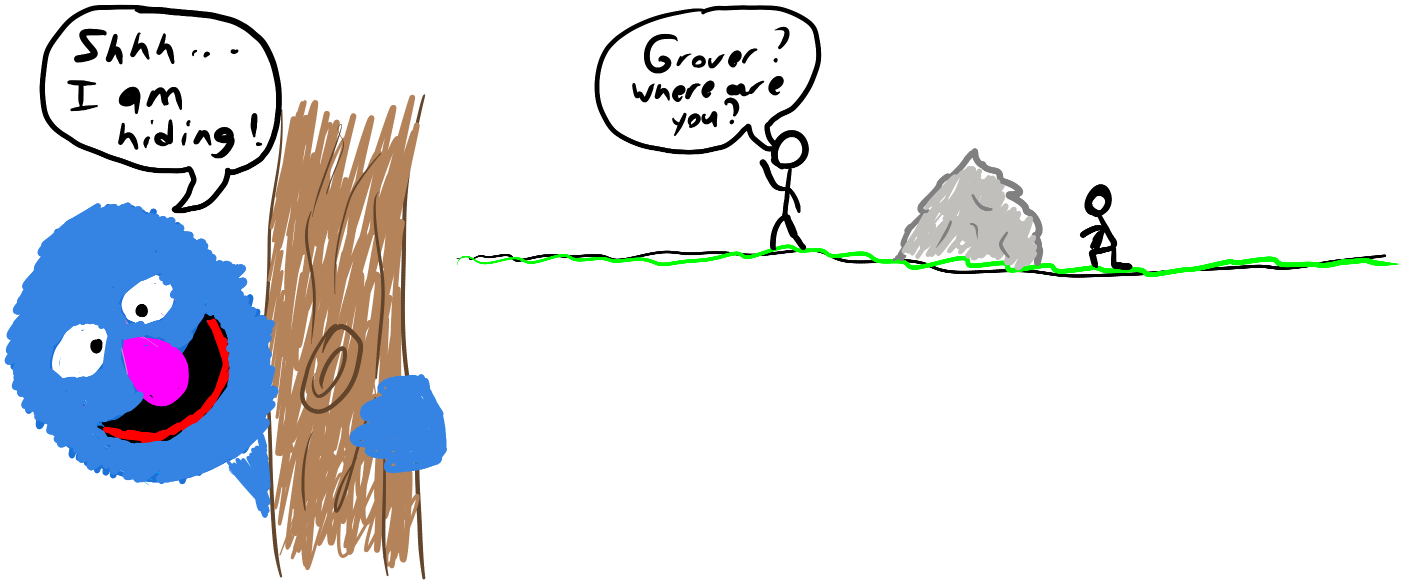
CMPT 476 Lecture 25

Grover's Search



Finally we come to the last of the classic quantum algorithms – Grover's 1996 search algorithm. This algorithm is intrinsically different from Fourier-based algorithms, and encompasses the other main approach to quantum speed-ups: Amplitude amplification. In contrast to Fourier-based algorithms, the quantum speed-up due to Grover's algorithm is only polynomial, and so it won't itself move intractable problems to the tractable pile, but the algorithmic components are used in many other algorithms, and theoretically a polynomial speed-up may still be useful in some practical contexts.

(Black-box Searching)

The problem that Grover's algorithm solves is the black-box or unstructured search problem.

Unstructured Search problem

input: a function $f : \{0,1\}^n \longrightarrow \{0,1\}$
goal: find $x \in \{0,1\}^n$ such that $f(x) = 1$

We call this an unstructured search problem because it amounts to brute force searching — trying all possible values $x \in \{0,1\}^n$ until a solution to $f(x) = 1$ is found.

Ex.

The SAT problem can be phrased as an unstructured search. Given a propositional formula φ, let $[\![\varphi]\!] : \{0,1\}^n \longrightarrow \{0,1\}$ be the function that evaluates φ on some assignment to its set of n variables. The SAT problem reduces to finding some x such that $[\![\varphi]\!]x = 1$.

