rangle}{|\alpha|} \sim |0\rangle$$

where

$$P_0|v\rangle = (|0\rangle\langle 0|)|v\rangle = |0\rangle\langle 0|v\rangle = \alpha|0\rangle$$

with probability

$$|P_0|v\rangle|^2 = \langle v|P_0|v\rangle = \langle v||0\rangle\langle 0||v\rangle = \langle v|0\rangle \langle 0|v\rangle = \overline{\alpha}\alpha = |\alpha|^2$$

Projectors

Example: measuring up to (bit equality)

$$V = S_e \oplus S_n$$

with S_e the subspace generated by $\{|00\rangle, |11\rangle\}$ in which the two bits are equal, and S_n its complement.

When measuring

$$v \;=\; \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with this device, yields a state in which the two bit values are equal with probability

$$\langle v|\mathrm{P}_e|v\rangle \;=\; (\sqrt{|\alpha_{00}|^2 + |\alpha_{11}|^2})^2 \;=\; |\alpha_{00}|^2 + |\alpha_{11}|^2$$

Of course, the measurement does not determine the value of the two bits, only whether the two bits are equal

Hermitian operators

Can the explicit decomposition be avoided?

Hermitian operators

- define a unique orthogonal subspace decomposition, their eigenspace decomposition, and
- for every such decomposition, there exists a corresponding Hermitian operator whose eigenspace decomposition coincides with it

Hermitian operators

$O : V \longrightarrow V$ is Hermitian if

$$O^\dagger = O$$

The relevant property is that, for every eigenvalue λ with eigenvector $|l\rangle$, $\lambda = \overline{\lambda}$, and thus all eigenvalues of a Hermitian operator are real, because

$$\lambda\langle l|l\rangle = \langle l|\lambda|l\rangle = \langle l|\left(O|l\rangle\right) = \left(\langle l|O^\dagger\right)|l\rangle = \left(O|l\rangle\right)^\dagger|l\rangle = \left(\lambda|l\rangle\right)^\dagger|l\rangle = \overline{\lambda}\langle l|l\rangle$$

Hermitian operators

Orthogonality

For any O, two distinct eigenvalues have disjoint eigenspaces, because, for any unit vector $|v\rangle$,

$$O|v\rangle = \lambda|v\rangle \text{ and } O|v\rangle = \lambda'|v\rangle \text{ and } (\lambda - \lambda')|v\rangle = 0$$

and thus $\lambda = \lambda'$.

For any Hermitian O, the eigenvectors for distinct eigenvalues must be orthogonal, because

$$\lambda\langle v|w\rangle \;=\; (\langle v|O^\dagger)\,|w\rangle \;=\; \langle v|\,(O|w\rangle) \;=\; \mu\langle v|w\rangle$$

for any pairs $(\lambda, |v\rangle), (\mu, |w\rangle)$ with $\lambda \neq \mu$.
Thus, $\langle v|w\rangle = 0$, because $\lambda \neq \mu$, and the corresponding subspaces are orthogonal.

Hermitian operators

Eigenspace decomposition of V for O

Any Hermitian O determines a unique decomposition for V

$$V = \oplus_{\lambda_i} S_{\lambda_i}$$

and any decomposition $V = \oplus_{i=1}^{k} S_i$ can be realized as the eigenspace decomposition of a Hermitian operator

$$O = \sum_i \lambda_i \mathrm{P}_i$$

where each P_i is the projector onto S_i and $L = \{\lambda_1, \cdots \lambda_k\}$ is a set of arbitrary, real k values

Hermitian operators

Thus, in a measurement, a subspace decomposition can be specified by a Hermitian operator

Note that the values in L are irrelevant — they are just labels for the corresponding subspaces, i.e. labels for the measurement outcomes.

