Photo by NICO BHLR on Unsplash

Grover's Algorithm
(quantum search)

ECE 592/CSC 591 – Fall 2019

Finding a Solution

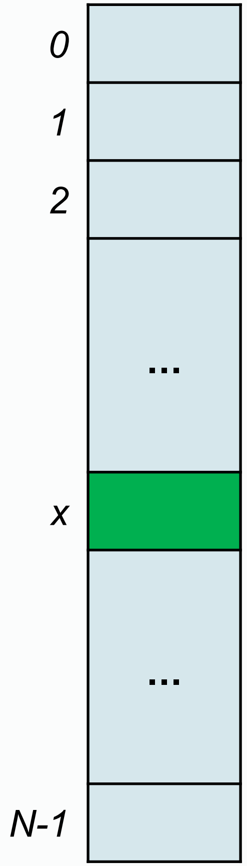
Set of values {0, ..., N-1}

Predicate (black box) function P: {0, ..., N-1} ⟶ {0, 1}

Find *x* such that P(*x*) = 1

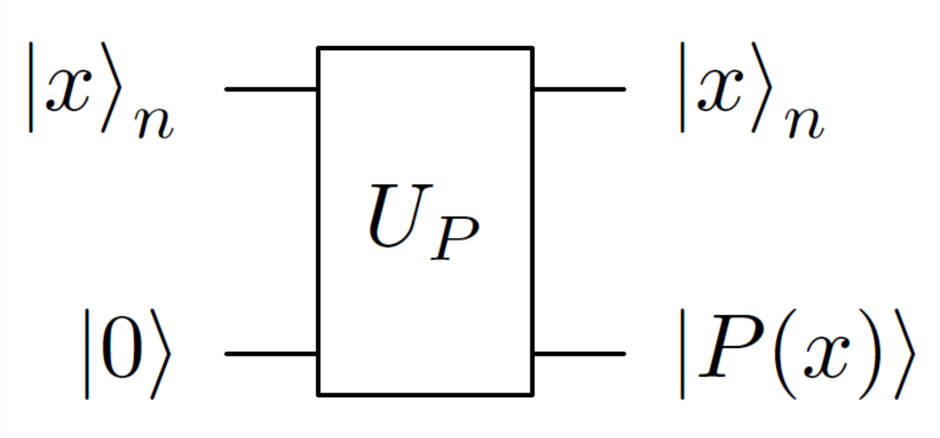
Values are "unstructured," so classically requires ~N/2 trials

Grover finds the solution with $O(\sqrt{N})$ evaluations of P



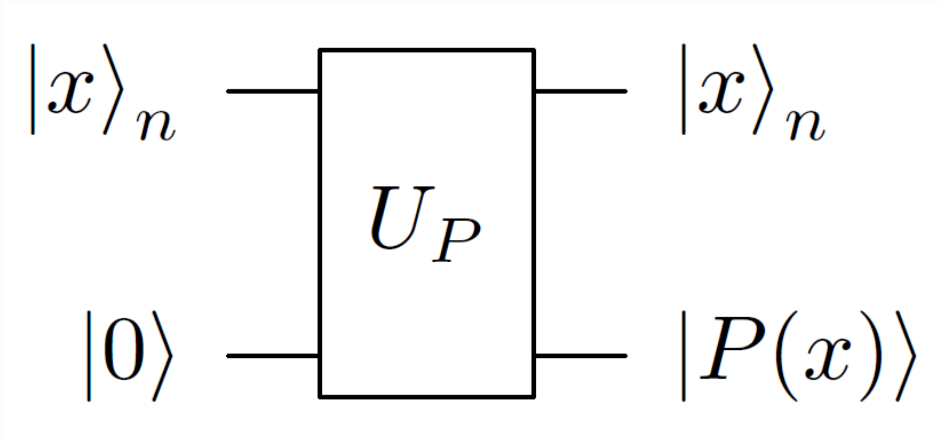
$N = 2^n$
Only 1 solution (for now)
P is efficient to execute, but not so structured as to give classical advantage

The Oracle: U_P



P(x) must be efficient to compute.
Exponential in N will negate advantage

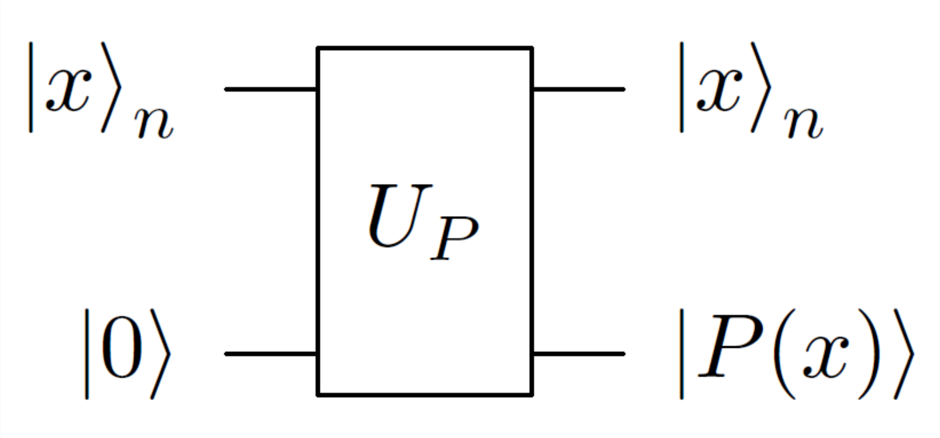
The Oracle: U_P



If we know P(x), don't we already "know" x?

