Grover’s Algorithm



A lecture series by IQM and HS RM

Authors: Stefan Seegerer, Mikio Nakahara

Last Updated 06/2025

www.meetiqm.com

In this session, we will learn Grover's algorithm to solve search and 3SAT problems

The search problem

Problem definition

- Suppose you have a telephone directory of N phone numbers and are asked to find an owner of a particular number.
  - Assume the numbers don't have any structure that help you search, e.g., they're not in order.
- Imagine labeling the first number 00…000, the second 00..001, etc.
  - We check if a label z is the correct "target" number x using an oracle $f(z)$ prepared by a friend:

$$f(z) = \begin{cases} 1 & \text{if } z = x \\ 0 & \text{if } z \neq x \end{cases}$$

- How many times do you need to use the oracle?
  - If you check each line one by one, it takes $O(N)$ uses (classical search).
  - There is a quantum algorithm, Grover's algorithm, which takes $O(\sqrt{N})$ uses!

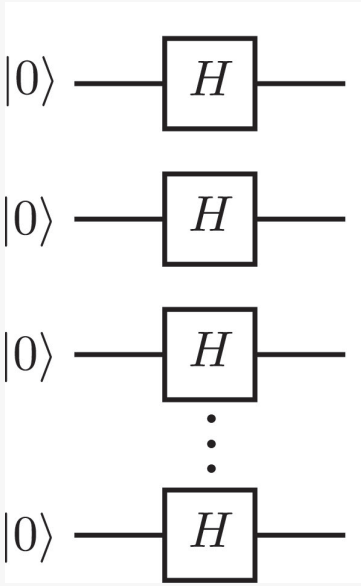
Grover’s algorithm

Grover's Algorithm

- A quantum algorithm called Grover's algorithm finds solutions by using the oracle $O(\sqrt{N})$ times.
- Assume that there is a unique z that satisfies $f(z) = 1$ for simplicity.

- For illustration, we're going to assume that we are searching through $16 = 2^4$ phone numbers labeled 0000, 0001, …, 1111, and that our target number is 1011.
  - We need a "register" of 4 qubits. Our goal is to make the qubits produce the target 1011.
  - Assume the qubits all start in the $|0\rangle$ state.

Grover's Algorithm

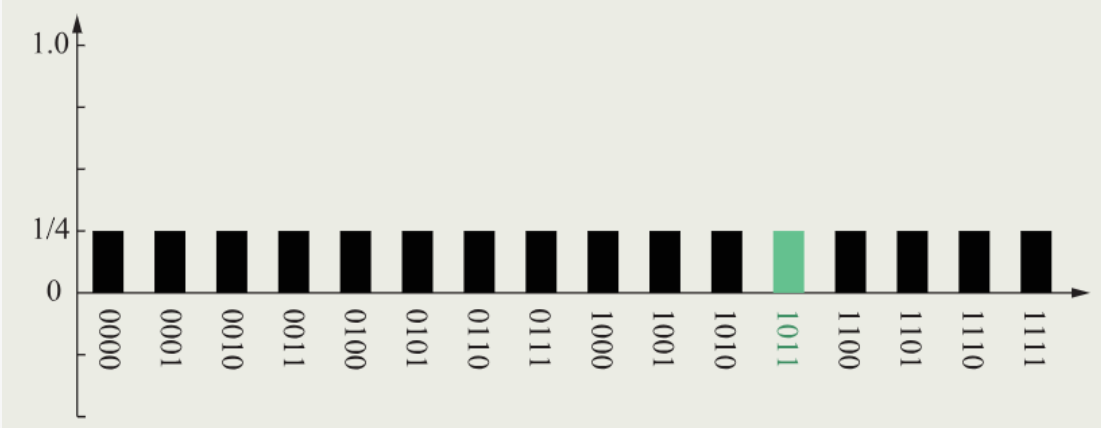


STEP 1: Make all outcomes equally likely

Produce equal superposition of all possible outcomes by acting the Hadamard gate on each register qubit.

$$H^{\otimes 4}|0000\rangle = \frac{1}{\sqrt{2^4}} \sum_{x=0}^{15} |x\rangle$$

The probability amplitude distribution for the register is:



- All states including the target 1011 contribute equally with amplitude $1/4$.

