
ITC
Enduring Value
classmate
MARVEL
AVENGERS
©MARVEL
NO TREE FROM NATURAL FOREST WAS CUT TO MAKE THIS NOTEBOOK
FOREST SAFE

soorajss1729@gmail.com +91-9400635788

INDEX

9

NAME: SOORAJ·S· STD.: SEC.: ROLL NO.: SUB.:

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks
		QUANTUM COMPUTATION		
		& QUANTUM INFORMATION		
		– Nielsen & Chuang		

Discrete Logarithms

The discrete logarithm problem (DLP):

Check Cryptography Diffie-Hellman key

Let 'a' be a generator of a group G which we can choose as $(\mathbb{Z}_p^*, \cdot)$ where p is a prime number. Then find the least positive integer value of s such that $b = a^s \mod p \in (\mathbb{Z}_p^*, \cdot)$.

Consider the function, $f(x_1, x_2) = b^{x_1} a^{x_2} \mod p$ which has a 2-tuple period (t_1, t_2) such that $f(x_1+t_1, x_2+t_2) = f(x_1, x_2)$. So,

$$b^{x_1+t_1} a^{x_2+t_2} \mod p = b^{x_1} a^{x_2} \mod p$$

$b^{t_1} a^{t_2} \bmod p = 1$

substituting $b = a^s \bmod p$,

Starke 12/6/2022

$(a^s)^{t_1} a^{t_2} \bmod p = a^{st_1} a^{t_2} \bmod p = 1$

$\Longrightarrow a^{st_1 + t_2} \bmod p = 1$

$\therefore$

$st_1 + t_2 = kr$ for some integer k.

where r is the order of the element $a \in (\mathbb{Z}_p^*, \cdot)$ such that $a^r \bmod p = 1$.

Let's take $k=0$ then

$st_1 + t_2 = 0 \Longrightarrow \boxed{s = -t_2/t_1}$

$$f(x_1, x_2) = b^{x_1} a^{x_2} \bmod p$$
$$= (a^s)^{x_1} a^{x_2} \bmod p$$
$$= a^{sx_1 + x_2} \bmod p.$$

$\therefore$

Determining the 2-tuple period of the function $f(x_1, x_2) = b^{x_1} a^{x_2} \bmod p = a^{sx_1+x_2} \bmod p$ allows us to find s, thereby solving the discrete logarithm problem (DLP).

(OR) Consider the function,

$$f(x_1, x_2) = a^{sx_1 + x_2} \bmod N = b^{x_1} a^{x_2} \bmod N$$

where all the variables are integers, and r is the smallest +ve integer for which $a^r \bmod N = 1$.

This function is periodic, since

$$f(x_1 + l, x_2 - ls) = f(x_1, x_2)$$

But now the period is a 2-tuple $(l, -ls)$ for integer l.

$$s = \frac{-(-ls)}{l}.$$

We can formulate a quantum algorithm which solves this problem using one query of a quantum black box U which performs the unitary transform

$$U|x_1\rangle|x_2\rangle|y\rangle \longrightarrow |x_1\rangle|x_2\rangle|y \oplus f(x)\rangle$$

$\oplus$: Bitwise addition modulo 2.

We assume knowledge of the minimum $r>0$ such that $a^r \bmod N = 1$, which can be obtained using the order-finding algorithm.

Algorithm : Discrete Logarithm

Inputs : ① A black box which performs the operation

$$U|x_1\rangle|x_2\rangle|y\rangle = |x_1\rangle|x_2\rangle|y \oplus f(x_1,x_2)\rangle$$

for $f(x_1,x_2) = b^{x_1} a^{x_2}$

② A state to store the function evaluation, initialized to $|0\rangle$

③ two $\boxed{t = O(\lceil \log r \rceil + \log(1/\epsilon))}$ qubit registers initialized to $|0\rangle$.

Outputs : The least +ve integer s such that $a^s = b$.

