Lecture 1:
Superposition and quantum interference

Luís Soares Barbosa

Universidade do Minho

HASLab
HIGH-ASSURANCE
SOFTWARE LABORATORY

INTERNATIONAL IBERIAN
NANOTECHNOLOGY
LABORATORY

Mestrado em Engenharia Física

Universidade do Minho, 2025-26

Quantum computation: The *motto*

Information is a physical entity. Any computation is a physical process

Thus, any abstract computational model has always to reflect what we know about reality, and quantum theory is our current best tool in this road.

Recall: The physical Church-Turing thesis

The class of functions computable in finite time by a physical device can be computed by a Turing machine.

which a statement about the physical universe, while the Church-Turing thesis — *The class of functions computable by a Turing machine corresponds exactly to the class of functions which can be described by an algorithm* — is a claim about what counts as an algorithm

Information is physical

How to represent information in a computational device?

Three basic ways ...

- Binary ... in a two-state device
- Probabilistic ... in a similar way but with uncertainty
- Quantum ... in a quantum device

Binary information

Computational / information states based on Boolean values 0 and 1 which 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:

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

Binary information

Examples

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

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

Binary information

Operations as matrices

$\boxed{\mathrm{I}(x) = x}$

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

$\boxed{\mathrm{X}(x) = \neg x}$

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

$\boxed{\underline{1}(x) = 1}$

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

$\boxed{\underline{0}(x) = 0}$

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

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

Binary information

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 information

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

State: is a vector of probabilities in $\mathcal{R}^n$

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

which expresses 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

Quantum information is a different story

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

A unit of information 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.

Quantum information is 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 $|\beta|^2$.

(Recall: $|\alpha| = \sqrt{\alpha\overline{\alpha}}$ for a complex α)

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.

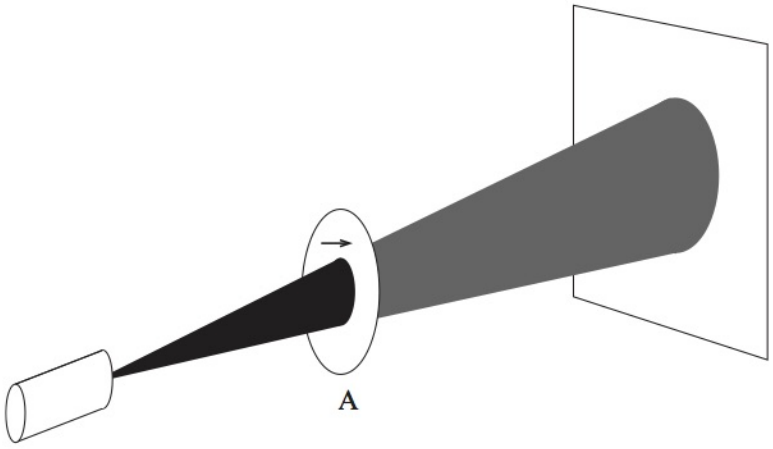
Quantum information is a different story

This quantum 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.

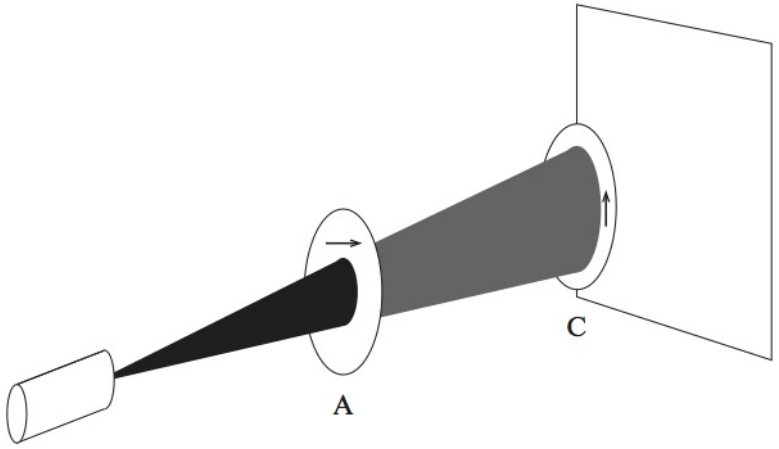
Amplitudes are not real numbers (e.g. probabilities) that can only increase when added, but complex so that they can cancel each other or lower their probability, thus capturing a fundamental quantum resource:

