The group permanent determines the finite abelian group

Mao-Sheng Li[a] Hanbin Zhang[b]

Submitted: Aug 26, 2024; Accepted: Oct 20, 2024; Published: Nov 15, 2024

Abstract

Let G be a finite abelian group of order n and $\mathcal{M}_G$ the Cayley table of G. Let $\mathcal{P}(G)$ be the number of formally different monomials occurring in $\mathsf{per}(\mathcal{M}_G)$, the permanent of $\mathcal{M}_G$. In this paper, for any finite abelian groups G and H, we prove the following characterization

$$\mathcal{P}(G) = \mathcal{P}(H) \;\Leftrightarrow\; G \cong H.$$

It follows that the group permanent determines the finite abelian group, which partially answers an open question of Donovan, Johnson and Wanless. In fact, $\mathcal{P}(G)$ is closely related to zero-sum sequences over finite abelian groups and we shall prove the above characterization by studying a reciprocity of zero-sum sequences over finite abelian groups. As an application of our method, we show that $\mathcal{P}(G) > \mathcal{P}(C_n)$ for any non-cyclic abelian group G of order n and thereby answer an open problem of Panyushev.

Mathematics Subject Classifications: 05A10, 11B13, 15A72

1 Introduction

Let $G = (\{x_0, \cdots, x_{n-1}\}, \dot{+})$ be a finite group of order n. Let $\mathcal{M}_G = (m_{ij})_{n\times n}$ (where $m_{ij} = x_i \dot{+} x_j$, $0 \leqslant i, j \leqslant n-1$) be the Cayley table of G. Recall that the determinant of $\mathcal{M}_G$ and the permanent of $\mathcal{M}_G$, denoted by $\mathsf{det}(\mathcal{M}_G)$ and $\mathsf{per}(\mathcal{M}_G)$, are the homogeneous polynomials of degree n in $\mathbb{C}[x_0, \cdots, x_{n-1}]$:

$$\mathsf{det}(\mathcal{M}_G) = \sum_{\tau\in S_n} (-1)^{\mathrm{sgn}(\tau)} \prod_{i=0}^{n-1} m_{i,\tau(i)} = \sum_{\tau\in S_n} (-1)^{\mathrm{sgn}(\tau)} \prod_{i=0}^{n-1} (x_i \dot{+} x_{\tau(i)})$$

[a]School of Mathematics, South China University of Technology, Guangzhou 510641, Guangdong, P.R. China, (li.maosheng.math@gmail.com).

[b]School of Mathematics (Zhuhai), Sun Yat-sen University, Zhuhai 519082, Guangdong, P.R. China, (zhanghb68@mail.sysu.edu.cn). (Corresponding author)

and

$$\mathsf{per}(\mathcal{M}_G) = \sum_{\tau \in S_n} \prod_{i=0}^{n-1} m_{i,\tau(i)} = \sum_{\tau \in S_n} \prod_{i=0}^{n-1} (x_i \dot{+} x_{\tau(i)}).$$

We call $\mathsf{det}(\mathcal{M}_G)$ (resp. $\mathsf{per}(\mathcal{M}_G)$) the group determinant (resp. group permanent) of G. The study of $\mathsf{det}(\mathcal{M}_G)$ can be traced back to pioneering works of Dedekind and Frobenius, which led to the development of representation theory; see [23]. Let $\mathcal{P}(G)$ be the number of formally different monomials occurring in $\mathsf{per}(\mathcal{M}_G)$. For example, let $x_0, \cdots, x_{n-1}$ be the natural ordering of C_n, we have

$$\mathcal{M}_{C_3} = \begin{pmatrix} x_0 & x_1 & x_2 \\ x_1 & x_2 & x_0 \\ x_2 & x_0 & x_1 \end{pmatrix},$$

$\mathsf{per}(\mathcal{M}_{C_3}) = x_0^3 + x_1^3 + x_2^3 + 3x_0x_1x_2$, and $\mathcal{P}(C_3) = 4$. There are several interesting results and problems on $\mathcal{P}(G)$. To state these results and problems, we first introduce the notion of zero-sum sequences over finite abelian groups.

Now, we focus on the case when G is abelian and $|G| = n$. Let k be a positive integer, we call $S = g_1 \bullet \ldots \bullet g_k$ a sequence over G if S is a collection of elements $g_1, \ldots, g_k$ from G where repetition is allowed but the ordering of the elements is disregarded. Here, k is called the length of S and we denote it by $|S| = k$. We define $\sigma(S) = g_1 \dot{+} \cdots \dot{+} g_k$ and call S a zero-sum sequence if $\sigma(S)$ equals 0_G, the identity of G. The studies of zero-sum sequences over finite abelian groups can be traced back to classical works of Erdős, Ginzburg and Ziv [9] and Olson [28, 29]; we refer to [12] for a survey on zero-sum theory. We denote

$$\mathsf{M}(G, k) = \{S \text{ is a sequence over } G \mid \sigma(S) = 0 \text{ and } |S| = k\}.$$

For any monomial $\prod_{i=0}^{n-1} m_{i,\tau(i)} = \prod_{i=0}^{n-1} (x_i \dot{+} x_{\tau(i)})$ in $\mathsf{per}(\mathcal{M}_G)$, it is easy to see that the sum of the n elements in this monomial is 0_G. Therefore, we have the relation $\mathcal{P}(G) \leqslant |\mathsf{M}(G, |G|)|$. In 1952, with an elegant constructive approach, Hall [19] proved that $\mathcal{P}(G) = |\mathsf{M}(G, |G|)|$. In this paper, we show that $\mathcal{P}(G)$ is a characterization for finite abelian groups.

Theorem 1. *Let G and H be finite abelian groups. We have*

$$\mathcal{P}(G) = \mathcal{P}(H) \iff G \cong H.$$

Let $f \in \mathbb{C}[x_1, \cdots, x_n]$ and $g \in \mathbb{C}[y_1, \cdots, y_n]$, we say that f and g are similar (denoted by $f \approx g$) if there is a bijection $\varphi : \{x_1, \cdots, x_n\} \to \{y_1, \cdots, y_n\}$ such that $f(\varphi(x_1), \cdots, \varphi(x_n)) = g(y_1, \cdots, y_n)$. In 1991, based on classical results of Frobenius and Dieudonné on group determinants, Formanek and Sibley [10] proved that, for any finite groups G and H, $\mathsf{det}(\mathcal{M}_G) \approx \mathsf{det}(\mathcal{M}_H)$ if and only if $G \cong H$; also see [22, 25]. Later in 2014, Donovan, Johnson and Wanless [5] showed that, for any finite groups G and H, if there is a bijection

$$\psi : \{x_g \mid g \in G\} \to \{x_h \mid h \in H\} \text{ (with } x_{0_G} \mapsto x_{0_H})$$

such that $\mathsf{per}(\mathcal{M}_G)$ is similar to $\mathsf{per}(\mathcal{M}_H)$ via the bijection ψ, then $G \cong H$. Moreover, they proposed an open question that whether the above result holds without the assumption that x_{0_G} maps to x_{0_H}.

Problem 2. ([5, Section 8]) Let G and H be finite groups. Is it true that

$$\mathsf{per}(\mathcal{M}_G) \approx \mathsf{per}(\mathcal{M}_H) \;\Leftrightarrow\; G \cong H?$$

It is easy to see that Theorem 1 answers Problem 2 in the abelian case.

Note that, based on Hall's result, Theorem 1 is equivalent to the statement that, for any abelian groups G and H, $|\mathsf{M}(G,|G|)| = |\mathsf{M}(H,|H|)|$ if and only if $G \cong H$. Therefore, we obtain a characterization of finite abelian groups in terms of number of zero-sum sequences. We remark that, there is also a long-standing and fascinating problem of characterizing finite abelian groups in terms of certain factorization property of zero-sum sequences, we refer to [13, 14, 15, 16] for detailed discussions and some recent progress.

To prove Theorem 1, it is natural to consider a counting formula for $\mathcal{P}(G)$ (equivalently, for $|\mathsf{M}(G,|G|)|$). In fact, Theorem 1 is essentially a consequence in our study of the following combinatorial problem on $|\mathsf{M}(G,k)|$.

Let C_n be a cyclic group with n elements. In 1975, Fredman [11] observed the following very interesting reciprocity

$$|\mathsf{M}(C_n,m)| = |\mathsf{M}(C_m,n)| \tag{1}$$

using generating functions as well as a necklace interpretation. Later in 1999, Elashvili, Jibladze and Pataraia [7, 8] rediscovered the same result with different method from invariant theory. It was remarked in [8, Introduction] that N. Alon also independently proved (1) when $(n,m) = 1$. Meanwhile, G. Andrews, N. Alon and R. Stanley independently obtained the counting formula for $\mathsf{M}(C_n,m)$; see [8, Introduction and Section 3]. In 2011, Panyushev [30] provided an extension of Fredman's reciprocity in terms of symmetric tensor exterior algebras.

Assume that $G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$, where $1 < n_1 | \cdots | n_r \in \mathbb{N}$. For any positive integer m, recall the following counting formula

$$|\mathsf{M}(G,m)| = \frac{1}{n+m} \sum_{d|(n,m)} \varphi_G(d) \binom{n/d + m/d}{n/d}, \tag{2}$$

where

$$\varphi_G(d) = \sum_{\ell | d} \mu(\frac{d}{\ell}) \prod_{i=1}^{r} (n_i, \ell)$$

is the number of elements in G of order d; see [21, 26] for proofs. It follows immediately from (2) that, if

$$\varphi_G(d) = \varphi_H(d) \text{ for any } d|(|G|,|H|), \tag{3}$$

then we have

$$|\mathsf{M}(G,|H|)| = |\mathsf{M}(H,|G|)|. \tag{4}$$

In particular, if $(|G|, |H|) = 1$, then

$$|\mathsf{M}(G, |H|)| = |\mathsf{M}(H, |G|)| = \frac{1}{|G| + |H|}\binom{|G| + |H|}{|G|, |H|}, \tag{5}$$

which are called the rational Catalan numbers. Recently, Han and the second author [21] provided a combinatorial interpretation of (5) using rational Catalan combinatorics, based on a correspondence between zero-sum sequences and rational Dyck paths.

