Grover's Search algorithm: Explanation and implementation in pyQuil

Dawid Kopczyk, Quantee

Warsaw Quantum Computing meeting - part IV

25.02.2019

Outline

Introduction

Objectives

- Grover's Search algorithm **is a great start**
- You will learn **basics about the algorithm** - not why, but how it works
- You will learn to **implement the algorithm in Rigetti pyQuil**

Introduction

Assumptions

- Introduction to quantum computing: gates, Dirac notation, etc.
- Introduction to pyQuil
- A little bit of Python

Introduction

About me

Quantee

BOHR

Algorithm

History

L.K. Grover, *A fast quantum mechanical algorithm for database search*, (1996)

Advantage

Grover's Search is a quantum algorithm that speeds up solving an unstructured search problem **quadratically**.

Purpose

The Grover's algorithm is not directly intended to find an element in a database, its purpose is **searching through a function inputs** to check whether the function returns **true for a particular input**.

Algorithm

Unordered array of $N = 2^n$ binary strings of length n:

x	**f(x)**
00000000	0
00000001	0
...	
01101010	1
01101011	0
01101100	0
...	
11111110	0
11111111	0

$$n = 8$$

$$N = 2^8 = 256$$

Algorithm

Classical

- In the worst case, takes N queries
- In average, takes $N/2$ queries
- In summary, $\mathcal{O}(N)$

Quantum

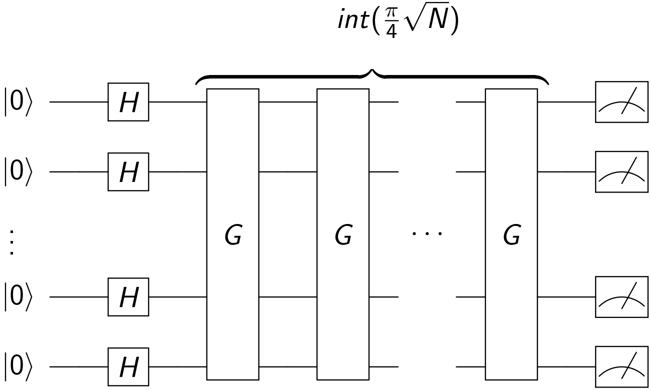
- Does the job in $\mathcal{O}(\sqrt{N})$ queries

Algorithm

Grover's search algorithm is **probabilistic**, in the sense that it gives the correct answer with high probability. The probability of failure can be decreased by repeating the algorithm.

Algorithm

Quantum Circuit



Initialization

We begin with the initialized state:

$$|\psi_0\rangle = |00\ldots0\rangle \tag{1}$$

Initialization

Quantum Circuit

$|0\rangle$ —

$|0\rangle$ —

$\vdots$

$|0\rangle$ —

$|0\rangle$ —

$|\psi_0\rangle$

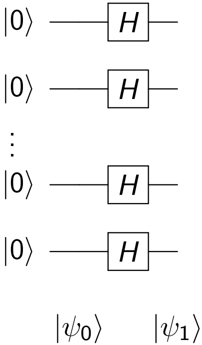
Superposition

We put the computer in equal superposition state

$$\begin{aligned} |\psi_1\rangle &= H^{\otimes n} |\psi_0\rangle \\ &= \frac{1}{\sqrt{N}} (|00\ldots0\rangle + |00\ldots1\rangle + \cdots + |11\ldots1\rangle) \end{aligned} \tag{2}$$

Superposition

Quantum Circuit



Quantum Oracle

Let's consider a simple $n = 2$ example.

Consider the function:

$$f(x) = \begin{cases} 1 & x = \text{'10'} \\ 0 & x \neq \text{'10'} \end{cases} \tag{3}$$

We need to represent function $f(x) : \{0, 1\}^2 \rightarrow \{0, 1\}$ as quantum oracle O.

