Generating the symmetric group by three prefix reversals

Saúl A. Blanco[a], Mikhail P. Golubyatnikov[b,c], Elena V. Konstantinova[d,e,f,*], Natalia V. Maslova[b,c], Luka A. Nikiforov[f]

[a] *Indiana University, 700 N Woodlawn Ave, Bloomington, IN 47408, USA*
[b] *Krasovskii Institute of Mathematics and Mechanics UB RAS, 16 S. Kovalevskaya Str., Yekaterinburg, 620077, Russia*
[c] *Ural Mathematical Center, 16 S. Kovalevskaya Str., Yekaterinburg, 620077, Russia*
[d] *Three Gorges Mathematical Research Center, China Three Gorges University, 8 University Avenue, Yichang 443002, Hubei Province, China*
[e] *Sobolev Institute of Mathematics, Ak. Koptyug av. 4, Novosibirsk 630090, Russia*
[f] *Novosibirsk State University, Pirogova Str. 2, Novosibirsk, 630090, Russia*

Abstract

The cubic pancake graphs are Cayley graphs over the symmetric group Sym_n generated by three prefix reversals. There is the following open problem: characterize all the sets of three prefix reversals that generate Sym_n. We present a partial answer to this problem, in particular, we characterize all generating sets of three elements that contain at least one of the prefix reversals r_2, r_3, r_{n-2}, and r_{n-1}. We also give some computational results relating to the diameter and the girth of some cubic pancake graphs.

Keywords: cubic pancake graph; prefix reversal; generating set; symmetric group

2010 MSC: 05C25, 05E15

1. Introduction

A classical and celebrated result [1] states that two random permutations of a set of n elements almost surely generate either the symmetric or the alternating group of degree n, and similar results hold when more generators are considered. In particular, the symmetric group can always be generated by the transposition $(1\ 2)$ together with the n-cycle $(1\ 2\ 3 \dots n)$, or by any set of $n-1$ transpositions. Two well-known generating sets of $n-1$ transpositions are the Coxeter generators $\{(i\ (i+1)) \mid 1 \leqslant i < n\}$ and the star generators $\{(1\ i) \mid 1 < i \leqslant n\}$, which give rise to two Cayley graphs known respectively as the *bubble-sort graph* and the *star graph* (see [2, 3, 4, 5]).

*Corresponding author

Email addresses: sblancor@iu.edu (Saúl A. Blanco), mike_ru1@mail.ru (Mikhail P. Golubyatnikov), e_konsta@ctgu.edu.cn (Elena V. Konstantinova), butterson@mail.ru (Natalia V. Maslova), l.nikiforov@g.nsu.ru (Luka A. Nikiforov)

The symmetric group Sym_n is also generated by a set of $n-1$ involutions known as *prefix reversals*, defined by

$$r_i = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & n \\ i & i-1 & \dots & 2 & 1 & i+1 & \dots & n \end{pmatrix}, \tag{1}$$

where $1 < i \leqslant n$. The action of r_i is to reverse the order of the first i elements while leaving the remaining $n-i$ elements fixed. Equivalently, r_i is the product of $\lfloor i/2 \rfloor$ disjoint transpositions, $r_i = (1\ i)(2\ (i-1)) \cdots (\lfloor i/2 \rfloor\ \lceil i/2 \rceil)$.

The Cayley graph generated by the set $\{r_2, r_3, \dots, r_n\}$ is called the *pancake graph*, denoted by $\mathcal{P}_n$. The pancake graph is famous because of the long-standing open problem, known as the *pancake problem*, which asks for the diameter of $\mathcal{P}_n$ [6]. The *girth* of a graph Γ refers to the length of the shortest cycle of Γ, and the *circumference* of Γ refers to the length of the largest cycle in Γ. Moreover, Γ is said to be *weakly pancyclic* if Γ has a cycle of length ℓ for all $g(\Gamma) \leqslant \ell \leqslant c(\Gamma)$, where $g(\Gamma)$ and $c(\Gamma)$ refer to the girth and circumference of Γ, respectively. Since the pancake graph is weakly pancyclic [7, 8] (in fact, a larger family of graphs that include $\mathcal{P}_n$, called the *generalized pancake graphs*, are known to be weakly pancyclic [9, 10]), this problem remains difficult to resolve.

Our interest lies in describing sets of three prefix reversals that generate the entire symmetric group Sym_n.

The importance of fixed-degree pancake graphs, in particular, cubic pancake graphs as models of networks was shown in [11]. The authors have considered cubic pancake graphs as induced subgraphs of the pancake graph $\mathcal{P}_n$ and have identified the following combinatorial necessary conditions for a triple of distinct prefix reversals $\{r_i, r_j, r_k\}$ to generate the symmetric group $\mathrm{Sym_n}$:

(1) One of the prefix reversals must be r_n, since otherwise no element can be moved to or from position n.

(2) One of the prefix reversals, say r_i, must satisfy $\lfloor n/2 \rfloor < i < n$, since otherwise if we take $g \in \langle r_n, r_j, r_i \rangle$ with $i < j \leqslant n/2$, and if $u < v \leqslant j$ then either $g(u) \leqslant n/2$ and $g(v) \leqslant n/2$ or $g(u) > n/2$ and $g(v) > n/2$. Thus, in this case, 2-transitivity is lost, while $\mathrm{Sym_n}$ is known to be 2-transitive for each n. Moreover, if n is odd, then $i > \lceil n/2 \rceil$ since otherwise $\lceil n/2 \rceil$ will remain fixed.

(3) At least one prefix reversal must have an even index, since otherwise no element can be moved from an odd-numbered position to an even-numbered position.

(4) At least one prefix reversal must be an odd permutation, since otherwise the generated group consists only of even permutations.

(5) The generating set must contain at least two prefix reversals with relatively prime indices. Otherwise, if $\gcd(i, j, k) = \ell > 1$, then the elements of $\{1, 2, \dots, n\}$ are partitioned into blocks of ℓ consecutive positions that can never be separated. In particular, not all indices can be even.

Using these necessary conditions, in [11] it was shown that the symmetric group is generated by the following six sets: $\{r_n, r_{n-1}, r_2\}$ for any $n \geqslant 4$; $\{r_n, r_{n-1}, r_3\}$ for any odd $n \geqslant 5$; $\{r_n, r_{n-1}, r_{n-2}\}$ for any $n \geqslant 4$; $\{r_n, r_{n-1}, r_{n-3}\}$ for any odd $n \geqslant 4$; $\{r_n, r_{n-2}, r_3\}$ for any even $n \geqslant 6$; and $\{r_n, r_{n-2}, r_{n-3}\}$ for any $n \geqslant 5$. The authors have used the following approach. For each of the sets above, it was shown that the set can simulate the three generators of the shuffle-exchange permutation network generated by the following three permutations written in cycle notation: $(n\ 1\ 2\ \ldots\ n-1)$ (right shuffle), $(2\ 3\ \ldots\ n\ 1)$ (left shuffle), and $(1\ 2)$ (transposition of the first two elements). Using the same approach, it was shown in [12] that the set $\{r_n, r_{n-2}, r_2\}$ for any odd $n \geqslant 5$ is also a generating set of the symmetric group.

