김일성종합대학학보 주체109(2020)년
수 학 제66권 제1호

표수가 2인 유한체우에서 $k-$부분모임합문제의 가해성

최혁, 최충혁

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

《수학, 물리학, 화학, 생물학과 같은 기초과학부문에서 과학기술발전의 원리적, 방법론적기초를 다져나가면서 세계적인 연구성과들을 내놓아야 합니다.》

부분모임합문제는 부호리론과 암호학, 그라프리론 등 수학의 많은 응용분야들에서 중요하게 제기된다. 이 문제들가운데는 NP－곤난문제로 알려진 $k-$부분모임합문제도 있다. 일반적으로 $k-$부분모임합문제는 풀기가 어렵지만 특정한 대수적구조를 가지는 모임인 경우에는 풀수 있다.

F_q(여기서 $q:=p^s$ 인데 p는 씨수이고 $s\ge1$)는 유한체이고 D는 F_q의 비지 않은 부분모임이며 k는 $1\le k\le|D|$인 정의 옹근수라고 하자. 그리고 $b(\in F_q)$에 대하여

$$N_D(k,\ b):=\left|\left\{S\subseteq D\ \middle|\ \sum_{a\in S}a=b,\ |S|=k\right\}\right|$$

로 놓자. 이때 주어진 $D,\ k,\ b$에 대하여 $N_D(k,\ b)$를 구하는 문제를 $k-$부분모임합문제라고 부른다.[3] 여기서 $N_D(k,\ b)=N_D\left(|D|-k,\ \sum_{a\in D}a-b\right)$이기때문에 $k\le|D|/2$라고 해도 일반성을 잃지 않는다.[3] 그런데 이 문제는 풀기가 어렵기때문에 보통은 $N_D(k,\ b)>0$을 판정하는 문제를 $k-$부분모임합문제라고 부르고 간단히 $k-\mathrm{SSP}$로 표시한다.[5]

$k-\mathrm{SSP}$와 관련한 선행연구들에서는 일부 경우들에 대하여 $N_D(k,\ b)$를 구하는 공식 또는 근사공식을 얻거나 $N_D(k,\ b)>0$이라는것을 밝혔다. 선행연구[2]에서는 $F_q\setminus D$의 농도가 작은 경우에 $N_D(k,\ b)$의 점근공식이 얻어졌고 선행연구[4]에서는 D가 F_q의 지표가 2인 곱하기에 관한 부분군인 경우 $N_D(k,\ b)$를 구하는 공식이 얻어졌다. 그리고 선행연구[3, 5]에서는 D가 표수가 홀수인 유한체 F_q의 곱하기에 관한 부분군인 경우에 $N_D(k,\ b)>0$이기 위한 충분조건이 얻어졌다. 그러나 선행연구들에서는 표수가 2인 유한체에서 k가 ($|D|/2$에 가까운)큰 수인 경우 $N_D(k,\ b)>0$이기 위한 충분조건을 얻지 못하였다.

론문에서는 이 경우에 $k-\mathrm{SSP}$의 가해성을 연구하기 위하여 $N_D(k,\ b)>0$이 성립하기 위한 한가지 충분조건을 얻으려고 한다.

F_q는 $q(:=2^s)$개의 원소들로 이루어진 유한체라고 하자. 그리고 D는 유한체 F_q의 부분모임이고 k는 $k\le|D|$인 정의 옹근수이며 F_q의 비자명한 더하기지표 ψ에 대하여

$$S_D(k,\ \psi):=\sum_{\substack{x_1,\ \cdots,\ x_k\in D\\ x_i:\text{서로 다름}}}\psi(x_1+\ \cdots\ +x_k)$$

로 놓자.

보조정리 1 D는 $|D|\geq 3$인 F_q의 부분모임이고 ψ는 F_q의 비자명한 더하기지표라고 하자. 이때

$$S_D(k,\ \psi)=S_D(1,\ \psi)^2-|D|$$

이며 $3\leq k\leq |D|$일 때 다음의 식이 성립한다.

$$S_D(k,\ \psi)=S_D(1,\ \psi)S_D(k-1,\ \psi)-(|D|-k+2)(k-1)S_D(k-2,\ \psi)$$

증명 F_q의 표수가 2라는것을 고려하면 다음의 식이 얻어진다.

$$\begin{aligned}S_D(2,\ \psi)&=\sum_{\substack{x_1,\ x_2\in D\\ x_1\neq x_2}}\psi(x_1+x_2)=\sum_{x_1\in D}\ \sum_{x_2\in D\setminus\{x_1\}}\psi(x_1+x_2)=\\ &=\sum_{x_1\in D}\psi(x_1)\sum_{x_2\in D\setminus\{x_1\}}\psi(x_2)=\sum_{x_1\in D}\psi(x_1)(S_D(1,\ \psi)-\psi(x_1))=\\ &=\sum_{x_1\in D}(\psi(x_1)\cdot S_D(1,\ \psi)-1)=S_D(1,\ \psi)^2-|D|\end{aligned}$$

