Discrete Mathematics 123 (1993) 179–188
North-Holland

Cycle index of direct product of permutation groups and number of equivalence classes of subsets of Z_v

Wan-Di Wei
Department of Mathematics, Sichuan University, Chengdu 610064, China

Ju-Yong Xu
Department of Mathematics, Wuhan Institute of Urban Construction, Wuhan, China

Received 3 August 1990

Abstract

Let v be a positive integer and Z_v the residue class ring modulo v. Two subsets D_1 and D_2 of Z_v are said to be equivalent if there exist $t, s \in Z_v$ with $\gcd(t, v) = 1$ such that $D_1 = tD_2 + s$. We are interested in the number of equivalence classes of k-subsets of Z_v and the number of equivalence classes of subsets of Z_v. We first find the cycle index of the direct product of permutation groups, and then use it to obtain the numbers mentioned above which can be viewed as upper bounds, respectively, for the number of inequivalent (v, k, λ) cyclic difference sets (when $k(k-1) = \lambda(v-1)$) and for the number of inequivalent cyclic difference sets in Z_v.

1. Introduction

Let v be a positive integer and Z_v the residue class ring modulo v. Motivated by the concept of equivalence of cyclic difference sets (cf. [1,2 or 5]), Wei et al. [6] have introduced a similar equivalence relation among the subsets of Z_v, and studied the number of equivalence classes. Two subsets D_1 and D_2 of Z_v are said to be equivalent, denoted by $D_1 \sim D_2$, if there exist $t, s \in Z_v$ with $\gcd(t, v) = 1$ such that $D_1 = tD_2 + s$.

Obviously, the relation $\sim$ is an equivalence relation, under which the set of subsets of Z_v are partitioned into disjoint equivalence classes, and the subsets in one equivalence class have the same cardinality.

Let

$$T_v = \{(t, s) \mid t, s \in Z_v,\ \gcd(t, v) = 1\}. \tag{1.1}$$

Then $|T_v| = \varphi(v)v$, where $\varphi(v)$ is the Euler's phi-function. One can associate each element $(t,s) \in T$ with the following permutation on Z_v:

$$\sigma(t,s) = \begin{pmatrix} 0 & 1 \cdots d \cdots v-1 \\ s & t+s \cdots td+s \cdots t(v-1)+s \end{pmatrix}$$

Let $G_v = \{\sigma(t,s) \mid (t,s) \in T_v\}$. For $\sigma(t,s), \sigma(t',s') \in G_v$, we define

$$(\sigma(t,s) \cdot \sigma(t',s'))d = \sigma(t,s)(\sigma(t',s')d), \quad d \in Z_v.$$

Then

$$\sigma(t,s) \cdot \sigma(t',s') = \sigma(tt', ts'+s) \in G_v, \tag{1.2}$$

and G_v is a permutation group on Z_v. Denote the cycle index of G_v (cf. [3] or [4]) by

$$P_{G_v}(x_1, x_2, \ldots, x_v) = \frac{1}{|G_v|} \sum_{g \in G_v} x_1^{n_1(g)} x_2^{n_2(g)} \cdots x_v^{n_v(g)}, \tag{1.3}$$

where $n_i(g)$ $(1 \leqslant i \leqslant v)$ is the number of cycles of length i in the decomposition of g into disjoint cycles. Wei et al. [6] proved the following theorem.

Theorem 1.1. *The number of equivalence classes of k-subsets of Z_v is*

$$\frac{1}{k!}\left[\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^k P_{G_v}(x+1, x^2+1, \ldots, x^v+1)\right]_{x=0}, \tag{1.4}$$

and the number of equivalence classes of subsets of Z_v is

$$P_{G_v}(2,2,\ldots,2). \tag{1.5}$$

According to this theorem, the problem of finding the number of equivalence classes of k-subsets (or subsets) of Z_v is reduced to finding the cycle index of the permutation group G_v. When v is a prime power p^α, Wei et al. [6] have found $P_{G_{p^\alpha}}(x_1, x_2, \ldots, x_{p^\alpha})$ as in the following theorems.

