# Exact diameter of the symmetric group with LX generators

S. Uskov[1], A. Chervov[2], F. Levkovich-Maslyuk[3], I. Litvak[4], A. Smolensky[5], and A. Soibelman[6]

[1] *Independent researcher,* specm32@gmail.com
[2] *Institute Imagine, Paris, France,* al.chervov@gmail.com
[3] *Centre for Mathematical Science, City St George's, University of London, Northampton Square, EC1V 0HB, London, UK,* fedor.levkovich@gmail.com
[4] *Independent researcher,* Vanya.litvak@gmail.com
[5] *Neapolis University Pafos, Cyprus,* andrei.smolensky@gmail.com
[6] *IHES, France,* asoibelman@gmail.com

hexagon:2611.00039v1

**Abstract**

We prove an exact formula for the diameter of the directed Cayley graph for the symmetric group $S_n$ with generators $L$ (left cyclic shift) and $X$ (exchange of the first two elements). For every $n \geq 5$, we show that the diameter equals $(3n^2-8n+12)/4$ for even $n$ and $(3n^2-8n+9)/4$ for odd $n$. This resolves a longstanding question first proposed in the 1960's and refined in more recent work. The proof is AI-assisted and is based on a variety of combinatorial arguments. We also describe the agentic system we developed that led to this proof and looks highly promising for attacking other questions of this type. An accompanying Lean 4 formalization rigorously verifies the result.

## Contents

**1 Introduction** **3**
1.1 Agentic system . . . . . 3
1.2 AI statement . . . . . 4

**2 Related work** **4**

**3 The moves** **4**

**4 The exact formula** **5**

**5 Eleven moves on five cards** **5**

**6 Cards on a circle and the starting marker** **6**

**7 Move conventions and position labels** **7**

**8 Constructing a sorting scan** **8**
8.1 Why the scan uses no more shifts than another solution . . . . . 8

**9 A table of backward-arrow counts** **9**

**10 Counting heights, swaps, and shifts** **10**
10.1 From table height to a swap bound . . . 10
10.2 What a card's backward-swap count means . . . 11
10.3 How many shifts the swap queue requires . . . 12
10.4 An arrow of almost maximum depth . . . 12
10.5 How many initial positions can be fixed . . . 13
10.6 Which minimum heights remain . . . 14
10.7 Odd size with all heights equal . . . 14
10.8 Finishing a scan at a minimum-height table . . . 16

**11 Even size: incompatible values of the second card** **16**
11.1 Why the first card must be zero . . . 17
11.2 Why the second card must be $n-1$ . . . 18

**12 Restrictions on an odd counterexample** **18**
12.1 Why at most one offset is exceptional . . . 19
12.2 A preliminary window count without a height bound . . . 19
12.3 Excluding heights above $h+2$ . . . 20
12.4 Geometry of an exceptional table . . . 21
12.5 Excluding a minimum initial height . . . 21
12.6 Why the initial gap is 1 or 2 . . . 22
12.7 Why the initial gap is smallest at height $h+1$ . . . 22

**13 Selecting positions: an upper bound on their number** **23**

**14 Counting offsets: the opposite bound** **23**

**15 Permutations that attain the bound** **25**

**16 Counting swaps with two colours** **25**

**17 A lower bound on shifts** **26**
17.1 Which turns are possible in a solution shorter than $B$ . . . 27
17.2 What changes when one turn is added . . . 28
17.3 Even size: excluding the bottom of the band . . . 28
17.4 Even size: ordinary and exceptional final markers . . . 29
17.5 Odd size: all final residues . . . 30
17.6 Why the first cards delay the entire scan . . . 32
17.7 Counting inversions in the exceptional tables . . . 32
17.8 A complete seven-card example . . . 33

**18 Combining the bounds** **33**

**19 Formalization and computational provenance** **33**

**20 Acknowledgements** **34**

# 1 Introduction

In this paper we study the following problem. Consider a permutation of the integers $1, 2, \ldots, n$, and consider two operations: $L$, a left cyclic shift, and $X$, exchange of the first two elements. How many operations does it take to sort the sequence, in the worst case? Despite its elementary formulation, this combinatorial problem is far from trivial. In group theory terms, it provides the diameter of the directed Cayley graph of the permutation group $S_n$ when generated by elements $L$ and $X$ (notice the graph is directed here because we do not include the inverse $L^{-1}$ generator).

