CS 593/MA 592 - Intro to Quantum Computing
Spring 2024
Tuesday, March 26 - Lecture 11.1

Today's scribe: Runwei Zhou [Note: note proofread by Eric]

Agenda:

1. Continued fractions
2. Shor's order
3. Finding algorithm
4. Time-permitting: finishing up the last lecture

1 Continued Fractions

An example of infinite ctd fraction is:

$$x = \frac{1}{5+\frac{1}{5+\frac{1}{5+\cdots}}} \Leftrightarrow x = \frac{1}{5+x},\ x = \sqrt{5}-1 \text{ (informal)} \tag{1}$$

Every real number admits a more or less unique ctd fraction representative. A real number is rational if and only if it has a finite ctd fraction representative.

Definition.

$$[a_0, a_1, \cdots, a_N] = a_0 + \frac{1}{a_1 + \frac{1}{a_2+\frac{1}{\cdots+\frac{1}{a_N}}}} \tag{2}$$

The n^{th} convergent is the "truncated" continued fraction $[a_0, a_1, \cdots, a_N]$.

Theorem 1. *Given a rational number x expressed as a binary fraction with L bits, we can find a continued fraction presentation of x in (classical) poly time* $O(L^3)$

For example, we have:

$$\frac{77}{65} = 1 + \frac{12}{65} = 1 + \frac{1}{\frac{65}{12}} = 1 + \frac{1}{5+\frac{5}{12}} = \cdots = 1 + \frac{1}{5+\frac{1}{2+\frac{1}{2+\frac{1}{2}}}} = [1,5,2,2,2] \tag{3}$$

Theorem 2. *Let x be any real number, and suppose $\frac{p}{q}$ is a rational number such that*

$$\|\frac{p}{q} - x\| \leq \frac{1}{q^2} \tag{4}$$

Then $\frac{p}{q}$ is a convergent of any continued fraction representation of x

Among all rational approximations to x with a given denominator q, the best ones come from the convergence of the combined fraction representation of x. In particular, if x is a binary fraction. These "best approximations" can be formed in time $O(L^3)$.

2 Shor's Order Finding Algorithm

Definition (Order-Finding problem)**.** *The input and output of order-finding problem is:*

INPUT: two integrers N (with L bits), x written in binary with $1 \leq x \leq N$*,* $\gcd(x,N) = 1$.

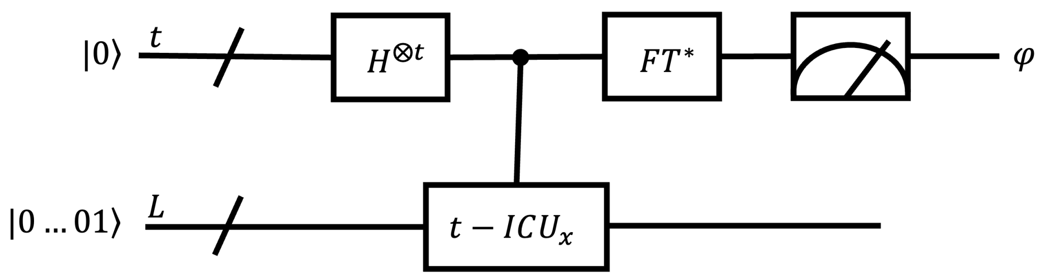
OUTPUT: r, the order of x $\bmod N$*, i.e. smallest* $r \geq 1$ *such that* $x^r = 1 \mod N$.

We can define $U_x : (\mathbb{C}^2)^{\otimes 2} \to (\mathbb{C}^2)^{\otimes 2}$ *by:*

$$U_x|y\rangle = \begin{cases} |xy \mod N\rangle & \text{if } 0 \leq y \leq N-1 \\ |y\rangle & \text{else} \end{cases} \tag{5}$$

We hope to find U_x *who encodes the fraction* $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z}$*,* $y \to xy$*.*

We will find order r by applying phase estimation to U_x (In following, $t = 2L + 1 + [\log(2 + \frac{1}{\varepsilon})]$ will ensure phase estimation returns best $2L+1$ bit approximation to a phase with high confidence).



