

Partitions and compositions over finite fields

Muratović-Ribić

Department of Mathematics
University of Sarajevo
Zmaja od Bosne 33-35, 71000 Sarajevo, Bosnia and Herzegovina
amela@pmf.unsa.ba

Qiang Wang *

School of Mathematics and Statistics
Carleton University
Ottawa, K1S 5B6, Canada
wang@math.carleton.ca

Submitted: Aug 31, 2012; Accepted: Feb 3, 2013; Published: Feb 12, 2013
Mathematics Subject Classifications: 11B30, 05A15, 11T06

Abstract

In this paper we find an exact formula for the number of partitions of an element z into m parts over a finite field, i.e. we find the number of nonzero solutions of the equation $x_1 + x_2 + \cdots + x_m = z$ over a finite field when the order of terms does not matter. This is equivalent to counting the number of m -multi-subsets whose sum is z . When the order of the terms in a solution does matter, such a solution is called a composition of z . The number of compositions is useful in the study of zeta functions of toric hypersurfaces over finite fields. We also give an application in the study of polynomials of prescribed ranges over finite fields.

1 Introduction

Let n and m be positive integers. A *composition* of n is an ordered list of positive integers whose sum is n . A *m -composition* of n is an ordered list of m positive integers (m parts) whose sum is n . It is well known that there is a bijection between all m -compositions of n and $(m-1)$ -subsets of $[n-1] = \{1, 2, \dots, n-1\}$ and thus there are $\binom{n-1}{m-1}$ m -compositions of n and 2^{n-1} compositions of n . Similarly, a *weak composition* of n is an ordered list of non-negative integers whose sum is n and a *weak m -composition* of n is an ordered list of m non-negative parts whose sum is n . Using substitution of variables, we can easily

*Supported by NSERC of Canada.

obtain that the number of weak m -compositions of n (i.e., the number of non-negative integer solutions to $x_1 + x_2 + \cdots + x_m = n$) is equal to the number of m -compositions of $n + m$ (i.e., the number of positive integer solutions to $x_1 + x_2 + \cdots + x_m = n + m$), which is $\binom{n+m-1}{m-1} = \binom{n+m-1}{n}$. The combinatorial interpretation of $\binom{n+m-1}{m-1} = \binom{n+m-1}{n}$ is the number of ways in selecting n -multisets from a set M with m elements, which is sometimes called n -combinations of M with repetitions. Disregarding the order of the summands, we have the concepts of partitions of n into m parts, partitions of n into at most m parts, and so on. For more details we refer the reader to [9].

Let \mathbb{F}_q be a finite fields of $q = p^r$ elements. The subset problem over a subset $D \subseteq \mathbb{F}_q$ is to determine for a given $z \in \mathbb{F}_q$, if there is a nonempty subset $\{x_1, x_2, \dots, x_m\} \subseteq D$ such that $x_1 + x_2 + \cdots + x_m = z$. This subset sum problem is known to be *NP*-complete. In the study of the subset sum problem over finite fields, Li and Wan [4] estimated the number, $N(m, z, D) = \#\{\{x_1, x_2, \dots, x_m\} \subseteq D \mid x_1 + x_2 + \cdots + x_m = z\}$, of m -subsets of $D \subseteq \mathbb{F}_q$ whose sum is $z \in \mathbb{F}_q$. In particular, exact formulas are obtained in cases that $D = \mathbb{F}_q$ or \mathbb{F}_q^* or $\mathbb{F}_q \setminus \{0, 1\}$. Similarly, we are interested in the number $S(m, z, D) = \#\{(x_1, x_2, \dots, x_m) \in D \times D \times \cdots \times D \mid x_1 + x_2 + \cdots + x_m = z\}$, that is, the number of ordered m -tuples whose sum is z and each coordinate belongs to $D \subseteq \mathbb{F}_q$, as well as the number $M(m, z, D)$ which counts the number of m -multisets of $D \subseteq \mathbb{F}_q$ whose sum is $z \in \mathbb{F}_q$. In particular, when $D = \mathbb{F}_q$ or \mathbb{F}_q^* , this motivated us to introduce the following.

Definition 1. A *partition* of $z \in \mathbb{F}_q$ into m parts is a multiset of m nonzero elements in \mathbb{F}_q^* whose sum is z . The m nonzero elements are the parts of the partition. We denote by $M(m, z, \mathbb{F}_q^*)$ or $\tilde{P}_m(z)$ the number of partitions of z into m parts over \mathbb{F}_q . Similarly, we denote by $M(m, z, \mathbb{F}_q)$ or $\hat{P}_m(z)$ the number of partitions of z into at most m parts over \mathbb{F}_q and by $\tilde{P}(z)$ the total number of partitions of z over finite field \mathbb{F}_q .

We remark that $N(m, z, \mathbb{F}_q^*)$ is the number of partitions of an element z over finite field \mathbb{F}_q such that all summands are distinct, and $M(m, z, \mathbb{F}_q^*)$ is the number of partitions of an element z into m parts over finite field \mathbb{F}_q , dropping the restriction that all summands are distinct.

We also remark that in the study of polynomials of prescribed ranges over finite fields [5] there has arisen a need as well for counting the number $M(m, 0, \mathbb{F}_q)$ of partitions of 0 with at most m parts over finite field \mathbb{F}_q , which in turn leads us to answer a recent conjecture by Gács et al on polynomials of prescribed ranges over finite fields [3].

In this article we first obtain an exact formula for the number of partitions of an element $z \in \mathbb{F}_q$ into m parts over \mathbb{F}_q .

Theorem 1. Let m be a non-negative integer, \mathbb{F}_q be a finite field of $q = p^r$ elements with prime p , and $z \in \mathbb{F}_q$. The number of partitions of z into m parts over \mathbb{F}_q is given by

$$\tilde{P}_m(z) = \frac{1}{q} \binom{q+m-2}{m} + D_m(z),$$

where

$$D_m(z) = \begin{cases} 0, & \text{if } m \not\equiv 0 \pmod{p} \text{ and } m \not\equiv 1 \pmod{p}; \\ \frac{q-1}{q} \binom{q/p-1+j}{j}, & \text{if } m = jp, j \geq 0, \text{ and } z = 0; \\ -\frac{q-1}{q} \binom{q/p-1+j}{j}, & \text{if } m = jp + 1, j \geq 0, \text{ and } z = 0; \\ -\frac{1}{q} \binom{q/p-1+j}{j}, & \text{if } m = jp, j \geq 0, \text{ and } z \in \mathbb{F}_q^*; \\ \frac{1}{q} \binom{q/p-1+j}{j}, & \text{if } m = jp + 1, j \geq 0, \text{ and } z \in \mathbb{F}_q^*. \end{cases}$$

Similarly, we have the following definition of compositions over finite fields.

