Hidden subgroup problem ~~...~~ Fourier Transform

נתונה חבורה סופית G.

נסמן $\mathbb{C}[G] = \{f: G \to \mathbb{C}\}$

- $\mathbb{C}[G]$ מ"ו מעל $\mathbb{C}$

$$(f+g)(x) = f(x)+g(x)$$
$$(c\cdot f)(x) = c\cdot f(x)$$

נגדיר מ"פ

$$\langle f,g\rangle = \sum_{x\in G} \overline{f(x)}\, g(x)$$

- לבדוק שזו מ"פ.

- $\dim \mathbb{C}[G] = |G|$

בסיס סדור!

$$f_x(y) = \begin{cases} 1 & y=x \\ 0 & y\neq x \end{cases}$$

$\{f_x \mid x\in G\}$ בסיס ל $\mathbb{C}[G]$.

כי הם פורשים ב"ת, והם בסיס אורתו' ביחס למ"פ.

הגדרה: קרקטר של G הוא הומו' מ G ל $\mathbb{C}^*$ (החבורה הכפלית של $\mathbb{C}$)
ג'ויר

$$\chi: G \to \mathbb{C}\setminus\{0\}$$

לכל $a,b\in G$

$$\chi(a\cdot b) = \chi(a)\cdot\chi(b)$$

כפל ב G ↑ ... כפל ב $\mathbb{C}$

<u>דוגמא 1</u>: $G = (C_n, +)$ חיבור $(\mod n)$, n

יהי χ קרקטר

$$\chi(0) = \chi(0+0) = \chi(0)\cdot\chi(0)$$

ולכן $\boxed{\chi(0) = 1}$

$$1 = \chi(0) = \chi(n\cdot 1) = (\chi(1))^n$$

ולכן $\chi(1) = \omega_s$ שורש יחידה מסדר n.

ואז, $\chi(t) = (\chi(1))^t = \omega_s^t$.

ולכן כל χ נקבע ע"י ערכו $\chi(1)$

וערך זה הוא שורש יחידה מסדר n.

מצד שני, לכל שורש יחידה, יש העתקה לקרקטר.

ולכן $\hat{G} = \{\chi \in K[G] \mid \chi \text{ קרקטר}\}$ הוכחנו $|\hat{G}| = n = |G|$

מאפרמטר, ע"י נסמן $\chi_t(l) = \omega^{t\cdot l} = \omega_t^l$

כאשר ω שורש יחידה פרימיטיבי מסדר n.

וכן $\hat{G} = \{\chi_t \mid 0 \le t \le n-1\}$

ומתקיים $\langle \chi_t, \chi_s \rangle = \sum_{x=0}^{n-1} \overline{\chi_t(x)}\, \chi_s(x)$

$$= \sum_x \omega^{-tx}\omega^{sx}$$

$$= \sum_{x=0}^{n-1} \underbrace{\left(\omega^{(s-t)}\right)^x}_{\text{טור הנדסי}} = \begin{cases} n & s=t \\ 0 & s\neq t \end{cases}$$

ולכן χ_t מהווים בסיס א"נ ל $\mathbb{C}[G]$.

②

הטרנספורם U שמעביר את הבסיס הנ"ל $\{f_x\}$
לבסיס הנ"ל $\{\chi_k\}$
הוא <u>אוניטרי</u>
כי הוא מעביר בסיס א"נ לבסיס א"נ
והוא נקרא טרנספורם <u>פוריה</u> של G.

$$|k\rangle \to \underbrace{\sum_{x\in G} \chi_k(x)|x\rangle}_{\text{מנורמל } \frac{1}{\sqrt{|G|}}}$$

<u>דוגמא</u>: (1) $(\mathbb{Z}_2, \oplus)$

$$\chi_0(x) = 1$$
$$\chi_1(x) = (-1)^x$$

והטרנספורם

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

נרמול ↑ ; ↑ $\begin{pmatrix}1\\0\end{pmatrix}$ $\begin{pmatrix}0\\1\end{pmatrix}$

(2) $(\mathbb{Z}_3, + \bmod 3)$

$$\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

χ_0 χ_1 χ_2

ובאופן כללי, ל $(\mathbb{Z}_n, + \bmod n)$: $\left(\omega^{ij}\right)$

(3) <u>הגדרה</u>: הגדר כפל על $\hat{G}$ והראה ש $\hat{G}$ איזומורפית ל G.

עכשיו נניח $G = G_1 \times G_2$

ונניח שידועים $\hat{G}_1, \hat{G}_2$.

נניח $\chi : G \to \mathbb{C}^*$

אז $\chi(a,b) = \chi(0,b) \cdot \chi(a,0)$

לכן χ נקבעת ע"י $\chi_1(a) = \chi(a,0)$:

ו $\chi_2(b) = \chi(0,b)$

ומתקיים $\chi_1 \in \hat{G}_1$, $\chi_2 \in \hat{G}_2$ (בדוק!)

ולהפך לכל $\chi_1 \in \hat{G}_1$, $\chi_2 \in \hat{G}_2$ קובעות $\chi \in \hat{G}$ בדרך הנ"ל.

