INTRO TO QUANTUM COMPUTING

LECTURE #21

Quantum Search Algorithm

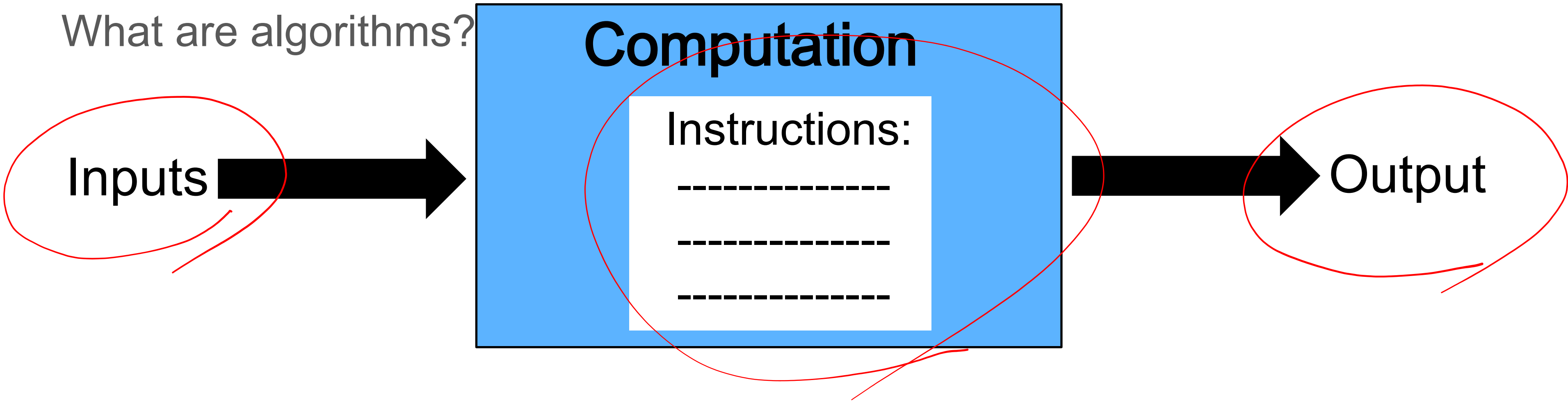
Amir Karamlou

03/28/2021

ANNOUNCEMENTS

Recap

What are algorithms?



Algorithm: a sequence of well-defined, instructions to perform a computatio

THE QUANTUM ALGOS LANDSCAPE

Deutsch -Josza

First theoretical demonstration of quantum advantage!

Uses an Oracle

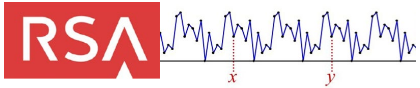
$$O(1) \ll O(2^n)$$

Exponential Quantum Speedup!

QUANTUM ADVANTAGE

Shor's Algorithm

Super -polynomial speedup for factoring using the QFT!



Cracking RSA Requires Factoring & Period Finding

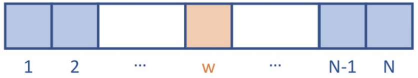
The Quantum Fourier Transform Encodes Frequency in Phase

$$O(\log(n)^3) \ll O(n^{1.9})$$

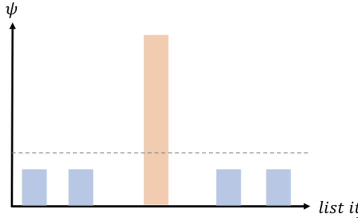
Super-Polynomial Quantum Speedup!

Grover Search

Quadratic speedup for search using amplitude amplification!



Unstructured Search



Leverages Amplitude Amplification

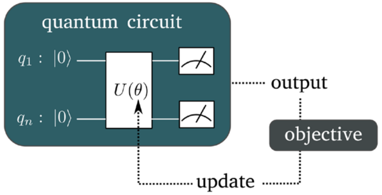
Classical

$$O(\sqrt{n}) \ll O(n)$$

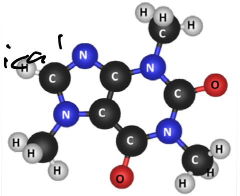
Quadratic Quantum Speedup!

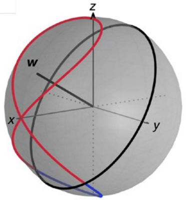
Near -Term Algos

Applications of noisy, small available quantum devices!



Hybrid Quantum -Classical Algos





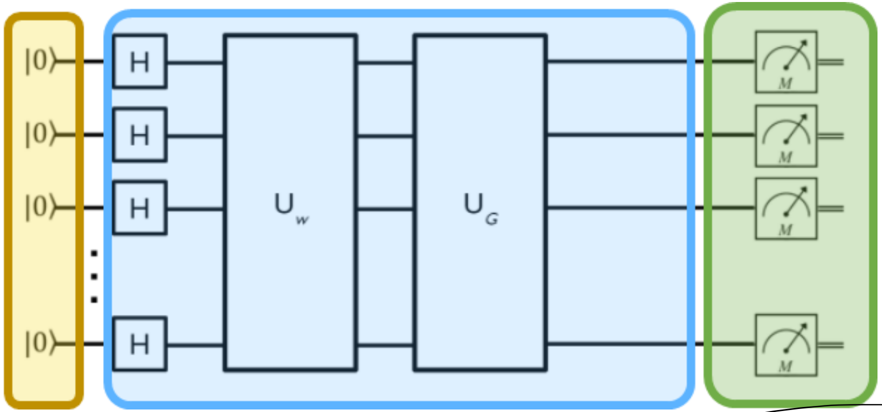
Using Quantum to Solve Important Problems!

Recap

Problem: Searching assuming *no* data structure

Why do we care?: Search is everywhere – i.e. databases

Method:



States Gates Measurement

Grover Search Algorithm

- **Goal**: Search an unsorted list of length N for a specific element
- **Assumption:** Already know ***what*** we're looking for, we just don't know ***where*** it is

Grover Search Algorithm

Classical search algorithm

$O(N)$

Quantum search algorithm

$O(\sqrt{N})$

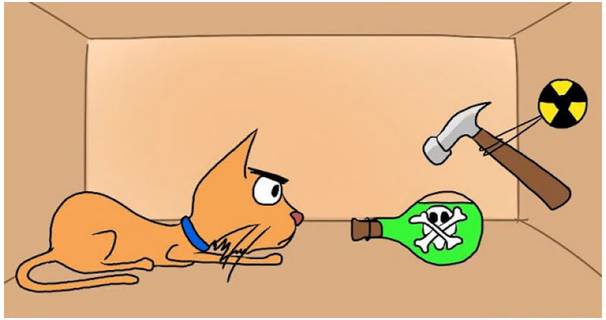
Let's assume a list of size 1,000,000

- Classical: 1,000,000 queries

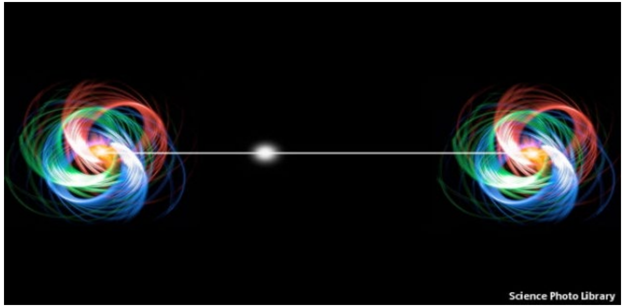
- Quantum: 1,000 queries

High level why?

SUPERPOSITION

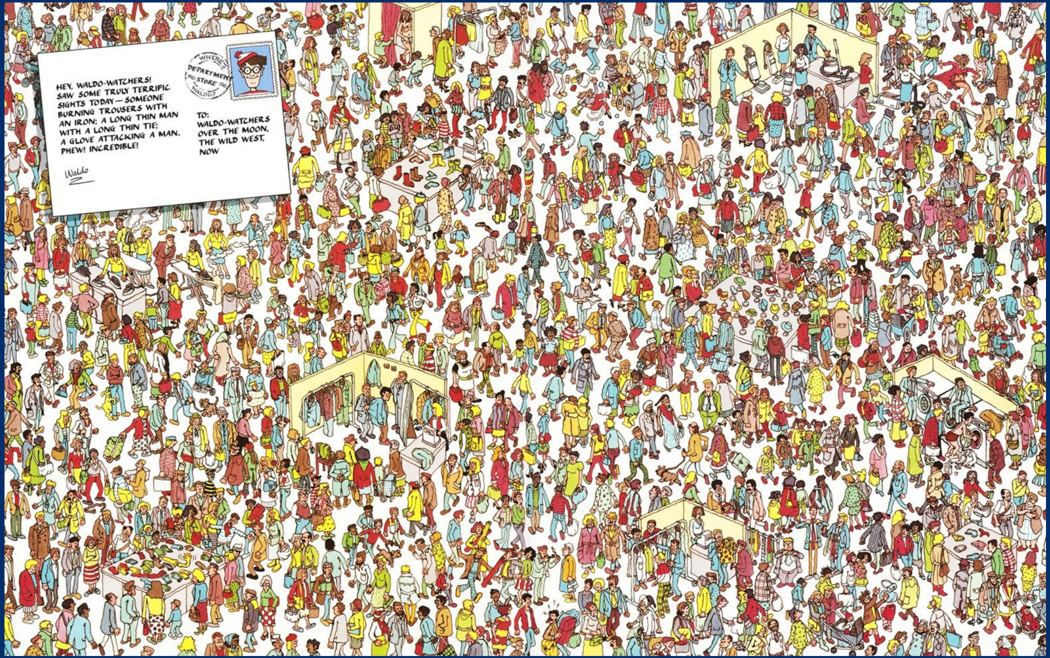


ENTANGLEMENT



QUANTUM INTERFERENCE

Where's Waldo?

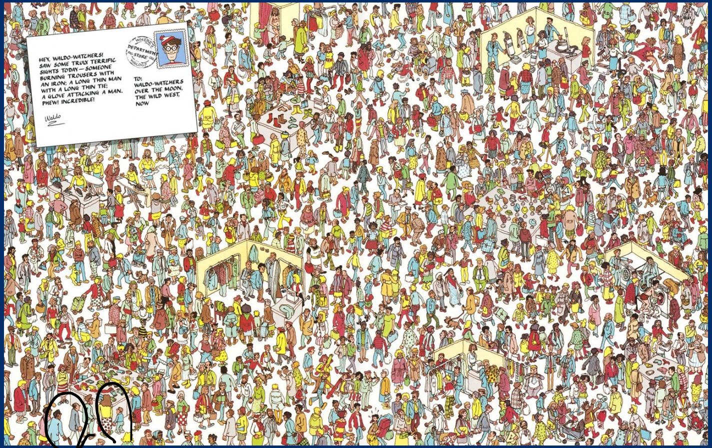


We are looking for:

- Tall, skinny man
- Blue jeans
- Red and white striped shirt
- Glasses
- Red and white winter hat
- Cane
- Smile

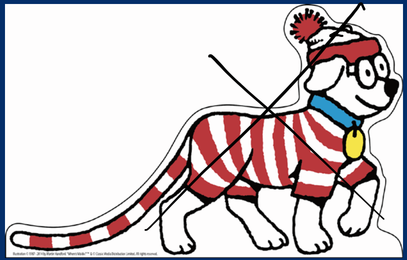
NOT

What if you had to find Waldo using a classical search algorithm?