This question was first proposed in the 1960's in [1], while a precise conjecture for the result was stated recently in [2] (a more detailed review of the literature is given in the next section). Here we prove this conjecture and thus resolve this longstanding open question. Ultimately, one of our motivations is attacking the celebrated Babai-type conjecture of establishing a polynomial bound on the $S_n$ diameter with *arbitrary* generators [3, 4, 5, 6, 7] which is however far beyond the scope of the present work.[1]

Initially we attempted to attack the problem by usual LLM tools – direct conversations with LLMs such as GPT Astra or Claude Fable 5.1/Opus 5.5. In our experiments we found that this approach does not lead to success (or perhaps would require a huge token budget). This highlights the difficulty of this problem. For example, the models typically get stuck at pursuing microscopic improvements of known upper bounds for the desired quantity (diameter) rather than developing new ideas.

Remarkably, we were able to circumvent this obstacle and indeed obtain a proof – by developing an LLM-powered agentic system. We describe it in more detail in the next subsection. We also provide a Lean formalization of the result, see section 19. While currently we have not understood the proof in detail, we hope that, together with a description of our workflow, it will still be of use to the community.

Our agentic system has shown itself to be quite powerful while staying at reasonable amounts of token spend and compute. It is this system that obtained the proof we present (with relatively minor human intervention that mainly amounted to agent orchestration rather than mathematical input). We already have evidence of its high efficiency in obtaining proofs of other conjectures of this type. We hope to explore its highly promising full capabilities in the future.

## 1.1 Agentic system

To obtain the proof presented in this paper we used an agentic system developed primarily by one of the authors (S. Uskov) and available at the public GitHub repository (link). It establishes a 'Research Team' consisting of several agents powered by an LLM (we mainly used GPT Astra in this work). The system provides skills and instructions including reasoning frameworks that encourage the agents to use a range of reasoning strategies and tricks – such as looking for counterexamples, trying to reformulate the problem in different ways, etc. Overall it is a prototype platform for coordinating AI-assisted research in mathematics, under human supervision. It combines a web interface, a Go server, and a persistent database to organize conjectures, lemmas, dependencies, research tasks, and attempts at problems. Configurable agents –including Codex, Claude Code, OpenCode, and Coddy Agent – take on distinct tasks such as finding proofs, searching for counterexamples, formalizing arguments in Lean, and reviewing results. A planner proposes overall research strategies, while execution and repair cycles advance approved tasks. Lean code is used to check candidates against a fixed formal statement, and the human operator provides final acceptance of the results in some cases. The system also records versioned evidence, reviews, failed approaches, and reusable accepted lemmas, allowing research results to accumulate across attempts (and, when enabled, across projects). Full technical details can be found at the repository linked to above.

[1] We also hope the results of this work and proofs for other related settings may help advance the 'holographic'-like duality conjectured in [8].

### 1.2 AI statement

Section 1 of the paper is mostly human-written, while the subsequent text and figures, including the proof, are AI-generated with minor human edits. The proof was obtained by our agentic system with relatively minor human intervention that amounted mostly to workflow orchestration. We mainly used GPT-6 Astra (with reasoning level from Medium to Ultra) within the agentic system as well as within OpenAI Codex. We also used Opus 5.5 for minor checks and editing.

## 2 Related work

**The original problem and earlier bounds.** The two-generator LX problem goes back to Glushkov's work on 'completeness of operation systems' in computers [1]. The historical account by Glukhov and Zubov [9, pp. 20–21] records Glushkov's upper bound $2n^2$, Pogorelov's subsequent quadratic bounds in 1973 [10], and Zubov's asymptotic result $D(n) \sim 3n^2/4$, attributed there to 1979. Zubov's later paper treats diameter bounds for a complete cycle and a transposition [11]. His subsequent work studies representations using generalized inversions and sorting using circular inversions [12, 13]. These early results do not specify the parity-dependent constant terms in the exact formula proved here.

**The precise conjecture and computations.** The exact formula for the diameters was conjectured very recently by Chervov and collaborators in their CayleyPy growth paper [2]. They report exhaustive diameter computations through $n = 15$. Thus the attribution distinguishes Glushkov's original problem from this later precise conjecture. The directed diameter sequence is recorded as OEIS A039745 [14]. Moreover, OEIS A378881 records computational examples of permutations at maximum directed distance [15]. The present argument proves the conjectured formula uniformly for all $n \geq 5$.