Definition 2. A *composition* of $z \in \mathbb{F}_q$ with m parts is a solution (x_1, x_2, \dots, x_m) to the equation

$$z = x_1 + x_2 + \dots + x_m, \quad (1)$$

with each $x_i \in \mathbb{F}_q^*$. Similarly, a *weak composition* of $z \in \mathbb{F}_q$ with m parts is a solution (x_1, x_2, \dots, x_m) to Equation (1) with each $x_i \in \mathbb{F}_q$. We denote the number of compositions of z having m parts by $S(m, z, \mathbb{F}_q^*)$ or $S_m(z)$. The number of weak compositions of z with m parts is denoted by $S(m, z, \mathbb{F}_q)$. The total number of compositions of z over \mathbb{F}_q is denoted by $S(z)$.

A formula for the number of compositions over \mathbb{F}_p can be found on page 295 in [1]. A general formula for $S_m(z)$ over \mathbb{F}_q for arbitrary q and nonzero z can be obtained using a remark on the normalized Jacobi sum of the trivial character given in [2] (see Remark 1 on page 144). In fact, the numbers $S_m(1)$ are the simplest example of the number of rational points on an affine toric variety over a finite field (namely a toric hyperplane); see for example [6], [7], and [8]. In order to compare with the formula for partitions, we only present a recurrence formula for compositions as follows.

Proposition 1. Let $m > 2$, \mathbb{F}_q be a finite field of $q = p^r$ elements with prime p , and $z \in \mathbb{F}_q$. The number of compositions of z with m parts over \mathbb{F}_q is given by

$$S_m(z) = (q-1)^{m-2}(q-2) + S_{m-2}(z).$$

It follows that

$$S_m(0) = \frac{(q-1)^m + (-1)^m(q-1)}{q}$$

and

$$S_m(z) = \frac{(q-1)^m - (-1)^m}{q}, \quad \text{if } z \neq 0.$$

Using the fact that additive group $(\mathbb{F}_q, +)$ is isomorphic to the additive group $(\mathbb{F}_p^r, +)$, we obtain that the numbers of partitions and compositions of elements over \mathbb{F}_p^r are the same as the numbers of partitions and compositions of corresponding elements over \mathbb{F}_q .

Finally, we demonstrate an application of Theorem 1 in the study of polynomials of prescribed range. First let us recall that the *range* of the polynomial $f(x) \in \mathbb{F}_q[x]$ is a multiset M of size q such that $M = \{f(x) : x \in \mathbb{F}_q\}$ as a multiset (that is, not only values, but also multiplicities need to be the same). Here and also in the following sections we

abuse the set notation for multisets as well. In [3], there is a nice connection between polynomials with prescribed ranges and hyperplanes in vector spaces over finite fields. We refer the reader to this paper for more details. In this paper, we obtain the following result as an application of Theorem 1.

Theorem 2. Let \mathbb{F}_q be a finite field of $q = p^r$ elements. For every ℓ with $\frac{q}{2} \leq \ell < q - 3$ there exists a multiset M with $\sum_{b \in M} b = 0$ and the highest multiplicity ℓ achieved at $0 \in M$ such that every polynomial over the finite field \mathbb{F}_q with the prescribed range M has degree greater than ℓ .

We note that Theorem 2 generalizes Theorem 1 in [5] which disproves Conjecture 5.1 in [3]. In the following sections, we give the proofs of Theorems 1-2 respectively.

2 Proof of Theorem 1

In this section we prove Theorem 1. First of all we prove a few technical lemmas.

Lemma 1. Let $a \in \mathbb{F}_q^*$ and m be a positive integer. Then $\tilde{P}_m(a) = \tilde{P}_m(1)$.

Proof. Let $x_1 + x_2 + \dots + x_m = 1$. The following mapping between two multisets defined by

$$\{x_1, x_2, \dots, x_m\} \mapsto \{ax_1, ax_2, \dots, ax_m\}$$

for some $a \in \mathbb{F}_q^*$ is one-to-one and onto, which results in $ax_1 + ax_2 + \dots + ax_m = a$. Thus $\tilde{P}_m(a) = \tilde{P}_m(1)$. \square

It is obvious to see that $\tilde{P}_1(z) = 1$ if $z \in \mathbb{F}_q^*$ and $\tilde{P}_1(0) = 0$. However, we can show that $\tilde{P}_m(0) = \tilde{P}_m(z)$ if $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$ as follows.

Lemma 2. Let m be any positive integer satisfying $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$. Then $\tilde{P}_m(0) = \tilde{P}_m(1)$.

Proof. Let $x_1 + x_2 + \dots + x_m = 0$ be a partition of 0 into m parts. Then $(x_1 + 1) + (x_2 + 1) + \dots + (x_m + 1) = m$ is a partition of $m \in \mathbb{F}_q^*$ with at most m parts (if $x_j = p - 1$ then $x_j + 1 = 0$), but since $x_j \neq 0$ there is no $x_j + 1 = 1$. Moreover, there is a bijective correspondence of multisets $\{x_1, \dots, x_m\} \mapsto \{x_1 + 1, \dots, x_m + 1\}$. Therefore, in order to find the number $\tilde{P}_m(0)$ of partitions of 0 into m parts over \mathbb{F}_q , we need to find the number of partitions of m with at most m parts but no element is equal to 1. This means these partitions of m can have parts equal to the zero.

Let $x_1 + x_2 + \dots + x_m = m$. We assume that the parts equal to 1 (if any) appear in the beginning of the list: x_1, x_2, \dots, x_m . If $x_1 = 1$ then $x_1 + x_2 + \dots + x_m = m$ implies $x_2 + \dots + x_m = m - 1$. Conversely, each partition of m into $m - 1$ parts can generate a partition of m into m parts with the first part equal to 1. So the number of partitions of m into m parts with at least one part equal to 1 is equal to the number of partitions of $m - 1$ into $m - 1$ parts. Let U_0 be the family of partitions of m into m parts without zero elements and no part is equal to 1. Therefore $|U_0| = \tilde{P}_m(m) - \tilde{P}_{m-1}(m - 1)$.

