Quantum Systems

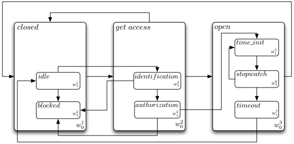
(Lecture 1: Introduction: From bits to qubits)

Luís Soares Barbosa

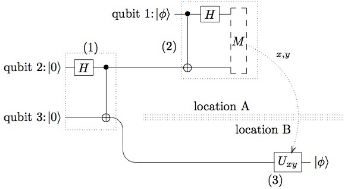
Universidade do Minho

Interaction and Concurrency

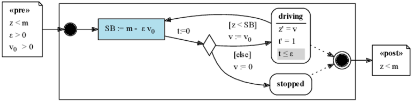
reactive systems
classical discrete interaction



quantum systems
quantum interaction



cyber-physical systems
classical continuous interaction



Why studying quantum computation?

Quantum is trendy ...

Research on quantum technologies is speeding up, and has already created first operational and commercially available applications.

For the first time the viability of quantum computing may be demonstrated in a number of problems and its utility discussed across industries.

Efforts, at national or international levels, to further scale up this research and development are in place.

Why studying quantum computation?

… and full of promises …

- Classical computer technology is running up against fundamental size limitations (Moore's law),

- Real difficult, complex problems remain out of reach of classical supercomputers

Why studying quantum computation?

Prime factorization

1230186684530117755130494958384962720772853569595334792197322452151726400507
2636575187452021997864693899564749427740638459251925573263034537315482680791
70261221429134616704292143116022212404
79274737794080665351419597459856902143413 =
? * ?

- Classically believed to be superpolynomial in $\log n$, i.e. as n increases the worst case time grows faster than any power of $\log n$.
- From the best current estimation (factoring a 130 digit number takes 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)

Why studying quantum computation?

However, a quantum algorithm exists such that

$\boxed{\text{Factoring is achieved in polynomial time}}$

Actually,

- Quantum computing will have a substantial impact on societies,
- even if, being a so radically different technology, it is difficult to anticipate its evolution.

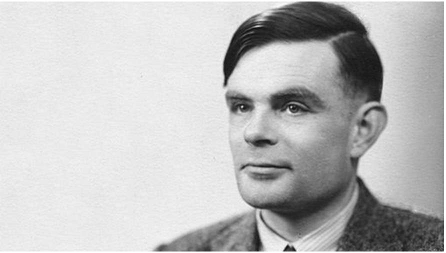
Quantum Mechanics ‘meets’ Computer Science

Two main intelectual achievements of the 20th century met

- Computer Science and Information theory progressed by abstracting from the physical reality. This was the key of its success to an extent that its origin was almost forgotten.
- On the other hand quantum mechanics ubiquitously underlies ICT devices at the implementation level, but had no influence on the computational model itself ...
- ... until now!

Quantum Mechanics 'meets' Computer Science

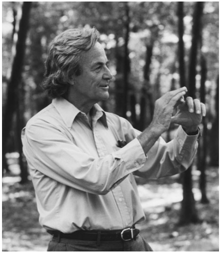
Alan Turing (1912 - 1934)



On Computable Numbers, with an Application to the Entscheidungsproblem (1936)

Quantum Mechanics 'meets' Computer Science

Richard Feynman (1918 - 1988)



Simulating Physics with Computers (1982)
(quantum reality as a computational resource)

Quantum effects as computational resources

Superposition

Our perception is that an object — e.g. a bit — exists in a well-defined state, even when we are not looking at it.
However: A quantum state holds information of both possible classical states.

Entanglement

Our perception is that objects are directly affected only by nearby objects, i.e. the laws of physics work in a local way.
However: two qubits can be connected, or entangled, st an action performed on one of them can have an immediate effect on the other even at distance.