Runtime : One use of U, and $\boxed{O(\lceil \log r \rceil^2)}$ operations. Succeeds with probability $\boxed{O(1)}$

Procedure :

① $|0\rangle|0\rangle|0\rangle$ initial state

② $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|0\rangle$ create superposition.

③ $\rightarrow \frac{1}{2^t}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1}|x_1\rangle|x_2\rangle|f(x_1,x_2)\rangle$ apply U

$$\approx \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\sum_{x_1=0}^{2^t-1}\sum_{x_2=0}^{2^t-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}|x_1\rangle|x_2\rangle|\hat{f}(sl_2,l_2)\rangle$$

$$= \frac{1}{2^t\sqrt{r}}\sum_{l_2=0}^{r-1}\left[\sum_{x_1=0}^{2^t-1} e^{2\pi i(sl_2x_1)/r}|x_1\rangle\right]\left[\sum_{x_2=0}^{2^t-1} e^{2\pi i(l_2x_2)/r}|x_2\rangle\right]|\hat{f}(sl_2,l_2)\rangle$$

④ $\rightarrow \frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}|\widetilde{sl_2/r}\rangle|\widetilde{l_2/r}\rangle|\hat{f}(sl_2,l_2)\rangle$ Apply inverse Fourier transform to the 1st two registers

⑤ $\rightarrow (\widetilde{sl_2/r}, \widetilde{l_2/r})$ measure 1st two registers

⑥ $\rightarrow s$ apply generalized continued fraction algorithm.

Ex: 5.22

Show that

$$|\hat{f}(l_1,l_2)\rangle = \sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r} |f(x_1,x_2)\rangle$$

$$= \frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle$$

and we are constrained to have $l_1/s - l_2$ be an integer multiple of r for this expression to be non-zero.

Ans: $$|\hat{f}(l_1,l_2)\rangle = \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r} |f(x_1,x_2)\rangle$$

$$= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{x_2=0}^{r-1} e^{-2\pi i(l_1x_1+l_2x_2)/r} |f(0,sx_1+x_2)\rangle$$

$$= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i(l_1x_1+l_2(j-sx_1))/r} |f(0,j)\rangle$$

$$= \frac{1}{r}\sum_{x_1=0}^{r-1}\sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i(l_1x_1+l_2j-l_2sx_1)/r} |f(0,j)\rangle$$

$$= \frac{1}{r}\sum_{x_1=0}^{r-1} e^{-2\pi i s x_1(l_1/s-l_2)/r} \sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i l_2 j} |f(0,j)\rangle$$

Take $j' = j - sx_1 \Rightarrow j = j' + sx_1$

$j : sx_1 \to r-1+sx_1 \Rightarrow j' : 0 \to r-1$

$$\sum_{j=sx_1}^{r-1+sx_1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle = \sum_{j'=0}^{r-1} e^{-2\pi i l_2 (j'+sx_1)/r} |f(0,j'+sx_1)\rangle$$

$$= \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle$$

Since $e^{-2\pi i l_2 j/r} |f(0,j)\rangle$ is periodic.

$\therefore$

$$|f(l_1,l_2)\rangle = \frac{1}{r} \sum_{x_1=0}^{r-1} \sum_{x_2=0}^{r-1} e^{-2\pi i (l_1 x_1 + l_2 x_2)/r} |f(x_1,x_2)\rangle$$

$$= \frac{1}{r} \sum_{x_1=0}^{r-1} e^{-2\pi i s x_1 (l_1/s - l_2)/r} \times \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle$$