interference

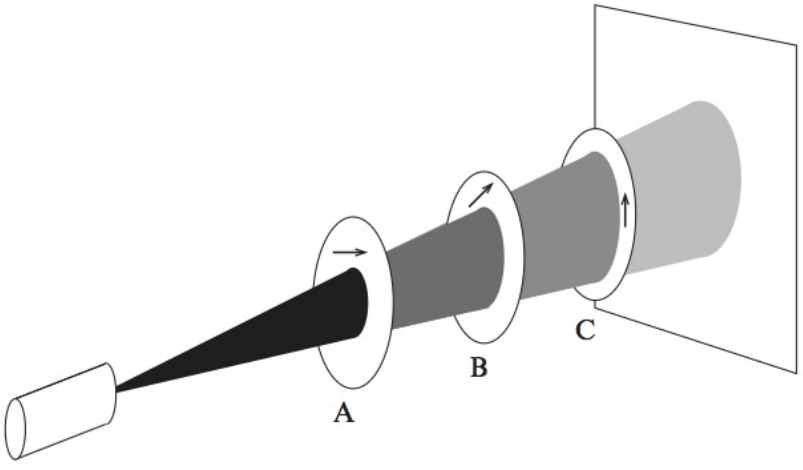
Quantum information: An experiment with a photon



$|0\rangle$ - horizontal polarization



$|1\rangle$ - vertical polarization



(from [Reifell & Polak, 2011])

Quantum information: An experiment with a photon

An explanation for a *single* photon experiment

- The photon's polarization state is modelled by a unit vector, for example the following linear combination of $|0\rangle$ and $|1\rangle$:

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

  which corresponds to a polarization of 45 degrees.

- On passing a polaroid the photon will be absorbed or leave the polaroid with its polarization aligned with the polaroid's axis.
- The probability to go through the polaroid is the square of the magnitude of the amplitude of its polarization in the direction of the polaroid's axis.

Quantum information: An experiment with a photon

- Polarization of polaroid B is $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- This vector, together with $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ forms a basis for the 2-dimensional vector space
- of which $\{|0\rangle, |1\rangle\}$ is another one (the so-called computational basis).
- Expressing $|0\rangle$ in terms of $|+\rangle$ and $|-\rangle$ yields

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

which explains why a visible effect appears in the wall:

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

Why aren't probabilities enough?

Computation is always a physical process

That's our *motto*!

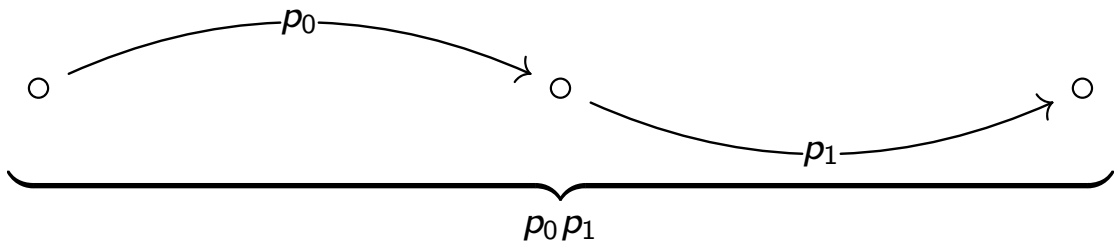
In several cases, the language of probability theory can describe the actual physical evolution of a system, i.e.

