Grover's algorithm


FOUND IT
motifake.com

Problem statement

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

How many calls to f to determine x?

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

How many calls to f to determine x?

E.g. finding element in array of $n = 2^N$ elements

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

How many calls to f to determine x?

E.g. finding element in array of $n = 2^N$ elements

Classically (even probabilistic): $O(n) = O(2^N)$

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

How many calls to f to determine x?

E.g. finding element in array of $n = 2^N$ elements

Classically (even probabilistic): $O(n) = O(2^N)$

Quantumly: $O(\sqrt{n}) = O(2^{N/2})$

Problem statement

Given a function $f : \{0,1\}^N \to \{0,1\}$

$\exists x$ such that $f(x) = 1$ and $\forall y,\ y \neq x\ f(y) = 0$

How many calls to f to determine x?

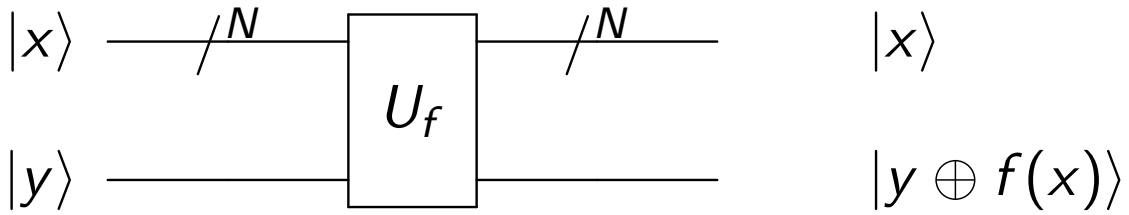
E.g. finding element in array of $n = 2^N$ elements

Classically (even probabilistic): $O(n) = O(2^N)$

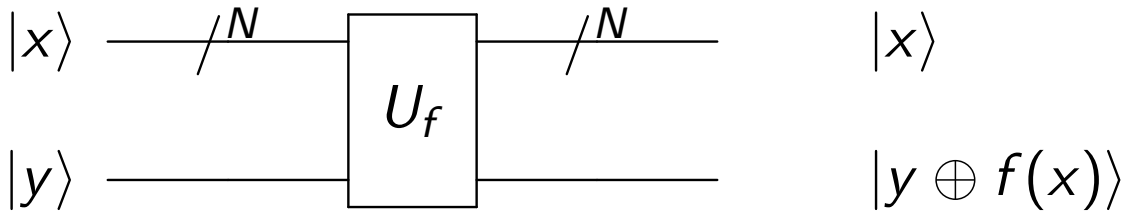
Quantumly: $O(\sqrt{n}) = O(2^{N/2})$

It's proven optimal!
(in the quantum case)

Unstructured search

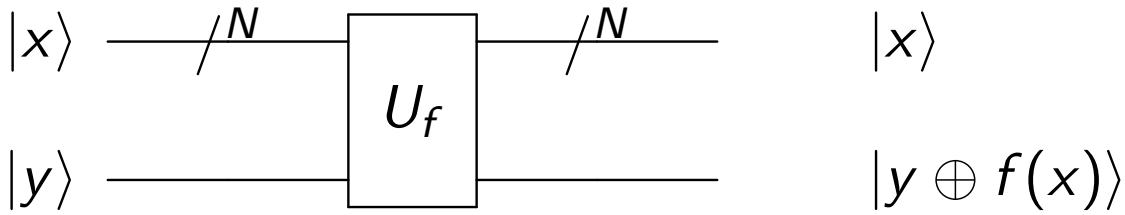


Unstructured search



As expected...

Unstructured search

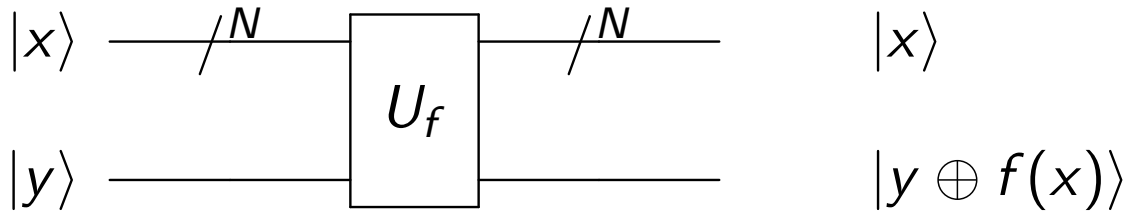


As expected...

First input $\sum_{x \in \{0,1\}^N} \frac{1}{\sqrt{2^N}} |x\rangle$

Second input $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Unstructured search



As expected...

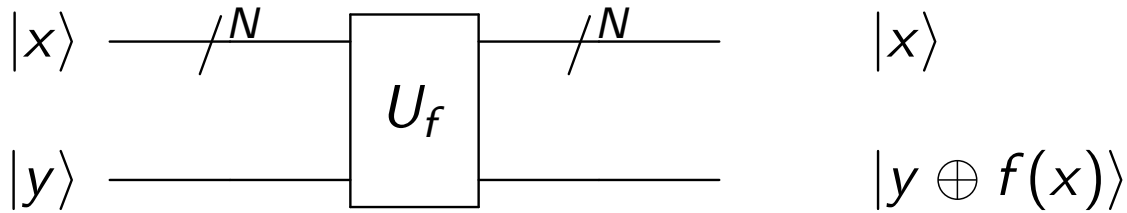
First input $\sum_{x \in \{0,1\}^N} \frac{1}{\sqrt{2^N}} |x\rangle$

Second input $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

And we get

$$\frac{1}{\sqrt{2^N}} \sum_{x \in \{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Unstructured search



As expected...