Hermitian operators

The measurement postulate

- Any measurement is specified by a Hermitian operator O
- The possible outcomes of measuring a state $|v\rangle$ with O are labeled by the eigenvalues of O
- The probability of obtaining the outcome labelled by λ_i is

$$|\mathrm{P}_i|v\rangle|^2$$

- The state after measurement is the normalized projection

$$\frac{\mathrm{P}_i|v\rangle}{|\mathrm{P}_i|v\rangle|}$$

onto the λ_i-eigenspace S_i. Thus, the state after measurement is a unit length eigenvector of O with eigenvalue λ_i

Hermitian operators

Notes

- A measurement is not modelled by the action of a Hermitian operator on a state, but of the corresponding projectors.
- Actually, Hermitian operators are only a bookeeping trick
- A Hermitian operator uniquely specifies a subspace decomposition
- For a given subspace decomposition there are many Hermitian operators whose eigenspace decomposition is that decomposition.

Hermitian operators

Example: Measuring a single qubit in the Hadamard basis

- Projectors:

$$
\begin{aligned}
P_{+} &= |+\rangle\langle+| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \\
P_{-} &= |-\rangle\langle-| = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|)
\end{aligned}
$$

- Hermitian:

$$
X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}
$$

for an arbitrary choice of $\lambda_{+} = 1$ and $\lambda_{-} = -1$

Hermitian operators

Example: Measuring of the first qubit in the standard basis

$$EB = |00\rangle\langle 00| + |01\rangle\langle 01| + \pi|10\rangle\langle 10| + |11\rangle\langle 11| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \pi & 0 \\ 0 & 0 & 0 & \pi \end{bmatrix}$$

specifies measurement of a two-qubit system with respect to the decomposition

$$V = \{|00\rangle, |01\rangle\} \oplus \{|10\rangle, |11\rangle\}$$

Exercise: What is the Hermitian for measuring bit equality?

Composing Hermitian operators

- $O_1 \otimes O_2$ is an Hermitian operator over space $V_1 \otimes V_2$ if each O_i is such over V_i.
- Its eigenvalues are the product of eigenvalues of the original operators, in multiple ways.
- However, most Hermitian operators O on $V_1 \otimes V_2$ cannot be written as a tensor product of two Hermitian operators acting separately in each space.

Composing Hermitian operators

but only if

each subspace in the subspace decomposition described by O can be written as $S = S_1 \otimes S_2$, for S_i the subspace decomposition associated to O_i

Example

$$Z \otimes Z \;=\; |00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11|$$

specifies the measurement for bit equality.

Composing Hermitian operators

Not all measurements are tensor products of single-qubit measurements
Example

$$O = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

O determines whether both bits are set to one. The result of a measurement with O is a state in the subspace spanned by

$$\{|11\rangle\} \text{ or by } \{|00\rangle, |01\rangle, |10\rangle\}$$

Composing Hermitian operators

Measuring with O is quite different from measuring both qubits in the standard basis and composing the results: e.g. state

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

is unchanged when measured by O.
Exercise: but what results from measuring both qubits?

Measurement

A Hermitian operator of the form

$$I \otimes \cdots \otimes O \otimes \cdots \otimes I$$

on a n-qubit system forms a single-qubit measurement of that system

Measurement operators in the standard basis, when combined with transformations, are sufficient to perform arbitrary quantum measurements.

In particular, all possible subspace decompositions of the state space can be obtained by starting with a subspace decomposition in which all of the subspaces are generated by standard basis vectors and transforming (because there are quantum operations taking any basis to any other)

Exercise: How many classical bits does a single measurement of an n-qubit system reveal?

Closed systems

... transformations that map the state space of the quantum system to itself

Exercise: Is measurement one of these transformations?

- All quantum transformations on n-qubit quantum systems can be expressed as a sequence of transformations on 1-qubit and 2-qubit subsystems.
- Efficiency of a quantum transform (quantified in terms of the number of 1- or 2-qubit gates used) will not be addressed here.

