Main Quantum Algorithms: Shor and Grover

Ronald de Wolf

Centrum Wiskunde & Informatica

Overview

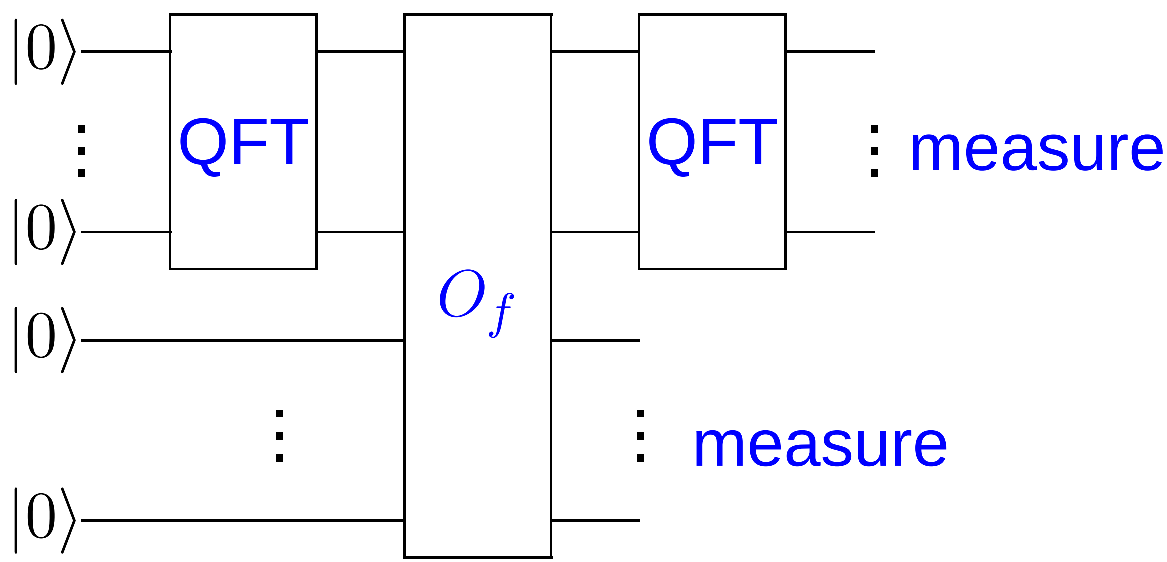
- Recap of previous lecture:
  - Quantum algorithm: circuit of elementary gates (such as Hadamard)
  - This transforms starting state to final state
  - Measurement of final state yields (classical) output
  - Algorithm is efficient it it uses few elementary gates
  - Examples: Deutsch-Jozsa and Simon algorithms
- Today's lecture:
  1. Shor's quantum algorithm for factoring
  2. Grover's quantum algorithm for search
  3. Other algorithms

Factoring

- Given $N = p \cdot q$, compute the prime factors p and q
- Fundamental mathematical problem since Antiquity
- Fundamental computational problem on $\log N$ bits
- Best known classical algorithms use time $2^{(\log N)^\alpha}$, where $\alpha = 1/2$ or $1/3$
- Its assumed computational hardness is basis of public-key cryptography (RSA)
- A quantum computer can break this,
  using Shor's efficient quantum factoring algorithm!

Overview of Shor's algorithm

- Classical reduction: choose random $x \in \{2, \ldots, N-1\}$. It suffices to find period r of $f(a) = x^a \bmod N$
- Shor's quantum algorithm for period-finding uses the quantum Fourier transform



- Overall complexity: roughly $(\log N)^2$ elementary gates

Reduction to period-finding

- Pick a random integer $x \in \{2, \ldots, N-1\}$, gcd(x, N)=1
- The sequence $x^0, x^1, x^2, x^3, \ldots$ mod N cycles:

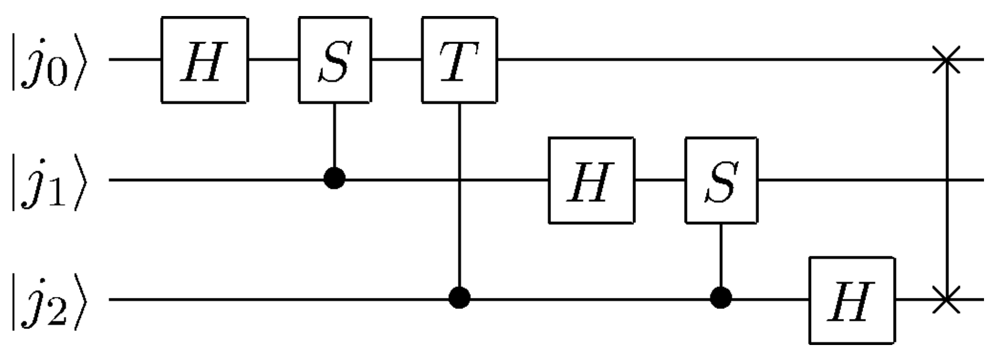
  has an unknown period r (min $r > 0$ s.t. $x^r \equiv 1$ mod N)
- For at least $1/4$ of the x's:
  r is even and $x^{r/2} \pm 1 \not\equiv 0$ mod N
- Then:

