QML-Mod4-From Quantum Computing to QML

Riccardo Marega

March 2025

Indice

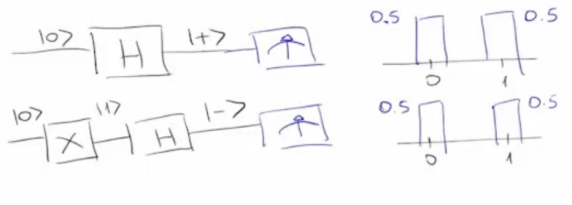
1 From Quantum Computing to QML-23/05/2025

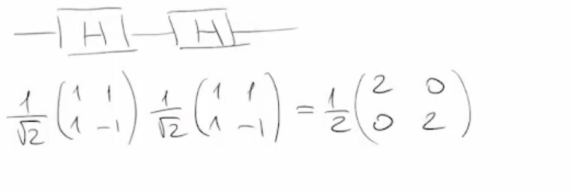
1.1 Hadamard Gate (H)

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

$$\begin{cases} H \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |+\rangle \\ H \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-\rangle \end{cases}$$

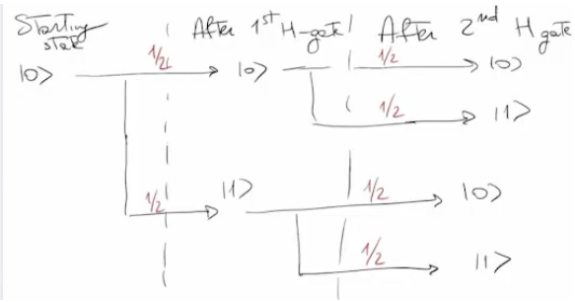
Two Hadamard gates placed one after the other compose the identity gate.



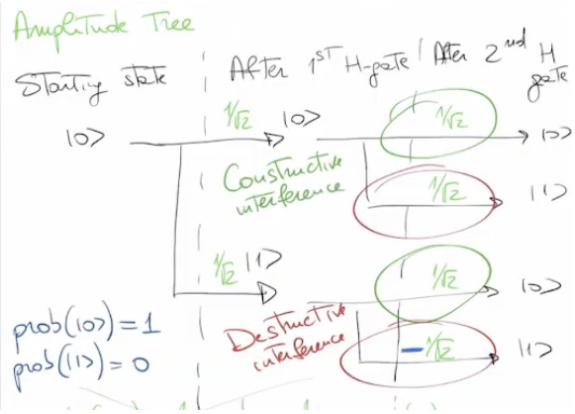


$= \textit{Identity matrix}$

Using amplitude tree we get that, starting from $|0\rangle$, after applying a Hadamard gate we have a probability of 0.5 of getting either $|1\rangle$ or $|0\rangle$. Suppose now applying an Hadamard gate what we get is an overall probability of finding half of the time $|0\rangle$ and the other half $|1\rangle$ but that is not what we expected given the fact that we told that applying twice in a row an Hadamard gate corresponds to obtain the identity gate.



The problem is that we have to be careful when applying the Hadamard gate to $|1\rangle$ because the probability of finding $|1\rangle$ is not $\frac{1}{2}$ but it is $|\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}|^2$ (first all the amplitudes are summed than the modulus square is computed). We talk in this case of destructive interference while for $|0\rangle$ we have constructive interference.



Probability is fully characterized by its magnitude while the Amplitude has also a Phase factor.

1.2 Composite systems

$$H_{1+\ldots+n} = H_1 \otimes \ldots \otimes H_n$$

1.2.1 Tensor Product

$$\psi_1 \otimes \psi_2 = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \begin{pmatrix} \alpha_1\,\alpha_2 \\ \alpha_1\,\beta_2 \\ \beta_1\,\alpha_2 \\ \beta_1\,\beta_2 \end{pmatrix}.$$

Definition If $|\psi\rangle = (2^n) = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes ... \otimes \begin{pmatrix}\alpha_n\\ \beta_n\end{pmatrix}$ than it is called a **product state**.

$$\begin{cases}\textbf{product states} & 2n\\ \textbf{entangled states} & 2^n\end{cases}$$

We start by computing

$$|0\rangle_1 \otimes |0\rangle_2 = |00\rangle = \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$

in the same way

$$|0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

and so on for the other combinations.
In general a two qubit state has the form

$$\begin{pmatrix}a_{00}\\a_{01}\\a_{10}\\a_{11}\end{pmatrix}$$

where $a_{ij} \in C$. We recall that is possible to expand it on a given basis

$$|\psi\rangle = a_{00}\begin{pmatrix}1\\0\\0\\0\end{pmatrix} + a_{01}\begin{pmatrix}0\\1\\0\\0\end{pmatrix} + a_{10}\begin{pmatrix}0\\0\\1\\0\end{pmatrix} + a_{11}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Examples: Can we decomposed the following states in a tensor product?

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0+\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\1\end{pmatrix} = |1+\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = ?$$

In order to solve that we have to solve for

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}\otimes\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}$$

applying the conditions given from the problem. What we find is that impossible to find $\alpha_1, \alpha_2, \beta_1$ and β_2 able to solve for the previous problem: the state is said to be entangled.
Another example is

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 0\\ 0\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

and that is also an entangled state, moreover, being the relative phase maximum ($e^{i\phi} = -1$) that is called **maximum entangled state**.
We can compute the remaining combinations and we'll find that both of them are also entangled states.
Maximum entangled states (Bell states) compose an orthonormal basis

$$\begin{cases}|\beta_{00}\rangle\\ |\beta_{10}\rangle\\ |\beta_{01}\rangle\\ |\beta_{11}\rangle\end{cases}$$

1.3 How gates are composed?

$$1\otimes 1 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & 0\\ 0 & \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\end{pmatrix}$$

In the same way

$$X\otimes 1 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\otimes\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}0 & \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\\ \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & 0\end{pmatrix}$$

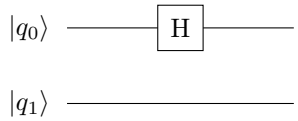
and so on for all other possible gate combinations.
Indeed, we continue by considering the case:

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

We get:

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

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$



For n qubits on which an Hadamard transformation is applied we have:

$$\frac{1}{\sqrt{2}} \sum_{j=0}^{2^n-1} |j\rangle$$

1.3.1 Two-qubit gate

We want a gate able to interact with two qubits, transforming them at the same time. The most general n-qubit gate is described by $2^n \times 2^n$ unitary matrix.

