Quantum Computing

Lecture $|02\rangle$

The Quantum Bit

Paolo Zuliani

zuliani@di.uniroma1.it

Outline

- Probabilistic algorithms
- The Quantum Bit (qubit)
- Qubit operations

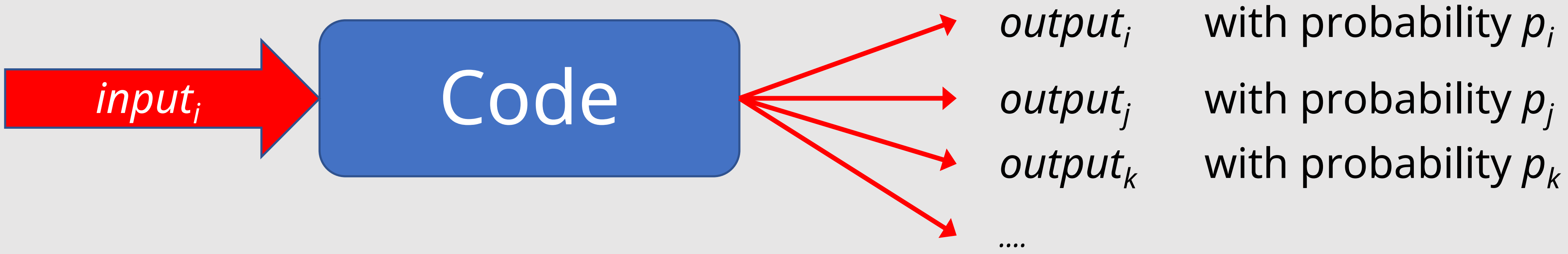
Probabilistic Algorithms

- Most of the algorithms you've seen so far are <u>deterministic</u>
- For <u>a given input</u> they'll produce the <u>same output</u>
  - (assuming your code doesn't crash or hangs ☺)

- ***Note***: multiple input values *a*, *b*, *c*, *etc*. can "map" to the same output value
  - This is OK – think about a program for a simple calculator!

Probabilistic Algorithms

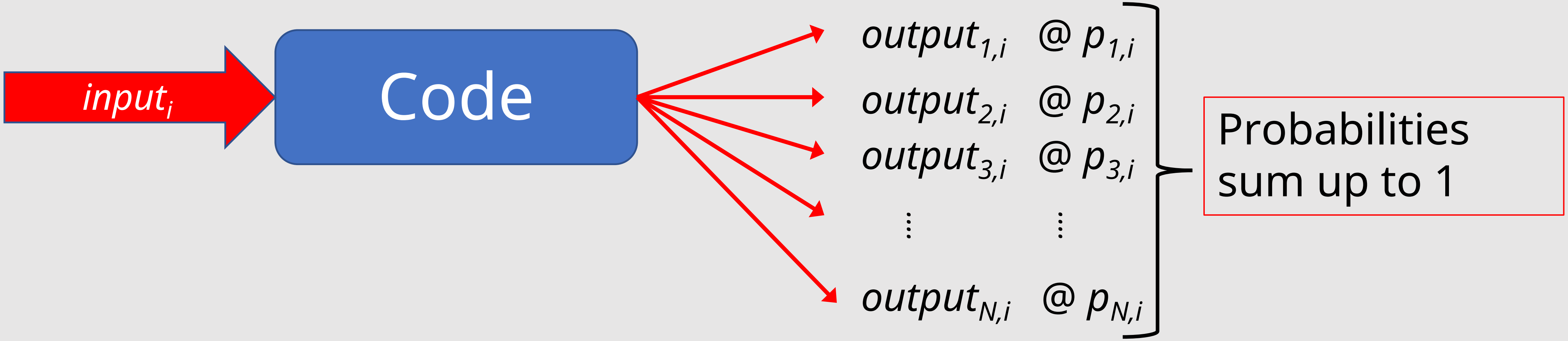
- With stochastic (probabilistic) algorithms it can be that



- We assume that the number of possible outputs is finite (say N)
  - but not necessarily so the number of inputs