P(x) is a checker function. It might be easy to verify that an input satisfies P(x), but hard to find such an input.
Examples: factoring, SAT, ...

The Oracle: U_P

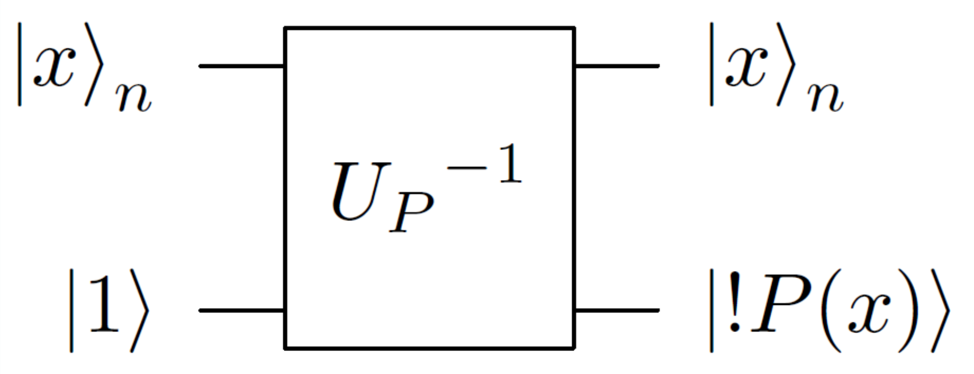


Can't we just calculate P(x) on all inputs at once?

Yes, but we only get one output when we measure.
This is equivalent to random sampling in the classical version.

When n is large, need lots of trials (shots) to be confident that we will see P(x) = 1.

The Oracle: U_P

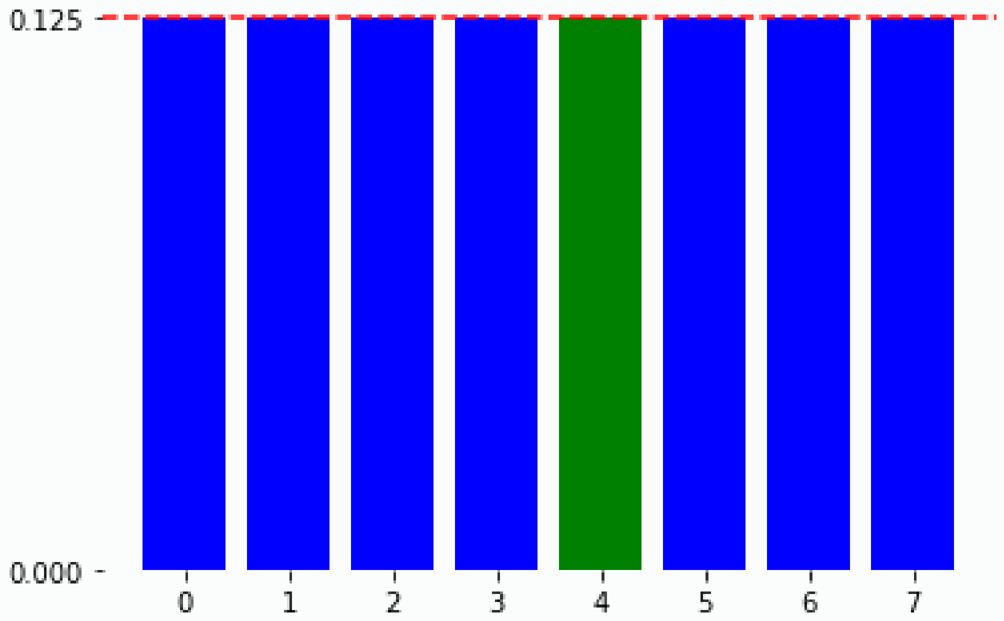


Can we run it in reverse?

Yes, but there's no advantage.
Can't "pin" output to 0, so still sampling from all possible outputs.

Compare to quantum annealing, where setting output P(x) = 1 as a low-energy state can improve odds of finding solution.

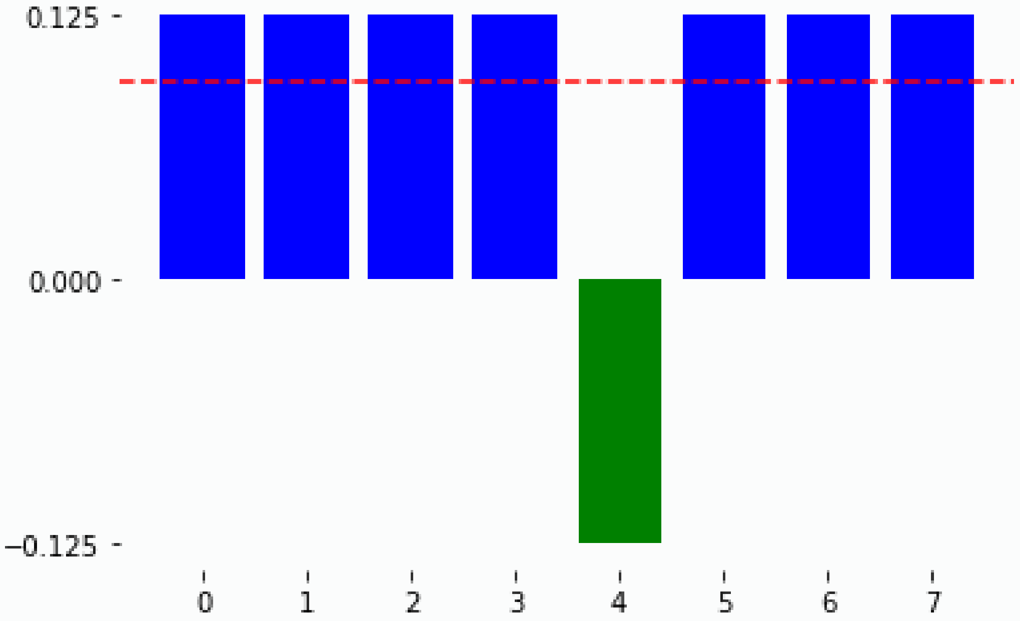
Amplitude Amplification



Input = equal superposition.
All amplitudes are equal, so chances of measuring solution (green) is the same as any other.