In this paper, we prove that (3) is not only a sufficient condition but also a necessary condition for the reciprocity (4) to hold. This answers the Problem 5.2 in [21].

Theorem 3. *Let G and H be two finite abelian groups. Then we have*

$$|\mathsf{M}(G, |H|)| = |\mathsf{M}(H, |G|)|$$

if and only if $\varphi_G(d) = \varphi_H(d)$ for any $d|(|G|, |H|)$.

We will see that Theorem 1 is essentially a consequence of Theorem 3. It is possible to extend Theorem 3 to the non-abelian setting in terms of invariant theory and we shall provide some results in Section 4.

In [30], Panyushev observed that $\mathcal{P}(C_2 \oplus C_2) > \mathcal{P}(C_4)$, and he speculated that $\mathcal{P}(G) \geqslant \mathcal{P}(C_n)$ when $|G| = n$. More generally, Panyushev proposed the following interesting problem (using our notation).

Problem 4. ([30, Problem 3]) Let G be a finite abelian group of order n and C_n a cyclic group of order n. For any integer $m \geqslant 2$, is it true that

$$|\mathsf{M}(G, m)| \geqslant |\mathsf{M}(C_n, m)|?$$

As an application of our method, we answer Problem 4 affirmatively (see Proposition 11). In particular, Proposition 11 implies that $\mathcal{P}(G) > \mathcal{P}(C_n)$ for any non-cyclic abelian group G of order n. This result is also related a more general open question of Donovan, Johnson and Wanless [5, Section 8] concerning the latin squares of a given order n.

The rest of this paper is organized as follows. In Section 2, we introduce some definitions as well as some auxiliary lemmas. In Section 3, we prove our main results. In Section 4, we consider an extension of Theorem 3 to the non-abelian setting in terms of invariant theory. In Section 5, we provide some further discussions.

2 Preliminaries

In this section, we introduce some definitions and notation, as well as some auxiliary results.

Let $\mathbb{C}$ be the field of complex numbers. Denote by $\mathbb{N}$ the set of positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Let G be a finite abelian group. By the fundamental theorem of finite abelian groups we have

$$G \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$$

where $1 < n_1 | \cdots | n_r \in \mathbb{N}$ are positive integers. Moreover, $n_1, \ldots, n_r$ are uniquely determined by G. We denote by $\mathrm{ord}(g)$ the order of an element g in a group. For any prime p, we denote by $\mathrm{Syl}_p(G)$ the Sylow p-subgroup of G.

Now, we prove some auxiliary lemmas, which will be repeatedly used in the subsequent proofs. The first two technical lemmas are some inequalities involving binomial coefficients.

Lemma 5. *Let $m, n, a, b \geqslant 2$ be integers and $a, b | (m, n)$.*

(i) *If $b > a$, we have*

$$\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} \Big/ \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \geqslant (1 + \frac{m}{n})^{n(\frac{1}{a} - \frac{1}{b})} (1 + \frac{a}{b} \frac{n}{m})^{m(\frac{1}{a} - \frac{1}{b})}.$$

Consequently, $\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} > \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}}$.

(ii) *If $b \geqslant 2a$, we have*

$$a \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} > \max\{m, n\} \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}}.$$

Proof. (i) Since $b > a$, we have

$$\begin{aligned}
\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} &= \frac{(\frac{m+n}{a})!}{\frac{m}{a}! \frac{n}{a}!} = \frac{\prod_{i=\frac{m+n}{b}+1}^{\frac{m+n}{a}} i}{\prod_{j=\frac{m}{b}+1}^{\frac{m}{a}} j \prod_{k=\frac{n}{b}+1}^{\frac{n}{a}} k} \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \\
&= \prod_{j=\frac{m}{b}+1}^{\frac{m}{a}} \frac{\frac{n}{b} + j}{j} \prod_{k=\frac{n}{b}+1}^{\frac{n}{a}} \frac{\frac{m}{a} + k}{k} \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \\
&\geqslant \prod_{j=\frac{m}{b}+1}^{\frac{m}{a}} \frac{\frac{n}{b} + \frac{m}{a}}{\frac{m}{a}} \prod_{k=\frac{n}{b}+1}^{\frac{n}{a}} \frac{\frac{m}{a} + \frac{n}{a}}{\frac{n}{a}} \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \\
&= (1 + \frac{m}{n})^{n(\frac{1}{a} - \frac{1}{b})} (1 + \frac{a}{b} \frac{n}{m})^{m(\frac{1}{a} - \frac{1}{b})} \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}},
\end{aligned}$$

as desired.

(ii) Without loss of generality, we assume that $m \geqslant n$. Note that

$$a \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} = a \frac{\frac{m+n}{a} \cdots (\frac{m}{a} + 2)(\frac{m}{a} + 1)}{\frac{n}{a}(\frac{n}{a} - 1) \cdots 2 \cdot 1} \geqslant (m + a) \prod_{j=2}^{\frac{n}{a}} \frac{\frac{m}{a} + j}{j}.$$

Using the fact that $\frac{n}{a} - 1 \geqslant \frac{n}{b}$ and that $\frac{b}{a} \geqslant 2 \geqslant \frac{j+1}{j}$ (which implies $\frac{\frac{m}{a}+j+1}{j+1} \geqslant \frac{\frac{m}{b}+j}{j}$) for all $j \geqslant 1$, we have

$$\prod_{j=2}^{\frac{n}{a}} \frac{\frac{m}{a} + j}{j} = \prod_{j=1}^{\frac{n}{a}-1} \frac{\frac{m}{a} + j + 1}{j + 1} \geqslant \prod_{j=1}^{\frac{n}{b}} \frac{\frac{m}{a} + j + 1}{j + 1} \geqslant \prod_{j=1}^{\frac{n}{b}} \frac{\frac{m}{b} + j}{j} = \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}}.$$

It follows that

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} \geqslant (m+a)\prod_{j=2}^{\frac{n}{a}}\frac{\frac{m}{a}+j}{j} > m\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}.$$

This completes the proof. $\square$

Lemma 6. *Let $n=p^{\alpha}q^{\beta}n', m=p^{\gamma}q^{\delta}m'$ be positive integers, where p and q are distinct primes, $(n',pq)=(m',pq)=1$, and $\alpha,\beta,\gamma,\delta\in\mathbb{N}$. Suppose that $a=p^s$, $b=q^t$ $(s,t\geqslant 1)$ satisfy $b<2a$ and $a,b|(m,n)$. Denote*

$$\Delta_{m,n}(a,b) := p^{\alpha+\gamma-2s-1}q^{\beta-t}m'n'.$$

(i) *If $n(\frac{1}{a}-\frac{1}{b})\geqslant 3$ and $\{a,b\}\neq\{2,3\}$, then*

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}\Big/\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} > 2\Delta_{m,n}(a,b)q^{\delta}.$$

Consequently, if $\Delta_{m,n}(a,b)\geqslant 1$, then we have

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} - (q^{\delta}-q^{t})\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} > 2b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}. \tag{6}$$

Moreover, (6) *always holds when $\{a,b\}=\{2,3\}$.*

(ii) *If $n(\frac{1}{a}-\frac{1}{b})=2$, and $\{a,b\}\neq\{2,3\}$, then*

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}\Big/\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} > \Delta_{m,n}(a,b)q^{\delta}.$$

Consequently, if $\Delta_{m,n}(a,b)\geqslant 1$, then we have

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} - (q^{\delta}-q^{t})\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} > b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}. \tag{7}$$

Proof. Without loss of generality, we assume that $m\geqslant n$.

(i) As $n(\frac{1}{a}-\frac{1}{b})\geqslant 3$, by Lemma 5, we have

$$\begin{aligned}
a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}\Big/\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} &\geqslant a(1+\tfrac{m}{n})^{n(\frac{1}{a}-\frac{1}{b})}(1+\tfrac{a}{b}\tfrac{n}{m})^{m(\frac{1}{a}-\frac{1}{b})}\\
&> a\left(\tfrac{m}{n}n(\tfrac{1}{a}-\tfrac{1}{b})+\tfrac{m^2}{n^2}n(\tfrac{1}{a}-\tfrac{1}{b})\right)n(\tfrac{1}{a}-\tfrac{1}{b})\tfrac{a}{b}\\
&\geqslant 2amn(\tfrac{1}{a}-\tfrac{1}{b})^2\tfrac{a}{b}\\
&= 2\frac{mn}{pa^2bq^{\delta}}q^{\delta}\left((b-a)^2\frac{pa^2}{b^2}\right)\\
&= 2\Delta_{m,n}(a,b)q^{\delta}\left((b-a)^2\tfrac{pa^2}{b^2}\right).
\end{aligned}$$

It suffices to prove that $(b-a)^2\frac{pa^2}{b^2}\geqslant 1$. If $b-a\geqslant 2$, as $b<2a$, then we have $(b-a)^2\frac{pa^2}{b^2}\geqslant \frac{4a^2}{b^2}p>p$. Therefore, we may assume that $b=a+1$. In this setting, as $\{a,b\}\neq\{2,3\}$, we have $a\geqslant 3$ and $(b-a)^2\frac{pa^2}{b^2}=\frac{pa^2}{(a+1)^2}=\frac{p}{(1+1/a)^2}\geqslant\frac{9}{16}p>1$.

Now, we consider the case $\{a,b\}=\{2,3\}$. In this case, we have $(b-a)^2\frac{pa^2}{b^2}=\frac{8}{9}$, where $p=2$. As $n(\frac{1}{2}-\frac{1}{3})\geqslant 3$, we have $n\geqslant 18$. Now, it is easy to check that $\Delta_{m,n}(a,b)\geqslant 2$ and therefore $\Delta_{m,n}(a,b)(b-a)^2\frac{pa^2}{b^2}>1$. Consequently, we have

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}>2\Delta_{m,n}(a,b)q^{\delta}\left((b-a)^2\frac{pa^2}{b^2}\right)\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}>2q^{\delta}\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}},$$

and (6) follows.

