Journal of Integer Sequences, Vol. 14 (2011),
Article 11.3.2

On the Permutations Generated by Cyclic Shift

Stéphane Legendre
Team of Mathematical Eco-Evolution
Ecole Normale Supérieure
75005 Paris
France
legendre@ens.fr

Philippe Paclet
Lycée Chateaubriand
00161 Roma
Italy
paclet@dada.it

Abstract

The set of permutations generated by cyclic shift is studied using a number system coding for these permutations. The system allows to find the rank of a permutation given how it has been generated, and to determine a permutation given its rank. It defines a code describing structural and symmetry properties of the set of permutations ordered according to generation by cyclic shift. The code is associated with an Hamiltonian cycle in a regular weighted digraph. This Hamiltonian cycle is conjectured to be of minimal weight, leading to a combinatorial Gray code listing the set of permutations.

1 Introduction

It is well known that any natural integer a can be written uniquely in the factorial number system

$$a = \sum_{i=1}^{n-1} a_i \, i!, \quad a_i \in \{0, \ldots, i\},$$

where the uniqueness of the representation comes from the identity

$$\sum_{i=1}^{n-1} i \cdot i! = n! - 1. \tag{1}$$

Charles-Ange Laisant showed in 1888 [2] that the factorial number system codes the permutations generated in lexicographic order. More precisely, when the set of permutations is ordered lexicographically, the rank of a permutation written in the factorial number system provides a code determining the permutation. The code specifies which interchanges of the symbols according to lexicographic order have to be performed to generate the permutation.

In this study, a lesser-known number system on the finite ring $\mathbb{Z}_{n!}$ is used to describe properties of the set $\mathcal{S}_n$ of permutations on n symbols generated by cyclic shift. When $\mathcal{S}_n$ is ordered according to generation by cyclic shift, the rank of a permutation written in this number system entirely specifies how the permutation is generated.

This number system is a special case of a large class of methods presented by Knuth [1, §7.2.1.2] for generating $\mathcal{S}_n$. Here, an explicit and self-contained description is given.

Example 1. As will be shown, any number α in $\mathbb{Z}_{5!}$ can be written uniquely

$$\alpha = \alpha_3 \varpi_{5,3} + \alpha_2 \varpi_{5,2} + \alpha_1 \varpi_{5,1} + \alpha_0 \varpi_{5,0}$$

with the digits

$$\alpha_3 \in \mathbb{Z}_2, \quad \alpha_2 \in \mathbb{Z}_3, \quad \alpha_1 \in \mathbb{Z}_4, \quad \alpha_0 \in \mathbb{Z}_5,$$

and the base elements

$$\varpi_{5,3} = 3 \cdot 4 \cdot 5 = 60, \quad \varpi_{5,2} = 4 \cdot 5 = 20, \quad \varpi_{5,1} = 5, \quad \varpi_{5,0} = 1.$$

For example,

$$84 = 1 \cdot 60 + 1 \cdot 20 + 0 \cdot 5 + 4 \cdot 1 = 1104_\varpi.$$

We use the digits of 1104_ϖ to generate by cyclic shift a permutation on 5 symbols. The generation scheme is

$$(1) \xrightarrow{\alpha_3=1} (21) \xrightarrow{\alpha_2=1} (132) \xrightarrow{\alpha_1=0} (1324) \xrightarrow{\alpha_0=4} (51324),$$

and is established as follows. The orbit of the permutation (1) under cyclic shift is

$$\begin{array}{rl} 0: & (12) \\ 1: & \underline{(21)}. \end{array}$$

We select the permutation (21) whose exponent of the cyclic shift is the leftmost digit $\alpha_3 = 1$. Next, the orbit of (21) under cyclic shift is

$$\begin{array}{rl} 0: & (213) \\ 1: & \underline{(132)} \\ 2: & (321). \end{array}$$

The digit $\alpha_2 = 1$ leads to (132). Next, the orbit of (132) under cyclic shift is

$$\begin{array}{rl} 0: & \underline{(1324)} \\ 1: & (3241) \\ 2: & (2413) \\ 3: & (4132). \end{array}$$

The digit $\alpha_1 = 0$ leads to (1324). Finally, the last digit $\alpha_0 = 4$ leads to (51324). This permutation has rank $1104_{\varpi} = 84$ in the set of permutations on 5 symbols generated by cyclic shift, indexed from 0.

We shall describe properties of $\mathcal{S}_n$ generated by cyclic shift:

1. A decomposition into k-orbits;

2. The symmetries;

3. An infinite family of regular digraphs associated with $\{\mathcal{S}_n; n \geq 1\}$;

4. A conjectured combinatorial Gray code generating the permutations on n symbols. The adjacency rule associated with this code is that the last symbols of each permutation match the first symbols of the next optimally.

2 Number system

For any positive integer a, the ring $(\mathbb{Z}/a\mathbb{Z}, +, \times)$ of integers modulo a is denoted $\mathbb{Z}_a$. The set $\mathbb{Z}_a$ is identified with a subset of the set $\mathbb{N}$ of natural integers.

Proposition 2. *For $n \geq 2$, any element $\alpha \in \mathbb{Z}_{n!}$ can be uniquely represented as*

$$\alpha = \sum_{i=0}^{n-2} \alpha_i \varpi_{n,i}, \quad \alpha_i \in \mathbb{Z}_{n-i},$$

with the base elements

$$\varpi_{n,0} = 1, \qquad \varpi_{n,i} = n(n-1)\cdots(n-i+1), \qquad i = 1, \ldots, n-2.$$

The α_i's are the *digits* of α in this number system, which we call the *ϖ-system* for short. Any element of $\mathbb{Z}_{n!}$ can be written uniquely

$$\alpha = \alpha_{n-2} \cdots \alpha_1 \alpha_{0_{\varpi}}.$$

Unless $\alpha_{n-2} = 1$, the leftmost digits are set to 0, so that the representation always involves $n-1$ elements, indexed $0, \ldots, n-2$.

