Introduction to Quantum Computing

Gerardo Pelosi, Alessandro Barenghi

Dipartimento di Elettronica, Informazione e Bioingegneria - DEIB
Politecnico di Milano

March 4th, 2022

Quantum Key Distribution

Purpose

- Have two endpoints share a secret bitstring, using only a public, single-qubit communication channel, and a classical channel

Exploit the properties of measurements

- Bennett and Brassard in 1984 found a way to exploit the properties of the measurements with eigenvectors, $(|0\rangle, |1\rangle)$ and $(|+\rangle, |-\rangle)$
- In particular, a classical bit $\mathtt{b}$ encoded as

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = |+\rangle$$

$$(1-\mathtt{b})\,|0\rangle + \mathtt{b}\,|1\rangle \qquad \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix} = |-\rangle$$

will yield a fair coin toss if measured with an apparatus associated to M_{pol}, having $|\ell_{i,M_{pol}}\rangle \in \{|+\rangle, |-\rangle\}$, $\lambda_{i,M_{pol}} \in \{1,-1\}$, $i \in \{0,1\}$

Proving Bennett and Brassard's intuition

Assuming $\mathtt{b}$ encoded as $|\psi\rangle = (1-\mathtt{b})|0\rangle + \mathtt{b}|1\rangle$

$$\textsc{Meas}(|\psi\rangle, M_{comp}) = \begin{cases} 0 & \text{with } \Pr = \langle\psi|0\rangle\langle 0|\psi\rangle = (1-\mathtt{b})^2 = (1-\mathtt{b}) \\ 1 & \text{with } \Pr = \langle\psi|1\rangle\langle 1|\psi\rangle = \mathtt{b}^2 = \mathtt{b} \end{cases}$$

The outcome of $\textsc{Meas}(|\psi\rangle, M_{comp})$ is decoded as $0 \mapsto \mathtt{b}=0,\ 1 \mapsto \mathtt{b}=1$

$$\textsc{Meas}(|\psi\rangle, M_{pol}) = \begin{cases} 1 & \text{with } \Pr = \langle\psi|+\rangle\langle +|\psi\rangle = (\frac{1-\mathtt{b}}{\sqrt{2}} + \frac{\mathtt{b}}{\sqrt{2}})^2 = \frac{1}{2} \\ -1 & \text{with } \Pr = \langle\psi|-\rangle\langle -|\psi\rangle = (\frac{1-2b}{\sqrt{2}})^2 = \frac{1}{2} \end{cases}$$

The outcome of $\textsc{Meas}(|\psi\rangle, M_{pol})$ is decoded as $1 \mapsto \mathtt{b}=0,\ -1 \mapsto \mathtt{b}=1$

Proving Bennett and Brassard's intuition

Assuming $\mathtt{b}$ encoded as $|\psi\rangle = (1-\mathtt{b})\,|+\rangle + \mathtt{b}\,|-\rangle$

$$\textsc{Meas}(|\psi\rangle, M_{comp}) = \begin{cases} 0 & \text{with } \Pr = \langle\psi\,|\,0\rangle\,\langle 0\,|\,\psi\rangle = \left(\frac{-1^{\mathtt{b}}+-1^{(1-\mathtt{b})}}{\sqrt{2}}\right)^2 = \frac{1}{2} \\ 1 & \text{with } \Pr = \langle\psi\,|\,1\rangle\,\langle 1\,|\,\psi\rangle = \left(\frac{-1^{\mathtt{b}}+-1^{(1-\mathtt{b})}}{\sqrt{2}}\right)^2 = \frac{1}{2} \end{cases}$$

The outcome of $\textsc{Meas}(|\psi\rangle, M_{comp})$ is decoded as $0 \mapsto \mathtt{b}=0,\ 1 \mapsto \mathtt{b}=1$

$$\textsc{Meas}(|\psi\rangle, M_{pol}) = \begin{cases} 1 & \text{with } \Pr = \langle\psi\,|\,+\rangle\,\langle +\,|\,\psi\rangle = (1-\mathtt{b})^2 = (1-\mathtt{b}) \\ -1 & \text{with } \Pr = \langle\psi\,|\,-\rangle\,\langle -\,|\,\psi\rangle = \mathtt{b}^2 = \mathtt{b} \end{cases}$$

The outcome of $\textsc{Meas}(|\psi\rangle, M_{pol})$ is decoded as $1 \mapsto \mathtt{b}=0,\ -1 \mapsto \mathtt{b}=1$

The Bennett-Brassard protocol (BB84)

1. Message and measurement base choice
   - Alice generates a random classical bit sequence
   - Alice generates a random sequence of elements in $\{M_{comp}, M_{pol}\}$ of the same length of the classical bit sequence
   - Bob generates a random sequence of elements in $\{M_{comp}, M_{pol}\}$
2. Transmission and measurement
   - Alice sends the random bits, encoding them to be measurable properly according to the sequence of $\{M_{comp}, M_{pol}\}$ of her choice
   - Bob measures the qubit sequence according to his choice of $\{M_{comp}, M_{pol}\}$
3. Bob sends his choice of $\{M_{comp}, M_{pol}\}$
4. Alice compares the Bob's choice with hers and sends him the positions where they match
5. Both Alice and Bob employ only the bits which have been correctly measured: only Alice and Bob know the values of these bits

Alice encrypt the ptx by applying her random encryption sequence bit on bit.
Bob decrypts it with its measure seq.