- Physics identify the system's structure and assigns numerical probabilities to elementary transition steps.
- Probability theory, i.e. the Kolmogorov axioms, ensure mathematical consistency and helps in calculating probabilities along paths of evolution.

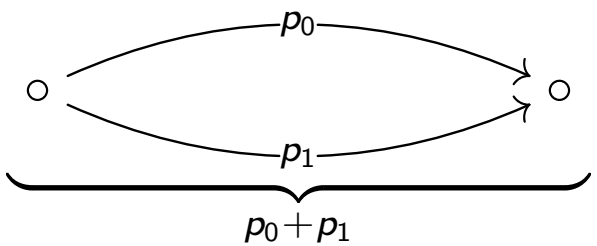
but not always!

Probabilistic systems, probabilistic computation

Sequential paths



Alternative, mutually exclusive paths



(Kolmogorov (1903-1987) additivity axiom)

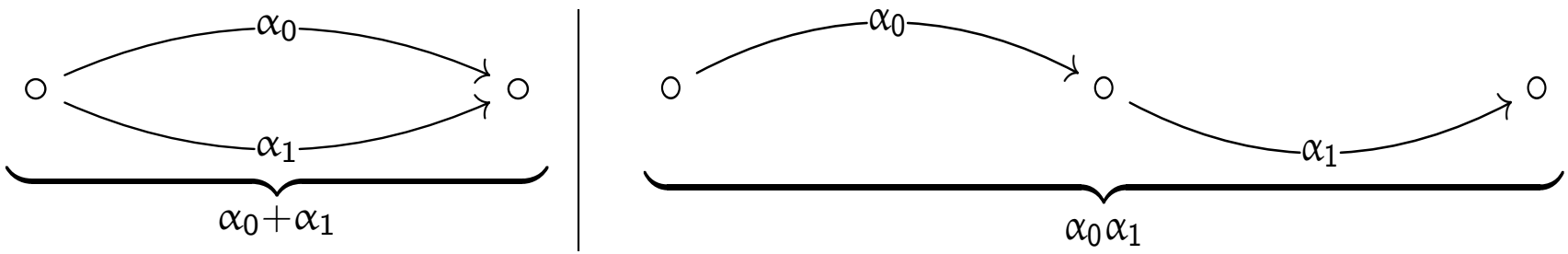
Quantum systems, quantum computation

Many common quantum phenomena, however, cannot be described this way, but are accommodated by a modified 'probability theory':

Transitions are labelled by complex numbers, called their amplitudes, whose norms squared are interpreted as transition probabilities through

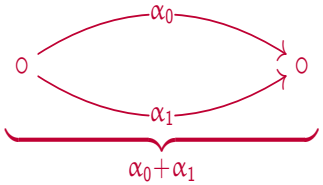
$$\text{Born's rule} \quad p = |\alpha|^2$$

(for Max Born, 1882-1970)



Quantum systems, quantum computation

Let's compute the total probability in



$$
\begin{aligned}
p &= |\alpha_0 + \alpha_1|^2 \\
&= \overline{(\alpha_0 + \alpha_1)}(\alpha_0 + \alpha_1) \\
&= (\overline{\alpha_0} + \overline{\alpha_1})(\alpha_0 + \alpha_1) \\
&= |\alpha_0|^2 + |\alpha_1|^2 + \overline{\alpha_0}\alpha_1 + \alpha_0\overline{\alpha_1} \\
&= p_0 + p_1 + |\alpha_0||\alpha_1| \left(e^{i(\varphi_1 - \varphi_0)} + e^{-i(\varphi_1 - \varphi_0)} \right) \\
&= p_0 + p_1 + \underbrace{2\sqrt{p_0 p_1}\cos(\varphi_1 - \varphi_0)}_{\text{interference}}
\end{aligned}
$$

(expressing α_j in polar form $|\alpha_j|\, e^{i\theta_j}$
and resorting to $e^{i\theta} + e^{-i\theta} = 2\cos\theta$)

Quantum systems, quantum computation

$$p = p_0 + p_1 + \underbrace{2\sqrt{p_0 p_1}\cos(\varphi_1 - \varphi_0)}_{\text{interference}}$$

- The total probability is the sum of the probabilities of the individual transitions modified by the interference term.
- Depending on term $\varphi_1 - \varphi_0$ the interference can be either negative or positive.
- The important quantity is the relative phase $\varphi_1 - \varphi_0$ rather than individual φ_0, φ_1.
- If the system's evolution depends only on that difference then the system must have, somehow, experienced both paths.