**Related questions.** The CayleyPy reinforcement-learning study [16] supplies pathfinding methods and diameter bounds chiefly for the three-generator system $L, R, X$, where $R = L^{-1}$ also costs one move. Its bounds therefore concern a different metric from the directed $L, X$ metric of this paper. Kuppili and Chitturi [17] use the same two moves, calling them $L, E$, but study sorting the reversed permutation rather than the maximum distance over all permutations.

The same directed graph is also called the sigma–tau graph. Williams' preprint [18] and the later work of Sawada and Williams [19] concern Hamilton paths and cycles in that graph. Their objective is to visit every permutation, rather than to determine the longest shortest path. Adin, Alon, and Roichman [20] determine the adjacent-swap diameter for circular permutations, where cyclic rotations identify arrangements. That problem does not charge shifts or specify a final starting marker, whereas both are essential to the constants in the present formula.

The proof below includes its combinatorial estimates explicitly. For background on comparing ordinary inversion count with total absolute displacement, see Diaconis and Graham [21].

Note added: we learned that after our proof was completed A. Guerrieri also independently obtained [22] the proof of several related conjectures from [2] (though not specifically the one we prove here).

## 3 The moves

We will describe the setting of the problem in the following way. We start with cards labelled $0, 1, \ldots, n-1$, where $n$ is the number of cards. All labels are distinct. We have the following L and X moves:

**Shift L:** Left cyclic shift. Equivalently, we remove the first card and place it at the end.

**Swap** X**:** exchange the first and second cards. Figure 1 shows both operations applied to the same row.

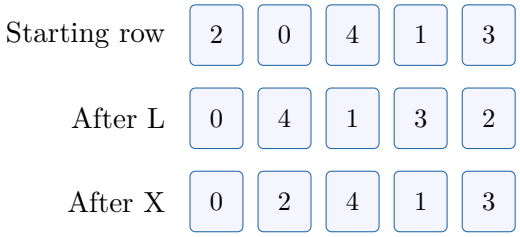



Figure 1: Two operations on five cards. The shift moves card 2 to the end; the swap exchanges cards 2 and 0.

The target row is $(0, 1, 2, \ldots, n-1)$. A backward shift is not a single permitted move: moving the last card to the front using L requires $n-1$ shifts.

For each starting row, take the length of a shortest solution. The maximum of these lengths is the **diameter**, denoted by $D(n)$. For example, $D(5) = 11$ asserts both that every row of five cards can be sorted in at most 11 moves and that some row cannot be sorted in 10 moves.

The same diameter governs transitions between arbitrary pairs of rows. Given a target row, rename its first card 0, its second card 1, and so on. The target becomes the increasing row. Renaming cards changes neither operation and therefore preserves the length of every shortest transition.

## 4 The exact formula

For $n \geq 5$, the result is

$$D(n) = \begin{cases} \frac{3}{4}n^2 - 2n + 3, & n \text{ even}, \\ \frac{3}{4}n^2 - 2n + \frac{9}{4}, & n \text{ odd}. \end{cases}$$

Write $B$ for the appropriate right-hand side. To prove $D(n) = B$, we prove that every row has a solution of length at most $B$, and that some row has no solution shorter than $B$. These are the upper and lower bounds.

For six and seven cards, respectively,

$$D(6) = \frac{3}{4} \cdot 36 - 12 + 3 = 27 - 12 + 3 = 18, \qquad D(7) = \frac{3}{4} \cdot 49 - 14 + \frac{9}{4} = 25.$$

| $n$ | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|
| $D(n)$ | 11 | 18 | 25 | 35 | 45 | 58 |

This is the formula of [2, Conjecture 11]. The formulas for the even and odd cases differ only in their constant terms. A function given by different polynomials for different residue classes is called a **quasipolynomial**; here the residue class is the parity of $n$.

An explicit route proves only an upper bound for its starting row. Proving that a route is shortest requires excluding every shorter solution.

## 5 Eleven moves on five cards

Consider the row $(1, 0, 3, 4, 2)$.

| Step | Operation | Row after the operation |
|---|---|---|
| 0 | – | $(1, 0, 3, 4, 2)$ |
| 1 | L | $(0, 3, 4, 2, 1)$ |
| 2 | L | $(3, 4, 2, 1, 0)$ |
| 3 | L | $(4, 2, 1, 0, 3)$ |
| 4 | L | $(2, 1, 0, 3, 4)$ |
| 5 | X | $(1, 2, 0, 3, 4)$ |
| 6 | L | $(2, 0, 3, 4, 1)$ |
| 7 | L | $(0, 3, 4, 1, 2)$ |
| 8 | X | $(3, 0, 4, 1, 2)$ |
| 9 | L | $(0, 4, 1, 2, 3)$ |
| 10 | X | $(4, 0, 1, 2, 3)$ |
| 11 | L | $(0, 1, 2, 3, 4)$ |

There are eight shifts and three swaps. After step 10, the circular order is already correct. The last shift makes the row begin with 0, and it must be included in the exact move count.