그리고 $k\geq 3$이면

$$\begin{aligned}S_D(k,\ \psi)&=\sum_{\substack{x_1,\cdots,\ x_k\in D\\ x_i:\text{서로 다름}}}\psi(x_1+\ \cdots\ +x_k)=\sum_{\substack{x_1,\cdots,\ x_{k-1}\in D\\ x_i:\text{서로 다름}}}\ \sum_{x_k\in D\setminus\{x_1,\cdots,\ x_{k-1}\}}\psi(x_1+\ \cdots\ +x_k)=\\ &=\sum_{\substack{x_1,\cdots,\ x_k\in D\\ x_i:\text{서로 다름}}}\psi(x_1+\ \cdots\ +x_{k-1})\sum_{x_k\in D\setminus\{x_1,\cdots,\ x_{k-1}\}}\psi(x_k)=\\ &=\sum_{\substack{x_1,\cdots,\ x_k\in D\\ x_i:\text{서로 다름}}}\psi(x_1+\ \cdots\ +x_{k-1})(S_D(1,\ \psi)-\sum_{i=1}^{k-1}\psi(x_i))=\\ &=S_D(1,\ \psi)S_D(k-1,\ \psi)-\sum_{\substack{x_1,\cdots,\ x_k\in D\\ x_i:\text{서로 다름}}}\sum_{i=1}^{k-1}\psi(x_1+\ \cdots\ +x_{i-1}+x_{i+1}+\ \cdots\ +x_{k-1})=\\ &=S_D(1,\ \psi)S_D(k-1,\ \psi)-\sum_{i=1}^{k-1}\sum_{\substack{x_1,\cdots,\ x_{k-1}\in D\\ x_i:\text{서로 다름}}}\psi(x_1+\ \cdots\ +x_{i-1}+x_{i+1}+\ \cdots\ +x_{k-1})=\\ &=S_D(1,\ \psi)S_D(k-1,\ \psi)-\\ &\quad-\sum_{i=1}^{k-1}\sum_{\substack{x_1,\cdots,\ x_{i-1},\ x_{i+1},\ \cdots,\ x_{k-1}\in D\\ x_j:\text{서로 다름}}}\ \sum_{\substack{x_i\in D\\ x_i\neq x_j\ (\forall j\neq i)}}\psi(x_1+\ \cdots\ +x_{i-1}+x_{i+1}+\ \cdots\ +x_{k-1})=\\ &=S_D(1,\ \psi)S_D(k-1,\ \psi)-\\ &\quad-\sum_{i=1}^{k-1}\sum_{\substack{x_1,\cdots,\ x_{i-1},\ x_{i+1},\ \cdots,\ x_{k-1}\in D\\ x_j:\text{서로 다름}}}(|D|-k+2)\cdot\psi(x_1+\ \cdots\ +x_{i-1}+x_{i+1}+\ \cdots\ +x_{k-1})=\\ &=S_D(1,\ \psi)S_D(k-1,\ \psi)-\sum_{i=1}^{k-1}(|D|-k+2)\cdot S_D(k-2,\ \psi)=\end{aligned}$$

$$= S_D(1,\ \psi)S_D(k-1,\ \psi) - (|D|-k+2)(k-1)S_D(k-2,\ \psi)$$

이다.(증명끝)

보조정리 2 D는 $|D|\ge 4$인 F_q의 부분모임이고 ψ는 F_q의 비자명한 더하기지표라고 하자. 이때 만일 $1/16$을 넘지 않는 어떤 상수 c가 존재하여

$$\left|\sum_{x\in D}\psi(x)\right| \le c\,|D|$$

이면 $k\le |D|/2$인 임의의 정의 옹근수 k에 대하여 다음의 부등식이 성립한다.

$$|S_D(k,\ \psi)| = \left(\frac{9}{16}|D|\right)^k$$

증명 $r := 9/16$로 놓자. 그리고 k에 관한 귀납법으로 증명하자.

$k=1$인 경우에 $|S_D(k,\ \psi)| \le c\,|D| \le r\,|D|$이므로 결과가 성립한다.

$k=2$인 경우에도 보조정리 1에 의하여 $|S_D(k,\ \psi)| < (c\,|D|)^2 + |D| < (r\,|D|)^2$이므로 결과가 성립한다.

