Integer Representations of Complex Reflection Groups

HASAN ARSLAN*,1, MARIAM ZAAOUR*,2, ALNOUR ALTOUM*3
*Department of Mathematics, Faculty of Science, Erciyes University, 38039, Kayseri, Turkey
1hasanarslan@erciyes.edu.tr 2mariamzaarour94@gmail.com 3alnouraltoum178@gmail.com

Abstract

In this paper, we construct a mixed-base number system over a complex reflection group $G(m, 1, n)$, the generalized symmetric group. We also introduce one-to-one correspondence between positive integers and elements of $G(m, 1, n)$ after constructing the subexceedant function in relation to this group. In addition, we provide a new enumeration system for $G(m, 1, n)$ by defining the inversion statistic on $G(m, 1, n)$.

Keywords: Weyl group, Complex reflection group, Subexceedant function, Integer representation.

2020 Mathematics Subject Classification: 20F55, 20C30.

1 Introduction

The main purpose of this paper is to construct the integer representations of the complex reflection group $G(m, 1, n)$. It is well-known that if $m = 1$, then $G(1, 1, n)$ is the symmetric group $S_n$ which is a Weyl group of type $A_{n-1}$; for $m = 2$, $G(2, 1, n)$ is the hyperoctahedral group which is a Weyl group of type $B_n$; and $G(2, 2, n)$ is a Weyl group of type $D_n$ (see [10]). In particular, the integer representations of the classical Weyl groups of types $A_{n-1}$, $B_n$, $D_n$ were studied in [6], [8] and [1], respectively. In our work, $\varepsilon$ denotes the $m$-th root of unity. For a fixed $m > 1$, $G(m, 1, n)$ denotes the complex reflection group which consists of all permutations $\pi$ acting on the set $I^m_n = \{\varepsilon^k i | i = 1, \ldots, n; k = 1, \ldots, m\}$. In other words, it consists of all bijections $\pi$ of the set $I^m_n$ onto itself providing that $\pi(\varepsilon^k i) = \varepsilon^k \pi(i)$ for all $i = 1 \cdots n; k = 1, \ldots, m$. Let $S_n$ be the symmetric group on $\{1, \cdots, n\}$ and $C_m$ be the cyclic group of order $m$. Then $G(m, 1, n)$ is a split group extension of
$C^n_m$ by $S_n$, where $C^n_m$ is the direct product of $n$ copies of $C_m$. The representation of $G(m, 1, n)$ is given by the following form (see [4]):

$$G(m, 1, n) = (s_1, \cdots, s_{n-1}, t_1, \cdots, t_n : s_i^2 = (s_i s_{i+1})^2 = (s_i s_j)^2 = e, |i - j| > 1;$$

$$t_i^m = e, t_i t_j = t_j t_i, s_i t_i s_i = t_i t_j, s_i t_j = t_j s_i, j \neq i, i + 1).$$

The group $G(m, 1, n)$ has a Cohen (Dynkin) diagram with respect to the set of generators $S = \{t_1, s_1, \cdots, s_{n-1}\}$ as follows:

$$B_n^{(m)} : \begin{array}{c}
\bullet \\
-1 \sqrt{2} \\
\bullet \\
\hline
m & s_1 & s_2 & s_{n-2} & s_{n-1} \\
\hline
\end{array}$$

The group $S_n$ is generated by $\{s_1, \cdots, s_{n-1}\}$, where $s_i$ ($i = 1, \cdots, n-1$) is described with the transposition $(i, i+1)$. Here, $t_i$ ($i = 1, \cdots, n$) may be defined as the permutation

$$t_i = (\frac{1}{1} \frac{2}{2} \cdots \frac{i-1}{i-1} \frac{i+1}{i} \cdots \frac{n}{n}).$$

From the above relations, we obtain that $\sigma t_i \tau^{-1} = t_{\sigma(i)}$ for any $\tau \in S_n$ and $i = 1, \cdots, n$. Hence, we conclude for all $i = 1 \cdots, n - 1$ that $t_{i+1} = s_i t_i s_i$ is a reduced expression and the length of each $t_j$ ($j = 1, \cdots, n$) equals to $2j - 1$.

