Week 9: Quantum algorithms for search and counting

COMS 4281 (Fall 2023)

Admin

1. Worksheet and Quiz 5 out.

Recap of Grover search

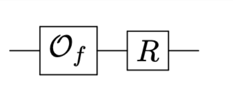
Given query access to $f : \{0,1\}^n \rightarrow \{0,1\}$, find a **marked input** x such that $f(x) = 1$.

- Classical algorithms: Need at least $\sim N$ queries to f.
- Grover's algorithm: $\sim \sqrt{N}$ queries suffices.

(Remember that $N = 2^n$)

The algorithm:

1. Start with $|+\rangle^{\otimes n}$.
2. Run $k = O(\sqrt{N})$ iterations of the **Grover iterate**



where $R = 2\,|+\rangle\langle+|^{\otimes n} - I$ is the Grover diffusion operator.

Analysis of Grover's algorithm (attempt #2)

Let x^* denote the unique marked input.

Important fact: The intermediate states of Grover's algorithm are linear combinations of

$$|x^*\rangle \qquad \text{and} \qquad |\Delta\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq x^*} |x\rangle$$

We can prove this via induction.

Base case

Base case: initial state

$$|+\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle = \sqrt{\frac{2^n - 1}{2^n}} |\Delta\rangle + \frac{1}{\sqrt{2^n}} |x^*\rangle$$

Inductive step

Assume that an intermediate state of Grover's algorithm has form $|\psi\rangle = \alpha\,|\Delta\rangle + \beta\,|x^*\rangle$.

Claim: $O_f\,|\psi\rangle$ is linear combination of $|\Delta\rangle\,, |x^*\rangle$.

Proof:

$$\begin{aligned} O_f(\alpha\,|\Delta\rangle + \beta\,|x^*\rangle) &= \alpha O_f\,|\Delta\rangle + \beta O_f\,|x^*\rangle \\ &= \alpha\,|\Delta\rangle - \beta\,|x^*\rangle\ . \end{aligned}$$

Dirac notation interlude

When we write $|+\rangle\langle+|$, we mean the outer product

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix}\ .$$

Dirac notation interlude

When we write $|+\rangle\langle+|$, we mean the outer product

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1\\1 & 1\end{pmatrix} .$$

When we write $|+\rangle\langle+|^{\otimes n}$, we mean

$$|+\rangle\langle+| \otimes |+\rangle\langle+| \otimes \cdots \otimes |+\rangle\langle+| = (|+\rangle\langle+|)^{\otimes n} .$$

which is an n-qubit **matrix** of size $2^n \times 2^n$.

Dirac notation interlude

When we write $|+\rangle^{\otimes n}$, we mean the tensor product

$$|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle$$

which is a 2^n-dimensional **column vector**.

Dirac notation interlude

When we write $|+\rangle^{\otimes n}$, we mean the tensor product

$$|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle$$

which is a 2^n-dimensional **column vector**. Similarly, $\langle +|^{\otimes n}$ is a 2^n-dimensional **row vector**.

Dirac notation interlude

When we write $|+\rangle^{\otimes n}$, we mean the tensor product

$$|+\rangle \otimes |+\rangle \otimes \cdots \otimes |+\rangle$$

which is a 2^n-dimensional **column vector**. Similarly, $\langle +|^{\otimes n}$ is a 2^n-dimensional **row vector**. The outer product

$$|+\rangle^{\otimes n} \langle +|^{\otimes n}$$

is a $2^n \times 2^n$ **matrix** .

Dirac notation interlude

These are three different ways of writing the same thing!

$$|+\rangle^{\otimes n} \langle +|^{\otimes n} = (|+\rangle\langle +|)^{\otimes n} = |+\rangle\langle +|^{\otimes n} \ .$$

Inductive step

Assume that an intermediate state of Grover's algorithm has form $|\psi\rangle = \alpha |\Delta\rangle + \beta |x^*\rangle$.

Claim: $R|\psi\rangle$ is linear combination of $|\Delta\rangle, |x^*\rangle$.

