Lecture 23: Quantum Computation

Lecturer: *Sanjeev Arora* Scribe: *Zhifeng Chen, Jia Xu*

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)
There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof

We describe Kitaev's proof of this result since it uses eigenvalues, a more familiar and intuitive concept than the Fourier transforms used in Shor's algorithm.

DEFINITION 2 (EIGENVALUE) *λ is an* eigenvalue *of matrix M if there is a vector e (called the* eigenvector*) , s.t.:*

$$M \cdot e = \lambda e$$

Fact: If M is unitary, then $|\lambda| = 1$. In other words there is a $\theta \in [0, 1)$ such that

$$\lambda = e^{2\pi i\theta} = \cos(2\pi\theta) + i\sin(2\pi\theta).$$

Fact: If $M \cdot e = \lambda e$ then $M^k \cdot e = \lambda^k e$. Hence e is still an eigenvector of M^k and λ^k is the corresponding eigenvalue.

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)
There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof

PROOF: Let N be the number to be factored. As usual, Z_N^* is the set of numbers mod N that are co-prime to N. Simple number theory shows that for every $a \in Z_N^*$ there is a smallest integer r such that $a^r \equiv 1 \pmod N$; this r is called the *order* of a. The algorithm uses the well-known fact that if we can compute the order of random elements of Z_N^* then we can factor N with high probability. The reason is that if $(a^r - 1) \equiv 0 \pmod N$, then $(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \pmod N$. If a is random, with probability $\geq \frac{1}{2}$, $a^{\frac{r}{2}} \neq 1 \pmod N$, $a^{\frac{r}{2}} \neq -1 \pmod N$ (this is a simple exercise using the Chinese remainder theorm) and hence $gcd(N, a^{\frac{r}{2}} - 1) \neq N, 1$. Thus, knowing r we can compute $a^{r/2}$ and compute $gcd(N, a^{\frac{r}{2}} - 1)$. With probability at least 1/2 (over the choice of a) this method yields a factor of N.

Sketch of Kitaev's quantum circuit for factoring integers

The factoring algorithm is a mixture of a classical and a quantum algorithm. Using classical random bits it generates a random $a \in Z_N^*$ and then constructs a quantum circuit. Observing the output of this quantum circuit a few times followed by some more classical computation allows it to obtain r, the order of a, with reasonable probability. (Of course, we could in principle describe the entire algorithm as a quantum algorithm instead of as a mixture of a classical and a quantum algorithm, but our description isolates exactly where quantum mechanics is crucial.)

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)

There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

Consider a classical reversible circuit that acts on numbers in Z_N^*, and is described by $U(x) = ax \pmod N$. Then we can view this circuit as a quantum circuit operating on a quantum register. If the quantum register is in the superposition[1]

$$\sum_{x \in Z_N^*} \alpha_x |x\rangle,$$

then applying U gives the superposition

$$\sum_{x \in Z_N^*} \alpha_x \,|\, ax \pmod N\rangle.$$

Interpret this quantum circuit as an $N \times N$ matrix —also denoted U—and consider its eigenvalues.

Since $U(x) = ax \pmod N$ and $a^r \equiv 1 \pmod N$;

This implies $U(x)^r = a^r x \pmod N \equiv 1 \pmod N$ so $U^r = I$

Since $U^r = I$, we can easily check that each eigenvalue has the form $e^{2\pi i\theta}$ where $\theta = \frac{j}{r}$ for some $j \le r$. The algorithm will try to obtain a random eigenvalue. It thus obtains —in binary expansion— a number of form $\frac{j}{r}$ where j is random. It turns out that the chance is pretty good that this j is coprime to r, which means that $\frac{j}{r}$ is an irreducible fraction. Even knowing only the first $2 \log N$ bits in the binary expansion of $\frac{j}{r}$, the algorithm can round off to the nearest fraction whose denominator is at most N (this can be done; easy number theory) and then it reads off r from the denominator.

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)
There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

Recall: λ *is an* eigenvalue *of matrix* **U** *if there is a vector e (called the* eigenvector*) , s.t.:*

$$\mathbf{U} \cdot e = \lambda e$$

Now we describe how to compute the first $2 \log N$ bits of a random eigenvalue of U. Assume for now that the algorithm has a quantum register whose state is a superposition, denoted $\vec{e}$, corresponding to a random eigenvector of U. (See below for details on how to put a register in such a state.) Then applying U gives the final state $\lambda\vec{e}$, where λ is the eigenvalue associated with $\vec{e}$. Thus the register's state has undergone a *phase shift* —i.e., multiplication by a scalar— although there is yet no direct way to measure λ.