Many problems can be phrased as or solved by unstructured search:

- Collision finding
- Hash function inversion
- NP-complete decision problems
- Combinatorial optimization problems
- Unordered databases
- etc.

(Classical complexity of unstructured search)

Informally, if there are many solutions, we can find one with decently high probability using just a few queries on a classical computer. So instead, imagine the worst-case scenario: f has exactly one solution.

Worst-case query complexity

Let $f:\{0,1\}^n \longrightarrow \{0,1\}$ have exactly one solution $f(x)=1$. Then $O(2^n)$ queries are needed classically to find the solution with at least $\frac{1}{2}$ probability.

Intuitively, each query has a $\frac{1}{2^n}$ probability of being the unique solution, assuming f is arbitrary, so we need to check at least $\frac{2^n}{2}=2^{n-1}$ of the possible inputs to find the solution with $1/2$ probability.

(Grover's quantum algorithm)

At first glance, unstructured search seems like a prime candidate for quantum computation:

1. Prepare $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|0\rangle$
2. Compute $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$
3. ???
4. Profit!

If we tried to find $f(x)=1$ by measuring $|f(x)\rangle$ in step 3. we would find such an x with probability just $\left|\frac{1}{\sqrt{2^n}}\right|^2 = \frac{1}{2^n}$ since

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle = \frac{1}{\sqrt{2^n}} \sum_{x|f(x)=0} |x\rangle|0\rangle + \frac{1}{\sqrt{2^n}} \sum_{x|f(x)=1} |x\rangle|1\rangle$$

$$= \frac{\sqrt{2^n-1}}{\sqrt{2^n}} |\psi_{f(x)=0}\rangle|0\rangle + \frac{1}{\sqrt{2^n}} |x\rangle|1\rangle$$

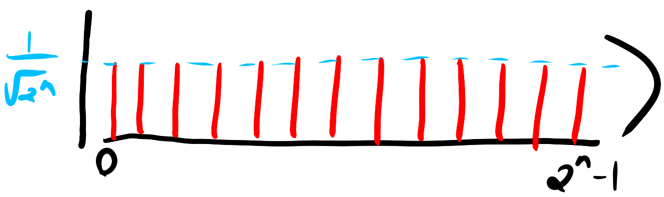
What we instead need to do is amplify the amplitude of the correct state $|x\rangle|1\rangle$.

Grover showed that we can do this by switching to the phase oracle and inverting about the mean.

(Inversion about the mean)

Suppose we prepare the equal weight superposition of bit strings $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$.

We can visualize this state as 2^n equal, positive real numbers



What happens if we apply the phase oracle

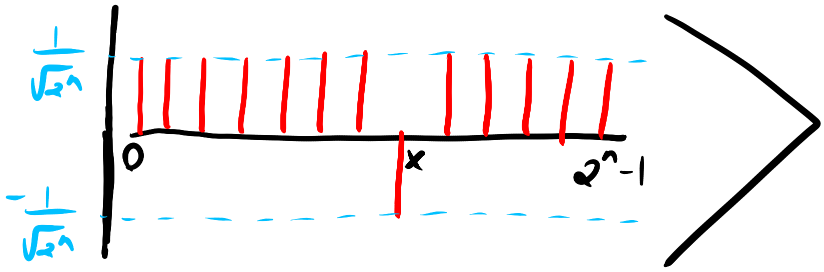
$$U_f : |x\rangle \longmapsto (-1)^{f(x)} |x\rangle$$

to this state, where $f(x)=1$ for exactly one x?

