Title
An asymptotic formula for counting subset sums over subgroups of finite fields

Permalink
https://escholarship.org/uc/item/9x9940kz

Journal
Finite Fields and Their Applications, 18(1)

ISSN
1071-5797

Authors
Zhu, Guizhen
Wan, Daqing

Publication Date
2012

DOI
10.1016/j.ffa.2011.07.010

Peer reviewed

An Asymptotic Formula For Counting Subset Sums Over Subgroups Of Finite Fields

Guizhen Zhu
Institute For Advanced Study
Tsinghua University, Beijing, P.R. China
zhugz08@mails.tsinghua.edu.cn

Daqing Wan
Department of Mathematics
University of California, Irvine, CA 92697-3875, USA
dwan@math.uci.edu

2010.12.26

Abstract

Let $\mathbb{F}_q$ be the finite field of q elements. Let $H \subseteq \mathbb{F}_q^*$ be a multiplicative subgroup. For a positive integer k and element $b \in \mathbb{F}_q$, we give a sharp estimate for the number of k-element subsets of H which sum to b.

1 Introduction

Let $\mathbb{F}_q$ be the finite field of q elements of characteristic p. Let $H \subseteq \mathbb{F}_q$ be a subset. Let $1 \leq k \leq |H|$ be a positive integer. For $b \in \mathbb{F}_q$, let $M_H(k, b)$ denote the number of k-element subsets $S \subseteq H$ such that

$$\sum_{a \in S} a = b.$$

The decision version of the k-subset sum problem for H is to determine if $M_H(k, b) > 0$. This problem arises naturally from a number of important applications in coding theory and cryptography. It is a well known NP-complete problem, and thus there is not much more one can say about the solution number $M_H(k, b)$ in such a generality. The main difficulty comes from the combinatorial flexibility in choosing the subset H and thus the lack of algebraic structure for the subset H. From algorithmic point of view, the dynamic

[1] MSC: 05A15 11T24 11T99 12E20

[2] Keywords: distinct coordinate sieve, subset sum problem, finite fields, character sum, inclusive-exclusive principle

algorithm [2] can be used to show that the decision version of the k-subset sum problem can be solved in polynomial time if H is a large subset of $\mathbb{F}_q$ in the sense that $|H|$ is of size q^ϵ for some constant $\epsilon > 0$. From mathematical point of view, we are more interested in the actual value of the solution number $M_H(k,b)$. Ideally, we would like to have an explicit formula or an asymptotic formula for the solution number $M_H(k,b)$. This is apparently too much to hope for in general. However, we believe that it should be possible to obtain an asymptotic formula for the number $M_H(k,b)$ for k in certain range if H is close to a large subset of $\mathbb{F}_q$ with certain algebraic structure. For example, it is shown in [4] that if $\mathbb{F}_q - H$ is a small set, then a good asymptotic formula for $M_H(k,b)$ can be obtained. In addition, if $H = \mathbb{F}_q$, or $\mathbb{F}_q^*$ or any additive subgroup of $\mathbb{F}_q$, then an explicit formula for $M_H(k,b)$ (with no error term) is obtained in [4][5].

When H is close to a multiplicative subgroup of $\mathbb{F}_q$, the situation is more complicated as the multiplication operation is different from the addition operation in the subset sum problem. A multiplicative subgroup is far from the additive structure. The subset sum problem in this case becomes a highly non-linear algebraic problem with combinatorial constraints. In this paper, we study the case that H is a multiplicative subgroup of $\mathbb{F}_q^*$ and obtain a sharp asymptotic formula for the number $M_H(k,b)$ if the index $[\mathbb{F}_q^* : H]$ is reasonably small. Our main tool is the new sieve formula from [5] together with standard character sum arguments over finite fields.

From now on, we let H be a multiplicative subgroup of $\mathbb{F}_q^*$ with index m. Thus, $|H| = (q-1)/m$. The number of k-subsets of H is $\binom{(q-1)/m}{k}$, and the sum could be any element b of the field $\mathbb{F}_q$. One expects that in favorable cases that the k-subset sums are equally distributed and thus $M_H(k,b)$ should be about $\frac{1}{q}\binom{(q-1)/m}{k}$. The key is then reduced to estimating the error term. Our main result is the following

Theorem 1.1. *Let $1 \leq k \leq (q-1)/m$. For $b \in \mathbb{F}_q^*$, we have the asymptotic formula*

$$\left| M_H(k,b) - \frac{1}{q}\binom{(q-1)/m}{k} \right| \leq \frac{2}{\sqrt{q}} \binom{\sqrt{q} + k + \frac{q}{mp}}{k};$$

and for $b = 0$, we have

$$\left| M_H(k,0) - \frac{1}{q}\binom{(q-1)/m}{k} \right| \leq \binom{\sqrt{q} + k + \frac{q}{mp}}{k},$$

where p is the characteristic of $\mathbb{F}_q$.

Because of the obvious symmetry

$$M_H(k,b) = M_H(|H| - k, \sum_{a \in H} a - b),$$

we may without loss of generality assume that $k \leq |H|/2 = (q-1)/2m$.

Corollary 1.2. *Let $p > 2$. There is an effectively computable absolute constant $0 < c < 1$ such that if $m < c\sqrt{q}$ and $6 \ln q < k \leq \frac{q-1}{2m}$, then $M_H(k,b) > 0$ for all $b \in \mathbb{F}_q$.*

Note that even in the case that H is a multiplicative subgroup of $\mathbb{F}_q^*$, we still do not know a complete polynomial time algorithm to decide if $M_H(k,b) > 0$, if m is large. The result in above corollary gives a partial answer to this algorithmic question. The case that k is small (say, $k \leq 6 \ln q$) can be treated using an easier Brun sieve approach [1], but to get a non-trivial lower bound, one needs to assume that m is significantly smaller. For example, in the case $k = 2$, one may need to assume that $m < q^{1/4}$ to guarantee the existence of a non-trivial $\mathbb{F}_q$-rational point on the curve $X_1^m + X_2^m = b$. For algorithmic purpose, the small k case can often be done by a quick exhaustive search or by using the more efficient dynamic algorithm.

