Turk J Math
() : –

Integer representations of classical Weyl groups

Hasan ARSLAN[1,*], **Alnour ALTOUM**[2,3] , **Mariam ZAAROUR**[2,4]
[1]Department of Mathematics, Faculty of Sciences, Erciyes University, Kayseri, Turkey,
ORCID iD: https://orcid.org/0000-0002-0430-8737
[2]Graduate School of Natural and Applied Sciences, Erciyes University, Kayseri, Turkey,
ORCID iD[3]: https://orcid.org/0000-0003-1380-270X
ORCID iD[4]: https://orcid.org/0000-0001-6363-8042

Received: .202 • **Accepted/Published Online:** .202 • **Final Version:** ..202

Abstract: In this paper, we define a mixed-base number system over a Weyl group D_n, the group of even-signed permutations. We introduce one-to-one correspondence between the positive integers of the set $\{1, \cdots, 2^{n-1}n!\}$ and elements of this group, after constructing the subexceedant function associated with the group. Thus, the integer representations of all the classical Weyl groups are now completed. Furthermore, we present an inversion statistic on the group D_n by using an decomposition of a positive root system of this reflection group. This inversion statistic is compatible with the length function on the group D_n. Then we derive some combinatorial properties for the inversion statistic. In addition, we prove that the *D-major index* is equi-distributed with this inversion statistic on D_n. Finally, we propose a public-key cryptosystem based on both the generalized hidden discrete logarithm problem and the integer representation over the group D_n.

Key words: Even-signed permutation group, permutation statistic, inversion number, public-key cryptography, hidden discrete logarithm problem

1. Introduction

Integer representation of any element of a classical Weyl group W is a crucial tool to understand the structure of the group and to use efficiently the elements of the group in the encryption-decryption process. Throughout this paper, for any two m and n integers such that $m \leq n$, we assume that $[m, n] := \{m, m+1, \cdots, n\}$. Let S_n be the symmetric group of order $n!$, which is a Weyl group of type A_{n-1}. In the case of the symmetric group, first of all, Laisant established factoriadic number system in [8], and then Doliskani et al. [5] introduced a bijection map between positive integers and elements of symmetric groups. Using this map, they proposed a Generalized El-Gamal cryptosystem over S_n. Due to the algebraic properties of S_n, the proposed system resists attacks by algorithms like Pohlig-Hellman on the discrete logarithm problem.

When W is a hyperoctahedral group, Raharinirina described the hyperoctahedral base system and studied the integer representations of the elements of this group [13]. Subsequently, some robust cryptosystems resistant to Silver-Pohlig-Helman's attacks were developed in [13].

The group D_n is a group of even-signed permutations acting on the set $I_n = \{-n, \cdots, -1, 1, \cdots, n\}$

*Correspondence: hasanarslan@erciyes.edu.tr
2010 *AMS Mathematics Subject Classification:* 20F55, 94A60

such that any element of D_n has an even number of negative entries in its image, where the group operation is the composition of the bijections. As a convention, when multiplying permutations, the rightmost permutation acts first, as usual. Let $\mathbb{R}^n$ be the Euclidean space with $\{e_1, \cdots, e_n\}$ the set of standard basis vectors. In fact, a finite real reflection group $D_n \subset GL_n(\mathbb{R})$ is generated by the canonical reflections $s_0, s_1, \cdots, s_{n-1}$ of order 2 associated with the roots $e_2 + e_1, e_2 - e_1 \cdots, e_n - e_{n-1}$, respectively. It is well-known that D_n is a semi-direct product of the form $D_n = S_n \rtimes \mathcal{T}_n'$, where S_n is the symmetric group generated by $\{s_1, \cdots, s_{n-1}\}$ and $\mathcal{T}_n'$ is a reflection subgroup of D_n generated by $\{t_1 t_i \ : \ 2 \leq i \leq n\}$, $t_{i+1} := s_i t_i s_i$ for each $1 \leq i \leq n-1$. Moreover, each t_i, $1 \leq i \leq n$ is a reflection of order 2 associated with the root e_i. Note that $s_0 = t_1 s_1 t_1$. Therefore, the cardinality of the group D_n is $2^{n-1} n!$ and each element $w \in D_n$ can be uniquely written in the form

$$w = \begin{pmatrix} 1 & 2 & \cdots & n \\ (-1)^{r_1}\beta_1 & (-1)^{r_2}\beta_2 & \cdots & (-1)^{r_n}\beta_n \end{pmatrix} = \beta \prod_{k=1}^{n} t_k^{r_k},$$

where $r_i \in \{0,1\}$, the sum $\sum_{i=1}^{n} r_i$ is even, $\beta = \begin{pmatrix} 1 & 2 & \cdots & n \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} = \beta_1 \cdots \beta_n \in S_n$, and $\beta_i = \beta(i)$ for all $i = 1, \cdots, n$. Along this paper, we will represent any element w of the group D_n in the window notation as:

$$w = [k_1\beta_1, \cdots, k_n\beta_n],$$

where $k_i \in \{-1, 1\}$ for all $i \in \{1, \cdots, n\}$. If we consider the group D_n as a real reflection group with the following root system

$$\Psi = \{\pm e_j \pm e_i \ : \ 1 \leq i \neq j \leq n\},$$

then we have the sets of positive and negative roots regarding with Ψ, which are, respectively, defined as follows:

$$\Psi^+ = \{e_j - e_i, \quad e_j + e_i \quad : \quad 1 \leq i < j \leq n\},$$

and $\Psi^- = -\Psi^+$. From [7], the root system Ψ can be decomposed as $\Psi = \Psi^+ \bigsqcup \Psi^-$. The length function l on D_n associated with the root system Ψ is defined as

$$l \ : \ D_n \to \mathbb{N}_0, \quad l(w) = \mid w(\Psi^+) \cap \Psi^- \mid. \tag{1.1}$$