$$x^r = (x^{r/2})^2 \equiv 1 \text{ mod } N \iff$$
$$(x^{r/2}+1)(x^{r/2}-1) \equiv 0 \text{ mod } N \iff$$
$$(x^{r/2}+1)(x^{r/2}-1) = kN \text{ for some } k$$

- $x^{r/2} \pm 1$ shares a factor with N
- This factor of N can be extracted using gcd-algorithm

Quantum Fourier transform

- Fourier basis (dimension q): $|\chi_j\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{\frac{2\pi i j k}{q}} |k\rangle$
- Quantum Fourier Transform: $|j\rangle \mapsto |\chi_j\rangle$
- If $q = 2^\ell$, then can do this with $O(\ell^2)$ gates. $|\chi_{j_0 j_1 j_2}\rangle =$
  $\frac{1}{\sqrt{8}}(|0\rangle + e^{2\pi i 0.j_2}|1\rangle)(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)(|0\rangle + e^{2\pi i 0.j_0 j_1 j_2}|1\rangle)$



- For Shor: choose q power of 2 in $(N^2, 2N^2]$

Easy case: $r|q$

1. Apply QFT to 1st register of $|0\ldots0\rangle|0\ldots0\rangle$:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|0\rangle$$

2. Compute x^a mod N (repeated squaring)

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|a\rangle|x^a \text{ mod } N\rangle$$

3. Observing 2nd register gives $|x^s \text{ mod } N\rangle$ (random $s < r$)
   1st register collapses to superposition of

$$|s\rangle, |r+s\rangle, |2r+s\rangle, \ldots, |q-r+s\rangle$$

Easy case: $r|q$ (continued)

Recall: 1st register is in superposition $\sum_{j=0}^{q/r-1} |jr + s\rangle$

4. Apply QFT once more:

$$\sum_{j=0}^{q/r-1} \sum_{b=0}^{q-1} e^{2\pi i \frac{(jr+s)b}{q}} |b\rangle = \sum_{b=0}^{q-1} e^{2\pi i \frac{sb}{q}} \underbrace{\left(\sum_{j=0}^{q/r-1} \left(e^{2\pi i \frac{rb}{q}} \right)^j \right)}_{\text{geometric sum}} |b\rangle$$

Sum $\neq 0$ iff $e^{2\pi i \frac{rb}{q}} = 1$ iff $\frac{rb}{q}$ is an integer

Only the b that are multiples of $\frac{q}{r}$ have non-zero amplitude!

Easy case: $r|q$ (continued)

5. Observe 1st register: random multiple $b = c\frac{q}{r}$, $c \in [0, r)$:

$$\frac{b}{q} = \frac{c}{r}$$

- b and q are known; c and r are unknown
- c and r are coprime with probability $\Omega(1/\log\log r)$
- Then: we know r by writing $\frac{b}{q}$ in lowest terms
- Since we can find r, we can factor!

Hard case: $r \not| q$

- We do not have $\frac{b}{q} = \frac{c}{r}$ anymore
- Still, we probably observe a b such that $\left|\frac{b}{q} - \frac{c}{r}\right| \le \frac{1}{2q}$
- There is at most one fraction with denominator $< N$ in an interval of length $\frac{1}{q} < \frac{1}{N^2}$
- This fraction must be $\frac{c}{r}$
- Can compute $\frac{c}{r}$ from $\frac{b}{q}$ by continued fraction expansion
- Again, if c and r are coprime, then we know r

Summary for Shor's algorithm

- Reduce factoring to finding the period r of modular exponentiation function $f(a) = x^a \bmod N$
- Use quantum Fourier transform to find a multiple of q/r
- Repeat a few times to find r
- Overall complexity:
  - QFT takes $O(\log q)^2 \approx O(\log N)^2$ elementary gates
  - Modular exponentiation: $\approx (\log N)^2 \log\log N$ gates; classical computation by repeated squaring (use Schönhage-Strassen for fast multiplication)
  - Everything repeated $O(\log\log N)$ times
  - Classical postprocessing takes $O(\log N)^2$ gates
- Roughly $(\log N)^2$ elementary gates in total