C-U (Controlled U) gate in this case we have a control qubit and a target qubit. Mathematically this gate is represented by

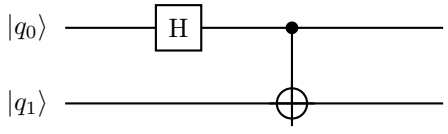
$$|xy\rangle \rightarrow |x\rangle U^x |y\rangle$$

$$\begin{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & 0 \\ 0 & U \end{pmatrix}$$

The C-NOT gate is the controlled NOT gate and it is composed assigning U = X. We can now compute as excercise:

$$U_{CNOT} \times (X \otimes X) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

1.3.2 Hadamard and CNOT gate



$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

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

$$U_{\text{total}} = \text{CNOT}\left(H \otimes I_2\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

2 From Quantum Computing to QML part 2 -24/05/2025

Suppose being in the state $\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and performing a measurement: the probability of measuring $|00\rangle$ is the same of $|11\rangle$, which is $\frac{1}{2}$.

2.1 Bell Measurement

To perform a Bell measurement we apply to the state β first the CNOT gate followed by the Hadamard gate. What we get is:

$$\beta_{00} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xrightarrow{CNOT+H} |00\rangle$$

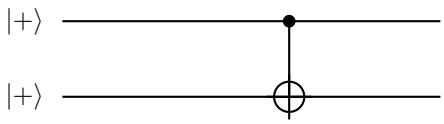
$$\beta_{01} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \xrightarrow{CNOT+H} |01\rangle$$

$$\beta_{10} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xrightarrow{CNOT+H} |10\rangle$$

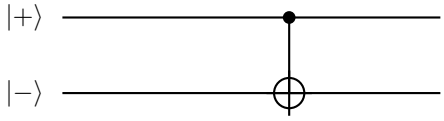
$$\beta_{11} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xrightarrow{CNOT+H} |11\rangle$$

2.2 CNOT and $|\pm\rangle$ states

Both qubits are in a superposition.



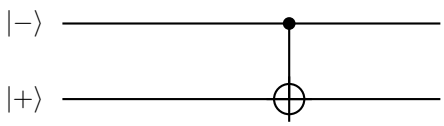
$$|++\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{CNOT} \frac{1}{2}(|00\rangle + |01\rangle + |11\rangle + |10\rangle) = |++\rangle$$



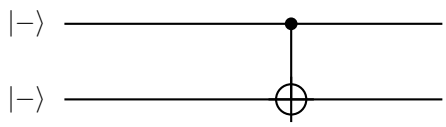
$$|+-\rangle \xrightarrow{CNOT} \frac{1}{2}(|00\rangle - |01\rangle + |11\rangle - |10\rangle) = \frac{1}{2}|[0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)]$$

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

. This is called phase kick-back: the target remains the same but is the controller who is changed (also called π shift).



$$|-+\rangle \xrightarrow{CNOT} \frac{1}{2}(|00\rangle + |01\rangle - |11\rangle - |10\rangle) = |-+\rangle.$$

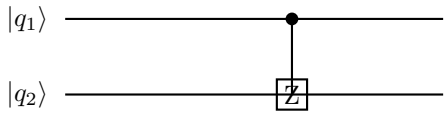


$$|--\rangle \xrightarrow{CNOT} \frac{1}{2}(|00\rangle - |01\rangle - |11\rangle + |10\rangle) = \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle) + \frac{1}{\sqrt{2}}|1\rangle(|0\rangle - |1\rangle) = |+-\rangle.$$

Once again we are affecting the control.

2.3 CZ

The CZ gate is a gate that, as the CNOT, uses a control gate on a qubit and applies a Z gate on the other qubit.



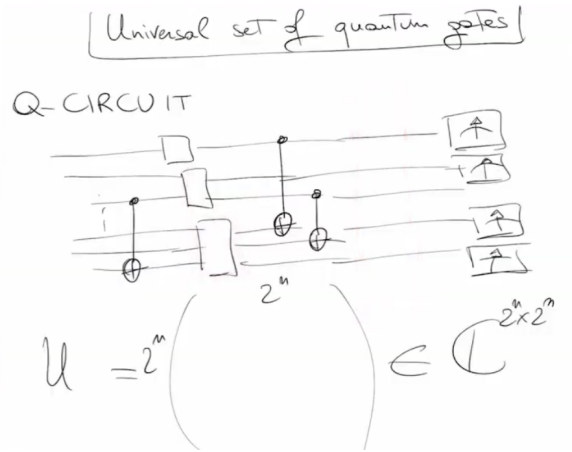
$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |10\rangle \\ |11\rangle \to -|11\rangle \end{cases}$$

Symmetric role of control and target qubits.
Note that applying $\xrightarrow{H-Z-H} \equiv \xrightarrow{X}$ as also $\xrightarrow{H-X-H} \equiv \xrightarrow{Z}$. It's possible proving that by simply computing all the matrix multiplications.
The most general type of gate is a unitary matrix $\in C^{2^n \times 2n}$. It's possible to demonstrate that this unitary matrix can be decomposed thanks to the tensor product decomposition.

Theorem:

$$\{CX, X, R_Z(\sigma), H\}$$

is called the universal set of quantum gates and their combination (tensor product combination) permits to construct an infinite type of gates.
The operation of expanding a gate on the universal set is called transpiling.



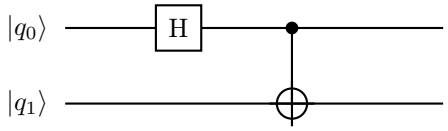
Theorem Given a gate characterized by an error ϵ and a quantum circuit composed on N gates applied to n qubits, than

$$\epsilon_{tot} \leq N\epsilon.$$

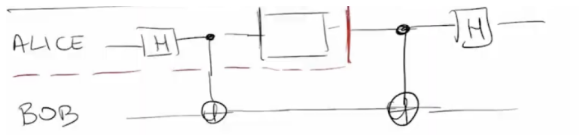
2.4 Quantum algorithms

2.4.1 Superdense coding

Given A (sender) and B (receiver). A prepare a state $|\psi\rangle$ of 2 qubit (using H followed by CNOT), the goal is to send to B 2 bits.



