

5/12/2010

Modular subgroup problem

Fourier Transform

$$\phi: G \rightarrow \mathbb{C}^*$$

$$\phi[f] = \sum_{x \in G} f(x) \phi(x)$$

$$(f+g)(x) = f(x) + g(x) \quad \phi \text{ in } \phi[f]$$

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

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

$$\dim \phi[f] = 1$$

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

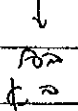
$$\phi[f] = \sum_{x \in G} f(x) \phi(x)$$

$\phi \in \text{Hom}(G, \mathbb{C}^*)$ ϕ^* Γ G \rightarrow \mathbb{C}^* ϕ^* Γ G \rightarrow \mathbb{C}^*

$$\chi: G \rightarrow \mathbb{C}^*$$

$$a, b \in G \rightarrow \chi(a \cdot b)$$

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



$u, (mod n) \text{ invertible} \quad \phi = (C_n, +) \quad \text{level}$

group of \mathbb{Z}

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

$\chi(0) = 1$

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

$\therefore \chi(1) = u$

$\chi(t) = (\chi(1))^t = u^t$

$\chi(0) = 1$ is the identity element of the group \mathbb{Z} under addition. $\chi(n) = 1$ is the identity element of the group $\mathbb{Z}/n\mathbb{Z}$ under addition.

Let χ be a character of \mathbb{Z} . Then $\chi(n) = 1$ for all $n \in \mathbb{Z}$.

$\chi(n) = 1 \implies \chi = \chi_0 = \{ \chi_k \mid k \in \mathbb{Z} \}$

$\chi_k(x) = u^{k \cdot x} = u^x$

$\chi_k(x) = u^{k \cdot x} = u^x$ is a character of \mathbb{Z} .

$\hat{G} = \{ \chi_k \mid 0 \leq k < n \}$

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

$= \sum_{x=0}^{n-1} u^{-kx} u^{lx}$

$= \sum_{x=0}^{n-1} (u^{(l-k)x}) = \begin{cases} n & l=k \\ 0 & l \neq k \end{cases}$

$\phi: \mathbb{Z} \rightarrow \hat{G}$ is an isomorphism.

$\{x\}$ \rightarrow $\sum_{x \in G} \chi(x) |x\rangle$ χ \in $\text{Char}(G)$

$\{x\}$ \rightarrow $\sum_{x \in G} \chi(x) |x\rangle$

$\chi(x) = 1$

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

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

$$|x\rangle \rightarrow \sum_{x \in G} \chi(x) |x\rangle$$

(\mathbb{Z}_2, \oplus) $\text{Char}(\mathbb{Z}_2)$

$$\chi_0(x) = 1$$

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

$\text{Char}(\mathbb{Z}_3)$

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

$$\begin{matrix} \uparrow & \uparrow \\ (0) & (1) \end{matrix}$$

$(\mathbb{Z}_3, + \text{ mod } 3)$ $\text{Char}(\mathbb{Z}_3)$

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

χ_0, χ_1, χ_2

$$\begin{pmatrix} \chi_0 \\ \chi_1 \\ \chi_2 \end{pmatrix} \text{Char}(\mathbb{Z}_3)$$

χ_0, χ_1, χ_2 \in $\text{Char}(\mathbb{Z}_3)$ \uparrow \mathbb{Z}_3 $\text{Char}(\mathbb{Z}_3)$ $\text{Char}(\mathbb{Z}_3)$ $\text{Char}(\mathbb{Z}_3)$ $\text{Char}(\mathbb{Z}_3)$

$$G = G_1 \times G_2 \quad \text{NY } 1000$$

$$\hat{G}_1, \hat{G}_2 \quad \text{NY } 1000$$

$$\chi(a, b) = \chi(a, b) \cdot \chi(a, a) \quad \text{NY } 1000$$

$$\chi_1(a) = \chi(a, a) \quad \text{NY } 1000$$

$$\chi_2(b) = \chi(b, b) \quad \text{NY } 1000$$

$$(1, 1) \quad \chi_1 \in \hat{G}_1, \chi_2 \in \hat{G}_2 \quad \text{NY } 1000$$

$$\hat{G} \cong \hat{G}_1 \times \hat{G}_2 \quad \text{NY } 1000$$

$$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{NY } 1000$$

$$\hat{G} = \{ \chi_{a,b} \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_2 \} \quad \text{NY } 1000$$