Let U_1 be the family of partitions of m with m parts with exactly one element equal to 0 and no element equal to 1. Let $x_1 + x_2 + \cdots + x_m = m$ be a partition in U_1 and $x_1 = 0$ and $x_j \neq 0, 1$ for $j = 2, \dots, m$. Obviously, it is equivalent to a partition $x_2 + \cdots + x_m = m$ of m into $m - 1$ parts with all parts not equal to 1. Similarly as in the case for U_0 we have $|U_1| = \tilde{P}_{m-1}(m) - \tilde{P}_{m-2}(m - 1)$.

More generally, let U_i be the family of partitions with m parts with i parts equal to the zero, say $x_1 = x_2 = \dots = x_i = 0$, and $x_j \neq 0, 1$ for $j = i + 1, \dots, m$. Then we have a partition of m into $m - i$ parts, $x_{i+1} + \cdots + x_m = m$, such that no part is equal to 1. Similarly, we have $|U_i| = \tilde{P}_{m-i}(m) - \tilde{P}_{m-i-1}(m - 1)$. In particular, for $i = m - 1$ there is only one solution of the equation $x_m = m$ and thus $|U_{m-1}| = \tilde{P}_1(m) = 1$.

We note that these families of U_i 's are pairwise disjoint and their union is the family of partitions of m into m parts with no part equal to 1. Therefore we have $\tilde{P}_m(0) = |U_0| + |U_1| + \cdots + |U_{m-1}| = (\tilde{P}_m(m) - \tilde{P}_{m-1}(m - 1)) + (\tilde{P}_{m-1}(m) - \tilde{P}_{m-2}(m - 1)) + \cdots + (\tilde{P}_2(m) - \tilde{P}_1(m - 1)) + \tilde{P}_1(m)$.

If $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$, then $m - 1$ and m are both nonzero elements in \mathbb{F}_q . By Lemma 1, we can cancel $\tilde{P}_i(m - 1) = \tilde{P}_i(m)$ for $i = 1, \dots, m - 1$. Hence $\tilde{P}_m(0) = \tilde{P}_m(m) = \tilde{P}_m(1)$. \square

Using the above two lemmas, we obtain the exact counts of $\tilde{P}_m(z)$ when $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$.

Lemma 3. If $z \in \mathbb{F}_q$ and m is any positive integer satisfying $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$ then we have

$$\tilde{P}_m(z) = \frac{1}{q} \binom{q + m - 2}{m}.$$

Proof. We note that there are $\binom{(q-1)+m-1}{m}$ multisets of m nonzero elements from \mathbb{F}_q in total and the sum of elements in each multiset can be any element in \mathbb{F}_q . Using Lemmas 1 and 2 we have

$$\sum_{s \in \mathbb{F}_q} \tilde{P}_m(s) = q \tilde{P}_m(1) = \binom{(q-1) + m - 1}{m}$$

and therefore

$$\tilde{P}_m(z) = \tilde{P}_m(1) = \frac{1}{q} \binom{q + m - 2}{m}$$

for every $z \in \mathbb{F}_q$. \square

In order to consider other cases, we use an interesting result by Li and Wan [4], which gives the number $N(k, b, \mathbb{F}_q^*)$ of sets with (all distinct) k nonzero elements that sums to $b \in \mathbb{F}_q$. Namely,

$$N(k, b, \mathbb{F}_q^*) = \frac{1}{q} \binom{q-1}{k} + (-1)^{k+[k/p]} \frac{\nu(b)}{q} \binom{q/p-1}{[k/p]}, \quad (2)$$

where $\nu(b) = -1$ if $b \neq 0$ and $\nu(b) = q - 1$ if $b = 0$ (see Theorem 1.2 in [4]).

First we can prove

Lemma 4. Let $N(k, b, \mathbb{F}_q^*)$ be the number of sets with k nonzero elements that sums to $b \in \mathbb{F}_q$ and $m > 1$ be a positive integer. Then

$$\begin{aligned} \tilde{P}_m(0) &= \left((q-1)N(1, 1, \mathbb{F}_q^*)\tilde{P}_{m-1}(1) + N(1, 0, \mathbb{F}_q^*)\tilde{P}_{m-1}(0) \right) \\ &\quad - \left((q-1)N(2, 1, \mathbb{F}_q^*)\tilde{P}_{m-2}(1) + N(2, 0, \mathbb{F}_q^*)\tilde{P}_{m-2}(0) \right) \\ &\quad + \dots \\ &\quad + (-1)^{m-1} \left((q-1)N(m-2, 1, \mathbb{F}_q^*)\tilde{P}_2(1) + N(m-2, 0, \mathbb{F}_q^*)\tilde{P}_2(0) \right) \\ &\quad + (-1)^m (q-1)N(m-1, 1, \mathbb{F}_q^*) + (-1)^{m+1}N(m, 0, \mathbb{F}_q^*). \end{aligned}$$

Proof. Denote by \mathcal{U} the family of all multisets of m nonzero elements that sums to zero, i.e. $\tilde{P}_m(0) = |\mathcal{U}|$. Let \mathcal{B}_a be the family of all multisets of m nonzero elements such that a is a member of each multiset and the sum of elements of each multiset is equal to 0. Namely, $B_a \in \mathcal{B}_a$ implies $\sum_{s \in B_a} s = 0$ and $a \in B_a$. Obviously, $\mathcal{U} = \bigcup_{a \in \mathbb{F}_q^*} \mathcal{B}_a$.

Now we will use the principle of inclusion-exclusion to find the cardinality of \mathcal{U} . For distinct $a_1, \dots, a_k \in \mathbb{F}_q^*$ and $k > m$, it is easy to see that

$$\mathcal{B}_{a_1} \cap \mathcal{B}_{a_2} \cap \dots \cap \mathcal{B}_{a_k} = \emptyset,$$

because each multiset B_{a_1} contains only m nonzero elements. Moreover, if $k = m$ then the number of multisets in the union of intersections is $N(m, 0, \mathbb{F}_q^*)$.

