QUANTUM COMPUTING

MGS 2025 - Sheffield

Venanzio Capretta

LECTURE 1:

- Introduction
- Quantum Hardware
- Superposition, Measurement, Entanglement, Interference
- Qubits and Quantum Gates
- Quantum Circuits

Quantum Computing promises to be the next revolution in information technology

Recently the technology has seen dramatic advances
But it is not yet mature enough for concrete applications

There are many competing hardware realizations:

- Quantum-dot electron-spin qubits
- Nitrogen-vacancy centers in diamonds
- Transmon qubits (superconducting circuits used by IBM et al)
- Topological qubits (Marjorana fermions)

All these technologies still have limitations:

- Qubits must be cooled to near-absolute zero
- Short decoherence time
- Scalability (number of qubits)

Qubits : In classical computing, the basic data element is a bit:
a unit of information with two possible states: 0 and 1

Similarly, in quantum computing the unit of information is a qubit
which can have two discrete states: $|0\rangle$ and $|1\rangle$

The difference is that a qubit can be in a state of
superposition of the two values

Informally, we can say that the qubit has
"both values at the same time"

Formally, the state of the qubit is a complex linear combination:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{with } \alpha, \beta \in \mathbb{C}$$

We can never observe this quantum state
If we measure the qubit, we randomly get either $|0\rangle$ or $|1\rangle$
with probabilities determined by α and β

4 Principles of Quantum Mechanics

(1) A quantum system is in a superposition of several classical states

Eg: a qubit has state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$

(2) When we perform a measurement / observation the result will be one of the classical components (randomly, with probabilities determined by the complex coefficients, amplitudes)

If we measure $|\psi\rangle$ we get: $|0\rangle$ with probability $|\alpha|^2$
$|1\rangle$ with probability $|\beta|^2$

After the measurement, the system will be in the observed state, all other components are lost (wave function collapse)

(3) Several components of the system can be entangled so that the results of their measurements are correlated

Eg: Two qubits can be entangled so that they give the same result on measurement

(4) Several entangled components of a system can evolve to reach the same state.
Their amplitudes either add up or cancel each other.

This phenomenon is called interference

It is at the root of quantum algorithms

Quantum State Standard Form

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

Dirac Notation

α, β probability amplitudes

$\alpha, \beta \in \mathbb{C}$

- Probability of observing $|0\rangle$: $|\alpha|^2$
- Probability of observing $|1\rangle$: $|\beta|^2$

The total probability must be 100%: $|\alpha|^2 + |\beta|^2 = 1$

A quantum state is a vector in the space with basis $\{|0\rangle, |1\rangle\}$

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

The corresponding row vector has as components the complex conjugate of the amplitudes:

$$\langle\psi| = [\bar{\alpha} \quad \bar{\beta}]$$

"bra" - "ket"

Dirac's bra-ket notation

Quantum Gates

Quantum algorithms can be formulated as quantum circuits composed of gates

A quantum gate describes an operation to be performed on the quantum state of one or more qubits

Quantum gate operations are always: linear, reversible, and preserve the total probability

i.e. they are unitary transformations

EXAMPLES:

- The NOT gate (also called Pauli X gate):

$$\sigma_x |0\rangle = |1\rangle$$
$$\sigma_x |1\rangle = |0\rangle$$

linearity means that the operation is fully determined by its values on the basis elements

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

In matrix form: $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

- The Pauli Z gate (phase flip)

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

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

σ_z doesn't change the probabilities of observing $|0\rangle$ or $|1\rangle$

The Hadamard Gate

It is used to create a superposition from a basis state:

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

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

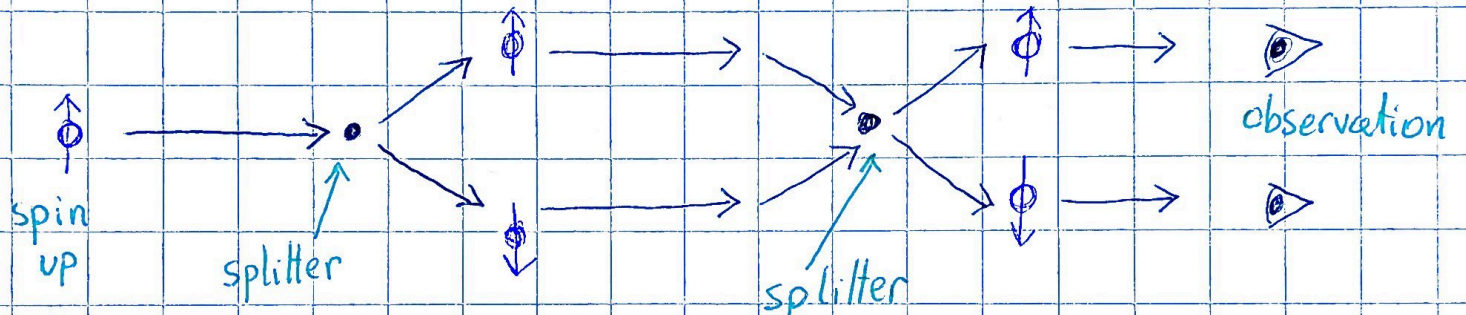
$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

H is often applied to the input qubits to create a superposition of all possible states

Then it is applied again at the end of the algorithm to put the system back in a state from which a useful observation can be made.