Unitary transformations

- All transformations are linear:

$$U(\alpha_1|v_1\rangle + \cdots + \alpha_k|v_k\rangle) \;=\; \alpha_1 U|v_1\rangle + \cdots + \alpha_2 U|v_k\rangle$$

- Unit length vectors map to unit length vectors, thus orthogonal subspaces map to orthogonal subspaces.

These properties hold iff U preserves inner product:

$$\langle v|U^\dagger U|w\rangle \;=\; \langle v|w\rangle$$

which entails

$$U^\dagger U \;=\; I \qquad\qquad U \text{ is unitary}$$

Unitary transformations

- Unitary operators map orthonormal bases to orthonormal bases, since they preserve the inner product
- Moreover, any linear transformation that maps an orthonormal basis to an orthonormal basis is unitary
- If given in matrix form, being unitary means that the set of columns of its matrix representation are orthonormal (because the ith column is the image of $U|i\rangle$).
- equivalently, rows are orthonormal (why?)

$\boxed{\text{Unitary transformations are reversible}}$

Unitary transformations

New transformations from old

Both $U_1 U_1$ and $U_1 \otimes U_2$ are unitary.

But linear combinations of unitary operators, however, are not in general unitary.

The no-cloning theorem

Linearity implies that quantum states cannot be cloned

Let $U(|a\rangle|0\rangle) = |a\rangle|a\rangle$ and consider state $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$ for $|a\rangle$ and $|b\rangle$ orthogonal. Then

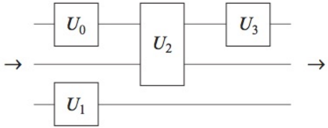
$$\begin{aligned} U(|c\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) \\ &= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle) \\ &\neq \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle) \\ &= |c\rangle|c\rangle \\ &= U(|c\rangle|0\rangle) \end{aligned}$$

This result, however, does not preclude the construction of a known quantum state from a known quantum state.

Quantum gates

A gate is a transformation that acts on only a small number of qubits
Differently from the classical case, they do not necessarily correspond to physical objects

Notation



Is there a complete set?

In general no: there are uncountably many quantum transformations, and a finite set of generators can only generate countably many elements.

However, it is possible for finite sets of gates to generate arbitrarily close approximations to all unitary transformations.

Quantum gates

Pauli gates

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X = |1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad Y = ZX = -|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

Hadamard gate

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

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The *CNOT* gate

Acts on the standard basis for a 2-qubit system, flipping the second bit if the first bit is 1 and leaving it unchanged otherwise.

$$
\begin{aligned}
CNOT &= |0\rangle\langle 0| \otimes I \;+\; |1\rangle\langle 1| \otimes X \\
&= |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) \;+\; |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) \\
&= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}
\end{aligned}
$$

CNOT is unitary and is its own inverse, and cannot be decomposed into a tensor product of two 1-qubit transformations

The $CNOT$ gate

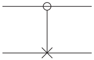
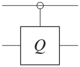
The importance of $CNOT$ is its ability to change the entanglement between two qubits, e.g.

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

Since it is its own inverse, it can take an entangled state to an unentangled one.
Note that entanglement is not a local property in the sense that transformations that act separately on two or more subsystems cannot affect the entanglement between those subsystems:

$$(U \otimes V)\,|v\rangle \quad \text{is entangled iff } |v\rangle \text{ is}$$

Generalising the *CNOT* gate

From  to 

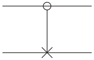
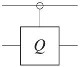
$$C_Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$$

In the standard basis

$$C_Q = \begin{bmatrix} 1 & 0 \\ 0 & Q \end{bmatrix}$$

Controlled phase shift gate

Changes the phase of the second bit iff the control bit is 1:

From  to 

$$e^{i\theta} = |00\rangle\langle 00| + |01\rangle\langle 01| + e^{i\theta}|10\rangle\langle 10| + e^{i\theta}|11\rangle\langle 11|$$