Proof. For simplicity, we momentarily denote $\varpi_i = \varpi_{n,i}$. For $n = 2$, there is a single base element, $\varpi_0 = 1$, and the result clearly holds. For $n \geq 3$, and $\alpha \in \mathbb{Z}_{n!}$, we set

$$\alpha^{(0)} = \alpha,$$

$$\alpha_i = \alpha^{(i)} \bmod (n-i), \quad \alpha^{(i+1)} = \alpha^{(i)} \operatorname{div} (n-i), \quad i = 0, \ldots, n-2,$$

where div denotes integer division. These relations imply

$$\alpha^{(i)} = (n-i)\alpha^{(i+1)} + \alpha_i, \quad i = 0, \ldots, n-2.$$

We multiply by ϖ_i on both sides. For $i = 0, \ldots, n-3$, we use the identity

$$\varpi_{i+1} = (n-i)\varpi_i, \tag{2}$$

and for $i = n-2$, we use the identity $2\varpi_{n-2} = 0$ in $\mathbb{Z}_2$, to get

$$\begin{array}{rcll} \varpi_i\alpha^{(i)} - \varpi_{i+1}\alpha^{(i+1)} & = & \alpha_i\varpi_i, & i = 0, \ldots, n-3, \\ \varpi_{n-2}\alpha^{(n-2)} & = & \alpha_{n-2}\varpi_{n-2}. & \end{array}$$

Adding these relations together, and accounting for telescoping cancellation on the left side,

$$\varpi_0\alpha^{(0)} = \alpha_{n-2}\varpi_{n-2} + \cdots + \alpha_0\varpi_0.$$

As and $\alpha^{(0)} = \alpha$, we obtain the representation

$$\alpha = \alpha_{n-2}\varpi_{n-2} + \cdots + \alpha_0\varpi_0.$$

By construction, $\alpha_i \in \mathbb{Z}_{n-i}$ for $i = 0, \ldots, n-2$. The existence of the decomposition also holds in $\mathbb{N}$.

We now prove the uniqueness of the decomposition in $\mathbb{N}$, and momentarily introduce the element $\varpi_{n-1} = n!$. In $\mathbb{N}$, the identities

$$\sum_{i=0}^{k-1}(n-i-1)\varpi_i = \varpi_k - 1, \quad k \in \{1, \ldots n-1\} \tag{3}$$

are easily shown using induction and (2) (such identities are general to mixed radix number systems). Assume that $\alpha \in \mathbb{N}$ has two different decompositions. Then, with obvious notations,

$$\sum_{i=0}^{n-2}(\alpha_i - \alpha_i')\varpi_i = 0. \tag{4}$$

Let k be the largest index such that $\alpha_i \neq \alpha_i'$. If $k = 0$, then $\alpha_0 \neq \alpha_0'$ and $\alpha_i = \alpha_i'$ for $i > 0$. From (4) we deduce $\alpha_0 = \alpha_0'$, a contradiction. If $k > 0$, then

$$\sum_{i=0}^{k-1}(\alpha_i - \alpha_i')\varpi_i = (\alpha_k' - \alpha_k)\varpi_k. \tag{5}$$

We may assume $\alpha_k' > \alpha_k$ with no loss of generality, so that the right hand term in (5) is larger than ϖ_k. As α_i and α_i' are less than $n - i - 1$, the left hand term is less than $\varpi_k - 1$ by (3), a contradiction. The uniqueness of the decomposition also holds in $\mathbb{Z}_{n!}$. $\square$

Arithmetics can be performed in the ring $(\mathbb{Z}_{n!}, +, \times)$ endowed with the ϖ-system. The computation of the sum and product works in the usual way of positional number systems, using the ring structure of $\mathbb{Z}_{n-i}$ for the operations on the digits of the operands. There is no carry to propagate after the leftmost digit.

Lemma 3. *The base elements verify*

$$\varpi_{n,i+k} = \varpi_{n-k,i}\varpi_{n,k}, \tag{6}$$

$$\sum_{i=0}^{k-1}(n-i-1)\varpi_{n,i} = \varpi_{n,k} - 1, \quad k \in \{1, \dots n-2\}, \tag{7}$$

$$\sum_{i=0}^{n-2}(n-i-1)\varpi_{n,i} = -1. \tag{8}$$

Proof. The verification of the first relation is straightforward. The identities (3) written in $\mathbb{Z}_{n!}$ give (7) and (8). For (8), we use the fact that $n! - 1 = -1$ in $\mathbb{Z}_{n!}$. □

Corollary 4. *For $\alpha, \alpha' \in \mathbb{Z}_{n!}$, with digits $\alpha_i, \alpha'_i \in \mathbb{Z}_{n-i}$,*

$$\alpha + \alpha' = -1 \iff \alpha_i + \alpha'_i = -1, \quad i = 0, \dots, n-2.$$

Proof. We write

$$\alpha + \alpha' = \sum_{i=0}^{n-2}(\alpha_i + \alpha'_i)\varpi_{n,i}.$$

In $\mathbb{Z}_{n-i}$, $\alpha_i+\alpha'_i = -1$ if and only if $\alpha_i+\alpha'_i = n-i-1$. By the uniqueness of the decomposition in the ϖ-system, the result follows from (8). □