Throughout this paper, we assume that the length function $l$ on $G(m, 1, n)$ is the function $G(m, 1, n) \rightarrow \mathbb{N}_0$ associated with the set of generators $S$ in the sense of [2]. It is well-known that the cardinality of $G(m, 1, n)$ is $m^n n!$. Therefore, any element $\pi$ of the group $G(m, 1, n)$ is written as follows (see [3]):

$$\pi = (e^{\iota_1} e^{\iota_2} e^{\iota_n} \cdots e^{\iota_{n-1}}) = \beta \prod_{k=1}^{n} t_k^r \in G(m, 1, n),$$

where $1 \leq r_k \leq m$, $\beta = (1 \beta_2 \cdots \beta_n) \in S_n$, and $\beta_i = \beta(i)$ for all $i = 1, \cdots, i$. Let

$$\sigma = (e^{\iota_1} \gamma_1 e^{\iota_2} \gamma_2 \cdots e^{\iota_{n-1}} \gamma_n) \in G(m, 1, n),$$

where $\gamma = (1 \gamma_2 \cdots \gamma_n) \in S_n$, $1 \leq v_i \leq m$. Hence, based on [3] we obtain that

$$\pi \sigma = (e^{\iota_1} e^{\iota_2} e^{\iota_{n-1}} e^{\iota_n}) (e^{\iota_1} \gamma_1 e^{\iota_2} \gamma_2 \cdots e^{\iota_{n-1}} \gamma_n)$$

$$= (e^{\iota_1} e^{\iota_2} \cdots e^{v_n}) \beta_n \cdots \beta_2 \beta_1 \beta_n \cdots \beta_2 \beta_1 \beta_n).$$

As a convention, we assume throughout this paper that the rightmost permutation acts first in the multiplication of permutations.
The longest element \( w_0 = \prod_{k=1}^{n} t_k^{m-1} \) of the complex reflection group \( G(m, 1, n) \) can be written in the following form:

\[
w_0 = \left( \varepsilon_{m-1} \begin{array}{cccc}
1 & 1 & \cdots & 1 \\
2 & 2 & \cdots & 2 \\
\vdots & \vdots & \ddots & \vdots \\
\end{array} \right) \in G(m, 1, n).
\]

Thus we may declare from [2] that the length of any reduced expression in \( G(m, 1, n) \) can not exceed \( n(n + m - 2) \), that is the length of \( w_0 \).

This paper is organised as follows: In the second section, we construct the \( G_{m,n} \)-type number system and give its combinatorial descriptions. In section 3, we establish subexceedant function for the complex reflection groups \( G(m, 1, n) \) and show that there exists a one-to-one correspondence between any arbitrary positive integer and an element of a complex reflection group. In section 4, we study the inversion statistic on the complex reflection group. Indeed, using the inversion notion we propose a new enumeration system for \( G(m, 1, n) \).

## 2 Construction of \( G_{m,n} \)-type Number System

Let \( G(m, 1, n) \) be a complex reflection group where \( m \) and \( n \) be two fixed positive integers. In this section, we introduce the \( G_{m,n} \)-type number system and give some of its properties. To understand the \( G_{m,n} \)-type number system, we start with the following definition.

**Definition 2.1.** Every positive integer \( x \) can always be expressed in the following form:

\[
x = \sum_{i=0}^{n-1} d_i G_i
\]

where \( 0 \leq d_i \leq m(i + 1) - 1 \) and \( G_i = m^i! \) for all the \( 0 \leq i \leq n - 1 \).

Throughout the following work, we will represent any positive integer \( x \) in the \( G_{m,n} \)-type number system as follows:

\[
x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0).
\]

**Theorem 2.2.** Any positive integer can be expressed in a unique way in the \( G_{m,n} \)-type number system.

To prove Theorem 2.2 we need the following lemmas, which concern with some fundamental properties of the \( G_{m,n} \)-type number system. In particular, these properties have a structure similar to those of the factoriadic number system of type \( A_{n-1} \) and the hyperoctahedral base system of type \( B_n \).

The two lemmas listed below generalize the results presented in [8] for hyperoctahedral groups.
Lemma 2.3. For any $x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$ in the $G_{m,n}$-type number system, we have

$$0 \leq x \leq G_n - 1.$$  \hfill (2)

As a result of Lemma 2.3, we have exactly $m^n n!$ numbers in the $G_{m,n}$-type number system.

