A NEW SIEVE FOR RESTRICTED MULTISET COUNTING

JIYOU LI AND XIANG YU

Abstract. The Li–Wan sieve [11] is extended to multisets when the underlying set is symmetric. The main ingredient of the proof is the Mobius inversion formula on the poset of partitions of $\{1, 2, \ldots, k\}$ ordered by refinement. As illustrative applications, we investigate the problems of partitions over finite fields and zero-sum multisets over the additive group $\mathbb{Z}/n\mathbb{Z}$.

1. Introduction

1.1. **Distinct coordinate counting.** For a positive integer k, let D^k be the Cartesian product of k copies of a set D. Let X be a subset of D^k. Each element $x \in X$ can be written in a vector form $x = (x_1, x_2, \ldots, x_k)$ with $x_i \in D$. Motivated by various problems arising from coding theory and number theory [2, 3, 4, 16], we are interested in understanding the structure of the set $\overline{X}$ which consists of "distinct coordinate vectors" in X:

$$\overline{X} = \{(x_1, x_2, \ldots, x_k) \in X : x_i \neq x_j,\ \forall\, 1 \leq i \neq j \leq k\}, \tag{1.1}$$

In particular, when $\overline{X}$ is finite, we want to compute its cardinality, or more generally, evaluate complex function sums defined over $\overline{X}$.

A natural way to compute $|\overline{X}|$ is using the inclusion-exclusion principle. For integers $1 \leq i < j \leq k$, let $X_{ij} = \{(x_1, x_2, \ldots, x_k) \in X : x_i = x_j\}$. Then the classical inclusion-exclusion principle gives

$$|\overline{X}| = |X \setminus \bigcup_{1\leq i<j\leq k} X_{ij}| = |X| - \sum_{1\leq i<j\leq k} |X_{ij}| + \sum_{1\leq i<j\leq k, 1\leq s<t\leq k} |X_{ij} \bigcap X_{st}| - \cdots + (-1)^{\binom{k}{2}} |\bigcap_{1\leq i<j\leq k} X_{ij}|. \tag{1.2}$$

However, the number of terms in the above summation is $2^{\binom{k}{2}}$, which easily causes large total errors. In fact, this is a major bottle-neck of the inclusion-exclusion sieve. In most applications, people use Bonferroni inequalities to get weaker bounds such as

$$|\overline{X}| \geq |X| - \sum_{1\leq i<j\leq k} |X_{ij}|. \tag{1.3}$$

These bounds play important roles in many problems in combinatorics, number theory, probability theory and theoretical computer sciences. However, they are usually restrictive. For example, (1.3) is only nontrivial when $|X| > \binom{k}{2}$. A natural question is then to find simpler explicit formulas or sharper bounds.

A formula discovered by Li and Wan [11] gives an approach to compute $|\overline{X}|$ through a simpler way. The new formula, which will be described in Theorem 1.1, shows that there exists a large number of cancellations on the right-hand side of (1.2). The number of terms in the summation is significantly reduced from $2^{\binom{k}{2}}$ to $k!$, or even fewer, to the partition function $p(k)$ if X is symmetric.

There is a natural action of the symmetric group S_k on elements of X defined as follows. For $\tau \in S_k$ and $x = (x_1, x_2, \ldots, x_k) \in X$, define $\tau \circ x := (x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)})$. Let X_τ be the set of elements in

This work was supported in part by the National Science Foundation of China (11771280, 12031011) and a GRF grant (Project no. CityU 11303718) from the Research Grants Council of the Government of HKSAR, China.

X that are invariant under the action by τ. Since each $\tau \in S_k$ can be written as a product of disjoint cycles $\tau = \tau_1\tau_2\cdots\tau_{c(\tau)}$ uniquely up to the order of the cycles, clearly we have

$$X_\tau = \{(x_1, x_2, \ldots, x_k) \in X : x_i = x_j,\ \forall\, i, j \in \tau_m,\ 1 \le m \le c(\tau)\}.$$

Theorem 1.1 ([11], Theorem 1.1). *For $\tau \in S_k$, let $\operatorname{sign}(\tau)$ be the signature of τ which is defined by $\operatorname{sign}(\tau) = (-1)^{k-c(\tau)}$, where $c(\tau)$ is the number of disjoint cycles of τ. Then*

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

In particular, if X is symmetric, that is, invariant under the action of S_k, then

$$|\overline{X}| = \sum_{\tau \in C_k} \operatorname{sign}(\tau)C(\tau)|X_\tau|, \tag{1.4}$$

where $C(\tau)$ is the size of the conjugacy class of S_k that contains τ and $|X_\tau|$ is naturally defined over C_k, the set of all conjugacy classes of S_k.

It is quite surprising that Theorem 1.1 was not known before since the Möbius inversion over Π_k was known in the 1960s, where Π_k is the poset of all partitions of $\{1, 2, \ldots, k\}$ ordered by refinement. Precisely, the Möbius inversion formula gives the following formula for $|\overline{X}|$:

$$|\overline{X}| = \sum_{\tau \in \Pi_k} \mu(\mathbf{0}, \tau)|X_\tau|.$$

In the case of partition lattice Π_k, an explicit expression for the Möbius function $\mu(\mathbf{0}, \tau)$ (see Proposition 2.2) was given independently by Schützenberger in 1954, and Frucht and Rota [21] in 1964. However, the above formula is not convenient to use. One reason is that counting problems over set partitions seem more complicated than those over permutations, as explained below.

We now explain further why counting over permutations might be simpler. Suppose that a permutation $\tau \in S_k$ is of type $(c_1, c_2, \ldots, c_k)$, that is, it has exactly c_i cycles of length i. It is well-known that the size of the conjugacy class of S_k that contains τ is given by

$$C(\tau) = N(c_1, c_2, \ldots, c_k) = \frac{k!}{1^{c_1}c_1!2^{c_2}c_2!\cdots k^{c_k}c_k!},$$

since two permutations in S_k are conjugate if and only if they have the same type. This makes (1.4) computable for many interesting cases via the exponential generating function defined by

$$\sum_{k=0}^{\infty} \sum_{\sum ic_i = k} N(c_1, c_2, \ldots, c_k)t_1^{c_1}t_2^{c_2}\cdots t_k^{c_k}\frac{u^k}{k!} = \exp\Big(t_1u + t_2\frac{u^2}{2} + t_3\frac{u^3}{3} + \cdots\Big). \tag{1.5}$$

The readers are referred to [11, 12] for more details and the proof of Theorem 1.1. It turns out that the sieve formula (1.4) has played an important role in many interesting problems in number theory and coding theory.

First, the sieve formula gives an elementary way for enumerating subsets S of $\mathbb{F}_q^*$ with the property that $\sum_{x\in S} x^m = b$, which was first studied by Odlyzko and Stanley for prime q [20]. We remark that it has the advantage when used to count the number of k-subsets S of $\mathbb{F}_q^*$ satisfying the same equality [8, 23].