The set $\{r_n, r_{n-1}, r_{n-2}\}$ is known as Big-3 flips, and the corresponding cubic pancake graph generated by this set is called the Big-3 pancake network [13] for which it was conjectured that there exists a cyclic Gray code. The girths and the diameters of the cubic pancake graphs generated by the above seven sets were studied in [14] and [15].

1.1. Our contributions

In this paper, we focus on the following three problems.

Problem 1. *Are there other generating sets of three prefix reversals for the symmetric group?*

Problem 2. *What are other necessary conditions for the set of three prefix reversals to generate the symmetric group?*

Problem 3. *What are sufficient conditions for the set of three prefix reversals to generate the symmetric group?*

In addressing the above problems, we prove the following Theorem.

MAIN THEOREM. The following statements hold.

(1) *Let* $2 \leqslant k < n - l < n$ *and* n *be sufficiently large. If* $l \geqslant 2k + 1$ *then* $\langle r_n, r_{n-l}, r_k \rangle < \mathrm{Sym_n}$.

(2) *Let* $n \geqslant 6$ *and* $l \geqslant k + 1$. *If* l *divides* $n + 1$ *then* $\langle r_n, r_{n-l}, r_k \rangle < \mathrm{Sym_n}$.

(3) *The set* $\{r_n, r_m, r_2\}$, *with* $2 < m < n$ *and* $n \geqslant 4$, *generates* $\mathrm{Sym_n}$ *if and only if one of the following conditions holds*:

- (*i*) n *is even and* $m = n - 1$;
- (*ii*) n *is odd and*
  - (*a*) $m \in \{n - 1, n - 2\}$ *if* $n \equiv 2 \pmod 3$ *or if* $n \equiv 0 \pmod 3$;
  - (*b*) $m \in \{n - 3, n - 2, n - 1\}$ *if* $n \equiv 1 \pmod 3$.

(4) *The set* $\{r_n, r_m, r_3\}$, *with* $3 < m < n$ *and* $n \geqslant 5$, *generates* $\mathrm{Sym_n}$ *if and only if one of the following conditions holds*:

(*i*) n *is even and* $m = n - 2$;

(*ii*) $m \in \{n-3, n-1\}$ *and* $n \equiv 1, 5 \pmod 6$;

(*iii*) $m = n - 1$ *if* $n \equiv 3 \pmod 6$.

(5) *The set* $\{r_n, r_{n-1}, r_k\}$*, with* $2 \leqslant k \leqslant n-2$*, generates* $\mathrm{Sym_n}$ *if and only if one of the following conditions holds:*

(*i*) *If* n *is even and* k *is even;*

(*ii*) $n \equiv 3 \pmod 4$ *and* $2 \leqslant k \leqslant n-2$*;*

(*iii*) $n \equiv 1 \pmod 4$ *and* $k \equiv 2, 3 \pmod 4$.

(6) *The set* $\{r_n, r_{n-2}, r_k\}$*, with* $2 \leqslant k < n-2$ *and* $n \geqslant 5$*, generates* $\mathrm{Sym_n}$ *if and only if* k *and* n *are of different parity.*

The organization of the rest of the paper is as follows. In Section 2, we describe group theory techniques, including some developed by the authors, that provide necessary and sufficient conditions for $\{r_n, r_m, r_k\}$ to generate $\mathrm{Sym_n}$. In Section 3, we present our main results relating to triples of prefix reversals that generate $\mathrm{Sym_n}$. Lastly, in Section 4, we discuss some computational results relating to the cubic pancake graphs such as their diameters, girths, and hamiltonicity, and formulate conjectures for future research.

2. Preliminaries

The following notation is used. Let Ω denote the set $\{1, 2, \ldots, n\}$, and let $\mathrm{Sym_n}$ and $\mathrm{Alt_n}$ denote the symmetric group and alternating group of degree n, respectively. For $\sigma, \pi \in \mathrm{Sym_n}$, we compose them using right-to-left multiplication, so $\sigma\pi(i) = \sigma(\pi(i))$, for all $1 \leqslant i \leqslant n$.

We now proceed to describe some tools from group theory that will be needed in the proofs of our results. Let G be a finite group acting on a finite set Ω. The *G-orbit of $x \in \Omega$*, or simply the *orbit of x*, refers to the set $\{g(x) : g \in G\}$. The action is said to be *transitive* on Ω if for each $x, y \in \Omega$ there is $g \in G$ such that $g(x) = y$. A nonempty subset $B \subseteq \Omega$ is called a *block of imprimitivity* (or simply a *block*) for the action if for every $g \in G$ either $g(B) = B$ or $g(B) \cap B = \varnothing$, where $g(B) = \{g(b) : b \in B\}$. Moreover, the family $\{g(B) : g \in G\}$ of translates of a block B forms a G-invariant partition of Ω, called a *block system*. There are at least two block systems for every action: $\{x\}$ for $x \in \Omega$ and Ω itself, and one refers to these as *trivial blocks*. The action of G on Ω is *primitive* if it is transitive and the only blocks are the trivial ones. Otherwise, a transitive action is said to be *imprimitive*. Additionally, if H is a proper subgroup of G, we write $H < G$.

In our proofs, we utilize a few results from group theory regarding generating sets of $\mathrm{Sym_n}$.

Lemma 1 ([16, Theorem 13.3]). *Let $H \leqslant Sym(\Omega) = \mathrm{Sym_n}$ be a permutation group acting naturally on the set $\Omega = \{1, \dots, n\}$ such that there exists a transposition $h \in H$. Then $H = Sym(\Omega)$ if and only if H is primitive on Ω.*

The following fact is well-known, see, for example, [17, Theorem 1.1].

Lemma 2. *$H = \langle (1\ 2 \dots\ n), (a\ b) \rangle = \mathrm{Sym_n}$, $1 \leqslant a < b \leqslant n$, if and only if $\gcd(b - a, n) = 1$.*

A more general result relating to generating sets of $\mathrm{Sym_n}$ formed by one n-cycle and one transposition is proved in [18].

Lemma 3 ([18, Corollary 4]). *Let σ be an n-cycle and $\tau = (a\ b)$ be a transposition. Let q be an integer satisfying $\sigma^q(a) = b$. Then $\langle \sigma, \tau \rangle = \mathrm{Sym_n}$ if and only if $\gcd(q, n) = 1$.*

The following result proved in [17] is also used in our proofs.

Lemma 4 ([17, Theorem 1.3]). *Let G be the permutation subgroup of $\mathrm{Sym_n}$ generated by the n-cycle $(1\ 2\ \dots\ n)$ and the 3-cycle $(a\ b\ c)$ with $1 \leqslant a < c < b \leqslant n$. Then,*

(i) If n is even, then $G = \mathrm{Sym_n}$ if and only if $\gcd(b - a, c - a, n) = 1$.

(ii) If n is odd, then $G = \mathrm{Alt_n}$ if and only if $\gcd(b - a, c - a, n) = 1$.

