Week 11: Quantum counting, and starting quantum error correction

COMS 4281 (Fall 2025)

Admin

1. Practice worksheet 6, quiz out Wednesday.
2. Problem Set 2:
   2.1 Theory: due November 26
   2.2 Programming: due December 12 (week after Final)
3. In-class Final: December 4. Cumulative, but with more weight on the second half of class.

Last time

Let $N = 2^n$. We learned about Grover's algorithm for finding a marked input of an arbitrary boolean function $f : \{0,1\}^n \to \{0,1\}$ with $O(\sqrt{N})$ queries to f,

Last time

Let $N = 2^n$. We learned about Grover's algorithm for finding a marked input of an arbitrary boolean function $f : \{0,1\}^n \to \{0,1\}$ with $O(\sqrt{N})$ queries to f, assuming the function f has a unique solution.

Last time

Let $N = 2^n$. We learned about Grover's algorithm for finding a marked input of an arbitrary boolean function $f : \{0,1\}^n \to \{0,1\}$ with $O(\sqrt{N})$ queries to f, assuming the function f has a unique solution.

If there are M solutions, then a marked input can be found with $O(\sqrt{N/M})$ queries.

If there are M solutions, then the success probability curve of Grover's search algorithm after k iterations is given by

$$|\psi_k\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|\Gamma\rangle$$

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

$$|\Delta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \qquad \text{and} \qquad |\Gamma\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle \ .$$

If there are M solutions, then the success probability curve of Grover's search algorithm after k iterations is given by

$$|\psi_k\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|\Gamma\rangle$$

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

$$|\Delta\rangle = \frac{1}{\sqrt{N-M}} \sum_{x:f(x)=0} |x\rangle \qquad \text{and} \qquad |\Gamma\rangle = \frac{1}{\sqrt{M}} \sum_{x:f(x)=1} |x\rangle \ .$$

What is the distribution of outcomes if we measure $|\psi_k\rangle$?

If there are M solutions, then the success probability curve of Grover's search algorithm after k iterations is given by

$$|\psi_k\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|\Gamma\rangle$$

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

If we knew M, then we can pick k so that $\sin^2((2k+1)\theta)$ is close to 1.

If there are M solutions, then the success probability curve of Grover's search algorithm after k iterations is given by

$$|\psi_k\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|\Gamma\rangle$$

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

If we knew M, then we can pick k so that $\sin^2((2k+1)\theta)$ is close to 1. This entails choosing k to be approximately

$$\frac{\pi}{4\theta} - \frac{1}{2}\,.$$

If there are M solutions, then the success probability curve of Grover's search algorithm after k iterations is given by

$$|\psi_k\rangle = \cos((2k+1)\theta)\,|\Delta\rangle + \sin((2k+1)\theta)\,|\Gamma\rangle$$

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

If we knew M, then we can pick k so that $\sin^2((2k+1)\theta)$ is close to 1. This entails choosing k to be approximately

$$\frac{\pi}{4\theta} - \frac{1}{2}\,.$$

If we assume $M \ll N$, then we can use small-angle approximation $\sin\varphi \approx \varphi$, which implies $\theta \approx \sqrt{M/N}$. This means choosing

$$k \approx \frac{\pi}{4}\sqrt{\frac{N}{M}}$$

is essentially optimal.

What if the number of solutions M is not known in advance?

