Quantum searching in unsorted database: Grover's algorithm

Katalin Friedl

Dept. of Computer Science and Information Theory

BME

MŰEGYETEM 1782

November 21, 2019

Search problem

Basic version

Given elements $a_0, a_2, \ldots, a_{N-1}$ and b — find a k s.t. $a_k = b$

General version

Given $f : \{0, \ldots, N-1\} \to \{0, 1\}$ — find k s.t. $f(k) = 1$

Here f is given by **black box**:

$$x \longrightarrow \boxed{\;f\;} \longrightarrow f(x)$$

Goal

Minimize the number of queries

Deterministic algorithm

Number of queries

- worst case: N
- average case: $\approx N/2$

Goal

Minimize the number of queries

Deterministic algorithm

Number of queries

- worst case: N
- average case: $\approx N/2$

Probabilistic algorithm

Number of queries

- for success prob. 0.1: $\approx N/10$

Quantum search

Also called as **Grover's Search**

Quantum search

Also called as **Grover's Search**

Quantum search

Also called as **Grover's Search**

Lov K. Grover, 1996

Quantum search in $O(\sqrt{N})$ queries

finds a solution with large probability

needs a **quantum box**

Quantum search

Also called as **Grover's Search**

Lov K. Grover, 1996
Quantum search in $O(\sqrt{N})$ queries
finds a solution with large probability

needs a **quantum box**

$$\sum_x \alpha_x \, |x\rangle \longrightarrow \boxed{f} \longrightarrow \sum_x (-\mathbf{1})^{\mathbf{f(x)}} \alpha_x \, |x\rangle$$

Quantum search

Also called as **Grover's Search**

Lov K. Grover, 1996
Quantum search in $O(\sqrt{N})$ queries
finds a solution with large probability

needs a **quantum box**

$$\sum_x \alpha_x \, |x\rangle \longrightarrow \boxed{f} \longrightarrow \sum_x (-\mathbf{1})^{\mathbf{f(x)}} \alpha_x \, |x\rangle$$

Number of queries for N elements, t solutions: $O\left(\sqrt{\frac{N}{t}}\right)$

Applications

In any algorithm which uses search

- search in a huge database

Applications

In any algorithm which uses search

- search in a huge database
- break passwords

Applications

In any algorithm which uses search

- search in a huge database
- break passwords
- graph algorithms
  – graph traversals

    idea: looking for an unvisited neighbor is a search problem — use Grover's algorithm

    BFS, DFS : classical $O(N^2) \longrightarrow$ quantum $O(N^{3/2})$

  – shortest path : classical $O(N^2) \longrightarrow$ quantum $\tilde{O}(N^{3/2})$

Views

One algorithm – different views

Views

One algorithm – different views

- geometric – intuition
- algebraic – generalized tool
- quantum algorithm

Views

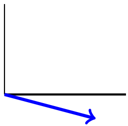
One algorithm – different views

- geometric – intuition
- algebraic – generalized tool
- quantum algorithm

Now assume: **exactly one** solution ($t = 1$)

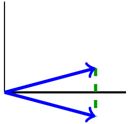
Geometry

Flipping the sign of one component — reflection



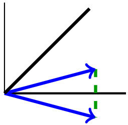
Geometry

Flipping the sign of one component — reflection



Geometry

Flipping the sign of one component — reflection

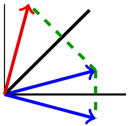


two reflections=one rotation by 2α
(α is the angle of the two vectors)

Geometry

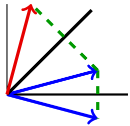
Flipping the sign of one component — reflection

two reflections=one rotation by 2α
(α is the angle of the two vectors)



Geometry

Flipping the sign of one component — reflection



two reflections=one rotation by 2α
(α is the angle of the two vectors)

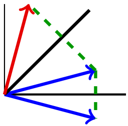
For larger dimensions

Reflection R to $v^\perp$, the hyperplane orthogonal to v:

$$Rv = -v, \quad Rw = w \text{ if } w \perp v$$

Geometry

Flipping the sign of one component — reflection



two reflections=one rotation by 2α (α is the angle of the two vectors)

For larger dimensions

Reflection R to $v^\perp$, the hyperplane orthogonal to v:

$$Rv = -v, \quad Rw = w \text{ if } w \perp v$$

U unitary $\Longrightarrow URU^{-1}$ is a reflection to $(Uv)^\perp$

$URU^{-1}(Uv) = -Uv,\ URU^{-1}(Uw) = Uw$ if $w \perp v$, i.e., $Uw \perp Uv$

Grover's idea

Setup

N elements $\longrightarrow$ N dimensional space
elements $\longrightarrow$ orthogonal basis
$a_x \mapsto |x\rangle$

Given: quantum box for f — reflection R to $|k\rangle^\perp$
(k is the only solution of $f(x) = 1$)

Goal: determine k — find the corresponding basis vector $|k\rangle$

Need: $N = 2^n$

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^{\perp}$

easy (conditional phase shift)

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^\perp$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$

(H is the Hadamard operator, $H = H^{-1}$)