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

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

$$G = \mathbb{Z}_2^m \quad \text{NY } 1000$$

$$\hat{G} = \{ \chi_{a_1, \dots, a_m} \mid a_1, \dots, a_m \in \mathbb{Z}_2 \}$$

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

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

G_1 & FFT H_1 n_1, m_1 n_1
 G_2 " " H_2 n_2, m_2 n_2

$$G_1 \otimes G_2 \dots H_1 \otimes H_2 \xrightarrow{\text{FFT}} H_1 \otimes H_2 \xrightarrow{\text{FFT}} H_1 \otimes H_2 \xrightarrow{\text{FFT}} H_1 \otimes H_2$$

(4)

(HSP)

The Hidden Subgroup problem

map, f: G -> A, H <= G, N <= G

sum over x of f(x) -> { e in G, f: G -> A, H <= G, N <= G }

H <= G, f: G -> A, N <= G

Simon (6 pages)

Example: H = {0, s}, G = Z_n

f(x) = f(x+s) -> f: G -> A, s = 1/2 (13 pages)

g is a primitive root mod p, with p prime

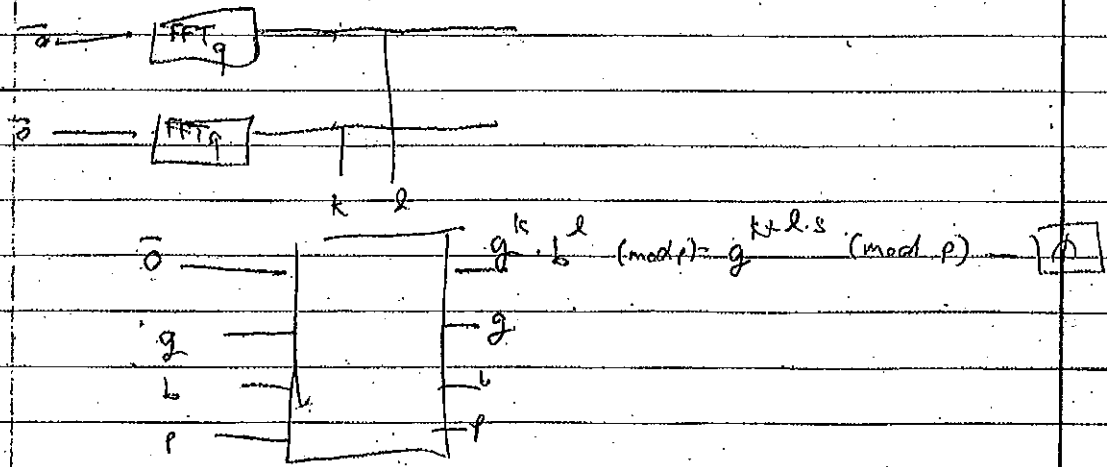
(0 < k < p-1, q = p/2) with p prime

g, p are coprime

b ∈ F_p

b = g^s, s ∈ [0, p-1]

Here is a diagram



g^c is a primitive root mod p

$$C_c = \{ (k, l) \in F_q \times F_q \mid k + l*s \equiv c \pmod{q} \}$$

$$H = \{ (k, l) \in F_q \times F_q \mid k + l*s \equiv 0 \pmod{q} \}$$

$$H < F_q \times F_q$$

for a coset $C = (a, 0) + H$

(6)

(1) $(H, k) = (S, l) \dots$ (GSP) $H \in \mathbb{Z}^n$ $k \in \mathbb{Z}$ $l \in \mathbb{Z}$