(ii) In this case, by Lemma 5, we have

$$\begin{aligned}a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}\Big/\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}} &\geqslant a(1+\tfrac{m}{n})^{n(\frac{1}{a}-\frac{1}{b})}(1+\tfrac{a}{b}\tfrac{n}{m})^{m(\frac{1}{a}-\frac{1}{b})}\\ &> am(\tfrac{1}{a}-\tfrac{1}{b})n(\tfrac{1}{a}-\tfrac{1}{b})\tfrac{a}{b}\\ &= amn(\tfrac{1}{a}-\tfrac{1}{b})^2\tfrac{a}{b}\\ &= \Delta_{m,n}(a,b)q^{\delta}\left((b-a)^2\tfrac{pa^2}{b^2}\right).\end{aligned}$$

Similar to the above, we have $(b-a)^2\frac{pa^2}{b^2}\geqslant 1$ and the desired result follows. □

The following three lemmas, whose proofs are based on the structure of finite abelian groups, are very useful in our subsequent proofs.

Lemma 7. *Let G (resp. H) be a finite abelian group of order n (resp. m). Denote*

$$\mathcal{E}_G:=\{d\in\mathbb{N}\mid \varphi_G(d)>\varphi_H(d)\text{ for }d|(|G|,|H|)\},$$
$$\mathcal{E}_H:=\{d\in\mathbb{N}\mid \varphi_G(d)<\varphi_H(d)\text{ for }d|(|G|,|H|)\}.$$

If $\mathcal{E}_G$ (resp. $\mathcal{E}_H$) is nonempty, then $\min\mathcal{E}_G$ (resp. $\min\mathcal{E}_H$) is a prime power.

Proof. Let

$$n=\prod_{i=1}^{\ell}p_i^{n_i},\quad m=\prod_{i=1}^{\ell}p_i^{m_i},$$

where $n_i,m_i\geqslant 0$ for $1\leqslant i\leqslant\ell$. First, we assume that $\mathcal{E}_G$ is nonempty.

For any $d|(n,m)$, let $d=\prod_{i=1}^{\ell}p_i^{d_i}$, where $d_i\geqslant 0$ and $d_i\leqslant\min\{m_i,n_i\}$ for $1\leqslant i\leqslant\ell$. Note that,

$$G=\mathrm{Syl}_{p_1}(G)\oplus\cdots\oplus\mathrm{Syl}_{p_\ell}(G).$$

Therefore, $g=(g_1,g_2,\cdots,g_\ell)\in G$ (where $g_i\in\mathrm{Syl}_{p_i}(G)$) has order d if and only if $\mathrm{ord}(g_i)=p_i^{d_i}$. It follows that

$$\varphi_G(d)=\prod_{i=1}^{\ell}\varphi_{\mathrm{Syl}_{p_i}(G)}(p_i^{n_i}).$$

Consequently, if $\varphi_G(d) > \varphi_H(d)$, we must have

$$\varphi_G(p_i^{d_i}) = \varphi_{\mathrm{Syl}_{p_i}(G)}(p_i^{d_i}) > \varphi_{\mathrm{Syl}_{p_i}(H)}(p_i^{d_i}) = \varphi_H(p_i^{d_i})$$

for some $i \in \{1, \cdots, \ell\}$. The desired result follows immediately. It is easy to see that the proof is similar when $\mathcal{E}_H$ is nonempty. ☐

Lemma 8. *Let G be a finite abelian group of order n and H a finite abelian group of order m. Let $n = q^\beta n'$ and $m = q^\delta m'$ with $(m', q) = (n', q) = 1$. Let*

$$\mathcal{E} = \{k \in \mathbb{N} \mid \varphi_G(q^k) \neq \varphi_H(q^k),\ q^k | (m, n)\}.$$

Suppose that $\mathcal{E}$ is nonempty and let $t = \min \mathcal{E}$. If $\varphi_G(q^t) < \varphi_H(q^t)$, then we have $q^{t+1}|m$, i.e., $\delta > t$. Moreover,

$$q^t \leqslant \varphi_H(q^t) - \varphi_G(q^t) \leqslant q^\delta - q^t.$$

Proof. Let

$$\mathrm{Syl}_q(G) = C_{q^{n_1}} \oplus \cdots \oplus C_{q^{n_c}}, \quad \mathrm{Syl}_q(H) = C_{q^{m_1}} \oplus \cdots \oplus C_{q^{m_d}},$$

where $1 \leqslant n_1 \leqslant \cdots \leqslant n_c$ and $1 \leqslant m_1 \leqslant \cdots \leqslant m_d$. As $\varphi_G(q^t) < \varphi_H(q^t)$, we have $m_d \geqslant t$. We claim that $d \geqslant 2$. Otherwise, we also have $c = 1$. In other words, both $\mathrm{Syl}_q(G)$ and $\mathrm{Syl}_q(H)$ are cyclic groups of order $\geqslant p^t$. So $\varphi_G(q^t) = q^t - q^{t-1} = \varphi_H(q^t)$ which contradicts our assumption. This proves the claim. Note that $d \geqslant 2$ implies $q^{m_1+m_d}|m$, that is $q^{t+1}|m$.

It is easy to show that $\sum_{i=0}^{t} \varphi_G(q^i) = q^{e_1}$ and $\sum_{j=0}^{t} \varphi_H(q^j) = q^{e_2}$ for some e_1 and e_2 with $t \leqslant e_1 < e_2 \leqslant \delta$. As $\varphi_H(q^i) = \varphi_G(q^i)$ for $i = 0, \cdots, t-1$, we have

$$\varphi_H(q^t) - \varphi_G(q^t) = \sum_{i=0}^{t} \left(\varphi_H(q^i) - \varphi_G(q^i)\right) = \sum_{i=0}^{t} \varphi_H(q^i) - \sum_{j=0}^{t} \varphi_G(q^j) = q^{e_2} - q^{e_1}.$$

Note that $q^t \leqslant q^{e_1}(q^{e_2-e_1} - 1) = q^{e_2} - q^{e_1} \leqslant q^\delta - q^t$. Therefore, we obtain

$$q^t \leqslant \varphi_H(q^t) - \varphi_G(q^t) \leqslant q^\delta - q^t.$$

This completes the proof. ☐

Lemma 9. *Let G (resp. H) be a finite abelian group of order n (resp. m). Let $n = p^\alpha n'$ and $m = p^\gamma m'$ with $(n', p) = (m', p) = 1$. Let*

$$\mathcal{E} = \{k \in \mathbb{N} \mid \varphi_G(p^k) \neq \varphi_H(p^k),\ p^k | (m, n)\}.$$

Suppose that $\mathcal{E}$ is nonempty and let $s = \min \mathcal{E}$. Assume that the following hold

1. *$s \geqslant 2$;*
2. *$p^{s+1} | (m, n)$;*

3. $\varphi_G(p^s) > \varphi_H(p^s)$*, but* $\varphi_G(p^{s+1}) < \varphi_H(p^{s+1})$*.*

Then we have $\alpha \geqslant s+2$ *and* $\gamma \geqslant s+2$*.*

Proof. Let

$$\mathrm{Syl}_p(G) = C_{p^{n_1}} \oplus \cdots \oplus C_{p^{n_c}} \text{ and } \mathrm{Syl}_p(H) = C_{p^{m_1}} \oplus \cdots \oplus C_{p^{m_d}},$$

where $1 \leqslant n_1 \leqslant \cdots \leqslant n_c$ and $1 \leqslant m_1 \leqslant \cdots \leqslant m_d$. Similar to the proof of Lemma 8, we have $c \geqslant 2$ and $n_c \geqslant s$, as $\varphi_G(p^k) = \varphi_H(p^k)$ for $k < s$ and $\varphi_G(p^s) > \varphi_H(p^s)$. Since $\varphi_G(p^{s+1}) < \varphi_H(p^{s+1})$, we have $m_d \geqslant s+1$. If $d=1$, then $\varphi_H(p) = p-1$. Therefore, we have $\varphi_G(p) = p^c - 1 \geqslant p^2 - 1 > p - 1 = \varphi_H(p)$ and $s \leqslant 1$, which contradicts the assumption that $s \geqslant 2$. Consequently, we have $d \geqslant 2$ and $p^{m_1+m_d} | m$, that is, $\gamma \geqslant s+2$.

Note that $\sum_{i=0}^{s} \varphi_G(p^i) = p^{e_1}$ and $\sum_{j=0}^{s} \varphi_H(p^j) = p^{e_2}$ for some positive integers e_1 and e_2. As $d \geqslant 2$ and $m_d \geqslant s+1$, we have $p^{e_2} \geqslant p^{s+1}$. Moreover, by the definition of s, we have $p^{e_1} > p^{e_2}$. Consequently, we obtain $e_1 > s+1$, which implies $\alpha \geqslant s+2$. □

3 Proofs of the main results

In this section, we finish the proofs of our main results. Firstly, we prove Theorem 3 and show that Theorem 3 implies a special case of Theorem 1. Then we provide the whole proof of Theorem 1. At the end of this section, we answer Problem 4 affirmatively.

Proof of Theorem 3. It suffices to prove that if $|\mathsf{M}(G, |H|)| = |\mathsf{M}(H, |G|)|$, then we have $\varphi_G(d) = \varphi_H(d)$ holds for any $d | (|G|, |H|)$. Assume to the contrary that there exists some $d | (|G|, |H|)$ such that $\varphi_G(d) \neq \varphi_H(d)$. Let $|G| = n$ and $|H| = m$.

Recall that

$$|\mathsf{M}(G, |H|)| = \frac{1}{m+n} \sum_{d|(m,n)} \varphi_G(d) \binom{\frac{m+n}{d}}{\frac{m}{d}, \frac{n}{d}}$$

and

$$|\mathsf{M}(H, |G|)| = \frac{1}{m+n} \sum_{d|(m,n)} \varphi_H(d) \binom{\frac{m+n}{d}}{\frac{m}{d}, \frac{n}{d}}.$$

Let

$$a = \min\{d \mid \varphi_G(d) \neq \varphi_H(d) \text{ for } d|(m,n)\}.$$

Without loss of generality, we assume that $\varphi_G(a) > \varphi_H(a)$. In this case, we shall prove that

$$|\mathsf{M}(G, |H|)| > |\mathsf{M}(H, |G|)|, \tag{8}$$

which contradicts our assumption.

