Lecture 10

Period finding in $\mathbb{Z}$. Also known as the Hidden Subgroup Problem (HSP) over $\mathbb{Z}$.

Comment: I decided to teach Shor's algorithm following the exposition in Section 3.3 of Jozsa's lecture notes which explains Shor's original approach. This is so that the similarity of the analysis of the query problem underlying Shor's algorithm, Period_N below, to the analysis of Simon's problem is self-evident. Indeed, Shor was directly inspired by Simon's algorithm when he came up with his algorithm: see this video. The exposition here differs from that of e.g., Nielsen and Chuang, which explains Kitaev's variant of Shor's algorithm.

We study the following query problem.

$$\text{Period}_N \colon D \subset (\mathbb{Z}_N)^{\mathbb{Z}} \to \{1, \dots, N\}, \tag{103}$$

where $x \in D$ if and only if there exists $r \in \mathbb{N}$ such that

$$x(s) = x(t) \iff s - t \in r\mathbb{Z} \coloneqq \{rz \mid z \in \mathbb{Z}\}, \tag{104}$$

Comment: In the language of the HSP, the ambiant group of this problem is $\mathbb{Z}$ and the hidden subgroup is $r\mathbb{Z}$.

Observe that for a given $x \in D$, the "r" associated with it is unique and we denote it by $\text{per}(x)$ (called "period of x"). (Proof: suppose both $r, r' \in \mathbb{N}$ are associated with x, then $x(0) = x(r) = x(r') \implies r - r' \in r\mathbb{Z} \cap r'\mathbb{Z} \implies r|(r-r')$ and $r'|(r-r') \implies r|r', r'|r \implies r = \pm r' \implies r = r'$ as $r, r' \in \mathbb{N}$.)

This does not technically fall into the query problem setup since the input x *can* be queried at an infinite number of points in $\mathbb{Z}$ but the algorithm we describe will only query x at points in $\{0, \dots, 2^n - 1\}$ for $n \coloneqq \lceil 2\log_2(N) \rceil + 1$.

The quantum algorithm uses the quantum Fourier transform.

Definition 19 (Quantum Fourier Transform)**.** For $M \in \mathbb{N}$, the quantum Fourier transform on $\mathbb{C}^M$ is the unitary $\text{QFT}_M \in \mathbb{C}^{M \times M}$ defined by

$$\text{QFT}_M |j\rangle = \sum_{k=0}^{M-1} \omega_M^{jk} |k\rangle , \tag{105}$$

for all $j \in \{0, 1 \dots, M-1\}$, where $w_M \coloneqq \exp(2\pi i/M)$. Comment: exercise: check that it is unitary.

Lemma 7 (Coprimality lemma)**.** *Let $r \in \mathbb{N}$ such that $r \geq 100$. The number of elements in $\{0, 1, \dots, r-1\}$ that are coprime to r (i.e., $\forall d \in \mathbb{N}, d|j, d|r \implies d = 1$), denoted $\phi(r)$ (Euler's totient function), satisfies*

$$\phi(r) \geq \frac{r}{5 \ln\ln(r)}, \tag{106}$$

where ln *is the natural logarithm.*

Remark 12. There's a more refined estimate: for $r \in \mathbb{N}, r \geq 3$, we have

$$\phi(r) \geq \frac{r}{e^\gamma \ln\ln(r) + \frac{3}{\ln\ln(r)}}, \tag{107}$$

where $e^\gamma \in [1.7810, 1.7812]$.

Proposition 11. $Q(\text{Period}_N) = O(\log\log(N))$.

Proof. Given input $x \in D$, let $r \coloneqq \text{per}(x)$. Assume wlog $N \geq 100$ as the claimed result is asymptotic. Assume wlog $r \geq 100$, else r will be found by classically querying $x(0), \dots, x(99)$. Observe that we must have $r \leq N$.

Let $n \coloneqq \lceil 2\log_2(N) \rceil + 1$ so that $2^n > N^2$ and write

$$2^n - 1 = Br + b, \tag{108}$$

in quotient remainder form, so that $B \in \{0, 1, \dots\}$ and $0 \leq b < r$.