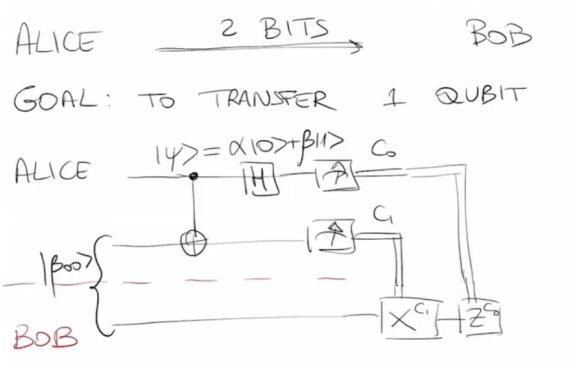
To do so, after applying the previous circuit, the second qubit is physically sent to B. They are now sharing a maximum entangled state. After transforming her qubit, A sends it to B. B then applies a CNOT followed by an Hadamard gate.

] 

[H]

$$\begin{cases} |\beta_{00}\rangle \to 00 \\ |\beta_{01}\rangle \to 01 \\ |\beta_{10}\rangle \to 10 \\ |\beta_{11}\rangle \to 11 \end{cases}$$

2.4.2 Quantum Teleportation



What we are witnessing now is the no-cloning theorem.

3 Quantum algorithms -30/05/2025

3.1 Quantum parallelism

We start by considering two Hadamard gates: $|00\rangle \xrightarrow{HH} |++\rangle$, $|01\rangle \xrightarrow{HH} |+-\rangle$ and $|11\rangle \xrightarrow{HH} |--\rangle$. In general for a single Hadamard gate we can write

$$H|x\rangle = \frac{1}{\sqrt{2}}[|0\rangle + (-1)^x|1\rangle]$$

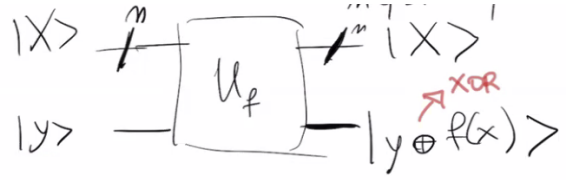
where x = 0,1. We can apply now n Hadamard gates on n qubits

$$|x_1x_2...x_n\rangle \xrightarrow{H_1...H_n} \frac{1}{2^{\frac{n}{2}}}\sum_y (-1)^{xy}|y\rangle$$

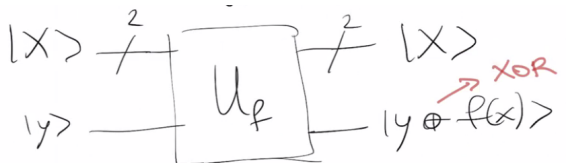
with y containing all n-bit strings. xy is called bitwise product and is defined as

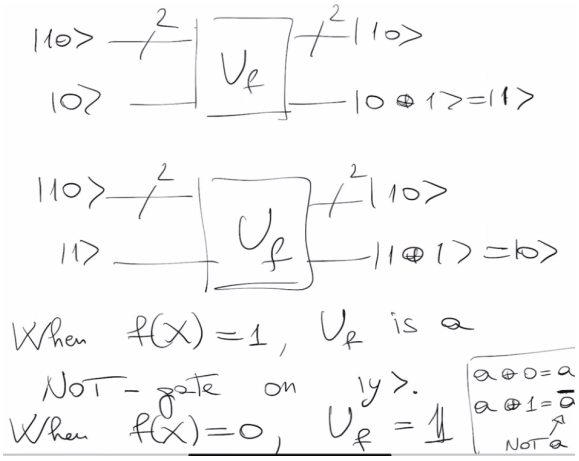
$$xy = x_1y_1 + ... + x_ny_n.$$

We note how this works like a XOR gate.
Suppose now having a function $f(x) : \{0,1\}^n \to \{0,1\}$: $|x\rangle \to |f(x)\rangle$.
Lets define $U_f : |X\rangle|y\rangle \to |X\rangle|y + f(x)\rangle$.

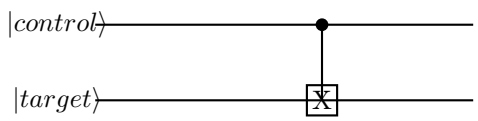


What follows is an example where n = 2.

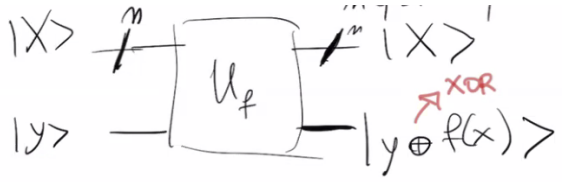




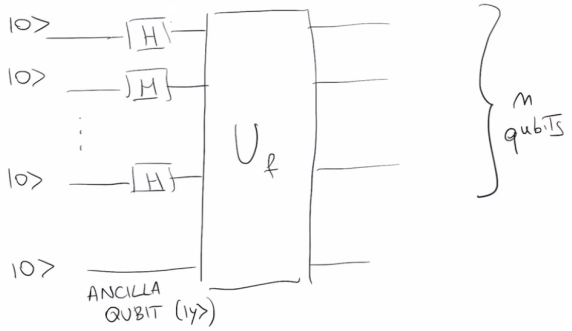
U_f is like a C-X gate on y but with the control on f(x) instead of x (as in C-X):



that is switched on if control c = 1, while



the X-gate acts on y if f(x) = 1.
Lets now consider the following circuit



$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

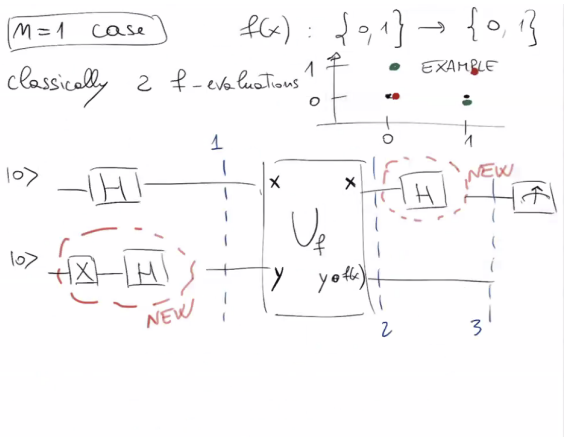
where x is all possible bit-string. Overall the state can be written as

$$\Rightarrow \frac{1}{\sqrt{2^n}} \sum_x |x\rangle f(x)$$

This is called quantum parallelism.
If we make now n measurements we loose these specific combinations.