Quantum systems, quantum computation

Indeed, the probabilistic assumption that one or the other transition occurs, or that the system presents one or the other configuration, but we just do not know which one, is inconsistent with many experiments:

Typically, a quantum state is a superposition of basic states, i.e. states that, mathematically, form a basis of the vector space in which such states live — e.g. $\{\, |e_i\rangle \mid i = 1 \cdots n \,\}$

$$|\varphi\rangle = \sum_i \alpha_i |e_i\rangle$$

Recall

Superposition in action: A random number generator

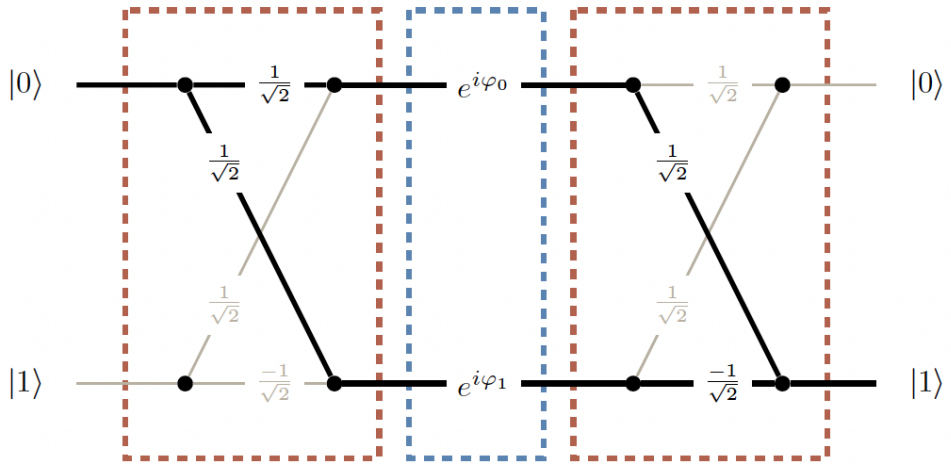
- Prepare quantum state

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

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

This algorithm produces a perfect random number even though no randomness has been used inside it.

Ramsey interference experiment



(from [Ekert *at al*, 2024])

Atoms are sent through two separate resonant interaction zones (which attempt to commute the atom between ground and excited states), separated by an intermediate dispersive interaction zone (which performs a phase shift).

The atoms are subsequently measured and found to be in one of the two basic energy states labeled as $|0\rangle$ and $|1\rangle$.

What is the probability of an atom going from $|0\rangle$ to $|1\rangle$?

First compute the amplitudes:

$$
\begin{aligned}
A_{10} &= \frac{1}{\sqrt{2}} e^{i\varphi_0} \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} e^{i\varphi_1} \frac{-1}{\sqrt{2}} \\
&= \frac{1}{2}\left(e^{i\varphi_0} - e^{i\varphi_1}\right) \\
&= \frac{1}{2}\left(e^{i\frac{\varphi_0+\varphi_1}{2}} e^{i\frac{\varphi_0-\varphi_1}{2}} - e^{i\frac{\varphi_0+\varphi_1}{2}} e^{-i\frac{\varphi_0-\varphi_1}{2}}\right) \\
&= \frac{1}{2} e^{i\frac{\varphi_0+\varphi_1}{2}} \left(e^{i\frac{\varphi_0-\varphi_1}{2}} - e^{-i\frac{\varphi_0-\varphi_1}{2}}\right) \\
&= \frac{1}{2} e^{i\frac{\varphi_0+\varphi_1}{2}} \left(2i \sin\frac{\varphi_0-\varphi_1}{2}\right) \\
&= -ie^{i\frac{\varphi_0+\varphi_1}{2}} \sin\frac{\varphi_1-\varphi_0}{2}
\end{aligned}
$$

resorting to $x = \frac{x+y}{2} + \frac{x-y}{2}$
and Euler formula $e^{i\varphi} = \cos\varphi + i\sin\varphi$