Theorem 1.2. *Let p be an odd prime and $\alpha \geqslant 1$. Then the cycle index of G_{p^α} is*

$$\begin{aligned} P_{G_{p^\alpha}}(x_1, x_2, \ldots, x_{p^\alpha}) = \frac{1}{p^{2\alpha-1}(p-1)} \Bigg\{ & \sum_{w=1}^{\alpha} p^{2(w-1)}(p-1) x_{p^w}^{p^{\alpha-w}} \\ & + \sum_{w=0}^{\alpha-1} \sum_{l \mid p-1} p^{w+\delta(l)(\alpha-w)} \varphi(p_l^w) x_1 x_l^{(p^{\alpha-w-1}-1)/l} \\ & \times \left(\prod_{u=0}^{w} x_{p^u l}\right)^{p^{\alpha-w-1}(p-1)/l} \Bigg\}, \end{aligned} \tag{1.6}$$

where

$$\delta(l) = \begin{cases} 1 & \text{if } l > 1, \\ 0 & \text{if } l = 1. \end{cases}$$

Theorem 1.3. *The cycle index of G_{2^α} is*

$$\tfrac{1}{2}(x_1^2+x_2) \quad \text{if } \alpha=1, \tag{1.7}$$

$$\tfrac{1}{8}(x_1^4+2x_1^2x_2+3x_2^2+2x_4) \quad \text{if } \alpha=2, \tag{1.8}$$

$$\begin{aligned}&\frac{1}{2^{2\alpha-1}}\Bigg\{2^{2(\alpha-1)}x_{2^\alpha}+\sum_{w=1}^{\alpha-1}(2^{2(w-1)}+\varphi(2^{w-1})2^{\alpha-1})x_{2^w}^{2^{\alpha-w}}\\ &\quad+\sum_{w=0}^{\alpha-2}\varphi(2^w)(2^w x_1^{2^{\alpha-w}}+2^{\alpha-1}x_1^2x_2^{2^{\alpha-w-1}}-1)\\ &\quad\times\left(\sum_{u=1}^{w}x_2u\right)^{2^{\alpha-w-1}}\Bigg\} \quad \text{if } \alpha\geqslant 3.\end{aligned} \tag{1.9}$$

In the present paper we will settle the general case when v has the factorization:

$$v=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}, \quad p_i\text{'s are distinct primes.} \tag{1.10}$$

To this end, we first study in Section 2 the index of the direct product of permutation groups, which also has its own independent interest and use it to find the cycle index of G_v, and then give in Section 3 formulas for the number of equivalence classes of k-subsets of Z_v as well as for the number of equivalence classes of subsets of Z_v. Naturally, these numbers can be viewed as upper bounds, respectively, for the number of inequivalent (v,k,λ) cyclic difference sets (when $k(k-1)=\lambda(v-1)$) and for the number of inequivalent cyclic difference sets in Z_v, although they are too coarse.

2. Cycle index of direct product of permutation groups

Let H_i be a permutation group on a finite set S_i and $|S_i|=v_i$ $(1\leqslant i\leqslant r)$. Let the cycle index of H_i be

$$P_{H_i}(x_1,x_2,\ldots,x_{v_i})=\frac{1}{|H_i|}\sum_{h_i\in H_i}\prod_{j=1}^{v_i}x_j^{n_{ij}(h_i)}. \tag{2.1}$$

Let $S=S_1\times S_2\times\cdots\times S_r$ be the Cartesian product of $S_1,S_2,\ldots,S_r$, and $H=H_1\times H_2\times\cdots\times H_r$ the direct product of $H_1,H_2,\ldots,H_r$. For an element $a=(a_1,a_2,\ldots,a_r)$ of S and an element $h=(h_1,h_2,\ldots,h_r)$ of H, we define the action of h on a by

$$h(a)=(h_1,h_2,\ldots,h_r)(a_1,a_2,\ldots,a_r)=(h_1(a_1),h_2(a_2),\ldots,h_r(a_r)). \tag{2.2}$$

Evidently, H is a permutation group on S. Denote by $C_h(a)$ the length of the cycle containing the element $a \in S$ in the decomposition of the permutation h into disjoint cycles, and by $C_{h_i}(a_i)$ the length of the cycle containing the element $a_i \in S_i$ in the decomposition of the permutation h_i into disjoint cycles. Then we can prove the following relation between $C_h(a)$ and $C_{h_i}(a_i)$ $(1 \leqslant i \leqslant r)$, where $a = (a_1, a_2, \ldots, a_r)$.