If $\varphi_G(d) \geqslant \varphi_H(d)$ holds for any $d|(m,n)$, then the desired result follows immediately. Therefore, we assume that $\varphi_G(d) < \varphi_H(d)$ holds for some $d|(m,n)$ and let

$$b = \min\{d \mid \varphi_G(d) < \varphi_H(d) \text{ for } d|(m,n)\}.$$

Clearly, we have $a < b$. Moreover, by Lemma 7, both a and b are prime powers. Recall that

$$\mathcal{E}_H = \{e \in \mathbb{N} \mid \varphi_G(e) < \varphi_H(e) \text{ and } e|(m,n)\}.$$

We denote

$$\mathcal{F} := \{e \in \mathbb{N} \mid \varphi_G(e) > \varphi_H(e),\ e > a,\ \text{and } e|(m,n)\},$$

and

$$S_{\mathcal{F}} := \sum_{e \in \mathcal{F}} (\varphi_G(e) - \varphi_H(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}}.$$

It is clear that $S_{\mathcal{F}} > 0$. Therefore, we have

$$\begin{aligned}
&(m+n)\left(|\mathsf{M}(G, |H|)| - |\mathsf{M}(H, |G|)|\right) \\
= &\sum_{d|(m,n)} (\varphi_G(d) - \varphi_H(d)) \binom{\frac{m+n}{d}}{\frac{m}{d}, \frac{n}{d}} \\
= &(\varphi_G(a) - \varphi_H(a)) \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} + S_{\mathcal{F}} + \sum_{e \in \mathcal{E}_H} (\varphi_G(e) - \varphi_H(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}} \\
= &(\varphi_G(a) - \varphi_H(a)) \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} + S_{\mathcal{F}} - \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}} \\
\geqslant &a \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} + S_{\mathcal{F}} - \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}},
\end{aligned}$$

where the last inequality follows from Lemma 8.

Therefore, in order to prove (8), it suffices to show that

$$a \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} + S_{\mathcal{F}} > \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}}. \tag{9}$$

As a and b are prime powers, we may assume that $a = p^s$ and $b = q^t$ (p and q are primes, but not necessarily distinct).

If $b \geqslant 2a$, i.e., $q^t \geqslant 2p^s$, then by Lemma 5.(ii), we have

$$a \binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} > m \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \geqslant \sum_{e \in \mathcal{E}_H} \varphi_H(e) \binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} \geqslant \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}},$$

and (9) follows immediately.

If $a < b < 2a$, i.e., $p^s < q^t < 2p^s$, then we have

$$q^{t-1} = \frac{q^t}{q} < \frac{2p^s}{q} \leqslant p^s.$$

Consequently, we have $p \neq q$. Moreover, by the definition of $a = p^s$, we have $t = \min\{i \in \mathbb{N} \mid \varphi_G(q^i) \neq \varphi_H(q^i)\}$ and $\varphi_G(q^t) < \varphi_H(q^t)$. By Lemma 8, we have $q^{t+1}|m$ and $p^{s+1}|n$. Assume that

$$n = p^\alpha q^\beta n', \quad m = p^\gamma q^\delta m',$$

where $(n', pq) = (m', pq) = 1$. Then we have $a = p^s < b = q^t < 2p^s$ and $1 \leqslant s < \alpha$, $1 \leqslant t < \delta$, and $s \leqslant \gamma$, $t \leqslant \beta$. Consequently, we have $p | n(\frac{1}{a} - \frac{1}{b})$, which implies $n(\frac{1}{a} - \frac{1}{b}) \geqslant p \geqslant 2$. We distinguish two cases.

Case 1: Assume that $n(\frac{1}{a} - \frac{1}{b}) = 2$, that is, $b - a = 1$ and $p = 2$. In this case, we have $n = p^{s+1}q^t$.

Subcase 1.1: Assume that $s \geqslant 2$. First, we claim that $\gamma = s$. In fact, as $p^s|(m, n)$, we have $\gamma \geqslant s$. If $\gamma \geqslant s + 1$, then

$$\sum_{i=0}^{s+1} \varphi_H(p^i) \geqslant p^{s+1} = \sum_{i=0}^{s+1} \varphi_G(p^i) > \sum_{i=0}^{s} \varphi_H(p^i).$$

Therefore, $\varphi_H(p^{s+1}) > 0$. On the other hand, we have $\varphi_G(p^{s+1}) = 0$, as $\mathrm{Syl}_p(G)$ can not be a cyclic group. Hence, $\varphi_H(p^{s+1}) > \varphi_G(p^{s+1})$. By Lemma 9, we obtain $p^{s+2}|n$, a contradiction. So $\gamma \leqslant s$. This completes the proof of the claim.

Let $d|(m, n)$. In this case, $\varphi_G(d) > \varphi_H(d)$ if and only if $d = p^s q^i$ for $i = 0, 1, \cdots, t$, and $\varphi_G(d) < \varphi_H(d)$ if and only if $d = p^j q^t$ for $j = 0, 1, \cdots, s$. By Lemma 8, we have $\varphi_H(b) - \varphi_G(b) \leqslant q^\delta - q^t$. Recall that $\Delta_{m,n}(a, b) = p^{\alpha+\gamma-2s-1} q^{\beta-t} m'n'$. It is easy to see that $\Delta_{m,n}(a, b) \geqslant 1$. Note that $\{a, b\} \neq \{2, 3\}$, as $a = p^s \geqslant 4$. Since $n(\frac{1}{a} - \frac{1}{b}) = p = 2$, by Lemma 6.(ii), we have

$$\begin{aligned}
& a\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} - \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}} \\
\geqslant\ & a\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} - (q^\delta - q^t)\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{j=1}^{t} \varphi_H(p^j b) \binom{\frac{m+n}{p^j b}}{\frac{m}{p^j b}, \frac{n}{p^j b}} \\
\geqslant\ & b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{j=1}^{t} \varphi_H(p^j b) \binom{\frac{m+n}{pb}}{\frac{m}{pb}, \frac{n}{pb}} \\
\geqslant\ & b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - m \binom{\frac{m+n}{pb}}{\frac{m}{pb}, \frac{n}{pb}} > 0,
\end{aligned}$$

where the last inequality follows from Lemma 5.(ii). Therefore, (9) follows.

Subcase 1.2: Assume that $s = 1$. Therefore, $p^s = 2$ and $2 = p^s < q^t < 2p^s = 4$ which implies $q^t = 3$ and $n = p^{s+1}q^t = 12$. In this case, $G = C_2 \oplus C_6$ and $H = C_{2^\gamma} \oplus H'$, where $|H'| = 3^\delta m'$. It is easy to verify that $2\binom{\frac{m}{2}+6}{6} > m\binom{\frac{m}{3}+4}{4}$ for all $m \geqslant 18$ and $6|m$. Therefore, we have

$$\begin{aligned}
& a\binom{\frac{m+n}{a}}{\frac{m}{a}, \frac{n}{a}} - \sum_{e \in \mathcal{E}_H} (\varphi_H(e) - \varphi_G(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}} \\
\geqslant\ & 2\binom{\frac{m+n}{2}}{\frac{n}{2}} - \sum_{e \in \mathcal{E}_H} \varphi_H(e) \binom{\frac{m+n}{3}}{\frac{n}{3}} \\
\geqslant\ & 2\binom{\frac{m}{2}+6}{6} - m\binom{\frac{m}{3}+4}{4} > 0.
\end{aligned}$$

Consequently, (9) follows.

Case 2: Assume that $n(\frac{1}{a}-\frac{1}{b})\geqslant 3$. Recall that $\Delta_{m,n}(a,b)=p^{\alpha+\gamma-2s-1}q^{\beta-t}m'n'$. As $\alpha+\gamma>2s$, $\Delta_{m,n}(a,b)\geqslant 1$. By Lemma 6.(i), we have

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}-(q^{\delta}-q^{t})\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}>2b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}. \tag{10}$$

We denote

$$\mathcal{E}_1:=\{e\in\mathcal{E}_H \mid b<e<2b\},\quad \mathcal{E}_2:=\{e\in\mathcal{E}_H \mid e\geqslant 2b\}.$$

By Lemma 8, we have $\varphi_H(b)-\varphi_G(b)\leqslant q^{\delta}-q^{t}$. Therefore, by (10), we obtain

$$\begin{aligned}
&S_{\mathcal{F}}+a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{m}{a}}-\sum_{e\in\mathcal{E}_H}(\varphi_H(e)-\varphi_G(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}\\
&\geqslant S_{\mathcal{F}}+a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{m}{a}}-(\varphi_H(b)-\varphi_G(b))\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e\in\mathcal{E}_1\cup\mathcal{E}_2}\varphi_H(e)\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}\\
&> S_{\mathcal{F}}+2b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_1\in\mathcal{E}_1}\varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1},\frac{n}{e_1}}-\sum_{e_2\in\mathcal{E}_2}\varphi_H(e_2)\binom{\frac{m+n}{e_2}}{\frac{m}{e_2},\frac{n}{e_2}}\\
&= S_{\mathcal{F}}+b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_1\in\mathcal{E}_1}\varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1},\frac{n}{e_1}}+b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_2\in\mathcal{E}_2}\varphi_H(e_2)\binom{\frac{m+n}{e_2}}{\frac{m}{e_2},\frac{n}{e_2}}.
\end{aligned}$$

Denote

$$\mathcal{S}_1:=S_{\mathcal{F}}+b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_1\in\mathcal{E}_1}\varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1},\frac{n}{e_1}}$$

and

$$\mathcal{S}_2:=b\binom{\frac{m+n}{b}}{\frac{m}{b}\,\frac{n}{b}}-\sum_{e_2\in\mathcal{E}_2}\varphi_H(e_2)\binom{\frac{m+n}{e_2}}{\frac{m}{e_2},\frac{n}{e_2}}.$$

In order to prove (9), it suffices to show that $\mathcal{S}_1>0$ and $\mathcal{S}_2>0$.

First, we consider $\mathcal{S}_2$, as it is easier to handle. If $\mathcal{E}_2$ is empty, then the desired result follows. Assume that $\mathcal{E}_2$ is not empty, let $c=\min\mathcal{E}_2$. By definition, we have $c\geqslant 2b$. Therefore, by Lemma 5.(ii), we have

$$\begin{aligned}
b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_2\in\mathcal{E}_2}\varphi_H(e_2)\binom{\frac{m+n}{e_2}}{\frac{m}{e_2},\frac{n}{e_2}} &\geqslant b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_2\in\mathcal{E}_2}\varphi_H(e_2)\binom{\frac{m+n}{c}}{\frac{m}{c},\frac{n}{c}}\\
&\geqslant b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-m\binom{\frac{m+n}{c}}{\frac{m}{c},\frac{n}{c}}>0.
\end{aligned}$$

Therefore, $\mathcal{S}_2>0$, as desired.

