The Statistic $\text{Pinv}$ For Number System*

Fanomezantsoa Patrick Rabarison†, Hery Randriamaro‡

Received 19 April 2019

Abstract

The number of inversions is a statistic on permutation groups measuring the degree to which the entries of a permutation are out of order. We provide a generalization of that statistic by introducing the statistic number of pseudoinversions on the colored permutation groups. The main motivation for studying that statistic is the possibility to use it to define a number system and a numeral system on the colored permutation groups. By means of the statistic number of $i$-pseudoinversions, we construct our number system, and a bijection between the set of positive integers and the colored permutation groups.

1 Introduction

A statistic over a group is a function from that group to the set of nonnegative integers. One of the most studied statistics is the number of inversions, defined by $\text{inv} := \# \{ (i, j) \in [n]^2 \mid i < j, \sigma(i) > \sigma(j) \}$, on the symmetric group $\mathfrak{S}_n$ over $[n]$. A well-known result is the equidistribution of $\text{inv}$ with the statistic major index proved by Foata [3]. Besides, the Lehmer code is based on that statistic. It is a particular way to encode each permutation of $n$ numbers, and an instance of a scheme for numbering permutations. Remark that Vajnovszki provided several permutation codes directly related to the Lehmer code [5]. In this article, we give a generalization of the statistic $\text{inv}$ on the colored permutation group in order to create a more general code. The colored permutation group of $m$ colors and $n$ elements is the wreath product $U_m \wr \mathfrak{S}_n$ of the group $U_m$ of all $m^{th}$ roots of unity by the symmetric group $\mathfrak{S}_n$ on $[n]$. We represent a colored permutation $\pi \in U_m \wr \mathfrak{S}_n$ by

$$
\pi = \left( \begin{array}{cccc}
1 & \zeta_{k_1} \sigma(1) & \cdots & \zeta_{k_n} \sigma(n) \\
2 & \zeta_{k_2} \sigma(2) & \cdots & \zeta_{k_n} \sigma(n) \\
\vdots & \vdots & \ddots & \vdots \\
\end{array} \right) \text{ with } \sigma \in \mathfrak{S}_n \text{ and } \zeta_j = e^{2\pi i j/m}.
$$

For $i, j \in \mathbb{Z}$ such that $i < j$, let $[i, j] := \{i, i+1, \ldots, j\}$.

Definition 1 The number of $i$-pseudoinversions of $\pi \in U_m \wr \mathfrak{S}_n$ is

$$
\text{pinv}_i \pi := k_i (n - i + 1) + | \{ j \in [i+1, n] \mid \sigma(i) > \sigma(j) \} |.
$$

And the number of pseudoinversions of $\pi \in U_m \wr \mathfrak{S}_n$ is

$$
\text{pinv}_i \pi := \sum_{i=1}^{n} \text{pinv}_i \pi.
$$

Example 1 Consider the element $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & \zeta_4 & \zeta_4 & 3 \end{pmatrix} \in U_5 \wr \mathfrak{S}_4$. We have $\text{pinv}_1 \pi = 1$, $\text{pinv}_2 \pi = 3$, $\text{pinv}_3 \pi = 9$, $\text{pinv}_4 \pi = 0$, and $\text{pinv} \pi = 13$.

The interest for investigating statistics on $U_m \wr \mathfrak{S}_n$ recently arose. Bagno et al., for example, introduced the statistics $(c, d)$-descents and computed their distributions [1, Proposition 1.1.]. We construct a number system by means of the cardinality $|U_m \wr \mathfrak{S}_n|$, and the statistic $\text{pinv}_i$.

*Mathematics Subject Classification: 05A19.
†Département de Mathématiques et Informatique, Université d’Antananarivo, 101 Antananarivo, Madagascar
‡Département de Mathématiques et Informatique, Université d’Antananarivo, 101 Antananarivo, Madagascar
Definition 2 Let \( A = (A_i)_{i \in \mathbb{N}} \), \( a = (a_i)_{i \in \mathbb{N}} \) be two sequences of positive integers. The pair \((A, a)\) is a number system if, for every integer \( n \in \mathbb{N} \), there exists \( k \in \mathbb{N} \) such that \( n = \sum_{i=0}^{k} \alpha_i A_i \) with \( \alpha_i \in [0, a_i] \), and this representation in terms of \( A_i \)’s and \( a_i \)’s is unique.

Using formal power series, Cantor provided a condition for a pair of positive integer sequences to be a number system [2, §2.]. We provide a more suitable condition for this work.

Proposition 1 Let \( A = (A_i)_{i \in \mathbb{N}} \) and \( a = (a_i)_{i \in \mathbb{N}} \) be two sequences of strictly positive integers. The pair of sequences \((A, a)\) is a number system if and only if

\[
A_0 = 1 \quad \text{and} \quad A_k = \prod_{i=0}^{k-1} (1 + a_i) \quad \text{for each} \quad k \in \mathbb{N}^*.
\]

We prove Proposition 1 in Section 2.