Grover's Algorithm

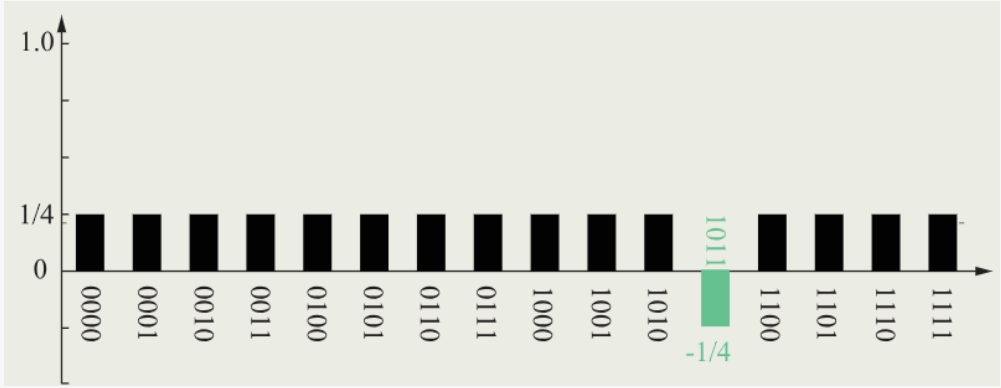
STEP 2: Mark the state we are looking for

- Assume we are given a quantum circuit that implements our oracle, meaning that

$$\text{oracle}\,|z\rangle = \begin{cases} -|z\rangle & \text{if } z = x \\ |z\rangle & \text{if } z \neq x \end{cases}$$

- The output of this circuit is →

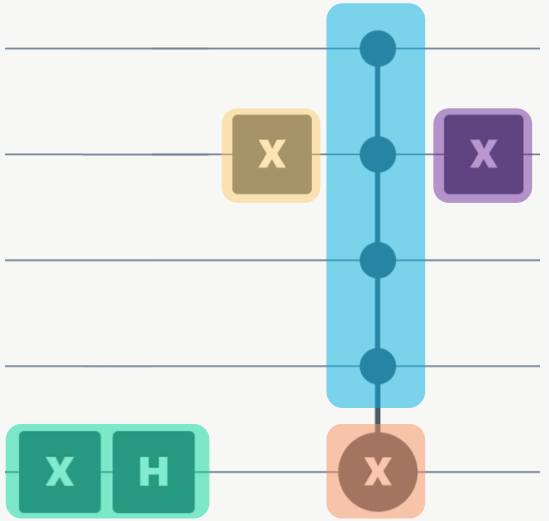
  Observe that the amplitude of 1011 flipped the sign.



Grover's Algorithm

ASIDE: How to make the oracle

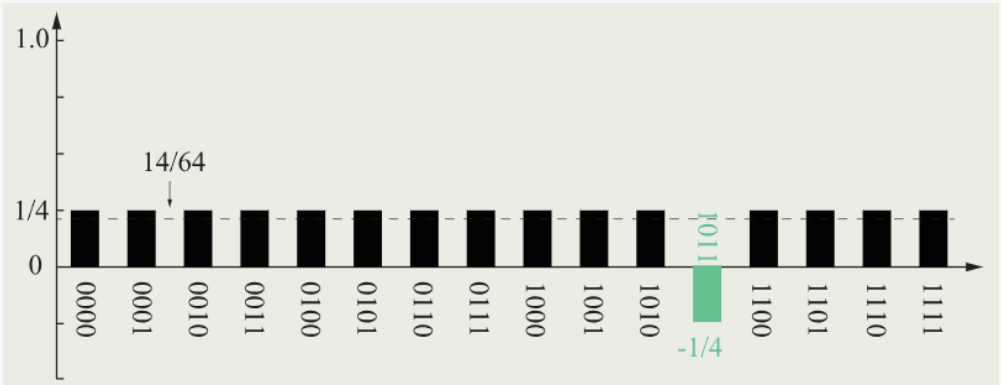
- To make the oracle, we need an ancilla in the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = HX|0\rangle$.
- Goal: flip the sign if and only if the register state is $|1011\rangle$.
  - Applying an X gate to the ancilla gives us a minus sign…
  - So we want to apply the X gate, but only when the input state is right. This is realized by a (multi-)controlled-X gate.
  - We have to flip the second qubit before applying the controlled-X gate to make sure the X is applied when the second qubit is 0.
  - This messes up qubit 2 - flip it back afterwards!

