UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Visión Electrónica
Más que un estado sólido
https://doi.org/10.14483/issn.2248-4728

VISIÓN ELECTRONICA
A RESEARCH VISION

Classic simulation of quantum algorithm

Simulación clásica de un algoritmo cuántico

Nelson Leonardo Cubillos-Castro[1], *Yesenia Sierra-Sáenz*[2], *Jairo Ernesto Castillo-Hernández*[3]

INFORMACIÓN DEL ARTICULO

Historia del articulo
Enviado: 23/09/2018
Recibido: 24/09/2018
Aceptado: 12/11/2018

Keywords
Algorithm,
Grover,
Quantum Computing,
Quantum gate,
Hadamard, Simulation.

Palabras clave:
Algoritmo,
Grover,
Computación cuántica,
compuerta cuántica,
Hadamard, Simulación.

ABSTRACT:

Classical computing there are multiple algorithms to efficiently locate a certain element within a disorganized database; however, quantum computing can be applied more assertively in the face of problems in which it is complicated to verify a solution and at the same time to test multiple and possible solutions. Therefore, this article presents an introduction to Quantum Computing, developing some concepts of quantum formalism, and then approach Grover's algorithm which exploits the principle of superposition to the maximum. Finally, a classic simulation of this algorithm is performed, and the results obtained are compared with classical algorithms such as sequential search and binary search method. A 95% is obtained as a result of greater effectiveness in times -when solving the same search-, revealing the potential advantages of quantum computing.

RESUMEN

En la computación clásica existen múltiples algoritmos para localizar de manera eficiente un determinado elemento dentro de una base de datos desorganizada; sin embargo, la computación cuántica puede aplicarse de manera más asertiva frente a tales problemas cuando es complejo verificar una solución y a la vez probar múltiples y posibles soluciones. Por lo anterior, en este artículo se presenta una introducción a la Computación Cuántica -desarrollando algunos conceptos del formalismo cuántico-, y luego se aborda el algoritmo de Grover el cual explota al máximo el principio de superposición. Finalmente se realiza una simulación clásica de dicho algoritmo, y los resultados obtenidos se comparan con otros algoritmos clásicos como el método de búsqueda lineal y búsqueda binaria. Se obtiene como resultado un %95 de mayor efectividad en tiempos -a la hora de resolver la misma búsqueda- logrando poner de manifiesto las ventajas potenciales de la computación cuántica.

[1] BSc. In Systems Technology, Universidad Distrital Francisco José de Caldas, Colombia. Research group FIZMAKO, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Coordinator of Information and Communications Technologies at the Colegio Colombiano de Psicólogos-COLPSIC. E-mail: nlcubillosc@correo.udistrital.edu.co ORCID: https://orcid.org/0000-0002-7089-1043

[2] BSc. In Systems Technology, Universidad Distrital Francisco José de Caldas, Colombia. Research group FIZMAKO, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Team Leader at Mercado Libre. E-mail: ysierras@correo.udistrital.edu.co. ORCID: https://orcid.org/0000-0001-5447-9131

[3] B.Sc. In Physics and M.Sc. In Physics, Universidad Rusa de la Amistad de los Pueblos, URSS. Research group FIZMAKO, Universidad Distrital Francisco José de Caldas, Colombia. Current position: Professor at Universidad Distrital Francisco José de Caldas, Colombia. E-mail: jcastillo@udistrital.edu.co. ORCID: https://orcid.org/0000-0002-4278-8161

Cite this article as: N. L. Cubillos Castro, Y. Sierra Sáenz, J. E. Castillo Hernández "Classic simulation of quantum algorithm", *Visión electrónica*, vol. 2, no. 1, Special edition, january-june 2019 . https://doi.org/10.14483/issn.2248-4728

1. Introduction

It is well known that since the mid-nineteenth century with the emergence of classical computing under the architecture of the Church-Turing and Von Neumann machines [1], it was possible to build a computer capable of performing basic operations such as addition and multiplication in a few seconds. Over the years, technological developments have allowed optimizing the response time of all kinds of operations; however, there are still a large number of mathematical calculations that would take decades to be solved (e.g., determining whether a large number is prime or not.). These types of complex calculations encouraged Paul Benioff [2, 3, 4] and Richard Feynman [5] to reconsider the idea of using computers under the principles of quantum physics, so they started working with classical computers that they adapted and operated with some of the main principles of quantum mechanics. On the other hand, every day it becomes more difficult to handle classical computing because of the constant demands of miniaturization that electronic components require, knowing that soon it will not be possible to reduce them anymore and the laws of classical physics will not be considered anymore. An example of this is that transistors have a limit where they simply stop working properly. This limit is met when the electrons escape from the channels where they are supposed to flow because of the so-called tunnel effect, that in other words means if a classical particle reaches an obstacle, normally this particle can go through it and bounces back, but the electrons are quantum particles which exhibit wave behavior keeping the possibility that a significant portion of these electrons may go through the walls where they are confined. In this way, the signal can interfere through channels where it is not supposed to, causing the chip to stop working [6]; therefore, at some point, the technical progress will come to an end leaving space to the development of quantum mechanics.