Corollary 1 Let \( m \in \mathbb{N}^* \). The pair of sequences \((G, g) = ((G_i)_{i \in \mathbb{N}}, (g_i)_{i \in \mathbb{N}})\) defined by

\[
G_i = m^i! \quad \text{and} \quad g_i = m(i+1) - 1
\]

is a number system.

Proof. We obtain the equality in Proposition 1 for number system from

\[
\prod_{i=0}^{k-1} (1 + g_i) = \prod_{i=0}^{k-1} m(i+1) = m^k k! = G_k.
\]

We particularly use the number system \((G, g)\) in this article. The number \( G_i \) is the cardinality of \( U_m \natural \mathfrak{S}_i \), and \( g_i \) is the maximal value of \( \text{pinv}_i \) relating to \( U_m \natural \mathfrak{S}_{i+1} \). The factorial number system introduced by Laisant [4] corresponds to the case \( m = 1 \) of \((G, g)\). We also construct a numeral system by means of the groups \( U_m \natural \mathfrak{S}_n \) and the statistic \( \text{pinv}_i \).

Definition 3 A numeral system is a notation for representing integers.

There exist several types of numeral systems depending on the historical context and the geographical location. We develop a numeral system based on the colored permutation groups. Write \( \gamma_k \cdot \gamma_{k-1} \cdots \cdot \gamma_1 \cdot \gamma_0 \) for the integer \( \sum_{i=0}^{k} \gamma_i G_i \), and \( \langle G, g \rangle_k \) for the integer set

\[
\langle G, g \rangle_k := \{ \gamma_k \cdot \gamma_{k-1} \cdots \cdot \gamma_1 \cdot \gamma_0 \mid \gamma_i \in [0, g_i] \}.
\]

Our numeral system stems from the following bijection.

Theorem 1 Let \( n \geq 1 \). The following map is bijective

\[
g : U_m \natural \mathfrak{S}_n \rightarrow \langle G, g \rangle_{n-1} \quad \pi \mapsto \text{pinv}_1(\pi), \text{pinv}_2(\pi), \ldots, \text{pinv}_n(\pi).
\]

We prove Theorem 1 in Section 3. The Lehmer code is built from the case \( m = 1 \).

Example 2 From Example 1, we have \( \pi = \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 3 \end{array} \right) = 1.3.9.0 \) which, is equal to 945 in decimal system.
Furthermore, we obtain the generating function of the statistic number of pseudoinversions. Denote the $q$-analog of the number $i$ by $[i]_q := 1 + q + \cdots + q^{i-1}$.

**Corollary 2** The generating function of the statistic $\text{pinv}$ on $U_m \setminus S_n$ is

$$
\sum_{\pi \in U_m \setminus S_n} q^\text{pinv}_\pi = \prod_{i=1}^n [mi]_q.
$$

**Proof.** The bijection of Theorem 1 implies that every element of $U_m \setminus S_n$ has a unique representation in $\langle G, g \rangle_{n-1}$. Then, we have

$$
\sum_{\pi \in U_m \setminus S_n} q^\text{pinv}_\pi = [\max \text{pinv}_n + 1]_q \cdots [\max \text{pinv}_2 + 1]_q [\max \text{pinv}_1 + 1]_q = \prod_{i=1}^n [mi]_q.
$$

\[ \blacksquare \]

**2 Proof of Proposition 1**

We provide a condition for a pair of integer sequences $(A, a)$ to be a number system.

**Lemma 1** Take a number system $(A, a)$, and let $n = \alpha_k \cdot \cdots \cdot \alpha_1 \cdot \alpha_0$ be a nonnegative integer. Then,

$$
\alpha_k A_k \leq n < (\alpha_k + 1)A_k.
$$

**Proof.** It is clear that $\alpha_k A_k \leq n$. Suppose that $n \geq (\alpha_k + 1)A_k$ which means $\sum_{i=0}^{k-1} \alpha_i A_i \geq A_k$. Then, there exist $\lambda_i$'s, $i \in [0, k-1]$, such that $0 \leq \lambda_i \leq \alpha_i$ and $\lambda_{k-1} \cdots \lambda_1 \cdot \lambda_0 = 1.0 \cdots 0.0$. That contradicts the uniqueness of the representation. \[ \blacksquare \]

**Lemma 2** Let $A = (A_i)_{i \in \mathbb{N}}$, $a = (a_i)_{i \in \mathbb{N}}$ be two sequences of positive integers. Then, the pair $(A, a)$ is a number system if and only if

$$
A_0 = 1 \quad \text{and} \quad A_k = \sum_{i=0}^{k-1} a_i A_i + 1 \quad \text{for each} \quad k \in \mathbb{N}^*.
$$

