Applied Mathematics E-Notes, 20(2020), 230-235 © ISSN 1607-2510
Available free at mirror sites of http://www.math.nthu.edu.tw/∼amen/

The Statistic `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 $\mathtt{inv}\,\sigma := \#\big\{(i,j) \in [n]^2 \mid i < j, \sigma(i) > \sigma(j)\big\}$, on the symmetric group $\mathfrak{S}_n$ over $[n]$. A well-known result is the equidistribution of `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 `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 $\mathbb{U}_m \wr \mathfrak{S}_n$ of the group $\mathbb{U}_m$ of all m^{th} roots of unity by the symmetric group $\mathfrak{S}_n$ on $[n]$. We represent a colored permutation $\pi \in \mathbb{U}_m \wr \mathfrak{S}_n$ by

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \zeta_{k_1}\sigma(1) & \zeta_{k_2}\sigma(2) & \dots & \zeta_{k_n}\sigma(n) \end{pmatrix} \text{ with } \sigma \in \mathfrak{S}_n \text{ and } \zeta_{k_j} = e^{2\pi i \frac{k_j}{m}}.$$

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

Definition 1 *The* number of i-pseudoinversions *of* $\pi \in \mathbb{U}_m \wr \mathfrak{S}_n$ *is*

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

And the number of pseudoinversions *of* $\pi \in \mathbb{U}_m \wr \mathfrak{S}_n$ *is*

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

Example 1 *Consider the element* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & \zeta_1 1 & \zeta_4 4 & 3 \end{pmatrix} \in \mathbb{U}_5 \wr \mathfrak{S}_4$. *We have* $\mathtt{pinv}_1\,\pi = 1$, $\mathtt{pinv}_2\,\pi = 3$, $\mathtt{pinv}_3\,\pi = 9$, $\mathtt{pinv}_4\,\pi = 0$, *and* $\mathtt{pinv}\,\pi = 13$.

The interest for investigating statistics on $\mathbb{U}_m \wr \mathfrak{S}_n$ recently arised. 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 $|\mathbb{U}_m \wr \mathfrak{S}_n|$, and the statistic $\mathtt{pinv}_i$.

*Mathematics Subject Classifications: 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* $\mathsf{A} = (\mathsf{A}_i)_{i\in\mathbb{N}}$, $\mathsf{a} = (\mathsf{a}_i)_{i\in\mathbb{N}}$ *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* $n = \sum_{i=0}^{k} \alpha_i \mathsf{A}_i$ *with* $\alpha_i \in [0, \mathsf{a}_i]$, *and this representation in terms of* A_i*'s and* α_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* $\mathsf{A} = (\mathsf{A}_i)_{i\in\mathbb{N}}$ *and* $\mathsf{a} = (\mathsf{a}_i)_{i\in\mathbb{N}}$ *be two sequences of strictly positive integers. The pair of sequences* (A, a) *is a number system if and only if*

$$\mathsf{A}_0 = 1 \quad \textit{and} \quad \mathsf{A}_k = \prod_{i=0}^{k-1}(1 + \mathsf{a}_i) \textit{ for each } k \in \mathbb{N}^*.$$

We prove Proposition 1 in Section 2.

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

$$\mathsf{G}_i = m^i i! \quad \textit{and} \quad \mathsf{g}_i = m(i+1) - 1$$

is a number system.

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

$$\prod_{i=0}^{k-1}(1 + \mathsf{g}_i) = \prod_{i=0}^{k-1} m(i+1) = m^k k! = \mathsf{G}_k.$$

■

We particularly use the number system (G, g) in this article. The number G_i is the cardinality of $\mathbb{U}_m \wr \mathfrak{S}_i$, and g_i is the maximal value of $\mathtt{pinv}_1$ relating to $\mathbb{U}_m \wr \mathfrak{S}_{i+1}$. 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 $\mathbb{U}_m \wr \mathfrak{S}_n$ and the statistic $\mathtt{pinv}_i$.

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 $\gamma_k \centerdot \gamma_{k-1} \centerdot \cdots \centerdot \gamma_1 \centerdot \gamma_0$ for the integer $\sum_{i=0}^{k} \gamma_i \mathsf{G}_i$, and $\langle \mathsf{G}, \mathsf{g}\rangle_k$ for the integer set

$$\langle \mathsf{G}, \mathsf{g}\rangle_k := \big\{\gamma_k \centerdot \gamma_{k-1} \centerdot \cdots \centerdot \gamma_1 \centerdot \gamma_0 \;\big|\; \gamma_i \in [0,\, \mathsf{g}_i]\big\}.$$

Our numeral system stems from the following bijection.

