Quantum Systems

(Lecture 2: From bits to qubits)

Luís Soares Barbosa

Universidade do Minho
HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY
INL
INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY
UNITED NATIONS UNIVERSITY
UNU-EGOV

Universidade do Minho

Bits as vectors

Classical bits, standing for Boolean values 0 and 1, can be represented by vectors:

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

If rows are labelled from 0 onwards, the presence of 1 in a cell identifies the number represented by the vector.

Larger state spaces are built with the (Kronecker) tensor product:

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix} \otimes \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} = \begin{bmatrix} p_0 \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \\ p_1 \begin{bmatrix} q_0 \\ q_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} p_0 q_0 \\ p_0 q_1 \\ p_1 q_0 \\ p_1 q_1 \end{bmatrix}$$

Bits as vectors

Examples: Putting bits together

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|4\rangle = |100\rangle = |1\rangle \otimes |0\rangle \otimes |0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Bits as vectors, operators as matrices

$\boxed{\mathrm{I}(x) = x}$ $\quad \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \quad \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$

$\boxed{\mathrm{X}(x) = \neg x}$ $\quad \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \quad \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$

$\boxed{\underline{1}(x) = 1}$ $\quad \begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix} \quad \begin{bmatrix}0 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}$

$\boxed{\underline{0}(x) = 0}$ $\quad \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} \quad \begin{bmatrix}1 & 1\\0 & 0\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix}$

$$\begin{aligned} I|0\rangle &= |0\rangle & I|1\rangle &= |1\rangle \\ X|0\rangle &= |1\rangle & X|1\rangle &= |0\rangle \\ \underline{1}|0\rangle &= |1\rangle & \underline{1}|1\rangle &= |1\rangle \\ \underline{0}|0\rangle &= |0\rangle & \underline{0}|1\rangle &= |0\rangle \end{aligned}$$

Composition

Sequential composition: matrix multiplication

Parallel composition: Kronecker product $\otimes$

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

for example

$$X \otimes \underline{1} \otimes I \, |101\rangle \; = \; X \otimes \underline{1} \otimes I \, (|1\rangle \otimes |0\rangle \otimes |1\rangle) \; = \; = \; X|1\rangle \otimes \underline{1}|0\rangle \otimes I|1\rangle \; = \; |011\rangle$$

Probabilistic bits

States: States are vectors of probabilities in $\mathcal{R}^n$

$$\left[p_0 \cdots p_n\right]^T \text{ such that } \sum_i p_1 = 1$$

which express indeterminacy about the exact system state

Operator: Double stochastic matrix where $M_{i,j}$ specifies the probability of evolution from state j to i

Evolution: computed through matrix multiplication of an operator M with a vector $|u\rangle$ of current probabilities, leading to the next state $M|u\rangle$.

Probabilistic bits

Measurement: the system is always in some well defined state, even if we do not know which.

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.

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

Qubits are a different story

A quantum state holds the information of both possible classical states:

A qubit lives in a 2-dimensional complex vector space:

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle$$

and thus possesses a continuum of possible values, so potentially, can store lots of classical data.

However, all this potential is hidden: when observed $|v\rangle$ collapses into a classic state: $|0\rangle$, with probability $\|\alpha\|^2$, or $|1\rangle$, with probability $\|\beta\|^2$.

Qubits are a different story

The outcome of an observation is probabilistic, which calls for a restriction to unit vectors, i.e. st

$$\| \alpha \|^2 + \| \beta \|^2 = 1$$

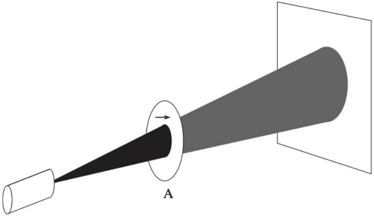
to represent quantum states.

But a superposition state is not a probabilistic mixture: it is not true that the state is really either $|u\rangle$ or $|u'\rangle$ and we just do not happen to know which.

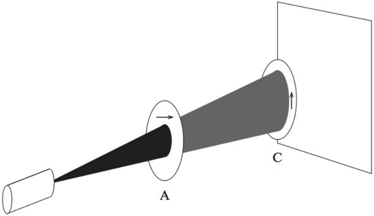
State $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results:

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

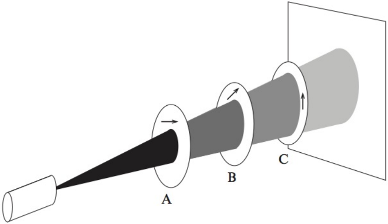
Qubits: An experiment with a photon



$|0\rangle$ - horizontal polarization



$|1\rangle$ - vertical polarization



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

(from [Reifell & Polak, 2011])

Qubits: An experiment with a photon

For a beam of light there is a classical explanation in terms of waves. But that does not work for a single photon experiment.

