Group-theoretical generalization of necklace polynomials

Young-Tak Oh

Abstract Let G be a group, U a subgroup of G of finite index, X a finite alphabet and q an indeterminate. In this paper, we study symmetric polynomials $M_G(X, U)$ and $M_G^q(X, U)$ which were introduced as a group-theoretical generalization of necklace polynomials. Main results are to generalize identities satisfied by necklace polynomials due to Metropolis and Rota in a bijective way, and to express $M_G^q(X, U)$ in terms of $M_G(X, V)$'s, where $[V]$ ranges over a set of conjugacy classes of subgroups to which U is subconjugate. As a byproduct, we provide the explicit form of the $GL_m(\mathbb{C})$-module whose character is $M_{\mathbb{Z}}^q(X, n\mathbb{Z})$, where m is the cardinality of X.

Keywords Necklace polynomial · G-set and G-orbit · Character · Free Lie algebra · Symmetric polynomial

1 Introduction

In the theory of algebraic combinatorics, it is well known that the number of non-periodic circular strings of n-beads out of x-beads (i.e., *primitive necklaces*) is given by the polynomial

$$M(x, n) := \frac{1}{n} \sum_{d|n} \mu(d) x^{\frac{n}{d}}, \tag{1.1}$$

where μ denotes the classical Möbius inversion function. In the literature, it is usually called a *necklace polynomial* (for instance, see [11]).

Y.-T. Oh (✉)
Department of Mathematics, Sogang University, Seoul 121-742, Korea
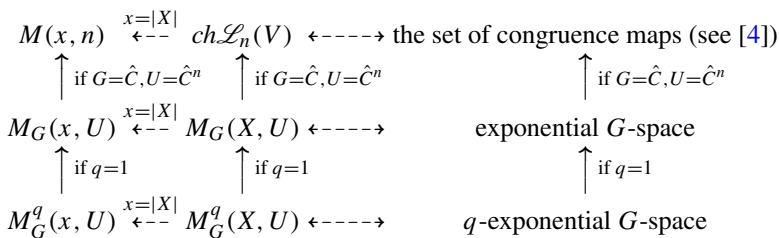e-mail: ytoh@sogang.ac.kr

Necklace polynomials are concerned with many algebraic objects such as free Lie algebras, Witt vectors, and so on. Let $\mathscr{L}(V)$ be the free Lie algebra generated by an m-dimensional vector space V over an arbitrary field k and $\mathscr{L}_n(V)\,(n \geq 1)$ its nth homogeneous component. In 1937, Witt [19] proved that when x is specialized into m, the above polynomial gives the dimension of $\mathscr{L}_n(V)$. In addition, $\mathscr{L}_n(V)$ can be viewed as a finite dimensional $GL_m(k)$-submodule of $V^{\otimes n}$. In 1944, Brandt [2] showed that when $V = \mathbb{C}^m$, the character of $\mathscr{L}_n(V)$ (i.e., the trace of diag$(x_1, x_2, \ldots, x_m)$ on $\mathscr{L}_n(V)$) is given by

$$ch\mathscr{L}_n(V) = \frac{1}{n} \sum_{d|n} \mu(d) p_d(X)^{\frac{n}{d}},$$

where $p_d(X) = x_1^d + \cdots + x_m^d$ is the dth power-sum symmetric polynomial. As for Witt vectors, Metropolis and Rota noticed some remarkable identities satisfied by necklace polynomials (more precisely, Theorems 1 through 6 in [11, Sect. 3]) and utilized them to demonstrate the beautiful connection between the ring of Witt vectors over $\mathbb{Z}$ and the ring of necklaces over $\mathbb{Z}$.

In the present paper, we study a group-theoretical generalization of $M(x, n)$ and $ch\mathscr{L}_n(V)$. A group-theoretical generalization of necklace polynomials was first introduced by Dress and Siebeneicher [3, 4] to construct an almost finite "exponential G-space", where G denotes an arbitrary profinite group. The polynomials thus obtained count the number of certain orbits in an exponential G-space and play a crucial role in showing that the Witt–Burnside ring of G over $\mathbb{Z}$ is isomorphic to the Burnside ring of G.

On the other hand, a group-theoretical generalization of $ch\mathscr{L}_n(V)$ first appeared implicitly in [14] to reveal the structure of Witt–Burnside ring of a profinite group G over an arbitrary special λ-ring. To be more precise, to each open subgroup U of G and a finite alphabet $X = \{x_1, \ldots, x_m\}$ we assign a new symmetric polynomial $M_G(X, U)$ in $x_1, \ldots, x_m$ which specializes to $ch\mathscr{L}_n(V)$ when $G = \hat{C}$ and $U = \hat{C}^n$. Here $\hat{C}$ denotes the profinite completion of the infinite cyclic group C and $\hat{C}^n$ a unique open subgroup of $\hat{C}$ of index n. Further, in [16], a q-analog of $M_G(X, U)$, denoted by $M_G^q(X, U)$, was introduced where q ranges over the set of integers. As one expects, it coincides with $M_G(X, U)$ when $q = 1$ (refer to Definition 2.9). When all x_i's are specialized into 1, $M_G^q(X, U)$ reduces to a polynomial $M_G(x, U)$ in $x = |X|$ and it counts the number of orbits isomorphic to G/U in a certain "q-exponential G-space". The above introduction can be illustrated well in the following diagram:

$$
\begin{array}{ccc}
M(x, n) & \overset{x=|X|}{\leftarrow\!-\!-} ch\mathscr{L}_n(V) & \leftarrow\!-\!-\!-\!\rightarrow \text{ the set of congruence maps (see [4])} \\
\big\uparrow \text{if } G=\hat{C}, U=\hat{C}^n & \big\uparrow \text{if } G=\hat{C}, U=\hat{C}^n & \big\uparrow \text{if } G=\hat{C}, U=\hat{C}^n \\
M_G(x, U) & \overset{x=|X|}{\leftarrow\!-\!-} M_G(X, U) \leftarrow\!-\!-\!-\!\rightarrow & \text{exponential } G\text{-space} \\
\big\uparrow \text{if } q=1 & \big\uparrow \text{if } q=1 & \big\uparrow \text{if } q=1 \\
M_G^q(x, U) & \overset{x=|X|}{\leftarrow\!-\!-} M_G^q(X, U) \leftarrow\!-\!-\!-\!\rightarrow & q\text{-exponential } G\text{-space}
\end{array}
$$

As in the case of $M_G(X, U)$'s, $M_G^q(X, U)$ play a crucial role in demonstrating structure of q Witt–Burnside ring over an arbitrary special λ-ring. The closed formula for

$M_G^q(X, U)$ can be found in [16, Theorem 3.6], which is stated as follows:

$$M_G^q(X, U) = \sum_{[W] \preceq [U]} \mu_G^q([U], [W]) q^{(G:W)-1} p_{(W:U)}(X)^{(G:W)}.$$

Here μ_G^q denotes q-Möbius function associated with the poset of the conjugacy classes of open subgroups of G, where $[W] \preceq [U]$ means that U is subconjugate to W.

Throughout this paper, we assume that G is a group such that the poset of all conjugacy classes of subgroups of finite index is locally finite, that is, every interval is finite. With this assumption, the first main result is to generalize the identities among necklace polynomials which are due to Metropolis and Rota (see Theorems 1 through 6 in [11, Sect. 3]). In fact, these identities can be deduced by comparing the cardinality and weight between two isomorphic G-sets, respectively (see Theorem 3.2, Theorem 3.6, and Theorem 3.11).

The second main result relates to connection between $M_G(x, U)$ (resp. $M_G(X, U)$) and $M_G^q(x, U)$ (resp. $M_G^q(X, U)$). More precisely, we express $M_G^q(x, U)$ as a linear combination of $M_G(x, V)$'s such as

$$M_G^q(x, U) = \sum_{\substack{[G] \preceq [V] \preceq [U] \\ (\text{in } \mathscr{C}(G))}} c_U(V) M_G(x, V),$$

where $[V]$ ranges over a set of conjugacy classes of subgroups containing U (see Theorem 4.1). Moreover, we give a combinatorial interpretation of $c_U(V)$. Indeed, when q is a positive integer, it turns out to be the number of $\bar{f} \in \mathscr{H}$ such that the isotropy subgroup of $\pi_2 \circ f$ is G-conjugate to V, where

$$\mathscr{H} := \left\{ \bar{f} \in (\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim : G \cdot \bar{f} \cong G/U, \bar{f} \text{ is aperiodic} \right\}$$

(see Theorem 4.5). As a byproduct, we show that when $G = \mathbb{Z}$, $U = n\mathbb{Z}$, $M_G^q(X, U)$ is a character of some $GL_n(\mathbb{C})$-module (see Example 4.7).

This paper is organized as follows. Section 2 involves basic definitions and notation on our group-theoretical generalization of $M(x, n)$ and $ch\mathscr{L}_n(V)$. In Sect. 3, we generalize Theorems 1 through 6 in [11, Sect. 3] and provide their combinatorial interpretation. In Sect. 4, we express $M_G^q(x, U)$ as a linear combination of $M_G(x, V)$'s, and using this we find relations between $M_G^q(X, U)$'s and $M_G(X, U)$'s. In the final section, some interesting relations among necklace polynomials will be dealt with.

2 Group-theoretical generalization of necklace polynomials

2.1 Group-theoretical generalization of $M(x, n)$

Let G be a group. Denote by $\mathscr{C}(G)$ the set of subgroups U of G such that G/U is finite. And we denote by $\overline{\mathscr{C}}(G)$ the set of conjugacy classes of subgroups in $\mathscr{C}(G)$. For instance, if G is a finitely generated profinite group, then $\mathscr{C}(G)$ coincides with

the set of open subgroups of G (see [13]). Given subgroups U and V of G, we say that U is *subconjugate* to V if U is a subgroup of some conjugates of V. This induces a partial-ordering on $\overline{\mathscr{C}}(G)$, and will be denoted by $[V] \preceq [U]$.

Recall that for any two subgroups U and V of G, G/U is isomorphic to G/V as a G-set if and only if U and V are G-conjugate. It follows that the set of isomorphism classes of finite transitive G-sets is in one to one correspondence with $\overline{\mathscr{C}}(G)$.

Convention Throughout the present paper, we will assume that $\overline{\mathscr{C}}(G)$ is locally finite, that is, every interval of $\overline{\mathscr{C}}(G)$ is finite.

A G-set X is said to be *essentially finite* if X^U, the set of U-invariant elements in X, is finite for all $U \in \mathscr{C}(G)$, and said to be *almost finite* if it is essentially finite and every element lies in a finite orbit. Note that if X is almost finite, then every orbit in X is finite and there are only finitely many orbits isomorphic to G/U for all $U \in \mathscr{C}(G)$. Let us form the Burnside–Grothendieck ring $\hat{\Omega}(G)$ of the (virtual) isomorphism classes of almost-finite G-sets whose addition is defined via disjoint-union and whose multiplication via Cartesian product. The notation $[X]$ will be used to denote an element of $\hat{\Omega}(G)$.

For any two G-sets S and T, the set T^S of maps from S into T is made into a G-set by supplying the standard G-action defined by $(g \cdot f)(s) = g \cdot f(g^{-1}s)$ for all $g \in G$, $f \in T^S$, and $s \in S$. Letting $X = \{x_1, x_2, \ldots, x_m\}$ be a finite alphabet, it is a G-set with the trivial G-action. Given a subgroup $U \in \mathscr{C}(G)$, let us consider $\mathrm{Hom}_U(G, X)$, the set of U-invariant maps in X^G. Note that $\mathrm{Hom}_U(G, X)$ can be naturally identified with $X^{U \backslash G}$ and the cardinality of $X^{U \backslash G}$ is given by $m^{(G:U)}$.[1] On the other hand, each U-invariant element in X^G appears in an orbit isomorphic to G/V such that U is subconjugate to V. Let $M_G(m, V)$ denote the number of orbits in X^G isomorphic to G/V. This notation makes sense since it depends only on the cardinality of X, not on X. As a consequence, one has the following formula:

$$m^{(G:U)} = \sum_{[G] \preceq [V] \preceq [U]} \varphi_U(G/V) M_G(m, V), \qquad (2.1)$$

where $\varphi_U(G/V)$ means the number of U-invariant elements in G/V. Substituting x for m we obtain an integral-valued polynomial $M_G(x, U) \in \mathbb{Q}[x]$ for all $[U] \in \overline{\mathscr{C}}(G)$.