Comment: a lot of the technical complications of this proof can be avoided if we assume $r|2^n$, as explained in Lecture 11.

Create the state

$$\frac{1}{\sqrt{2^n}} \sum_{s=0}^{2^n-1} |s\rangle |x(s)\rangle . \tag{109}$$

Measure the second register. Then the state of the first register becomes

$$\frac{1}{\sqrt{A+1}} \sum_{k=0}^{A} |x_0 + kr\rangle , \tag{110}$$

for some $x_0 \in \{0, 1, \ldots, r-1\}$, where $A = B$ if $x_0 \leq b$ and $A = B - 1$ if $x_0 > b$. Comment: draw picture.

Now we apply the QFT_M to Eq. (110) to obtain

$$\frac{1}{\sqrt{2^n(A+1)}} \sum_{y=0}^{2^n-1} \sum_{k=0}^{A} \omega^{(x_0+kr)y} |y\rangle = \frac{1}{\sqrt{2^n(A+1)}} \sum_{y=0}^{2^n-1} \omega^{x_0 y} \Big(\sum_{k=0}^{A} \omega^{kry} \Big) |y\rangle \,, \tag{111}$$

where $\omega := \omega_{2^n}$.

We analyze the sum in brackets:

$$1 + \omega^{ry} + \cdots + \omega^{Ary}. \tag{112}$$

As y goes from 0 to $2^n - 1$, $ry/2^n$ goes from 0 to $r - r/2^n \in (r-1, r)$ in increments of $r/2^n$. For $j \in \{0, 1, \ldots, r-1\}$, let $y_j \in \{0, 1, \ldots, 2^n - 1\}$ be such that $ry_j/2^n$ is closest to j (if there's a tie, let y_j be the smaller). Comment: draw number line from 0 to r, mark the integers and the increments. Then, we have

$$\left| \frac{ry_j}{2^n} - j \right| \leq \frac{1}{2} \frac{r}{2^n}. \tag{113}$$

and so we can write

$$\frac{ry_j}{2^n} = j + \eta_j, \tag{114}$$

where $|\eta_j| \leq r/2^{n+1} < N/(2N^2) = 1/(2N)$. Then

$$S_j := \sum_{k=0}^{A} \omega^{kry_j} = \sum_{k=0}^{A} \exp(2\pi i \cdot kry_j/2^n) = \sum_{k=0}^{A} \exp(2\pi i \cdot k\eta_j). \tag{115}$$

Two cases:

1. $\eta_j = 0$. Then $S_j = A + 1$.
2. $\eta_j \neq 0$. Then

$$\begin{aligned}
|S_j|^2 =& \left| \frac{1 - \exp(2\pi i \cdot (A+1)\eta_j)}{1 - \exp(2\pi i \cdot \eta_j)} \right|^2 && \text{sum geometric series} \\
=& \left| \frac{\exp(-\pi i \cdot (A+1)\eta_j) - \exp(\pi i \cdot (A+1)\eta_j)}{\exp(-\pi i \cdot \eta_j) - \exp(\pi i \cdot \eta_j)} \right|^2 \\
=& \frac{\sin^2(\pi(A+1)\eta_j)}{\sin^2(\pi\eta_j)} \\
\geq& \frac{\sin^2(\pi(A+1)\eta_j)}{\pi^2\eta_j^2} && \forall \theta \in \mathbb{R}, \sin(\theta)^2 \leq \theta^2
\end{aligned}$$