A run of the Bennett-Brassard protocol

Step	Action	Data						
1	A draws rnd key	0	0	1	0	0	1	1
1	A draws rnd base	M_{pol}	M_{pol}	M_{comp}	M_{pol}	M_{comp}	M_{pol}	M_{pol}
1	B draws rnd base	M_{comp}	M_{pol}	M_{comp}	M_{comp}	M_{pol}	M_{pol}	M_{comp}
2	A sends	$\|+\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$	$\|-\rangle$	$\|-\rangle$
2	B Measures	\$	$\|+\rangle$	$\|1\rangle$	\$	\$	$\|-\rangle$	\$
3	B sends	M_{comp}	M_{pol}	M_{comp}	M_{comp}	M_{pol}	M_{pol}	M_{comp}
4	A sends	$\times$	$\checkmark$	$\checkmark$	$\times$	$\times$	$\checkmark$	$\times$
5	Both use		0	1			1	

Mismatches in the agreed key will be detected sending a (classically encrypted) fixed confirmation message with it

Considerations on the Bennett-Brassard protocol

Transmission costs

- The choices on the bases made by Alice and Bob are expected to agree with $\Pr = \frac{1}{2}$
- Two classical bits are sent for each qubit being sent
- On average, to share an l bit string we send $2l$ qubits and $4l$ bits

Security of the protocol against eavesdropper

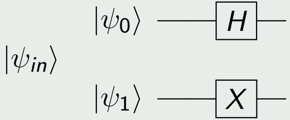
- Eve measures $\frac{1}{4}$ of the qubits correctly without being detected
- Eve measures $\frac{1}{2}$ of the (non dropped) qubits incorrectly, with a $\frac{1}{2}$ probability of being detected for each incorrect measure
- Eve is detected with $\Pr = 1 - \frac{1}{2^{l/4}}$ where l is the length of the key

→ High probability to detect if an intruder is in the middle of the connection

Actor	Measurement/Encoding choice			
Alice	M_{comp}	M_{comp}	M_{pol}	M_{pol}
Bob	M_{comp}	M_{pol}	M_{comp}	M_{pol}
Eve	M_{comp}	M_{comp}	M_{comp}	M_{comp}
Outcome	Eve sees b	A/B Drop b	A/B Drop b	Eve alters b

→ Detection.

Building circuits with more than one (unentangled) qubit



$|\psi_{out}\rangle =??$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}, \quad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

Reinterpreting single qubit gates

The two single-qubit gates can be seen as a single, two-qubit gate acting jointly on the entire state $|\psi_{in}\rangle = |\psi_0\rangle \otimes |\psi_1\rangle$

$$|\psi_{out}\rangle = (H \otimes X)\,|\psi_{in}\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} & \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\\ \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} & \begin{bmatrix}0 & -1\\ -1 & 0\end{bmatrix}\end{bmatrix}|\psi_{in}\rangle$$

Quantum circuits with single qubit gates and more qubits

An equivalent way of doing calculations

Equivalently, we can compute $|\psi_{out}\rangle$ evaluating each component of the fundamental computational basis separately (this allows us to concentrate on a single qubit at a time!)

$$|\psi_{in}\rangle = |0\rangle \otimes |0\rangle \quad \rightarrow \quad |\psi_{out}\rangle = H|0\rangle \otimes X|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

Checking the equivalence :

$$|\psi_{out}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$$

Bit commitment

Example of choosing who does the dishes by tossing a coin by telephone call

Goal

- Alice wants to commit on a yes-no decision of a choice, at a given time instant, but does not want to reveal the decision until later (hiding)
- Bob wants to be sure that Alice does not change her mind between the commitment and the moment in which she reveals the choice (binding)

Possible solutions

- Classical committments typically rely on the assumed hardness of a computational problem for either the binding or the hiding property
- Is it possible to exploit the properties of quantum computation to build a hiding and binding commitment scheme?