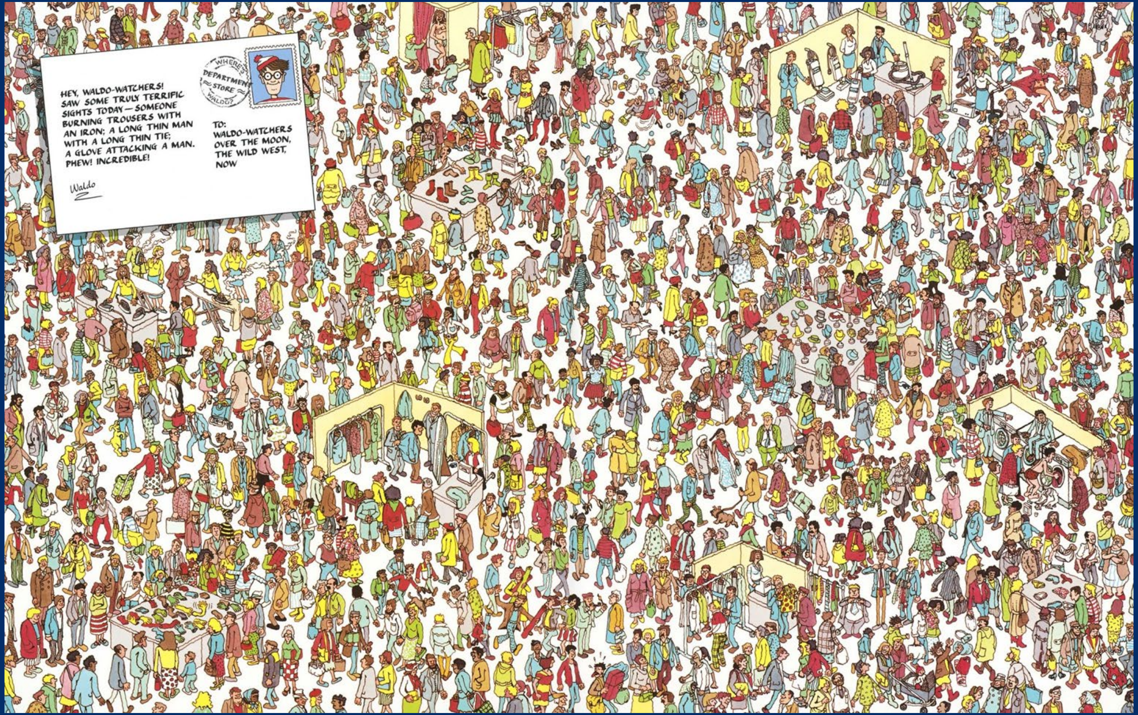
"Are you Waldo?"

"Are you Waldo?"

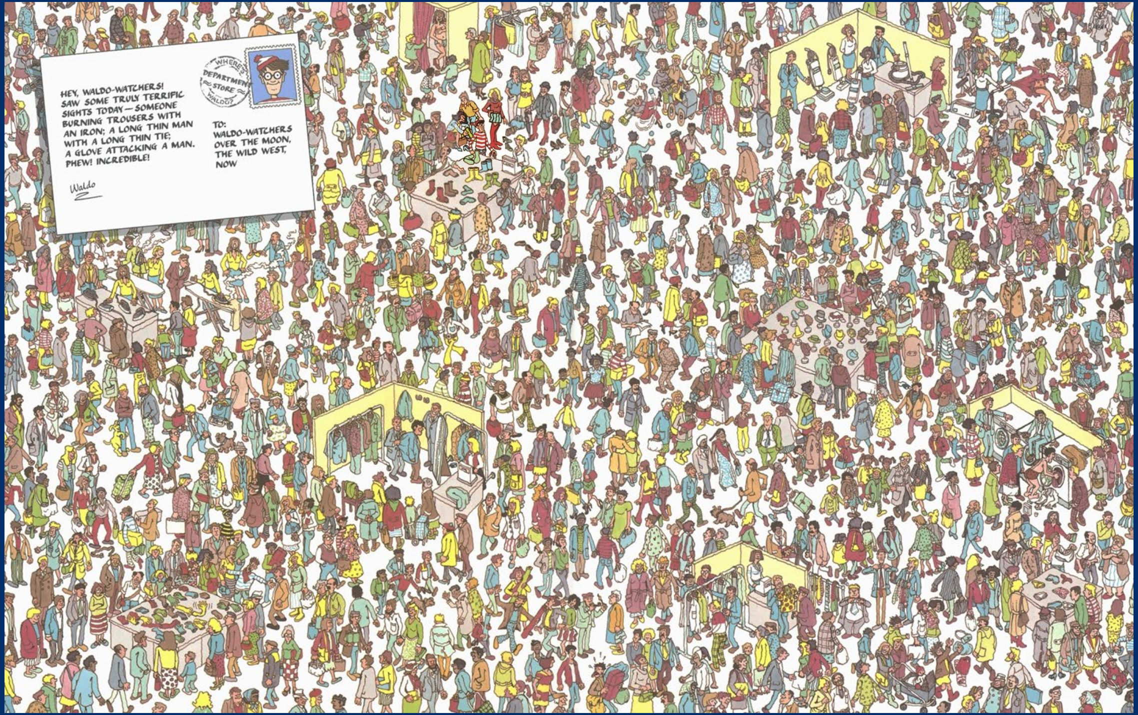


"Are you Waldo?"

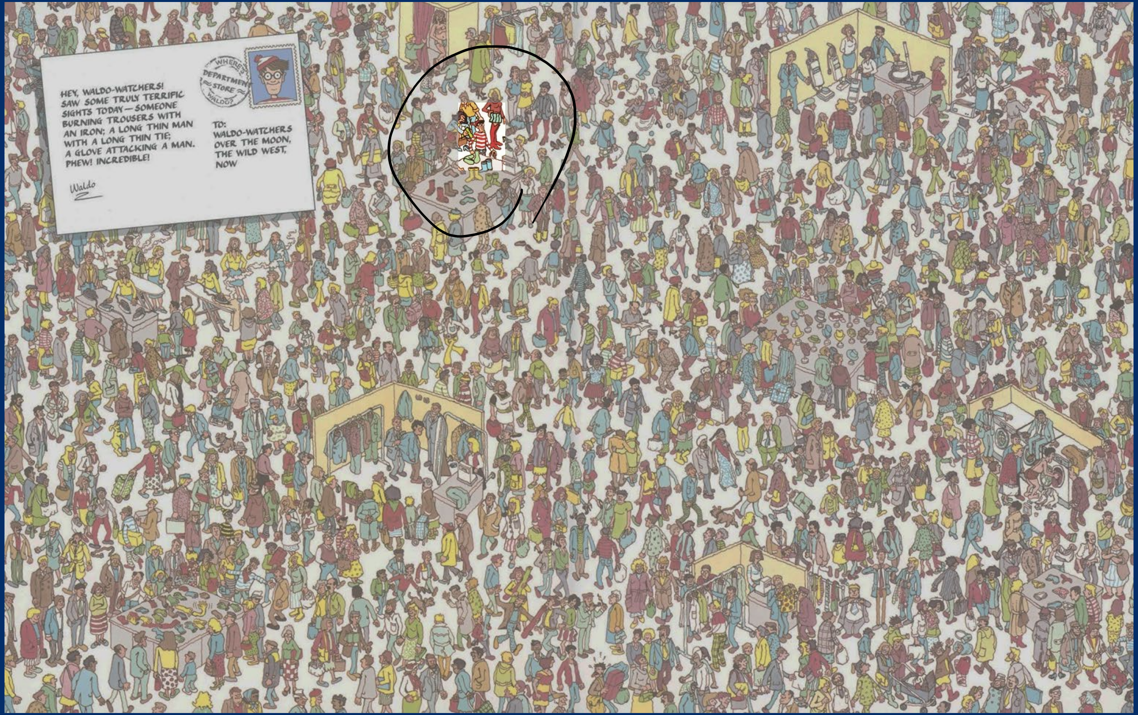
...it's not very efficient.



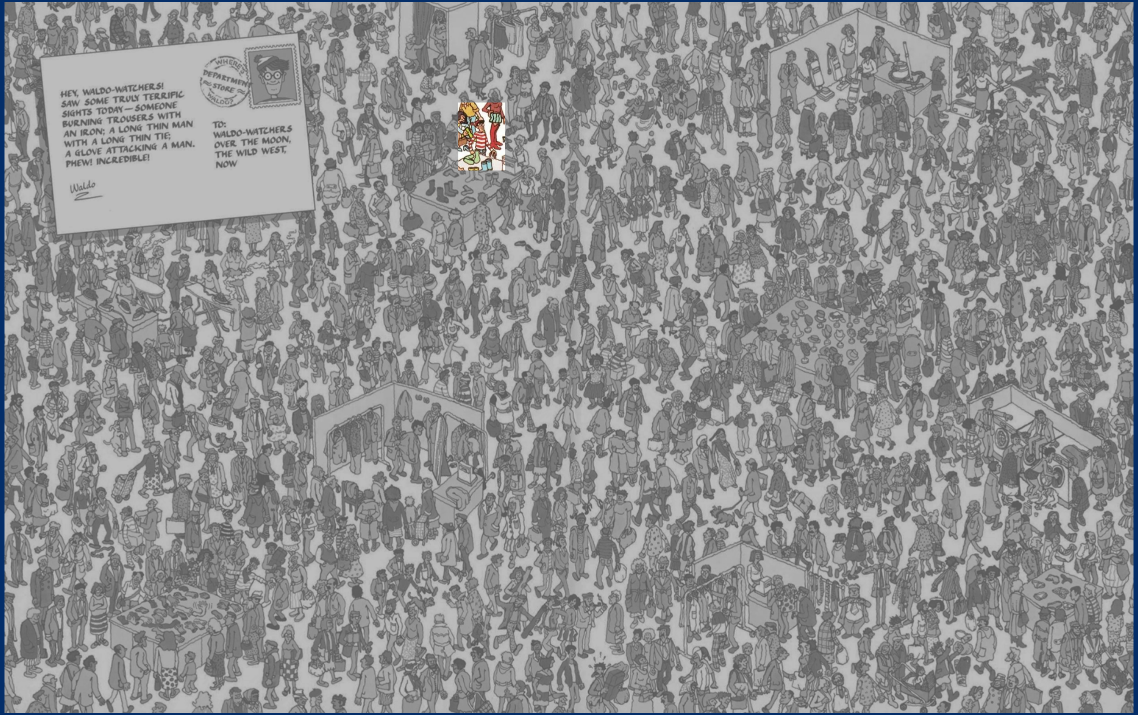
What if we could use a quantum search algorithm, like Grover's Algorithm?



