Grover’s algorithm

Raffaele Solcà
Assistant: Dr. Alejandro Daleo

17.03.2008

Contents

1. Introduction

➢ What is Grover's algorithm?

- An Algorithm based on quantum computation.
- It provides a solution of the search problem.

➢ Simple example of the search problem

- We have a phonebook and we are looking for a person who has a specific phone number.
- With a classical algorithm we need $O(N)$ steps to find the person.
- With Grover's algorithm we need only $O(\sqrt{N})$ steps.

1. Introduction

- A quantum computer operates on qubits…
  - State of a qubit: $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$
- … using quantum gates
  - Unitary transformation
  - They are reversible
  - Can act on single or many qubits
- Measurement of qubits
  - The wavefunction collapses in one of the states.

$$|\varphi\rangle = \sum_i \alpha_i |i\rangle \rightarrow |j\rangle \text{ with probability } |\alpha_j|^2$$

1. Introduction

Some gates we will need:

➢ Hadamard Gate

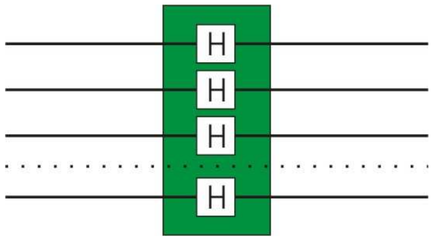
- Generate superposition
- Defined as: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

➢ Walsh-Hadamard Gate

- Generalization of H for many qubits
- Equivalent to apply H on each qubit

$|\gamma_1\rangle \otimes \cdots \otimes |\gamma_n\rangle$

$\gamma_i \in \{0,1\}$



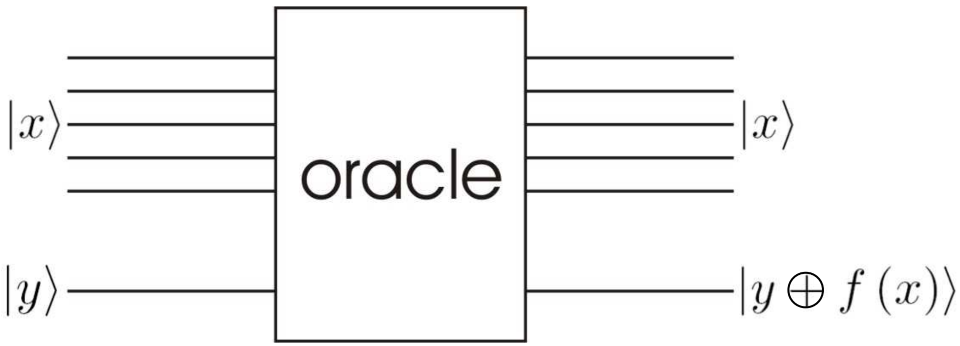
$H|\gamma_1\rangle \otimes \cdots \otimes H|\gamma_n\rangle$

- Matrix : $W_{ij} = \frac{1}{\sqrt{N}}(-1)^{\bar{i}\cdot\bar{j}}$

1. Introduction

➢ Oracle

- Is a quantum mechanical operator.
- It is defined as



- If the second register is initialized with $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$

  it simply swaps the sign of the amplitude of the state with $f(x) = 1$

2. The algorithm

- The abstracted problem
  - Define a function $f : A \to \{0,1\}$
    A is a set with $N = 2^n$ elements
    There is only an element $s \in A$ with $f(s) = 1$
  - We are looking for the element x for which $f(x) = 1$

2. The algorithm

➢ Design of the algorithm

- The steps of the algorithm:
  i. Initialization of first register in the superposition state:
  $$\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \ldots, \frac{1}{\sqrt{N}}\right)$$

  ii. Repeat the following operation $O\left(\sqrt{N}\right)$ times:
     a. Apply the oracle
     b. Apply the diffusion matrix $D_{ij} = -\delta_{ij} + 2\frac{1}{N}$

  iii. Measure the resulting state of first register.

2. The algorithm

- Example with N=4 elements (n=2 qubits), we assume that the solution is the state $|2\rangle = |10\rangle$

  - We will see that we only need to apply step ii. once.