Part 2:

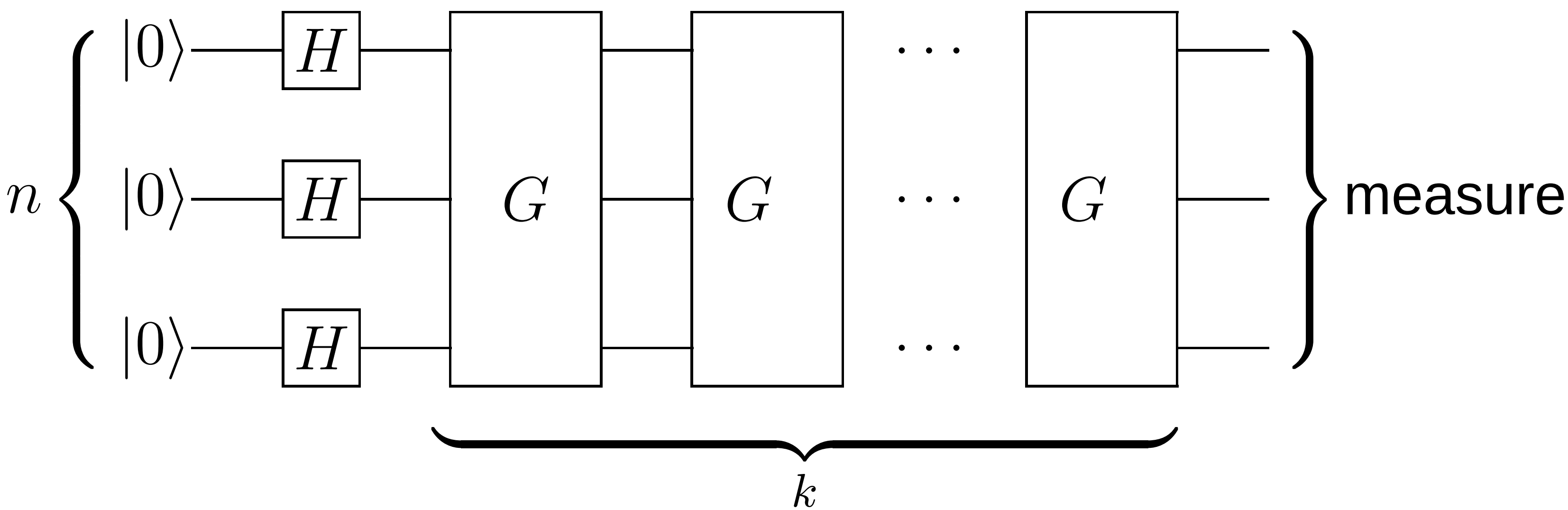
Grover's algorithm

The search problem

- We want to search for some good item in an unordered N-element search space
- Model this as function $f:\{0,1\}^n \to \{0,1\}$ ($N = 2^n$)
  $f(x) = 1$ if x is a solution
- We can query f:
  $O_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
  or
  $O_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$
- Goal: find a solution
- Classically this takes $O(N)$ steps (queries to f)
- Grover's algorithm does it in $\sqrt{N}$ steps

Grover's algorithm

- Define Grover iteration $G = H^{\otimes n} R H^{\otimes n} O_f$, where R negates $|x\rangle$ for all $x \neq 0^n$
- Apply G k times on uniform starting state



- Rough idea: each iteration moves $\frac{1}{\sqrt{N}}$ amplitude towards solutions $\Rightarrow k \approx \sqrt{N}$ iterations should suffice

Example

- $N = 4$, $f(00) = f(10) = f(11) = 0$, $f(01) = 1$, 1 iteration
- Starting state: $|00\rangle$
- After $H^{\otimes 2}$: $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
- The 4 parts of one Grover iterate G:
  - After O_f: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$
  - After $H^{\otimes 2}$: $\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$
  - After R: $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
  - After $H^{\otimes 2}$: $|01\rangle$, this is the index of the solution!
- We found the solution in a space of size 4, with 1 query!