ILLUSTRATION OF Interference:

A simple physical experiment sending a polarized particle through a splitter twice:

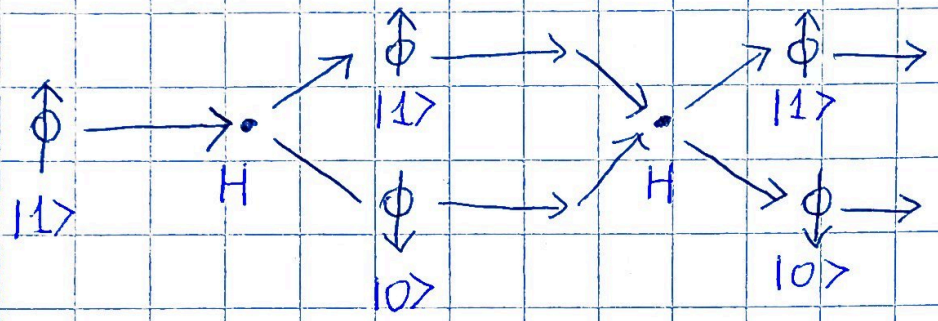


The splitter takes a particle with spin up (or down) and puts it in a superposition of up and down
The observation at the end always returns spin up (or down if we started down)

But if we observe either branch after the first splitter, the final observation will be 50% up, 50% down

EXPLANATION:

The splitter is a Hadamard gate



$$|1\rangle \xmapsto{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

if we observe after the first splitter, we get one of these,

$$|1\rangle \xmapsto{H} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

linearity

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

MULTIPLE QUBIT STATES

To perform useful computations,
we must work with many qubits simultaneously
We use all the possible combinations of values as a basis
Eg: for two qubits we have the basis:

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$ (lexicographic order)

A quantum state with 2 qubits has the form:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}$$

Fore convenience, we may use "decimal" notation:

$|i\rangle_n$ basis element on n qubits with a binary sequence corresponding to the decimal number i

Eg: $|0\rangle_3 = |000\rangle, |1\rangle_3 = |001\rangle, |2\rangle_3 = |010\rangle, \ldots, |7\rangle_3 = |111\rangle$

So we can write: $$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle_n$$

MULTIPLE QUBIT GATES:

- **CNOT** controlled NOT gate on 2 qubits
  if the first qubit is $|1\rangle$, it applies NOT to the second
  otherwise it leaves the state unchanged

$$\text{CNOT}|00\rangle = |00\rangle \qquad \text{CNOT}|10\rangle = |11\rangle$$
$$\text{CNOT}|01\rangle = |01\rangle \qquad \text{CNOT}|11\rangle = |10\rangle$$

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- **SWAP** gate : interchanges the values of the two qubits

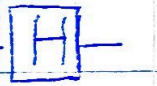
$$\text{SWAP}|00\rangle = |00\rangle \qquad \text{SWAP}|10\rangle = |01\rangle$$
$$\text{SWAP}|01\rangle = |10\rangle \qquad \text{SWAP}|11\rangle = |11\rangle$$

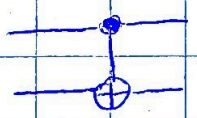
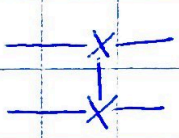
$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

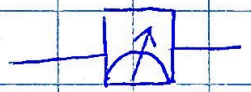
QUANTUM CIRCUITS:

A quantum circuit is a diagram specifying quantum computations:

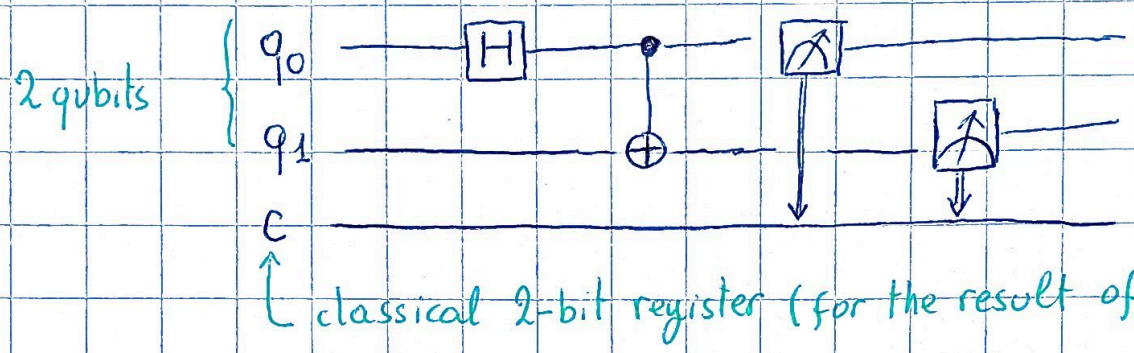
- Wires represent qubits
- Boxes and other symbols represent gates

NOT gate:  , Pauli Z:  , Hadamard: 

Controlled NOT (CNOT):  , SWAP: 

- Measurement is indicated by 

EXAMPLE CIRCUIT:



Usually a quantum circuit is run by starting the qubits in initial state $|0\rangle$ and performing the operations:

$$|00\rangle \xrightarrow{H \text{ on } q_0} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

($|00\rangle$: q_0 q_1)

measure q_0:

- 50% → 0 → $|00\rangle$ → measure q_1: 100% → 0 → $|00\rangle$
- 50% → 1 → $|11\rangle$ → measure q_1: 100% → 1 → $|11\rangle$

entanglement: the measurement of the second qubit is the same as the first