Introduction to Quantum Computing (Lecture 3)

Gerardo Pelosi

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

March 11th, 2022

Elitzur-Vaidman bomb tester (1/5)

- The Elitzur–Vaidman bomb-tester is a quantum mechanics thought experiment that uses interaction-free measurements to verify that a bomb is functional without having to detonate it.
- It is interesting because there is no classical alternative that allows us to do the same ! It proves that quantum physical phenomena are quite different from the ones we have experience upon in our macroscopic world.
- It was conceived in 1993 by Avshalom Elitzur and Lev Vaidman. Since their publication, real-world experiments have confirmed that their theoretical method works as predicted.
- The bomb tester takes advantage of two characteristics of elementary particles, such as photons or electrons: nonlocality and wave–particle duality. By placing the particle in a quantum superposition, it is possible for the experiment to verify that the bomb works without triggering its detonation, although there is still a 50% chance that the bomb will detonate in the effort.

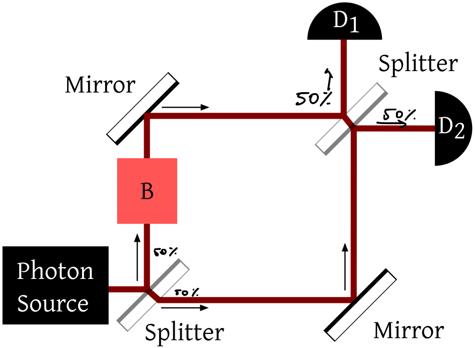
Elitzur-Vaidman bomb tester (2/5)

A thought experiment [1]

Is it possible to detect whether a box contains a light sensitive explosive, without detonating the explosive itself?

- Assumption: a box not containing the explosive (i.e., a dud) will let anything pass through, an explosive detecting box (i.e., an actual bomb triggered by a light sensor) will absorb the single photon emitted from the source once in two times
- Solution: place the box in one of the two light paths of a Mach-Zehnder interferometer.

  Tune distances among mirrors and splitters so that with an empty MZ interferometer only D_2 is lit up (or clicks), while the destructive interference on D_1 leaves it in the dark.
- A physical realization of the experiment was performed in [2]



Elitzur-Vaidman bomb tester (3/5)

Modeling the components

- Denote a photon passing through the first splitter as $|0\rangle$ and one going up as $|1\rangle$
- 50-50 splitters are modeled by the following unitary operator $B = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}$
    - $B|0\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, B|1\rangle = \frac{i|0\rangle + |1\rangle}{\sqrt{2}}$
- Mirrors are modeled by the following unitary operator $M = \begin{bmatrix}0 & i\\ i & 0\end{bmatrix}$
    - $M|0\rangle = i|1\rangle, M|1\rangle = i|0\rangle$

Elitzur-Vaidman bomb tester (4/5)

Modeling the components when the box is empty (=transparent)

- recalling that: $B\left|0\right\rangle = \frac{\left|0\right\rangle + i\left|1\right\rangle}{\sqrt{2}}, B\left|1\right\rangle = \frac{i\left|0\right\rangle + \left|1\right\rangle}{\sqrt{2}}$ and $M\left|0\right\rangle = i\left|1\right\rangle, M\left|1\right\rangle = i\left|0\right\rangle$
- assume a $\left|0\right\rangle$ photon state is emitted. It will thus evolve as $BMB\left|0\right\rangle = BM\left[\frac{1}{\sqrt{2}}(\left|0\right\rangle + i\left|1\right\rangle)\right] = B\left[\frac{1}{\sqrt{2}}(-\left|0\right\rangle + i\left|1\right\rangle)\right] = -\left|0\right\rangle$
- assume a $\left|1\right\rangle$ photon state is emitted. It will thus evolve as $BMB\left|1\right\rangle = BM\left[\frac{1}{\sqrt{2}}(i\left|0\right\rangle + \left|1\right\rangle)\right] = B\left[\frac{1}{\sqrt{2}}(i\left|0\right\rangle - \left|1\right\rangle)\right] = -\left|1\right\rangle$
- If the photon emitted from the source is a superimposition of the previous cases, the linearity guarantees the same conclusions
- Photons pass through unchanged (save for an unmeasurable global phase change) and only detector D_2 is lit up.

Elitzur-Vaidman bomb tester (5/5)

Modeling the components when the box contains a bomb

M-Z interferometer

- The bomb actively blocks the vertical branch of the MZI (up B and M are not met). Denote as $|s\rangle$ the state of the photon being scattered by the bomb
- a $|0\rangle$ photon state will thus evolve as $BMB|0\rangle = BM\left[\frac{1}{\sqrt{2}}(|0\rangle + i|s\rangle)\right] = B\left[\frac{1}{\sqrt{2}}(i|1\rangle + i|s\rangle)\right] = \frac{i}{\sqrt{2}}B|s\rangle + \frac{1}{2}(i|1\rangle - |0\rangle)$
- If a bomb is present, both detectors 50%-50% detect a photon, if there is no bomb (see previous slides) only one of them will (D_2)
- If a photon is detected by D_2 nothing can be told, but if a photon is detected by D_1 a bomb is present (and it has not been triggered)
  - A photon detected by D_1 occurs with $\Pr = \frac{1}{4}$, as the scattering occurs with $\Pr = \frac{1}{2}$ and D_2 may click if a bomb is present with $\Pr = \frac{1}{4}$)

→ it is possible to set mirror distances in order to reach this situation ?

