5/12/2010

Hidden subgroup problem — התמרת Fourier Transform

נתונה חבורה סופית G.
נסמן $\mathbb{C}[G]=\{f: G\to\mathbb{C}\}$

* $\mathbb{C}[G]$ הוא 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 סטנדרטי:
$$f_x(y)=\begin{cases}1 & y=x\\ 0 & y\neq x\end{cases}$$

$\{f_x \mid x\in G\}$ בסיס ל $\mathbb{C}[G]$,
כי הם בת"ל, ויש כמות מתאימה.

הגדרה: קרקטר של G הוא הומו' מ G ל $\mathbb{C}^*$ (החבורה הכפלית של $\mathbb{C}$)
כלומר
$$\chi: G\to\mathbb{C}\setminus\{0\}$$
לכל $a,b\in G$
$$\chi(a\cdot b)=\chi(a)\cdot\chi(b)$$
(כפל ב G) (כפל ב $\mathbb{C}$)

שאלה 1 $G=(C_n,+)$ חיבור $(\mathrm{mod}\ n)$, 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.

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

ולכן כל χ נקבע ע"י ערכו ב $\chi(1)$

ומכך זה הוא שורש יחידה מסדר n

מצד שני, לכל שורש יחידה, יש התאמה לקרקטר.

ולכן $\hat{G}=\{\chi\in\mathbb{C}[G]\ |\ \chi \text{ קרקטר}\}$ מוכל, $|\hat{G}|=n=|G|$

כאשר נסמן $\chi_t(l)=\omega^{t\cdot l}=\omega_1^{l}$

כש ω שורש יחידה הראשוני מסדר n.

ולכן $\hat{G}=\{\chi_t\ |\ 0\le t\le n-1\}$

ומתקיים

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

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

$$=\sum_{x=0}^{n-1}\Big(\underbrace{\omega^{(s-t)}}_{\text{שורש יחידה}}\Big)^x=\begin{cases} n & s=t\\ 0 & s\neq t\end{cases}$$

ולכן χ_s מהווה בסיס אנ"ל ל $\mathbb{C}[G]$

הטרנספורם U שעובר מהבסיס הרגיל $\{|x\rangle\}$
לבסיס הבא $\{\chi_k\}$

הוא <u>אוניטרי</u>
כי הוא מעביר בסיס א"נ לבסיס א"נ
והוא נקרא טרנספורם <u>פוריה</u> של G.

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

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

$$\chi_0(x) = 1$$

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

זה טרנספורם

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

נרמול $\uparrow$ $\quad$ $\binom{1}{0}$ $\binom{0}{1}$

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

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

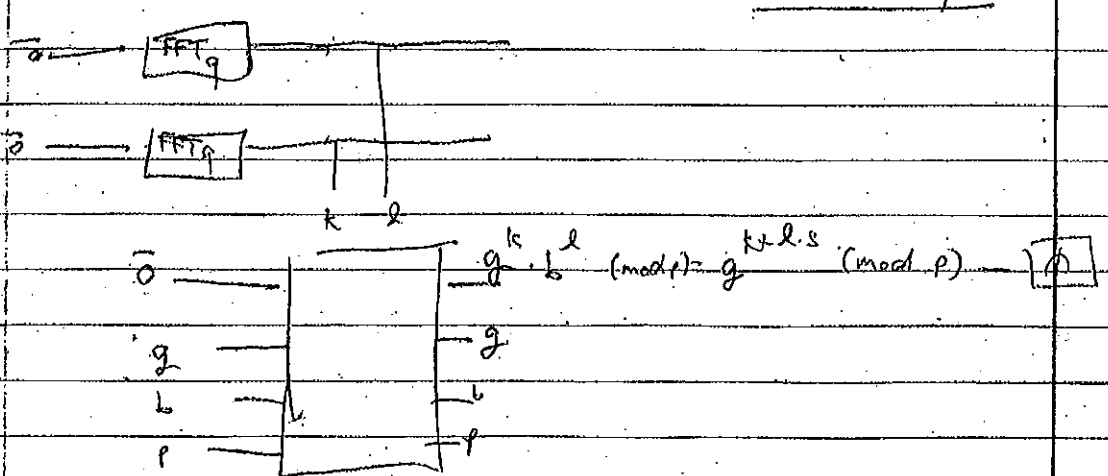
$\chi_0(x)$ $\chi_1(x)$ $\chi_2(x)$

ובאופן כללי, ב-$(\mathbb{Z}_n, + \bmod n)$

$$\left(\omega^{ij}\right)$$

(3) <u>תרגיל:</u> הגדר כפל ב-$\hat{G}$ הראה ש-$\hat{G}$ איזומורפי ל-G.

The Hidden Subgroup problem (HSP)


FFT_q
FFT_q
k
l
g^k · b^l (mod p) = g^{k+l·s} (mod p)
g
b
p

$$s \equiv \frac{k}{d} \pmod{\tilde{E}}$$

מה עושה טרנספורם פוריה ל coset של תת-חבורה?

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

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

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

$\chi_z : G \to \mathbb{C}$ קרקטר

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

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

ולכן, שורדים רק z כך ש $\chi_z = \chi_e$ ב H.