Next, we consider $\mathcal{S}_1$. If $\mathcal{E}_1$ is empty, then the desired result follows. So, we may assume that $\mathcal{E}_1$ is not empty. First, we claim that $\mathcal{E}_1$ consists of powers of distinct primes, i.e., $\mathcal{E}_1=\{q_1^{t_1},q_2^{t_2},\cdots,q_v^{t_v}\}$, where $q_i\neq q_j$ for $i\neq j$. For each $e_1\in\mathcal{E}_1$, by definition, $\varphi_G(e_1)<\varphi_H(e_1)$ and $q^t<e_1<2q^t$. Therefore, there is some prime power ℓ^k such that

$e_1 = \ell^k e_1'$ ($e_1' \in \mathbb{N}$) and $\varphi_G(\ell^k) < \varphi_H(\ell^k)$. If $e_1' \geqslant 2$, we have $\ell^k = \frac{e_1}{2} < \frac{2q^t}{2} = q^t$ which contradicts the definition of $b = q^t$. Therefore, we have $e_1' = 1$. This completes the proof of the claim.

Denote

$$\mathcal{E}_1^G := \{\ell^k \in \mathcal{E}_1 \mid \ell \neq p \text{ and } \varphi_G(\ell^i) > \varphi_H(\ell^i) \text{ for some } i < k\}.$$

For any $\ell^k \in \mathcal{E}_1^G$, let $u = \min\{i \in \mathbb{N} \mid \varphi_G(\ell^i) > \varphi_H(\ell^i)\}$. Moreover, by the definitions of b and $\mathcal{E}_1$, we also have

$$u = \min\{i \in \mathbb{N} \mid \varphi_G(\ell^i) \neq \varphi_H(\ell^i)\}.$$

By Lemma 8, we have $\varphi_G(\ell^u) - \varphi_H(\ell^u) \geqslant \ell^u$. By Lemma 5.(ii), we have

$$(\varphi_G(\ell^u) - \varphi_H(\ell^u))\binom{\frac{m+n}{\ell^u}}{\frac{m}{\ell^u}, \frac{n}{\ell^u}} \geqslant \ell^u \binom{\frac{m+n}{\ell^u}}{\frac{m}{\ell^u}, \frac{n}{\ell^u}} > \varphi_H(\ell^k)\binom{\frac{m+n}{\ell^k}}{\frac{m}{\ell^k}, \frac{n}{\ell^k}}. \tag{11}$$

Recall that $S_{\mathcal{F}} = \sum_{e\in\mathcal{F}} (\varphi_G(e) - \varphi_H(e)) \binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}}$. Since $\mathcal{E}_1^G$ consists of powers of distinct primes (which are different from p, q), by (11), we obtain

$$\begin{aligned}
& S_{\mathcal{F}} + b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{e_1\in\mathcal{E}_1} \varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1}, \frac{n}{e_1}} \\
= \;& S_{\mathcal{F}} - \sum_{e\in\mathcal{E}_1^G} \varphi_H(e)\binom{\frac{m+n}{e}}{\frac{m}{e}, \frac{n}{e}} + b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{e_1\in\mathcal{E}_1\setminus\mathcal{E}_1^G} \varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1}, \frac{n}{e_1}} \\
\geqslant \;& b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{e_1\in\mathcal{E}_1\setminus\mathcal{E}_1^G} \varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1}, \frac{n}{e_1}}.
\end{aligned}$$

As a result, in order to prove $\mathcal{S}_1 > 0$, it suffices to show that

$$b\binom{\frac{m+n}{b}}{\frac{m}{b}, \frac{n}{b}} - \sum_{e_1\in\mathcal{E}_1\setminus\mathcal{E}_1^G} \varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1}, \frac{n}{e_1}} > 0. \tag{12}$$

If $\mathcal{E}_1 \setminus \mathcal{E}_1^G$ is empty, then clearly we have $\mathcal{S}_1 > 0$. Therefore, suppose that $\mathcal{E}_1 \setminus \mathcal{E}_1^G$ is nonempty. Without loss of generality, we may assume that

$$\mathcal{E}_1 \setminus \mathcal{E}_1^G = \{q_1^{t_1}, \cdots, q_L^{t_L}\},$$

where $L \leqslant v$ and $q_1^{t_1} < \cdots < q_L^{t_L}$. We denote $b_0 := b$ (with $q_0 := q$ and $t_0 := t$) and $b_i := q_i^{t_i}$ for $i = 1, 2, \cdots, L$. Therefore, $b_0 < b_1 < b_2 < \cdots < b_L < 2b = 2q^t$. For each $i = 0, 1, \cdots, L-1$, let

$$n = q_i^{\beta_i} q_{i+1}^{\beta_{i+1}} n_i, \quad m = q_i^{\delta_i} q_{i+1}^{\delta_{i+1}} m_i,$$

where $(n_i, q_i q_{i+1}) = (m_i, q_i q_{i+1}) = 1$, and denote

$$\Delta_{m,n}(b_i, b_{i+1}) := q_i^{\beta_i+\delta_i-2t_i-1} q_{i+1}^{\beta_{i+1}-t_{i+1}} m_i n_i.$$

In the following, we shall prove that

$$b_i\binom{\frac{m+n}{b_i}}{\frac{m}{b_i},\frac{n}{b_i}}-\varphi_H(b_{i+1})\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}}>b_{i+1}\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}},\quad i=0,1,\cdots,L-1. \tag{13}$$

Note that, if (13) holds, then we have

$$\sum_{i=0}^{L-1}\left(b_i\binom{\frac{m+n}{b_i}}{\frac{m}{b_i},\frac{n}{b_i}}-\varphi_H(b_{i+1})\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}}\right)>\sum_{i=0}^{L-1}b_{i+1}\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}},$$

which implies

$$b_0\binom{\frac{m+n}{b_0}}{\frac{m}{b_0},\frac{n}{b_0}}-\sum_{i=0}^{L-1}\varphi_H(b_{i+1})\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}}>b_L\binom{\frac{m+n}{b_L}}{\frac{m}{b_L},\frac{n}{b_L}}.$$

Therefore, we have

$$b\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}-\sum_{e_1\in\mathcal{E}_1\setminus\mathcal{E}_1^G}\varphi_H(e_1)\binom{\frac{m+n}{e_1}}{\frac{m}{e_1},\frac{n}{e_1}}>b_L\binom{\frac{m+n}{b_L}}{\frac{m}{b_L},\frac{n}{b_L}}>0,$$

and (12) follows.

Now, we prove (13). Note that, for each $i=0,1,\cdots,L-1$,

- if $q_i=p$, then we have $q_i^{t_i}=p^{s+1}$, as $q_i^{t_i}<2b<4p^s$;
- if $q_i\neq p$, by Lemma 8 (note that $t_i=\min\{j \mid \varphi_G(q_i^j)\neq\varphi_H(q_i^j)\}$ and that $\varphi_G(q_i^{t_i})<\varphi_H(q_i^{t_i})$ as $b_i=q_i^{t_i}\in\mathcal{E}_1\setminus\mathcal{E}_1^G$), we have $\delta_i>t_i$;
- we have $\{b_i,b_{i+1}\}\neq\{2,3\}$, as $b_i>q^t\geqslant 2$.

We distinguish three cases.

Subcase 2.1: Assume that $b_{i+1}\neq p^{s+1}$. It is easy to verify that, if n has at least three different prime divisors, then $n(\frac{1}{b_i}-\frac{1}{b_{i+1}})\geqslant 3$.

If $b_i\neq p^{s+1}$, as mentioned above, we have $\delta_i>t_i$. Therefore, p, q_i, and q_{i+1} are different prime divisors of n.

If $b_i=p^{s+1}$, we have q, p, and q_{i+1} are different prime divisors of n. Moreover, we have $q^t|n_i$ and $\frac{n_i}{q_i}\geqslant\frac{q^t}{q_i}\geqslant\frac{q^t}{p^s}>1$, where $q_i=p$.

Therefore, we always have that $n(\frac{1}{b_i}-\frac{1}{b_{i+1}})\geqslant 3$ and $\Delta_{m,n}(b_i,b_{i+1})\geqslant 1$. By Lemma 6.(i), we have

$$b_i\binom{\frac{m+n}{b_i}}{\frac{m}{b_i},\frac{n}{b_i}}>2\Delta_{m,n}(b_i,b_{i+1})q_{i+1}^{\delta_{i+1}}\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}}\geqslant 2q_{i+1}^{\delta_{i+1}}\binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}},\frac{n}{b_{i+1}}}.$$

As $b_{i+1}<q_{i+1}^{\delta_{i+1}}$ and $\varphi_H(b_{i+1})<q_{i+1}^{\delta_{i+1}}$, (13) follows.

Subcase 2.2: Assume that $b_{i+1} = p^{s+1}$ and $s \geqslant 2$. In this case, by Lemma 9, we have $p^{s+2}|n$. Consequently, $p|n(\frac{1}{b_i} - \frac{1}{b_{i+1}})$, which implies $n(\frac{1}{b_i} - \frac{1}{b_{i+1}}) \geqslant 2$. Moreover, as $\delta_i > t_i$ and $\beta_{i+1} \geqslant s+2 > s+1 = t_{i+1}$, we have $\Delta_{m,n}(b_i, b_{i+1}) \geqslant p \geqslant 2$. By Lemma 6, we obtain

$$b_i \binom{\frac{m+n}{b_i}}{\frac{m}{b_i}, \frac{n}{b_i}} > \Delta_{m,n}(b_i, b_{i+1}) p^{\delta_{i+1}} \binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}}, \frac{n}{b_{i+1}}} \geqslant 2p^{\delta_{i+1}} \binom{\frac{m+n}{b_{i+1}}}{\frac{m}{b_{i+1}}, \frac{n}{b_{i+1}}}.$$

As $b_{i+1} < p^{\delta_{i+1}}$ and $\varphi_H(b_{i+1}) < p^{\delta_{i+1}}$, (13) follows.