3.2 Deutsch-Josza algorithm

Given $f : \{0,1\}^n \to \{0,1\}$ where f(x) can be either constant or balanced ($f(x) = 0$ for half values of x and 1 otherwise). The goal of this algorithm is to say whether it is constant or balanced. The question is: how many function evaluations do we need classically? $2^{n-1} + 1 \to O(2^n)$. The best classical algorithm has a computational complexity of $O(2^n)$. What we are going to see is that using quantum computing we'll get a computational power of $O(1)$ (just one evaluation), we'll witness what is called quantum exponential speedup.



At checkpoint 1 we have $|\psi_1\rangle = |+-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}\sum_{x=0}^{1} |0\rangle(|0\rangle - |1\rangle)$.
At checkpoint 2 we have $|\psi_2\rangle = \frac{1}{2}\sum_{x=0}^{1} |x\rangle \otimes (|0 XOR f(0)\rangle - |1 XOR f(1)\rangle) = \frac{1}{2}\sum_{x=0}^{1}(-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$.
At checkpoint 3 we have $|\psi_3\rangle = \frac{1}{2}\sum_x (-1)^{f(x)} \frac{1}{2^{\frac{n}{2}}} \sum_y (-1)^{f(x)}|y\rangle(|0\rangle - |1\rangle) =$

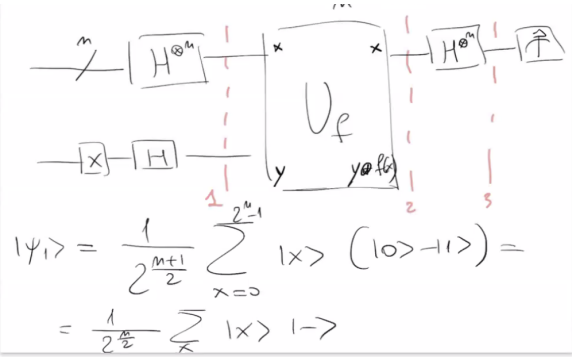
$$= \frac{1}{\sqrt{2^3}} \sum_x (-1)^{f(x)} \sum_y (-1)^{f(x)}|y\rangle|-\rangle$$

What's the probability of finding 0 measuring the first qubit?

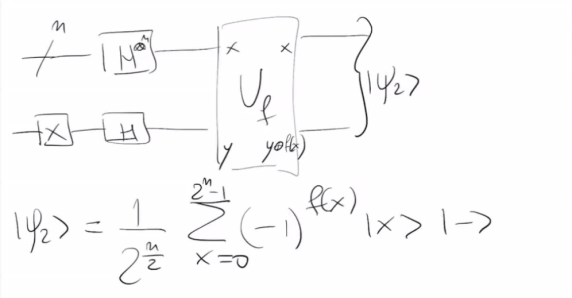
$$prob(|0\rangle_1) = |\frac{1}{2}\sum_{x=0}^{1}(-1)^{f(x)}|^2$$

$$\begin{cases} 0 & \text{if f(x) is balanced} \\ 1 & \text{if f(x) is constant} \end{cases}$$

n-bit case $f(x) : \{0,1\}^n \to \{0,1\}$.



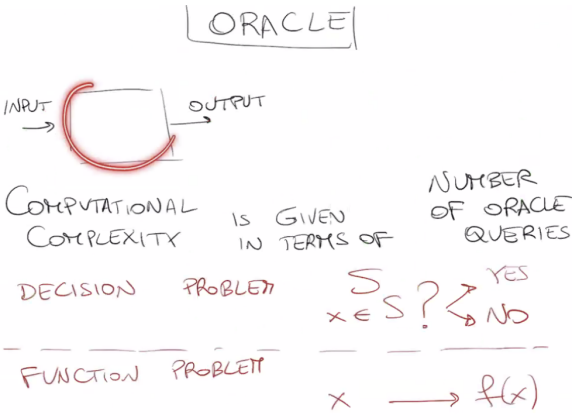
The probability of $|0\rangle^{\otimes n} = |\frac{1}{2^n}\sum_x^{2^n-1}(-1)^{f(x)}|^2$.
The solution is that 1 run of the quantum circuit (f-evaluation) followed by a final measurement gives that if all bits are 0 than the function is constant otherwise if at least one bit is 1 than the function is balanced.
We note that ψ_2 is a state composed by a linear combination where if f(x)=1 has a negative sign.