It is important to stress that a quantum computer can perform all kinds of tasks that a classical computer does thanks to the fact that computability is the same, the difference lies in the time of convergence in the results obtained by the running algorithms since quantum computers have the ability to process information in parallel in a massive way. This is known as the superposition principle or superposition property; superposition is the fundamental law of quantum mechanics which defines the collection of all possible states that an object can have, meaning that a system can even be in two or more of its states at the same time, which allows the development of new and innovating algorithms.

Grover's algorithm is one of the most important algorithms of the quantum computing illustrating the fundamental quantum superposition principle by searching N records in an unordered sequence inspecting all possible combinations simultaneously, causing a significant reduction of the response time to $O(\sqrt{N})$ steps compared with a classical algorithm. Grover's algorithm is defined as a probabilistic algorithm, so the correct answer is obtained with a certain error probability that, at the same time, can be as low as desired by running more iterations. This algorithm receives a list of numbers and simultaneously the specific data to be found; afterward, a function of which its primary goal is to assign the state $f(x) = 0$ if the element that is being searched is not requested; otherwise, the assigned state is $f(x) = 1$. As soon as the desired data matches a record, the amplitude of the mentioned state is modified without affecting the other elements, obtaining that in the end, the probability of one state differs completely from the rest. The simplicity and helpfulness of this algorithm stand out the speed on response times intended to implement in the computers of the future.

In [7-12]: Feynman, Benioff, and Deutsch, Shor, among others, build theoretically the elementary gates for quantum computation that we know today.
Different search and investigations are currently being developed. In the papers [13-19] achieved information-theoretic and analytic about Grover's algorithm and the Quantum Computing and Quantum information formal world. In [20-24] gives Criteria for Quantum Teleportation and concepts about Quantum vs Classical Computing model to simulating physics problems. In papers [25-29] reviews the Quantum Computing for computer scientists through Shor's Factorization Algorithm, Grover's Search Algorithm, and the Deutsch problem. In [30] Grover explained the fast quantum mechanical algorithm for database search, and simulations as Rough Counting and weighted targets was defined in [31-36]. In [37], [38], [39] other applications are describing: quantum searching on routing algorithm, and weighting marked items. The implementing and simulating in-situ on computers, fuzzy systems, and signal detection for MIMO-OFDM systems, and CAD Accelerator, are showed in [40-45].
On the other hand, in [46-52] are demonstrate improvements in Grover's algorithm and its applications on directed diffusion, in the distributed geometric machine, comparing two Data-Encoding

Methods on Quantum Costs, in numerical Quantum Optimal Control, and Quantum Cryptanalysis.

Finally, to try to understand the operation of quantum physics, there are also several applications of the Grover algorithm as a security measure when using encryption techniques and user detection protocols [53-61], and simulations that satisfy the resolution of complex problems such as the transcendental logarithm problem, [62], [57].

This paper has been organized in the following way: First of all, preliminary concepts are introduced and some concepts of the formalisms of quantum mechanics are illustrated which will allow introducing Grover's algorithm that will be covered in the second part. Last of all, a classical simulation of Grover's algorithm is carried out and the results are compared with other classical algorithms.

2. Preliminary concepts.

2.1. About the superposition principle

Following Penrose [58], "think of the position of an electron." As we know, in a classical image, the electron by an indivisible particle could be located in position A or position B, however in the mechanical quantum-image, in some sense it has the possibility of occupying both positions simultaneously. Let |A> be the state for the electron in position A and be |B> the state of the electron in position B. According to the quantum theory (principle of superposition), there are other possible states open to the electron that is written as w |A>+ z |B> where w and z are complex weight factors. If the weight factors are taken as real numbers (not negative), then it could be considered that this combination represents, in a certain sense, a weighted probability of the expected value for the position of the electron, where w and z represent the weighted probabilities of the electron in the position A or in the position B. If w = 0 then the electron would certainly be in B, and if z = 0 it would be in A. If w = z = 1, then it represents equal possibilities for the electron in A or in B. But w and z are Complex, so that such an interpretation does not make any sense. As Penrose [58] states, we cannot say, in familiar and everyday terms, what "means" that an electron is in a state of superposition of two places at the same time with complex w and z weights. For the moment, we must simply accept that this is really the kind of description we have to adopt for quantum-level systems. In fact, quantum superposition gives rise to many directly observable effects, such as the interference peaks of a wave electron in the double-slit experiment, the last of them made in 2008 [59] its most ambitious form, electron to electron, thus proving the quantum-mechanical hypothesis.

2.2. Quantum bits and unitary transformations.

In classical computation the minimum unit of information is the bit, which can be a 0 or 1 state. A quantum bit or qubit can be in a state that is a superposition of states 0 and 1. In mathematical formalism a qubit is a Hilbert space vector C^2.

Definition 2.1 A qubit or quantum bit is a normalized vector of the space of C^2

Considering the base {|O>, |1>} of C^2, any qubit can be written as |ψ> = α| 0> + β|1>, with |α|2 + |β|2=1

Definition 2.2 A system of n-qubits is a space vector $C^{2n=}\otimes^{n}_{i=1}C^{2}$

Definition 2.3 A quantum algorithm consists of the evolution of a system represented by n-qubits.