The state becomes

$$\frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{x|f(x)=0}|x\rangle - \frac{1}{\sqrt{2^n}}\sum_{x|f(x)=1}|x\rangle$$

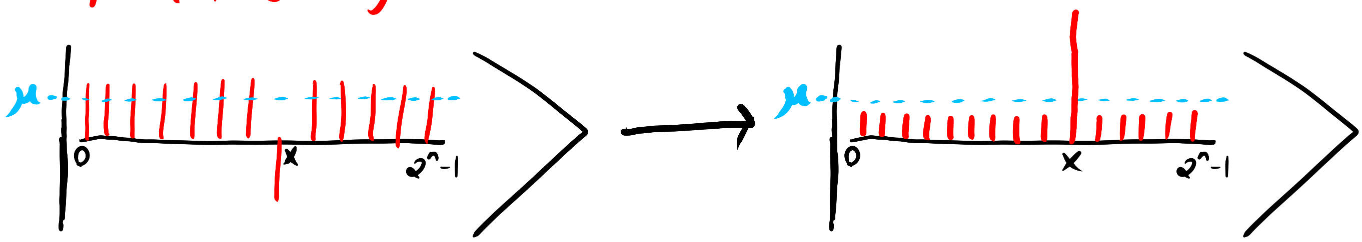
Which we can visualize as



Now, what is the average or mean μ of the amplitudes?

$$\mu = \frac{1}{\sqrt{2^n}}\left(\frac{2^n-1-1}{2^n}\right) = \frac{1}{\sqrt{2^n}}\left(1-\frac{1}{2^{n-1}}\right) \approx \frac{1}{\sqrt{2^n}}$$

The term inverting about the mean means reflecting about the mean line, i.e.