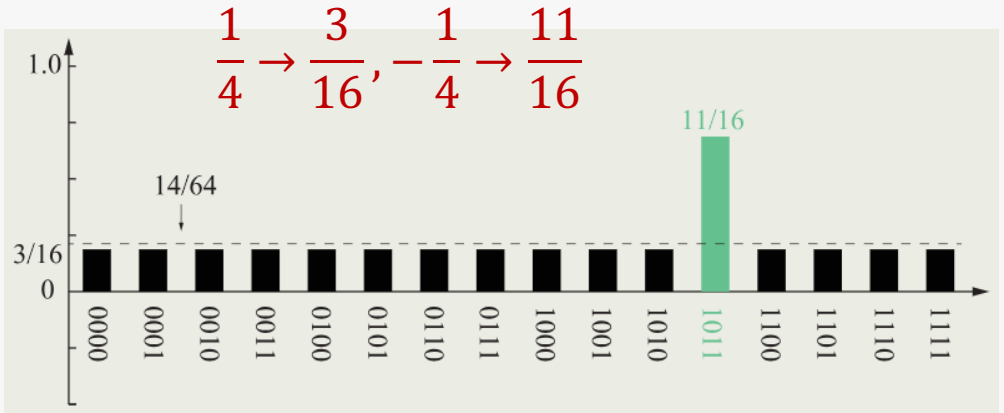


Grover's Algorithm

STEP 3: Increase likelihood of measuring the target

- The marking does not change the **likelihood** of measuring 1011. To amplify the probability, each amplitude is inverted with respect to the mean of amplitudes (dashed line) as

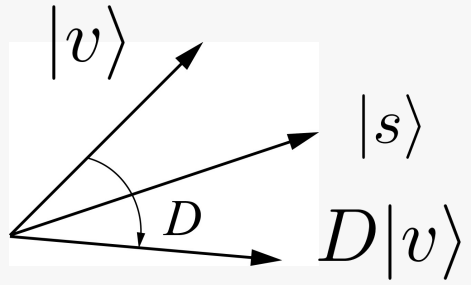




- How do we do this?

Grover's Algorithm

- Goal: mirror amplitudes with respect to the average.

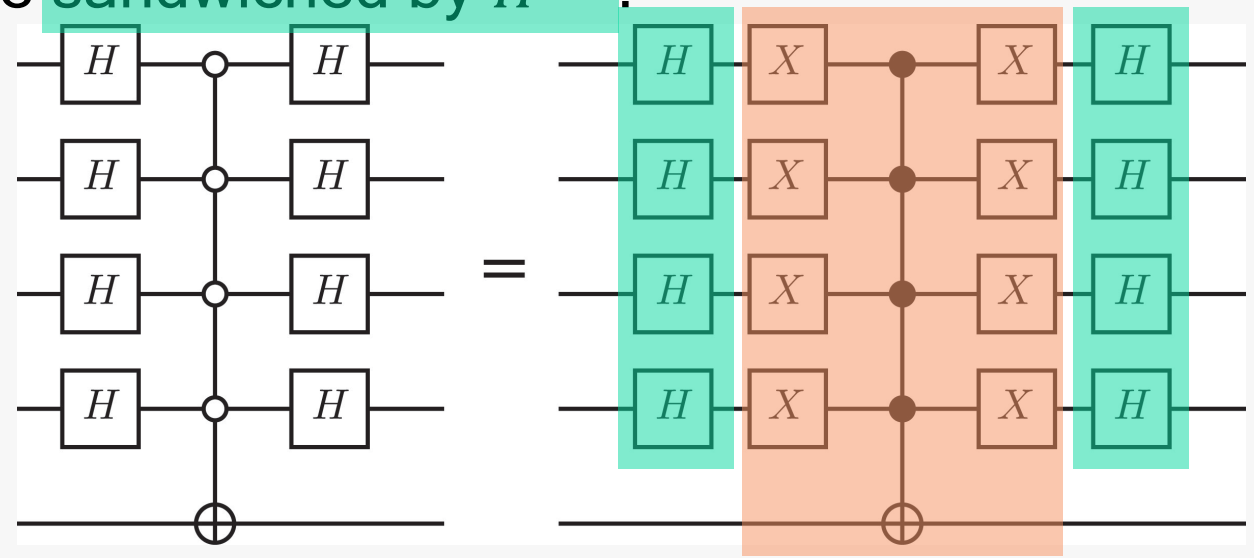


- Let D be an operator that mirrors a vector with respect to $|s\rangle = \frac{1}{\sqrt{16}}\sum_{x=0}^{15}|x\rangle$.
  - D satisfies $D|s\rangle = |s\rangle$ and $D|s_\perp\rangle = -|s_\perp\rangle$, where $|s_\perp\rangle$ is a vector orthogonal to $|s\rangle$.
  - Check that $D = 2|s\rangle\langle s| - I = H^{\otimes 4}(2|0000\rangle\langle 0000| - I)H^{\otimes 4}$.
- Let $|\phi\rangle = \sum_{x=0}^{15} a_x|x\rangle$ be any arbitrary vector.
  - Can show with straightforward math that $D|\phi\rangle = \sum_{i=0}^{15}(2\bar{a} - a_x)|x\rangle$, where $\bar{a} = \frac{1}{16}\sum_{x=0}^{15} a_x$ is the average of $\{a_x\}$. This shows that D in fact mirrors the amplitude with respect to the average $\bar{a}$.
- Let's consider the quantum circuit that implements D next.