To describe the states of a quantum system, the Dirac representation and notation is usually used [60].

Instead of writing the vector as →Vthe notation ket |v> is used. In particular, the base {|O>, |1>} of C^2, is written as:

$$|0>=\left(\frac{1}{0}\right) \text{ and } |1>=\left(\frac{0}{1}\right) \quad (1)$$

Therefore, in C^2, any vector representing the state of a quantum system is written as:

$$|\psi> = \alpha|\,0> + \beta|1> = \alpha\left(\frac{1}{0}\right) + \beta\left(\frac{0}{1}\right) \quad (2)$$

Definition 2.4 We all ket a vector of the form:

$$|\psi\rangle = \begin{pmatrix} \\ a_1 \\ a_2 \\ a_3 \\ . \\ . \\ . \\ a_n \end{pmatrix} \quad (3)$$

And bra a vector of the form:

$$|\psi\rangle = (\alpha_1 *, \alpha_2 *, \ldots \ldots . \alpha_n *) \quad (4)$$

Definition 2.5 the scalar product of bras and kets, we call it "braket":

$$\langle\psi|\varphi\rangle = (\alpha_1 *, \alpha_2 *, \ldots \ldots . \alpha_n *) \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_n \end{pmatrix} = \alpha \in C \quad (5)$$

Definition 2.6 Given a set $B = \{|u_1\rangle, |u_2\rangle, u_3\rangle, \ldots \ldots u_n\rangle,$ B is an orthonormal basis of C^n if and only if for all i, j we have

$$\langle u_i|u_j\rangle = \delta_{ij} = \begin{cases} 1 \; if \; i = j \\ 0 \; if \; i \neq j \end{cases}$$

Theorem 2.1 Let $B = \{|u_1\rangle, |u_2\rangle, u_3\rangle, \dots \dots u_n\rangle\}$ be an orthonormal basis, then $\sum_{i=1}^{N} |u_1\rangle \langle u_2| = I$

Demonstration

As

$$I \bigg| \psi\rangle = (\sum_{i=1}^{N} (|u_i\rangle \langle u_i| \bigg) (\sum_{j=1}^{N} a_j |u_i\rangle) = \sum_{i=1}^{N} \sum_{j=1}^{N} \langle a_j | u_i \rangle \langle u_i | u_j \rangle = \sum_{i=1}^{N} \langle a_i | u_i \rangle = |\psi\rangle$$

Definition 2.7 An operator *A* of C^n is a square matrix of dimension N and complex coefficients.

Definition 2.8 The tensor product ⊗, also called the external product between two matrices *A* and *B*, is defined as the matrix.

$$C = A \otimes \mathrm{B} = \begin{pmatrix} a_{11}B \;..\;..\; a_{1m}B \\ \\ \\ a_{n1}B \;..\;..\; a_{nm}B \end{pmatrix} \qquad (6)$$

Definition 2.9. The adjunct of an operator *A* is denoted by A^t and is defined as the transposed and conjugated operator of *A*. That is, if $a_{ij} = \langle u_i | A | u_j \rangle$ are the components of A the components of A^t, are

$a^*{}_{ij} = \langle u_j | A | u_i \rangle * = \langle u_i | A^t | u_j \rangle^*$

Definition 2.10. An operator *A* is Hermitic if $A = A^t$. If it is Hermitic it's diagonal must be real, since $a_{ij} = a^*{}_{ji}$, therefore $a_{ii} = a^*{}_{ii}$ that is, their eigenvalues are real.

Definition 2.11 An operator U is unitary if $U^tU = UU^t = I$

Definition 2.12 To the operators of the form $P = |\varphi\rangle\langle\varphi|$ they are called proyectors, since they project orthogonally any ket $|\Phi\rangle$ on a ket $|\varphi\rangle$

$$P|\Phi\rangle = |\varphi\rangle\langle\varphi|\Phi\rangle = a|\varphi\rangle \qquad (7)$$

Definition 2.13 A set of projectors $\{M_1, M_2 .... M_l\}$ is said to be a measurement operator if

$$\sum_{i=1}^{l} M_i M_i{}^t = I \qquad (8)$$

Definition 2.14 Unitary and Hermitic operators are called quantum gates.

Definition 2.15 It is said that a system represented by a ket $|\varphi\rangle$ evolves into system $|\varphi\rangle$ when one of the following operations is carried out:

$$|\psi\rangle \overset{U}{\rightarrow} |\varphi\rangle \; o \; |\psi\rangle \overset{M}{\rightarrow} |\varphi\rangle \qquad (9)$$

Definition 2.16 Quantum gates. The most important quantum gates, for their usefulness in the design of algorithms, are the following:

Gate *H* of Walsh-**Hadamard**.