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

לכל z כזה, נקבל הסתברות $\frac{|H|}{|G|}\,|\chi_z(c)|^2 = \frac{|H|}{|G|}$

כלומר הסתברות שווה (ובפרט לא תלוי ב c).

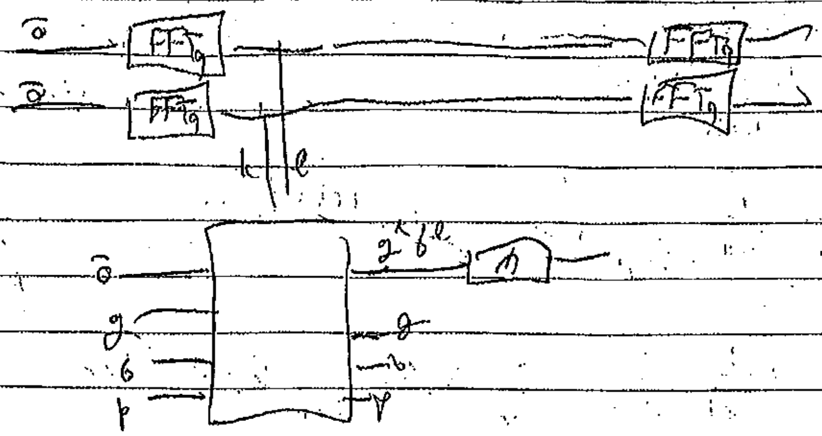
למשל באלגוריתם של Simon קיבלנו z רק אם $(\chi_z)|_H = \chi_e$

כלומר: $(-1)^{z\cdot s} = (-1)^0$

$z\cdot s = 0 \pmod 2$

$z \perp s$

עולה   !סיכום



נקבל! k,l כך

$x_{k,l}\big|_H := x_e$

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

$\omega^{-sk+l} = \omega^0$

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

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

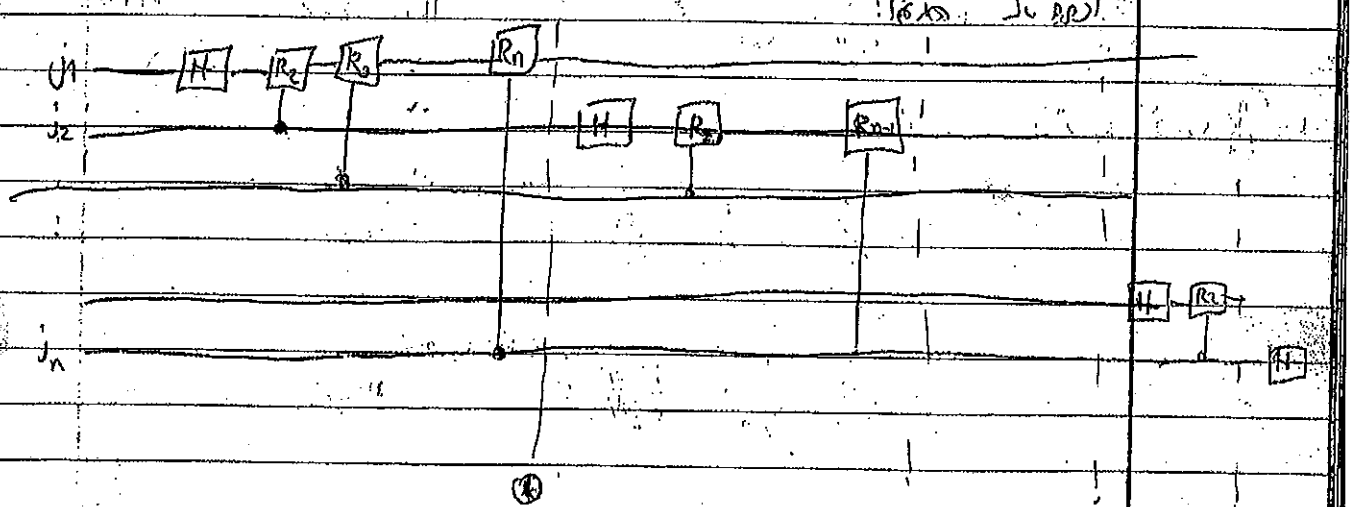
הנחנו ש- $k \neq 0$ ב-F_q
שקורה רק בסיכוי $\frac{1}{q}$

$0.b_{p}\dots b_{m}$

$$= \frac{b_1}{2} + \frac{b_2}{2^2} + \dots + \frac{b_m}{2^m}$$

$$|j_1 \dots j_n\rangle \to \bigotimes_{l=1}^{n} \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i (0.j_{n-l+1}\dots j_n)}|1\rangle\right)$$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$



$$\left(|0\rangle + e^{2\pi i \sum_{m=1}^{n} j_m 2^{-m}}|1\rangle\right) \otimes |j_1 \dots j_n\rangle$$

$$= \left(|0\rangle + e^{2\pi i 0.j_l \dots j_n}|1\rangle\right) \otimes |j_2 \dots j_n\rangle$$

$$FFT_N = (W^{kj})$$

$$FFT_N^{-1} = (W^{-kj})$$

FFT_N ... N ...