Oracle Function



Oracle Function

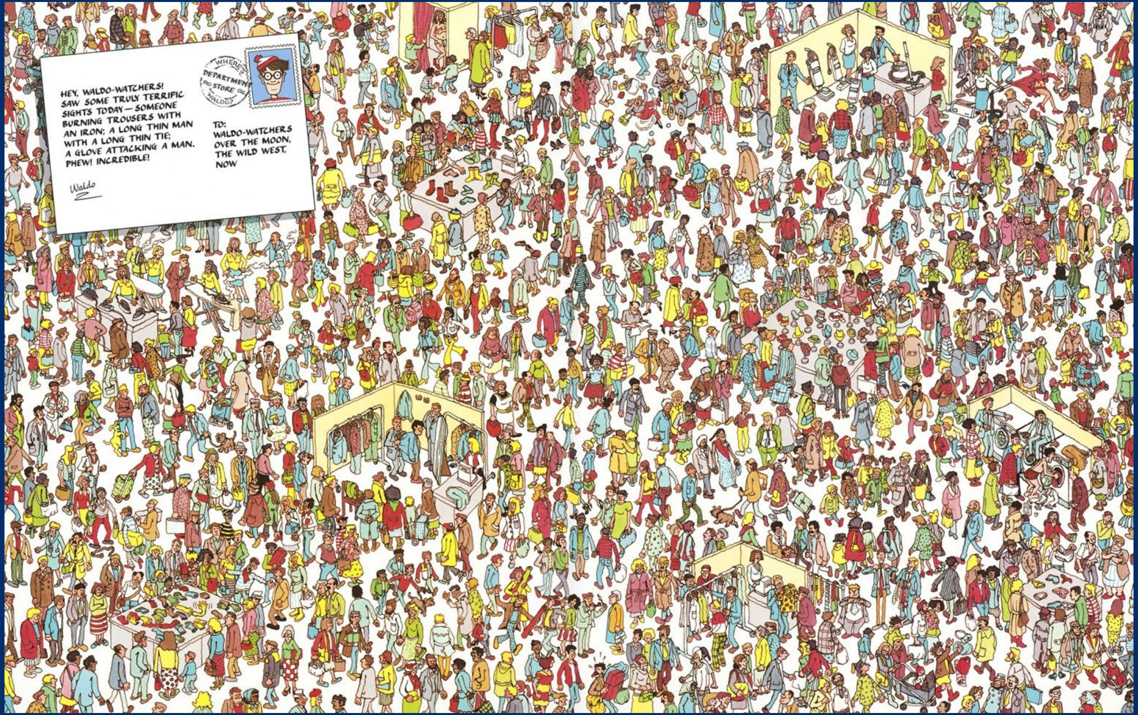


Oracle Function

Oracle Function


HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC SIGHTS TODAY — SOMEONE BURNING TROUSERS WITH AN IRON; A LONG THIN MAN WITH A LONG THIN TIE; A GLOVE ATTACKING A MAN. PHEW! INCREDIBLE!
Waldo
TO: WALDO-WATCHERS OVER THE MOON, THE WILD WEST, NOW

Ta Da!



See the difference?

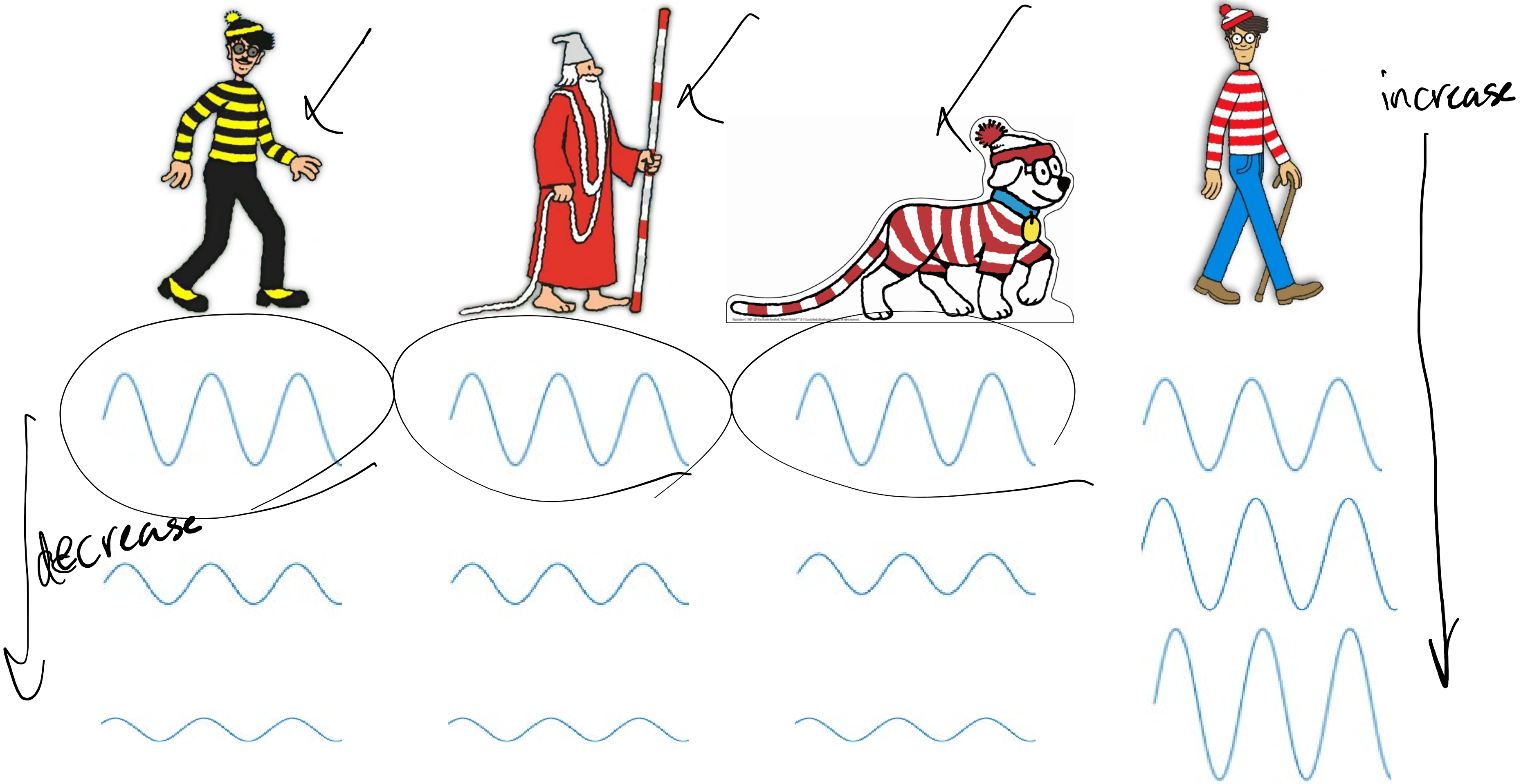
What makes Grover’s “quantum”?

Reminder from the beginning of the semester:

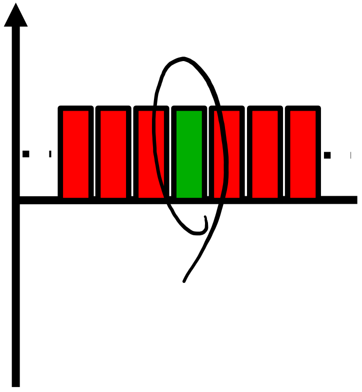
Qubits behave as **particles** and **waves**.

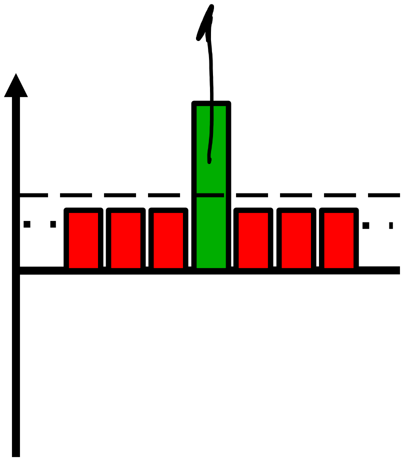
We can put all of these choices into superposition because of the wave properties of qubits.

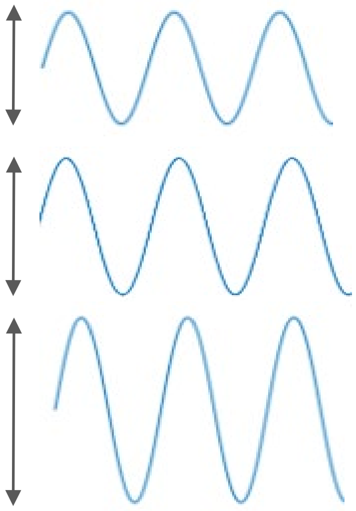
Since they’re waves, they can interfere with each other.



Incorrect solutions get destructively interfered. Correct solutions get constructively interfered.







Later in this lecture, we will plot the
amplitude of these waves.

Grover's algorithm steps

STEP 1. Equal superposition

STEP 2. Amplitude amplification

STEP 3. Measurement

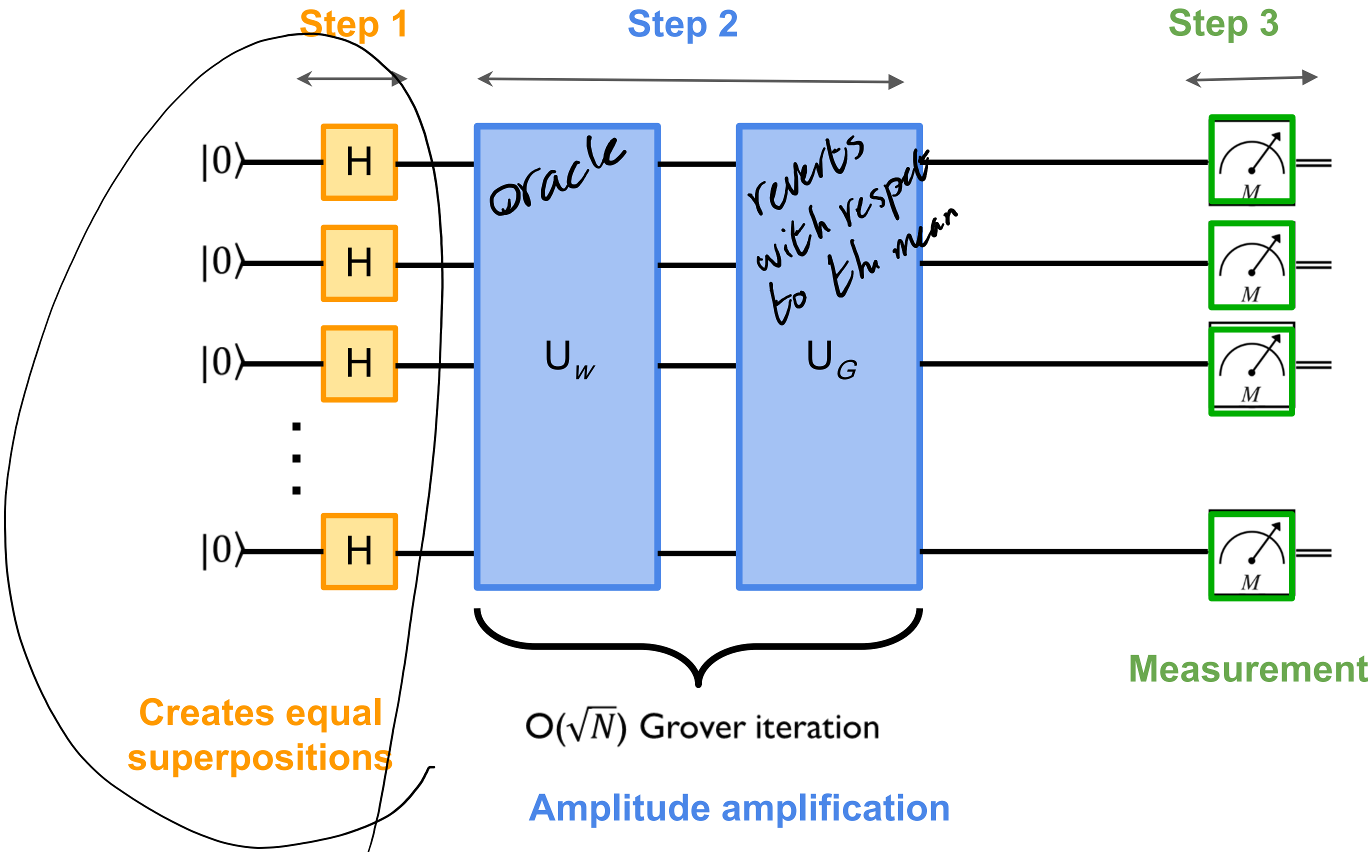
Grover's algorithm steps

STEP 1. Equal superposition: Start by assigning equal probability to every cell being the right answer

STEP 2. Amplitude amplification: Use quantum interference to transform the superposition so the correct cell has a significantly higher probability

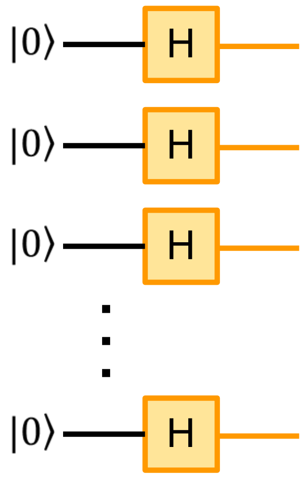
STEP 3. Measurement: Measure the state, with high probability the result is the right cell.