Theorem 1 *Let* $n \geq 1$. *The following map is bijective*

$$g : \begin{array}{ccc} \mathbb{U}_m \wr \mathfrak{S}_n & \to & \langle \mathsf{G}, \mathsf{g}\rangle_{n-1} \\ \pi & \mapsto & \mathtt{pinv}_1(\pi) \centerdot \mathtt{pinv}_2(\pi) \centerdot \cdots \centerdot \mathtt{pinv}_n(\pi) \end{array}.$$

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

Example 2 *From Example 1, we have* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & \zeta_1 1 & \zeta_4 4 & 3 \end{pmatrix} = 1 \centerdot 3 \centerdot 9 \centerdot 0$ *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* pinv *on* $\mathbb{U}_m \wr \mathfrak{S}_n$ *is*

$$\sum_{\pi \in \mathbb{U}_m \wr \mathfrak{S}_n} q^{\mathtt{pinv}\,\pi} = \prod_{i=1}^{n} [mi]_q.$$

Proof. The bijection of Theorem 1 implies that every element of $\mathbb{U}_m \wr \mathfrak{S}_n$ has a unique representation in $\langle \mathsf{G}, \mathsf{g} \rangle_{n-1}$. Then, we have

$$\sum_{\pi \in \mathbb{U}_m \wr \mathfrak{S}_n} q^{\mathtt{pinv}\,\pi} = [\max \mathtt{pinv}_n + 1]_q \ldots [\max \mathtt{pinv}_2 + 1]_q \, [\max \mathtt{pinv}_1 + 1]_q = \prod_{i=1}^{n} [mi]_q.$$

■

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* $n = \alpha_k \centerdot \cdots \centerdot \alpha_1 \centerdot \alpha_0$ *be a nonnegative integer. Then,*

$$\alpha_k \mathsf{A}_k \leq n < (\alpha_k + 1)\mathsf{A}_k.$$

Proof. It is clear that $\alpha_k \mathsf{A}_k \leq n$. Suppose that $n \geq (\alpha_k + 1)\mathsf{A}_k$ which means $\sum_{i=0}^{k-1} \alpha_i \, \mathsf{A}_i \geq \mathsf{A}_k$. Then, there exist λ_i's, $i \in [0, k-1]$, such that $0 \leq \lambda_i \leq \alpha_i$ and $\lambda_{k-1} \centerdot \cdots \centerdot \lambda_1 \centerdot \lambda_0 = 1 \centerdot \overbrace{0 \centerdot \cdots \centerdot 0}^{k \text{ times}} \centerdot 0$. That contradicts the uniqueness of the representation. ■

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

$$\mathsf{A}_0 = 1 \quad \textit{and} \quad \mathsf{A}_k = \sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1 \textit{ for each } k \in \mathbb{N}^*.$$

Proof. Suppose that (A, a) is a number system. It is obvious that we must have $\mathsf{A}_0 = 1$. Let $n = \mathsf{a}_k \centerdot \cdots \centerdot \mathsf{a}_1 \centerdot \mathsf{a}_0$. From the second inequality of Lemma 1, we get $\sum_{i=0}^{k} \mathsf{a}_i \mathsf{A}_i = n < (\mathsf{a}_k + 1)\mathsf{A}_k$. Then,

$$\sum_{i=0}^{k} \mathsf{a}_i \mathsf{A}_i + 1 \leq (\mathsf{a}_k + 1)\mathsf{A}_k \quad \text{i.e.} \quad \sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1 \leq \mathsf{A}_k.$$

As $\sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1 \notin \langle \mathsf{A}, \mathsf{a} \rangle_{k-1}$, the only possibility is $\sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1 = \mathsf{A}_k$.