We furthermore develop tools to detect when the action of $\langle r_n, r_m, r_k \rangle$ on Ω is intransitive, from which it follows that $\langle r_n, r_m, r_k \rangle < \mathrm{Sym_n}$.

2.1. Intransitive actions

Proposition 1. *Let $H = \langle r_n, r_{n-l}, r_k \rangle$ for a sufficiently large n and $1 < k < n - l$. If $l \geqslant 2k + 1$, then $H < \mathrm{Sym_n}$.*

Proof. Let

$$\Phi = \{1, \dots, k\} \cup r_n(\{1, \dots, k\}) = \{1, \dots, k\} \cup \{n - k + 1, \dots, n\}.$$

Then $|\Phi| = 2k$ and Φ is an $\langle r_n, r_k \rangle$-orbit. Let

$$\Delta = \{t : t \equiv s \pmod{l} \text{ for } s \in \Phi\}.$$

We claim that Δ is a proper H-invariant subset of Ω (i. e. Δ is a union of H-orbits). Indeed, let $x \equiv s \pmod{l}$, where $s \in \Phi$. We have $x = s + w \cdot l$ for some w and $r_n(x) = n - x + 1 = n - s + 1 - w \cdot l \equiv n - s + 1 \pmod{l}$, and $n - s + 1 = r_n(s) \in \Phi$. If $x \leqslant k$ then $r_k(x) = k + 1 - x = k - s + 1 - w \cdot l \equiv k - s + 1 \pmod{l}$, and $k - s + 1 = r_k(s) \in \Phi$; if $x > k$ then $r_k(x) = x$. If $x \leqslant n - l$ then $r_{n-l}(x) = n - x - l + 1 \equiv r_n(x) \pmod{l}$, otherwise $r_{n-l}(x) = x$. Thus, Δ is a union of H-orbits. Moreover, since $|\Phi| < l$, we see that Δ is a proper subset of Ω. Thus, $H < \mathrm{Sym_n}$. □

Proposition 2. *Let $H = \langle r_n, r_{n-l}, r_k \rangle$ for $n \geqslant 6$ and $l \geqslant k+1$. If l divides $n+1$, then*

$$\Delta = \{t : l \text{ divides } t\}$$

is a proper H-invariant subset of Ω (i. e. Δ is a union of H-orbits), therefore $H < \mathrm{Sym_n}$.

Proof. If l divides $n+1$ and l divides i, then $r_k(i) = i$, l divides $r_n(i) = n-i+1$ and l divides $r_{n-l}(i) = n-l-i+1$. □

Since r_k for $k \in \{2,3\}$ is a transposition, by Lemma 1 we have $H = \mathrm{Sym_n}$ if and only if H is primitive on Ω. The following two lemmas are useful to establish which actions of the groups of the form $\langle r_n, r_m, r_k \rangle$, with $k < m < n$ and $k \in \{2,3\}$ acting naturally on Ω, are transitive.

Lemma 5. *If the set $\{r_n, r_m, r_2\}$, $2 < m < n$, generates $\mathrm{Sym_n}$, $n \geqslant 7$, then $m \geqslant n-4$. Furthermore, if n is odd, then $m \geqslant n-3$.*

Proof. We prove that $\langle r_n, r_m, r_2 \rangle$ acting on Ω cannot be transitive if $n - m \geqslant 4$. Indeed, one can compute that the orbit of 1 under the natural action of $\langle r_n, r_m, r_2 \rangle$ has the form

$$\{n-1, n\} \cup \{a(n-m)+1, a(n-m)+2\} \cup \{(b+1)m - bn - 1, (b+1)m - bn\},$$

with $a, b \in \mathbb{Z}$.

Therefore, the orbit contains elements that are congruent to at most four integers: $1, 2, m$, and $m-1$ modulo $n-m$. Thus, if $n - m \geqslant 5$, the action cannot be transitive.

Now, if $n-m = 4$, then the set $\{a(n-m)+1, a(n-m)+2\}$ gives the integers congruent to 1 and 2 modulo 4 in the orbit of 1. Since $(b+1)(n-4) - bn = n - 4(b+1)$ and $(b+1)(n-4) - bn - 1 = n - 4(b+1) - 1$, if we are to have integers that are also congruent to 0 and 3 modulo 4 in the orbit of 1 then n must be a multiple of 4. Hence, if n is odd and $m = n-4$, then $\langle r_n, r_m, r_2 \rangle$ is intransitive on Ω. □

Remark 1. *Notice that if $m = n-3$ and $n \equiv 2, 5 \pmod 6$ then the elements of the set $\{1, 2, m, m-1\}$ are congruent to 2 or 1 modulo 3. Therefore, if $m = n-3$ and $n \equiv 2, 5 \pmod 6$ then $\langle r_n, r_{n-3}, r_2 \rangle < \mathrm{Sym_n}$ since the orbit of 1 does not contain any multiple of 3.*

Similarly, we have the following lemma.

Lemma 6. *If the set $\{r_n, r_m, r_3\}$, $3 < m < n$, generates $\mathrm{Sym_n}$, $n \geqslant 8$, then $m \geqslant n-4$. Furthermore, if n is odd, then $m \geqslant n-3$.*

Proof. The proof is similar to that of Lemma 5. In this case, the orbit of 1 has the following form:

$$\{n-2, n\} \cup \{a(n-m)+1, a(n-m)+3\} \cup \{(b+1)m - bn - 2, (b+1)m - bn\},$$

where $a, b \in \mathbb{Z}$. These elements are congruent to one of the elements of $\{1, 3, m, m-2\}$ modulo $n-m$. □

Remark 2. *If n is odd and $m = n-4$, then notice the elements in $\{1, 3, m, m-2\}$ are congruent to 1 or 3 modulo $n - m = 4$. Therefore, $\langle r_n, r_{n-4}, r_3\rangle < \mathrm{Sym_n}$ if n is odd, as the orbit of 1 under the action of $\langle r_n, r_{n-4}, r_3\rangle$ does not contain any even integers.*

Having described the necessary lemmas, we are now ready to state and prove our main results.

3. Main results

The following special cases are used in the proofs in this section.

Special Case 1 (See [11]). *$H = \langle r_n, r_{n-1}, r_2\rangle = \mathrm{Sym_n}$ for any $n \geqslant 4$.*

Special Case 2 (See [12]). *$H = \langle r_n, r_{n-2}, r_2\rangle = \mathrm{Sym_n}$ for any odd $n \geqslant 5$.*

Special Case 3 (See [11]). *$H = \langle r_n, r_{n-2}, r_3\rangle = \mathrm{Sym_n}$ for any even $n \geqslant 6$.*

In the rest of the section, these special cases are extended.

3.1. Case $k \in \{2, 3\}$

Proposition 3. *The set $\{r_n, r_m, r_2\}$, where $2 < m < n$ and $n \geqslant 4$, generates $\mathrm{Sym_n}$ if and only if*

(i) n is even and $m = n - 1$, or

(ii) n is odd and

(a) $m \in \{n-1, n-2\}$ if $n \equiv 2 \pmod 3$ or if $n \equiv 0 \pmod 3$, or

(b) $m \in \{n-3, n-2, n-1\}$ if $n \equiv 1 \pmod 3$.