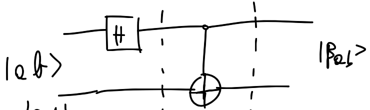
- If the bottom splitter leaves the photon pass through 99.9% of the times, the probability of an explosion becomes 0.1% and the probability of a bomb detection w/o detonating it (D_1) is ≈ 50%

Eckert QKD protocol (1/3)

$|+-\rangle = |+\rangle \times |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = \frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)$

Entangled

- Use EPR pairs $|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{2}$; the first qubit is sent to Alice, the second to Bob
- Recall that:
  - $|-+\rangle = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)$
  - $|+-\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
- Note that: $\frac{|01\rangle-|10\rangle}{\sqrt{2}} = \frac{|-+\rangle \ - \ |+-\rangle}{\sqrt{2}}$
- Consider the effects of measuring the first qubit:



$a,b \in \{0,1\}$

$|\beta_{11}\rangle = CNOT((H|1\rangle \otimes I|0\rangle) = CNOT\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}|1\rangle\right) =$
$= CNOT\left(\frac{|01\rangle-|11\rangle}{\sqrt{2}}\right) = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$

$$\textsc{Meas}(|\beta_{11}\rangle, M_{comp}) = \begin{cases} 0 & \text{with Pr} = |\alpha_0|^2 = \frac{1}{2} \text{ leaving } |\beta_{11}\rangle \text{ as } \sqrt{2}\frac{1}{\sqrt{2}}|0\rangle|1\rangle = |01\rangle \\ 1 & \text{with Pr} = |\alpha_1|^2 = \frac{1}{2} \text{ leaving } |\beta_{11}\rangle \text{ as } \sqrt{2}(-\frac{1}{\sqrt{2}})|1\rangle|0\rangle = -|10\rangle \end{cases}$$

$$\textsc{Meas}(|\beta_{11}\rangle, M_{pol}) = \begin{cases} 1 & \text{with Pr} = |\alpha_+|^2 = \frac{1}{2} \text{ leaving } |\beta_{11}\rangle \text{ as } \sqrt{2}(-\frac{1}{\sqrt{2}})|+\rangle|-\rangle = -|+-\rangle \\ -1 & \text{with Pr} = |\alpha_-|^2 = \frac{1}{2} \text{ leaving } |\beta_{11}\rangle \text{ as } \sqrt{2}\frac{1}{\sqrt{2}}|-\rangle|+\rangle = |-+\rangle \end{cases}$$

Eckert QKD protocol (2/3)

Exploited properties

- Key point 1: regardless of the basis in which the first qubit is measured $|\beta_{11}\rangle$ yields one of the two eigenvalues as a fair coin toss
- Key point 2: regardless of the basis in which the first qubit is measured $|\beta_{11}\rangle$ will collapse the two qubits into a base state, where the second qubit is the "opposite" of the first

The protocol

1. n $|\beta_{11}\rangle$ EPR pairs are prepared, one qubit from each is sent to Alice, the other to Bob
2. Alice and Bob randomly draw a sequence of n items from $\{M_{comp}, M_{pol}\}$ and measure the sequence of qubits they receive according to the drawn sequence of measurement operators
3. Once they both completed the measurements, they reveal each other the sequence of $\{M_{comp}, M_{pol}\}$ they used:
   the results of the measurements made in the same way become the shared key; (...Bob must flip his bits to get the same string as Alice)

Eckert QKD protocol (3/3)

Detecting eavesdroppers

- Eve measures either the qubits being delivered to Alice or the ones delivered to Bob (breaking the entanglement of the EPR)
- This can be detected computing a sample "Index" (...a formula fed with hundreds of samples...) on the classical bits measured by Alice and Bob when they chose different measurement bases. If this Index (aka "correlation") is < 2 then the "Bell's thm" guarantees that the measurements done can be explained/emulated w/o considering the entanglement ⇒ there were an evesdropper

Efficiency

1. Eckert's protocol has the same transmission efficiency of BB84 (1 key bit requires 2 qubits+4 bits on average) but reuses ill-measured qubits for adversary detection (*better* than BB84 where the adversary is detected after the agreement via a confirmation message)

   in this case the confirmation message is not necessary.

2. if Eve measures with the same operator of Alice and Bob, then she successfully forces them to agree on a bit that she also knows (... this occurs with 25% probability – same as BB84)

Quantum circuits with two qubits - Quantum Teleportation

Teleportation problem

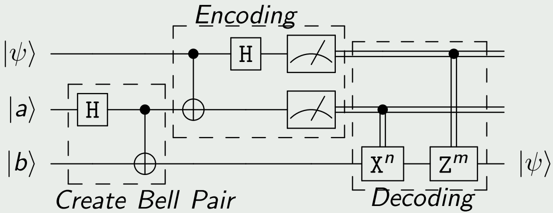
In a communication scenario, one of the two endpoints (e.g., Alice and Bob), wants to transfer the knowledge of a single qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to her/his counterpart.

