CPEN 400Q Lecture 10
Grover's algorithm

Wednesday 7 February 2024

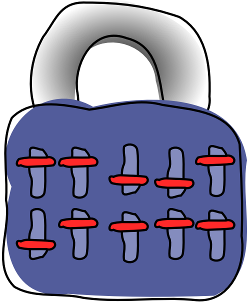
Announcements

- A2 and literacy assignment due next week
- Project details to be posted on PrairieLearn by end of week
- Quiz 4 beginning of class Monday

Last time

We modeled the problem of breaking a lock as a function:

$$f(x) = \begin{cases} 1 & x = s \quad \text{correct combo.} \\ 0 & \text{otherwise} \end{cases}$$



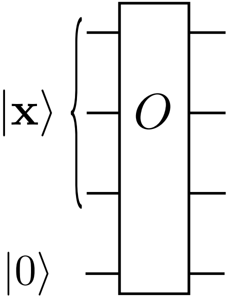
Trying a combination corresponds to querying an *oracle* that evaluates this function.

Image credit: Codebook node A.1

Last time

We discussed query complexity and two ways to query an oracle in a quantum circuit.

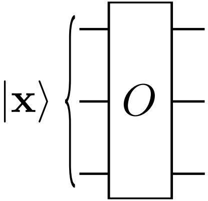
$$O\left(|x\rangle|y\rangle\right) = |x\rangle|y \oplus f(x)\rangle$$



$$
\begin{aligned}
O|000\rangle|0\rangle &= |000\rangle|0\rangle \\
O|001\rangle|0\rangle &= |001\rangle|0\rangle \\
O|010\rangle|0\rangle &= |010\rangle|0\rangle \\
O|011\rangle|0\rangle &= |011\rangle|0\rangle \\
O|100\rangle|0\rangle &= |100\rangle|0\rangle \\
O|101\rangle|0\rangle &= |101\rangle|0\rangle \\
O|110\rangle|0\rangle &= |110\rangle|1\rangle \\
O|111\rangle|0\rangle &= |111\rangle|0\rangle
\end{aligned}
$$

We discussed query complexity and two ways to query an oracle in a quantum circuit.

$$O|x\rangle = (-1)^{f(x)}|x\rangle$$



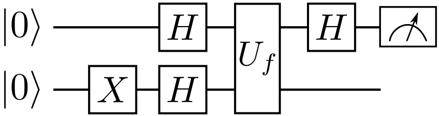
$$\begin{aligned}
O|000\rangle &= |000\rangle\\
O|001\rangle &= |001\rangle\\
O|010\rangle &= |010\rangle\\
O|011\rangle &= |011\rangle\\
O|100\rangle &= |100\rangle\\
O|101\rangle &= |101\rangle\\
O|110\rangle &= -|110\rangle\\
O|111\rangle &= |111\rangle
\end{aligned}$$

Last time

We applied Deutsch's quantum algorithm to determine if a function is *constant* or *balanced* using one oracle query (instead of 2)!

Name	Action	Name	Action
f_1	$f_1(0) = 0$ $f_1(1) = 0$	f_2	$f_2(0) = 1$ $f_2(1) = 1$
f_3	$f_3(0) = 0$ $f_3(1) = 1$	f_4	$f_4(0) = 1$ $f_4(1) = 0$

1 query to oracle



$|0\rangle$ if f is constant
$|1\rangle$ if f is balanced

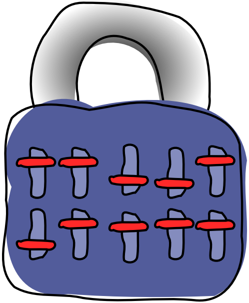
Learning outcomes

$$|\psi\rangle = \alpha|00\ldots0\rangle + \beta|0\ldots01\rangle + \ldots$$

amplitudes

- Describe the strategy of amplitude amplification
- Visualize Grover's algorithm in two different ways
- Implement basic oracle circuits in PennyLane
- Implement Grover's search algorithm

Let's break that lock!