  - We need to know the number of iterations needed because we will see that the probability does not increase monotonically with them.

$$D_{ij} = -\delta_{ij} + 2\frac{1}{N}$$

2. The algorithm

- Apply the steps of Grover's algorithm on the example.

i. Initial state $\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$

ii. a. Application of the oracle $\left(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2}\right)$

ii. b. Application of D

$$-\left(\frac{1}{2},\frac{1}{2},-\frac{1}{2},\frac{1}{2}\right)+2\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4}\right)=(0,0,1,0)$$

iii. Measurement $|2\rangle = |1\,0\rangle$

with probability $p=1$

2. The algorithm

- Analysis of the steps.

   i. Initialization of first register in the superposition state:

$$\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \dots, \frac{1}{\sqrt{N}}\right)$$

   To reach this superposition we can initialize the first register in the state $(1,0,\dots,0)$ and apply the Walsh-Hadamard gate.

- For instance we apply the Walsh-Hadamard gate to the n=2 initialized state $|\psi_0\rangle = |0\,0\rangle$

$$|\psi\rangle = W|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = \frac{1}{2}\sum_{i=0}^{3}|i\rangle$$

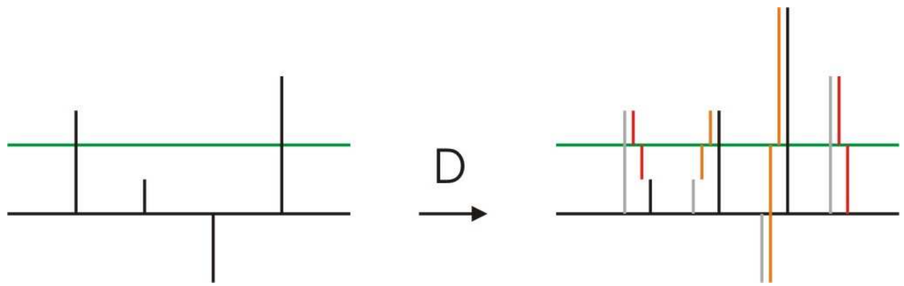
2. The algorithm

- Analysis of the steps.
  - ii. Repeat the following operation $O(\sqrt{N})$ times:
    - a. Apply the oracle
    - b. Apply the diffusion matrix $D_{ij} = -\delta_{ij} + 2\frac{1}{N}$

a. The application of the oracle changes the sign of the amplitude of the component for which $f(x) = 1$

b. We prove that D is unitary

- An example of an application of D



$$D_{ij} = -\delta_{ij} + 2\frac{1}{N}$$

2. The algorithm

Implementation with local transformations

- A local transformation acts on single states.
- We implement the algorithm with local transformations because these transformations can be implemented with elementary quantum gates.

- We prove that D can be represented as a product of local transformations:
  $D = W(R_1 - I)W$
  where
  $R_{1,00} = 2$ and $R_{1,ij} = 0$ for j or $i \neq 0$

- $W, (R_1 - I)$ are local transformations.

We have seen

- The search problem
- A classical solution
- A quantum mechanical solution: Grover's algorithm
  - How it is defined
  - How it works: Example with n=2

We will see

- Geometrical interpretation
  - An application of step ii.
  - The number of iterations we need to find the right answer
- The case with t solution

3. Geometrical interpretation

- Why can we do a simple geometrical representation?
  - All amplitudes are real
  - The amplitudes of the non-searched states are equal

  $\Rightarrow$ We can represent all the states of the algorithm as a linear combination of :
    - the state of the searched element $|s\rangle$
    - the linear combination of the other states

$$|u\rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{i=1 \\ i \neq s}}^{N} |i\rangle$$