What is the probability of an atom going from $|0\rangle$ to $|1\rangle$?

Then the probability:

$$\begin{aligned} P_{10} &= |A_{10}|^2 \\ &= \left| -ie^{i\frac{\varphi_0+\varphi_1}{2}} \sin\frac{\varphi_1-\varphi_0}{2} \right|^2 \\ &= \left| \sin\frac{\varphi_1-\varphi_0}{2} \right|^2 \\ &= \frac{1}{2} - \underbrace{\frac{1}{2}\cos\left(\varphi_1-\varphi_0\right)}_{\text{interference}} \end{aligned}$$

resorting to $\cos 2\theta = 1 - 2\sin^2\theta$

A bulk calculation ...

The results of these calculations for all pairs begin-end states can be expressed as follows:

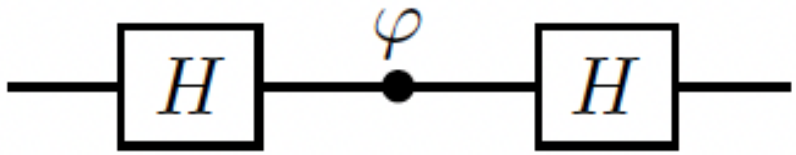
- the effect of each interaction is described by a matrix of transition amplitudes, and
- one resorts to matrix multiplication to compose the sequence of independent interactions.

$$A = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} e^{i\varphi_0} & 0 \\ 0 & e^{i\varphi_1} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$$

$$= e^{i\frac{\varphi_0+\varphi_1}{2}} \begin{bmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix} \quad \text{making } \varphi = \varphi_1 - \varphi_0$$

$$\equiv \begin{bmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix} \quad \text{ignoring global phase, to discuss later ...}$$

My first quantum circuit



- A wire represents a two-dimensional state (a qubit)
- Three gates describing quantum operations:

$$\underbrace{H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}}_{\text{Hadamard gate}} \quad \text{and} \quad \underbrace{P_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}}_{\text{Phase shift gate}}$$

A simple matrix multiplication yields

$$A = HP_\varphi H = \begin{bmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix} = \begin{bmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{bmatrix}$$

My first quantum circuit

which, expressed in a functional way, gives

$$\begin{aligned} A|0\rangle &= \cos\frac{\varphi}{2}|0\rangle + -i\sin\frac{\varphi}{2}|1\rangle \\ A|1\rangle &= -i\sin\frac{\varphi}{2}|0\rangle + \cos\frac{\varphi}{2}|1\rangle \end{aligned}$$

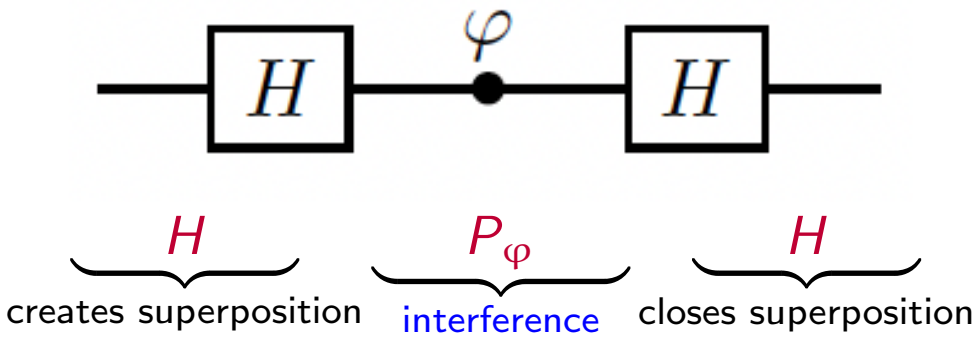
as read from

$$A = HP_\varphi H = \begin{bmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{bmatrix}$$