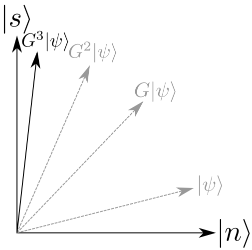


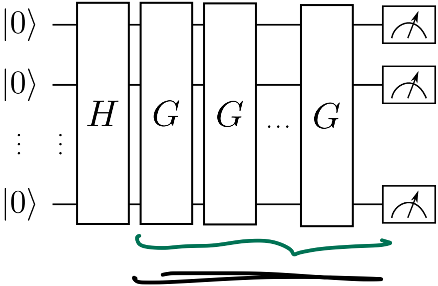
Classical: in the worst case, $O(2^n)$ oracle queries
Quantum: $O(\sqrt{2^n})$ queries with Grover's algorithm

polynomial speedup

Image credit: Codebook node A.1

The idea behind Grover's search algorithm is to start with a uniform superposition and then *amplify* the amplitude of the state corresponding to the solution.





$n=2$: $|+\rangle \otimes |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) = \frac{1}{2}\sum_{x\in\{0,1\}^n} |\vec{x}\rangle$

In other words we want to go from the uniform superposition

$\{0,1\}^n$ = n-bit strings

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |\vec{x}\rangle = |+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle$$

to something that looks more like this:

$$|\psi'\rangle = (\text{big number})|\vec{s}\rangle + (\text{small number})\sum_{\vec{x}\neq\vec{s}} |\vec{x}\rangle$$

makes the solution most likely to measure

Grover's algorithm: amplitude visualization

Assume we have an oracle with the following action on computational basis states:

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

Start with the uniform superposition.

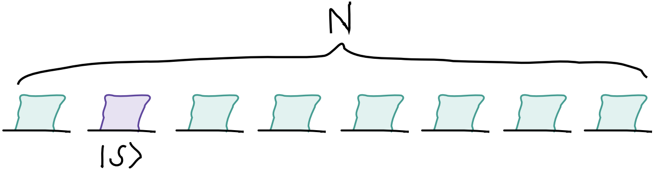


Image credit: Codebook node G.1

If we apply the oracle, we flip the sign for the solution state:

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

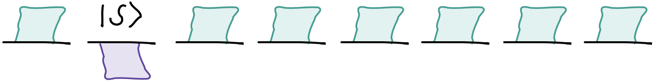
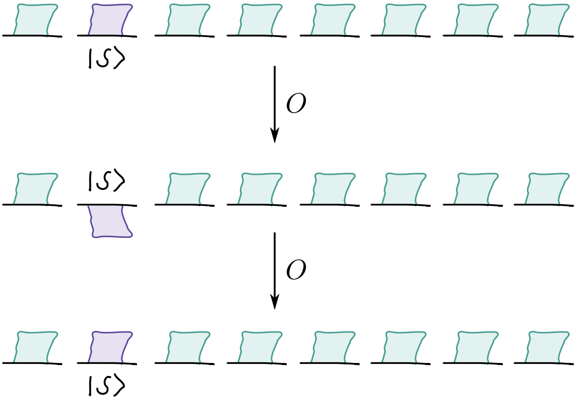


Image credit: Codebook node G.1

Now what?

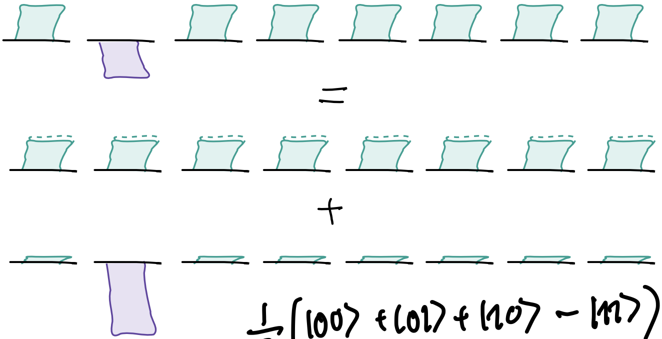


Can't just apply the oracle again... need to do something different.