If $B \in \mathcal{B}_{a_1} \cap \mathcal{B}_{a_2} \cap \dots \cap \mathcal{B}_{a_k}$ and $k \leq m-1$ then

$$B = \{a_1, a_2, \dots, a_k, x_{k+1}, \dots, x_m\}.$$

Because $x_{k+1} + \dots + x_m = -(a_1 + \dots + a_k)$, the number of elements in the intersection $\mathcal{B}_{a_1} \cap \mathcal{B}_{a_2} \cap \dots \cap \mathcal{B}_{a_k}$ is the same as the number of partitions of $-(a_1 + \dots + a_k)$ into $m-k$ parts, i.e.

$$|\mathcal{B}_{a_1} \cap \mathcal{B}_{a_2} \cap \dots \cap \mathcal{B}_{a_k}| = \tilde{P}_{m-k}(-a_1 - \dots - a_k).$$

We note that none of a_i 's ($i = 1, \dots, k$) is equal to zero and $N(k, b, \mathbb{F}_q^*) = N(k, 1, \mathbb{F}_q^*)$ for any $b \in \mathbb{F}_q^*$. In particular, if $k < m-1$, then the sum $a_1 + \dots + a_{m-1}$ can be any element in \mathbb{F}_q and thus there are $(q-1)N(k, 1, \mathbb{F}_q^*)\tilde{P}_{m-k}(1) + N(k, 0, \mathbb{F}_q^*)\tilde{P}_{m-k}(0)$ such multisets $B \in \mathcal{B}_{a_1} \cap \mathcal{B}_{a_2} \cap \dots \cap \mathcal{B}_{a_k}$ for all choices of nonzero distinct a_1, \dots, a_k .

If $k = m-1$ then the sum $a_1 + \dots + a_{m-1}$ can not be equal to the zero, there are in total $(q-1)N(m-1, 1, \mathbb{F}_q^*)$ such multisets contained in the intersection of $m-1$ families of \mathcal{B}_{a_i} 's.

Finally we combine the above cases and use the principle of inclusion-exclusion to complete the proof. \square

In the sequel we also need the following identity which is a special instance of Chu-Vandermonde identity.

Lemma 5. For all positive integers s , we have

$$\sum_{j=1}^s (-1)^{j+1} \binom{q-1}{j} \binom{q-2+s-j}{s-j} = \binom{q-2+s}{s}$$

Proof. The result follows from Chu-Vandermonde theorem ${}_2F_1(-s; -(q-1); -(q-2+s); 1) = 0$. Here we also include a direct proof. Multiplying $(1+x)^{q-1} = \sum_{k=0}^{q-1} \binom{q-1}{k} x^k$ and series

$$\frac{1}{(1+x)^{q-1}} = \sum_{k=0}^{\infty} \binom{q-2+k}{k} (-1)^k x^k,$$

We obtain

$$\begin{aligned} 1 &= (1+x)^{q-1} \cdot \frac{1}{(1+x)^{q-1}} = \left(\sum_{k=0}^{q-1} \binom{q-1}{k} x^k \right) \left(\sum_{k=0}^{\infty} \binom{q-2+k}{k} (-1)^k x^k \right) = \\ & \sum_{s=0}^{\infty} \left(\sum_{j=0}^s (-1)^{s-j} \binom{q-1}{j} \binom{q-2+s-j}{s-j} \right) x^s. \end{aligned}$$

Therefore for $s \geq 1$ we have $\sum_{j=0}^s (-1)^{s-j} \binom{q-1}{j} \binom{q-2+s-j}{s-j} = 0$. This implies

$$\sum_{j=1}^s (-1)^{s-j+1} \binom{q-1}{j} \binom{q-2+s-j}{s-j} = (-1)^s \binom{q-2+s}{s}.$$

Finally multiplying both sides of the last equality by $(-1)^s$ we complete the proof. \square

Next we prove Theorem 1. In order to do so, we let

$$\tilde{P}_m(z) = \frac{1}{q} \binom{q-2+m}{m} + D_m(z). \quad (3)$$

Without loss of generality, we can assume $q > 2$. Obviously, by Lemma 3, we have $D_m(z) = 0$ for any $z \in \mathbb{F}_q$ if $m \not\equiv 0 \pmod{p}$ and $m \not\equiv 1 \pmod{p}$. Further $D_m(z) = D_m(1)$ by Lemma 1 for all $z \neq 0$. Because $\tilde{P}_m(0) + (q-1)\tilde{P}_m(1) = \binom{q-2+m}{m}$, we have

$$D_m(0) + (q-1)D_m(1) = 0, \text{ i.e., } D_m(1) = -\frac{1}{q-1}D_m(0). \quad (4)$$

Next we use the convention that $\tilde{P}_0(0) = 1$ and $\tilde{P}_0(1) = 0$ so that $D_0(0) = \frac{q-1}{q}$ and $D_0(1) = -\frac{1}{q}$. Similarly, $\tilde{P}_1(0) = 0$ and $\tilde{P}_1(1) = 1$ and thus $D_1(0) = -\frac{q-1}{q}$ and $D_1(1) = \frac{1}{q}$. For the rest of this section, we only need to compute $D_m(0)$ when $m = jp$ or $m = jp + 1$ for some positive integer j because of Equation (4). To do this, we apply Lemmas 4 and 5, along with Equations (2) (3), and the following equation

$$(q-1)N(m, 1, \mathbb{F}_q^*) + N(m, 0, \mathbb{F}_q^*) = \binom{q-1}{m}. \quad (5)$$

Let us consider $m = up$ first. In this case, by Lemma 4 and Equation (3), we have:

$$\begin{aligned} \tilde{P}_m(0) &= \sum_{s=1}^{m-2} (-1)^{s+1} \left[\frac{1}{q} \binom{q-2+m-s}{m-s} \left((q-1)N(s, 1, \mathbb{F}_q^*) + N(s, 0, \mathbb{F}_q^*) \right) \right. \\ & \quad \left. + (q-1)N(s, 1, \mathbb{F}_q^*)D_{m-s}(1) + N(s, 0, \mathbb{F}_q^*)D_{m-s}(0) \right] \\ & \quad + (-1)^m (q-1)N(m-1, 1, \mathbb{F}_q^*) + (-1)^{m+1}N(m, 0, \mathbb{F}_q^*). \end{aligned}$$

