CPEN 400Q Lecture 21
Grover's algorithm

Monday 27 March 2023

Announcements

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

Today is the final content lecture!

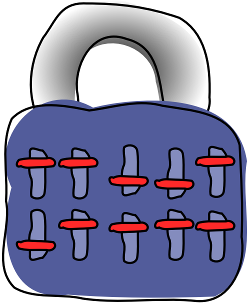
Project presentations Friday/Monday.

- Quiz 9 beginning of class today last quiz!
- Literacy assignment 3 due Wednesday at 23:59
- Assignment 3 available; due end of term (13 April)

Last time

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

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



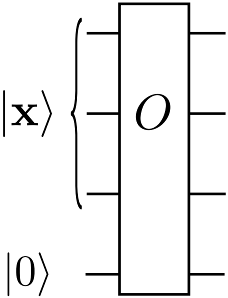
We modeled trying a particular combination as one query to an *oracle* that will evaluate this function.

Image credit: Codebook node A.1

Last time

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

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

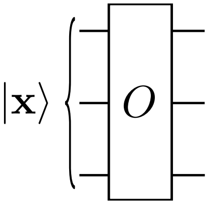


$$\begin{aligned}
O|000\rangle|0\rangle &= |000\rangle|0\rangle \\
O|001\rangle|0\rangle &= |001\rangle|0\rangle \\
O|010\rangle|0\rangle &= |010\rangle|0\rangle \\
O|011\rangle|0\rangle &= |011\rangle|0\rangle \\
O|100\rangle|0\rangle &= |100\rangle|0\rangle \\
O|101\rangle|0\rangle &= |101\rangle|0\rangle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

Last time

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

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

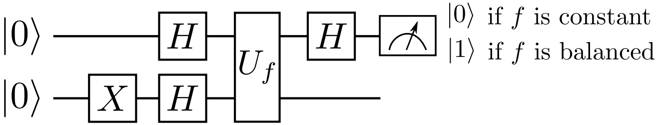


$$
\begin{aligned}
O|000\rangle &= |000\rangle \\
O|001\rangle &= |001\rangle \\
O|010\rangle &= |010\rangle \\
O|011\rangle &= |011\rangle \\
O|100\rangle &= |100\rangle \\
O|101\rangle &= |101\rangle \\
O|110\rangle &= -|110\rangle \\
O|111\rangle &= |111\rangle
\end{aligned}
$$

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	$f_4(0) = 1$ $f_4(1) = 0$

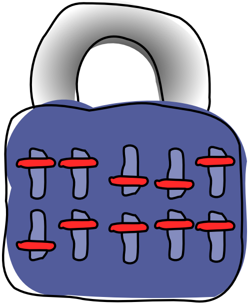


Learning outcomes

- 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

Grover's quantum search algorithm

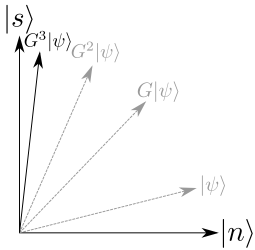
Let's break that lock!

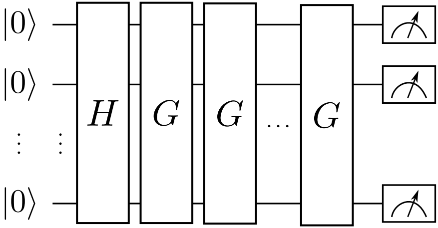


Classical: in the worst case, 2^n oracle queries
Quantum: $O(\sqrt{2^n})$ queries with Grover's algorithm

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.





In other words we want to go from the uniform superposition

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} |\mathbf{x}\rangle$$

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

to something that looks more like this:

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

$|\psi\rangle =$ (big amplitude) $|$solution$\rangle$ + (small amplitude) $|$everything else$\rangle$

Grover's algorithm: amplitude visualization

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

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

Start with the uniform superposition.

