

Quantum Computing. Notes.

Roberto Maestre (rmaestre@gmail.com)

1 Electron's spin

The electron's spin, is a quantum property in which electron behaves as a magnet but with only two possible vertical directions: up or down (North-South, South-North). Next figure represents these two positions when an electron is observed.

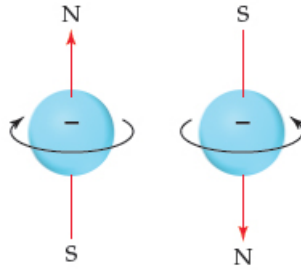


Figure 1: Spin

This phenomenon can be observed (and was experimentally demonstrated) with the Stern-Gerlach experiment. It demonstrates that the spatial orientation of angular momentum is quantized. The screen (points 4,5 in figure) reveals discrete points of accumulation rather than a continuous distribution, owing to the quantum nature of spin.

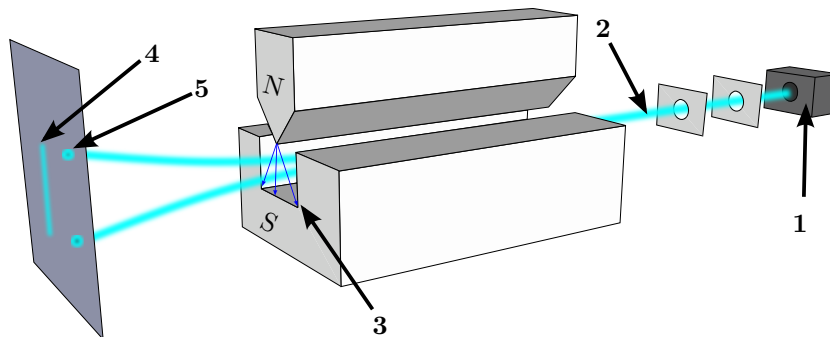


Figure 2: Stern-Gerlach experiment.

2 Quantum state and qubit

The quantum state of the system, can be defined as:

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad (1)$$

where $\alpha, \beta \in \mathbb{C}$. The quantum theory predicts the probability to find the electron's spin up with $|\alpha|^2$ and that the probability to find the electron's spin down with $|\beta|^2$.

Qubits represent 0 and 1 using quantum phenomenon like the nuclear spin direction of individual atoms. Conventionally, these two states are taken to be $|0\rangle$ and $|1\rangle$.

Quantum **superposition** is a fundamental principle of quantum mechanics. It states that that every quantum state can be represented as a sum of two or more other distinct states. Thus a Qubit is represented as a lineal superposition of:

$$\alpha|0\rangle + \beta|1\rangle \quad (2)$$

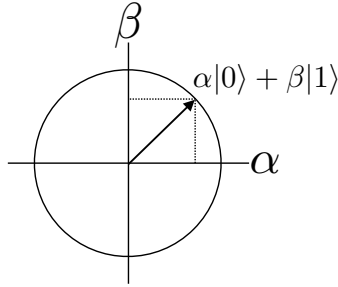


Figure 3: Qubit

Notice that n classical bits can only be in 1 state, while n qubits can be in a state comprised of all possible 2^n states. Thus a quantum computer has the potential to do 2^n calculations in a single step.

3 System measurement

A **measure** of a qubit, causes the system collapses to the observed state, with probability $|\alpha|^2$ for state $|0\rangle$ and $|\beta|^2$ for state $|1\rangle$ (for $\alpha, \beta \in \mathbb{C}$ satisfying $|\alpha|^2 + |\beta|^2 = 1$). Graphically, we can represent the next squares as a qbit states with probabilities $1, \frac{1}{2}, \frac{1}{4}, \dots$:

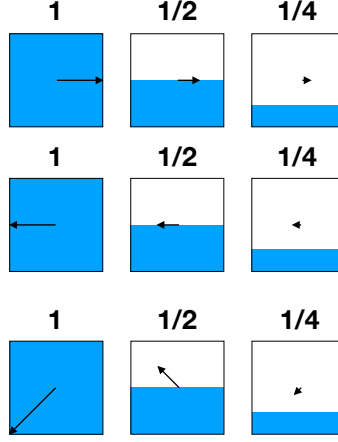


Figure 4: Graphical representation of a qbit (Probability is given by the "blue area" inside each square, and spin direction is defined by the arrow's head)

As we mentioned before, a qbit can hold different states. Next Figure proposes three examples of states s_1, \dots, s_4 is defined as a lineal combination in the next form $\alpha|0\rangle + \beta|1\rangle$ and the probability of observe $|0\rangle$ or $|1\rangle$ are $|\alpha|^2, |\beta|^2$ for $|0\rangle, |2\rangle$ respectively.

qbA	s_0	s_1	s_2	s_3
0				
1				

Figure 5: Examples of possible qbit states

Before states are formally defined as follows:

$$\begin{aligned}
 s_0 &= 1|0\rangle + 0|1\rangle \\
 s_1 &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\
 s_2 &= 0|0\rangle - 1|1\rangle \\
 s_3 &= -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle
 \end{aligned} \tag{3}$$

If we measure s_0 we get $|0\rangle$ with probability 1, measuring s_1 we get $|0\rangle$ or $|1\rangle$ with probability $\frac{1}{2}$, s_2 measurement returns $|1\rangle$ with probability 1 and s_3 $|0\rangle$

or $|1\rangle$ with probability $\frac{1}{2}$. Notice that the spin direction does not affect to the probability.

We also can combined state of two qubits in the next form:

$$\begin{aligned}
 |\psi_1\rangle &= \alpha_1|0\rangle + \beta_1|1\rangle \\
 |\psi_2\rangle &= \alpha_2|0\rangle + \beta_2|1\rangle \\
 |\psi_1\rangle|\psi_2\rangle &= (\alpha_1|0\rangle + \beta_1|1\rangle)(\alpha_2|0\rangle + \beta_2|1\rangle) \\
 &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle
 \end{aligned} \tag{4}$$

Again, if we measure the state of these qubits, we will obtain one of $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ with probability $|\alpha_1\alpha_2|^2, |\alpha_1\beta_2|^2, |\beta_1\alpha_2|^2, |\beta_1\beta_2|^2$ respectively.

Suppose that we have two qbits with the a state represented by the next Figure. Notice that the system state representing for the two qbits are in a super





qbA	qbB	s ₀
0	0	
0	1	
1	0	
1	1	

Figure 6: Probabilities values are 0.06, 0.5, 0.15, 0.29 given by $|\alpha_1\alpha_2|^2, |\alpha_1\beta_2|^2, |\beta_1\alpha_2|^2, |\beta_1\beta_2|^2$ respectively.

If we repeatedly measure these two qbits (independently from state s_0), we will get the next histogram:

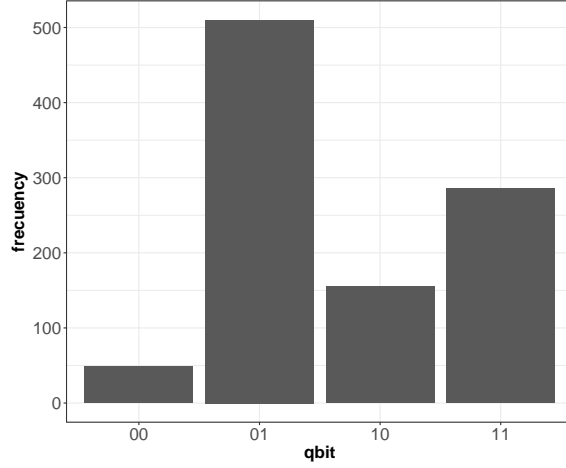


Figure 7: 1000 measurement experiment over qbA and qbB

An interesting result arises from the fact that the a system measurement is a probabilistic outcome (i.e.: one of $|00\rangle, \dots, |11\rangle$).