Using Equations (5) and (2), we obtain

$$\begin{aligned}
\tilde{P}_m(0) &= \frac{1}{q} \sum_{s=1}^{m-2} (-1)^{s+1} \binom{q-1}{s} \binom{q-2+m-s}{m-s} \\
&+ \sum_{s=1}^{m-2} (-1)^{s+1} \frac{1}{q} \binom{q-1}{s} ((q-1)D_{m-s}(1) + D_{m-s}(0)) \\
&+ \sum_{s=1}^{m-2} (-1)^{s+1} (q-1) (-1)^{s+\lfloor s/p \rfloor} \frac{1}{q} \binom{q/p-1}{\lfloor s/p \rfloor} (-D_{m-s}(1) + D_{m-s}(0)) \\
&+ (-1)^m (q-1) \frac{1}{q} \binom{q-1}{m-1} + (-1)^{m+1} \frac{1}{q} \binom{q-1}{m} \\
&+ (-1)^m (q-1) (-1)^{m-1+\lfloor (m-1)/p \rfloor} \frac{-1}{q} \binom{q/p-1}{\lfloor (m-1)/p \rfloor} \\
&+ (-1)^{m+1} (-1)^{m+\lfloor m/p \rfloor} \frac{q-1}{q} \binom{q/p-1}{\lfloor m/p \rfloor}
\end{aligned}$$

After rearranging terms, we use Lemma 5, Lemma 3, Equations (3) and (4) to simplify the above as follows:

$$\begin{aligned}
&= \frac{1}{q} \sum_{s=1}^m (-1)^{s+1} \binom{q-1}{s} \binom{q-2+m-s}{m-s} \\
&+ \sum_{\substack{1 \leq s \leq m-2 \\ s \equiv 0, 1 \pmod{p}}} (-1)^{s+1} (-1)^{s+\lfloor s/p \rfloor} \binom{q/p-1}{\lfloor s/p \rfloor} D_{m-s}(0) \\
&+ (-1)^{u-1} \frac{q-1}{q} \left[\binom{q/p-1}{u-1} + \binom{q/p-1}{u} \right] \\
&= \frac{1}{q} \binom{q-2+up}{up} + \sum_{\substack{1 \leq s \leq up \\ s \equiv 0, 1 \pmod{p}}} (-1)^{1+\lfloor s/p \rfloor} \binom{q/p-1}{\lfloor s/p \rfloor} D_{up-s}(0),
\end{aligned}$$

where we use Lemma 5 and $-D_0(0) = D_1(0) = -\frac{q-1}{q}$ to obtain the last equality. Now let us rewrite this as

$$\begin{aligned}
\tilde{P}_{up}(0) &= \frac{1}{q} \binom{q-2+up}{up} + \sum_{t=0}^{u-1} (-1)^{1+(u-t)} \binom{q/p-1}{u-t} D_{tp}(0) \\
&+ \sum_{t=0}^{u-1} (-1)^{(u-t)} \binom{q/p-1}{u-t-1} D_{tp+1}(0). \tag{6}
\end{aligned}$$

Similarly, for $m = up + 1$, we have

$$\begin{aligned} \tilde{P}_{up+1}(0) &= \frac{1}{q} \binom{q-2+(up+1)}{up+1} + \sum_{\substack{1 \leq s \leq up-1 \\ s \equiv 0, 1 \pmod{p}}} (-1)^{1+\lfloor s/p \rfloor} \binom{q/p-1}{\lfloor s/p \rfloor} D_{up+1-s}(0) \\ &= \frac{1}{q} \binom{q-2+up+1}{up+1} + \sum_{t=1}^{u-1} (-1)^{1+u-t} \binom{q/p-1}{u-t} (D_{tp}(0) + D_{tp+1}(0)) - D_{up}(0). \end{aligned}$$

Next we show $D_{up+1}(0) = -D_{up}(0)$ for all $u \geq 0$ by mathematical induction. The base case $u = 0$ holds because $D_1(0) = D_0(0) = -\frac{q-1}{q}$. Assume now $-D_{sp}(0) = D_{sp+1}(0)$ for all $0 \leq s < u$ and plug into the above formula we obtain

$$\tilde{P}_{up+1}(0) = \frac{1}{q} \binom{q-2+up+1}{up+1} - D_{up}(0)$$

Because $\tilde{P}_{up+1}(0) = \frac{1}{q} \binom{q-2+up+1}{up+1} + D_{up+1}(0)$, we conclude that $D_{up+1}(0) = -D_{up}(0)$. Hence it is true for all $u \geq 0$. Using this relation we simplify Equation (6) to

$$\begin{aligned} \tilde{P}_{up}(0) &= \frac{1}{q} \binom{q-2+up}{up} + \sum_{t=0}^{u-1} (-1)^{u-t+1} \left(\binom{q/p-1}{u-t} + \binom{q/p-1}{u-t-1} \right) D_{tp}(0) \\ &= \frac{1}{q} \binom{q-2+up}{up} + \sum_{t=0}^{u-1} (-1)^{u-t+1} \binom{q/p}{u-t} D_{tp}(0) \end{aligned} \quad (7)$$

and by using $\tilde{P}_{up}(0) = \frac{1}{q} \binom{q-2+up}{up} + D_{up}(0)$ we obtain

$$D_{up}(0) = \sum_{t=0}^{u-1} (-1)^{u-t+1} \binom{q/p}{u-t} D_{tp}(0). \quad (8)$$

Let $f(x) = \sum_{j=0}^{\infty} D_{jp}(0)x^j$ be the generating function of the sequence $\{D_{up}(0) : u = 0, 1, 2, \dots\}$. Then

$$\begin{aligned} (1-x)^{q/p} f(x) &= \left(\sum_{l=0}^{q/p} \binom{q/p}{l} (-1)^l x^l \right) \left(\sum_{j=0}^{\infty} D_{jp}(0)x^j \right) \\ &= D_0(0) + \sum_{u=1}^{\infty} \left(\left(\sum_{t=0}^{u-1} \binom{q/p}{u-t} (-1)^{u-t} D_{tp}(0) \right) + D_{up}(0) \right) x^u \\ &= D_0(0) + \sum_{u=1}^{\infty} (-D_{up}(0) + D_{up}(0)) x^u = D_0(0) = \frac{q-1}{q}. \end{aligned}$$