Quantum Oracle

- First guess: $O\left|x\right\rangle = \left|f(x)\right\rangle$

Quantum Oracle

- ~~First guess:~~ $\cancel{O\left|x\right\rangle = \left|f(x)\right\rangle}$ Not unitary!
- However, there exists a method of constructing the quantum oracle as:

$$O\left|x\right\rangle = (-1)^{f(x)}\left|x\right\rangle . \tag{4}$$

$$O\left|x\right\rangle = \begin{cases} -\left|x\right\rangle & x = '10' \\ +\left|x\right\rangle & x \neq '10' \end{cases}$$

Quantum Oracle

In that particular example the quantum oracle acts on two input qubits and is expressed as the matrix:

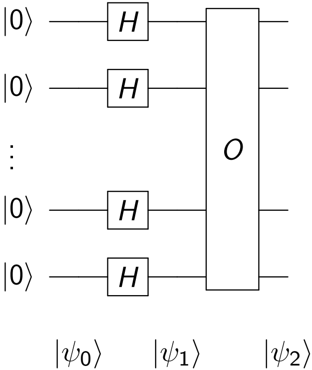
$$O = \begin{array}{c c} & \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{array}{c} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} & \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}. \tag{5}$$

Quantum Oracle

At this point it is important to realize that building quantum oracle for that example has already unveiled for which input the function returns true. However, this is just for presentation purposes and in practice we have a **black-box** quantum oracle that is already given to the algorithm.

Quantum Oracle

Quantum Circuit



Quantum Oracle

We apply quantum oracle to the state in equal superposition

$$
\begin{aligned}
|\psi_2\rangle &= O\,|\psi_1\rangle \\
&= \frac{1}{\sqrt{N}}\left(O\,|00\ldots0\rangle + O\,|00\ldots1\rangle + \cdots + O\,|11\ldots1\rangle\right) \\
&= \frac{1}{\sqrt{N}}\left(|00\ldots0\rangle + |00\ldots1\rangle + \cdots - |10\ldots0\rangle + \cdots + |11\ldots1\rangle\right)
\end{aligned} \tag{6}
$$

Quantum Oracle

Example

Starts in a equal superposition of four states:

$$|\psi_1\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

The oracle picks out string 10:

$$|\psi_2\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

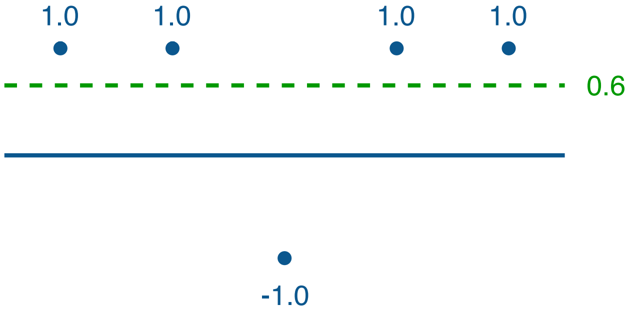
but $|\frac{1}{2}|^2 = |-\frac{1}{2}|^2 = \frac{1}{4}$

Inversion about the mean

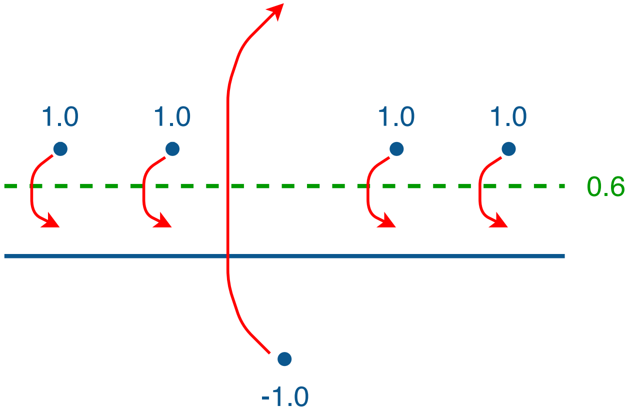
Let's say we start with a vector:

$$\begin{bmatrix} 1 & 1 & -1 & 1 & 1 \end{bmatrix}^T$$

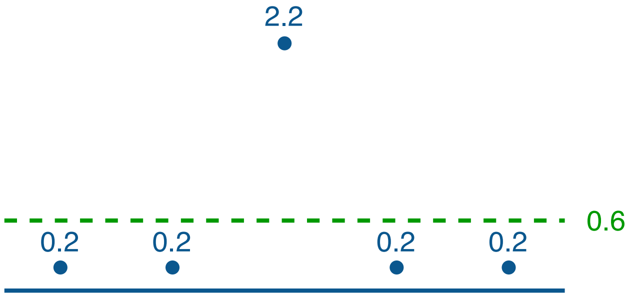
Inversion about the mean



Inversion about the mean



Inversion about the mean



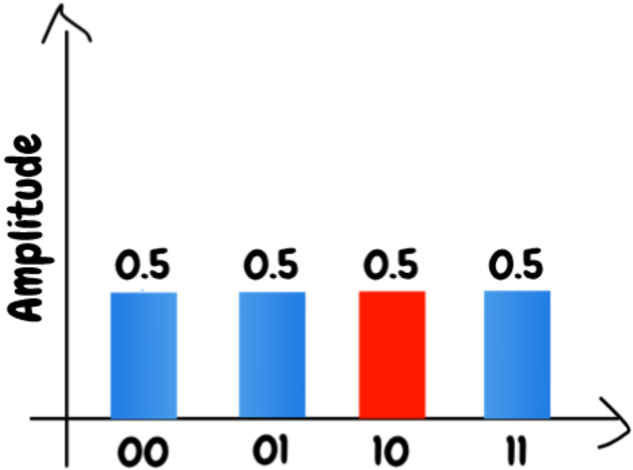
Inversion about the mean

Numeric example for $n = 2$. Picks out string "10".

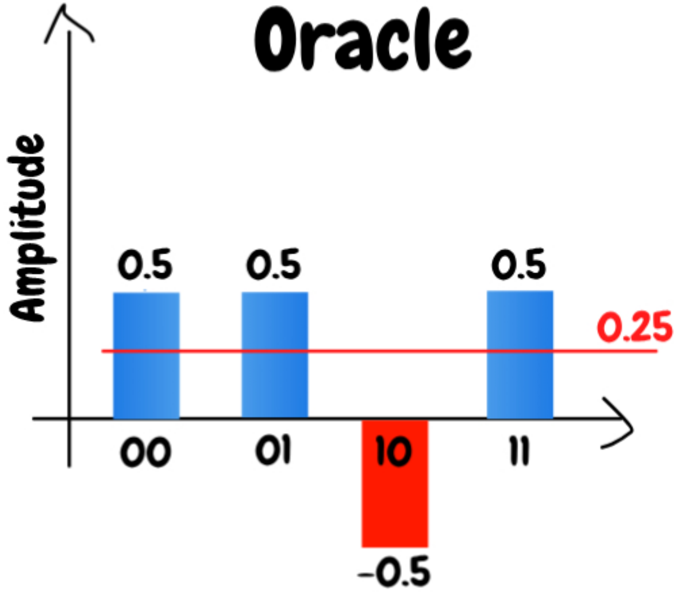
We start with

$$|\psi_1\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$
$$= 0.5\left(\begin{bmatrix}1\\0\\0\\0\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}0\\0\\1\\0\end{bmatrix} + \begin{bmatrix}0\\0\\0\\1\end{bmatrix}\right) = \begin{bmatrix}0.5\\0.5\\0.5\\0.5\end{bmatrix}$$