**Proof.** Suppose that $(A, a)$ is a number system. It is obvious that we must have $A_0 = 1$. Let $n = a_k \cdot \cdots \cdot a_1 \cdot a_0$. From the second inequality of Lemma 1, we get $\sum_{i=0}^{k} a_i A_i = n < (a_k + 1)A_k$. Then,

$$
\sum_{i=0}^{k} a_i A_i + 1 \leq (a_k + 1)A_k \quad \text{i.e.} \quad \sum_{i=0}^{k-1} a_i A_i + 1 \leq A_k.
$$

As $\sum_{i=0}^{k} a_i A_i + 1 \notin (A, a)_{k-1}$, the only possibility is $\sum_{i=0}^{k-1} a_i A_i + 1 = A_k$.

Now, suppose that $A_0 = 1$ and $A_k = \sum_{i=0}^{k-1} a_i A_i + 1$ for each $k \in \mathbb{N}^*$. Let $n \in \mathbb{N}^*$, and assume that every integer $m \leq n - 1$ has a unique representation $\alpha_k \cdot \alpha_{k-1} \cdot \cdots \cdot \alpha_1 \cdot \alpha_0$ with $\alpha_i \in [0, a_i]$. If $n - 1 = \sum_{i=0}^{k} A_i$, then
let \( j = \max \{ l \in [0, k] \mid \forall i \in [0, l] : \alpha_i = a_i \} \). Then,
\[
n = A_{j+1} + \sum_{i=j+1}^{k} \alpha_i A_i.
\]

About the uniqueness, suppose that \( n \) has two different representations \( \sum_{i=0}^{k} \alpha_i A_i \) and \( \sum_{i=0}^{k'} \alpha_i' A_i' \):

- If \( k' > k \), then \( \sum_{i=0}^{k'} \alpha_i' A_i' \geq (\alpha_{k'}') - 1)A_{k'} + \sum_{i=0}^{k'-1} a_i A_i + 1 > \sum_{i=0}^{k} \alpha_i A_i. \)

- Otherwise, let \( l = \max \{ i \in [0, k] \mid \alpha_i \neq \alpha_i' \} \), and assume that \( \alpha_i' > \alpha_i \). We have
\[
\sum_{i=0}^{l-1} \alpha_i' A_i + \alpha_i' A_i + \sum_{i=l+1}^{k} \alpha_i A_i
\]
\[
\geq \sum_{i=l+1}^{k} \alpha_i A_i + \alpha_i' A_i
\]
\[
= \sum_{i=l+1}^{k} \alpha_i A_i + (\alpha_i' - 1)A_l + \sum_{i=0}^{l-1} a_i A_i + 1
\]
\[
> \sum_{i=0}^{l} \alpha_i A_i.
\]

As that result is absurd, it is therefore impossible to have two different representations of \( n \). ■

We can now proceed to the proof of Proposition 1: From Lemma 2, we deduce that \((A, a)\) is a number system if and only if \( A_0 = 1 \) and
\[
A_k = \sum_{i=0}^{k-1} a_i A_i + 1 = a_{k-1} A_{k-1} + \sum_{i=0}^{k-2} a_i A_i + 1 = a_{k-1} A_{k-1} + A_{k-1}
\]
\[
= (a_{k-1} + 1) A_{k-1} = (a_{k-1} + 1)(a_{k-2} + 1) \cdots (a_0 + 1) = \prod_{i=0}^{k-1} (1 + a_i).
\]

### 3 Proof of Theorem 1

We finally prove that there is a one-to-one correspondence between the permutations
\[
\pi = \left( \begin{array}{cccc}
1 & 2 & \cdots & n \\
\zeta_{k_1} \sigma(1) & \zeta_{k_2} \sigma(2) & \cdots & \zeta_{k_n} \sigma(n) \\
\end{array} \right)
\]
and the numbers \( \gamma_{n-1} \cdot \gamma_{n-2} \cdots \cdot \gamma_1 \cdot \gamma_0 \) by means of \( \text{pinv}_1(\pi) \cdot \text{pinv}_2(\pi) \cdots \cdot \text{pinv}_n(\pi) = \gamma_{n-1} \cdot \gamma_{n-2} \cdots \cdot \gamma_1 \cdot \gamma_0. \)

Consider the function \( g : \mathbb{U}_m \times \mathcal{G}_n \rightarrow \mathbb{N} \) defined by \( g(\pi) := \text{pinv}_1(\pi) \cdot \text{pinv}_2(\pi) \cdots \cdot \text{pinv}_n(\pi) \). Since \( \min g = \min(G, g)_{n-1} = 0 \) and \( \max g = \max(G, g)_{n-1} = G_{n-1} \), then \( g(\mathbb{U}_m \times \mathcal{G}_n) \subseteq (G, g)_{n-1} \). The surjectivity proof remains.