Second, since a subset can be naturally regarded as a vector with distinct coordinates, the sieve formula provides a new counting approach for investigating the subset sum problem, a well-known **#P-complete** problem, from a mathematical point of view. Precisely, it is possible to explicitly enumerate subsets of a finite subset $D \subseteq G$ that sum to a given element in G, where G is an abelian group. For example, G could be the additive group of a finite field, the multiplicative group of a finite field, the rational group of an elliptic curve over finite fields, etc., and D could be a subset with algebraic structure (a subgroup, for example) or an arbitrarily large subset of G. Many explicit or asymptotic formulas were obtained for different subsets D in these situations; see for example [6, 10, 12, 13, 23]. Further applications can be found in [7, 9, 15].

In this paper, we extend the Li–Wan sieve to multisets when X is symmetric. This extension allows us to count more complicated combinatorial objects naturally, as shown in Section 3.

1.2. **Motivations for restricted multiset counting.** We first give the definition of restricted multiset.

Definition 1.2. Let D^k be the Cartesian product of k copies of a set D. A subset X of D^k is said to be *symmetric* if $(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)}) \in X$ for any $(x_1, x_2, \ldots, x_k) \in X$ and any $\tau \in S_k$. From now on, we always assume that X is symmetric. A k-multiset $[x_1, x_2, \ldots, x_k]$ is said to satisfy the *restriction* X if the ordered k-tuple $(x_1, x_2, \ldots, x_k)$ is in X. We denote by $\mathcal{M}(X)$ the set of all k-multisets satisfying the restriction X, that is,

$$\mathcal{M}(X) := \{[x_1, x_2, \ldots, x_k] : (x_1, x_2, \ldots, x_k) \in X\}.$$

Example 1.3. Let $D = \mathbb{F}_q$ be a finite field of q elements, and let X be the set $X = \{(x_1, x_2, \ldots, x_k) \in D^k : x_1 + x_2 + \cdots + x_k = 0\}$. Then $\mathcal{M}(X)$ consists of k-multisets over $\mathbb{F}_q$ whose elements sum to 0.

Remark 1.4. It is not hard to check that the restriction X is well-defined, since X is a symmetric subset of D^k. One can also think of the set of k-multisets satisfying the restriction X as the image of X under the map that sends the ordered k-tuple $(x_1, x_2, \ldots, x_k)$ to the k-multiset $[x_1, x_2, \ldots, x_k]$.

The problem of counting restricted multisets arises naturally from combinatorics. Some interesting problems are listed as follows.

1.2.1. *Polynomials with prescribed range.* In studying permutations, hyperplanes and polynomials over finite fields, Gács et al. proposed the following conjecture on polynomials with prescribed range.

Conjecture 1.5 ([5], Conjecture 5.1)**.** *Suppose that $M = [a_1, a_2, \ldots, a_q]$ is a multiset over a finite field $\mathbb{F}_q$ with $a_1 + a_2 + \cdots + a_q = 0$, where $q = p^h$ with p prime. Let $m < \sqrt{p}$. If there is no polynomial with range M of degree less than $q - m$, then M contains an element of multiplicity at least $q - m$.*

Here a multiset M on $\mathbb{F}_q$ is said to be the range of the polynomial $f \in \mathbb{F}_q[x]$ if $M = [f(x) : x \in \mathbb{F}_q]$ as a multiset (that is, not only values, but also multiplicities need to be the same). To prove or disprove the conjecture by a counting argument, a key step is to estimate the cardinality of the set $\mathcal{M}(X)$, where X is the set of ordered k-tuples in $(\mathbb{F}_q \setminus \{0\})^k$ that sum to zero. In the case $m = 2$, the conjecture holds by Theorem 2.2 in [5]; in the case $m \geq 3$, the conjecture was disproved by Muratović-Ribić and Wang [18] using an estimation they obtained for $|\mathcal{M}(X)|$.

1.2.2. *Bijection between necklaces and zero-sum multisets.* We may further partition $\mathcal{M}(X)$ into various classes. For instance, consider the set of k-multisets in $\mathcal{M}(X)$ with the multiplicity of each element no greater than a given number. For an integer $j \geq 1$, we define

$$\mathcal{M}_j(X) = \{[x_1, x_2, \ldots, x_k] \in \mathcal{M}(X) : \text{the multiplicity of each } x_i \text{ is no greater than } j,\ 1 \leq i \leq k\},$$

The set $\mathcal{M}_j(X)$ arises from the bijective proof problem of necklaces and zero-sum multisets [1], which asks for a bijection between cyclic necklaces of length n with at most q-colors and zero-sum multisets over $\mathbb{Z}/n\mathbb{Z}$ with the multiplicity of each element strictly less than q, when n and q are coprime. Note that the latter is the set $\bigcup_{k=0}^{n(q-1)} \mathcal{M}_{q-1}(X_k)$, where X_k is the set of ordered k-tuples in $(\mathbb{Z}/n\mathbb{Z})^k$ that sum to zero. Recently, Chan [1] gave a surprising bijective construction for this problem when q is a prime power using tools from finite fields. Specializing to the case $q = 2$ answers a question raised by Stanley (see [22], Page 136), which was open for many years. The problem remains open when q is not a prime power. We believe that our results on restricted multisets might give some new insights into this problem.

1.2.3. *List sizes of Reed Solomon codes.* Let $\mathbb{F}_q$ be a finite field of order q. Let $1 \le n \le q$ be a positive integer and $D = \{x_1, x_2, \dots, x_n\} \subset \mathbb{F}_q$ be a subset of cardinality $|D| = n > 0$. For $1 \le k \le n$, the Reed-Solomon code $\mathcal{RS}_{n,k}$ consists of all vectors of the form

$$(f(x_1), f(x_2), \dots, f(x_n)) \in \mathbb{F}_q^n,$$

where f runs over all polynomials in $\mathbb{F}_q[x]$ of degree at most $k-1$. Reed-Solomon codes play important roles in coding theory. It is well-known that the minimum distance of the Reed-Solomon code is $n-k+1$. For simplicity we consider the special case $D = \mathbb{F}_q$ and the corresponding code $\mathcal{RS}_{q,k}$ is called the standard Reed-Solomon code.

Given a received word u, it is a challenging problem to determine the distance distribution having u as the center. In particular, it is an important open problem to obtain list sizes beyond the Jonson bound. That is, for a non-negative integer i, compute the number $N_i(u)$ of codewords in $\mathcal{RS}_{q,k}$ whose distance to u is exactly i. In [14], the authors reduce a list size decoding problem of Reed Solomon codes to a multiset counting problem. For interested readers we restated it as follows.