3 Code

The set of permutations on n symbols $x_1, \dots, x_n$ is denoted $\mathcal{S}_n$. From a permutation q on the $n-1$ symbols $x_1, \dots, x_{n-1}$, n permutations on n symbols are generated by inserting x_n to the right and permuting the symbols cyclically. The insertion of x_n to the right defines an injection

$$\begin{array}{ccc} \mathcal{S}_{n-1} & \xrightarrow{\iota} & \mathcal{S}_n \\ q = (a_1 \cdots a_{n-1}) & \longmapsto & (a_1 \cdots a_{n-1}x_n) = \tilde{q}. \end{array}$$

We define the *cyclic shift* $S : \mathcal{S}_{n-1} \to \mathcal{S}_n$ by $S = C\iota$, where $C : \mathcal{S}_n \to \mathcal{S}_n$ is the circular permutation, so that

$$\begin{array}{rcl} S^0 q &=& (a_1 a_2 \cdots a_{n-1} x_n) = C^0 \tilde{q} = \tilde{q}, \\ S^1 q &=& (a_2 \cdots a_{n-1} x_n a_1) = C^1 \tilde{q}, \\ &\vdots& \\ S^{n-1} q &=& (x_n a_1 a_2 \cdots a_{n-1}) = C^{n-1}\tilde{q}. \end{array}$$

The set $\mathcal{O}(q) = \{S^0 q, \dots, S^{n-1} q\}$ is the *orbit* of q. As $S^i = S^j$ is equivalent to $i = j \bmod n$, the exponents of the cyclic shift are elements of $\mathbb{Z}_n$.

Lemma 5. *The set of permutations $\mathcal{S}_n$ is the disjoint union of the orbits $\mathcal{O}(q)$ for $q \in \mathcal{S}_{n-1}$.*

Proof. If $q, r \in \mathcal{S}_{n-1}$, their orbits are disjoint subsets of $\mathcal{S}_n$. Indeed, if $S^i q = S^j r$, there exists $k \in \mathbb{Z}_n$ such that $S^k q = S^0 r = \tilde{r}$. The only possibility is $k = 0$, implying $S^0 q = \tilde{q} = \tilde{r}$, and $q = r$. There are $(n-1)!$ disjoint orbits, each of size n, so that they span $\mathcal{S}_n$. $\square$

According to Lemma 5, the set $\mathcal{S}_n$ can be generated by cyclic shift. The generation by cyclic shift defines an order on the set of permutations, $\mathcal{S}_n = \{p_0, \ldots, p_{n!-1}\}$, a cyclic order in fact. For this order, the rank α of a permutation $p_\alpha \in \mathcal{S}_n$ is an element of $\mathbb{Z}_{n!}$.

The generation by cyclic shift of $p \in \mathcal{S}_n$ from $(1) \in \mathcal{S}_1$ can be schematized:

$$\left\{ \begin{array}{c} p^{(1)} = (1) \xrightarrow{\alpha_{n-2}} p^{(2)} \longrightarrow \cdots \xrightarrow{\alpha_2} p^{(n-2)} \xrightarrow{\alpha_1} p^{(n-1)} \xrightarrow{\alpha_0} p^{(n)} = p, \\ \\ p^{(n-i)} = S_{n-i}^{\alpha_i} p^{(n-i-1)}, \end{array} \right\} \tag{9}$$

where $p^{(n-i)} \in \mathcal{S}_{n-i}$ is generated from $p^{(n-i-1)} \in \mathcal{S}_{n-i-1}$ by the cyclic shift

$$S_{n-i} : \mathcal{S}_{n-i-1} \longrightarrow \mathcal{S}_{n-i}$$

with the exponent $\alpha_i \in \mathbb{Z}_{n-i}$ (Example 1).

Definition 6. The sequence of exponents $\alpha_i \in \mathbb{Z}_{n-i}$ associated with successive cyclic shifts leading from $(1) \in \mathcal{S}_1$ to $p \in \mathcal{S}_n$ is the *code* of p in the ϖ-system:

$$\alpha = \alpha_{n-2} \cdots \alpha_{0\,\varpi} \in \mathbb{Z}_{n!}.$$

Theorem 7. *The rank of a permutation on n symbols generated by cyclic shift is given by its code. A permutation on n symbols generated by cyclic shift is determined by writing its rank in the ϖ-system.*

Proof. We use induction on n. For $n = 2$, in $\mathcal{S}_2 = \{(12), (21)\}$, the rank of the permutation (12) is $0 = 0_\varpi$, and the rank of the permutation (21) is $1 = 1_\varpi$. For $n > 2$, let $p = p_\alpha \in \mathcal{S}_n$ of rank α, generated by cyclic shift from $q = q_\beta \in \mathcal{S}_{n-1}$ of rank β. Then $p = S_n^{\alpha_0} q$ for some $\alpha_0 \in \mathbb{Z}_n$, α_0 being the rank of p within the orbit of q. As the orbits contain n elements and as β is the rank of q in $\mathcal{S}_{n-1}$, the rank of p in $\mathcal{S}_n$ is

$$\alpha = \beta n + \alpha_0 = \beta \varpi_{n,1} + \alpha_0 \varpi_{n,0}.$$

By induction hypothesis, the rank β of q is given by the code

$$\beta = \sum_{i=0}^{n-3} \beta_i \varpi_{n-1,i}, \quad \beta_i \in \mathbb{Z}_{n-1-i}.$$