First input $\sum_{x\in\{0,1\}^N} \frac{1}{\sqrt{2^N}} |x\rangle$

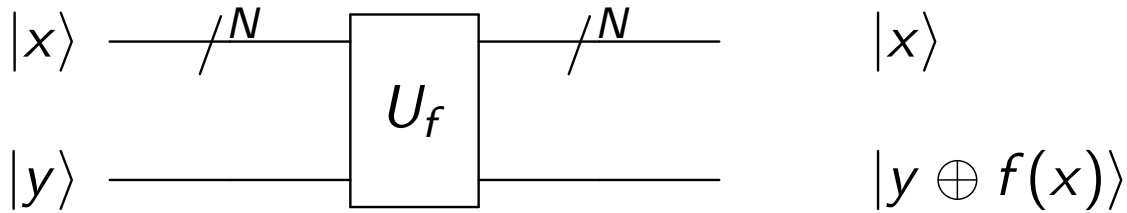
Second input $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

And we get

$$\frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

But now $f(x) = 1$ only for the solution (call it s)

Unstructured search



As expected...

First input $\sum_{x\in\{0,1\}^N} \frac{1}{\sqrt{2^N}} |x\rangle$

Second input $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

And we get

$$\frac{1}{\sqrt{2^N}} \sum_{x\in\{0,1\}^N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

But now $f(x) = 1$ only for the solution (call it s)

So the first state is actually:

$$\frac{1}{\sqrt{2^N}}(\sum_{x\neq s} |x\rangle - |s\rangle)$$

Unstructured search

Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

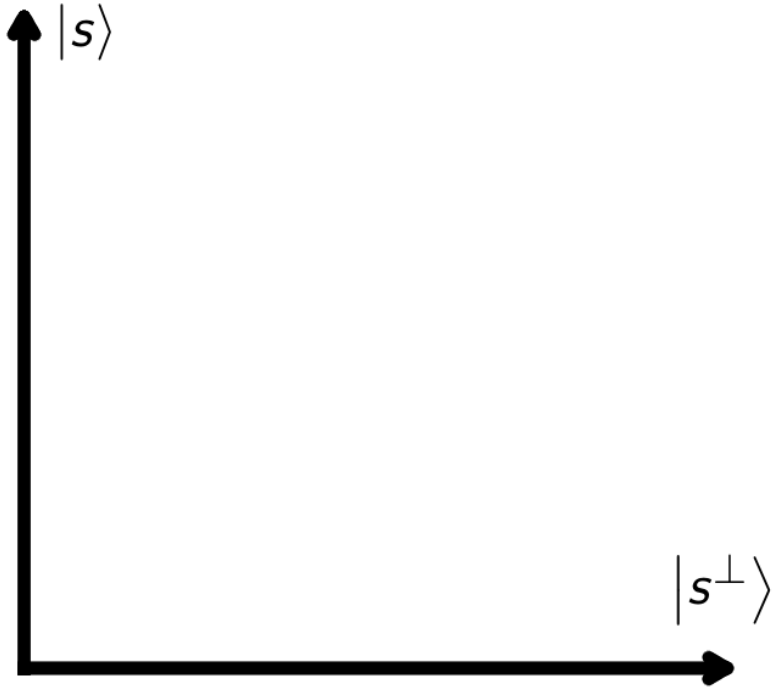
They are orthogonal!

Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

They are orthogonal!

Denote $\left|s^{\perp}\right\rangle = \frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$



Unstructured search

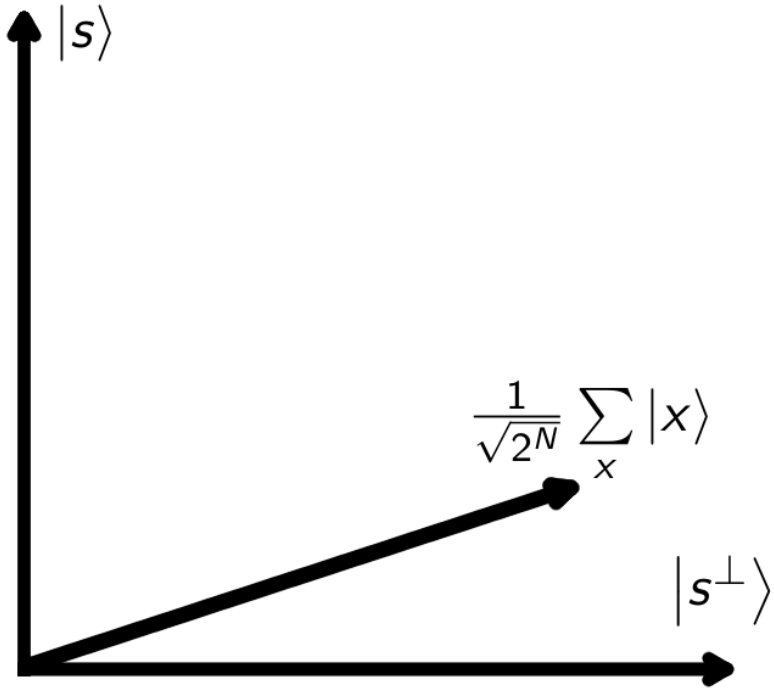
Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

They are orthogonal!

