A bijection between necklaces and multisets with divisible subset sum

Swee Hong Chan

Department of Mathematics
Cornell University
New York, U.S.A.

sweehong@math.cornell.edu

Submitted: Apr 19, 2018; Accepted: Feb 4, 2019; Published: Mar 8, 2019

Abstract

Consider these two distinct combinatorial objects: (1) the necklaces of length n with at most q colors, and (2) the multisets of integers modulo n with subset sum divisible by n and with the multiplicity of each element being strictly less than q. We show that these two objects have the same cardinality if q and n are mutually coprime. Additionally, when q is a prime power, we construct a bijection between these two objects by viewing necklaces as cyclic polynomials over the finite field of size q. Specializing to $q = 2$ answers a bijective problem posed by Richard Stanley (Enumerative Combinatorics Vol. 1 Chapter 1, Problem 105(b)).

Mathematics Subject Classifications: 05A19, 05E99

1 Introduction

Let q be and n be two coprime positive integers. The main characters of this paper are the following two combinatorial objects:

- The set $\mathcal{N}$ of necklaces (i.e., equivalent up to cyclic rotations) of length n for which the color of each bead is drawn from a color set of size q.
- The set $\mathcal{F}$ of functions $f : \mathbb{Z}_n \to \{0, 1, \dots, q-1\}$ for which their (linearly) weighted sum is divisible by n, i.e.,

$$\mathcal{F} := \left\{ f \;\middle|\; \sum_{z \in \mathbb{Z}_n} z\, f(z) = 0 \pmod{n} \right\},$$

where $\mathbb{Z}_n$ denotes the ring of integers modulo n.

Equivalently, $\mathcal{F}$ is the set of multisets of $\mathbb{Z}_n$ with subset sum divisible by n and with the multiplicity of each element being at most $q-1$. The set $\mathcal{F}$ for the case $q = 2$ has been studied in different areas of mathematics, such as coding theory [SY72], number theory [OS78], and toric arrangements [ACH15, AC17].

It was known that $\mathcal{N}$ and $\mathcal{F}$ have the same cardinality when $q = 2$ (see [Sta12, Problem 105(b) Chapter 1]). We extend this result to all values of q.

Theorem 1.1. *Let q and n be two coprime positive integers. Then*

$$|\mathcal{N}| = |\mathcal{F}| = \sum_{I\subseteq\{1,\ldots,m\}} \frac{\gcd(n, \gcd(s_i)_{i\in I})}{n} \prod_{i\in I}(q^{\ell_i} - 1),$$

where m, s_i, and ℓ_i are as in Definition 2.1.

We remark that Theorem 1.1 gives a new expression for the cardinality of $\mathcal{N}$ and $\mathcal{F}$. This expression is different from the formulas in [KP93, Theorem 11] and [Kus14, Section 4.2], which involve the Möbius function and the Euler's totient function. We also remark that the condition that n and q are coprime is necessary, as there are examples for which $|\mathcal{N}|$ is not equal to $|\mathcal{F}|$ when $\gcd(n, q) > 1$. One such example is when $n = q = 2$, which gives us $|\mathcal{N}| = 3$ and $|\mathcal{F}| = 2$.

The proof of Stanley for the case $q = 2$ is not bijective in nature, and neither is our proof of Theorem 1.1. In [Sta12, Problem 105(b) Chapter 1], Stanley asked for a bijective proof of Theorem 1.1 for the case $q = 2$. We answer this question here by constructing a bijection between the two sets when q is a prime power.

Our bijection starts by viewing necklaces with q colors as cyclic polynomials over the finite field $\mathbb{F}_q$. Each necklace can then be associated to a coset of a finite abelian group by taking the remainder of the division of the cylic polynomial by irreducible factors of $X^n - 1$. On the other hand, a function in $\mathcal{F}$ can be associated to an element of the same finite abelian group by evaluating the function on the cyclotomic cosets of $\mathbb{Z}_n$. It will follow from the construction that, for any given necklace, the corresponding coset contains exactly one group element that is associated to a function in $\mathcal{F}$. We take this unique function as the image of the necklace under our bijection. The full definition of this bijection is given in §4.

Theorem 1.2. *Let q be a prime power, and let n be a positive integer that is coprime to q. Then the map $\widehat{\psi} : \mathcal{N} \to \mathcal{F}$ in Definition 4.12 is a bijection.*

See Example 4.13 for an example of the bijection $\widehat{\psi}$ when $q = 2$ and $n = 3$. A bijection for general values of q remains an open problem.

This paper is structured as follows. In §2, we review algebraic tools that will be used in the proofs of the main theorems. In §3, we present a proof of Theorem 1.1 in §3. In §4, we present a proof of Theorem 1.2. In §5, we present two open bijective problems that extend Theorem 1.2.

2 Preliminaries

In this section, we review algebraic tools that will be used in the proof of Theorem 1.1 and Theorem 1.2.

Throughout this paper, q and n are two positive integers such that $\gcd(n, q) = 1$.

Definition 2.1. Consider the equivalence relation on $\mathbb{Z}_n$ that takes all multiplications by q as equivalent. Fix integers $s_1, s_2, \ldots, s_m$ as the representatives of the equivalence classes of this relation. The *cyclotomic cosets* $S_1, \ldots, S_m$ of $\mathbb{Z}_n$ are

$$S_i := \{s_i, q\, s_i, q^2 s_i, \ldots, q^{\ell_i - 1} s_i\} \qquad (i \in \{1, \ldots, m\}),$$

where ℓ_i is the smallest positive integer such that $q^{\ell_i} s_i = s_i$ (mod n). △

When q is a prime power, we view the set of necklaces $\mathcal{N}$ from the following algebraic perspective. Let $\mathcal{Q}$ be the quotient

$$\mathcal{Q} := \frac{\mathbb{F}_q[X]}{(X^n - 1)},$$

of the polynomial ring over the finite field $\mathbb{F}_q$ of order q in a single variable X by the ideal generated by $X^n - 1$. Each element of $\mathcal{Q}$ corresponds to an n-character string over an alphabet of size q by taking its coefficient vector. The set $\mathcal{N}$ can then be viewed as

$$\mathcal{N} := \left\{ \{\alpha, X\alpha, \ldots, X^{n-1}\alpha\} \;\middle|\; \alpha \in \mathcal{Q} \right\},$$

the set of equivalence classes of the relation in $\mathcal{Q}$ that takes all multiplications by X as equivalent.