Lemma 2.1. *For any element* $a = (a_1, a_2, \ldots, a_r) \in S$, *we have*

$$C_h(a) = [C_{h_1}(a_1), C_{h_2}(a_2), \ldots, C_{h_r}(a_r)], \tag{2.3}$$

where $[C_{h_1}(a_1), C_{h_2}(a_2), \ldots, C_{h_r}(a_r)]$ *denotes the lcm of* $C_{h_1}(a_1), C_{h_2}(a_2), \ldots, C_{h_r}(a_r)$.

Proof. From $h^{c_h(a)}(a) = a$, we have

$$(h_1^{c_h(a)}(a_1), h_2^{c_h(a)}(a_2), \ldots, h_r^{c_h(a)}(a_r)) = (a_1, a_2, \ldots, a_r),$$

i.e.

$$h_i^{c_h(a)}(a_i) = a_i \quad (1 \leqslant i \leqslant r).$$

Thus, $C_{h_i}(a_i) \mid C_h(a)$ $(1 \leqslant i \leqslant r)$, and then

$$[C_{h_1}(a_1), C_{h_2}(a_2), \ldots, C_{h_r}(a_r)] \mid C_h(a). \tag{2.4}$$

Write $m = [C_{h_1}(a_1), C_{h_2}(a_2), \ldots, C_{h_r}(a_r)]$, and $l_i = m / C_{h_i}(a_i)$ $(1 \leqslant i \leqslant r)$. Then

$$h^m(a) = (h_1^{c_{h_1}(a_1) l_1}(a_1), h_2^{c_{h_2}(a_2) l_2}(a_2), \ldots, h_r^{c_{h_r}(a_r) l_r}(a_r)). \tag{2.5}$$

From this and

$$h_i^{c_{h_i}(a_i) l_i}(a_i) = \underbrace{h_i^{c_{h_i}(a_i)} \ldots h_i^{c_{h_i}(a_i)}}_{l_i}(a_i) = a_i \quad (1 \leqslant i \leqslant r)$$

we get

$$h^m(a) = (a_1, a_2, \ldots, a_r) = a.$$

Therefore,

$$C_h(a) \mid m. \tag{2.6}$$

Combining (2.4) and (2.6), we prove the theorem. $\square$

We introduce a special kind of product as follows.

Definition 2.2. Let $f(x_1, x_2, \ldots, x_u) = \sum a_{i_1 i_2 \cdots i_u} x_1^{i_1} x_2^{i_2} \ldots x_u^{i_u}$ and $g(x_1, x_2, \ldots, x_v) = \sum b_{j_1 j_2 \cdots j_v} x_1^{j_1} x_2^{j_2} \cdots x_v^{j_v}$ be two polynomials. The $\divideontimes$-product of $f(x_1, x_2, \ldots, x_u)$ and

$g(x_1, x_2, \ldots, x_v)$, denoted by $f(x_1, x_2, \ldots, x_u) \divideontimes g(x_1, x_2, \ldots, x_v)$, is defined to be

$$f(x_1, x_2, \ldots, x_u) \divideontimes g(x_1, x_2, \ldots, x_v) = \sum a_{i_1 i_2 \cdots i_u} b_{j_1 j_2 \cdots j_v}$$

$$\times \prod_{\substack{1 \leq l \leq u \\ 1 \leq m \leq v}} (x_l^{i_l} \divideontimes x_m^{j_m}), \tag{2.7}$$

where

$$x_l^{i_l} \divideontimes x_m^{j_m} = x_{[l,m]}^{l i_l m j_m / [l,m]}. \tag{2.8}$$

Some useful properties of $\divideontimes$-multiplication are listed in the following lemma.

Lemma 2.3. (a) *The $\divideontimes$-multiplication is commutative*:

$$f(x_1, x_2, \ldots, x_u) \divideontimes g(x_1, x_2, \ldots, x_v) = g(x_1, x_2, \ldots, x_v) \divideontimes f(x_1, x_2, \ldots, x_u).$$