An explanation

- The photon's polarization state is modelled by a unit vector, for example $|+\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle$, which corresponds to a polarization of 45 degrees.
- ... or, in general, by a vector

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle$$

where α, β are (complex) amplitudes.

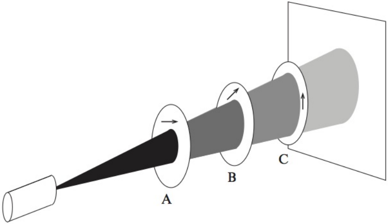
If α, β are both non-zero, $|v\rangle$ is said a superposition of $|0\rangle$ and $|1\rangle$

Qubits: An experiment with a photon

- Each polaroid has also a polarization axis.
- On passing a polaroid the photon becomes polarized in the direction of that axis.
- The probability that a photon passes through the polaroid is the square of the magnitude of the amplitude of its polarization in the direction of the polaroid's axis.

For example, if the photon is polarized as $|v\rangle$ it will go through A with probability $\| \alpha \|^2$ and be absorbed with $\| \beta \|^2$.

Qu bits: An experiment with a photon



The polarization of polaroid B is

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

i.e. represented as a superposition of vectors $|0\rangle$ and $|1\rangle$

Qubits: An experiment with a photon

The photon reaches polaroid B with polarization $|0\rangle$, which is expressed in the Hadamard basis

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

as

$$|0\rangle = \frac{1}{\sqrt{2}}|-\rangle + \frac{1}{\sqrt{2}}|+\rangle$$

which explains why a visible effect appears in the wall:

the photon goes through C with 50% of probability (i.e. $\| \frac{1}{\sqrt{2}} \|^2 = \frac{1}{2}$).

Qubits

Photon's polarization states are represented as unit vectors in a 2-dimensional complex vector space, typically as a

non trivial linear combination $\equiv$ superposition of vectors in a basis

$$|v\rangle = \alpha|0\rangle + \beta|1\rangle$$

A basis provides an observation (or measurement) tool, e.g.

$$\bigcirc\frown\bigcirc = \{|0\rangle, |1\rangle\} \quad \text{or} \quad \bigcirc\frown\bigcirc = \{|+\rangle, |-\rangle\}$$

The space of possible polarization states of a photon is an example of a qubit

Qubits

Observation of a state

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

transforms the state into one of the basis vectors in

$$\bigcirc\frown\bigcirc = \{|u\rangle, |u'\rangle\}$$

In other (the quantum mechanics) words:

measurement collapses $|v\rangle$ into a classic, non superimposed state: $|u\rangle$ or $|u'\rangle$, with probability $\|\,\alpha\,\|^2$ or $\|\,\beta\,\|^2$, respectively.

Qubits

The probability that observed $|v\rangle$ collapses into $|u\rangle$ is the square of the modulus of the amplitude of its component in the direction of $|u\rangle$, i.e.

$$\| \alpha \|^2$$

where, for a complex γ, $\| \gamma \| = \sqrt{\overline{\gamma}\gamma}$

A subsequent measurement wrt the same basis returns $|u\rangle$ with probability 1

This observation calls for a restriction to unit vectors, i.e. st

$$\| \alpha \|^2 + \| \beta \|^2 = 1$$

to represent quantum states.

Superposition and interference

The notion of superposition is basis-dependent: all states are superpositions with respect to some bases and not with respect to others.

But it is not a probabilistic mixture: it is not true that the state is really either $|u\rangle$ or $|u'\rangle$ and we just do not happen to know which.

State $|v\rangle$ is a definite state, which, when measured in certain bases, gives deterministic results, while in others it gives random results:

The photon with polarization

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

behaves deterministically when measured with respect to the Hadamard basis but non deterministically with respect to the standard basis

Superposition and interference

In a sense $|v\rangle$ 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, thus capturing another fundamental quantum resource:

interference

Summing up

Any quantum system (e.g. photon polarization, electron spin, and the ground state together with an excited state of an atom) that can be modelled by a two-dimensional complex vector space, forms a

quantum bit (qubit)

which has a continuum of possible values.

- In practice it is not yet clear which two-state systems will be most suitable for physical realizations of qubits: it is likely that a variety of physical representation will be used.
- and they are fragile and unstable which entails the need for qubits' strong isolation, typically very hard to achieve.

Summing up

A qubit has ... a continuum of possible values

- potentially, it can store lots of classical data
- but the amount of information that can be extracted from a qubit by measurement is severely restricted: a single measurement yields at most a single classical bit of information;
- as measurement changes the state, one cannot make two measurements on the original state of a qubit.
- as an unknown quantum state cannot be cloned, it is not possible to measure a qubit's state in two ways, even indirectly by copying its state and measuring the copy.