Analysis

- Suppose y is the only solution, so $f(x) = 1$ iff $x = y$
- Define "good" and "bad" states:

$$|G\rangle = |y\rangle \qquad\qquad |B\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq y} |x\rangle$$

- All intermediate states are in span$\{|G\rangle, |B\rangle\}$
- Initial uniform state is $\sin(\theta)|G\rangle + \cos(\theta)|B\rangle$ for $\theta = \arcsin(1/\sqrt{N})$
- Grover iteration is a rotation over angle 2θ: after k iterations the state is

$$\sin((2k+1)\theta)|G\rangle + \cos((2k+1)\theta)|B\rangle$$

How many iterations do we need?

- Success probability after k iterations:

$$\sin^2((2k+1)\theta), \text{ with } \theta = \arcsin(1/\sqrt{N}) \approx 1/\sqrt{N}$$

- If $k = \dfrac{\pi}{4\theta} - \dfrac{1}{2}$, then success probability is $\sin^2(\pi/2) = 1$
- Example: $N = 4 \Rightarrow k = 1$
- Choose k nearest integer (small error)
- Query complexity is $k \approx \dfrac{\pi}{4}\sqrt{N}$
- Gate complexity is $O(\sqrt{N}\log N)$

Executive summary

- Quantum computers can search any N-element space in about $\sqrt{N}$ iterations
- That's $\sqrt{N}$ queries, and $\sqrt{N} \log N$ elementary gates
- If there are t solutions, then $\sqrt{\frac{N}{t}}$ iterations suffice
- The algorithm has a small error probability, but can be modified to error 0 *if* we know t

Application: Speed up NP problems

- Given a propositional formula $f(x_1, \ldots, x_n)$
  Computable in time poly(n)

  Question: is f satisfiable?

- This is a typical NP-complete problem
- Search space of $N = 2^n$ possibilities
- Classically: exhaustive search is the best we know.
  This takes about N steps
- Quantumly: Grover finds a satisfying assignment in
  $\sqrt{N} \cdot$ poly(n) steps

Other applications & generalizations

- Minimize $f : [N] \to \mathbb{R}$ in $\sqrt{N}$ steps
- Find collision in r-to-1 f in $(N/r)^{1/3}$ steps
- Approximate counting
- Amplitude amplification
- Find shortest path between 2 vertices in N-vertex graphs in $N^{3/2}$ steps
- Minimum spanning tree, other graph problems, . . .
- Faster sorting if we have limited space

Lower bound (BBBV 93)

- Fix a T-query quantum search algorithm
  $|\phi_y^t\rangle$ = state before t-th query, on f where only $f(y) = 1$
  α_y^t = amplitude on query y in $|\phi_\emptyset^t\rangle$ (constant-0 f)
  Compare constant-0 f with all other f
- Easy: $\| \phi_\emptyset^{t+1} - \phi_y^{t+1} \| \leq \| \phi_\emptyset^t - \phi_y^t \| + 2|\alpha_y^t|$, so
  $$\frac{1}{2} \leq \| \phi_\emptyset^{T+1} - \phi_y^{T+1} \| \leq 2 \sum_{t=1}^{T} |\alpha_y^t|$$
- Sum over all y: $\displaystyle \frac{N}{2} \leq \sum_{y \in \{0,1\}^n} 2 \sum_{t=1}^{T} |\alpha_y^t| = 2 \sum_{t=1}^{T} \sum_{y \in \{0,1\}^n} |\alpha_y^t|$
  $$\stackrel{\text{C.S.}}{\leq} 2 \sum_{t=1}^{T} \sqrt{N} \sqrt{\sum_{y \in \{0,1\}^n} |\alpha_y^t|^2} \leq 2T\sqrt{N} \Rightarrow \frac{\sqrt{N}}{4} \leq T$$

Other quantum algorithms

- Generalizations of Shor's algorithm
  - Discrete logarithm (Shor), elliptic curves
  - Hidden subgroup problem (Kitaev)
  - Pell's equation (Hallgren)

- Quantum random walks
  - Element distinctness (Ambainis)
  - Verifying $AB = C$ for matrices (Buhrman & Špalek)
  - Computing formulas (Farhi et al)

Summary: quantum algorithms

- Shor's algorithm (1994) factors an n-bit integer in roughly n^2 elementary quantum gates. This is
  - exponential speed-up over best known classical algo
  - breaks a lot of public-key cryptography
- Grover's algorithm (1996) searches a size-N search space in $\sim \sqrt{N}$ time
  - quadratic speed-up over classical
  - widely applicable
- Many other quantum algorithms discovered since then
- Next lecture: quantum communication