לכן

$$\hat{G} \cong \hat{G}_1 \times \hat{G}_2$$

דוגמה $G = \mathbb{Z}_2 \times \mathbb{Z}_3$

אז $\hat{G} = \{ \chi_{a,b} \mid a \in [\mathbb{Z}_2], b \in [3] \}$

ו

$$\chi_{a,b}(c,d) = \chi_a(c) \cdot \chi_b(d)$$

$\chi_{a,b} = \chi_a \otimes \chi_b$ $$= (\omega_2)^{ac} \cdot (\omega_3)^{bd}$$

בכלליות $G = \mathbb{Z}_2^m$

$$\hat{G} = \{ \chi_{a_1,\dots,a_m} \mid a_1,\dots,a_m \in [2] \}$$

ו $\chi_{a_1,\dots,a_m}(b_1,\dots,b_m) = (-1)^{a_1 b_1} \cdot \ldots \cdot (-1)^{a_m b_m}$

$$= (-1)^{\sum a_i b_i}$$

באופן כללי, אם H_1 FFT ל G_1

G_2 " " H_2

אז $H_1 \otimes H_2$ " " $G_1 \otimes G_2$.

לכן $H^{\otimes m}$ הוא FFT ל $G = \mathbb{Z}_2^m$,

The Hidden Subgroup problem (HSP)

G אבלית סופית, $H \leq G$ תת-חבורה נורמלית.

נתונה $f: G \to V$ כאשר V קבוצה סופית כלשהי, כך ש:

1. f קבועה על כל coset של H.
2. f שונה על כל coset שונה של H.

$$\sum_x |x, f(x)\rangle$$

מטרה: למצוא יוצרים של H.

דוגמה: בעיית Simon

$G = \mathbb{Z}_2^n$, $H = \{0, s\}$ תת-חבורה מסדר 2.

$f: G \to V$ כך ש- $f(x) = f(x \oplus s)$ ושונה על כל coset שונה.

מטרה: למצוא את s.

$$k + ls \equiv 0 \pmod{q}$$

$$\boxed{s \equiv \frac{-k}{l} \pmod{\tilde{q}}}$$

מה עושה טרנספורם פוריה על coset של תת-חבורה?

נניח שיש לנו: $|cH\rangle = \frac{1}{\sqrt{|H|}} \sum_{h\in H} |ch\rangle$

$$\xrightarrow{FT} \frac{1}{\sqrt{|H|}} \sum_{h\in H} \frac{1}{\sqrt{|G|}} \sum_{z\in G} \chi_z(ch)\,|z\rangle$$

$$= \frac{1}{\sqrt{|G|}} \frac{1}{\sqrt{|H|}} \sum_{z\in G} \chi_z(c) \underbrace{\sum_{h\in H} \chi_z(h)}\ |z\rangle$$

$\chi_z : G \to \mathbb{C}$ קרקטר

ואם גם הצמצום $\chi_z : H \to \mathbb{C}$ קרקטר של H.

שאם הצמצום אינו זהות 1, אז $\sum_{h\in H} \chi_z(h) = 0$

ולכן, שורדים רק z-ים ש $\chi_z = \chi_e$ על H.

$$= \sqrt{\frac{|H|}{|G|}} \sum_{z\in G} \chi_z(c)\,|z\rangle$$

$\chi_z =_H \chi_e$

וכל z כזה, נמדד בהסתברות $\frac{|H|}{|G|} \cdot |\chi_z(c)|^2 = \frac{|H|}{|G|}$

כלומר בהסתברות שווה (ובפרט לא תלוי במשתנה c).

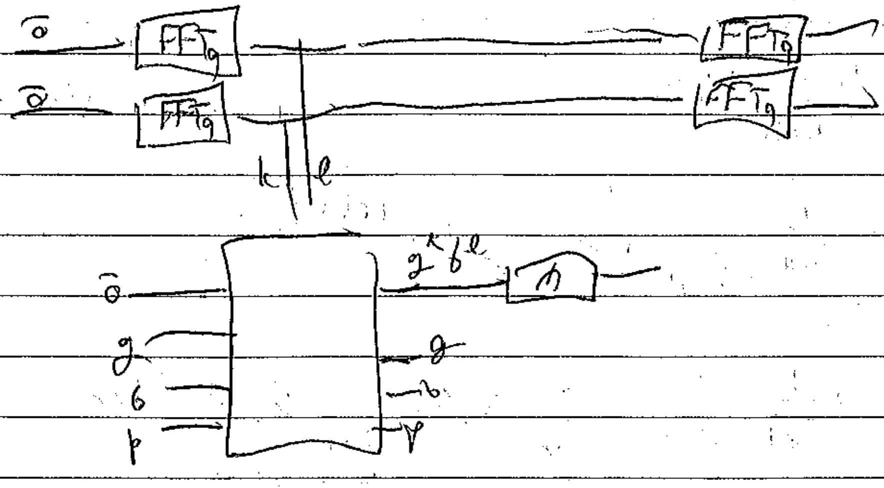
למשל: באלגוריתם של Simon קיבלנו z כך ש $(\chi_z)|_H = \chi_e$

כלומר: $(-1)^{z\cdot s} = (-1)^0$

$z \cdot s = 0 \pmod 2$

$z \perp s$.

עבור DLog!



נקבל: k, l כך

$$x_{k,l}\Big|_H \stackrel{?}{=} x_e$$

$$w_{k,l}(-s,1) = 1$$

$$w^{-sk+l} = w^0$$

$$l - sk = 0 \quad (q)$$

$$\boxed{s = \frac{l}{k} \pmod q}$$

ההנחה ש $k \neq 0$ ב F_q
שקורה חוץ מסיכוי $\frac{1}{q}$