Grover's Algorithm

$$D = H^{\otimes 4}\ (2|0000\rangle\langle 0000| - I)\ H^{\otimes 4}$$

This is just like the circuit we used for our oracle, which flips the sign of the ancilla when the input state is $|1011\rangle$, which is replaced with $|0000\rangle$ here. Then the control nodes are sandwiched by $H^{\otimes 4}$:

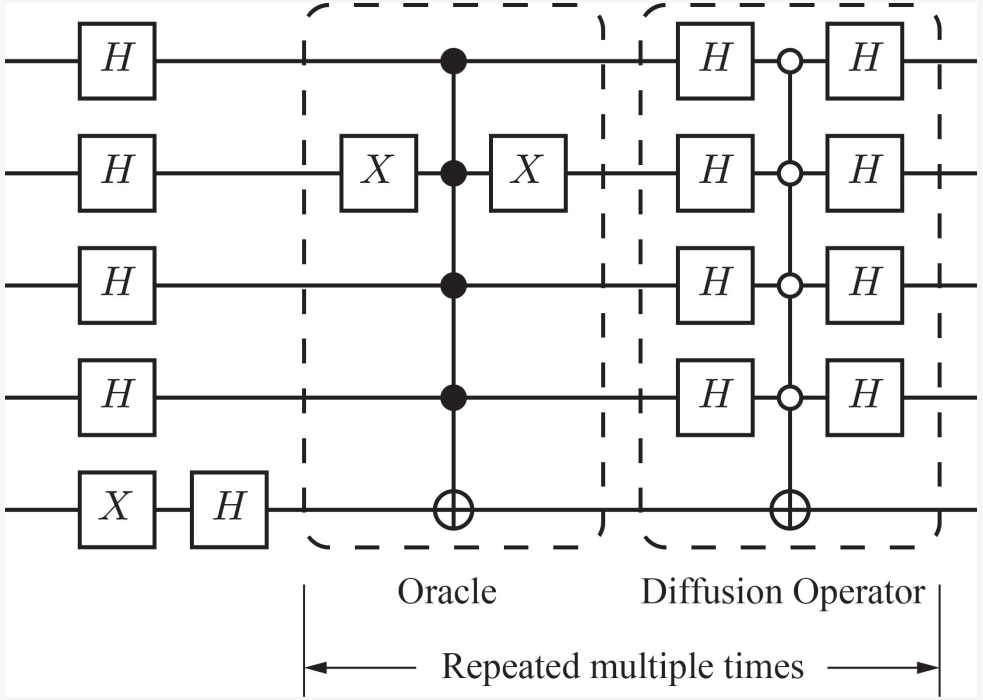


(note – we're assuming our ancilla qubit is still in the state $|-\rangle$ from when we used it in the oracle)