Probabilistic Algorithms

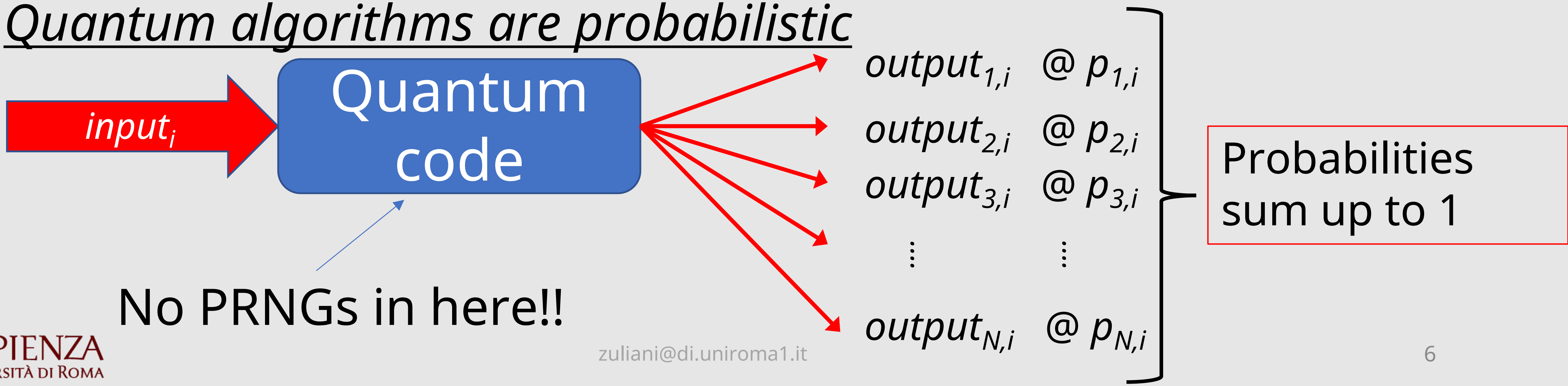
- For any input *i* we have at most *N* possible outputs, and they satisfy



- The program will output something with *probability 1*
  - Essentially, we are asking for (*probabilistic*) termination!

Probabilistic Algorithms

- Classical (non-quantum) algorithms introduce probabilistic behaviour via ***pseudo-random number generators*** (PRNGs)
  - PRNGs produce, say, a sequence of integers such that given an element of the sequence it is difficult to predict the next one (*i.e.*, the best one can do is "to guess" randomly)
  - ***Note***: PRNGs necessarily produce finite sequences: after *many* elements are produced, the sequence repeats itself (*i.e.*, it is no longer random!)
- *Quantum algorithms are probabilistic*



The Quantum Bit (Qubit)

- A classical bit is a <u>bi</u>nary digi<u>t</u>: it's either "0" or "1".
- The quantum equivalent are given by the ***vectors***

$$\text{"0"}=|0\rangle = \binom{1}{0} \qquad\qquad \text{"1"}=|1\rangle = \binom{0}{1}$$

- There's more! The "true" state of a qubit is the ***superposition***

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

where α, β are ***complex numbers*** and satisfy $|\alpha|^2 + |\beta|^2 = 1$.

The Quantum Bit (Qubit)

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

α, β are ***<u>probability amplitudes</u>***. (Recall that $|\alpha|^2 + |\beta|^2 = 1$.)

Example:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right] = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

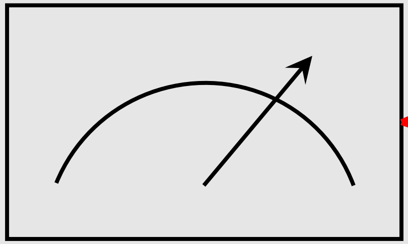
zuliani@di.uniroma1.it

The Quantum Bit (Qubit)

- The “true” state of a qubit ***CANNOT*** be observed
  - We cannot in principle find out precisely the value of α, β

- Qubits are ***<u>measured</u>***

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



Measurement operation

$|0\rangle$ with probability $|\alpha|^2$

$|1\rangle$ with probability $|\beta|^2$

- We know <u>for sure</u> that after measurement the qubit is (*a multiple*) either $|0\rangle$ or $|1\rangle$.

The Quantum Bit (Qubit)

- Note that for any complex α, $|i\alpha| = |\alpha|$.
- In general, $|z\alpha| = |\alpha|$ if $|z| = 1$. (Easy to prove.)
- But this means that for any complex $|z| = 1$, the qubit states

$$z\alpha|0\rangle + z\beta|1\rangle \qquad (|\alpha|^2 + |\beta|^2 = 1)$$

CANNOT be distinguished by any measurement!!!

Qubit Operations

- Quantum transformations (*except* measurements) are ***linear***

$$T(\alpha|0\rangle + \beta|1\rangle) = \alpha T(|0\rangle) + \beta T(|1\rangle)$$

- Any linear transformation (on a vector space) can be represented by a matrix
- The "do nothing" transformation is the 2x2 identity matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad I|0\rangle = |0\rangle \qquad I|1\rangle = |1\rangle$$

(Check that $I|\Phi\rangle = |\Phi\rangle$, where $|\Phi\rangle$ is the general qubit state above.)

Qubit Operations: NOT

- The equivalent of the NOT gate on classical bits

$$\mathrm{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x$$

is one of the three Pauli matrices (much used in quantum physics and computation!)

$$\mathrm{NOT}\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$\Longrightarrow \quad \mathrm{NOT}\ \mathrm{NOT} = I$$

$$\mathrm{NOT}\,|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Qubit Operations: more Pauli Matrices

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\sigma_y|0\rangle = i|1\rangle \qquad \sigma_y|1\rangle = -i|0\rangle$$

$$\sigma_z|0\rangle = |0\rangle \qquad \sigma_z|1\rangle = -|1\rangle$$

- Verify the equalities above!
- Exercise: What are σ_x^2, σ_y^2, σ_z^2?