The Hadamard gate applied to *n-qubits*, is known as the Walsh-Hadamard transformation and produces the superposition off all 2^n possible states.
This transformation is defined as:

$$W = H \otimes \mathrm{H} \otimes \mathrm{H} \otimes \dots \dots .. \otimes \mathrm{H} \qquad (10)$$

Where $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ For example, the transformation of Walsh-Hadamard applied to *n=2* qubits is defined as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \qquad (11)$$

3. Grover's algorithm

This algorithm is one of the most important of quantum computing since it exploits the principle of superposition to the maximum. It is a very attractive algorithm, since it can be used both to efficiently locate a certain element in a disorganized database, and to solve those problems in which it is very difficult to find a solution, but at the same time very simple Test possible candidates. That is, a list of size *N* is available. The classical theory needs, on average, to read $\frac{n}{2}$ values, however, the Grover algorithm requires only $\sqrt{N}$ interactions.
Mathematically the problem can be reduced to finding a $x \in \{0,1,2,3, \dots .N\}$ with with $N = 2^n$, such that $f(x) = \alpha$ for a α known. The idea proposed by Grover is based on the implementation of a function *f* such that, if *w*

denoted the x sought, then:

$$f(x)=\begin{cases}0\ if, & x\neq w\\ 1\ if, & x=w\end{cases} \quad (12)$$

From the perspective of a quantum computer, what is needed is a unitary

Transformation U$_f$ such that $U_f|x\rangle=(-1)^{f(x)}|x\rangle=\begin{cases}|x\rangle, & x\neq w\\ -|x\rangle, & x=w\end{cases}$

As we can observe in the previous equation, if it is a state x which is not the mark, then the transformation will have no effect on the state $|x\rangle$ Yes, now $U_f|w\rangle=(-1)^{f(w)}|w\rangle$ then the result will be $U_f|w\rangle=-|w\rangle$ The geometric interpretation is that the unitary matrix U_f makes a reflection in its amplitude to the marked within the set of N elements.

Grover's algorithm works in three steps as follows:

Step No1. It consists in the normalization of the amplitudes of all the states, which is achieved with a transformation of Hadamard $s\rangle=H^{\otimes \mathrm{n}}|0\rangle$ therefore, in the instant $t=0$, $|\psi_{t=0}\rangle$, $|\psi_0\rangle$, $|s\rangle$ that is, all states have the same amplitude of probability.

Step No2. The reflection U_f is applied to all states: $|\psi_t\rangle=U_f\ |\psi_0\rangle$. If $|\psi_t\rangle$ is the state $|w\rangle$ then it can be interpreted as a reflection negative $-|w\rangle$ and if they are the non-marked states $|x\rangle$ the transformation has not effect. Mathematically the transformation U_f has the following form:

$$U_f=I-2|w\rangle\langle w| \quad (13)$$

It is not difficult to observe that:

$$U_f\,|w\rangle=(I-2|w\rangle\langle w|)|w\rangle=I\,|w\rangle-2|w\rangle\langle w|w\rangle=|w\rangle-2|w\rangle=-|w\rangle$$

And that since

$$U_f\,|x\rangle=(I-2|w\rangle\langle w|)|x\rangle=I\,|x\rangle-2|w\rangle\langle w|x\rangle=I|x\rangle=|x\rangle$$

since $\langle w|x\rangle=0$.

The transformation (13) could classically be interpreted as an If-then-else selection operator.

Step No3. The third step is to apply a reflection to the state

$$U_s=2|s\rangle\langle s|-I \quad (14)$$

The transformation (14) modifies all the states to $U_S|\psi_t\rangle$ and thus completes the transformation:

$$|\psi_{t+1}\rangle=U_sU_f|\psi_0\rangle=U_S|\psi_t\rangle \quad (15)$$

The transformation (15) is amplified by the amplitude of the element marked on the average of the amplitudes.

Mathematically:

$$|\psi_t\rangle=\sum_{x''=0}^{N-1}a''_x\,|x''\rangle,\qquad U_s=\left(2(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{x'=0}^{N-1}\langle x'|)-1\right) \quad (16)$$

Therefore:

$$U_S|\psi_t\rangle=\left(2(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\right)\left(\frac{1}{\sqrt{N}}\sum_{x'=0}^{N-1}\langle x'|)-1\right)\ \sum_{x''=0}^{N-1}a''_x|x''\rangle$$

or

$$U_S|\psi_t\rangle=(\frac{2}{N}\sum_{x=0\ ,x'=0,\ \ x''=0}^{N-1}a''_x|x\rangle\langle x'|x''\rangle-\sum_{x=0}^{N-1}a_x|x\rangle$$

or

$$U_S|\psi_t\rangle=(\frac{2}{N}\sum_{x''=0}^{N-1}a''_x\sum_{x=0}^{N-1}|x\rangle-\sum_{x=0}^{N-1}a_x|x\rangle$$

from where:

$$U_S|\psi_t\rangle=\sum_{x=0}^{N-1}2\sum_{x''=0}^{N-1}\frac{a''_x}{N}-\ a_x)\,|x\rangle=\sum_{x=0}^{N-1}(2A-a_x)|x\rangle$$

Where A is the average of each a_x.

$$A=\sum_{x''=0}^{N-1}\frac{a''_x}{N} \quad (17)$$

After some reductions by the summations and the average for the state $|\psi_{t+1}\rangle$ we have:

$$|\psi_{t+1}\rangle=U_sU_f|\psi_t\rangle=\begin{cases}\dfrac{2^{n+1}+2^n-4}{2^n\sqrt{2^n}}|x\rangle, & if\ \ x=w\\ \dfrac{2^{n+1}-2^n-4}{2^n\sqrt{2^n}}\ |x\rangle, & if\ \ x\neq w\end{cases} \quad (18)$$

When implementing the algorithm in a quantum computer it repeats the three steps, and a response with greater amplitude of probability is obtained.