이제 $k\ge 3$이라고 하고 $k-1$이하에 대하여 명제가 성립한다고 가정하자. 그러면 보조정리 1과 귀납가정으로부터

$$\begin{aligned}|S_D(k,\ \psi)| &\le |S_D(1,\ \psi)S_D(k-1,\ \psi)| + (|D|-k+2)(k-1)\,|S_D(k-2,\ \psi)| \le \\ &\le c\,|D|\cdot(r\,|D|)^{k-1} + \left(\frac{|D|}{2}+2\right)\left(\frac{|D|}{2}-1\right)(r\,|D|)^{k-2} < \\ &< c\,|D|\cdot(r\,|D|)^{k-1} + \frac{9|D|^2}{32}(r\,|D|)^{k-2} = (r\,|D|)^k\left(\frac{c}{r}+\frac{9}{32r^2}\right) \le (r\,|D|)^k\end{aligned}$$

이 얻어진다.(증명끝)

정리 1 D는 F_q의 부분모임이고 k는 $3.05s < k \le |D|/2$를 만족시키는 정의 옹근수라고 하자. 이때 만일 $1/16$을 넘지 않는 어떤 상수 c가 존재하여 F_q의 임의의 비자명한 더하기지표 ψ에 대하여

$$\left|\sum_{x\in D}\psi(x)\right| \le c\,|D|$$

이면 임의의 $b(\in F_q)$에 대하여 $N_D(k,\ b) > 0$이 성립한다.

증명 B를 F_q의 더하기지표들전부가 이루는 군이라고 하자. 그러면 지표합의 성질 [1]로부터

$$N_D(k,\ b) = \frac{1}{q}\sum_{\substack{x_i\in D\\ x_i:\text{서로 다름}}}\ \sum_{\psi\in B}\psi(x_1+x_2+\cdots+x_k-b)$$

가 성립한다. 그러므로 보조정리 2에 의하여

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

$$\le \max_{\substack{\psi\in B\\ \psi\ne 1}}\left\{\left|\sum_{\substack{x_i\in D\\ x_i:\text{서로 다름}}}\psi(x_1+x_2+\cdots+x_k)\right|\right\}=\max_{\substack{\psi\in B\\ \psi\ne 1}}\{|S_D(k,\ \psi)|\}<\left(\frac{9}{16}|D|\right)^k$$

이 얻어진다. 여기서 $x\in\mathbf{R},\ k\in\mathbf{N}$에 대하여 $(x)_k:=x(x-1)\cdots(x-k+1)$이다. 한편

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

$$>\frac{1}{q}\left(\frac{9}{16}|D|\right)^k\cdot\left(\frac{16}{9\sqrt{2}}\right)^k>\frac{1}{q}\left(\frac{9}{16}|D|\right)^k\cdot\left(\frac{16}{9\sqrt{2}}\right)^{3.05s}>\frac{1}{q}\left(\frac{9}{16}|D|\right)^k\cdot 2^s=\left(\frac{9}{16}|D|\right)^k$$

이므로

$$N_D(k,\ b)>\frac{1}{q}(|D|)_k-\left(\frac{9}{16}|D|\right)^k>0$$

이다.(증명끝)

정리 2 $s\ge 8$이고 D는 $|D|>5q^{2/3}$인 F_q의 부분모임이며 k는 $3\le k\le\sqrt{|D|}$를 만족시키는 정의 옹근수라고 하자. 이때 만일 F_q의 임의의 비자명한 더하기지표 ψ에 대하여

$$\left|\sum_{x\in D}\psi(x)\right|\le\frac{1}{\sqrt[3]{2q}}|D|$$

이면 임의의 $b(\in F_q)$에 대하여 $N_D(k,\ b)>0$이 성립한다.

이제 $s\ge 11$이라고 하자. 그러면 $1/\sqrt[3]{2q}\le 1/16$이기때문에 정리 1, 2를 결합하여 다음과 같은 정리를 얻을수 있다.

정리 3 $s\ge 11$이고 D는 $|D|>\max\{5q^{2/3},\ (3.05s)^2\}$인 F_q의 부분모임이며 k는 $3\le k\le |D|/2$를 만족시키는 정의 옹근수라고 하자. 이때 만일 F_q의 임의의 비자명한 더하기지표 ψ에 대하여

$$\left|\sum_{x\in D}\psi(x)\right|\le\frac{1}{\sqrt[3]{2q}}|D|$$

이면 임의의 $b(\in F_q)$에 대하여 $N_D(k,\ b)>0$이 성립한다.

참 고 문 헌

[1] 김률, 유한체; **김일성**종합대학출판사, 250～300, 주체100(2011).

[2] J. Li et al.; Finite Fields Appl., 14, 911, 2008.

[3] W. Wang et al.; Finite Fields Appl., 51, 204, 2018.

[4] W. Wang et al.; Finite Fields Appl., 43, 106, 2017.

[5] G. Zhu et al.; Finite Fields Appl., 18, 192, 2012.

주체108(2019)년 9월 15일 원고접수

Solvability of the k – Subset Sum Problem over Finite Fields of Characteristic 2

Choe Hyok, Choe Chung Hyok

In this paper, we study the solvability of the k – subset sum problem over finite fields of characteristic 2.

Keywords: subset sum, k – SSP