Proof. The cases with $n \leqslant 7$ are easily verified to hold. So we shall assume that $n \geqslant 7$. The sufficient condition for the case $m = n - 2$ is given by Special Case 2, and the sufficient condition for the case $m = n - 1$ is given by Special Case 1. Thus, we can assume that $m \leqslant n - 3$.

If n is even, then since $m \geqslant n - 4$ by Lemma 5 and not all three prefix reversals can have an even index if they generate $\mathrm{Sym_n}$ (see Observation (5) in the Introduction), the only possible value for m is $n - 3$. If n is odd, then by Lemma 5, $m \geqslant n - 3$. Thus, all that remains is the case $m = n - 3$.

If $n \equiv 0 \pmod 3$ then the set

$$\mathcal{B}_a = \{3a + b : 1 \leqslant b \leqslant 3\} \text{ with } 0 \leqslant a \leqslant n/3 - 1$$

forms a non-trivial block system of $\langle r_n, r_{n-3}, r_2\rangle$ acting on Ω. Hence, by Lemma 1, $\langle r_n, r_{n-3}, r_2\rangle < \mathrm{Sym_n}$.

If $n \equiv 2, 5 \pmod 6$ then Remark 1 gives that $\langle r_n, r_{n-3}, r_2\rangle < \mathrm{Sym_n}$.

If $n \equiv 4 \pmod 6$ then the set

$$\mathcal{B}_b = \{6a + b, 6a + b + 1, 6a + b + 2 : a \geqslant 0\} \text{ with } b \in \{0, 3\}$$

forms a non-trivial block system of $\langle r_n, r_{n-3}, r_2\rangle$ acting on Ω. Therefore $\langle r_n, r_{n-3}, r_2\rangle < \mathrm{Sym_n}$.

If $n \equiv 1 \pmod 6$ then $r_n r_{n-3} r_2$ is the n-cycle:

$$\sigma = (1\ 5\ 8\ 11\ \ldots\ (6s-1)\ 3\ 6\ 9\ 12\ \ldots\ 6s\ 2\ 4\ 7\ 10\ 13\ \ldots (6s+1)),$$

where $s = \lfloor n/6 \rfloor$. Notice that $\sigma^{4s}(1) = 2$, and $\gcd(4s, n) = \gcd(4s, 6s+1) = 1$. Moreover, since $r_2 = (1\ 2)$ it follows that $\langle r_n, r_{n-3}, r_2\rangle = \mathrm{Sym_n}$ by Lemma 3. □

Proposition 4. *The set* $\{r_n, r_m, r_3\}$, *with* $3 < m < n$ *and* $n \geqslant 5$, *generates* $\mathrm{Sym_n}$ *if and only if*

(i) n *is even and* $m = n-2$, *or*

(ii) $m \in \{n-3, n-1\}$ *and* $n \equiv 1, 5 \pmod 6$, *or*

(iii) $m = n-1$ *if* $n \equiv 3 \pmod 6$.

Proof. The cases $n \leqslant 8$ are easily verified by direct computation.

By Lemma 6, it follows that $m \geqslant n-4$. Notice that *(i)* is given by Special case 3. Let us consider the case $m = n-4$ and n even, for which we show that $\langle r_n, r_{n-4}, r_3\rangle < \mathrm{Sym_n}$. Notice that n must be congruent to 0 or 2 modulo 4. If $n \equiv 0 \pmod 4$ then the set

$$\mathcal{B}_a = \{4a+1, 4a+2, 4a+3, 4a+4\} \text{ with } 0 \leqslant a \leqslant n/4 - 1$$

forms a non-trivial block system of $\langle r_n, r_{n-4}, r_3\rangle$ acting on Ω.

Additionally, if $n \equiv 6 \pmod 8$ then the set

$$\mathcal{B}_1 = \{8a + b : a \geqslant 0 \text{ and } 0 \leqslant b \leqslant 3\}$$

along with the set

$$\mathcal{B}_2 = \{8a + b : a \geqslant 0 \text{ and } 4 \leqslant b \leqslant 7\}$$

form a non-trivial block system of $\langle r_n, r_{n-4}, r_3\rangle$ acting on Ω.

Finally, if $n \equiv 2 \pmod 8$ then the set

$$\mathcal{B}_1 = \{8a + d : a \geqslant 0 \text{ and } b \in \{1, 3, 4, 6\}\}$$

along with the set

$$\mathcal{B}_2 = \{8a + d : a \geqslant 0 \text{ and } b \in \{0, 2, 5, 7\}\}$$

form a non-trivial block system of $\langle r_n, r_{n-4}, r_3\rangle$ acting on Ω.

Thus, $\langle r_n, r_{n-4}, r_3\rangle < \mathrm{Sym_n}$ by Lemma 1.

Now, let us suppose that n is odd, and by Lemma 6, it follows that $m \geqslant n-3$. Additionally, m cannot be $n-2$ since then r_3, r_m, and r_n would all have an odd index. So the only remaining values to consider are $m = n-1$ and $m = n-3$.

Notice that $r_n r_{n-1} = (1\ 2 \ldots n-1\ n)$ and $r_3 = (1\ 3) \in \langle r_n, r_{n-1}, r_3 \rangle$. Now, Lemma 2 gives that $\langle r_n r_{n-1}, r_3 \rangle = \mathrm{Sym_n}$, therefore $\{r_n, r_{n-1}, r_3\}$ generates $\mathrm{Sym_n}$.

Moreover, if $n \equiv 3 \pmod 6$ then $\{r_n, r_{n-3}, r_3\}$ cannot generate $\mathrm{Sym_n}$ since $\gcd(n, n-3, 3) = 3$ (see Observation (5) in the Introduction).

We are now only left with the cases $n \equiv 1, 5 \pmod 6$ and $m = n-3$.

If $n \equiv 1 \pmod 6$ then $r_n r_{n-3} r_3$ is the n-cycle:

$$\sigma_1 = (1\ 6\ 9\ 12\ \ldots\ 6s\ 2\ 5\ 8\ 11\ \ldots\ (6s-1)\ 3\ 4\ 7\ 10\ \ldots\ (6s+1)),$$

where $s = \lfloor n/6 \rfloor$. Notice that $\sigma_1^{4s}(1) = 3$ and that $\gcd(4s, n) = \gcd(4s, 6s+1) = 1$. Therefore, since $r_3 = (1\ 3)$, the set $\{r_n, r_{n-3}, r_3\}$ generates $\mathrm{Sym_n}$ by Lemma 3.