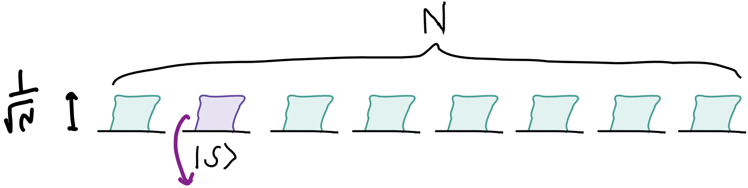
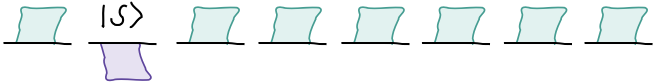


Image credit: Codebook node G.1

Grover's algorithm: amplitude visualization

If we apply the oracle, we flip the sign of the amplitude of the solution state:

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



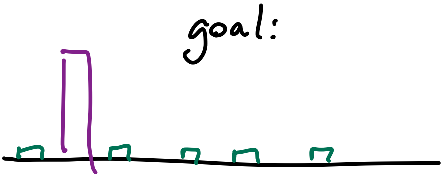
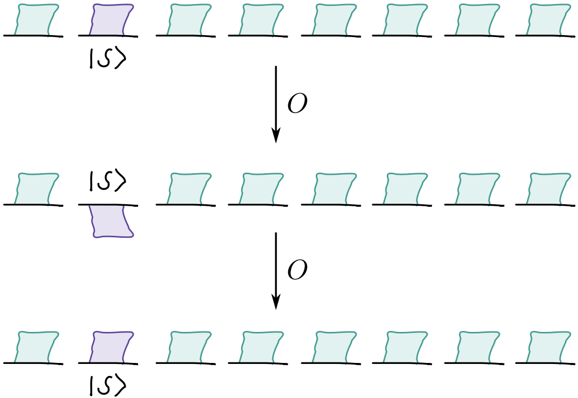


Image credit: Codebook node G.1

Grover's algorithm: amplitude visualization

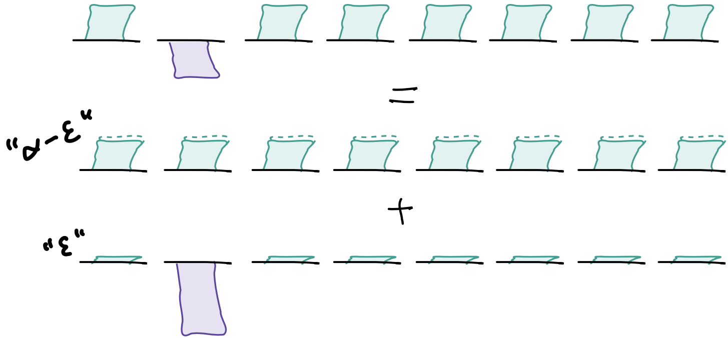
Now what?



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:

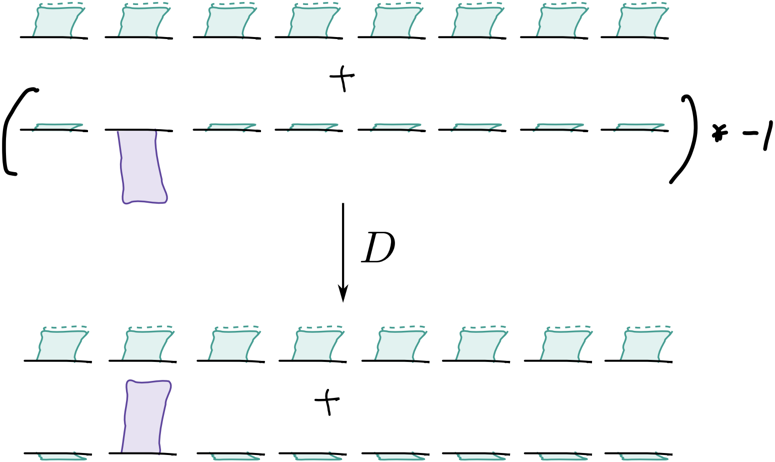


$$\alpha|x\rangle + \beta|y\rangle = (\alpha-\varepsilon)|x\rangle + \varepsilon|x\rangle + (\beta-\varepsilon)|y\rangle + \varepsilon|y\rangle$$

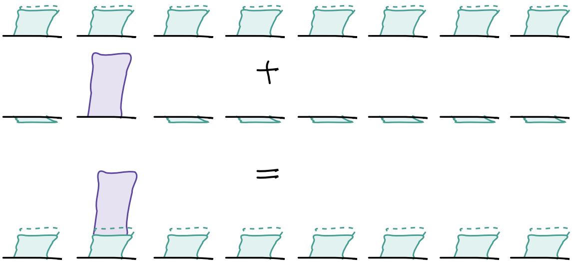
Why does this help?