Grover Search Algorithm: Circuit



Grover Search Algorithm

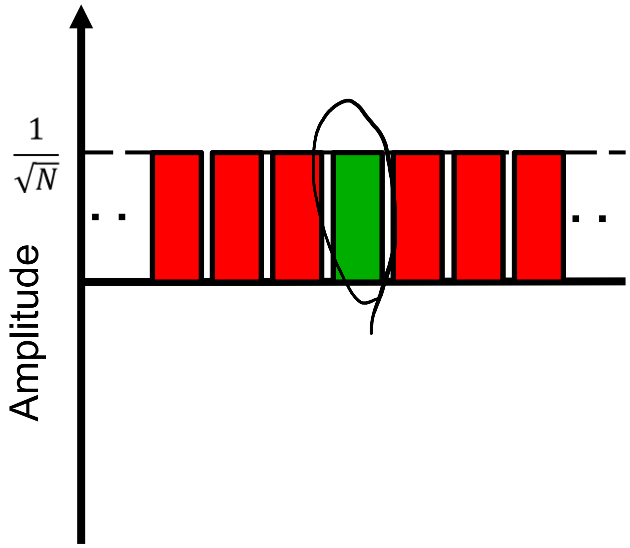
STEP 1: Start by assigning equal probability to every cell being the right answer (equal superposition)



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

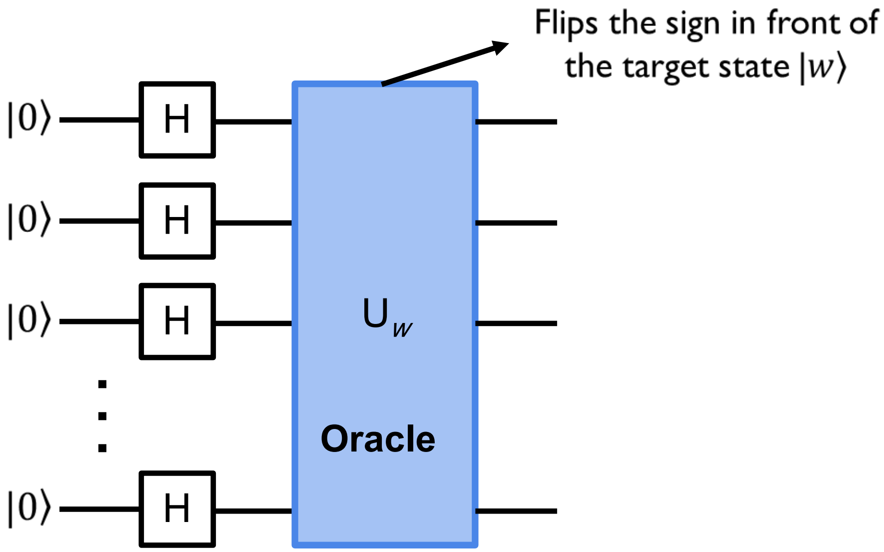
probability amps.

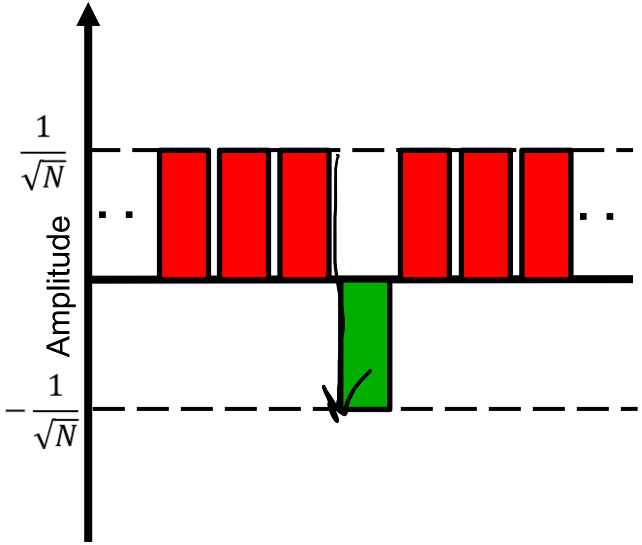
$P = \left(\frac{1}{\sqrt{N}}\right)^2 = \frac{1}{N}$



Grover Search Algorithm

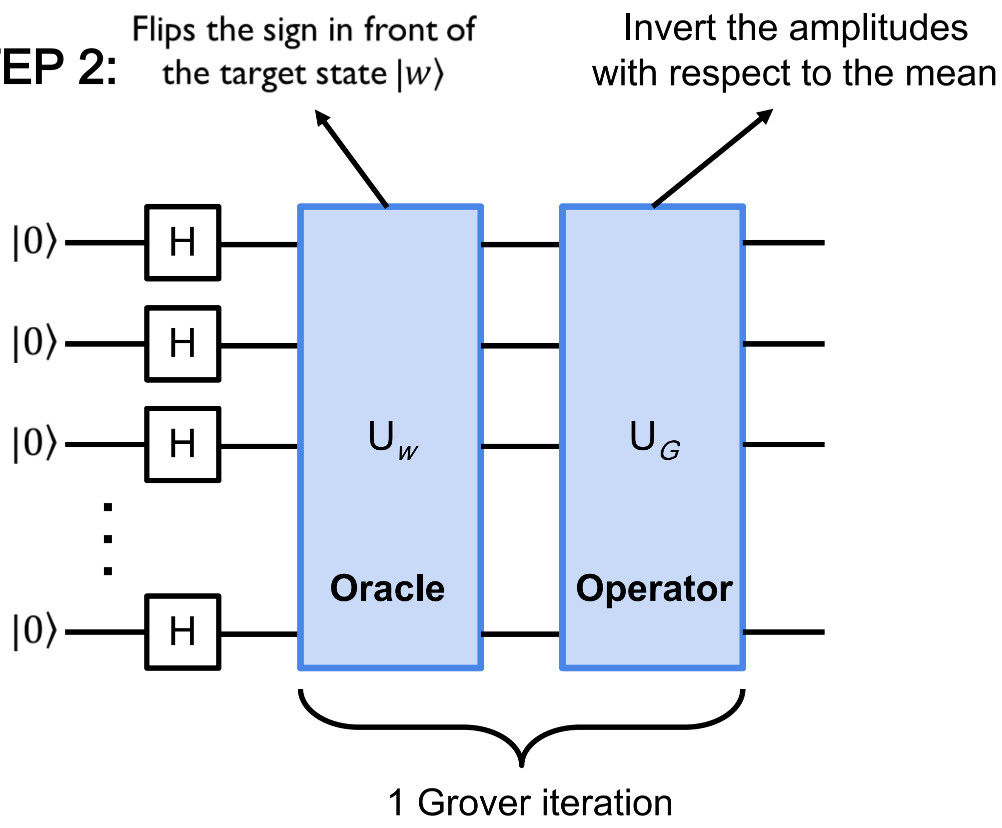
STEP 2: Use quantum interference to transform the superposition so the correct cell has a significantly higher probability

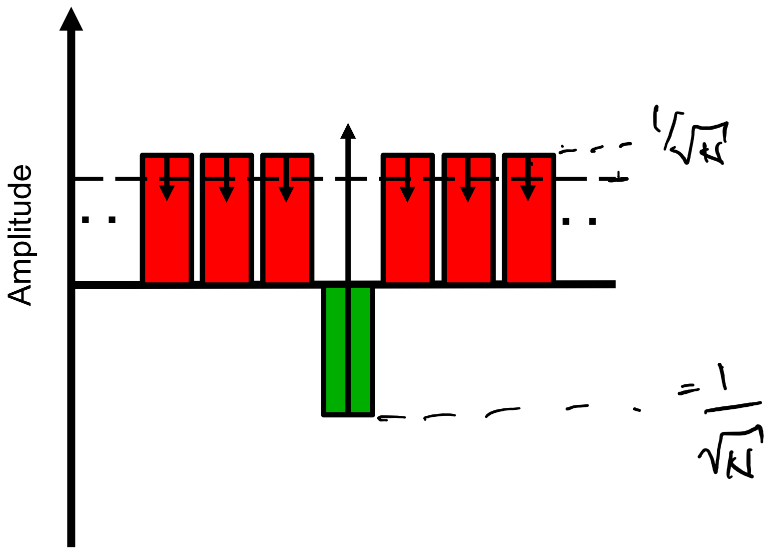




Grover Search Algorithm

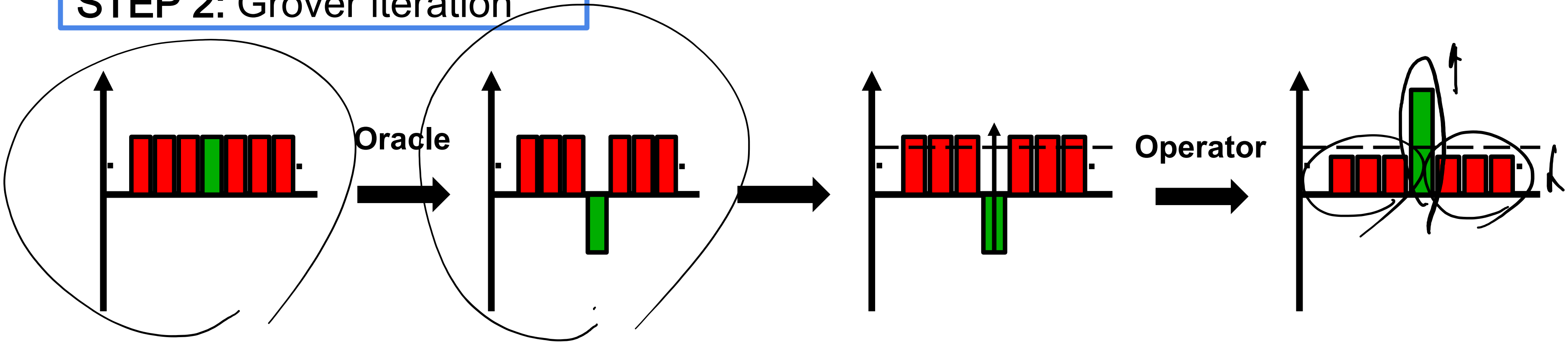
STEP 2:





Grover Search Algorithm

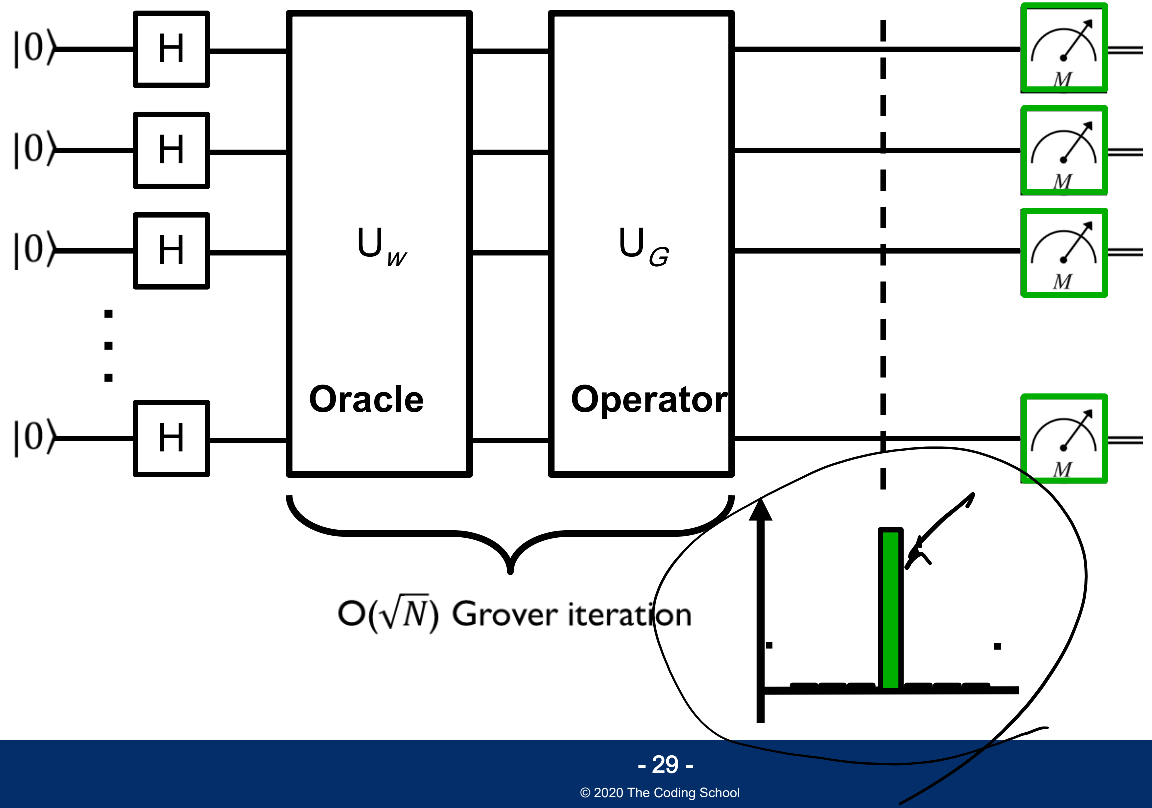
STEP 2: Grover iteration



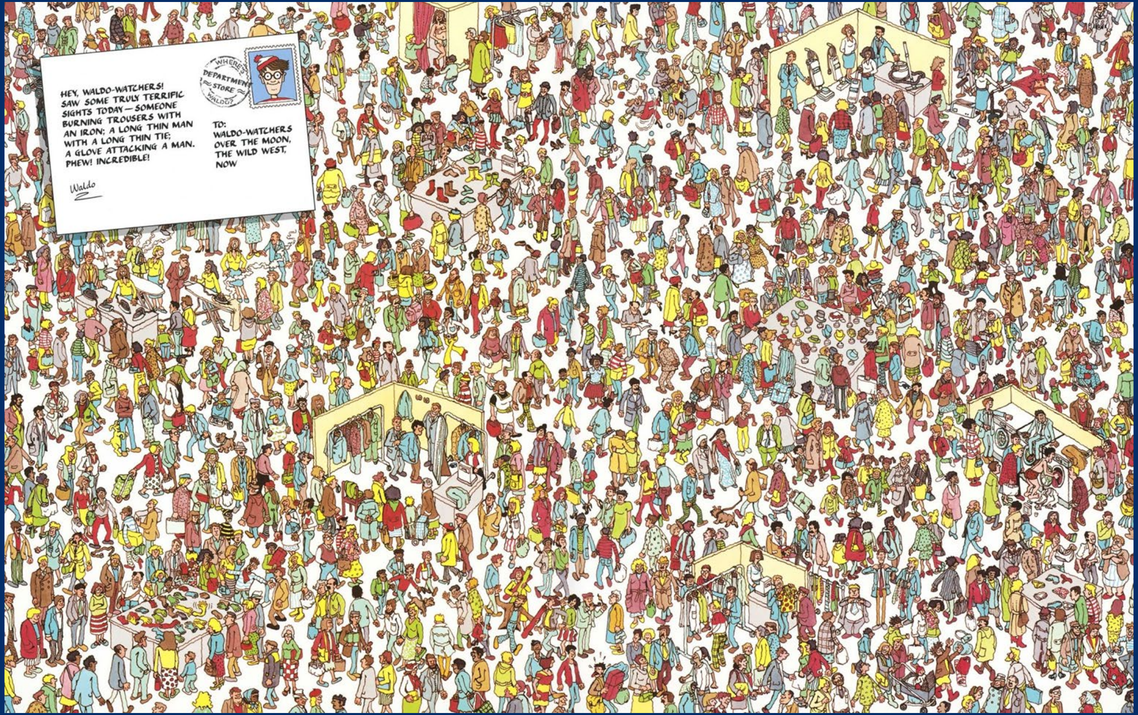
- At every step we amplify the amplitude of the target cell
- After O($\sqrt{N}$) iterations the target amplitude is near optimal
- These class of quantum algorithms are referred to as ***Amplitude Amplification***

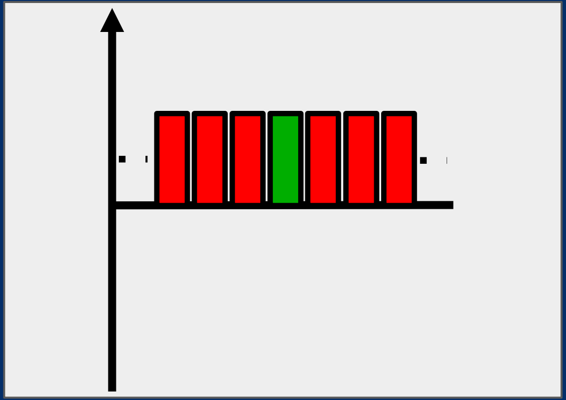
Grover Search Algorithm

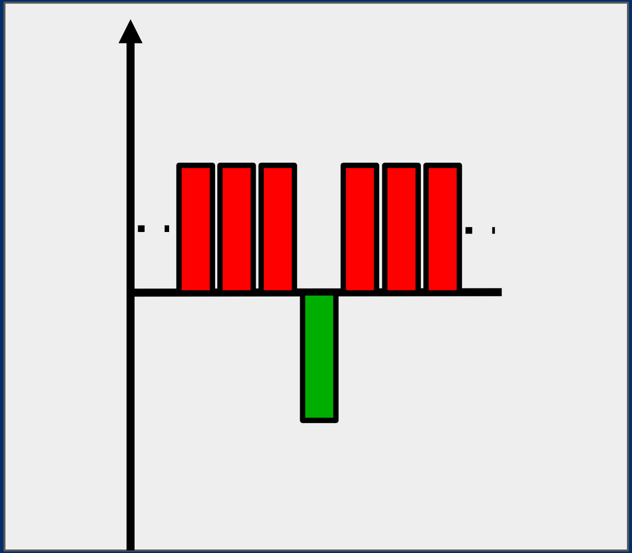
STEP 3: Measure the state, with high probability the result is the right cell.

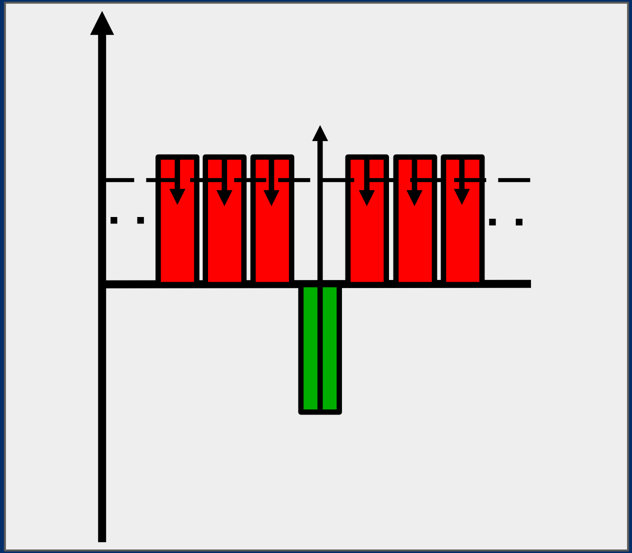


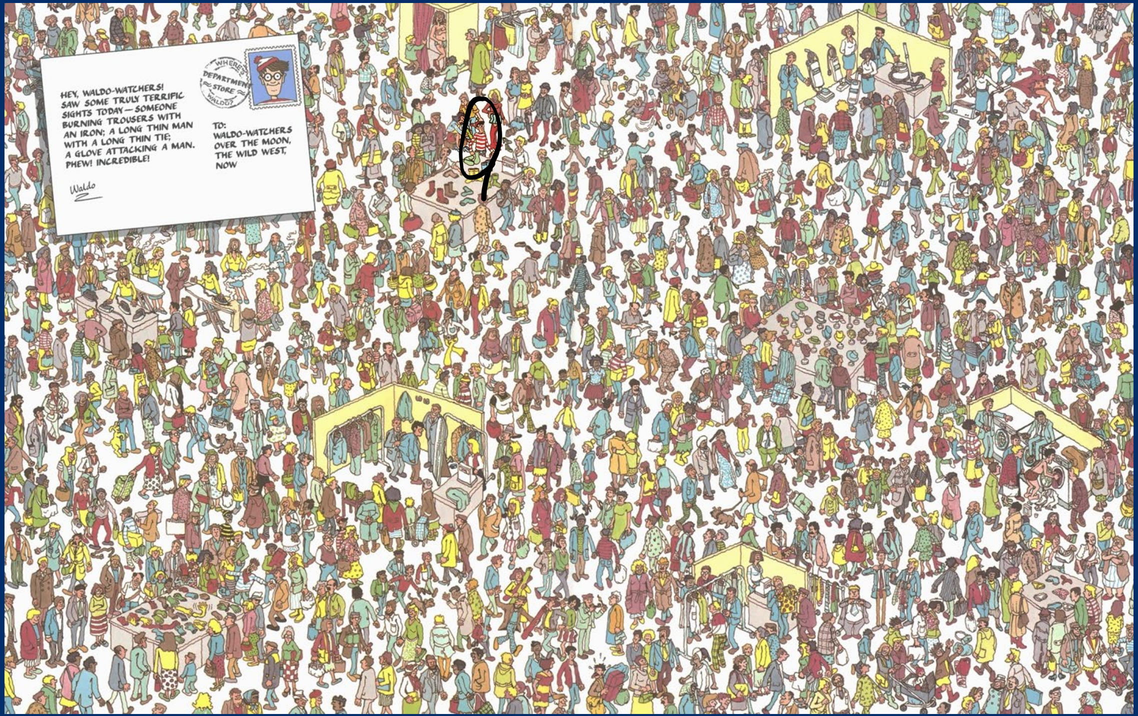
Revisiting "Where's Waldo?"