Lemma 2.4. Let $x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$ be a number in $G_{m,n}$-type number system, then we have

$$d_{n-1} G_{n-1} \leq x < (d_{n-1} + 1) G_{n-1}. \hfill (3)$$

Proof of Theorem 2.2

Assume that a positive integer $x$ has two representations in the $G_{m,n}$-type number system as follows:

$$x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0) = (e_{m-1} : e_{m-2} : \cdots : e_1 : e_0),$$

where $d_{n-1} \neq 0$ and $e_{m-1} \neq 0$. The facts that both $d_{n-1}$ and $e_{m-1}$ are at least 1 lead to

$$G_{n-1} \leq d_{n-1} G_{n-1} \leq x \quad \text{and} \quad G_{m-1} \leq e_{m-1} G_{m-1} \leq x. \hfill (4)$$

Now, we suppose that $n \neq m$. Without loss of generality, we can assume that $n < m$. Then by Lemma 2.3 and the right side of equation (4), we obtain

$$x < G_n \leq G_{m-1} \leq x,$$

which is a contradiction. Thus, we get $n = m$.

By induction on the number of digits, we will show that $d_i = e_i$ for all $0 \leq i \leq n - 1$. From equation (1), the assertion is clear for $x = (d_0) = (e_0)$. We assume that a positive integer $x$ with $k(< n)$ digits in the $G_{m,n}$-type number system has a unique representation. Now let $(d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$ and $(e_{n-1} : e_{n-2} : \cdots : e_1 : e_0)$ be two representations of $x$ in the $G_{m,n}$-type number system. Assume that $d_{n-1} \neq e_{n-1}$. Without loss of generality, take $d_{n-1} < e_{n-1}$. Thus, from Lemma 2.4 we get

$$x < (d_{n-1} + 1) G_{n-1} \leq e_{n-1} G_{n-1} \leq x,$$

which is a contradiction and hence $d_{n-1} = e_{n-1}$. Since $d_{n-1} = e_{n-1}$ and by the induction hypothesis, the integer \( x - d_{n-1} G_{n-1} = x - e_{n-1} G_{n-1} \) has a unique representation and so $d_i = e_i$ for all $0 \leq i \leq n - 2$. This completes the proof.

Now, we will explain how to express any positive integer $x$ in terms of the $G_{m,n}$-type number system:
The algorithm proceeds in a series of steps. In the first step of the algorithm, $x$ is divided by $m$ and the reminder is set to be $r_0 = d_0$ in the division process

$$x = mq_0 + r_0.$$ 

Then divide $q_0$ by $2m$ and the reminder is set to be $r_1 = d_1$ in the division process

$$q_0 = 2m.q_1 + r_1.$$ 

By continuing in this way, i.e., by dividing $q_{i-1}$ by $m(i + 1)$ and getting $r_i = d_i$ in the expression

$$q_{i-1} = (i + 1).m.q_i + r_i$$

until the quotient $q_t = 0$ is zero for some integer $t$. Eventually, we write the number $x$ as

$$x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$$

in $G_{m,n}$-type base system.

**Remark 2.5.** By applying the above procedure, having initially selected any fixed positive integer $m$, we can write any positive integer $x$ in the $G_{m,n}$-type number system. Here, $n$ is the number of digits that we obtain when we apply the above procedure to the positive integer $x$. Hence, $n$ is revealed at the end of the operations.

We propose to use the following Python algorithm to convert any positive integer into a number in $G_{m,n}$-type base system:

**Algorithm 1:**

```python
x=int(input('Enter a positive integer:'))
m=int(input('Enter a positive integer:'))
for i in range(1,x):
    d=x%(m*i)
    if x > 0:
        x=x//(m*i)
    else:
        break
print(d, end=':')
```

Let us give an example of how this algorithm works:

**Example 2.6.** The expression of positive integer $x = 199761$ in $G_{7,5}$-type base system is $x = (3 : 13 : 1 : 5 : 2)$.

Alternatively, the following Python algorithm can be used to convert any number in the $G_{m,n}$-type number system into a positive integer:
Algorithm 2:
n=int(input('enter the indeks of $G_{m,n}$ base:'))
m=int(input('enter the value of $m$'))
f=1
x=0
for i in range(0,n):
d=int(input('enter a number in $G_{m,n}$-type number system:'))
if i == 0 or i == 1:
f = 1
else:
f = f * i
t = m ** (i) * f
z = d * t
x += z
print('The decimal number is:', x)

Example 2.7. Let $x = (56 : 238 : 8 : 270 : 218 : 133 : 236 : 210 : 204 : 102 : 63 : 208 : 157 : 94 : 171 : 89 : 19 : 20 : 50 : 67 : 121 : 134 : 75 : 30 : 37 : 58 : 97 : 104 : 58 : 2 : 75 : 31 : 42 : 24 : 43 : 2 : 17 : 3 : 16 : 16 : 0 : 3)$ be a number in $G_{7,42}$-type number system. It corresponds to the positive integer
847269328185736775326682798778327079883274857780833279866982328472693276
65908932687971.