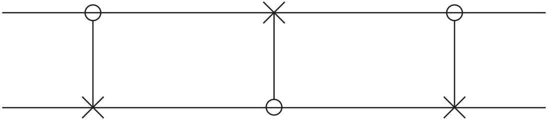
$$e^{i\theta} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$$

Transforming a global into a local phase

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

Exercise

Discuss



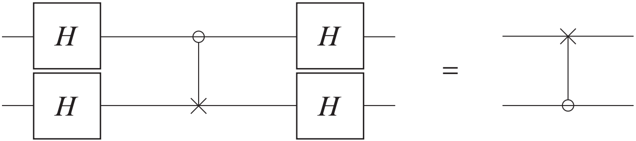
Notes

- A unitary transformation on the complex vector space is completely determined by its action on a basis, but not by specifying what states the states corresponding to basis states are sent to.
  Example: $e^{i\theta}$ takes the four quantum states to themselves (because $|10\rangle$ and $e^{i\theta}|10\rangle$ represent the same state, but a global phase can be transformed into a local one, as above).

- The notions of control/target bit depends on the basis.
  Example: Apply $CNOT$ in the Hadamard basis to get

$$|++\rangle \mapsto |++\rangle \quad |+-\rangle \mapsto |--\rangle \quad |-+\rangle \mapsto |-+\rangle \quad |--\rangle \mapsto |+-\rangle$$

and



Dense coding

Aim: encode and transmit two classical bits with one qubit and a shared EPR pair.

This result is surprising, since only one bit can be extracted from a qubit

The idea is that, since entangled states can be distributed ahead of time, only one qubit needs to be physically transmitted to communicate two bits of information.
Let Alice (Bob) be sent and operate the first (second) qubit of pair

$$|r\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

EPR pairs

... are entangled states
named after Einstein, Podolsky, and Rosen, from the *hidden-variable* controversy

Dense coding

Alice

wishes to transmit the state of two classical bits encoding one of the numbers 0 through 3. Depending on this number, Alice performs one of the Pauli transformations on her qubit of the entangled pair $|r\rangle$, and sends her qubit to Bob.

	Transformation	New state
0	$\|r\rangle = (I \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$\|r_1\rangle = (X \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$\|r_3\rangle = (Z \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
3	$\|r_3\rangle = (Y \times I)\|r\rangle$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$

Dense coding

Bob

to decode the information, applies a $CNOT$ to the two qubits of the entangled pair and then H to the first qubit:

$$CNOT \longrightarrow \begin{bmatrix} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) \\ \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \\ \frac{1}{\sqrt{2}}(-|11\rangle + |01\rangle) \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) \otimes |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(-|1\rangle + |0\rangle) \otimes |1\rangle \end{bmatrix}$$

$$H \otimes I \longrightarrow \begin{bmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{bmatrix}$$

Bob then measures the two qubits in the standard basis to obtain the 2-bit binary encoding of the number Alice wished to send

Teleportation

Aim: to transmit, using two classical bits, the state of a single qubit.

Surprisingly,

- shows that two classical bits suffice to communicate a qubit state (which has an infinite number of configurations)
- provides a mechanism for the transmission of an unknown quantum state (in spite of the no-cloning theorem)

Note that the original state cannot be preserved (precisely because of the no-cloning result), which motivates the name of the protocol ...

Teleportation

Alice

... has a qubit whose state $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ she does not know, but wants to send to Bob through classical channels.

The starting point is the 3-qubit state whose first 2 qubits are controlled by Alice and the last by Bob:

$$
\begin{aligned}
|v\rangle \otimes |r\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|00\rangle + |11\rangle)) \\
&= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)
\end{aligned}
$$

Teleportation

Alice

... then she applies $CNOT \otimes I$ and $H \otimes I \otimes I$ to obtain

$$
\begin{aligned}
& (H \otimes I \otimes I)(CNOT \otimes I)(|v\rangle \otimes |r\rangle) \\
= \; & (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle) \\
= \; & \frac{1}{2}\left(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)\right) \\
= \; & \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + \\
& + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))
\end{aligned}
$$

Teleportation

Alice

Alice measures the first two qubits and obtains one of the four standard basis states, $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, with equal probability.
Depending on the result of her measurement, the state of Bob's qubit is projected to

$$\alpha|0\rangle + \beta|1\rangle,\ \alpha|1\rangle + \beta|0\rangle,\ \alpha|0\rangle - \beta|1\rangle,\ \alpha|1\rangle - \beta|0\rangle$$

Then, Alice sends the result of her measurement as two classical bits to Bob.