To illustrate our ideas, we will also consider the following related but somewhat simpler problem of counting points on diagonal equations with distinct coordinates. Since H is a subgroup of $\mathbb{F}_q^*$ with index $m|(q-1)$, we have $H = \{x^m | x \in \mathbb{F}_q^*\}$. For $0 \leq k \leq q-1$, let $N_m^*(k,b)$ denote the number of solutions of the diagonal equation

$$x_1^m + x_2^m + \cdots + x_k^m = b,$$

where the x_i's are in $\mathbb{F}_q^*$ and the x_i's are distinct. There is an obvious way to compute $N_m^*(k,b)$ via the classical inclusion-exclusion principle. Define

$$X = \{(x_1, x_2, \ldots, x_k) \in (\mathbb{F}_q^*)^k | x_1^m + x_2^m + \cdots + x_k^m = b\}.$$

Then

$$N_m^*(k,b) = \#\{(x_1, x_2, \ldots, x_k) \in X | x_i \neq x_j, i \neq j\}.$$

Let

$$X_{ij} = \{(x_1, x_2, \ldots, x_k) \in X | x_i = x_j, i \neq j\}, \quad X_{ij}^c = X - X_{ij}.$$

Applying the classical inclusion-exclusion principle, we obtain

$$\begin{aligned} N_m^*(k,b) &= |\bigcap_{1 \leq i \leq j \leq k} X_{ij}^c| \\ &= |X| - \sum_{1 \leq i \leq j \leq k} |X_{ij}| + \sum_{\substack{1 \leq i \leq j \leq k \\ 1 \leq s \leq t \leq k}} |X_{ij} \bigcup X_{st}| - \cdots + (-1)^{\binom{k}{2}} |\bigcap_{1 \leq i \leq j \leq k} X_{ij}|. \end{aligned}$$

Each term on the right side can be estimated using some basic properties of Gauss sum and Jacobi sum. The main terms are of at most $O(q^k)$. However, the number of terms in the above inclusion-exclusion is $2^{\binom{k}{2}}$ which can add up to a total error term which may be greater than the main term $O(q^k)$ as soon as k is greater than $\Omega(\sqrt{q})$. Fortunately in [5], J.Y.Li and D. Wan presented a new sieve for distinct coordinate counting problem which can be used for our estimation. This sieve reduces the number of total terms from $2^{\binom{k}{2}}$ to $k!$, allowing us to deduce non-trivial information for k as large as a fraction of q (and thus much larger than $O(\sqrt{q})$. We will introduce their sieve briefly in Section 2. Now we state our main asymptotic formula for the number $N_m^*(k,b)$.

Theorem 1.3. *For all $b \in \mathbb{F}_q^*$, we have*

$$\left| N_m^*(k,b) - \frac{(q-1)_k}{q} \right| \leq \frac{2}{\sqrt{q}} \left(m\sqrt{q} + k + \frac{q}{p} \right)_k, \tag{1.1}$$

and for $b = 0$, we have

$$\left| N_m^*(k,0) - \frac{(q-1)_k}{q} \right| \leq \left(m\sqrt{q} + k + \frac{q}{p} \right)_k,$$

where $(t)_k = t(t-1)\cdots(t-k+1)$ for a real number t.

Again, we have the symmetry

$$N_m^*(k,b) = N_m^*(q-1-k, \sum_{a \in H} a^m - b).$$

Thus, we may assume that $0 \leq k \leq (q-1)/2$.

Corollary 1.4. *Let $p > 2$. There is an effectively computable absolute constant $0 < c < 1$ such that if $m < c\sqrt{q}$ and $6 \ln q < k \leq \frac{q-1}{2}$ then $N_m^*(k,b) > 0$ for all $b \in \mathbb{F}_q$.*

Some preliminaries will be introduced briefly in section 2. In section 3, we will illustrate the asymptotic formula for the number $N_m^*(k,b)$. The punchline will be our asymptotic formula for $M_H(k,b)$.

2 Preliminaries

2.1 Li-Wan's new sieve

In [5], J.Y. Li and D. Wan presented a new sieve for the distinct coordinate counting problem. We will introduce it briefly.

Let D be a finite set. For a positive integer k, let $D^k = D \times D \times \cdots \times D$ be the Cartesian product of k copies of D. Let $X \subset D^k$. Every element $x \in X$ can be written as $x = (x_1, \ldots, x_k)$ with $x_i \in D$. We are interested in counting the number of elements in X with distinct coordinates, i.e., the cardinality of the set

$$\overline{X} = \{(x_1, \ldots, x_k) \in X | x_i \neq x_j, i \neq j\}.$$

Let S_k be the symmetric group. For a given permutation $\tau \in S_k$, write its disjoint cycle product as $\tau = (i_1 \cdots i_{a_1})(j_1 \cdots j_{a_2}) \cdots (l_1 \cdots l_{a_s})$, where $a_i \geq 1, 1 \leq i \leq s$. Define the sign of τ as $sign(\tau) = (-1)^{k-l(\tau)}$,where $l(\tau)$ is the number of disjoint cycles in τ. Define

$$X_\tau = \{(x_1, \ldots, x_k) \in X | x_{i_1} = \cdots = x_{i_{a_1}}, \ldots, x_{l_1} = \cdots = x_{l_{a_s}}\}.$$

We have the following theorem:

Theorem 2.1.

$$|\overline{X}| = \sum_{\tau \in S_k} sign(\tau)|X_\tau|.$$

Moreover, the group S_k acts on D^k by permuting its coordinates, that is

$$\tau \circ (x_1, \dots, x_k) = (x_{\tau(1)}, \dots, x_{\tau(s)}).$$

If X is invariant under the action of S_k, we call it symmetric. A permutation $\tau \in S_k$ is said to be of type $(c_1, \dots, c_k)$ if τ has exactly c_i cycles of length i. Let $N(c_1, \dots, c_k)$ denote the number of permutations of type $(c_1, \dots, c_k)$ in S_k. We have the following theorem which will be used in our main results of this paper.

Theorem 2.2. *If X is symmetric, then*

$$|\overline{X}| = \sum_{\sum ic_i = k} (-1)^{k - \sum c_i} N(c_1, \dots, c_k)|X_\tau|.$$

2.2 Some combinatorial formulas

In order to prove the main results in this paper, we need to know some combinational formulas as follows. Their proofs can be found in [5]. Let $N(c_1, \dots, c_k)$ be the number of permutations of type $(c_1, \dots, c_k)$ in S_k. From [6], we can see:

$$N(c_1, \dots, c_k) = \frac{k!}{1^{c_1}c_1!2^{c_2}c_2! \cdots k^{c_k}c_k!}.$$

Lemma 2.3. *Define the generating function*

$$C_k(t_1, \dots, t_k) = \sum_{\sum ic_i = k} N(c_1, \dots, c_k) t_1^{c_1} \cdots t_k^{c_k}.$$

(1) If $t_1 = \cdots = t_k = q$, then

$$C_k(q, \dots, q) = (q + k - 1)_k.$$

(2) If $q \geq d$, $d|(q-s)$ and $t_i = q$ for $d|i$, $t_i = s$ for $d \nmid i$, then

$$C_k(\overbrace{s, \dots, s}^{d-1}, q, \overbrace{s, \dots, s}^{d-1}, q, \dots) = k! \sum_{i=0}^{\lfloor \frac{k}{d} \rfloor} \binom{\frac{q-s}{d} + i - 1}{\frac{q-s}{d} - 1} \binom{s + k - di - 1}{s - 1}. \tag{2.1}$$