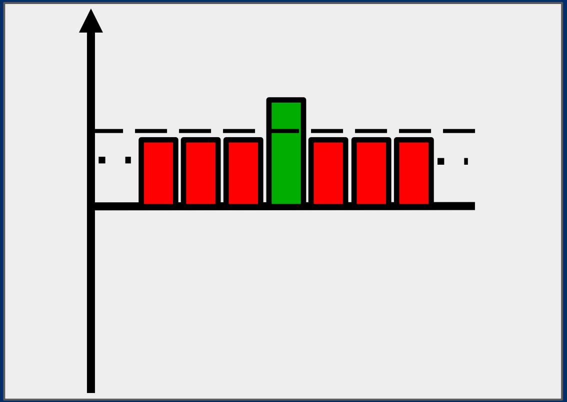


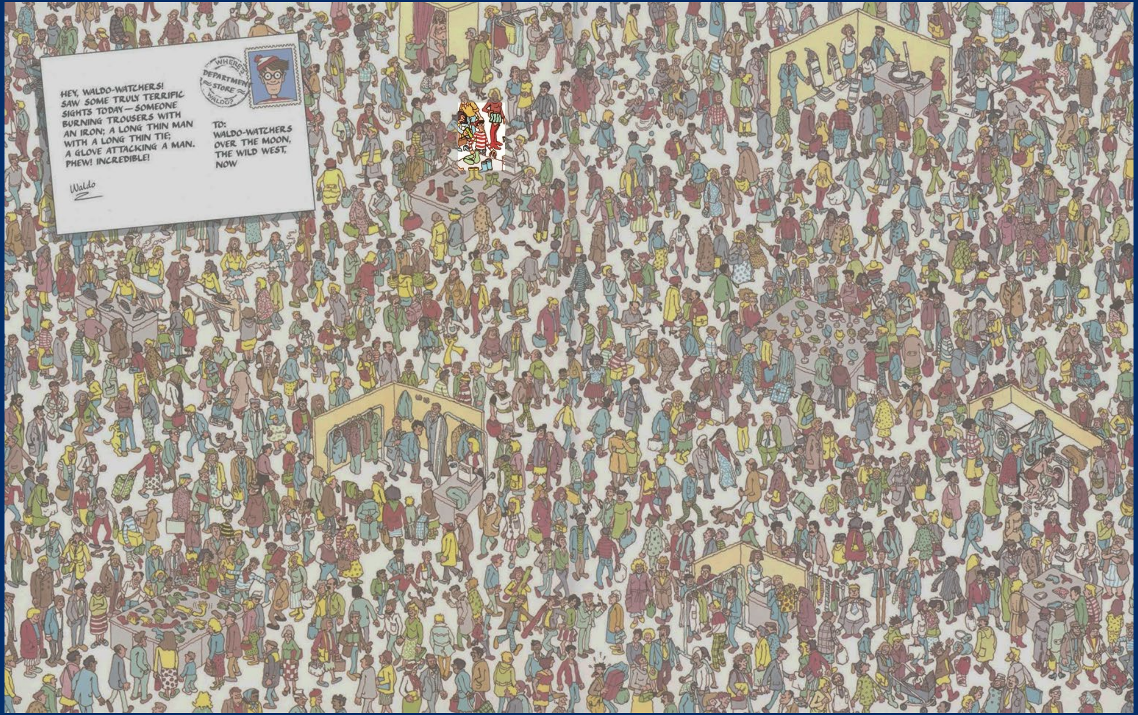


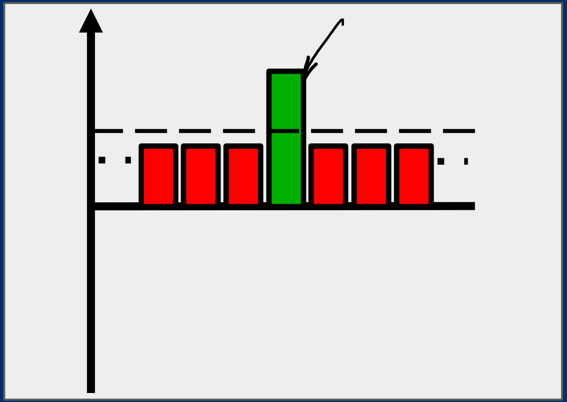


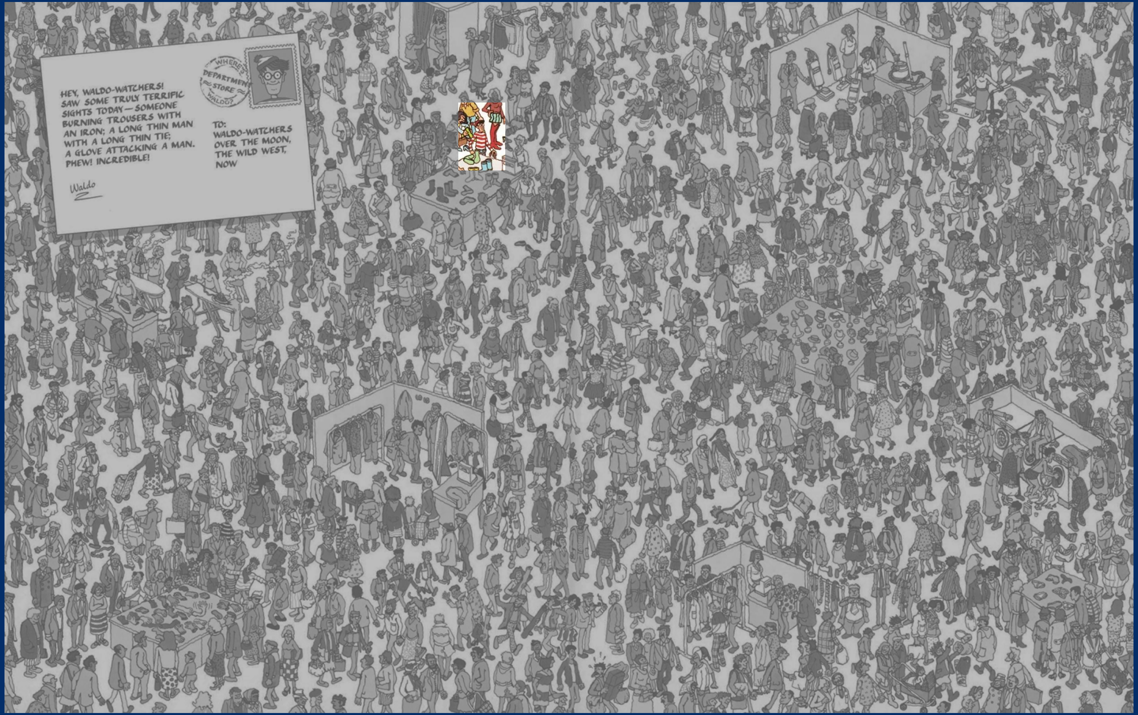



HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC
SIGHTS TODAY—SOMEONE
BURNING TROUSERS WITH
AN IRON; A LONG THIN MAN
WITH A LONG THIN TIE;
A GLOVE ATTACKING A MAN.
PHEW! INCREDIBLE!
Waldo
WHERE'S WALDO? DEPARTMENT STORE
TO:
WALDO-WATCHERS
OVER THE MOON,
THE WILD WEST,
NOW

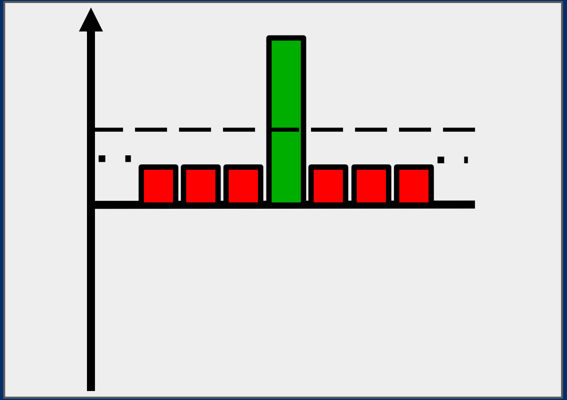



HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC SIGHTS TODAY—SOMEONE BURNING TROUSERS WITH AN IRON; A LONG THIN MAN WITH A LONG THIN TIE; A GLOVE ATTACKING A MAN. PHEW! INCREDIBLE!
Waldo
WHERE'S WALDO? DEPARTMENT STORE
TO: WALDO-WATCHERS OVER THE MOON, THE WILD WEST, NOW

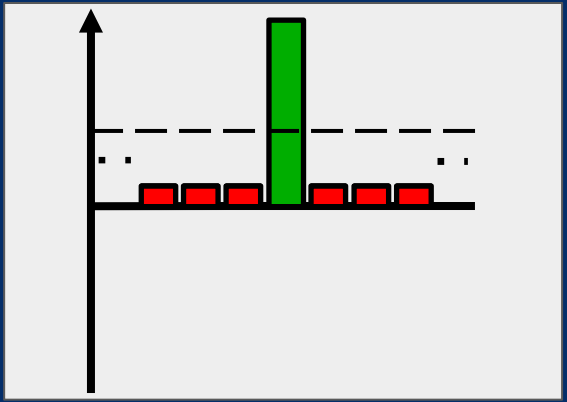




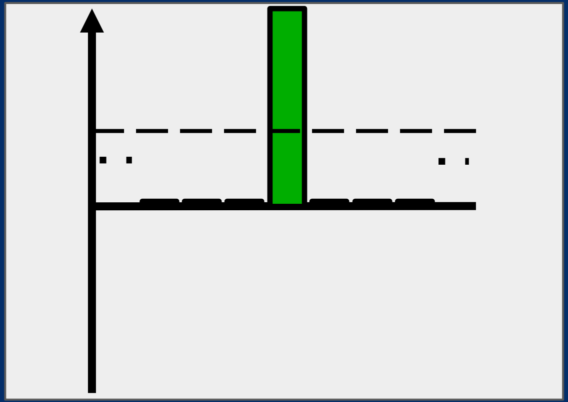
HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC
SIGHTS TODAY—SOMEONE
BURNING TROUSERS WITH
AN IRON; A LONG THIN MAN
WITH A LONG THIN TIE;
A GLOVE ATTACKING A MAN.
PHEW! INCREDIBLE!
Waldo
WHERE'S WALDO? DEPARTMENT STORE
TO:
WALDO-WATCHERS
OVER THE MOON,
THE WILD WEST,
NOW




HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC
SIGHTS TODAY—SOMEONE
BURNING TROUSERS WITH
AN IRON; A LONG THIN MAN
WITH A LONG THIN TIE;
A GLOVE ATTACKING A MAN.
PHEW! INCREDIBLE!
Waldo
TO:
WALDO-WATCHERS
OVER THE MOON,
THE WILD WEST,
NOW




HEY, WALDO-WATCHERS!
SAW SOME TRULY TERRIFIC SIGHTS TODAY—SOMEONE BURNING TROUSERS WITH AN IRON; A LONG THIN MAN WITH A LONG THIN TIE; A GLOVE ATTACKING A MAN. PHEW! INCREDIBLE!
Waldo
TO: WALDO-WATCHERS OVER THE MOON, THE WILD WEST, NOW



Grover Search Algorithm

Applications:

- Speeding up database search
- Speeding up optimal scheduling
- Speeding up mean and median estimation
- Speeding up element counting

State of the art research

- How to efficiently load a classical database to a quantum computer
  - QRAM (quantum RAM)? active area of research
- Optimal construction of the Oracle
- Relation with other quantum algorithms

10 MIN BREAK!

return 2:49 pm EST

for N elements, we will $n = \lceil \log_2(N) \rceil$

with n qubits, we can represent $N = 2^n$

Grover Search Algorithm

How does the quantum search speed-up work? $O(\sqrt{N})$

Let's assume we're searching over 4 elements (with 2 qubits)

$|0\rangle, |1\rangle, |2\rangle, |3\rangle$ are ortho-normal

$(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$

$$\langle i|j\rangle \rightarrow \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

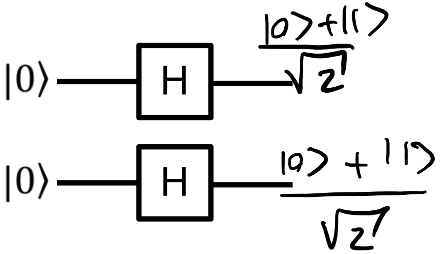
Looking for state $|w\rangle = |2\rangle$

STEP 1: Grover Search Algorithm

Start by assigning equal probability to every cell being the right answer (equal superpos

$$|s\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$$

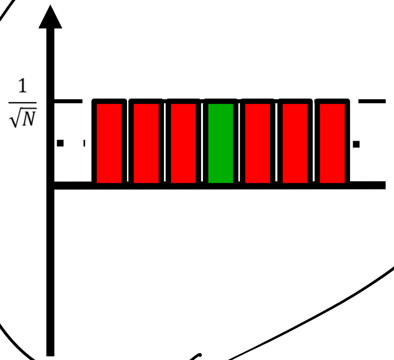
$$P(|0\rangle) = P(|1\rangle) = P(|2\rangle) = P(|3\rangle) = 1/4$$



for the circuit

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{4}}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$= \frac{1}{\sqrt{4}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$$



