The Number System of the Permutations Generated by Cyclic Shift

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

Abstract

A number system coding for the permutations generated by cyclic shift is described. 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 the symmetry properties of the set of permutations generated by cyclic shift. This code is conjectured to be a combinatorial Gray code listing the set of permutations: this corresponds to an Hamiltonian path of minimal weight in an appropriate regular digraph.

1 Introduction

Since the work of Laisant in 1888 [4] – and even since Fischer and Krause in 1812 [1] according to Hall and Knuth [2] –, it is known that the factorial number system codes for the permutations generated in lexicographic order. More precisely, when the set of all permutations on $n$ symbols is ordered by lexicographic order, the rank of a permutation written in the factorial 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. Conversely, the rank of a permutation can be computed from its code. This coding has been rediscovered several times since (e.g., Lehmer [5]).

In this study, we describe a number system on the finite ring $\mathbb{Z}_n!$ coding for the permutations generated by cyclic shift. When the set $S_n$ of permutations is ordered according to generation by cyclic shift, the rank of a permutation written in this number system entirely specifies how the permutation has been generated. Conversely, the rank can be computed from the code. This number system is a special case of a large class of methods presented by Knuth [3] for generating $S_n$.

We shall describe properties of $S_n$ generated by cyclic shift:

1. A decomposition into $k$-orbits;

2. The symmetries;
3. An infinite family of regular digraphs associated with \( \{S_n; n \geq 1\} \);

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 1.** 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

\[
\varpi_{n,0} = 1, \quad \varpi_{n,i} = n(n-1) \cdots (n-i+1), \quad i = 1, \ldots, n-2.
\]

The \( \alpha_i \)'s are the *digits* of \( \alpha \) in this number system, which we call the \( \varpi \)-system. 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 rightmost digits are set to 0, so that the sum always involves \( n - 1 \) elements, indexed \( 0, \ldots, n-2 \).

For example, in \( \mathbb{Z}_{5!} \) the base is \( \{\varpi_{5,0} = 1, \varpi_{5,1} = 5, \varpi_{5,2} = 20, \varpi_{5,3} = 60\} \). The element 84 writes

\[
84 = 1 \times 60 + 1 \times 20 + 0 \times 5 + 4 \times 1 = 1104_{\varpi},
\]

and the element 35 writes

\[
35 = 0 \times 60 + 1 \times 20 + 3 \times 5 + 0 \times 1 = 0130_{\varpi}.
\]

**Proof.** For simplicity, we 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

\[
\alpha^{(0)} = \alpha,
\]

\[
\alpha_i = \alpha^{(i)} \mod (n-i), \quad \alpha^{(i+1)} = \alpha^{(i)} \div (n-i), \quad i = 0, \ldots, n-2,
\]

where \( \div \) denotes the integer division. These relations imply

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

We multiply by \( \varpi_i \) on both sides. For \( i = 0, \ldots, n-3 \), we use the identity \( \varpi_{i+1} = (n-i)\varpi_i \), and for \( i = n-2 \), we use the identity \( 2\varpi_{n-2} = 0 \) in \( \mathbb{Z}_{2} \), to get

\[
\varpi_i\alpha^{(i)} - \varpi_{i+1}\alpha^{(i+1)} = \alpha_i\varpi_i, \quad i = 0, \ldots, n-3,
\]

\[
\varpi_{n-2}\alpha^{(n-2)} = \alpha_{n-2}\varpi_{n-2}.
\]
Adding these relations together, and accounting for telescoping cancellation on the left side,
\[ \varpi_0\alpha^{(0)} = \alpha_{n-2}\varpi_{n-2} + \cdots + \alpha_0\varpi_0. \]

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 digits \( \alpha_i \) are uniquely determined, so that the representation is unique.

Arithmetics can be performed in the ring \((\mathbb{Z}_n!, +, \times)\) endowed with the \( \varpi \)-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 rightmost digit.