Now, suppose that $\mathsf{A}_0 = 1$ and $\mathsf{A}_k = \sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1$ for each $k \in \mathbb{N}^*$. Let $n \in \mathbb{N}^*$, and assume that every integer $m \leq n - 1$ has a unique representation $\alpha_k \centerdot \alpha_{k-1} \centerdot \cdots \centerdot \alpha_1 \centerdot \alpha_0$ with $\alpha_i \in [0, \mathsf{a}_i]$. If $n - 1 = \sum_{i=0}^{k} \alpha_i \mathsf{A}_i$,

let $j = \max\left\{l \in [0,k] \;\middle|\; \forall i \in [0,l] : \alpha_i = \mathsf{a}_i\right\}$. Then,

$$n = \mathsf{A}_{j+1} + \sum_{i=j+1}^{k} \alpha_i \mathsf{A}_i.$$

About the uniqueness, suppose that n has two different representations $\sum_{i=0}^{k} \alpha_i \mathsf{A}_i$ and $\sum_{i=0}^{k'} \alpha'_i \mathsf{A}_i$:

- If $k' > k$, then $\sum_{i=0}^{k'} \alpha'_i \mathsf{A}_i \geq \alpha'_{k'} \mathsf{A}_{k'} = (\alpha'_{k'} - 1)\mathsf{A}_{k'} + \sum_{i=0}^{k'-1} \mathsf{a}_i \mathsf{A}_i + 1 > \sum_{i=0}^{k} \alpha_i \mathsf{A}_i$.
- Otherwise, let $l = \max\left\{i \in [0,k] \;\middle|\; \alpha_i \neq \alpha'_i\right\}$, and assume that $\alpha'_l > \alpha_l$. We have

$$\begin{aligned}
\sum_{i=0}^{k} \alpha'_i \mathsf{A}_i &= \sum_{i=0}^{l-1} \alpha'_i \mathsf{A}_i + \alpha'_l \mathsf{A}_l + \sum_{i=l+1}^{k} \alpha'_i \mathsf{A}_i \\
&\geq \sum_{i=l+1}^{k} \alpha'_i \mathsf{A}_i + \alpha'_l \mathsf{A}_l \\
&= \sum_{i=l+1}^{k} \alpha_i \mathsf{A}_i + (\alpha'_l - 1)\mathsf{A}_l + \sum_{i=0}^{l-1} \mathsf{a}_i \mathsf{A}_i + 1 \\
&> \sum_{i=0}^{k} \alpha_i \mathsf{A}_i.
\end{aligned}$$

As that result is absurd, it is therefore impossible to have two different represention 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 $\mathsf{A}_0 = 1$ and

$$\begin{aligned}
\mathsf{A}_k =& \sum_{i=0}^{k-1} \mathsf{a}_i \mathsf{A}_i + 1 = \mathsf{a}_{k-1}\mathsf{A}_{k-1} + \sum_{i=0}^{k-2} \mathsf{a}_i \mathsf{A}_i + 1 = \mathsf{a}_{k-1}\mathsf{A}_{k-1} + \mathsf{A}_{k-1} \\
=& (\mathsf{a}_{k-1} + 1)\mathsf{A}_{k-1} = (\mathsf{a}_{k-1} + 1)(\mathsf{a}_{k-2} + 1)\ldots(\mathsf{a}_0 + 1) = \prod_{i=0}^{k-1} (1 + \mathsf{a}_i).
\end{aligned}$$

3 Proof of Theorem 1

We finally prove that there is a one-to-one correspondence betweenthe permutations

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \zeta_{k_1}\sigma(1) & \zeta_{k_2}\sigma(2) & \ldots & \zeta_{k_n}\sigma(n) \end{pmatrix}$$

and the numbers $\gamma_{n-1}.\gamma_{n-2}.\cdots.\gamma_1.\gamma_0$ by means of $\mathtt{pinv}_1(\pi).\mathtt{pinv}_2(\pi).\cdots.\mathtt{pinv}_n(\pi) = \gamma_{n-1}.\gamma_{n-2}.\cdots.\gamma_1.\gamma_0$.

Consider the function $g : \mathbb{U}_m \wr \mathfrak{S}_n \to \mathbb{N}$ defined by $g(\pi) := \mathtt{pinv}_1(\pi) \,.\, \mathtt{pinv}_2(\pi) \,.\, \cdots \,.\, \mathtt{pinv}_n(\pi)$. Since $\min g = \min\langle \mathsf{G}, \mathsf{g}\rangle_{n-1} = 0$ and $\max g = \max\langle \mathsf{G}, \mathsf{g}\rangle_{n-1} = \mathsf{G}_n - 1$, then $g(\mathbb{U}_m \wr \mathfrak{S}_n) \subseteq \langle \mathsf{G}, \mathsf{g}\rangle_{n-1}$. The surjectivity proof remains.