3.1. Simulation of Grover's algorithm.

Grover's algorithm is a search algorithm that returns the match with the highest probability to be correct from an unordered sequence of data with N elements. The running time from the classical point of view has an order of 2^n but the quantum version has an order of $2n$. This simulation [61] intends to show how the running time of a quantum algorithm in a classical computer is crucial when the goal is reducing response times.

This simulation consists of three important parts:

1. The initialization of the amplitudes of the different states obtained by the superposition, in other words, when the state of the system if

$$t = 0\ ,\ |\psi_{t=0}\rangle = |\psi_0\rangle = |s\rangle = H^{\otimes \mathrm{n}}\,|0\rangle$$

2. The reflection to all states, this means $|\psi_t\rangle = U_f|\psi_0\rangle$ where only the marked state will be affected.

3. And finally, the reflection that modifies all the states $|\psi_{t+1}\rangle = U_s|\psi_t\rangle$ completing this way the transformation.

4. Implementation and experimentation

This simulation needs the number of qubits=Qubits that will consider executing the search. This will determine the number of records.

```
System.out.println("Enter number of qubits:");
numQubits = scan.nextInt();
```

At the same time, it requires the expected record:

```
System.out.println("Enter the value you.re searching for:");
value = scan.nextInt();
```

4.1. Data processing

This process starts by executing the initializeBinary() method which will allow printing the bit string provided by the user in binary, getting as a result a bra-ket notation array using Walsh-Hadamar transform.

```
public void initializeBinary()
{
Integer i = 0;
double amplitude = 1 / Math.sqrt(Math.pow(2, numQubits));
System.out.print(amplitude);
System.out.print("(");
for (i = 0; i < Math.pow(2, numQubits) - 1; i++)
{
System.out.print("j" + Integer.toBinaryString(i) + "> + ");
}
System.out.println("j" + Integer.toBinaryString(i) + ">)");
}
```

In addition, the simulation executes the initialize() method with the purpose of printing to the screen the bit string in decimal numbers.

```
public void initialize()
{
int i = 0;
double amplitude = 1 / Math.sqrt(Math.pow(2, numQubits));
System.out.print(amplitude);
System.out.print("(");
for (i = 0; i < Math.pow(2, numQubits) - 1; i++)
{
System.out.print("j" + i + "> + ");
}
System.out.println("j" + i + ">)");
}
```

After that, the phaseInversion() method is called and this method will be responsible for the phase inversion equation (14) from Grover's algorithm, obtaining as an output, the same array but with the sign value changed.

```
public void phaseInversion()
{
double element = 0;
element = array.get(value);
System.out.println(element+"element ok");
if (element < 0);
else
{
element = -1 * element;
array.set(value, element);
System.out.println("array else"+array);
}
}
```

At the same time, the inversionMean() method is being called which calculates the reflection over the mean value, equation (14). The output shows the change of the amplitudes from the initial array, so the chance that the state collapse is higher.

```
public void inversionMean()
{
double average = 0;
double element = 0;
for (int i = 0; i < array.size(); i++)
{
average += array.get(i);
}
average = average / array.size();
for (int j = 0; j < array.size(); j++)
{
element = array.get(j);
element = (average - element) + average;
array.set(j, element);
System.out.println("array"+array);
}

}
```

Output

Finally, the simulation calculates the probability using the amplitude to the second power using the findProbability() method.

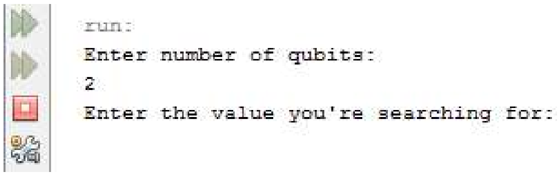
```
public double findProbability()
{
double probability = vector.get(value)/(Math.sqrt((Math.pow(2, numQubits))));
probability = Math.pow(probability, 2);
return probability;
}
```

And from the createArray() method, it is created a matrix of 2n slots obtaining the new array that will be sent to Grover's algorithm

```
public ArrayList<Double> createArray()
{
ArrayList<Double> newVector = new ArrayList<Double>();
for (int i = 0; i < Math.pow(2, numQubits); i++)
{
newVector.add(1.0);
}
return newVector;
}
```

4.2. Tests and results

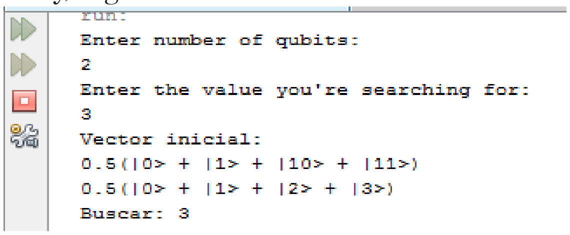
Step 1: Capture the size of the vector and the number you want to find, Figure 1:



```
run:
Enter number of qubits:
2
Enter the value you're searching for:
```

Figure 1. Entry of the number of qubits. Source: own.

