Quantum Search

Renato Neves

Universidade do Minho

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY

Table of Contents

Grover's Problem

The Problem

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

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

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

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

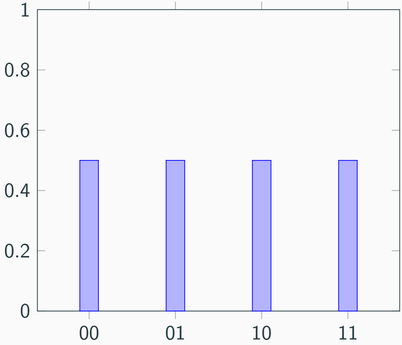
Key Ideas

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

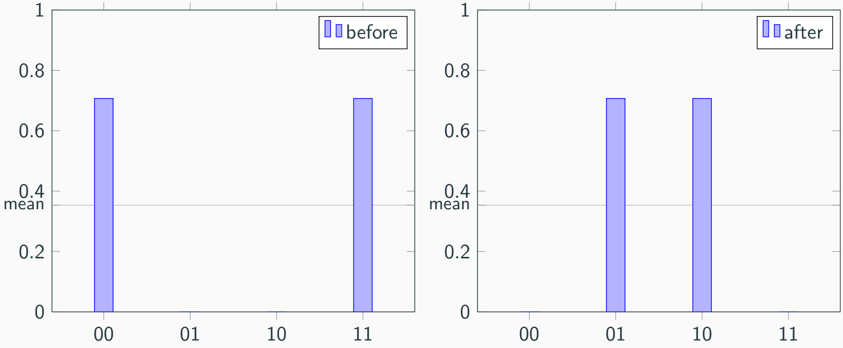
Take $f : \{0,1\}^2 \to \{0,1\}$ with $f(10) = 1$



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

Key Ideas: Interference pt. I

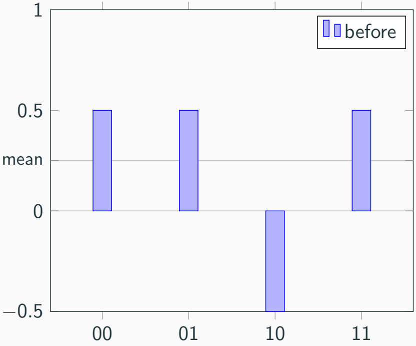
Inversion about the mean: $(x \mapsto (-x + mean) + mean)$

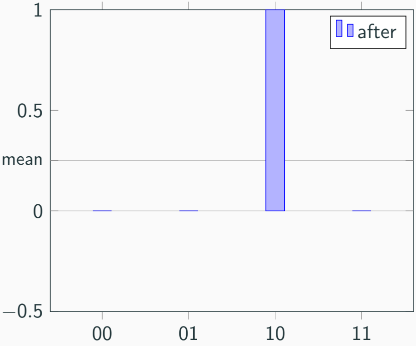


Intuitively mass of some states was given to others

Key Ideas: Interference pt. II

Mind the following particular case of inversion about the mean





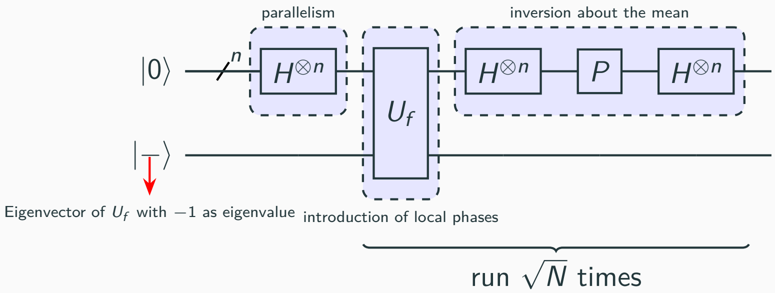
Intuitively, mass of wrong answers was given to the right one