3 Integer Representation of Complex Reflecton Groups

Mantaci and Rakotondrajao [7] introduced subexceedant functions for the symmetric group $S_n$ and showed that there is one-to-one correspondence between permutations in $S_n$ and the subexceedant functions. The subexceedant function is an important tool for constructing integer representations of the classical Weyl groups, (see [1],[5],[8]). Depending more on the structure of the group $G(m,1,n)$ and inspiring by [3], [7] and [8], we will define subexceedant functions for $G(m,1,n)$.

Definition 3.1 ([7]). A subexceedant function $f$ on the set $\{1, \cdots, n\}$ is a map such that
\[ 1 \leq f(i) \leq i, \text{ for all } 1 \leq i \leq n. \] (6)

We denote the set of all subexceedant functions on $\{1, \cdots, n\}$ by $\mathcal{F}_n$ and hence $|\mathcal{F}_n| = n!$. The subexceedant function $f$ on $\{1, \cdots, n\}$ is, in general, identified
with the word $f(1); \cdots; f(n)$. Furthermore, the map

$$
\psi : F_n \mapsto S_n, \quad \psi(f) = (nf(n)) \cdots (2f(2))(1f(1))
$$

(7)
is a bijection and $(i f(i))$ is a transposition for each $i = 1, \cdots, n$ [7].

Now, let $\beta = (\beta_1 \beta_2 \cdots \beta_n)$ be an element of $S_n$. In [7], Mantaci and Rakotondrajao defined the subexceedant function $f$ corresponding to $\beta$ according to the map $\psi$ with the following steps:

- Set $f(n) = \beta_n$.
- Then, take the image of $\beta^{-1}(n)$ in the permutation $\beta = (\beta_1 \beta_2 \cdots \beta_n)$ as $\beta_n$. Thus, a new permutation $\beta'$ that contains $n$ as a fixed point is obtained. Hence, $\beta'$ can be considered as an element of $S_{n-1}$.
- Set $f(n-1) = \beta'_n$.
- Apply the same procedure for the permutation $\beta'$, i.e., exchange the image of $\beta'(n-1)$ in the permutation $\beta'$ and $\beta'_n$, and determine in this manner $f(n-2)$.
- Continue this iteration until you find all the $f(i)$ values for each $1 \leq i \leq n$.

Now, we will define the subexceedant functions for the complex reflection group $G(m, 1, n)$.

**Definition 3.2.** Let $x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$ be a number with the $n$-digits in the $G_{m,n}$-type number system. We define the subexceedant function $f$ on the set \{1, \cdots, n\} as follows:

$$
f(i) = 1 + \left\lfloor \frac{d_{i-1}}{m} \right\rfloor, \text{ for all } 1 \leq i \leq n.
$$

(8)

It is clear that $1 \leq f(i) \leq i$ since $0 \leq d_{i-1} \leq m.i - 1$ for all $1 \leq i \leq n$.

Having defined the coefficient $c_i = \varepsilon^{d_{i-1}}$ for all $1 \leq i \leq n$, we associate each $x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$ in the $G_{m,n}$-type number system to a unique permutation

$$
\pi_x = (c_1\beta_1 c_2\beta_2 \cdots c_n\beta_n) \in G(m, 1, n),
$$

where $\beta_f = (\beta_1 \beta_2 \cdots \beta_n) \in S_n$ is the permutation of $S_n$, that is the image $\psi(f)$ of the subexceedant function $f$ under $\psi$ given in equation (7).