$\frac{l_1}{s} - l_2 = kr$

$$= \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle .$$

else the expression becomes zero

Ex: 5.23 Compute $\frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{+2\pi i(l_1 x_1 + l_2 x_2)/r} |\hat{f}(l_1, l_2)\rangle$

and show that the result is $|f(x_1, x_2)\rangle$

Ans: $$\frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1} e^{2\pi i(l_1 x_1 + l_2 x_2)/r} |\hat{f}(l_1, l_2)\rangle =$$

$$= \frac{1}{r}\sum_{l_1=0}^{r-1}\sum_{l_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i(l_1 x_1 + l_2 x_2 - l_2 j)/r} |f(0,j)\rangle$$

where we substituted for, $|\hat{f}(l_1, l_2)\rangle = \sum_{j=0}^{r-1} e^{-2\pi i l_2 j/r} |f(0,j)\rangle$

$\frac{l_1}{s} - l_2 = mr \Longrightarrow l_1 = smr + sl_2$ where $m \in \mathbb{Z}$

$$= \frac{1}{r}\sum_{l_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i(smrx_1 + sl_2 x_1 + l_2 x_2 - l_2 j)/r} |f(0,j)\rangle$$

$$= \frac{1}{r}\sum_{l_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i smx_1} \times e^{2\pi i l_2(sx_1 + x_1 - j)/r} |f(0,j)\rangle$$

$$= \frac{1}{r}\sum_{l_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i l_2(sx_1 + x_1 - j)/r} |f(0,j)\rangle$$

$$= \delta_{s x_1 + x_2 - j, 0} \sum_{j=0}^{r-1} |f(0,j)\rangle$$

$$= |f(0, s x_1 + x_2)\rangle$$

$$= |f(x_1, x_2)\rangle$$

The key to understanding this algorithm is step 3, in which we introduce the state.

$$\left|\hat{f}(l_1, l_2)\right\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{-2\pi i l_2 j / r} \left|f(0, j)\right\rangle$$

the Fourier transform of $\left|f(x_1, x_2)\right\rangle$.

In this eqn. the values of l_1 and l_2 must satisfy

$$\sum_{k=0}^{r-1} e^{2\pi i k (l_1/s - l_2)/r} = r$$

otherwise the amplitude of $\left|\hat{f}(l_1, l_2)\right\rangle$ is nearly zero.

$$\frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1} e^{2\pi i(sl_2x_1+l_2x_2)/r}\,|\hat{f}(sl_2,l_2)\rangle =$$

$$=\frac{1}{\sqrt{r}}\sum_{l_2=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{j=0}^{r-1} e^{2\pi i(sl_2x_1+l_2x_2-l_2j)/r}\,|f(0,j)\rangle$$

$$=\frac{1}{r}\sum_{l_2=0}^{r-1}\sum_{j=0}^{r-1} e^{2\pi i l_2(sx_1+x_2-j)/r}\,|f(0,j)\rangle$$

$$=\delta_{sx_1+x_2-j,0}\sum_{j=0}^{r-1}|f(0,j)\rangle$$

$$=|f(0,sx_1+x_2)\rangle = |f(x_1,x_2)\rangle$$

The Hidden Subgroup Problem

- Let H be a subgroup of a group G, and let $x \in G$. The set $Hx = \{hx \mid h \in H\}$ is called a right coset of H in G.

The element x is a representative of Hx.

Similarly,
the left coset of H in G is defined as, $xH = \{xh \mid h \in H\}$.

Note: If the group operation is $+$, then the right and left cosets of H in $(G,+)$ represented by $x \in G$ are:

$H+x = \{h+x \mid h \in H\}$ and $x+H = \{x+h \mid h \in H\}$.

G.T
②

- Let H be a subgroup of a group G. We define a relation '$\sim$' on G by $x \sim y$ iff $Hx = Hy$ where $x, y \in G$.

i.e., $x \sim y$ iff $xy^{-1} \in H$

- Let H be a subgroup of a group G. Then the relation '$\sim$' defined by $x \sim y$ iff $xy^{-1} \in H$ (i.e., $x \sim y$ iff $Hx = Hy$) is an equivalence relation.

The equivalence classes are the right cosets of H in G, i.e., $[x] = Hx$.