Quantum bit commitment protocol

Using an n qubit register to commit to a single bit yes-no choice

- Alice picks an integer n tuning the probability of the committment to be binding as $1 - \frac{1}{2^n}$
- Alice draws a random n classical bits string x
- Alice encodes x in an n unentangled qubits string $|\chi\rangle$
  - encoding each bit $\mathtt{b}$ as $(1-\mathtt{b})\,|0\rangle + \mathtt{b}\,|1\rangle$ to obtain a "yes" commitment
  - encoding each bit $\mathtt{b}$ as $(1-\mathtt{b})\,|+\rangle + \mathtt{b}\,|-\rangle$ to obtain a "no" commitment
- Alice sends $|\chi\rangle$ to Bob, who will store them
- Alice sends x to Bob and tells him to perform one of the following:
  - To measure $|\chi\rangle$ with M_{comp}, and match the measure with $x \rightarrow$ reveals "yes"
  - To measure $|\chi\rangle$ with M_{pol}, and match the measure with $x \rightarrow$ reveals "no"
- Correctness: if Alice and Bob follow the protocol, Bob will acknowledge correctly Alice's commitment every time

Quantum bit commitment protocol

Hiding property

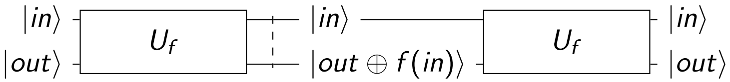
- Bob may try to violate the hiding property measuring $|\chi\rangle$. Assume Alice committed "no":
  - Measuring with M_{comp}, Bob obtains a sequence of uniformly random chosen bits as it is measuring information encoded in $\{|+\rangle, |-\rangle\}$ with M_{comp}
  - Measuring with M_{pol}, Bob obtains the exact value of x ... which is also a bit sequence picked from a uniform distribution!
- Bob cannot tell apart the randomness coming from Alice from the one coming from an ill-performed measurement

Quantum bit commitment protocol

Binding property

- Alice may try to violate the binding property revealing a different base for measurement. Assume Alice is trying to change her commitment after sending $|\chi\rangle$ to Bob
  - If she tries to change from "yes" to "no": $|\chi\rangle$ has each bit $\mathtt{b}$ encoded as $(1-\mathtt{b})|0\rangle + \mathtt{b}|1\rangle$ and Alice needs to send the expected outcome of the measure x, when $|\chi\rangle$ is measured in M_{pol}
  - If she tries to change from "no" to "yes": $|\chi\rangle$ has each bit $\mathtt{b}$ encoded as $(1-\mathtt{b})|+\rangle + \mathtt{b}|-\rangle$ and Alice needs to send the expected outcome of the measure x, when $|\chi\rangle$ is measured in M_{comp}
- In both cases Alice needs to predict the outcome of a measurement which will yield a fair coin toss for each bit. Resorting to guessing will yield a correct guess in 2^n on average.
- It looks like everything is ok... but we'll come back later to this

General model of quantum computation



Quantum circuits

- Computing a generic function with a quantum computer requires the computation to be reversible
- Since we want to compute any arbitrary (possibly non reversible) function $f(in)$ of the input *in*, we need a framework to express it in reversible form
- The most general one is to consider a circuit equivalent to the computation $U_f |in\rangle |out\rangle = |in\rangle |out \oplus f(in)\rangle$, where U_f is a unitary operator
- The operation is reversible, applying U_f to the result yields the inputs back $\rightarrow$ U_f is its own inverse, thus $U_f = U_F^\dagger$ thus U_f is real.

General model of quantum computation

Getting real valued operators

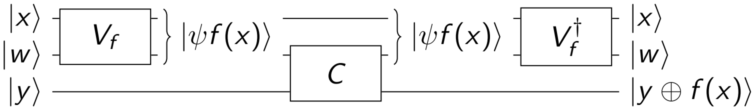
Bennet-Bernstein-Brassard-Vazirani in [1] proved that, given a complex unitary operator U, acting on n qubits, it is always possible to build another operator U' such that

- U' has only real coefficients (thus, $U' = U'^{\dagger}$)
- U' acts on $n+1$ qubits
- U' computes, on its first n qubits the same function as U
- U' uses the additional qubit as an additional dimension to store, during computation, the real and imaginary parts of the complex values of U

Rewrite $U\left|x\right\rangle$ on n qubits as either:

$$U'(\left|x\right\rangle\left|0\right\rangle) = [\underbrace{\Re(U)}_{\text{Real part}}\left|x\right\rangle]\left|0\right\rangle + [\underbrace{\Im(U)}_{\text{Imaginary part}}\left|x\right\rangle]\left|1\right\rangle \text{ or } U'\left|x\right\rangle\left|1\right\rangle = (-\Im(U)\left|x\right\rangle)\left|0\right\rangle + \Re(U)\left|x\right\rangle\left|1\right\rangle$$