Now,

$$|\pi(A+1)\eta_j| = \pi(A+1)|\eta_j| \leq \pi(B+1)r/2^{n+1} \leq \pi/2 + \pi r/2^{n+1} < \pi/2 + \pi/(2N) \leq 0.505\pi, \tag{116}$$

where the last inequality uses $N \geq 100$. But $\sin^2(\theta) \geq \theta^2/3$ for all $\theta \in [-0.505\pi, 0.505\pi]$ Comment: for safety, I've used a rather loose bound here, so

$$|S_j|^2 \geq \frac{(A+1)^2}{3}. \tag{117}$$

Therefore, if we measure the state in Eq. (111) in the computational basis, the probability of the measurement outcome being y_j for some $j \in \{0, 1, \ldots, r-1\}$ that is coprime to r is at least:

$$\begin{aligned}
& \frac{r}{5\ln\ln(r)} \cdot \frac{1}{2^n(A+1)} \cdot \frac{(A+1)^2}{3} \\
=& \frac{1}{\ln\ln(r)} \frac{r(A+1)}{15 \cdot 2^n} \\
\geq& \frac{1}{\ln\ln(r)} \frac{rB}{15 \cdot 2^n} \\
=& \frac{1}{\ln\ln(r)} \frac{2^n - 1 - b}{15 \cdot 2^n} \\
\geq& \frac{1}{\ln\ln(r)} \frac{2^n - r}{15 \cdot 2^n} \\
\geq& \frac{1}{\ln\ln(r)} \frac{1}{15} \Big(1 - \frac{1}{N}\Big) && r/2^n \leq N/2^n < N/N^2 = 1/N \\
\geq& \frac{1}{\ln\ln(r)} 0.05 && N \geq 100
\end{aligned}$$

Comment: it took many lines above to nail down the details but the point is just that at the second line we have $r(A+1) \approx 2^n$.

The overall algorithm is described as follows:

Set $r^* = N + 1$.

Repeat the following $10000 \ln \ln(N)$ times.

Run the procedure described above and let z be the outcome of the measurement. Compute some $r' \in \mathbb{N}$, $r' \leq N$ and $j' \in \{0, 1, \ldots, r' - 1\}$ coprime to r' such that

$$\left| \frac{z}{2^n} - \frac{j'}{r'} \right| \leq \frac{1}{2} \frac{1}{2^n}. \tag{118}$$

There are two cases:

(a) If no such pairs r', j' exist, then skip to the next repeat.

(b) If r', j' exist, verify if $x(0) = x(r')$ using 2 queries. If $r' \leq r^*$, set $r^* = r'$.

After all repeats are finished, output r^*.

Comment: (i) verifying $r' = \text{per}(x)$ is harder than verifying $x(0) = x(r')$ as r' could be a multiple of the period; (ii) the computation can be done by trying all possible pairs r', j' – we don't care about the cost of this for query complexity. However, this takes $\Omega(N)$ steps and is *emphatically not* what we would do if we want a $O(\text{poly}(\log(N)))$ *time* quantum algorithm, see later lectures.

We now argue that with very high probability, this procedure will yield the period r. We consider the following two cases at each repeat. Let z denote the measurement outcome.

1. z is indeed y_j for some j coprime to r. Then
$$\left| \frac{rz}{2^n} - j \right| \leq \frac{1}{2} \frac{r}{2^n} \tag{119}$$
and so
$$\left| \frac{z}{2^n} - \frac{j}{r} \right| \leq \frac{1}{2} \frac{1}{2^n}. \tag{120}$$
So certainly r', j' exist. But $r' \in \mathbb{N}$, $r' \leq N$ and $j' \in \{0, 1, \ldots, r' - 1\}$ is coprime to r' satisfies
$$\left| \frac{z}{2^n} - \frac{j'}{r'} \right| \leq \frac{1}{2} \frac{1}{2^n}, \tag{121}$$
Then we must have $j/r = j'/r'$, since
$$jr' \neq j'r \implies \left| \frac{j}{r} - \frac{j'}{r'} \right| = \left| \frac{jr' - j'r}{rr'} \right| \geq \frac{1}{N^2}, \tag{122}$$
but
$$\left| \frac{j}{r} - \frac{j'}{r'} \right| \leq \frac{1}{2^n} < \frac{1}{N^2}, \tag{123}$$
which is a contradiction. Comment: we've not used co-primeness before this, only $r, r' \leq N$: the above analysis shows that for any $a \in \mathbb{R}$ there can be at most one fraction with denominator less than or equal to N that approximates a to precision $< 1/N^2$; this fact is what motivated the choice of n to be $\lceil 2 \log_2(N) \rceil + 1$ But j is coprime to r and j' is coprime to r' so $j/r = j'/r' \implies j = j'$ and $r = r'$. Therefore, $r' = r$ and r^* is set to r.