Subcase 2.3: Assume that $b_{i+1} = p^{s+1}$ and $s = 1$. In this case, we have $p \leqslant 3$. In fact, as $b < 2p^s \leqslant p^{s+1} < 2b$, we have $p/2 = p^{s+1}/2p^s < 2b/b = 2$.

Subcase 2.3.1: Assume that $p = 2$. In this case, we have that $a = p^s = 2$ and $b = q^t = 3$ and $\mathcal{E}_1 \setminus \mathcal{E}_1^G \subseteq \{4, 5\}$. Therefore, it suffices to consider the case $b_0 = q^{t_0} = 3$ and $b_1 = p^{s+1} = 4$. Note that $n(\frac{1}{a} - \frac{1}{b}) \geqslant 3$. Therefore, $n \geqslant 18$. Hence $n(\frac{1}{b_0} - \frac{1}{b_1}) \geqslant \frac{18}{16} > 1$ which implies that $n(\frac{1}{b_0} - \frac{1}{b_1}) \geqslant 2$. If $n(\frac{1}{3} - \frac{1}{4}) = 2$ (i.e., $n = 24$), then $\Delta_{m,n}(b_0, b_1) \geqslant 2$ (as $\delta_0 > t_0$ and $\beta_1 = 3$ and $t_1 = 2$). Therefore, by Lemma 6.(ii), we have

$$b_0 \binom{\frac{m+n}{b_0}}{\frac{m}{b_0}, \frac{n}{b_0}} > \Delta_{m,n}(b_0, b_1) 2^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}} \geqslant 2 \cdot 2^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}}.$$

If $n(\frac{1}{3} - \frac{1}{4}) \geqslant 3$, as $\Delta_{m,n}(b_0, b_1) \geqslant 1$, by Lemma 6.(i),

$$b_0 \binom{\frac{m+n}{b_0}}{\frac{m}{b_0}, \frac{n}{b_0}} > 2\Delta_{m,n}(b_0, b_1) 2^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}} \geqslant 2 \cdot 2^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}}.$$

As $b_1 < 2^{\delta_1}$ and $\varphi_H(b_1) < 2^{\delta_1}$, (13) follows.

Subcase 2.3.2: Assume that $p = 3$. In this case, $q^t \in \{4, 5\}$. If $q^t = 4$, then $\mathcal{E}_1 \setminus \mathcal{E}_1^G \subseteq \{5, 7\}$, which contains no powers of p. Therefore, we only need to consider $q^t = 5$. As a result, we have $a = p^s = 3$ and $b = q^t = 5$, and $\mathcal{E}_1 \setminus \mathcal{E}_1^G \subseteq \{7, 8, 9\}$. It suffices to consider the following three cases

$$(1): \ \{b_0, b_1\} = \{5, 9\}, \quad (2): \ \{b_0, b_1\} = \{7, 9\}, \quad (3): \ \{b_0, b_1\} = \{8, 9\}.$$

Clearly, we have $\Delta_{m,n}(b_0, b_1) \geqslant 1$, as $\delta_0 > t_0$. For the case (1), we have $n(\frac{1}{5} - \frac{1}{9}) \geqslant 4$ as $5|n$ and $9|n$. For the cases (2) and (3), n has at least three different prime divisors. Therefore, we always have $n(\frac{1}{b_0} - \frac{1}{b_1}) \geqslant 3$. By Lemma 6.(i),

$$b_0 \binom{\frac{m+n}{b_0}}{\frac{m}{b_0}, \frac{n}{b_0}} > 2\Delta_{m,n}(b_0, b_1) 3^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}} \geqslant 2 \cdot 3^{\delta_1} \binom{\frac{m+n}{b_1}}{\frac{m}{b_1}, \frac{n}{b_1}}.$$

As $b_1 < 3^{\delta_1}$ and $\varphi_H(b_1) < 3^{\delta_1}$, (13) follows. This completes the proof. □

The following proposition is an easy consequence of Theorem 3.

Proposition 10. *Let G and H be abelian groups of order n, then we have*

$$|\mathsf{M}(G,n)| = |\mathsf{M}(H,n)| \Leftrightarrow G \cong H,$$

or equivalently

$$\mathcal{P}(G) = \mathcal{P}(H) \Leftrightarrow G \cong H.$$

Proof. It is easy to see that, (3) holds if and only if for all primes $p|(|G|,|H|)$, either $\mathrm{Syl}_p(G) \cong \mathrm{Syl}_p(H)$, or $\mathrm{Syl}_p(G)$ and $\mathrm{Syl}_p(H)$ are both cyclic. As $|G| = |H| = n$ and $|\mathsf{M}(G,n)| = |\mathsf{M}(H,n)|$, by Theorem 3 and the above discussion, we have $\mathrm{Syl}_p(G) \cong \mathrm{Syl}_p(H)$ for all primes $p|n$, which implies that $G \cong H$. $\square$

Note that Proposition 10 is a special case of Theorem 1. Now, we finish the proof of Theorem 1.

Proof of Theorem 1. By Proposition 10, it suffices to consider the case when G and H have different orders. Without loss of generality, we may assume that $|G| = n > m = |H|$.

Recall the counting formulas

$$|\mathsf{M}(G,n)| = \frac{1}{2n}\sum_{d|n}\varphi_G(d)\binom{2n/d}{n/d}$$

and

$$|\mathsf{M}(H,m)| = \frac{1}{2m}\sum_{d|m}\varphi_H(d)\binom{2m/d}{m/d}.$$

Let p be the smallest prime divisor of m. It is easy to see that

$$|\mathsf{M}(G,n)| > \frac{1}{2n}\binom{2n}{n}$$

and, by Lemma 5,

$$\frac{1}{2m}\left(\binom{2m}{m} + m\binom{2m/p}{m/p}\right) > |\mathsf{M}(H,m)|.$$

Therefore, it suffices to prove

$$\frac{1}{2n}\binom{2n}{n} > \frac{1}{2m}\left(\binom{2m}{m} + m\binom{2m/p}{m/p}\right). \tag{14}$$

By routine calculation (note that $n > m$ and $p \geqslant 2$), it can be verified that

$$\frac{1}{2n}\binom{2n-1}{n} > \frac{1}{2m}\binom{2m}{m} \tag{15}$$

and

$$\frac{1}{2n}\binom{2n-1}{n} > \frac{1}{2}\binom{2m/p}{m/p}. \tag{16}$$

By (15) and (16), we obtain (14) and the desired result follows. $\square$

Now, we answer Problem 4 by proving the following result.

Proposition 11. *Let G be a finite abelian group of order n and C_n a cyclic group of order n. Then for any integer $m \geqslant 2$, we have*

$$|\mathsf{M}(G,m)| \geqslant |\mathsf{M}(C_n,m)|,$$

where the equality holds if and only if either $(n,m)=1$ or for all primes $p|(n,m)$, $\mathrm{Syl}_p(G)$ is cyclic.

Proof. Note that

$$|\mathsf{M}(G,m)| = \frac{1}{m+n}\sum_{d|(m,n)} \varphi_G(d)\binom{\frac{m+n}{d}}{\frac{m}{d},\frac{n}{d}}$$

and

$$|\mathsf{M}(C_n,m)| = \frac{1}{m+n}\sum_{d|(m,n)} \varphi_{C_n}(d)\binom{\frac{m+n}{d}}{\frac{m}{d},\frac{n}{d}}.$$

If either $(n,m)=1$ or for all primes $p|(n,m)$, $\mathrm{Syl}_p(G)$ is cyclic, then clearly we have $|\mathsf{M}(G,m)| = |\mathsf{M}(C_n,m)|$.

Assume that $(n,m)>1$ and that there exists a prime $p|(n,m)$ such that $\mathrm{Syl}_p(G)$ is not cyclic. We shall prove that

$$|\mathsf{M}(G,m)| > |\mathsf{M}(C_n,m)|. \tag{17}$$

Let

$$a = \min\{p \mid \mathrm{Syl}_p(G) \text{ is not cyclic for prime } p|(m,n)\},$$

and

$$b = \min\{d \mid \varphi_G(d) < \varphi_{C_n}(d) \text{ for } d|(m,n)\}.$$

Note that $\varphi_G(a^t) < \varphi_{C_n}(a^t)$ for some $t \geqslant 2$. Clearly, we have $a<b$. We denote

- $\mathcal{E}_{C_n} := \{e \in \mathbb{N} \bigm| \varphi_G(e) < \varphi_{C_n}(e) \text{ and } e|(m,n)\}$;
- $\mathcal{F} := \{e \in \mathbb{N} \bigm| \varphi_G(e) > \varphi_{C_n}(e),\ e>a, \text{ and } e|(m,n)\}$;
- $S_{\mathcal{F}} := \sum_{e\in\mathcal{F}} (\varphi_G(e) - \varphi_{C_n}(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}$.

It is clear that $S_{\mathcal{F}}>0$. Therefore, we have

$$\begin{aligned}
&(m+n)\left(|\mathsf{M}(G,m)| - |\mathsf{M}(C_n,m)|\right)\\
=\ & \sum_{d|(m,n)} (\varphi_G(d) - \varphi_{C_n}(d))\binom{\frac{m+n}{d}}{\frac{m}{d},\frac{n}{d}}\\
=\ & (\varphi_G(a) - \varphi_{C_n}(a))\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} + S_{\mathcal{F}} + \sum_{e\in\mathcal{E}_{C_n}} (\varphi_G(e) - \varphi_{C_n}(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}\\
=\ & (\varphi_G(a) - \varphi_{C_n}(a))\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} + S_{\mathcal{F}} - \sum_{e\in\mathcal{E}_{C_n}} (\varphi_{C_n}(e) - \varphi_G(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}\\
\geqslant\ & a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}} + S_{\mathcal{F}} - \sum_{e\in\mathcal{E}_{C_n}} (\varphi_{C_n}(e) - \varphi_G(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}},
\end{aligned}$$

where the last inequality follows from Lemma 8.