Lemma 2.4. *For any giver positive integers m, n, q and l, we have*

$$\sum_{i \geq 0} \binom{l+i}{n} \binom{q-i}{m} \leq \binom{l+q+1}{m+n+1}.$$

As a corollary, we get

Corollary 2.5. *For any given positive integers s, d, k, q with $q \geq s$ and $d|(q-s)$, we have*

$$C_k(\overbrace{s,\dots,s}^{d-1},q,\overbrace{s,\dots,s}^{d-1},q,\dots) \leq \left(s+k+\frac{q-s}{d}-1\right)_k.$$

Proof.

$$\begin{aligned}
C_k(\overbrace{s,\dots,s}^{d-1},q,\overbrace{s,\dots,s}^{d-1},q,\dots) &= k!\sum_{i=0}^{\lfloor\frac{k}{d}\rfloor}\binom{\frac{q-s}{d}+i-1}{\frac{q-s}{d}-1}\binom{s+k-di-1}{s-1} \\
&\leq k!\sum_{i=0}^{\lfloor\frac{k}{d}\rfloor}\binom{\frac{q-s}{d}+i-1}{\frac{q-s}{d}-1}\binom{s+k-i-1}{s-1} \\
&\leq k!\binom{s+k+\frac{q-s}{d}-1}{k} = \left(s+k+\frac{q-s}{d}-1\right)_k.
\end{aligned}$$

2.3 Gauss sums and Jacobi sums

In this subsection, we review and prove some basic properties of Gauss-Jacobi sums that are needed in our proof.

Definition 2.6. A multiplicative character on $\mathbb{F}_q^*$ is a map χ from $\mathbb{F}_q^*$ to the nonzero complex numbers $\mathbb{C}^*$ that satisfies $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_q^*$. We extend the definition to the whole field $\mathbb{F}_q$ by defining

$$\chi(0) = \begin{cases} 1, & \chi = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Definition 2.7. Let χ be a multiplicative character on $\mathbb{F}_q$ and $a \in \mathbb{F}_q$. Set

$$g_a(\chi) = \sum_{t\in\mathbb{F}_q}\chi(t)\zeta^{\mathrm{Tr}(at)},$$

where $\zeta = e^{2\pi i/p}$ and Tr denotes the trace map from $\mathbb{F}_q$ to $\mathbb{F}_p$. The sum $g_a(\chi)$ is called a Gauss sum on $\mathbb{F}_q$ and we often denote $g_1(\chi)$ by $g(\chi)$.

Proposition 2.8. *If $\chi \neq 1$, then $|g(\chi)| = \sqrt{q}$.*

It's proof can be seen in [3] when $q = p$, where p is a prime. For $q = p^r$, the proof is similar.

Definition 2.9. Let $\chi_1, \dots, \chi_n$ be multiplicative characters on $\mathbb{F}_q$. We define the following four Jacobi type sums by

$$J(\chi_1,\dots,\chi_n) = \sum_{y_1+\cdots+y_n=1}\chi_1(y_1)\chi_2(y_2)\dots\chi_n(y_n).$$

$$J_0(\chi_1,\dots,\chi_n) = \sum_{y_1+\cdots+y_n=0}\chi_1(y_1)\chi_2(y_2)\dots\chi_n(y_n).$$

$$J^*(\chi_1,\dots,\chi_n) = \sum_{\substack{y_1+\cdots+y_n=1\\ \text{all } y_i\neq 0}} \chi_1(y_1)\chi_2(y_2)\dots\chi_n(y_n).$$

$$J_0^*(\chi_1,\dots,\chi_n) = \sum_{\substack{y_1+\cdots+y_n=0\\ \text{all } y_i\neq 0}} \chi_1(y_1)\chi_2(y_2)\dots\chi_n(y_n).$$

The first two sums are standard Jacobi sums. The last two sums are related to the first two sums. These Jacobi type sums have the following properties:

Proposition 2.10. *Let $\chi_{i_1} = \cdots = \chi_{i_e} = 1$ but $\chi_{i_{e+1}} \neq 1, \dots, \chi_{i_n} \neq 1$. Then,*

$$J(\chi_1,\chi_2,\dots,\chi_n) = \begin{cases} q^{n-1}, & \text{if } e=n,\\ 0, & \text{if } 1\le e<n.\end{cases}$$

$$J_0(\chi_1,\chi_2,\dots,\chi_n) = \begin{cases} q^{n-1}, & \text{if } e=n,\\ 0, & \text{if } 1\le e<n,\\ 0, & \text{if } e=0,\ \chi_1\chi_2\dots\chi_n\neq 1,\\ \chi_n(-1)(q-1)J(\chi_1,\chi_2,\dots,\chi_{n-1}) & \text{otherwise.}\end{cases}$$

$$J^*(\chi_1,\chi_2,\dots,\chi_n) = \begin{cases} \frac{1}{q}[(q-1)^n-(-1)^n], & \text{if } e=n,\\ (-1)^e J(\chi_{i_{e+1}},\chi_{i_{e+2}},\dots,\chi_{i_n}), & \text{if } 0\le e<n.\end{cases}$$

$$J_0^*(\chi_1,\chi_2,\dots,\chi_n) = \begin{cases} \frac{1}{q}[(q-1)^n-(q-1)(-1)^{n-1}], & \text{if } e=n,\\ (-1)^e J_0(\chi_{i_{e+1}},\chi_{i_{e+2}},\dots,\chi_{i_n}), & \text{if } 0\le e<n.\end{cases}$$

Proof. If $y_1,y_2,\dots,y_{n-1}$ are chosen arbitrarily in $\mathbb{F}_q$, then y_n is uniquely determined by the condition $y_1+y_2+\cdots+y_n=0$. Thus $J_0(1,1,\dots,1) = J(1,1,\dots,1) = q^{n-1}$. An application of the inclusion-exclusion principle gives

$$\begin{aligned} J^*(1,1,\dots,1) &= \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0}} 1\\ &= q^{n-1} - \binom{n}{1}q^{n-2} + (-1)^2\binom{n}{2}q^{n-3} + \cdots + (-1)^{n-1}\binom{n}{n-1}q^0\\ &= \frac{1}{q}[(q-1)^n-(-1)^n]. \end{aligned}$$

Similarly,

$$\begin{aligned} J_0^*(1,1,\dots,1) &= \sum_{\substack{y_1+\cdots+y_n=0\\ y_i\neq 0}} 1\\ &= \sum_{s\in\mathbb{F}_q^*}\ \sum_{\substack{y_1+\cdots+y_{n-1}=-s\\ y_i\neq 0}} 1\\ &= (q-1)J^*(\chi_1,\dots,\chi_{n-1})\\ &= \frac{1}{q}[(q-1)^n-(q-1)(-1)^{n-1}]. \end{aligned}$$

If $e = 0$, then none of the χ_i is trivial and thus $\chi_i(0) = 0$. We obtain

$$\sum_{y_1+\cdots+y_n=1} \chi_1(y_1)\chi_2(y_2)\ldots\chi_n(y_n) = \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0}} \chi_1(y_1)\chi_2(y_2)\ldots\chi_n(y_n),$$

as the term $\chi_1(y_1)\chi_2(y_2)\ldots\chi_n(y_n)$ yields 0 if there is some $y_i = 0$. Hence, we complete the proof of $J^*(\chi_1, \chi_2, \ldots, \chi_n) = J(\chi_1, \chi_2, \ldots, \chi_n)$. The proof of $J_0^*(\chi_1, \chi_2, \ldots, \chi_n) = J_0(\chi_1, \chi_2, \ldots, \chi_n)$ is similar.