As a result of the above facts, we match each positive integer $x$ expressed in the $G_{m,n}$-type number system with an element of the complex reflection group.
$G(m, 1, n)$. On the other hand, we will now show how to convert any element of this group to a positive integer. For this reason, we take any permutation

$$\sigma = (\varepsilon_1^{r_1} \varepsilon_2^{r_2} \cdots \varepsilon_n^{r_n}) \in G(m, 1, n),$$

where $\gamma = (\varepsilon_1^{r_1} \varepsilon_2^{r_2} \cdots \varepsilon_n^{r_n}) \in S_n$, $1 \leq r_i \leq m$. First of all, we determine the subexceedent function $f$ in relation to $\gamma$ in the following manner:

1. Let $f = \psi^{-1}(\gamma) \in \mathcal{F}_n$.

2. Set $d_i = m(f(i+1) - 1) + r_{i+1}$, for all $0 \leq i \leq n - 1$.

3. Compute $x = (d_{n-1} : d_{n-2} : \cdots : d_1 : d_0)$.

Based on the above facts, we will state the following theorem without proof.

**Theorem 3.3.** There is one-to-one correspondence between positive integers and elements of the complex reflection groups.

**Example 3.4.** The corresponding integer representation of $x = 2161$ in the $G_{3, 5}$-type number system is $(1 : 1 : 3 : 0 : 1)$. We obtain the subexceedant function of $x$ based on equation (8) as $f = f(1); f(2); f(3); f(4); f(5) = 1; 1; 2; 1; 1$. Hence, we get $\pi_x = (\varepsilon_1^{3} \varepsilon_2^{2} \varepsilon_3^{4} \varepsilon_4^{5}) \in G(3, 1, 5)$, where $\gamma = (\varepsilon_1^{3} \varepsilon_2^{2} \varepsilon_3^{4} \varepsilon_4^{5} \varepsilon_5^{1}) \in S_5$.

**Example 3.5.** Let $\sigma = (\varepsilon_1^{2} \varepsilon_2^{3} \varepsilon_3^{4} \varepsilon_4^{5} \varepsilon_5^{6}) \in G(4, 1, 6)$, where $\gamma = (\varepsilon_1^{2} \varepsilon_2^{3} \varepsilon_3^{4} \varepsilon_4^{5} \varepsilon_5^{6}) \in S_5$. We obtain the subexceedant function associated with $\gamma$ as

$$f = f(1); f(2); f(3); f(4); f(5); f(6) = 1; 1; 3; 1; 5; 5.$$

Thus, the integer representation of $\sigma$ is

$$406433 = (13 : 14 : 0 : 7 : 3 : 2).$$

Moreover, we deduce that the subexceedant function $f$ associating with the longest element $w_0$ of $G(m, 1, n)$ is $f(1); f(2); \cdots; f(n) = 1; 2; \cdots; n$.

**Corollary 3.6.** Let $w_0$ be the longest element of the complex reflection group $G(m, 1, n)$. Then the integer representation of $w_0$ in the $G_{m,n}$-type number system has the following form:

$$w_0 = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1 : d_0) = (nm-1 : (n-1)m-1 : \cdots : 3m-1 : 2m-1 : m-1).$$

Therefore, it is clear that the order of group $G(m, 1, n)$ is

$$|G(m, 1, n)| = \prod_{i=0}^{n-1} (d_i + 1) = m^n n!.$$
The following algorithm is useful for finding the subexceedant function corresponding to any number $d$ in the $G_{m,n}$-type number system:

**Algorithm 3:**
```
from math import floor
n=int(input('Enter the value of n:'))
m=int(input('Enter the value of m:'))
c=[]
for i in range(1,n+1):
    d=int(input('Enter digit in $G_{(m,n)}$ base system:'))
    f = 1 + floor(d/m)
    c.append(f)
print("The values of subexceedant function is: ", c)
```

**Example 3.7.** Let $d = (17 : 14 : 11 : 8 : 5 : 2) \in G_{3,6}$-type number system, the corresponding subexceedant function of $d$ is obtained as $f(1); f(2); f(3); f(4); f(5); f(6) = 1; 2; 3; 4; 5; 6$.