Need to increase solution amplitude and reduce others.

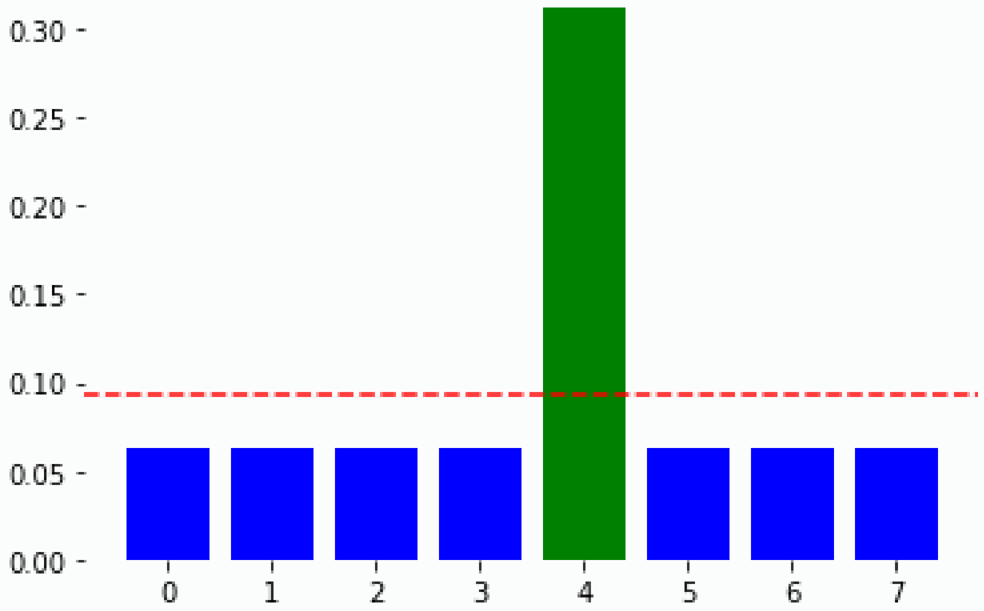
Amplitude Amplification



Step 1: Inject relative phase for solution state.

Note that mean (dotted line) has changed.

Amplitude Amplification

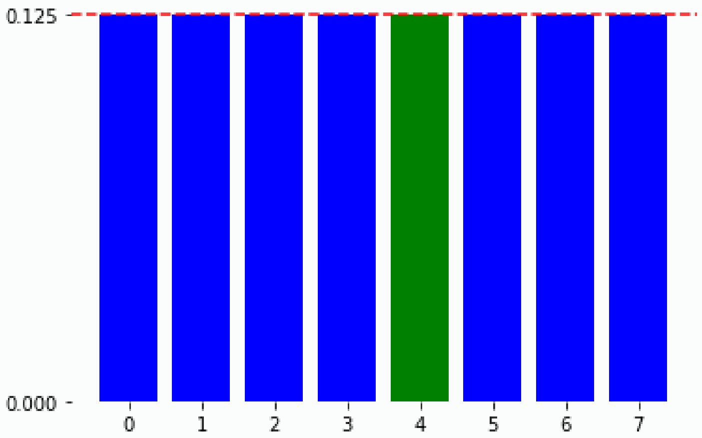


Step 2: Invert around the mean.