Proof:

$$\begin{aligned} R_f |\psi\rangle &= (2|+\rangle\langle+|^{\otimes n} - I)|\psi\rangle \\ &= 2|+\rangle^{\otimes n} \underbrace{(\langle+|^{\otimes n}|\psi\rangle)}_{\textbf{number!}} - |\psi\rangle \end{aligned}$$

Inductive step

Assume that an intermediate state of Grover's algorithm has form $|\psi\rangle = \alpha |\Delta\rangle + \beta |x^*\rangle$.

Claim: $R|\psi\rangle$ is linear combination of $|\Delta\rangle, |x^*\rangle$.

Proof:

$$\begin{aligned} R_f |\psi\rangle &= (2|+\rangle\langle+|^{\otimes n} - I)|\psi\rangle \\ &= 2|+\rangle^{\otimes n} \underbrace{(\langle+|^{\otimes n}|\psi\rangle)}_{\textbf{number!}} - |\psi\rangle \end{aligned}$$

Recall $|+\rangle^{\otimes n}$ is a linear combination of $|\Delta\rangle, |x^*\rangle$, and so is $|\psi\rangle$ by assumption.

Thus $R_f|\psi\rangle$ is a linear combination of $|\Delta\rangle, |x^*\rangle$.

Analysis of Grover's algorithm

Claim: After k Grover iterations, the state of the algorithm is

$$|\psi\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|x^*\rangle$$

where $\theta = \sin^{-1}(\sqrt{1/N})$.

Analysis of Grover's algorithm

Claim: After k Grover iterations, the state of the algorithm is

$$|\psi\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|x^*\rangle$$

where $\theta = \sin^{-1}(\sqrt{1/N})$.

We prove this by induction.

Base case: $k = 0$. The initial state can be written as

$$|+\rangle^{\otimes n} = \sqrt{\frac{N-1}{N}}\,|\Delta\rangle + \sqrt{\frac{1}{N}}\,|x^*\rangle \ .$$

Analysis of Grover's algorithm

Claim: After k Grover iterations, the state of the algorithm is

$$|\psi\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|x^*\rangle$$

where $\theta = \sin^{-1}(\sqrt{1/N})$.

Analysis of Grover's algorithm

Claim: After k Grover iterations, the state of the algorithm is

$$|\psi\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|x^*\rangle$$

where $\theta = \sin^{-1}(\sqrt{1/N})$.

Inductive step: Assume true for $k \geq 1$. Then one more Grover iteration yields

$$\begin{aligned} RO_f\,|\psi\rangle &= \cos((2k+1)\theta) RO_f\,|\Delta\rangle + \sin((2k+1)\theta) RO_f\,|x^*\rangle \\ &= \cos((2k+1)\theta) R\,|\Delta\rangle - \sin((2k+1)\theta) R\,|x^*\rangle \end{aligned}$$

Analysis of Grover's algorithm

$$R\,|\Delta\rangle = (2\,|+\rangle\langle+|^{\otimes n} - I)\,|\Delta\rangle$$

Analysis of Grover's algorithm

$$
\begin{aligned}
R\,|\Delta\rangle &= (2\,|+\rangle\langle+|^{\otimes n} - I)\,|\Delta\rangle \\
&= 2\,|+\rangle^{\otimes n}\left(\langle+|^{\otimes n}\,|\Delta\rangle\right) - |\Delta\rangle
\end{aligned}
$$

Analysis of Grover's algorithm

$$
\begin{aligned}
R\,|\Delta\rangle &= (2\,|+\rangle\langle+|^{\otimes n} - I)\,|\Delta\rangle \\
&= 2\,|+\rangle^{\otimes n}\left(\langle+|^{\otimes n}\,|\Delta\rangle\right) - |\Delta\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\,|+\rangle^{\otimes n} - |\Delta\rangle
\end{aligned}
$$