Similarly, if $n \equiv 5 \pmod 6$ then $r_n r_{n-3} r_3$ is the n-cycle:

$$\sigma_2 = (1\ 6\ 9\ 12\ \ldots\ (6s+3)\ 3\ 4\ 7\ 10\ \ldots\ (6s+4)\ 2\ 5\ 8\ 11\ \ldots\ (6s+5)),$$

where $s = \lfloor n/6 \rfloor$. As before, $\sigma_2^{2s+1}(1) = 3$ and $\gcd(2s+1, n) = \gcd(2s+1, 6s+5) = 1$. Hence, $\{r_n, r_{n-3}, r_3\}$ generates $\mathrm{Sym_n}$ in this case as well by Lemma 3. This concludes the proof. □

3.2. Case $m = n-1$

Proposition 5. *Let $H = \langle r_n, r_{n-1}, r_k \rangle$, where $2 \leqslant k \leqslant n-2$ and $n \geqslant 4$. Then $H = \mathrm{Sym_n}$ if and only if*

(*i*) *n is even and k is even, or*

(*ii*) *$n \equiv 3 \pmod 4$ and $2 \leqslant k \leqslant n-2$, or*

(*iii*) *$n \equiv 1 \pmod 4$ and $k \equiv 2, 3 \pmod 4$.*

Proof. Consider the following two permutations:

$$L = (1\ 2 \ldots n-1\ n) = r_n r_{n-1} = R^{-1},$$
$$R = (n\ n-1 \ldots 2\ 1) = r_{n-1} r_n = L^{-1}.$$

By direct computations, we obtain the following 3-cycle:

$$\sigma = r_k \cdot L \cdot r_k \cdot L \cdot r_k \cdot R \cdot r_k \cdot R = (1\ k\ k+2).$$

Let

$$d = \gcd(k-1, k+1, n) = \gcd(2, k+1, n) = \begin{cases} 1, & \text{if } n \text{ is odd;} \\ 1, & \text{if } n \text{ is even and } k \text{ is even;} \\ 2, & \text{if } n \text{ is even and } k \text{ is odd.} \end{cases}$$

Let $H_1 = \langle L, \sigma \rangle \leqslant H$. By Lemma 4, $H_1 \geqslant \mathrm{Alt}_n$ if and only if $d = 1$. In the case $d = 2$, H_1 is imprimitive.

If n is odd, then $H_1 \geqslant \mathrm{Alt}_n$. If $n \equiv 3 \pmod 4$ then $r_n \in \mathrm{Sym_n} \setminus \mathrm{Alt}_n$, and therefore, $H_1 < H = \mathrm{Sym_n}$. If $n \equiv 1 \pmod 4$ then $r_n \in \mathrm{Alt}_n$ and $r_{n-1} \in \mathrm{Alt}_n$, and $r_k \notin \mathrm{Alt}_n$ if and only if $k \equiv 2, 3 \pmod 4$.

If both n and k are even then $H \geqslant H_1 = \mathrm{Sym_n}$ by Lemma 4.

It remains to show that in the case of even n and odd k, the group H is imprimitive. Let $D = \langle L, r_n \rangle \leqslant H_1 \leqslant H$. Then D is isomorphic to the dihedral group D_{2n} of order $2n$, and we claim that

$$\mathcal{B}_1 = \{t \mid t \equiv 1 \pmod 2\} \text{ and } \mathcal{B}_2 = \{t \mid t \equiv 0 \pmod 2\}$$

are blocks of imprimitivity of D. Indeed, $L(\mathcal{B}_i) = \mathcal{B}_j$ and $r_n(\mathcal{B}_i) = \mathcal{B}_j$ for $j \in \{1, 2\} \setminus \{i\}$. Now we claim that r_k and r_{n-1} also preserve blocks $\mathcal{B}_1$ and $\mathcal{B}_2$. Indeed, since both k and $n-1$ are odd then $r_k(\mathcal{B}_i) = \mathcal{B}_i$ and $r_{n-1}(\mathcal{B}_i) = \mathcal{B}_i$ for each $i \in \{1, 2\}$. Thus, $\{\mathcal{B}_1, \mathcal{B}_2\}$ is a non-trivial block system of H acting on Ω, and so $H < \mathrm{Sym_n}$. □

3.3. Case $m = n - 2$

Proposition 6. *Let $H = \langle r_n, r_{n-2}, r_k \rangle$, with $2 \leqslant k < n - 2$ and $n \geqslant 5$. Then $H = \mathrm{Sym_n}$ if and only if n and k are of different parities.*

Proof. The cases $k = 2, 3$ were already handled in Propositions 3 and 4, respectively. Therefore, one can assume that $k > 3$. We first establish the sufficient statement. Suppose n is even and k is odd. Then H contains the following n-cycle:

$$r_{n-2}r_n = (n\ n-2\ n-4 \ldots 2\ n-1\ n-3 \ldots\ 3\ 1).$$

It can be shown by direct computations and an easy inductive argument that the following two equations hold:

$$(r_{n-2}r_n)^{\frac{k-3}{2}} r_k = (1\ 3)\underbrace{(\ldots\ldots\ldots\ldots\ldots)}_{(n-3)\text{-cycle}},$$

$$((r_{n-2}r_n)^{\frac{k-3}{2}} r_k)^{n-3} = (1\ 3).$$

Thus, having the n-cycle $r_{n-2}r_n$ and the transposition $(1\ 3)$ that swaps two adjacent entries in this cycle, by Lemma 3, we have $H = \mathrm{Sym_n}$.

Now, let us assume that n is odd and k is even. Then we have:

$$r_{n-2}r_n = (n\ n-2\ n-4 \ldots 1)(n-1\ n-3 \ldots 2)$$

and by similar arguments as above we obtain:

$$(r_{n-2}r_n)^{\frac{k-2}{2}} r_k = (1\ 2)\underbrace{(\ldots\ldots\ldots\ldots\ldots)}_{(n-2)\text{-cycle}},$$

$$((r_{n-2}r_n)^{\frac{k-2}{2}} r_k)^{n-2} = (1\ 2).$$

Since the lengths of the two cycles in the permutation $r_{n-2}r_n$ are coprime as they differ exactly by 1, it follows that for any odd a and even b there is $m \in \mathbb{N}$

such that $(r_n r_{n-2})^m (1\ 2)(r_{n-2} r_n)^m = (a\ b)$. Thus, H contains all transpositions of two adjacent elements of a permutation, and therefore $H = \mathrm{Sym_n}$ (see [2]).

For the necessary statement, notice that if both n, k have the same parity, then all generators of H have indices that are all of the same parity. Therefore, by the combinatorial necessary conditions (3) and (5) in the Introduction, $H < \mathrm{Sym_n}$. This completes the proof. □

4. Conjectures and computational results

4.1. Generating sets

For a given n and a set $\{r_n, r_m, r_k\}$, $2 \leqslant k < m < n$, it is natural to ask the following question: which fraction of pairs $\{r_m, r_k\}$ along with r_n generate the entire Sym_n? From computational results of a numerical experiment over all pairs (m, k) for each $6 \leqslant n \leqslant 70$, we have the following conjecture.