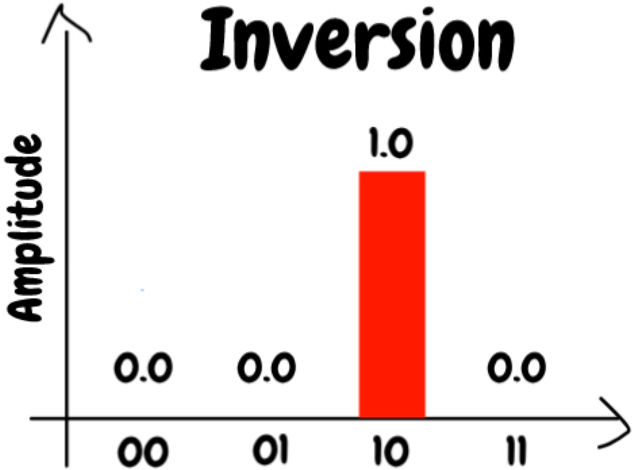
Inversion about the mean



Inversion about the mean



Inversion about the mean



Inversion about the mean

Operator representing inversion of amplitudes around the mean:

$$\mathcal{D} = -I + 2A = \begin{bmatrix} -1 + \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & -1 + \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & -1 + \frac{2}{2^n} \end{bmatrix} \tag{7}$$

Inversion about the mean

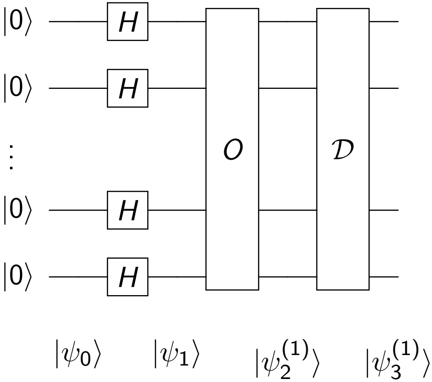
Example for $n = 2$:

$$|\psi_3\rangle = \mathcal{D}\,|\psi_2\rangle =$$

$$= \begin{bmatrix} -0.5 & 0.5 & 0.5 & 0.5 \\ 0.5 & -0.5 & 0.5 & 0.5 \\ 0.5 & 0.5 & -0.5 & 0.5 \\ 0.5 & 0.5 & 0.5 & -0.5 \end{bmatrix} \begin{bmatrix} 0.5 \\ 0.5 \\ -0.5 \\ 0.5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

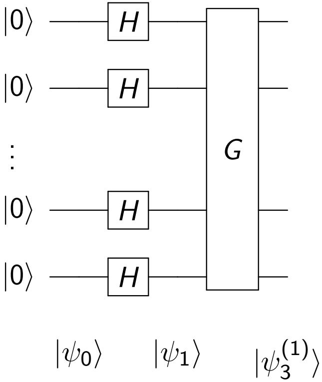
Inversion about the mean

Quantum Circuit



Inversion about the mean

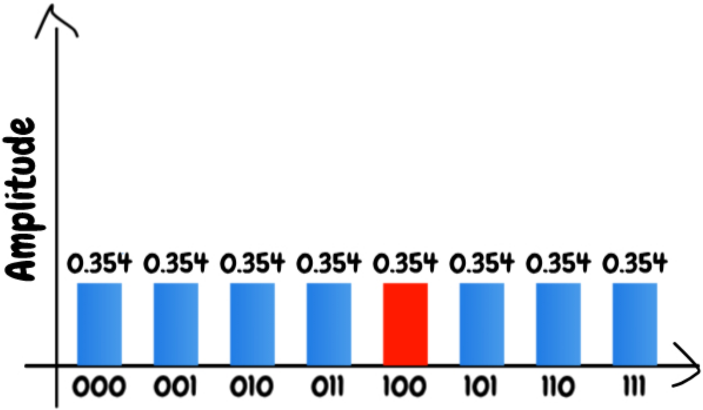
Quantum Circuit



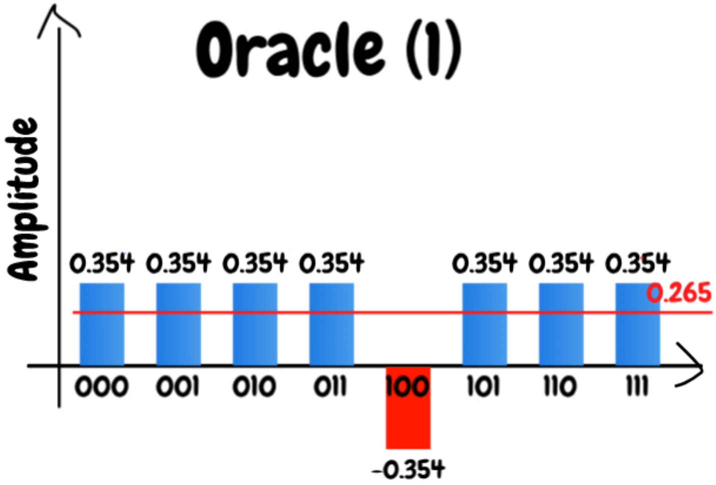
Inversion about the mean

Numeric example for $n = 3$. Picks out string 100.