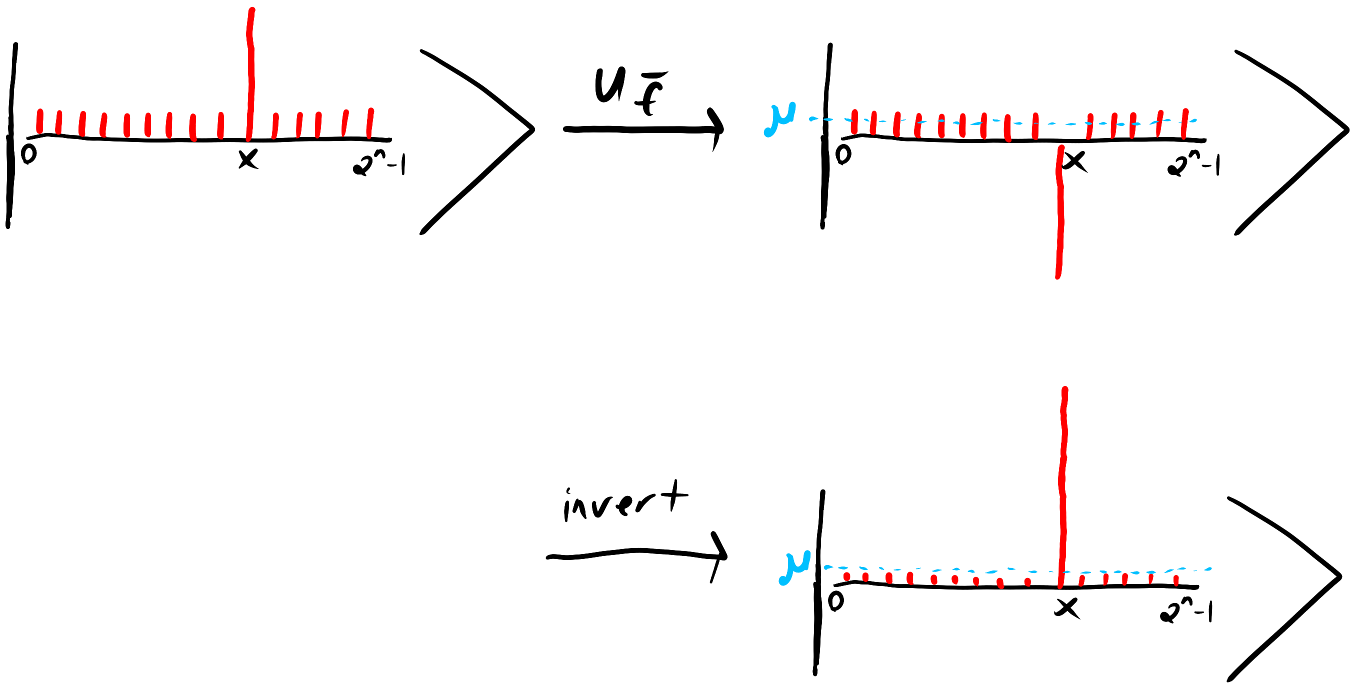


Now the amplitude of x is much bigger! Mathematically, we send α to α' such that $\mu-\alpha = -(\mu-\alpha')$, so $\alpha' = 2\mu-\alpha$ and the amplitude of x is hence

$$\approx \frac{2}{\sqrt{2^n}} - \left(\frac{-1}{\sqrt{2^n}}\right) = \frac{3}{\sqrt{2^n}}$$

after inversion.

Now, what happens if we repeat this process?



This is basically Grover's algorithm. We do still need to figure out how we might invert about the mean however.

(Inversion about the mean)

The inversion about the mean subroutine, like the QFT in Shor's algorithm, is the heart of Grover's search algorithm. Specifically, observe that

$$U_{diff} : \sum_x \alpha_x |x\rangle \longmapsto \sum_x (2\mu - \alpha_x)|x\rangle$$

inverts about the mean, where $\mu = \frac{1}{2^n} \sum_x \alpha_x$. U_{diff} is called the Grover diffusion operator and can be verified to be unitary, notably since it is self-inverse with the mean remaining invariant.

So how can we implement it?

(Implementing Grover's diffusion operator)

To implement U_{diff}, it will be helpful to use our intuition of it as a reflection. First, what state(s) does U_{diff} fix? (i.e. $U_{diff}|\psi\rangle = |\psi\rangle$). Well, if $\alpha_x = \mu$ for all x ($|\psi\rangle$ is a uniform superposition $\frac{1}{\sqrt{2^n}}\sum_x |x\rangle$), then

$$U_{diff}\left(\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\right) = \sum_x \left(2\mu - \frac{1}{\sqrt{2^n}}\right)|x\rangle$$

$$= \sum_x \frac{1}{\sqrt{2^n}}|x\rangle \quad \text{since } \mu = \frac{1}{\sqrt{2^n}}$$

$$= \frac{1}{\sqrt{2^n}}\sum_x |x\rangle$$

So U_{diff} fixes the uniform superposition. Now, what state(s) does U_{diff} reflect (i.e. $U_{diff}|\psi\rangle = -|\psi\rangle$). We know such a state must be orthogonal to the uniform superposition $|S\rangle = \frac{1}{\sqrt{2^n}}\sum_x |x\rangle$, as it is a -1 eigenvector. What states does $|S\rangle^\perp$ contain?

$$\frac{1}{\sqrt{2^n}}\sum_z (-1)^{y\cdot z}|z\rangle \in |S\rangle^\perp$$

for any $y \neq 00\cdots0$ because $y\cdot z = 1$ for exactly half the values of z, hence

$$\left(\frac{1}{\sqrt{2^n}}\sum_z (-1)^{y\cdot z}\langle z|\right)\left(\frac{1}{\sqrt{2^n}}\sum_x |x\rangle\right) = \frac{1}{2^n}\sum_z (-1)^{y\cdot z}\langle z|z\rangle$$

$$= 0$$

Now, what does U_{diff} do to those vectors? Well, since $\sum_z (-1)^{y\cdot z} = 0$, their mean is 0, hence

$$U_{diff}|\psi\rangle = -|\psi\rangle$$

Finally, noting that all $\frac{1}{\sqrt{2^n}}\sum_z (-1)^{y\cdot z}|z\rangle$ are linearly independent (and in fact equal to $H^{\otimes n}|y\rangle$) and there are $2^n - 1$ such orthogonal vectors, they must span the entire subspace orthogonal to $|s\rangle$.