Image credit: Codebook node G.1

Let's write the amplitudes in a different way:

After oracle



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

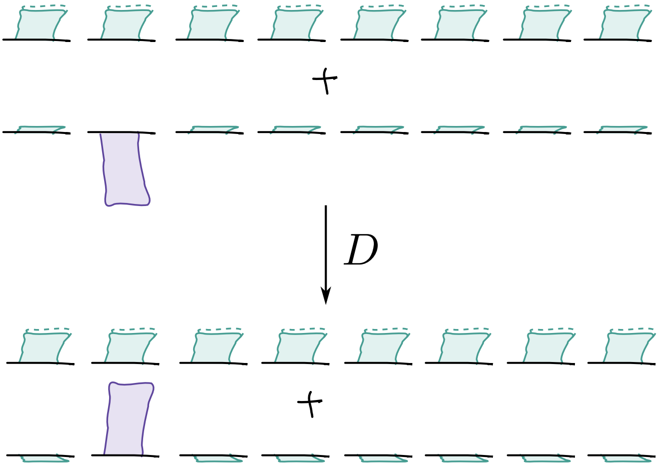
$$= 0.488\cdots\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$+ 0.xx\left(|00\cdots\rangle + \cdots - \text{big}|11\rangle\right)$$

Why does this help?

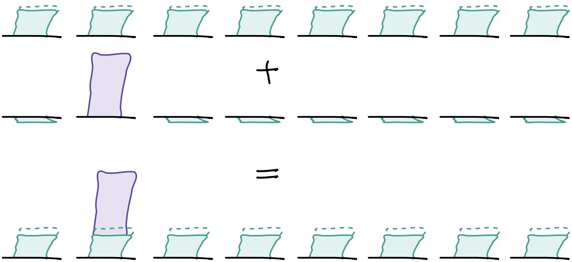
Image credit: Codebook node G.1

What if we had an operation that would flip everything in the second part of the linear combination?



Grover's algorithm: amplitude visualization

Let's add these back together...



We have "stolen" some amplitude from the other states, and added it to the solution state!

Image credit: Codebook node G.1

Grover's algorithm: amplitude visualization

Doing this sequence once is one "iteration":

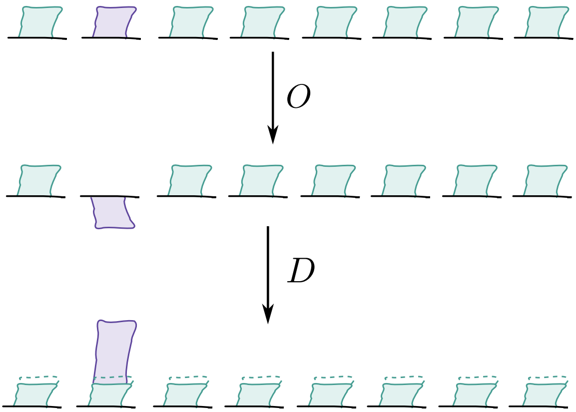
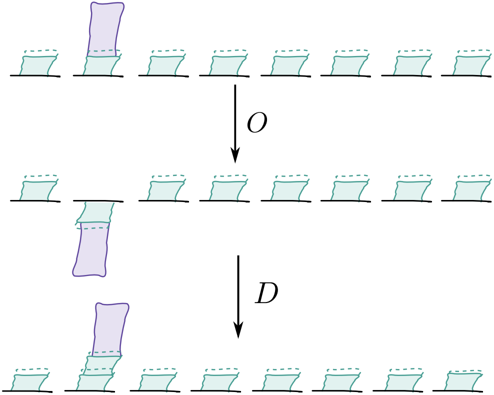


Image credit: Codebook node G.1

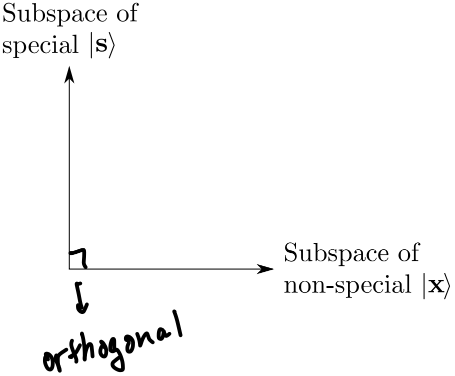
Grover's algorithm: amplitude visualization

If we do it again, we can steal even more amplitude!



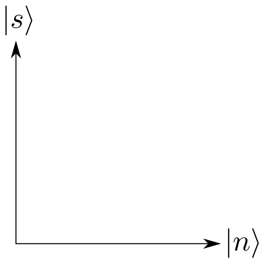
Grover's algorithm works by iterating this sequence multiple times until the probability of observing the solution state is maximized.