If $1 \leq e < n$, without loss of generality, we may assume that $\chi_1, \chi_2, \ldots, \chi_e$ are trivial and the rest are nontrivial. Then

$$\begin{aligned}
&\sum_{y_1+\cdots+y_n=0} \chi_1(y_1)\chi_2(y_2)\ldots\chi_n(y_n)\\
&= q^{e-1} \sum_{y_{e+1},y_{e+2},\ldots,y_n} \chi_{e+1}(y_{e+1})\chi_{e+2}(y_{e+2}),\ldots,\chi_n(y_n)\\
&= q^{e-1} \sum_{y_{e+1}} \chi_{e+1}(y_{e+1}) \sum_{y_{e+2}} \chi_{e+2}(y_{e+2}) \cdots \sum_{y_n} \chi_n(y_n) = 0.
\end{aligned}$$

Thus $J_0(\chi_1, \chi_2, \ldots, \chi_n) = 0$, and similarly for $J(\chi_1, \chi_2, \ldots, \chi_n)$. For J^* Jacobi sum, we can apply the inclusion-exclusion principle and deduce

$$\begin{aligned}
J^*(\chi_1, \chi_2, \ldots, \chi_n) &= \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0, 1\leq i\leq n}} \chi_{e+1}(y_{e+1})\ldots\chi_n(y_n)\\
&= \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0, 1\leq i\leq e}} \chi_{e+1}(y_{e+1})\ldots\chi_n(y_n)\\
&= \sum_{y_1+\cdots+y_n=1} \chi_{e+1}(y_{e+1})\ldots\chi_n(y_n) - \sum_{y_2+\cdots+y_n=1} \chi_{e+1}(y_{e+1})\ldots\chi_n(y_n)\\
&+ \cdots + (-1)^e \sum_{y_{e+1}+\cdots+y_n=1} \chi_{e+1}(y_{e+1})\ldots\chi_n(y_n)\\
&= J(1, \ldots, 1, \chi_{e+1}, \ldots, \chi_n) + \cdots + (-1)^e J(\chi_{e+1}, \ldots, \chi_n)\\
&= (-1)^e J(\chi_{e+1}, \ldots, \chi_n).
\end{aligned}$$

The proof for $J_0^*(\chi_1, \chi_2, \ldots, \chi_n)$ is similar.

Finally, if $e = 0$, then

$$J_0(\chi_1, \chi_2, \ldots, \chi_n) = \sum_s \sum_{y_1+y_2+\cdots+y_{n-1}=-s} \chi_1(y_1)\chi_2(y_2)\ldots\chi_{n-1}(y_{n-1})\chi_n(s)$$

We can assume $s \neq 0$ in the above sum and define $y_i' = -y_i/s$. Then

$$\begin{aligned}
&\sum_{y_1+\cdots+y_{n-1}=-s} \chi_1(y_1)\chi_2(y_2)\ldots\chi_{n-1}(y_{n-1})\\
&= \chi_1\chi_2\ldots\chi_{n-1}(-s) \sum_{y_1'+y_2'+\cdots+y_{n-1}'=1} \chi_1(y_1')\chi_2(y_2')\ldots\chi_{n-1}(y_{n-1}')\\
&= \chi_1\chi_2\ldots\chi_{n-1}(-s) J(\chi_1, \chi_2, \ldots, \chi_{n-1}).
\end{aligned}$$

Combining these results, we have

$$J_0(\chi_1,\chi_2,\dots,\chi_n)=\chi_1\chi_2\dots\chi_{n-1}(-1)J(\chi_1,\chi_2,\dots,\chi_{n-1})\sum_{s\neq 0}\chi_1\chi_2\dots\chi_n(s).$$

The last sum is 0 if $\chi_1\chi_2\dots\chi_n\neq 1$ and $q-1$ if $\chi_1\chi_2\dots\chi_n=1$. The proposition is proved.

Proposition 2.11. *If $\chi_1,\chi_2,\dots,\chi_n$ are nontrivial and $\chi_1\chi_2\dots\chi_n\neq 1$, we have*

$$g(\chi_1)g(\chi_2)\dots g(\chi_n)=J(\chi_1,\chi_2,\dots,\chi_n)g(\chi_1\chi_2\dots\chi_n).$$

Corollary 2.12. *If $\chi_1,\chi_2,\dots,\chi_n$ are nontrivial and $\chi_1\chi_2\dots\chi_n=1$, then*

(1)

$$g(\chi_1)g(\chi_2)\dots g(\chi_n)=\chi_n(-1)qJ(\chi_1,\chi_2,\dots,\chi_{n-1}).$$

(2)

$$J(\chi_1,\chi_2,\dots,\chi_n)=-\chi_n(-1)J(\chi_1,\chi_2,\dots,\chi_{n-1}).$$

Proof. The proofs of Proposition and corollary above 2.11 can also be seen in [3] when $q=p$, and when $q=p^r$, the proofs are similar.

Proposition 2.13. *Assume that $\chi_1,\chi_2,\dots,\chi_n$ are nontrivial.*

(1) If $\chi_1\chi_2\dots\chi_n\neq 1$, then

$$|J(\chi_1,\chi_2,\dots,\chi_n)|=q^{(n-1)/2}.$$

(2) If $\chi_1\chi_2\dots\chi_n=1$, then

$$|J_0(\chi_1,\chi_2,\dots,\chi_n)|=(q-1)q^{(n/2)-1}.$$

and

$$|J(\chi_1,\chi_2,\dots,\chi_n)|=q^{(n/2)-1}.$$

As a corollary, if all the χ_i are nontrivial, we have

$$|J(\chi_1,\chi_2,\dots,\chi_n)|\leq q^{(n-1)/2}. \tag{2.2}$$

Proof. Their proofs are directly from Proposition 2.11, Proposition 2.8, Proposition 2.10 and Corollary 2.12.

3 Solutions with distinct coordinates

Recall that $M_H(k,b)$ denotes the number of k-element subsets $S\subseteq H$ such that $\sum_{a\in S}a=b$. Namely, $M_H(k,b)$ is the number of unordered k-tuples $(x_1,x_2,\dots,x_k)$ with distinct $x_i\in H$ such that

$$x_1+x_2+\cdots+x_k=b. \tag{3.1}$$

If we denote $N_H(k,b)$ be the number of ordered k-tuples with distinct coordinates satisfying the equation above, it's clear that $N_H(k,b) = k!M_H(k,b)$.