**Lemma 1.** The base elements verify

\[ \varpi_{n,i+k} = \varpi_{n-k,i}\varpi_{n,k}; \quad (1) \]

\[ \sum_{i=0}^{k-1} (n-i-1)\varpi_{n,i} = \varpi_{n,k} - 1, \quad k \in \{1, \ldots n-2\}, \quad (2) \]

\[ \sum_{i=0}^{n-2} (n-i-1)\varpi_{n,i} = -1. \quad (3) \]

**Proof.** The verification of the first relation is straightforward. For the two other relations, let

\[ \xi = \sum_{i=0}^{k-1} \alpha_i\varpi_{n,i}, \quad \alpha_i = n - i - 1 \in \mathbb{Z}_{n-i}. \]

In \( \mathbb{Z}_{n-i} \), \( \alpha_i + 1 = 0 \). Therefore, when computing \( \xi + 1 \), the carry propagates from \( \alpha_0 \) up to \( \alpha_{k-1} \), and the \( \alpha_i \)'s are set to 0. If \( k \leq n-2 \), the digit \( \alpha_k = 0 \) gets the carry and is replaced by 1. In this case, \( \xi + 1 = \varpi_{n,k} \). If \( k = n-1 \), there is no carry to propagate after the rightmost digit, and all digits of \( \xi + 1 \) are set to 0. In this case, \( \xi + 1 = 0 \).

**Corollary 1.** For \( \alpha, \alpha' \in \mathbb{Z}_n! \), with digits \( \alpha_i, \alpha'_i \in \mathbb{Z}_{n-i} \),

\[ \alpha + \alpha' = -1 \iff \alpha_i + \alpha'_i = -1, \quad i = 0, \ldots, n-2. \]

**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 uniqueness of the decomposition in the \( \varpi \)-system, the result follows from (3).
It can be noted that (3) leads in \( \mathbb{N} \) to the identity
\[
\sum_{i=0}^{n-2} (n - i - 1) \frac{n!}{(n - i)!} = n! - 1,
\]
which is related to the identity
\[
\sum_{i=1}^{n-1} i \cdot i! = n! - 1,
\]
associated with the factorial number system. Identities (2) and (3) are instances of general identities of mixed radix number systems.

## 3 Code

The set of permutations on \( n \) symbols \( x_1, \ldots, x_n \) is denoted \( \mathcal{S}_n \). From a permutation \( q \) on the \( n - 1 \) symbols \( x_1, \ldots, x_{n-1} \), \( n \) permutations on \( n \) symbols are generated by inserting \( x_n \) to the right and cyclically permuting the symbols. The insertion of \( x_n \) to the right defines an injection
\[
\mathcal{S}_{n-1} \ni q = (a_1 \cdots a_{n-1}) \rightarrow \mathcal{S}_n \ni (a_1 \cdots a_{n-1} x_n) = \tilde{q}.
\]
We define the cyclic shift \( S : \mathcal{S}_{n-1} \rightarrow \mathcal{S}_n \) by \( S = C \circ \iota \), where \( C : \mathcal{S}_n \rightarrow \mathcal{S}_n \) is the circular permutation, so that
\[
S^0 q = (a_1 a_2 \cdots a_{n-1} x_n) = C^0 \tilde{q} = \tilde{q},
S^1 q = (a_2 \cdots a_{n-1} x_n a_1) = C^1 \tilde{q},
\]
\[
\vdots
S^{n-1} q = (x_n a_1 a_2 \cdots a_{n-1}) = C^{n-1} \tilde{q}.
\]
The set \( \mathcal{O}(q) = \{ S^0 q, \ldots, S^{n-1} q \} \) is the orbit of \( q \). As \( S^i = S^j \) is equivalent to \( i = j \mod n \), the exponents of the cyclic shift are elements of \( \mathbb{Z}_n \).