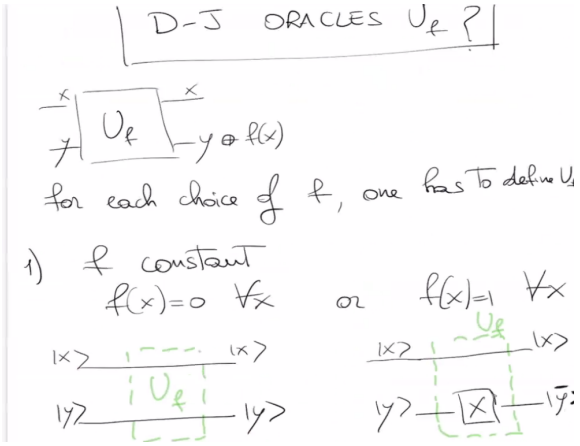


We are moving from this state

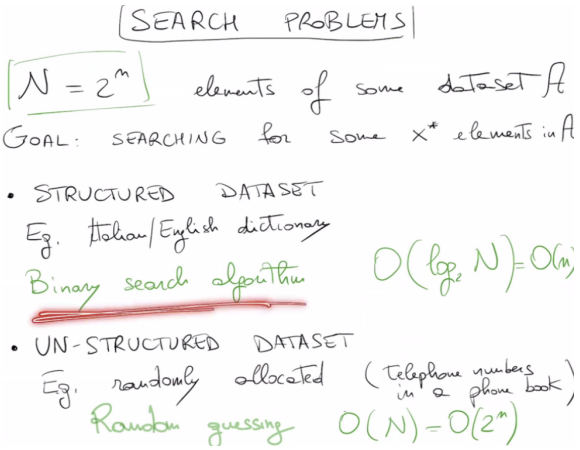
$$|+\rangle^{\otimes n} = \frac{1}{2^{\frac{n}{2}}} \sum_x |x\rangle.$$

to a state where the only difference is the negative sign. What happens is that we are marking $|x\rangle$ with a minus sign if f(x)=1.





3.3 Search problem



SAT-problem

A string of bits $x_1 x_2 x_3$ satisfying a set of Boolean conditions

3-SAT problem

$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee x_3) \wedge \dots$

$x_1 \vee x_2 \vee \bar{x}_3$

WD $x_1 \vee \bar{x}_2 \vee x_3$

} all clauses have to be TRUED

001 is not a solution

111 is a solution

FINDING A SOLUTION (very hard problem) $\neq$ CHECKING A SOLUTION (EASY)

ORACLE: marking a solution

Decision problem: f If $x \in A$, YES; otherwise NO

$U = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & -1 \end{pmatrix} \begin{matrix} \\ \\ \xrightarrow{x_j \in A} j \end{matrix}$

INPUT

$U|x\rangle = \begin{cases} |x\rangle & \text{if } x \notin A \text{ (NO)} \\ -|x\rangle & \text{if } x \in A \text{ (YES)} \end{cases}$

Answer (OUTPUT)

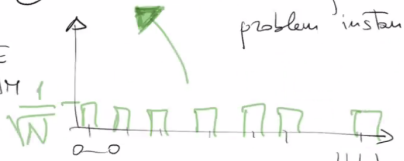
$f(x) = \begin{cases} 1 & x \in A \\ 0 & \text{otherwise} \end{cases}$

GROVER ALGORITHM

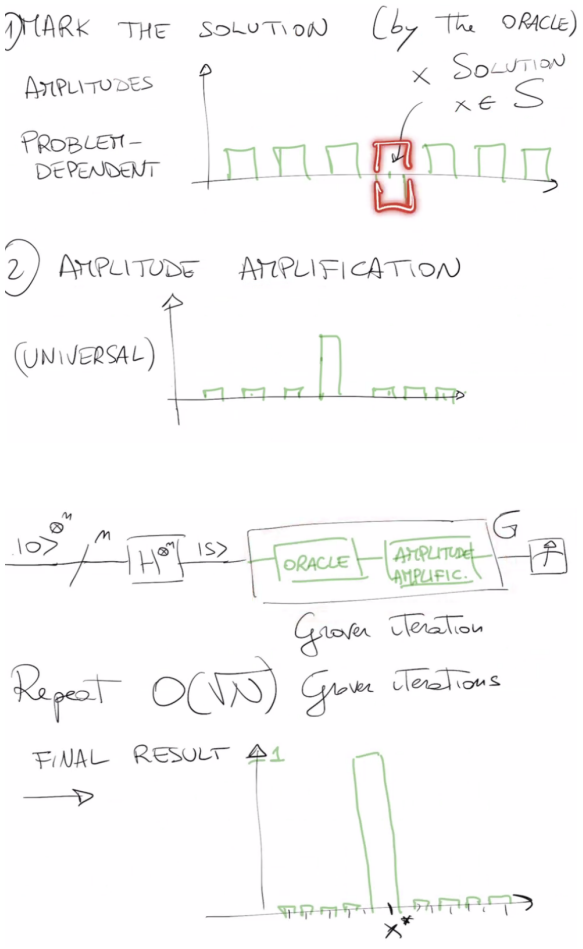
$|S\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x\rangle$ $\uparrow$ all possible problem instances

H H H } n

AMPLITUDE HYSTOGRAM



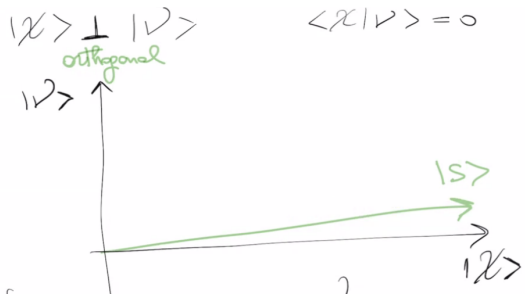
$N = 2^n$


1) MARK THE SOLUTION (by the ORACLE)
AMPLITUDES
PROBLEM-DEPENDENT
x SOLUTION
x ∈ S
2) AMPLITUDE AMPLIFICATION
(UNIVERSAL)
|0⟩^⊗n
n
H^⊗n
|s⟩
ORACLE
AMPLITUDE AMPLIFIC.
G
Grover iteration
Repeat O(√N) Grover iterations
FINAL RESULT
1
x*

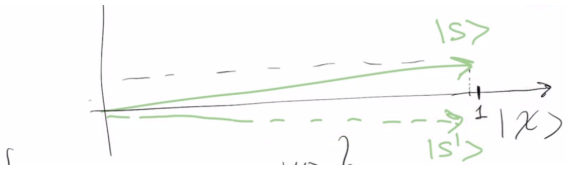
4 Quantum Algorithms part 2 -31/05/2025

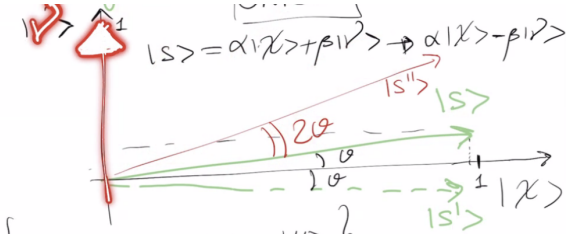
4.0.1 Example

Given 3 bits, we have 8 instances (000,001,...). Suppose that the solution is 100 for example, we should run classically the algorithm O(N) times (via random guessing). We define now a state $|\nu\rangle = |100\rangle$ and a state $|\chi\rangle = \frac{1}{\sqrt{7}}(|000\rangle + ...)$ where in general $|s\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle$.