Image credit: Codebook node G.1



Partition the computational basis states into two subspaces:

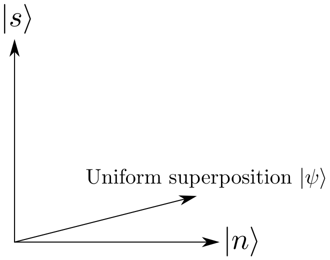
1. The special state $|\mathbf{s}\rangle$
2. All the other states



Let's write these out as superpositions:

$|s\rangle$ solution

$$|n\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{\substack{x \in \{0,1\}^n \\ x \neq s}} |x\rangle$$

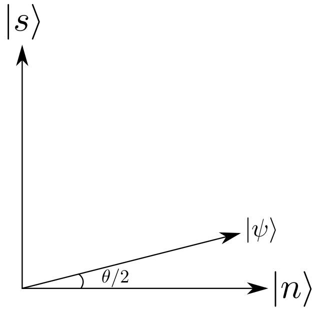


$$
\begin{aligned}
|s\rangle &= |\mathbf{s}\rangle \\
|n\rangle &= \frac{1}{\sqrt{2^n - 1}} \sum_{\mathbf{x} \neq \mathbf{s}} |\mathbf{x}\rangle
\end{aligned}
$$

We can write the uniform superposition in terms of these subspaces:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} |s\rangle + \frac{\sqrt{2^n-1}}{\sqrt{2^n}} |n\rangle$$

$$= \frac{1}{\sqrt{2^n}} |s\rangle + \frac{\cancel{\sqrt{2^n-1}}}{\sqrt{2^n}} \cdot \frac{1}{\cancel{\sqrt{2^n-1}}} \sum_{x \neq s} |x\rangle$$



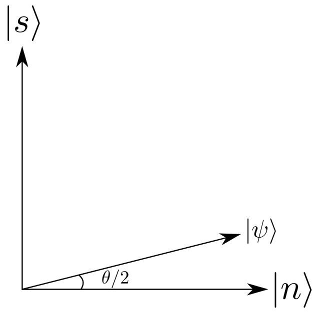
Instead of working with these complicated coeffients:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}|s\rangle + \frac{\sqrt{2^n - 1}}{\sqrt{2^n}}|n\rangle,$$

let's rexpress them in terms of an angle θ:

$$|\psi\rangle = \sin\frac{\theta}{2}\,|s\rangle + \cos\frac{\theta}{2}\,|n\rangle$$

$$\sin\frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$$

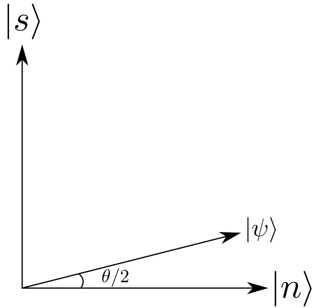


Now we want to apply some operations to this state

$$|\psi\rangle = \sin\left(\frac{\theta}{2}\right)|s\rangle + \cos\left(\frac{\theta}{2}\right)|n\rangle$$

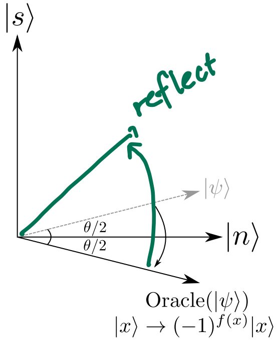
to increase the amplitude of $|s\rangle$ while decreasing that of $|n\rangle$.

Grover's algorithm: geometric visualization



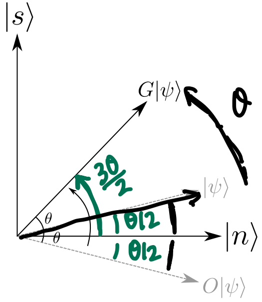
Two steps:

1. Apply the oracle O to 'pick out' the solution
2. Apply a 'diffusion operator' D to adjust the amplitudes.



The effect of the oracle, $O|\psi\rangle$ *flips* the amplitudes of the basis states that are special.

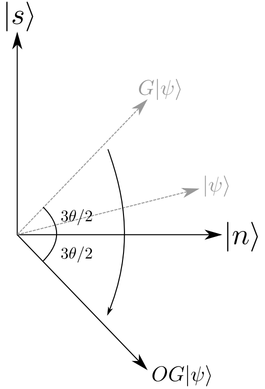
We can visualize this as a *reflection about the subspace* of non-special elements.