Summing up

Simulating a computation with qubits in a classical computer would be extremely hard, i.e. extremely inefficient as the number of qubits increases:

- For 100 qubits the state space would require to store $2^{100} \approx 10^{30}$ complex numbers!
- And what about rotating a vector in a vector space of dimension 10^{30}?

Moreover, there is a fundamental limitation due to Bell's theorem. Thus,

Quantum computing as using quantum reality as a computational resource

Richard Feynman, *Simulating Physics with Computers* (1982)

What can be expected from quantum computation?

- The meaning of computable remains the same ...
- ... but the order of complexity may change

Factoring in polynomial time - $\mathcal{O}((ln\, n)^3)$

Peter Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer* (1994)

What can be expected from quantum computation?

Factoring in polynomial time - $\mathcal{O}((ln\, n)^3)$

- Classically believed to be superpolynomial in log n, i.e. as n increases the worst case time grows faster than any power of log n.
- The best classical algorithm requires approximately

$$e^{1.9(\sqrt[3]{\ln\, n}\sqrt[3]{(\ln\, \ln\, n)^2})}$$

- From the best current estimation (the 65 digit factors of a 130 digit number can be found in around one month in a massively parallel computer network) one can extrapolate that to factor a 400 digit number will take about the age of the universe (10^{10} years)

Computing with qubits

States: 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 $\| \alpha_i \|^2$ — 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.

Some operators

The X gate

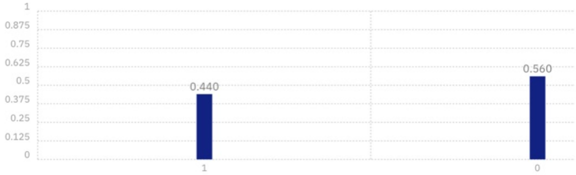
e.g.

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

$$X(\alpha|0\rangle + \beta|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

Some operators

The H gate



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

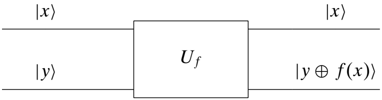
The H gate creates superpositions:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = |+\rangle$$

The Deutsch problem

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

Oracle



where $\oplus$ stands for exclusive or, i.e. addition module 2.

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

The Deutsch problem

Preparing the first qubit as $|x\rangle$ is the (quantum version of) input x:

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|f(0)\rangle \\ |1\rangle|0\rangle &\mapsto |1\rangle|f(1)\rangle \end{aligned}$$

But in the quantum world, one can better: input a superposition of $|0\rangle$ and $|1\rangle$ to get

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

The Deutsch problem

...

$$
\begin{aligned}
U_f\left(\frac{1}{\sqrt{2}}|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,|0\rangle\right) &= \frac{1}{\sqrt{2}}U_f|0\rangle|0\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|0\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle|0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f(1)\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|f(1)\rangle
\end{aligned}
$$

- The value of f on both possible inputs (0 and 1) was computed simultaneously in superposition
- Double evaluation — the bottleneck in a classical solution — was avoided by superposition

Is such quantum parallelism useful?

NO

Although both values have been computed simultaneously, only one of them is retrieved upon measurement in the computational basis: Actually, 0 or 1 will be retrieved with identical probability (why?).

YES

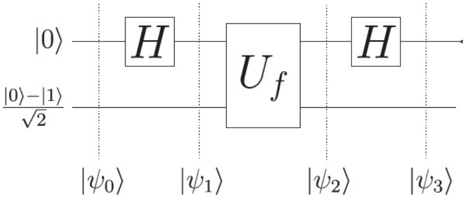
The Deutsch problem is not interested on the concrete values f may take, but on a global property of f: whether it is constant or not, technically on the value of

$$f(0) \oplus f(1)$$

The Deutsch algorithm explores another quantum resource — interference — to obtain that global information on f

Deutsch algorithm

Idea: Avoid double evaluation by superposition and interference



The circuit computes:

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

Deutsch algorithm

After the oracle, at ψ_2, one obtains

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

For $|x\rangle$ a superposition:

$$|\psi_2\rangle = \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$
$$= \begin{cases} (\pm 1) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ constant} \\ (\pm 1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \Leftarrow f \text{ not constant} \end{cases}$$

Deutsch algorithm

$$
\begin{aligned}
|\psi_3\rangle &= H|\psi_2\rangle \\
&= \begin{cases} (\pm 1)\,|0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ constant} \\ (\pm 1)\,|1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \Leftarrow f \text{ not constant} \end{cases}
\end{aligned}
$$

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

Note

As the initial state in the second qubit can be prepared as $H|1\rangle$, the circuit is equivalent to

$$
(H \otimes I)\, U_f\, (H \otimes I) \left(|0, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\rangle\right) = (H \otimes I)\, U_f\, (H \otimes H)(|01\rangle)
$$