Quantum Computing - Assignment 4

Kishlaya Jaiswal

December 14, 2020

Exercise 1

Let $x \in \mathbb{Z}_N^*$ where $N = p_1^{\alpha_1} \dots p_l^{\alpha_l}$.
Let r be the order of $x \pmod N$ and r_i be the order of $x \pmod{p_i^{\alpha_i}}$. Notice that r is the lcm of $r_1, r_2, \dots, r_l$
Denote by $\nu_2(n)$ the largest power of 2 dividing n.
Note that $r_i \mid r$ for each $1 \le i \le l$. So if r is odd then so are r_i; otherwise if $x^{r/2} \equiv -1 \pmod N$ then $x^{r/2} \equiv -1 \pmod{p_i^{\alpha_i}}$ and so $r_i \nmid (r/2) \implies \nu_2(r) = \nu_2(r_i)$ for each $1 \le i \le l$. We get

$$P(r \text{ is odd or } x^{r/2} \equiv -1 \pmod N) \le P(\text{largest power of 2 that divides each } r_i \text{ is same})$$

Now we quote a lemma (from Nielsen and Chuang) which uses the fact that $\mathbb{Z}_{p^\alpha}^*$ is cyclic for odd prime p, to estimate the fraction of elements with particular largest power of 2 in the order of any element of $\mathbb{Z}_{p^\alpha}^*$:

Lemma. *Let p be an odd prime. Let $\nu_2\left(\left|\mathbb{Z}_{p^\alpha}^*\right|\right) = d$. Then*

$$P(2^d \textit{ divides order of a randomly chosen element of } \mathbb{Z}_{p^\alpha}^*) = \frac{1}{2}$$

As a corollary, we immediately get that if y is chosen randomly from $\mathbb{Z}_{p^\alpha}^*$ then for any n

$$P(\nu_2(y) = n) \le \frac{1}{2}$$

Using Chinese Remainder Theorem and that $|\mathbb{Z}_N^*| = |\mathbb{Z}_{p_1^{\alpha_1}}^*| \dots |\mathbb{Z}_{p_l^{\alpha_l}}^*|$, we get that choosing x at random from $\mathbb{Z}_N^*$ is equivalent to choosing x_i at random from $\mathbb{Z}_{p_i^{\alpha_i}}^*$ independently for each $1 \le i \le l$. We argue by induction on $l \ge 2$, that $P(\text{largest power of 2 that divides each } r_i, 1 \le i \le l, \text{ is same}) = P(\nu_2(r_1) = \dots = \nu_2(r_l)) \le \frac{1}{2^{l-1}}$
If $l = 2$, then set $m = \nu_2\left(\left|\mathbb{Z}_{p_2^{\alpha_2}}^*\right|\right)$

$$\begin{aligned}
P(\nu_2(r_1) = \nu_2(r_2)) &= \sum_{k=0}^{m} P(\nu_2(r_1) = \nu_2(r_2), \nu_2(r_2) = k) \\
&= \sum_k P(\nu_2(r_1) = k) P(\nu_2(r_2) = k) \\
&\le \frac{1}{2} \sum_k P(\nu_2(r_1) = k) \\
&\le \frac{1}{2} P(\nu_2(r_1) \ge 0) \\
&= \frac{1}{2}
\end{aligned}$$

Suppose it is true for some $l-1 \geq 2$, then set $m = \nu_2\left(\left|\mathbb{Z}^*_{p_l^{\alpha_l}}\right|\right)$

$$\begin{aligned}
P(\nu_2(r_1) = \cdots = \nu_2(r_l)) &= \sum_{k=0}^{m} P(\nu_2(r_1) = \cdots = \nu_2(r_l), \nu_2(r_l) = k) \\
&= \sum_{k} P(\nu_2(r_1) = \cdots = \nu_2(r_{l-1}) = k) P(\nu_2(r_l) = k) \\
&\leq \frac{1}{2} \sum_{k} P(\nu_2(r_1) = \cdots = \nu_2(r_{l-1}) = k) \\
&\leq \frac{1}{2} P(\nu_2(r_1) = \cdots = \nu_2(r_{l-1})) \\
&\leq \frac{1}{2}\left(\frac{1}{2^{l-2}}\right) \text{ (by inductive hypothesis)} \\
&= \frac{1}{2^{l-1}}
\end{aligned}$$