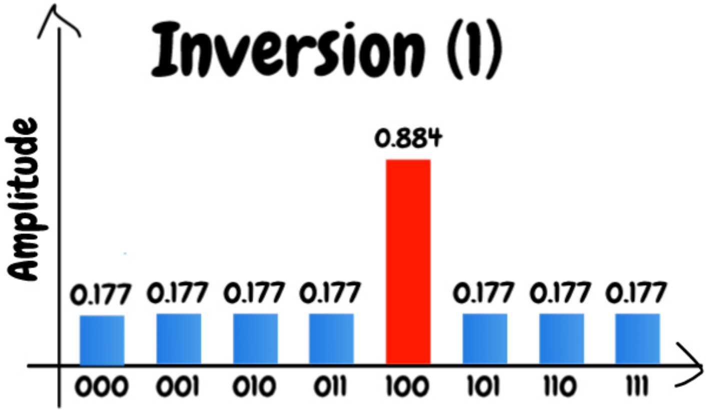
Inversion about the mean



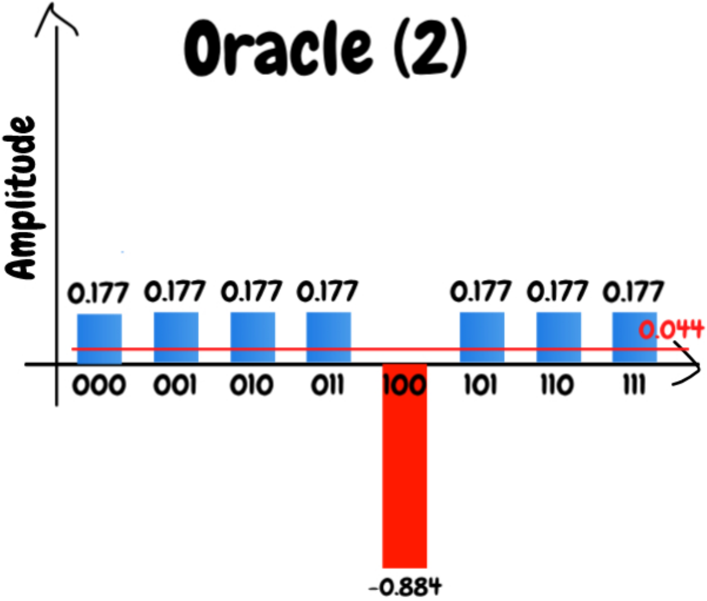
Inversion about the mean



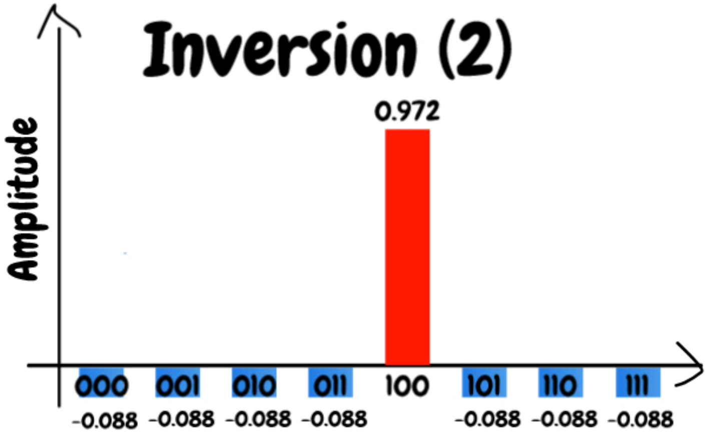
Inversion about the mean



Inversion about the mean

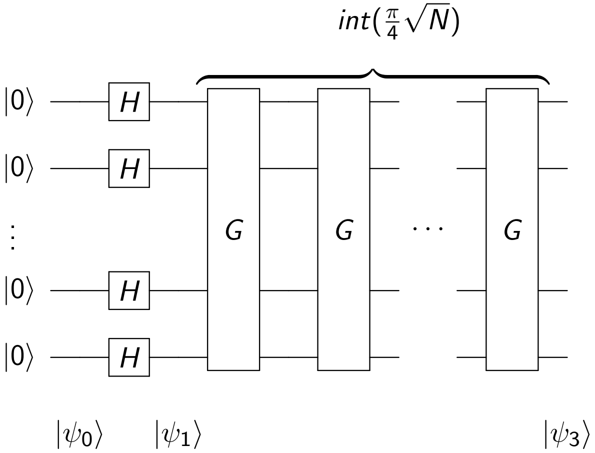


Inversion about the mean



Inversion about the mean

Quantum Circuit



Why $r = int(\frac{\pi}{4}\sqrt{N})$?

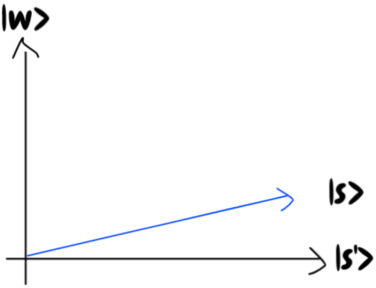
Let's analyze two perpendicular states:

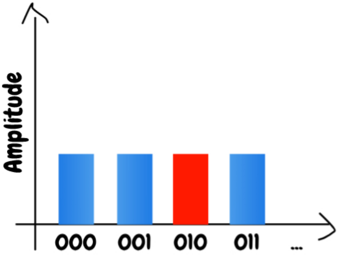
- $|w\rangle$ - solution to the search problem
- $|s'\rangle$ - sum over all states that are not solution

We start with $|\psi_1\rangle = |s\rangle$ state:

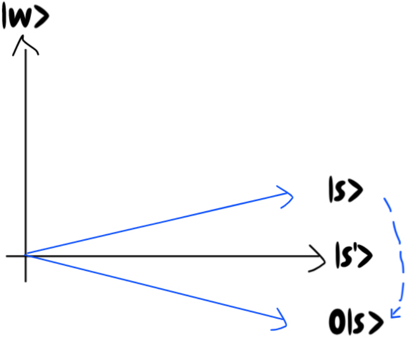
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

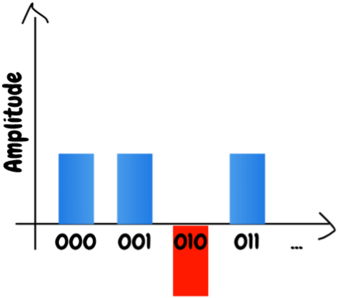
Why $r = int(\frac{\pi}{4}\sqrt{N})$?



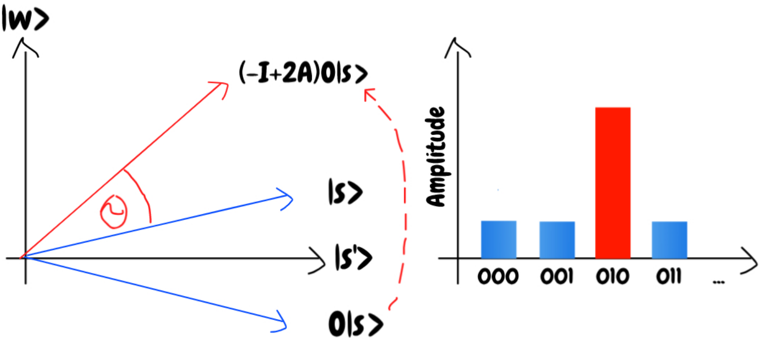


Why $r = int(\frac{\pi}{4}\sqrt{N})$?