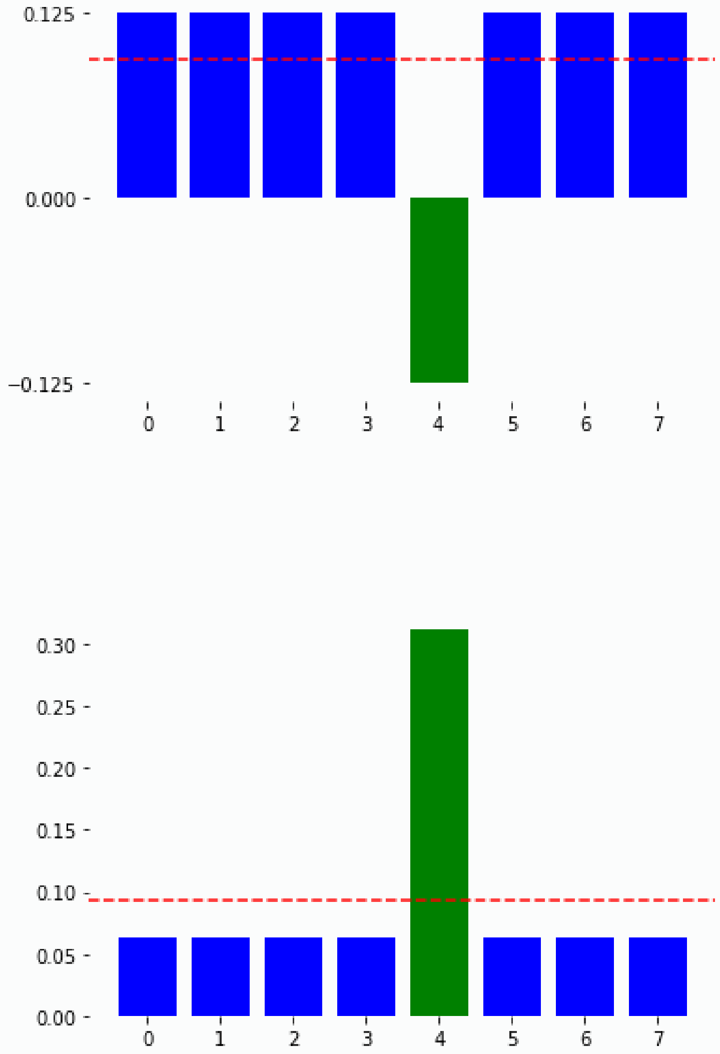
$$a_i \to 2A - a_i$$

This is the "Grover iteration." We do it $O(\sqrt{N})$ times.

