김일성종합대학학보 주체108(2019)년
수 학 제65권 제3호

표수 2인 유한체우에서 $k-$부분모임합문제

최혁, 최충혁

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《현시대는 과학기술의 시대이며 과학기술의 발전수준은 나라의 종합적국력과 지위를 규정하는 징표로 됩니다.》

부분모임합문제는 부호리론과 암호학, 그라프리론 등 많은 응용분야들에서 중요하게 제기된다. 그가운데는 $k-$부분모임합문제도 있는데 이것은 NP－곤난문제로서 일반적으로 풀기가 매우 어려운것으로 인정되고있다. 그러나 특정한 대수적구조를 가지는 모임에 대하여서는 이 문제가 풀릴수 있다.

F_q를 유한체(여기서 $q=p^s$, p는 씨수, $s\ge 1$), D를 F_q의 부분모임, k는 $1\le k\le |D|$인 정의 옹근수이고 $b\in F_q$에 대하여 $N_D(k,\ b):=\left|\left\{S\subseteq D\left|\sum_{a\in S}a=b,\ |S|=k\right.\right\}\right|$라고 정의하자.

$D,\ k,\ b$가 주어졌을 때 $N_D(k,\ b)$를 구하는 문제를 $k-$부분모임합문제(간단히 $k-$SSP)라고 부른다.[5] 여기서 $N_D(k,\ b)=N_D\left(|D|-k,\ \sum_{a\in D}a-b\right)$이기때문에 $1\le k\le \frac{|D|}{2}$라고 해도 일반성을 잃지 않는다.

$k-$SSP와 관련한 선행연구들에서는 $N_D(k,\ b)$의 정확한 평가식 또는 점근공식을 구하는 방법으로 $N_D(k,\ b)>0$이라는것을 판정하였다.

선행연구[4]에서는 $F_q\setminus D$의 농도가 작은 경우에 $N_D(k,\ b)$의 점근공식을 얻었고 선행연구[6]에서는 D가 F_q의 지표 2인 곱하기부분군인 경우 $N_D(k,\ b)$를 구하는 공식을 얻었다. 그리고 선행연구[2, 5]에서는 D가 홀수표수를 가지는 유한체 F_q의 지표 m인 곱하기부분군인 경우 $N_D(k,\ b)>0$이기 위한 충분조건을 얻었다.

론문에서는 선행연구들에서 연구되지 않은 유한체의 표수가 2이고 k가 $|D|/2$에 가까운 큰 수인 경우 $k-$SSP에 대하여 연구하였다.

X를 D^k의 부분모임, $\overline{X}:=\{(x_1,\ \cdots,\ x_k)\in X\,|\,x_i\ne x_j(i\ne j)\}$라고 하고 X우에서 정의된 복소수값함수 $f(x_1,\ x_2,\ \cdots,\ x_k)$에 대하여 $F=\sum_{x\in\overline{X}}f(x_1,\ x_2,\ \cdots,\ x_k)$라고 놓자.

k차치환 $\tau\in S_k$가 서로 비교차하는 $i-$순환 c_i개들의 적으로 표시될 때 τ를 $(c_1,\ \cdots,\ c_k)$형태의 치환이라고 하고 $N(c_1,\ \cdots,\ c_k)$를 S_k에서 $(c_1,\ \cdots,\ c_k)$형태의 치환의 개수라고 하면 $N(c_1,\ \cdots,\ c_k)=\dfrac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!}$이다.

이제 $C_k(t_1,\ \cdots,\ t_k):=\sum_{\sum ic_i=k}N(c_1,\ \cdots,\ c_k)t_1^{c_1}t_2^{c_2}\cdots t_k^{c_k}$이라고 약속하자.