Problem 1.6. *Let $1 \le k \le q$ and $-k \le m \le q-k-1$. Given a monic polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $k+m$ and an integer $0 \le r \le k+m$, count $N(f(x), r)$, the number of polynomials $g(x) \in \mathbb{F}_q[x]$ with $\deg g(x) \le k-1$ such that $f(x)+g(x)$ has exactly r distinct roots in $\mathbb{F}_q$.*

This leads to another refinement of $\mathcal{M}(X)$ and a generalization of the set $\overline{X}$ defined in (1.1). It is the set of k-multisets in $\mathcal{M}(X)$ which have exactly d distinct elements, that is,

$$\overline{\mathcal{M}}_d(X) = \{[x_1, x_2, \dots, x_k] \in \mathcal{M}(X) : [x_1, x_2, \dots, x_k] \text{ has exactly } d \text{ distinct elements}\}.$$

For $a \in D$, let P_a be the property that a multiset contains a as an element, and for $A \subseteq D$, let N_A be the number of k-multisets satisfying the restriction X and the property P_a for each $a \in A$. Then the weighted version of the inclusion-exclusion principle [17] gives

$$|\overline{\mathcal{M}}_d(X)| = \sum_{\{a_1,a_2,\dots,a_d\} \subset D} N_{\{a_1,a_2,\dots,a_d\}} - \binom{d+1}{d} \sum_{\{a_1,a_2,\dots,a_{d+1}\} \subset D} N_{\{a_1,a_2,\dots,a_{d+1}\}} + \cdots .$$

However, $N_{\{a_1,a_2,\dots,a_i\}}$ is usually depending on $\{a_1, a_2, \dots, a_i\}$ and thus it seems infeasible to use this formula to obtain a nice bound on $|\overline{\mathcal{M}}_d(X)|$.

Clearly, the restricted multiset sum problem is a natural generalization of the subset sum problem and thus is **#P-complete**. In this paper, we try to study the counting version of this problem. We establish several combinatorial identities, which in some cases give interesting closed-form expressions.

1.3. **Main results.** Our idea for computing $|\mathcal{M}(X)|$, $\mathcal{M}_j(X)$ and $|\overline{\mathcal{M}}_d(X)|$ is based on the Möbius inversion formula on Π_k, the poset of all partitions of $\{1, 2, \dots, k\}$ ordered by refinement. The method first appeared in [12]. Given a permutation $\tau \in S_k$, suppose again that we have a disjoint cycle factorization $\tau = \tau_1\tau_2\cdots\tau_{c(\tau)}$ and the length of the cycle τ_i is ℓ_i, $1 \le i \le c(\tau)$. For an integer $j \ge 1$ we define

$$w_j(\tau) := (1-(j+1)1_{(j+1)|\ell_1})(1-(j+1)1_{(j+1)|\ell_2})\cdots(1-(j+1)1_{(j+1)|\ell_{c(\tau)}}), \tag{1.6}$$

where $1_{(j+1)|\ell_i}$ denotes the indicator function of the statement $(j+1) \mid \ell_i$ which is equal to 1 if $(j+1) \mid \ell_i$ and 0 otherwise. Let d be an integer with $1 \le d \le k$, we define

$$\overline{w}_d(\tau) := [x^d](1-(1-x)^{\ell_1})(1-(1-x)^{\ell_2})\cdots(1-(1-x)^{\ell_{c(\tau)}}). \tag{1.7}$$

Now we can state our main results. Recall that X is a symmetric subset of D^k and $\mathcal{M}(X)$ is defined as $\mathcal{M}(X) = \{[x_1, x_2, \dots, x_k] : (x_1, x_2, \dots, x_k) \in X\}$.

Theorem 1.7. *Let j be a positive integer and let $\mathcal{M}_j(X)$ be the set of k-multisets in $\mathcal{M}(X)$ with the multiplicity of each element no greater than j. Then we have*

$$|\mathcal{M}_j(X)| = \frac{1}{k!} \sum_{\tau \in S_k} w_j(\tau)|X_\tau|, \tag{1.8}$$

In particular, specializing to $j \geq k$, we have

$$|\mathcal{M}(X)| = \frac{1}{k!} \sum_{\tau \in S_k} |X_\tau|. \tag{1.9}$$

Remark 1.8. The formula (1.8) can be further simplified by employing the symmetry of X. We notice that X_τ has the same cardinality for τ in a conjugacy class of S_k, since X is symmetric. This leads to the simplification of (1.8) as

$$|\mathcal{M}_j(X)| = \frac{1}{k!} \sum_{\tau \in C_k} w_j(\tau) C(\tau) |X_\tau|, \tag{1.10}$$

where C_k and C_τ are defined as in Theorem 1.1. We prefer (1.8) as it looks cleaner.

Specializing to $j = 1$, we see from (1.6) that

$$w_1(\tau) = (1 - 2 \cdot 1_{2|\ell_1})(1 - 2 \cdot 1_{2|\ell_1}) \cdots (1 - 2 \cdot 1_{2|\ell_{c(\tau)}}) = (-1)^{k - c(\tau)},$$

where we used $1 - 2 \cdot 1_{2|\ell_i} = (-1)^{\ell_i - 1}$ and $\ell_1 + \ell_2 + \cdots + \ell_{c(\tau)} = k$. Thus when $j = 1$, the sieve formula (1.8) is indeed the Li–Wan sieve (Theorem 1.1).

Theorem 1.9. *Let d be a positive integer and let $\overline{\mathcal{M}}_d(X)$ be the set of k-multisets in $\mathcal{M}(X)$ which have exactly d distinct elements. Then*

$$|\overline{\mathcal{M}}_d(X)| = \frac{1}{k!} \sum_{\tau \in S_k} \overline{w}_d(\tau) |X_\tau|. \tag{1.11}$$

Theorem 1.7 and Theorem 1.9 have natural weighted versions.

Theorem 1.10. *Let $f : X \to \mathbb{C}$ be a symmetric function ("symmetric" means $f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(k)}) = f(x_1, x_2, \ldots, x_k)$ for any $(x_1, x_2, \ldots, x_k) \in X$ and any $\tau \in S_k$). Then we have*

$$\sum_{[x_1, x_2, \ldots, x_k] \in \mathcal{M}_j(X)} f(x_1, x_2, \ldots, x_k) = \frac{1}{k!} \sum_{\tau \in S_k} w_j(\tau) \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k).$$

In particular, specializing to $j \geq k$, we have

$$\sum_{[x_1, x_2, \ldots, x_k] \in \mathcal{M}(X)} f(x_1, x_2, \ldots, x_k) = \frac{1}{k!} \sum_{\tau \in S_k} \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k).$$

Theorem 1.11. *Let $f : X \to \mathbb{C}$ be a symmetric function. Then we have*

$$\sum_{[x_1, x_2, \ldots, x_k] \in \overline{\mathcal{M}}_d(X)} f(x_1, x_2, \ldots, x_k) = \frac{1}{k!} \sum_{\tau \in S_k} \overline{w}_d(\tau) \sum_{x \in X_\tau} f(x_1, x_2, \ldots, x_k).$$

This paper is organized as follows. In Section 2, we prove the sieve formulas, Theorem 1.7 and Theorem 1.9, via the Möbius inversion formula. Then we give two illustrative applications of the sieve formulas in Section 3,

Notation. To distinguish between sets and multisets, we use the square bracket notation to denote multisets. Thus for instance, the multiset $\{a, a, b\}$ is denoted by $[a, a, b]$. If $F(x) = \sum_{n=0}^\infty a_n x^n$ is a formal power series, then we use $[x^n]F(x) = a_n$ to denote the coefficient of x^n in $F(x)$. If S is a statement, we use 1_S to denote the indicator function of S, thus $1_S = 1$ when S is true and $1_S = 0$ when S is false. We often abbreviate partially ordered set as poset. We use $\mathbf{0}$ and $\mathbf{1}$ to denote the least element and the greatest element in a poset, respectively.