Image credit: Codebook node G.1

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



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

Doing this sequence once is one "iteration":

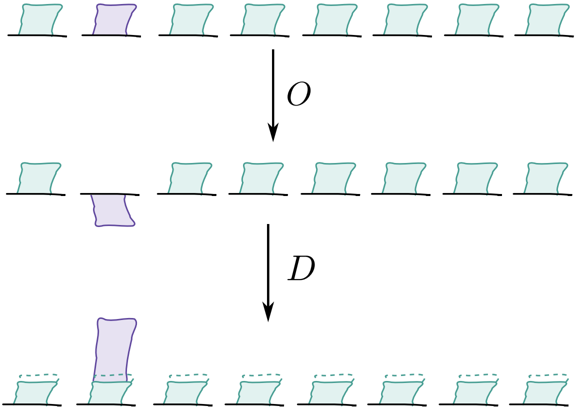
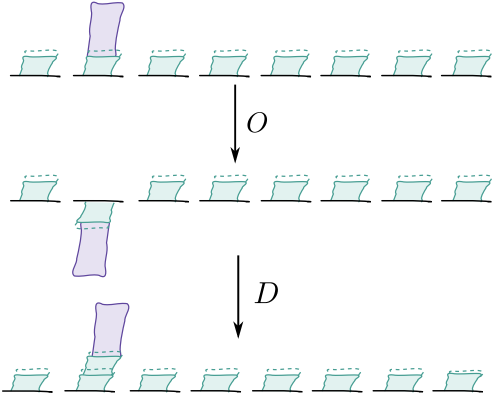


Image credit: Codebook node G.1

Grover's algorithm: amplitude visualization

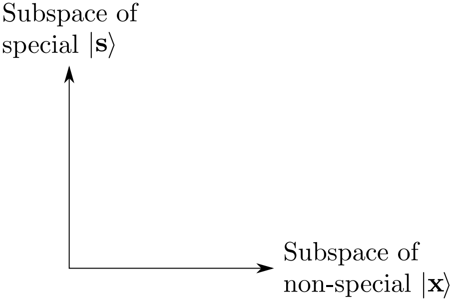
If we do it again, we can steal even more amplitude!



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

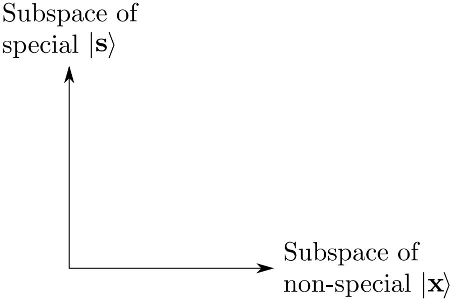
Grover's algorithm: geometric visualization



Partition the computational basis states into two subspaces:

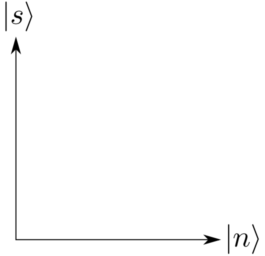
1. The special state $|\mathbf{s}\rangle$

Grover's algorithm: geometric visualization



Partition the computational basis states into two subspaces:

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

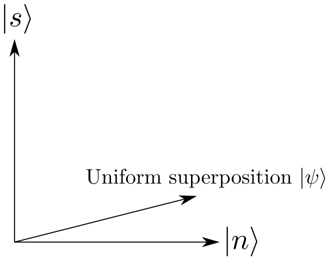


Let's write these out as superpositions:

$$|s\rangle = |s\rangle$$

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

Grover's algorithm: geometric visualization

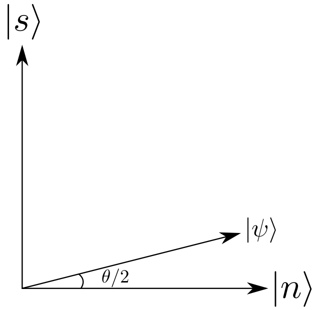


$$
\begin{aligned}
|s\rangle &= |\mathbf{s}\rangle \\
|n\rangle &= \frac{1}{\sqrt{2^n - 1}} \sum_{\mathbf{x} \neq \mathbf{s}} |\mathbf{x}\rangle
\end{aligned}
$$

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

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

Grover's algorithm: geometric visualization

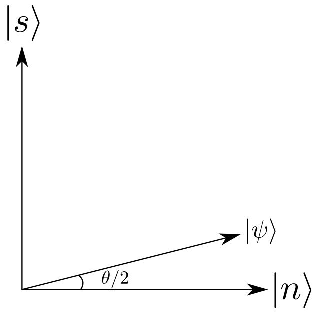


Instead of working with these complicated coeffients:

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

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

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

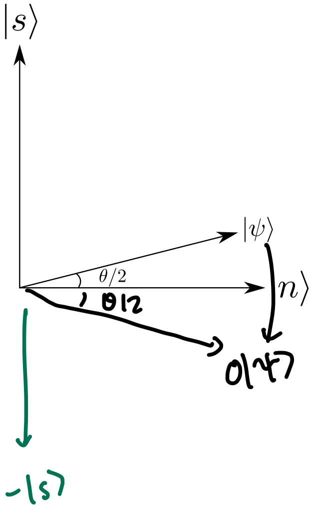


Now we want to apply some operations to this state

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

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

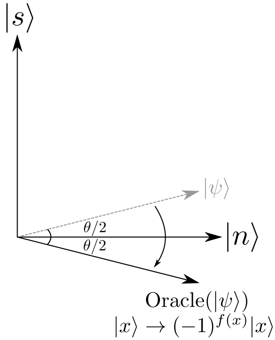
$$|x\rangle \to (-1)^{f(x)}|x\rangle$$



Two steps:

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

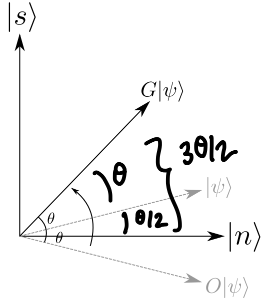
$$O \begin{cases} |s\rangle \to -|s\rangle \\ |\text{other}\rangle \to |\text{other}\rangle \end{cases}$$



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.

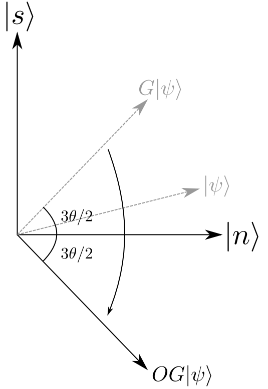
Grover's algorithm: geometric visualization



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

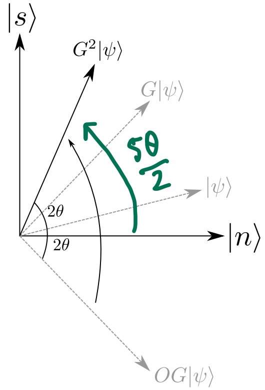
$$G\left(\sin\left(\frac{\theta}{2}\right)|s\rangle + \cos\left(\frac{\theta}{2}\right)|n\rangle\right) = \sin\left(\frac{3\theta}{2}\right)|s\rangle + \cos\left(\frac{3\theta}{2}\right)|n\rangle$$



Now we repeat this...

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

Grover's algorithm: geometric visualization

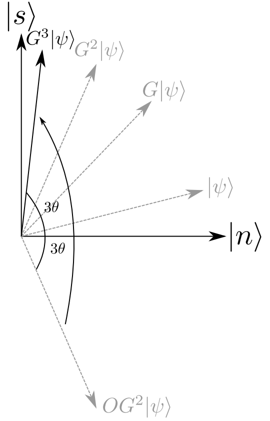


Apply the diffusion operator and reflect about the uniform superposition to boost the amplitude of the special state.

Grover's algorithm: geometric visualization

After k Grover iterations we will have the state

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



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

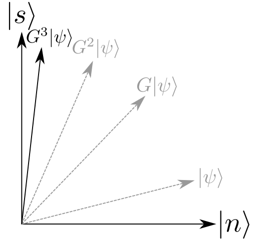
$$k \leq \left\lceil \frac{\pi}{4}\sqrt{2^n} \right\rceil$$

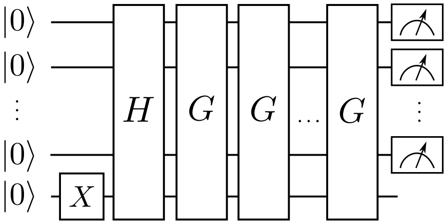
After k operations we will be most likely to obtain the special state when we measure.