(b) *The $\divideontimes$-multiplication is associative*:

$$(f(x_1, x_2, \ldots, x_u) \divideontimes g(x_1, x_2, \ldots, x_v)) \divideontimes q(x_1, x_2, \ldots, x_w)$$

$$= f(x_1, x_2, \ldots, x_u) \divideontimes (g(x_1, x_2, \ldots, x_v) \divideontimes q(x_1, x_2, \ldots, x_w)),$$

and in general, the $\divideontimes$-product of r polynomials is the same no matter how to associate the factors, so we can use the symbols:

$$\mathop{\divideontimes}_{i=1}^{T} f_i(x_1, x_2, \ldots, x_{v_i}) = f_1(x_1, x_2, \ldots, x_{v_1}) \divideontimes f_2(x_1, x_2, \ldots, x_{v_2})$$

$$\divideontimes \cdots \divideontimes f_r(x_1, x_2, \ldots, x_{v_r}).$$

Moreover,

$$\mathop{\divideontimes}_{j=1}^{r} x_{i_j}^{n_j} = x_{[i_1, i_2, \ldots, i_r]}^{i_1 n_1 i_2 n_2 \cdots i_r n_r / [i_1, i_2, \ldots, i_r]}. \tag{2.9}$$

(c) $(x_i^{n_i})^m \divideontimes (x_j^{n_i})^l = (x_i^{n_i} \divideontimes x_j^{n_i})^{ml}$.

(d) $$\mathop{\divideontimes}_{j=1}^{r} P_{H_j}(x_1, x_2, \ldots, x_{v_j}) = \frac{1}{\prod_{j=1}^r |H_j|} \sum_{(h_1, h_2, \ldots, h_r) \in H_1 \times H_2 \times \cdots \times H_r}$$

$$\times \prod_{u \geq 1} x_u^{1/u \sum_{[u_1, u_2, \ldots, u_r] = u (1 \leq u_j \leq v_j)} \prod_{j=1}^r u_j n_{j u_j}(h_j)}. \tag{2.10}$$

Proof. (a) follows from (2.7), for its right-hand side is independent of the order of $x_l^{i_l}$ and $x_m^{j_m}$. (b) follows from

$$(x_i^{n_i} \divideontimes x_j^{n_j}) \divideontimes x_m^{n_m} = x_{[i,j]}^{i n_i j n_j / [i,j]} \divideontimes x_m^{n_m} = x_{[[i,j],m]}^{i n_i j n_j m n_m / [[i,j],m]}$$

$$= x_{[i,[j,m]]}^{i n_i j n_j m n_m / [i,[j,m]]} = x_i^{n_i} \divideontimes (x_j^{n_j} \divideontimes x_m^{n_m}).$$

Based on this we get (2.9) by mathematical induction. The verification of (c) is straightforward. We now prove (d):

$$\mathop{\text{※}}_{j=1}^{r} \frac{1}{|H_j|} \sum_{h_i \in H_j} \prod_{u=1}^{v_i} x_u^{n_{ju}(h_j)} = \frac{1}{\prod_{i=1}^{r} |H_i|} \sum_{\substack{h_1 \in H_1 \\ h_2 \in H_2 \\ \cdots \\ h_r \in H_r}} \prod_{\substack{1 \leqslant u_1 \leqslant v_1 \\ 1 \leqslant u_2 \leqslant v_2 \\ \cdots \\ 1 \leqslant u_r \leqslant v_r}} \mathop{\text{※}}_{j=1}^{r} x_{u_j}^{n_{ju_j}(h_j)}$$

$$= \frac{1}{\prod_{i=1}^{r} |H_i|} \sum_{\substack{h_1 \in H_1 \\ h_2 \in H_2 \\ \cdots \\ h_r \in H_r}} \prod_{\substack{1 \leqslant u_1 \leqslant v_1 \\ 1 \leqslant u_2 \leqslant v_2 \\ \cdots \\ 1 \leqslant u_r \leqslant v_r}} x_{[u_1, u_2, \ldots, u_r]}^{u_1 n_{1u_1}(h_1) u_2 n_{2u_2}(h_2) \cdots u_r n_{ru_r}(h_r)/[u_1, u_2, \ldots, u_r]}$$

$$= \frac{1}{\prod_{i=1}^{r} |H_i|} \sum_{\substack{(h_1, h_2, \ldots, h_r) \\ \in H_1 \times H_2 \times \cdots \times H_r}} \prod_{u \geqslant 1} x_u^{1/u \sum_{[u_1, u_2, \ldots, u_r] = u (1 \leqslant u_j \leqslant v_j)} \prod_{j=1}^{r} u_j n_{ju_j}(h_j)}.$$

This proves the lemma. □

We are now in a position to prove the main result of this section.