4 Hadamard

The "Hadamard operator" is a special quantum operator that can be applied to qubits. It is a one-qbit rotation, mapping the states $|0\rangle, |1\rangle$ to two superposition states with equal weight in $|0\rangle, |1\rangle$ i.e.:

$$|0\rangle \text{ to } \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1\rangle \text{ to } \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (5)$$

In Diract notation the operator is defined as:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (6)$$

Next figure represents the operator over two states and its main properties:

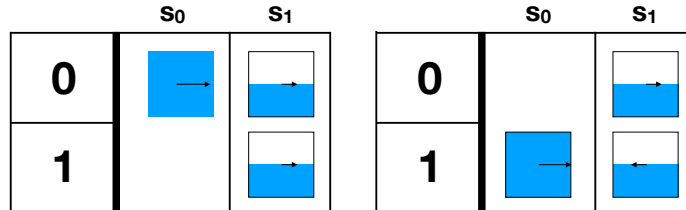


Figure 8: Hadamard operator

On the left we observe that applying Hadamard operator in state $s_0(\begin{bmatrix} 1 \\ 0 \end{bmatrix})$ with probability $|\alpha|^2 = 1.0, |\beta|^2 = 0.0$ is transformed to a state $s_1(\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix})$ with probabilities $|\alpha|^2 = \frac{1}{2}$ and $|\beta|^2 = \frac{1}{2}$ conserving the same spin direction.

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} * \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 \frac{1}{\sqrt{2}} + 0 \frac{1}{\sqrt{2}} \\ 1 \frac{1}{\sqrt{2}} + 0 \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \quad (7)$$

On the right Hadamard operator in state $s_0(\begin{bmatrix} 0 \\ 1 \end{bmatrix})$ with probability $|\alpha|^2 = 0.0, |\beta|^2 = 1.0$ is transformed to a state $s_1(\begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix})$ with probabilities $|\alpha|^2 = \frac{1}{2}$ and $|\beta|^2 = \frac{1}{2}$ however the spin direction in $|1\rangle$ is modified.

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} * \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 \frac{1}{\sqrt{2}} + 1 \frac{1}{\sqrt{2}} \\ 0 \frac{1}{\sqrt{2}} + 1 \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \quad (8)$$

5 Quantum interference

Another main concept is "quantum interference". The process of phases causing possible outcomes to cancel or re-enforce is what physicists call interference. Next Figure shows cancel and re-enforce interference when Hadamard operator is applied twice.

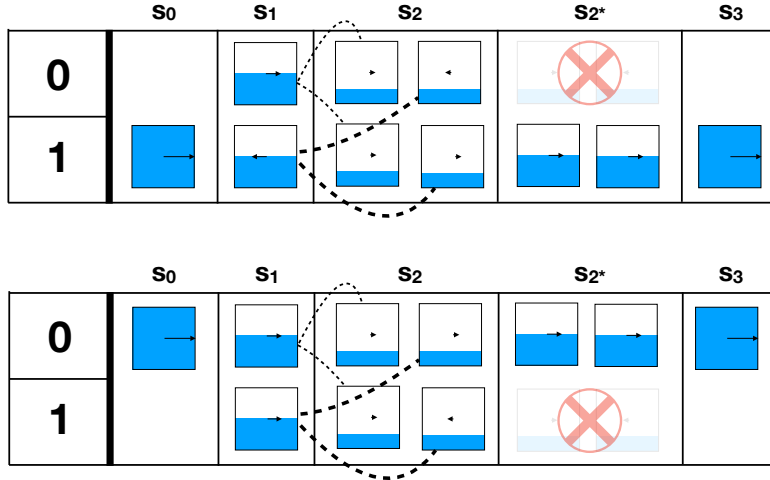


Figure 9: Hadamard operator applied twice

Valid states are s_0, s_1, s_2, s_3 in which the constrain defined by $|\alpha|^2 + |\beta|^2 = 1$ is hold. The state s_{2*} is defined to visually represents the outcome cancellation and re-enforce given the specific phases.