Denote $\left|s^{\perp}\right\rangle = \frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

In between them is $\frac{1}{\sqrt{2^N}} \sum_{x} |x\rangle$

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^{\perp}\right\rangle + \frac{1}{\sqrt{2^N}} |s\rangle$$



Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

They are orthogonal!

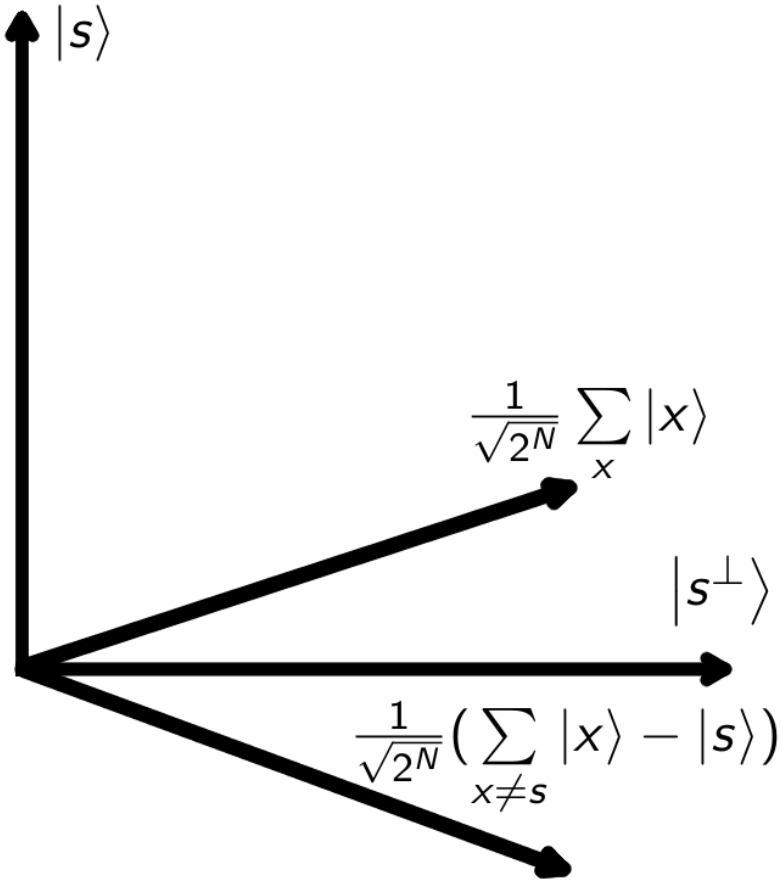
Denote $\left|s^{\perp}\right\rangle = \frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

In between them is $\frac{1}{\sqrt{2^N}} \sum_{x} |x\rangle$

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^{\perp}\right\rangle + \frac{1}{\sqrt{2^N}} |s\rangle$$

And on the other side

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^{\perp}\right\rangle - \frac{1}{\sqrt{2^N}} |s\rangle$$



Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

They are orthogonal!

Denote $\left|s^\perp\right\rangle = \frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

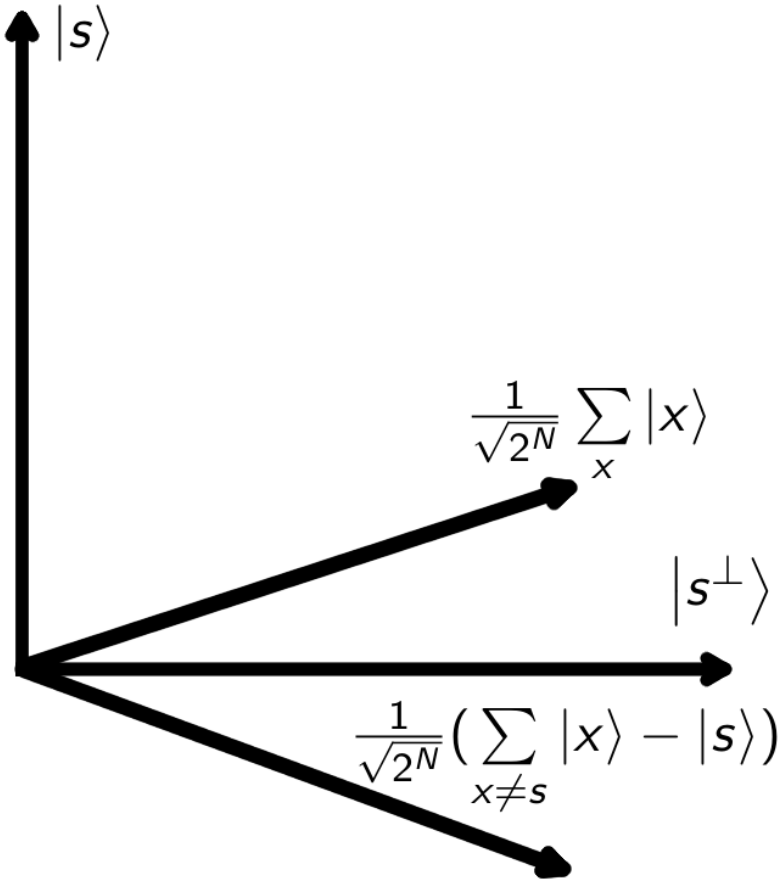
In between them is $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^\perp\right\rangle + \frac{1}{\sqrt{2^N}} |s\rangle$$