$\Rightarrow$ Any subgroup H of a group G partitions G into disjoint right cosets.

HSP

For a hidden subgroup problems, we are given a group G and a function which is constant on the cosets of G with respect to some subgroup H.

i.e., any 2 elements of the same coset have same function value and any 2 elements of a different cosets have different value.

The function is given as a black box, i.e., there is an oracle to find the value of a function on any element of G.

The problem is to find the hidden subgroup H (or its generators).

Hidden Subgroup Problem:

For a group G and its subgroup H (hidden), we are given a function f (as oracle), constant on cosets and different on different cosets of H. Find the generators of H.

Nielsen & Chuang – HSP

If we are given a periodic function, even when the structure of the periodicity is quite complicated, we can often use a quantum algorithm to determine the period efficiently. However, not all periods of periodic functions can be determined

HSP: Let f be a function from a finitely generated group G to a finite set X, i.e., $f: G \to X$, such that f is constant on the cosets of a subgroup K $(K \leq G)$, and distinct on each coset. Given a quantum blackbox for performing the unitary transform, $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$, for $g \in G$, $h \in X$, and $\oplus$ is appropriately chosen binary operation on X, find a generating set for K.

Examples

① Deutsch problem :

For a given $f : \{0,1\} \to \{0,1\}$ the problem is whether $f(0) = f(1)$ (constant) or not (balanced).

The oracle function is the same as the function f in the Deutsch problem.

The group $G = \mathbb{Z}_2 = \{0,1\}$ with binary operation $\oplus$.

x	y	$x \oplus y$
0	0	0
0	1	1
1	0	1
1	1	0

XOR on CNOT

When f is constant,

$$H = G = \{0,1\}$$

$$\left.\begin{aligned} H \oplus 0 &= \{0\oplus 0, 1 \oplus 0\} = \{0,1\} \\ H \oplus 1 &= \{0 \oplus 1, 1 \oplus 1\} = \{1,0\} \end{aligned}\right] \text{ is the only coset}$$

When f is balanced,

$$H = \{0\}.$$

$H \oplus 0 = \{0\}$ & $H \oplus 1 = \{1\}$ are the 2 distinct cosets

$\Rightarrow$ The HSP problem would be distinguishing between $H = \{0\}$ vs $H = \{0,1\}$.

② Period Finding :

For a given function $f: \mathbb{Z} \to \mathbb{R}$, we knew that f is periodic with period of r,

$$f(x) = f(x+r) \quad \forall x$$

and $f(x) \neq f(y) \quad \forall \; 0 \le x < y < r$

The goal was to find the period r.

The oracle is the same as the f function.

The group $G = \mathbb{Z}$ with the binary operation '+'.

H is a subgroup generated by r

$H = \{0, r, 2r, \dots\}$ where $r \in G$.

H+0

H+1

• The case fall

$H+0 = \{0, r, 2r, \ldots\}$

$H+1 = \{1, 1+r, 1+2r, \ldots\}$ such that

$$f(1) = f(1+r) = f(1+2r) = \ldots$$

- The order finding problem is a special case of the Period Finding Problem & falls in this category of HSP problems.

③ Discrete Logarithm :

An integer $p>0$, 'a' be a generator for $\mathbb{Z}_p^*$, $b \in \mathbb{Z}_p^*$, $r = |\mathbb{Z}_p^*|$

we need to find smallest s, such that $b = a^s$.

The function we used was,

$$f : \mathbb{Z}_r \times \mathbb{Z}_r \to \mathbb{Z}_p : (x_1, x_2) \to b^{x_1} a^{x_2} \bmod p$$
$$= a^{sx_1 + x_2} \bmod p$$

This function was designed such that it is constant on the coset of $H = \langle (1, -s) \rangle$ in $G = \mathbb{Z}_r \times \mathbb{Z}_r$.

We use the function f as a HSP instantiation and can extract s as the generator of H.