Now $(1-x)^{q/p} f(x) = \frac{q-1}{q}$ implies

$$f(x) = \frac{q-1}{q} \frac{1}{(1-x)^{q/p}} = \frac{q-1}{q} \sum_{t=0}^{\infty} \binom{q/p-1+t}{t} x^t.$$

Hence $D_{jp}(0) = \frac{q-1}{q} \binom{q/p-1+j}{j}$ for $j = 0, 1, 2, \dots$. Moreover, we use Equation (4) and $D_{jp+1}(0) = -D_{jp}(0)$ to conclude

$$\begin{aligned} D_{jp}(0) &= \frac{q-1}{q} \binom{q/p-1+j}{j}; & D_{jp}(1) &= -\frac{1}{q} \binom{q/p-1+j}{j}; \\ D_{jp+1}(0) &= -\frac{q-1}{q} \binom{q/p-1+j}{j}; & D_{jp+1}(1) &= \frac{1}{q} \binom{q/p-1+j}{j}. \end{aligned}$$

Finally, together with Lemma 3 we complete the proof of Theorem 1.

Finally we note that it is straightforward to derive the following corollary.

Corollary 1. Let m be a non-negative integer, \mathbb{F}_q be a finite field of $q = p^r$ elements with prime p , and $z \in \mathbb{F}_q$. The number of partitions of z into at most m parts over \mathbb{F}_q is given by

$$\hat{P}_m(z) = \sum_{k=0}^m \tilde{P}_k(z) = \frac{1}{q} \binom{q-1+m}{m} + \tilde{D}_m(z),$$

where

$$\tilde{D}_m(z) = \begin{cases} D_m(z), & \text{if } m \equiv 0 \pmod{p}; \\ 0, & \text{otherwise.} \end{cases}$$

3 Proof of Theorem 2

Let $\ell = q - m$. The assumption $\frac{q}{2} \leq \ell < q - 3$ implies that $4 \leq m \leq \frac{q}{2}$. As in [5], we denote by \mathcal{T} the family of all subsets of \mathbb{F}_q of cardinality m , i.e.,

$$\mathcal{T} = \{T \mid T \subseteq \mathbb{F}_q, |T| = m\}.$$

Denote by \mathcal{M} the family of all multisets M of order q containing 0 with the highest multiplicity $\ell = q - m$ and the sum of elements in M is equal to 0, i.e.,

$$\mathcal{M} = \{M \mid 0 \in M, \text{multiplicity}(0) = q - m, \sum_{b \in M} b = 0\}.$$

We note that the polynomial with the least degree $q - m$ such that it sends $q - m$ values to 0 can be represented by

$$f_{(\lambda, T)}(x) = \lambda \prod_{s \in \mathbb{F}_q \setminus T} (x - s), \tag{9}$$

which uniquely determines a mapping

$$\mathcal{F} : \mathbb{F}_q^* \times \mathcal{T} \rightarrow \mathcal{M}, \tag{10}$$

defined by

$$(\lambda, T) \mapsto \text{range}(f_{\lambda, T}(x)).$$

In Lemma 2 [3] we found an upper bound for the number $|\text{range}(\mathcal{F})|$ of the images of the polynomial with the least degree $q-m$ such that it sends $q-m$ values to 0, when $m < p$. Using this upper bound, we proved that, for every m with $3 < m \leq \min\{p-1, q/2\}$, there exists a multiset M with $\sum_{b \in M} b = 0$ and the highest multiplicity $q-m$ achieved at $0 \in M$ such that every polynomial over \mathbb{F}_q with the prescribed range M has degree greater than $q-m$ (Theorem 1, [5]). This result disproved Conjecture 5.1 in [3]. In this section, we drop the restriction of $m < p$ and then use the formula obtained in Theorem 1 to prove Theorem 2, which generalizes Theorem 1 in [5]. First of all, we prove the following result.

Lemma 6. Let q be a prime power, $m \leq \frac{q}{2}$ be a positive integer and $d = \gcd(q-1, m-1)$. Let $\mathcal{F} : \mathbb{F}_q^* \times \mathcal{T} \rightarrow \mathcal{M}$ be defined as in Equation (10). Then

$$|\text{range}(\mathcal{F})| \leq \frac{(q-1)(q-2)\dots(q-m+1)}{m!} + \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \frac{\delta(q-1)}{q} \binom{q/p}{m/p},$$

where $\delta = 1$ if $p \mid m$ and zero otherwise.

Proof. As in Lemma 2 of [3] we consider the group \mathcal{G} of all non-constant linear polynomials in $\mathbb{F}_q[x]$ acting on the set $\mathbb{F}_q^* \times \mathcal{T}$ with action $\Phi : (cx + b, (\lambda, T)) \mapsto (c^{m-1}\lambda, cT + b)$. All the elements of the same orbit in $\mathbb{F}_q^* \times \mathcal{T}$ are all mapped to the same range $M \in \mathcal{M}$. Thus we need to find the number N of orbits under this group action. Using the Burnside's Lemma, we need to find the number of fixed points $|(\mathbb{F}_q^* \times \mathcal{T})_g|$ in $\mathbb{F}_q^* \times \mathcal{T}$ under the action of $g(x) = cx + b$. As in Lemma 2 [3], for $g(x) = x$ there are $(q-1)\binom{q}{m}$ elements fixed by $g(x)$. Moreover, if $g(x) = cx + b$, $c \neq 1$ then elements are fixed by $g(x)$ only if $i = \text{ord}(c) \mid d = \gcd(q-1, m-1)$ and in this case we have $|(\mathbb{F}_q^* \times \mathcal{T})_g| = (q-1)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}$. Under the assumption $m < p$ in Lemma 2 [3], we don't need to consider $g(x) = x + b$, $b \neq 0$, because it has p -cycles of the form $(x, x + b, \dots, x + (p-1)b)$ and has no fixed elements. However, for arbitrary m , we must consider this case. In fact, if $g(x) = x + b$ fixes some subset T of \mathbb{F}_q with m elements then we must have $p \mid m$ and T consists of p -cycles. In particular, there are $\binom{\frac{q}{p}}{\frac{m}{p}}$ of such subsets T fixed by $g(x) = x + b$ for each $b \in \mathbb{F}_q^*$. Varying λ and b , we therefore obtain $|(\mathbb{F}_q^* \times \mathcal{T})_g| = \delta(q-1)^2 \binom{q/p}{m/p}$. Now using Burnside's Lemma we obtain