**Lemma 2.** 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 2 the set \( \mathcal{S}_n \) can be generated by cyclic shift. The generation by cyclic shift defines an order on the set of permutations, \( \mathcal{S}_n = \{ p_0, \ldots, p_{n!-1} \} \), indexed from 0 (a cyclic order in fact). For this order, the rank \( \alpha \) 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:
\[
\begin{cases}
p^{(1)} = (1) \xrightarrow{\alpha_{n-2}} p^{(2)} \xrightarrow{\alpha_n} \cdots \xrightarrow{\alpha_2} p^{(n-2)} \xrightarrow{\alpha_1} p^{(n-1)} \xrightarrow{\alpha_0} p^{(n)} = p, \\
p^{(n-i)} = S^{\alpha_{n-i}}_{n-i} p^{(n-i-1)},
\end{cases}
\]

(5)
where \( p^{(n-i)} \in S_{n-i} \) is generated from \( p^{(n-i-1)} \in S_{n-i-1} \) by the cyclic shift

\[
S_{n-i} : S_{n-i-1} \rightarrow S_{n-i}
\]

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

**Definition 1.** The sequence of exponents associated with successive cyclic shifts leading from \( (1) \in S_1 \) to \( p \in S_n \) is the code of \( p \) in the \( \varpi \)-system:

\[
\alpha = \alpha_{n-2} \cdots \alpha_0 \varpi \in \mathbb{Z}_n!.
\]

**Theorem 1.** 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 \( \varpi \)-system.

For example, the permutation \( p_{84} = (51324) \in S_5 \) is generated:

\[
(1) \xrightarrow{\alpha_3=1} (21) \xrightarrow{\alpha_2=1} (132) \xrightarrow{\alpha_1=0} (1324) \xrightarrow{\alpha_0=4} (51324).
\]

Its code is \( 1104_{\varpi} = 84 \).

**Proof.** We use induction on \( n \). For \( n = 2 \), in \( S_2 = \{(12), (21)\} \), 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 \( p = p_\alpha \in S_n \) of rank \( \alpha \), generated by cyclic shift from \( q = q_\beta \in S_{n-1} \) of rank \( \beta \). Then \( p = S_{\text{rank}} q \) for some \( \alpha_0 \in \mathbb{Z}_n, \alpha_0 \) being the rank of \( p \) within the orbit of \( q \). As the orbits contain \( n \) elements and as \( \beta \) is the rank of \( q \) in \( S_{n-1} \), the rank of \( p \) in \( S_n \) is

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

By induction hypothesis, the rank \( \beta \) of \( q \) is given by the code

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

For \( k = 1 \), Eq. (1) gives

\[
\varpi_{n,i+1} = \varpi_{n-1,i} \varpi_{n,1},
\]

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 \( p_\alpha \). Conversely, let \( p_\alpha \in S_n \). We write the rank \( \alpha \) in the \( \varpi \)-system, \( \alpha = \alpha_{n-2} \cdots \alpha_0 \varpi \), and use scheme (5) – from right to left – with the exponents \( \alpha_0, \ldots, \alpha_{n-2} \) to determine \( p_\alpha \).
We end the section by a package of algorithms performing the correspondence rank ↔ permutation of Theorem 1. Permutations are represented by strings indexed from 1. Algorithm C in Knuth generates $S_n$ by cyclic shift in a simple version of the scheme described in this section.

```
INT2Num(n, α) { conversion from integer to $\varpi$-system }
for i ← 0 to n – 2 do
    A[i] ← α mod (n – i)
    α ← α div (n – i)
end for
return A

NUM2Int(n, A) { conversion from $\varpi$-system to integer }
α ← 0
base ← 1
for i ← 0 to n – 2 do
    α ← α + A[i] * base
    base ← base * (n – i)
end for
return α

CIRC(m, k, p) { Circular permutation of exponent k on m symbols }
for i ← 1 to k do
    c ← p[1]
    for j ← 2 to m do
        p[j – 1] ← p[j]
    end for
    p[m] ← c
end for
return p

Pos(m, p) { Position of $x_m$ in a permutation $p$ on m symbols }
for j ← 1 to m do
    if p[j] = $x_m$ then
        return m – j
    end if
end for

PERM2Rank(n, p) { Find the rank of a given permutation p }
for i ← 0 to n – 2 do
    m ← n – i
    A[i] ← Pos(m, p)
    p ← CIRC(m, m – A[i], p)
end for
α ← NUM2Int(n, A)
return A

RANK2PERM(n, α) { Determine a permutation given its rank α }
A ← INT2Num(n, α)
```
\begin{verbatim}
p ← x_1
for i ← n - 2 downto 0 do
    m ← n - i
    p ← CIRC(m, A[i], p + x_m)
end for
return p
\end{verbatim}