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)

There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

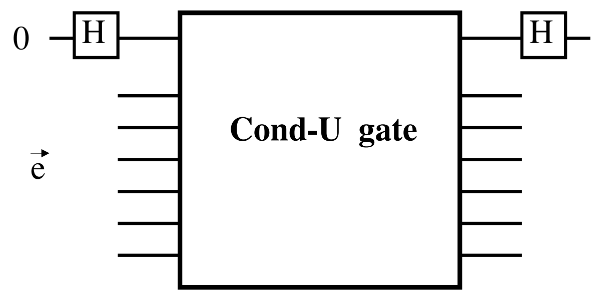

Figure 7: Basic block: Conditional-U gate and two Hadamard gates.

Using cond-U circuit and two Hadamard gates, we can build a quantum circuit shown in Figure 7. When this is applied to a quantum register whose first bit is 0 and the remaining bits are in a state $\vec{e}$, then we can measure the corresponding eigenvalue λ by repeated measurement of the first output bit.

$$\begin{aligned} |0\rangle\,|e\rangle &\xrightarrow{H_1} \frac{1}{\sqrt{2}}\,|0\rangle\,|e\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|e\rangle \\ &\xrightarrow{\text{cond-U}} \frac{1}{\sqrt{2}}\,|0\rangle\,|e\rangle + \frac{\lambda}{\sqrt{2}}\,|1\rangle\,|e\rangle \\ &\xrightarrow{H_2} \frac{1}{2}((1+\lambda)\,|0\rangle\,|e\rangle + (1-\lambda)\,|1\rangle\,|e\rangle) \end{aligned} \tag{8}$$

Thus the probability of measuring a 0 in the first bit is proportional to $|1+\lambda|$. We will refer to this bit as the *phase bit*, since repeatedly measuring it allows us to compute better and better estimates to λ. Actually, instead of repeated measuring we can just design a quantum circuit to do the repetitions by noticing that the output is just a scalar multiple of $\vec{e}$ again, so we can just feed it into another basic block with a fresh phase bit, and so on (see Figure 8). We measure phase bits all at once at the end.

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)

There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

Are we done? Unfortunately, no. Obtaining an estimate to the first m bits of λ would involve a circuit with 2^m phase bits (this is a simple exercise about probabilistic estimation), and when $m = 2\log N$, this number is about N, whereas we are hoping for a circuit size of $\mathrm{poly}(\log N)$. Thus simple repetition is a very inefficient way to obtain accurate information about λ.

A more efficient technique involves the observation that U has a special property: powers of U also have small circuits. Specifically, $U^{2^k}(x) = a^{2^k}x \pmod N$, and a^{2^k} is computable by circuits of size $\mathrm{poly}(\log N + \log k)$ using fast exponentiation.

Thus we can implement a conditional-U^{2^k} gate using a quantum circuit of size $\mathrm{poly}(\log N + k)$. The eigenvalues of U^{2^k} are λ^{2^k}. If $\lambda = e^{2\pi i\theta}$ where $\theta \in [0, 1)$ (see Figure 9) then $\lambda^{2^k} = e^{2\pi i\theta 2^k}$. Of course, $e^{2\pi i\theta 2^k}$ is the same complex number as $e^{2\pi i\alpha}$ where $\alpha = 2^k\theta \pmod 1$. Thus measuring λ^{2^k} gives us $2^k\theta \pmod 1$ and in particular the most significant bit of $2^k\theta \pmod 1$ is nothing but the kth bit of θ. Using $k = 0, 1, 2, \ldots 2\log N$ we can obtain the first $2\log N$ bits of θ.