Eq. (6) gives, for $k = 1$,

$$\varpi_{n,i+1} = \varpi_{n-1,i} \varpi_{n,1},$$

so that

$$\beta \varpi_{n,1} = \sum_{i=0}^{n-3} \beta_i \varpi_{n-1,i} \varpi_{n,1} = \sum_{i=0}^{n-3} \beta_i \varpi_{n,i+1} = \sum_{i=1}^{n-2} \beta_{i-1} \varpi_{n,i}.$$

Let $\alpha_i = \beta_{i-1}$ for $i = 1, \ldots, n-2$. As $\beta_i \in \mathbb{Z}_{n-1-i}$, $\alpha_i \in \mathbb{Z}_{n-i}$. We obtain that

$$\alpha = \beta\varpi_{n,1} + \alpha_0\varpi_{n,0} = \sum_{i=0}^{n-2} \alpha_i \varpi_{n,i}, \quad \alpha_i \in \mathbb{Z}_{n-i},$$

is the code of p_α. Conversely, let $p_\alpha \in \mathcal{S}_n$. We write the rank α in the ϖ-system, $\alpha = {\alpha_{n-2} \cdots \alpha_0}_\varpi$, and use scheme (9) with the exponents $\alpha_{n-2}, \ldots, \alpha_0$ to determine p_α. $\square$

α	p_α	α_2	α_1	α_0
0	1234	0	0	0
1	2341	0	0	1
2	3412	0	0	2
3	4123	0	0	3
4	2314	0	1	0
5	3142	0	1	1
6	1423	0	1	2
7	4231	0	1	3
8	3124	0	2	0
9	1243	0	2	1
10	2431	0	2	2
11	4312	0	2	3
12	2134	1	0	0
13	1342	1	0	1
14	3421	1	0	2
15	4213	1	0	3
16	1324	1	1	0
17	3241	1	1	1
18	2413	1	1	2
19	4132	1	1	3
20	3214	1	2	0
21	2143	1	2	1
22	1432	1	2	2
23	4321	1	2	3

Table 1: The codes of the permutations of $\{1, 2, 3, 4\}$ generated by cyclic shift.

Algorithm C in Knuth [1, §7.2.1.2] generates $\mathcal{S}_n$ by cyclic shift in a simple version of the scheme described in this section.

In the sequel, we assume that $\mathcal{S}_n$ is ordered according to generation by cyclic shift.

4 k-orbits

The ϖ-system is a family of number systems indexed by n, which are compatible in a sense precised in the next proposition. The compatibility relies on relation (6).

Proposition 8. *Let $k \in \{0, \ldots, n-2\}$ and $p_\alpha \in \mathcal{S}_n$ with code $\alpha \in \mathbb{Z}_{n!}$. There exists a permutation $q_\beta \in S_{n-k}$ with code $\beta \in \mathbb{Z}_{(n-k)!}$ such that*

$$\alpha = \beta\varpi_{n,k} + \gamma, \quad \gamma \in \{0, \ldots, \varpi_{n,k} - 1\}. \tag{10}$$

The code β is made of the $n-k-1$ leftmost digits of α, and γ is made of the k rightmost digits of α.

Proof. We have the decomposition

$$\alpha = \alpha_{n-2}\cdots\alpha_{0_\varpi} = \alpha_{n-2}\cdots\alpha_k 0\cdots 0_\varpi + 0\cdots 0\alpha_{k-1}\cdots\alpha_{0_\varpi} = \tilde{\alpha} + \gamma.$$

Let $\beta_i = \alpha_{i+k}$ for $i = 0, \ldots, n-k-2$, so that the β's are the $n-k-1$ leftmost digits of α. As $\alpha_i \in \mathbb{Z}_{n-i}$, $\beta_i = \alpha_{i+k} \in \mathbb{Z}_{n-k-i}$. Hence

$$\beta = \sum_{i=0}^{n-k-2} \beta_i \varpi_{n-k,i}, \quad \beta_i \in \mathbb{Z}_{n-k-i},$$

is an element of $\mathbb{Z}_{(n-k)!}$ which is the code of a permutation $q_\beta \in \mathcal{S}_{n-k}$. Using relation (6), we obtain

$$\tilde{\alpha} = \sum_{i=k}^{n-2} \alpha_i \varpi_{n,i} = \sum_{i=0}^{n-k-2} \alpha_{i+k} \varpi_{n,i+k} = \sum_{i=0}^{n-k-2} \alpha_{i+k} \varpi_{n-k,i} \varpi_{n,k} = \left(\sum_{i=0}^{n-k-2} \beta_i \varpi_{n-k,i} \right) \varpi_{n,k}.$$

The term

$$\gamma = \sum_{i=0}^{k-1} \alpha_i \varpi_{n,i}$$

is made of the k rightmost digits of α. It is an element of $\mathbb{Z}_{n-k+1} \times \cdots \times \mathbb{Z}_n$ ranging from 0 to $\sum_{i=0}^{k-1}(n-i-1)\varpi_{n,i}$, which equals $\varpi_{n,k} - 1$ by (7). We obtain

$$\alpha = \tilde{\alpha} + \gamma = \beta \varpi_{n,k} + \gamma.$$

$\square$

Definition 9. For $k \in \{0, \ldots, n-2\}$ and $q_\beta \in \mathcal{S}_{n-k}$, the *$k$-orbit* of q_β is the following subset of $\mathcal{S}_n$:

$$\mathcal{O}_{n,k}(q_\beta) = \{p_\alpha \in S_n; \quad \alpha = \beta\varpi_{n,k} + \gamma, \quad \gamma = 0, \ldots, \varpi_{n,k} - 1\}.$$