Two issues must be addressed:

1. How to build a quantum circuit for $t - ICU_x$?
2. How can we identify and prepare a/an (eigen) state of U_x such that running phase estimation on it will return a φ that tells us something useful about r?

Here are the corresponding answers:

1. Modular exponentiation trick. This is "easy" but it is the step that is most painful part of Shor's algorithm. It will require aqunatum circuit that uses $O(L^3)$ gates.
2. Eigenfunctions of U_x are fairly straight forward. Use continued factions to extract r from φ.

2.1 More on modular exponetiation

So what does $I - ICU_x$ do?

Write $z = z_t z_{t-1} \cdots z_1$ and let $y \in \mathbb{Z}/N\mathbb{Z}$, so y is a bit string of length L with $0 \leq y \leq N-1$.

$$\begin{aligned} t - ICU_x|k,y\rangle &= |z, U_x^{z_t 2^{t-1}} U_x^{z_{t-1} 2^{t-2}} \cdots U_x^{z_1 2^0} y\rangle \\ &= |z, x^{z_t 2^{t-1}} x^{z_{t-1} 2^{t-2}} \cdots x^{z_1 2^0} y\rangle \\ &= |z, x^z y\rangle \end{aligned} \tag{6}$$

So that $t - ICU_x$ multiplies contents of second register (i.e. y) by a power of x with the power determined by contents of first register (i.e. z)

Definition (Modular exponentiation trick)**.** *Given x, N(N has L bits,* $1 < x \leq N$*), one can compute the function*

$$z \leftarrow x^z \mod N \tag{7}$$

Where z has $O(L)$ *bits. Classically in time* $O(L^3)$

One can dilate a classical Boolean circuit into a unitary circuit in the ”usual way” to get a circuit that implements $t - ICU_x$.

2.2 More details on eigenstates of U_x

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp \frac{-2\pi isk}{r} |x^k \pmod{N}\rangle \tag{8}$$

Then $0 \leq s \leq r-1$,

$$\begin{aligned} U_x|u_{>s}\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp \frac{-2\pi isk}{r} |x^{k+1} \pmod{N}\rangle \\ &= \exp \frac{2\pi is}{r} |U_s\rangle \end{aligned} \tag{9}$$

Where do these formulas come from?

Let $H = \langle x \rangle \leq (\mathbb{Z}/N\mathbb{Z})^*$ be the finite cyclic group guaranteed by x (under multiplication). U_x is basically the same thing as specifying a representation:

$$\rho : H \to U(\mathbb{C}[\mathbb{Z}/N\mathbb{Z}]) \leq (\mathbb{C}^2)^{\otimes 2} \tag{10}$$

Where $\rho^n|y\rangle = |hy \mod N\rangle$.[1]

Running QPE with U_x and $|u_s\rangle$ returns φ, the best $2L+1$ bit approximation to $\frac{s}{r}$(with high probability) in particular $\|\frac{s}{r} - \varphi\| \leq \frac{1}{2r^2}$. Thus, $\frac{s}{r}$ occurs as a convergent of the continued fraction representation of φ. We can find the continued fraction representation of φ in time $O(L^3)$ classically. So, as long as $\gcd(s,r) = 1$, we can get r by finding among the demoninators of the convergence of φ.

2.3 Lost remaining problem

Now do we prepare the state $|u_s\rangle$ for some s that is coprime to r? WE CAN’T!

Because we don’t already know r. Instead, we will plug in $|1\rangle = |1 \mod N\rangle = |0,0,\cdots,0,1\rangle$ (L bits) to QPF.

$$|1\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle \tag{11}$$

With this φ will be best $2L+1$ bit approximation to $\frac{s}{r}$ for s, a uniformly randomly chosen value in $0 \leq s \leq r+1$.

[1] $\|H\| = r$