The diffusion operator is a bit less intuitive to interpret - it performs a *reflection about the uniform superposition* state.

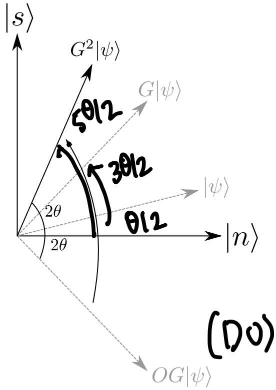
A full Grover iteration $G = DO$ sends

$$G\left(\sin\left(\frac{\theta}{2}\right)|s\rangle + \cos\left(\frac{\theta}{2}\right)|n\rangle\right) = \sin\left(\frac{3\theta}{2}\right)|s\rangle + \cos\left(\frac{3\theta}{2}\right)|n\rangle$$



Now we repeat this...

Apply the oracle and reflect about the non-special elements.



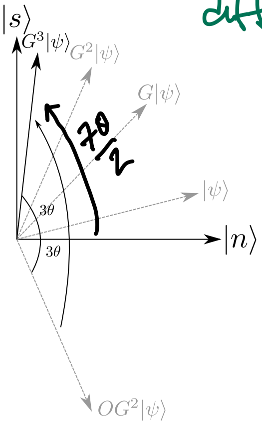
Apply the diffusion operator and reflect about the uniform superposition to boost the amplitude of the special state.

$$(DO)(DO)|\psi\rangle = \sin\frac{5\theta}{2}|s\rangle + \cos\frac{5\theta}{2}|n\rangle$$

After k Grover iterations we will have the state

$$G^k|\psi\rangle = \underbrace{\sin\left(\frac{(2k+1)\theta}{2}\right)}_{\text{differentiate}}|s\rangle + \cos\left(\frac{(2k+1)\theta}{2}\right)|n\rangle$$

$\sin\frac{\theta}{2} = \frac{1}{\sqrt{2^n}}$



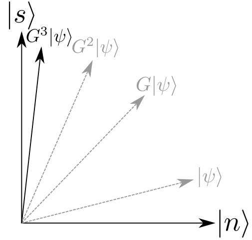
It *is* possible to over-rotate! We can differentiate to find the optimal k:

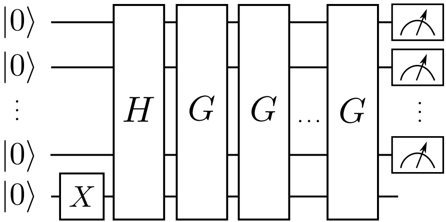
$$k \leq \left\lceil \frac{\pi}{4}\sqrt{2^n} \right\rceil$$

After k operations we will be most likely to obtain the special state when we measure.

Multiple approaches depending on the format of the oracle. We will use this one:

$$O|\mathbf{x}\rangle|y\rangle = |\mathbf{x}\rangle|y \oplus f(\mathbf{x})\rangle$$





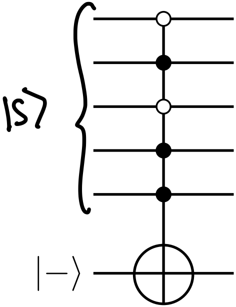
What do circuits for the oracle and diffusion look like?

$$|x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$

Exercise: show that a multicontrolled X gate, controlled on **s**, can be used as an oracle:

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

01011



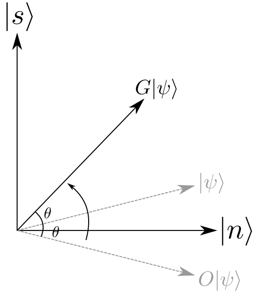
$$O(|s\rangle|-\rangle) = -|s\rangle|-\rangle$$

$$X|-\rangle = \frac{1}{\sqrt{2}}(-|0\rangle + |1\rangle) = -|-\rangle$$

$$O(|x\rangle|-\rangle) = |x\rangle|-\rangle$$

The diffusion circuit

The diffusion operator performs a reflection about the uniform superposition state.



uniform sup.