So

U_{diff} is a reflection along the line $|\psi\rangle$ which we can write as

$$U_{diff} = 2|s\rangle\langle s| - I$$

Alternatively, we see that U_{diff} has $+1$ eigenspace $\{|s\rangle\}$ and -1 eigenspace $\mathbb{C}^{2^n} - \{|s\rangle\}$, so by the spectral theorem

$$U_{diff} = |s\rangle\langle s| - (I - |s\rangle\langle s|)$$
$$= 2|s\rangle\langle s| - I$$

(A concrete circuit)

To devise a circuit for U_{diff}, note that

$$H^{\otimes n}|0\rangle = |s\rangle$$

So,

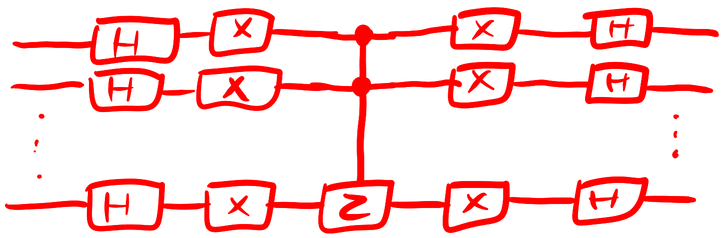
$$U_{diff} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I$$
$$= H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n}$$

Now, $2|0\rangle\langle 0| - I$ sends $|0\rangle \longmapsto -|0\rangle$
$|x\rangle \longmapsto |x\rangle \quad \forall x \neq 0$

This is exactly the $n-1$ controlled Z gate with 0 & 1 swapped! That is,

$$2|0\rangle\langle 0| - I = X^{\otimes n}(2|1\rangle\langle 1| - I)X^{\otimes n}$$
$$= X^{\otimes n}(C^{n-1}Z)X^{\otimes n}$$

So, we can implement U_{diff} with the circuit

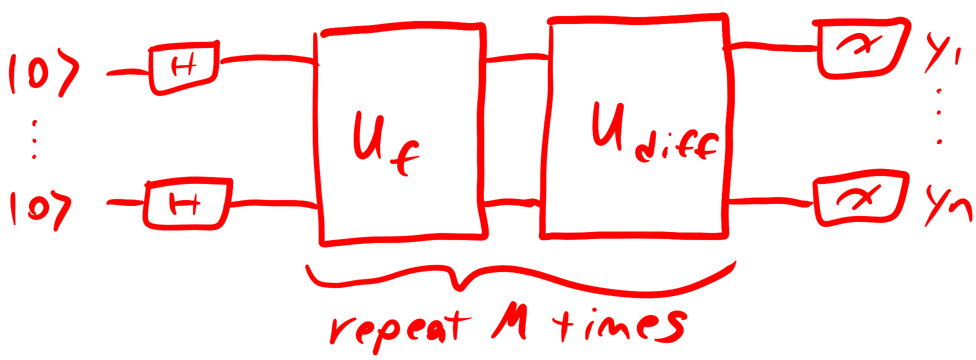


(Grover's search algorithm)

Given a classical function $f:\{0,1\}^n \to \{0,1\}$, Grover's algorithm proceeds as follows:

1. Prepare $|s\rangle = H^{\otimes}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
2. For $i = 1$ to M
3. Apply $U_{diff} U_f$
4. Measure to get $|y\rangle$, $y \in \{0,1\}^n$

As a circuit,



We still need to figure out a value of M, but for now let's just say $M \approx \sqrt{2^n}/2$ since each iteration adds $2\mu \approx \frac{2}{\sqrt{2^n}}$ amplitude to the good state. We'll do the full analysis next class for the generalized version —

Amplitude Amplification