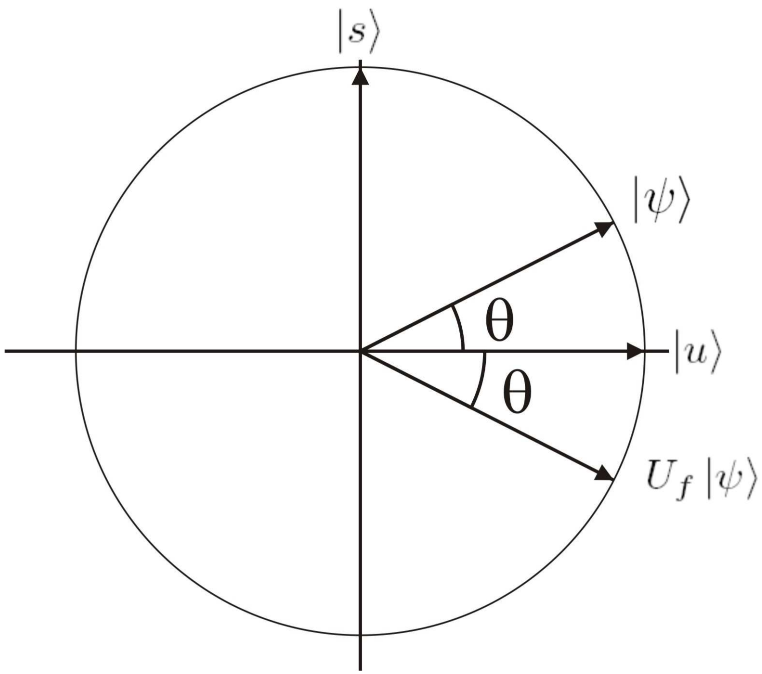
- Why do we make a geometrical representation?
  - Easy understanding of the algorithm
  - Easy determination of the number of steps we have to apply

3. Geometrical interpretation

Observation

- Define θ as $\sin(\theta) = \frac{1}{\sqrt{N}}$

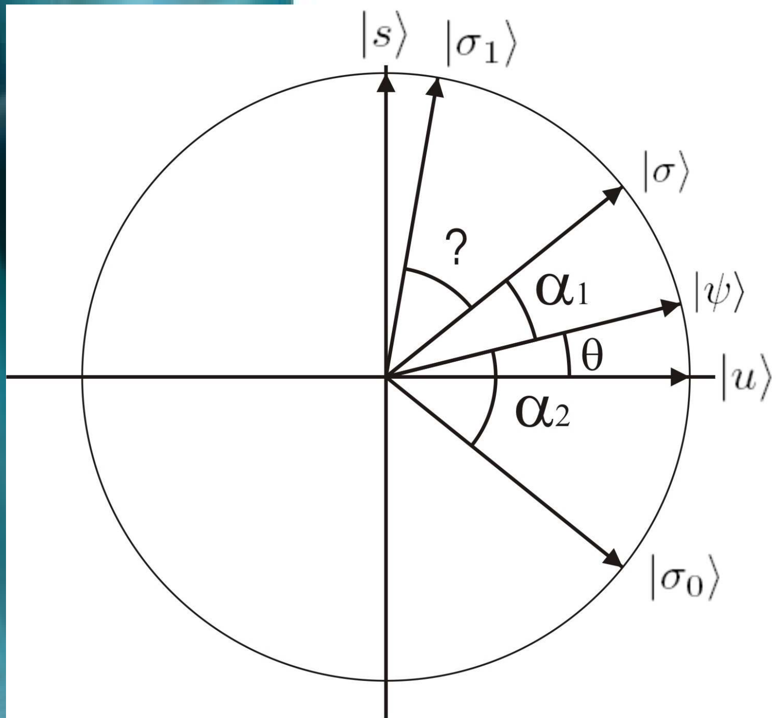
- Observe that the application of the oracle is a reflection around the horizontal axis



$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$$

3. Geometrical interpretation

- Application of step ii. on a generic state as in figure



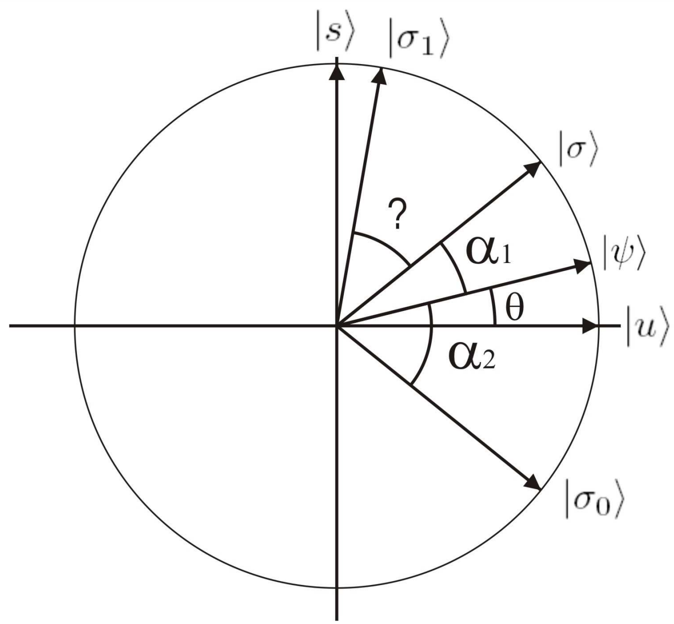
$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle$$