Quantum effects as computational resources

$\boxed{\text{God plays dice indeed}}$

Our perception is that the laws of Physics are deterministic: there is a unique outcome to every experiment.
However: one can only know the probability of the outcome, for example the probability of a system in a superposition to collapse into a specific state when measured.

$\boxed{\text{Uncertainty is a feature, not a bug}}$

Our perception is that with better tools we will be able to measure whatever seems relevant for a problem.
However: there are inherent limitations to the amount of knowledge that one can ascertain about a physical system

Quantum Computation

Davis Deutsch (1953)

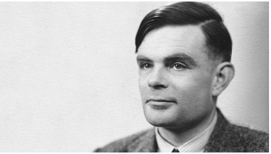
Quantum theory, the Church-Turing principle and the universal quantum computer (1985)
(quantum computability and computational model:
first example of a quantum algorithm that is exponentially faster than any possible deterministic classical one)

Quantum Computation

quantum resources

quantum algorithms

computability



Time to go deeper ...

- Quantum information: From bits to qubits
- Quantum computation: Computing with qubits

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

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

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

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

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

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

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

State: is a vector 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 system's exact physical configuration

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

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.

Qubits are a different story

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 $|\beta|^2$.

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.

Qubits are a different story

But a superposition state is not a probabilistic mixture: it is not true that the state is really either $|0\rangle$ or $|1\rangle$ and we just do not happen to know which.

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.

Superposition in action: A random number generator

By preparing deterministically a single qubit and measuring in the standard basis, we can achieve a task that it is impossible classically: a true random numbers generator.

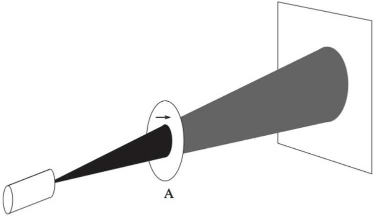
- Prepare quantum state

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

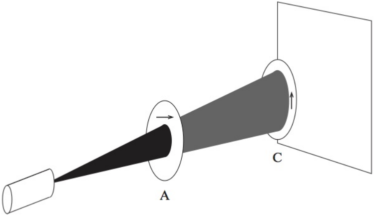
- Measure $|+\rangle$ in the computational basis to obtain either 0 or 1 with equal probability ($|\frac{1}{\sqrt{2}}|^2 = 0.5$)

This algorithm allows us to produce a perfect random number even though no randomness has been used inside it

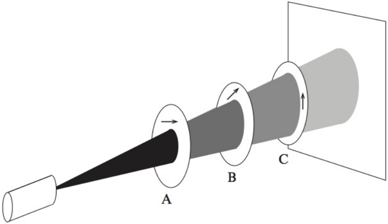
Quantum bits: An experiment with a photon



$|0\rangle$ - horizontal polarization



$|1\rangle$ - vertical polarization



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

(from [Reifell & Polak, 2011])

Quantum bits: 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, a vector

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

where α, β are (complex) amplitudes.

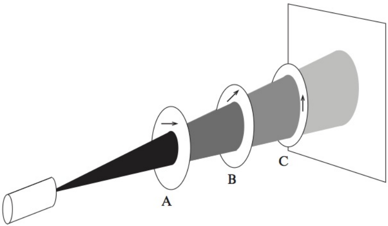
If α, β are both non-zero, $|v\rangle$ is said a superposition of $|0\rangle$ and $|1\rangle$

Quantum bits: 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 $|\beta|^2$.

Quantum bits: An experiment with a photon



The polarization of polaroid C is

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

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

Quantum bits: An experiment with a photon

Expressing $|0\rangle$ in terms of the Hadamard basis

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

yields

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

which explains why a visible effect appears when the last polaroid is introduced:
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

Superposition and interference

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

Superposition and interference

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 $|u\rangle$ 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 $|u\rangle$ 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, thus capturing another fundamental quantum resource:

interference

Qubits

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.

Qubits

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.

Can we play the quantum game with a classical computer?

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}?

Thus,

Quantum computing as using quantum reality as a computational resource

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