Conjecture 1. *Let $f(n)$ be the number of pairs (m, k) such that $2 \leqslant k < m < n$ and $\langle r_n, r_m, r_k \rangle = \mathrm{Sym}_n$. Then*

$$f(n) = \begin{cases} \frac{1}{13} n^2 + O(n) & n = 0 \pmod 4; \\ \frac{1}{9} n^2 + O(n) & n = 1 \pmod 4; \\ \frac{1}{10} n^2 + O(n) & n = 2 \pmod 4; \\ \frac{1}{7} n^2 + O(n) & n = 3 \pmod 4. \end{cases}$$

Figure 1 illustrates this conjecture. The plot displays the values of the function $f(n)$ for all $n \leqslant 100$. Four distinct subsets are highlighted, each corresponding to a residue class of n modulo 4. For each subset, the best quadratic approximation with rational coefficients was computed using the Least Squares Method. For every fitted curve, the parameters of the quadratic function and the Root Mean Square Error (RMSE) metric are provided.

In addition, there seems to be a connection between the sets of triples generating the whole group of degree n modulo 4 and modulo 2. Based on results of computational experiments for $n \leqslant 100$ the following conjectures can be stated assuming that $2 \leqslant k < m < n$.

Conjecture 2. *If $\langle r_n, r_m, r_k \rangle = \mathrm{Sym}_n$ then $\langle r_{n+4}, r_{m+4}, r_{k+4} \rangle = \mathrm{Sym}_{n+4}$.*

Conjecture 3. *For any $n \equiv 0, 1 \pmod 4$, if $\langle r_n, r_m, r_k \rangle = \mathrm{Sym}_n$ then $\langle r_{n+2}, r_{m+2}, r_{k+2} \rangle = \mathrm{Sym}_{n+2}$.*

Conjecture 4. *If n is even and $m+k < n$ then $\langle r_n, r_m, r_k \rangle < \mathrm{Sym_n}$. Moreover, if n is odd and $m + k < n - 1$ then $\langle r_n, r_m, r_k \rangle < \mathrm{Sym_n}$.*

These conjectures arise naturally by visualizing the set of triples $\{r_n, r_m, r_k\}$ that generate the whole group for a fixed value of n. Indeed, in Figure 2 and

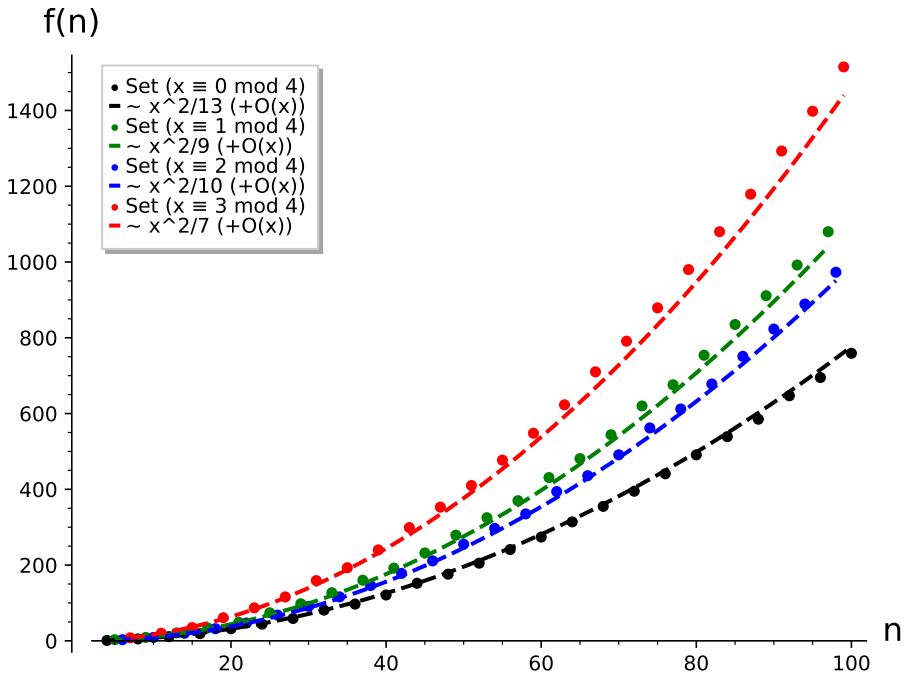

Figure 1: Visualization of Conjecture 1. The figure depicts the number $f(n)$ of pairs (m,k) so that $\langle r_n, r_m, r_k\rangle = \mathrm{Sym_n}$ for several values of n. Four colors are used representing the residue r of n modulo 4. The curves represent the best rational model $(x^2+ux+v)/q$:
$r=0$ (black): $q=13$, $u=-0.5$, $v=5$, RMSE $=3.343$;
$r=1$ (green): $q=9$, $u=5$, $v=-45$, RMSE $=12.132$;
$r=2$ (blue): $q=10$, $u=-1$, $v=0$, RMSE $=11.408$;
$r=3$ (red): $q=7$, $u=3$, $v=-14$, RMSE $=38.677$.

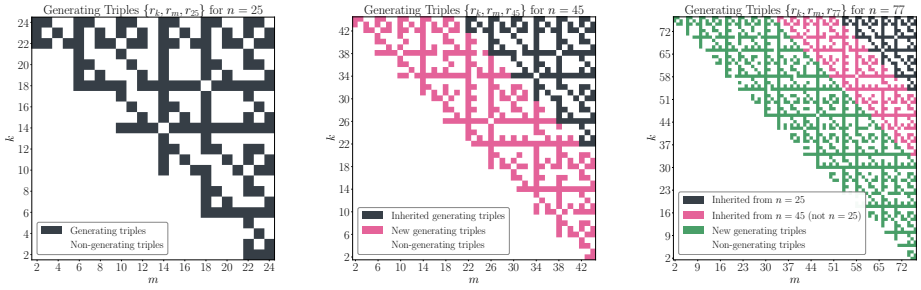

Figure 2: Visualization of Conjecture 2 to illustrate that as n grows, the previous triples are "preserved" (mod 4). The left-most figure depicts all pairs (m,k) so that $\langle r_n, r_m, r_k\rangle = \mathrm{Sym_n}$. These pairs give rise to generating triples for $n = 25+4\times 5$ by adding 4×5 to each index, and these are depicted in the middle figure (shown in black). There are other generating triples that are not inherited from the $n=45$ case (shown in pink). The right-most figure is built similarly by adding 4×8 to each index for the triples for $n=45$. We see again that the previous pairs in black and pink are preserved for $n=77$ by adding 4×8 to each index.