**SetPerm(n) \{ Generation of the permutations on n symbols \}**

for \( \alpha \leftarrow 0 \) to \( n! - 1 \) do
    \( p \leftarrow \text{Rank2Perm}(n, \alpha) \)
end for

In the sequel, we assume that the set of permutations \( S_n \) is ordered according to generation by cyclic shift.

| \( \alpha \) | \( p_\alpha \) | \( \alpha_2 \) | \( \alpha_1 \) | \( \alpha_0 \) |
|---|---|---|---|---|
| 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.

### 4 \( k \)-orbits

In this section, structural properties of \( S_n \) are described using the \( \omega \)-system.
Proposition 2. Let \( k \in \{0, \ldots, n-2\} \) and \( p_\alpha \in S_n \) 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

\[
\alpha = \beta \varpi_{n,k} + \gamma, \quad \gamma \in \{0, \ldots, \varpi_{n,k} - 1\}.
\]

The code \( \beta \) is made of the \( n-k-1 \) leftmost digits of \( \alpha \), and \( \gamma \) is made of the \( k \) rightmost digits of \( \alpha \).

Proof. We have the decomposition

\[
\alpha = \alpha_{n-2} \cdots \alpha_0 = \alpha_{n-2} \cdots \alpha_k 0 \cdots 0_0 + 0 \cdots 0 \alpha_{k-1} \cdots \alpha_0 = \bar{\alpha} + \gamma.
\]

Let \( \beta_i = \alpha_{i+k} \) for \( i = 0, \ldots, n-k-2 \), so that the \( \beta \)'s are the \( n-k-1 \) leftmost digits of \( \alpha \). 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 \( q_\beta \in S_{n-k} \). Using relation \((1)\), we obtain

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

The term

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

is made of the \( k \) rightmost digits of \( \alpha \). 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 \((2)\). We obtain

\[
\alpha = \bar{\alpha} + \gamma = \beta \varpi_{n,k} + \gamma.
\]

\( \square \)

Definition 2. For \( k \in \{0, \ldots, n-2\} \), and \( q_\beta \in S_{n-k} \), the \( k \)-orbit of \( q_\beta \) in \( S_n \) is the subset

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

For \( k = 0 \), the 0-orbit of \( q \in S_n \) is \( \{ q \} \). Indeed, for \( k = 0 \), \( \varpi_{n,0} = 1 \), \( \gamma = 0 \), and \( p = p_\alpha \). For \( k \geq 1 \), a \( k \)-orbit \( \mathcal{O}_{n,k}(q) \) can be described as the subset of \( S_n \) generated from \( q \in S_{n-k} \) by \( k \) successive cyclic shifts. Indeed, by Proposition 2, 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 \( q_\beta \). By scheme \((5)\), the digits \( \alpha_{k-1}, \ldots, \alpha_0 \) describe the generation of \( p_\alpha \) from \( q_\beta \). In particular, for \( k = 1 \), the 1-orbit \( \mathcal{O}_{n,1}(q) \) of \( q \in S_{n-1} \) is the orbit \( \mathcal{O}(q) \). We may further define the \((n-1)\)-orbit \( \mathcal{O}_{n,n-1}(q) \) as the whole set \( S_n \), with \( q = (1) \in S_1 \).

We have the following generalization of Lemma 2.
Proposition 3. For \( k \in \{0, \ldots, n-2\} \), the set of permutations \( S_n \) is the disjoint union of the \( k \)-orbits \( O_{n,k}(q) \) for \( q \in S_{n-k} \).