2. Proofs of the main results

In this section, we prove Theorem 1.7 and Theorem 1.9 via the Möbius inversion formula. We first recall the Möbius inversion formula on posets.

Proposition 2.1 ([22], Proposition 3.7.1). *Let $(P, \leq)$ be a poset. Define the Möbius function μ of P recursively by*

$$\mu(x,x) = 1 \quad \text{for all } x \in P, \quad \mu(x,y) = -\sum_{x \leq z < y} \mu(x,z) \quad \text{for all } x < y \text{ in } P.$$

Then for $f, g : P \to K$, where K is a field, we have

$$g(x) = \sum_{x \leq y} f(y) \quad \text{for all } x \in P$$

if and only if

$$f(x) = \sum_{x \leq y} \mu(x,y) g(y) \quad \text{for all } x \in P.$$

Let Π_k be the set of all partitions of $\{1, 2, \ldots, k\}$. Define a partial order $\leq$ on Π_k by refinement. That is, declare $\tau \leq \sigma$ if every block of τ is contained in a block of σ. Computing the Möbius function μ of the poset $(\Pi_k, \leq)$ is a non-trivial result in enumerative combinatorics. We cite it directly from [22] without a proof.

Proposition 2.2 ([22], Example 3.10.4). *Let $\tau, \sigma \in \Pi_k$ and $\tau \leq \sigma$. Suppose that $\sigma = \{B_1, B_2, \ldots, B_\ell\}$ and that B_i, $1 \leq i \leq \ell$ is partitioned into λ_i blocks in τ. Then the Möbius function $\mu(\tau, \sigma)$ is given by*

$$\mu(\tau, \sigma) = (-1)^{\lambda_1 - 1}(\lambda_1 - 1)!(-1)^{\lambda_2 - 1}(\lambda_2 - 1)! \cdots (-1)^{\lambda_\ell - 1}(\lambda_\ell - 1)!. \tag{2.1}$$

In analogy to the type of a permutation, a partition $\tau \in \Pi_k$ is said to be of type $(a_1, a_2, \ldots, a_k)$ if it has exactly a_i blocks of size i, $1 \leq i \leq k$. It is not hard to see that the number of partitions in Π_k of type $(a_1, a_2, \ldots, a_k)$ is given by

$$\widetilde{N}(a_1, a_2, \ldots, a_k) = \frac{k!}{1!^{a_1} a_1! 2!^{a_2} a_2! \cdots k!^{a_k} a_k!}. \tag{2.2}$$

For the purpose of our proof, we need two combinatorial equalities.

Lemma 2.3. *Let $\widetilde{N}(a_1, a_2, \ldots, a_k)$ be defined as in (2.2) and let j be a positive integer. Then we have*

$$\sum_{\substack{\sum i a_i = k \\ a_{j+1} = \cdots = a_k = 0}} \widetilde{N}(a_1, \ldots, a_k) 1!^{a_1} \cdots k!^{a_k} (-1)^{a_1 + \cdots + a_k - 1}(a_1 + \cdots + a_k - 1)! = (k-1)!(1 - (j+1)1_{(j+1)|k}).$$

Proof. Substituting (2.2) into the above equation, we see that the left-hand side is

$$\begin{aligned}
\text{LHS} &= k! \sum_{\sum i a_i = k} (-1)^{a_1 + \cdots + a_j - 1} \frac{(a_1 + \cdots + a_j - 1)!}{a_1! \cdots a_j!} \\
&= k! \sum_{\sum i a_i = k} \frac{(-1)^{a_1 + \cdots + a_j - 1}}{a_1 + \cdots + a_j} \binom{a_1 + \cdots + a_j}{a_1, \ldots, a_j} \\
&= k! \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} \sum_{\substack{\sum i a_i = k \\ \sum a_i = m}} \binom{m}{a_1, \ldots, a_j} \\
&= k! \sum_{m=1}^{\infty} \frac{(-1)^{m-1}}{m} [x^k](x + x^2 + \cdots + x^j)^m \\
&= k! [x^k] \log(1 + x + \cdots + x^j)
\end{aligned}$$

$$= k![x^k](\log(1-x^{j+1}) - \log(1-x))$$
$$= (k-1)!(1-(j+1)1_{(j+1)|k}).$$

This proves the lemma. □

Lemma 2.4. *Let $\widetilde{N}(a_1, a_2, \ldots, a_k)$ be defined as in (2.2) and let d be an integer with $1 \le d \le k$. Then we have*

$$\sum_{\substack{\sum ia_i = k\\ a_1+\cdots+a_k=d}} \widetilde{N}(a_1,\ldots,a_k)1!^{a_1}\cdots k!^{a_k}(-1)^{a_1+\cdots+a_k-1}(a_1+\cdots+a_k-1)! = (k-1)!(-1)^{d-1}\binom{k}{d}.$$

Proof. Similar to the proof of the previous lemma, a substitution of (2.2) into the above equation yields

$$\begin{aligned}
\text{LHS} &= k!\frac{(-1)^{d-1}}{d}\sum_{\substack{\sum ia_i=k\\ a_1+\cdots+a_k=d}} \frac{d!}{a_1!\cdots a_k!}\\
&= k!\frac{(-1)^{d-1}}{d}[x^k](x+x^2+\cdots+x^k)^d\\
&= k!\frac{(-1)^{d-1}}{d}[x^k](x-x^{k+1})^d(1-x)^{-d}\\
&= (k-1)!(-1)^{d-1}\binom{k}{d}.
\end{aligned}$$

The lemma then follows. □

Now we prove Theorem 1.7.