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,

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

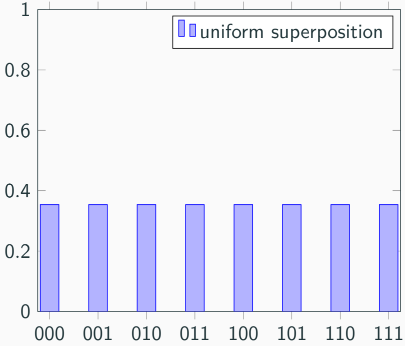
Inversion About the Mean pt. II

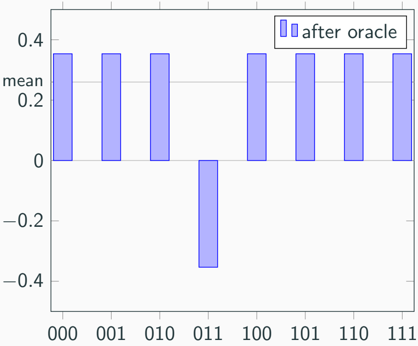
1. Prove that $|\psi\rangle\langle\psi| = \frac{1}{N}\sum_{x,y\in N} |x\rangle\langle y|$ with $N = 2^n$
2. Prove that $2|\psi\rangle\langle\psi| - I$ is the desired inversion about the mean

Inversion About the Mean pt. III

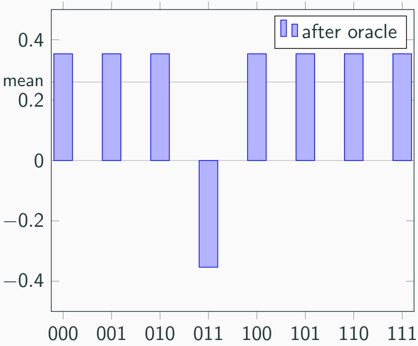
$$\left(2\tfrac{1}{N}\textstyle\sum_{x,y\in N}|x\rangle\langle y| - I\right)\textstyle\sum_{k\in N}\alpha_k|k\rangle$$
$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}|x\rangle\langle y|\left(\textstyle\sum_{k\in N}\alpha_k|k\rangle\right) - \textstyle\sum_k \alpha_k|k\rangle$$
$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}\left(\textstyle\sum_{k\in N}\alpha_k\langle y,k\rangle|x\rangle\right) - \textstyle\sum_k \alpha_k|k\rangle$$
$$= 2\tfrac{1}{N}\textstyle\sum_{x,y\in N}\alpha_y|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$
$$= \underbrace{2\,\frac{1}{N}\sum_{y\in N}\alpha_y}_{\text{mean - }\alpha}\textstyle\sum_{x\in N}|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$
$$= \textstyle\sum_{x\in N} 2\alpha\,|x\rangle - \textstyle\sum_k \alpha_k|k\rangle$$
$$= \textstyle\sum_{k\in N}(-\alpha_k + 2\alpha)\,|k\rangle$$

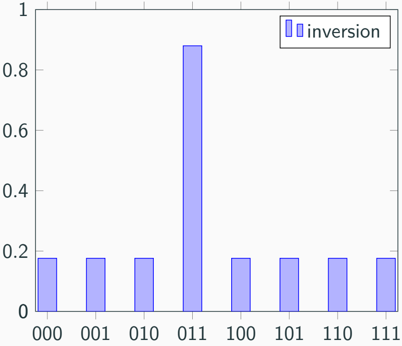
Example: $N = 2^3 = 8, w = 011$



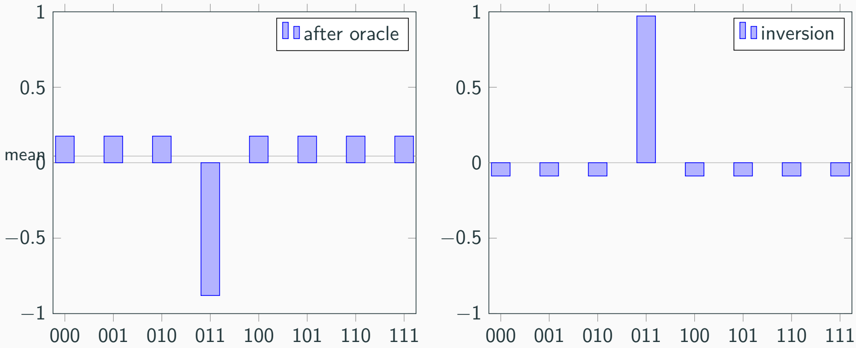


Example: $N = 2^3 = 8, w = 011$





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



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

Table of Contents

Setting a Geometric Stage pt. I

In order to analyse Grover's performance, it is useful to take the following 2-dimensional geometrical perspective

Setting a Geometric Stage pt. I

In order to analyse Grover's performance, it is useful to take the following 2-dimensional geometrical perspective