Example 2.1 Let $G = \mathbb{Z}$ and $U = n\mathbb{Z}$. Then (2.1) implies that

$$x^n = \sum_{d | n} d M_{\mathbb{Z}}(x, d\mathbb{Z}), \quad n \in \mathbb{N}.$$

Using Möbius inversion formula one can see that $M_{\mathbb{Z}}(x, n\mathbb{Z})$ is identical to the neck-lace polynomial $M(x, n)$ in (1.1). Also, by considering the identity

$$\sum_{n \geq 1} x^n t^{n-1} = \sum_{n \geq 1} \sum_{d | n} d M_{\mathbb{Z}}(x, d\mathbb{Z}) t^{n-1},$$

---

[1] It should be mentioned that $X^{G \backslash U}$ denotes the set of maps from $G \backslash U$ to X, not the set of $U \backslash G$-invariant elements in X, especially in the case where G is an abelian group.

one can deduce the well known *cyclotomic identity* [5, 11]:

$$\frac{1}{1-xt} = \left(\frac{1}{1-t^n}\right)^{M(x,n)}.$$

For variations of necklace polynomials and cyclotomic identity, refer to [8, 9, 12].

2.2 Group-theoretical generalization of $ch\mathscr{L}_n(V)$

To begin with, we will introduce the notion of *weight* of an arbitrary element in $\mathrm{Hom}_U(G, X)$ for all $U \in \mathscr{C}(G)$. To do this let us choose a set of representatives of left-cosets of U in G, say $\{u_1 = e, u_2, \ldots, u_{(G:U)}\}$. Here e means the identity of G.

Definition 2.2 Let $U \in \mathscr{C}(G)$.

(a) Let $f \in \mathrm{Hom}_U(G, X)$. The U-weight of f, denoted by $\mathrm{wt}_U(f)$, is defined by

$$\prod_{1 \leq i \leq (G:U)} f(u_i).$$

(b) The U-weight of $\mathrm{Hom}_U(G, X)$, denoted by $\mathrm{wt}_U(\mathrm{Hom}_U(G, X))$, is defined by

$$\sum_{f \in \mathrm{Hom}_U(G,X)} \mathrm{wt}_U(f).$$

(c) The polynomial $S_G(X, U)$ is defined by

$$\sum_{\substack{f \in X^G \\ G \cdot f \cong G/U}} \mathrm{wt}_{G_f}(f),$$

where G_f denotes the isotropy subgroup of f in G.

(d) The polynomial $M_G(X, U)$ is defined by

$$\sideset{}{'}\sum_{\substack{f \in X^G \\ G \cdot f \cong G/U}} \mathrm{wt}_{G_f}(f).$$

Here the symbol $\sum'$ is meant to indicate that for each orbit isomorphic to G/U in X^G exactly one summand has to be taken.

Remark 2.3

(a) Note that

$$M_G(X, U) = \sideset{}{'}\sum_{\substack{f \in \mathrm{Hom}_U(G,X) \\ G \cdot f \cong G/U}} \mathrm{wt}_U(f)$$

since we can always choose a U-invariant element f in $G \cdot f \cong G/U$.

(b) From the above definition it follows that $S_G(X, U) = (G : U)M_G(X, U)$. Also, it should be remarked that $M_G(X, U)$ depends only on the conjugacy class of U, not on U.

(c) In the same manner, we can define $S_G(x, U)$ to be the number of elements in $\mathrm{Hom}_U(G, X)$ whose isotropy subgroup is G-conjugate to U. Then $S_G(x, U) = (G : U)M_G(x, U)$.

It is all but obvious that $M_G(X, U)$ is a symmetric polynomial in $x_1, \ldots, x_m$ over $\mathbb{Z}$, and thus we can consider $p_n(X) \circ M_G(X, U)$, where $\circ$ denotes the *plethysm* and $p_n(X)$ the nth power-sum symmetric polynomial in $x_1, \ldots, x_m$ (see [10]). Since $\mathrm{wt}_U(\mathrm{Hom}_U(G, X)) = p_1(X)^{(G:U)}$ for all $U \in \mathscr{C}(G)$, it follows that

$$p_1(X)^{(G:U)} = \sum_{[V] \leq [U]} \varphi_U(G/V) \, p_{(V:U)}(X) \circ M_G(X, V). \tag{2.2}$$

A closed formula $M_G(X, U)$ can be found in [16, Sect. 3]. For instance, if G is abelian, then we have

$$M_G(X, U) = \frac{1}{(G : U)} \sum_{U \subseteq W} \mu_G(U, W) \, p_{(W:U)}(X)^{(G:W)}, \tag{2.3}$$

where μ_G denotes the Möbius function of $\mathscr{C}(G)$.

Example 2.4 Let $G = \mathbb{Z}$ and $U = n\mathbb{Z}$. In view of (2.3), one can see that $M_G(X, U)$ coincides with $ch\mathscr{L}_n(V)$. In addition, by (2.2) we have

$$p_1(X)^n = \sum_{d|n} d \, p_{\frac{n}{d}}(X) \circ M_{\mathbb{Z}}(X, d\mathbb{Z}), \quad \forall n \geq 1.$$

This gives the identity

$$\sum_{n \geq 1} p_1(X)^n t^{n-1} = \sum_{n \geq 1} \left(\sum_{d|n} d \, p_{\frac{n}{d}}(X) \circ M_{\mathbb{Z}}(X, d\mathbb{Z}) \right) t^{n-1},$$

and which induces a generalized version of the cyclotomic identity:

$$\frac{1}{1 - p_1(X)t} = \prod_{n=1}^{\infty} \exp\left(\sum_{r=1}^{\infty} \frac{1}{r} p_r(X) \circ M(X, n) t^{nr} \right).$$

2.3 q-analog

As before, G is an arbitrary group such that $\overline{\mathscr{C}}(G)$ is locally finite and $U, V \in \mathscr{C}(G)$. In this section, we will consider q-analogs of $M_G(X, V)$ and $M_G(x, V)$. To begin with, q is assumed to be a positive integer. Consider $\mathbb{Z}/q\mathbb{Z} \times X$ which will be regarded as a $\mathbb{Z}/q\mathbb{Z} \times G$-set with respect to the action defined by

$$(\bar{c}, g) \cdot (\bar{a}, x) = (\bar{a} + \bar{c}, g \cdot x), \quad \forall \, \bar{a}, \bar{c} \in \mathbb{Z}/q\mathbb{Z}, g \in G, x \in X.$$

In a similar way, $(\mathbb{Z}/q\mathbb{Z} \times X)^G$ becomes a $\mathbb{Z}/q\mathbb{Z} \times G$-set with respect to the action given by

$$\big((\bar{c}, g) \cdot f\big)(h) = \big(\bar{c} + \pi_1 \circ f(h), \big(g \cdot (\pi_2 \circ f)\big)(h)\big)$$

for all $\bar{a}, \bar{c} \in \mathbb{Z}/q\mathbb{Z}$, $g, h \in G$, and $f \in (\mathbb{Z}/q\mathbb{Z} \times X)^G$. Here π_i, $(i = 1, 2)$ denotes the i-th projection map. Given any two elements $f, f' \in (\mathbb{Z}/q\mathbb{Z} \times X)^G$, let $f \sim f'$ if $f' = \bar{c} \cdot f$ for some $\bar{c} \in \mathbb{Z}/q\mathbb{Z}$. One can see that if $f \sim f'$ then $g \cdot f \sim g \cdot f'$ for all $g \in G$ and thus $(\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim$ can be viewed as a G-set. Use $\bar{f}$ to indicate the equivalence class of f with respect to the equivalence relation "$\sim$".

Given a subgroup $U \in \mathscr{C}(G)$, we can view $\mathrm{Hom}_U(G, \mathbb{Z}/q\mathbb{Z} \times X) / \sim$ as a G-set since $\mathrm{Hom}_U(G, \mathbb{Z}/q\mathbb{Z} \times X)$ is closed under the above $\mathbb{Z}/q\mathbb{Z}$-action. Note that the cardinality of $\mathrm{Hom}_U(G, \mathbb{Z}/q\mathbb{Z} \times X) / \sim$ is equal to $q^{(G:U)-1} m^{(G:U)}$. Let $\overline{M}_G^q(m, V)$ denote the number of orbits in $(\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim$ isomorphic to G/V. Note that it depends only on the cardinality of X, not on X. Then it follows that

$$q^{(G:U)-1} m^{(G:U)} = \sum_{[V] \leq [U]} \varphi_U(G/V) \overline{M}_G^q(m, V).$$

By multiplying either side of the above identity by q one can easily derive that

$$\overline{M}_G^q(m, V) = \frac{1}{q} M_G(qm, V).$$

Now, regard q as a variable and substitute x for m. Then one can obtain a polynomial $\overline{M}_G^q(x, V) \in \mathbb{Q}[q][x]$ for all $[V] \in \overline{\mathscr{C}}(G)$. Clearly $\overline{M}_G^q(x, V)$ coincides with $M_G(x, V)$ at $q = 1$. Note that these polynomials take integer values if q, x are integers.

Example 2.5 Let $G = \mathbb{Z}$, $U = n\mathbb{Z}$, and $q = -1$. For every positive integer n, it follows from [18, Sect. 3] that

$$M^{-1}(x, n) = \begin{cases} M(x, n) & \text{if } n \text{ is odd,} \\ -\sum_{i=1}^{k} M(x, 2^i n') & \text{if } n = 2^k n' \text{ where } k \geq 1 \text{ and } n' \text{ is odd.} \end{cases}$$

In the rest of this section, we will introduce another q-analog of $M_G(x, V)$ which is of main interest in this paper. For this purpose, we need to count $\mathrm{Hom}_U(G, \mathbb{Z}/q\mathbb{Z} \times X) / \sim$ using so called *aperiodic functions*. For the time being, q is assumed to be a positive integer.

Definition 2.6 (cf. [16]) Assume that $h \in \mathrm{Hom}_V(G, \mathbb{Z}/q\mathbb{Z} \times X)$ for some open subgroup V of G. Given an open subgroup W of G, we say that h has a period W if

1. $G_h \subseteq W$, and
2. for $1 \leq i \leq (G : W)$, there exists an element $h_W \in \mathrm{Hom}_W(G, \mathbb{Z}/q\mathbb{Z} \times X)$ and $s_j \in \mathbb{Z}/q\mathbb{Z}$, $1 \leq j \leq (W : G_h)$, such that

$$h(t_j w_i) = s_j \cdot h_W(w_i).$$

Here, $\{w_i : 1 \leq i \leq (G : W)\}$ is a set of right-coset representatives of W in G and $\{t_j : 1 \leq j \leq (W : G_h)\}$ a set of right-coset representatives of G_h in W.

If h has no period other than G_h, then it is called *aperiodic*.