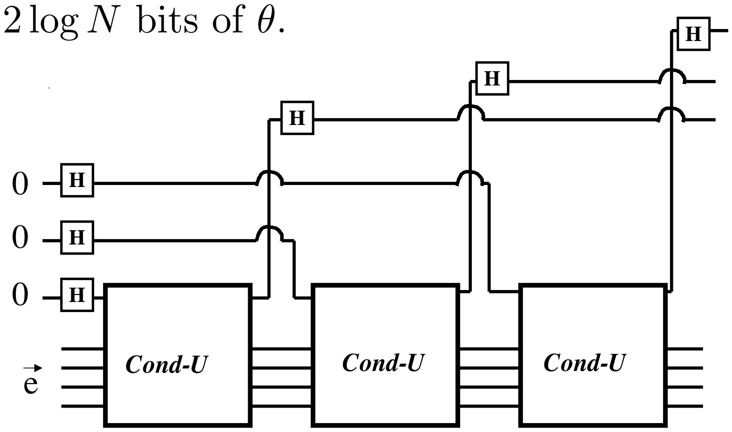

Figure 8: Repeating the basic experiment to get better estimate of λ.

As in Figure 8, we can bundle these steps into a single cascading circuit where the output of the conditional-$U^{2^{k-1}}$ circuit feeds into the conditional-U^{2^k} circuit. Each circuit has its own set of $O(\log N)$ phase bits; measuring the phase bits of the kth circuit gives an estimate of the kth bit of θ that is correct with probability at least $1 - 1/N$. All phase bits are measured in a single stroke at the end.

To finish, we show how to put a quantum register into a state corresponding to an eigenvector.

Factoring integers using a quantum computer

Theorem 3 (Shor 1994)

There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

6.1 Uniform superpositions of eigenvectors of U

Actually, we show how to put the quantum register into a uniform superposition of eigenvectors of U. This suffices for our cascading circuit, as we will argue shortly.

First we need to understand what the eigenvectors look like. Recall that $\{1, a, a^2, \ldots, a^{r-1}\}$ is a subgroup of Z_N^*. Let B be a set of representatives of all cosets of this subgroup. In other words, for each $x \in Z_N^*$ there is a unique $b \in B$ and $l \in \{0, 1, \ldots, r-1\}$ such that $x = ba^l \pmod N$. Then the following is the complete set of eigenvectors, where $\omega = e^{\frac{2\pi i}{r}}$:

$$\forall j \in \{0, 1, \ldots, r-1\}, \forall b \in B \qquad \vec{e}_{j,b} = \sum_{l=0}^{r-1} \omega^{jl} \left| ba^l \pmod N \right\rangle \tag{9}$$

The eigenvalue associated with this eigenvector is $\omega^{-j} = e^{-\frac{2\pi ij}{r}}$.

Fix b and consider the uniform superposition:

$$\frac{1}{r} \sum_{j=0}^{r-1} \vec{e}_{j,b} = \frac{1}{r} \sum_{j=0}^{r-1} \sum_{l=0}^{r-1} \omega^{jl} \left| ba^l \pmod N \right\rangle \tag{10}$$

$$= \frac{1}{r} \sum_{l=0}^{r-1} \sum_{j=0}^{r-1} \omega^{jl} \left| ba^l \pmod N \right\rangle. \tag{11}$$

Separating out the terms for $l = 0$ and using the formula for sums of geometric series:

$$= \frac{1}{r} \left(\sum_{j=0}^{r-1} |b\rangle + \sum_{l=1}^{r-1} \frac{(\omega^l)^r - 1}{\omega^l} \left| ba^l \pmod N \right\rangle \right) \tag{12}$$

since $\omega^r = 1$ we obtain

$$= |b\rangle \tag{13}$$

□

Thus if we pick an arbitrary b and feed the state $|b\rangle$ into the quantum register, then that can also be viewed as a uniform superposition $\frac{1}{r} \sum_j \vec{e}_{j,b}$.

Factoring integers using a quantum computer

THEOREM 3 (SHOR 1994)

There is a polynomial size quantum circuit that factors integers.

Kitaev's Proof, Continued

6.2 Uniform superposition suffices

Now we argue that in the above algorithm, a uniform superposition of eigenvectors is just as good as a single eigenvector.

Fixing b, the initial state of the quantum register is

$$\frac{1}{r}\sum_j \left|\vec{0}\right\rangle \left|\vec{e}_{j,b}\right\rangle,$$

where $\vec{0}$ denotes the vector of phase bits that is initialized to 0. After applying the quantum circuit, the final state is

$$\frac{1}{r}\sum_j \left|c_j\right\rangle \left|\vec{e}_{j,b}\right\rangle,$$

where $|c_j\rangle$ is a state vector for the phase bits that, when observed, gives the first $2\log N$ bits of j/r with probability at least $1-1/N$. Thus observing the phase bits gives us whp a random eigenvalue.