Thus applying the Hadamard operator twice always returns the qubit to its original value. More formally:




$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} * \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 \frac{1}{\sqrt{2}} + 0 \frac{1}{\sqrt{2}} \\ 1 \frac{1}{\sqrt{2}} + 0 \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \quad (9)$$

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

6 Multiple qubits

As we defined in equation 4, if we have two qbits qbA and qbB , a superposition of these two qbits is a four dimensional vector. For instance, in figure 10 (on the left) the state s_0 is defined as $[1 \ 0 \ 0 \ 0]^T$ and state s_1 is defined as: $[\frac{1}{\sqrt{2}} \ 0 \ \frac{1}{\sqrt{2}} \ 0]^T$.

Next figure visually represents, on the left Hadamard operator applied on qbA , and on the right applied on qbB .

qbA	qbB	s0	s1
0	0		
0	1		
1	0		
1	1		




qbA	qbB	s0	s1
0	0		
0	1		
1	0		
1	1		

Figure 10: Hadamard operator on two qubits system. On the left is applied on qbitA, on the right is applied on qbitB.

More formally, the application of Hadamard (H) operator on qbA (left on figure 10) is defined as follows:

$$\begin{aligned}
H \otimes I &= \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \\
H \otimes I &\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}
\end{aligned} \tag{10}$$

Following the definition of mixed states in equation 4, we get that $\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}$ and $\beta_1\alpha_2 = \frac{1}{\sqrt{2}}$; thus the probability of $|00\rangle, |10\rangle$ are $\frac{1}{2}$ respectively.

Applying Hadamard operator in the qdB is defined as:

$$\begin{aligned}
I \otimes H &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \\
H \otimes I &\begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix}
\end{aligned} \tag{11}$$

Therefore $\alpha_1\alpha_2 = \frac{1}{\sqrt{2}}$ and $\alpha_1\beta_2 = -\frac{1}{\sqrt{2}}$. The probabilities in $|00\rangle, |01\rangle$ are $\frac{1}{2}$ respectively.

In a general way, we can apply a Hadamard way over n-qubits as follows:

$$H^{\otimes n} \tag{12}$$

For instance:

$$H^{\otimes 2} = H \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} \end{bmatrix} \tag{13}$$

Next figure 11 represents the application of Hadamard gate on two qubits at once.






qbA	qbB	s_0	s_1
0	0		
0	1		
1	0		
1	1		

Figure 11: Hadamard operator on all qubits.

Thus, if vector representing s_0 is $\begin{bmatrix} \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \end{bmatrix}$, Hadamard operator over all qubits can be applied as follows:

$$H^{\otimes 2} s_0 = \begin{bmatrix} \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & -\frac{1}{\sqrt{2^2}} & \frac{1}{\sqrt{2^2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \\ \frac{1}{\sqrt{2^2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (14)$$

Notice that all states, s_0, s_1 , always holds $|\alpha|^2 + |\beta|^2 = 1$.

7 Applications

7.1 Quantum Search over 2 Qubits

Gover's Search Algorithm finds the unique input to a function that produces a particular output value, using just $O(\sqrt{N})$ evaluations of the function. The analogous problem in classical computation cannot be solved in fewer than $O(N)$ (in the worst case).

Lets propose a simple example consisting in one function, that returns 1 (or *true*) if $x = 1$ and 0 (or *false*) otherwise. Thus, we define this function as follows:

$$f(x) = \begin{cases} 1 & \text{if } x \in \{0, 2, 3\} \\ 0 & \text{if } x = 1 \end{cases} \quad (15)$$

So, if we want to find the number, among a set of numbers $\{0, 1, 2, 3\}$, that returns $f(x) = 1$ we need to execute the function f four times checking the

result i.e.: $f(1), f(2), f(3), f(4)$. However in a quantum computer we only need to execute five operations over the entire set of numbers. Thus, if we have a 500 qbits computer each operation will be performed over 2^{500} numbers. Next figure shows an example of quantum search over 2 qbits taking into account the function defined in equation 15.