The following Python algorithm is also used to convert any text message into its numerical value:

**Algorithm 4:**
```
print("Enter a string: ", end="")
text = input()
for char in text:
    ascii = ord(char)
    print(ascii, end="")
```

**Example 3.8.** Taking the sentence THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG, then its ASCII code is [84, 72, 69, 32, 81, 85, 73, 67, 75, 32, 66, 82, 79, 87, 78, 32, 70, 79, 88, 32, 74, 85, 77, 80, 83, 32, 79, 86, 69, 82, 32, 84, 72, 69, 32, 76, 65, 90, 89, 32, 68, 79, 71]. If we choose $m=7$, then we obtain the integer representation of 84726932818573677532668279877832707988327485778083327986698232847269327665908932687971 in $G_{7,42}$-type number system as (56 : 238 : 8 : 270 : 218 : 133 : 236 : 210 : 204 : 102 : 63 : 208 : 157 : 94 : 171 : 89 : 19 : 20 : 50 : 67 : 121 : 134 : 75 : 30 : 37 : 58 : 97 : 104 : 58 : 2 : 75 : 31 : 42 : 24 : 43 : 2 : 17 : 3 : 16 : 16 : 0 : 3) using Algorithm 1.
4 Inversion Statistic on \( G(m, 1, n) \)

A finite Weyl group has two canonical length functions, essentially identical, which reveal a great deal of facts about the structure of the group. The first length function is defined as the length of the reduced expressions in terms of the set of standard generators, while the other length function is defined by the effect of \( W \) on the positive root system. For complex reflection groups, the length function \( l \) defined by reduced expressions with respect to the set of the canonical generators \( S = \{ t_1, s_1, \cdots, s_{n-1} \} \), is unfortunately not a very useful tool for studying the structure of such groups. For this reason, Bremke and Malle defined a new length function based on the generalized root system in [2].

Let \( V \) be a complex vector space \( \mathbb{C}^n \) with the standard unitary inner product. Let \( \{ e_1, \cdots, e_n \} \) be the set of standard basis vectors of \( V \). Actually, the imprimitive complex reflection group \( G(m, 1, n) \subset GL_n(\mathbb{C}) \) is generated by the reflections \( s_1, \cdots, s_{n-1} \) of order 2 associated with the roots \( e_2 - e_1, \cdots, e_n - e_{n-1} \), respectively, and a (complex) reflection \( t_1 \) of order \( m \) with root \( e_1 \). Our next aim is to describe a new statistic on \( G(m, 1, n) \). To introduce this new statistic on \( G(m, 1, n) \), it would make more sense to think of \( G(m, 1, n) \) as a complex reflection group with the following root system given in [2]:

\[
\Phi = \{ \varepsilon^i e_j - \varepsilon^k e_l \mid \varepsilon^i e_j \neq \varepsilon^k e_l, \ 0 \leq i, k \leq m - 1, \ 1 \leq j, l \leq n \}.
\]

Positive and negative root systems are defined in the following way, respectively:

\[
\Phi^+ = \{ \varepsilon^i e_j - \varepsilon^k e_l \in \Phi \mid 0 \leq i < k \leq m - 1, \ 1 \leq j \leq n \}
\]

\[
\cup \{ e_j - \varepsilon^k e_l \in \Phi \mid 0 \leq k \leq m - 1, \ 1 \leq l < j \leq n \}
\]

\[
\cup \{ \varepsilon^i e_j - \varepsilon^k e_l \in \Phi \mid 0 \leq i, k \leq m - 1, \ k \neq 0, \ 1 \leq j < l \leq n \},
\]

and \( \Phi^- = \Phi \setminus \Phi^+ = -\Phi^+ \). It is clear that \( |\Phi| = mn(mn - 1) \) and \( |\Phi^+| = |\Phi^-| = \frac{|\Phi|}{2} \).

Now, let

\[
\Delta = \{ e_j - \varepsilon^k e_l \in \Phi \mid 0 \leq k \leq m - 1, \ 1 \leq l \leq j \leq n \} \subset \Phi^+.
\]

Note that, \( \Delta \) is a subset of \( \Phi^+ \) and it contains only one root for each reflection in \( G(m, 1, n) \). Therefore, a triple \((\Phi, \Phi^-, \Delta)\) is so-called a root system for the complex reflection group \( G(m, 1, n) \) (see [2]). From [2], the length function \( L \) connected with the root system \((\Phi, \Phi^-, \Delta)\) is defined as

\[
L : G(m, 1, n) \to \mathbb{N}_0, \quad L(w) = |w(\Delta) \cap \Phi^-|.
\]

Moreover, one can check the fact that

\[
w_0(\Delta) = \varepsilon^{m-1} \Delta \subset \Phi^-.
\]
holds, where \( w_0 = (e_{m-1}^1 e_{m-2}^2 \cdots e_{m-n}^n) \in G(m, 1, n) \) is the longest element \( (l(w_0) = n(n + m - 1)) \) of \( G(m, 1, n) \) in relation to the length function \( l \), which is defined by reduced expressions with respect to the set of the canonical generators \( S \).