Fix a primitive n-th root of unity ω in the algebraic closure of $\mathbb{F}_q$. Such ω exists because q is coprime to n.

Definition 2.2. Let q be a prime power. Let $P_1, \ldots, P_m$ be the irreducible factors of $X^n - 1$ over the field $\mathbb{F}_q$. That is, for any $i \in \{1, \ldots, m\}$,

$$P_i := \prod_{k \in S_i} (X - \omega^k).$$

We denote by G_i the set

$$G_i := (\mathcal{Q}/P_i\mathcal{Q})^\times,$$

of nonzero elements of the quotient ring $\mathcal{Q}/P_i\mathcal{Q}$. △

Definition 2.3. Let q be a prime power. For any $\alpha \in \mathcal{Q}$, we denote by $\alpha_i := \alpha \mod P_i$ the image of α in $\mathcal{Q}/P_i\mathcal{Q}$ under the quotient map. In particular, X_i is the image of X in $\mathcal{Q}/P_i\mathcal{Q}$. △

We now present examples of the objects discussed above for the case that $q = 2$ and $n = 3$. This case will be our running example throughout this paper.

Example 2.4. Let $q = 2$ and $n = 3$. We make the following choices of cyclotomic cosets from Definition 2.1:

$$s_1 = 0, \quad S_1 = \{0\}; \qquad \text{and} \qquad s_2 = 1, \quad S_2 = \{1, 2\}.$$

We represent a function $f : \mathbb{Z}_3 \to \{0, 1\}$ as the set $\{z \in \mathbb{Z}_3 \mid f(z) = 1\}$. In this notation, the sets $\mathcal{N}$ and $\mathcal{F}$ are given by

$$\begin{aligned}\mathcal{N} =& \{\{0\}, \{1, X, X^2\}, \{1 + X, X + X^2, 1 + X^2\}, \{1 + X + X^2\}\},\\ \mathcal{F} =& \{\varnothing, \{0\}, \{1, 2\}, \{0, 1, 2\}\}.\end{aligned}$$

The polynomials $P_i \in \mathcal{Q}$ from Definition 2.2 are given by

$$P_1 = 1 + X; \qquad P_2 = 1 + X + X^2. \qquad \triangle$$

We refer to [Wan03] for the proofs of the following properties of $\mathcal{Q}/P_i\mathcal{Q}$ and G_i.

Lemma 2.5 ([Wan03, Section 9])**.** *Let q be a prime power, and let n be a positive integer coprime to q. For any $i \in \{1, \ldots, m\}$,*

(i) *$\mathcal{Q}/P_i\mathcal{Q}$ is a finite field of order q^{ℓ_i}.*

(ii) *G_i is a cyclic group of order $q^{\ell_i} - 1$ under multiplication.*

(iii) *X_i is an element of G_i with multiplicative order $\frac{n}{\gcd(n, s_i)}$.* $\square$

We will use the following versions of the Chinese remainder theorem in the proof of Theorem 1.1 and Theorem 1.2.

Theorem 2.6 (Chinese remainder theorem [Hun80, Theorem 2.25])**.**

(i) *Let n be a positive integer with prime factorization $n = p_1^{a_1} \ldots p_\ell^{a_\ell}$. Then the following map is an isomorphism:*

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_\ell^{a_\ell}\mathbb{Z}\\ x \bmod n &\mapsto (x \bmod p_1^{a_1}, \ldots, x \bmod p_\ell^{a_\ell}).\end{aligned}$$

(ii) *Let q be a prime power and let n be a positive integer coprime to q. Then the following map is an isomorphism:*

$$\begin{aligned}&\mathcal{Q} \to \mathcal{Q}/P_1\mathcal{Q} \times \cdots \times \mathcal{Q}/P_m\mathcal{Q}\\ &\alpha \mapsto (\alpha \bmod P_1, \ldots, \alpha \bmod P_m).\end{aligned} \qquad \square$$

The following lemma is a consequence of Theorem 2.6(i).

Lemma 2.7. *Let n and $d_1, \ldots, d_k$ be positive integers. Then there exists a group automorphism $\phi : \prod_{i=1}^k \mathbb{Z}_{\frac{n}{\gcd(n,d_i)}} \to \prod_{i=1}^k \mathbb{Z}_{\frac{n}{\gcd(n,d_i)}}$ such that*

$$d_1 h_1 + \cdots + d_k h_k = \gcd(n, d_1, \ldots, d_k) \pmod{n},$$

where h_i is the i-th coordinate of $\phi(1, \ldots, 1)$.

Proof. By the Chinese remainder theorem (Theorem 2.6(i)), the group and the sum in the lemma can be decomposed into their corresponding prime parts. Therefore, it suffices to prove the lemma for when n is a prime power p^a.

For any $i \in \{1, \ldots, k\}$, let a_i be the integer such that $p^{a_i} = \gcd(n, d_i)$, and let t_i be an integer coprime to n such that $t_i d_i = \gcd(n, d_i) \pmod{n}$. Note that $a_i \leqslant a$ by definition. By reindexing if necessary, we can without loss of generality assume that $a_1 \leqslant \cdots \leqslant a_k$.

Let e_i be the group element $(\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$. We define $\phi(e_i)$ to be

$$\phi(e_i) := \begin{cases} t_1 e_1 - \sum_{j=2}^{k} e_j & \text{if } i = 1; \\ e_i & \text{if } i \in \{2, \ldots, k\}. \end{cases}$$

We claim that ϕ can be extended to a group automorphism of $\prod_{i=1}^k \mathbb{Z}_{\frac{n}{\gcd(n,d_i)}}$.

Since a_1 is chosen to be the minimum value of a_i's, we have

$$\frac{n}{\gcd(n, d_i)}\, \phi(e_i) = \begin{cases} t_1 \left(p^{a-a_1} e_1\right) - \sum_{j=2}^{k} p^{a_j - a_1} \left(p^{a-a_j} e_j\right) = 0 & \text{if } i = 1; \\ p^{a-a_i} e_i = 0 & \text{if } i \in \{2, \ldots, k\}, \end{cases}$$

and so ϕ extends to a group homomorphism.

Tha map ϕ is an automorphism since the corresponding matrix is triangular and all the diagonal entries are coprime to n. Finally, we have

$$\phi(1, \ldots, 1) = \sum_{j=1}^{k} \phi(e_i) = t_1 e_1 - \sum_{j=2}^{k} e_j + \sum_{j=2}^{k} e_j = t_1 e_1 = (t_1, 0, \ldots, 0),$$

which implies that

$$d_1 h_1 + \ldots + d_k h_k = d_1 t_1 = \gcd(n, d_1) \pmod{n} = \gcd(n, d_1, \ldots, d_k) \pmod{n},$$

where the last equality is a consequence of a_1 being the minimum value of a_i's. This proves the claim. $\square$

We will use the following version of Dirichlet's prime number theorem in the proof of Theorem 1.1.