Consider the number \( \gamma_{n-1} \cdot \gamma_{n-2} \cdots \cdot \gamma_1 \cdot \gamma_0 \in (G, g)_{n-1} \). For \( i \in [0, n-1] \), let

- \( h_i \) be the integer in \([0, m-1]\) such that \( \gamma_i \in [h_i(i+1), h_i(i+1) + i] \).
• \(s_{n-i}\) be the integer \(\gamma_i - h_i(i + 1) \in [0, i]\).

We form a permutation \(\tau \in \mathfrak{S}_n\) such that, for \(i \in [n]\), \(s_i = |\{j \in [i+1, n] \mid \tau(i) > \tau(j)\}|.

Example 3 We compute the colored permutation in \(U_4 \iota \mathfrak{S}_5\) corresponding to the number \(7.11.0.5.2 \in (G, g)_4\) for \(G_i = 4!\) and \(g_1 = 4i + 3\).

With slight calculations, we obtain \(h_0 = 2, h_1 = 2, h_2 = 0, h_3 = 2,\) and \(h_4 = 1\).

Then, \(s_5 = 0, s_4 = 1, s_3 = 0, s_2 = 3,\) and \(s_1 = 2\).

For \(x_5\), we get \(x_1 > x_2 > x_3 > x_4 > \tau(5)\).

For \(x_4\), we get \(x_1 > x_2 > x_3 > \tau(4) > \tau(5)\).

For \(x_3\), we get \(x_1 > x_2 > \tau(4) > \tau(5) > \tau(3)\).

For \(x_2\), we get \(x_1 > \tau(2) > \tau(4) > \tau(5) > \tau(3)\).

For \(x_1\), we get \(\tau(2) > \tau(4) > \tau(1) > \tau(5) > \tau(3)\).

Hence, \(\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}\), and the aimed colored permutation is \(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \zeta_{13} & \zeta_{25} & \zeta_01 & \zeta_4 & \zeta_{22} \end{pmatrix}\).

4 A Simple Example of Application

Here is an example of cryptosystem based on Theorem 1. Suppose that we want to encrypt a message of \(c\) characters using an alphabet of \(l\) symbols. Consider the colored permutation group \(U_l \iota \mathfrak{S}_c\) and its corresponding number system \((G, g)_{c-1}\). The message can be considered as the element \(x = \gamma_{c-1} \cdots \gamma_1 \cdots \gamma_0\) of \((G, g)_{c-1}\), where \(\gamma_{c-i}\) is the symbol order of the \(i\)th character. Choose a key \(\kappa \in U_l \iota \mathfrak{S}_c\). Define the encrypting function \(\varepsilon : (G, g)_{c-1} \rightarrow (G, g)_{c-1}\) by the function composition

\[
\varepsilon : (G, g)_{c-1} \rightarrow U_l \iota \mathfrak{S}_c \rightarrow U_l \iota \mathfrak{S}_c \rightarrow (G, g)_{c-1}
\]

The encrypted message is \(y = \varepsilon(x)\). The decrypting function \(\delta : (G, g)_{c-1} \rightarrow (G, g)_{c-1}\) is defined by

\[
\delta : (G, g)_{c-1} \rightarrow U_l \iota \mathfrak{S}_c \rightarrow U_l \iota \mathfrak{S}_c \rightarrow (G, g)_{c-1}
\]

Example 4 We use the 26 letters of the English alphabet \(E\) as symbols. The message is written with the number system \((G, g)\) as follows: a word \(w_0w_{n-1} \ldots w_1\) written with \(E\) is represented by \(\gamma_{n-1} \cdots \gamma_{n-2} \cdots \gamma_0\) where, if \(w_i\) is the \(i\)th letter of the alphabet, then \(\gamma_{i-1} = j - 1\). The message “pinv” is represented by \(15, 8, 13, 21\) corresponding to \(\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_5 & \zeta_4 & \zeta_6 & \zeta_3 \end{pmatrix}\). Let us agree that, if the message is composed by \(n\) letters, then the key is the first \(n\) letters of a secret text. In our case, if that text is the abstract of this article, then the key is “then”. Its representation is \(19, 7, 4, 13\) corresponding to \(\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_{14} & \zeta_{21} & \zeta_{22} & \zeta_{19} \end{pmatrix}\).

Hence, the encrypted message is \(\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_{25} & \zeta_{3} & \zeta_4 & \zeta_{19} \end{pmatrix}\) corresponding to \(100, 13, 11, 19\).

Acknowledgment. The authors are thankful to the International Centre for Theoretical Physics for having hosted them at the beginning of their research.

References