Analysis of Grover's algorithm

$$
\begin{aligned}
R\,|\Delta\rangle &= (2\,|+\rangle\langle+|^{\otimes n} - I)\,|\Delta\rangle \\
&= 2\,|+\rangle^{\otimes n}\left(\langle+|^{\otimes n}\,|\Delta\rangle\right) - |\Delta\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\,|+\rangle^{\otimes n} - |\Delta\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\left(\sqrt{\frac{N-1}{N}}\,|\Delta\rangle + \sqrt{\frac{1}{N}}\,|x^*\rangle\right) - |\Delta\rangle
\end{aligned}
$$

Analysis of Grover's algorithm

$$
\begin{aligned}
R\left|\Delta\right\rangle &= \left(2\left|+\right\rangle\left\langle+\right|^{\otimes n} - I\right)\left|\Delta\right\rangle \\
&= 2\left|+\right\rangle^{\otimes n}\left(\left\langle+\right|^{\otimes n}\left|\Delta\right\rangle\right) - \left|\Delta\right\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\left|+\right\rangle^{\otimes n} - \left|\Delta\right\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\left(\sqrt{\frac{N-1}{N}}\left|\Delta\right\rangle + \sqrt{\frac{1}{N}}\left|x^*\right\rangle\right) - \left|\Delta\right\rangle \\
&= \frac{N-2}{N}\left|\Delta\right\rangle + \frac{2\sqrt{N-1}}{N}\left|x^*\right\rangle
\end{aligned}
$$

Analysis of Grover's algorithm

$$
\begin{aligned}
R\,|\Delta\rangle &= (2\,|+\rangle\langle+|^{\otimes n} - I)\,|\Delta\rangle \\
&= 2\,|+\rangle^{\otimes n}\,\Big(\langle+|^{\otimes n}\,|\Delta\rangle\Big) - |\Delta\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\,|+\rangle^{\otimes n} - |\Delta\rangle \\
&= 2\sqrt{\frac{N-1}{N}}\Big(\sqrt{\frac{N-1}{N}}\,|\Delta\rangle + \sqrt{\frac{1}{N}}\,|x^*\rangle\Big) - |\Delta\rangle \\
&= \frac{N-2}{N}\,|\Delta\rangle + \frac{2\sqrt{N-1}}{N}\,|x^*\rangle \\
&= \cos(2\theta)\,|\Delta\rangle + \sin(2\theta)\,|x^*\rangle \ .
\end{aligned}
$$

Analysis of Grover's algorithm

Similarly,

$$R\,|x^*\rangle = \sin(2\theta)\,|\Delta\rangle + \cos(2\theta)\,|x^*\rangle \ \ .$$

Analysis of Grover's algorithm

Similarly,

$$R\left|x^*\right\rangle = \sin(2\theta)\left|\Delta\right\rangle + \cos(2\theta)\left|x^*\right\rangle \ .$$

Thus we get

$$\begin{aligned} RO_f\left|\psi\right\rangle = \cos((2k+1)\theta)\Big(\cos(2\theta)\left|\Delta\right\rangle + \sin(2\theta)\left|x^*\right\rangle\Big) \\ - \sin((2k+1)\theta)\Big(\sin(2\theta)\left|\Delta\right\rangle + \cos(2\theta)\left|x^*\right\rangle\Big) \end{aligned}$$

as desired.

Analysis of Grover's algorithm

Similarly,

$$R\,|x^*\rangle = \sin(2\theta)\,|\Delta\rangle + \cos(2\theta)\,|x^*\rangle \ .$$

Thus we get

$$\begin{aligned} RO_f\,|\psi\rangle &= \cos((2k+1)\theta)\Big(\cos(2\theta)\,|\Delta\rangle + \sin(2\theta)\,|x^*\rangle\Big) \\ &\qquad - \sin((2k+1)\theta)\Big(\sin(2\theta)\,|\Delta\rangle + \cos(2\theta)\,|x^*\rangle\Big) \\ &= \cos((2k+3)\theta)\,|\Delta\rangle + \sin((2k+3)\theta)\,|x^*\rangle \end{aligned}$$

as desired.

Multiple solutions

If there are $M > 1$ solutions, then can find a solution with $O(\sqrt{N/M})$ queries.

