Quantum algorithms (CO 781, Winter 2008)
Prof. Andrew Childs, University of Waterloo

LECTURE 5: Period finding from $\mathbb{Z}$ to $\mathbb{R}$

In the last lecture, we defined a periodic function over $\mathbb{R}$ whose period is an irrational number (the regulator) encoding the solutions of Pell's equation. In this lecture we will review Shor's approach to period finding, and show how it can be adapted to find an irrational period.

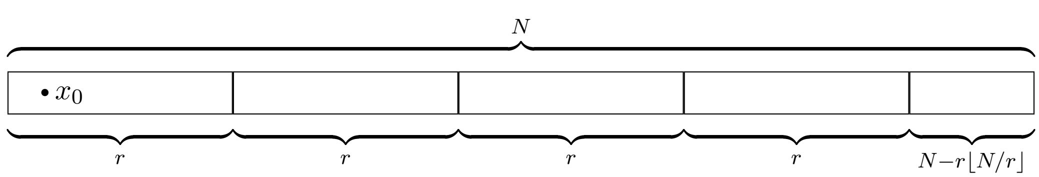
Period finding over the integers Shor's algorithm for factoring the number L works by finding the period of the function $f : \mathbb{Z} \to \mathbb{Z}_L$ defined by $f(x) = a^x \bmod L$ (where a is chosen at random). In other words, we are trying to find the smallest positive integer r such that $a^x \bmod L = a^{x+r} \bmod L$ for all $x \in \mathbb{Z}$. Note that since the period does not, in general, divide a known number N, we cannot simply reduce this task to period finding over $\mathbb{Z}_N$; rather, we should really think of it as period finding over $\mathbb{Z}$ (or, equivalently, the hidden subgroup problem over $\mathbb{Z}$).

Of course, we cannot hope to represent arbitrary integers on a computer with finitely many bits of memory. Instead, we will consider the function only on the inputs $\{0, 1, \ldots, N-1\}$ for some chosen N, and we will perform Fourier sampling over $\mathbb{Z}_N$. We will see that this procedure can work even when the function is not precisely periodic over $\mathbb{Z}_N$. Of course, this can only have a chance of working if the period is sufficiently small, since otherwise we could miss the period entirely. Later, we will see how to choose N if we are given an a priori upper bound of M on the period. If we don't initially have such a bound, we can simply start with $M = 2$ and repeatedly double M until it's large enough for period finding to work. The overhead incurred by this procedure is only $\mathrm{poly}(\log r)$.

Given a value of N, we prepare a uniform superposition over $\{0, 1, \ldots, N-1\}$ and compute the function in another register, giving

$$\frac{1}{\sqrt{N}} \sum_{x \in \{0,\ldots,N-1\}} |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{x \in \{0,\ldots,N-1\}} |x, f(x)\rangle. \tag{1}$$

Next we measure the second register, leaving the first register in a uniform superposition over those values consistent with the measurement outcome. When f is periodic with minimum period r, we obtain a superposition over points separated by the period r. The number of such points, n, depends on where the first point, $x_0 \in \{0, 1, \ldots, r-1\}$, appears. When restricted to $\{0, 1, \ldots, N-1\}$, the function has $\lfloor N/r \rfloor$ full periods and $N - r\lfloor N/r \rfloor$ remaining points, as depicted below. Thus $n = \lfloor N/r \rfloor + 1$ if $x_0 < N - r\lfloor N/r \rfloor$ and $n = \lfloor N/r \rfloor$ otherwise.



Discarding the measurement outcome, we are left with the quantum state

$$\mapsto \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |x_0 + jr\rangle \tag{2}$$

where x_0 occurs nearly uniformly random (it appears with probability n/N) and is unknown. To obtain information about the period, we apply the Fourier transform over $\mathbb{Z}_N$, giving

$$\mapsto \frac{1}{\sqrt{nN}} \sum_{j=0}^{n-1} \sum_{k \in \mathbb{Z}_N} \omega_N^{k(x_0+jr)} |k\rangle \tag{3}$$

$$= \frac{1}{\sqrt{nN}} \sum_{k \in \mathbb{Z}_N} \omega_N^{kx_0} \sum_{j=0}^{n-1} \omega_N^{jkr} |k\rangle. \tag{4}$$

Now if we were lucky enough to choose a value of N for which $r|N$, then in fact $n = N/r$ regardless of the value of x_0, and the sum over j above is if $r|N$ then $n = N/r$ for all x_0, i.e.