For $k = 0$, the 0-orbit of $q \in \mathcal{S}_n$ is $\{q\}$. Indeed, for $k = 0$, $\varpi_{n,0} = 1$, $\gamma = 0$, and $q = p_\alpha$. For $k \geq 1$, a k-orbit $\mathcal{O}_{n,k}(q)$ can be described as the subset of $\mathcal{S}_n$ generated from $q \in \mathcal{S}_{n-k}$ by k successive cyclic shifts. Indeed, by Proposition 8, the code of $p_\alpha \in \mathcal{O}_{n,k}(q_\beta)$ is obtained by appending $\alpha_{k-1}\cdots\alpha_0$ to the code $\beta_{n-k-2}\cdots\beta_{0_\varpi}$ of q_β. By scheme (9), the digits $\alpha_{k-1}, \ldots, \alpha_0$ describe the generation of p_α from q_β. In particular, for $k = 1$, the 1-orbit $\mathcal{O}_{n,1}(q)$ of $q \in \mathcal{S}_{n-1}$ is the orbit $\mathcal{O}(q)$. We may further define the $(n-1)$-orbit $\mathcal{O}_{n,n-1}(q)$ as the whole set $\mathcal{S}_n$, with $q = (1) \in \mathcal{S}_1$.

We have the following generalization of Lemma 5:

Proposition 10. *For $k \in \{0, \ldots, n-2\}$, the set of permutations $\mathcal{S}_n$ is the disjoint union of the k-orbits $\mathcal{O}_{n,k}(q)$ for $q \in \mathcal{S}_{n-k}$.*

Proof. The k-orbits are disjoint by the uniqueness of the decomposition (10). They are $(n-k)!$ in number, and contain $\varpi_{n,k}$ elements each. As $(n-k)!\varpi_{n,k} = n!$ in $\mathbb{N}$, the k-orbits span $\mathcal{S}_n$. □

In decomposition (10), β specifies to which k-orbit p_α belongs and γ specifies the rank of p_α within the k-orbit. The first element of the k-orbit has rank $\alpha^{first} = \beta\varpi_{n,k}$ (i.e., $\gamma = 0$). The last element has rank $\alpha^{last} = \beta\varpi_{n,k} + \varpi_{n,k} - 1$ (i.e., $\gamma = \varpi_{n,k} - 1$). The element next to the last has rank $\alpha^{last} + 1 = \beta\varpi_{n,k} + \varpi_{n,k} = (\beta+1)\varpi_{n,k}$. It is the first element of the next k-orbit $\mathcal{O}_{n,k}(q_{\beta+1})$, where $q_{\beta+1}$ is the element next to q_β in $\mathcal{S}_{n-k}$.

Lemma 11. *Let $p_\alpha \in \mathcal{S}_n$. There exists a largest $k \in \{0, \ldots, n-2\}$ and $q_\beta \in \mathcal{S}_{n-k}$ such that p_α is the last element of the k-orbit $\mathcal{O}_{n,k}(q_\beta)$, and not the last element of the $(k+1)$-orbit containing this k-orbit.*

Proof. If p_α is not the last element of the 1-orbit it belongs to, it is the last element of the 0-orbit $\{p_\alpha\}$. In this trivial case, $k = 0$ and $p_\alpha = q_\beta$. Otherwise the rightmost digit of α is $\alpha_0 = n-1$. There exists a largest $k \geq 1$ such that $\alpha_i = n-i-1$ for $i = 0, \ldots, k-1$, and $\alpha_k \neq n-k-1$. This means that p_α is the last element of nested j-orbits, $j = 1, \ldots, k$, and not the last element of the $(k+1)$-orbit containing these nested j-orbits. □

5 Symmetries

For compatibility with the cyclic shift, we adopt the convention that the positions of the symbols in a permutation are computed from the right, and are considered as elements of $\mathbb{Z}_n$ (the position of the last symbol is 0 and the position of the first symbol is $n-1$).

According to scheme (9), the symbol x_{n-i} $(i \geq 2)$ appears at step $n-i$ with the digit α_i as exponent of the cyclic shift. Its position in the generated permutation $p^{(n-i)}$ is therefore

$$\mathrm{pos}_{n-i}(x_{n-i}, p^{(n-i)}) = \alpha_i.$$

In particular,

$$\mathrm{pos}_n(x_n, p^{(n)}) = \alpha_0. \tag{11}$$

For a permutation $p = (a_1 a_2 \cdots a_{n-1} a_n) \in \mathcal{S}_n$, we introduce the *mirror image* of p, $\overline{p} = (a_n a_{n-1} \cdots a_2 a_1)$.

Proposition 12. *The permutations p_α and $p_{\alpha'}$ are the mirror image of one another if and only if their ranks α and α' verify in $\mathbb{Z}_{n!}$*

$$\alpha + \alpha' = -1.$$

For example, in $\mathbb{Z}_{5!}$ we have $84 + 35 = -1$, and in $\mathcal{S}_5$, $p_{84} = (51324)$ is the mirror image of $p_{35} = (42315)$.