Multiple solutions

If there are $M > 1$ solutions, then can find a solution with $O(\sqrt{N/M})$ queries.

The intermediate states of the algorithm are in the span of

- $|\Gamma\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle$, uniform superposition over all **solutions**
- $|\Delta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle$, uniform superposition over all **non-solutions**

In the end, the output is a **random** solution.

Multiple solutions

What if you wanted to output **all** solutions?

There is $O(\sqrt{NM})$ query solution:

1. Use $\sqrt{\frac{N}{M}}$ queries to find the first solution x_1.

Multiple solutions

What if you wanted to output **all** solutions?

There is $O(\sqrt{NM})$ query solution:

1. Use $\sqrt{\frac{N}{M}}$ queries to find the first solution x_1.
2. Run Grover search with updated oracle f_1 where x_1 is excluded. This finds solution x_2 with $\sqrt{\frac{N}{M-1}}$ queries.

Multiple solutions

What if you wanted to output **all** solutions?

There is $O(\sqrt{NM})$ query solution:

1. Use $\sqrt{\frac{N}{M}}$ queries to find the first solution x_1.
2. Run Grover search with updated oracle f_1 where x_1 is excluded. This finds solution x_2 with $\sqrt{\frac{N}{M-1}}$ queries.
3. Update the oracle to exclude x_2. Find another solution x_3, etc.

Multiple solutions

The total number of queries is

$$\sqrt{\frac{N}{M}} + \sqrt{\frac{N}{M-1}} + \cdots + \sqrt{\frac{N}{1}}$$

Multiple solutions

The total number of queries is

$$\sqrt{\frac{N}{M}} + \sqrt{\frac{N}{M-1}} + \cdots + \sqrt{\frac{N}{1}}$$

$$= \sum_{j=0}^{M-1} \sqrt{\frac{N}{M-j}} \leq \int_0^{M-1} \sqrt{\frac{N}{M-x}} \mathrm{d}x$$

$$\leq O(\sqrt{NM})$$

Quantum counting

What if you wanted to **count** the number of solutions, not just find them?

Given query access to $f : \{0,1\}^n \to \{0,1\}$, output an estimate $\tilde{M}$ of the number of marked inputs M, such that

$$(1-\epsilon)M \leq \tilde{M} \leq (1+\epsilon)M.$$

Quantum counting

What if you wanted to **count** the number of solutions, not just find them?

Given query access to $f : \{0,1\}^n \to \{0,1\}$, output an estimate $\tilde{M}$ of the number of marked inputs M, such that

$$(1-\epsilon)M \leq \tilde{M} \leq (1+\epsilon)M.$$

Solution: Grover search + phase estimation.

Quantum counting

Quantum counting

Recall that for Phase Estimation, we need:

Quantum counting

Recall that for Phase Estimation, we need:

1. (Controlled) unitary U (and its powers)
2. An eigenvector of U with eigenvalue $e^{i\theta}$

We output an estimate $\tilde{\theta}$ for θ.

Quantum counting

Unitary: we'll use the Grover iterate $G = RO_f$.

Quantum counting

Unitary: we'll use the Grover iterate $G = RO_f$.

On the 2-dimensional subspace $\mathrm{span}\{|\Gamma\rangle, |\Delta\rangle\}$, this is the rotation matrix

$$\begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

where $\sin\theta = \sqrt{M/N}$. The eigenvalues of this are $e^{i2\theta}$ and $e^{-i2\theta}$.

Quantum counting

The nontrivial eigenvectors of G are:

$$|\psi_\pm\rangle = \frac{1}{\sqrt{2}}\Big(|\Gamma\rangle \pm i\, |\Delta\rangle \Big).$$

Quantum counting

The nontrivial eigenvectors of G are:

$$|\psi_\pm\rangle = \frac{1}{\sqrt{2}}\Big(|\Gamma\rangle \pm i\,|\Delta\rangle \Big).$$

We run Phase Estimation with the state $|+\rangle^{\otimes n}$, which satisfies

$$|+\rangle^{\otimes n} = \alpha\,|\psi_+\rangle + \beta\,|\psi_-\rangle$$

for some $\alpha, \beta \in \mathbb{C}$.

