Quantum Search

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Table of Contents

Grover's Problem

The Problem

Take a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$

There exists one $x \in \{0, 1\}^n$ such that $f(x) = 1$

Discover the x

Classically, need to evaluate f 2^n times in the worst case

Grover's Problem

The Problem

Take a function $f : \{0,1\}^n \to \{0,1\}$

There exists one $x \in \{0,1\}^n$ such that $f(x) = 1$

Discover the x

Classically, need to evaluate f 2^n times in the worst case

Grover's Problem

The Problem

Take a function $f : \{0,1\}^n \to \{0,1\}$

There exists one $x \in \{0,1\}^n$ such that $f(x) = 1$

Discover the x

Classically, need to evaluate f 2^n times in the worst case

Quantumly, need to evaluate f around $\sqrt{2^n}$ times

Applications

Grover's problem occurs in a multitude of scenarios

- Searching through unstructured databases
- Finding passwords
- Route planning
- Solving SAT problems
- NP-problems in general

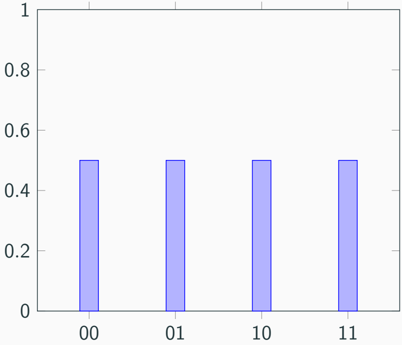
Key Ideas

Like in all previous quantum algorithms, we will rely on

1. superposition
2. interference (to decrease amplitude of wrong answers and increase amplitude of the right ones)

Key Ideas: Superposition

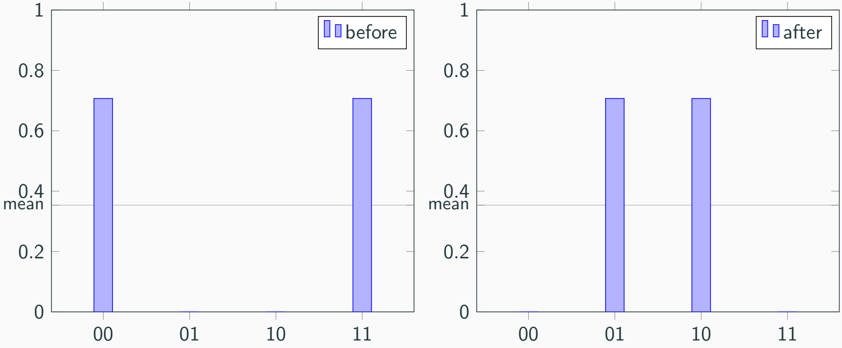
Take $f : \{0,1\}^2 \to \{0,1\}$ with $f(10) = 1$



$$\frac{1}{2}\Big(|00\rangle + |01\rangle + |10\rangle + |11\rangle \Big)$$

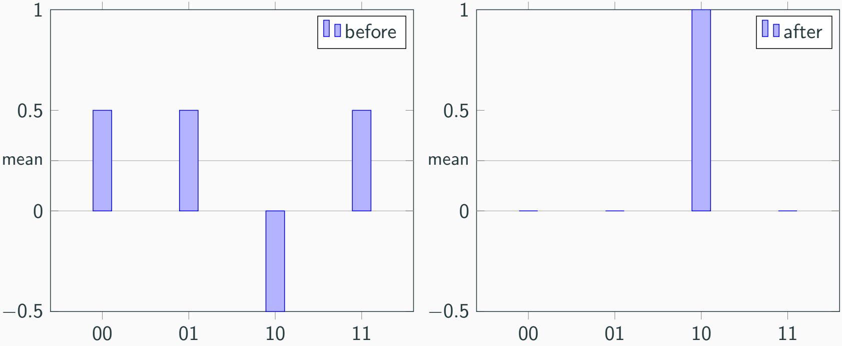
Key Ideas: Interference pt. I

Inversion about the mean: $(x \mapsto (-x + \mathit{mean}) + \mathit{mean})$



Intuitively mass of some states was given to others

Mind the following particular case of inversion about the mean



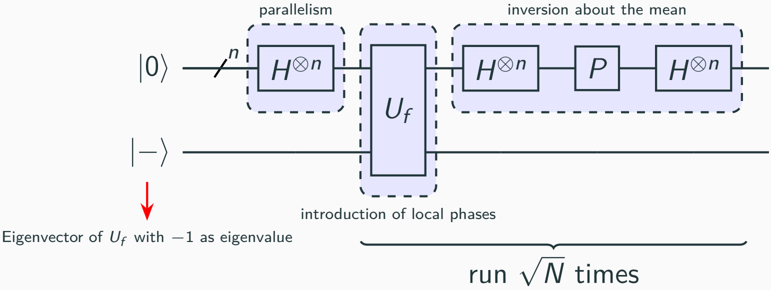
Intuitively, mass of wrong answers was given to the right one