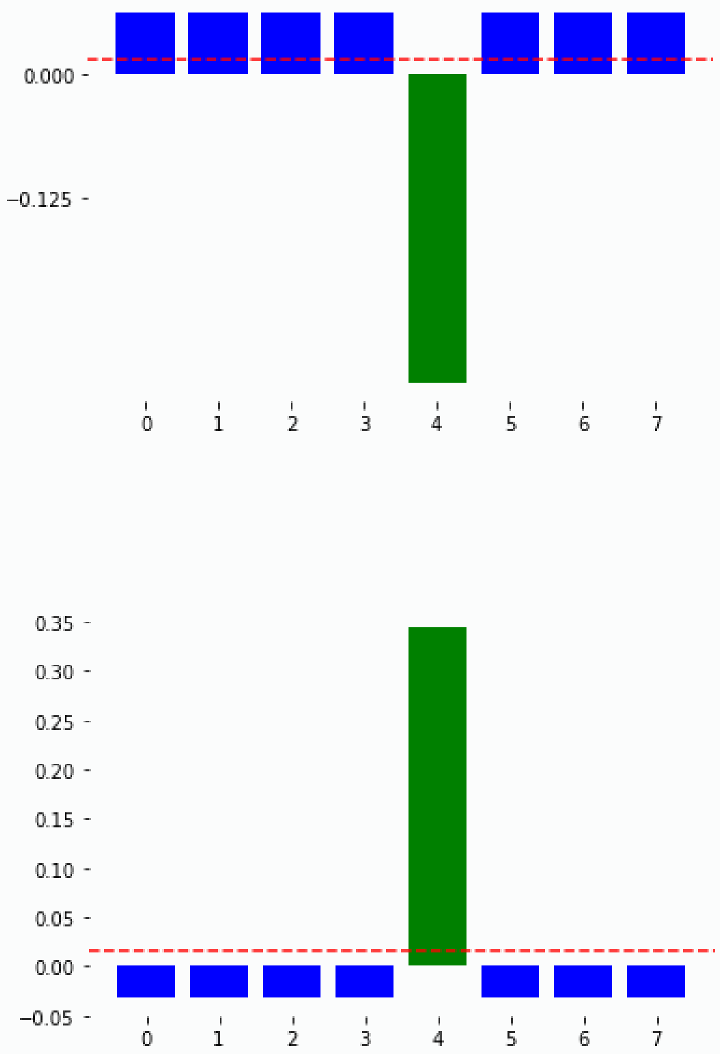
Start



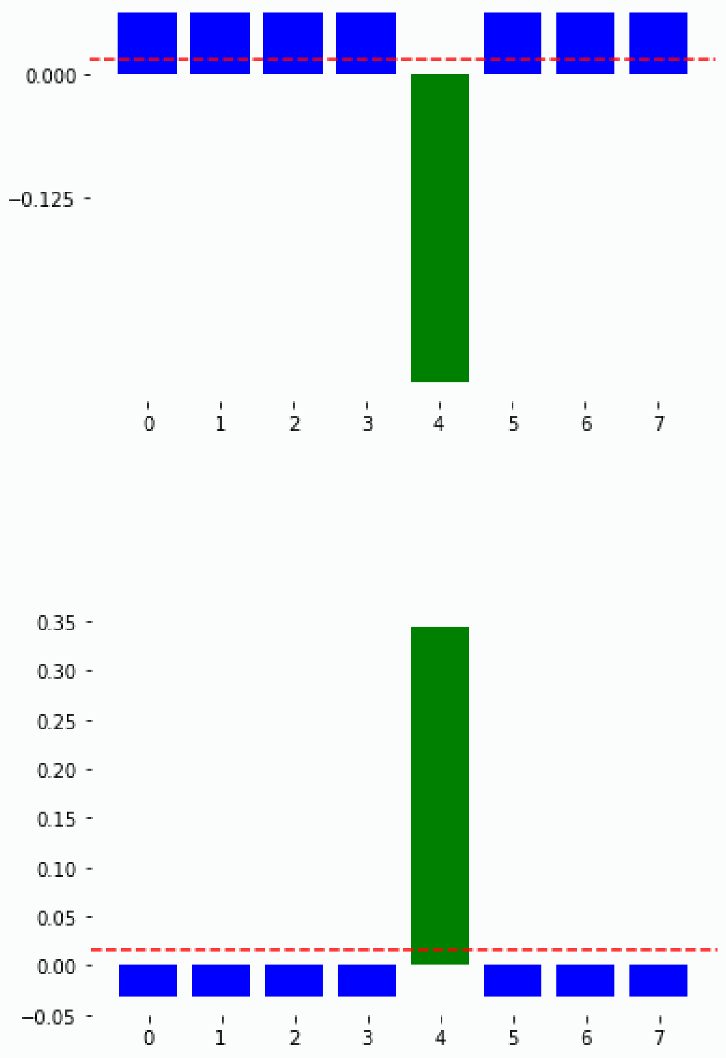
Iteration 1



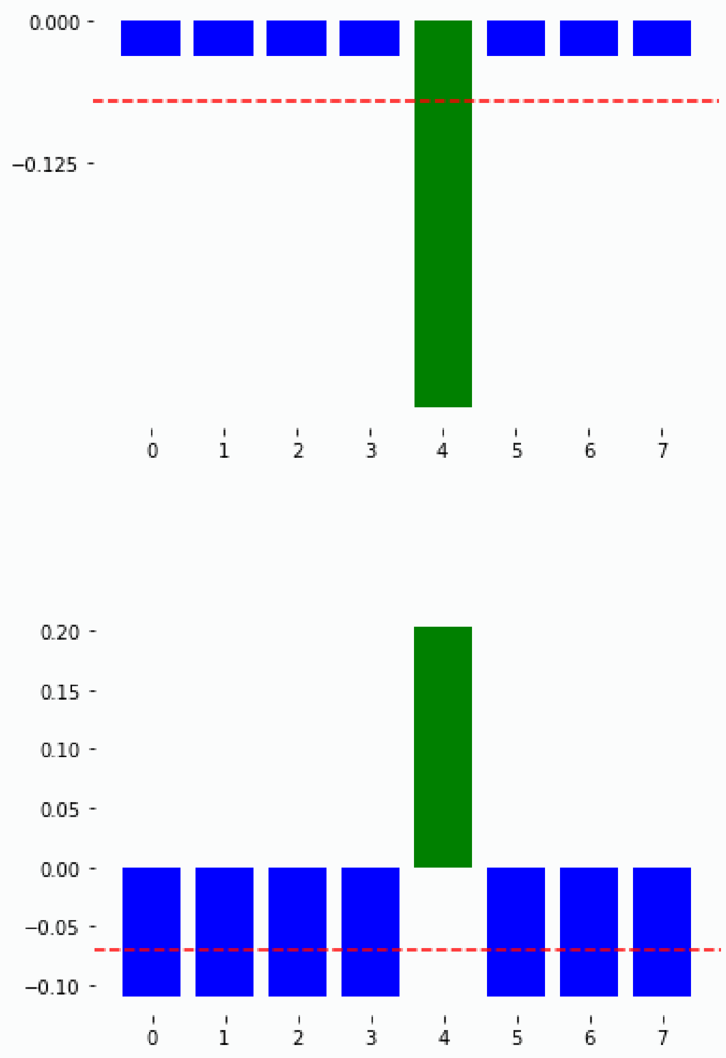
Iteration 2



Iteration 2



Iteration 3

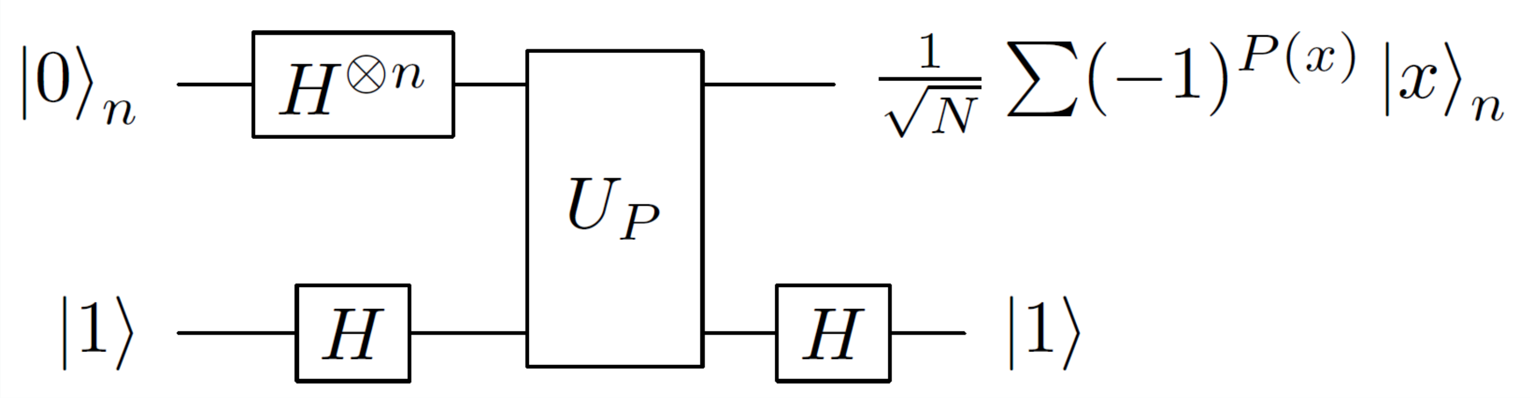


If you do too many iterations, the amplitude reduces.

Here comes the math...