Moreover, the length $l(w)$ of w is also equal to the length of the minimal expression for w in terms of elements of $\{s_0, s_1, \cdots, s_{n-1}\}$. Note here that the length of any reduced expression in D_n is at most $n^2 - n$. For further information about the classical Weyl groups, one can see [7].

A function $f : S_n \to \mathbb{N}$ is called as a *permutation statistic*. That is, a permutation statistic is a function mapping S_n into the nonnegative integers. Recently, permutation statistics have played a very important fundamental role in enumerative combinatorics. Let $\sigma = \sigma_1 \cdots \sigma_n \in S_n$. As is well-known, the inversion, the descent set and the major index of σ are respectively defined as follows (see [14]):

$$\begin{aligned} inv(\sigma) =& |\{(i,j) \in [1,n] \times [1,n] \ : \ i < j \ and \ \sigma_i > \sigma_j\}| \\ Des(\sigma) =& \{i \in [1, n-1] \ : \ \sigma_i > \sigma_{i+1}\} \\ maj(\sigma) =& \sum_{i \in Des(\sigma)} i. \end{aligned}$$

MacMahon algebraically proved in [10] that the major index maj and the number of inversions inv are equi-distributed over the symmetric group S_n, that is,

$$\sum_{\sigma \in S_n} q^{maj(\sigma)} = \sum_{\sigma \in S_n} q^{inv(\sigma)} = [n]_q! \tag{1.2}$$

where $[n]_q! := [1]_q[2]_q \cdots [n-1]_q[n]_q$ is the usual q-analogue of $n!$. The first bijective proof of this equi-distribution in the equation (1.2) was given by Foata in [6]. Second bijective proof, essentially due to Carlitz in [4]. In MacMahon's honor, if any permutation statistic is equi-distributed with the length function, i.e., the number of inversions, then it is said to be *Mahonian*.

For any $w \in D_n$, let $neg(w) = |\{i \in [n] : w(i) < 0\}|$ and $Des(w) := \{i \in [n-1] : w(i) > w(i+1)\}$. In [2], Biagioli introduced the *D-negative descent multiset* as

$$DDes(w) = Des(w) \cup \{-w(i) - 1 : i \in neg(w)\} \backslash \{0\}$$

and then defined *D-major index*, which is denoted by *dmaj*, permutation statistic in the following way:

$$dmaj(w) = \sum_{i \in DDes(w)} i.$$

Biagioli proved in [2] that dmaj is Mahonian, that is,

$$\sum_{w \in D_n} q^{dmaj(w)} = \sum_{w \in D_n} q^{l(w)} = [2]_q[4]_q \cdots [2n-2]_q[n]_q,$$

where l is the length function in the equation (1.1).

There are essentially two motivations for the paper. The first of these is to pave the way for using the elements of this reflection group effectively in encryption-decryption operations. For this purpose, we construct a one-to-one correspondence between the positive integers and the elements of this group. Any word or sentence can be expressed as a unique element of this group after converting it to a positive integer by using ASCII codes. Then its encryption or decryption process is performed. The second motivation of this study is to introduce an inversion statistic which is equally distributed with dmaj over D_n.

The following definition describes the hidden discrete logarithm problem (HDLP) and the generalized hidden discrete logarithm problem (GHDLP):

Definition 1.1 *Let G be a non-commutative group. Given two elements $g, h \in G$ such that $h = wg^x w^{-1}$ for an integer x and an w element of G. The hidden discrete logarithm problem is to find the pair (x, w) from the relation $h = wg^x w^{-1}$ [11]. Moreover, the generalized hidden discrete logarithm problem is to obtain the pair of integers (x, y) from the relation $k = (w)^y g^x (w)^{-y}$ for $g, k, w \in G$ [12].*

The rest of this paper is organized as follows: In Section 2, we define a mixed-base number system over the group D_n. In Section 3, we give a one-to-one correspondence between positive integers of the set $\{1, \cdots, 2^{n-1}n!\}$ and the elements of this group by means of subexceedant functions. In Section 4, we define the concept of inversion statistic on the group D_n and investigate its properties. Then, we will give an inversion table of all elements of the group D_3. Furthermore, we propose a new cryptosystem based on the generalized hidden discrete logarithm problem (GHDLP) over the group D_n in Section 5. The algebraic properties of D_n make the system resistant to attacks like the Pohlig-Hellman algorithm.

2. Construction of D_n-type Number System

In this section, we first define the D_n-type number system and describe its structure.