Table of Contents

The Steps

1. Put all possible answers in uniform superposition
2. Negate phases of the right answer
3. Invert about the mean
4. Repeat steps 2 and 3 until ensured we will measure the right answer with high probability ($\approx \sqrt{2^n}$ times)

The Circuit



N.B. It is often convenient to omit the bottom qubit

Adding Local Phases

Recall from last lectures the notion of phase kickback and that

$$U_f \left|x\right\rangle \left|-\right\rangle = (-1)^{f(x)} \left|x\right\rangle \left|-\right\rangle$$

In particular, if x is as solution of f we obtain a phase flip

$$U_f \left|x\right\rangle \left|-\right\rangle = (-1) \left|x\right\rangle \left|-\right\rangle$$

Inversion About the Mean pt. I

We start with the operation that phase flips basis states different from $|0\rangle$, *i.e.*

$$P = 2\,|0\rangle\,\langle 0| - I$$

Then we calculate

$$\begin{aligned}
&H^{\otimes n}(2\,|0\rangle\,\langle 0| - I)H^{\otimes n} \\
&= (H^{\otimes n}(2\,|0\rangle\,\langle 0|) - H^{\otimes n})H^{\otimes n} \\
&= H^{\otimes n}(2\,|0\rangle\,\langle 0|)H^{\otimes n} - H^{\otimes n}H^{\otimes n} \\
&= 2H^{\otimes n}\,|0\rangle\,\langle 0|\,H^{\otimes n} - I
\end{aligned}$$

Denoting $H^{\otimes n}\,|0\rangle$ by $|\psi\rangle$ we obtain,

$$2\,|\psi\rangle\,\langle\psi| - I$$

Inversion About the Mean pt. II

1. Prove that $|\psi\rangle\langle\psi| = \frac{1}{N}\sum_{x,y\in N}|x\rangle\langle y|$ with $N = 2^n$
2. Prove that $2|\psi\rangle\langle\psi| - I$ is the desired inversion about the mean

Inversion About the Mean pt. III

$$\left(2\tfrac{1}{N}\textstyle\sum_{x,y\in N}|x\rangle\langle y| - I\right)\textstyle\sum_{k\in N}\alpha_k|k\rangle$$

$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}|x\rangle\langle y|\left(\textstyle\sum_{k\in N}\alpha_k|k\rangle\right) - \textstyle\sum_k \alpha_k|k\rangle$$

$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}\left(\textstyle\sum_{k\in N}\alpha_k\langle y,k\rangle|x\rangle\right) - \textstyle\sum_k \alpha_k|k\rangle$$

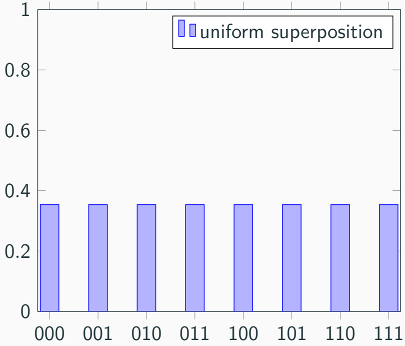
$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}\alpha_y|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$

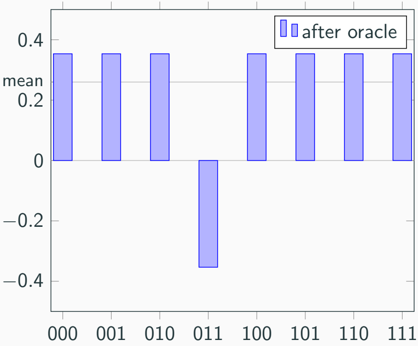
$$= 2\underbrace{\frac{1}{N}\sum_{y\in N}\alpha_y}_{\text{mean - }\alpha}\textstyle\sum_{x\in N}|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$

$$= \textstyle\sum_{x\in N}2\alpha|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$