Clearly, for $\varphi = 0$, i.e. in the absence of any phase shift, $A|0\rangle = |0\rangle$ and $A|1\rangle = |1\rangle$, leading to conclude that

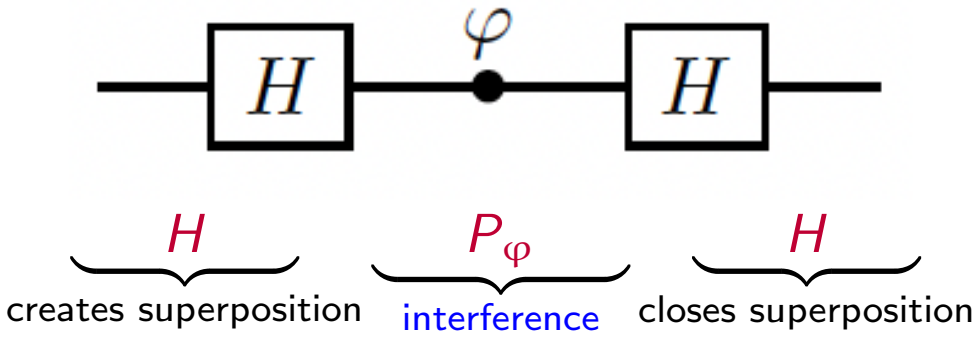
$$HH = Id$$

The golden pattern



- H creates/closes a uniform superposition: it is the source of a natural parallelism,
- but the crucial role in controlling interference is located in P_φ.

Lessons learnt for what follows



generalizes to a basic recipe in quantum algorithms (to be discussed).

What is quantum computation?

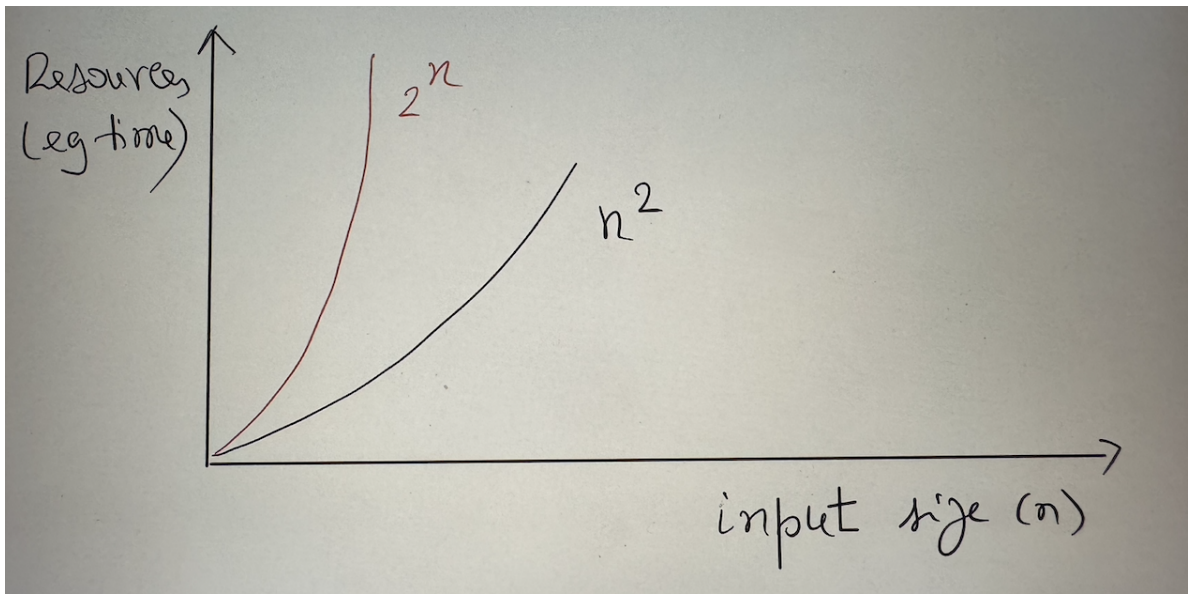
A complex multi-particle quantum interference involving many computational paths through a computing device.