And on the other side

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^\perp\right\rangle - \frac{1}{\sqrt{2^N}} |s\rangle$$

We started with $a\left|s^\perp\right\rangle + b|s\rangle$



Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

They are orthogonal!

Denote $\left|s^\perp\right\rangle = \frac{1}{\sqrt{2^N-1}} \sum_{x \neq s} |x\rangle$

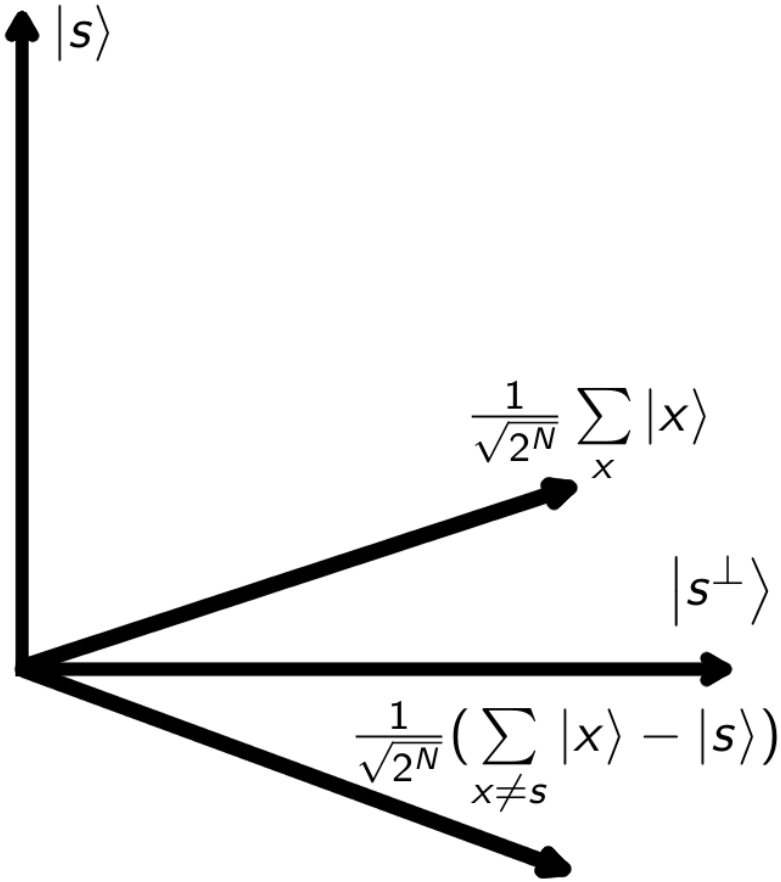
In between them is $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^\perp\right\rangle + \frac{1}{\sqrt{2^N}} |s\rangle$$

And on the other side

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}} \left|s^\perp\right\rangle - \frac{1}{\sqrt{2^N}} |s\rangle$$

We started with $a\left|s^\perp\right\rangle + b|s\rangle$
And ended with $a\left|s^\perp\right\rangle - b|s\rangle$



Unstructured search

Let's look more closely at $|s\rangle$ and $\frac{1}{\sqrt{2^N-1}}\sum_{x\neq s}|x\rangle$

They are orthogonal!

Denote $\left|s^\perp\right\rangle = \frac{1}{\sqrt{2^N-1}}\sum_{x\neq s}|x\rangle$