Note that:

- The sender does not know the exact status of the qubit $|\psi\rangle$ (s/he cannot measure it without destroying it)
- the no-cloning theorem prevents her/him to make a copy
- the sender can still transfer classic bits on classic communication channels to her/him counterpart

The two endpoints can succeed in solving the problem, employing an EPR pair $|\beta_{ab}\rangle\,,\ a, b \in \{0, 1\}$

Quantum Teleportation

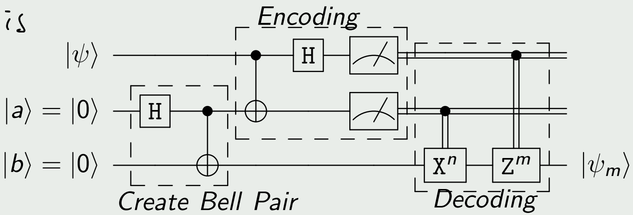


- Sender and receiver generates a EPR pair $|\beta_{ab}\rangle$, with $a, b \in \{0, 1\}$ and are able to keep, at their own side, one of the two (entangled) EPR qubits
- the sender combines $|\psi\rangle$ with her/his own qubit of the EPR pair and applies a `C-NOT` gate followed by a `H` gate and proceeds to measure
- after a measurement, 2 classic bits, named m and n in the figure, are sent to the receiver
- The receiver employs her/his own qubit of the EPR pair, say it $|\varphi\rangle$, and applies the gate $\mathtt{X}^n\ \mathtt{Z}^m$ re-deriving $|\psi\rangle$ as $|\psi\rangle = \mathtt{X}^n\ \mathtt{Z}^m\,|\varphi\rangle$

Quantum Teleportation

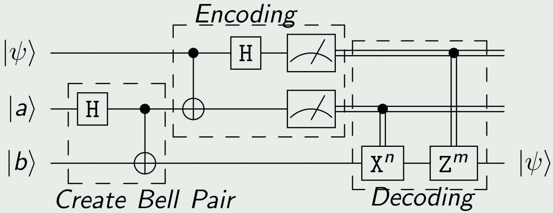
How the receiver is able to build up again the ψ from φ and n,m? Lets analyze this example.

$a = b = |0>$



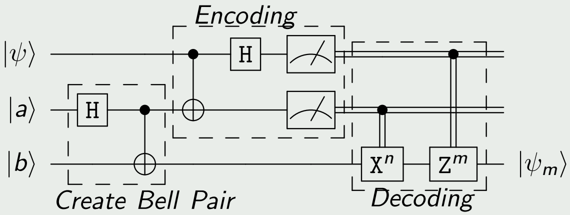
- just before the "Encoding stage" of the circuit, at the sender side we have:
  $|\psi\rangle\,|\beta_{ab}\rangle = \frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\right]$ $\psi = \alpha|0> + \beta \cdot |1>, |\alpha^2| + |\beta|^2 = 1$ $, \beta_{00} = |00$
- after the C-NOT gate
  $$\frac{1}{\sqrt{2}}\left[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\right]$$
- after the H gate
  $$\frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

Quantum Teleportation



- the state of the qubits just before the measurement can be rewritten as:
  $\frac{1}{2}\left[|00\rangle\left(\alpha|0\rangle+\beta|1\rangle\right)+|01\rangle\left(\alpha|1\rangle+\beta|0\rangle\right)\right]+$
  $+\frac{1}{2}\left[|10\rangle\left(\alpha|0\rangle-\beta|1\rangle\right)+|11\rangle\left(\alpha|1\rangle-\beta|0\rangle\right)\right]$
- after the measurement on the pair of qubits available to her, the sender gets $\mathtt{mn}\in\{00,01,10,11\}$
- possible states of the other qubit in the EPR pair can be:
  $\mathtt{mn}=00\Rightarrow\alpha|0\rangle+\beta|1\rangle$ $\mathtt{mn}=01\Rightarrow\alpha|1\rangle+\beta|0\rangle$
  $\mathtt{mn}=10\Rightarrow\alpha|0\rangle-\beta|1\rangle$ $\mathtt{mn}=11\Rightarrow\alpha|1\rangle-\beta|0\rangle$

Quantum Teleportation



- state of the qubits just before the measurement:
  $\frac{1}{2}\left[|00\rangle(\alpha|0\rangle+\beta|1\rangle)+|01\rangle(\alpha|1\rangle+\beta|0\rangle)\right]+\frac{1}{2}\left[|10\rangle(\alpha|0\rangle-\beta|1\rangle)+|11\rangle(\alpha|1\rangle-\beta|0\rangle)\right]$