$$\begin{aligned} |\sigma_1\rangle &= D\, U_f\, |\sigma\rangle \\ &= (2\,|\psi\rangle\langle\psi| - I)\, U_f\, |\sigma\rangle \\ &= 2\,\langle\psi|\, U_f\, |\sigma\rangle\, |\psi\rangle - U_f\, |\sigma\rangle \\ &= 2\,\langle\psi\, |\sigma_0\rangle\, |\psi\rangle - |\sigma_0\rangle \\ &= 2\cos\alpha_2\, |\psi\rangle - |\sigma_0\rangle \end{aligned}$$

3. Geometrical interpretation

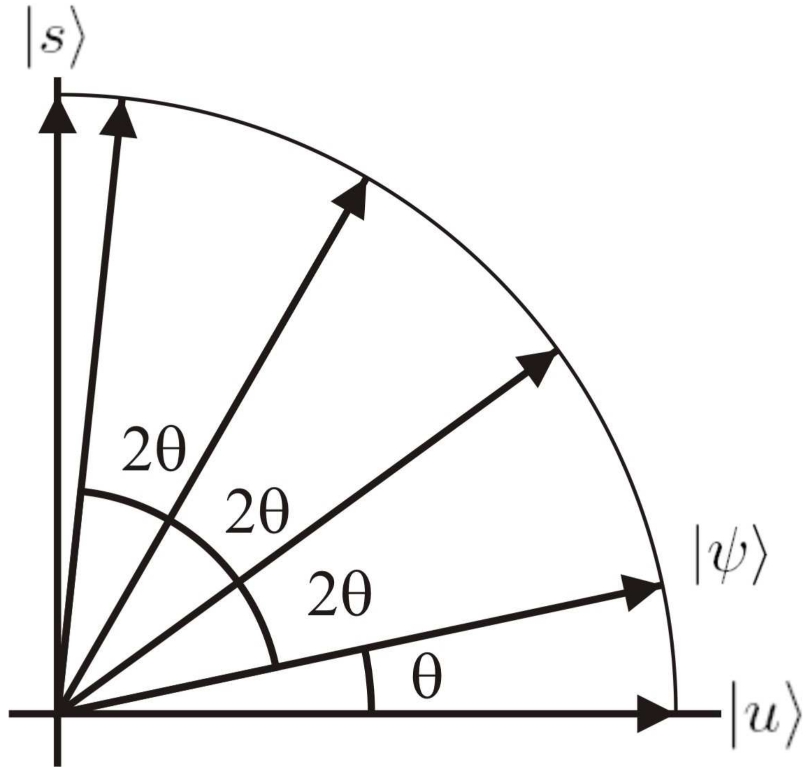
- The angle between the states before and after the application of step ii.:

$$\begin{aligned}\langle\sigma|\sigma_1\rangle &= 2\cos\alpha_2\langle\sigma|\psi\rangle - \langle\sigma|\sigma_0\rangle \\ &= 2\cos\alpha_2\cos\alpha_1 - \cos(\alpha_1+\alpha_2) \\ &= \cos(\alpha_2-\alpha_1) = \cos 2\theta\end{aligned}$$