Grover's Algorithm

STEP 4: Do it all over again and again

- Now the oracle followed by the diffusion operator D looks like

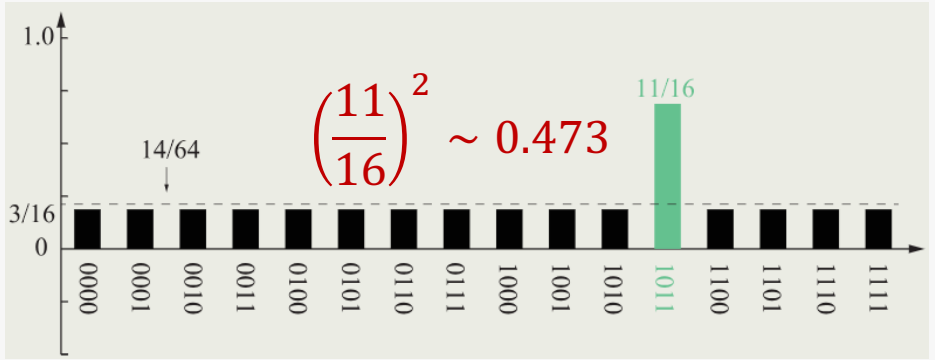


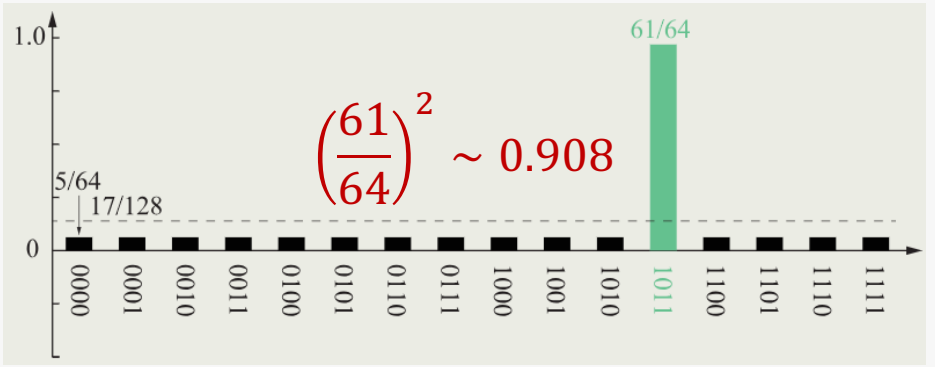
- Let's check the probability of getting 1011 is enhanced.

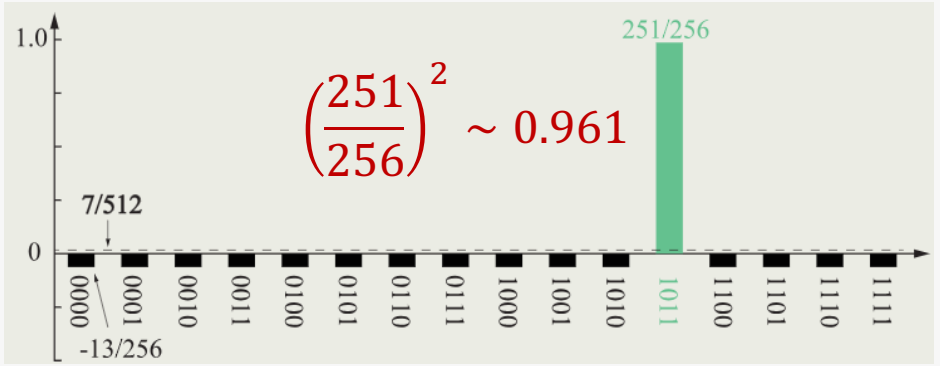
Grover's Algorithm

- The amplitude of 1011 has changed from -1/4 to 11/16. The probability has changed from $\left(\frac{1}{4}\right)^2 = 0.0625$ to $\left(\frac{11}{16}\right)^2 \sim 0.473$.
- The probability is further enhanced if the oracle+diffusion operator is applied again

and again.

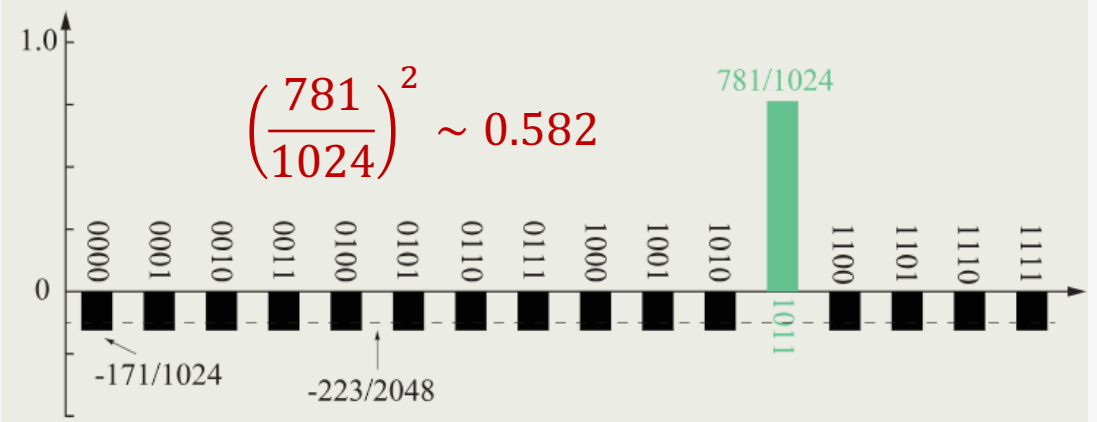






Grover's Algorithm

- What if we repeat this further? The probability goes down on the 4th iteration. There is an optimal number of iterations, 3 in our case.