**Definition 4.1.** Let \( \sigma \in S_n \). A pair \((\sigma_i, \sigma_j)\) is called an inversion \( \sigma \) if \( i < j \) and \( \sigma_i > \sigma_j \).

Now, we define

\[
\Delta_i = \{ e_i - \varepsilon^k e_i \in \Delta : 0 < k \leq m - 1 \} \\
\cup \{ e_j - \varepsilon^k e_i \in \Delta : 0 \leq k \leq m - 1, \ i < j \leq n \}.
\]

for all \( i = 1, \cdots, n \). Furthermore, the length of the longest element of \( w_0 \) of \( G(m, 1, n) \) (with respect to the definition in (10)) is equal to \( L(w_0) = |\Delta| = n(m - 1) + \frac{nm(n-1)}{2} \). Clearly, \( |\Delta_i| = m(n - i + 1) - 1 \) for all \( i = 1, \cdots, n \).

**Definition 4.2.** For any \( w \in G(m, 1, n) \), we define the number of \( i \)-inversions of \( w \) for all \( i = 1, \cdots, n \) as follows:

\[
\text{inv}_i(w) = |w(\Delta_i) \cap \Phi^-|.
\]

Based on the definitions of the concepts \( \Delta_i \) and \( \text{inv}_i(w) \), we can conclude the following theorem.

**Theorem 4.3.** We have the following combinatorial properties:

1. The set \( \Delta \) given in (9) can be decomposed as

\[
\Delta = \bigsqcup_{i=1}^{n} \Delta_i.
\]

2. The length of any \( w \in G(m, 1, n) \) is expressed as \( L(w) = \sum_{i=1}^{n} \text{inv}_i(w) \).

3. For any \( w \in G(m, 1, n) \) and for all \( i = 1, \cdots, n \), we have

\[
0 \leq \text{inv}_i(w) \leq m(n - i + 1) - 1.
\]

As a consequence of part (2) of Theorem 4.3, we deduce that the sum of the \( i \)-inversions of any given element \( w \in G(m, 1, n) \) can be actually used to calculate the length of the element depending on the length function \( L \). Denote the inversion sequence of \( i \)-inversions of \( w \) by \((\text{inv}_1(w) : \cdots : \text{inv}_n(w))\). As a result of equation (12), we say that the inversion sequence \((\text{inv}_1(w) : \cdots : \text{inv}_n(w))\) possesses the
same properties as a number in the $G_{m,n}$-type number system. Therefore, this enable us to introduce a new kind of classification of all elements of $G(m, 1, n)$. When we enumerate all the elements of the group $G(m, 1, n)$ in lexicographic order, we assign each element of the group to a different integer in the following manner: Given the inversion sequence $(inv_1(w) : \cdots : inv_n(w))$ of $w$, then we define the rank of $w$ as $x + 1$, where $x$ is the positive integer corresponding to the number $(inv_1(w) : \cdots : inv_n(w))$ in the $G_{m,n}$-type number system. This means that a new enumeration system is created on $G(m, 1, n)$.

Example 4.4. Let $(\Phi, \Phi^-, \Delta)$ be the root system of type $B_3^{(3)}$, where

\[
\Delta = \{e_1 - e e_1, e_1 - e^2 e_1, e_2 - e_1, e_2 - e e_1, e_2 - e^2 e_1, e_3 - e_1, e_3 - e e_1, e_3 - e^2 e_1\}
\cup \{e_2 - e e_2, e_2 - e^2 e_2, e_3 - e_2, e_3 - e e_2, e_3 - e^2 e_2\}
\cup \{e_3 - e e_3, e_3 - e^2 e_3\}
\]

and

\[
\Phi^- = \{e^k e_j - e^l e_j \in \Phi \mid 0 \leq i < k \leq 2, \ 1 \leq j \leq 3\}
\cup \{e^k e_l - e^l e_j \in \Phi \mid 0 \leq k \leq 2, \ 1 \leq l < j \leq 3\}
\cup \{e^k e_l - e^l e_j \in \Phi \mid 0 \leq i, k \leq 2, \ k \neq 0, \ 1 \leq j < l \leq 3\}.
\]