Exercise: Show that the unitary matrix given by

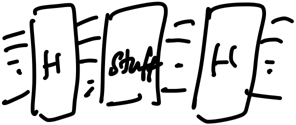
$$D = 2|\psi\rangle\langle\psi| - I$$

correctly implements the diffusion operation.

$$D|\psi\rangle = 2|\psi\rangle\underbrace{\langle\psi|\psi\rangle}_{=1} - |\psi\rangle = 2|\psi\rangle - |\psi\rangle = |\psi\rangle$$

$$D|\psi^{\perp}\rangle = \cancel{2|\psi\rangle\langle\psi|\psi^{\perp}\rangle} - |\psi^{\perp}\rangle = -|\psi^{\perp}\rangle$$

Recall that the uniform superposition is



$$|\psi\rangle = (H \otimes H \otimes \cdots \otimes H)|00\cdots0\rangle = H^{\otimes n}|0\rangle^{\otimes n}$$

We can rewrite D as

$$(H\otimes\cdots\otimes H)(H\otimes\cdots\otimes H)$$

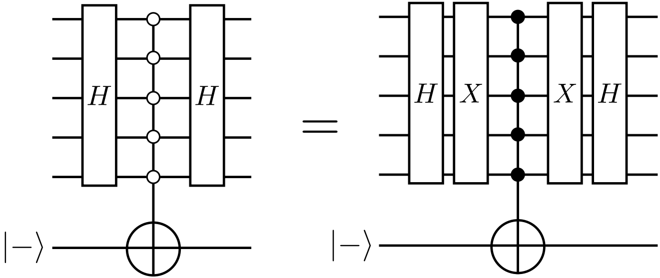
$$D = 2|\psi\rangle\langle\psi| - I$$

$$= 2\,(H\otimes\cdots\otimes H)|0\cdots0\rangle\langle0\cdots0|(H\otimes\cdots\otimes H) - I$$

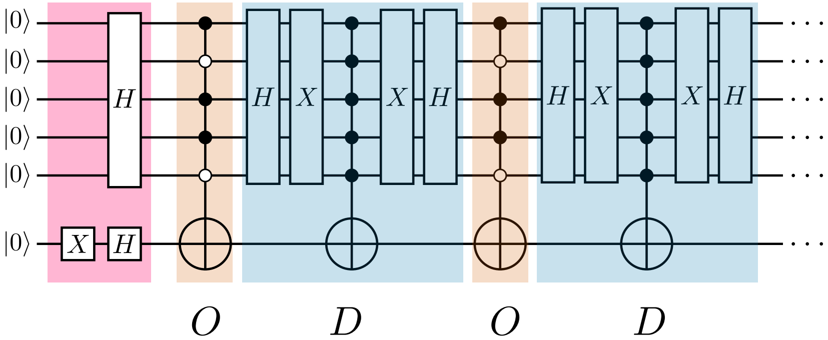
$$= (H\otimes\cdots\otimes H)\big(2|0\cdots0\rangle\langle0\cdots0| - I\big)(H\otimes\cdots\otimes H)$$

The diffusion circuit

$= -D$

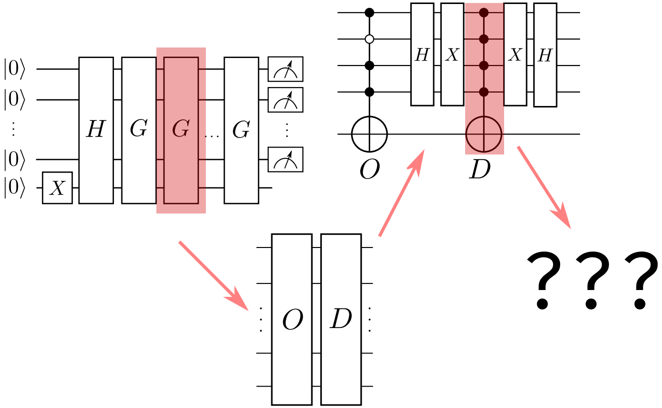


The full Grover circuit



The full Grover circuit

Clearly, each of the $O(\sqrt{2^n})$ queries requires some number of gates... how much does Grover *really* cost?



Next class: we will look deeper inside the black box!

Next time

Content:

- Introduction to quantum compilation and resource estimation
- Quiz 4

Action items:

1. Literacy assignment 1
2. Assignment 2

Recommended reading:

- Codebook nodes G.1-G.5
- Nielsen & Chuang 6.1