Proof of Theorem 1.7. For a partition $\tau \in \Pi_k$, define X_τ° to be the set of ordered k-tuples $(x_1, x_2, \ldots, x_k)$ such that $(x_1, x_2, \ldots, x_k) \in X_\tau$ but $(x_1, x_2, \ldots, x_k) \notin X_\sigma$ for any $\sigma > \tau$. It is not hard to check that $|X_\tau| = \sum_{\tau \le \sigma} |X_\sigma^\circ|$. Then the Möbius inversion formula (Proposition 2.1) gives

$$|X_\tau^\circ| = \sum_{\tau \le \sigma} \mu(\tau,\sigma)|X_\sigma|. \tag{2.3}$$

Suppose that $\tau = \{B_1, B_2, \ldots, B_\ell\}$ and the size of B_i is m_i, $1 \le i \le \ell$. We observe from the definition of X_τ° that the multiplicities of elements in the multiset $[x_1, x_2, \ldots, x_k]$ with $(x_1, x_2, \ldots, x_k) \in X_\tau^\circ$ are $m_1, m_2, \ldots, m_\ell$. Thus for $(x_1, x_2, \ldots, x_k) \in X_\tau^\circ$, the multiplicity of each element in $[x_1, x_2, \ldots, x_k]$ that is no greater than j is equivalent to the size of each block of τ that is no greater than j. Since the number of permutations of this multiset is $\binom{k}{m_1, m_2, \ldots, m_\ell}$, the number of k-multiset satisfying the restriction X_τ° is

$$|\mathcal{M}(X_\tau^\circ)| = \frac{m_1!m_2!\cdots m_\ell!}{k!}|X_\tau^\circ|. \tag{2.4}$$

Note that $X = \bigcup_{\tau \in \Pi_k} X_\tau^\circ$ is a disjoint union of X_τ, so we conclude that

$$|\mathcal{M}_j(X)| = \sum_{\tau \in \Pi_k:\text{the size of each block of } \tau \le j} |\mathcal{M}(X_\tau^\circ)|.$$

Substituting (2.3) and (2.4) into the above equation, we obtain

$$\begin{aligned}
|\mathcal{M}_j(X)| &= \sum_{\tau \in \Pi_k: m_i \le j, 1 \le i \le \ell} \frac{m_1!m_2!\cdots m_\ell!}{k!}|X_\tau^\circ|\\
&= \frac{1}{k!}\sum_{\sigma \in \Pi_k}\Big(\sum_{\tau \le \sigma: m_i \le j, 1\le i\le \ell} m_1!m_2!\cdots m_\ell!\mu(\tau,\sigma)\Big)|X_\sigma|.
\end{aligned}$$

Note that here m_i and ℓ should be $m_i(\tau)$ and $\ell(\tau)$ respectively, but we omit the variable τ for notational simplicity.

Since the number of cyclic permutations of length k in S_k is $(k-1)!$, a partition σ in Π_k with block sizes $n_1, n_2, \ldots, n_r$ corresponds to $(n_1-1)!(n_2-1)!\cdots(n_r-1)!$ permutations in S_k. Thus to prove (1.8), it suffices to show

$$\sum_{\tau\leq\sigma: m_i\leq j, 1\leq i\leq \ell} m_1!m_2!\cdots m_\ell!\mu(\tau,\sigma) = (n_1-1)!(n_2-1)!\cdots(n_r-1)!w_j(\sigma), \tag{2.5}$$

where $m_1, m_2, \ldots, m_\ell$ are the block sizes of τ and $n_1, n_2, \ldots, n_r$ are the block sizes of σ. We observe from (2.1) that the sum on the left-hand side of (2.5) can be written as a product of the same sum taken over each block of σ. In view of this and the definition of $w_j(\sigma)$, it suffices to show (2.5) for partition σ with a single block (that is, $\sigma = \mathbf{1}$), as the general case follows from this special case.

Thus we may assume that $\sigma = \mathbf{1}$ and we need to show

$$\sum_{\tau\in\Pi_k: m_i\leq j, 1\leq i\leq \ell} m_1!m_2!\cdots m_\ell!\mu(\tau,\mathbf{1}) = (k-1)!(1-(j+1)1_{(j+1)|k}). \tag{2.6}$$

Using (2.1), the left-hand side can be simplified as

$$\begin{aligned}
\sum_{\tau\leq\mathbf{1}: m_i\leq j, 1\leq i\leq \ell} m_1!m_2!\cdots m_\ell!\mu(\tau,\mathbf{1}) &= \sum_{\sum ia_i=k}\ \sum_{\substack{\tau\in\Pi_k:\mathrm{type}(\tau)=(a_1,\ldots,a_k)\\ a_{j+1}=\cdots=a_k=0}} 1!^{a_1}\cdots k!^{a_k}\mu(\tau,\mathbf{1})\\
&= \sum_{\substack{\sum ia_i=k\\ a_{j+1}=\cdots=a_k=0}} \widetilde{N}(a_1,\ldots,a_k)1!^{a_1}\cdots k!^{a_k}(-1)^{a_1+\cdots+a_k-1}(a_1+\cdots+a_k-1)!\\
&= (k-1)!(1-(j+1)1_{(j+1)|k}).
\end{aligned}$$

The last step is due to Lemma 2.3. This completes the proof. $\square$

Next we prove Theorem 1.9.

Proof of Theorem 1.9. A similar argument as in the previous proof yields

$$|\overline{\mathcal{M}}_d(X)| = \sum_{\tau\in\Pi_k:\tau \text{ has eaxctly } d \text{ blocks}} |\mathcal{M}(X_\tau^\circ)|.$$

Substituting (2.3) and (2.4) into the above equation, we obtain

$$\begin{aligned}
|\overline{\mathcal{M}}_d(X)| &= \sum_{\tau\in\Pi_i} \frac{m_1!m_2!\cdots m_d!}{k!}|X_\tau^\circ|\\
&= \frac{1}{k!}\sum_{\sigma\in\Pi_k}\sum_{\tau\leq\sigma} m_1!m_2!\cdots m_d!\mu(\tau,\sigma)|X_\sigma|,
\end{aligned}$$

Again, as in the previous proof, the proof will be completed if we can show

$$\sum_{\tau\leq\sigma} m_1!m_2!\cdots m_d!\mu(\tau,\sigma) = (n_1-1)!(n_2-1)!\cdots(n_r-1)!\overline{w}_d(\sigma),$$

where $m_1, m_2, \ldots, m_d$ are the block sizes of τ and $n_1, n_2, \ldots, n_r$ are the block sizes of σ, and it can be further reduced to the case that $\sigma = \mathbf{1}$. Thus we need to show

$$\sum_{\tau\in\Pi_k} m_1!m_2!\cdots m_d!\mu(\tau,\mathbf{1}) = (k-1)![x^d](1-(1-x)^k).$$

Again, using (2.1), the left-hand side can be simplified as

$$\begin{aligned}\sum_{\tau\in\Pi_k} m_1!m_2!\cdots m_d!\mu(\tau,\mathbf{1}) &= \sum_{\sum ia_i=k}\ \sum_{\substack{\tau\in\Pi_k:\text{type}(\tau)=(a_1,\ldots,a_k)\\ a_1+\cdots+a_k=d}} 1!^{a_1}\cdots k!^{a_k}\mu(\tau,\mathbf{1})\\ &= \sum_{\substack{\sum ia_i=k\\ a_1+\cdots+a_k=d}} \widetilde{N}(a_1,\ldots,a_k)1!^{a_1}\cdots k!^{a_k}(-1)^{a_1+\cdots+a_k}(a_1+\cdots+a_k-1)!\\ &= (k-1)!(-1)^{d-1}\binom{k}{d}\\ &= (k-1)![x^d](1-(1-x)^k).\end{aligned}$$

where we used Lemma 2.4. This completes the proof. □

The proofs of the weighted versions are omitted since they are completely similar.