명제 1[3] 만일 $\begin{cases} t_i = a, & p \nmid i \\ t_i = b, & p \mid i \end{cases}$ 이면

$$C_k\left(\overbrace{a, \cdots, a}^{p-1}, b, \overbrace{a, \cdots, a}^{p-1}, b, \cdots\right) = k! \sum_{t=0}^{\lfloor k/p \rfloor} \binom{(b-a)/p+i-1}{i} \binom{a+k-pi-1}{k-pi} \le \left(a+k+\frac{b-a}{p}-1\right)_k$$

이다. 여기서 $(x)_k = x(x-1)(x-2)\cdots(x-k+1)$ 이다.

k 차대칭군 S_k 는 $\sigma \circ (x_1, \cdots, x_k) = (x_{\sigma(1)}, \cdots, x_{\sigma(k)})$ ($\sigma \in S_k$, $(x_1, \cdots, x_k) \in D^k$)에 의해 D^k 에 작용하는데 부분모임 X 가 S_k 의 이 작용에 의해서 변하지 않을 때 대칭적이라고 부른다.

τ 의 완전분해를 $\tau = (i_1 \ \cdots \ i_{a_1}) \cdots (l_1 \ \cdots \ l_{a_s})$ 라고 할 때

$$X_\tau := \{(x_1, \cdots, x_k) \mid x_{i_1} = \cdots = x_{i_{a_1}}, \cdots, x_{l_1} = \cdots = x_{l_{a_s}}\}, \quad F_\tau := \sum_{x \in X_\tau} f(x_1, x_2, \cdots, x_k)$$

라고 정의하자.

X 가 대칭적이고 $\tau, \tau' (\in S_k)$ 들이 서로 공액일 때

$$\sum_{x \in X_\tau} f(x_1, x_2, \cdots, x_k) = \sum_{x \in X_{\tau'}} f(x_1, x_2, \cdots, x_k)$$

를 만족시키면 X 우의 복소수값함수 f 는 X 우에서 불변이라고 말한다.

명제 2[3] 만일 f 가 X 우에서 불변이면 $F = \sum_{\sum ic_i = k} (-1)^{k - \sum c_i} N(c_1, \cdots, c_k) F_\tau$ 가 성립된다.

명제 3[1] n 차다항식 $f \in F_q[x]$ 와 임의의 비자명한 더하기지표 $\psi : (F_q, +) \to \mathbf{C}$ 에 대하여 $\left| \sum_{x \in F_q} \psi(f(x)) \right| \le (n-1)\sqrt{q}$ 가 성립된다. 여기서 $\gcd(n, q) = 1$ 이다.

정리 1 D 를 $|D| > 6s\sqrt{q}$ 인 유한체 F_q 의 부분모임(여기서 $q = 2^s$, $s \ge 1$), k 는 $|D|/3 < k \le |D|/2 - \sqrt{q}$ 를 만족시키는 정의 옹근수라고 하자.

만일 임의의 비자명한 더하기지표 $\psi : (F_q, +) \to \mathbf{C}$ 에 대하여 $\left| \sum_{x \in D} \psi(x) \right| \le \sqrt{q}$ 이면 임의의 $b \in F_q$ 에 대하여 $N_D(k, b) > 0$ 이다.

증명 B 를 F_q 의 더하기지표들이 이루는 군이라고 하자.

지표합의 성질로부터 $N_D(k, b) = \dfrac{1}{q} \sum_{\substack{x_i \in D \\ x_i \ne x_j}} \sum_{\psi \in B} \psi(x_1 + x_2 + \cdots + x_k - b)$ 이다.

자명한 지표를 옮기고 합기호를 바꾸면

$$\left| N_D(k, b) - \frac{1}{q}(|D|)_k \right| = \frac{1}{q} \left| \sum_{\substack{\psi \in B \\ \psi \ne 1}} \psi(b)^{-1} \sum_{\substack{x_i \in D \\ x_i \ne x_j}} \psi(x_1 + x_2 + \cdots + x_k) \right| \le \max_{\substack{\psi \in B \\ \psi \ne 1}} \left| \sum_{\substack{x_i \in D \\ x_i \ne x_j}} \psi(x_1 + x_2 + \cdots + x_k) \right|$$

가 성립된다.