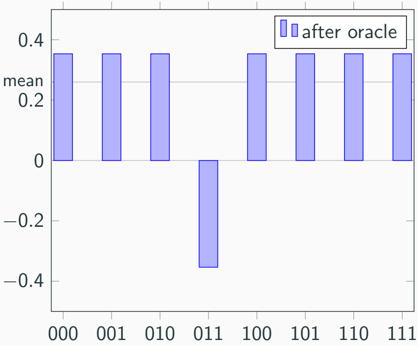
$$= \textstyle\sum_{k\in N}(-\alpha_k + 2\alpha)|k\rangle$$

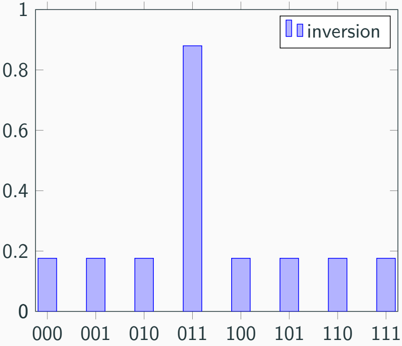
Example: $N = 2^3 = 8, w = 011$



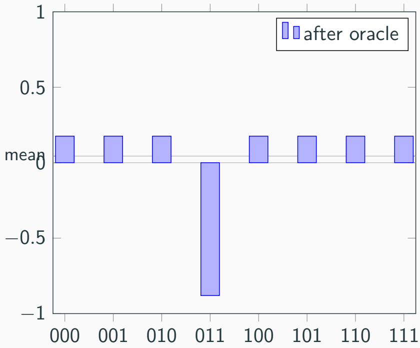


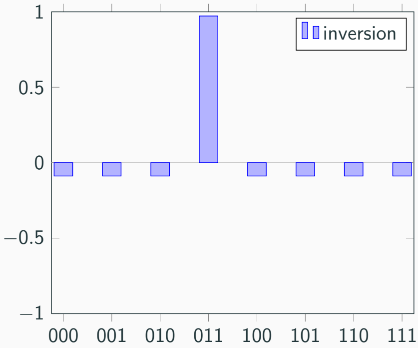
Example: $N = 2^3 = 8, w = 011$





Example: $N = 2^3 = 8, w = 011$





At the end probability of measuring 011 is $\approx 94.5\%$

Table of Contents

Setting the Stage pt. I

In order to further analyse Grover's algorithm, it is useful to take a 2-dimensional geometrical perspective

Setting the Stage pt. I

In order to further analyse Grover's algorithm, it is useful to take a 2-dimensional geometrical perspective

Take the vectors $|w\rangle$ and $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$. We obtain a 2-dimensional vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Setting the Stage pt. I

In order to further analyse Grover's algorithm, it is useful to take a 2-dimensional geometrical perspective

Take the vectors $|w\rangle$ and $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$. We obtain a 2-dimensional vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Additionally, the uniform superposition $|\psi\rangle$ can be rewritten as

$$\frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle$$

Setting the Stage pt. I

In order to further analyse Grover's algorithm, it is useful to take a 2-dimensional geometrical perspective

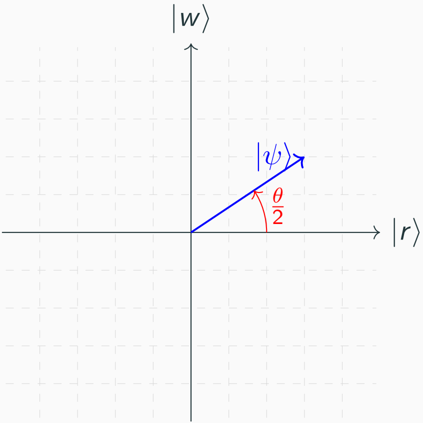
Take the vectors $|w\rangle$ and $|r\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$. We obtain a 2-dimensional vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Additionally, the uniform superposition $|\psi\rangle$ can be rewritten as

$$\frac{1}{\sqrt{N}} |w\rangle + \sqrt{\frac{N-1}{N}} |r\rangle$$

This gives . . .

Setting the Stage pt. II



where $\sin(\frac{\theta}{2}) = \frac{1}{\sqrt{N}}$. Our goal is to rotate the vector to become as close as possible to $|w\rangle$