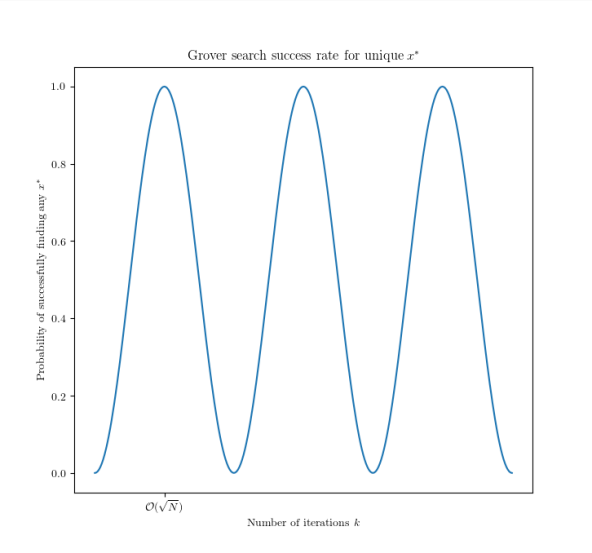
What if the number of solutions M is not known in advance?

What if we wanted to **count** the number of solutions?

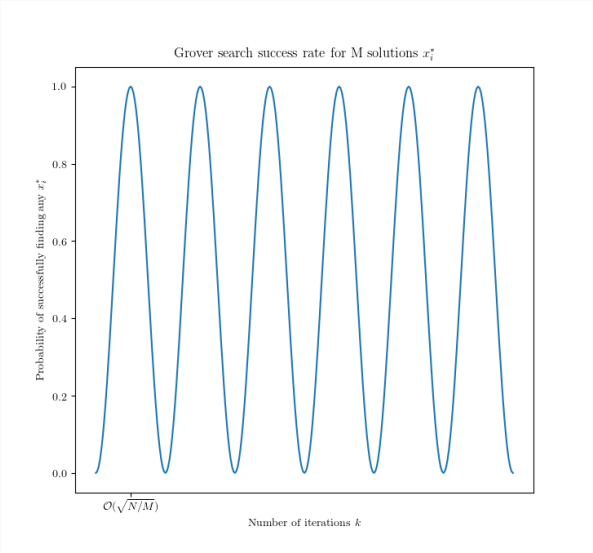
Quantum search with unknown number of solutions

Randomized stopping

Suppose the number of solutions M is unknown. The success probability curve of Grover's algorithm as a function of the number of iterations k could look like any of

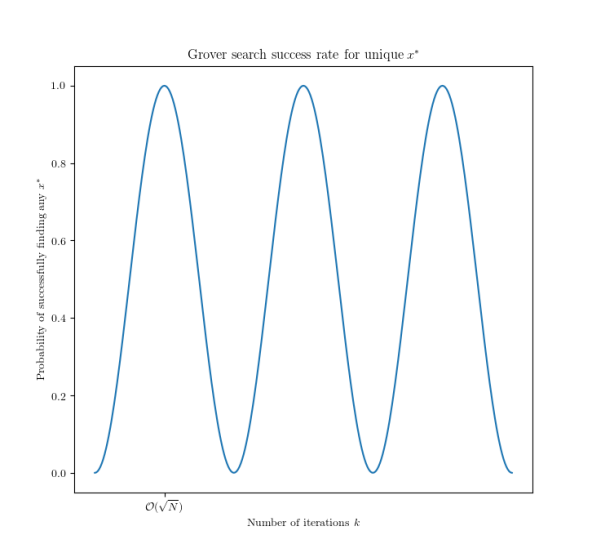


. . .

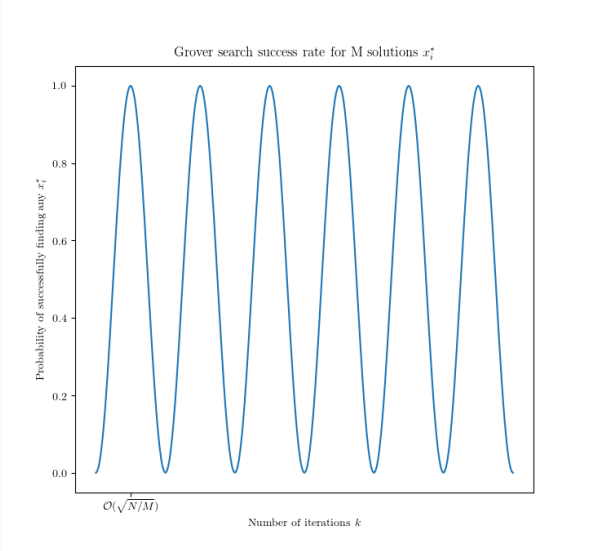


Randomized stopping

We can consider a variant of Grover's algorithm where the number of iterations k is chosen *randomly* between 1 and $\sqrt{N}$.