General model of quantum computation



A typical construction

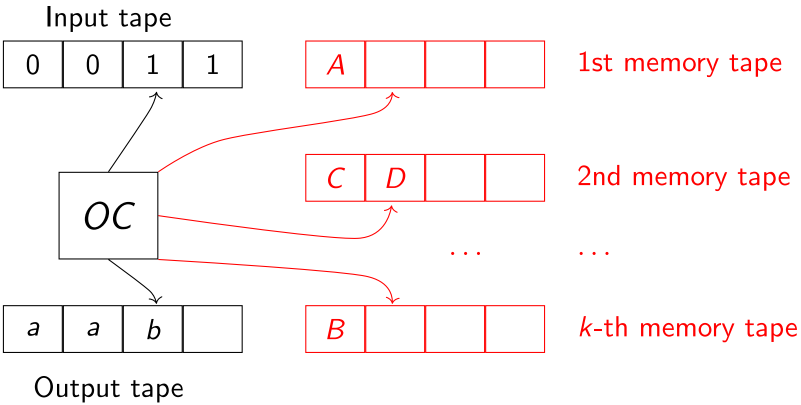
- Auxiliary qubits (a.k.a. ancillae/garbage) $|w\rangle$ are often employed, and are initialized to a fixed, known state, independent from $|x\rangle$
- While it is possible to build a single unitary operator U_f, the typical algorithm design strategy proceeds as follows
  1. Compute the required function, writing the result $f(x)$ to a subset of qubits of $|xw\rangle$ (operator V_f)
  2. Add the results to a set of dedicated qubits for output ($|y\rangle$) via an appropriate operator C
  3. Revert the computation made by V_f to free the $|xw\rangle$ qubits for further use (uncompute phase)
- C can be built as a set of n two-qubit unitary gates

What can we compute?

- Which computations can we express in the quantum circuit formalism?
- Can we emulate a classical circuit computation? At which cost?
- Can we emulate any classical computation?

Turing machine model

Proposed in [6] to model general computation



Classical Computability refresher

Church-Turing thesis

Every effectively computable function can be computed by a TM.

- effectively computable = computed by a procedure written before seeing the input, terminating in finite time for any input

Turing equivalence

- It can be proved that the following models are equivalent to a TM
  - A machine with (infinite) Randomly Accessible Memory and a finite controller implementing a program (RAM machine, often shortened in just "RAM")
    - This includes a concrete implementation where the controller is realized as a Boolean circuit accessing addressable memory
  - Programs expressed as flowcharts allowing instruction sequences, selection constructs and conditional loops → can be computed by a TM.

Classical Computability refresher

Boolean Circuits and computability

- It is possible to implement any TM with a synchronous circuit with Boolean gates, and single-bit synchronous memory elements
- Removing the memory elements prevents the program from having a state, making it impossible to model infinite/input dependant loops
- Countable loops can still be unrolled, obtaining the corresponding Boolean circuits

NAND completeness

- It is possible to prove that a combination of NAND gates, corresponding to the Boolean function $f_{\mathrm{NAND}}(a, b) = \overline{ab}$, is sufficient to build any combinatorial Boolean circuit

Turning functions into reversible functions

Showing emulatability of classical Boolean Functions

- Classic logic gates may be irreversible (e.g., `AND`, `XOR`, `NAND`) while quantum gates are unit operators and therefore reversible
- How do we represent classic computations as unit transformations?
- The first step is to transform every irreversible classic computation in a reversible one. To this end, the function at hand (the one that must be "quantumly" evaluated) must be a **bijection** (i.e., injective and surjective)

Transforming a function in a bijection

Given a function $f : \{0,1\}^k \mapsto \{0,1\}^m$ we can define a bijective relation

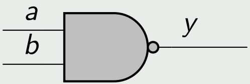
$$\widetilde{f} : \{0,1\}^{k+m} \mapsto \{0,1\}^{k+m}, \qquad (x, 0^m) \mapsto (x, f(x))$$

where 0^m denotes m null (classic) bits

A classical reversible NAND exists

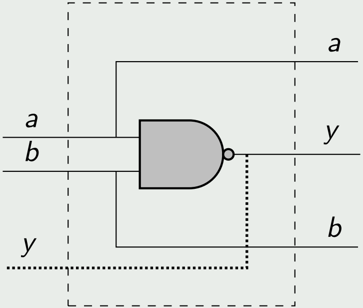
Building a reversible NAND gate is enough to reversibly compose any Boolean function. A reversible NAND exists, thus all Boolean functions can be written reversibly

Classic NAND $y = \overline{ab}$



We now "just" need a quantum equivalent of the reversible NAND gate to perform full emulation

Reversible NAND $y = \overline{ab}$



The aim is building the same gate exploiting quantum principles.

A first 2-qubit quantum gate

The C-NOT Gate

It is described by a permutation matrix swapping the amplitudes of $|10\rangle$ and $|11\rangle$ in the computational basis decomposition of the two-qubit input state.

$$\texttt{C-NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

if $b_0 = 0 \Rightarrow b_1$ is not negated

if $b_0 = 1 \Rightarrow b_1$ is negated

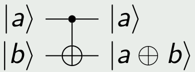
$\texttt{C-NOT}\,|00\rangle = |00\rangle$ 1st matrix col.

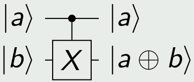
$\texttt{C-NOT}\,|01\rangle = |01\rangle$ 2nd matrix col.

$\texttt{C-NOT}\,|10\rangle = |11\rangle$ 3rd matrix col.

$\texttt{C-NOT}\,|11\rangle = |10\rangle$ 4th matrix col.