Proof. The \( k \)-orbits are disjoint by uniqueness of the decomposition \( [5] \). They are in number \((n-k)!\) and contain \( \omega_{n,k} \) elements each. As \((n-k)!\omega_{n,k} = n! \) in \( \mathbb{N} \), the \( k \)-orbits span \( S_n \). \( \square \)

In decomposition \( [4] \), \( \beta \) specifies to which \( k \)-orbit \( p_\alpha \) belongs and \( \gamma \) specifies the rank of \( p_\alpha \) within the \( k \)-orbit. The first element of the \( k \)-orbit has rank \( \alpha^{\text{first}} = \beta \omega_{n,k} \) (i.e., \( \gamma = 0 \)). The last element has rank \( \alpha^{\text{last}} = \beta \omega_{n,k} + \omega_{n,k} - 1 \) (i.e., \( \gamma = \omega_{n,k} - 1 \)). The element next to the last has rank \( \alpha^{\text{last}} + 1 = \beta \omega_{n,k} + \omega_{n,k} = (\beta + 1) \omega_{n,k} \). It is the first element of the next \( k \)-orbit \( O_{n,k}(q_{\beta+1}) \), where \( q_{\beta+1} \) is the element next to \( q_\beta \) in \( S_{n-k} \).

Proposition 4. For \( k \in \{0, \ldots, n-2\} \), the digit \( \alpha_k \) of the code of \( p_\alpha \) is the rank of the \( k \)-orbit within the \((k+1)\)-orbit containing \( p_\alpha \).

For example, Table [1] shows that \( S_4 \) contains two 2-orbits within the 3-orbit \( S_4 \). The ranks 0, 1 of these 2-orbits in \( S_4 \) are specified by the digit \( \alpha_2 \).

Proof. The number of \( k \)-orbits within a \((k+1)\)-orbit is \( n-k \) (indeed, \((n-k)!/(n-(k+1))! = n-k \)). When performing \( \beta \to \beta + 1 \), the digit \( \beta_0 = \alpha_k \) ranges from 0 to \( n-k-1 \) in \( \mathbb{Z}_{n-k} \). It specifies the rank of the \( k \)-orbit within the \((k+1)\)-orbit. \( \square \)

Lemma 3. Let \( p_\alpha \in S_n \). There exists a largest \( k \in \{0, \ldots, n-2\} \) and \( q_\beta \in S_{n-k} \) such that \( p_\alpha \) is the last element of the \( k \)-orbit \( O_{n,k}(q_\beta) \), and not the last element of the \((k+1)\)-orbit containing this \( k \)-orbit.

Proof. If \( p_\alpha \) 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 last digit of \( p_\alpha \) 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 \( \alpha_k \neq n-i-1 \). This means that \( p_\alpha \) is the last element of nested \( j \)-orbits, \( j = 1, \ldots, k \). \( \square \)

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 \( [5] \), symbol \( x_{n-i} \) \( (i \geq 2) \) appears at step \( n-i \) with the digit \( \alpha_i \) as exponent of the cyclic shift. Its position in the generated permutation \( p^{(n-i)} \) is therefore

\[
\text{pos}_{n-i}(x_{n-i}, p^{(n-i)}) = \alpha_i.
\]

In particular,

\[
\text{pos}_n(x_n, p^{(n)}) = \alpha_0.
\]

For a permutation \( p = (a_1a_2\cdots a_{n-1}a_n) \in S_n \), we introduce the mirror image of \( p \), \( \overline{p} = (a_na_{n-1}\cdots a_2a_1) \).
Proposition 5. The permutations $p_\alpha$ and $p_{\alpha'}$ are the mirror image of one another if and only if

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

For example, in $\mathbb{Z}_5!$ we have $84 + 35 = -1$, and in $S_5$, $p_{84} = (51324)$ 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 $0 + 1 = -1$ in $\mathbb{Z}_2$. Let $n > 2$. By Proposition 6,

$$\alpha = \beta \omega_n, 1 + \alpha_0' \omega_n, \quad \alpha' = \beta' \omega_n, 1 + \alpha'_0 \omega_n, \quad q_\beta, q_{\beta'} \in S_{n-1}, \quad \alpha_0, \alpha'_0 \in \mathbb{Z}_n.$$  

By Corollary 1, the condition $\alpha + \alpha' = -1$ is equivalent to $\beta + \beta' = -1$ and $\alpha_0 + \alpha'_0 = -1$. By induction hypothesis, $q_\beta$ is the mirror image of $q_{\beta'}$ in $S_{n-1}$ 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 $\alpha_0$ and $\alpha'_0$ are symmetrical in $\mathbb{Z}_n$. As these ranks are the positions of symbol $x_n$ when $p_\alpha$ and $p_{\alpha'}$ are generated by cyclic shift from $q_\beta$ and $q_{\beta'}$ respectively, we obtain the result.