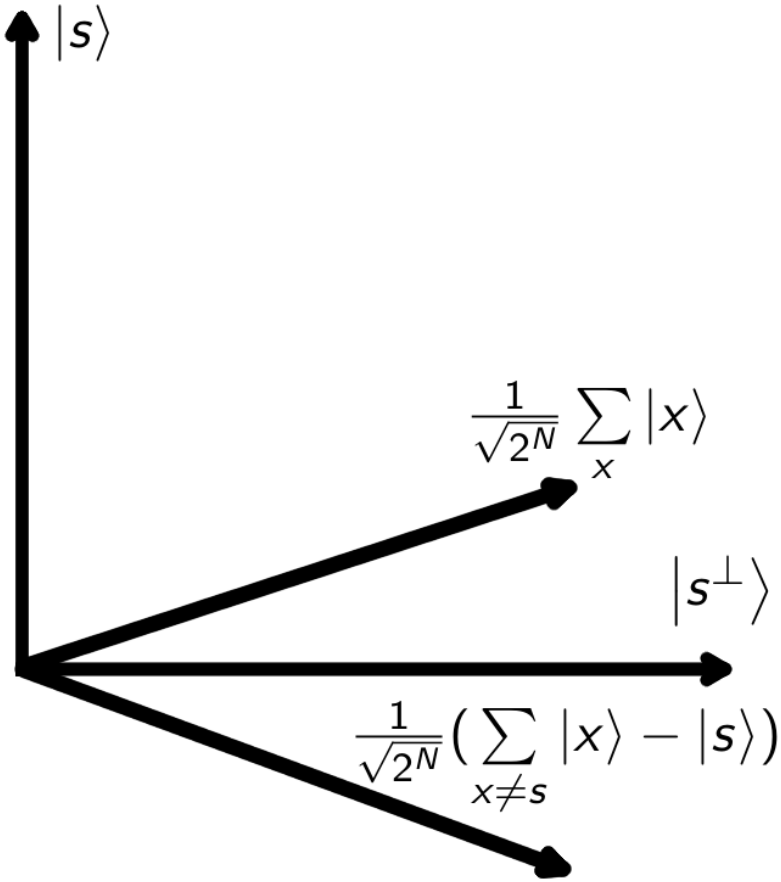
In between them is $\frac{1}{\sqrt{2^N}}\sum_{x}|x\rangle$

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}}\left|s^\perp\right\rangle + \frac{1}{\sqrt{2^N}}|s\rangle$$

And on the other side

$$\frac{\sqrt{2^N-1}}{\sqrt{2^N}}\left|s^\perp\right\rangle - \frac{1}{\sqrt{2^N}}|s\rangle$$

We started with $a\left|s^\perp\right\rangle + b|s\rangle$
And ended with $a\left|s^\perp\right\rangle - b|s\rangle$

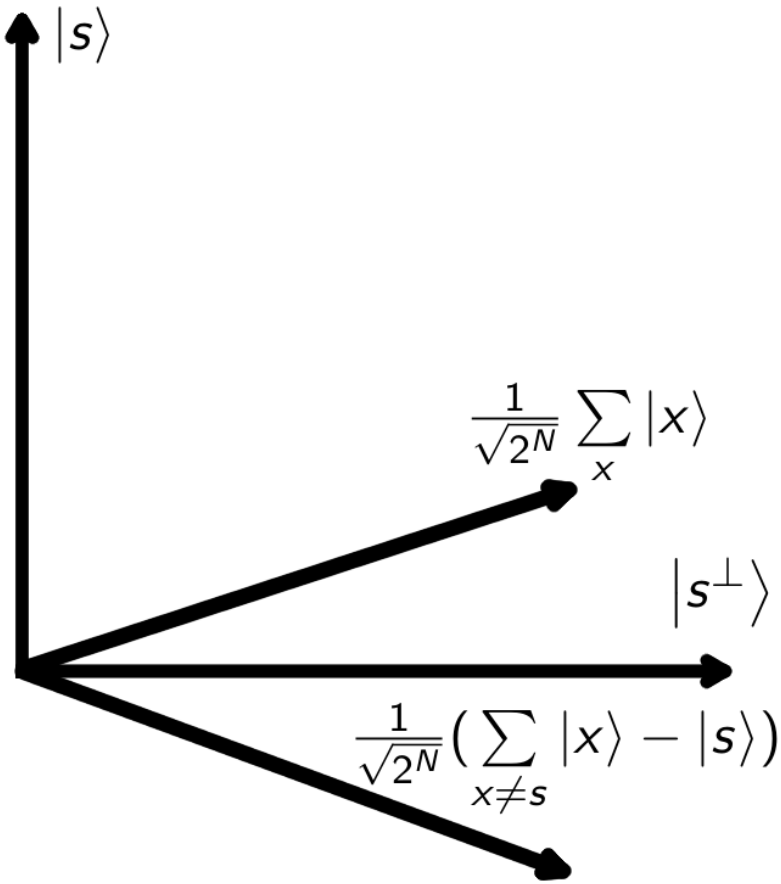


Reflection!