Note that $H = \{y^m | y \in \mathbb{F}_q^*\}$. If $(x_1, x_2, \ldots, x_k)$ is a k-tuple satisfying the equation above, then there exist some $y_i \in \mathbb{F}_q^*$ such that $x_i = y_i^m, 1 \leq i \leq k$, and $(y_1, y_2, \ldots, y_k)$ is a k-tuple satisfying the following equation

$$y_1^m + y_2^m + \cdots + y_k^m = b. \tag{3.2}$$

Let $N_m^*(k,b)$ be the number of ordered k-tuples $(y_1, y_2, \ldots, y_k)$ with distinct $y_i \in \mathbb{F}_q^*$ satisfying equation (3.2).

Remark 3.1. The number of solutions with distinct coordinates in H for equation (3.1) (i.e.$N_H(k,b)$) is not equal to the number of solutions with distinct coordinates in $\mathbb{F}_q^*$ for equation (3.2)(i.e.$N_m^*(k,b)$). However there exists a delicate relationship between them, which will be described in details later.

3.1 Estimate for $N_m^*(k,b)$ with $b \neq 0$

As defined above,

$$N_m^*(k,b) = \#\{(x_1, x_2, \ldots, x_k) \in (\mathbb{F}_q^*)^k | x_1^m + x_2^m + \cdots + x_k^m = b, \quad x_i \text{ distinct for } 1 \leq i \leq k\}.$$

For a positive integer d and element $a \in \mathbb{F}_q$, we shall use the following well known relation:

$$\#\{x \in \mathbb{F}_q | x^d = a\} = \sum_{\chi^d = 1} \chi(a),$$

where χ runs over all multiplicative characters of $\mathbb{F}_q$ of order dividing d.

In this subsection, we will estimate $N_m^*(k,b)$ for $b \in \mathbb{F}_q^*$.

Lemma 3.2. *Let $d_1, \cdots, d_n$ be positive integers. Define*

$$N^* = \#\{(x_1, \ldots, x_n) \in (\mathbb{F}_q^*)^n | a_1 x_1^{d_1} + \cdots + a_n x_n^{d_n} = b\},$$

where $b, a_i (1 \leq i \leq n)$ are in $\mathbb{F}_q^*$. Then, we have

$$\left| N^* - \frac{1}{q}[(q-1)^n - (-1)^n] \right| \leq \sum_{e=0}^{n-1} \sum_{1 \leq i_{e+1} < i_{e+2} < \cdots < i_n \leq n} \prod_{j=e+1}^{n} (d_{i_j} - 1) \sqrt{q}^{n-e-1}. \tag{3.3}$$

Proof. Without loss of generality, we can assume $b = 1$ and $d_i|(q-1)$.

$$\begin{aligned}
N^* &= \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0}} \prod_{i=1}^{n} \#\{a_i x_i^{d_i} = y_i\} = \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0}} \prod_{i=1}^{n} \sum_{\chi_i^{d_i}=1} \chi_i(\frac{y_i}{a_i}) \\
&= \sum_{\chi_1^{d_1}=\cdots=\chi_n^{d_n}=1} \prod_{i=1}^{n} \chi^{-1}(a_i) \sum_{\substack{y_1+\cdots+y_n=1\\ y_i\neq 0}} \chi_1(y_1)\cdots\chi_n(y_n) \\
&= \frac{1}{q}[(q-1)^n - (-1)^n] \\
&+ \sum_{e=0}^{n-1} \sum_{\substack{\chi_1^{d_1} = \cdots = \chi_n^{d_n} = 1\\ \chi_{i_1} = \cdots = \chi_{i_e} = 1\\ \chi_{i_{e+1}},\ldots,\chi_{i_n} \neq 1}} \prod_{i=1}^{n} \chi^{-1}(a_i) J^*(\chi_1,\ldots,\chi_n) \\
&= \frac{1}{q}[(q-1)^n - (-1)^n] \\
&+ \sum_{e=0}^{n-1} \sum_{\substack{\chi_1^{d_1} = \cdots = \chi_n^{d_n} = 1\\ \chi_{i_1} = \cdots = \chi_{i_e} = 1\\ \chi_{i_{e+1}},\ldots,\chi_{i_n} \neq 1}} \prod_{i=1}^{n} \chi^{-1}(a_i)(-1)^e J(\chi_{i_{e+1}},\ldots,\chi_{i_n}).
\end{aligned}$$

With Proposition 2.13, we have

$$\left| N^* - \frac{1}{q}[(q-1)^n - (-1)^n] \right| \leq \sum_{e=0}^{n-1} \sum_{1\leq i_{e+1}<i_{e+2}<\cdots<i_n\leq n} \prod_{j=e+1}^{n} (d_{i_j}-1)\sqrt{q}^{n-e-1}.$$

As a corollary, if $d_i = m$, for all $1 \leq i \leq k$, then

$$\begin{aligned}
\left| N^* - \frac{1}{q}[(q-1)^n - (-1)^n] \right| &\leq \sum_{e=0}^{n-1} \binom{n}{e} (m-1)^{n-e} \sqrt{q}^{n-e-1} && (3.4)\\
&< (1+(m-1)\sqrt{q})^n/\sqrt{q}. && (3.5)
\end{aligned}$$

Theorem 3.3. *For all $b \in \mathbb{F}_q^*$, we have*

$$\left| N_m^*(k,b) - \frac{(q-1)_k}{q} \right| < \frac{2}{\sqrt{q}} \left(m\sqrt{q} + k + \frac{q}{p} \right)_k.$$

Proof. Let $X^* = \{(x_1,\ldots,x_k) \in (\mathbb{F}_q^*)^k | x_1^m + \cdots + x_k^m = b\}$. As X^* is symmetric, we can apply

$$N_m^*(k,b) = \sum_{\sum ic_i = k} (-1)^{k-\sum c_i} N(c_1,\ldots,c_k)|X_\tau^*|,$$

where τ is of type $(c_1,\ldots,c_k)$, and $X_\tau^* = \{(x_{11},\ldots,x_{kc_k}) \in (\mathbb{F}_q^*)^{\sum c_i} | x_{11}^m + \cdots + x_{1c_1}^m + 2x_{21}^m + \cdots + 2x_{2c_2}^m + \cdots + kx_{k1}^m + \cdots + kx_{kc_k}^m = b\}$. In order to compute $N_m^*(k,b)$, we should compute $|X_\tau^*|$ first. Denote

$$\delta_i(p) = \begin{cases} 0, & p \nmid i; \\ 1, & p|i \end{cases}$$

and $n=\sum c_i(1-\delta_i(p))$. Then,

$$|X_\tau^*|=(q-1)^{\sum c_i\delta_i(p)}\#\{(\cdots,x_{it_i},\cdots)\in(\mathbb{F}_q^*)^n|\sum_{\substack{1\le i\le k;1\le t_i\le c_i,\\ p\nmid i}} ix_{it_i}^m=b\}.$$