Therefore, we get

$$\begin{aligned}
P(x \text{ is good}) &= 1 - P(x \text{ is not good}) \\
&= 1 - P(r \text{ is odd or } x^{r/2} \equiv -1 \pmod{N}) \\
&\geq 1 - P(\text{largest power of 2 that divides each } r_i \text{ is same}) \\
&\geq 1 - \frac{1}{2^{l-1}}
\end{aligned}$$

Exercise 2

Let $a_0, a_1, \ldots$ be a sequence of positive reals then denote by

$$[a_0, \ldots a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

We have the following lemma (from Nielsen and Chuang):

Lemma. *Let $a_0, a_1, \ldots$ be a sequence of positive reals and sequences p_n, q_n defined inductively by $p_0 = a_0, p_1 = 1 + a_0 a_1$ and $q_0 = 1, q_1 = a_1$ and for all $n \geq 2$*

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

then $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$

As a corollary we immediately get the following results

Corollary. *Let $a_0, a_1, \ldots$ be a sequence of positive integers and $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ then $\forall n \geq 0$*

- *p_n, q_n are positive integers*
- *$q_n p_{n-1} - p_n q_{n-1} = (-1)^n$*
- *$(p_n, q_n) = 1$*
- *Both p_n and q_n are strictly increasing sequence*

Proof. Clearly $p_0 = a_0, p_1 = 1 + a_0a_1$ and $q_0 = 1, q_1 = a_1$ are integers. Now using strong induction we get that $p_n = a_np_{n-1} + p_{n-2}, q_n = a_nq_{n-1} + q_{n-2}$ are integers.

For $n = 1$, $q_1p_0 - p_1q_0 = a_0a_1 - (1 + a_0a_1) = (-1)$. Assume $q_{n-1}p_{n-2} - p_{n-1}q_{n-2} = (-1)^{n-1}$, then we have

$$q_np_{n-1} - p_nq_{n-1} = (a_nq_{n-1} + q_{n-2})p_{n-1} - (a_np_{n-1} + p_{n-2})q_{n-1} = -(q_{n-1}p_{n-2} - p_{n-1}q_{n-2}) = (-1)^n$$

If $d \mid p_n$ and $d \mid q_n$ then $d \mid q_np_{n-1} - p_nq_{n-1} \implies d \mid (-1)^n$. Hence $(p_n, q_n) = 1$.
As p_n and q_n are both strictly positive sequence and a_n is a positive integer, we get $p_n = a_np_{n-1} + p_{n-2} > a_np_{n-1} \geq p_{n-1}$. Similarly $q_n > q_{n-1}$. □

Now suppose $x \in \mathbb{Q}$ and that $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$
We can assume $(p, q) = 1$ because otherwise write $p/q = p'/q'$ where $(p', q') = 1$ and note that $\left|x - \frac{p'}{q'}\right| < \frac{1}{2q^2} < \frac{1}{2q'^2}$ and so we can replace p/q with p'/q'.

Let $[a_0, \ldots, a_n]$ be the continued fraction for $\frac{p}{q}$ and $[a_0, \ldots, a_i] = \frac{p_i}{q_i}$, $\forall 0 \leq i \leq n$. Then $p_n = p$ and $q_n = q$ as both $(p, q) = (p_n, q_n) = 1$

If $x = \frac{p}{q}$, then $[a_0, \ldots, a_n]$ is the continued fraction expansion for x and so p/q is a convergent of the continued fraction expansion of x.
If $\frac{p}{q} = [a_0]$ then $p = a_0, q = 1$. So $|x - a_0|$ is a rational less than $\frac{1}{2}$.
If $x > a_0$ then $0 < x - a_0 < 1 \implies x - a_0 = [0, b_0, \ldots, b_m] \implies x = [a_0, b_0, \ldots, b_m]$
Otherwise if $x < a_0$ then in this case we first note that $p/q = [a_0] = [a_0 - 1, 1]$ and since $\frac{1}{2} < x - a_0 + 1 < 1 \implies x - a_0 + 1 = [0, 1, b_1 \ldots, b_m] \implies x = [a_0 - 1, 1, b_1, \ldots, b_m]$ and so in both the cases, p/q is a convergent of the continued fraction expansion of x

Otherwise let $x = [a_0, \ldots, a_n, y]$ $(n > 0)$ and we solve for y as follows:

$$x = \frac{yp_n + p_{n-1}}{yq_n + q_{n-1}} \text{ (by above lemma)}$$

$$\implies y = \frac{p_{n-1} - xq_{n-1}}{xq_n - p_n} = \frac{q_np_{n-1} - p_nq_{n-1}}{q_n^2(x - \frac{p_n}{q_n})} - \frac{q_{n-1}}{q_n} = \frac{(-1)^n}{q_n^2(x - \frac{p_n}{q_n})} - \frac{q_{n-1}}{q_n}$$