Theorem 2.4. *The cycle index of the permutation group* $H = H_1 \times H_2 \times \cdots \times X_r$ is

$$P_{H_1 \times H_2 \times \cdots \times H_r}(x_1, x_2, \ldots, x_{v_1 v_2 \cdots v_r}) = \mathop{\text{※}}_{i=1}^{r} P_{H_i}(x_1, x_2, \ldots, x_{v_i}).$$

Proof. Let $h = (h_1, h_2, \ldots, h_r)$ be a given element of $H_1 \times H_2 \times \cdots \times H_r$ and $a = (a_1, a_2, \ldots, a_r)$ a given element of $S_1 \times S_2 \times \cdots \times S_r$. Let a_i be in a cycle of length l_i of the decomposition of the permutation h_i into disjoint cycles $(1 \leqslant i \leqslant r)$. By Lemma 2.1, a is in a cycle of length $[l_1, l_2, \ldots, l_r]$ of the decomposition of the permutation h into disjoint cycles. Since the cycle indicator of h_i is

$$x_1^{n_{i1}(h_i)} x_2^{n_{i2}(h_i)} \cdots x_{v_i}^{n_{iv_i}(h_i)} \quad (1 \leqslant i \leqslant r),$$

there are $\prod_{i=1}^{r} (n_{il_i}(h_i) l_i)$ elements of S that are in one of the cycles of length $[l_1, l_2, \ldots, l_r]$. Thus, there are $\prod_{i=1}^{r} (l_i n_{il_i}(h_i))/[l_1, l_2, \ldots, l_r]$ cycles of length $[l_1, l_2, \ldots, l_r]$ in the decomposition of h into disjoint cycles. Therefore, the cycle indicator of $h = (h_1, h_2, \ldots, h_r)$ is

$$\prod_{\substack{1 \leqslant l_1 \leqslant v_1 \\ 1 \leqslant l_2 \leqslant v_2 \\ \cdots \\ 1 \leqslant l_r \leqslant v_r}} x_{[l_1, l_2, \ldots, l_r]}^{l_1 n_{1l_1}(h_1) l_2 n_{2l_2}(h_2) \cdots l_r n_{rl_r}(h_r)/[l_1, l_2, \ldots, l_r]}.$$

Hence,

$$
\begin{aligned}
&P_{H_1\times H_2\times\cdots\times H_r}(x_1,x_2,\ldots,x_{v_1v_2\cdots v_r})\\
&=\frac{1}{\prod_{i=1}^{r}|H_i|}\sum_{\substack{(h_1,h_2,\ldots,h_r)\\ \in H_1\times H_2\times\cdots\times H_r}}\prod_{\substack{1\leqslant l_1\leqslant v_1\\ 1\leqslant l_2\leqslant v_2\\ \cdots\\ 1\leqslant l_r\leqslant v_r}} x_{[l_1,l_2,\ldots,l_r]}^{l_1n_{1l_1}(h_1)l_2n_{2l_2}(h_2)\ldots l_rn_{rl_r}(h_r)/[l_1,l_2,\ldots,l_r]}\\
&=\mathop{※}_{i=1}^{r} P_{H_i}(x_1,x_2,\ldots,x_{v_i}).
\end{aligned}
$$

This proves the theorem. □

3. Enumeration of equivalence classes

In this section we will first find the cycle index of the permutation group G_v, and then use it to obtain an enumeration formula for the number of equivalence classes of subsets (or k-subsets) of Z_v.

Let v be a positive integer and have the factorization (1.10). From number theory, there are integers $z_1, z_2, \ldots, z_r$ such that

$$\sum_{i=1}^{r} z_i \prod_{\substack{j\neq i\\ 1\leqslant j\leqslant r}} p_j^{\alpha_j}=1.$$

For any $t\in Z_v$, set

$$t_i\equiv tz_i \prod_{\substack{j\neq i\\ 1\leqslant j\leqslant r}} p_j^{\alpha_j} \pmod{p_i^{\alpha_i}} \quad (1\leqslant i\leqslant r).$$

Then the map β:

$$\beta(t)=(t_1,t_2,\ldots,t_r) \tag{3.1}$$

is an isomorphism from Z_v to $\bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$. And it is easy to see that $\gcd(t,v)=1$ if and only if $\gcd(t_i,p_i)=1$ $(1\leqslant i\leqslant r)$.