Unstructured search

Unstructured search

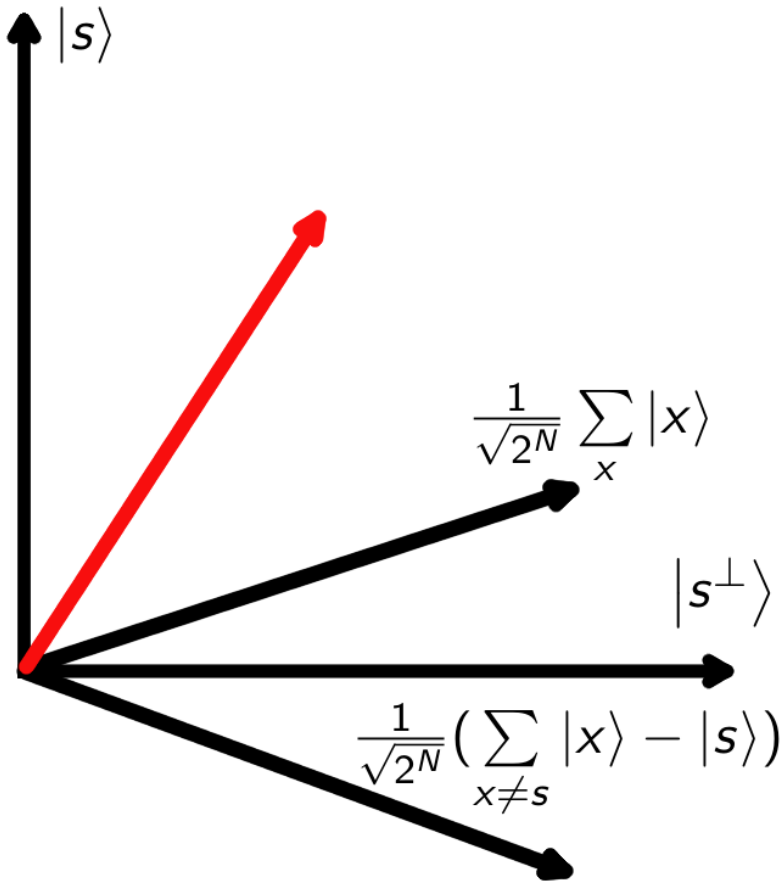
We've reflected our input with respect to $\left|s^{\perp}\right\rangle$



Unstructured search

We've reflected our input with respect to $\left|s^{\perp}\right\rangle$

Reflect back, with respect to $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

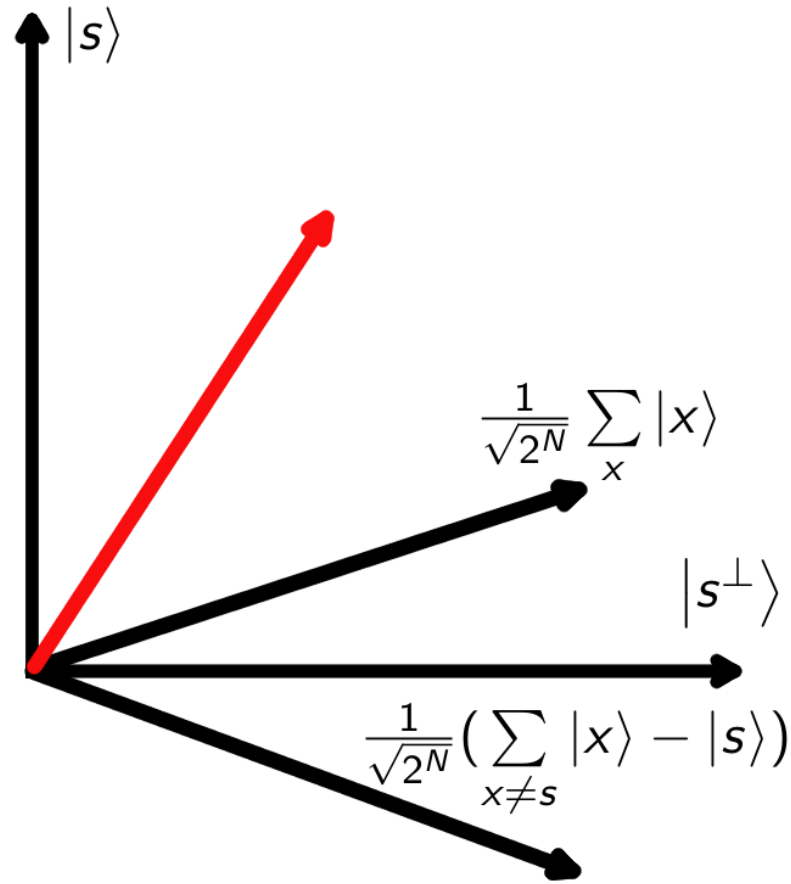


Unstructured search

We've reflected our input with respect to $|s^{\perp}\rangle$

Reflect back, with respect to $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

This brings us closer to $|s\rangle$!