Theorem 2.8 ([JJ98, Dirichlet's prime number theorem])**.** *Let a and b be two coprime positive integers. Then there are infinitely many positive integers k such that $a + kb$ is a prime number.* $\square$

3 Proof of Theorem 1.1

In this section, we present a proof of Theorem 1.1, starting with the case that q is a prime power.

Let m and S_i be as in Definition 2.1, and P_i be as in Definition 2.2. For any function $f : \mathbb{Z}_n \to \{0, 1, \dots, q-1\}$, the *level set* $L_{q-1}(f)$ of f at $q-1$ is the set $\{z \in \mathbb{Z}_n \mid f(z) = q-1\}$.

Definition 3.1. Let q be a prime power. For any $I \subseteq \{1, \dots, m\}$, the sets $\mathcal{N}_I$ and $\mathcal{F}_I$ are given by

$$\mathcal{N}_I := \left\{ \{\alpha, X\alpha, \dots, X^{n-1}\alpha\} \in \mathcal{N} \;\middle|\; P_i \text{ divides } \alpha \text{ iff } i \notin I \right\},$$
$$\mathcal{F}_I := \{f \in \mathcal{F} \mid L_{q-1}(f) \cap S_i = S_i \text{ iff } i \notin I\}. \qquad \triangle$$

By definition $\{\mathcal{N}_I\}_{I\subseteq\{1,\dots,m\}}$ and $\{\mathcal{F}_I\}_{I\subseteq\{1,\dots,m\}}$ form a partition of $\mathcal{N}$ and $\mathcal{F}$, respectively.

Example 3.2. Continuing from Example 2.4, the sets $\mathcal{F}_I$ and $\mathcal{N}_I$ from Definition 3.1 are given by

$$\begin{aligned}
&\mathcal{N}_\varnothing = \{\{0\}\}, && \mathcal{F}_\varnothing = \{\{0,1,2\}\};\\
&\mathcal{N}_{\{1\}} = \{\{1 + X + X^2\}\}, && \mathcal{F}_{\{1\}} = \{\{1,2\}\};\\
&\mathcal{N}_{\{2\}} = \{\{1 + X, X + X^2, 1 + X^2\}\}, && \mathcal{F}_{\{2\}} = \{\{0\}\};\\
&\mathcal{N}_{\{1,2\}} = \{\{1, X, X^2\}\}, && \mathcal{F}_{\{1,2\}} = \{\varnothing\}. \qquad \triangle
\end{aligned}$$

We now show that $\mathcal{N}_I$ and $\mathcal{F}_I$ have the same cardinality for any $I \subseteq \{1, \dots, m\}$.

Let s_i and ℓ_i be as in Definition 2.1.

Lemma 3.3. *Let q be a prime power, let n be a positive integer coprime to q, and let $I \subseteq \{1, \dots, m\}$. Then*

$$|\mathcal{N}_I| = \frac{\gcd(n, \gcd(s_i)_{i\in I})}{n} \prod_{i\in I} (q^{\ell_i} - 1).$$

Proof. Recall the definition of G_i from Definition 2.2 and the definition of α_i and X_i from Definition 2.3. In particular, if α is an element of $\mathcal{Q}$ that is not divisible by P_i, then α_i is contained in G_i. Consider the map

$$\begin{aligned}
\xi : \{\alpha \in \mathcal{Q} \mid P_i \text{ divides } \alpha \text{ iff } i \notin I\} &\to \prod_{i\in I} G_i\\
\alpha &\mapsto (\alpha_i)_{i\in I}.
\end{aligned}$$

The map ξ is a bijection by Theorem 2.6(ii).

Denote by C_I the cyclic subgroup of $\prod_{i\in I} G_i$ generated by $(X_i)_{i\in I}$. Note that $\mathcal{N}_I$ is in bijection with cosets of C_I in $\prod_{i\in I} G_i$ by the map ξ. Hence we have

$$|\mathcal{N}_I| = \left|\prod_{i\in I} G_i \Big/ C_I\right| = \frac{1}{|C_I|}\prod_{i\in I}|G_i|. \tag{1}$$

On the other hand, we also have

$$\begin{aligned}
|G_i| &= q^{\ell_i} - 1 \qquad \text{(by Lemma 2.5(ii))};\\
|C_I| &= \min\{k>0 \mid (X_i)^k \text{ is the identity element of } G_i \text{ for all } i\in I\}\\
&= \operatorname{lcm}\left(1, \left(\frac{n}{\gcd(n,s_i)}\right)_{i\in I}\right) \qquad \text{(by Lemma 2.5(iii))}\\
&= \frac{n}{\gcd(n,\gcd(n,s_i)_{i\in I})}.
\end{aligned}$$

The conclusion of the lemma now follows from (1). □

Lemma 3.4. *Let q and n be two coprime positive integers, and let $I \subseteq \{1,\dots,m\}$. Then*

$$|\mathcal{F}_I| = \frac{\gcd(n,\gcd(s_i)_{i\in I})}{n}\prod_{i\in I}(q^{\ell_i}-1).$$

Proof. Let $\mathcal{E}_I$ denote the set

$$\mathcal{E}_I := \{f:\mathbb{Z}_n \to \{0,1,\dots,q-1\} \mid L_{q-1}(f)\cap S_i = S_i \text{ iff } i\notin I\}.$$

Let $\eta_I : \mathcal{E}_I \to \prod_{i\in I}\mathbb{Z}_{q^{\ell_i}-1}$ be the map defined by

$$f \mapsto \left(\sum_{j=0}^{\ell_i-1} q^j f(q^j s_i) \mod q^{\ell_i}-1\right)_{i\in I}.$$

The map η_I is surjective by the definition of $\mathcal{E}_I$.

Let f be any function in $\mathcal{E}_I$. For any $i\in I$, the sum $\sum_{j=0}^{\ell_i-1} q^j f(q^j s_i)$ is strictly less than $q^{\ell_i}-1$ since $L_{q-1}(f)\cap S_i \neq S_i$. This implies that the i-th coordinate of $\eta_I(f)$ determines $f(s_i),\dots,f(q^{\ell_i-1}s_i)$ for any $i\in I$. Furthermore, we have $(f(s_i),\dots,f(q^{\ell_i-1}s_i)) = (q-1,\dots,q-1)$ for any $i\notin I$ by the definition of $\mathcal{E}_I$. Therefore, we conclude that η_I is an injective map.