Qubit Operations: Hadamard Transform

- Critically important in quantum computing:

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

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left[\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

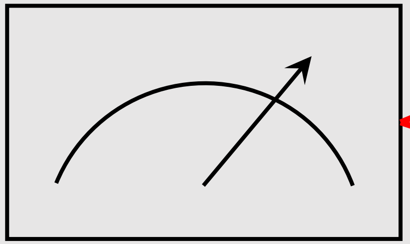
- From a classical state we obtain a ***superposition***!
- What happens if we measure it?

Qubit Operations: Hadamard Transform

- A “true”, random bits generator!

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

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



Measurement operation

$|0\rangle$ with probability $\frac{1}{2}$

$|1\rangle$ with probability $\frac{1}{2}$

(Exercise: try $H|1\rangle$.)

Quantum Evolution

- Is any matrix an allowed quantum transformation?
- NO! Matrices must preserve the ***norm*** of their input vectors

$v = \alpha|0\rangle + \beta|1\rangle$ $\quad\quad$ $\|v\| = \sqrt{|\alpha|^2 + |\beta|^2}$ is the norm of v

- In quantum computing we already have $|\alpha|^2 + |\beta|^2 = 1$, so $\|v\| = 1$ for any qubit state v.
- Intuitively, after a measurement the qubit is in some state with probability 1.

Quantum Evolution

- These norm-preserving matrices are called ***unitary***.

Definition: A matrix is called *unitary* if and only if

$$\|Uv\| = \|v\| \qquad \text{for any qubit state } v$$

- Intuitively, unitary transforms "preserve the probabilities" (not necessarily the amplitudes!)

- (Check that the Pauli and Hadamard matrices are unitary.)

“Picturing” Qubits

- $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with α, β complex and $|\alpha|^2 + |\beta|^2 = 1$
- [Polar coordinates: any complex number z can be written as $z = |z|(\cos\theta + i\sin\theta)$ for some angle θ.]
- By rewriting α and β in polar coordinates our qubit becomes

$$|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$$

where γ, φ and θ are *real* numbers.

- $\left|e^{i\gamma}\right| = 1$, so it has no observable effect and we may write

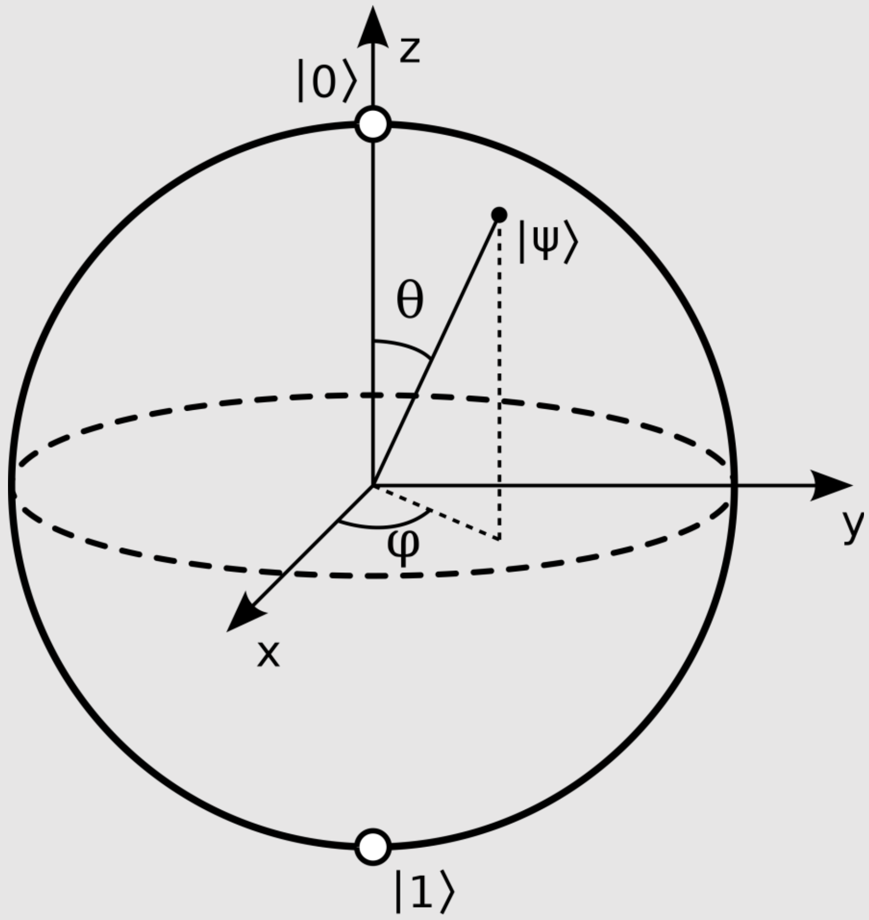
$$|\psi\rangle = (\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle)$$

"Picturing" Qubits: the Bloch Sphere

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

where $0 < \theta < \pi$ and $0 < \varphi < 2\pi$

There is no simple Block sphere equivalent for two or more qubits…



https://commons.wikimedia.org/wiki/File:Bloch_sphere.svg