Lemma 2.7 *Assume that* $h \in \mathrm{Hom}_V(G, \mathbb{Z}/q\mathbb{Z} \times X)$ *for some open subgroup V of G. Then we have the following*:

(a) *If h is aperiodic and $h \sim h'$, then h' is also aperiodic.*
(b) *Let $g \in G$. If h is aperiodic, then $g \cdot h$ is also aperiodic.*

Proof (a) is straightforward since $G_h = G_{h'}$. For (b), note that the isotropy subgroup of $g \cdot h$ is given by gG_hg^{-1}. Assume that $g \cdot h$ is not aperiodic. Then it has a period W with $gG_hg^{-1} \subsetneq W$. Now, we will show that h has a period $g^{-1}Wg$ which contains G_h strictly. Let $\{w_i : 1 \leq i \leq (G : W)\}$ be a set of right-coset representatives of W in G and $\{t_j : 1 \leq j \leq (W : gG_hg^{-1})\}$ a set of right-coset representatives of gG_hg^{-1} in W. Then $\{g^{-1}w_ig : 1 \leq i \leq (G : W)\}$ is a set of right-coset representatives of $g^{-1}Wg$ in G and $\{g^{-1}t_jg : 1 \leq j \leq (W : gG_hg^{-1})\}$ a set of right-coset representatives of G_h in W. Let $g \cdot h(t_jw_i) = s_j \cdot h_W(w_i)$ for all i, j. Then

$$
\begin{aligned}
h\big((g^{-1}t_jg)(g^{-1}w_ig)\big) &= g \cdot h(t_jw_ig) \\
&= s_j \cdot h_W(w_ig) \\
&= s_j \cdot (g^{-1} \cdot h_W)(g^{-1}w_ig).
\end{aligned}
$$

This justifies our assertion since the isotropy subgroup of $g^{-1} \cdot h_W$ is given by $g^{-1}Wg$. But this is absurd since h is aperiodic. As a consequence, $g \cdot h$ should be aperiodic. $\qquad\square$

Let us say that $\bar{f}$ is *aperiodic* if f is aperiodic. This definition makes sense due to Lemma 2.7(a). Define $M_G^q(m, U)$ to be the cardinality of aperiodic functions in $(\mathbb{Z}/q\mathbb{Z} \times X)^G/\sim$.

Lemma 2.8 [16] *For every $[U] \in \overline{\mathscr{C}}(G)$ and every positive integer m, we have*

$$
q^{(G:U)-1}m^{(G:U)} = \sum_{[V] \leq [U]} \varphi_U(G/V)q^{(V:U)-1}M_G^q(m, V). \tag{2.4}
$$

As before, let us obtain a polynomial $M_G^q(x, U) \in \mathbb{Q}[q][x]$ from $M_G^q(m, U)$ for all $[U] \in \overline{\mathscr{C}}(G)$ by substituting x for m and regarding q as an indeterminate. Applying mathematical induction on the degree to (2.4) one can easily show that $M_G^q(x, U)$ is a polynomial of degree $(G : U)$ and the leading coefficient is given by $q^{(G:U)-1}/(N_G(U) : U)$. In addition, it coincides with $M_G(x, U)$ at $q = 1$.

Definition 2.9 Let q be any positive integer and G be a group. For every $[U] \in \overline{\mathscr{C}}(G)$, we define $M_G^q(X, U)$ by the weight generating polynomial

$$\sideset{}{'}\sum_{\substack{G \cdot \bar{f} \cong G/U \\ \bar{f} \text{ is aperiodic}}} \text{wt}_{G_{\pi_2 \circ f}} (\pi_2 \circ f)^{(G_{\pi_2 \circ f}:U)}.$$

Here the symbol $\sum'$ is meant to indicate that for each orbit isomorphic to G/U in $(\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim$ exactly one summand has to be taken.

Note that $M_G^q(X, U)$ is a symmetric polynomial in $x_1, \ldots, x_m$ over $\mathbb{Z}$ of degree $(G : U)$ if q is a positive integer. If we regard q as an indeterminate, it can be viewed as a symmetric polynomial in $x_1, \ldots, x_m$ over $\mathbb{Q}[q]$.

Lemma 2.10 [16] *For every $[U] \in \overline{\mathscr{C}}(G)$ and an indeterminate q, we have*

$$q^{(G:U)-1} p_1(X)^{(G:U)} = \sum_{[V] \preceq [U]} \varphi_U(G/V) \, q^{(V:U)-1} p_{(V:U)}(X) \circ M_G^q(X, V).$$

Proposition 2.11 *For every $[U] \in \overline{\mathscr{C}}(G)$ and an indeterminate q, we have $M_G^q(1, G) = 1$ and $M_G^q(1, U) = 0$ for all $[U] \not\succeq [G]$.*

Proof The desired result can be obtained by applying inductive argument on the index to the following identity:

$$q^{(G:U)-1}(x_1 + x_2 + \cdots + x_m)^{(G:U)}$$
$$= \sum_{[G] \preceq [V] \preceq [U]} \varphi_U(G/V) \, q^{(V:U)-1} p_{(V:U)}(X) \circ M_G^q(X, V)$$

for every $[U] \in \overline{\mathscr{C}}(G)$. $\qquad \square$

It is worthwhile to mention that the fact that $M_G^q(1, U) = 0$ for all $[U] \not\succeq [G]$ can be interpreted combinatorially. To do this, we first assume that $G \cdot f \cong G/U$ for some $f \in (\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim$. Fix a set of right-coset representatives $\{u_i : 1 \leq i \leq (G : U)\}$ of U in G. Then $G = \bigcup_{1 \leq i \leq (G:U)} U u_i$. Notice that f is U-invariant and

$$f(u_i) = (\bar{c} \cdot f_G)(e), \quad \forall 1 \leq i \leq (G : U),$$

where $f(u_i) = (\bar{c}, 1)$ and $f_G \in (\mathbb{Z}/q\mathbb{Z} \times \{1\})^G / \sim$ is a constant function such that $f_G(g) = (\bar{0}, 1)$ for all $g \in G$. It implies that the period of f is G and thus there is no U-invariant function whose period equals U unless $U = G$.

3 Generalizing identities among necklace polynomials

The purpose of this section is to generalize identities among necklace polynomials observed by Metropolis and Rota in [11] and provide their bijective proofs.

Throughout this section, we assume that X and Y alphabets $\{x_1, x_2, \ldots, x_m\}$ and $Y = \{y_1, y_2, \ldots, y_l\}$, respectively. Then XY is defined to be the alphabet $XY = \{x_a y_b : 1 \le a \le m, \ 1 \le b \le l\}$ and X^k $(k \ge 1)$ the alphabet of all monomials in x_i's of degree k.

Definition 3.1 Let G be a group and U, W, W' subgroups of G. Define $a_{W,W'}(U)$ to be the number of double coset representatives, g, of W and W' in G satisfying that $W \cap gW'g^{-1}$ is G-conjugate to U.

Theorem 3.2 *For every subgroup $U \in \mathscr{C}(G)$, we have*

$$M_G(xy, U) = \sum_{[W],[W']\in\overline{\mathscr{C}}(G)} a_{W,W'}(U)M_G(x, W)M_G(y, W'). \qquad (3.1)$$

Proof Note that $\Phi : (XY)^G \to X^G \times Y^G, \ f \mapsto \Phi(f) = (f_1, f_2)$ is an isomorphism of G-sets, where $f_1(g) = \pi_1 \circ f(g)$ and $f_2(g) = \pi_2 \circ f(g)$ for all $g \in G$. Here π_i $(i = 1, 2)$ represents the i-th projection. Let $\mathscr{A} := \{f \in (XY)^G : G \cdot f \cong G/U\}$ and $\mathscr{B} := \{h \in X^G \times Y^G : G \cdot h \cong G/U\}$. Then $\Phi|_{\mathscr{A}} : \mathscr{A} \to \mathscr{B}$ is also an isomorphism of G-sets. Recall that the cardinality of $\mathscr{A}$ is $S_G(ml, U)$ by definition. Now, let us compute the cardinality of $\mathscr{B}$. Given $W, W' \in \mathscr{C}(G)$, the number of orbits in X^G (resp. Y^G) isomorphic to G/W (resp. G/W') is $M_G(m, W)$ (resp. $M_G(l, W')$). On the other hand, by Mackey's formula

$$G/W \times G/W' \cong \bigcup_{V g W}^{\bullet} G/W \cap gW'g^{-1}$$

where g ranges over a set of double coset representatives of W and W' in G. As a consequence, the total number of $h \in X^G \times Y^G$ such that $G \cdot h \cong G/U$ is given by

$$\sum_{[W],[W']\in\overline{\mathscr{C}}(G)} a_{W,W'}(U)M_G(m, W)M_G(l, W')(G : U).$$

Substituting x, y for m, l, respectively, and then dividing both sides of

$$S_G(ml, U) = \sum_{[W],[W']\in\overline{\mathscr{C}}(G)} a_{W,W'}(U)M_G(m, W)M_G(l, W')(G : U),$$

by $(G : U)$ we obtain the desired result. $\square$

Let G be an abelian group. In this case, the total number of $h \in X^G \times Y^G$ such that $G \cdot h \cong G/U$ in the proof of Theorem 3.2 has a very simple form. To be more precise, it is exactly equal to the cardinality of the set

$$\left\{h = (f_1, f_2) \in X^G \times Y^G : G_f = W \text{ and } G_{f'} = W' \text{ with } W \cap W' = U\right\}$$

since

$$G \cdot (f_1, f_2) \cong G/G_f \times G/G_{f'} \cong \bigcup_{G_f g G_{f'}}^{\bullet} G/G_f \cap G_{f'}.$$

This implies the identity

$$S_G(ml, U) = \sum_{\substack{W, W' \in \mathscr{C}(G) \\ W \cap W' = U}} S_G(m, W) S_G(l, W').$$

Substituting x, y for m, l, respectively, we have

Theorem 3.3 *Let G be an abelian group. Then, for every subgroup $U \in \mathscr{C}(G)$, we have*

$$S_G(xy, U) = \sum_{\substack{W, W' \in \mathscr{C}(G) \\ W \cap W' = U}} S_G(x, W) S_G(y, W'). \tag{3.2}$$

Remark 3.4

(a) Equation (3.2) can be derived directly by multiplying either side of (3.1) by $(G : U)$ since $a_{W, W'}(U) = (G : W + W')$. However, we will focus on the combinatorial proof throughout this paper.

(b) If G is abelian, (3.1) has a very simple form such as

$$M_G(xy, U) = \sum_{\substack{W, W' \in \mathscr{C}(G) \\ W \cap W' = U}} (G : W + W') M_G(x, W) M_G(y, W'). \tag{3.3}$$

In particular, when $G = \mathbb{Z}, U = n\mathbb{Z}$, (3.2) and (3.3) reduces to [11, Theorem 1 and Theorem 2], respectively.

Corollary 3.5 *For every subgroup $U \in \mathscr{C}(G)$, we have*

$M_G(XY, U)$

$$= \sum_{[W], [W'] \in \overline{\mathscr{C}}(G)} a_{W, W'}(U) \left(p_{(W:U)}(X) \circ M_G(X, W) \right) \left(p_{(W':U)}(X) \circ M_G(Y, W') \right).$$

Proof For $f \in \mathscr{A}$, let $\Phi(f) = (f_1, f_2)$. Note that G_f is G-conjugate to U and

$$G_f = G_{(f_1, f_2)} = G_{f_1} \cap G_{f_2}.$$

Now our assertion follows from the following identity:

$$\mathrm{wt}_{G_f}(f) = \mathrm{wt}_{G_{f_1}}(f_1)^{(G_{f_1} : G_f)} \, \mathrm{wt}_{G_{f_2}}(f_2)^{(G_{f_2} : G_f)}. \qquad \square$$

Next, we will generalize [11, Theorem 3 and Theorem 4].

Theorem 3.6 *For any subgroups $U, V \in \mathscr{C}(G)$ with $U \subseteq V$, we have*

$$S_V(x^{(G:V)}, U) = \sum_{[W] \in \overline{\mathscr{C}}(G)} b_{V, W}(U) \, M_G(x, W)(V : U), \tag{3.4}$$

where $b_{V,W}(U)$ is the number of double coset representatives, g, of V and W in G satisfying that $V \cap gWg^{-1}$ is V-conjugate to U.