$$\begin{aligned} N &= \frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} |(\mathbb{F}_q^* \times \mathcal{T})_g| \\ &= \frac{1}{q(q-1)} \left((q-1) \binom{q}{m} + q(q-1) \sum_{i>0, i|d} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \delta(q-1)^2 \binom{q/p}{m/p} \right) \\ &= \frac{1}{q} \binom{q}{m} + \sum_{i>0, i|d} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \frac{\delta(q-1)}{q} \binom{q/p}{m/p}. \end{aligned}$$

□

In order to prove Theorem 2 it is clear that we only need to show

$$\frac{(q-1)(q-2)\dots(q-m+1)}{m!} + \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \frac{\delta(q-1)}{q} \binom{q/p}{m/p} < \tilde{P}_m(0). \quad (11)$$

By Theorem 1, it is enough to show

$$\frac{(q-1)\dots(q-m+1)}{m!} + \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \frac{q-1}{q} \binom{\frac{q}{p}-1+j}{j} < \frac{1}{q} \binom{q+m-2}{m}. \quad (12)$$

for $m = jp + 1$ and

$$\frac{(q-1)(q-2)\dots(q-m+1)}{m!} + \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} < \frac{1}{q} \binom{q+m-2}{m}, \quad (13)$$

for all other cases, because $\frac{q-1}{q} \binom{q/p}{m/p} = \frac{q-1}{q} \binom{q/p}{j} \leq \frac{q-1}{q} \binom{q/p-1+j}{j}$ when $m = jp$ and $j \geq 1$.

For the cases $m = 4$ and $m = 5$, because $q \geq 2m$, we can check directly that Inequality (13) holds and thus Inequality (11) holds.

We now show Inequalities (12) and (13) hold for $m > 5$ by using a combinatorial argument. Let $G = \langle a \rangle$ be a cyclic group of order $q - 1$ with generator a . Let \mathcal{M}' be the set of all multisets with m elements chosen from G . Then $|\mathcal{M}'| = \binom{q-2+m}{m}$. To estimate the left hand side of Inequalities (12) and (13) we count now the number of multisets in some subsets of \mathcal{M}' defined as follows. These subsets of multisets of m elements are defined from subsets of k -subsets of G when $k \leq m$. First of all, let \mathcal{M}_0 be the set of all subsets of G with m elements. So $\mathcal{M}_0 \subseteq \mathcal{M}'$ and $|\mathcal{M}_0| = \binom{q-1}{m}$.

Let \mathcal{A} be the set of all subsets of G with $m - 1$ elements. For each $A = \{a^{u_1}, a^{u_2}, \dots, a^{u_{m-1}}\} \in \mathcal{A}$ where $0 \leq u_1 < u_2 < \dots < u_{m-1} < q - 1$ we can find a multiset $M = \{a^{u_1}, a^{u_1}, a^{u_2}, a^{u_3}, \dots, a^{u_{m-1}}\}$ corresponding to A in the unique way. We can use notation $s^{(i)}$ to denote an element s in a multiset M with multiplicity i . Hence the above multiset M can also be denoted by

$$M = \{(a^{u_1})^{(2)}, a^{u_2}, a^{u_3}, \dots, a^{u_{m-1}}\}.$$

The set of all these multisets M , denoted by \mathcal{M}_1 , has $|\mathcal{A}| = \binom{q-1}{m-1}$ elements. Moreover $\mathcal{M}_0 \cap \mathcal{M}_1 = \emptyset$. Now let $\mathcal{M}_{01} = \mathcal{M}_0 \cup \mathcal{M}_1$. Then $|\mathcal{M}_{01}| = \binom{q-1}{m} + \binom{q-1}{m-1} = \binom{q}{m}$.

For each i satisfying $m - 1 > i \geq 2$ and $i | d$, we let $S_i = \langle a^i \rangle$ be a cyclic subgroup of G with $\frac{q-1}{i}$ elements. From each set \mathcal{C}_i of all subsets of S_i with $\frac{m-1}{i}$ elements, we can define two disjoint subclasses of \mathcal{M} containing multisets with m elements in G corresponding to \mathcal{C}_i .

First, let $B = \{a^{u_1 i}, a^{u_2 i}, \dots, a^{u_{\frac{m-1}{i}} i}\}$ be a subset of S_i where $0 \leq u_1 < u_2 < \dots < \frac{q-1}{i}$. For each fixed t such that $0 \leq t < i$ and $\gcd(i, t) = 1$, we can construct a multiset corresponding to B as follows:

$$M = \{(a^t a^{u_1 i})^{(i)}, (a^t a^{u_2 i})^{(i)}, \dots, (a^t a^{u_{\frac{m-1}{i}} i})^{(i)}, a_m\}$$

where a_m is arbitrarily element in G . For each fixed t this class of multisets formed from \mathcal{C}_i is denote by \mathcal{M}_i^t . Then $|\mathcal{M}_i^t| = (q-1)\binom{\frac{q-1}{i}}{\frac{m-1}{i}}$.

Secondly, for $B = \{a^{u_1 i}, a^{u_2 i}, \dots, a^{u_{\frac{m-1}{i}} i}\} \in \mathcal{C}_i$ and each fixed t , we can construct another multiset

$$\tilde{M} = \{(\mathbf{a}^{t+1} \mathbf{a}^{u_1 i})^{(i)}, (a^t a^{u_2 i})^{(i)}, \dots, (a^t a^{u_{\frac{m-1}{i}} i})^{(i)}, \mathbf{1}\},$$

corresponding to B . The set of these multisets is denoted by $\tilde{\mathcal{M}}_i^t$. Then $|\tilde{\mathcal{M}}_i^t| = \binom{\frac{q-1}{i}}{\frac{m-1}{i}}$.