- With some math (see supplemental slides), can show that the probability of measuring the target is $\sin^2((2k+1)\theta)$ after k iterations, where $\theta \approx \frac{1}{\sqrt{16}}$.
  - This probability is maximized when $(2k+1)\theta \sim (2k+1)\sqrt{\frac{1}{16}} \sim \frac{\pi}{2}$.
  - We find $k = \frac{\sqrt{16}}{4}\pi - \frac{1}{2} \sim 3$

The 3SAT problem

The previous example is a little unnatural…

- To use Grover's algorithm in the previous example, there must be someone or something who knows the solution in order to make the oracle.
- Let's consider the 3SAT problem, which is an example of the Boolean Satisfiability (SAT) problem, which is known to be NP-complete (classically hard).
  - Grover's algorithm can be adapted to solve it faster than simple classical algorithms, and we can make the oracle without knowing the solution.

3SAT Problem

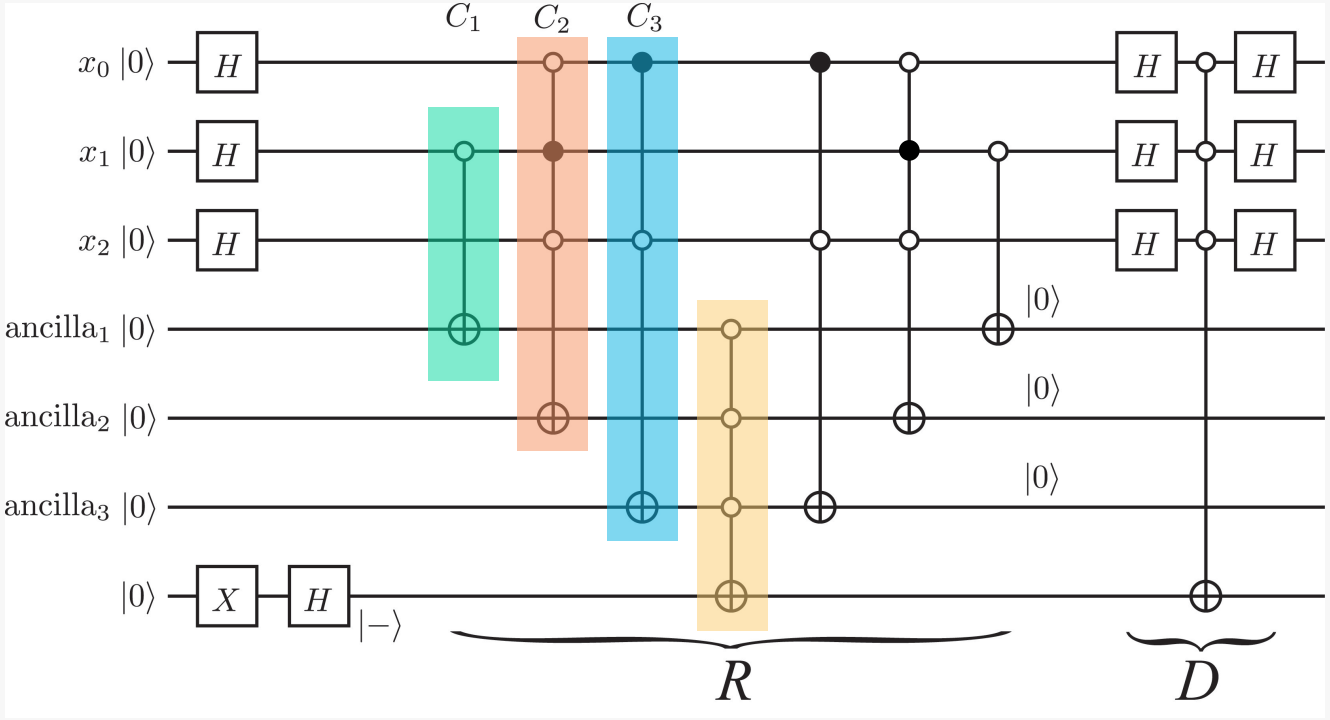
- We have n variables which can each be true (1) or false (0). We are given a set of N clauses.
  - A clause takes the form $C_k = (u_{k_1} OR\ u_{k_2} OR\ u_{k_3})$, where each u_{k_i} (a literal) is either some x_{k_i} or $NOT\ x_{k_i}$ (also denoted $\neg x_{k_i}$).
  - C_k is assumed to have at most 3 literals (hence the 3 in 3SAT).
- The problem is to tell whether there is a choice of $\{x_1, x_2, \ldots, x_n\}$ that makes **all** of the clauses true, i.e., to make the 3SAT instance $C_1\ AND\ C_2\ AND\ \ldots AND\ C_N$ true.

- Naïve classical solution: Try all $N = 2^n$ possible values for all n variables. Takes $O(N)$ attempts. Grover's algorithm cuts this down to $O(\sqrt{N})$ calls to the oracle.
  - Aside: there is a faster classical algorithm available for this particular problem, but it's possible that Grover could be combined with it to get an even faster algorithm.