Applying (3.4), we have

$$\begin{aligned}\left||X_\tau^*|-\frac{1}{q}(q-1)^{\sum c_i}\right| &\le (q-1)^{\sum c_i\delta_i(p)}+(q-1)^{\sum c_i\delta_i(p)}(1+(m-1)\sqrt{q})^{\sum c_i(1-\delta_i(p))}/\sqrt{q}\\ &< 2(q-1)^{\sum c_i\delta_i(p)}(1+(m-1)\sqrt{q})^{\sum c_i(1-\delta_i(p))}/\sqrt{q}.\end{aligned}$$

Then apply Theorem 2.2 and Corollary 2.5, we have

$$\begin{aligned}\left|N_m^*(k,b)-\frac{(q-1)_k}{q}\right| &< \frac{2}{\sqrt{q}}\left((m-1)\sqrt{q}+k+\frac{q-(m-1)\sqrt{q}}{p}\right)_k\\ &\le \frac{2}{\sqrt{q}}\left((m-1)\sqrt{q}+k+\frac{q-1}{p}\right)_k\\ &\le \frac{2}{\sqrt{q}}\left(m\sqrt{q}+k+\frac{q}{p}\right)_k.\end{aligned}$$

Theorem 3.4. *Let $p>2$. There is an effectively computable absolute constant $0<c<1$ such that if $m<c\sqrt{q}$ and $3\ln 4q<k\le\frac{q-1}{2}$ then $N_m^*(k,b)>0$ for all $b\in\mathbb{F}_q^*$.*

Proof. Replacing c by a smaller constant if necessary, we may assume that $m<c\sqrt{q-1}<\sqrt{q}$, then $(m-1)\sqrt{q}\le m\sqrt{q-1}$. By Theorem 3.3, it is sufficient to prove

$$\frac{(q-1)_k}{q}\ge\frac{2}{\sqrt{q}}\left(\frac{q-1}{p}+k+m\sqrt{q-1}\right)_k,$$

that is

$$\frac{(q-1)_k}{(\frac{q-1}{p}+k+m\sqrt{q-1})_k}\ge 2\sqrt{q}.$$

This holds obviously when the following inequality holds:

$$\frac{q-1}{\frac{q-1}{p}+k+m\sqrt{q-1}}\ge(4q)^{\frac{1}{2k}}.$$

Since $m<c\sqrt{q-1}$ and $k\le\frac{q-1}{2}$, it is sufficient to prove the following inequality holds:

$$\frac{q-1}{\frac{q-1}{p}+k+m\sqrt{q-1}}\ge\frac{1}{\frac{1}{p}+\frac{1}{2}+c}\ge(4q)^{\frac{1}{2k}}.$$

Now, $p\ge 3$ and thus $1/p+1/2\le 5/6$. It is sufficient to choose a positive constant c satisfying the inequality $c\le\frac{1}{(4q)^{\frac{1}{2k}}}-\frac{5}{6}$. This is possible if $(4q)^{\frac{1}{2k}}<e^{1/6}$, where e is the natural number. That is, if $k>3\ln 4q$. The proof is complete.

3.2 Estimate for $N_m^*(b,0)$

We now turn to the study of the number $N_m^*(k,b)$ when $b=0$.

Lemma 3.5. *Let $d_1,\cdots,d_n$ be positive integers. Let*

$$N_0^* = \#\{(x_1,\ldots,x_n)\in(\mathbb{F}_q^*)^n | a_1x_1^{d_1}+\cdots+a_nx_n^{d_n}=0\},$$

where $a_i\in\mathbb{F}_q^*$. Then,

$$\left|N_0^*-\frac{1}{q}(q-1)^n\right| \le \frac{q-1}{q}+\sum_{e=0}^{n-1}\sum_{\substack{\frac{l_{i_{e+1}}}{d_{i_{e+1}}}+\cdots+\frac{l_{i_n}}{d_{i_n}}\in\mathbb{Z}\\ 1\le l_{i_j}\le d_{i_j}-1}}(q-1)q^{\frac{n-e}{2}-1}. \tag{3.6}$$

Proof. Without loss of generality, we can assume $d_i|(q-1)$.

$$\begin{aligned}
N_0^* &= \sum_{\substack{y_1+\cdots+y_n=0\\ y_i\neq 0}}\prod_{i=1}^n \#\{a_ix_i^{d_i}=y_i\} = \sum_{\substack{y_1+\cdots+y_n=0\\ y_i\neq 0}}\prod_{i=1}^n\sum_{\chi_i^{d_i}=1}\chi_i(\frac{y_i}{a_i})\\
&= \sum_{\chi_1^{d_1}=\cdots=\chi_n^{d_n}=1}\prod_{i=1}^n\chi^{-1}(a_i)\sum_{\substack{y_1+\cdots+y_n=0\\ y_i\neq 0}}\chi_1(y_1)\cdots\chi_n(y_n)\\
&= \frac{1}{q}[(q-1)^n-(q-1)(-1)^{n-1}]\\
&+\sum_{e=0}^{n-1}\sum_{\substack{\chi_1^{d_1}=\cdots=\chi_n^{d_n}=1\\ \chi_{i_1}=\cdots=\chi_{i_e}=1\\ \chi_{i_{e+1}},\ldots,\chi_{i_n}\neq 1}}\prod_{i=1}^n\chi^{-1}(a_i)J_0^*(\chi_1,\ldots,\chi_n)\\
&= \frac{1}{q}[(q-1)^n-(q-1)(-1)^{n-1}]\\
&+\sum_{e=0}^{n-1}\sum_{\substack{\chi_1^{d_1}=\cdots=\chi_n^{d_n}=1\\ \chi_{i_1}=\cdots=\chi_{i_e}=1\\ \chi_{i_{e+1}},\ldots,\chi_{i_n}\neq 1\\ \chi_{i_{e+1}}\chi_{i_{e+2}}\cdots\chi_{i_n}=1}}\prod_{i=1}^n\chi^{-1}(a_i)(-1)^eJ_0(\chi_{i_{e+1}},\ldots,\chi_{i_n}).
\end{aligned}$$

By the estimation for the sums J_0 and J in Proposition 2.13, we have

$$\left|N_0^*-\frac{1}{q}(q-1)^n\right| \le \frac{q-1}{q}+\sum_{e=0}^{n-1}\sum_{\substack{\frac{l_{i_{e+1}}}{d_{i_{e+1}}}+\cdots+\frac{l_{i_n}}{d_{i_n}}\in\mathbb{Z}\\ 1\le l_{i_j}\le d_{i_j}-1\\ 1\le i_{e+1}<\cdots<i_n\le n}}(q-1)q^{\frac{n-e}{2}-1}.$$

In particular, when $d_i=m$ for all $1\le i\le n$, we have

$$\begin{aligned}
\left|N_0^*-\frac{1}{q}(q-1)^n\right| &\le \frac{q-1}{q}+\frac{q-1}{q}[\sum_{e=0}^{n-1}\binom{n}{e}(m-1)^{n-e}\sqrt{q}^{n-e}]\\
&= \frac{q-1}{q}(1+(m-1)\sqrt{q})^n \le (1+(m-1)\sqrt{q})^n.
\end{aligned}$$