Proof Let $\{a_i : 1 \le i \le (G:V)\}$ be a set of right-coset representatives of V in G. Note that

$$\Phi : \mathrm{Res}_V^G(X^G) \to \overbrace{X^V \times \cdots \times X^V}^{(G:V)\text{-times}}, \quad f \mapsto \Phi(f) = (f_1, \dots, f_{(G:V)}) \tag{3.5}$$

is a V-set isomorphism, where $f_i(v) = f(va_i)$ for all $v \in V$ and $1 \le i \le (G:V)$. To see that Φ preserves V-action, observe that

$$(g \cdot f)_i(v) = (g \cdot f)(va_i) = f\big(g^{-1}va_i\big)$$

and

$$(g \cdot f_i)(v) = f_i(g^{-1}v) = f\big(g^{-1}va_i\big)$$

for all $g, v \in V$ and $1 \le i \le (G:V)$. Also, note that

$$\mathrm{Id} : \overbrace{X^V \times \cdots \times X^V}^{(G:V)\text{-times}} \to \big(X^{(G:V)}\big)^V, \quad (f_1, \dots, f_{(G:V)}) \mapsto f_1 \cdots f_{(G:V)}$$

is a V-set isomorphism, where $f_1 \cdots f_{(G:V)}(v) := f_1(v) \cdots f_{(G:V)}(v)$ for all $v \in V$. Let $\mathscr{D} := \{f \in \mathrm{Res}_V^G(X^G) : V \cdot f \cong V/U\}$ and $\mathscr{E} := \{h \in (X^{(G:V)})^V : V \cdot h \cong V/U\}$. Then $\mathrm{Id} \circ \Phi|_{\mathscr{D}} : \mathscr{D} \to \mathscr{E}$ is also a V-set isomorphism. The cardinality of $\mathscr{D}$ can be computed in the following way: Given $W \in \mathscr{C}(G)$, the number of orbits in X^G isomorphic to G/W is given by $M_G(m, W)$. Note that

$$\mathrm{Res}_V^G(G/W) \cong \dot{\bigcup_{VgW}} V/V \cap gWg^{-1} \quad \text{(as a } V\text{-set)},$$

where g ranges over a set of double coset representatives of V and W in G. As a result, the total number of $f \in X^G$ such that $V \cdot f \cong V/U$ as a V-set is given by

$$\sum_{[W] \in \overline{\mathscr{C}}(G)} b_{V,W}(U) \, M_G(m, W)(V:U),$$

whereas the cardinality of $\mathscr{E}$ is $S_V(m^{(G:V)}, U)$, we obtain the identity

$$S_V\big(m^{(G:V)}, U\big) = \sum_{[W] \in \overline{\mathscr{C}}(G)} b_{V,W}(U) \, M_G(m, W)(V:U).$$

Finally, by replacing m by x one can derive the desired result. $\square$

If we assume that G is an abelian group, then the cardinality of $\mathscr{D}$ (in the proof of Theorem 3.6) is exactly given by that of the set $\{f \in X^G : G_f = W \text{ with } V \cap$

$W = U$}. Immediately this induces the equality:

$$S_V\big(m^{(G:V)}, U\big) = \sum_{\substack{W \in \mathscr{C}(G) \\ V \cap W = U}} S_G(m, W).$$

Substituting x, y for m, l, respectively, we have

Theorem 3.7 *Let G be an abelian group. Then, for any subgroups $U, V \in \mathscr{C}(G)$ with $U \subseteq V$, we have*

$$S_V\big(x^{(G:V)}, U\big) = \sum_{\substack{W \in \mathscr{C}(G) \\ V \cap W = U}} S_G(x, W). \tag{3.6}$$

As a corollary of Theorem 3.6, we have

Corollary 3.8 *For subgroups $U, V \in \mathscr{C}(G)$ with $U \subseteq V$, we have*

$$M_V\big(x^{(G:V)}, U\big) = \sum_{[W] \in \overline{\mathscr{C}}(G)} b_{V,W}(U)\, M_G(x, W), \tag{3.7}$$

and

$$M_V\big(X^{(G:V)}, U\big) = \sum_{[W] \in \overline{\mathscr{C}}(G)} b_{V,W}(U)\, p_{(W:U)}(X) \circ M_G(X, W). \tag{3.8}$$

Proof (a) is straightforward. For (b), given a subgroup $W \in \mathscr{C}(G)$, let $\{w_i : 1 \le i \le (G:W)\}$ be a set of right-coset representatives of W in G. Let $f \in \mathscr{D}$ with $G_f = W$. Then $\mathrm{wt}_W f = \prod_{1 \le i \le (G:W)}$. Now, let us compute the weight of $\mathrm{Id} \circ \Phi(f)$. Note that the isotropy subgroup of $\mathrm{Id} \circ \Phi(f)$ is $W \cap V$ which is V-conjugate to U. Let $\{u_j : 1 \le j \le (V : W \cap U)\}$ be a set of right-coset representatives of $V \cap W$ in V. Let $\{v_i : 1 \le i \le (G : V)\}$ be a set of right-coset representatives of V in G. Then the U-weight of $\mathrm{Id} \circ \Phi(f)$ in V is given by

$$\mathrm{wt}_{W \cap V}(\mathrm{Id} \circ \Phi(f)) = \prod_{1 \le j \le (V:V \cap W)} f_1(u_j) f_2(u_j) \cdots f_{(G:V)}(u_j)$$

$$= \prod_{\substack{1 \le i \le (G:V) \\ 1 \le j \le (V:V \cap W)}} f(u_j v_i)$$

$$= (\mathrm{wt}_W f)^{(W:V \cap W)}.$$

This implies the desired result. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Example 3.9 If G is an abelian group, then $b_{V,W}(U) = (G : V + W)$. Hence (3.7) is simplified as

$$M_V\big(x^{(G:V)}, U\big) = \sum_{\substack{W \in \mathscr{C}(G) \\ V \cap W = U}} (G : V + W)\, M_G(x, W). \tag{3.9}$$

Note that (3.6) and (3.9) reduce to [11, Theorem 3 and Theorem 4], respectively, when $G = \mathbb{Z}$, $V = r\mathbb{Z}$, $U = rn\mathbb{Z}$. And this specialization, when applied to (3.8), gives rise to the formula: For any positive integers a and n, we have

$$M(X^a, n) = \sum_{\substack{j \geq 1 \\ [j,a]=an}} \frac{j}{n} \, p_{\frac{an}{j}}(X) \circ M(X, j),$$

equivalently,

$$ch\mathscr{L}_n((\mathbb{C}^m)^{\otimes a}) = \sum_{\substack{j \geq 1 \\ [j,a]=an}} \frac{j}{n} \, p_{\frac{an}{j}}(X) \circ ch\mathscr{L}_j(\mathbb{C}^m).$$

In the rest of this section, we focus on a generalization of [11, Theorem 5 and Theorem 6].

Lemma 3.10 [3] *Let G be a profinite group. For any two open subgroups U, V of G and all $x \in \hat{\Omega}(U)$, $y \in \hat{\Omega}(V)$, one has*

$$\mathrm{Ind}_U^G(x) \, \mathrm{Ind}_V^G(y) = \sum_{UgV \subseteq G} \mathrm{Ind}_{U \cap gVg^{-1}}^G \big(\mathrm{Res}_{U \cap gVg^{-1}}^U(x) \, \big(\mathrm{Res}_{U \cap gVg^{-1}}^V(g)(y)\big)\big).$$

$$(3.10)$$

Here g ranges over a set of double coset representatives of U and V and $\mathrm{Res}_{U \cap gVg^{-1}}^V(g)$ is induced from the embedding $U \cap gVg^{-1} \hookrightarrow V : x \mapsto g^{-1}xg$.

It is easy to show that Lemma 3.10 is also applicable to an arbitrary group if $U, V \in \mathscr{C}(G)$. Using this lemma, we can obtain the following identity:

Theorem 3.11 *For any subgroups $U, V, W \in \mathscr{C}(G)$ with $[U], [V] \preceq [W]$, one has*

$$\sum_{UgV} \sum_{\substack{[Z] \in \overline{\mathscr{C}}(U \cap gVg^{-1}) \\ Z \text{ is } G\text{-conjugate to } W}} M_{U \cap gVg^{-1}}\big(x^{(U:U \cap gVg^{-1})} y^{(V:U \cap gVg^{-1})}, Z\big)$$

$$= \sum_{\substack{[S],[T] \in \overline{\mathscr{C}}(G) \\ SgT \subseteq G \\ S \cap gTg^{-1} \text{ is } G\text{-conjugate to } W}} \left(\sum_{\substack{[Z] \in \overline{\mathscr{C}}(U) \\ Z \text{ is } G\text{-conjugate to } S}} M_U(x, Z) \right)$$

$$\times \left(\sum_{\substack{[Z'] \in \overline{\mathscr{C}}(V) \\ Z' \text{ is } G\text{-conjugate to } T}} M_V(y, Z') \right). \qquad (3.11)$$

Here g (resp. h) ranges over a set of double coset representatives of U and V (resp. S and T) in G satisfying that $V \cap gWg^{-1}$ (resp. $S \cap hTh^{-1}$) is G-conjugate to W.

Proof Let $x = [X^U]$, $y = [Y^V]$. Then we have the following relation (in $\hat{\Omega}(G)$):

$$\text{Ind}_U^G(x) = \sum_{[S] \in \mathscr{C}(G)} \left(\sum_{\substack{[Z] \in \mathscr{C}(U) \\ Z \text{ is } G\text{-conjugate to } S}} M_U(m, Z) \right) [G/S],$$

$$\text{Ind}_V^G(y) = \sum_{[T] \in \overline{\mathscr{C}}(G)} \left(\sum_{\substack{[Z'] \in \mathscr{C}(V) \\ Z' \text{ is } G\text{-conjugate to } T}} M_V(l, Z') \right) [G/T].$$

Therefore, given any $[W] \in \overline{\mathscr{C}}(G)$, the coefficient of $[G/W]$ in $\text{Ind}_U^G(x) \circ \text{Ind}_V^G(y)$ is given by the right hand side of (3.11). On the other hand, in view of (3.5), one has

$$\text{Res}_{U \cap gVg^{-1}}^U(x) = \left[\left(X^{(U:U \cap gVg^{-1})} \right)^{U \cap gVg^{-1}} \right]$$

and

$$\text{Res}_{U \cap gVg^{-1}}^V(g)(x) = \left[\left(Y^{(V:U \cap gVg^{-1})} \right)^{U \cap gVg^{-1}} \right].$$

As a result, we have

$$\text{Res}_{U \cap gVg^{-1}}^U(x) \text{Res}_{U \cap gVg^{-1}}^V(g)(x) = \left[\left(X^{(U:U \cap gVg^{-1})} Y^{(V:U \cap gVg^{-1})} \right)^{U \cap gVg^{-1}} \right].$$

Thus the coefficient of $[G/W]$ on the right hand side of (3.10) is given by the left hand side of (3.11). Finally by substituting x, y for m, l, respectively, we obtain the desired result. $\qquad \square$

Example 3.12 If G is abelian, then (3.11) can be simplified in the following form: For any subgroups $U, V, W \in \mathscr{C}(G)$ with $W \subseteq U \cap V$ we have

$$(G : U + V) M_{U \cap V}\left(x^{(U:U \cap V)} y^{(V:U \cap V)}, W \right)$$

$$= \sum_{\substack{Z \in \mathscr{C}(U), Z' \in \mathscr{C}(V) \\ Z \cap Z' = W}} (G : Z + Z') M_U(x, Z) M_V(y, Z'). \qquad (3.12)$$

In particular, letting $G = \mathbb{Z}$, $U = r\mathbb{Z}$, $V = s\mathbb{Z}$, $W = n[r, s]\mathbb{Z}$, $Z = pr\mathbb{Z}$, and $Z' = qs\mathbb{Z}$, then (3.12) is written as

$$(r, s) M_{[r,s]\mathbb{Z}}\left(x^{\frac{[r,s]}{r}} y^{\frac{[r,s]}{s}}, n[r, s]\mathbb{Z} \right)$$

$$= \sum_{\substack{p, q \geq 1 \\ pr\mathbb{Z} \cap qs\mathbb{Z} = n[r,s]\mathbb{Z}}} (G : pr\mathbb{Z} + qs\mathbb{Z}) M_{r\mathbb{Z}}(x, pr\mathbb{Z}) M_{s\mathbb{Z}}(y, qs\mathbb{Z}).$$

Equivalently,

$$(r, s) M\left(x^{\frac{[r,s]}{r}} y^{\frac{[r,s]}{s}}, n \right) = \sum_{\substack{p, q \\ [pr, qs] = n[r,s]}} (pr, qs) M(x, p) M(y, q).$$

Since $\frac{[r,s]}{r} = \frac{s}{(r,s)}$, $\frac{[r,s]}{s} = \frac{r}{(r,s)}$ and $\frac{pq}{(pr,qs)} = \frac{n}{(r,s)}$, the above identity is exactly equal to [11, Theorem 6].