We determine $\Delta_1 = \{e_1 - e e_1, e_1 - e^2 e_1, e_2 - e_1, e_2 - e e_1, e_2 - e^2 e_1, e_3 - e_1, e_3 - e e_1, e_3 - e^2 e_1\}$, $\Delta_2 = \{e_2 - e e_2, e_2 - e^2 e_2, e_3 - e_2, e_3 - e e_2, e_3 - e^2 e_2\}$ and $\Delta_3 = \{e_3 - e e_3, e_3 - e^2 e_3\}$. Since $w_0(\Delta) = \varepsilon^2(\Delta) \subset \Phi^-$ for $w_0 \in G(3,1,3)$, then we obtain the inversion sequence for $w_0$ as $(inv_1 w_0 : inv_2 w_0 : inv_3 w_0) = (8 : 5 : 2)$. Thus the rank of $w_0$ is 162, which is the order of the group $G(3,1,3)$. If we take another element $w = (\frac{1}{e_3} \ e_1 \ e_2)\frac{3}{2}$ of $G(3,1,3)$, then we find the inversion sequence of $w$ as $(inv_1 w : inv_2 w : inv_3 w) = (4 : 1 : 0)$, where $w(\Delta_1) \cap \Phi^- = \{e^2 e_3 - e_3, e^2 e_3 - e e_3, e_1 - e_3, e_2 - e_3\}$, $w(\Delta_2) \cap \Phi^- = \{e e_1 - e_1\}$ and $w(\Delta_3) \cap \Phi^- = \emptyset$. The rank of $w$ is 76.

5 Conclusion

In this paper, we define a mixed-radix number system over complex reflection group $G(m, 1, n)$. In addition, we introduce a one-to-one correspondence between the positive integers of the set $\{1, \ldots, m^n!\}$ and the elements of the complex reflection group $G(m, 1, n)$. With this integer representation, we can use the elements of this group more effectively in cryptography. In other words, the integer representation for $G(m, 1, n)$ may allow to build robust cryptographic algorithms based on the structure of this group because of the use of two special parameters (these are $m$
and $n$). For the applications in the cryptography of classical Weyl groups, (see [1,5,8]). It is a natural question to ask whether such integer representations also exist for the other complex reflection groups such as $G(m,m,n)$ and $G(m,p,n)$, where $p$ is prime such that $p|m$ and $G(m,m,n) \subset G(m,p,n) \subset G(m,1,n)$. As a matter of fact, $i$-inversion statistics of Weyl group $A_{n-1}$ and $B_{n}$ were studied in [6] and [9], respectively. We introduce and study $i$-inversion concept for any element of a complex reflection group. Then we use it as an efficient tool to provide a new enumeration system for $G(m,1,n)$.

References

[1] Arslan H., Altoum A., Zaarour M., Integer Representations of Classical Weyl Groups, https://doi.org/10.48550/arxiv.2211.00427, 2022.

[2] Bremke K., Malle G., Reduced Words and a Length Function for $G(e,1,n)$, Indagationes Mathematicae, 8(4): 453-469, 1997.

[3] Can H., Representations of Generalized Symmetric Groups, Contributions to Algebra and Geometry, 37(2):289-307, 1996.

[4] Davies J. W., Morris A. O., The Schur Multiplier of the Generalized Symmetric Group, Journal of the London Mathematical Society, s2-8(4):615-620, 1974.

[5] Doliskani J., Malekian E., Zakerolhosseini A., A Cryptosystem Based on the Symmetric Group $S_{n}$, International Journal of Computer Science and Network Security, 8(2), (2008).

[6] Laisant, C. A., Sur la numeration factorielle, application aux permutations, Bulletin de la Societe Mathematique de France, 16:176-183, 1888.

[7] Mantaci R., Rakotondrajao F., A permutations representation that knows what "Eulerian" means, Discrete Mathematics and Theoretical Computer Science, 4(2): 101-108, 2001.

[8] Raharinirina I. V., Use of Signed Permutations in Cryptography, https://arxiv.org/abs/1612.05605, 2016.

[9] Raharinirina I. V., On hyperoctahedral enumeration system, application to signed permutations, Asian Research Journal of Mathematics, 16(8):40-49, 2020.
[10] Read E., On the Finite Imprimitive Unitary Reflection Groups, Journal of Algebra, 45:439-452, 1977.

[11] Stanley R. P., Enumerative Combinatorics: Volume 1, Cambridge University Press, USA, 2nd edition, 2011.