Theorem 3.6. *We have*

$$\left|N_m^*(k,0)-\frac{(q-1)_k}{q}\right|\le\left(m\sqrt{q}+k+\frac{q}{p}\right)_k. \tag{3.7}$$

Proof. Let $X_0^*=\{(x_1,\dots,x_k)\in(\mathbb{F}_q^k)^*|x_1^m+\cdots+x_k^m=0\}$. As X is symmetric we can apply

$$N_m^*(k,0)=\sum_{\sum ic_i=k}(-1)^{k-\sum c_i}N(c_1,\dots,c_k)|X_{0\tau}^*|,$$

where τ is of type $(c_1,\dots,c_k)$, and $X_{0\tau}^*=\{(x_{11},\dots,x_{kc_k})\in(\mathbb{F}_q^*)^{\sum c_i}|x_{11}^m+\cdots+x_{1c_1}^m+2x_{21}^m+\cdots+2x_{2c_2}^m+\cdots+kx_{k1}^m+\cdots+kx_{kc_k}^m=0\}$. In order to compute $N_m^*(k,0)$, we need to compute $X_{0\tau}^*$ first. Let $\delta_i(p),n$ be defined the same way as before. We have

$$|X_{0\tau}^*|=(q-1)^{\sum c_i\delta_i(p)}\#\{(\cdots,x_{it_i},\cdots)\in(\mathbb{F}_q^*)^n|\sum_{\substack{1\le i\le k;1\le t_i\le c_i,\\ p\nmid i}}ix_{it_i}^m=0\}.$$

With the result of Lemma 3.5, we can conclude

$$\left||X_{0\tau}^*|-\frac{(q-1)^{\sum c_i}}{q}\right|\le(q-1)^{\sum c_i\delta_i(p)}(1+(m-1)\sqrt{q})^n.$$

Applying Theorem 2.2 and Corollary 2.5, we have

$$\begin{aligned}\left|N_m^*(k,0)-\frac{(q-1)_k}{q}\right|&\le\sum_{\sum_{ic_i=k}}N(c_1,c_2,\dots,c_k)(q-1)^{\sum c_i\delta_i(p)}(1+(m-1)\sqrt{q})^n\\&\le\left((m-1)\sqrt{q}+k+\frac{q-1}{p}\right)_k\\&\le\left(m\sqrt{q}+k+\frac{q}{p}\right)_k.\end{aligned}$$

Theorem 3.7. *Let* $p>2$. *There is an effectively computable absolute constant* $0<c<1$ *such that if* $m<c\sqrt{q}$ *and* $6\ln q<k\le\frac{q-1}{2}$ *then* $N_m^*(k,0)>0$.

Proof. The proof is similar to the proof of Theorem 3.4.

4 The subset sum problem

Suppose H is a subgroup of $\mathbb{F}_q^*$, so $H=\{x^m|x\in\mathbb{F}_q^*\}$, as $\mathbb{F}_q^*$ is a cyclic group. Our goal is to estimate $N_H(k,b)$ (and thus $M_H(k,b)$), which is the number of solutions with distinct coordinates in H of the following equation

$$x_1+x_2+\cdots+x_k=b.$$

Actually, let

$$\widetilde{X}=\{(x_1,x_2,\dots,x_k)\in H^k|x_1+x_2+\cdots+x_k=b\}.$$

Then

$$N_H(k,b) = \#\{(x_1, x_2, \ldots, x_k) \in \widetilde{X} | x_i \text{ distinct}\},$$

Obviously, $\widetilde{X}$ is symmetric. So we can apply Li-Wan's new sieve formula to compute $N_H(k,b)$.

4.1 Estimate for $N_H(k,b)$ with $b \neq 0$

Similar to the analysis above, we need to compute $\widetilde{X}_\tau$ first, where τ is a permutation of type $(c_1, c_2, \ldots, c_k)$ in S_k, and $\widetilde{X}_\tau = \{(x_{11}, \ldots, x_{1c_1}, \ldots, x_{kc_k}) \in H^{\sum c_i} | x_{11} + \cdots + x_{1c_1} + \cdots + kx_{kc_k} = b\}$. Note that $\sum ic_i = k$.

Theorem 4.1. *For any $b \in \mathbb{F}_q^*$, we have*

$$\left| N_H(k,b) - \frac{1}{q} \binom{\frac{q-1}{m}}{k} \right| \leq \frac{2}{\sqrt{q}} \left(\sqrt{q} + k + \frac{q}{mp} \right)_k.$$

Proof. As $H = \{x^m | x \in \mathbb{F}_q^*\}$, we can write $x_{it_i} = y_{it_i}^m$ for some $y_{it_i} \in \mathbb{F}_q^*$, where $1 \leq i \leq k, 1 \leq t_i \leq c_i$. So $\widetilde{X}_\tau$ equals the following

$$X_\tau^* = \{(y_{11}, \ldots, y_{1c_1}, \ldots, y_{kc_k}) \in (\mathbb{F}_q^*)^{\sum c_i} | y_{11}^m + \cdots + y_{1c_1}^m + \cdots + ky_{kc_k}^m = b\}.$$

Note that $y^m = (y')^m$ iff $y = y'\xi$, where ξ is an m-th root of unity. The number of variables in $\widetilde{X}_\tau$ is $\sum c_i$, so

$$|\widetilde{X}_\tau| = \frac{|X_\tau^*|}{m^{\sum c_i}},$$

where $|X_\tau^*|$ has been computed in section 3.1. Then $|\widetilde{X}_\tau|$ is given by

$$\frac{1}{m^{\sum c_i}} (q-1)^{\sum c_i \delta_i(p)} \#\{(\cdots, x_{it_i}, \cdots) \in (\mathbb{F}_q^*)^n | \sum_{\substack{1 \leq i \leq k \\ 1 \leq t_i \leq c_i, p \nmid i}} i x_{it_i}^m = 0\}.$$

Thus

$$\left| |\widetilde{X}_\tau| - \frac{1}{q} (\frac{q-1}{m})^{\sum c_i} \right| \leq \frac{2(q-1)^{\sum c_i \delta_i(p)} (1 + (m-1)\sqrt{q})^{\sum c_i (1 - \delta_i(p))}}{m^{\sum c_i} \sqrt{q}}.$$

As analyzed above, applying Theorem 2.2 and Corollary 2.5, we can conclude

$$\begin{aligned}
\left| N_H(k,b) - \frac{1}{q} \binom{\frac{q-1}{m}}{k} \right| &\leq \frac{2}{\sqrt{q}} \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k) \left(\frac{q-1}{m} \right)^{\sum c_i \delta_i(p)} \left(\frac{1 + (m-1)\sqrt{q}}{m} \right)^n \\
&\leq \frac{2}{\sqrt{q}} \left(\frac{(m-1)\sqrt{q} + 1}{m} + k - 1 + \frac{q-1}{mp} \right)_k \\
&\leq \frac{2}{\sqrt{q}} \left(\sqrt{q} + k + \frac{q}{mp} \right)_k.
\end{aligned}$$