Let ζ_I be the map defined by

$$\begin{aligned}
\zeta_I : \prod_{i\in I}\mathbb{Z}_{q^{\ell_i}-1} &\to \mathbb{Z}_n\\
(z_i)_{i\in I} &\mapsto \sum_{i\in I} s_i z_i \mod n.
\end{aligned}$$

The map ζ_I is a well defined group homomorphism as n divides $s_i(q^{\ell_i}-1)$ for all $i \in \{1,\dots,m\}$ by Definition 2.1. Furthermore, by the definition of gcd, the image of ζ_I is $\gcd(n, \gcd(s_i)_{i\in I})\mathbb{Z}_n$.

Now note that, for any $f \in \mathcal{E}_I$,

$$\begin{aligned}\sum_{z\in\mathbb{Z}_n} zf(z) =& \sum_{i\in I}\sum_{j=0}^{\ell_i-1} q^j s_i f(q^j s_i) + \sum_{i\notin I}(q^{\ell_i}-1)s_i \\ =& \sum_{i\in I} s_i \sum_{j=0}^{\ell_i-1} q^j f(q^j s_i) \pmod n \\ =& \zeta_I(\eta_I(f)).\end{aligned}$$

Since η_I is a bijection, it then follows from the definition of $\mathcal{F}_I$ (Definition 3.1) that the kernel of ζ_I is equal to $\eta_I(\mathcal{F}_I)$.

Combining all those observations, we conclude that

$$\begin{aligned}|\mathcal{F}_I| =& |\eta_I(\mathcal{F}_I)| = |\ker(\zeta_I)| = \frac{|\prod_{i\in I}\mathbb{Z}_{q^{\ell_i}-1}|}{|\gcd(n,\gcd(s_i)_{i\in I})\mathbb{Z}_n|} \\ =& \frac{\gcd(n,\gcd(s_i)_{i\in I})}{n}\prod_{i\in I}(q^{\ell_i}-1),\end{aligned}$$

as desired. □

We now complete the proof of Theorem 1.1.

Proof of Theorem 1.1. Fix an arbitrary positive integer n. Let $r \in \{0,\dots,n-1\}$ be such that $\gcd(n,r)=1$. Let x be a variable, and let $q = xn+r$ throughout this proof. Note that $\gcd(n,r)=\gcd(n,q)=1$.

Since the integers m, s_i, and ℓ_i from Definition 2.1 depend only on n and r, we have the function

$$x \mapsto \sum_{I\subseteq\{1,\dots,m\}} \frac{\gcd(n,\gcd(s_i)_{i\in I})}{n}\prod_{i\in I}((xn+r)^{\ell_i}-1) \tag{2}$$

is a polynomial of x.

By Lemma 3.3, Lemma 3.4, and the fact that $\{\mathcal{N}_I\}_{I\subseteq\{1,\dots,m\}}$ and $\{\mathcal{F}_I\}_{I\subseteq\{1,\dots,m\}}$ form a partition of $\mathcal{N}$ and $\mathcal{F}$ respectively, we have that $|\mathcal{N}|$ and $|\mathcal{F}|$ are equal to the polynomial in (2) when $q = xn+r$ is a prime power. Since $\gcd(n,r)=1$, we have by Theorem 2.8 that there are infinitely many positive integers x for which $xn+r$ is a prime. Hence it suffices to show that $|\mathcal{N}|$ and $|\mathcal{F}|$ are polynomials of x.

For any $i \in \{1,\dots,n\}$, let $\mathrm{col}(i)$ be the number of necklaces of length n with colors chosen from $\{0,\dots i-1\}$, and such that all i colors are used. Then

$$|\mathcal{N}| = \sum_{i=1}^{n}\mathrm{col}(i)\binom{q}{i} = \sum_{i=1}^{n}\frac{\mathrm{col}(i)}{i!}\prod_{j=0}^{i-1}(xn+r-j).$$

This shows that $|\mathcal{N}|$ is a polynomial of x.

Let V denote the set

$$V := \left\{ R \in \{0,\dots,n-1\}^{\mathbb{Z}_n} \;\middle|\; \sum_{z\in\mathbb{Z}_n} zR_z = 0 \pmod{n} \right\}.$$

We then have

$$\begin{aligned}
|\mathcal{F}| &= \sum_{R\in V} \{f : \mathbb{Z}_n \to \{0,1,\dots,q-1\} \;\mid\; f(z) = R_z \pmod{n} \text{ for all } z \in \mathbb{Z}_n\} \\
&= \sum_{R\in V} \prod_{z\in\mathbb{Z}_n} |\{k \geqslant 0 \mid kn + R_z < q\}| \\
&= \sum_{R\in V} (x+1)^{|\{z\in\mathbb{Z}_n \,\mid\, R_z<r\}|}\, x^{|\{z\in\mathbb{Z}_n \,\mid\, R_z\geqslant r\}|}.
\end{aligned}$$

This shows that $|\mathcal{F}|$ is a polynomial of x. This completes the proof. □

4 Proof of Theorem 1.2

In this section, we present a proof of Theorem 1.2. Throughout this section, q is a prime power and n is a positive integer that is coprime to q.

Let $\mathcal{Q}$ be as defined in Section 2, and let $\mathcal{E}$ be the set of all functions from $\mathbb{Z}_n$ to $\{0,1,\dots,q-1\}$. Suppose that there exists a map $\psi : \mathcal{Q} \to \mathcal{E}$ that satisfies the following conditions:

(C1) The map ψ is a bijection from $\mathcal{Q}$ to $\mathcal{E}$; and

(C2) For any $\alpha \in \mathcal{Q}$ there exists a unique $\beta \in \{\alpha, X\alpha, \dots, X^{n-1}\alpha\}$ such that $\psi(\beta)$ is contained in $\mathcal{F}$.

We could then define the map $\widehat{\psi} : \mathcal{N} \to \mathcal{F}$ by

$$\{\alpha, X\alpha, \dots, X^{n-1}\alpha\} \mapsto \psi(\beta).$$

It would follow that $\widehat{\psi}$ is a bijection between $\mathcal{N}$ and $\mathcal{F}$, which would prove Theorem 1.2. In this section, we will construct a map $\psi : \mathcal{Q} \to \mathcal{E}$ that satisfies (C1) and (C2).