Corollary 2. The word constructed by concatenating the symbols of the permutations generated by cyclic shift is a palindrome.

Proof. Let $p_\alpha \in S_n$. The rank symmetrical to $\alpha$ in $\mathbb{Z}_n!$ is $(n! - 1) - \alpha = -(\alpha + 1)$. By Proposition 5 $p_{-(\alpha+1)}$ is the mirror image of $p_\alpha$.

The set $S_n$ has in fact deeper symmetries, coming from the recursive structure of the $k$-orbits.

According to Theorem 1, the generation of $S_n$ by cyclic shift is obtained by performing $\alpha \to \alpha + 1$ for $\alpha \in \mathbb{Z}_n!$, and writing $\alpha$ in the $\omega$-system. This determines each permutation $p_\alpha$. As $\alpha$ runs through $\mathbb{Z}_n!$, $p_\alpha$ runs through the $k$-orbits of $S_n$. For a fixed $k$, and by Proposition 6, $p_\alpha$ leaves a $k$-orbit to enter the next when, in the computation of $\alpha + 1$, the carry propagates up to the digit $\alpha_k$, incrementing the rank $\beta$ of the $k$-orbit. This occurs when $\alpha = \beta \omega_n, k + \omega_n, k - 1$.

Proposition 6. Any two successive permutations of $S_n$ are written as

$$p_\alpha = \overline{AB}, \quad p_{\alpha + 1} = BA,$$

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

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

For example, in $S_5$, $p_{39} = (54231\overline{1})$ and $p_{40} = (3\overline{1}245)$, with $39 = 0134_{\omega}$ and $40 = 0200_{\omega}$.

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

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

The result holds with $A = (a_1)$, $B = (a_2 \cdots a_n)$, and this corresponds to $k = 0$. Otherwise, by Lemma 3 there exists a largest $k \geq 1$ such that $p_\alpha$ 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 \(q_\beta \in S_{n-k}\). 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 \(S_{n-k}\) is generated by cyclic shift, \(q_{\beta+1} = C_{n-k} q_\beta\), with \(C_{n-k}\) the circular permutation in \(S_{n-k}\). We can now write

\[
\begin{align*}
p_\alpha &= (x_n \cdots x_{n-k+1} b_1 b_2 \cdots b_{n-k}) = AB \\
p_{\alpha+1} &= (b_2 \cdots b_{n-k} b_1 x_{n-k+1} \cdots x_n) = BA,
\end{align*}
\]

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

According to the Proposition, \(k + 1\) symbols have to be erased to the left of \(p_\alpha\) so that the last symbols of \(p_\alpha\) match the first symbols of \(p_{\alpha+1}\). We define the weight \(e_n(\alpha) \in \{1, \ldots, n-1\}\) of the transition \(\alpha \rightarrow \alpha + 1\) as the number of symbols of \(A\) in the above decomposition of \(p_\alpha\) and \(p_{\alpha+1}\).