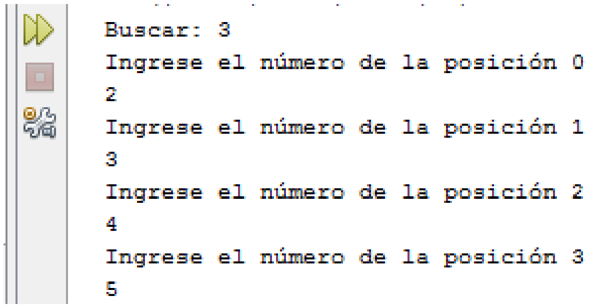
Step 2: View of the initial vector in decimal and in binary, Figure 2:



```
run:
Enter number of qubits:
2
Enter the value you're searching for:
3
Vector inicial:
0.5(|0> + |1> + |10> + |11>)
0.5(|0> + |1> + |2> + |3>)
Buscar: 3
```

Figure 2. View of the initial vector. Source: own.

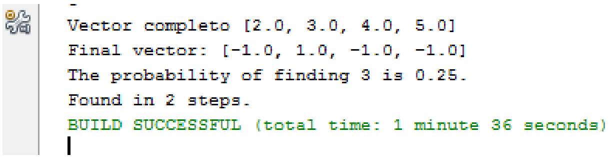
Step 3: Capture of the numbers that the vector will store, Figure 3:



```
Buscar: 3
Ingrese el número de la posición 0
2
Ingrese el número de la posición 1
3
Ingrese el número de la posición 2
4
Ingrese el número de la posición 3
5
```

Figure 3. Capture of the numbers. Source: own.

Step 4: View of the complete vector and the final vector after the completion of the search, Figure 4:



```
Vector completo [2.0, 3.0, 4.0, 5.0]
Final vector: [-1.0, 1.0, -1.0, -1.0]
The probability of finding 3 is 0.25.
Found in 2 steps.
BUILD SUCCESSFUL (total time: 1 minute 36 seconds)
```

Figure 4. Complete vector. Source: own.

4.3. Comparison of results with other classical algorithms

The simulation of a quantum search using Grover's algorithm (G) and the simulations of sequential search (SS) and binary search (BS), allow determining the efficiency of the quantum algorithm compared to a simple search algorithm. After analyzing five different sizes of arrays, each with a sample of 20 measurements, it is possible to obtain an average which is illustrated in the next table. In the three algorithms, the simulation uses an unordered list with *N* elements, Table 1.

Vector size	Algorithm	N° of Interactions	Response time
4	G	2	0,0028369
	BS	4	0,32 98
	BB	3	0,28
16	G	4	0,00328628
	BS	16	0,3845
	BB	5	0,3
32	G	5	0,003958214
	BS	32	0,3911
	BB	6	0,3096
64	G	8	0,00523802
	BS	64	0,3997
	BB	10	0,3141
128	G	11	0,01546982
	BS	128	0,4009
	BB	12	0,3299

Table 1. Comparison of results with other classical algorithms. Source: own.

5. Conclusions

The development of this simulation allowed us to compare the speed of response of two algorithms that at first sight fulfill the same function but behind there are a number of advantages of the quantum algorithm with respect to the classical, such as a reduced number of interactions to obtain the same result, a percentage of error that is proportional to the same number of interactions (the more, the better), an opening to the resolution of mathematical problems of all kinds that, today are impossible to solve and last but not least , a good use of resources if time is concerned. In the results obtained after the comparison of Sequential, Binary and Grover search algorithms, it is evident that the Grover algorithm is 95% more effective in search times. These significant results in the decrease of time in the search, will give way to what we know as classical computing have transcendental changes and generate a revolution in computing and in all technology.

At the same time, understanding the scope and potential of quantum computing in the technology of the future, tells us that it is only necessary to create new tools that allow implementing algorithms such as those of Grover, to leave behind all the algorithms that are currently in charge to move the world, but that are vulnerable to current supercomputers based on Spintronics [62].

Acknowledgments

We thank the research group FIZMAKO, for giving us the opportunity to address an issue as important as quantum computing, there is no doubt that it is a science that still needs much to explore, however it is very valuable to understand some concepts and their operation, We also thank the SciBas group.

References

[1] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines”, *J. Stat. Phys.*, vol. 22, pp. 563—591, 1980. https://doi.org/10.1007/BF01011339

[2] P. Benioff. “Quantum mechanical Hamiltonian models of Turing machines”, *J. Stat. Phys.*, vol. 29, pp. 515—546, 1982. https://doi.org/10.1007/BF01342185

[3] P. Benioff. Quantum mechanical models of Turing machines that dissipate no energy. Phys. Rev. Lett. vol. 48, pp. 1581—1585, 1982. https://doi.org/10.1103/PhysRevLett.48.1581

[4] R. P. Feynman. Simulating physics with computers. Int. J. Theor. Phys. 21, pp. 467—488, 1982. https://doi.org/10.1007/BF02650179

[5] R. P. Feynman. Quantum mechanical computers. Opt. News, 1985. https://doi.org/10.1364/ON.11.2.000011

[6] V. Moret-Bonillo. Principios fundamentales de computación cuántica, 2013, Universidad de La Coruña.