Measure mn	third qubit	Corrections	Final output
00	$\alpha\|0\rangle+\beta\|1\rangle$	X^0Z^0	$\|\psi\rangle=\alpha\|0\rangle+\beta\|1\rangle$
01	$\alpha\|1\rangle+\beta\|0\rangle$	X^1Z^0	$\|\psi\rangle=\alpha\|0\rangle+\beta\|1\rangle$
10	$\alpha\|0\rangle-\beta\|1\rangle$	X^0Z^1	$\|\psi\rangle=\alpha\|0\rangle+\beta\|1\rangle$
11	$\alpha\|1\rangle-\beta\|0\rangle$	X^1Z^1	$\|\psi\rangle=\alpha\|0\rangle+\beta\|1\rangle$

Quantum Transmissions

- With quantum teleportation, we can transfer n qubits via the transmission of $2n$ classic bits... Is it worth it? (⇒ Yes, as classically reproducing the teleported information would require an exponential amount of classical bits)

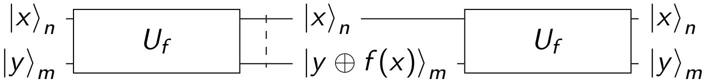
Classical Bits:

- with n classic bits we can encode a single integer value between 0 and $2^n - 1$
- A classic computation acts on a single configuration of n bits at a time

Quantum Bits:

- n qubits encode all the possible 2^n configurations of n classic bits, simultaneously
- For instance, $\alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle$ encodes all integers from 0 to 7
- A quantum computation acts simultaneously on every amplitude value of the 2^N basis configurations... not in parallel applying the same transformation to each bit...
  How? ⇒ Quantum Algorithms!

Reminder: General model of quantum computation

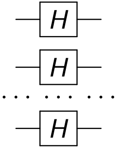


Quantum circuits

- Computing a generic Boolean function with a quantum computer requires the computation to be reversible (thus, input and output registers must be kept separate!)
- Since we want to compute any arbitrary (possibly non reversible) function $f(x)$ of the input x, we need the above framework to express it in reversible form
- The most general one is to consider a circuit equivalent to the computation $U_f \, |x\rangle_n |y\rangle_m = |x\rangle_n |y \oplus f(x)\rangle_m$, where U_f is a unitary operator $(U_f U_f^\dagger = I)$
- Note that applying U_f to the result yields the inputs back (i.e., $U_f = U_f^{-1}$). This allows us to infer that U_f is real (i.e., $U_f = U_f^\dagger$), because $U_f^{-1} = U_f^\dagger$.

Notable trick in QC repertoire: Walsh-Hadamard Transformation

Given a quantum register with n qubits (thus a state in a space $\subseteq \mathbb{C}^{\otimes n}$), the joint application of Hadamard gates to each qubit is denoted as $\mathtt{H}^{\otimes n}$



- when it is applied to a register $|00\cdots0\rangle$, a uniform superimposition of all 2^n configurations of n (classic) bits is built:

$$\mathtt{H}^{\otimes n}|00\cdots0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_n = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{2^n-1}|i\rangle_n$$

- With $n = 2$ qubits, we have:

$$\mathtt{H}^{\otimes 2}|00\rangle = \mathtt{H}|0\rangle \otimes \mathtt{H}|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

Notable trick in QC repertoire

A 2-quit and n-qubit example

$$H^{\otimes 2}\left|0\right\rangle_2 = H\left|0\right\rangle \otimes H\left|0\right\rangle = \frac{1}{2}\left(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\right) = \frac{1}{2}\sum_{0\leq x<2^2}\left|x\right\rangle_2$$

$$H^{\otimes n}\left|0\right\rangle_n = H\left|0\right\rangle \otimes H\left|0\right\rangle \otimes \cdots \otimes H\left|0\right\rangle = \frac{1}{2^{n/2}}\sum_{0\leq x<2^n}\left|x\right\rangle_n$$

$H^{\otimes n}$ applied to the $\left|0\right\rangle_n\left|0\right\rangle_m$ initial state in a generic quantum computation

$$U_f(H^{\otimes n}\otimes I_m)\left|0\right\rangle_n\left|0\right\rangle_m = \frac{1}{2^{n/2}}\sum_{0\leq x<2^n}U_f(\left|x\right\rangle_n\left|0\right\rangle_m) = \frac{1}{2^{n/2}}\sum_{0\leq x<2^n}\left|x\right\rangle_n\left|f(x)\right\rangle_m$$

The final state cannot be specified/learned without knowing 2^n evaluations of $f(x) \Rightarrow$ *quantum parallelism*! After a measurement, the Born rule allows us to learn a single value of $f(x_0)$ out of 2^n possible ones with equal probability. Note that x_0 is a random pick among the inputs mapped into $f(x_0)$... learning more values of $f(\cdot)$ cannot be done (with a single run of the circuit) because the no-cloning thm. forbids us to learn more values of $f(\cdot)$ making copies of the output state before measurement.

However, differently from classical computing, it is often possible to measure only once the output and learn a relation among multiple values $f(\cdot)$ (... a set property) instead of their individual values (*uncertainty principle*).

Evaluating a single bit Boolean function on a superimposition

Deutsch's problem: distinguish if a single bit function is one of the two constant functions or not

It is the simplest example of the forced quantum tradeoff between the individual knowledge of multiple outcomes from the computation of a function $f(\cdot)$ and the learning of a particular relational information among such outcomes.