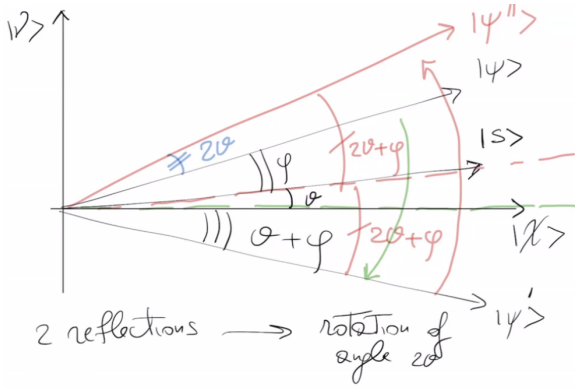


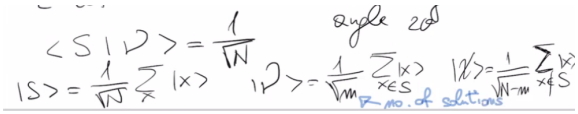
The oracle is marking the solution. Since $|s\rangle = \alpha|\chi\rangle + \beta|\nu\rangle$, after the oracle we get $\alpha|\chi\rangle - \beta|\nu\rangle$.





And that is given using an amplifier (or diffuser).
What we want now is to make it more precise.





where m = 1.

$$\frac{1}{|N|} = |s| \sin(\theta) = \sin(\theta)$$

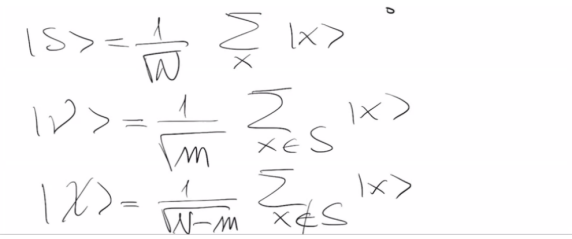
For real-world application $N \to \infty$.

$$2\theta \sim \frac{2}{\sqrt{N}}$$

The question now is: how many G iterations do I need to solve the problem?

$$\begin{cases} O(\sqrt{N}) & \text{Quadratic speedup} \\ O(N) & \text{Random guessing} \end{cases}$$

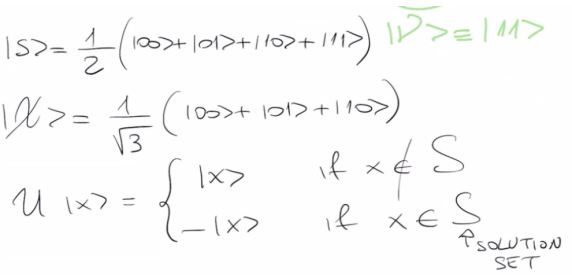
We now move to the case where m $>$ 1.

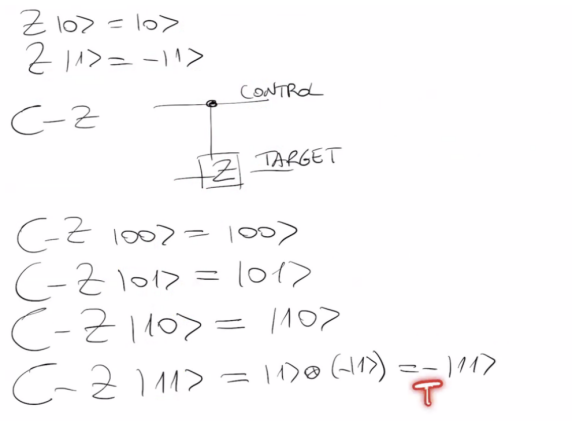


$$\langle s|\nu\rangle = \sqrt{\frac{m}{N}} \sim_{m<<<N} \theta$$

4.1 Grover Oracles

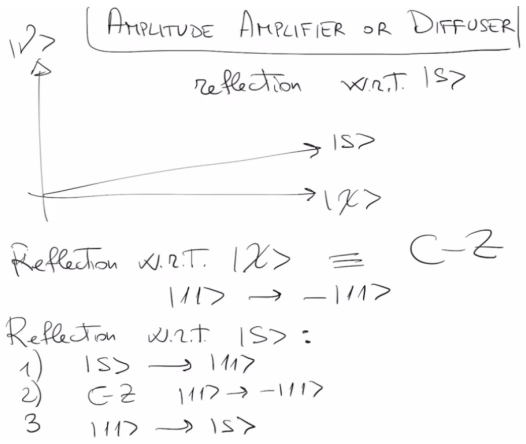
Given 2 qubits.



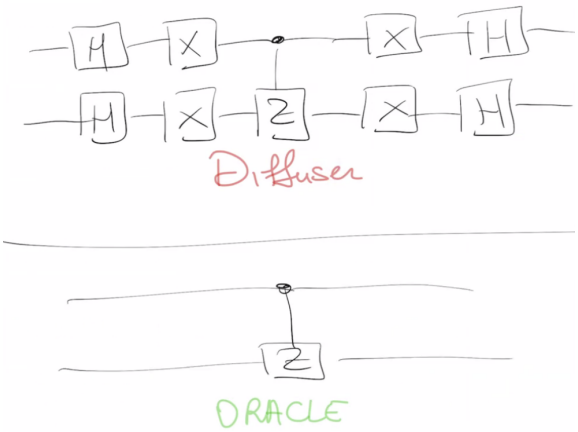


We got a phase kickback. In this case U is exactly C-Z.