$$\sum_{j=0}^{n-1} \omega_N^{jkr} = \sum_{j=0}^{n-1} \omega_n^{jk} \tag{5}$$

$$= n\delta_{k \bmod n,0}. \tag{6}$$

In this especially simple case, the quantum state is

$$\frac{n}{\sqrt{nN}} \sum_{k \in \mathbb{Z}_N} \omega_N^{kx_0} \delta_{k \bmod n,0} = \frac{1}{\sqrt{r}} \sum_{k \in n\mathbb{Z}_r} \omega_N^{kx_0} |k\rangle, \tag{7}$$

and measurement of k is guaranteed to give an integer multiple of $n = N/r$, with each of the r multiples occurring with probability $1/r$. But more generally, the sum over j in (4) is the geometric series

$$\sum_{j=0}^{n-1} \omega_N^{jkr} = \frac{\omega_N^{krn} - 1}{\omega_N^{kr} - 1} \tag{8}$$

$$= \omega_N^{(n-1)kr/2} \frac{\sin \frac{\pi krn}{N}}{\sin \frac{\pi kr}{N}}. \tag{9}$$

The probability of seeing a particular value k is given by the normalization factor $1/nN$ times the magnitude squared of this sum, namely

$$\Pr(k) = \frac{\sin^2 \frac{\pi krn}{N}}{nN \sin^2 \frac{\pi kr}{N}}. \tag{10}$$

From the case where $n = N/r$, we expect this distribution to be strongly peaked around values of k that are close to integer multiples of N/r. The probability of seeing $k = \lfloor jN/r \rceil = jN/r + \epsilon$ for some $j \in \mathbb{Z}$, where $\lfloor x \rceil$ denotes the nearest integer to x, is

$$\Pr(k = \lfloor jN/r \rceil) = \frac{\sin^2(\pi jn + \frac{\pi \epsilon rn}{N})}{nN \sin^2(\pi j + \frac{\pi \epsilon r}{N})} \tag{11}$$

$$= \frac{\sin^2 \frac{\pi \epsilon rn}{N}}{nN \sin^2 \frac{\pi \epsilon r}{N}}. \tag{12}$$

Now using the inequalities $x^2 - \frac{1}{3}x^4 \le \sin^2 x \le x^2$ (which can easily be proved by looking at the Taylor expansion of $\sin^2 x$), we have

$$\begin{aligned}
\Pr(k = \lfloor jN/r \rceil) &\ge \frac{(\frac{\pi\epsilon r n}{N})^2 - \frac{1}{3}(\frac{\pi\epsilon r n}{N})^4}{nN(\frac{\pi\epsilon r}{N})^2} && (13)\\
&= \frac{n^2 - \frac{1}{3}(\frac{\pi\epsilon r}{N})^2 n^4}{nN} && (14)\\
&\ge \frac{1}{r}\left(1 - \frac{\pi^2}{12}\right) + o(1/r) && (15)
\end{aligned}$$

where the second inequality follows because we can assume $-1/2 \le \epsilon \le 1/2$ (and the $o(1/r)$ term appears simply because n could be either slightly larger or slightly smaller than N/r). This bound shows that Fourier sampling produces a value of k that is the closest integer to one of the r integer multiples of N/r with probability lower bounded by a constant.

To discover r given one of the values $\lfloor jN/r \rceil$, we can divide by N to obtain a rational approximation to j/r that deviates by at most $1/2N$. Now we compute the continued fraction expansion

$$\frac{\lfloor jN/r \rceil}{N} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}, \qquad (16)$$

which gives a sequence of successively better approximations to $\lfloor jN/r \rceil / N$ by fractions (called the *convergents* of the expansion). We carry out this expansion until we obtain the closest convergent to $\lfloor jN/r \rceil / N$ whose denominator is smaller than M, our a priori upper bound on the period. (This can be done in polynomial time using standard techniques; see for example the second volume of Knuth's *The Art of Computer Programming*.) Since two distinct rational numbers, each with denominator less than M, can be no closer than $1/M^2$ (Proof: $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd} \ge \frac{1}{bd}$), the resulting denominator is guaranteed to be r provided we choose $N > M^2$.

Period finding over the reals Now suppose we are given a function $f : \mathbb{R} \to S$ satisfying $f(x + r) = f(x)$ for some $r \in \mathbb{R}$, and as usual, assume that f is injective within each (minimal) period. Now we'll see how to adapt Shor's procedure to find an approximation to r, even if it happens to be irrational.

To perform period finding on a digital computer, we must of course discretize the function. We have to be careful about how we perform this discretization. For example, suppose that $S = \mathbb{R}$. If we simply evaluate f at equally spaced points and round the resulting values (perhaps rescaled) to get integers, there is no reason for the function values corresponding to inputs separated by an amount close to the period to be related in any way whatsoever. It could be that the discretized function is injective, carrying absolutely no information about the period.