If G is an abelian group, then one can see immediately that the cardinality of the set

$$\left\{ f \in \text{Ind}_U^G(X^U) \times \text{Ind}_V^G(Y^V) : G \cdot f = G/W \right\}$$

is given by the following formula:

$$\sum_{\substack{Z \in \mathscr{C}(U), Z' \in \mathscr{C}(V) \\ Z \cap Z' = W}} S_U(x, Z) S_V(y, Z'),$$

whereas the cardinality of the set

$$\left\{ f \in \bigcup_{U g V \subseteq G}^{\cdot} \text{Ind}_{U \cap V}^G \big(\text{Res}_{U \cap V}^U(X^U) \times (\text{Res}_{U \cap V}^V(Y^V)\big) : G \cdot f = G/W \right\}$$

is given by $S_{U \cap V}(x^{(U:U \cap V)} y^{(V:U \cap V)}, W)$. As a consequence, we have the following identity:

Theorem 3.13 *Let G be an abelian group. Given any $U, V, W \in \mathscr{C}(G)$ with $W \subseteq U \cap W$, we have*

$$S_{U \cap V}\big(x^{(U:U \cap V)} y^{(V:U \cap V)}, W\big) = \sum_{\substack{Z \in \mathscr{C}(U), Z' \in \mathscr{C}(V) \\ Z \cap Z' = W}} S_U(x, Z) S_V(y, Z').$$

Example 3.14 If $G = \mathbb{Z}$, $U = r\mathbb{Z}$, $V = s\mathbb{Z}$, $W = n[r,s]\mathbb{Z}$, $Z = pr\mathbb{Z}$, and $Z' = qs\mathbb{Z}$,

$$S_{[r,s]\mathbb{Z}}\Big(x^{\frac{[r,s]}{r}} y^{\frac{[r,s]}{s}}, n[r,s]\mathbb{Z}\Big)$$

$$= \sum_{\substack{p,q \geq 1 \\ pr\mathbb{Z} \cap qs\mathbb{Z} = n[r,s]\mathbb{Z}}} S_{r\mathbb{Z}}(x, pr\mathbb{Z}) S_{s\mathbb{Z}}(y, qs\mathbb{Z}).$$

Equivalently,

$$S\Big(x^{\frac{[r,s]}{r}} y^{\frac{[r,s]}{s}}, n\Big) = \sum_{\substack{p,q \geq 1 \\ [pr,qs] = n[r,s]}} S(x, p) S(y, q).$$

In particular, if r, s are relatively prime, then the above identity reduces to

$$S\big(x^s y^r, n\mathbb{Z}\big) = \sum_{\substack{p,q \geq 1 \\ [pr,qs] = nrs}} s(x, p) s(y, q).$$

Note that this identity was first provided in [11, Theorem 6].

Corollary 3.15 *For any subgroups $U, V, W \in \mathscr{C}(G)$ with $[U], [V] \preceq [W]$, one has*

$$\sum_{UgV} \sum_{\substack{[Z]\in\overline{\mathscr{C}}(U\cap gVg^{-1}) \\ Z \text{ is } G\text{-conjugate to } W}} M_{U\cap gVg^{-1}}\big(X^{(U:U\cap gVg^{-1})}Y^{(V:U\cap gVg^{-1})}, Z\big)$$

$$= \sum_{\substack{[S],[T]\in\overline{\mathscr{C}}(G) \\ SgT\subseteq G \\ S\cap gTg^{-1} \text{ is } G\text{-conjugate to } W}} p_{(S:W)}(X) \circ \left(\sum_{\substack{[Z]\in\overline{\mathscr{C}}(U) \\ Z \text{ is } G\text{-conjugate to } S}} M_U(X,Z) \right)$$

$$\times\, p_{(T:W)}(Y) \circ \left(\sum_{\substack{[Z']\in\overline{\mathscr{C}}(V) \\ Z' \text{ is } G\text{-conjugate to } T}} M_V(Y,Z') \right),$$

where g (resp. h) ranges over a set of double coset representatives of U and V (resp. S and T) in G satisfying that $V \cap gWg^{-1}$ (resp. $S \cap hTh^{-1}$) is G-conjugate to W.

Proof Let $\Psi : \mathscr{F} \to \mathscr{G}$ be a G-set isomorphism, where

$$\mathscr{F} := \big\{ (f,g) \in \operatorname{Ind}_U^G(X^U) \times \operatorname{Ind}_V^G(Y^V) : G \cdot (f,g) \cong G/W \big\}$$

and

$$\mathscr{G} := \left\{ \eta \in \bigcup_{UgV\subseteq G}^{\textstyle\cdot} \operatorname{Ind}_{U\cap gVg^{-1}}^G\Big(\operatorname{Res}_{U\cap gVg^{-1}}^U(X^U) \times \operatorname{Res}_{U\cap gVg^{-1}}^V(g)(Y^V)\Big) : G \cdot \eta \cong G/W \right\}.$$

Given $(f, f') \in \mathscr{F}$, let $\Psi(f, f') = (f_1 f_2, \ldots, f_i, f_1', f_2', \ldots, f_j')$, where $i = (U : U \cap gVg^{-1})$ and $j = (V : U \cap gVg^{-1})$. Note that $G_{(f,f')}$ is G-conjugate to W and $G_{(f,f')} = G_f \cap G_{f'}$. Now our assertion follows from the identity

$$\operatorname{wt}_{G_{(f,f')}}\big(\Psi(f,f')\big) = \operatorname{wt}_{G_f}(f)^{(G_f:G_{(f,f')})} \operatorname{wt}_{G_{f'}}(f')^{(G_g:G_{(f,f')})},$$

which can be shown in the same manner as Corollary 3.8 was proven. $\qquad\square$

Remark 3.16 Letting $G = \mathbb{Z}$, $U = r\mathbb{Z}$, $V = s\mathbb{Z}$, $W = k[r,s]\mathbb{Z}$, one has

$$(r,s)M\left(X^{\frac{[r,s]}{r}} Y^{\frac{[r,s]}{s}}, k\right)$$

$$= \sum_{\substack{i,j \\ [ri,sj]=k[r,s]}} (ri,sj)\big(p_{\frac{k[r,s]}{ri}}(X) \circ M(X,i)\big)\big(p_{\frac{k[r,s]}{sj}}(Y) \circ M(Y,j)\big).$$

It should be remarked that [15, Theorem 3.9(C)] was wrongly stated. There $\Psi^{\frac{[\frac{s}{(r,s)},i]}{i}}$ should appear as $\Psi^{\frac{[\frac{ks}{(r,s)},i]}{i}}$ and $\Psi^{\frac{[\frac{r}{(r,s)},j]}{j}}$ should appear as $\Psi^{\frac{[\frac{kr}{(r,s)},j]}{j}}$. This is because

$$\frac{k[r,s]}{ri} = \frac{ks}{i(r,s)} = \frac{[\frac{ks}{(r,s)},i]}{i} \quad \text{and} \quad \frac{k[r,s]}{sj} = \frac{kr}{j(r,s)} = \frac{[\frac{kr}{(r,s)},j]}{j}.$$

4 Expressing $M_G^q(x, U)$ as a linear combination of $M_G(x, V)$'s

The aim of this section is to express $M_G^q(x, U)$ (resp. $M_G^q(X, U)$) in terms of $M_G(x, V)$'s (resp. $M_G(X, V)$'s), where $[V] \preceq [U]$. To begin with, let us observe that $M_G^q(x, G) = x = M_G(x, G)$ and $M_G^q(X, G) = p_1(X) = M_G(X, G)$. So, we will assume that $U \neq G$ throughout this section.

The first main theorem of this section can be stated as follows:

Theorem 4.1 *For every $U \in \mathscr{C}(G)$ with $U \neq G$, we have*

$$M_G^q(x, U) = \sum_{\substack{[G] \preceq [V'] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} c_U(V') \, M_G(x, V'), \qquad (4.1)$$

where $c_U(V')$ is given by

$$\sum_{\substack{[U_i] \in \overline{\mathscr{C}}(V') \\ U_i \text{ is } G\text{-conjugate to } U}} M_{V'}\big(q^{(G:V')-1}, U_i\big).$$

Proof Let us proceed the proof in the following two steps.

  Step 1: In the first step, we will show that $c_U(V')$ is given by

$$\sum_{[V'] \preceq [W] \preceq [U] \text{ (in } \overline{\mathscr{C}}(G))} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q\left(\frac{1}{q}, S\right) \right) \left(\sum_{[V] \in \overline{\mathscr{C}}(G)} a_{V,V'}(W) M_G(q, V) \right)$$

(4.2)

Here $a_{V,V'}(W)$ denotes the number of double coset representatives, g, of V and V' in G satisfying that $V \cap gV'g^{-1}$ is G-conjugate to W.

  Let q, r be indeterminates and $[U] \in \overline{\mathscr{C}}(G)$. From [17, Sect. 2] it follows that

$$q M_G^q(rx, U) = \sum_{\substack{[G] \preceq [W] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} g_{[U],[W]}(r, q) \, r \, M_G^r(qx, W), \qquad (4.3)$$

where $g_{[U],[W]}(r, q)$ is given by

$$\frac{q}{r} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q\left(\frac{r}{q}, S\right) \right).$$

Thus (4.3), when r specializes into 1, reduces to the following identity:

$$M_G^q(x, U) = \sum_{\substack{[G] \preceq [W] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q\left(\frac{1}{q}, S\right) \right) M_G(qx, W). \qquad (4.4)$$

On the other hand, from Theorem 3.2 it follows that

$$M_G(qx, W) = \sum_{\substack{[G] \preceq [V], [V'] \preceq [W] \\ (\text{in } \overline{\mathscr{C}}(G))}} a_{V, V'}(W) M_G(q, V) M_G(x, V'), \qquad (4.5)$$

where $a_{V, V'}(W)$ is the number of double coset representatives, g, of V and V' in G satisfying that $V \cap g V' g^{-1}$ is G-conjugate to W. Hence, by applying (4.5) to the right hand side of (4.4), we can express $M_G^q(x, U)$ as

$$\sum_{\substack{[G] \preceq [W] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ \text{is } G\text{-conjugate to } U}} M_W^q \left(\frac{1}{q}, S \right) \right)$$

$$\times \left(\sum_{\substack{[G] \preceq [V], [V'] \preceq [W] \\ (\text{in } \overline{\mathscr{C}}(G))}} a_{V, V'}(W) M_G(q, V) M_G(x, V') \right). \qquad (4.6)$$

Writing the above summation as a linear combination of $M_G(x, V')$'s we have

$$M_G^q(x, U) = \sum_{\substack{[G] \preceq [V'] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} c_U(V') M_G(x, V'),$$

where $c_U(V') \in \mathbb{Q}[q]$ is given by

$$\sum_{\substack{[V'] \preceq [W] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q \left(\frac{1}{q}, S \right) \right) \left(\sum_{[V] \in \overline{\mathscr{C}}(G)} a_{V, V'}(W) M_G(q, V) \right).$$

This proves the first step.