Definition 2.1 *The D_n-type number system is a radix base system in which every positive integer x can be expressed in the following form:*

$$x = \sum_{i=1}^{n-1} d_i D_i \tag{2.1}$$

where $d_i \in \{0, 1, 2, \cdots, 2i+1\}$ and $D_i = 2^{i-1} i!$ for all $1 \leq i \leq n-1$.

Then, for any positive integer x in the D_n-type number system, we use the notation

$$x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}.$$

According to the following theorem, there is a one-to-one correspondence between positive integers and the D_n-type number system.

Theorem 2.2 *Every positive integer in the set $\{1, \cdots, 2^{n-1} n!\}$ is represented in a unique way in the D_n-type base system.*

In order to prove the theorem, we need the following lemmas, which concern some fundamental properties of the D_n-type number system. In fact, these properties have a similar structure to those of the factoriadic number system and the hyperoctahedral base system.

Lemma 2.3 *For any $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$, we have*

$$0 \leq x \leq D_n - 1. \tag{2.2}$$

Proof Due to the fact that $d_i \in \{0, 1, 2, \cdots, 2i+1\}$ and $D_i = 2^{i-1} i!$ for all $1 \leq i \leq n-1$, thus

$$0 \leq \sum_{i=1}^{n-1} d_i D_i \leq \sum_{i=1}^{n-1} (2i+1) D_i.$$

On the other hand, we have

$$(2i+1) D_i = D_{i+1} - D_i$$

for each $1 \leq i \leq n-1$, hence by direct calculations we conclude that $0 \leq \sum_{i=1}^{n-1} d_i D_i \leq D_n - 1$. □

As a result of Lemma 2.3, we can deduce that there are exactly $2^{n-1} n!$ numbers in the D_n-type number system for any positive integer $n \geq 2$.

Lemma 2.4 *Let $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$ be a number in D_n-type number system, then we have*

$$d_{n-1} D_{n-1} \leq x < (d_{n-1} + 1) D_{n-1}. \tag{2.3}$$

Proof If we take y as $x - d_{n-1}D_{n-1} = (d_{n-2} : \cdots : d_2 : d_1)_{D_n}$, then from the equation (2.2), we can write y in the following way:

$$0 \leq y \leq D_{n-1} - 1. \tag{2.4}$$

By adding $d_{n-1}D_{n-1}$ to each side of the equation (2.4), we conclude that the proof is completed, as desired. □

As a result of Lemma 2.3 and 2.4, we can provide the proof of Theorem 2.2.

***Proof of Theorem* 2.2**:
Assume that a positive integer x has two representations in the D_n-type number system as follows:

$$x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n} = (e_{m-1} : e_{m-2} : \cdots : e_2 : e_1)_{D_n},$$

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 give rise to

$$D_{n-1} \leq d_{n-1}D_{n-1} \leq x \quad \text{ and } \quad D_{m-1} \leq e_{m-1}D_{m-1} \leq x. \tag{2.5}$$

Now, suppose that $n \neq m$. Without loss of generality, we can assume that $n < m$. Then by Lemma 2.3 and the inequality in the right hand side of equation (2.5), we obtain

$$x < D_n \leq D_{m-1} \leq x,$$

which is a contraction. Thus we get $n = m$.

Now we show that $d_i = e_i$ for all $1 \leq i \leq n-1$. In what follows, we proceed by induction on the number of digits. From the equation (2.1), the assertion is clear for $x = (d_1)_{D_n} = (e_1)_{D_n}$. Assume that a positive integer x with k $(< n-1)$ digits in the D_n-type number system has a unique representation. Suppose that $d_{n-1} \neq e_{n-1}$. Without loss of generality, take $d_{n-1} < e_{n-1}$. Thus, we get from Lemma 2.4

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

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

Now, we will explain how any positive integer x can be written in the D_n-type number system:
The algorithm proceeds in a series of steps. In the first step of the algorithm, x is divided by 4 and the reminder is set to be $r_1 = d_1$ in the division process

$$x = 4q_1 + r_1.$$

Then divide q_1 by 6 and the reminder is assigned to be $r_2 = d_2$ in the following division process

$$q_1 = 6q_2 + r_2.$$

Continue these operations by dividing q_{i-1} by $2(i+1)$ and taking $r_i = d_i$ in the expression

$$q_{i-1} = 2(i+1)q_i + r_i$$

until the quotient q_{n-1} is zero for some integer n. Thus, at the final step, we get

$$q_{n-2} = 2nq_{n-1} + r_{n-1}$$

and set r_{n-1} as d_{n-1}. Eventually, we write the number x as

$$x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n} \tag{2.6}$$

in D_n-type base system.

Any positive integer can be written in the form (2.6) using the following Python algorithm below:

Algorithm 1:

```
x=int(input('Enter a positive integer:'))
h=4
for i in range(1,x):
d = x%h
if x > 0 :
x = x//h
h=h+2
else:
break
print(d, end=':')
```

The following example illustrates how this algorithm works:

Example 2.5 *We choose an integer* $x = 151100130419$. *The expression of integer* x *in* D_{12}*-type base system is* $x = (3 : 15 : 6 : 9 : 8 : 5 : 4 : 5 : 7 : 2 : 3)_{D_{12}}$.