Proof. The proof is by induction on n. For $n = 2$, $p_0 = (12)$, $p_1 = (21)$, and $0 + 1 = 1 = -1$ in $\mathbb{Z}_2$. Let $n > 2$. By Proposition 8,

$$\alpha = \beta\varpi_{n,1} + \alpha_0\varpi_{n,0}, \quad \alpha' = \beta'\varpi_{n,1} + \alpha'_0\varpi_{n,0}, \quad q_\beta, q_{\beta'} \in \mathcal{S}_{n-1}, \quad \alpha_0, \alpha'_0 \in \mathbb{Z}_n.$$

By Corollary 4, the condition $\alpha + \alpha' = -1$ is equivalent to $\beta + \beta' = -1$ and $\alpha_0 + \alpha'_0 = -1$. By induction hypothesis, q_β is the mirror image of $q_{\beta'}$ in $\mathcal{S}_{n-1}$ if and only if $\beta + \beta' = -1$. The condition $\alpha + \alpha'_0 = -1$ is equivalent to $\alpha'_0 = n - 1 - \alpha_0$, i.e., the ranks of α_0 and α'_0 are symmetrical in $\mathbb{Z}_n$. By (11), these ranks are the positions of symbol x_n when p_α and $p_{\alpha'}$ are generated by cyclic shift from q_β and $q_{\beta'}$ respectively. This gives the result. $\square$

Corollary 13. *The word constructed by concatenating the symbols of the permutations generated by cyclic shift is a palindrome.*

Proof. Let $p_\alpha \in \mathcal{S}_n$. The rank symmetrical to α in $\mathbb{Z}_{n!}$ is $(n! - 1) - \alpha = -(\alpha + 1)$. By Proposition 12, $p_{-(\alpha+1)}$ is the mirror image of p_α. $\square$

The set $\mathcal{S}_n$ has in fact deeper symmetries, coming from the recursive structure of the k-orbits.

According to Theorem 7, the generation of $\mathcal{S}_n$ by cyclic shift is obtained by performing $\alpha \to \alpha + 1$ for $\alpha \in \mathbb{Z}_{n!}$, and writing α in the ϖ-system. This determines each permutation p_α. For a fixed k, as α runs through $\mathbb{Z}_{n!}$, p_α runs through the k-orbits of $\mathcal{S}_n$, and leaves a k-orbit to enter the next when, in the computation of $\alpha + 1$, the carry propagates up to the digit α_k, incrementing the rank β of the k-orbit.

Proposition 14. *Any two successive permutations of $\mathcal{S}_n$ are written as*

$$p_\alpha = \overline{A}B, \qquad p_{\alpha+1} = BA,$$

with an integer $k \in \{0, \ldots, n-2\}$ such that

$$|A| = k + 1.$$

For example, in $\mathcal{S}_5$, $p_{39} = (542\underline{31})$ and $p_{40} = (\underline{31}245)$.

Proof. If p_α and $p_{\alpha+1}$ are in the same 1-orbit then

$$p_\alpha = (a_1 a_2 \cdots a_n), \qquad p_{\alpha+1} = (a_2 \cdots a_n a_1).$$

The result holds with $A = (a_1)$, $B = (a_2 \cdots a_n)$, and this corresponds to $k = 0$. Otherwise, by Lemma 11, there exists a largest $k \geq 1$ such that p_α is the last element of a k-orbit, and not the last element of a $(k+1)$-orbit. The elements of a k-orbit are generated by successively inserting the symbols $x_{n-k+1}, \ldots, x_n$ from a permutation $q_\beta \in \mathcal{S}_{n-k}$. The last element is

$$(x_n \cdots x_{n-k+1} b_1 \cdots b_{n-k}),$$

where $q_\beta = (b_1 \cdots b_{n-k})$ is a permutation of the symbols $x_1, \ldots, x_{n-k}$. The first element of the next k-orbit is

$$(c_1 \cdots c_{n-k} x_{n-k+1} \cdots x_n),$$

where $q_{\beta+1} = (c_1 \cdots c_{n-k})$. As $\mathcal{S}_{n-k}$ is generated by cyclic shift, $q_{\beta+1} = C_{n-k} q_\beta$, with C_{n-k} the circular permutation in $\mathcal{S}_{n-k}$. We obtain

$$\begin{array}{lll} p_\alpha & = (x_n \cdots x_{n-k+1} b_1 b_2 \cdots b_{n-k}) & = \overline{A}B \\ p_{\alpha+1} & = (b_2 \cdots b_{n-k} b_1 x_{n-k+1} \cdots x_n) & = BA, \end{array}$$

where $A = (b_1 x_{n-k+1} \cdots x_n)$ contains $k + 1$ symbols. $\square$

According to Proposition 14, $k+1$ symbols (the symbols of A) have to be erased to the left of p_α so that the last symbols of p_α (the symbols of B) match the first symbols of $p_{\alpha+1}$.

Definition 15. The *weight* $e_n(\alpha)$ of the transition $\alpha \to \alpha+1$ is the number of symbols that have to be erased to the left of p_α so that the last symbols of p_α match the first symbols of $p_{\alpha+1}$. The *ϖ-ruler sequence* is the sequence of weights:

$$E_n = \{e_n(\alpha); \quad \alpha = 0, \dots, n!-2\}.$$

Proposition 16. *The ϖ-ruler sequence is a palindrome.*

Proof. If the ranks α and α' are symmetrical in $\mathbb{Z}_{n!}$, $\alpha + \alpha' = -1$. Then $\alpha_i + \alpha'_i = -1$ for $i = 0, \dots, n-2$ by Corollary 4. By the definition of $e_n(\alpha)$ (the weight associated with the transition $\alpha \to \alpha+1$), we want to show that $e_n(\alpha) = e_n(\alpha'-1)$. If p_α is the last element of a k-orbit, $k \geq 1$, then $\alpha_i = -1$ for $i = 0, \dots, k-1$, so that $\alpha'_i = 0$ for $i = 0, \dots, k-1$: $p_{\alpha'}$ is the first element of a k-orbit, and $p_{\alpha'-1}$ is the last element of the previous k-orbit. Hence $e_n(\alpha) = e_n(\alpha'-1) = k+1$. If p_α is not the last element of a k-orbit, then $\alpha_0 \neq -1$. Hence $\alpha'_0 \neq 0$, and $p_{\alpha'}$ is not the first element of a 1-orbit. In this case $e_n(\alpha) = e_n(\alpha'-1) = 1$. ☐