[7] R. P. Feynman, International Journal of Theoretical Physics, 1982. https://doi.org/10.1007/BF02650179

[8] P. Benioff, Physical Review Letters, 1982. https://doi.org/10.1103/PhysRevLett.48.1581

[9] D. Deutsch, Proceedings of the Royal Society of London Series A., 1985.

[10] D. Deutsch, Proceedings of the Royal Society of London, 1989. https://doi.org/10.1098/rspa.1989.0099

[11] A. Barenco, Charles H. Bennett, Richard Cleve David P. DiVincenzo, Norman Margolus Peter Shor Tycho Sleator, John Smolin y Harald Weinfurter, “Elementary gates for quantum computation”, *Phys. Rev. A*, vol. 52, no. 5, pp. 3457-3467, 1995. https://doi.org/10.1103/PhysRevA.52.3457

[12] Serway, R. A., Jewett, J. W., Hernández, A. E. G., & López, E. F. “Física para ciencias e ingeniería”, vol. 6, Thomson, 2006.

[13] E. Arikan. “An information-theoretic analysis of Grover's algorithm”, 2003. [En línea]. https://doi.org/10.1109/ISIT.2003.1228418

[14] J. Richard, W. Kenneth. “Grover's Algorithm”, 2014. [En línea]. Disponible en: https://ieeexplore.ieee.org/xpl/ebooks/bookPdfWithBanner.jsp?fileName=7010444.pdf&bkn=7008157&pdfType=chapter

[15] D. Deutsch. Quantum theory, the Church-Turing principle and the universal Quantum computer. *Proc. Roy. Soc. Lond*, pp. 97-117, 1985. https://doi.org/10.1098/rspa.1985.0070

[16] S. Aarón; Viviana; S. Esteban, “Un análisis profundo del fenómeno dualidad onda partícula para la comprensión del mundo cuántico”, *Latin-American Journal of Physics Education*, 2012, vol. 6, no 1.

[17] B. José Enrique. G. Pablo. S José Javier. Introducción al formalismo de la mecánica cuántica. Editorial UNED, 2010.

[18] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information", Cambridge University Press, 2000.

[19] Meglicki, Z., "Quantum Computing without Magic: Devices", The MIT Press, 2008. https://doi.org/10.7551/mitpress/7724.001.0001

[20] Gisin, N., "Nonlocality Criteria for Quantum Teleportation", *Phys. Rev. Lett. A*, vol. 210, pp. 151-156, 1996. https://doi.org/10.1016/S0375-9601 96)80001-6

[21] Grupo de Computación Cuántica, Departamento de Matemática Aplicada, E.U. Informática, U. Politécnica Madrid, "Introducción al Modelo Cuántico de Computación", TECHNICAL REPORT Nº 19, 2003.

[22] R. P. Feynman, "Conferencias Sobre Computación", Crítica eds., 2003.

[23] R. P. Feynman, "Simulating Physics with Computers", International Journal of Theoretical Physics, vol. 21, pp. 467-488, 1982. https://doi.org/10.1007/BF02650179

[24] E. Desurvire, "Classical and Quantum Information Theory", Cambridge University Press. 2009. https://doi.org/10.1017/CBO9780511803758

[25] J. Laverde, H. Cárdenas, "Estado del arte en computación cuántica", *Visión Electrónica*, 2018.

[26] N. S. Yanofsky, and M. A. Mannucci, "Quantum Computing for Computer Scientists", Cambridge University Press, 2008. https://doi.org/10.1017/CBO9780511813887

[27] S. Andrés. Algunos elementos introductorios acerca de la computación cuántica. Memorias VII Encuentro ERM, Universidad de Antioquia, Medellín, 1999, vol. 23.

[28] S. Andrés; V. Mario; G. Fredy; G. Cathalina; O. Luis; P. Carlos. et al. Introduction to Quantum Computing through Shor's Factorization Algorithm and Grover's Search Algorithm. 1999.

[29] S. Andrés; V. Mario; P. Carlos. Paralelismo cuántico: el problema de Deutsch.

[30] L. K. Grover, "A fast quantum mechanical algorithm for database search", Proceeding of the 28th Annual ACM Symposium on Theory of Computing, 1996. https://doi.org/10.1145/237814.237866

[31] X. Xue, H. Chen, K. Chen, Z. Li. "On the Research of BDD Based Simulation of Grover's Algorithm", 2008. [En línea]. https://doi.org/10.1109/WGEC.2008.87

[32] X. Li, K. Song, N. Sun, C. Zhao. "Phase matching in grover's algorithm", 2013. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/6640838

[33] I. Hamouda, M. Bahaa-Eldin, H. Said. "A generalized Grover's algorithm with access control to quantum databases", 2016. https://doi.org/10.1109/ICCES.2016.7822015

[34] N. Benchasattabuse, P. Chongstitvatana, Ch. Apomtewan. "Quantum Rough Counting and Its Application to Grover's Search Algorithm", 2018. https://doi.org/10.1109/CCOMS.2018.8463331

[35] L. Panchi, L. Shiyong. "Grover quantum searching algorithm based on weighted targets", 2008. https://doi.org/10.1016/S1004-4132 , 08)60093-6