On the other hand, given any number in the D_n-type number system, the following Python algorithm provides facilities to turn this number into a positive integer:

Algorithm 2:

```
n=int(input('Enter the index of D_n base system '))
f=1
x=0
for i in range(1,n):
d=int(input('Enter a number in D_n-type number system'))
f = f * i
t = 2 ** (i - 1) * f
z=d*t
x +=z
print('The decimal number is: ',x)
```

Example 2.6 *Let* $x = (4 : 8 : 9 : 1 : 2 : 3 : 4 : 1 : 1 : 2 : 0 : 3 : 3 : 1 : 2 : 2)_{D_{17}}$ *be a number in* D_{17}*-type number system. It corresponds to the positive integer* $x = 2920246490038677730$.

3. Integer Representations of Even-Signed Permutations

Mantaci and Rakotondrajao [9] defined subexceedant functions for the symmetric group S_n and showed that there was a one-to-one correspondence between permutations and the subexceedant functions. Subexceedant function is a fundamental tool to provide integer representations of the classical Weyl groups, see [5, 13]. We will define the subexceedant functions for the group of even-signed permutations by inspiring [13] and depending on the structure of the group D_n.

Definition 3.1 ([9]) *A subexceedant function on the set* $\{1, \cdots, n\}$ *is a map* $f : \{1, \cdots, n\} \longmapsto \{1, \cdots, n\}$, *such that*

$$1 \leq f(i) \leq i \quad \textit{for} \quad \textit{all} \quad 1 \leq i \leq n. \tag{3.1}$$

Denote by $\mathcal{F}_n$ the set of all subexceedant functions on $\{1, \cdots, n\}$ and hence $\mid \mathcal{F}_n \mid= n!$. The subexceedant function f on $\{1, \cdots, n\}$ is, in general, expressed by the word $f(1); \cdots ; f(n)$. Moreover, the map

$$\varphi : \mathcal{F}_n \mapsto S_n, \quad \varphi(f) = (nf(n)) \cdots (2f(2))(1f(1)) \tag{3.2}$$

is a bijection and $(if(i))$ is a transposition for each $1 \leq i \leq n$ [9].

Now let $\beta = [\beta_1, \cdots, \beta_n]$ be an element of S_n, which is given in the window notation. In [9], Mantaci and Rakotondrajao described the subexceedant function f corresponding to β under the map φ with the following steps:

- Set $f(n) = \beta_n$.
- Then multiply β on the left by the transposition $(n\beta(n))$, that is, exchange the image of $\beta^{-1}(n)$ in the window notation of β and β_n. Thus a new permutation β' that contains n as a fixed point is obtained and so β' can be think of as an element of S_{n-1}.
- Set $f(n-1) = \beta'_{n-1}$.
- Continue the same procedure for the permutation β' by exchanging the image of ${\beta'}^{-1}(n-1)$ in the window notation of β' and β'_{n-1} and then determine in this manner $f(n-2)$.
- Proceed with this iteration until you find all the $f(i)$ values for each $1 \leq i \leq n$.

Definition 3.2 *Let* $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$ *be a number with the* $(n-1)$*-digits in the* D_n*-type number system. We define the subexceedant function* f *for the group* D_n *as follows:*

$$f(1) = 1, \quad f(i) = 1 + \lfloor \frac{d_{i-1}}{2} \rfloor \quad \textit{for} \quad \textit{all} \quad 2 \leq i \leq n \tag{3.3}$$

where $\lfloor \cdot \rfloor$ *denotes the floor function.*

It is clear here that $1 \leq f(i) \leq i$ for all $1 \leq i \leq n$. We define $\tau(x) :=$ the number of odd integer components appearing in the expression $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$. Having defined the sign $k_i = (-1)^{d_{i-1}}$ for all $2 \leq i \leq n$ and taken the sign $k_1 = (-1)^{\tau(x)}$, we associate each $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$ in the D_n-type number system with a unique even-signed permutation

$$\alpha_x = [k_1\beta_1, \cdots, k_n\beta_n],$$

where $\beta_f = [\beta_1, \cdots, \beta_n]$ is the image $\varphi(f)$ of the subexceedant function f under φ given in equation (3.2).

Thus, we map each positive integer x given in the D_n-type number system to an element of the group of even-signed permutations. Conversely, we will now show how to associate any element of this group with a positive integer. For this purpose, we take any even-signed permutation $\pi = [k_1\gamma_1, \cdots, k_n\gamma_n]$, where $\gamma \in S_n$. First of all, we determine the subexceedant function f in relation to π in the following manner:

1. Let $f = \varphi^{-1}(\gamma) \in \mathcal{F}_n$
2. For all $1 \leq i \leq n-1$, define $r_i = \begin{cases} 0 & k_{i+1} > 0 \\ 1 & k_{i+1} < 0 \end{cases}$
3. Set $d_i = 2(f(i+1) - 1) + r_i$, for all $1 \leq i \leq n-1$
4. Establish $x = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n}$.

By checking the sign k_1 in the even-signed permutation π, it can be verified that the number of odd integer components contained in the expression of x in D_n-type base system is odd or even. As a result of the above facts, we can state the following theorem without proof.