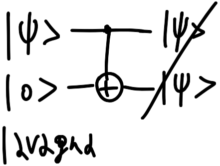
It is often thought as some sort of "quantum analogue" of the classic XOR gate:





If the *control qubit* $|a\rangle$ is in the fundamental state $|1\rangle$, then the *target qubit* $|b\rangle$ becomes $|a \oplus b\rangle$, i.e., becomes the "negated version" of $|b\rangle$ (...same as applying an X gate to it)

No-cloning



Is it possible to build a circuit that makes a copy of a qubit?

- You may be tempted to use a `C-NOT` with
  - the input *control qubit* in a generic state $|x\rangle$
  - the input *target qubit* in the fundamental state $|0\rangle$

  In such a way to get a copy of the state of the input control qubit into the output target qubit.
- The previous reasoning is flawed! Indeed, such a derivation can be applied only to classic bits (i.e., when picking the inputs among the fundamental states).
  It cannot be applied for an input state $|\psi\rangle|0\rangle$, with $|\psi\rangle = a|0\rangle + b|1\rangle$.
- The actual output of the circuit is: $|\psi_{\mathtt{out}}\rangle = a|00\rangle + b|11\rangle$, while the desired output state would be

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

  this state cannot be equal to the actual output, $|\psi_{\mathtt{out}}\rangle$, of the circuit unless $ab = 0$

No-cloning Theorem

Theorem

There is no unit operator U such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ for a generic $|\psi\rangle$.

Proof by contradiction.

Assume that U such that $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ exists.
We can pick two qubits $|\psi\rangle$ and $|\phi\rangle$ with $0 < \langle\psi\,|\,\phi\rangle < 1$:
$|\psi\rangle = |0\rangle$ and $|\phi\rangle = |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ where $\langle\psi|\phi\rangle = \frac{1}{\sqrt{2}}(\langle 0|0\rangle + \langle 0|1\rangle) = \frac{1}{\sqrt{2}}$.
By contrad. hypothesis U clones both: $U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle, \quad U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$

Computing the $\langle\cdot\,|\,\cdot\rangle$ of the left and right members, member-wise:

1. $\langle U\psi 0\,|\,U\phi 0\rangle = \left\langle U^\dagger U\psi 0\,\middle|\,\phi 0\right\rangle = \langle\psi\,|\,\phi\rangle\langle 0\,|\,0\rangle = \langle\psi\,|\,\phi\rangle$
2. $\langle\psi\psi\,|\,\phi\phi\rangle = \langle\psi\,|\,\phi\rangle\langle\psi\,|\,\phi\rangle$

the conclusion that $\langle\psi\,|\,\phi\rangle = \langle\psi\,|\,\phi\rangle^2$ contradicts the hypothesis!

Syntactic sugar

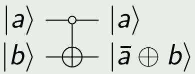
Reverse-controlled CNOT

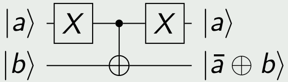
A reverse-controlled CNOT swaps the amplitudes of $|01\rangle$ and $|00\rangle$

$$\texttt{RC-NOT} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\texttt{RC-NOT}\,|00\rangle = |01\rangle$ 1st matrix col.
$\texttt{RC-NOT}\,|01\rangle = |00\rangle$ 2nd matrix col.
$\texttt{RC-NOT}\,|10\rangle = |10\rangle$ 3rd matrix col.
$\texttt{RC-NOT}\,|11\rangle = |11\rangle$ 4th matrix col.

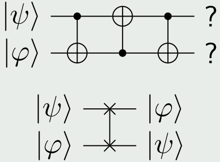
Its name is justified by the behaviour on classical bits encoded in the computational basis: it effectively considers the opposite value of the controller bit and acts as a CNOT





Composing CNOTs

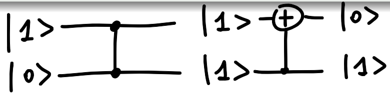
Consider the following quantum circuit, and its effects on the two input qubits



$|00\rangle \quad |01\rangle \quad |10\rangle \quad |11\rangle$

swapping operation

What is the unit matrix of the swap operator ?



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

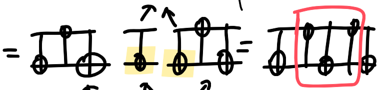
$\Rightarrow sw|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|10\rangle + \alpha_{10}|01\rangle + \alpha_{11}|11\rangle$

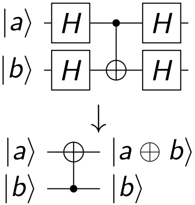
Interesting equivalences

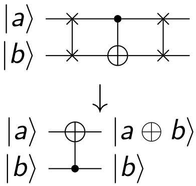
$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \ldots = \alpha_{00}|00\rangle + \alpha_{11}|01\rangle + \alpha_{10}|10\rangle + \alpha_{01}|11\rangle$