[36] M. Li, Q. Yang, H. Zhang. "Microwave Simulation of Grover's Quantum Search Algorithm", 2018. https://doi.org/10.1109/MAP.2006.277153

[37] M. Li-min, S. Xin-yu, Z. Kai. "Research on routing algorithm for MANET based on Grover searching theory", 2010. https://doi.org/10.1109/ICWITS.2010.5611812

[38] X. Li, K. Song, N. Sun, Ch. Zhao. "Quantum searching algorithm based on the weighting marked items", 2013. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/6640837/

[39] K. Arima, N. Shigei, H. Miyajima. "A Proposal of a Quantum Search Algorithm", 2009. https://doi.org/10.1109/ICCIT.2009.126

[40] A. Mandviwalla, K. Ohshiro, B. Ji. "Implementing Grover's Algorithm on the IBM Quantum Computers", 2018. https://doi.org/10.1109/BigData.2018.8622457

[41] A. Giovanni, F. Luongo, A. Vitiello. "Quantum Implementation of Fuzzy Systems through Grover's Algorithm", 2018. https://doi.org/10.1109/FUZZ-IEEE.2018.8491579

[42] A. Avila, R. Reiser, A. Yamin, M. Pilla. "Efficient In-Situ Quantum Computing Simulation of Shor's and Grover's

Algorithms", 2017. https://doi.org/10.1109/SBAC-PADW.2017.19

[43] F. Li, Li. Zhou, L. Liu, H. Li. "A quantum search based signal detection for MIMO-OFDM systems", 2011. https://doi.org/10.1109/CTS.2011.5898934

[44] P. Zuliani. "A Formal Derivation of Grover's Quantum Search Algorithm", 2007. https://doi.org/10.1109/TASE.2007.3

[45] L. Li, M. Thornton, M. Perkowski. "A Quantum CAD Accelerator Based on Grover's Algorithm for Finding the Minimum Fixed Polarity Reed-Muller Form", 2006.

[46] K. Kang, "Two improvements in Grover's algorithm", 2015. https://doi.org/10.1109/CCDC.2015.7162096

[47] A. Bushnag, A. Alessa, M. Li, K. Elleithy. "Directed diffusion based on weighted Grover's quantum algorithm DWGQ", 2015. https://doi.org/10.1109/LISAT.2015.7160216

[48] A. Avila, R. Reiser, A. Yamin, M. Pilla. "Parallel simulation of Shor's and Grover's algorithms in the distributed geometric machine", 2017. https://doi.org/10.1109/FSKD.2017.8393304

[49] S. Dhawan, M. Perkowski. "Comparison of Influence of Two Data-Encoding Methods for Grover Algorithm on Quantum Costs", 2011. https://doi.org/10.1109/ISMVL.2011.29

[50] M. Li, Q. Yang, H. Zhang. "A Numerical Quantum Optimal Control with Grover Iteration", 2018. https://doi.org/10.23919/ChiCC.2018.8483175

[51] S. Jordan, Y. Liu. "Quantum Cryptanalysis: Shor, Grover, and Beyond", 2018. https://doi.org/10.1109/MSP.2018.3761719

[52] F. P. Zen, A. N. Atmaja, and S. Sigit, "Pencarian data dengan indeks tak-terurut menggunakan algoritma kuantum ", Indonesian Journal of Physics, no.4, October 2003.

[53] Z. Sakhi, R. Kabil, A. Tragha, M. Bennai. "Quantum cryptography based on Grover's algorithm", 2012. https://doi.org/10.1109/INTECH.2012.6457788

[54] A. Saha, A. Chongder, S. Mandal, A. Chakrabarti. "Multiuser detection based on Grover's algorithm", 2015. https://doi.org/10.1109/ISCAS.2006.1693688

[55] Z. Qu, Z. Li, G. Xu, S. Wu, X. Wang. "Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm", 2019. https://doi.org/10.1109/ACCESS.2019.2909906

[56] Y. Tang, S. Su. "Application of Grover's Quantum Search Algorithm to Solve the Transcendental Logarithm Problem", 2014. https://doi.org/10.1109/CIS.2014.166

[57] A. Saha, A. Chongder, S. Mandal, A. Chakrabarti. "Synthesis of Vertex Coloring Problem Using Grover's Algorithm", 2015. https://doi.org/10.1109/iNIS.2015.55

[58] P. Roger; S. Javier García. Las sombras de la mente. Ed. Crítica, 1996.

[59] H. T. Schmid et al., "Evidence of wave-particle duality for single fast hydrogen atom. Phys. Rev. Lett.https://doi.org/10.1103/PhysRevLett.101.083201

[60] P. A. M. Dirac. The principles of quantum Mechanics. 1958 No. 27. Oxford University Press

[61] DK Lee, D. Derek. 2016. Grover_Algorithm, San José CA. Recuperado de https://github.com/dqdang/Grover-Algorithm/blob/5f6cb123ef5aad6585c392487a472e59dbdc71e0/src/Driver.java#L1-L76

[62] J. A. Olarte, M. C. Cifuentes, "Espintrónica: principios básicos y aplicaciones". Visión Electrónica, algo más que un estado sólido, vol. 8, No. 2, 155-161, julio-diciembre de 2014.