Step 2: In the second step, we will show that (4.2) is equal to

$$\sum_{\substack{[T] \in \overline{\mathscr{C}}(V') \\ T \text{ is } V'\text{-conjugate to } U}} M_{V'} \left(q^{(G:V')-1}, T \right).$$

To begin with, assume that q is a positive integer. Then one can show that

$$\sum_{[V] \in \overline{\mathscr{C}}(G)} a_{V, V'}(W) M_G(q, V)$$

means the number of orbits isomorphic to G/W in the G-set $G/V' \times \overline{q}^G$, where $\overline{q}^G$ is the set of maps from G to $\overline{q} := \{1, 2, \ldots, q\}$. To be more precise, it can be done by combining the fact that $[\overline{q}] = \sum_{[V] \in \overline{\mathscr{C}}(G)} M_G(q, V)[G/V]$ in $\hat{\Omega}(G)$ with Mackey's

theorem (for example, see [3, (2.6.1)]). One can also see that

$$
\begin{aligned}
G/V' \times \overline{q}^G &= \mathrm{Ind}_{V'}^G (V'/V') \times \overline{q}^G \\
&= \mathrm{Ind}_{V'}^G \big(V'/V' \times \mathrm{Res}_{V'}^G (\overline{q}^G) \big) \\
&= \mathrm{Ind}_{V'}^G \big(\overline{q^{(G:V')}}^{V'} \big).
\end{aligned}
$$

The second equality follows from Frobenius reciprocity (for example, see [3, (2.10.3)]) and the third one from Theorem 3.6. Note that the number of orbits isomorphic to G/W in $\mathrm{Ind}_{V'}^G (\overline{q^{(G:V')}}^{V'})$ is given by

$$
\sum_{\substack{[T] \in \overline{\mathscr{C}}(V') \\ T \text{ is } V'\text{-conjugate to } W}} M_{V'} \big(q^{(G:V')}, T \big).
$$

Combining the result thus obtained with the identity

$$
\left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q \left(\frac{1}{q}, S \right) \right)
$$

$$
= \sum_{\substack{[U_i] \in \overline{\mathscr{C}}(W) \\ U_i \text{ is } G\text{-conjugate to } U}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } W\text{-conjugate to } U_i}} M_W^q \left(\frac{1}{q}, S \right) \right),
$$

one can immediately rewrite (4.2) in the following form:

$$
\sum_{\substack{[V'] \preceq [W] \preceq [U] \\ (\text{in } \overline{\mathscr{C}}(G))}} \sum_{\substack{[U_i] \in \overline{\mathscr{C}}(W) \\ U_i \text{ is } G\text{-conjugate to } U}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } W\text{-conjugate to } U_i}} M_W^q \left(\frac{1}{q}, S \right) \right)
$$

$$
\times \left(\sum_{\substack{[T] \in \overline{\mathscr{C}}(V') \\ T \text{ is } V'\text{-conjugate to } W}} M_{V'} \big(q^{(G:V')}, T \big) \right),
$$

and which can be expressed much simpler in the following way:

$$
\sum_{\substack{[U_i] \in \overline{\mathscr{C}}(V') \\ U_i \text{ is } G\text{-conjugate to } U}} \sum_{\substack{[V'] \preceq [T] \preceq [U_i] \\ (\text{in } \overline{\mathscr{C}}(V'))}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(T) \\ S \text{ is } W\text{-conjugate to } U_i}} M_W^q \left(\frac{1}{q}, S \right) \right) M_{V'} \big(q^{(G:V')}, T \big).
$$

Finally, by (4.4), the above summation can be written as

$$
\sum_{\substack{[U_i] \in \overline{\mathscr{C}}(V') \\ U_i \text{ is } G\text{-conjugate to } U}} M_{V'} \big(q^{(G:V')-1}, U_i \big).
$$

This completes the proof.   □

If G is an abelian group, then (4.1) turns out to be very simple.

Corollary 4.2 *Let G be an abelian group. Then, for any subgroup $U \in \mathscr{C}(G)$ with $U \neq G$, we have*

$$M_G^q(x, U) = \sum_{U \subseteq W \subsetneq G} M_W^q\big(q^{(G:W)-1}, U\big)\, M_G(x, W). \tag{4.7}$$

For understanding of readers, let us give an example of the above corollary.

Example 4.3 Let p be a prime and let $G = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In this case there are $p+1$ subgroups of order p, say $H_1, H_2, \ldots, H_{p+1}$. Note that, for every $1 \leq i \leq p+1$, one has

$$M_G^q(x, H_i) = q^{p-1}\, \frac{(x^p - x)}{p}$$

$$= M_{H_i}\big(q^{(G:H_i)-1}, H_i\big) M_G(x, H_i)$$

since $q^{p-1} = M_{H_i}(q^{(G:H_i)-1}, H_i)$. Also one can see immediately that

$$M_G^q\big(x, \{0\}\big) = \frac{q^{p^2-1}}{p^2}\big(q^{p^2-1}x^{p^2} - (p+1)q^{2(p-1)}x^p + \big((p+1)q^{2(p-1)} - q^{p^2-1}\big)x\big)$$

$$= q^{p^2-1} M_G(x, \{0\}) + \sum_{1 \leq i \leq p+1} \frac{q^{p-1}}{p}\big(q^{p(p-1)} - q^{p-1}\big) M_G(x, H_i)$$

$$= M_{\{0\}}\big(q^{(G:\{0\})-1}, \{0\}\big) M_G(x, \{0\})$$

$$+ \sum_{1 \leq i \leq p+1} M_{H_i}\big(q^{(G:H_i)-1}, \{0\}\big) M_G(x, H_i).$$

In the following, we will provide a combinatorial interpretation of the coefficient $c_U(V')$ in (4.1). First of all, let us assume that q is a positive integer and x the cardinality of X. It should be remarked that they will be regarded as an indeterminate later. Let

$$\mathscr{H} := \big\{ \bar{f} \in (\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim\, : G \cdot \bar{f} \cong G/U,\, \bar{f} \text{ is aperiodic}\big\}. \tag{4.8}$$

Then it is easily seen that, for every element $\bar{f} \in \mathscr{H}$, the isotropy subgroup of $\pi_2 \circ f$ is G-conjugate to some subgroup $V' \in \mathscr{C}(G)$ to which U is subconjugate. Here π_2 is the projection map to the second component and thus it induces a function,

$$G \xrightarrow{f} \mathbb{Z}/q\mathbb{Z} \times X \xrightarrow{\pi_2} X,$$

from G to X. As a consequence, it is possible to write $M_G^q(x, U)$ as

$$\sum_{[V'] \preceq [U]\ (\text{in } \overline{\mathscr{C}}(G))} d_U(V')\, M_G(x, V'),$$

where $d_U(V')$ is the number of elements, say $\bar{f} \in \mathscr{H}$, such that the isotropy subgroup of $\pi_2 \circ f$ is G-conjugate to V'. But it should be noted that it is never obvious that $d_U(V')$ is equal to $c_U(V')$ since $\{M_G(x, V') : [V'] \preceq [U]\}$ is not linearly independent (over $\mathbb{Q}[q]$) in general (for example, refer to Example 4.3). In the rest of this section, we will show that this is indeed true.

As the first step, let us decompose $\mathscr{C}(G, \mathbb{Z}/q\mathbb{Z} \times X)/\sim$ into disjoint G-orbits and then consider its union, say

$$\dot{\bigcup_{\bar{h}}} G\bar{h},$$

in which the number of orbits isomorphic to G/U is given by $M_G^q(x, U)$. Recall that if $G \cdot \bar{h} \cong G/U$, then $G \cdot (\pi_2 \circ h) \cong G/V$ for some $U \subseteq V$.

Lemma 4.4 *Let $U \in \mathscr{C}(G)$ with $U \neq G$ and $[G] \preceq [V] \preceq [U]$ in $\overline{\mathscr{C}}(G)$. For each $f \in X^G$ with $G \cdot f \cong G/V$, let $\mathcal{A}$ be the set of functions $h \in \mathscr{C}(G, \mathbb{Z}/q\mathbb{Z} \times X)$ satisfying the conditions* (C1)–(C3):

(C1) $\pi_2 \circ h = f$,
(C2) $G \cdot h \cong G/U$, *and*
(C3) h *is aperiodic.*

And we let $\mathcal{B}$ be the set of functions $\tau \in \mathscr{C}(G_f, \mathbb{Z}/q\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z})^{(G:V)-1})$ satisfying the conditions (C'1)–(C'2):

(C'1) $G_f \cdot \tau \cong G_f/U_i$ *for some $U_i \in \mathscr{C}(G_f)$ which is G-conjugate to U, and*
(C'2) τ *is aperiodic.*

Then $\mathcal{A}, \mathcal{B}$ have the same cardinality.

Proof Let us construct a bijection $\Xi : \mathcal{B} \to \mathcal{A}$. Given a function $\tau \in \mathcal{B}$, we will define $\Xi(\tau)$ in the following steps:

Step 1:

For simplicity of notation, let $V' = G_f$. First, we choose a set of right-coset representatives

$$\{a_1(=e), a_2, \ldots, a_{(G:V)}\}$$

of V' in G, and also a set of right-coset representatives

$$\{b_1(=e), b_2, \ldots, b_{(V:U)}\}$$

of V'_τ in V'. Then the set

$$\{b_j a_i : 1 \leq i \leq (G : V), \quad 1 \leq j \leq (V : U)\}$$

becomes a set of coset representatives of V'_τ in G. Equivalently

$$G = \dot{\bigcup_{\substack{1 \leq i \leq (G:V) \\ 1 \leq j \leq (V:U)}}} V'_\tau (b_j a_i).$$

Step 2:
Define $\varXi(\tau)$ as follows:

$$\varXi(\tau): G \to \mathbb{Z}/q\mathbb{Z} \times X,$$

$$u(b_j a_i) \mapsto \begin{cases} (c_{1j}, f(a_1)) & \text{if } i = 1, \ j = 1, 2, \dots, (V:U) \\ (c_{ij} + c_{1j} - c_{11}, f(a_i)) & \text{otherwise,} \end{cases}$$

for all $u \in V_\tau$. Here $\tau(b_j) = (c_{1j}, (c_{2j}, \dots, c_{(G:V)j}))$. We claim that $\varXi$ is indeed a bijection. To prove this the followings should be checked.

(i) Firstly, we will show that $\varXi$ is well defined, that is, $\varXi(\tau) \in \mathcal{A}$.

By definition of $\varXi(\tau)$, the condition (C1) is straightforward. To show that the condition (C2) is satisfied, we note that $V'_\tau \subseteq G_{\varXi(\tau)} \subseteq V'$. Hence every element $g \in G_{\varXi(\tau)}$ can be written uniquely as $u_0 b_m$ for some $1 \leq m \leq (V:U)$ and $u_0 \in V'_\tau$. For all $1 \leq i \leq (G:V)$, $1 \leq j \leq (V:U)$, it holds that

$$g \cdot \varXi(\tau)(b_j a_i) = \varXi(\tau)\big(b_m^{-1} u_0^{-1} b_j a_i\big) = \varXi(\tau)(b_j a_i)$$

since $g \in G_{\varXi(\tau)}$. Note that if $b_m^{-1} u_0^{-1} b_j = u' b_k$ for some k with $1 \leq k \leq (V:U)$ and $u' \in V_\tau$, then the above equality implies that

$$\begin{cases} c_{1j} = c_{1k} & \text{if } i = 1, \\ c_{ij} + c_{1j} - c_{11} = c_{ik} + c_{1k} - c_{11} & \text{otherwise.} \end{cases}$$

This gives that $c_{ij} = c_{ik}$. But, since i's are arbitrary, $\tau(b_m^{-1} u_0^{-1} b_j) = \tau(b_j)$ for all $1 \leq j \leq (V:U)$ and thus g stabilizes τ. However, it is a contradiction to the condition (C'1) unless $V'_\tau = G_{\varXi(\tau)}$. Finally, let us show that $\varXi(\tau)$ satisfies the condition (C3). If $\varXi(\tau)$ is of period W with $V'_\tau \subsetneq W \subseteq V'$, then there exists a function $h_W \in \mathrm{Hom}_W(G, \mathbb{Z}/q\mathbb{Z} \times X)$ and $s_k \in \mathbb{Z}/q\mathbb{Z}$, $1 \leq k \leq (W:U)$, such that

$$\varXi(\tau)(t_k w_1) = s_k \cdot h_W(w_1)$$

$$\varXi(\tau)(t_k w_2) = s_k \cdot h_W(w_2)$$

$$\vdots \tag{4.9}$$

$$\varXi(\tau)(t_k w_{(G:W)}) = s_k \cdot h_W(w_{(G:W)}).$$

Here $\{w_l : 1 \leq l \leq (G:W)\}$ is a set of right-coset representatives of W in G and $\{t_k : 1 \leq k \leq (W:V'_\tau)\}$ a set of right-coset representatives of V'_τ in W. In particular, we may assume that $s_1 = 0$. Choose a set of right-coset representatives $\{z_m : 1 \leq m \leq (V:W)\}$ of W in V' so that

$$w_{(G:V)(i-1)+m} = z_m a_i,$$

$$t_k z_m = b_{(W:U)(m-1)+k} \tag{4.10}$$

for all $1 \leq i \leq (G : V)$, $1 \leq m \leq (V : W)$ and $1 \leq k \leq (W : U)$. Then the requirement (4.9) forces that, for every m with $1 \leq m \leq (V : W)$, we have

$$c_{1,(W:U)(m-1)+2} = c_{1,(W:U)(m-1)+1} + s_2$$

$$c_{1,(W:U)(m-1)+3} = c_{1,(W:U)(m-1)+1} + s_3$$

$$\vdots$$

$$c_{1,(W:U)m} = c_{1,(W:U)(m-1)+1} + s_{(W:U)},$$

and, for every i with $1 < i \leq (G : V)$ and for every m with $1 \leq m \leq (V : W)$,

$$c_{i,(W:U)(m-1)+2} + c_{1,(W:U)(m-1)+2} - c_{11} = c_{i,(W:U)(m-1)+1} + c_{1,(W:U)(m-1)+1}$$
$$- c_{1,1} + s_2$$

$$c_{i,(W:U)(m-1)+3} + c_{1,(W:U)(m-1)+3} - c_{11} = c_{i,(W:U)(m-1)+1} + c_{1,(W:U)(m-1)+1}$$
$$- c_{1,1} + s_3$$

$$\vdots$$

$$c_{i,(W:U)m} + c_{1,(W:U)m} - c_{11} = c_{i,(W:U)(m-1)+1} + c_{1,(W:U)(m-1)+1} - c_{1,1} + s_{(W:U)}.$$