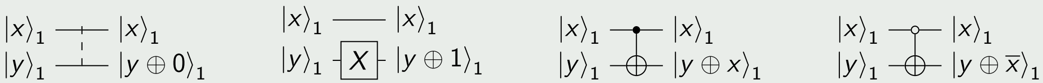
Consider the four possible Boolean functions $\{0,1\} \mapsto \{0,1\}$:

x	$f_0(x)$
0	0
1	0

x	$f_1(x)$
0	1
1	1

x	$f_a(x)$
0	0
1	1

x	$f_{\bar{a}}(x)$
0	1
1	0



Classically solving the Deutsch's problem

Deutsch's problem: distinguish if a single bit function is one of the two constant functions or not

Given the four Boolean functions

x	$f_0(x)$
0	0
1	0

x	$f_1(x)$
0	1
1	1

x	$f_a(x)$
0	0
1	1

x	$f_{\bar{a}}(x)$
0	1
1	0

and an opaque function $f : \{0, 1\} \mapsto \{0, 1\},\; y = f(x)$, we want to know if $f(\cdot) \in \{f_0, f_1\}$ or $f(\cdot) \in \{f_a, f_{\bar{a}}\}$

$$\text{Evaluate } f(0) = \begin{cases} 0 & \text{then } f \in \{f_0, f_a\} \\ 1 & \text{then } f \in \{f_1, f_{\bar{a}}\} \end{cases} \qquad \text{Evaluate } f(1) = \begin{cases} 0 & \text{then } f \in \{f_0, f_{\bar{a}}\} \\ 1 & \text{then } f \in \{f_1, f_a\} \end{cases}$$

A single classical evaluation of $f(\cdot)$ does not yield enough information to solve the problem.

Quantumly solving the Deutsch's problem (1/3)

Deutsch's problem: distinguish if a single bit function is one of the two constant functions or not

Given the four Boolean functions

x	$f_0(x)$
0	0
1	0

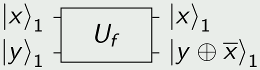
x	$f_1(x)$
0	1
1	1

x	$f_a(x)$
0	0
1	1

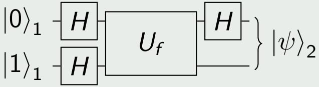
x	$f_{\bar{a}}(x)$
0	1
1	0

and a unitary operator U_f realizing the transformation $|xy\rangle \mapsto |x, y \oplus f(x)\rangle$, where $f : \{0,1\} \mapsto \{0,1\},\ y = f(x)$, we want to know if $f(\cdot) \in \{f_0, f_1\}$ or $f(\cdot) \in \{f_a, f_{\bar{a}}\}$

Instead of running:

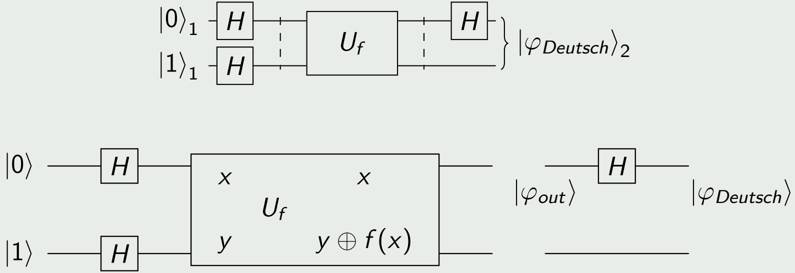


Evaluate:



Quantumly solving the Deutsch's problem (2/3)

Deutsch's problem: distinguish if a single bit function is one of the two constant functions or not



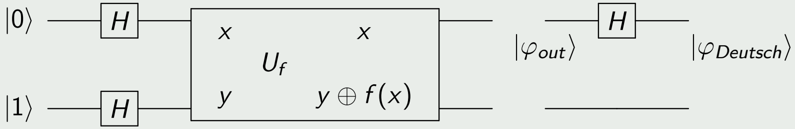
The input state $|\varphi_0\rangle = |01\rangle$ is transformed into $|\varphi_1\rangle = \underbrace{\frac{|0\rangle+|1\rangle}{\sqrt{2}}}_{H|0\rangle} \otimes \underbrace{\frac{|0\rangle-|1\rangle}{\sqrt{2}}}_{H|1\rangle}$, then the application of U_f does not modify the first qubit $|x\rangle$, but only the second.

If $f(x) = 0$ then $|\varphi_{out}\rangle = |x\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

If $f(x) = 1$ then $|\varphi_{out}\rangle = |x\rangle \otimes \frac{|1\rangle-|0\rangle}{\sqrt{2}} = (-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

Quantumly solving the Deutsch's problem (3/3)

Deutsch's problem: distinguish if a single bit function is one of the two constant functions or not



$|\varphi_0\rangle = |01\rangle$ becomes $|\varphi_1\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left(|0\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}} + |1\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.