Instead we will discretize in such a way that the resulting function is *pseudoperiodic*. We say that $f : \mathbb{Z} \to S$ is *pseudoperiodic at* $k \in \mathbb{Z}$ *with period* $r \in \mathbb{R}$ if for each $\ell \in \mathbb{Z}$, either $f(k) = f(k + \lfloor \ell r \rfloor)$ or $f(k) = f(k - \lceil \ell r \rceil)$. We say that f is ϵ*-pseudoperiodic* if it is pseudoperiodic for at least an ϵ fraction of the values $k = 0, 1, \ldots, \lfloor r \rfloor$. We will require that the discretized function is ϵ-pseudoperiodic for some constant ϵ, and that it is injective on the subset of inputs where it is pseudoperiodic. Note that the periodic function encoding the regulator of Pell's equation can be constructed so that it satisfies these conditions.

Now let's consider what happens when we apply Fourier sampling to a pseudoperiodic function. As before, we will Fourier sample over $\mathbb{Z}_N$, with N to be determined later (again, depending on some a priori upper bound M on the period r). We start by computing the pseudoperiodic function on a uniform superposition:

$$\sum_{x \in \{0,\ldots,N-1\}} |x\rangle \mapsto \sum_{x \in \{0,\ldots,N-1\}} |x, f(x)\rangle. \tag{17}$$

Now measuring the second register gives, with constant probability, a value for which f is pseudoperiodic. Say that this value is $f(x_0)$ where $0 \le x_0 \le r$. As before, we see $n = \lfloor N/r \rfloor + 1$ points if $x_0 < N - r\lfloor N/r \rfloor$ or $n = \lfloor N/r \rfloor$ points otherwise (possibly offset by 1 depending on how the rounding occurs for the largest value of x, but let's not be concerned with this detail). We will write $[\ell]$ to denote an integer that could be either $\lfloor \ell \rfloor$ or $\lceil \ell \rceil$. With this notation, we obtain

$$\mapsto \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |x_0 + [jr]\rangle. \tag{18}$$

Next, performing the Fourier transform over $\mathbb{Z}_N$ gives

$$\begin{aligned} &\mapsto \frac{1}{\sqrt{nN}} \sum_{j=0}^{n-1} \sum_{k \in \mathbb{Z}_N} \omega_N^{k(x_0+[jr])} |k\rangle && (19)\\ &= \frac{1}{\sqrt{nN}} \sum_{k \in \mathbb{Z}_N} \omega_N^{kx_0} \sum_{j=0}^{n-1} \omega_N^{k[jr]} |k\rangle. && (20) \end{aligned}$$

Now we have $[jr] = jr + \delta_j$, where $-1 < \delta_j < 1$, so the sum over j is

$$\sum_{j=0}^{n-1} \omega_N^{k[jr]} = \sum_{j=0}^{n-1} \omega_N^{kjr} \omega_N^{k\delta_j}. \tag{21}$$

We would like this to be close to the corresponding sum in the case where the offsets δ_j are zero (which, when normalized, is $\Omega(1/\sqrt{r})$ by the same calculation as in the case of period finding over $\mathbb{Z}$). Consider the deviation in amplitude,

$$\begin{aligned} \left| \sum_{j=0}^{n-1} \omega_N^{kjr} \omega_N^{k\delta_j} - \sum_{j=0}^{n-1} \omega_N^{kjr} \right| &\le \sum_{j=0}^{n-1} |\omega_N^{k\delta_j} - 1| && (22)\\ &= \frac{1}{2} \sum_{j=0}^{n-1} \left| \sin \frac{\pi k \delta_j}{N} \right| && (23)\\ &\le \frac{1}{2} \sum_{j=0}^{n-1} \left| \frac{\pi k \delta_j}{N} \right| && (24)\\ &\le \frac{\pi k n}{2N}. && (25) \end{aligned}$$

At least insofar as this bound is concerned, the amplitudes may not be close for all values of k. However, suppose we only consider values of k less than $N/\log r$. (We will obtain such a k with probability about $1/\log r$, so we can condition on this event with only polynomial overhead.) For such a k, we have

$$\left|\frac{1}{\sqrt{nN}}\sum_{j=0}^{n-1}\omega_N^{k\lfloor jr\rceil}\right| = \Omega(1/\sqrt{r}) - O\big(\tfrac{1}{\sqrt{nN}}\cdot\tfrac{n}{\log r}\big) \tag{26}$$

$$= \Omega(1/\sqrt{r}) - O\big(\tfrac{1}{\sqrt{r}\log r}\big) \tag{27}$$

$$= \Omega(1/\sqrt{r}). \tag{28}$$

Thus, as in the case of period finding over $\mathbb{Z}$, Fourier sampling allows us to sample from a distribution for which some value $k = \lfloor jN/r\rceil$ (with $j \in \mathbb{Z}$) appears with reasonably large probability (now $\Omega(1/\operatorname{poly}(\log r))$ instead of $\Omega(1)$).