Step 1: Phase change

We already know how to do this…



Step 1: Phase change

$G = \{x | P(x)\}$ — good elements, $|G| << N$

$B = \{x | \neg P(x)\}$ — bad elements

$$|\psi_G\rangle = \frac{1}{\sqrt{|G|}} \sum_{x \in G} |x\rangle$$

$$|\psi_B\rangle = \frac{1}{\sqrt{|B|}} \sum_{x \notin G} |x\rangle$$

$$|\psi\rangle = W|0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{2^n-1} |x\rangle = g_0 |\psi_G\rangle + b_0 |\psi_B\rangle$$

$$g_0 = \sqrt{|G|/N}, b_0 = \sqrt{|B|/N}$$

phase change

$$S_G^{\pi} |\psi\rangle = -g_0 |\psi_G\rangle + b_0 |\psi_B\rangle$$

Step 2: Inversion about the Mean

$$\sum_{i=0}^{N-1} a_i \left|x_i\right\rangle \to \sum_{i=0}^{N-1} (2A - a_i) \left|x_i\right\rangle$$

$$2A - a_i = \frac{2}{N} \sum_i a_i - a_i$$

$$D = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{bmatrix}$$

Step 2: Inversion about the Mean

$$D = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{bmatrix} = -WS_0^\pi W$$

❶

$$S_0^\pi = \begin{bmatrix} -1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots \\ 0 & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix}$$

❷

$$R = \begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots \\ 0 & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix}, \quad \text{and } S_0^\pi = I - R$$

❸ Since $R_{ij} = 0$ for $i \neq 0$ or $j \neq 0$,

$$(WRW)_{ij} = W_{i0}R_{00}W_{0j} = \frac{2}{N}$$

❹

$$-WS_0^\pi W = WRW - I = D$$

Step 2: Alternate Description

$$D = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{bmatrix} = W(2\left|0\right\rangle\left\langle 0\right| - I)W = 2\left|\psi\right\rangle\left\langle\psi\right| - I$$

$$R = \begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots \\ 0 & \cdots & \cdots & 0 \\ 0 & \cdots & 0 & 0 \end{bmatrix}$$

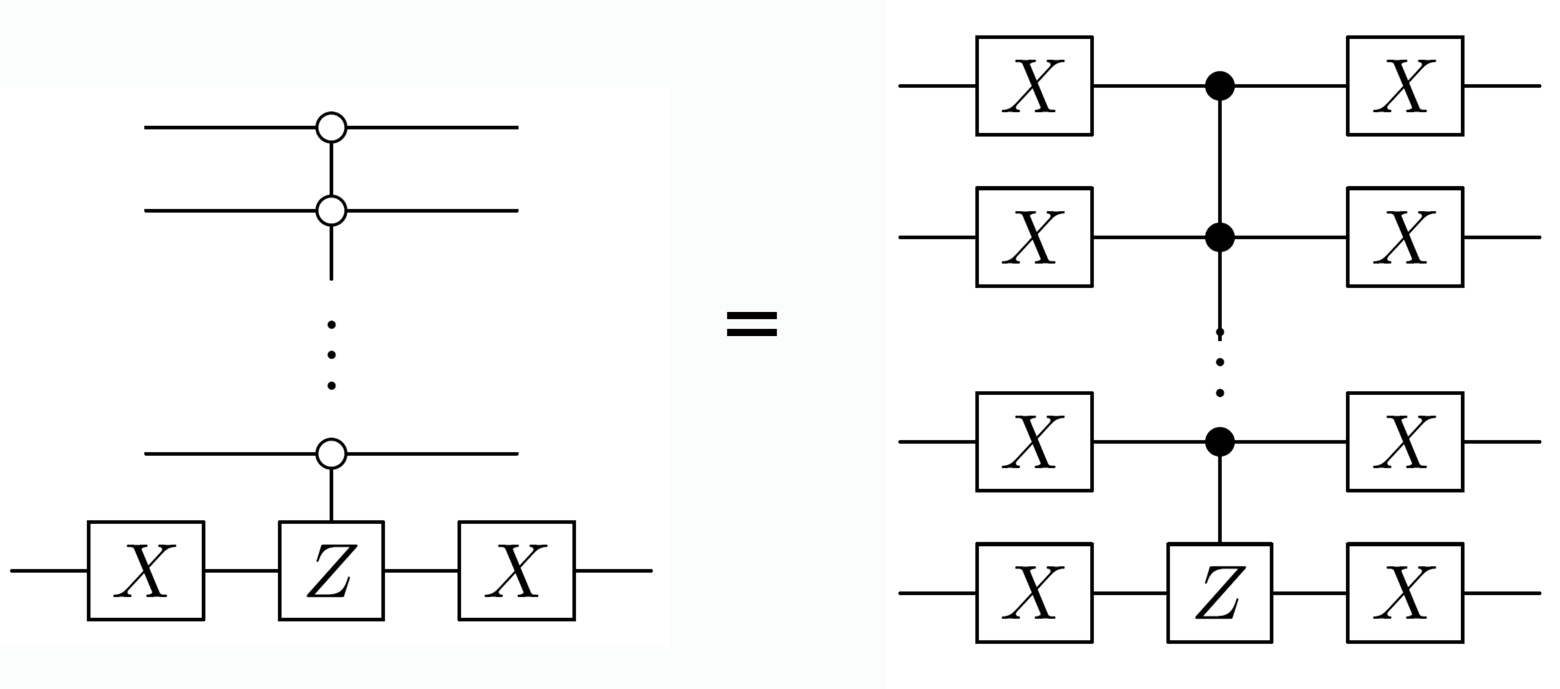
$$\begin{bmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{bmatrix}$$