Recall the definition of m, s_i, and ℓ_i from Definition 2.1, the definition of G_i from Definition 2.2, and the definition of X_i from Definition 2.3.

Let $i \in \{1,\dots,m\}$. Since G_i is a cyclic group of order $q^{\ell_i} - 1$ (Lemma 2.5(ii)) and X_i is an element of G_i with order $\frac{n}{\gcd(n,s_i)}$ (Lemma 2.5(iii)), the group G_i contains a group generator such that X_i is $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$-th power of this generator.

Definition 4.1. For any $i \in \{1,\dots,m\}$, let g_i be a group generator of G_i such that X_i is the $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$-th power of g_i. △

Recall the definition of P_i from Definition 2.2 and the definition of α_i from Definition 2.3.

Definition 4.2 (Discrete logarithm)**.** Let $i \in \{1, \ldots, m\}$, and let α be an element of $\mathcal{Q}$ not divisible by P_i. The *discrete logarithm* $\log_{g_i}(\alpha)$ is the smallest non-negative integer k such that $\alpha_i = g_i^k$ in G_i. △

By Lemma 2.5(ii), the integer $\log_{g_i}(\alpha)$ is contained in $\{0, \ldots, q^{\ell_i} - 2\}$.

Definition 4.3. Let $i \in \{1, \ldots, m\}$, and let α be an element of $\mathcal{Q}$ not divisible by P_i. We denote by $a_i(\alpha)$ and $b_i(\alpha)$ the quotient and the remainder of the division of $\log_{g_i}(\alpha)$ by $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$, respectively. △

In particular, the nonnegative integers $a_i(\alpha)$ is strictly less than $\frac{n}{\gcd(n,s_i)}$ and $b_i(\alpha)$ is strictly less than $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$. We compute these integers for the case $n = 3$ below.

Example 4.4. Continuing from Example 3.2, we make the following choices of g_1 and g_2 that satisfy the condition in Definition 4.1:

$$g_1 = 1 \bmod 1 + X \quad \text{and} \quad g_2 = X \bmod 1 + X + X^2.$$

Note that $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n} = 1$ for $i \in \{1, 2\}$; we remark that this equality is special to this example and is false for large values of n and q.

The following is the value of $\log_{g_1}(\alpha)$, $a_1(\alpha)$ and $b_1(\alpha)$ for different α's:

- If $\alpha = 1 \pmod{1 + X}$, then
$$\log_{g_1}(\alpha) = 0; \qquad a_1(\alpha) = 0; \qquad b_1(\alpha) = 0.$$

The following is the value of $\log_{g_2}(\alpha)$, $a_2(\alpha)$ and $b_2(\alpha)$ for different α's:

- If $\alpha = 1 \pmod{1 + X + X^2}$, then
$$\log_{g_2}(\alpha) = 0; \qquad a_2(\alpha) = 0; \qquad b_2(\alpha) = 0.$$
- If $\alpha = X \pmod{1 + X + X^2}$, then
$$\log_{g_2}(\alpha) = 1; \qquad a_2(\alpha) = 1; \qquad b_2(\alpha) = 0.$$
- If $\alpha = 1 + X \pmod{1 + X + X^2}$, then
$$\log_{g_2}(\alpha) = 2; \qquad a_2(\alpha) = 2; \qquad b_2(\alpha) = 0.$$ △

Lemma 4.5. *Let q be a prime power, let n be a positive integer coprime to q, and let $i \in \{1, \ldots, m\}$. Then*

(i) $a_i(X) = 1$ *and* $b_i(X) = 0$*; and*

(ii) *For any* $k \geqslant 0$ *and any* $\alpha \in \mathcal{Q}$*,*

$$\begin{aligned} a_i(X^k\alpha) &= k + a_i(\alpha) \quad \left(\operatorname{mod} \frac{n}{\gcd(n, s_i)}\right); \text{ and} \\ b_i(X^k\alpha) &= b_i(\alpha). \end{aligned}$$

Proof. Part (i) follows directly from Definition 4.1 and Definition 4.3.

By Definition 4.2, we have for any non-negative integer k and any $\alpha \in \mathcal{Q}$ that

$$\begin{aligned} \log_{g_i}(X^k\alpha) &= \log_{g_i}(\alpha) + k\log_{g_i}(X) \pmod{q^{\ell_i} - 1} \\ &= (k + a_i(\alpha))\frac{(q^{\ell_i} - 1)\gcd(n, s_i)}{n} + b_i(\alpha) \pmod{q^{\ell_i} - 1}. \end{aligned}$$

Part (ii) now follows from Definition 4.3. □

Definition 4.6. Let I be a subset of $\{1, \ldots, m\}$. Let ϕ_I be a group automorphism of $\prod_{i \in I} \mathbb{Z}_{\frac{n}{\gcd(n,s_i)}}$ that satisfies

$$\sum_{i \in I} s_i h_{i,I} = \gcd(n, \gcd(s_i)_{i \in I}) \pmod{n}, \tag{3}$$

where $h_{i,I}$ is the i-th coordinate of $\phi_I(1, \ldots, 1)$. The function ϕ_I exists for any $I \subseteq \{1, \ldots, m\}$ by Lemma 2.7. △

We present an explicit example of the function ϕ_I for the case $n = 3$ below.

Example 4.7. Continuing from Example 4.4, we choose ϕ_I to be the identity map on $\prod_{i \in I} \mathbb{Z}_{\frac{n}{\gcd(n,s_i)}}$ for any $I \subseteq \{1, 2\}$. The map ϕ_I satisfies (3) by the following computation:

- When $I = \varnothing$, the condition in (3) is vacuously true.
- When $I = \{1\}$, we have

$$s_1 h_{1,\{1\}} = 0 \cdot 1 = 3 \pmod{3}.$$

- When $I = \{2\}$, we have

$$s_2 h_{2,\{2\}} = 1 \cdot 1 = 1 \pmod{3}.$$

- When $I = \{1, 2\}$,we have

$$s_1 h_{1,\{1,2\}} + s_2 h_{2,\{1,2\}} = 0 \cdot 1 + 1 \cdot 1 = 1 \pmod{3}.$$ △

Recall that $L_{q-1}(f) = \{z \in \mathbb{Z}_n \mid f(z) = q-1\}$. For any $I \subseteq \{1, \ldots, m\}$, write

$$\mathcal{Q}_I := \left\{ \alpha \in \mathcal{Q} \;\middle|\; P_i \text{ divides } \alpha \text{ iff } i \notin I \right\};$$
$$\mathcal{E}_I := \{ f \in \mathcal{E} \mid L_{q-1}(f) \cap S_i = S_i \text{ iff } i \notin I \}.$$

By definition $\{\mathcal{Q}_I\}_{I \subseteq \{1,\ldots,m\}}$ and $\{\mathcal{E}_I\}_{I \subseteq \{1,\ldots,m\}}$ form a partition of $\mathcal{Q}$ and $\mathcal{E}$, respectively.