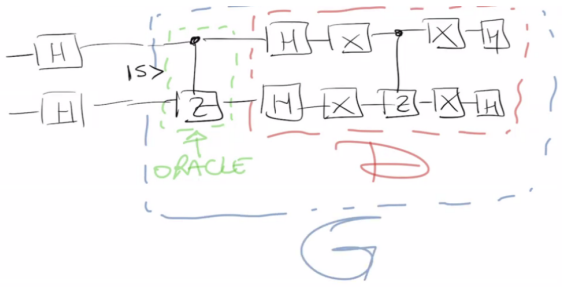
4.2 Amplitude Amplifier or Defuser



Going back from $|s\rangle$ to $|11\rangle$ you have to apply $H^{\otimes 2}$ followed by $X^{\otimes 2}$.

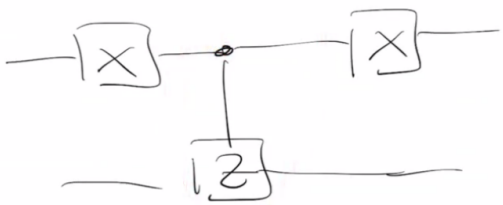


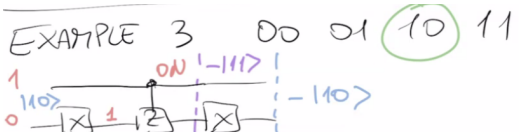
The latter quantum circuit is represented on quantum IBM by two dots. A Grover Block is obtained concatenating these two.

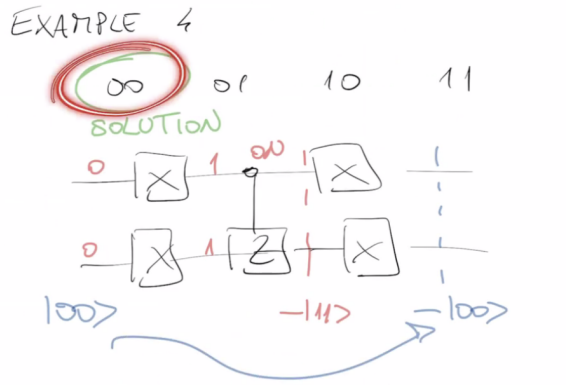


4.2.1 Examples

Give the solution equals to $|01\rangle$.
Oracle: $|01\rangle \rightarrow -|01\rangle$







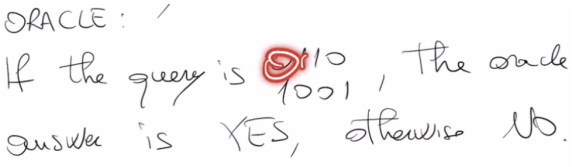
4.3 From Grover to Sudoku problem

We start by considering the binary Sudoku (2 x 2 table).

We ask ourselves: what are the solutions? {0110} and {1001}.
Let us impose the constraints

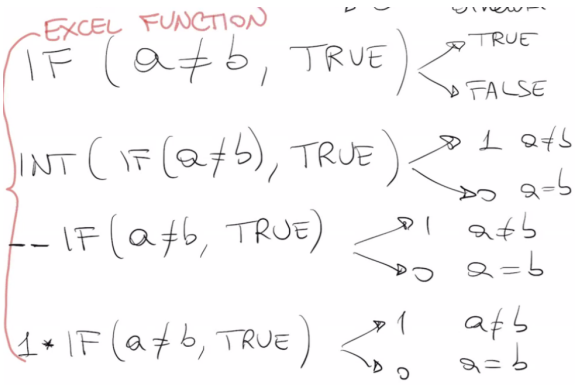
$$\begin{cases} a_0 \neq a_1 \\ a_0 \neq a_2 \\ a_2 \neq a_3 \\ a_1 \neq a_3 \end{cases}$$

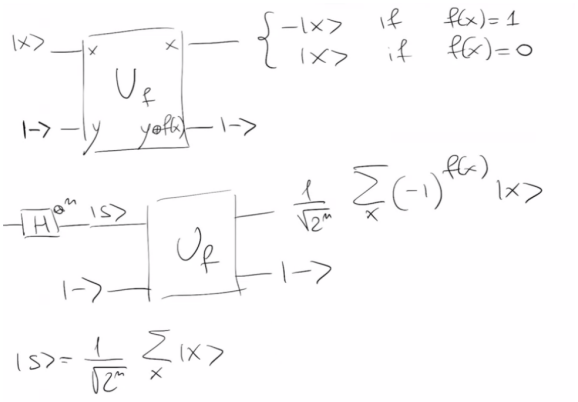
That is a decision problem connected to a function problem.



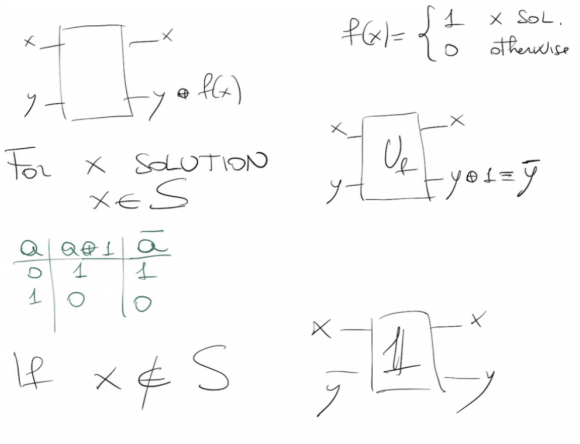
$$f(x) = \begin{cases} 1 & \text{x solution} \\ 0 & \text{otherwise} \end{cases}$$

$a \neq b : f = \begin{cases} 1 & \text{if } a \neq b \\ 0 & \text{otherwise} \end{cases}$ that can be computed using excel (? :_)).