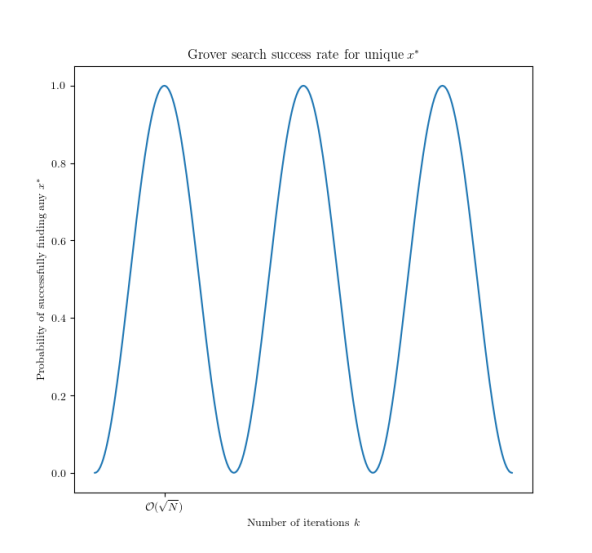


. . .

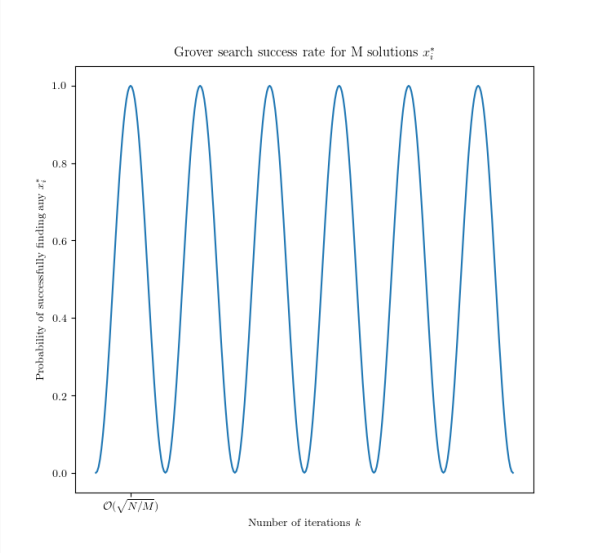


Randomized stopping

We can consider a variant of Grover's algorithm where the number of iterations k is chosen *randomly* between 1 and $\sqrt{N}$.



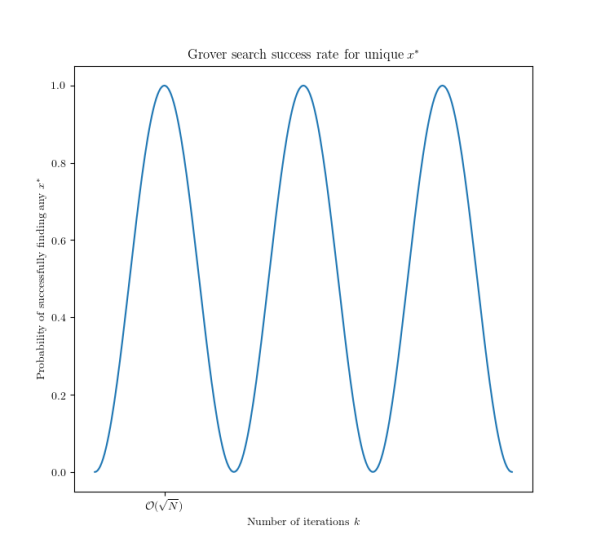
...