Let $i \in I$, and let α be any element of Q_I. We denote by $\phi_{i,I}(\alpha)$ the i-th coordinate of $\phi_I((a_i(\alpha))_{i \in I})$, which corresponds to a nonnegative integer strictly less than $\frac{n}{\gcd(n,s_i)}$.

Since $b_i(\alpha)$ is a nonnegative integer strictly less than $\frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$ and $\phi_{i,I}(\alpha)$ is a nonnegative integer strictly less than $\frac{n}{\gcd(n,s_i)}$, we have

$$0 \leqslant b_i(\alpha) \frac{n}{\gcd(n, s_i)} + \phi_{i,I}(\alpha) < q^{\ell_i} - 1. \tag{4}$$

We denote by $c_{i,0}(\alpha), \ldots, c_{i,\ell_i-1}(\alpha) \in \{0, \ldots, q-1\}$ the unique integers that satisfy

$$\sum_{j=0}^{\ell_i - 1} c_{i,j}(\alpha)\, q^j = b_i(\alpha) \frac{n}{\gcd(n, s_i)} + \phi_{i,I}(\alpha). \tag{5}$$

By (4), the sequence of integers $(c_{i,0}, \ldots, c_{i,\ell_i-1})$ is well defined and is not equal to $(q-1, \ldots, q-1)$.

Let $f_\alpha : \mathbb{Z}_n \to \{0, 1, \ldots, q-1\}$ be given by

$$f_\alpha(q^j s_i) := \begin{cases} q-1 & \text{if } i \notin I; \\ c_{i,j}(\alpha) & \text{if } i \in I. \end{cases} \tag{6}$$

The function f_α has the property that $L_{q-1}(f_\alpha) \cap S_i$ is a strict subset of S_i for any $i \in I$ since $(c_{i,0}, \ldots, c_{i,\ell_i-1})$ is is not equal to $(q-1, \ldots, q-1)$. This implies that f_α is contained in $\mathcal{E}_I$.

Definition 4.8. Let $I \subseteq \{1, \ldots, m\}$. We define $\psi_I : \mathcal{Q}_I \to \mathcal{E}_I$ to be the map that sends $\alpha \in \mathcal{Q}_I$ to the function f_α. $\triangle$

Example 4.9. Continuing from Example 4.7, we present the image of the function ψ_I for different α's (recall that we represent a function $f : \mathbb{Z}_3 \to \{0, 1\}$ as the set $\{z \in \mathbb{Z}_3 \mid f(z) = 1\}$):

- The case $I = \varnothing$: When $\alpha = 0$, the map $\psi_\varnothing$ sends α to $\{0, 1, 2\}$.
- The case $I = \{1\}$: When $\alpha = 1 + X + X^2$, we have

  $$b_1(\alpha) + \phi_{1,\{1\}}(\alpha) = 0 + 0 = 0 = 0 \cdot 2^0.$$

  The map $\psi_{\{1\}}$ then sends α to $\{1, 2\}$.

- The case $I = \{2\}$:
  - When $\alpha = 1 + X$, we have
$$3\,b_2(\alpha) + \phi_{2,\{2\}}(\alpha) = 3 \cdot 0 + 2 = 2 = 0 \cdot 2^0 + 1 \cdot 2^1.$$
    The map $\psi_{\{2\}}$ then sends α to $\{0, 2\}$.
  - When $\alpha = X + X^2$, we have
$$3\,b_2(\alpha) + \phi_{2,\{2\}}(\alpha) = 0 \cdot 0 + 0 = 0 = 0 \cdot 2^0 + 0 \cdot 2^1.$$
    The map $\psi_{\{2\}}$ then sends α to $\{0\}$.
  - When $\alpha = 1 + X^2$, we have
$$3\,b_2(\alpha) + \phi_{2,\{2\}}(\alpha) = 3 \cdot 0 + 1 = 1 = 1 \cdot 2^0 + 0 \cdot 2^1.$$
    The map $\psi_{\{2\}}$ then sends α to $\{0, 1\}$.
- The case $I = \{1, 2\}$:
  - When $\alpha = 1$, we have
$$\begin{aligned} b_1(\alpha) + \phi_{1,\{1,2\}}(\alpha) &= 0 + 0 = 0 = 0 \cdot 2^0; \\ 3\,b_2(\alpha) + \phi_{2,\{1,2\}}(\alpha) &= 3 \cdot 0 + 0 = 0 = 0 \cdot 2^0 + 0 \cdot 2^1. \end{aligned}$$
    The map $\psi_{\{1,2\}}$ then sends α to $\varnothing$.
  - When $\alpha = X$, we have
$$\begin{aligned} b_1(\alpha) + \phi_{1,\{1,2\}}(\alpha) &= 0 + 0 = 0 = 0 \cdot 2^0; \\ 3\,b_2(\alpha) + \phi_{2,\{1,2\}}(\alpha) &= 3 \cdot 0 + 1 = 1 = 1 \cdot 2^0 + 0 \cdot 2^1. \end{aligned}$$
    The map $\psi_{\{1,2\}}$ then sends α to $\{1\}$.
  - When $\alpha = X^2$, we have
$$\begin{aligned} b_1(\alpha) + \phi_{1,\{1,2\}}(\alpha) &= 0 + 0 = 0 = 0 \cdot 2^0; \\ 3\,b_2(\alpha) + \phi_{2,\{1,2\}}(\alpha) &= 3 \cdot 0 + 2 = 2 = 0 \cdot 2^0 + 1 \cdot 2^1. \end{aligned}$$
    The map $\psi_{\{1,2\}}$ then sends α to the function $\{2\}$. $\triangle$

Lemma 4.10. *Let q be a prime power, let n be a positive integer coprime to q, and let $I \subseteq \{1, \ldots, m\}$. Then the map $\psi_I : \mathcal{Q}_I \to \mathcal{E}_I$ is a bijection.*