Theorem 3.3 *There is a one-to-one correspondence between positive integers and elements of the group of even-signed permutations.*

Since $f(1) = 1$, the following algorithm is helpful to find all $f(i)$ values of the subexceedant function corresponding to any given positive integer, where $2 \leq i \leq n$.

Algorithm 3:

```
from math import floor
x = int(input('Enter a positive integer:'))
m = 4
for i in range(2, x):
d = x%m
f = 1 + floor(d/2)
if x > 0 :
x = x//m
m=m+2
else:
break
print(f, end=';')
```

Example 3.4 *Let* $x = 151100130419 = (3 : 15 : 6 : 9 : 8 : 5 : 4 : 5 : 7 : 2 : 3)_{D_{12}}$. *Determine the subexceedant function by applying algorithm 3 as* $f = f(1); f(2); f(3); f(4); f(5); f(6); f(7); f(8); f(9); f(10); f(11); f(12) = 1; 2; 2; 4; 3; 3; 3; 5; 5; 4; 8; 2$. *Since* $\tau(x) = 7$, *hence we get* $\alpha_x = [-1, -11, -12, 10, -6, 7, -3, 9, -5, -4, 8, -2] \in D_{12}$.

Example 3.5 *Let* $\pi = [4, 3, 8, 12, -9, -7, -10, -11, 1, 5, -2, -6] \in D_{12}$. *We obtain the subexceedant function associated with* π *as* $f = f(1); f(2); f(3); f(4); f(5); f(6); f(7); f(8); f(9); f(10); f(11); f(12) = 1; 2; 2; 1; 1; 5; 5; 2; 1; 5; 2; 6$. *Thus, the integer representation of* π *is*

$$455941042762 = (11 : 3 : 8 : 0 : 3 : 9 : 9 : 1 : 0 : 2 : 2)_{D_{12}}.$$

The longest element w_0 of the Weyl group of type D_n can be expressed in the window notation as follows:

$$w_0 = \begin{cases} [-1, -2, \cdots, -n], & n \text{ is even}, \\ [1, -2, \cdots, -n], & n \text{ is odd}. \end{cases}$$

Furthermore, we conclude that the subexceedant function f corresponding to w_0 is $f(1); f(2); \cdots; f(n) = 1; 2; \cdots; n$.

Corollary 3.6 *Let w_0 be the longest element of the Weyl group of type D_n. Then the integer representation of w_0 is*

$$w_0 = (d_{n-1} : d_{n-2} : \cdots : d_2 : d_1)_{D_n} = (2n-1 : 2n-3 : \cdots : 7 : 5 : 3)_{D_n}.$$

Therefore, it is clear that the order of group D_n is

$$\mid D_n \mid = \prod_{i=1}^{n-1} (d_i + 1) = 2^{n-1} n!.$$

4. Inversion Statistic on the Group D_n

Many researchers have studied to define and discover an appropriate analogue of inversion number and major index for these kind of reflection groups, for example [1–3]. Now we define

$$\Psi_i = \{e_{n+1-i} \pm e_j \ : \ j < n+1-i \leq n\} \ \text{ and } \ inv_i(w) = \mid w(\Psi_i) \cap \Psi^- \mid$$

for each $i = 1, \cdots, n-1$. The sequence $I(w) = (inv_1(w) : \cdots : inv_{n-1}(w))$ is called the *inversion table* of an element $w \in D_n$. It must also be noticed that, in opposition to the integer representation, we will not use D_n as a subscript in order to denote the inversion table of w. Now let $inv(w)$ denote the sum of i-inversions of the permutation $w \in D_n$. It is obvious that $l(w) = inv(w)$. One can practically obtain the inversion table of $w \in D_n$ without using the root system structure with the help of the following theorem.

Theorem 4.1 *For $w = \beta \prod_{k=1}^{n} t_k^{r_k} \in D_n$, we have*

$$inv_i(w) = 2. \mid \{(j, n+1-i) : j < n+1-i \leq n, \ \beta_j < \beta_{n+1-i}, r_{n+1-i} = 1\} \mid + inv_i(\beta) \tag{4.1}$$

for all $i = 1, \cdots, n-1$, where $inv_i(\beta) = \mid \{(j, n+1-i) : j < n+1-i \leq n, \quad \beta_j > \beta_{n+1-i}\} \mid$ in S_n. More precisely, we write $inv_i(w) = inv_i(\beta)$ when $r_{n+1-i} = 0$. For all $i = 1, \cdots, n-1$, we get $inv_i(w) \in [0, 2(n-i)]$.