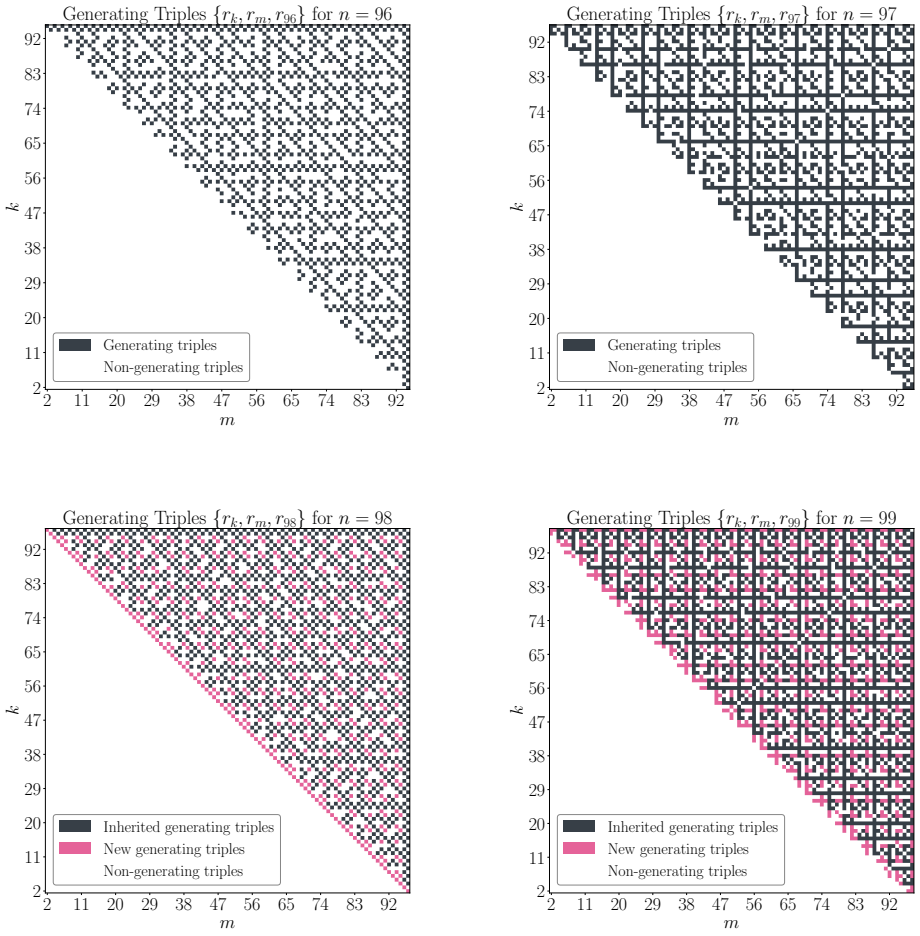

Figure 3: Visualization of Conjecture 3 to show on how the n case is "embedded" to the $n+2$ case. In the first pictures in the left-most column, we depict all generating triples for $n = 96$. All of these triples give rise to generating triples for $n = 98$ by adding 2 to each index (depicted in pink). The figures in the right-most column are built in a similar fashion.

Figure 3, we plot the pairs (m, k) that generate $\mathrm{Sym_n}$. Then, to visualize Conjectures 2 and 3 in terms of these graphs notice that that triples seem to be preserved by adding the same number to each of the indices. Moreover, Conjecture 4 can be seen as the white triangle on the plots below the diagonal.

Both from Figures 2 and 3, one can see that for each "row" it is either "almost full" or contains only half of the black dots. This observation along with other computational results gives us the following conjecture.

Conjecture 5. *Let*

$$F_k(n) = \{m \,:\, k < m < n,\, \langle r_n, r_m, r_k\rangle = \mathrm{Sym_n}\},$$

then

$$\max_{n>k+1} |F_k(n)| = \begin{cases} k+1 & \text{if } k \text{ is even,} \\ \frac{k+1}{2} & \text{if } k \text{ is odd.} \end{cases}$$

The code is available at the following link: https://github.com/Luka5s5/prefix_reversal_triples.

4.2. Hamiltonicity, diameter, girth

One of the open problems on Cayley graphs is the conjecture stating that every connected Cayley graph over a finite group has a Hamiltonian cycle. The conjecture was inspired by an open problem about hamiltonicity of vertex-transitive graphs [19]. Hamiltonicity of all 1939864 cubic Cayley graphs on up to 5000 vertices is confirmed (see https://graphsym.net/).

For the Big-3 flips $\{r_n, r_{n-1}, r_{n-2}\}$, it was conjectured in [13] that the corresponding Big-3 pancake graph has cyclic Gray codes for any $n \geqslant 4$, which means it has a Hamiltonian cycle. We have checked that this graph is Hamiltonian for $n = 4, 5, 6, 7, 8$. We furthermore verified that other generating triples have corresponding graphs that are Hamiltonian. For instance, there are eight generating triples (n, m, k) for $n = 7$:

$$(7,4,2), (7,5,2), (7,6,2), (7,4,3), (7,6,3), (7,5,4), (7,6,4), (7,6,5),$$

and the corresponding graphs are also Hamiltonian. Diameters, girths and the shortest cycles were found for all the corresponding cubic pancake graphs, and the results are summarized in Table 1. In these tables, cycles $C_\ell = r_{i_0} \dots r_{i_{\ell-1}}$ with $2 \leqslant i_j \leqslant n$, and $i_j \neq i_{j+1}$ for any $0 \leqslant j \leqslant \ell - 1$, of the shortest cycles are given. We denote these cycles using a canonical form by taking the lexicographically maximal sequence of indices $i_0 \dots i_{\ell-1}$. Contracted forms are also used in the table such as $(r_a r_b)^k$ corresponds to the cycle $C_\ell = r_a r_b \dots r_a r_b$, where $\ell = 2\,k$, $a \neq b$, and $r_a r_b$ appears exactly k times. A similar notation is used for a cycle of forms $(r_a r_b r_c r_d)^2$ and $(r_a r_b r_c)^4$. Forms of the shortest cycles are obtained by Lemma 1 from [20], Theorem 1.3 from [21], and computational experiments.

Graph	diameter	girth	shortest cycles
(7,4,2)	20	8	$(r_4r_2)^4$, $(r_7r_2)^4$, $(r_7r_4r_7r_2)^2$
(7,5,2)	20	8	$(r_5r_2)^4$, $(r_7r_2)^4$, $(r_7r_5r_7r_2)^2$
(7,6,2)	18	8	$(r_6r_2)^4$, $(r_7r_2)^4$,
(7,4,3)	20	8	$(r_4r_3)^4$, $(r_7r_4r_7r_3)^2$
(7,6,3)	16	8	$(r_6r_3)^4$
(7,5,4)	17	10	$(r_5r_4)^5$, $(r_7r_5r_7r_4r_5r_7r_4r_7r_5r_4)$
(7,6,4)	15	12	$(r_6r_4)^6$, $(r_7r_6r_4)^4$, $(r_7r_6r_7r_4r_7r_4)^2$, $(r_7r_6r_7r_6r_4r_6)^2$
(7,6,5)	15	8	$(r_7r_6r_5r_6)^2$

Table 1: Diameters, girths and shortest cycles for all cubic pancake graphs when $n = 7$.

Table 1 shows that for $n = 7$, the minimal diameter among all the corresponding cubic pancake graphs are associated with the graphs whose generating triples are $(7, 6, 4)$ and $(7, 6, 5)$. Meanwhile, girths of these graphs are different; indeed, the graph generated by $(7, 6, 4)$ has the maximal girth and the graph generated by $(7, 6, 5)$ has the minimal girth among them.

In the case $n = 8$ there are only five possible triples that generate the symmetric group. Diameters, girths and the shortest cycles of all the corresponding cubic pancake graphs in this case are shown in Table 2.