Therefore, in order to prove (17), it suffices to show that

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}+S_{\mathcal{F}}>\sum_{e\in\mathcal{E}_{C_n}}(\varphi_{C_n}(e)-\varphi_G(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}}. \tag{18}$$

As b is a prime power by Lemma 7, we may assume that $b=q^s$ for some prime q and $s\geqslant 2$.

Assume that $a<b<2a$. In this case, we have $q^{s-1}=\frac{q^s}{q}<\frac{2a}{q}\leqslant a$, which contradicts the definition of a. Therefore, it suffices to consider the case $b\geqslant 2a$. In this case, by Lemma 5, we have

$$a\binom{\frac{m+n}{a}}{\frac{m}{a},\frac{n}{a}}>n\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}\geqslant\sum_{e\in\mathcal{E}_{C_n}}\varphi_{C_n}(e)\binom{\frac{m+n}{b}}{\frac{m}{b},\frac{n}{b}}\geqslant\sum_{e\in\mathcal{E}_{C_n}}(\varphi_{C_n}(e)-\varphi_G(e))\binom{\frac{m+n}{e}}{\frac{m}{e},\frac{n}{e}},$$

and (18) follows immediately. This completes the proof. □

4 General case

In this section, we discuss Theorem 3 from the viewpoint of invariant theory and consider an extension of Theorem 3 to finite groups (not necessarily abelian). Let G be a finite group and $\rho: G\to GL(V)$ be a finite dimensional linear representation of G over $\mathbb{C}$. Let $\mathbb{C}[V]$ denote the graded algebra of polynomial functions on V. We can regard $\mathbb{C}[V]$ as the symmetric algebra on V^*, the dual space of V. Equivalently, if $z_1,\ldots,z_n\in V^*$ is a basis, then $\mathbb{C}[V]$ is just the polynomial ring $\mathbb{C}[z_1,\ldots,z_n]$, whose elements are the homogeneous polynomials in the linear forms $z_1,\ldots,z_n$ with coefficient in $\mathbb{C}$. The action of G on V (through the representation ρ) naturally induces a right action of G on V^* as follows:

$$x^g(v)=x(g\cdot v)=x(\rho(g)v).$$

Moreover, this action can be naturally extended to an action on $\mathbb{C}[V]$. The central topic of invariant theory is to study the algebra of polynomial invariants which is defined as follows:

$$\mathbb{C}[V]^G=\{f\in\mathbb{C}[V]\mid f^g=f,\ \text{for all } g\in G\}.$$

Recall that $\mathbb{C}[V]^G$ is finitely generated and that $\mathbb{C}[V]^G$ is a graded $\mathbb{C}$-algebra; see [27]. We denote by $\dim\mathbb{C}[V]^G_m$ the dimension of the m-th component of $\mathbb{C}[V]^G$ as a vector space over $\mathbb{C}$. In particular, if G is a finite abelian group and V is the regular representation of G over $\mathbb{C}$, then for any positive integer m we have

$$\dim\mathbb{C}[V]^G_m=|\mathsf{M}(G,m)|$$

(see [21, Section 3] for a discussion). Now, we can restate Theorem 3 in terms of invariant theory as follows.

Theorem 12. *Let G and H be two finite abelian groups. Let V (resp. V') be the regular representation of G (resp. H). Then we have*

$$\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}$$

if and only if $\varphi_G(d) = \varphi_H(d)$ for any $d|(|G|, |H|)$.

For any finite group G of order n and its regular representation V over $\mathbb{C}$, Almkvist and Fossum [1, Section V 1.8] proved that

$$\dim \mathbb{C}[V]^G_m = \frac{1}{n+m} \sum_{d|(n,m)} \varphi_G(d) \binom{n/d + m/d}{n/d}, \tag{19}$$

where $\varphi_G(d)$ is the number of elements in G of order d. Note that (19) has the same form as (2). Consequently, for any finite group H and its regular representation V' over $\mathbb{C}$, if (3) holds, then we have

$$\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}. \tag{20}$$

Based on this observation and Theorem 3, it is natural to consider whether (3) is a necessary condition for the reciprocity (20) to hold. In fact, we prove some positive results on this problem.

Theorem 13. *Let G and H be two finite groups. Let V (resp. V') be the regular representation of G (resp. H). Assume that one of the following holds:*

1. *$G = D_{2p}$ is the dihedral group of order $2p$, where $p \geqslant 5$ is a prime;*
2. *$|H| \geqslant |G|^2$ and $|G|$ does not contain two divisors $d_1, d_2 > 1$ with $d_1 - d_2 = 1$.*

Then we have

$$\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}$$

if and only if $\varphi_G(d) = \varphi_H(d)$ for any $d|(|G|, |H|)$.

Proof. (1) Firstly, we assume that

$$G = D_{2p} = \langle x, y \mid x^2 = 1 = y^p,\ xyx = y^{-1} \rangle$$

is the dihedral group of order $2p$, where $p \geqslant 5$ is a prime.

It suffices to prove that if $\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}$, then we have $\varphi_G(d) = \varphi_H(d)$ holds for any $d|(|G|, |H|)$. As $|G| = 2p$, $d|(|G|, |H|)$ if and only if $d \in \{1, 2, p, 2p\}$. The desired result follows easily if $(|G|, |H|) \in \{1, 2, p\}$. Therefore, it suffices to consider the case $(|G|, |H|) = 2p$, i.e., $2p|m$.

Note that $\varphi_H(p) \geqslant \varphi_G(p) = p - 1$, and $\varphi_H(2p) \geqslant \varphi_G(2p) = 0$. If $\varphi_H(2) \geqslant \varphi_G(2)$, by the formula (19), we have the desired result. Now, suppose that $\varphi_H(2) < \varphi_G(2) = p$. Let

$|H| = m = 2\ell p$ where $\ell \in \mathbb{N}$. In this case, we have

$$\begin{aligned} & (m+2p)(\dim \mathbb{C}[V]^G_{|H|} - \dim \mathbb{C}[V']^H_{|G|}) \\ = & \sum_{d|2p} (\varphi_G(d) - \varphi_H(d)) \binom{\frac{m+2p}{d}}{\frac{m}{d}, \frac{2p}{d}} \\ \geqslant & (\varphi_G(2) - \varphi_H(2)) \binom{\frac{m+2p}{2}}{\frac{m}{2}, \frac{2p}{2}} - \varphi_H(p) \binom{\frac{m+2p}{p}}{\frac{m}{p}, \frac{2p}{p}} - \varphi_H(2p) \binom{\frac{m+2p}{2p}}{\frac{m}{2p}, \frac{2p}{2p}} \\ \geqslant & \binom{\frac{m+2p}{2}}{\frac{m}{2}, \frac{2p}{2}} - m \binom{\frac{m+2p}{p}}{\frac{m}{p}, \frac{2p}{p}} = \binom{\ell p + p}{p} - m \binom{2\ell+2}{2}. \end{aligned}$$

Moreover, as $p \geqslant 5$, we have

$$\begin{aligned} \binom{\ell p + p}{p} &= \prod_{i=1}^{p} \frac{\ell p + i}{i} \geqslant \ell p (\prod_{i=2}^{p} \frac{\ell p + i}{i}) \\ &> \ell p \prod_{i=2}^{p} (\ell + 1) \geqslant m \frac{(\ell+1)^4}{2} > m \binom{2\ell+2}{2}. \end{aligned}$$

Therefore, we obtain $\dim \mathbb{C}[V]^G_{|H|} > \dim \mathbb{C}[V']^H_{|G|}$, a contradiction.

(2) Secondly, we assume that $|H| \geqslant |G|^2$ and $|G|$ does not contain two divisors $d_1, d_2 > 1$ with $d_1 - d_2 = 1$. As before, it suffices to prove that if $\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}$, then we have $\varphi_G(d) = \varphi_H(d)$ holds for any $d|(|G|, |H|)$. Assume to the contrary that $\varphi_G(d) \neq \varphi_H(d)$ for some $d|(|G|, |H|)$. Let $|G| = n$ and $|H| = m$.

Let

$$a = \min\{d \mid \varphi_G(d) \neq \varphi_H(d) \text{ for } d|(n,m)\}.$$

Case 1: Assume that $\varphi_G(a) < \varphi_H(a)$. If $\varphi_G(d) \leqslant \varphi_H(d)$ holds for any $d|(n,m)$, then the desired result follows. Therefore, we assume that $\varphi_G(d) > \varphi_H(d)$ holds for some $d|(n,m)$ and let

$$b = \min\{d \mid \varphi_G(d) > \varphi_H(d) \text{ for } d|(n,m)\}.$$

Clearly, we have $a < b$. Now, we show that

$$(\varphi_H(a) - \varphi_G(a)) \binom{\frac{n+m}{a}}{\frac{n}{a}, \frac{m}{a}} > \left(\sum_{e \geqslant b} \varphi_G(e) \right) \binom{\frac{n+m}{b}}{\frac{n}{b}, \frac{m}{b}}. \tag{21}$$

In fact, (21) follows from the following stronger result

$$\binom{\frac{n+m}{a}}{\frac{n}{a}, \frac{m}{a}} > n \binom{\frac{n+m}{b}}{\frac{n}{b}, \frac{m}{b}}. \tag{22}$$

In order to prove (22), by Lemma 5.(i), we only need to prove that

$$(1 + \frac{m}{n})^{n(\frac{1}{a} - \frac{1}{b})} (1 + \frac{a}{b} \frac{n}{m})^{m(\frac{1}{a} - \frac{1}{b})} > n. \tag{23}$$

It is easy to see that, as $\frac{n}{a} - \frac{n}{b} \geqslant 1$ and $m \geqslant n^2$,

$$(1+\frac{m}{n})^{n(\frac{1}{a}-\frac{1}{b})}(1+\frac{a}{b}\frac{n}{m})^{m(\frac{1}{a}-\frac{1}{b})} > 1+\frac{m}{n} > n,$$

and therefore (22) follows. By (21) and the formula (19), it is easy to see that $\dim \mathbb{C}[V']^H_{|G|} > \dim \mathbb{C}[V]^G_{|H|}$, a contradiction.