Consider the number $\gamma_{n-1} \,.\, \gamma_{n-2} \,.\, \cdots \,.\, \gamma_1 \,.\, \gamma_0 \in \langle \mathsf{G}, \mathsf{g}\rangle_{n-1}$. For $i \in [0, n-1]$, let

- h_i be the integer in $[0, m-1]$ such that $\gamma_i \in \left[h_i(i+1), h_i(i+1) + i\right]$,

- 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 $i \in [n]$, $s_i = \big|\big\{j \in [i+1, n] \;\big|\; \tau(i) > \tau(j)\big\}\big|$.

Example 3 *We compute the colored permutation in* $\mathbb{U}_4 \wr \mathfrak{S}_5$ *corresponding to the number* $7.11.0.5.2 \in \langle \mathsf{G}, \mathsf{g}\rangle_4$ *for* $\mathsf{G}_i = 4^i i!$ *and* $\mathsf{g}_i = 4i + 3$.

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* $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \zeta_1 3 & \zeta_2 5 & \zeta_0 1 & \zeta_1 4 & \zeta_2 2 \end{pmatrix}$.

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 $\mathbb{U}_l \wr \mathfrak{S}_c$ and its corresponding number system $\langle \mathsf{G}, \mathsf{g}\rangle_{c-1}$. The message can be considered as the element $x = \gamma_{c-1}.\cdots.\gamma_1.\gamma_0$ of $\langle \mathsf{G}, \mathsf{g}\rangle_{c-1}$, where γ_{c-i} is the symbol order of the i^{th} character. Choose a key $\kappa \in \mathbb{U}_l \wr \mathfrak{S}_c$. Define the encrypting function $\mathfrak{e} : \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} \to \langle \mathsf{G}, \mathsf{g}\rangle_{c-1}$ by the function composition

$$\mathfrak{e} : \begin{array}{ccccccc} \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} & \to & \mathbb{U}_l \wr \mathfrak{S}_c & \to & \mathbb{U}_l \wr \mathfrak{S}_c & \to & \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} \\ x & \mapsto & g^{-1}(x) & \mapsto & g^{-1}(x) \circ \kappa & \mapsto & g\big(g^{-1}(x) \circ \kappa\big) \end{array} .$$

The encrypted message is $y = \mathfrak{e}(x)$. The decrypting function $\mathfrak{d} : \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} \to \langle \mathsf{G}, \mathsf{g}\rangle_{c-1}$ is defined by

$$\mathfrak{d} : \begin{array}{ccccccc} \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} & \to & \mathbb{U}_l \wr \mathfrak{S}_c & \to & \mathbb{U}_l \wr \mathfrak{S}_c & \to & \langle \mathsf{G}, \mathsf{g}\rangle_{c-1} \\ y & \mapsto & g^{-1}(y) & \mapsto & g^{-1}(y) \circ \kappa^{-1} & \mapsto & g\big(g^{-1}(y) \circ \kappa^{-1}\big) \end{array} .$$

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* $w_n w_{n-1} \dots w_1$ *written with E is represented by* $\gamma_{n-1}.\gamma_{n-2}.\cdots.\gamma_0$ *where, if* w_i *is the* j^{th} *letter of the alphabet, then* $\gamma_{i-1} = j - 1$. *The message "pinv" is represented by* $15.8.13.21$ *corresponding to* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_3 4 & \zeta_2 3 & \zeta_6 2 & \zeta_{21} 1 \end{pmatrix}$. *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* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_4 4 & \zeta_2 2 & \zeta_2 1 & \zeta_{13} 3 \end{pmatrix}$.

Hence, the encrypted message is $\begin{pmatrix} 1 & 2 & 3 & 4 \\ \zeta_{25} 1 & \zeta_4 3 & \zeta_5 4 & \zeta_{19} 2 \end{pmatrix}$ *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

[1] E. Bagno, D. Garber and T. Mansour, Counting descent pairs with prescribed colors in the colored permutation groups, Sém. Lothar. Combin., 60(2009), Art. B60e, 12 pp.

[2] G. Cantor, Ueber die einfachen zahlensysteme, Z. Math. Phys., 14(1869), 121–128.

[3] D. Foata, On the netto inversion number of a sequence, Proc. Amer. Math. Soc., 19(1968), 236–240.

[4] C.-A. Laisant, Sur la numération factorielle, Application aux Permutations, Bull. Soc. Math. France, 16(1888), 176–183.

[5] V. Vajnovszki, Lehmer code transforms and mahonian statistics on permutations, Discrete Math., 313(2013), 581–589.