Graph	diameter	girth	shortest cycles
(8,7,2)	24	8	$(r_7r_2)^4$
(8,6,3)	24	8	$(r_6r_3)^4$
(8,7,4)	27	8	$(r_8r_4)^4$, $(r_8r_4r_7r_4)^2$
(8,6,5)	20	12	$(r_6r_5)^6$, $(r_8r_6r_8r_5r_8r_5)^2$
(8,7,6)	16	8	$(r_8r_7r_6r_7)^2$

Table 2: Diameters, girths and shortest cycles for all cubic pancake graphs with $n = 8$.

In Table 3, all generating sets are presented for the cubic pancake graphs that have minimal diameters and girths among all possible cubic pancake graphs with a given n, where $4 \leqslant n \leqslant 10$. As one can see from the table, for any $n \geqslant 6$, the minimal girth is 8. These computational results are correlated with theoretical results from [14]. All generating sets of the cubic pancake graphs with maximal diameters and girths are given in Table 4.

Acknowledgements

Elena V. Konstantinova thanks N.N. Krasovskii Institute of Mathematics and Mechanics hosted her visit to Yekaterinburg in 2023 when this project has been initiated. She was supported by the Mathematical Center in Akademgorodok, under agreement No. 075-15-2022-281 with the Ministry of Science and Higher Education of the Russian Federation. Mikhail Golubyatnikov and

n	min diameter	min diameter triples	min girth	min girth triples
4	4	(4,3,2)	6	(4,3,2)
5	7	(5,3,2), (5,4,2)	6	(5,3,2)
6	12	(6,5,2), (6,4,3), (6,5,4)	8	(6,5,2), (6,4,3), (6,5,4)
7	15	(7,6,4), (7,6,5)	8	(7,4,2), (7,5,2), (7,6,2), (7,4,3), (7,6,3), (7,6,5)
8	20	(8,6,5)	8	(8,7,2), (8,6,3), (8,7,4), (8,7,6)
9	23	(9,6,4), (9,7,6)	8	(9,7,2), (9,8,2), (9,8,3), (9,6,4), (9,7,4), (9,8,7)
10	27	(10,9,6), (10,8,7)	8	(10,9,2), (10,8,3), (10,9,4), (10,6,5), (10,8,5), (10,9,8)

Table 3: Minimal diameters and girths among all possible cubic pancake graphs generated by prefix-reversal triples (n, m, k) for a given n, where $n \leqslant 10$ and $2 \leqslant k < m < n$.

n	max diameter	max diameter triples	max girth	max girth triples
4	4	(4,3,2)	6	(4,3,2)
5	8	(5,4,3)	8	(5,4,2), (5,4,3)
6	12	(6,5,2), (6,4,3), (6,5,4)	8	(6,5,2), (6,4,3), (6,5,4)
7	20	(7,4,2), (7,5,2), (7,4,3)	12	(7,6,4)
8	27	(8,7,4)	12	(8,6,5)
9	42	(9,7,2)	12	(9,6,5), (9,7,6), (9,8,6)
10	39	(10,9,2), (10,8,3)	16	(10,8,7)

Table 4: Maximal diameters and girths among all possible cubic pancake graphs generated by prefix-reversal triples (n, m, k) for a given n, where $n \leqslant 10$ and $2 \leqslant k < m < n$.

Maslova were supported by the Ural Mathematical Center, under agreement with the Ministry of Science and Higher Education of the Russian Federation. Saúl A. Blanco thanks Elena Konstantinova for her kind hospitality during the G2A2 Conference in Novosibirsk where part of this work was discussed.

References

[1] J. D. Dixon, The probability of generating the symmetric group, Electronic J. Combinatorics 12 (2005) #R56, 1–5.

[2] S. M. Johnson, Generation of permutations by adjacent transposition, Mathematics of Computation 17 (83) (1963) 282–285.

[3] J. Friedman, On Cayley graphs on the symmetric group generated by transpositions, Combinatorica 20 (2000) 505–519.

[4] S. Akers, B. Krishnamurthy, A group-theoretic model for symmetric interconnection networks, IEEE Transactions on Computers 38 (4) (1989) 555–566.

[5] E. Konstantinova, Some problems on Cayley graphs, Linear Algebra and its Applications 429 (11) (2008) 2754–2769.

[6] H. Dweighter, Problems and solutions: Elementary problems: E2569, American Mathematical Monthly 82 (10) (1975) 1010.

[7] A. Kanevsky, C. Feng, On the embedding of cycles in pancake graphs, Parallel Computing 21 (6) (1995) 923–936.

[8] J.-J. Sheu, J. J. Tan, K.-T. Chu, Cycle embedding in pancake interconnection networks, Proc. 23rd Workshop on Combinatorial Mathematics and Computation Theory (2006) 85–92.

[9] S. A. Blanco, C. Buehrle, A. Patidar, Cycles in the burnt pancake graph, Discrete Appl. Math. 271 (2019) 1–14.

[10] S. A. Blanco, C. Buehrle, Lengths of cycles in generalized pancake graphs, Discrete Math. 346 (12) (2023) 113624.

[11] D. W. Bass, I. Sudborough, Pancake problems with restricted prefix reversals and some corresponding Cayley networks, Journal of Parallel and Distributed Computing 63 (3) (2003) 327–336.

[12] E. G. Son, Cycle structure of the cubic pancake graphs, Master Thesis (in Russian) (2022) 1–48.

[13] J. Sawada, A. Williams, Successor rules for flipping pancakes and burnt pancakes, Theoretical Computer Science 609 (1) (2016) 60–75.

[14] E. V. Konstantinova, E. G. Son, The girths of the cubic pancake graphs, Trudy Inst. Mat. i Mekh. UrO RAN 28 (2) (2022) 274–296.

[15] A. Chervov, D. Fedoriaka, E. Konstantinova, et al., CayleyPy growth: Efficient growth computations and hundreds of new conjectures on Cayley graphs (brief version) (2025). doi:https://doi.org/10.48550/arXiv.2509.19162.

[16] H. Wielandt, Finite permutation groups, Academic Press, 1964.

[17] M. N. Iradmusa, R. Taleb, On minimal generating sets for symmetric and alternating groups, Bull. Iran. Math. Soc. 44 (2018) 1457–1470.

[18] G. Janusz, Permutation groups generated by a transposition and another element, L'Enseignement Mathématique. IIe Série 38 (01 1992).

[19] L. Lovász, Problem 11, in: Combinatorial Structures and Their Applications : Proceedings of the Calgary International Conference on Combinatorial Structures and Their Applications, University of Calgary, Alberta, Canada, June, 1969, Gordon and Breach, 1970, pp. 243–246.

[20] E. Konstantinova, A. Medvedev, Independent even cycles in the pancake graph and greedy prefix–reversal gray codes, Graphs and Combinatorics 32 (2016) 1965–1978.

[21] E. V. Konstantinova, A. N. Medvedev, Small cycles in the pancake graph, Ars Math. Contemp. 7 (2014) 237–246.