Quantum Processes

(The computational model)

Luís Soares Barbosa

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

UNITED NATIONS UNIVERSITY
UNU-EGOV

IC
May 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:

$$\text{qubit state space} \quad \neq \quad \text{complex vector space used for representation}$$

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!

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

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

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 $\dim(\mathrm{V} \oplus \mathrm{W}) = \dim(\mathrm{V}) + \dim(\mathrm{W})$
- 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

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

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:

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

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

$$|0\rangle\langle 1| + |1\rangle\langle 0| \,(|0\rangle) = |0\rangle\langle 1| \,(|0\rangle) + |1\rangle\langle 0| \,(|0\rangle) = 0 + |1\rangle = |1\rangle$$
$$|0\rangle\langle 1| + |1\rangle\langle 0| \,(|1\rangle) = |0\rangle\langle 1| \,(|1\rangle) + |1\rangle\langle 0| \,(|1\rangle) = |0\rangle + 0 = |0\rangle$$

represented by the following matrix in the standard basis:

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

Example: $|10\rangle\langle 11| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01|$

Maps $|00\rangle \mapsto |11\rangle$ and $|11\rangle \mapsto |00\rangle$

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 ...

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:

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

- 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

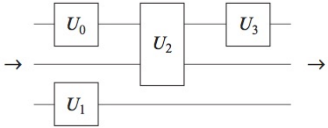
$$\begin{aligned}
U(|c\rangle|0\rangle) &= \frac{1}{\sqrt{2}}(U(|a\rangle|0\rangle) + U(|b\rangle|0\rangle)) \\
&= \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |b\rangle|b\rangle) \\
&\neq \frac{1}{\sqrt{2}}(|a\rangle|a\rangle + |a\rangle|b\rangle + |b\rangle|a\rangle + |b\rangle|b\rangle) \\
&= |c\rangle|c\rangle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

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

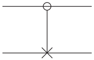
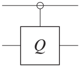
The importance of *CNOT* is its ability to change the entanglement between two qubits, e.g.

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

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 

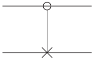
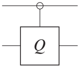
$$C_Q = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Q$$

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

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

A quantum machine

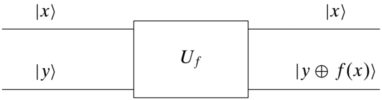
Structure of a quantum algorithm

1. State preparation (fix initial setting): typically the qubits in the initial classical state are put into a superposition of many states;
2. Transform, through unitary operators applied to the superposed state;
3. Measure, i.e. projection onto a basis vector associated with a measurement tool.

My first quantum program

$\boxed{\text{Is } f : \mathbf{2} \longrightarrow \mathbf{2} \text{ constant, with a unique evaluation?}}$

Oracle



where $\oplus$ stands for exclusive disjunction.

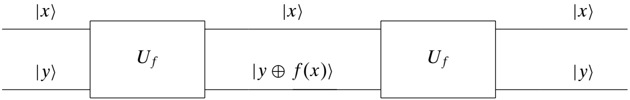
- The oracle takes input $|x, y\rangle$ to $|x, y \oplus f(x)\rangle$
- for $y = 0$ the output is $|x, f(x)\rangle$

My first quantum program

Is $f : \mathbf{2} \longrightarrow \mathbf{2}$ constant, with a unique evaluation?

Oracle

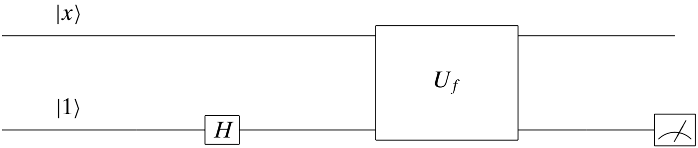
- The oracle is a unitary, i.e. reversible gate



$$|x, (y \oplus f(x)) \oplus f(x)\rangle \;=\; |x, y \oplus (f(x) \oplus f(x))\rangle \;=\; |x, y \oplus 0\rangle \;=\; |x, y\rangle$$

My first quantum program

Idea: Avoid double evaluation by superposition

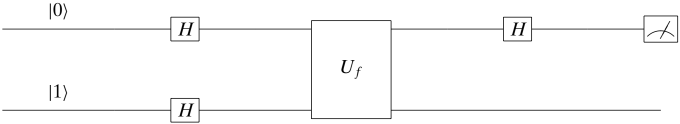


The circuit computes:

$$
\begin{aligned}
\text{output} &= |x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}} \\
&= \begin{cases} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} & \Leftarrow f(x) = 0 \\ |x\rangle \frac{|1\rangle - |2\rangle}{\sqrt{2}} & \Leftarrow f(x) = 1 \end{cases} \\
&= (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}
\end{aligned}
$$

My first quantum program

Idea: Avoid double evaluation by superposition



$$(H \otimes I)\, U_f\, (H \otimes H)(|01\rangle)$$

Input in superposition

$$|\sigma_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

My first quantum program

$$
\begin{aligned}
|\sigma_2\rangle &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\
&= \begin{cases} (\pm 1)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases}
\end{aligned}
$$

$$
\begin{aligned}
|\sigma_3\rangle &= H|\sigma_2\rangle \\
&= \begin{cases} (\pm 1)\,|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\,|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases}
\end{aligned}
$$

To answer the original problem is now enough to measure the first qubit: if it is in state $|0\rangle$, then f is constant.

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

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

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

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

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)