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^\perp$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$
(H is the Hadamard operator, $H = H^{-1}$)

Use R_uR several times — rotations by angle 2α

Grover's idea

What to do

Construct R_0, the reflection to $|0\rangle^\perp$

easy (conditional phase shift)

Use Hadamard to obtain $R_u = HR_0H^{-1} = HR_0H$

(H is the Hadamard operator, $H = H^{-1}$)

Use R_uR several times — rotations by angle 2α

Stop when target $|k\rangle$ is close

Angle

Angle of rotations $= 2\alpha$

$\alpha =$ angle of the vectors $|k\rangle$ and $H|0\rangle$,

$H|0\rangle = N^{-1/2}\sum_x |x\rangle$

α can be computed by **inner product**

This is $N^{-1/2} = \cos\alpha$ (unit vectors)

So for large N $\alpha \approx \pi/2$, $2\alpha \approx \pi$ **too large**

Reducing the angle

2D

Replacing R_u by $-R_u$ gives reflection to the orthogonal direction

the **new angle** is $\alpha' = \pi/2 - \alpha$

then $\cos\alpha = \sin\alpha' = N^{-1/2}$

so, $\alpha' \approx N^{-1/2}$ for large N

angle of rotation: $2\alpha' \approx \frac{2}{\sqrt{N}}$

Reducing the angle

2D

Replacing R_u by $-R_u$ gives reflection to the orthogonal direction

the **new angle** is $\alpha' = \pi/2 - \alpha$

then $\cos\alpha = \sin\alpha' = N^{-1/2}$

so, $\alpha' \approx N^{-1/2}$ for large N

angle of rotation: $2\alpha' \approx \dfrac{2}{\sqrt{N}}$

Grover operator

$$G = -R_u R = H(-R_0)HR$$

Algorithm

- Start with basis vector $|0\rangle$
- Apply H
- Apply $\left\lceil \dfrac{\pi/2}{2\alpha'} \right\rceil$ times the Grover operator $G = H(-R_0)HR$
- Measure

Here

$N = 2^n$

$H_2 = \dfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $H = H_2^{\otimes n}$

$(-R_0) =$ conditional phase shift: $|x\rangle \mapsto \begin{cases} |x\rangle & \text{if } x = 0 \\ -|x\rangle & \text{if } x \neq 0 \end{cases}$

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

The result can be checked —

and if it is not a solution then repeat the process

Repeating several times increases the success probability.

Result

Theorem

The vector obtained at the end is the (unique) solution $|k\rangle$ with constant probability.

The number of queries is $\left\lceil \frac{\pi}{4}\sqrt{N} \right\rceil$.

The result can be checked —

and if it is not a solution then repeat the process

Repeating several times increases the success probability.

Careful only a few further step does not necessarily improve the approximation!

Remarks

Looking the geometry in 2D is not cheating:

- Interesting things happen only in the span of $|k\rangle$ and $H|0\rangle$
- Vectors in the orthogonal subspace are fixed (or the signs are changed)

When there are $t > 1$ solutions

- if t is known
$$\frac{1}{\sqrt{t}} \sum_{f(k)=1} |k\rangle \quad \text{replaces} \quad |k\rangle$$
angle of rotation $\approx 2\sqrt{t/N}$
number of queries $O(\sqrt{N/t})$
- if t is unknown
similarly to binary search or
random number of iterations works (with large probability)

Algebraic view

$R_0 = I - 2P_0$, where P_0 is a **projection** to $|0\rangle$

$HR_0H = I - 2P$, where P is a **projection** to $H|0\rangle = \sum_x |x\rangle$

In matrix form

$$HR_0H = \begin{pmatrix} 1-\frac{2}{N} & -\frac{2}{N} & \cdots & -\frac{2}{N} \\ -\frac{2}{N} & 1-\frac{2}{N} & \cdots & -\frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ -\frac{2}{N} & -\frac{2}{N} & \cdots & 1-\frac{2}{N} \end{pmatrix}$$

Algebraic view

The action of $H(-R_0)H$ on a vector is

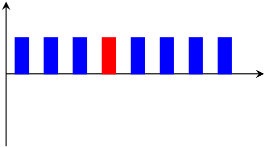
$$\sum_x \alpha_x |x\rangle \mapsto \sum_x (2A - \alpha_x) |x\rangle$$

where A is the average $A = \dfrac{\sum_x \alpha_x}{N}$

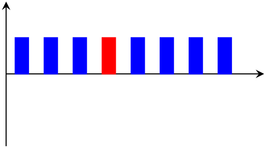
Transformation of coordinates: $\alpha_x \mapsto 2A - \alpha_x = A + (A - \alpha_x)$ is