$|\varphi_{out}\rangle = \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}} + (-1)^{f(1)}|1\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

if $f(0) = f(1)$, then $|\varphi_{Deutsch}\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} + \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \Rightarrow |\varphi_{Deutsch}\rangle = (-1)^{f(0)}|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

if $f(0) \neq f(1)$, then $|\varphi_{Deutsch}\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} - \frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \Rightarrow |\varphi_{Deutsch}\rangle = (-1)^{f(0)}|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

To obtain the former note that if $f(0) \neq f(1)$, then $(-1)^{f(1)} = -(-1)^{f(0)}$

$$|\varphi_{Deutsch}\rangle = \pm\,|f(0) \oplus f(1)\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Measuring the 1st qubit we get with 100% prob. if the $f(\cdot)$ is constant or not

Deutsch-Jozsa Problem (1/2)

It is a problem requiring an exponential time on a classic computer (assuming $P \neq NP$), while it has a $\mathcal{O}(1)$ complexity when evaluated by a quantum circuit (i.e., a single evaluation of the circuit)

Definition

Considering the set of all Boolean functions $f(\cdot) : \{0,1\}^n \mapsto \{0,1\}$, with an n-bit input and a single-bit output, that are either

- *constant* (i.e., each of them always yields the same output value – there are only two of them)
- *balanced* (i.e., each of them yields 0 when it is evaluated in half of the input configurations and 1 when it is evaluated in the other half – there are $\binom{2^n}{2^{n-1}} \approx 2^n$ of them)

Given a randomly chosen $f(\cdot)$ from the set, state if $f(\cdot)$ is constant or balanced.

Classically solving the Deutsch-Jozsa Problem

Given an opaque $f(\cdot)$, in the worst case, it is necessary to evaluate the function on $2^{n-1}+1$ input configurations (i.e., the recognition of a constant function)

Observation on the Walsh-Hadamard Transformation

We saw the action of the gate H on a single qubit initialized as $|0\rangle$, when the qubit is in a generic basis state its action can be compactly summarized as:

$$x \in \{0,1\}, \quad H|x\rangle_1 = \frac{1}{\sqrt{2}}\left(|0\rangle_1 + (-1)^x |1\rangle_1\right) = \frac{1}{\sqrt{2}} \sum_{z=0}^{2^1-1} (-1)^{x \circ z} |z\rangle_1$$

configuration of the computational basis

if len$(x) = 1 \Rightarrow x \circ z = x$ AND $z = x \cdot z$

if $|x| = |z| > 1 \Rightarrow x \circ z \triangleq x_{n-1} \cdot z_{n-1} \oplus \ldots \oplus x_0 \cdot z_0$

logical AND

where $x \circ z$ is the internal product between two classical bits (i.e., their Boolean and)

The result of $H^{\otimes n}|0\rangle_n$ is the uniform superimposition of every possible basis state.
When the gate $H^{\otimes n}$ is applied to a generic n-quibit basis state:

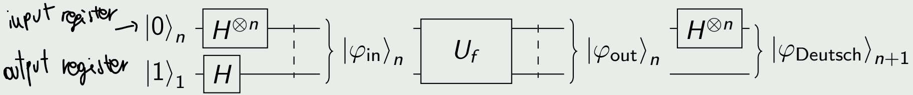
$$x \in \{0,1\}^n, \quad H^{\otimes n}|x\rangle_n = H|x\rangle_n \otimes H|x\rangle_n \otimes \cdots = \frac{1}{\sqrt{2}} \sum_{z_0=0}^{1} (-1)^{x_0 \circ z_0} |z_0\rangle \otimes \frac{1}{\sqrt{2}} \sum_{z_1=0}^{1} (-1)^{x_1 \circ z_1} |z_1\rangle \otimes \cdots$$

$$H^{\otimes n}|x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z_{n-1}=0}^{1} \cdots \sum_{z_1=0}^{1} \sum_{z_0=0}^{1} (-1)^{x_{n-1} \circ z_{n-1}} \cdots (-1)^{x_1 \circ z_1} \cdot (-1)^{x_0 \circ z_0} |z_{n-1} \cdots z_1 z_0\rangle_n$$

$$H^{\otimes n}|x\rangle_n = \frac{1}{\sqrt{2^n}} \sum_{z \in \{0,1\}^n} (-1)^{x \circ z} |z\rangle_n$$

Deutsch-Jozsa Problem

Quantumly solving the Deutsch-Jozsa Problem (2/2)


input register
output register
$|0\rangle_n$
$|1\rangle_1$
$H^{\otimes n}$
H
$|\varphi_{\text{in}}\rangle_n$
U_f
$|\varphi_{\text{out}}\rangle_n$
$H^{\otimes n}$
$|\varphi_{\text{Deutsch}}\rangle_{n+1}$

$$|\varphi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

if $f(z)=1$ then they are

$$|\varphi_{\text{out}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{f(z)} |z\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$ (obs.: when $f(z)$=0, the basis states of $|-\rangle$ are unchanged, oth. flipped)

$$|\varphi_{\text{Deutsch}}\rangle = \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \sum_{w\in\{0,1\}^n} (-1)^{w\circ z + f(z)} |w\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

- if $f(z)$ is constant over $z \in \{0,1\}^n$ then the amplitude of $|0\rangle_n$ is $\frac{1}{2^n}\sum_z (-1)^{f(z)}$. As a consequence, measuring on the input register after the computation of $f(\cdot)$ will give us a classical n-bit null string.
- if $f(z)$ is balanced, the measurement will yield us any state except 0^n because in this case the amplitude of $|0\rangle_n$ is exactly zero.