Proof. Let α and α' be two elements of $\mathcal{Q}_I$ with the same image under ψ_I. By (5), (6), and the definition of ψ_I, we have
$$b_i(\alpha)\frac{n}{\gcd(n, s_i)} + \phi_{i,I}(\alpha) = b_i(\alpha')\frac{n}{\gcd(n, s_i)} + \phi_{i,I}(\alpha') \quad \text{for any } i \in I.$$

Since $\phi_{i,I}(\alpha)$ and $\phi_{i,I}(\alpha')$ are both nonnegative integers strictly less than $\frac{n}{\gcd(n,s_i)}$, and the equation above then implies that

$$\phi_{i,I}(\alpha) = \phi_{i,I}(\alpha') \qquad \text{and} \qquad b_i(\alpha) = b_i(\alpha') \quad \text{for any } i \in I.$$

Since ϕ_I is chosen to be a bijection by Definition 4.6, we conclude that

$$a_i(\alpha) = a_i(\alpha') \quad \text{and} \quad b_i(\alpha) = b_i(\alpha') \quad \text{for any } i \in I.$$

It then follows from Definition 4.1 and Definition 4.3 that

$$\alpha = \alpha' \pmod{P_i} \quad \text{for any } i \in I.$$

On the other hand, by the definition of $\mathcal{Q}_I$, we have

$$\alpha = 0 = \alpha' \pmod{P_i} \quad \text{for any } i \notin I.$$

By Theorem 2.6(ii), we then conclude that $\alpha = \alpha'$. This proves the injectivity of ψ_I.

Let f be an arbitrary element of $\mathcal{E}_I$. For any $i \in I$, let b_i and $\phi_{i,I}$ be the quotient and the remainder of the division of the sum $\sum_{j=0}^{\ell_i-1} q^j f(q^j s_i)$ by $\frac{n}{\gcd(n,s_i)}$. The sum $\sum_{j=0}^{\ell_i-1} q^j f(q^j s_i)$ is a nonnegative integer strictly less than $q^{\ell_i}-1$ by the assumption that $L_{q-1}(f) \cap S_i \neq S_i$. This implies that b_i and $\phi_{i,I}$ satisfy the inequalities $0 \leqslant b_i < \frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n}$ and $0 \leqslant \phi_{i,I} < \frac{n}{\gcd(n,s_i)}$.

Write $(a_i)_{i\in I} := \phi_I^{-1}((\phi_{i,I})_{i\in I})$. By Theorem 2.6(ii) there exists a unique $\alpha \in \mathcal{Q}$ that satisfies the following equations:

$$\begin{aligned} \log_{g_i}(\alpha) &= a_i \frac{(q^{\ell_i}-1)\gcd(n,s_i)}{n} + b_i \qquad (\text{for } i \in I); \\ \alpha &= 0 \pmod{P_i} \qquad (\text{for } i \notin I). \end{aligned}$$

The element α is contained in $\mathcal{Q}_I$ as α is divisible by P_i if and only if $i \notin I$. Furthermore, the map ψ_I maps α to f, as the construction above mirrors the construction of ψ_I with steps taken in the reverse order. This proves the surjectivity of ψ_I. □

Lemma 4.11. *Let q be a prime power, let n be a positive integer coprime to q, and let $I \subseteq \{1, \ldots, m\}$. Then, for any $\alpha \in \mathcal{Q}_I$,*

(i) $\displaystyle\sum_{z\in\mathbb{Z}_n} z f_\alpha(z) = \sum_{i\in I} s_i \phi_{i,I}(\alpha) \pmod{n}$*; and*

(ii) *There exists unique $\beta \in \{\alpha, X\alpha, \ldots, X^{n-1}\alpha\}$ such that $\psi_I(\beta)$ is contained in $\mathcal{F}$.*

Proof. We start with proving part (i). We have

$$\begin{aligned}
\sum_{z\in\mathbb{Z}_n} zf_\alpha(z) &= \sum_{i\in I}\sum_{j=0}^{\ell_i-1} q^j s_i c_{i,j}(\alpha) + \sum_{i\notin I}\sum_{j=0}^{\ell_i-1} q^j s_i(q-1) \qquad \text{(by (6))}\\
&= \sum_{i\in I}\sum_{j=0}^{\ell_i-1} q^j s_i c_{i,j}(\alpha) + \sum_{i\notin I}(q^{\ell_i}-1)s_i\\
&= \sum_{i\in I}\sum_{j=0}^{\ell_i-1} q^j s_i c_{i,j}(\alpha) \pmod n \qquad \text{(by Definition 2.1)}\\
&= \sum_{i\in I} s_i\left(b_i(\alpha)\frac{n}{\gcd(n,s_i)} + \phi_{i,I}(\alpha)\right) \pmod n \qquad \text{(by (5))}\\
&= \sum_{i\in I} s_i\phi_{i,I}(\alpha) \pmod n.
\end{aligned}$$

This proves part (i).

We now prove part (ii). We have

$$|\{\alpha, X\alpha, \dots, X^{n-1}\alpha\}| = \min\{k>0 \mid X^k\alpha=\alpha\} = \operatorname{lcm}(1, (\text{order of } X \text{ in } G_i)_{i\in I}),$$

where the last equality is a consequence of Theorem 2.6(ii) and the assumption that $\alpha\in\mathcal{Q}_I$. By Lemma 2.5(iii), we have

$$\operatorname{lcm}(1, (\text{order of } X \text{ in } G_i)_{i\in I}) = \operatorname{lcm}\left(1, \left(\frac{n}{\gcd(n,s_i)}\right)_{i\in I}\right) = \frac{n}{\gcd(n, \gcd(s_i)_{i\in I})}.$$

Combining the two equations above, we get

$$|\{\alpha, X\alpha, \dots, X^{n-1}\alpha\}| = \frac{n}{\gcd(n, \gcd(s_i)_{i\in I})}.$$