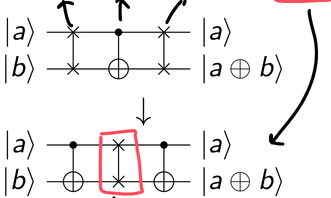
can be removed, for some reason

swap operator









swap operator

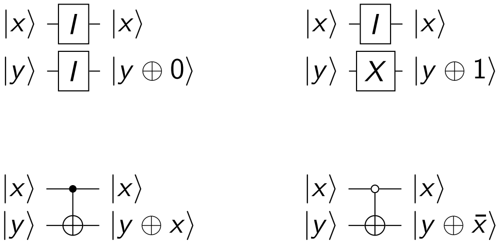
$$|\psi\rangle = \frac{1}{2}\left(a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle = \right.$$

$$= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle \ldots$$

Implementing all single qubit $f(x)$ in the general framework

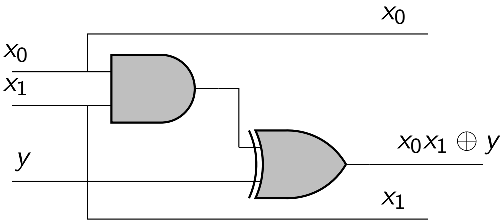
As an example, we show how to implement in the general computation model all four classical, single qubit functions

Function $f(x)$	Input 0	1
$f(x) = 0$	$f(0) = 0$	$f(1) = 0$
$f(x) = 1$	$f(0) = 1$	$f(1) = 1$
$f(x) = x$	$f(0) = 0$	$f(1) = 1$
$f(x) = \bar{x}$	$f(0) = 0$	$f(1) = 1$



The classic Toffoli gate

In 1980 Tommaso Toffoli [5] proposed a universal reversible classical gate with the goal of achieving low-power classical reversible computing:



$T(a,b,c) = ab \oplus c$

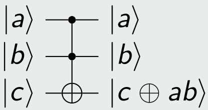
The Toffoli gate is Boolean complete, as the NAND gate is: it is sufficient to set input y to 1.

A three qubit quantum gate

The function computed by the classical Toffoli gate is also quantum constructible. Its version acting on qubits is known as `CCNOT`.

Controlled-Controlled NOT `C-CNOT`

$$
\begin{aligned}
\texttt{C-CNOT}\,|000\rangle &= |000\rangle \\
\texttt{C-CNOT}\,|001\rangle &= |001\rangle \\
\texttt{C-CNOT}\,|010\rangle &= |010\rangle \\
\texttt{C-CNOT}\,|011\rangle &= |011\rangle \\
\texttt{C-CNOT}\,|100\rangle &= |101\rangle \\
\texttt{C-CNOT}\,|101\rangle &= |100\rangle \\
\texttt{C-CNOT}\,|110\rangle &= |111\rangle \\
\texttt{C-CNOT}\,|111\rangle &= |110\rangle
\end{aligned}
$$



What is the matrix representation of the `C-CNOT`?

A three qubit quantum gate

Controlled-Controlled NOT ($\texttt{C-CNOT}$)

$$|\psi\rangle = \sum_{k=0}^{7} \alpha_{\texttt{bin}(k)} |\texttt{bin}(k)\rangle$$

$$\texttt{CCNOT} |\psi\rangle = \alpha_{111} |110\rangle + \alpha_{110} |111\rangle + \sum_{k=0}^{5} \alpha_{\texttt{bin}(k)} |\texttt{bin}(k)\rangle$$

$$\texttt{C-CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

- In a generic three-qubit state, it swaps α_{110} with α_{111}
- Computes the Toffoli gate on classical bits, each one encoded as $\{|0\rangle, |1\rangle\}$
- It is its own inverse (it represents a permutation between two elements)

Boolean emulation universality

CCNOT is Boolean-emulation universal

- The CCNOT gate emulates the classical NAND gate if each input bit $\mathtt{b}$ is encoded as $(1 - \mathtt{b})|0\rangle + \mathtt{b}|1\rangle$ classical bits and $|c\rangle$ is set to $|1\rangle$.
- It is thus possible to emulate any Boolean circuit with a quantum circuit with an appropriate combination of CCNOTs
- Emulating a NAND with a CCNOT costs 1 gate and 3 qubits; the number of qubits needed is at most linear in the number of NANDs
- Note: the CNOT alone does not allow complete Boolean emulation

On emulating classical computing

Matching classic TMs

- We have described how, with a quantum circuit, we can emulate a classical one
  - This is sufficient to show that any finite-time classical computation can be quantum-emulated
- To obtain Turing completeness, we need to handle arbitrary loops
  - Quantum Turing machines [2] meet the requirement but tells us little on their realizability

A concrete fitting model

- A recent model [3] proposes to employ a RAM augmented with a qubit register
- The RAM machine may either execute classical assembly on the classical memory, or apply quantum gates to the qubit register
- The model fits how actual quantum computers are designed, and is Turing complete

Summing up: QC have the same expressivity, the interesting part will be efficiency

The Z gate

The Z gate provides a fundamental building block in many algorithms.