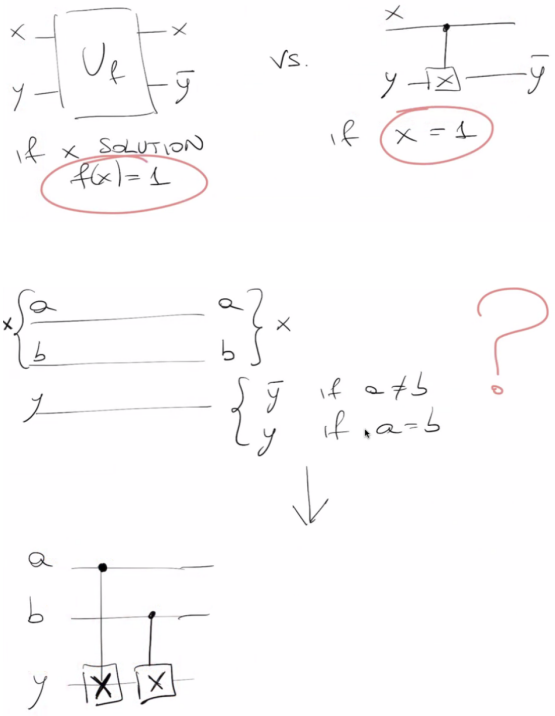


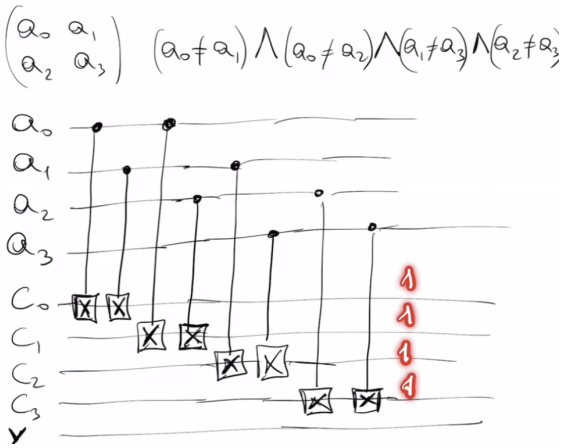


The first circuit is the oracle for any problem where f(x) is 1 if and only f x is a solution.

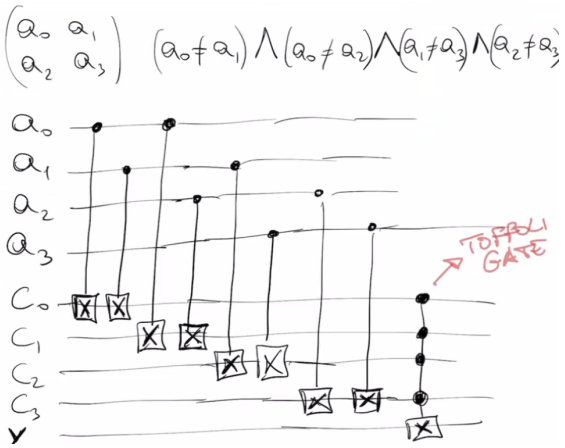


And that goes for any Grover oracle for any search problem.

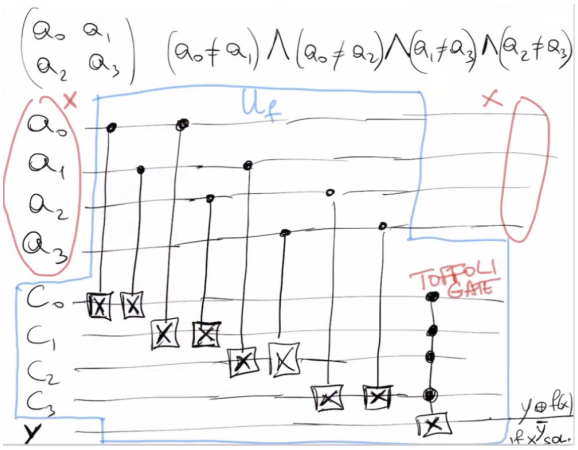


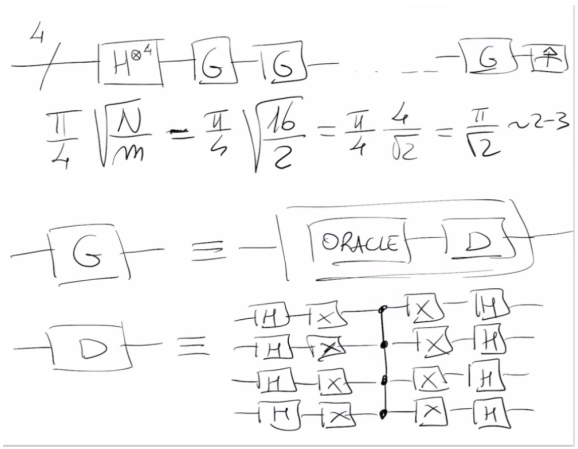


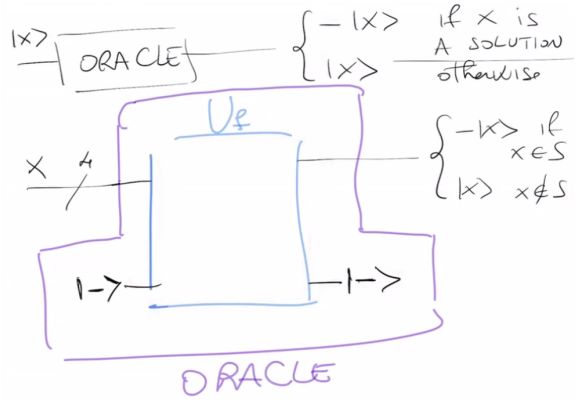
The solution is given only when all c_i are 1. What we obtain is



we can now conclude that if all a_i are a solution then I'll get 1 as y.


$(a_0 \neq a_1) \wedge (a_0 \neq a_2) \wedge (a_1 \neq a_3) \wedge (a_2 \neq a_3)$
U_f
TOFFOLI GATE
$y \oplus f(x)$
if $x \in S$


4
$H^{\otimes 4}$
G
G
G
$\frac{\pi}{4}\sqrt{\frac{N}{m}} = \frac{\pi}{4}\sqrt{\frac{16}{2}} = \frac{\pi}{4}\frac{4}{\sqrt{2}} = \frac{\pi}{\sqrt{2}} \sim 2\text{-}3$
ORACLE
D


$|x\rangle$
ORACLE
$-|x\rangle$ if x is A SOLUTION
$|x\rangle$ otherwise
U_f
X
4
$-|x\rangle$ if $x \in S$
$|x\rangle$ $x \notin S$
$|-\rangle$
$|-\rangle$
ORACLE