Why $r = int(\frac{\pi}{4}\sqrt{N})$?



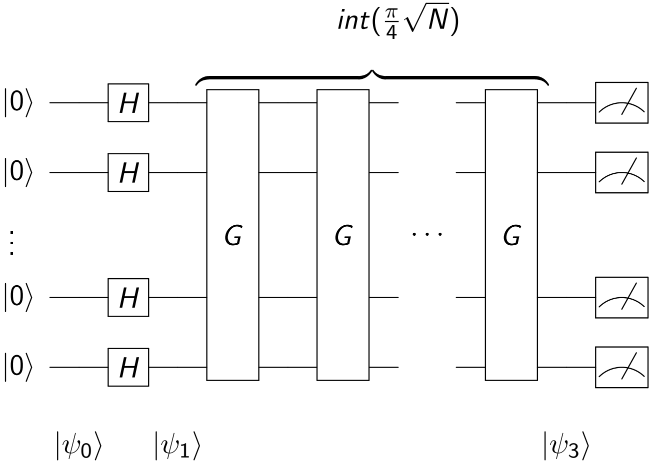
Why $r = int(\frac{\pi}{4}\sqrt{N})$?

$$\theta = 2\arcsin\frac{1}{\sqrt{N}}$$

$$\sin^2\left(\left(r+\frac{1}{2}\right)\theta\right)$$

Measurement

Quantum Circuit



Side Notes

Alternative oracle definition

The definition of oracle action:

$$O|x\rangle = (-1)^{f(x)}|x\rangle$$

is equivalent to:

$$O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$$

for $|q\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

Side Notes

Quantum Parallelism

We can construct an oracle that represents f(x):

$$O\left|x\right\rangle\left|q\right\rangle = \left|x\right\rangle\left|q \oplus f(x)\right\rangle$$

Then, if the first registry is in superposition $\frac{1}{\sqrt{N}}\sum_x \left|x\right\rangle$ and $\left|q\right\rangle = \left|0\right\rangle$, we get:

$$\frac{1}{\sqrt{N}}\sum_x \left|x\right\rangle\left|0\right\rangle \xrightarrow{O} \frac{1}{\sqrt{N}}\sum_x \left|x\right\rangle\left|f(x)\right\rangle$$

Almost as if we have evaluated $f(x)$ for all values of x simultaneously.

Side Notes

Decomposition of Inversion

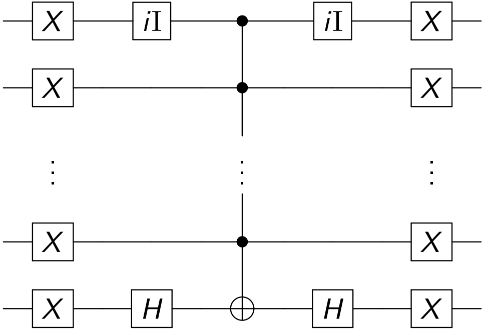


Figure 1: Source: C. Lavor, L.R.U. Manssur, R. Portugal, *Grover's Algorithm: Quantum Database Search*, (2003)

Limitations

- The operation of the algorithm is limited due to **quantum noise** which is a reality in today's quantum computers
- Sensitive to the number of iterations - incorrect selection of this parameter can **overcook the solution**
- Oracle implementation

Let's code

Extensions

- **Quantum Search:** Instead of 1 matching entry, there are k matching entries
- **Quantum Counting:** How many of solutions k?
- **Quantum Minimization:** C. Durr and P. Høyer, *A quantum algorithm for finding the minimum*, (1996).

Further read

- Nielsen, M., Chuang, I. (2010). *Quantum Computation and Quantum Information*
- `https://github.com/dawidkopczyk/training/blob/master/WQCG/grover.ipynb`
- `http://dkopczyk.quantee.co.uk/category/quantum_computing/`
- Rigetti Grove library
- Quantum Approximate Optimization Algorithm (QAOA)