Bernstein-Vazirani Problem (1/4)

Definition

Let a and x be two positive numbers less than 2^n, each of which encoded with n classical bits.
Let $f(x)$ be the Boolean function computing the following internal product:
$f(x) = a \circ x = a_0 x_0 \oplus a_1 x_1 \oplus \cdots \oplus a_{n-1} x_{n-1}$.

How many evaluations of $f(\cdot)$ are needed to infer correctly the value of a?

m position (from right)

$0..0\overset{\downarrow}{1}0...0$

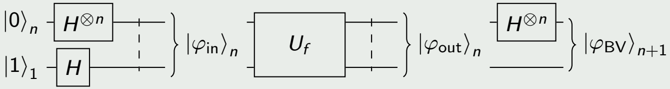
Classical solution of the Bernstein-Vazirani problem: requires n evaluations

Given the opaque function $f(\cdot)$, evaluating it in $x = 2^m$ with $m \in \{0, 1, 2, \ldots, n-1\}$, allows us to determine the m-th bit of the binary encoding of a because: $a_m = f(2^m)$.

The quantum solution to the Bernstein-Vazirani Problem will require a single run of the circuit realized to evaluate the function $f(\cdot)$ (... a speedup more than exponential as in the Deutsch-Josza problem)

Bernstein-Vazirani Problem (2/4)

Quantumly solving the Bernstein-Vazirani Problem


$|0\rangle_n$
$H^{\otimes n}$
$|1\rangle_1$
H
$|\varphi_{\text{in}}\rangle_n$
U_f
$|\varphi_{\text{out}}\rangle_n$
$H^{\otimes n}$
$|\varphi_{\text{BV}}\rangle_{n+1}$

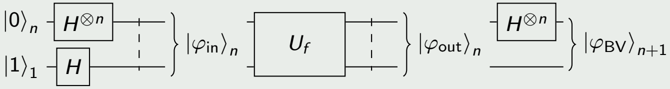
$$|\varphi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\varphi_{out}\rangle = U_f\,|\varphi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{f(z)}\,|z\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\varphi_{BV}\rangle = H^{\otimes n}\,|\varphi_{out}\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{f(z)} \left(\frac{1}{\sqrt{2^n}} \sum_{w\in\{0,1\}^n} (-1)^{z\circ w}\,|w\rangle\right) \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Bernstein-Vazirani Problem (3/4)

Quantumly solving the Bernstein-Vazirani Problem


$|0\rangle_n$
$H^{\otimes n}$
$|1\rangle_1$
H
$|\varphi_{\text{in}}\rangle_n$
U_f
$|\varphi_{\text{out}}\rangle_n$
$H^{\otimes n}$
$|\varphi_{\text{BV}}\rangle_{n+1}$

$$|\varphi_{BV}\rangle = \frac{1}{2^n}\sum_{w\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}(-1)^{z\circ(a+w)}\,|w\rangle\otimes\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = \frac{1}{2^n}\sum_{w\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}\prod_{j=0}^{n-1}(-1)^{z_j\circ(a_j\oplus w_j)}\,|w\rangle\otimes\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

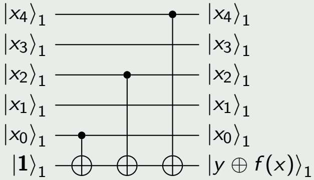
$$|\varphi_{BV}\rangle = \frac{1}{2^n}\sum_{w\in\{0,1\}^n}\prod_{j=0}^{n-1}\sum_{z_j=0}^{1}(-1)^{z_j\circ(a_j\oplus w_j)}\,|w\rangle\otimes\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

- when $w \neq a$ the summation indexed by w adds up 2^n zero values, therefore the amplitude of $|w\rangle$ is null.
- when $a = w$ the amplitude of $|w\rangle$ is 1 and the value a is read out from the input register

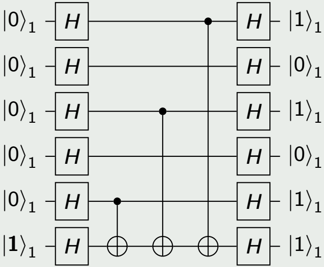
B-V Problem (4/4): read out the unknown a with one measurement on the $f(x)=a \circ x$ circuit

- The structure of the quantum circuit solving the problem reveal the value of the unknown a, without performing any measurement
- Consider for the sake of argument that the operator U_f corresponds to $f(x) = a \circ x$; with $a = 10101_{\mathtt{bin}}$ and $f(x) = x_4 \oplus x_2 \oplus x_0$.

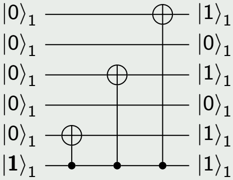
Circuit computing U_f



BV solver circuit for U_f



Circuit equivalent to the BV solver



Simon's Problem (1/4)

- A quantum solution will enjoy a linear number of runs w.r.t. the exponential number exhibited by a classical, thus benefiting from a an exponential speedup
- It points out another peculiar feature of quantum computation, which is learning a problem solution on a probabilistic basis (... with more than one run of the circuit and the corresponding measures)

Definition

Given a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}^{n-1}$, such that $f(x) = f(y)$ if and only if $x \oplus y = a$, with $a \neq 0$ and $a, x, y \in \{0,1\}^n$; find the unknown a.