Recall that it is defined by the following unit matrix $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi} \end{bmatrix}$ → phase factor

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

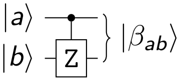
Is a swap operator for |+> and |-> bases

Effects of the Z gate

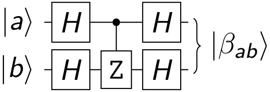
- The Z gate changes the sign amplitude of the $|1\rangle$ component
- This has no measurable effect on the eigenvec.s of M_{comp}
- Acts as "an analog" for X for the eigenvec.s of M_{pol}

The Controlled-Z gate

$$\mathtt{CZ} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$ visually represented similarly to the `CNOT`



It is interesting to analyze the effect of the following circuit:



- $HZH\,|00\rangle = HZH\,|{+}{+}\rangle = H\frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ -1 \end{bmatrix}$
- $HZH\,|10\rangle = HZH\,|{-}{+}\rangle = H\frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix}$
- $HZH\,|01\rangle = HZH\,|{+}{-}\rangle = H\frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix}$
- $HZH\,|11\rangle = HZH\,|{-}{-}\rangle = H\frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = |11\rangle$

Quantum universality

CCNOT decomposition

A CCNOT gate can be decomposed as a combination of H, CNOT and T gates [4], where

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}; \text{ noting that } T^4 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

CCNOT and H are quantum universal

Any unitary operator can be built as a composition of CCNOTs and H gates.

Efficient approximation (Solovay-Kitaev)

- Given a set of universal quantum gates, and a desired approximation precision ϵ for the output amplitudes of a generic unitary operator U acting on a finite number of qubits, it is possible to approximate it with a combination of the universal gates in polylog$(\frac{1}{\epsilon})$

What we can compute with quantum circuits

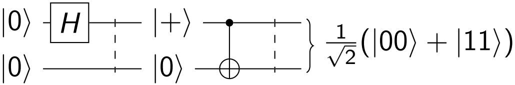
- Which computations can we express in the quantum circuit formalism?
  - All boolean functions (=total effectively computable functions) can be computed, as they run in finite time (=finite circuit depth)
- Can we emulate a classical circuit computation with a quantum circuit? At which cost?
  - Yes. Translating a classical gate into a quantum gate can be done with constant computation time (=circuit depth overhead). The spatial overhead may grow: we need extra qubits to store the intermediate results as destructive overwriting is not allowed.
- Can we emulate any classical computation with a quantum circuit?
  - Provided it is non-countable loop free, yes. Turing completeness requires an external controller and memory to model infinite loops.
- Models for quantum TMs and RAMs have been proposed: their expressive power is equivalent to their classical analogues

A closer look at CNOT

- A CNOT acting on basis states is fully classically emulatable (computing a classical linear function in $\mathbb{F}_2$
- Consider now a CNOT acting on $|+\rangle\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle$:

$$|+\rangle\,|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \quad H(|+\rangle\,|0\rangle) = H\left(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- The outcome is a two-qubits entangled state!



Generalized Born Rule (GBR) - an operative description

Goal

Given a n qubit state $|\psi\rangle$, we want to:

- measure one or more of its qubits, but not all of them,
- find out both the probabilities of the measurement outcomes
- find the states into which the system collapses after measurement

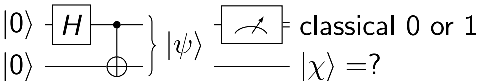
Reminder: the GBR states that, if more than a qubit is measured, the order of the measurements does not matter $\rightarrow$ we consider a single-qubit measurement. We will measure with an apparatus represented by M_{comp}.

Generalized Born Rule (GBR) - an operative description

Procedure

1. Suppose you want to measure the i-th qubit of the state
2. Fully decompose $|\psi\rangle$ in the computational basis $|\psi\rangle = \sum_{a=0}^{2^n-1} \alpha_a |bin(a)\rangle$
3. Collect in two sets $\mathbf{S}_0, \mathbf{S}_1$ the components of $|\psi\rangle$ with their amplitudes according to the value taken by the qubit you want to measure in them.
   - $\mathbf{S}_0$ will contain all the components of $|\psi\rangle$ where a_i in $bin(a) = (a_{n-1}, \ldots, a_0)_2$ equals 0
   - $\mathbf{S}_1$ will contain all the components of $|\psi\rangle$ where a_i in $bin(a) = (a_{n-1}, \ldots, a_1)_2$ equals 1
4. Obtain the probability of measuring $b \in \{0, 1\}$, $p_b = \displaystyle\sum_{\alpha_i |bin(i)\rangle \in \mathbf{S}_b} |\alpha_i|^2$
5. Obtain the state in which the system collapses after measuring b, $|\psi_b\rangle = \frac{1}{\sqrt{p_b}} \displaystyle\sum_{s \in \mathbf{S}_b} s$
   - note that the i-th qubit of all the elements in S_b is equal to b