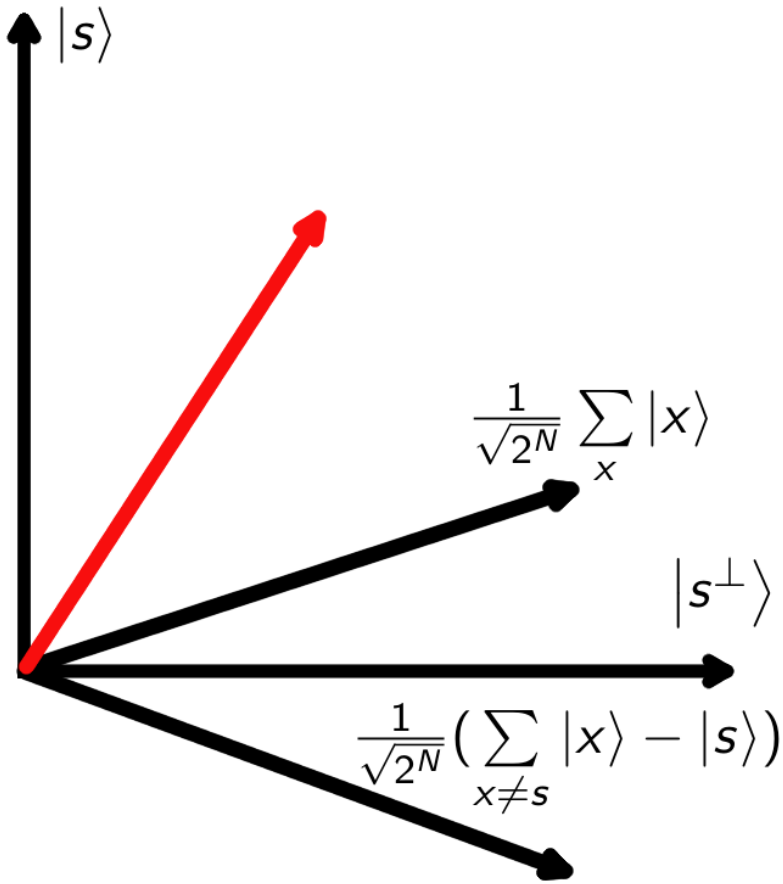
Unstructured search

We've reflected our input with respect to $|s^{\perp}\rangle$

Reflect back, with respect to $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

This brings us closer to $|s\rangle$!

Repeat until we reach $|s\rangle$



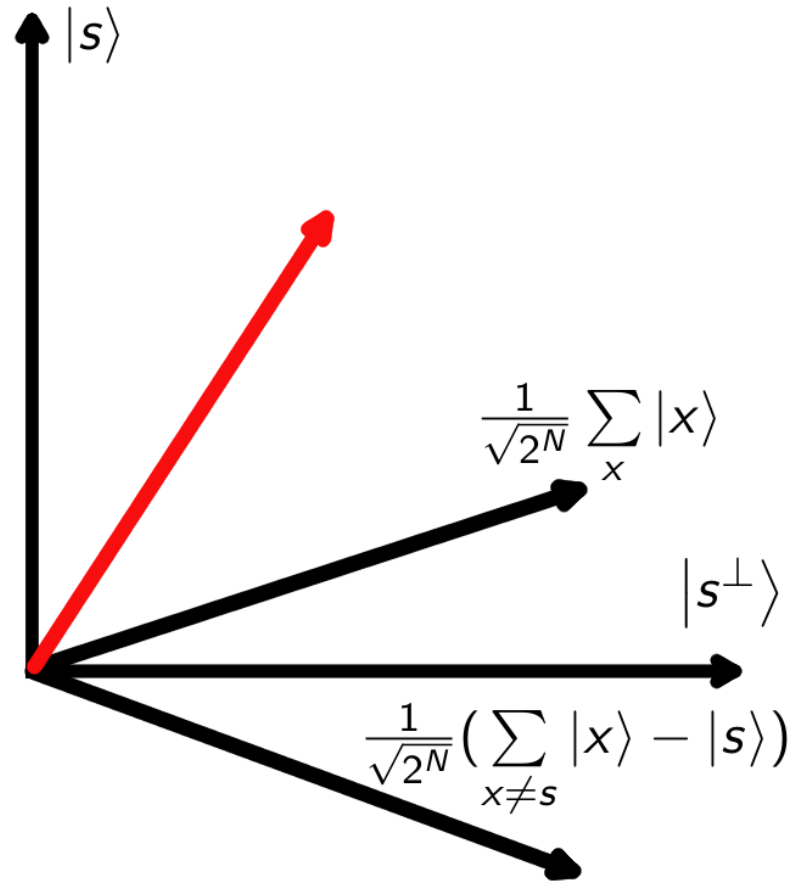
Unstructured search

We've reflected our input with respect to $|s^{\perp}\rangle$

Reflect back, with respect to $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

This brings us closer to $|s\rangle$!

Repeat until we reach $|s\rangle$



How many times?