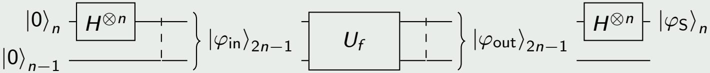
Obs.: Given a pair (x_i, x_j) of colliding inputs with distance $x_i \oplus x_j = a$, $i \neq j$, if x_k is also colliding then $x_k = x_i$ or $x_k = x_j$

Classical solution to the Simon's problem

The effort of a collision search is quantified by the *birthday paradox*. On average to get 50% chances to pick two colliding random inputs x_i, x_j (i.e., such that $f(x_i) = f(x_j)$) you need to perform $\approx 1.17\sqrt{2^n}$ evaluations.

Simon's Problem (2/4)

Quantumly solving the Simon's Problem

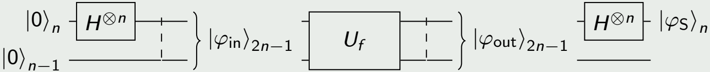

$|0\rangle_n$
$H^{\otimes n}$
$|0\rangle_{n-1}$
$|\varphi_{\text{in}}\rangle_{2n-1}$
U_f
$|\varphi_{\text{out}}\rangle_{2n-1}$
$H^{\otimes n}$
$|\varphi_{\text{S}}\rangle_n$

$$x \in \{0,1\}^n \qquad |\varphi_{\text{in}}\rangle_{2n-1} = H^{\otimes n}|0\rangle_n |0\rangle_{n-1} = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle_n |0\rangle_{n-1}$$

$$|\varphi_{\text{out}}\rangle_{2n-1} = U_f\,|\varphi_{\text{in}}\rangle_{2n-1} = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} U_f\left(|z\rangle_n |0\rangle_{n-1}\right) = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle_n |f(z)\rangle_{n-1}$$

Simon's Problem (3/4)

Quantumly solving the Simon's Problem

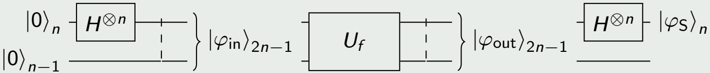


$$|\varphi_{\text{out}}\rangle_{2n-1} = U_f\,|\varphi_{\text{in}}\rangle_{2n-1} = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} U_f\left(|z\rangle_n\,|0\rangle_{n-1}\right) = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |z\rangle_n\,|f(z)\rangle_{n-1}$$

1. if we measure only the output register portion of the state $|\varphi_{\text{out}}\rangle_{2n-1}$, we will get a random $(n-1)$-classic-bit outcome from $f(z)$ and the state will collapse, by the GRBorn rule, into the uniform superimposition: $\frac{1}{\sqrt{2}}(|z_0\rangle + |z_0 \oplus a\rangle) \otimes |f(z_0)\rangle$
2. if now we measure on the input register, we will get z_0 or $z_0 \oplus a$, which will appear as random values ... unuseful! [**Obs.**:. z_0 here denotes a n classic-bit string!]

Simon's Problem (4/4)

Quantumly solving the Simon's Problem



3. let's apply the operator $H^{\otimes n}$ on the input register after the measurement at step 1.

$$|\varphi_S\rangle = H^{\otimes n}\frac{1}{\sqrt{2}}(|z_0\rangle + |z_0 \oplus a\rangle) = \frac{1}{\sqrt{2^{n+1}}}\sum_{w\in\{0,1\}^n}\left((-1)^{z_0\circ w} + (-1)^{(z_0\oplus a)\circ w}\right)|w\rangle = \ldots = \frac{1}{\sqrt{2^{n+1}}}\sum_{a\circ w=0}(-1)^{z_0\circ w}|w\rangle$$

4. Measuring the input register now, we get an n-classic-bit string $w^{(1)}$ such that $a \circ w^{(1)} = 0$
5. Running the whole computation from the beginning $n-1$ times more (actually $n-1+x$ times more, $x \geq 20$, see Appendix G of the textbook) will allow us to collect n (linearly independent) simultaneous binary equations $a \circ w^{(i)} = 0$ with n unknowns $a_i \in \{0,1\}$ and $1 \leq i \leq n$ ($a = \sum_{i=1}^{n} a_i 2^{i-1}$), that can be solved classically in polynomial time (... $\tilde{\mathcal{O}}(n^3)$)

Textbook references

- Chapter 2
- Chapter 6
- Appendix G

Bibliography I

Avshalom C Elitzur and Lev Vaidman.
Quantum mechanical interaction-free measurements.
Foundations of Physics, 23(7):987–997, 1993.

Duc M. Tran, Duy V. Nguyen, Bin Ho Le, and Hung Q. Nguyen.
Experimenting quantum phenomena on nisq computers using high level quantum programming.
EPJ Quantum Technology, 9, 2022.