3. Geometrical interpretation

- Determination of the steps needed to approximate the solution



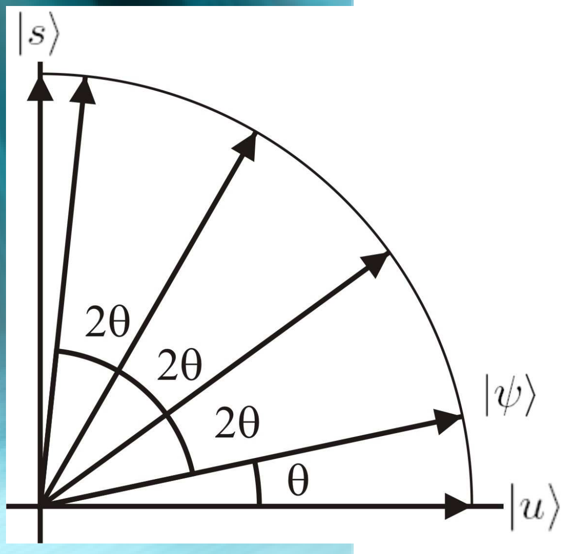
3. Geometrical interpretation

- Determination of the number of applications of step ii.

  - After m applications of step ii. we have the state
    $|\psi_m\rangle = \sin((2m+1)\theta)|s\rangle + \cos((2m+1)\theta)|u\rangle$

  - The probability of finding the searched state is
    $p_s = \sin^2((2m+1)\theta)$

  - If we want to have a probability of about 1 we have to choose
    $$(2m+1)\theta \approx \frac{\pi}{2} \quad \Leftrightarrow \quad m \approx \frac{\pi}{4\theta} - \frac{1}{2}$$
    Clearly we need an integer number of iterations m
    $$\Rightarrow \quad m \approx \left\lfloor \frac{\pi}{4\theta} \right\rfloor$$



3. Geometrical interpretation

- For small θ (big N) $\left(\theta \approx \sin\theta = \frac{1}{\sqrt{N}}\right)$

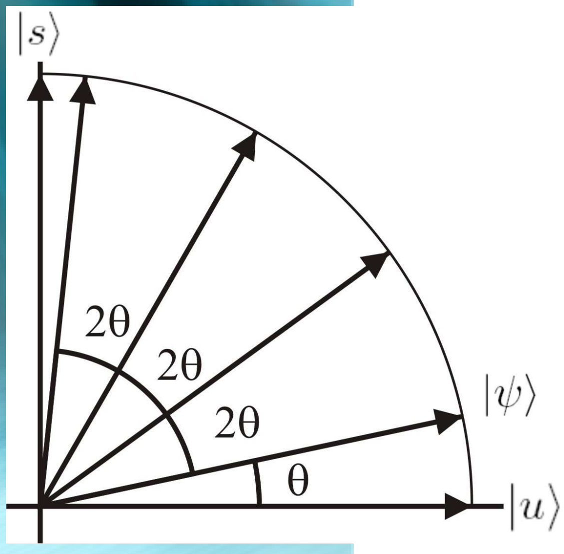
  - We can approximate $m \approx \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$

- Probability of failure

  - The probability of failure is given by

$$p_u = \cos^2\left((2m+1)\theta\right)$$

$$= \sin^2\left(\frac{\pi}{2} - (2m+1)\theta\right) < \sin^2\theta = \frac{1}{N}$$