Proposition 17. *The number of terms of the ϖ-ruler sequence such that $e_n(\alpha) = k$ is*

$$(n-k)(n-k)!.$$

The sum of its $n!-1$ terms is

$$W_n = 1! + 2! + \dots + n! - n.$$

Proof. We have $e_n(\alpha) = k$ if and only if p_α is the last element of a $(k-1)$-orbit, and not the last element of a k-orbit. The number of $(k-1)$-orbits within a k-orbit is $n-k+1$. We exclude the last $(k-1)$-orbit within the k-orbit (otherwise p_α would be the last element of the k-orbit). This gives $n-k$ possibilities for $e_n(\alpha) = k$ in a k-orbit. As the number of k-orbits is $(n-k)!$, there are $(n-k)(n-k)!$ possibilities for $e_n(\alpha) = k$.

The formula for the sum is shown by induction. We have $W_2 = 1 = 1! + 2! - 2$, and for $n > 2$,

$$\begin{aligned} W_n &= \sum_{k=1}^{n-1} k(n-k)(n-k)! = \sum_{k=0}^{n-2} (k+1)(n-1-k)(n-1-k)! \\ &= \sum_{k=1}^{n-2} k(n-1-k)(n-1-k)! + \sum_{k=0}^{n-2} (n-1-k)(n-1-k)! \\ &= W_{n-1} + \sum_{i=1}^{n-1} i \cdot i! = 1! + \dots + (n-1)! - (n-1) + n! - 1 = 1! + \dots + n! - n. \end{aligned}$$

In the last line, the induction hypothesis and identity (1) have been used. ☐

The ϖ-ruler sequence is analogous to the binary ruler function (A001511 in Sloane [3]). The terms of the ruler function give the position of the bit to flip when the binary numbers are listed according to the binary reflected Gray code. They represent the binary division of an inch. The ϖ-ruler sequence differs in that the number of intermediate ticks increases with n (Table 2).

n	E_n
2	1
3	$1^2 2 1^2$
4	$1^3 2 1^3 2 1^3 3 1^3 2 1^3 2 1^3$
5	$1^4 2 1^4 2 1^4 2 1^4 3 1^4 2 1^4 2 1^4 2 1^4 3 1^4 2 1^4 2 1^4 2 1^4 4 1^4 2 1^4 2 1^4 2 1^4 3 1^4 2 1^4 2 1^4 2 1^4 3 1^4 2 1^4 2 1^4 2 1^4$

Table 2: The ϖ-ruler sequence for $n = 2, 3, 4, 5$ (1^j denotes 1 repeated j times).

6 Combinatorial Gray code

A combinatorial Gray code is a method for generating combinatorial objects so that successive objects differ by some pre-specified adjacency rule involving a minimality criterion (Savage [4]). Such a code can be formulated as an Hamiltonian path or cycle in a graph whose vertices are the combinatorial objects to be generated. Two vertices are joined by an edge if they differ from each other in the pre-specified way.

The code associated with the ϖ-system corresponds to an Hamiltonian path in a weighted directed graph G_n.

Definition 18. The vertices of the digraph G_n are the elements of $\mathcal{S}_n$. For two permutations (vertices) p_α and $p_{\alpha'}$, there is an arc from p_α to $p_{\alpha'}$ if and only if the last symbols of p_α match the first symbols of $p_{\alpha'}$ (there is no arc when there is no match). Let $p_\alpha, p_{\alpha'} \in \mathcal{S}_n$ be two connected vertices in G_n. The *weight* $f_n(\alpha, \alpha') \in \{1, \ldots, n-1\}$ associated with the arc $(p_\alpha, p_{\alpha'})$ is the number of symbols that have to be erased to the left of p_α so that the last symbols of p_α match the first symbols of $p_{\alpha'}$.

By Proposition 14, for each α, there is an arc of weight $e_n(\alpha) = f_n(\alpha, \alpha + 1)$ joining p_α to $p_{\alpha+1}$. This allows to define the Hamiltonian path

$$\mathbf{w}_n = \{(p_\alpha, p_{\alpha+1});\ \alpha = 0, \ldots, n! - 2\}$$

joining successive permutations. This path has total weight $W_n = 1! + \cdots + n! - n$ by Proposition 17. The path $\mathbf{w}_n$ can be closed into an Hamiltonian cycle by joining the last permutation $p_{n!-1}$ to the first p_0 by an arc of weight $n - 1$:

$$(x_n \cdots x_2 x_1) \xrightarrow{n-1} (x_1 x_2 \cdots x_n).$$

Hence, an oriented path exists from any vertex to any other, so that G_n is strongly connected.

Table 3 displays the adjacency matrix of the weighted digraph G_4 and the Hamiltonian path $\mathbf{w}_4$.