Review: outer product

Outer product is just a matrix!

ket bra

$$|0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|+\rangle\langle +| = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| + \langle 1|}{\sqrt{2}}\right)$$

$$= \tfrac{1}{2}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|\right) = \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \left(|0\rangle\langle 0|\right)|0\rangle = |0\rangle\left(\underbrace{\langle 0|0\rangle}_{1}\right) = |0\rangle$$

STEP 2: Grover Search Algorithm

Use a blackbox that gives us an output for a given input for free (Orac

$f(x) = 0$ if $x \neq w$ (if x is not the target state)

$f(x) = 1$ if $x = w$ (if x is the target state

$U_w : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$

if $|x\rangle$ is the target : $|x\rangle \rightarrow -|x\rangle$

if $|x\rangle$ is not the target: $|x\rangle \rightarrow |x\rangle$

Now let's define a quantum operation for it:

1-2|w><w|

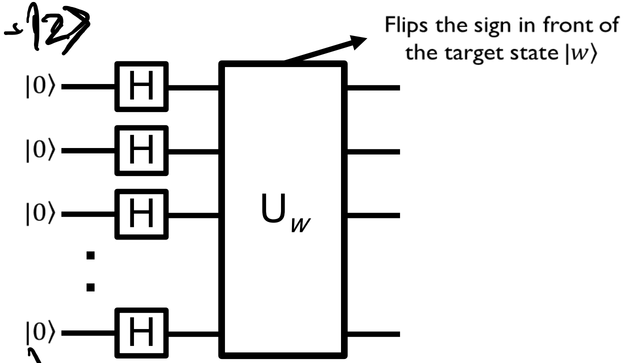
if $w = 2 \rightarrow I - 2|2\rangle\langle 2|$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Grover Search Algorithm

Use quantum interference to transform the superposition so the correct cell has a significantly higher probability

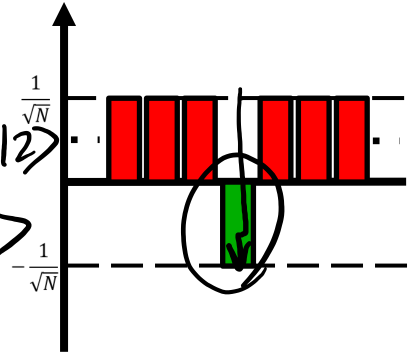
$U_w = I - 2|w\rangle\langle w| \quad |w\rangle = |2\rangle$



$|s\rangle = \frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle)$

$= \frac{1}{\sqrt{4}}|2\rangle + \frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |3\rangle)$

$\rightarrow U_w|s\rangle = I - 2|2\rangle\langle 2| \left(\frac{1}{\sqrt{4}}|2\rangle + \frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |3\rangle)\right)$



$U_w|2\rangle = (I - 2|2\rangle\langle 2|)|2\rangle = |2\rangle - 2|2\rangle\underbrace{\langle 2|2\rangle}_{1} = -|2\rangle$

$U_w|0\rangle = (I - 2|2\rangle\langle 2|)|0\rangle = |0\rangle \cancel{- 2|2\rangle\underbrace{\langle 2|0\rangle}_{0}} = |0\rangle$

$U_w|s\rangle = -\frac{1}{\sqrt{4}}|2\rangle + \frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |3\rangle)$

Grover Search Algorithm

Now let's see how to reverse about the mean in our quantum computer:

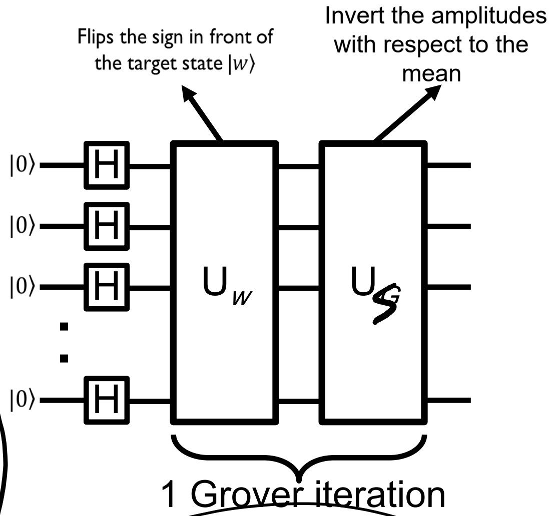
$$|s\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle + |1\rangle + |2\rangle + |3\rangle\right)$$

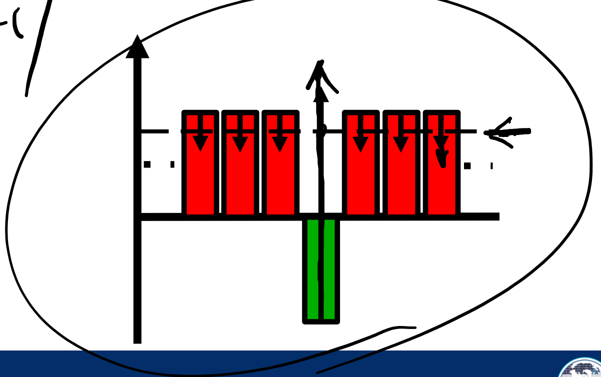
U_s: $2|s\rangle\langle s| - 1$

$$\frac{2}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

$$U_s\left(U_w|s\rangle\right) = \underbrace{\left(U_s U_w\right)}_{U_G}|s\rangle$$

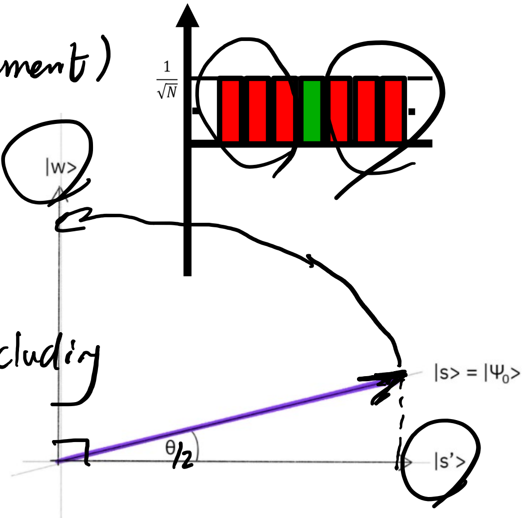
U_G grover operator





Grover Search Algorithm

Let's use these tools to see how the algorithm works (N element)



$$|s\rangle = \frac{1}{\sqrt{N}}\left(|0\rangle + |1\rangle + \cdots + |N-1\rangle\right)$$

let's assume $|w\rangle$ is the target

assume: $|s'\rangle = \frac{1}{\sqrt{N-1}}\left(|0\rangle + |1\rangle + \cdots + |N-1\rangle\right)$ not including $|w\rangle$

$$|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle$$

$\langle w|w\rangle = 1$ $\quad \langle w|s'\rangle = 0$

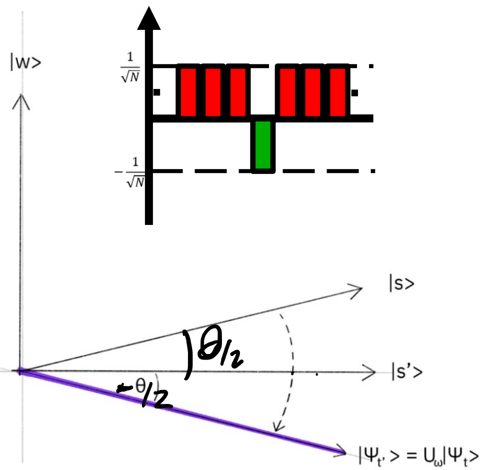
$\langle s'|s'\rangle = 1$

$$\sin(\theta/2) = \frac{1}{\sqrt{N}} \rightarrow \theta/2 = \sin^{-1}\left(\frac{1}{\sqrt{N}}\right)$$

if θ is small $\rightarrow \theta/2 = \frac{1}{\sqrt{N}}$

Grover Search Algorithm

After applying the Oracle operator $|s\rangle = \frac{1}{\sqrt{N}}|w\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle$



$$U_w|s\rangle = -\frac{1}{\sqrt{N}}|w\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle$$

$$\sin(\theta'/2) = -\frac{1}{\sqrt{N}}$$

angle rotated from $\theta/2 \rightarrow -\theta/2$

Grover Search Algorithm

After applying U_s

we rotate around the $|s\rangle$ state

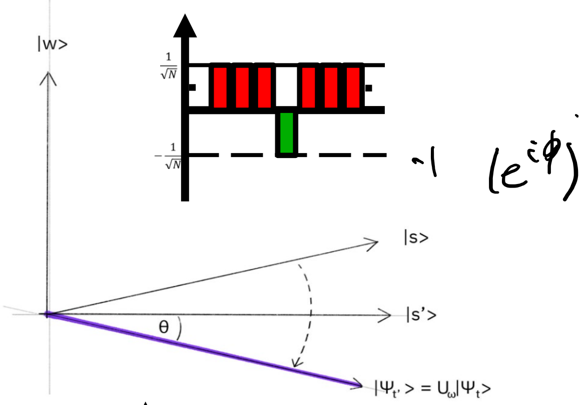
for the first iteration:

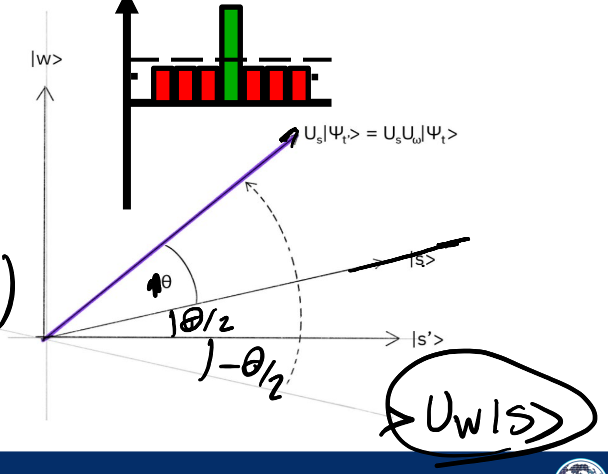
$$U_s \rightarrow -\theta/2 \rightarrow \theta + \theta/2$$

for the entire Grover iteration

$$\theta/2 \rightarrow \theta/2 + \theta$$

~~for~~ after t iterations $\theta_t = (t + 1/2)\,\theta \rightarrow 2\sin^{-1}\left(\frac{1}{\sqrt{N}}\right)$





Grover Search Algorithm

Algorithm runtime analysis: after t iteractions, the probability of measuring the $|w\rangle$ state is

$$\sin^2\left((t+1/2)\theta\right) \rightarrow \text{optimal when } (t+1/2)\theta = \pi/2$$

$$\theta \approx \frac{2}{\sqrt{N}}$$

$$\Rightarrow \quad t_{opt} \approx \pi/4 \sqrt{N} \rightarrow O(\sqrt{N})$$

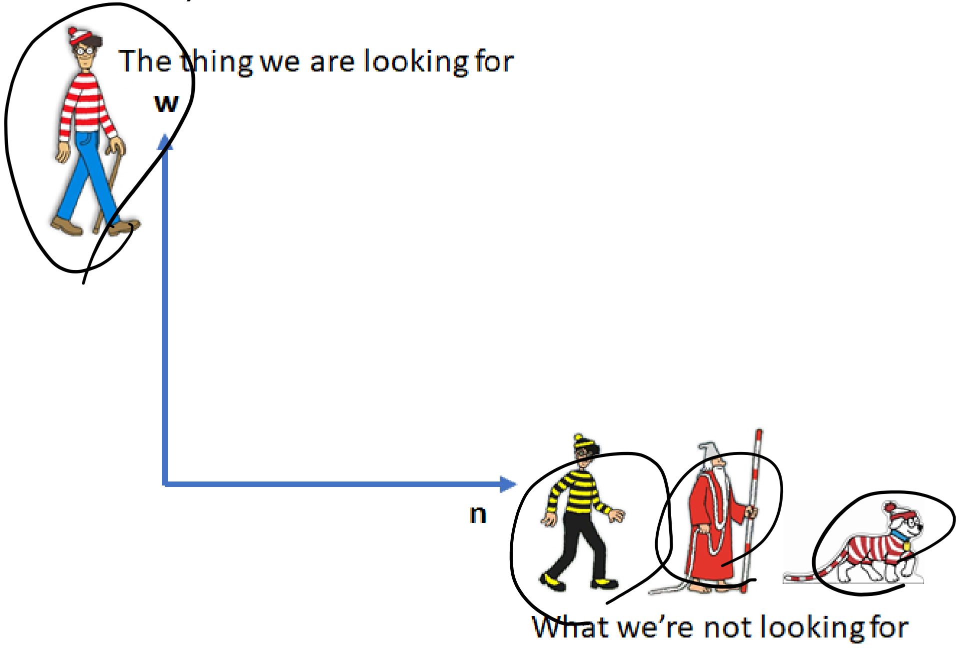
→ optimal runtime of Grover search is $O(\sqrt{N})$