Hence it suffices to show that there exists a unique $k\in\{0,\dots,\frac{n}{\gcd(n,\gcd(s_i)_{i\in I})}-1\}$ for which $\psi_I(X^k\alpha)$ is contained in $\mathcal{F}$, or equivalently,

$$\sum_{z\in\mathbb{Z}_n} zf_{X^k\alpha}(z) = 0 \pmod n.$$

By Lemma 4.5(ii), we have, for any $k\geqslant 0$,

$$\phi_I((a_i(X^k\alpha))_{i\in I}) = \phi_I((k+a_i(\alpha))_{i\in I}).$$

It then follows from the definition of $h_{i,I}$ and $\phi_{i,I}$ that, for any $i\in I$,

$$\phi_{i,I}(X^k\alpha) = k\,h_{i,I} + \phi_{i,I}(\alpha). \tag{7}$$

We then have, for any $k \geqslant 0$,

$$\begin{aligned}
&\sum_{z\in\mathbb{Z}_n} z f_{X^k\alpha}(z) = \sum_{i\in I} s_i\phi_{i,I}(X^k\alpha) \pmod n \qquad \text{(by part (i))}\\
=&\sum_{i\in I} s_i\left(k\,h_{i,I}+\phi_{i,I}(\alpha)\right) \pmod n \qquad \text{(by (7))}\\
=&k\sum_{i\in I} s_i h_{i,I}+\sum_{i\in I} s_i\phi_{i,I}(\alpha) \pmod n\\
=&k\gcd(n,\gcd(s_i)_{i\in I})+\sum_{i\in I} s_i\phi_{i,I}(\alpha) \pmod n \qquad \text{(by (3))}.
\end{aligned} \tag{8}$$

By the definition of gcd, the sum $\sum_{i\in I} s_i\phi_{i,I}(\alpha)$ is a multiple of $\gcd(n,\gcd(s_i)_{i\in I})$ modulo n. Hence there exists a unique $k \in \{0,1,\ldots,\frac{n}{\gcd(n,\gcd(s_i)_{i\in I})}-1\}$ for which the sum in (8) is equal to 0. This completes the proof. $\square$

Definition 4.12. Let $\widehat{\psi} : \mathcal{N} \to \mathcal{F}$ be the map defined by

$$\{\alpha, X\alpha, \ldots, X^{n-1}\alpha\} \mapsto \psi_I(\beta),$$

where I is the subset of $\{1,\ldots,m\}$ such that $\alpha \in \mathcal{Q}_I$, and β is the unique element of $\{\alpha, X\alpha, \ldots, X^{n-1}\alpha\}$ for which its image is contained in $\mathcal{F}$. $\triangle$

Proof of Theorem 1.2. Note that the maps ψ_I ($I \subseteq \{1,\ldots,m\}$) satisfy (C1) and (C2) by Lemma 4.10 and Lemma 4.11(ii), respectively. It then follows that the map $\widehat{\psi}$ in Definition 4.12 is a bijection. $\square$

Example 4.13. Continuing from Example 4.9, the map $\widehat{\psi} : \mathcal{N} \to \mathcal{F}$ is given by (recall that we represent a function $f : \mathbb{Z}_3 \to \{0,1\}$ as the set $\{z \in \mathbb{Z}_3 \mid f(z) = 1\}$):

- $\{0\}$ is being mapped to $\psi_\varnothing(0) = \{0,1,2\}$;
- $\{1+X+X^2\}$ is being mapped to $\psi_{\{1\}}(1+X+X^2) = \{1,2\}$;
- $\{1+X, X+X^2, 1+X^2\}$ is being mapped to $\psi_{\{2\}}(X+X^2) = \{0\}$;
- $\{1, X, X^2\}$ is being mapped to $\psi_{\{1,2\}}(1) = \varnothing$.

5 Some open bijective problems

We conclude with two bijective problems that refine Theorem 1.1 and Theorem 1.2.

1. Construct a bijection between $\mathcal{N}$ and $\mathcal{F}$ for any two coprime positive integers q and n. Note that the bijection in Theorem 1.2 relies on viewing the color for neckaces in $\mathcal{N}$ as being drawn from the finite field $\mathbb{F}_q$, and thus fails to work when q is not a prime power.

2. Let n be an odd positive integer, and let $k \in \{0, \ldots, n\}$. Give a bijective proof that these two sets have the same cardinality:

    - The set $\mathcal{N}_k$ of necklaces of length n with k black beads and $n-k$ white beads; and
    - The set $\mathcal{F}_k$ of functions $f : \mathbb{Z}_n \to \{0,1\}$ such that the sum $\sum_{z \in \mathbb{Z}_n} z f(z)$ is equal to 0 modulo n and the set $\{z \in \mathbb{Z}_n \mid f(z) \neq 0\}$ has cardinality k.

    One can show that $\mathcal{N}_k$ and $\mathcal{F}_k$ have the same cardinality by computing $|\mathcal{N}_k|$ and $|\mathcal{F}_k|$ separately. The cardinality of $\mathcal{N}_k$ was computed by [ACH15, Theorem 1.20] by using the orbit-counting theorem, and the cardinality of $\mathcal{F}_k$ can be computed by using the counting method developed in [KP93]. The same bijective problem was asked in [ACH15] for the case that k divides n.

    We remark that the bijection in Theorem 1.2 does not map $\mathcal{N}_k$ to $\mathcal{F}_k$, as can be seen from Example 4.13.

Acknowledgements

The author would like to thank Richard Stanley for sharing his knowledge on the status of the problem; Marcelo Aguiar, Henk D.L. Hollmann, and Lionel Levine for their invaluable advice and encouragement; Lila Greco, Viktor Kiss, José Bastidas Olaya, Connor Simpson, Karl Thomas Bååth Sjöblom, and Lilla Tóthmérész for constructive criticism of the paper; and the anonymous referee for their careful reading and insightful comments.

References

[AC17] Marcelo Aguiar and Swee Hong Chan. Toric arrangements associated to graphs. *Sém. Lothar. Combin.*, 78B:Art. 84, 12, 2017.

[ACH15] Federico Ardila, Federico Castillo, and Michael Henley. The arithmetic Tutte polynomials of the classical root systems. *Int. Math. Res. Not. IMRN*, (12):3830–3877, 2015.

[Hun80] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[JJ98] Gareth A. Jones and J. Mary Jones. *Elementary number theory*. Springer Undergraduate Mathematics Series. Springer-Verlag London, Ltd., London, 1998.

[KP93] Nitu Kitchloo and Lior Pachter. An interesting result about subset sums, 1993.

[Kus14] William Kuszmaul. A New Approach to Enumerating Statistics Modulo n. arXiv:1402.3839 , February 2014.

[OS78] Andrew M. Odlyzko and Richard P. Stanley. Enumeration of power sums modulo a prime. *J. Number Theory*, 10(2):263–272, 1978.

[Sta12] Richard P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.

[SY72] Richard P. Stanley and Michael F. Yoder. A study of Varshamov codes for asymmetric channels. *Jet Prop. Lab. Tech. Rep*, pages 32–1526, 1972.

[Wan03] Zhe-Xian Wan. *Lectures on finite fields and Galois rings.* World Scientific Publishing Co., Inc., River Edge, NJ, 2003.