Proof Let $e_{n+1-i} \pm e_j \in \Psi_i$. We denote $e_{n+1-i} \pm e_j$ by $e_{n+1-i} - (-1)^k e_j$, where k is 0 or 1. Then we have $w(e_{n+1-i} \pm e_j) = (-1)^{r_{n+1-i}} e_{\beta_{n+1-i}} - (-1)^{k+r_j} e_{\beta_j}$, which lies in Ψ^- if and only if either $\beta_j < \beta_{n+1-i}$ and $r_{n+1-i} = 1$ (where k takes exactly one of the values 0 or 1) or $\beta_j > \beta_{n+1-i}$ and $k + r_j = 2$. Therefore, we get the desired formula as follows:

$$inv_i(w) = 2. \mid \{(j, n+1-i) : j < n+1-i \leq n, \ \beta_j < \beta_{n+1-i}, r_{n+1-i} = 1\} \mid + inv_i(\beta).$$

In particular, if r_{n+1-i} is equal to 0, then we clearly obtain $inv_i(w) = inv_i(\beta)$. This completes the proof. $\square$

Example 4.2 *Let* $w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 1 & -3 & 6 & 7 & -5 & 8 \end{pmatrix} \in D_8$. *Taking into account the equation (4.1) we obtain the inversion table of* w *as* $I(w) = (0 : 10 : 0 : 0 : 5 : 2 : 0)$, *and so we conclude that the length of* w *is* $l(w) = 17$. *At the same time, the reduced expression of* w *is* $s_2s_0s_1s_2s_4s_3s_2s_0s_1s_2s_3s_4s_1s_3s_2s_5s_6$ *with respect to the generating set* $S = \{s_0, s_1, \cdots, s_7\}$, *and also* $l(w) = 17$ *from another perspective.*

Let $\pi = [\pi_1, \cdots, \pi_{n-1}] \in D_{n-1}$. We want to observe how the insertion of n (resp. $-n$) into the permutation π affects the inversion statistic. There are clearly n places where we can put n (resp. $-n$) into the permutation $[\pi_1, \cdots, \pi_{n-1}]$. More precisely, for each $i = 1, \cdots, n-1$ there is one place immediately after π_i which is called space i and there is one more place immediately before π_1 which we call space 0. We denote by $\pi_{n,i}$ (resp. $\pi_{-n,i}$) the permutation in D_n obtained by inserting n (resp. $-n$) into the place i in π.

Lemma 4.3 *Suppose that* $\pi = [\pi_1, \cdots, \pi_{n-1}]$ *is a permutation in* D_{n-1}. *Then we have*

1. $inv\pi_{n,i} = n - i - 1 + inv\pi$
2. $inv\pi_{-n,i} = n + i - 1 + inv\pi.$

Proof Assume that the inversion table of w is $I(\pi) = (a_1 : a_2 : \cdots : a_{n-1-i} : a_{n-i} : a_{n-i+1} : \cdots : a_{n-2})$. If we insert n into the place i in π, then we conclude from the equation (4.1) that $I(\pi_{n,i}) = (a_1 + 1 : a_2 + 1 : \cdots : a_{n-1-i} + 1 : 0 : a_{n-i} : a_{n-i+1} : \cdots : a_{n-2})$. Thus we obtain $inv\pi_{n,i} = n - i - 1 + inv\pi$. If we put $-n$ into the place i in π, then we get by using the equation (4.1) that $I(\pi_{-n,i}) = (a_1 + 1 : a_2 + 1 : \cdots : a_{n-1-i} + 1 : 2i : a_{n-i} : a_{n-i+1} : \cdots : a_{n-2})$. Hence, we find that $inv\pi_{-n,i} = n + i - 1 + inv\pi$. □

Example 4.4 *We consider* $\pi = [2, 4, 1, -3, 6, 7, -5, 8] \in D_8$. *Then the inversion table of* π *is* $I(\pi) = (0 : 10 : 0 : 0 : 5 : 2 : 0)$ *and* $inv\pi = 17$. *If* $\pi_{9,3} = [2, 4, 1, 9, -3, 6, 7, -5, 8]$, *then* $Inv\pi_{9,3} = (1 : 11 : 1 : 1 : 6 : 0 : 2 : 0)$ *and* $inv\pi_{9,3} = 22$. *If* $\pi_{-9,3} = [2, 4, 1, -9, -3, 6, 7, -5, 8]$, *then* $Inv\pi_{-9,3} = (1 : 11 : 1 : 1 : 6 : 6 : 2 : 0)$ *and* $inv\pi_{-6,2} = 28$.

As a result of Lemma 4.3, we immediately obtain the next lemma.

Lemma 4.5 *Let* $\pi = [\pi_1, \cdots, \pi_{n-1}] \in D_{n-1}$. *Then we have*

1. $\sum_{i=0}^{n-1} q^{inv\pi_{n,i}} = [n]_q q^{inv\pi}$,
2. $\sum_{i=0}^{n-1} q^{inv\pi_{-n,i}} = q^{n-1}[n]_q q^{inv\pi}$.

We are now in a position to give the following theorem.

Theorem 4.6 *Let* $inv(w)$ *be the sum of* i*-inversions of* $w \in D_n$. *Then*

$$\sum_{w \in D_n} q^{inv(w)} = [2]_q[4]_q \cdots [2n-2]_q[n]_q$$

where q *is an indeterminate and* $[i]_q$ *stands for* $\frac{1-q^i}{1-q}$ *for any positive integer* i.