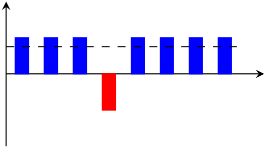
inversion about average

Amplitude amplification

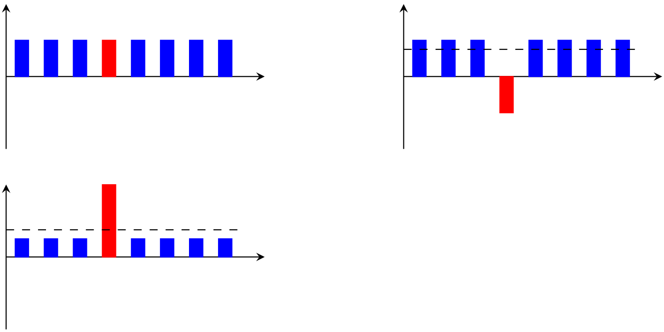


Amplitude amplification

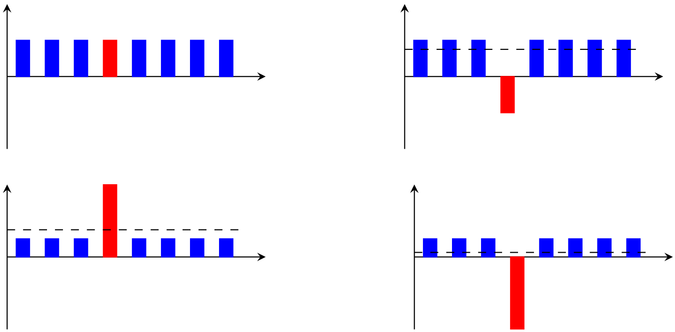




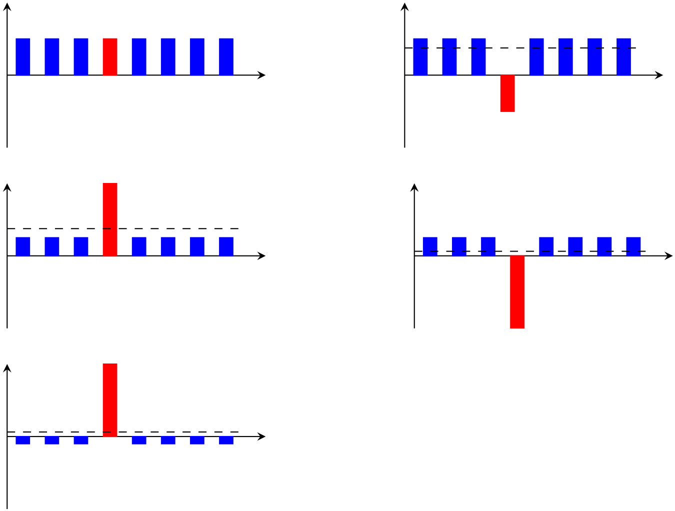
Amplitude amplification



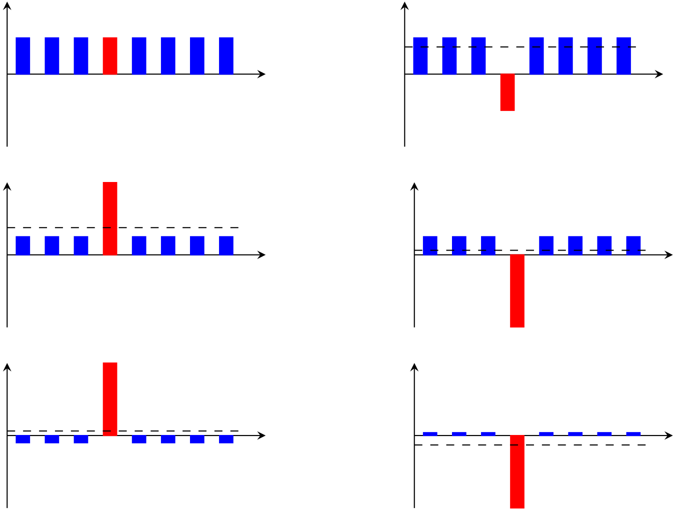
Amplitude amplification



Amplitude amplification

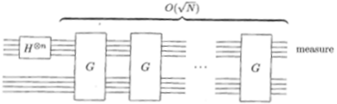


Amplitude amplification

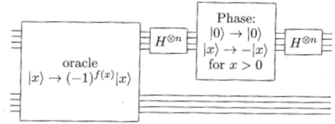


Circuit

Schematic circuit



Grover operation



Related problems

Smallest, largest elements

Grover's algorithm can be used $\quad O(\sqrt{N})$ queries

Approximate counting

Grover's algorithm + phase estimation

Ordered search

Very different — Grover does not help

classical: $\log n$ queries

Related problems

Smallest, largest elements

Grover's algorithm can be used $O(\sqrt{N})$ queries

Approximate counting

Grover's algorithm + phase estimation

Ordered search

Very different — Grover does not help

classical: $\log n$ queries

quantum **algorithm** $\approx 0.4 \log n$ (Child, Landahl, Parillo 2006)

quantum **lower bound** $\approx 0.22 \log n$ (Høyer, Neerbek, Shi 2001)

Summary

For unordered search among N elements
– classical algorithms need N queries
– quantum search needs only $O(\sqrt{N})$

Grover's algorithm is optimal (Bennett, Bernstein, Brassard, Vazirani, 1997)

Can speed up algorithms containing some search

Requires quantum box (quantum oracle) – not always easy to make