Let $|w\rangle$ be the "winner" state ($i.e.$ $f(w) = 1$) and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$

Setting a Geometric Stage pt. I

In order to analyse Grover's performance, it is useful to take the following 2-dimensional geometrical perspective

Let $|w\rangle$ be the "winner" state ($i.e.$ $f(w) = 1$) and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$

Both vectors yield 2-dimensional real vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Setting a Geometric Stage pt. I

In order to analyse Grover's performance, it is useful to take the following 2-dimensional geometrical perspective

Let $|w\rangle$ be the "winner" state (*i.e.* $f(w) = 1$) and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-1}} \sum_{x \neq w} |x\rangle$

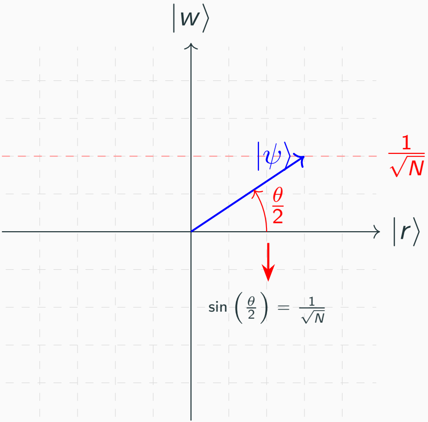
Both vectors yield 2-dimensional real vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Also, uniform superposition $|\psi\rangle = H^{\otimes n} |0\rangle$, *i.e.* our starting state, rewritten as

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

Setting a Geometric Stage pt. II

Last slide gives rise to



Goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Oracle and Inversion about the Mean, Geometrically

Also useful to revisit two operations under the light of the new vector space. Namely

- the oracle (U_f)
- and inversion about the mean ($2 |\psi\rangle \langle\psi| - I$)

Oracle and Inversion about the Mean, Geometrically

Also useful to revisit two operations under the light of the new vector space. Namely

- the oracle (U_f)
- and inversion about the mean ($2\left|\psi\right\rangle\left\langle\psi\right| - I$)

We will see that $(2\left|\psi\right\rangle\left\langle\psi\right| - I)U_f$ amounts to a counter-clockwise rotation of θ radians

The Oracle pt. I

It is defined by

$$\begin{cases} |x\rangle \mapsto |x\rangle & \text{if } x \neq w \\ |x\rangle \mapsto -|x\rangle & \text{otherwise} \end{cases}$$

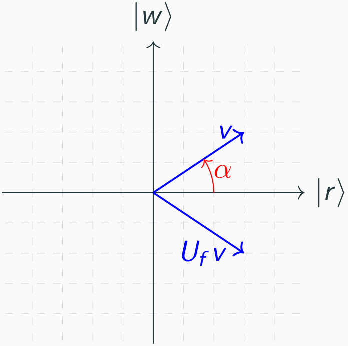
In particular for the basis $\{|w\rangle, |r\rangle\}$ we deduce

$$\begin{cases} |w\rangle \mapsto -|w\rangle \\ |r\rangle \mapsto |r\rangle \end{cases}$$

which corresponds to $2|r\rangle\langle r| - I$

The Oracle pt. II

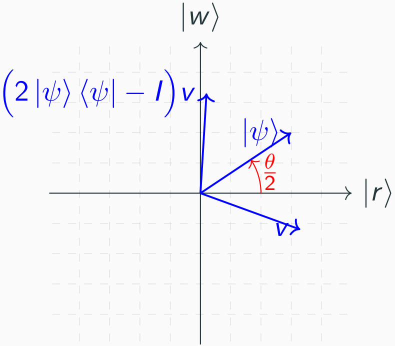
$\Big(2\,|r\rangle\,\langle r| - I\Big)(a\,|w\rangle + b\,|r\rangle) = -a\,|w\rangle + b\,|r\rangle$. Thus it corresponds to reflection about the $|r\rangle$-axis



$$\Big(2\,|r\rangle\,\langle r| - I\Big)(\sin\alpha\,|w\rangle + \cos\alpha\,|r\rangle) = \sin -\alpha\,|w\rangle + \cos -\alpha\,|r\rangle$$