3. Applications to partitions over finite fields and zero-sum multisets over $\mathbb{Z}/n\mathbb{Z}$

To illustrate the application of our sieve formula, we investigate two combinatorial problems which are partitions over finite fields and zero-sum multisets over the group of integers modulo n.

3.1. **Partitions over finite fields.** Motivated by the conjecture on polynomials with prescribed range, Muratović-Ribić and Wang [19] considered the problem of counting the number of partitions over finite fields. To be precise, let $\mathbb{F}_q$ be a finite field of q elements and $\mathbb{F}_q^*$ be its multiplicative group. A *partition* of an element $b\in\mathbb{F}_q$ into k parts is a multiset of k nonzero elements in $\mathbb{F}_q^*$ whose sum is b. We denote by $P_k(b)$ the number of partitions of b into k parts over $\mathbb{F}_q$. Using a previous result of Li [10] and the inclusion-exclusion principle, Muratović-Ribić and Wang obtained an explicit formula for $P_k(b)$. They proved the following theorem:

Theorem 3.1 ([19], Theorem 1)**.** *Let k be a non-negative integer, $\mathbb{F}_q$ be a finite field of $q=p^a$ elements, and $b\in\mathbb{F}_q$. Define $v(b)=q-1$ if $b=0$ and $v(b)=-1$ otherwise. The number of partitions of b into k parts over $\mathbb{F}_q$ is given by*

$$P_k(b)=\frac{1}{q}\binom{q+k-2}{k}$$

if $k\not\equiv 0,1 \mod p$,

$$P_k(b)=\frac{1}{q}\binom{q+k-2}{k}+\frac{v(b)}{q}\binom{q/p+k/p-1}{k/p}$$

if $k\equiv 0 \mod p$, and

$$P_k(b)=\frac{1}{q}\binom{q+k-2}{k}-\frac{v(b)}{q}\binom{q/p+k/p-1}{k/p}$$

if $k\equiv 1 \mod p$.

We apply the sieve formula (1.9) to give a direct proof of Theorem 3.1, which avoids using the inclusion-exclusion principle in Muratović-Ribić and Wang's proof. First of all, we state a lemma.

Lemma 3.2 ([11], Lemma 3.1)**.** *Assume $p\mid k$. Let $p(k,i)$ be the number of permutations in S_k of i cycles with the length of its each cycle divisible by p. Then we have*

$$\sum_{i=1}^{k} p(k,i)q^i = k!\binom{q/p+k/p-1}{k/p}.$$

Proof of Theorem 3.1. Denote by $\widetilde{P}_k(b)$ the number of partitions of b into at most k parts in $\mathbb{F}_q$, that is, the number of multisets of k elements in $\mathbb{F}_q$ whose sum is b. It is not hard to see that

$P_k(b) = \widetilde{P}_k(b) - \widetilde{P}_{k-1}(b)$. Thus it is sufficient to determine $\widetilde{P}_k(b)$ which, by definition, is the cardinality of the set $\mathcal{M}(X)$ with X given by

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

Applying the sieve formula (1.9), we have

$$\widetilde{P}_k(b) = \frac{1}{k!} \sum_{\tau \in S_k} |X_\tau|. \tag{3.1}$$

Suppose that τ has a disjoint cycle decomposition $\tau = \tau_1 \tau_2 \cdots \tau_m$ and the length of the cycle τ_i is ℓ_i, $1 \le i \le m$. Then we have

$$X_\tau = \{(x_1, x_2, \ldots, x_m) \in \mathbb{F}_q^m : \ell_1 x_1 + \ell_2 x_2 + \cdots + \ell_m x_m = b\}.$$

If all the ℓ_i's vanish in $\mathbb{F}_q$, that is, $p \mid \ell_i$ for $1 \le i \le m$, then the above linear equation has $(v(b) + 1)q^{m-1}$ solutions and thus $|X_\tau| = (v(b)+1)q^{m-1}$. In particular, in this case, we have $p \mid k$ since $\ell_1 + \ell_2 + \cdots + \ell_m = k$. Otherwise, the linear equation has q^{m-1} solutions and thus $|X_\tau| = q^{m-1}$.

When $p \nmid k$, the ℓ_i's cannot vanish simultaneously, so we have $|X_\tau| = q^{m-1}$, where m is the number of disjoint cycles of τ. Substituting this into (3.1), we conclude that

$$\widetilde{P}_k(b) = \frac{1}{k!} \sum_{i=1}^{k} c(k,i) q^{i-1} = \frac{1}{q} \binom{q+k-1}{k}, \tag{3.2}$$

where $c(k,i)$ denotes the unsigned Stirling number of the first kind which counts the number of permutations in S_k with exactly i cycles, and we used the equality $\sum_{i=0}^{k} c(k,i) x^k = (x+k-1)_k$.

When $p \mid k$, according to the previous discussion, we have

$$\begin{aligned}
\widetilde{P}_k(b) &= \frac{1}{k!} \Big(\sum_{i=1}^{k} (c(k,i) - p(k,i)) q^{i-1} + \sum_{i=1}^{k} p(k,i)(v(b)+1) q^{i-1} \Big) \\
&= \frac{1}{k!} \Big(\frac{1}{q} \sum_{i=1}^{k} c(k,i) q^i + \frac{v(b)}{q} \sum_{i=1}^{k} q^i \Big).
\end{aligned}$$

Using Lemma 3.2, we conclude that

$$\widetilde{P}_k(b) = \frac{1}{q} \binom{q+k-1}{k} + \frac{v(b)}{q} \binom{q/p + k/p - 1}{k/p}.$$

Finally, noting that $P_k(b) = \widetilde{P}_k(b) - \widetilde{P}_{k-1}(b)$, a discussion depending on whether $k \equiv 0 \mod p$ or $k \equiv 1 \mod p$ completes the proof.

□

3.2. **Bijection between necklaces and zero-sum multisets.** In his book [22], Stanley raised a bijective proof problem asking for a bijection between cyclic necklaces with at most two colors and subsets of $\mathbb{Z}/n\mathbb{Z}$ whose elements sum to zero, when n is odd. The problem was answered by Chan [1] recently and he generalized the problem to q-colored necklaces and multisets which is stated as follows.