We define the \(\varpi\)-ruler sequence as

\[
E_n = \{e_n(\alpha); \quad \alpha = 0, \ldots, n! - 2\}.
\]

**Proposition 7.** The \(\varpi\)-ruler sequence is a palindrome.

**Proof.** If the ranks of \(\alpha\) and \(\alpha'\) are symmetrical in \(\mathbb{Z}_n\), \(\alpha + \alpha' = -1\), and \(\alpha_i + \alpha'_i = -1\) for \(i = 0, \ldots, n - 2\) by Corollary [1]. By the definition of \(e_n(\alpha)\), we want to show that \(e_n(\alpha) = e_n(\alpha' - 1)\). If \(p_\alpha\) is the last element of a \(k\)-orbit, then \(\alpha_i = -1\) for \(i = 0, \ldots, k - 1\), so that \(\alpha'_i = 0\) for \(i = 0, \ldots, k - 1\): \(p_{\alpha'}\) 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 \(p_\alpha\) is not the last element of a \(k\)-orbit, then \(\alpha_0 \neq -1, \alpha'_0 \neq 0\), \(p_{\alpha'}\) is not the first element of a 1-orbit. In this case \(e_n(\alpha) = e_n(\alpha' - 1) = 1\). \(\square\)

**Proposition 8.** The number of terms of the \(\varpi\)-ruler sequence such that \(e_n(\alpha) = k\) is

\[
(n - k)(n - k)!.
\]

The sum of its \(n! - 1\) terms is

\[
W_n = 1! + 2! + \ldots + n! - n.
\]

**Proof.** We have \(e_n(\alpha) = k \geq 1\) if and only if \(p_\alpha\) 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 \(n - k + 1\) (see Proposition [4]). We exclude the last \((k - 1)\)-orbit, giving \(n - k\) possibilities. The number of \(k\)-orbits is \((n - k)!\) so that 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 \( n > 2 \),

\[
W_n = \sum_{k=1}^{n-1} k(n-k)(n-k)! = \sum_{k=0}^{n-2} (k+1)(n-1-k)(n-1-k)!
\]

\[
= \sum_{k=1}^{n-2} k(n-1-k)(n-1-k)! + \sum_{k=0}^{n-2} (n-1-k)(n-1-k)!
\]

\[
= W_{n-1} + \sum_{i=1}^{n-1} i.i! = 1! + \cdots + (n-1)! - (n-1) + n! - 1 = 1! + \cdots + n! - n.
\]

In the last line, we have used identity (1) and the induction hypothesis. \( \square \)

The \( \varpi \)-ruler sequence is analogous to the ruler sequence (sequence A001511 in Sloane [6]). The difference is that the number of intermediate ticks increases with \( n \) (Table 2).

| \( n \) | \( E_n \) |
|------|------|
| 2    | 1    |
| 3    | 1^2 21^2 |
| 4    | 1^3 21^3 31^3 21^3 21 |
| 5    | 1^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 21^4 |

Table 2: The \( \varpi \)-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 [7]). 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 \( \varpi \)-system corresponds to an Hamiltonian path in a weighted directed graph \( G_n \).

**Definition 3.** The vertices of the digraph \( G_n \) are the elements of \( S_n \). For two permutations (vertices) \( p_\alpha \) and \( p_\alpha' \), there is an arc from \( p_\alpha \) to \( p_\alpha' \) if and only if the last symbols of \( p_\alpha \) match the first symbols of \( p_\alpha' \) (there is no arc when there is no match). Let \( p_\alpha, p_\alpha' \in S_n \) 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 \( p_\alpha \) so that the last symbols of \( p_\alpha \) match the first symbols of \( p_\alpha' \).

By Proposition 3 for each \( \alpha \), there is an arc of weight \( e_n(\alpha) = f_n(\alpha, \alpha + 1) \) joining \( p_\alpha \) to \( p_{\alpha+1} \). This allows to define the Hamiltonian path

\[
w_n = \{(p_\alpha, p_{\alpha+1}); \ \alpha = 0, \ldots, n! - 2\} \]
joining successive permutations. This path has total weight $W_n = 1! + \ldots + n! - n$ by Proposition 8. The path $w_n$ 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 $n - 1$:

\[(x_n \cdots x_2x_1) \xrightarrow{n-1} (x_1x_2 \cdots x_n).\]

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

Table 3 displays the weighted adjacency matrix of the digraph $G_4$ and the Hamiltonian path $w_4$.