Inversion about the Mean

Analogously, $2\left|\psi\right\rangle\left\langle\psi\right| - I$ corresponds to reflection around the $\left|\psi\right\rangle$-axis



$$\left(2\left|\psi\right\rangle\left\langle\psi\right| - I\right)(\sin -\alpha \left|w\right\rangle + \cos -\alpha \left|r\right\rangle) = \sin(\alpha+\theta)\left|w\right\rangle + \cos(\alpha+\theta)\left|r\right\rangle$$

Analysis of Grover Iterations

Let $G = \Big(2\,|\psi\rangle\,\langle\psi| - I\Big)U_f$. Then

$$G\Big(\sin\alpha\,|w\rangle + \cos\alpha\,|r\rangle\Big) = \sin(\alpha+\theta)\,|w\rangle + \cos(\alpha+\theta)\,|r\rangle$$

Therefore

$$G^k\Big(\sin\alpha\,|w\rangle + \cos\alpha\,|r\rangle\Big) = \sin(\alpha+k\theta)\,|w\rangle + \cos(\alpha+k\theta)\,|r\rangle$$

In particular

$$G^k\,|\psi\rangle = \sin\left(\tfrac{\theta}{2}+k\theta\right)|w\rangle + \cos\left(\tfrac{\theta}{2}+k\theta\right)|r\rangle$$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Formally, need to find integer k s.t. $\sin\left(k\theta + \frac{\theta}{2}\right) = 1$ *i.e.*

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

Thus $k = \mathrm{c.i.}\left(\frac{\pi}{2\theta} - \frac{1}{2}\right)$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Formally, need to find integer k s.t. $\sin\left(k\theta + \frac{\theta}{2}\right) = 1$ *i.e.*

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

Thus $k = \mathrm{c.i.}\left(\frac{\pi}{2\theta} - \frac{1}{2}\right)$

For very large N, we have $\frac{\theta}{2} \approx \frac{1}{\sqrt{N}}$ and therefore

$$\begin{aligned} & \frac{\pi}{2\theta} - \frac{1}{2} \\ \approx\ & \frac{\pi}{\frac{4}{\sqrt{N}}} - \frac{1}{2} \\ =\ & \frac{\pi\sqrt{N}}{4} - \frac{1}{2} \end{aligned}$$

Thus Grover's algorithm has complexity $O(\sqrt{N})$

Table of Contents

Grover's Problem Generalised to Multiple Solutions

The Problem

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

There exist M elements $x \in \{0,1\}^n$ such that $f(x) = 1$

Discover one of such elements

Classically, need to evaluate f $(2^n - M)$ times in the worst case

Grover's Problem Generalised to Multiple Solutions

The Problem

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

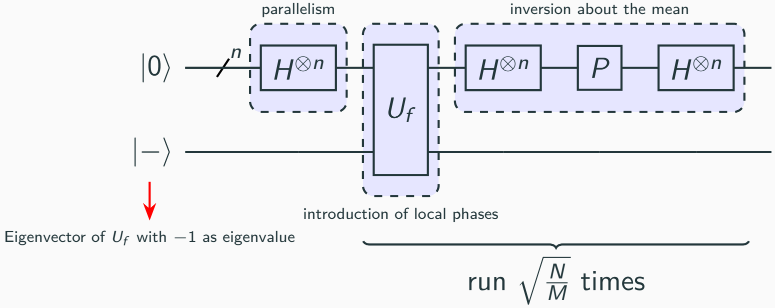
There exist M elements $x \in \{0,1\}^n$ such that $f(x) = 1$

Discover one of such elements

Classically, need to evaluate f $(2^n - M)$ times in the worst case

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

Same Circuit



Main difference is that inversion of local phases will be applied to M states, not necessarily one

Back to the Geometrical Perspective

Let $|w\rangle$ be the uniform superposition of "winner" states *i.e.* $\frac{1}{\sqrt{M}} \sum_{x \text{ a sol.}} |x\rangle$ and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-M}} \sum_{x \text{ not a sol.}} |x\rangle$

Back to the Geometrical Perspective

Let $|w\rangle$ be the uniform superposition of "winner" states *i.e.* $\frac{1}{\sqrt{M}} \sum_{x \text{ a sol.}} |x\rangle$ and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-M}} \sum_{x \text{ not a sol.}} |x\rangle$

Both vectors yield a 2-dimensional vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