Problem 3.3. *Consider these two distinct combinatorial objects: (1) the cyclic necklaces of length n with at most q colors, and (2) the multisets of integers modulo n with elements summing to zero and with the multiplicity of each element being strictly less than q. When q and n are coprime, show that these two objects have the same cardinality and construct a bijection between these two objects.*

In [1], Chan gave a proof of the equinumerosity of these two objects which is not bijective. Additionally, when q is a prime power, he constructed a bijection between these two objects by viewing necklaces as cyclic polynomials over the finite field of size q. Note that specializing to $q = 2$ answers the bijective proof problem raised by Stanely. Since the bijection that he constructed relies on finite fields, it fails to work when q is not a prime power. Thus the problem remains open when q is not a prime power.

We would like to use our sieve formula to give another proof of the equinumerosity of these two objects, which is not bijective either. We believe that this proof might give some new insights into this problem. We shall prove the following theorem:

Theorem 3.4. *Let q and n be two coprime positive integers. Let $\mathcal{N}$ denote the set of cyclic necklaces of length n for which the color of each bead is drawn from a color set of size q, and let $\mathcal{F}$ denote the set of multisets of elements in $\mathbb{Z}/n\mathbb{Z}$ with element summing to zero and with the multiplicity of each element being strictly less than q. Then we have*

$$|\mathcal{N}| = |\mathcal{F}| = \frac{1}{n}\sum_{e|n}\phi(e)q^{n/e}, \tag{3.3}$$

where ϕ is Euler's totient function.

Before proving the theorem, we state a lemma.

Lemma 3.5. *Let $N(c_1, c_2 \dots, c_k)$ be the number of permutations in S_k of type $(c_1, c_2, \dots, c_k)$ and let $t_i = (1-(j+1)1_{(j+1)|i})n1_{e|i}$. Then we have*

$$\sum_{\sum ic_i = k} N(c_1, c_2, \dots, c_k)t_1^{c_1}t_2^{c_2}\cdots t_k^{c_k} = k![u^k](1-u^e)^{-n/e}(1-u^{\operatorname{lcm}(e,j+1)})^{\gcd(e,j+1)n/e}.$$

Proof. Substituting $t_i = (1-(j+1)1_{(j+1)|i})n1_{e|i}$ into the exponential generating function (1.5), we see that the left-hand side of the above equation is

$$\begin{aligned}
\text{LHS} &= k![u^k]\exp\Big((1-(j+1)1_{(j+1)|e})n\frac{u^e}{e} + (1-(j+1)1_{(j+1)|2e})n\frac{u^{2e}}{2e} + \cdots\Big)\\
&= k![u^k]\exp\Big(\frac{n}{e}(u^e + \frac{u^{2e}}{2} + \cdots) - \frac{\gcd(e,j+1)n}{e}(u^{\operatorname{lcm}(e,j+1)} + \frac{u^{2\operatorname{lcm}(e,j+1)}}{2} + \cdots)\Big)\\
&= k![u^k]\exp\Big(-\frac{n}{e}\log(1-u^e) + \frac{\gcd(e,j+1)n}{e}\log(1-u^{\operatorname{lcm}(e,j+1)})\Big)\\
&= k!\,[u^k](1-u^e)^{-n/e}(1-u^{\operatorname{lcm}(e,j+1)})^{\gcd(e,j+1)n/e}.
\end{aligned}$$

This completes the proof. □

Proof of Theorem 3.4. The cyclic necklaces of length n with at most q color can be viewed as the equivalence class of functions from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, q\}$, under the action of the cyclic group C_n. Denote the set of the functions by X. Then Burnside's lemma gives

$$|\mathcal{N}| = \frac{1}{n}\sum_{g\in C_n}|X_g|,$$

where X_g denotes the set of elements in X that are fixed by g. Suppose that $g \in C_n$ is an element of order e. Then it is not hard to see that $|X^g| = q^{n/e}$. Since a cyclic group has $\phi(e)$ elements of order e, we conclude that

$$|\mathcal{N}| = \frac{1}{n}\sum_{e|n}\phi(e)q^{n/e}. \tag{3.4}$$

Now we consider the cardinality of set $\mathcal{F}$. We note that $\mathcal{F} = \bigcup_{k=0}^{n(q-1)}\mathcal{M}_{q-1}(X_k)$ is a disjoint union of $\mathcal{M}_{q-1}(X_k)$ with

$$X_k = \{(x_1, x_2, \dots, x_k) \in (\mathbb{Z}/n\mathbb{Z})^k : x_1 + x_2 + \cdots + x_k = 0\}.$$

We will use character sums to calculate $|\mathcal{M}_{q-1}(X_k)|$. Let G denote the additive group $\mathbb{Z}/n\mathbb{Z}$ of order n and let $\widehat{G}$ be the group of all characters on G. Using the fact that the sum of all characters over a nonzero element of G is equal to 0, we have

$$\begin{aligned}|\mathcal{M}_{q-1}(X_k)| &= \sum_{[x_1,x_2,\ldots,x_k]\in\mathcal{M}_{q-1}(G^k)} \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(x_1+x_2+\cdots+x_k)\\ &= \frac{1}{n}\sum_{\chi\in\widehat{G}}\sum_{[x_1,x_2,\ldots,x_k]\in\mathcal{M}_{q-1}(G^k)}\chi(x_1)\chi(x_2)\cdots\chi(x_k).\end{aligned}$$

Applying the sieve formula (1.8), we have

$$|\mathcal{M}_{q-1}(X_k)| = \frac{1}{n}\sum_{\chi\in\widehat{G}}\frac{1}{k!}\sum_{\tau\in S_k} w_j(\tau)\sum_{(x_1,x_2,\ldots,x_k)\in G^k_\tau}\chi(x_1)\chi(x_2)\cdots\chi(x_k). \tag{3.5}$$

Suppose that τ has a disjoint cycle decomposition $\tau = \tau_1\tau_2\cdots\tau_m$ and the length of τ_i is ℓ_i, $1 \le i \le m$. We see from the definition of G^k_τ that

$$\sum_{(x_1,x_2,\ldots,x_k)\in G^k_\tau}\chi(x_1)\chi(x_2)\cdots\chi(x_k) = \prod_{i=1}^{m}\Big(\sum_{x\in G}\chi^{\ell_i}(x)\Big). \tag{3.6}$$