Finally, we must obtain an approximation to r using these samples. Since r is not an integer, the procedure used in Shor's period-finding algorithm does not suffice. However, we can perform Fourier sampling sufficiently many times that we obtain two values $\lfloor jN/r\rceil, \lfloor j'N/r\rceil$ such that j and j' are relatively prime, again with only polynomial overhead. We prove below that if $N \geq 3r^2$, then j/j' is guaranteed to be one of the convergents in the continued fraction expansion for $\lfloor jN/r\rceil/\lfloor j'N/r\rceil$. Thus we can learn j, and hence compute $jN/\lfloor jN/r\rceil$, which gives a good approximation to r: in particular, $|r - \lfloor jN/\lfloor jN/r\rceil\rceil| \leq 1$.

Lemma. *If $N \geq 3r^2$, then j/j' appears a convergent in the continued fraction expansion of $\lfloor jN/r\rceil/\lfloor j'N/r\rceil$. Furthermore, $|r - \lfloor jN/\lfloor jN/r\rceil\rceil| \leq 1$.*

Proof. A standard result on the theory of approximation by continued fractions says that if $a, b \in \mathbb{Z}$ with $|x - \frac{a}{b}| \leq \frac{1}{2b^2}$, then a/b appears as a convergent in the continued fraction expansion of x (see for example Hardy and Wright, *An Introduction to the Theory of Numbers*, Theorem 184.) Thus it is sufficient to show that

$$\left|\frac{\lfloor jN/r\rceil}{\lfloor j'N/r\rceil} - \frac{j}{j'}\right| < \frac{1}{2j'^2}. \tag{29}$$

Letting $\lfloor jN/r\rceil = jN/r + \mu$ and $\lfloor j'N/r\rceil = jN/r + \nu$ with $|\mu|, |\nu| \leq 1/2$, we have

$$\left|\frac{\lfloor jN/r\rceil}{\lfloor j'N/r\rceil} - \frac{j}{j'}\right| = \left|\frac{jN/r+\mu}{j'N/r+\nu} - \frac{j}{j'}\right| \tag{30}$$

$$= \left|\frac{jN+\mu r}{j'N+\nu r} - \frac{j}{j'}\right| \tag{31}$$

$$= \left|\frac{r(\mu j' - \nu j)}{j'(j'N+\nu r)}\right| \tag{32}$$

$$\leq \left|\frac{r(j+j')}{2j'^2N + j'r}\right| \tag{33}$$

$$\leq \frac{r}{j'N - r/2} \tag{34}$$

where in the last step we have assumed $j < j'$ wlog. This is upper bounded by $1/2j'^2$ provided $j'N \geq r/2 + 2j'^2 r$, which certainly holds if $N \geq 3r^2$ (using the fact that $j' < r$).

Finally

$$r - \frac{jN}{\left\lfloor \frac{jN}{r} \right\rceil} = r - \frac{jN}{\frac{jN}{r} + \mu} \tag{35}$$

$$= r - \frac{jNr}{jN + \mu r} \tag{36}$$

$$= \frac{\mu r^2}{jN + \mu r} \tag{37}$$

which is at most 1 in absolute value since $N \geq 3r^2$, $|\mu| \leq 1/2$, and $j \geq 1$. □

Related algorithms When combined with the periodic function described in the last lecture, this period-finding procedure gives an efficient quantum algorithm for solving Pell's equation (in the sense of approximating the regulator). To conclude, we mention some further applications of quantum computing to computational algebraic number theory.

Hallgren's original paper on Pell's equation also solves another problem, the *principal ideal problem*, which is the problem of deciding whether an ideal is principal, and if so, finding a generator of the ideal. Factoring reduces to the problem of solving Pell's equation, and Pell's equation reduces to the principal ideal problem; but no reductions in the other direction are known. Motivated by the possibility that the principal ideal problem is indeed harder than factoring, Buchmann and Williams designed a key exchange protocol based on it. Hallgren's algorithm shows that quantum computers can break this cryptosystem.

Subsequently, further related algorithms for problems in algebraic number theory have been found by Hallgren and, independently, by Schmidt and Vollmer. Specifically, they found polynomial-time algorithms for computing the unit group and the class group of a number field of constant degree. These algorithms require generalizing period finding over $\mathbb{R}$ to a similar problem over $\mathbb{R}^d$.