Case 2: Assume that $\varphi_G(a) > \varphi_H(a)$. If $\varphi_G(d) \geqslant \varphi_H(d)$ holds for any $d|(n,m)$, then the desired result follows. Therefore, we assume that $\varphi_G(d) < \varphi_H(d)$ holds for some $d|(n,m)$ and let

$$b = \min\{d \mid \varphi_G(d) < \varphi_H(d) \text{ for } d|(n,m)\}.$$

Clearly, we have $a < b$. Similar to the above case, we show that

$$(\varphi_G(a) - \varphi_H(a))\binom{\frac{n+m}{a}}{\frac{n}{a}, \frac{m}{a}} > \left(\sum_{e \geqslant b} \varphi_H(e)\right)\binom{\frac{n+m}{b}}{\frac{n}{b}, \frac{m}{b}}. \tag{24}$$

In fact, (24) follows from the following stronger result

$$\binom{\frac{n+m}{a}}{\frac{n}{a}, \frac{m}{a}} > m\binom{\frac{n+m}{b}}{\frac{n}{b}, \frac{m}{b}}. \tag{25}$$

In order to prove (25), by Lemma 5.(i), we only need to prove that

$$(1+\frac{m}{n})^{n(\frac{1}{a}-\frac{1}{b})}(1+\frac{a}{b}\frac{n}{m})^{m(\frac{1}{a}-\frac{1}{b})} > m. \tag{26}$$

Note that, as n does not contain two divisors $d_1, d_2 > 1$ with $d_1 - d_2 = 1$, we have $n(\frac{1}{a} - \frac{1}{b}) \geqslant 2$. Since $m \geqslant n^2$, we have that

$$\left(1+\frac{m}{n}\right)^{n(\frac{1}{a}-\frac{1}{b})} \geqslant \left(1+\frac{m}{n}\right)^2 = 1 + 2\frac{m}{n} + \frac{m^2}{n^2} > m,$$

as desired. By (24) and the formula (19), it is easy to see that $\dim \mathbb{C}[V]^G_{|H|} > \dim \mathbb{C}[V']^H_{|G|}$, a contradiction. This completes the proof. □

5 Further discussions

Let $\mathcal{D}(G)$ be the number of formally different monomials occurring in $\mathsf{det}(\mathcal{M}_G)$. Due to possible cancellations, we have $\mathcal{D}(G) \leqslant \mathcal{P}(G)$. It is natural to consider an analog of Theorem 1 for $\mathcal{D}(G)$ (note that, such a result, if it is correct, is stronger than the result of Formanek and Sibley). Unlike $\mathcal{P}(G)$, there is no explicit formula for $\mathcal{D}(G)$. When G is cyclic, using ideas from symmetric functions and number theory, it was proved that $\mathcal{D}(G) = \mathcal{P}(G)$ if and only if $|G|$ is a prime power; see [2, 33]. For general abelian groups, it is still unknown whether there exists a similar relation between $\mathcal{D}(G)$ and $\mathcal{P}(G)$; see [11, Problem 1].

We have discussed several characterization results for finite groups in terms of the permanent or the determinant of $\mathcal{M}_G$. Note that, for an $n \times n$ matrix $\mathcal{M} = (m_{ij})_{1 \leqslant i,j \leqslant n}$, the permanent and the determinant are just special cases of the immanant

$$\mathsf{imm}_\lambda(\mathcal{M}) = \sum_{\tau \in S_n} \chi_\lambda(\tau) \prod_{i=1}^{n} m_{i,\tau(i)},$$

where χ_λ is an irreducible character of S_n indexed by the partition λ of n [24, Chapter VI] (the determinant and the permanent are the immanants corresponding to the sign character and the trivial character, respectively). Immanants appeared naturally and are very important in algebraic combinatorics [17, 18, 31, 32]. It would be interesting to see if there are some other immanents characterize the finite groups.

This paper provides some results on zero-sum sequences over finite abelian groups and polynomial invariants of finite groups. Recently, the relationship between zero-sum theory (also factorization theory) and invariant theory is getting closer; see [3, 4, 6, 20] for some recent studies. Based on Theorems 3, 12, and 13, it is natural to propose the following conjecture.

Conjecture 14. Let G and H be finite groups. Let V (resp. V') be the regular representation of G (resp. H). Then we have

$$\dim \mathbb{C}[V]^G_{|H|} = \dim \mathbb{C}[V']^H_{|G|}$$

if and only if $\varphi_G(d) = \varphi_H(d)$ for any $d|(|G|, |H|)$.

Acknowledgments

We would like to thank Prof. Alfred Geroldinger for very helpful comments and suggestions. We also thank Dr. Dongchun Han for very inspiring discussion. We are grateful to Prof. Ian M. Wanless for his very helpful comments and for bringing [5] to our attention. M.S. Li was supported by the National Science Foundation of China Grant No.12371458. H.B. Zhang was supported by the Guangdong Basic and Applied Basic Research Foundation Grant No.2024A1515012564 and No.2021A1515010216 and Fundamental Research Funds for the Central Universities, Sun Yat-sen University, No.24qnpy306.

References

[1] G. Almkvist and R. Fossum, *Decomposition of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$-modules in characteristic p and relations to invariants*, In: Séminaire d'Algèbre P. Dubreil, Paris, 1976-1977. Lecture Notes in Math., vol. 641, *Springer*, Berlin, (1978), 1–111.

[2] L. Colarte, E. Mezzetti, R. M. Miró-Roig and M. Salat, *On the coefficients of the permanent and the determinant of a circulant matrix Applications*, Proc. Amer. Math. Soc., 147 (2019), 547–558.

[3] K. Cziszter, M. Domokos and A. Geroldinger, *The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics*, In: Multiplicative Ideal Theory and Factorization Theory, Springer Proceedings in Mathematics and Statistics, vol. 170, *Springer*, Cham, (2016), 43–95.

[4] K. Cziszter, M. Domokos and I. Szőllősi, *The Noether numbers and the Davenport constants of the groups of order less than 32*, J. Algebra, 510 (2018), 513–541.

[5] D. Donovan, K. Johnson and I. M. Wanless, *Permanents and determinants of Latin squares*, J. Combin. Des., 24(3) (2016), 132–148.

[6] M. Domokos, *On Syzygies for Rings of Invariants of Abelian Groups*, In: Advances in Rings, Modules and Factorizations, Springer Proceedings in Mathematics and Statistics, vol. 321, *Springer*, Cham, (2020), 105–124.

[7] A. G. Elashvili and M. Jibladze, *Hermite reciprocity for the regular representations of cyclic groups*, Indag. Math., 9 (1998), 233–238.

[8] A. G. Elashvili, M. Jibladze and D. Pataraia, *Combinatorics of Necklaces and Hermite Reciprocity*, J. Algebraic Comb., 10 (1999), 173–188.

[9] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel, 10 (1961), 41–43.

[10] E. Formanek and D. Sibley, *The group determinant determines the group*, Proc. Amer. Math. Soc., 112(3) (1991), 649–656.

[11] M. Fredman, *A symmetry relationship for a class of partitions*, J. Combin. Theory Ser. A, 18 (1975), 199–202.

[12] W. D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math., 24 (2006), 337–369.

[13] A. Geroldinger, *Sets of lengths*, Amer. Math. Monthly, 123(10) (2016), 960–988.

[14] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math., vol. 278, *Chapman & Hall/CRC*, Boca Raton, FL, 2006.

[15] A. Geroldinger and W. A. Schmid, *A characterization of class groups via sets of lengths*, J. Korean Math. Soc., 56 (2019), 869–915.

[16] A. Geroldinger and Q. Zhong, *Factorization theory in commutative monoids*, Semigroup Forum, 100 (2020), 22–51.

[17] I. P. Goulden, D. M. Jackson, *Immanants of combinatorial matrices*, J. Algebra, 148(2) (1992), 305–324.

[18] M. Haiman, *Hecke Algebra Characters and Immanant Conjectures*, J. Amer. Math. Soc., 6(3) (1993), 569–595.

[19] M. Hall, *A combinatorial problem on abelian groups*, Proc. Amer. Math. Soc., 3 (1952), 584–587.

[20] D. C. Han and H. B. Zhang, *Erdős-Ginzburg-Ziv theorem and Noether number for* $C_m \ltimes_\varphi C_{mn}$, J. Number Theory, 198 (2019), 159–175.

[21] D. C. Han and H. B. Zhang, *A reciprocity on finite abelian groups involving zero-sum sequences*, SIAM J. Discrete Math., 35(2) (2021), 1077–1095.

[22] K. W. Johnson, *On the group determinant*, Math. Proc. Camb. Phil. Soc., 109 (1991), 299–311.

[23] K. W. Johnson, *Group Matrices, Group Determinants and Representation Theory. The Mathematical Legacy of Frobenius*, Lecture Notes in Math., vol. 2233, Springer, 2019.

[24] D. E. Littlewood, *The Theory of Group Characters and Matrix Representations of Groups*, Second ed. Oxford U. Press, London 1950.

[25] R. Mansfield, *A group determinant determines its group*, Proc. Amer. Math. Soc., 116(4) (1992), 939–941.

[26] A. Muratović-Ribić and Q. Wang, *The multisubset sum problem for finite abelian groups*, Ars Math. Contemp., 8(2) (2015), 417–423.

[27] M. D. Neusel and L. Smith, *Invariant theory of finite groups*, Mathematical Surveys and Monographs, vol. 94, *AMS*, Providence R.I., 2002.

[28] J. E. Olson, *A combinatorial problem on finite Abelian groups I*, J. Number Theory, 1 (1969), 8–10.

[29] J. E. Olson, *A combinatorial problem on finite Abelian groups II*, J. Number Theory, 1 (1969), 159–199.

[30] D. I. Panyushev, *Fredman's reciprocity, invariants of abelian groups, and the permanent of the Cayley table*, J. Algebraic Combin., 33 (2011), 111–125.

[31] R. Stanley, *Positivity problems and conjectures in algebraic combinatorics*, in Mathematics: Frontiers and Perspecives (V. Arnold, M. Atiyah, P. Lax, and B. Mazur, eds.), American Mathematical Society, Providence, RI, (2000), 295–319.

[32] J. Stembridge, *Immanants of totally positive matrices are nonnegative*, Bull. London Math. Soc., 23 (1991), 422–428.

[33] H. Thomas, *The number of terms in the permanent and the determinant of a generic circulant matrix*, J. Algebraic Combin., 20 (2004), 55–60.