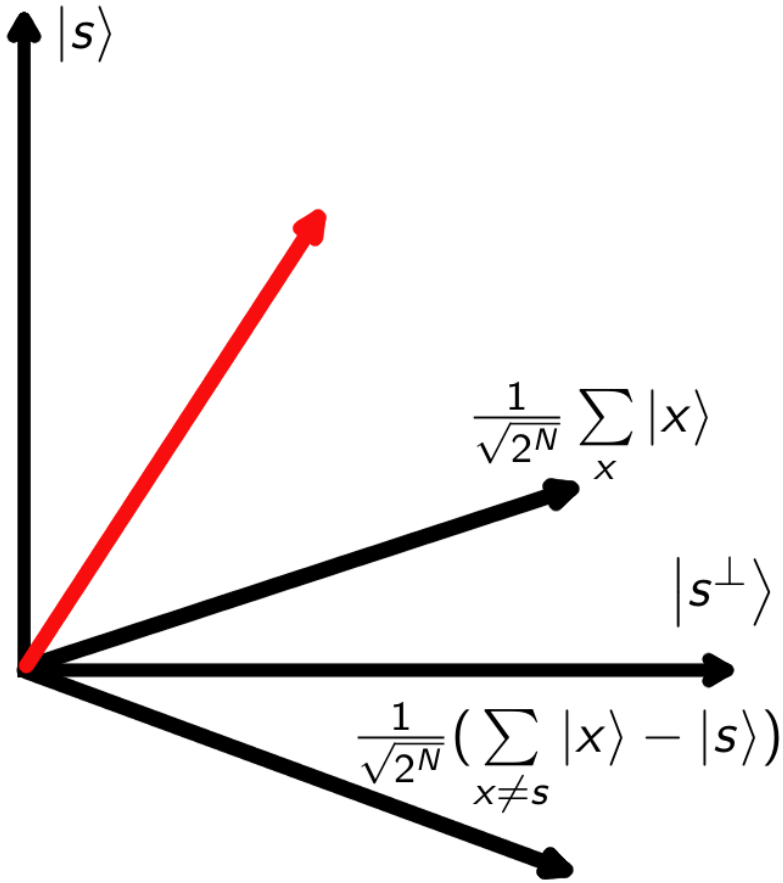
Unstructured search

We've reflected our input with respect to $|s^{\perp}\rangle$

Reflect back, with respect to $\frac{1}{\sqrt{2^N}} \sum_x |x\rangle$

This brings us closer to $|s\rangle$!

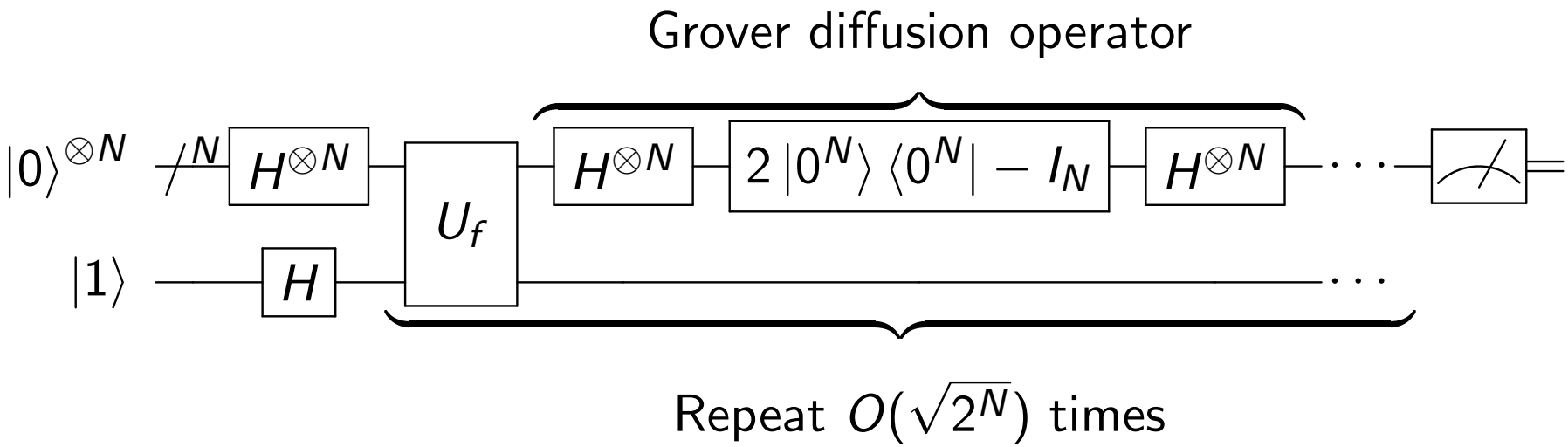
Repeat until we reach $|s\rangle$



How many times?

$$O(\sqrt{2^N}) = O(\sqrt{n})$$

Grover's algorithm



Applications

Applications

- Searching...

Applications

- Searching... for anything!

Applications

- Searching... for anything!
- Brute force attacks

Applications

- Searching... for anything!
- Brute force attacks
- Data mining

Applications

- Searching... for anything!
- Brute force attacks
- Data mining
- NP-hard problems (travelling salesman, Hamiltonian cycle)

Applications

- Searching... for anything!
- Brute force attacks
- Data mining
- NP-hard problems (travelling salesman, Hamiltonian cycle)
- Variants of Grover are useful for other problems (e.g. finding collisions)

2^N vs $2^{N/2}$

2^N vs $2^{N/2}$

Assume $N = 66$

2^N vs $2^{N/2}$

Assume $N = 66$

Number of instructions on classical computer: 2^{66}
Number of instructions on quantum computer: 2^{33}

2^N vs $2^{N/2}$

Assume $N = 66$

Number of instructions on classical computer: 2^{66}
Number of instructions on quantum computer: 2^{33}

Classical computer can do 10^9 instructions per second
Quantum computer can do 10^3 instructions per second

2^N vs $2^{N/2}$

Assume $N = 66$

Number of instructions on classical computer: 2^{66}
Number of instructions on quantum computer: 2^{33}

Classical computer can do 10^9 instructions per second
Quantum computer can do 10^3 instructions per second

Classical computer takes 2339 years to solve problem!

2^N vs $2^{N/2}$

Assume $N = 66$

Number of instructions on classical computer: 2^{66}
Number of instructions on quantum computer: 2^{33}

Classical computer can do 10^9 instructions per second
Quantum computer can do 10^3 instructions per second

Classical computer takes 2339 years to solve problem!

Quantum computer takes 100 days to solve problem!