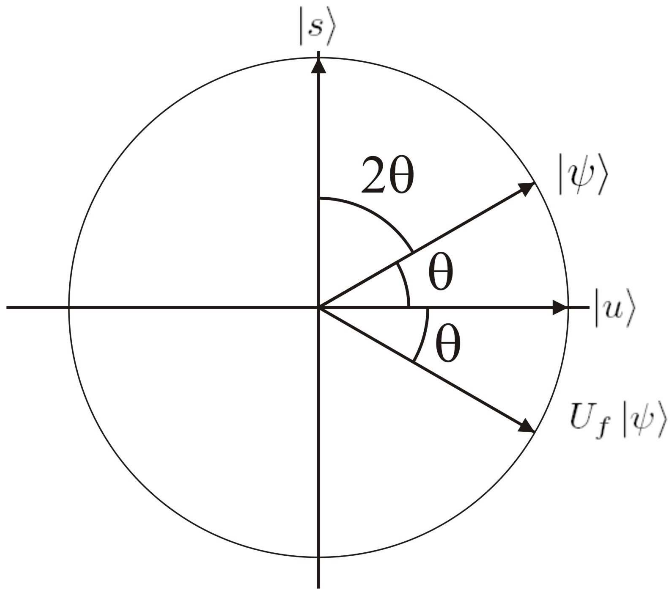


3. Geometrical interpretation

➢ Example with n=2

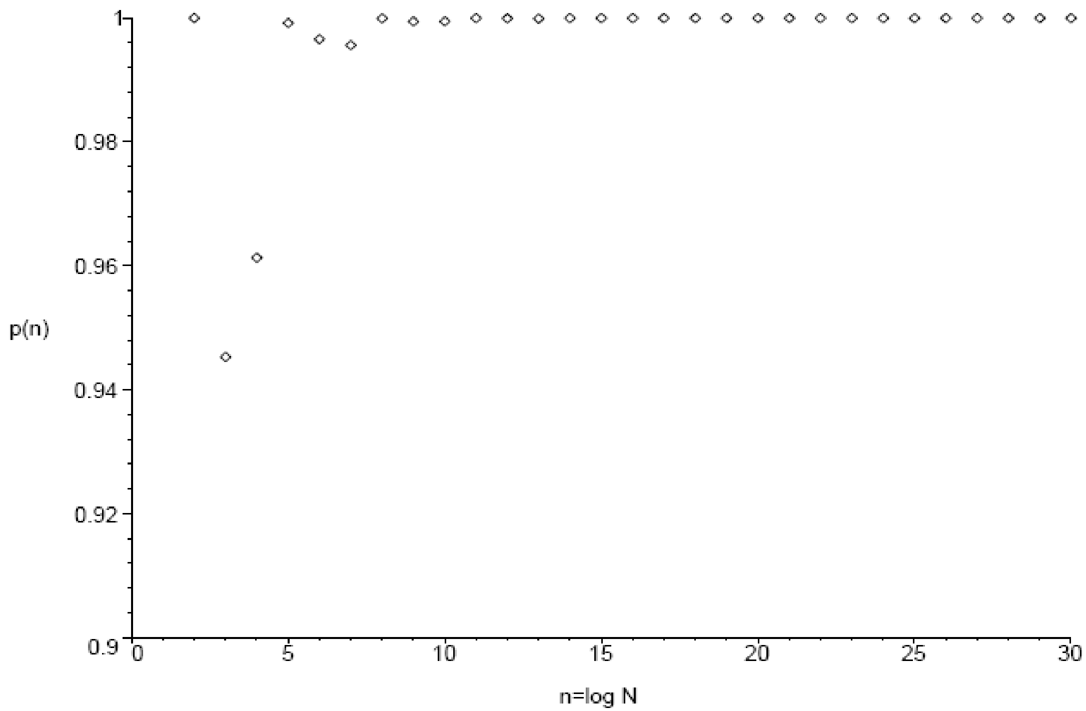
- By definition: $\sin(\theta)=\frac{1}{2} \Rightarrow \theta = 30°$

$\Rightarrow$ Only one application



3. Geometrical interpretation

- Probability of success as a function of n after $m = \left\lfloor \frac{\pi}{4\theta} \right\rfloor$ applications of step ii.



4. The case with t solutions

➢ Analyze the problem with t solutions

- We define: $\sin(\theta) = \frac{\sqrt{t}}{\sqrt{N}}$

$$|u\rangle = \sum_{f(i)=0} \frac{1}{\sqrt{N-t}} |i\rangle \qquad |s\rangle = \sum_{f(i)=1} \frac{1}{\sqrt{t}} |i\rangle$$

- After m applications of step ii. we have the state

$$|\psi_m\rangle = \sin((2m+1)\theta)|s\rangle + \cos((2m+1)\theta)|u\rangle$$

- As for one solution we need $m = \left\lfloor \frac{\pi}{4\theta} \right\rfloor$ steps

  with a probability of failure

$$p_u < \sin^2 \theta = \frac{t}{N}$$

Summary

- The search problem
  - The classical solution
  - A quantum mechanical solution: Grover's algorithm
- Grover's algorithm
  - How it is defined
  - How it works: Example with n=2
- Geometrical interpretation
  - The effect of the application of step ii.
  - How many step we have to apply
  - What is the probability of failure / of finding the correct answer
- The case with t solutions
  - Drawback: in order to have high probability of success we have to know the number t of solutions and t << N.