Its challenge is to shape quantum interference through a sequence of computational steps, enhancing probabilities of the correct outputs and suppressing probabilities of the wrong ones.

Superposition and interference what for?

Quantum computing has nothing to say on the boundaries of computability, but reduces the complexity of algorithms to address several problems.

The limits of practicality



Paying a visit to old acquaintances

EXP Problems requiring exponential time to be solved

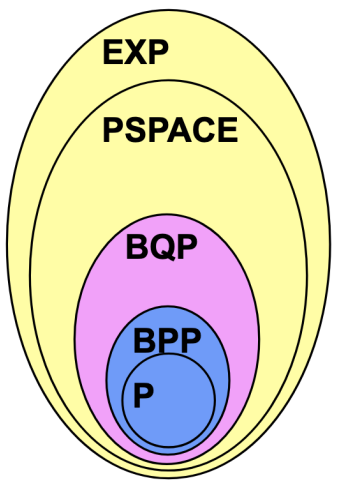
PSPACE Problems requiring polynomial space to be solved

BQP Problems solved in quantum machines in bounded error polynomial time

BPP Problems solved in probabilistic machines in bounded error polynomial time

P Problems solved in deterministic classical machines in polynomial time

$$\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}$$

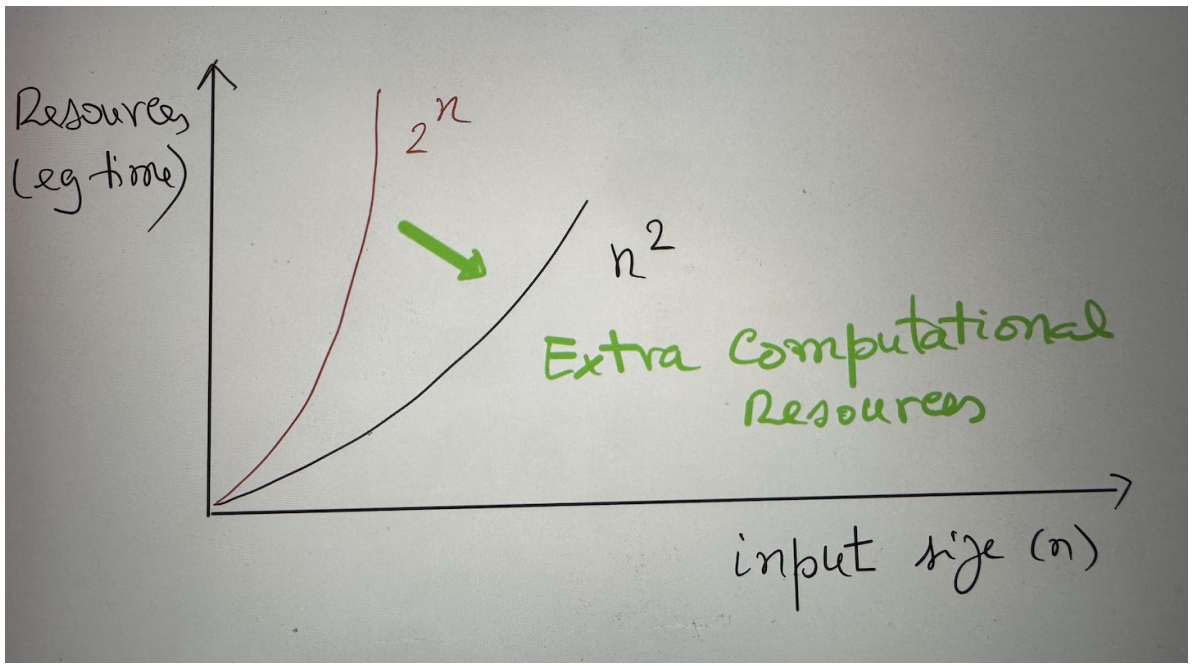


Superposition and interference as computational resources

A problem does not become tractable by increasing computational power: more of the same keeps similar circumnstances.