Proof For any $\pi \in D_{n-1}$, we can write from Lemma 4.3 and 4.5

$$\begin{aligned}\sum_{i=0}^{n-1}(q^{inv\pi_{n,i}}+q^{inv\pi_{-n,i}}) &= ([n]_q+q^{n-1}[n]_q)q^{inv\pi}\\ &= ([n-1]_q+q^{n-1}+q^{n-1}[n-1]_q+q^{2n-2})q^{inv\pi}\\ &= ([2n-2]_q+q^{n-1}+q^{2n-2})q^{inv\pi}.\end{aligned}$$

Since we have $(q^{n-1}+q^{2n-2})[n-1]_q=[2n-2]_qq^{n-1}$, then it is easy to prove by induction that

$$\sum_{wi\in D_n} q^{invw}=([2n-2]_q+q^{n-1}+q^{2n-2})\sum_{\pi\in D_{n-1}} q^{inv\pi}=[2]_q[4]_q\cdots[2n-2]_q[n]_q.$$

$\square$

Thus, according to Theorem 4.6, the following result holds.

Corollary 4.7 *The inversion statistic and dmaj index are equi-distributed on the even signed permutation group* D_n.

The inversion statistic that we defined is compatible with the length function on D_n, just as the inversion statistic in the symmetric group S_n is compatible with the length function on S_n.

Example 4.8 *In Table 1, one can respectively see all 1-inversions and 2-inversions, the lengths and dmaj indexes of the twenty-four elements of* D_3 *using the formula (4.1). In the following table, we will denote any permutation* w *in* D_3 *in one-line notation by* $w_1w_2w_3$.

Table 1. Inversion table of the group D_3.

w_1	w_2	w_3	$Inv(w)$	$l(w)$	$dmaj(w)$	w_1	w_2	w_3	$Inv(w)$	$l(w)$	$dmaj(w)$
1	2	3	(0:0)	0	0	-2	3	-1	(2:0)	2	3
2	1	3	(0:1)	1	1	-3	2	-1	(2:1)	3	4
-2	-1	3	(0:1)	1	1	3	-2	-1	(2:1)	3	2
-1	-2	3	(0:2)	2	2	2	-3	-1	(2:2)	4	3
1	3	2	(1:0)	1	2	-1	3	-2	(3:0)	3	3
3	1	2	(1:1)	2	1	-3	1	-2	(3:1)	4	5
-3	-1	2	(1:1)	2	2	3	-1	-2	(3:1)	4	4
-1	-3	2	(1:2)	3	3	1	-3	-2	(3:2)	5	4
2	3	1	(2:0)	2	2	-1	2	-3	(4:0)	4	4
3	2	1	(2:1)	3	3	-2	1	-3	(4:1)	5	5
-3	-2	1	(2:1)	3	3	2	-1	-3	(4:1)	5	5
-2	-3	1	(2:2)	4	4	1	-2	-3	(4:2)	6	6

One can see from the above table that inv and dmaj staistics are equi-distributed over D_3, that is, they have the same number of 0s, 1s, 2s, 3s, 4s, 5s and 6s. Therefore, the Poincaré polynomial for D_3 is in the following form:

$$\sum_{w\in D_3} q^{dmaj(w)}=\sum_{w\in D_3} q^{inv(w)}=\sum_{w\in D_3} q^{l(w)}=1+3q+5q^2+6q^3+5q^4+3q^5+q^6.$$

5. Cryptography on the Group D_n

In this section, we use cryptography as an application for the group of even-signed permutations. For this purpose, we propose a cryptosystem based on the difficulty of the generalized hidden discrete logarithm problem over the group D_n.

5.1. Description of the proposed cryptosystem

Assume that Alice and Bob want to communicate with each other over a public channel. Thus, the key selection, encryption, and decryption processes are figured out as follows:

Key Selection:

- Bob selects a large n for D_n.
- Generate $\sigma, \gamma \in D_n$.
- Select a random integers $1 \leq x, y \leq |D_n| - 1$ and compute $P_B = \gamma^y \sigma^x \gamma^{-y}$.
- Publish (σ, γ, P_B), and keep (x, y) as private keys.

Encryption:

Alice wants to send a message m to Bob, so she encrypts the message as follows:

- First, Alice translates m to $m' \in D_n$.
- Select a random integers $1 \leq r, s \leq |D_n| - 1$.
- Select an integer $t \leq |D_n| - 1$ and compute $\tau = \gamma^t$.
- Compute the elements $c_1 = \tau^s \sigma^r \tau^{-s}$ and $c_2 = m'(\tau^s P_B^r \tau^{-s})$ of D_n.
- Calculate a and b, which are respectively the corresponding positive integers to c_1 and c_2, by using integer representation.
- Send the pair (a, b) of positive integers to Bob.

Decryption: Bob decrypts the message as follows:

- Determine the elements c_1 and c_2 of the group, corresponding to a and b positive integers, respectively, with the help of integer representation.
- Compute $m' = c_2(\gamma^y c_1^x \gamma^{-y})^{-1}$.
- Covert m' to m by using integer representation.

The following python algorithm is used to convert any text message into its numerical value using ASCII code:

Algorithm 4:

```
print("Enter a string: ", end="")
text = input()
```

```
for char in text:
ASCII = ord(char)
print(ASCII, end=”,”)
```

5.2. A toy example of the proposed cryptosystem

Key Selection:

- **Bob's Private Key:** Bob chooses $x=2$ and $y=3$.
- **Bob's Public Key:**
  Bob generates $\sigma=[1,-11,-12,10,-6,7,-3,9,-5,-4,8,2]$, $\gamma=[4,3,8,12,-9,-7,-10,-11,1,5,-2,-6]\in D_{12}$ and computes $P_B=\gamma^y\sigma^x\gamma^{-y}=[1,-11,4,9,-2,6,7,-12,-10,8,3,5]$.