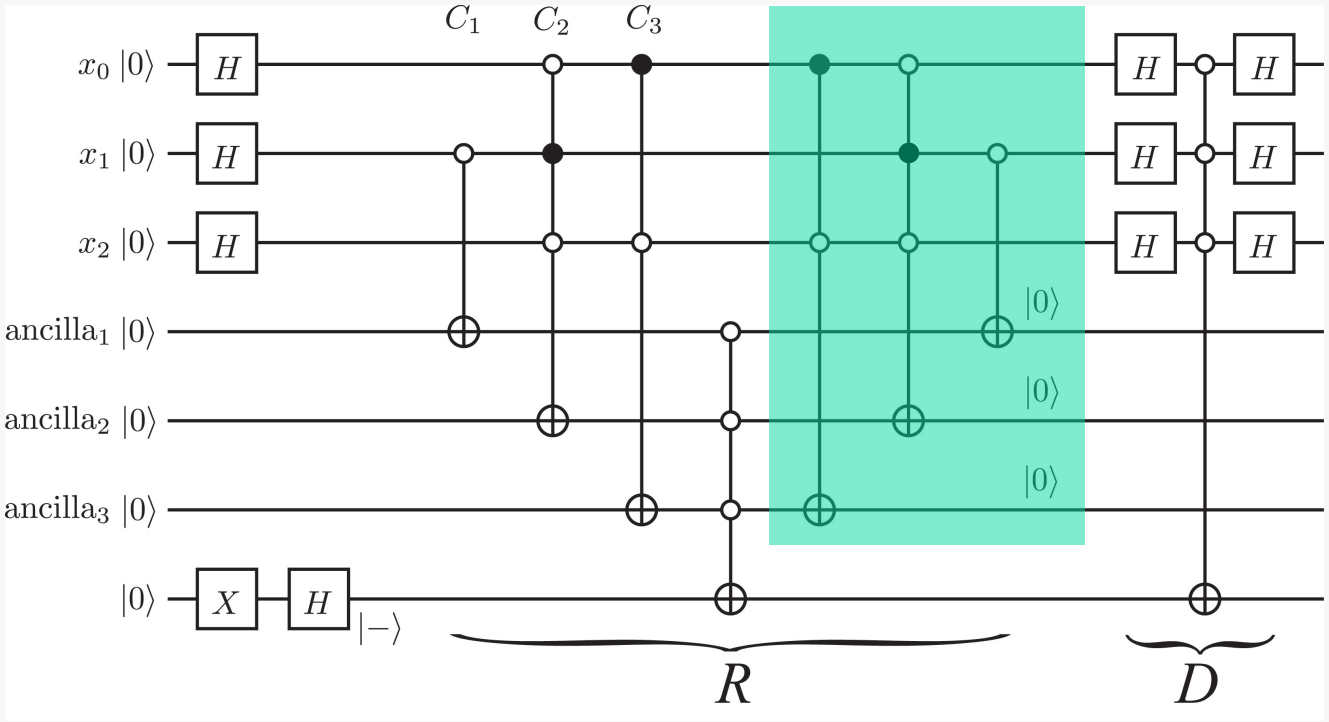
Making the oracle

$x_1\ AND\ (x_0\ OR\ \neg x_1\ OR\ x_2)\ AND\ (\neg x_0\ OR\ x_2)$

- We need to construct an oracle which flips the sign of the state for which the instance is true.
- We will need one ancilla per clause, plus one more ancilla.
  - Oracle flips ancilla k from $|0\rangle$ to $|1\rangle$ if and only if clause k is false.
- One more control gate applies X to the final qubit if all clauses are true
- D is the diffusion operator.
- For our example, $(x_0, x_1, x_2) = (1,1,1)$ is obtained with a good probability after 3 iterations.



Uncomputation



This is an “uncomputation” step. We are resetting the ancillas to their original state $|0\rangle$ so that we can reuse them when we repeat the oracle.

Summary

- Suppose one wants to pick up one specific item out of unstructured N items. In classical search, it takes $O(N)$ steps to find the item. The number of steps is reduced to $k \sim O(\sqrt{N})$ if Grover's algorithm is employed.
- We introduced number finding problem and the 3SAT problem to demonstrate the advantage of Grover's algorithm over classical counterpart.