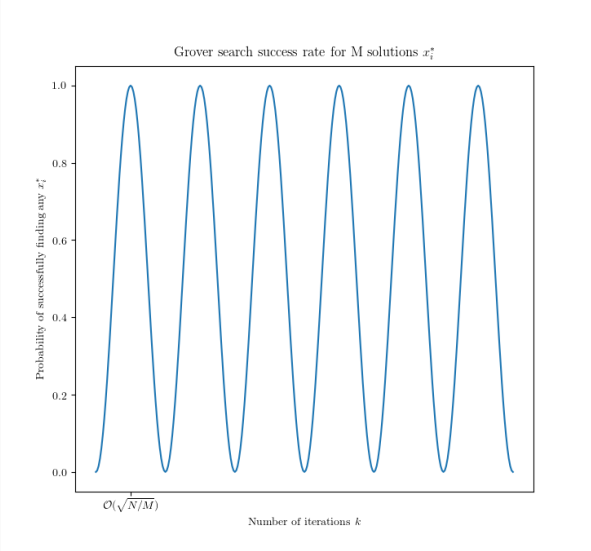
Then, no matter what M is, the *average* success probability should be at least some fixed percentage (say, close to 50%).

Randomized stopping

We can consider a variant of Grover's algorithm where the number of iterations k is chosen *randomly* between 1 and $\sqrt{N}$.



...



By running this variant, we can get a solution with roughly half probability. We can repeat a constant number of times to get a solution with high probability. You will explore this on the practice worksheet.

More efficient guessing

A smarter way is to try Grover with increasing number of iterations until a solution is found.

1: $R \leftarrow 1$
2: **while** $R \leq \sqrt{N}$ **do**
3: Choose k randomly from $\{1, \ldots, R\}$.
4: Run Grover with k iterations.
5: If a solution is found, exit.
6: Otherwise, let $R \leftarrow (4/3)R$.
7: **end while**

More efficient guessing

A smarter way is to try Grover with increasing number of iterations until a solution is found.

1: $R \leftarrow 1$
2: **while** $R \leq \sqrt{N}$ **do**
3: Choose k randomly from $\{1, \ldots, R\}$.
4: Run Grover with k iterations.
5: If a solution is found, exit.
6: Otherwise, let $R \leftarrow (4/3)R$.
7: **end while**

The range R of iterations grows exponentially:

$$R = 1, (4/3), (4/3)^2, (4/3)^3, \ldots \ .$$

More efficient guessing

A smarter way is to try Grover with increasing number of iterations until a solution is found.

1: $R \leftarrow 1$
2: **while** $R \leq \sqrt{N}$ **do**
3: Choose k randomly from $\{1, \ldots, R\}$.
4: Run Grover with k iterations.
5: If a solution is found, exit.
6: Otherwise, let $R \leftarrow (4/3)R$.
7: **end while**

In expectation, with $O(\sqrt{N/M})$ this algorithm will find a solution with high probability.

Quantum counting

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

Recall that for Phase Estimation, we need:

Quantum counting

Recall that for Phase Estimation, we need:

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

Quantum counting

Recall that for Phase Estimation, we need:

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

By querying powers up to U^{2^t}, phase estimation can obtain an estimate $\tilde{\theta}$ satisfying

$$\left|\theta - \tilde{\theta}\right| \leq 2^{-t} \ .$$

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

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

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

Let $\tilde{\theta}$ denote this approximation.

Quantum counting

The estimate of number of solutions is then

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

Quantum counting

The estimate of number of solutions is then

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

Let $t = \log\left(\frac{1}{\epsilon}\sqrt{\frac{N}{M}}\right)$. After some algebra, one can show that

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

Complexity of quantum counting

We're running phase estimation with precision 2^{-t}, 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

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

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

Complexity of quantum counting

This is at most

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

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 Error Correction.