Implementing Grover search

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

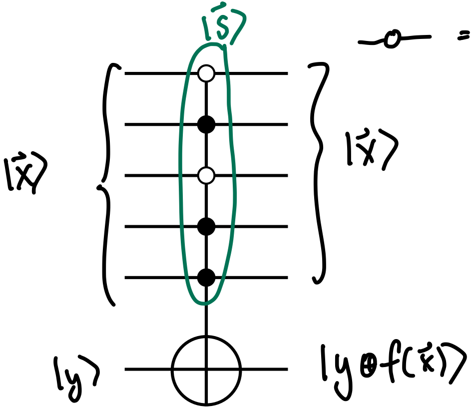
$$O|\mathbf{x}\rangle|y\rangle = |\mathbf{x}\rangle|y \oplus f(\mathbf{x})\rangle$$





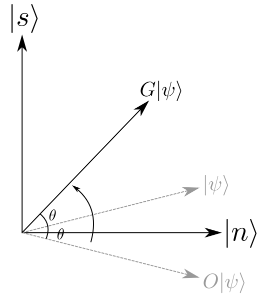
What do circuits for the oracle and diffusion look like?

We can use a multicontrolled X gate, where the state of the control qubits matches the solution state.



The diffusion circuit

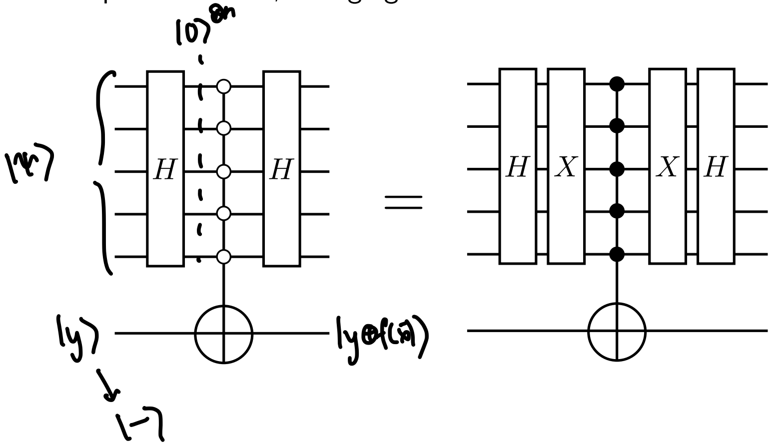
The diffusion operator performs a reflection about the uniform superposition state.



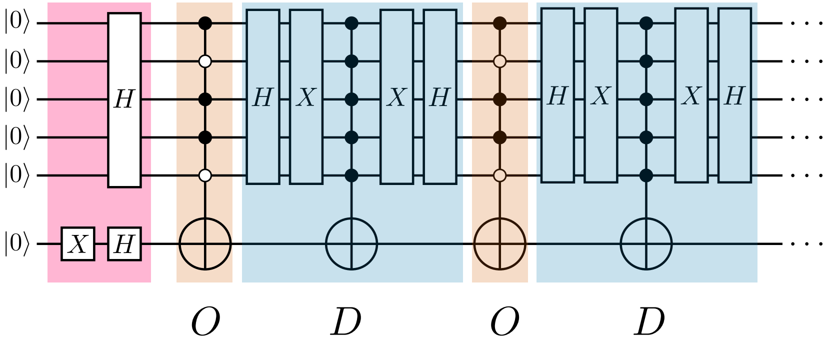
Recall that the uniform superposition is

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

We can implement the reflection by first applying a Hadamard to change to the computational basis; performing a reflection around the equivalent state; changing the basis back.

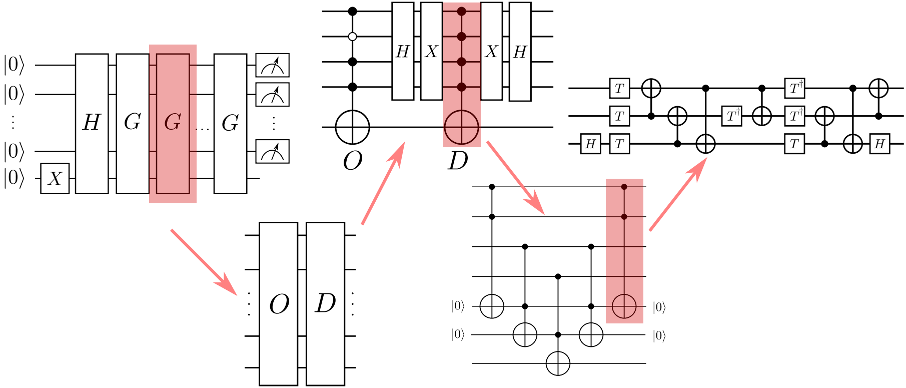


The full Grover circuit



The full Grover circuit

We will implement this at the level of the previous slide; but note that further decomposition is required and adds overhead.



Next time

Content:

- Presentations!

Action items:

1. Literacy assignment 3
2. Technical assignment 3

Recommended reading:

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