Back to the Geometrical Perspective

Let $|w\rangle$ be the uniform superposition of "winner" states *i.e.* $\frac{1}{\sqrt{M}} \sum_{x \text{ a sol.}} |x\rangle$ and $|r\rangle$ be the uniform superposition of the remaining states *i.e.* $\frac{1}{\sqrt{N-M}} \sum_{x \text{ not a sol.}} |x\rangle$

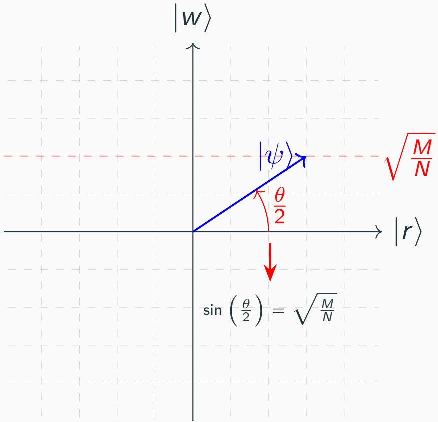
Both vectors yield a 2-dimensional vector space with orthonormal basis $\{|w\rangle, |r\rangle\}$

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

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

Back to the Geometrical Perspective

Last slide gives rise to



Goal is to rotate the vector to become as close as possible to $|w\rangle$

Oracle and Inversion Revisited

Oracle operation $2\,|r\rangle\,\langle r| - I$ still corresponds to a reflection about the $|r\rangle$-axis

Oracle and Inversion Revisited

Oracle operation $2\,|r\rangle\,\langle r| - I$ still corresponds to a reflection about the $|r\rangle$-axis

Inversion about the mean $2\,|\psi\rangle\,\langle\psi| - I$ still corresponds to a reflection about the $|\psi\rangle$-axis

Analysis of Grover Iterations

Let $G = \Big(2 \left|\psi\right\rangle \left\langle\psi\right| - I\Big) U_f$. Then

$$G\Big(\sin\alpha \left|w\right\rangle + \cos\alpha \left|r\right\rangle \Big) = \sin(\alpha + \theta) \left|w\right\rangle + \cos(\alpha + \theta) \left|r\right\rangle$$

Therefore

$$G^k\Big(\sin\alpha \left|w\right\rangle + \cos\alpha \left|r\right\rangle \Big) = \sin(\alpha + k\theta) \left|w\right\rangle + \cos(\alpha + k\theta) \left|r\right\rangle$$

In particular

$$G^k \left|\psi\right\rangle = \sin\left(\frac{\theta}{2} + k\theta\right) \left|w\right\rangle + \cos\left(\frac{\theta}{2} + k\theta\right) \left|r\right\rangle$$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Formally, need to find integer k s.t. $\sin\left(k\theta + \frac{\theta}{2}\right) = 1$ *i.e.*

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

Thus $k = \mathrm{c.i.}\left(\frac{\pi}{2\theta} - \frac{1}{2}\right)$

Determining Grover's Performance

Recall: goal is to rotate $|\psi\rangle$ so that it is as close as possible to $|w\rangle$

Formally, need to find integer k s.t. $\sin\left(k\theta + \frac{\theta}{2}\right) = 1$ *i.e.*

$$k\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

Thus $k = \mathrm{c.i.}\left(\frac{\pi}{2\theta} - \frac{1}{2}\right)$

When M much smaller than N, we have $\frac{\theta}{2} \approx \sqrt{\frac{M}{N}}$ and therefore

$$\begin{aligned} & \frac{\pi}{2\theta} - \frac{1}{2} \\ \approx\ & \frac{\pi}{4\sqrt{\frac{M}{N}}} - \frac{1}{2} \\ =\ & \frac{\pi\sqrt{N}}{4\sqrt{M}} - \frac{1}{2} \end{aligned}$$

Thus Grover's algorithm has complexity $O(\sqrt{\frac{N}{M}})$

Exercise

Let $N = 4$ and $M = 2$

What $n^{\underline{o}}$ of Grover iterations would you choose?

What is the probability of succeeding with the chosen $n^{\underline{o}}$ of iterations?

How to improve the probability of success?

To Follow . . .

Grover's algorithm assumes that one knows the *nº* of solutions of the problem *a priori*

To Follow . . .

Grover's algorithm assumes that one knows the *n*º of solutions of the problem *a priori*

In the following lectures we will see how to overcome such a limitation