After these transformations, crucial information about the original state $|v\rangle$ is contained in Bob's qubit, Alice's being destroyed ...

Teleportation

Bob

When Bob receives the two bits from Alice, he knows how the state of his half of the entangled pair compares to the original state of Alice's qubit.

Bob can reconstruct the original state of Alice's qubit, $|v\rangle$, by applying the appropriate decoding transformation to his qubit, originally part of the entangled pair.

Bits received	Bob's state	Transformation to decode
00	$\alpha\|0\rangle + \beta\|1\rangle$	I
01	$\alpha\|1\rangle + \beta\|0\rangle$	X
10	$\alpha\|0\rangle - \beta\|1\rangle$	Z
10	$\alpha\|1\rangle - \beta\|1\rangle$	Y

After decoding, Bob's qubit will be in the state Alice's qubit started.

Teleportation and dense coding are in some sense inverse protocols (why?)

A probabilistic machine

States: Given a set of possible configurations, states are vectors of probabilities in $\mathcal{R}^n$ which express indeterminacy about the exact physical configuration, e.g. $\left[p_0 \cdots p_n\right]^T$ st $\sum_i p_1 = 1$
Operator: double stochastic matrix (*must come (go) from (to) somewhere*), where $M_{i,j}$ specifies the probability of evolution from configuration j to i
Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current probabilities

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: the system is always in some configuration — if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$

A probabilistic machine

Composition:

$$p \otimes q \;=\; \begin{bmatrix} p_1 \\ 1-p_1 \end{bmatrix} \otimes \begin{bmatrix} q_1 \\ 1-q_1 \end{bmatrix} \;=\; \begin{bmatrix} p_1 q_1 \\ p_1(1-q_1) \\ (1-p_1)q_1 \\ (1-p_1)(1-q_1) \end{bmatrix}$$

- correlated states: cannot be expressed as $p \otimes q$, e.g.

$$\begin{bmatrix} 0.5 \\ 0 \\ 0 \\ 0.5 \end{bmatrix}$$

- Operators are also composed by $\otimes$ (Kronecker product):

$$M \otimes N \;=\; \begin{bmatrix} M_{1,1}N & \cdots & M_{1,n}N \\ \vdots & & \vdots \\ M_{m,1}N & \cdots & M_{m,n}N \end{bmatrix}$$

A quantum machine

States: given a set of possible configurations, states are unit vectors of (complex) amplitudes in $\mathcal{C}^n$
Operator: unitary matrix ($M^\dagger M = I$). The norm squared of a unitary matrix forms a double stochastic one.
Evolution: computed through matrix multiplication with a vector $|u\rangle$ of current amplitudes (wave function)

- $M|u\rangle$ (next state)
- $|u\rangle^T M^T$ (previous state)

Measurement: configuration i is observed with probability $|\alpha_i|^2$ if found in i, the new state will be a vector $|t\rangle$ st $t_j = \delta_{j,i}$
Composition: also by a tensor on the complex vector space; may exist entangled states

A quantum machine

Quantum computation

1. State preparation (fix initial setting)
2. Transform
3. Measure (projection onto a basis vector associated with a measurement tool)

To follow

- 11 April (whole day): Quantum algorithms (Grove, Shor) and hands-on session on IBM Q
- 12 April (whole day): Talks; dissertation pre-discussion

register until 31 March at `w3.math.uminho.pt/qdays2019`

- May: Quantum automata and processes