$(70, 9) = (k, l)$ $k+l=0 \pmod{9}$ $k+l=0$ $k=-l$

$(15, 9) = (k, l)$

$$s = \frac{-k}{9} \pmod{9}$$

$s \in \mathbb{Z}$

עבור קבוצת \$H\$ של \$G\$

$$|ch\rangle = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle$$

כאשר \$|H|\$ הוא מספר האיברים בקבוצת \$H\$

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

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

אם \$z \in H\$ אז \$\chi_z(h) = 1\$ לכל \$h \in H\$

אם \$z \notin H\$ אז \$\chi_z(h) = 0\$ לכל \$h \in H\$

$$\sum_{h \in H} \chi_z(h) = 0$$

לכן, \$\sum_{h \in H} \chi_z(h) = |H|\$ אם \$z \in H\$ ו-\$0\$ אחרת.

אם \$z \in H\$ אז \$\chi_z = \chi_e\$

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

כאשר \$z \in H\$

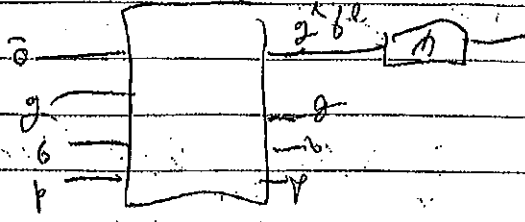
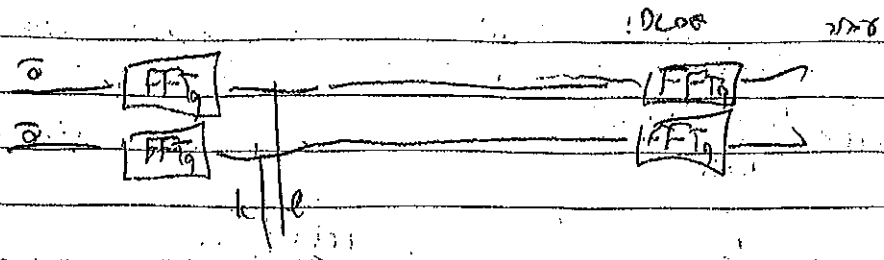
$$\frac{|H|}{|G|} = \frac{|H|}{|G|} \cdot |\chi_z(c)|^2$$

$$|\chi_z(c)| = 1 \iff z \in H$$

$$(-1)^{2 \cdot 5} = (-1)^0$$

$$2 \cdot 5 = 0 \pmod{2}$$

לכן



(7) k, l : Pap

$$W_{k,l} = \frac{1}{H} \sum_{n=0}^{l-1} W^{kn}$$

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

$$W_{k,l} = W^0$$

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

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

$$\frac{1}{q} \sum_{n=0}^{q-1} W^{kn} = \frac{1}{q} \sum_{n=0}^{q-1} W^{kn}$$

Case 2) $xy = (j \omega \dots)$

FFT $\frac{1}{N} \sum_{k=0}^{N-1} x[k] e^{-j2\pi k n/N}$

$$|j\rangle \rightarrow |2^j\rangle$$

$N=2^n$

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j(k) |k\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{k_0=0}^{N-1} e^{j2\pi ijk/N} |k\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} (|0\rangle + e^{j2\pi ijk/N} |1\rangle) \dots$$

$$|k\rangle = \sum_{k_1=0}^{N-1} e^{j2\pi ijk_1/N} \sum_{k_2=0}^{N-1} e^{j2\pi ijk_2/N} \dots |k_1, k_2, \dots\rangle$$

$$k_0 \cdot 2^{n-1} + k_1 \cdot 2^{n-2} + \dots + k_{n-1} \cdot 2^0$$

$$= \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} \dots e^{j2\pi ijk_1 \cdot 2^{n-1} + \dots} |k_1, k_2, \dots\rangle$$

$$= \sum_{k_1=0}^{N-1} \sum_{k_2=0}^{N-1} \dots e^{j2\pi ijk_1 \cdot 2^{n-1} + \dots} |k_1, k_2, \dots\rangle$$

$$(|0\rangle + e^{j2\pi ijk_1 \cdot 2^{n-1}} |1\rangle) \dots (|0\rangle + e^{j2\pi ijk_{n-1} \cdot 2^0} |1\rangle)$$