Grover Search Algorithm

We'll first divide all the possibilities into two sets:

- What we're looking for (w for winner or Waldo)
- What we're not looking for (n for not)

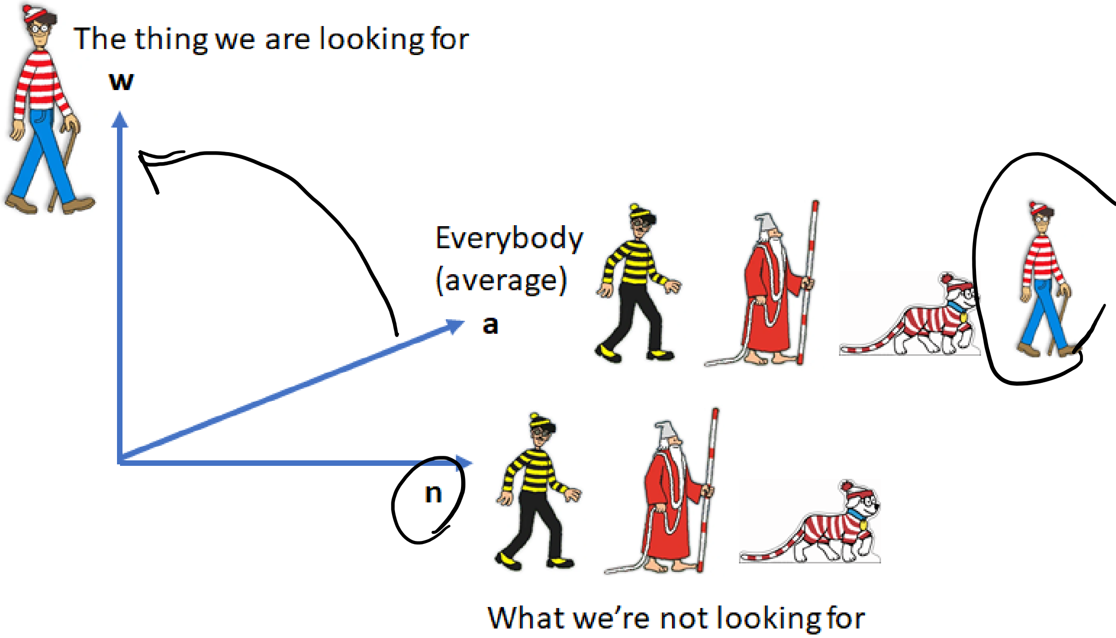
If we imagine these two sets as vectors, they'll be orthogonal, because they have nothing in common.



Grover Search Algorithm

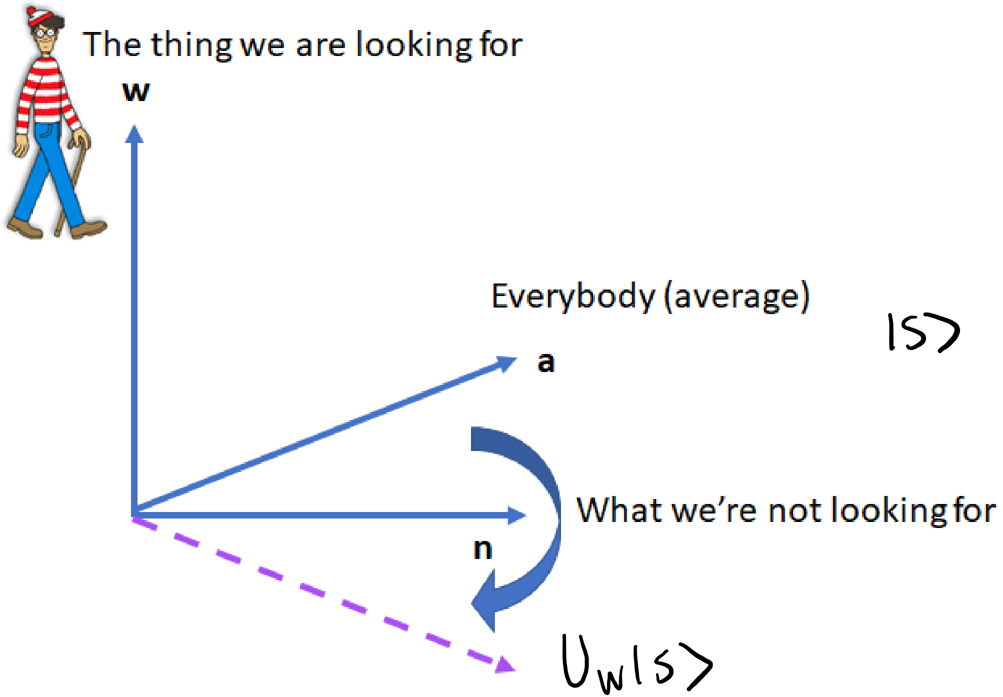
Now we can plot the vector that represents all of the choices, or the average (**a** for average).

This vector will be closer to **n** than **w** because it's a little bit Waldo but mostly everyone else. It's the **average**.

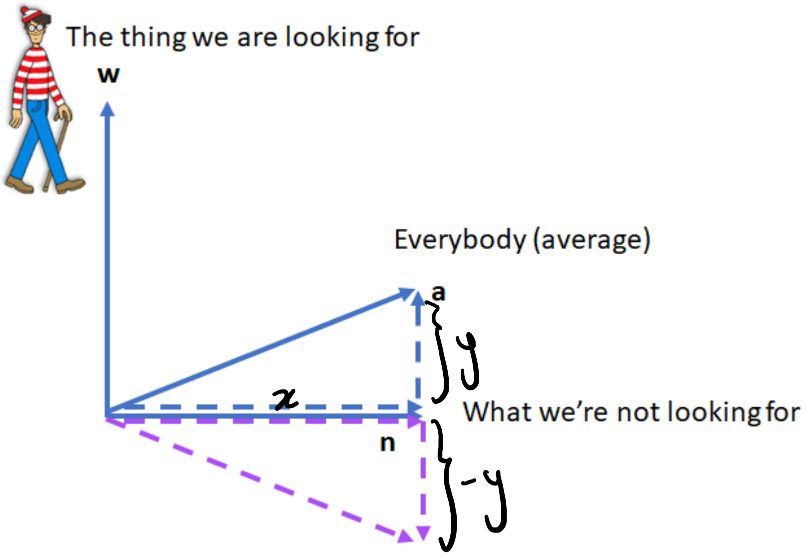


Grover Search Algorithm

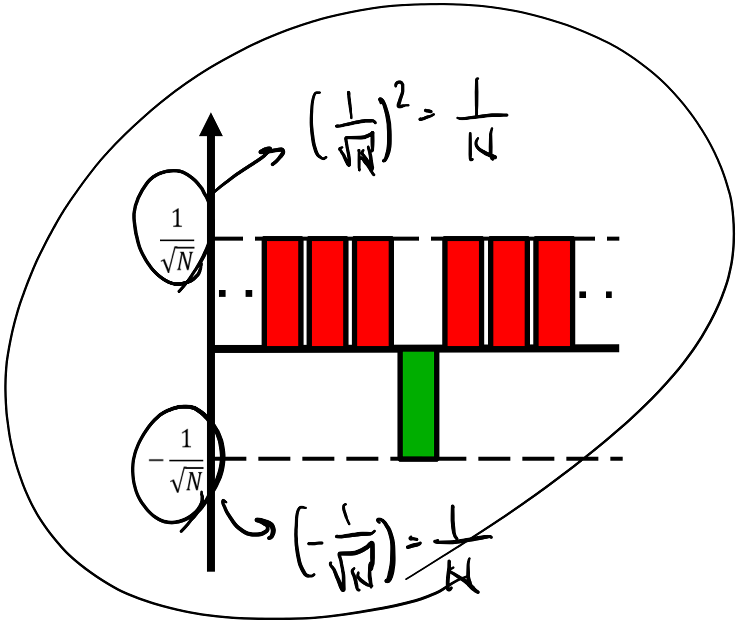
The oracle will flip **a** over **n**.



The oracle will flip **a** over **n**.



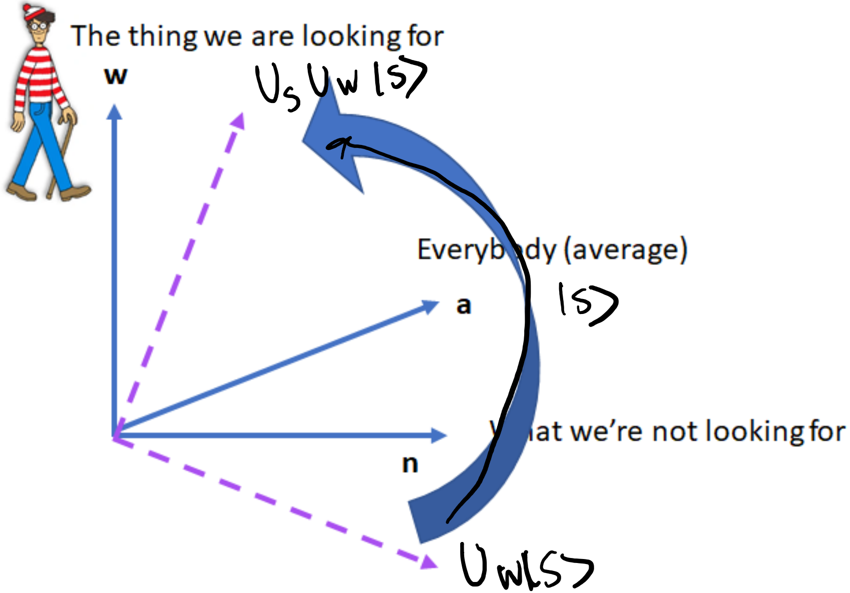
We can see that only the vertical component (or the Waldo component) actually flipped.

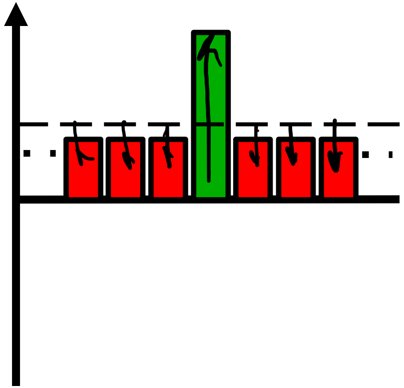


That's how we get this graph - only the target flipped!

Grover Search Algorithm

And then our operator will flip this new vector over the average (a).





This makes our vector much closer to Waldo. So if we measure it, we're more likely to get Waldo.