|    | 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 | 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 | 2 | 0 | 0 | 3 | 0 | 0 | 3 |
| 2  | 2 | 3 | 0 | 1 | 3 | 0 | 0 | 0 | 2 | 3 | 0 | 3 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 |
| 3  | 1 | 2 | 3 | 0 | 2 | 3 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 |
| 4  | 0 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 2 | 3 |
| 5  | 0 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 |
| 6  | 0 | 2 | 3 | 0 | 2 | 3 | 0 | 1 | 3 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 |
| 7  | 3 | 0 | 0 | 0 | 1 | 2 | 3 | 0 | 2 | 3 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 |
| 8  | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 1 | 2 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 |
| 9  | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 2 |
| 10 | 0 | 0 | 0 | 0 | 2 | 3 | 0 | 0 | 2 | 3 | 0 | 1 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 |
| 11 | 2 | 3 | 0 | 0 | 1 | 2 | 3 | 0 | 3 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 | 0 |
| 12 | 0 | 0 | 2 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 1 | 2 | 3 | 0 | 0 | 0 | 3 | 0 | 0 |
| 13 | 0 | 3 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 |
| 14 | 3 | 0 | 0 | 0 | 3 | 0 | 2 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 | 3 | 0 |
| 15 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 | 3 | 0 |
| 16 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 |
| 17 | 3 | 0 | 0 | 2 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 | 0 |
| 18 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 2 | 3 | 0 | 2 | 3 | 0 | 1 | 3 | 0 | 0 |
| 19 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 1 | 2 | 0 | 0 | 3 | 0 |
| 20 | 0 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 3 | 0 |
| 21 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 2 | 0 | 0 | 3 | 0 | 0 | 1 | 2 | 3 | 0 |
| 22 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 2 | 3 | 0 | 0 | 3 | 0 | 1 | 2 | 3 | 0 |
| 23 | 3 | 0 | 0 | 0 | 3 | 0 | 0 | 3 | 0 | 0 | 2 | 3 | 0 | 0 | 3 | 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. Bold entries on the upper diagonal indicate the Hamiltonian path corresponding to the \(\varepsilon\)-system code, and forming the \(\varepsilon\)-ruler sequence.

Proposition 9. Each vertex of $G_n$ has exactly $j!$ in-arcs of weight $j$ and $j!$ out-arcs of weight $j$, $j = 1, \ldots, n - 1$. Hence the vertices of $G_n$ have $L = 1! + \cdots + (n - 1)!$ as in- and out-degree, and $G_n$ is $L$-regular.

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

\[(a_1 \cdots a_jb_1 \cdots b_{n-j}) \xrightarrow{j} (b_1 \cdots b_{n-j}c_1 \cdots c_j),\]

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.

We conjecture that the Hamiltonian path $w_n$ joining successive permutations in the digraph $G_n$ is of minimal total weight. Assuming this conjecture we may state:

The \(\varepsilon\)-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 Acknowledgements

Marco Castera initiated the problem which motivated this study. Philippe Paclet discovered the weighted directed graph described in section 6.

References

[1] L. J. Fischer and K. C. Krause. 1812. Lehrbuch des Combinationslehre und der Arithmetik, Dresden.

[2] M. Hall and D. E. Knuth. 1965. Combinatorial analysis and computers. The American Mathematical Monthly, Vol. 72, No. 2, Part 2: Computers and Computing, 21-28.

[3] D. E. Knuth. 2005. The Art of Computer Programming, Vol. 4, Combinatorial Algorithms, Section 7.2.1.2, Generating All Permutations. Addison Wesley.

[4] C.-A. Laisant. 1888. Sur la numération factorielle, application aux permutations. Bulletin de la Société Mathématique de France, Vol. 16, 176–183.

[5] D. H. Lehmer. 1960. Teaching combinatorial tricks to a computer. Proc. Sympos. Appl. Math. Combinatorial Analysis, Amer. Math. Soc., Vol. 10, 179–193.

[6] Neil Sloane, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences

[7] C. Savage. 1997. A Survey of combinatorial Gray codes. SIAM Review, Vol. 39, Issue 4, 605–629.

2000 Mathematics Subject Classification: Primary 05A05.
Keywords: permutations, cyclic shift, number system, palindrome, combinatorial Gray code.