As a corollary, we have

Corollary 4.2. *For $b \in \mathbb{F}_q^*$, we have*

$$\left|M_H(k,b) - \frac{1}{q}\binom{\frac{q-1}{m}}{k}\right| \le \frac{2}{\sqrt{q}}\binom{\sqrt{q}+k+\frac{q}{mp}}{k}.$$

Theorem 4.3. *Let $p > 2$. There is an effectively computable absolute constant $0 < c < 1$ such that if $m < c\sqrt{q}$ and $3\ln 4q < k \le \frac{q-1}{2m}$ then $M_H(k,b) > 0$ for all $b \in \mathbb{F}_q^*$.*

Proof. Replacing c by a smaller constant if necessary, we may assume that $\sqrt{q} \le c\frac{q-1}{m}$. By Corollary 4.2, it is sufficient to prove

$$\frac{1}{q}(\frac{q-1}{m})_k \ge 2((c+\frac{1}{2})\frac{q-1}{m} + \frac{q-1}{mp})_k/\sqrt{q}.$$

That is,

$$\frac{(\frac{q-1}{m})_k}{((c+\frac{1}{2})\frac{q-1}{m} + \frac{q-1}{mp})_k} \ge 2\sqrt{q}.$$

This holds obviously when the following inequality holds:

$$\frac{1}{c+\frac{1}{2}+\frac{1}{p}} \ge (4q)^{\frac{1}{2k}},$$

equivalently,

$$c \le \frac{1}{(4q)^{\frac{1}{2k}}} - (\frac{1}{p}+\frac{1}{2}).$$

Since $p \ge 3$, we have $1/p + 1/2 \le 5/6$. The existence of such a positive constant c is possible if $(4q)^{\frac{1}{2k}} \le e^{1/6}$, where e is the natural number. That is if $k > 3\ln 4q$. The proof is complete.

4.2 Estimate for $M_H(k,0)$

In the following, we discuss the case when $b = 0$.

Let

$$\widetilde{X_0} = \{(x_1, x_2, \dots, x_k) \in H^k | x_1 + x_2 + \cdots + x_k = 0\}.$$

Then

$$N_H(k,0) = \#\{(x_1, x_2, \dots, x_k) \in \widetilde{X_0} | x_i \text{ distinct}\}.$$

Obviously, $\widetilde{X_0}$ is symmetric. So we can apply the new sieve formula to compute $N_H(k,0)$. Similar to the analysis above, we need to compute $\widetilde{X}_{0\tau}$ first, where τ is a permutation of type $(c_1, c_2, \dots, c_k)$ in S_k, and $\widetilde{X}_{0\tau} = \{(x_{11}, \dots, x_{1c_1}, \dots, x_{kc_k}) \in H^{\sum c_i} | x_{11} + \cdots + x_{1c_1} + \cdots + kx_{kc_k} = 0\}$. Note that $\sum ic_i = k$.

Theorem 4.4.

$$\left|N_H(k,0) - \frac{1}{q}\left(\frac{q-1}{m}\right)_k\right| \le \left(\sqrt{q}+k+\frac{q}{mp}\right)_k.$$

Proof. As $H = \{x^m | x \in \mathbb{F}_q^*\}$, we can write $x_{it_i} = y_{it_i}^m$ for some $y_{it_i} \in \mathbb{F}_q^*$, where $1 \le i \le k, 1 \le t_i \le c_i$. So $\widetilde{X}_{0\tau}$ is related to

$$X_{0\tau}^* = \{(y_{11}, \dots, y_{1c_1}, \dots, y_{kc_k}) \in (\mathbb{F}_q^*)^{\sum c_i} | y_{11}^m + \cdots + y_{1c_1}^m + \cdots + k y_{kc_k}^m = 0\}$$

by the formula

$$|\widetilde{X}_{0\tau}| = \frac{|X_{0\tau}^*|}{m^{\sum c_i}},$$

where $|X_{0\tau}^*|$ has been computed in section 3.2. It follows that $|\widetilde{X}_{0\tau}|$ is given by

$$\frac{1}{m^{\sum c_i}} (q-1)^{\sum c_i \delta_i(p)} \#\{(\dots, x_{it_i}, \dots) \in (\mathbb{F}_q^*)^n | \sum_{\substack{1 \le i \le k \\ 1 \le t_i \le c_i, p \nmid i}} i x_{it_i}^m = 0\}.$$

Thus

$$\left| |\widetilde{X}_{0\tau}| - \frac{1}{q} (\frac{q-1}{m})^{\sum c_i} \right| \le \frac{(q-1)^{\sum c_i \delta_i(p)} (1 + (m-1)\sqrt{q})^{\sum c_i (1 - \delta_i(p))}}{m^{\sum c_i}}.$$

As analyzed above, applying Theorem 2.2 and Corollary 2.5, we can conclude

$$\begin{aligned} \left| N_H(k, 0) - \frac{1}{q} (\frac{q-1}{m})_k \right| &\le \sum_{\sum i c_i = k} N(c_1, c_2, \dots, c_k) \left(\frac{q-1}{m}\right)^{\sum c_i \delta_i(p)} \left(\frac{1 + (m-1)\sqrt{q}}{m}\right)^n \\ &\le \left(\frac{(m-1)\sqrt{q} + 1}{m} + k - 1 + \frac{q-1}{mp}\right)_k \\ &\le \left(\sqrt{q} + k + \frac{q}{mp}\right)_k. \end{aligned}$$

As a corollary, we have

Corollary 4.5.

$$\left| M_H(k, 0) - \frac{1}{q} \binom{\frac{q-1}{m}}{k} \right| \le \binom{\sqrt{q} + k - 1 + \frac{q}{mp}}{k}.$$

Theorem 4.6. *Let* $p > 2$. *There is an effectively computable absolute constant* $0 < c < 1$ *such that if* $m < c\sqrt{q}$ *and* $6 \ln q < k \le \frac{q-1}{2m}$, *then* $M_H(k, 0) > 0$.

Proof. The proof is similar to the proof of Theorem 4.3.

Acknowledgments. This work was done while the first author was visiting the University of California at Irvine with a graduate fellowship from Tsinghua University. She would like to thank both institutions for their hospitality and financial support.

References

[1] Q. Cheng and D. Wan, *On the list and bounded distance decodability of Reed-Solomon codes*, SIAM J. Comput. **37** (2007), no. 1, 195-209.

[2] T.H. Cormen, C.E. Leiserson, R.L. Rivest and C. Stein, *Introduction to Algorithms*, MIT Press and McGraw-Hill, 2001.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory.* GTM 84.

[4] J. Y. Li and D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl, 2008, 14, 911-929.

[5] J. Y. Li and D. Wan, *A new sieve for distinct coordinate counting*, SCIENCE CHINA Mathematics, 2010, Vol.53, No.9, 2351-2362.

[6] R. P. Stanley, *Enumerative Combinatorics*, Vol.1., Cambridge University Press, 1997.