Proposition 19. *Each vertex of G_n has exactly $j!$ in-arcs of weight j and $j!$ out-arcs of weight j for $j = 1, \ldots, n-1$. Hence the vertices of G_n have $L = 1! + \cdots + (n-1)!$ as in- and out-degree, and G_n is L-regular. The total number of arcs is $Ln!$.*

Proof. Let us consider the arcs of weight $j \in \{1, \ldots, n-1\}$ joining a vertex to another in G_n:

$$(a_1 \cdots a_j b_1 \cdots b_{n-j}) \xrightarrow{j} (b_1 \cdots b_{n-j} c_1 \cdots c_j),$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
0	0	1	2	3	0	0	0	3	0	0	0	3	0	0	2	3	0	0	0	3	0	0	0	3
1	3	0	1	2	0	0	3	0	0	3	0	0	0	3	0	0	3	0	0	2	0	0	3	0
2	2	3	0	1	3	0	0	0	0	2	3	0	3	0	0	0	0	0	3	0	0	3	0	0
3	1	2	3	0	2	3	0	0	3	0	0	0	0	0	3	0	0	3	0	0	3	0	0	0
4	0	0	0	3	0	1	2	3	0	0	0	3	0	0	0	3	0	0	0	3	0	0	2	3
5	0	3	0	0	3	0	1	2	0	0	3	0	3	0	0	2	0	0	3	0	0	3	0	0
6	0	2	3	0	2	3	0	1	3	0	0	0	0	0	3	0	0	3	0	0	3	0	0	0
7	3	0	0	0	1	2	3	0	2	3	0	0	0	3	0	0	3	0	0	0	0	0	3	0
8	0	0	0	3	0	0	0	3	0	1	2	3	0	0	0	3	0	0	2	3	0	0	0	3
9	0	0	3	0	0	3	0	0	3	0	1	2	0	0	3	0	0	3	0	0	3	0	0	2
10	3	0	0	0	0	2	3	0	2	3	0	1	0	3	0	0	3	0	0	0	0	0	3	0
11	2	3	0	0	3	0	0	0	1	2	3	0	3	0	0	0	0	0	3	0	0	3	0	0
12	0	0	2	3	0	0	0	3	0	0	0	3	0	1	2	3	0	0	0	3	0	0	0	3
13	0	3	0	0	3	0	0	2	0	0	3	0	3	0	1	2	0	0	3	0	0	3	0	0
14	3	0	0	0	0	0	3	0	0	3	0	0	2	3	0	1	3	0	0	0	0	2	3	0
15	0	0	3	0	0	3	0	0	3	0	0	0	1	2	3	0	2	3	0	0	3	0	0	0
16	0	0	0	3	0	0	0	3	0	0	2	3	0	0	0	3	0	1	2	3	0	0	0	3
17	3	0	0	2	0	0	3	0	0	3	0	0	0	3	0	0	3	0	1	2	0	0	3	0
18	0	0	3	0	0	3	0	0	3	0	0	0	0	2	3	0	2	3	0	1	3	0	0	0
19	0	3	0	0	3	0	0	0	0	0	3	0	3	0	0	0	1	2	3	0	2	3	0	0
20	0	0	0	3	0	0	2	3	0	0	0	3	0	0	0	3	0	0	0	3	0	1	2	3
21	0	0	3	0	0	3	0	0	3	0	0	2	0	0	3	0	0	3	0	0	3	0	1	2
22	0	3	0	0	3	0	0	0	0	0	3	0	3	0	0	0	0	2	3	0	2	3	0	1
23	3	0	0	0	0	0	3	0	0	3	0	0	2	3	0	0	3	0	0	0	1	2	3	0

Table 3: The adjacency matrix of the digraph G_4. Lines delineate the 1-orbits. Double lines delineate the 2-orbits. Entries on the upper diagonal (in color) indicate the Hamiltonian path corresponding to the ϖ-system code, and forming the ϖ-ruler sequence.

where the c's are a permutation of the a's. There are $j!$ possibilities for the c's, the a's and the b's being fixed. Hence $j!$ arcs of weight j leave each vertex. Similarly, there are $j!$ possibilities for the a's, the b's and the c's being fixed, so that $j!$ arcs of weight j enter each vertex. By the degree sum formula, the sum of the in- or out-degrees of the $n!$ vertices, $n!(1! + \cdots + (n-1)!)$, equals the total number of arcs. □

The set $\{G_n;\ n \geq 1\}$ is an infinite family of strongly connected regular digraphs.

We conjecture that the Hamiltonian path $\mathbf{w}_n$ joining successive permutations in the digraph G_n is of minimal total weight. Assuming the conjecture, we may state:

The ϖ-system is a combinatorial Gray code listing the permutations generated by cyclic shift. The adjacency rule is that the minimal number of symbols is erased to the left of a permutation so that the last symbols of the permutation match the first symbols of the next permutation.

7 Acknowledgments

Marco Castera initiated the problem which motivated this study. The pertinent comments of the anonymous referee were very helpful.

References

[1] D. E. Knuth, *The Art of Computer Programming*, Vol. 4, Combinatorial Algorithms, Addison-Wesley, 2005.

[2] C.-A. Laisant, Sur la numération factorielle, application aux permutations, *Bull. Soc. Math. France* **16** (1888), 176–183.

[3] N. J. A. Sloane, *The On–Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences, 2010.

[4] C. Savage, A survey of combinatorial Gray codes, *SIAM Rev.* **39** (1997), 605–629.

2000 *Mathematics Subject Classification*: Primary 05A05, 11A63; Secondary 05C20, 05C38.
Keywords: permutations, cyclic shift, number system, palindrome, combinatorial Gray code.

(Concerned with sequences A000142, A001511, A007489, and A033312.)

Received September 21 2010; revised version received December 13 2010; February 14 2011. Published in *Journal of Integer Sequences*, March 25 2011.