Quantum counting

Running Phase Estimation, we get a state that is close to

$$\alpha |\psi_+\rangle |\widetilde{2\theta}\rangle + \beta |\psi_-\rangle |\widetilde{-2\theta}\rangle$$

Measuring the second register, we get an approximation of 2θ or -2θ with some probability. Assuming $\theta < \pi/2$, we can recover θ from either.

Quantum counting

Running Phase Estimation, we get a state that is close to

$$\alpha |\psi_+\rangle |\widetilde{2\theta}\rangle + \beta |\psi_-\rangle |\widetilde{-2\theta}\rangle$$

Measuring the second register, we get an approximation of 2θ or -2θ with some probability. Assuming $\theta < \pi/2$, we can recover θ from either.

Using t ancilla qubits, can estimate the phase to within 2^{-t}.

Quantum counting

The estimate of number of solutions is then

$$\tilde{M} = N(\sin\tilde{\theta})^2.$$

How far off is this from the true number of solutions?

Quantum counting

$$\left|\tilde{M} - M\right| = N\left|\sin(\theta + \delta)^2 - \sin(\theta)^2\right|$$

Quantum counting

$$\left|\tilde{M} - M\right| = N\left|\sin(\theta + \delta)^2 - \sin(\theta)^2\right|$$

$$= N\Big(\sin(\theta + \delta) + \sin(\theta)\Big)\Big(\sin(\theta + \delta) - \sin(\theta)\Big)$$

Quantum counting

$$\left|\tilde{M} - M\right| = N\left|\sin(\theta + \delta)^2 - \sin(\theta)^2\right|$$

$$= N\Big(\sin(\theta + \delta) + \sin(\theta)\Big)\Big(\sin(\theta + \delta) - \sin(\theta)\Big)$$

$$\leq N(2|\sin\theta| + \delta)\delta$$

Quantum counting

$$\left|\tilde{M} - M\right| = N\left|\sin(\theta + \delta)^2 - \sin(\theta)^2\right|$$

$$= N\Big(\sin(\theta + \delta) + \sin(\theta)\Big)\Big(\sin(\theta + \delta) - \sin(\theta)\Big)$$

$$\leq N(2|\sin\theta| + \delta)\delta$$

$$= N\left(2\sqrt{\frac{M}{N}} + \delta\right)\delta = 2\sqrt{NM}\delta + N\delta^2$$

Quantum counting

Thus the estimate satisfies

$$\left|\tilde{M} - M\right| \leq 2\sqrt{NM}\delta + N\delta^2$$

Quantum counting

Thus the estimate satisfies

$$\left|\tilde{M} - M\right| \leq 2\sqrt{NM}\delta + N\delta^2$$

Remember that $\delta \leq 2^{-t}$. Then choosing $t = \log\left(\frac{1}{\epsilon}\sqrt{\frac{N}{M}}\right)$ we get

$$(1-\epsilon)M \leq \tilde{M} \leq (1+\epsilon)M.$$

as desired.

Complexity of quantum counting

We're running phase estimation with t bits of precision, which means we're running $G, G^2, G^4, \cdots, G^{2^t}$ which means

$$1 + 2 + 4 + \cdots + 2^t = 2^{t+1} - 1$$

queries to O_f.

Complexity of quantum counting

This is at most

$$O\Big(\frac{1}{\epsilon}\sqrt{\frac{N}{M}}\Big)$$

queries – not much more than finding a **single** solution!

Complexity of quantum counting

This is at most

$$O\Big(\frac{1}{\epsilon}\sqrt{\frac{N}{M}}\Big)$$

queries – not much more than finding a **single** solution!

This also gives a way to find a solution without knowing M: first get estimate $\tilde{M}$, and then run $O(\sqrt{N/\tilde{M}})$ iterations!

Next time

Quantum complexity theory.