For five cards, all minimum distances can be checked by finite enumeration. Start at the increasing row. At each stage, construct predecessors of rows already found by applying X or moving the last card to the front. The backward shift is used to find a predecessor; it is not an allowed forward move in a solution.

Record each new row only when it first appears. The stage at which a row first appears is its minimum distance to the target using the permitted operations. The resulting counts are

| Distance | Rows | Distance | Rows |
|---|---|---|---|
| 0 | 1 | 6 | 15 |
| 1 | 2 | 7 | 20 |
| 2 | 3 | 8 | 22 |
| 3 | 5 | 9 | 19 |
| 4 | 8 | 10 | 11 |
| 5 | 12 | 11 | 2 |

The counts sum to $120 = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$, so they cover every permutation of five cards. The example first appears at stage 11. Its solution is therefore shortest, and $D(5) = 11$. This enumeration applies only to five cards.

## 6 Cards on a circle and the starting marker

Arrange the positions on a circle and label them $0, \ldots, n-1$. Add a marker indicating where the row currently starts.

Under L, the cards remain in their circular positions and the marker advances by one position. Under X, the cards at the marker and at the next position are exchanged. After $n$ shifts, the marker returns to its starting position.

To distinguish full turns, repeat the circle along an infinite line. After positions $0, \ldots, n-1$, put positions $n, \ldots, 2n-1$, then another copy, and continue. The line also extends to negative coordinates.

The displacement from coordinate 2 to coordinate 7 is $+5$, whereas that from 2 to 12 is $+10$. Both return to circular position 2, but they use different numbers of turns. Integer coordinates must therefore be retained when estimating the number of moves.

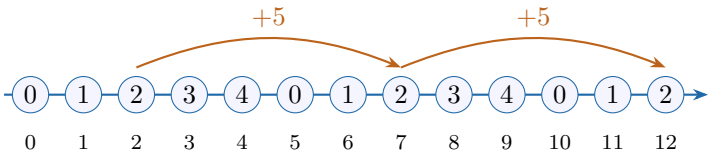



Figure 2: Unrolling a circle with five positions. Coordinates 2, 7, and 12 represent the same circular position on different turns.

## 7 Move conventions and position labels

We distinguish three quantities:

- the **label** written on a card;
- the card's **initial position**, before any move;
- the card's **target coordinate** on the unrolled line.

Let $p(i)$ be the label of the card initially at position $i$. The symbol $p$ denotes the entire starting row: $p(2) = 4$ means that position 2 initially contains card 4.

Let $T_i$ be the target coordinate of the card initially at position $i$. The index $i$ always refers to that initial position. The displacement of this card is

$$u_i = T_i - i.$$

A positive displacement is to the right and a negative displacement is to the left. Displacement is final coordinate minus initial coordinate. A card that moves back and forth can travel farther than the magnitude of its displacement.

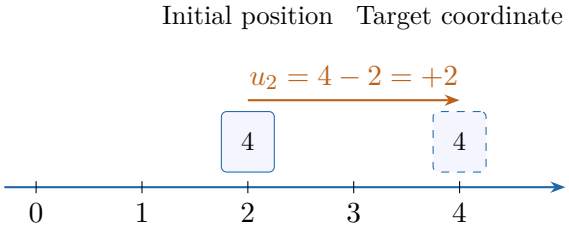



Figure 3: Card 4 starts at position 2. Assigning target coordinate 4 gives displacement +2. The card's label and its initial position differ.

For example, the row $(2, 0, 4, 1, 3)$ permits targets without additional turns:

| Initial position $i$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| Card label $p(i)$ | 2 | 0 | 4 | 1 | 3 |
| Target $T_i$ | 2 | 0 | 4 | 1 | 3 |
| Displacement $u_i$ | +2 | −1 | +2 | −2 | −1 |

The displacements sum to zero. A swap moves one card one position right and the other one position left. In the circular model, L moves only the marker and leaves the card coordinates unchanged.