An interesting effect of entanglement

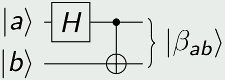


- Consider the quantum circuit above, assuming the measurement is modeled by M_{comp}.
- What is the value of $|\chi\rangle$ after the first qubit is measurement?
- Recalling the Generalized Born Rule:
  - The pre-measurement $|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ is rewritten as $\alpha_0|0\rangle|\phi_0\rangle + \alpha_1|1\rangle|\phi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$
  - We then obtain the post-measurement states as:
    - when 0 is measured (corresponding eigenv. $|\ell_{0,M_{comp}}\rangle = |0\rangle$) $|0\rangle|\phi_0\rangle = \frac{1}{\alpha_0}\gamma_0|0\rangle|0\rangle = |0\rangle|0\rangle$
    - when 1 is measured (corresponding eigenv. $|\ell_{1,M_{comp}}\rangle = |1\rangle$)$|1\rangle|\phi_1\rangle = \frac{1}{\alpha_1}\gamma_1|1\rangle|1\rangle = |1\rangle|1\rangle$
  - The measurement probabilities are $\alpha_0^2 = \frac{1}{2}$, $\alpha_0^2 = \frac{1}{2}$
- Measuring one qubit univocally determines the state of the other!

Quantum circuits with two qubits

Bell States or Enstein Podolsky Rosen (EPR) qubit pairs

These are quantum states that do not exhibit any similarity with a classic computational state. They are defined as the output (entangled) states $|\beta_{ab}\rangle$ of the following circuit



fed with one of the vectors of the fundamental basis in $\mathbb{C}^{\otimes 2}$: $|ab\rangle$, with $a, b \in \{0, 1\}$. They are

$$|\beta_{00}\rangle \mapsto \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\beta_{01}\rangle \mapsto \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad |\beta_{10}\rangle \mapsto \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |\beta_{11}\rangle \mapsto \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Measuring any single qubit out of two in them will collapse the other to a deterministic state

Going Back to Quantum Bit commitments

- Before analyzing entanglement, we had a perfectly hiding and statistically binding bit commitment technique.
- Focusing on the binding part, the technique went as:
    - Alice sends $|\psi\rangle$ an n qubit register to Bob, made of either a random sequence of $\{|0\rangle, |1\rangle\}$ (committing to "yes") or a random sequence of $\{|+\rangle, |-\rangle\}$ (committing to "no")
    - To reveal her committment, Alice reveals either M_{comp} (for "yes") or M_{pol} (for "no") and the expected value of the measurement to be made by Bob
- The commitment is binding if Alice cannot guess the outcome of a measurement with an instrument different from the one for which the commitment is built

A cheating strategy with entanglement

- Alice prepares n EPR pairs $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|{+}{+}\rangle + |{-}{-}\rangle)$, and sends the first qubit of each pair as $|\chi\rangle$ to Bob
  - Note that the qubits in $|\chi\rangle$ can only be fully described with the ones in Alice's possession
- To change the commitment to "yes" she measures the qubits in her possession with M_{comp}, obtaining the classic result x and sends x, M_{comp} to Bob
  - By measuring her qubits in M_{comp}, the ones in Bob's possession collapse to either $|0\rangle$ or $|1\rangle$ due to the entanglement, and Alice knows which one
- To change the commitment to "no" she measures the qubits in her possession with M_{pol}, obtaining the classic result x and sends x, M_{pol} to Bob
  - By measuring her qubits in M_{comp}, the ones in Bob's possession collapse to either $|+\rangle$ or $|-\rangle$ due to the entanglement, and Alice knows which one
- Designing a working quantum bit commitment protocol is an open problem

Textbook references

- Chapter 1
- Chapter 2 up to 2.3
- Chapter 6 up to 6.3

Bibliography I

Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani.
Strengths and weaknesses of quantum computing.
SIAM J. Comput., 26(5):1510–1523, 1997.

Ethan Bernstein and Umesh V. Vazirani.
Quantum complexity theory.
SIAM J. Comput., 26(5):1411–1473, 1997.

Samuel Jaques and John M. Schanck.
Quantum cryptanalysis in the RAM model: Claw-finding attacks on SIKE.
In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part I*, volume 11692 of *Lecture Notes in Computer Science*, pages 32–61. Springer, 2019.

Yaoyun Shi.
Both toffoli and controlled-not need little help to do universal quantum computation, 2002.

Tommaso Toffoli.
Reversible computing.
In J. W. de Bakker and Jan van Leeuwen, editors, *Automata, Languages and Programming, 7th Colloquium, Noordweijkerhout, The Netherlands, July 14-18, 1980, Proceedings*, volume 85 of *Lecture Notes in Computer Science*, pages 632–644. Springer, 1980.

A. M. Turing.
On computable numbers, with an application to the entscheidungsproblem.
Proceedings of the London Mathematical Society, s2-42(1):230–265, 1937.

Bibliography II