$|k\rangle = |k_1, k_2, \dots, k_{n-1}\rangle$ (reversed order)

$$\left[\sum_{k_1=0}^{N-1} e^{j2\pi ijk_1 \cdot 2^{n-1}} \dots \sum_{k_{n-1}=0}^{N-1} e^{j2\pi ijk_{n-1} \cdot 2^0} \right] = e^{j2\pi ijk/N}$$

$$j = \sum_{m=1}^{n-1} j_m 2^{n-m} + j_n 2^0$$

$$e^{j2\pi ijk/N} = e^{j2\pi ijk_1 2^{n-1} + \dots + j_{n-1} 2^0} = e^{j2\pi ijk/N}$$

(10) $\frac{1}{N}$

$$a \cdot b_1 \dots b_m$$

(10)

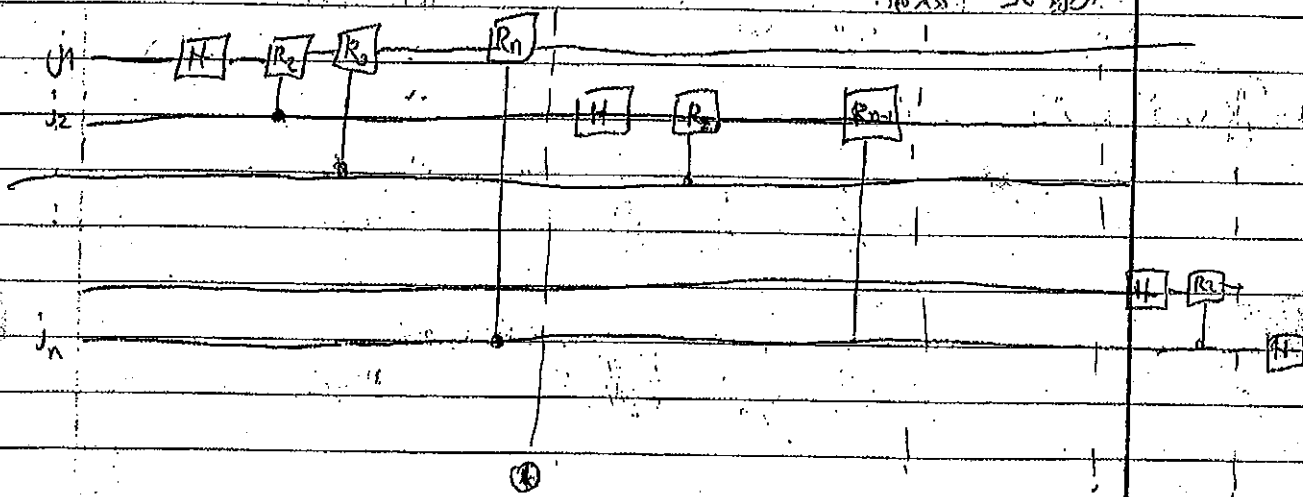
$$= \frac{b_1}{z} + \frac{b_2}{z^2} + \dots + \frac{b_m}{z^m}$$

$$jz \rightarrow \sum_{k=1}^n \frac{1}{z^k} (1 + e^{2\pi i (a_1 \cdot \dots \cdot a_n - j_n)}) \quad (11)$$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{a_n z^k} \end{bmatrix}$$

(10)

(10) (11) (12)



$$(1+z) e^{\sum_{m=1}^n j_m z^{-m}} \quad (12) \otimes (j_2 \dots j_n)$$

$$= (1+z) e^{2\pi i (a_1 \cdot \dots \cdot a_n - j_n)} \quad (12) \otimes (j_2 \dots j_n)$$

(10) (11) (12)

$$FFT = (W^k)^n$$

$$FFT^{-1} = (W^{-k})^n$$

... steps 7

2. FFT_N

(10) (11)