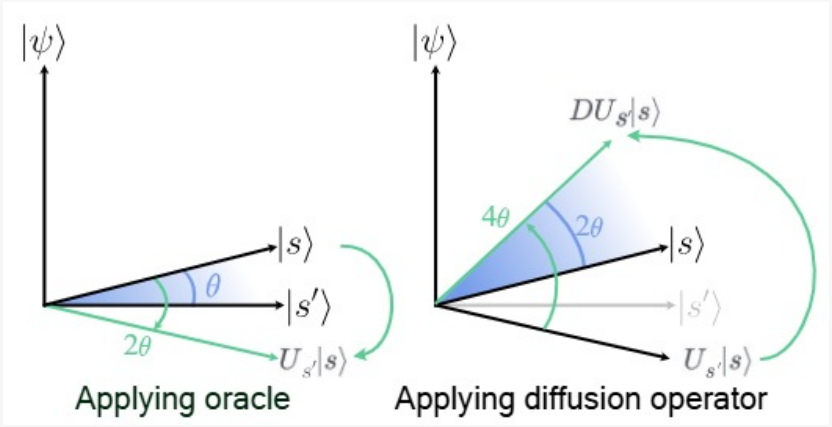
Optimal number of iterations for Grover

Let's look at the iteration process at each step.

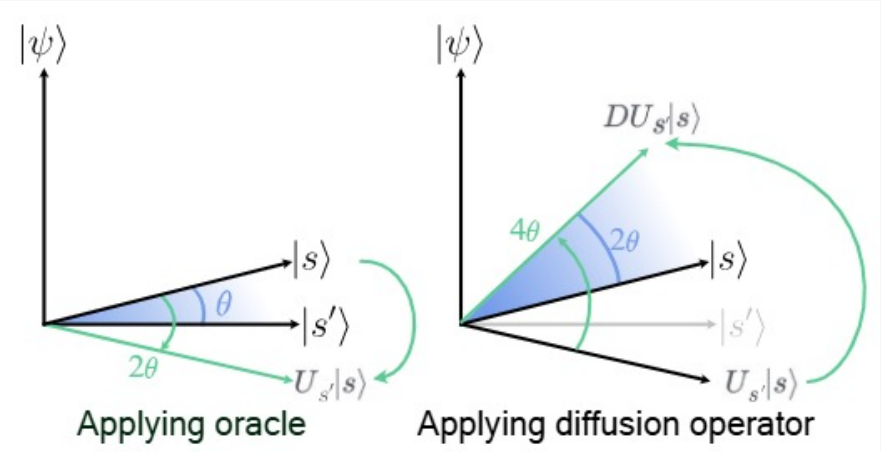
Let $|s\rangle = \frac{1}{\sqrt{16}}\sum_{x=0}^{15}|x\rangle$, $|s'\rangle = \frac{1}{\sqrt{15}}(\sum_{x=0}^{15}|x\rangle - |\psi\rangle)$, where $|\psi\rangle = |1011\rangle$ is the target state.

Then $\langle s'|s\rangle = \sqrt{\frac{15}{16}} = \cos\theta$ and $\sin\theta = \sqrt{\frac{1}{16}}$. Namely $|s\rangle = \cos\theta\,|s'\rangle + \sin\theta\,|\psi\rangle$.

The oracle applies an operator $U_{s'}|s\rangle = R(-2\theta)|s\rangle = \cos\theta\,|s'\rangle - \sin\theta\,|\psi\rangle$.



Grover's Algorithm



- Here $R(\alpha) = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$
- Diffusion operation is a rotation with angle 4θ.

  We find $DU_{s'}|s\rangle = R(4\theta)U_{s'}|s\rangle = \begin{pmatrix} \cos 4\theta & -\sin 4\theta \\ \sin 4\theta & \cos 4\theta \end{pmatrix} \begin{pmatrix} \cos\theta \\ -\sin\theta \end{pmatrix} = \begin{pmatrix} \cos 3\theta \\ \sin 3\theta \end{pmatrix}$
- The next iteration maps $\begin{pmatrix} \cos 3\theta \\ \sin 3\theta \end{pmatrix} \longrightarrow \begin{pmatrix} \cos 3\theta \\ -\sin 3\theta \end{pmatrix} \longrightarrow R(8\theta) \begin{pmatrix} \cos 3\theta \\ -\sin 3\theta \end{pmatrix} = \begin{pmatrix} \cos 5\theta \\ \sin 5\theta \end{pmatrix}$
- The probability of measuring the target $|\psi\rangle$ is $\sin^2((2k+1)\theta)$ after k iterations.
- The probability is maximized when $(2k+1)\theta \sim (2k+1)\sqrt{\frac{1}{16}} \sim \frac{\pi}{2}$. We find $k = \frac{\sqrt{16}}{4}\pi - \frac{1}{2} \sim 3$ in our case. In general, the oracle is called $k = O(\sqrt{N})$ times to find one specific item out of N items. This should be compared with $k = O(N)$ in classical case. $N = 16$ here.