Implementation

2nd phase change

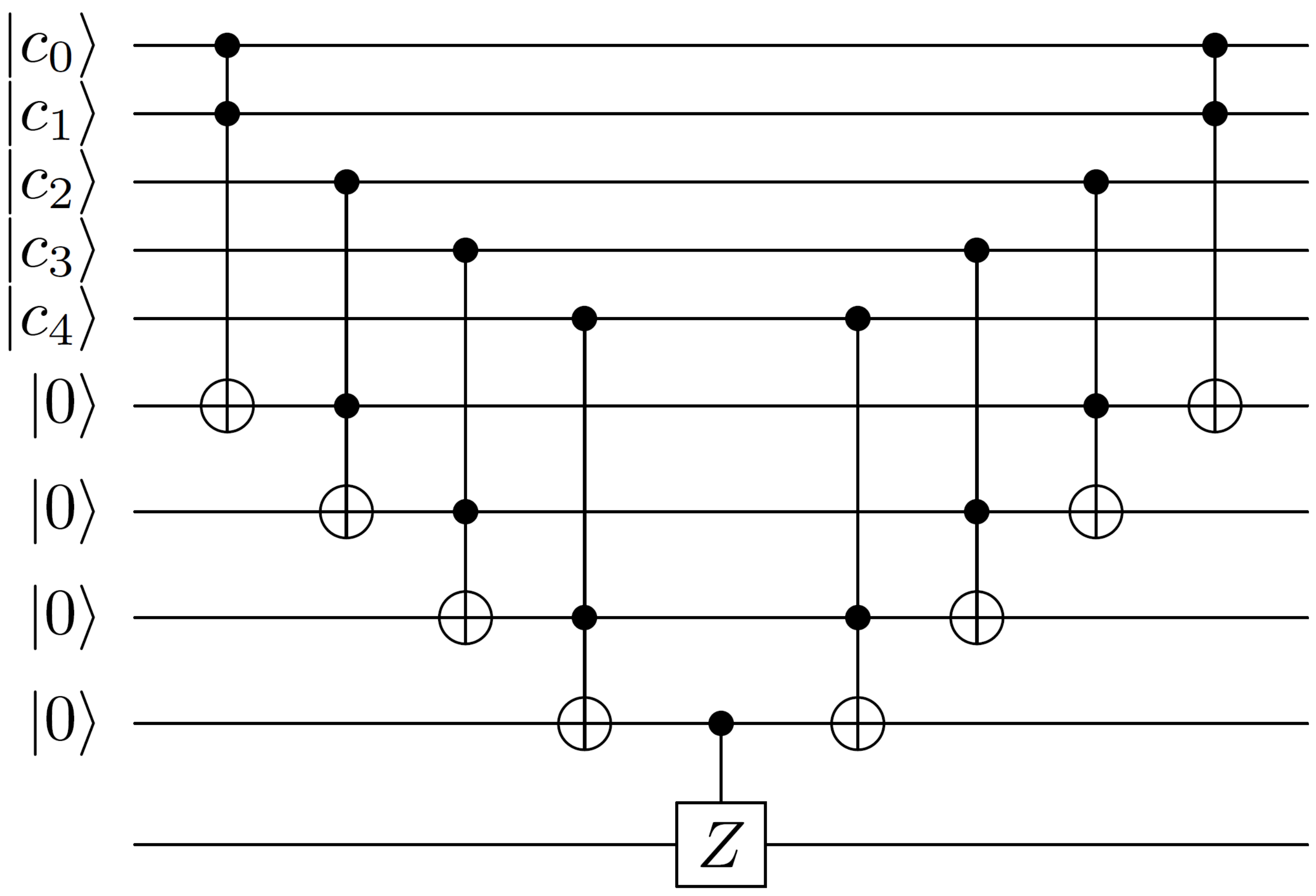
$$D = -W S_0^{\pi} W$$

Ignore the global phase (-) and implement the selective phase change S_0^{π}.

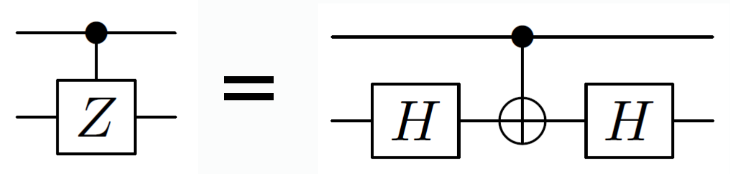


By adding and removing X, can change phase for any single pattern of 00..11..