Encryption:

- Alice wants to send a message m=PLANET to Bob. So, she converts m into its numerical representation $807665786984=(19:16:14:3:4:2:8:0:4:2:0)_{D_{12}}$ by using Algorithm 1 and Algorithm 4. After that, she computes the subexceedant function depending on the equation (3.3) as $f=f(1);f(2);f(3);f(4);f(5);f(6);f(7);f(8);f(9);f(10);f(11);f(12)=1;1;2;3;1;5;2;3;2;8;9;10$. Since $\tau(x)=2$, hence $m'=[4,6,7,12,1,5,11,3,-2,8,9,-10]\in D_{12}$.
- Alice chooses $r=2,s=3,t=2$ and computes $\tau=\gamma^2=[12,8,-11,-6,-1,10,-5,2,4,-9,-3,7]$.
- Alice computes $c_1=\tau^3\sigma^2\tau^{-3}=[-5,8,11,6,-2,3,9,-1,-4,10,7,12]$ and $c_2=m'(\tau^3P_B^2\tau^{-3})$ $=[-1,8,-12,4,9,-3,5,10,-6,2,11,7]$.
- Alice determines the positive integers $a=923249764528$ and $b=527899955494$ corresponding to c_1 and c_2, respectively, and sends the pair (a,b) to Bob.

Decryption:

- Bob converts a and b to the elements c_1 and c_2 of D_{12}, respectively.
- Bob computes $m'=c_2(\gamma^y c_1^x\gamma^{-y})^{-1}$.
- Bob finds the subexceedant function

$$
\begin{aligned}
f&=f(1);f(2);f(3);f(4);f(5);f(6);f(7);f(8);f(9);f(10);f(11);f(12)\\
&=1;1;2;3;1;5;2;3;2;8;9;10.
\end{aligned}
$$

  Hence, the integer representation of m' is $807665786984=(19:16:14:3:4:2:8:0:4:2:0)_{D_{12}}$. After that, he uses the ASCII code to convert the integer representation of m' into the message m.

6. Conclusion

In this paper, a mixed-base number system over the group D_n has been defined. A one-to-one correspondence between the elements of D_n and positive integers in the set $\{1,\cdots,2^{n-1}n!\}$ has been established after constructing subexceedant functions. In other words, any positive integer can be represented uniquely as an element of D_n. In addition, we constructed an inversion statistic for D_n and showed that it is equally distributed with dmaj statistic on D_n. Furthermore, a public-key cryptosystem based on the group of even signed permutations has been proposed. The scheme has some important properties, such as its non-commutativity, flexibility in key selection, fast and easy implementation. A relatively large memory requirement is the only disadvantage of the cryptosystem.

References

[1] Adin RM, Brenti F, Roichman Y. Descent numbers and major indices for the hyperoctahedral group, Advances in Applied Mathematics 2001; 27: 210-224.

[2] Biagioli R. Major and descent statistics for the even-signed permutation group, Advances in Applied Mathematics 2003; 31(1): 163-179.

[3] Biagioli R. Signed Mahonian polynomials for classical Weyl groups, European Journal of Combinatorics 2006; 27: 207-217.

[4] Carlitz L. A combinatorial property of q-Eulerian numbers, The American Mathematical Monthly 1975; 82: 51-54.

[5] Doliskani JN, Malekian E, Zakerolhosseini A. A cryptosystem based on the symmetric group S_n. International Journal of Computer Science and Network Security 2008; 8(2): 226–234.

[6] Foata D. On the Netto inversion number of a sequence, Proceedings of the American Mathematical Society 1968; 19(1) 236-240.

[7] Humphreys JE. Reflection Groups and Coxeter Groups. Cambridge University Press, Volume 29, 1990.

[8] Laisant CA. Sur la numeration factorielle, application aux permutations. Bulletin de la Societe Mathematique de France 1888; 16: 176-183. https://doi.org/10.24033/bsmf.378

[9] Mantaci R, Rakotondrajao F. A permutations representation that knows what "Eulerian" means. Discrete Mathematics and Theoretical Computer Science 2001; 4 (2): 101-108. https://doi.org/10.46298/dmtcs.271

[10] MacMahon PA. Combinatory Analysis. Cambridge University Press, Volume 1, London, 1915.

[11] Moldovyan D. Non-commutative finite groups as primitive of public key cryptosystems. Quasigroups and Related Systems 2010; 18 (2): 165–176.

[12] Moldovyan D. Post-quantum public key-agreement scheme based on a new form of the hidden logarithm problem. Computer Science Journal of Moldova 2019; 79 (1): 56–72.

[13] Raharinirina IV. Use of signed permutations in cryptography. Journal of Advances in Mathematics and Computer Science 2020; 35 (1): 23–38. https://doi.org/10.9734/jamcs/2020/v35i130237

[14] Stanley R. Enumerative Combinatorics I. Cambridge University Press, Volume I, 2011.