As a consequence, we have

$$c_{i,(W:U)(m-1)+1} = c_{i,(W:U)(m-1)+2} = \cdots = c_{i,(W:U)m}$$

for all $1 < i \leq (G : V)$ and $1 \leq m \leq (V : W)$. But this cannot happen due to the condition (C′2). To show this, consider a W-invariant function $\tau_W \in \mathscr{C}(G_f, \mathbb{Z}/q\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z})^{(G:V)-1})$ defined by

$$\tau_W(z_m) = (c_{1,(W:U)(m-1)+1}, (c_{2,(W:U)(m-1)+1}, \ldots, c_{(G:V),(W:U)(m-1)+1}))$$

for $1 \leq m \leq (V' : W)$. Then it is easy to see that, for every $1 \leq k \leq (W : U)$, we have

$$\tau(t_k z_1) = s_k \cdot \tau_W(z_1),$$

$$\tau(t_k z_2) = s_k \cdot \tau_W(z_2),$$

$$\vdots,$$

$$\tau(t_k z_{(V':W)}) = s_k \cdot \tau_W(z_{(V':W)}).$$

This means that W is a period of τ, but it is a contradiction to the condition (C′2). Consequently we can conclude that $\varXi(\tau)$ is aperiodic.

(ii) Secondly, let us prove the injectiveness of $\varXi$.

For $\tau, \tau' \in \mathcal{B}$, let us assume that $\varXi(\tau) = \varXi(\tau')$. Clearly $G_{\varXi(\tau)} = G_{\varXi(\tau')}$. But we have already shown in the above that $G_{\varXi(\tau)} = V'_\tau$ and $G_{\varXi(\tau')} = V'_{\tau'}$. As a consequence, $V'_\tau = V'_{\tau'}$, which says that $\tau = \tau'$.

(iii) Finally, let us prove the surjectiveness of Ξ.

Choose any function $h \in \mathcal{A}$. It is obvious that $G_h \subseteq G_f (= V')$. Let

$$\{b_1(=e), b_2, \ldots, b_{(V:U)}\}$$

be a set of right-coset representatives of G_h in V'. Now, consider a G_h-invariant function $\tau \in \mathscr{C}(V', \mathbb{Z}/q\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z})^{(G:V)-1})$ defined by

$$\tau(ub_j) = \big(d_1, (d_2, d_3, \ldots, d_{(G:V)})\big)$$

for all $u \in U$, where

$$d_i = \begin{cases} \pi_1 \circ h\,(b_j a_1) & \text{if } i = 1, \\ \pi_1 \circ h\,(b_j a_i) - \pi_1 \circ h\,(b_j a_1) + \pi_1 \circ h\,(b_1 a_1) & \text{otherwise} \end{cases}$$

for all $1 \leq j \leq (V:U)$. Here π_1 is the projection map to the first component. By our construction it is obvious that $\Xi(\tau) = h$. Thus, we have only to show that $\tau \in \mathcal{A}$. By its definition it is clear that τ is G_h-invariant. We claim that the isotropy subgroup V'_τ of τ is exactly the same as G_h. This is because if $V'_\tau \supsetneqq G_h$, then V'_τ is a period of h. But it is absurd since h is aperiodic. Thus we have shown that τ satisfies the condition (C'1). To show that τ satisfies the condition (C'2), assume that τ is of period W with $V'_\tau \subsetneqq W \subseteq V'$. Then there exists a W-invariant function $\tau_W \in \mathscr{C}(G_f, \mathbb{Z}/q\mathbb{Z} \times (\mathbb{Z}/q\mathbb{Z})^{(G:V)-1})$ and $s_k \in \mathbb{Z}/q\mathbb{Z}$, $1 \leq k \leq (W:U)$ such that, for every $1 \leq k \leq (W:U)$, we have

$$\tau(t_k z_1) = s_k \cdot \tau_W(z_1),$$

$$\tau(t_k z_2) = s_k \cdot \tau_W(z_2),$$

$$\vdots \tag{4.11}$$

$$\tau(t_k z_{(V':W)}) = s_k \cdot \tau_W(z_{(V':W)})$$

with $s_1 = 0$. Note that we are using sets of representatives $\{a_i : 1 \leq (G:V)\}$, $\{b_j : 1 \leq j \leq (V:U)\}$, $\{w_l : 1 \leq l \leq (G:W)\}$, $\{t_k, 1 \leq k \leq (W:U)\}$, $\{z_m, 1 \leq m \leq (V:W)\}$ satisfying the condition (4.10) in *Step 1 (i)*. Then (4.11) implies that, for every m with $1 \leq m \leq (V:W)$, we have

$$d_{1,(W:U)(m-1)+2} = d_{1,(W:U)(m-1)+1} + s_2$$

$$d_{1,(W:U)(m-1)+3} = d_{1,(W:U)(m-1)+1} + s_3$$

$$\vdots$$

$$d_{1,(W:U)m} = d_{1,(W:U)(m-1)+1} + s_{(W:U)}$$

and, for all $1 < i \leq (G:V)$ and $1 \leq m \leq (V:W)$, we have

$$d_{i,(W:U)(m-1)+1} = d_{i,(W:U)(m-1)+2} = \cdots = d_{i,(W:U)m}.$$

Using the notation $e_{ij} = \pi_1 \circ h(b_j a_i)$ for all $1 \le i \le (G : V)$, $1 \le j \le (V : U)$, the above equality can be expressed as follows: For every $1 \le i \le (G : V)$ and every $1 \le m \le (V : W)$, it holds that

$$e_{i,(W:U)(m-1)+2} = e_{1,(W:U)(m-1)+1} + s_2$$

$$e_{i,(W:U)(m-1)+3} = e_{1,(W:U)(m-1)+1} + s_3$$

$$\vdots$$

$$e_{i,(W:U)m} = e_{1,(W:U)(m-1)+1} + s_{(W:U)}.$$

Letting $h_W \in \mathrm{Hom}_W(G, \mathbb{Z}/q\mathbb{Z} \times X)$ be a W-invariant function defined by

$$h_W(w_i) = h(w_i), \quad 1 \le i \le (G : W),$$

it is obvious that

$$h(t_k w_1) = s_k \cdot h_W(w_1)$$

$$h(t_k w_2) = s_k \cdot h_W(w_2)$$

$$\vdots$$

$$h(t_k w_{(G:W)}) = s_k \cdot h_W(w_{(G:W)})$$

for $1 \le k \le (W : U)$ with $s_1 = 0$. From this it follows that W is a period of h. However, it is absurd since h is aperiodic. Therefore we can conclude that τ is aperiodic, and so we are done. $\square$

Theorem 4.5 *The cardinality of $\mathcal{A}/\sim$ is given by*

$$\sum_{\substack{[U_i] \in \mathscr{C}(V') \\ U_i \text{ is } G\text{-conjugate to } U}} M_{V'}\big(q^{(G:V')-1}, U_i\big).$$

Proof For each $\tau \in \mathcal{A}$, $[\tau]$ has $q^{(V:U)}$-elements. Similarly, for each $h \in \mathcal{B}$, $[h]$ has $q^{(V:U)}$-elements. As a consequence, $|\mathcal{A}/\sim| = |\mathcal{B}/\sim|$. $\square$

The subsequent corollary can be deduced by considering the degree of either side of (4.12) below. To be more precise,

Corollary 4.6 *For every $U \in \mathscr{C}(G)$ with $U \ne G$, we have*

$$M_G^q(X, U) = \sum_{[V'] \preceq [U] \text{ (in } \overline{\mathscr{C}}(G))} c_U(V') \, p_{(V':U)}(X) \circ M_G(X, V'). \qquad (4.12)$$

Proof Let

$$\mathscr{H} := \big\{ \bar{f} \in (\mathbb{Z}/q\mathbb{Z} \times X)^G / \sim : \ G \cdot \bar{f} \cong G/U, \ \bar{f} \text{ is aperiodic} \big\}.$$

For $\bar{f} \in \mathscr{H}$ note that the $G_{\bar{f}}$ weight of $\bar{f}$ is given by

$$\mathrm{wt}_{G_{\pi_2 \circ f}}(\pi_2 \circ f)^{(G_{\pi_2 \circ f}:G_{\bar{f}})}.$$

This implies the desired result.   □

Example 4.7

(a) Let G be an abelian group. Then, for any subgroup $U \in \mathscr{C}(G)$ with $U \neq G$, we have

$$M_G^q(X, U) = \sum_{U \subseteq W \subsetneq G} M_W^q\left(q^{(G:W)-1}, U\right) p_{(W:U)}(X) \circ M_G(X, W). \quad (4.13)$$

(b) In the case where $G = \hat{C}$, (4.13) reduces to

$$M^q(X, n) = \sum_{\substack{d \mid n \\ d > 1}} M^q\left(q^{d-1}, \frac{n}{d}\right) p_{\frac{n}{d}}(X) \circ M(X, d).$$

Note that if q is a positive integer, then $M^q(q^{d-1}, \frac{n}{d})$ is also a non-negative integer. Therefore one can see that $M^q(X, n)$ is a character of some $GL_m(\mathbb{C})$-module. Let us explain it in more detail. Let $\mathscr{L}(\mathbb{C}^m)$ be the free Lie algebra generated by $\mathbb{C}^m$ and $\mathscr{L}_n(\mathbb{C}^m)$ $(n \geq 1)$ its nth homogeneous component. For every positive integer $n \geq 2$, let

$$\tilde{\mathscr{L}}_n^q(\mathbb{C}^m) := \bigoplus_{\substack{d \mid n \\ d > 1}} \Psi^{\frac{n}{d}}\left(\mathscr{L}_d(V)\right)^{\oplus M^q\left(q^{d-1}, \frac{n}{d}\right)},$$

where $\Psi^{\frac{n}{d}}$ denotes the $\frac{n}{d}$-th Adams operation. Then $M^q(X, n) = ch\tilde{\mathscr{L}}_n(\mathbb{C}^m)$ (=the trace of $\mathrm{diag}(x_1, \ldots, x_m)$ on $\tilde{\mathscr{L}}_n(V)$).

Note that $c_U(V')$ can be easily calculated in the following cases.

Proposition 4.8 *For $U \in \mathscr{C}(G)$ with $U \neq G$, we have*
   (a) $c_U(G) = 0$.
   (b) $c_U(U) = q^{(G:U)-1}$.

