Finite Fields and Their Applications 43 (2017) 106–122

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Subset sums of quadratic residues over finite fields ☆

Weiqiong Wang [a,b], Li-Ping Wang [c,*], Haiyan Zhou [d]

[a] *School of Mathematics, Northwest University, Xi'an 710127, China*
[b] *School of Science, Chan'an University, Xi'an 710064, China*
[c] *Data Assurance and Communications Security Research Center, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[d] *School of Mathematics, Nanjing Normal University, Nanjing 210023, China*

ARTICLE INFO

Article history:
Received 25 June 2016
Accepted 20 September 2016
Available online xxxx
Communicated by Gary L. Mullen

MSC:
05A15
11T24

Keywords:
Subset sums
Quadratic residue
Character sum
Distinct coordinate sieve

ABSTRACT

In this paper, we derive an explicit combinatorial formula for the number of k-subset sums of quadratic residues over finite fields.

☆ Research is supported in part by 973 Program (2013CB834203), National Natural Science Foundation of China under Grant No. 61202437 and 11471162, in part by Natural Science Basic Research Plan in Shaanxi Province of China under Grant No. 2015JM1022 and Natural Science Foundation of the Jiangsu Higher Education Institutes of China under Grant No. 13KJB110016.

* Corresponding author.

E-mail addresses: wqwang@chd.edu.cn (W. Wang), wangliping@iie.ac.cn (L.-P. Wang), haiyanxiaodong@gmail.com (H. Zhou).

http://dx.doi.org/10.1016/j.ffa.2016.09.003

1. Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^s$ elements, where p is a prime and $s \geq 1$ is an integer. Let H be a subset of $\mathbb{F}_q$, and k $(1 \leq k \leq |H|)$ be a positive integer. For $b \in \mathbb{F}_q$, let $N_H(k, b)$ denote the number of k-element subsets $S \subseteq H$ such that

$$\sum_{a \in S} a = b. \tag{1.1}$$

Understanding the number $N_H(k, b)$ is the well known k-subset sum problem over finite fields. It arises from several applications in coding theory, cryptography, graph theory and some other fields. For example, it is directly related to the deep hole problem of generalized Reed–Solomon codes with evaluation set H [1–4]. It is also related to the spectrum and the diameter of the Wenger type graphs [5].

However, the k-subset sum problem over finite fields for general H is well known to be NP-hard. The difficulty mainly comes from the combinatorial flexibility of choosing the subset H and also the lack of algebraic structure of H. Due to the NP-hardness, there is little that we can say about the exact value of $N_H(k, b)$ in general. But from mathematic point of view, we would like to obtain an explicit formula or at least an asymptotic formula for $N_H(k, b)$. This is again out of our expectation in general. But if H is certain special subset with good algebraic structure, one can hope to obtain the exact value or asymptotic formula for $N_H(k, b)$. For example, it is known that if $\mathbb{F}_q - H$ is a small set, there is a simple asymptotic formula for $N_H(k, b)$ [6]. In addition, if $H = \mathbb{F}_q$, or $\mathbb{F}_q^*$, or any additive subgroup of $\mathbb{F}_q$, there is also an explicit combinatorial formula for $N_H(k, b)$ [6–8].

If H is a multiplicative subgroup of $\mathbb{F}_q$ of index m (thus m divides $q-1$), the subset sum problem becomes harder as it is a non-linear algebraic problem with many combinatorial constraints. Zhu and Wan [9] provided an asymptotic formula for $N_H(k, b)$ in this case. As a consequence, they proved that for small index $m = [\mathbb{F}_q^* : H]$ and $6 \ln q < k < \frac{q-1}{2m}$, $N_H(k, b) > 0$ for all $b \in \mathbb{F}_q$. This is the only known result in the case when H is a proper multiplicative subgroup.

The complexity of the subset sum problem grows as the index m of the subgroup H grows. In the simplest case $m = 1$, then $H = \mathbb{F}_q^*$ and an explicit combinatorial formula for $N_H(k, b)$ is known. In this paper, we study the next simplest case $m = 2$. Our main result is an explicit combinatorial formula for $N_H(k, b)$, where H is the subgroup of quadratic residues in $\mathbb{F}_q^*$, that is, $H = \{x^2 \mid x \in \mathbb{F}_q^*\}$. Equivalently, we obtain an explicit combinatorial formula for

$$N_H(k, b) = \frac{1}{k!} \sharp\{(y_1, y_2, \cdots, y_k) \in H^k \mid y_1 + y_2 + \cdots + y_k = b, y_i \neq y_j \text{ for } \forall\, i \neq j\}. \tag{1.2}$$

Note that there is the coefficient $\frac{1}{k!}$ because $N_H(k, b)$ denotes the number of the unordered k-tuples with distinct coordinates satisfying the equation $y_1 + y_2 + \cdots + y_k = b$ with $y_i \in H$. When $m \geq 3$, one should not expect an explicit formula for $N_H(k, b)$.