Let e be the order of the character χ. Then we have $\sum_{x\in G}\chi^{\ell_i}(x) = |G| = n$ if $e \mid \ell_i$ and $\sum_{x\in G}\chi^{\ell_i}(x) = 0$ otherwise. This implies that the sum in the right-hand side of (3.6) is equal to n^m if $e \mid \ell_i$ for $1 \le i \le m$ and 0 otherwise; in particular, $e \mid k$ in the former case since $k = \ell_1 + \ell_2 + \cdots + \ell_m$. Substituting this result into (3.5), we see that

$$\begin{aligned}&\frac{1}{k!}\sum_{\tau\in S_k} w_j(\tau)\sum_{(x_1,x_2,\ldots,x_k)\in G^k_\tau}\chi(x_1)\chi(x_2)\cdots\chi(x_k)\\ =&\frac{1}{k!}\sum_{\sum ic_i=k}\sum_{\tau\in S_k:\mathrm{type}(\tau)=(c_1,c_2,\ldots,c_k)}\prod_{i=1}^{k}(1-q1_{q|i})^{c_i}(n1_{e|i})^{c_i}\\ =&\frac{1}{k!}\sum_{\sum ic_i=k} N(c_1,c_2,\ldots,c_k)\prod_{i=1}^{k}(1-q1_{q|i})^{c_i}(n1_{e|i})^{c_i}\\ =&[u^k](1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e},\end{aligned}$$

where we used Lemma 3.5 in the last step. Therefore $|\mathcal{M}_{q-1}(X_k)|$ is simplified as

$$|\mathcal{M}_{q-1}(X_k)| = \frac{1}{n}\sum_{e|n,e|k}\phi(e)[u^k](1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e}.$$

Summing over k, we obtain

$$|\mathcal{F}| = \sum_{k=0}^{n(q-1)}|\mathcal{M}_{q-1}(X_k)| = \frac{1}{n}\sum_{e|n}\phi(e)\sum_{0\le k\le n(q-1):e|k}[u^k](1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e}. \tag{3.7}$$

Set $a = \mathrm{lcm}(e,q)/e$ and $b = \gcd(e,q)$. Then we have

$$\begin{aligned}(1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e} &= (1-u^e)^{-n/e}(1-u^{ae})^{bn/e}\\ &= \frac{(1-u^{ae})^{n/e}}{(1-u^e)^{n/e}}(1-u^{ae})^{(b-1)n/e}\\ &= (1+u^e+u^{2e}+\cdots+u^{(a-1)e})^{n/e}(1-u^{ae})^{(b-1)n/e}.\end{aligned}$$

This implies that

$$\sum_{0\le k\le n(q-1):e|k}[u^k](1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e} = q^{n/e}$$

if $\gcd(e, q) = 1$, and

$$\sum_{0 \le k \le n(q-1): e|k} [u^k](1-u^e)^{-n/e}(1-u^{\mathrm{lcm}(e,q)})^{\gcd(e,q)n/e} = 0$$

otherwise. Substituting this into (3.7), we see that

$$|\mathcal{F}| = \frac{1}{n} \sum_{e|n:\gcd(e,q)=1} \phi(e) q^{n/e}.$$

Since q and n are coprime, $|\mathcal{F}|$ can be simply written as

$$|\mathcal{F}| = \frac{1}{n} \sum_{e|n} \phi(e) q^{n/e},$$

which is exactly the same as (3.4). The proof is completed. $\square$

References

[1] S. Chan, *A bijection between necklaces and multisets with divisible subset sum*, Electron. J. Combin. **26** (2019), no. 1, P1.37.

[2] Q. Cheng, E. Murray, *On deciding deep holes of Reed-Solomon codes*, In: Proceedings of TAMC 2007, In: LNCS, **4484** (2007), 296–305.

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

[4] Q. Cheng, D. Wan, *Complexity of decoding positive-rate Reed-Solomon codes*, IEEE Trans. Inf. Theory **56** (2010), no. 10, 5217–5222.

[5] A. Gács, T. Héger, Z.L. Nagy, D. Pálvölgyi, *Permutations, hyperplanes and polynomials over finite fields*, Finite Fields Appl. **16** (2010), no. 5, 301–314.

[6] M. Kosters, *The subset problem for finite abelian groups*, J. Combin. Theory Ser. A **120** (2013), no. 3, 527–530.

[7] J. Li, *On the average sensitivity of the weighted sum function*, Inform. Process. Lett. **112** (2012), no. 4, 143–148.

[8] J. Li, *On the Odlyzko-Stanley enumeration problem and Waring's problem over finite fields*, J. Number Theory **133** (2013), no. 7, 2267–2276.

[9] J. Li, *On the Borwein conjecture*, Int. J. Number Theory, **16** (2020), no. 5, 1053–1066.

[10] J. Li, D. Wan, *On the subset problem over finite fields*, Finite Fields Appl. **14** (2008), no. 4, 911–929.

[11] J. Li, D. Wan, *A new sieve for distinct coordinate counting*, Sci. China Math. **53** (2010), no. 9, 2351–2362.

[12] J. Li, D. Wan, *Counting subset sums of finite abelian groups*, J. Combin. Theory Ser. A **119** (2012), no. 1, 170–182.

[13] J. Li, D. Wan, *Counting polynomial subset sums*, Ramanujan J. **47** (2018), no. 1, 67–84.

[14] J. Li, D. Wan, *Distance distribution problems in Reed-Solomon codes*, IEEE Trans. Inf. Theory **66** (2020), no. 5, 2743–2750.

[15] J. Li, D. Wan, J. Zhang, *On the minimum distance of elliptic curve codes*, In: Proceedings of the IEEE International Symposium on Information Theory (2015), 2391–2395.

[16] Y. Li, D. Wan *On error distance of Reed-Solomon codes*, Sci. China Ser. A, **51** (2008), no. 11, 1982–1988.

[17] J.H. van Lint, R.M. Wilson, A course in combinatorics, Second edition, Cambridge University Press, Cambridge, 2001.

[18] A. Muratović-Ribić, Q. Wang, *On a conjecture of polynomials with prescribed range*, Finite Fields Appl. **18** (2012), no. 4, 728–737.

[19] A. Muratović-Ribić, Q. Wang, *Partitions and compositions over finite fields*, Electron. J. Combin. **20** (2013), no. 1, P34.

[20] A.M. Odlyzko, R.P. Stanley, *Enumeration of power sums modulo a prime*, J. Number Theory **10** (1978), no. 2, 263–272.

[21] G.-C. Rota, *On the foundations of combinatorial theory. I. Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete **2** (1964), no. 4, 340–368.

[22] R.P. Stanley, Enumerative Combinatorics, vol. 1, Cambridge University Press, Cambridge, 1997.

[23] G. Zhu, D. Wan, *An asymptotic formula for counting subset sums over subgroups of finite fields*, Finite Fields Appl. **18** (2012), no. 1, 192-209.

Department of Mathematics, Shanghai Jiao Tong University, Shanghai, P.R. China
Email address: lijiyou@sjtu.edu.cn

Department of Mathematics, City University of Hong Kong, Kowloon Tong, Hong Kong
Email address: xianyu3-c@my.cityu.edu.hk