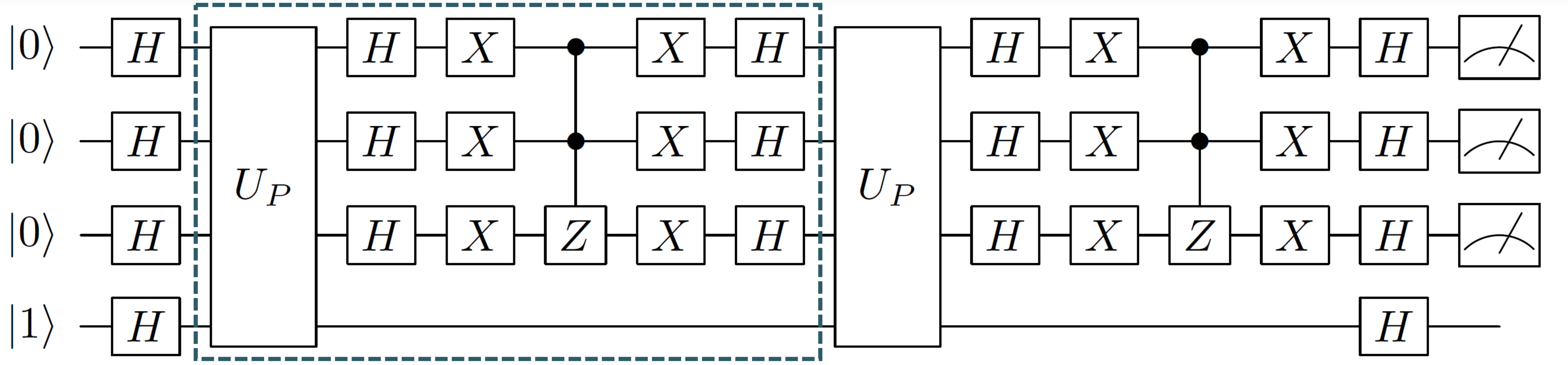
Multi-Controlled Gate



Not cheap!



3 qubits, 2 iterations



Here comes more math...

How many iterations?

$$\boxed{DS_G^{\pi} : g_i \left|\psi_G\right\rangle + b_i \left|\psi_B\right\rangle \rightarrow g_{i+1} \left|\psi_G\right\rangle + b_{i+1} \left|\psi_B\right\rangle}$$

❶ $$S_G^{\pi} : g_i \left|\psi_G\right\rangle + b_i \left|\psi_B\right\rangle \rightarrow -g_i \left|\psi_G\right\rangle + b_i \left|\psi_B\right\rangle$$

To the average A_i, the term $-g_i \left|\psi_G\right\rangle$ contributes $|G|$ amplitudes $\dfrac{-g_i}{\sqrt{|G|}}$ and $b_i \left|\psi_B\right\rangle$ contributes $|B|$ amplitudes $\dfrac{b_i}{\sqrt{|B|}}$

❷ $$A_i = \frac{\sqrt{|B|}b_i - \sqrt{|G|}g_i}{N}$$

How many iterations?

$$D : -g_i \left|\psi_G\right\rangle + b_i \left|\psi_B\right\rangle \quad \rightarrow \quad \sum_{x\in G}\left(2A_i + \frac{g_i}{\sqrt{|G|}}\right)|x\rangle + \sum_{x\in B}\left(2A_i - \frac{b_i}{\sqrt{|B|}}\right)|x\rangle$$

$$= \quad \left(2A_i\sqrt{|G|} + g_i\right)\left|\psi_G\right\rangle + \left(2A_i\sqrt{|B|} - b_i\right)\left|\psi_B\right\rangle$$

$$\boxed{g_{i+1} = 2A_i\sqrt{|G|} + g_i, \quad b_{i+1} = 2A_i\sqrt{|B|} - b_i}$$

How many iterations?

Let t be the probability that a random value in $\{0, \ldots, N-1\}$ satisfies P. Then $t = |G|/N$ and $1 - t = |B|/N$.

$$A_i\sqrt{|G|} = \frac{\sqrt{|B||G|}b_i - |G|g_i}{N} = \sqrt{t(1-t)}b_i - tg_i$$

$$A_i\sqrt{|B|} = \frac{|B|b_i - \sqrt{|B||G|}g_i}{N} = (1-t)b_i - \sqrt{t(1-t)}g_i$$

❸

$$\boxed{\begin{aligned} g_{i+1} &= 2A_i\sqrt{|G|} + g_i &&= (1-2t)g_i + 2\sqrt{t(1-t)}b_i \\ b_{i+1} &= 2A_i\sqrt{|B|} - b_i &&= (1-2t)b_i + 2\sqrt{t(1-t)}g_i \\ g_0 &= \sqrt{t} \\ b_0 &= \sqrt{1-t} \end{aligned}}$$

How many iterations?

A solution to these equations is:

$$g_i = \sin((2i+1)\theta)$$

❹

$$b_i = \cos((2i+1)\theta)$$

with $\sin\theta = \sqrt{t} = \sqrt{|G|/N}$

$$g_i = \sin((2i+1)\theta) \approx 1$$

$$(2i+1)\theta \approx \frac{\pi}{2}$$

$$i \approx \frac{\pi}{4}\left(\frac{1}{\theta}\right)$$

For $|G| << N$, $\sqrt{|G|/N} = \sin\theta \approx \theta$

$$i \approx \frac{\pi}{4}\sqrt{N/|G|}$$

For 3 qubits: $\frac{\pi}{4}\sqrt{8} = 2.22$

Observations

Observations

- Grover's algorithm is optimal. No quantum algorithm can solve exhaustive search better than $O(\sqrt{N})$.
- If more than one solution ($|G| > 1$), still works. Number of iterations is reduced accordingly: $\frac{\pi}{4}\sqrt{N/|G|}$.
- Approaches to solve if number of solutions is unknown.
- Can slightly tweak to get a guaranteed (not probabilistic) solution. With NISQ, probably not worth it.

Amplitude Amplification

- Instead of using W on input data, compute $U|0\rangle$ with some transform that provides a better starting point.

- Iterations = $\frac{\pi}{4}\sqrt{1/t}$

Practical Considerations

- Efficiency of U_P
- If there is structure in solution space, classical algorithms can take advantage.
  - Example: searching an alphabetically sorted list.
- If solutions cannot be enumerated easily,
  can take more time to set up quantum state than run the algorithm.
- Amplitude amplification has been shown to provide speedup for some algorithms. Only quadratic, so if algorithm requires exponential calls to U_P, it's still exponential.