Write

$$G_{p_i^{\alpha_i}}=\{\sigma_i(t_i,s_i)\mid(t_i,s_i)\in T_{p_i^{\alpha_i}}\} \quad (1\leqslant i\leqslant r), \tag{3.2}$$

where $\sigma_i(t_i,s_i)$ means the permutation on $Z_{p_i^{\alpha_i}}$ such that for $a_i\in Z_{p_i^{\alpha_i}}$, $\sigma_i(t_i,s_i)a_i=\langle t_ia_i+s_i\rangle_i$, where $\langle t_ia_i+s_i\rangle_i$ is the smallest nonnegative residue of $t_ia_i+s_i$ modulo $p_i^{\alpha_i}$ and is regarded as an element of $G_{p_i^{\alpha_i}}$ $(1\leqslant i\leqslant r)$.

We now prove the following theorem.

Theorem 3.1. *G_v is isomorphic to the direct product of $G_{p_i^{\alpha_i}}$ $(1 \leqslant i \leqslant r)$:*

$$G_v \cong \bigoplus_{i=1}^{r} G_{p_i^{\alpha_i}}, \tag{3.3}$$

and then

$$P_{G_v}(x_1, x_2, \ldots, x_v) = \mathop{\text{※}}_{i=1}^{r} P_{G_{p_i^{\alpha_i}}}(x_1, x_2, \ldots, x_{p_i^{\alpha_i}}). \tag{3.4}$$

Proof. Let (t, s) be a given element of T_v, β be as defined in (3.1), $\beta(t) = (t_1, t_2, \ldots, t_r)$, and $\beta(s) = (s_1, s_2, \ldots, s_r)$. Then we have $\gcd(t_i, p_i) = 1$ $(1 \leqslant i \leqslant r)$, so $(t_i, s_i) \in T_{p_i^{\alpha_i}}$ $(1 \leqslant i \leqslant r)$.

We can induce from $\sigma(t, s)$ a permutation $\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r))$ on $\bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$ as follows:

$$\begin{aligned} &\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r))(a_1, a_2, \ldots, a_r) \\ &\quad = (\langle t_1 a_1 + s_1 \rangle_1, \langle t_2 a_2 + s_2 \rangle_2, \ldots, \langle t_r a_r + s_r \rangle_r), \end{aligned} \tag{3.5}$$

where $(a_1, a_2, \ldots, a_r)$ is any element of $\bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$. Write

$$\bar{G}_v = \{\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r)) \mid (t_i, s_i) \in T_{p_i^{\alpha_i}} \ (1 \leqslant i \leqslant r)\}.$$

Then it is easily seen that

$$G_v \cong \bar{G}_v. \tag{3.6}$$

On the other hand, for $\sigma_i(t_i, s_i) \in G_{p_i^{\alpha_i}}$ and $a_i \in Z_{p_i^{\alpha_i}}$,

$$\sigma_i(t_i, s_i) a_i = \langle t_i a_i + s_i \rangle_i \quad (1 \leqslant i \leqslant r).$$

Combining this and (3.5), we have

$$\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r)) = (\sigma_1(t_1, s_1), \sigma_2(t_2, s_2), \ldots, \sigma_r(t_r, s_r)),$$

where $(\sigma_1(t_1, s_1), \sigma_2(t_2, s_2), \ldots, \sigma_r(t_r, s_r))$ means such a permutation on $\bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$ that for each $(a_1, a_2, \ldots, a_r) \in \bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$,

$$\begin{aligned} &(\sigma_1(t_1, s_1), \sigma_2(t_2, s_2), \ldots, \sigma_r(t_r, s_r))(a_1, a_2, \ldots, a_r) \\ &\quad = (\sigma_1(t_1, s_1) a_1, \sigma_2(t_2, s_2), \ldots, \sigma_r(t_r, s_r) a_r). \end{aligned}$$

Clearly, $\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r))$ and $(\sigma_1(t_1, s_1), \sigma_2(t_2, s_2), \ldots, \sigma_r(t_r, s_r))$ are uniquely determined from each other.