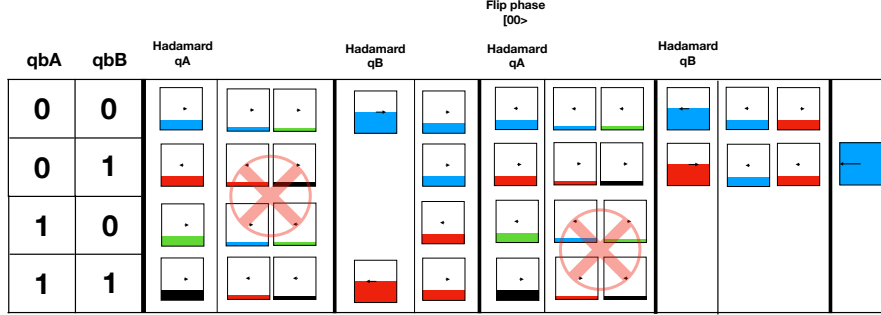


Figure 12: Quantum Search. Colors are used to easily follow the superposition created by the quantum operators. Algorithm starts with equal probability for all states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ but the spin direction of $|01\rangle$ is flipped. The algorithm ends with probability 1 in $|01\rangle$

7.2 Grover's algorithm

In a general form, Grover's algorithm searches one element in a non-sorted list of items. Using the example defined by equation 15 (oracle function), the Grover's algorithm follows the next pseudocode.

Algorithm 1 Grover's algorithm

- 1: Initialize state: $|0\rangle^{\otimes n}$
 - 2: **for** $i = 1, I$ **do** ▷ Number of iterations
 - 3: Call oracle function $f(x)$. Equation 15
 - 4: Apply Hadamard $H^{\otimes n}$
 - 5: Negate $|x\rangle, \forall x \neq 0^n$
 - 6: Apply Hadamard $H^{\otimes n}$
-

If we perform a search over a system with 13 Qubits ($2^{13} = 8192$ possibilities) and we plot the probability of the Qubit for which the oracle function is 1 we obtain the behaviour representing for the next figure:

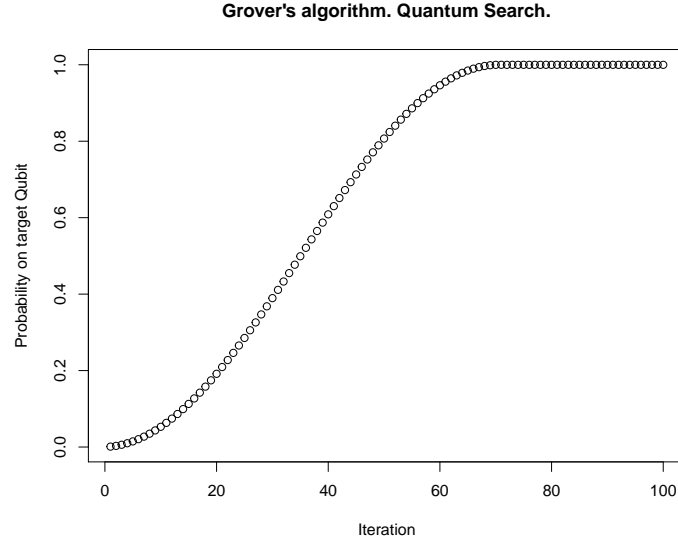


Figure 13: Probability on the targeted Qubit in each iteration

Notice that, each algorithm's iteration moves the amplitude $\frac{1}{\sqrt{n}}$ towards solutions. Next code implements (simulating) the pseudocode defined by algorithm 1.

7.3 Shor's algorithm.

7.4 Key sharing through foton polarization.

References