Proof

(a) By Theorem 4.1 $c_U(G)$ equals $M_G(1, U)$. But one can show that $M_G^q(1, U) = 0$ for $U \in \mathscr{C}(G)$ with $U \neq G$ by applying an inductive argument on index to Lemma 2.8.
(b) By Theorem 4.1 $c_U(U)$ equals $M_U(q^{(G:U)-1}, U)$, which equals $q^{(G:U)-1}$.   □

In the rest of this section, we provide some properties of the polynomials of the form $M_G(q^m, U)$ and $M_G^q(q^m, U)$ with $m \geq 1$. Indeed, these polynomials are in $\mathbb{Q}[q]$.

Lemma 4.9 *Let U be a subgroup of G with $U \in \mathscr{C}(G)$. If $x = q^m$ for some positive integer m, then $\frac{1}{q} M_G^q(x, U)$ is a numerical polynomial in q.*

Let us recall (4.4) again:

$$M_G^q(x, U) = \sum_{\substack{[G] \preceq [W] \preceq [U] \\ (\text{in } \mathscr{C}(G))}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q\left(\frac{1}{q}, S\right) \right) M_G(qx, W).$$

It would be worthwhile to remark that letting $q = 1$ and then replacing r by q in (4.3) yields the identity:

$$M_G(qx, U) = \sum_{[W] \preceq [U]} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W(q, S) \right) M_G^q(x, W). \qquad (4.14)$$

Let us introduce a notation. Let $\overline{\mathscr{C}}(G; [U])$ to denote a subposet of $\overline{\mathscr{C}}(G)$ which consist of $[W] \in \overline{\mathscr{C}}(G)$ with $[G] \preceq [W] \preceq [U]$. Fix an enumeration of this poset satisfying the condition:

$$\textit{If } [V] \preceq [U]\textit{, then } [V] \textit{ precedes } [U].$$

For the simplicity of notation, let $k_{[U]}$ to denote the cardinality of $\overline{\mathscr{C}}(G; [U])$.

Proposition 4.10

(a) *Let U be a subgroup of G with $U \in \mathscr{C}(G)$. If $x = q^m$ for some positive integer $m > 1$, then $\frac{1}{q} M_G(x, U)$ is a numerical polynomial in q.*

(b) *For any $W \in \mathscr{C}(G)$ with $[G] \preceq [W] \preceq [U]$,*

$$q^{k_{[U]}} \left(\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } U}} M_W^q\left(\frac{1}{q}, S\right) \right)$$

is a numerical polynomial in q.

Proof

(a) It can be obtained by combining (4.14) with Lemma 4.9.
(b) We also define a $\overline{\mathscr{C}}(G; [U]) \times \overline{\mathscr{C}}(G; [U])$ matrix ζ by

$$\zeta([V], [W]) = \begin{cases} \left(\displaystyle\sum_{\substack{[S] \in \overline{\mathscr{C}}(W) \\ S \text{ is } G\text{-conjugate to } V}} M_W(q, S) \right) & \text{if } [W] \preceq [V] \\ 0 & \text{otherwise.} \end{cases}$$

This matrix is upper triangular with diagonal entries q. Hence the determinant ζ is $q^{k[U]}$. On the other hand, the $([U], [W])$-th entry of the inverse of ζ is given by

$$
\zeta^{-1}([V], [W]) = \begin{cases} \left(\displaystyle\sum_{\substack{[S]\in\mathscr{C}(W) \\ S \text{ is } G\text{-conjugate to } V}} M_W(\tfrac{1}{q}, S) \right) & \text{if } [W] \preceq [V] \\ 0 & \text{otherwise.} \end{cases}
$$

Now our assertion is straightforward. □

5 Other relations

The final section is devoted to introducing a few more relations among necklace polynomials. To begin with, let us introduce necessary notation. For $X = \{x_1, x_2, \ldots, x_m\}$, let the notation $-X$ denote the alphabet $\{-x_a : 1 \le a \le m\}$. Also, for a positive integer k, the notation $\psi^k(X)$, which is introduced to be consistent with that of a λ-ring, will denote an alphabet $\{x_1^k, x_2^k, \ldots, x_s^k\}$. For the definition of λ-rings, see [1, 6, 7].

Recall that

$$
M(X, n) = \frac{1}{n} \sum_{d|n} \mu(d)\, p_d(X)^{\frac{n}{d}} = \frac{1}{n} \sum_{d|n} \mu(d)\, p_d\big(X^{\frac{n}{d}}\big). \tag{5.1}
$$

Therefore we have

$$
M\big(X, p^k\big) = \frac{1}{p^k}\big(X^{p^k} - p_p\big(X^{p^{k-1}}\big)\big), \quad \forall k \ge 1.
$$

This formula can be generalized further as follows:

Lemma 5.1 *Let $X = \{x_1, x_2, \ldots, x_m\}$ be an alphabet. We also let n be a positive integer n and p be a prime divisor of n. Write $n = n'\, p^k$ with $(n', p) = 1, k \ge 1$. Then*

(a)

$$
M(X, n) = \frac{1}{p^k}\big(M\big(X^{p^k}, n'\big) - p_p(X) \circ M\big(X^{p^{k-1}}, n'\big)\big). \tag{5.2}
$$

(b)

$$
M\big(X, p^k\big) = \frac{1}{p^{k-1}} M\big(X^{p^{k-1}}, p\big). \tag{5.3}
$$

(c)

$$
M(-X, n) = \begin{cases} -M(X, n) & \text{if } n \text{ is odd,} \\ M(X, n) & \text{if } 4|n, \\ M(X, n) + p_2(X) \circ M(X, \tfrac{n}{2}) & \text{if } 2|n, \text{ but } 4 \nmid n. \end{cases}
$$

Proof

(a) Note that $p_{ij}(X) = p_i(\psi^j(X))$ for all $i, j \geq 1$. Therefore, we have

$$\sum_{d|n} \mu(d) \, p_d(X)^{\frac{n}{d}} = \sum_{e|n'} \mu(e) \, p_e(X)^{\frac{n'}{e}p^k} + \sum_{e|n'} \mu(ep) \, p_{ep}(X)^{\frac{n'}{e}p^{k-1}}$$

$$= \sum_{e|n'} \mu(e) \, p_e\big(X^{\frac{n'}{e}p^k}\big) - \sum_{e|n'} \mu(e) \, \big(p_e\big(\psi^p(X)\big)\big)^{\frac{n'}{e}p^{k-1}}$$

$$= \sum_{e|n'} \mu(e) \, p_e\big(X^{\frac{n'}{e}p^k}\big) - \sum_{e|n'} \mu(e) \, p_e\big(\psi^p(X)^{p^{k-1}\frac{n'}{e}}\big).$$

Dividing both sides by n yields the desired result.

(b) Consider the case where $n' = 1$ in (5.2). Then the desired result follows from the identity that

$$M\big(X^{p^{k-1}}, p\big) = \frac{1}{p}\big(X^{p^k} - \psi^p(X)^{p^{k-1}}\big).$$

(c) We will prove only third case. Other cases can be verified in the exactly same way. Let $p = 2$. Then Lemma 5.1 implies that

$$M(X, n) = \frac{1}{2}\left(M\left(X^2, \frac{n}{2}\right) - M\left(\psi^2(X), \frac{n}{2}\right)\right), \quad \text{and}$$

$$M(-X, n) = \frac{1}{2}\left(M\left(X^2, \frac{n}{2}\right) + M\left(\psi^2(X), \frac{n}{2}\right)\right).$$

Now, our assertion is obvious.   □

Equations (5.2) and (5.3) can be interpreted representation-theoretically in the following way: Let $V = \mathbb{C}^m$. Then we have

$$ch\mathscr{L}_n(V) = \frac{1}{p^k}\big(ch\mathscr{L}_{n'}\big(V^{\otimes p^k}\big) - p_p(X) \circ ch\mathscr{L}_{n'}\big(V^{\otimes p^{k-1}}\big)\big)$$

and

$$ch\mathscr{L}_{p^k}(V) = \frac{1}{p^{k-1}} ch\mathscr{L}_p\big(V^{\otimes p^{k-1}}\big).$$

Also, if $2|n$, but $4 \nmid n$, the proof of Lemma 5.1(c) implies that

$$M(-X, n) = M\left(X^2, \frac{n}{2}\right) - M(X, n)$$

$$= ch\mathscr{L}_{\frac{n}{2}}\big(V^{\otimes 2}\big) - ch\mathscr{L}_n(V)$$

$$= ch\mathscr{L}_n(V) + p_2(X) \circ ch\mathscr{L}_{\frac{n}{2}}(V).$$

Finally, we close this section by providing the following connection between $M(X, n)$ and $M^{-1}(X, n)$ for all $n \geq 1$.

Proposition 5.2

(a) *For every positive integer $n = 2^k n'$ with n' odd and $k \geq 1$, we have*

$$\sum_{i=0}^{k} M\left(-\psi^{2^i}(X), \frac{n}{2^i}\right) = \sum_{i=0}^{k-1} M\left(\psi^{2^i}(X), \frac{n}{2^i}\right). \tag{5.4}$$

(b) *For every positive integer $n = 2^k n'$ with n' odd, we have*

$$M^{-1}(X, n) = \begin{cases} M(X, n) & \text{if } k = 0, \\ -\sum_{i=0}^{k-1} M(\psi^{2^i}(X), \frac{n}{2^i}) & \text{if } k \geq 1. \end{cases}$$

Proof It was shown in [18, Sect. 3] that

$$\sum_{i=0}^{k} M\left(-x, \frac{n}{2^i}\right) = \sum_{i=0}^{k-1} M\left(x, \frac{n}{2^i}\right).$$

(a) follows from this by considering the degree of either side of (5.4). (b) follows from Example 2.5. □

References

1. Atiyah, M.F., Tall, D.O.: Group representations, λ-rings and the J-homomorphism. Topology **8**, 253–297 (1969)
2. Brandt, A.: The free Lie ring and Lie representations of the full linear group. Trans. Am. Math. Soc. **352**, 528–536 (1944)
3. Dress, A., Siebeneicher, C.: The Burnside ring of profinite groups and the Witt vectors construction. Adv. Math. **70**, 87–132 (1988)
4. Dress, A., Siebeneicher, C.: The Burnside ring of the infinite cyclic group and its relation to the necklace algebra, λ-ring and the Universal ring of the Witt vectors. Adv. Math. **78**, 1–41 (1989)
5. Gauss, C.F.: Werke Band II, pp. 219–222. Königliche Gesellschaft der Wissenschaften, Göttingen (1863)
6. Hazewinkel, M.: Formal Groups and Applications. Academic Press, New York (1978)
7. Knutson, D.: λ-rings and the representation theory of the symmetric group. In: Lecture Notes in Math., vol. 308. Springer, Berlin (1973)
8. Labelle, G., Leroux, P.: An extension of the exponential formula in enumerative combinatorics. Electron. J. Comb. **3**(2), 1–14 (1996)
9. Lenart, C.: Formal group-theoretic generalization of the necklace algebra, including a q-deformation. J. Algebra **199**, 703–732 (1998)
10. Macdonald, I.G.: Symmetric Functions and Hall Polynomials, 2nd edn. Oxford University Press, London (1995)
11. Metropolis, N., Rota, G.-C.: Witt vectors and the algebra of necklaces. Adv. Math. **50**, 95–125 (1983)
12. Moree, P.: The formal series Witt transform. Discrete Math. **295**, 143–160 (2005)
13. Nikolov, N., Segal, D.: Finite index subgroups in profinite groups. C. R. Acad. Sci. Paris, Ser. I Math. **83**, 303–308 (2003)
14. Oh, Y.-T.: R-analogue of the Burnside ring of profinite groups and free Lie algebras. Adv. Math. **190**, 1–46 (2005)

15. Oh, Y.-T.: Necklace rings and logarithmic functions. Adv. Math. **205**(2), 434–486 (2006)
16. Oh, Y.-T.: q-deformation of Witt–Burnside rings. Math. Z. **207**, 151–191 (2007)
17. Oh, Y.-T.: q-analog of the Möbius function and the cyclotomic identity associated to a profinite group. Adv. Math. **219**, 852–893 (2008)
18. Oh, Y.-T.: q-deformed necklace rings and q-Möbius function. J. Algebra **320**(4), 1599–1625 (2008)
19. Witt, E.: Darstellung Liescher Ringe. J. Reine Angew. Math. **177**, 152–160 (1937)