Moreover, if also $(t', s') \in T_v$, $\beta(t') = (t'_1, t'_2, \ldots, t'_r)$, and $\beta(s') = (s'_1, s'_2, \ldots, s'_r)$, then for any $(a_1, a_2, \ldots, a_r) \in \bigoplus_{i=1}^{r} Z_{p_i^{\alpha_i}}$

$$\begin{aligned} &\bar{\sigma}((t'_1, t'_2, \ldots, t'_r), (s'_1, s'_2, \ldots, s'_r)) \bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r)) (a_1, a_2, \ldots, a_r) \\ &\quad = \bar{\sigma}((t'_1, t'_2, \ldots, t'_r), (s'_1, s'_2, \ldots, s'_r))(\sigma_1(t_1, s_1) a_1, \sigma_2(t_2, s_2) a_2, \ldots, \sigma_r(t_r, s_r) a_r) \\ &\quad = (\sigma_1(t'_1, s'_1) \sigma_1(t_1, s_1) a_1, \sigma_2(t'_2, s'_2) \sigma_2(t_2, s_2) a_2, \ldots, \sigma_r(t'_r, s'_r) \sigma_r(t_r, s_r) a_r). \end{aligned}$$

This implies that

$$\bar{\sigma}((t'_1, t'_2, \ldots, t'_r), (s'_1, s'_2, \ldots, s'_r))\bar{\sigma}((t_1, t_2, \ldots, t_r), (s_1, s_2, \ldots, s_r))$$
$$=(\sigma_1(t'_1, s'_1)\sigma_1(t_1, s_1), \sigma_2(t'_2, s'_2)\sigma_2(t_2, s_2), \ldots, \sigma_r(t'_r, s'_r)\sigma_r(t_r, s_r)).$$

Thus, we have proved

$$\bar{G}_v \cong \bigoplus_{i=1}^{r} G_{p_i^{\alpha_i}}. \tag{3.7}$$

Combining (3.6) and (3.7), we get (3.3). Since isomorphic groups have the same cycle index, we obtain (3.4). This completes the proof. □

From Theorems 1.1 and 3.1, we immediately obtain the following theorem.

Theorem 3.2. *The number of equivalence classes of k-subsets of Z_v is*

$$\frac{1}{k!}\left[\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^k \mathop{\text{※}}_{i=1}^{r} P_{G_{p_i^{\alpha_i}}}(x+1, x^2+1, \ldots, x^{p_i^{\alpha_i}}+1)\right]_{x=0},$$

where $P_{G_{p_i^{\alpha_i}}}$ are given in (1.6)–(1.9). And the number of equivalence classes of all subsets of Z_v is

$$\left[\mathop{\text{※}}_{i=1}^{r} P_{G_{p_i^{\alpha_i}}}(x+1, x^2+1, \ldots, x^{p_i^{\alpha_i}}+1)\right]_{x=1}.$$

Applying Theorem 3.2 to the number of inequivalent cyclic difference sets, we have the following theorem.

Theorem 3.3. *Let v, k, λ be positive integers and $\lambda(v-1)=k(k-1)$. Then the number of inequivalent (v, k, λ) cyclic difference sets is less than or equal to*

$$\frac{1}{k!}\left[\left(\frac{\mathrm{d}}{\mathrm{d}x}\right)^k \mathop{\text{※}}_{i=1}^{r} P_{G_{p_i^{\alpha_i}}}(x+1, x^2+1, \ldots, x^{p_i^{\alpha_i}}+1)\right]_{x=0},$$

and the number of all inequivalent nontrivial cyclic difference sets in Z_v is less than or equal to

$$\left[\mathop{\text{※}}_{i=1}^{r} P_{G_{p_i^{\alpha_i}}}(x+1, x^2+1, \ldots, x^{p_i^{\alpha_i}}+1)\right]_{x=1} - 2(v+1).$$

Of course, the upper bounds, in general, are very coarse.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182 (Springer, Berlin, 1972).
[2] M. Hall Jr, A survey of difference sets, Proc. Amer. Math. Soc. 7 (1956) 975–986.
[3] C. Ko and W.-D. Wei, Combinatorial Theory, Vol. 1 (Science Press, Peking, 1981, 1984).
[4] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und Chemische Verbindungen, Acta Math. 68 (1937) 145–254.
[5] W.-D. Wei, Combinatorial Theory, Vol. 2 (Science Press, Peking, 1987).
[6] W.-D. Wei, X.-H. Gao and B.-F. Yang, Equivalence relation on the set of subsets of Z_v and enumeration of the equivalence classes (Research Announcement), Adv. Math. 17 (1988) 326–327.