2. z is not y_j for some j coprime to r. Assume wlog that r', j' still exist and satisfies $x(0) = x(r')$ (else, nothing happens in this repeat). Then $r' - 0 \in r\mathbb{Z}$ so $r | r'$ so $r' \geq r$ and so r^* is set to an integer that is at least r.

The above analysis means if the first case occurs in at least one of the $10000 \ln \ln(N)$ repeats, then the output of the algorithm will be correct.

At each repeat, the probability that the first case occurs is at least

$$0.05 \frac{1}{\ln \ln(r)} \geq 0.05 \frac{1}{\ln \ln(N)}. \tag{124}$$

Therefore, the probability of the first case not occuring across all repeats (this is the probability of failure) is at most

$$\left(1 - 0.05 \frac{1}{\ln \ln(N)}\right)^{10000 \ln \ln(N)} \leq e^{-500} \leq 1/3, \tag{125}$$

as required.

□

Comment: we didn't cover the following in Lecture 10 but you may find it interesting, especially if you're worried about using Lemma 7 without knowing its proof.

We can prove a "poor man's version" the coprimality lemma (Lemma 7). Reference: Appendix 4, Problem 4.1 of Nielsen and Chuang. Since we can prove this lemma from first principles, it means that we can prove $Q(\text{Period}_N) = O(\log N)$ from first principles (which would also lead to a poly$(\log(N))$ time quantum algorithm for factoring $N \in \mathbb{N}$).

Lemma 8. *For $r \in \mathbb{N}$, let $\pi(r)$ denote the number of elements in $\{1, \ldots, 2r\}$ that are prime. Then*

$$\pi(2r) \geq \frac{r}{\log_2(2r)}, \tag{126}$$

in particular, $\phi(2r) \geq r/\log_2(2r) - 1$. Comment: -1 since $2r$ may be prime but is never coprime to itself.

Proof. First observe that

$$\binom{2r}{r} = \frac{(2r)}{r}\frac{(2r-1)}{r-1}\cdots\frac{r+1}{1} \geq 2^r. \tag{127}$$

Second, observe that for any $m \in \mathbb{N}$ and prime $p \in \mathbb{N}$, the number of times that p appears in m is

$$\left\lfloor \frac{m}{p} \right\rfloor + \ldots \left\lfloor \frac{m}{p^k} \right\rfloor, \tag{128}$$

where k is such that $p^k \leq m < p^{k+1}$. Comment: proof by example, $m = 5, p = 2$.

Therefore, the number of times a prime p appears in $\binom{2r}{r} = \frac{(2r)!}{(r!)^2}$ is given by

$$\left\lfloor \frac{2r}{p} \right\rfloor + \cdots + \left\lfloor \frac{2r}{p^{k_p}} \right\rfloor - 2\left(\left\lfloor \frac{r}{p} \right\rfloor + \cdots + \left\lfloor \frac{r}{p^{k_p}} \right\rfloor \right) \leq k_p, \tag{129}$$

where k_p is such that $p^{k_p} \leq 2r < p^{k_p+1}$ and we used the inequality $\forall x > 0, \lfloor 2x \rfloor - 2\lfloor x \rfloor \leq 1$.

Clearly, only primes p with $1 \leq p \leq 2r$ can appear in the factorization of $\binom{2r}{r}$. Therefore

$$2^r \leq \binom{2r}{r} \leq \prod_{\text{p prime },1 \leq p \leq 2r} p^{k_p} \leq (2r)^{\pi(2r)}. \tag{130}$$

Taking base-2 logarithms and rearranging yields the lemma. □