이제

$$X = D^k,\ \ \overline{X} = \{(x_1,\ x_2,\ \cdots,\ x_k) \in D^k \mid x_i \neq x_j (i \neq j)\},$$

$$f(x_1,\ x_2,\ \cdots,\ x_k) = \psi(x_1 + x_2 + \cdots + x_k) = \psi(x_1)\psi(x_2)\cdots\psi(x_k)$$

라고 하면 $F = \sum_{x \in \overline{X}} f(x) = \sum_{\substack{x_i \in D \\ x_i \neq x_j}} \psi(x_1 + x_2 + \cdots + x_k)$ 이다.

함수 $f(x_1,\ x_2,\ \cdots,\ x_k)$ 는 $x_1,\ \cdots,\ x_k$ 에 관하여 대칭이고 X 우에서 불변이므로 $(c_1,\ c_2,\ \cdots,\ c_k)$ 형태의 치환 $\tau \in S_k$ 에 대하여 명제 2를 적용하면

$$\left| N_D(k,\ b) - \frac{1}{q}(|D|)_k \right| \leq \left| \sum_{\sum ic_i = k} (-1)^{k - \sum c_i} N(c_1,\ \cdots,\ c_k) F_\tau \right| \leq \sum_{\sum ic_i = k} N(c_1,\ \cdots,\ c_k) |F_\tau|$$

이 얻어진다. 그런데

$$|F_\tau| = \left| \sum_{x \in X_\tau} \psi(x_{11}) \cdots \psi(x_{1c_1}) \cdots \psi^k(x_{k1}) \cdots \psi^k(x_{kc_k}) \right| \leq$$

$$\leq \left| \sum_{x_{11} \in D} \psi(x_{11}) \right| \cdots \left| \sum_{x_{1c_1} \in D} \psi(x_{1c_1}) \right| \cdots \left| \sum_{x_{k1} \in D} \psi^k(x_{k1}) \right| \cdots \left| \sum_{x_{kc_k} \in D} \psi^k(x_{kc_k}) \right|$$

이고 $\left| \sum_{d \in D} \psi^i(d) \right| \leq \begin{cases} \sqrt{q}, & 2 \nmid i \\ |D|, & 2 \mid i \end{cases}$ 이므로 명제 1에 의하여 다음의 식이 얻어진다.

$$\left| N_D(k,\ b) - \frac{1}{q}(|D|)_k \right| \leq C_k(\sqrt{q},\ |D|,\ \sqrt{q},\ |D|,\ \cdots) \leq$$

$$\leq \left(\sqrt{q} + k + \frac{|D| - \sqrt{q}}{2} - 1 \right)_k < \left(k + \frac{|D| + \sqrt{q}}{2} \right)_k$$

그러므로 $\frac{1}{q}(|D|)_k > \left(k + \frac{|D| + \sqrt{q}}{2} \right)_k$ 이면 $N_D(k,\ b) > 0$ 이다.

한편 부등식 $\frac{1}{q}(|D|)_k > \left(k + \frac{|D| + \sqrt{q}}{2} \right)_k$ 는 $\frac{|D|}{k + (|D| + \sqrt{q})/2} > q^{1/k}$ 이 성립되면 만족된다.

그런데 $k \leq |D|/2 - \sqrt{q}$ 이므로

$$\left(\frac{|D|}{k + |D| + \sqrt{q})/2} \right)^k \geq \left(\frac{|D|}{|D| - \sqrt{q}/2} \right)^k > \left(\frac{q}{q - \sqrt{q}/2} \right)^k = \left(1 + \frac{1}{2\sqrt{q} - 1} \right)^k > \left(1 + \frac{1}{2\sqrt{q}} \right)^k >$$

$$> \left(1 + \frac{1}{2\sqrt{q}} \right)^{|D|/3} > \left(1 + \frac{1}{2\sqrt{q}} \right)^{2s\sqrt{q}} = \left[\left(1 + \frac{1}{2\sqrt{q}} \right)^{2\sqrt{q}} \right]^s > 2^s = q$$

이고 따라서 우의 론의로부터 $N_D(k,\ b) > 0$ 이다.(증명끝)

이제 D 를 F_q^* 의 지표 m 인 부분군이라고 하면 $D = \{x^m \mid x \in F_q^*\}$ 이고 $|D| = (q-1)/m$ 이다.