Note that $i \leq \frac{m-1}{2}$ implies $\mathcal{M}_i^t \cap \tilde{\mathcal{M}}_i^t = \emptyset$. Hence we have

$$|\mathcal{M}_i| = \left| \bigcup_{\substack{1 \leq t < i \\ \gcd(i,t)=1}} \mathcal{M}_i^t \cup \tilde{\mathcal{M}}_i^t \right| = \phi(i) \left((q-1) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \binom{\frac{q-1}{i}}{\frac{m-1}{i}} \right) = q\phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}}.$$

Finally, if $m-1 \nmid q-1$ then we let $\mathcal{M}_m = \emptyset$. Otherwise, if $(m-1) \mid q-1$ then we let \mathcal{M}_{m-1}^t contains all the multisets of the form $M = \{(a^{t+j(m-1)})^{(m-1)}, a_m\}$, for $j = 0, 1, \dots, \frac{q-1}{m-1} - 1$, any positive integer $t < m-1$ with $\gcd(m-1, t) = 1$, and any $a_m \in G$. Let $\tilde{\mathcal{M}}_{m-1}^t$ contain all the multisets of the form $\{(a^{t+j(m-1)})^{(m-2)}, (a^{m-1})^{(2)}\}$. It is obvious that $a^{m-1} \neq a^{t+j(m-1)}$. By comparing the multiplicities of two multisets we see that $\mathcal{M}_{m-1}^t \cap \tilde{\mathcal{M}}_{m-1}^t = \emptyset$. Moreover,

$$\begin{aligned} |\mathcal{M}_{m-1}| &= \left| \bigcup_{\substack{1 \leq t < m-1 \\ \gcd(m-1,t)=1}} \mathcal{M}_{m-1}^t \cup \tilde{\mathcal{M}}_{m-1}^t \right| \\ &= \phi(m-1) \left((q-1) \binom{\frac{q-1}{m-1}}{1} + \binom{\frac{q-1}{m-1}}{1} \right) \\ &= q\phi(m-1) \binom{\frac{q-1}{m-1}}{\frac{m-1}{m-1}}. \end{aligned}$$

Finally, if $m \neq jp+1$ for some $j \geq 1$ we let $\mathcal{M}_m = \emptyset$. Otherwise, if $m = jp+1$ for some $j \geq 1$ we let $C = \{s_1, s_2, \dots, s_{q/p}\}$ be a subset of G with $q/p < q-1$ elements. For each subset of j elements from C we find a corresponding multiset M in \mathcal{M}_m from \mathcal{M} in the following way

$$M = \{s_1^{(p)}, s_2^{(p)}, \dots, s_j^{(p)}, a_m\}$$

where a_m is arbitrary chosen to be an element from G . Thus there are $(q-1)\binom{q/p+j-1}{j}$ multisets in \mathcal{M}_m . Obviously, \mathcal{M}_m is disjoint \mathcal{M}_i where $i \mid \gcd(m-1, q-1)$ because the multiplicity of at least one of its element is $p \nmid q-1$. Indeed, it could possibly have common elements only with \mathcal{M}_{m-1} but in this case $m-1 = jp \nmid q-1$ so $\mathcal{M}_{m-1} = \emptyset$. Now $|\mathcal{M}_m| = (q-1)\binom{q/p+j-1}{j}$.

Define $\delta' = 0$ if $m \neq jp + 1$ for some j and $\delta' = 1$ if $m = jp + 1$. Then we obtain

$$\begin{aligned} |\mathcal{M}_{LHS}| &:= \left| \mathcal{M}_{01} \cup \left(\bigcup_{\substack{i | \gcd(m-1, q-1) \\ i > 1}} \mathcal{M}_i \right) \cup \mathcal{M}_m \right| \\ &= \binom{q}{m} + q \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \delta'(q-1) \binom{q/p + (m-1)/p - 1}{(m-1)/p}. \end{aligned}$$

We note that the multiset $\{1, 1, 1, a, a^2, \dots, a^{m-3}\}$ is not included in the \mathcal{M}_{LHS} and thus $|\mathcal{M}_{LHS}| < |\mathcal{M}'|$. Dividing both sides by q , we have

$$\frac{1}{q} \binom{q}{m} + \sum_{i|d, i>1} \phi(i) \binom{\frac{q-1}{i}}{\frac{m-1}{i}} + \frac{\delta'(q-1)}{q} \binom{q/p + (m-1)/p - 1}{(m-1)/p} < \frac{1}{q} \binom{q+m-2}{m}. \quad (14)$$

Hence both Inequalities (12) and (13) are satisfied. This completes the proof of Theorem 2.

Acknowledgements

We would like to thank the anonymous referees for helpful suggestions, in particular, for pointing out the reference [2], and also thank Keith Conrad for useful suggestions and for bringing the papers [6, 7, 8] to our attention.

References

- [1] B. C. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi sums. Canadian Math. Soc. Series of Monographs and Advanced Texts. John Wiley & Sons, New York, 1998.
- [2] K. Conrad, Jacobi sums and Stickelberger's congruence, *Enseign. Math.* **41** (1995), 141-153.
- [3] A. Gács, T. Héger, Z. L. Nagy, D. Pálvölgyi, Permutations, hyperplanes and polynomials over finite fields, *Finite Field Appl.* **16** (2010), 301-314.
- [4] J. Li and D. Wan, On the subset sum problem over finite fields, *Finite Field Appl.*, **14** (2008), 911-929.
- [5] A. Muratović-Ribić and Q. Wang, On a conjecture of polynomials with prescribed range, *Finite Field Appl.*, **18** (2012), no. 4, 728-737.
- [6] D. Wan, Mirror symmetry for zeta functions, In Mirror Symmetry V, AMS/IP Studies in Advanced Mathematics, Vol.38, 2006, 159-184.
- [7] D. Wan, Lectures on zeta functions over finite fields (Gottingen Lecture Notes). in Higher Dimensional Geometry over Finite Fields, eds: D. Kaledin and Y. Tschinkel, IOS Press, 2008, 244-268.
- [8] C. F. Wong, Zeta functions of projective toric hypersurfaces over finite fields. Thesis (Ph.D.)—University of California, Irvine. 2008, <http://arxiv.org/pdf/0811.0887>
- [9] R. P. Stanley, Enumerative Combinatorics, Vol I, Cambridge University Press, 1997.