New ideas & new resources make a difference

The key: Quantum effects as computational resources



Decoherence

The laws of quantum computation just described assume a perfectly isolated system.

- In practice, any complex quantum system cannot avoid some spurious interactions with the environment.
- Thus, when computing the system's evolution, one must take into account not only its internal configurations but also those of its environment.

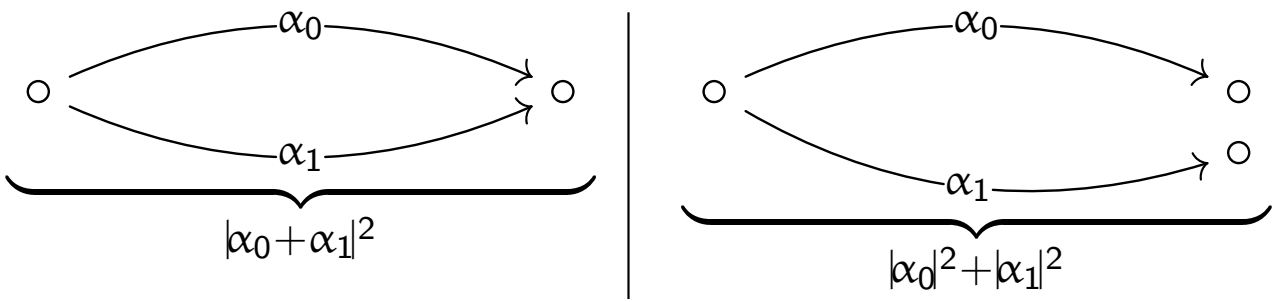
This is known as decoherence and explains why

- we hardly see quantum interference on a daily basis
- and isolation is a main technological challenge in the design/construction of quantum computing devices.

Two scenarios

- Perfect isolation: the environment does not hold any physical record of the path taken to produce an output.
- Total decoherence: the system produces an output but the environment has a record of the path taken: there are no alternative ways to reach that output, but a single path to each of the following situations (joint states):

  1. The output was produced, but the environment knows the path labelled by α_0 was taken,
  2. or similarly for α_1.



Two scenarios

- Perfect isolation: amplitudes are added and generate a probability for the output to be produced, taking both paths in superposition
- Total decoherence: probabilities are computed for each path and summed as such — interference provided by superposition is lost.

The general scenario

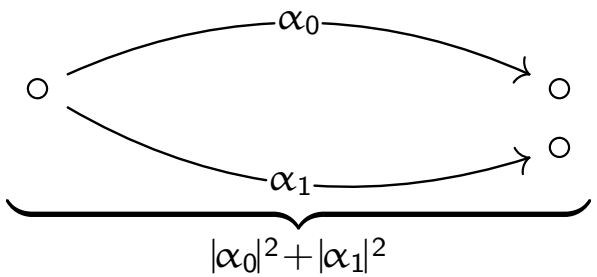
Interference is limited by a visibility parameter — ν — ranging from

- 0: total decoherence; no interference
- 1: no decoherence; full interference

The effect of decoherence

$$p_0 + p_1 + 2\nu\sqrt{p_0 p_1}\cos(\phi_1 - \phi_0)$$

Parameter ν quantifies the degree of distinguishability between the disrupted outputs: *the more the environment knows the less interference is observed more classic becomes the overall computation.*



Fact

Decoherence destroys (quantum) interference.