Now if $a_n = 1$, then we can re-write $[a_0, \ldots, a_{n-1}, a_n] = [a_0, \ldots, a_{n-1} + 1]$. Otherwise, we can re-write $[a_0, \ldots, a_{n-1}, a_n] = [a_0, \ldots, a_{n-1}, a_n - 1, 1]$. Therefore, we can appropriately modify n such that $(-1)^n \left(x - \frac{p_n}{q_n}\right) > 0$. Hence we get

$$y = \frac{1}{q_n^2\left|x - \frac{p_n}{q_n}\right|} - \frac{q_{n-1}}{q_n} > 1$$

because $q_n^2\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2}$ and $q_n > q_{n-1}$ as q_n is increasing.
Finally, since x is rational and p_n, q_n are integers, we get that y is a positive rational and we can find a continued fraction expansion for $y = [b_0, \ldots, b_m]$. Therefore, we get $x = [a_0, \ldots a_n, b_0, \ldots b_m]$ as required.

Exercise 3

Let X be the set of all search elements (needles) and $|\beta\rangle = \frac{1}{\sqrt{x}} \sum_{i \in X} |i\rangle$ where $x = |X|$
And let $|\alpha\rangle = \frac{1}{\sqrt{N-x}} \sum_{i \notin X} |i\rangle$ where N is the total number of items.
Denote by $|\psi\rangle$ the uniform superposition of all states, that is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum |i\rangle = \sqrt{1 - \frac{x}{N}} |\alpha\rangle + \sqrt{\frac{x}{N}} |\beta\rangle = \cos\theta |\alpha\rangle + \sin\theta |\beta\rangle$$

where $\cos\theta = \sqrt{1 - x/N}$. We define three operators:

- Oracle operator O where $O|i\rangle = -|i\rangle$ if $i \in X$ otherwise $O|i\rangle = |i\rangle$
- Diffusion operator D where $D = 2|\psi\rangle\langle\psi| - I$
- Grover operator $G = DO$

Note that $O|\alpha\rangle = |\alpha\rangle$ and $O|\beta\rangle = -|\beta\rangle$
Next note that, $\langle\psi|\alpha\rangle = \cos\theta$ and $\langle\psi|\beta\rangle = \sin\theta$ and so $D|\alpha\rangle = 2\cos\theta|\psi\rangle - |\alpha\rangle$ and $D|\beta\rangle = 2\sin\theta|\psi\rangle - |\beta\rangle$.
Let $|\phi\rangle = \cos x|\alpha\rangle + \sin x|\beta\rangle$ be any general vector in the plane P of $|\alpha\rangle$ and $|\beta\rangle$, then we have:

$$\begin{aligned}
G|\phi\rangle &= (\cos x)G|\alpha\rangle + (\sin x)G|\beta\rangle \\
&= (\cos x)D|\alpha\rangle - (\sin x)D|\beta\rangle \\
&= \cos x(2\cos\theta|\psi\rangle - |\alpha\rangle) - \sin x(2\sin\theta|\psi\rangle - |\beta\rangle) \\
&= (2\cos x\cos\theta - 2\sin x\sin\theta)|\psi\rangle - \cos x|\alpha\rangle + \sin x|\beta\rangle \\
&= (2\cos x\cos^2\theta - 2\sin x\sin\theta\cos\theta - \cos x)|\alpha\rangle + (2\cos x\cos\theta\sin\theta - 2\sin x\sin^2\theta + \sin x)|\beta\rangle \\
&= cos(2\theta + x)|\alpha\rangle + \sin(2\theta + x)|\beta\rangle
\end{aligned}$$

$$\implies G|\psi\rangle = cos(3\theta)|\alpha\rangle + \sin(3\theta)|\beta\rangle$$

Therefore, G is a counter-clockwise rotation (by 2θ) operator in P. And so it suffices to apply G on $|\psi\rangle$ k times such that

$$2k\theta \sim \frac{\pi}{2} - \theta \implies k = \left\lfloor \frac{\pi}{4}\left(\frac{1}{\theta}\right) - \frac{1}{2} \right\rfloor \leq \frac{\pi}{4\theta}$$

And using $\theta \geq \sin\theta = \sqrt{x/N}$, we get $\boxed{k \leq \frac{\pi}{4}\sqrt{\frac{N}{x}}}$
Hence after $O(\sqrt{N/x})$ oracle queries, with high probability, we can find one of the search elements.