More generally, the marker may finish at circular position $c$. Card $p(i)$ must then occupy position $p(i) + c$ modulo $n$. The unrolled targets satisfy

$$T_i \equiv p(i) + c \pmod{n}, \qquad \sum_i (T_i - i) = 0.$$

The first condition specifies the target modulo a full turn; the second specifies zero total displacement. Residues alone do not determine the move count, since different numbers of turns can require different routes.

# 8 Constructing a sorting scan

Fix target coordinates. At the marker, compare the targets of the two adjacent cards. If the left target exceeds the right target, apply X. Otherwise apply L and advance to the next comparison. The same operations take place in every periodic copy.

An **inversion** is a pair in the wrong target order. On a finite line, the left card should end to the right of the right card. On the periodic line, pairs from different copies must also be counted.

To obtain a finite count, take initial positions $i < j$ within one period. For each pair, count the copies of card $j$ that are on the wrong side of card $i$ relative to their targets. The contribution is

$$\left|\left\lfloor \frac{T_j - T_i}{n} \right\rfloor\right|.$$

The floor rounds down to an integer, and the outer bars take the absolute value. With $n = 5$, a target difference of $-2$ gives floor $-1$ and contribution 1. A difference of 6 also contributes 1: a copy of card $j$ from the preceding turn is on the wrong side of card $i$.

Summing over $i < j$ gives the number of **periodic inversions**. Pairs of copies are counted up to a common translation by a multiple of $n$. Each swap of an inverted adjacent pair decreases this number by one; a shift of the marker leaves it unchanged.

The scan terminates. If an inversion remains, some adjacent pair is inverted: otherwise every adjacent target, and hence every sequence of targets, would be increasing. Within $n$ shifts the marker encounters such a pair and a swap decreases the nonnegative integer inversion count. There can be only finitely many decreases.

After the last swap, the targets are increasing along the line. Every integer target occurs exactly once, since labels are distinct and copies repeat every $n$ positions. Consecutive targets therefore differ by one; a missing integer would have no place in the increasing sequence. Every card's target differs from its current coordinate by the same constant. The sum of remaining displacements over one period is zero, so that constant is zero. All cards have reached their targets. Some final shifts may still be needed to put the marker at the required start of the increasing row.

The total length is

$$\text{moves} = \text{swaps} + \text{shifts}.$$

Both terms matter. Even when swaps are already minimal, the next required swap may lie just behind the marker and require almost a full turn to reach.

For the upper bound we choose targets and estimate the scan length. If a row has no solution of length at most $B$, every scan we construct must be longer than $B$. These inequalities will restrict the starting row.

## 8.1 Why the scan uses no more shifts than another solution

Fix the targets and compare the scan, which swaps every inverted pair when it first reaches it, with any other swap schedule for the same targets.

Choose an integer threshold $t$. Call a card small if its target is at most $t$, and large otherwise. The scan always puts a small card before a large one when it compares them.

At each boundary, count the small cards to its right. This count is finite: sufficiently distant copies on the right have targets greater than $t$. A smaller count means that more small cards have passed to the left.

For two adjacent positions, let $A$ be the number of small cards starting at the left position, and $C$ the number strictly after the right position. After ordering the pair, the number starting at the right position is

$$\max(A-1, C).$$

If the pair contains zero small cards, the answer is $C$; if it contains one, that card goes on the left and the answer is again $C$; if it contains two, the answer is $C+1$. The formula gives all three values.

The function $\max(A-1, C)$ is nondecreasing in both variables. Thus inequalities between all such counts for two schedules survive the next comparison. Ordering the pair also gives the smallest possible count at the boundary inside it. Skipping the swap, or swapping a correctly ordered pair, cannot produce a smaller count.

Apply this argument successively at every comparison. After any given number of shifts, the scan has no more small cards to the right of any boundary than an arbitrary schedule. This holds for every threshold $t$.

If the other schedule has finished, no card to the right of position $i$ has target at most $i$. The same is true for the scan. Each scan card then has target at least its current position. The remaining displacements sum to zero, so they all vanish: the scan has also finished.

Consequently, **for fixed targets the scan uses no more shifts than any other schedule**. Its swap count is the inversion count, a lower bound for every schedule. If a final marker $c$ is required, append only the necessary residual shifts. The total length still does not exceed that of the other schedule. A lower bound for the scan with fixed targets is therefore a lower bound for every solution with those targets.

## 9 A table of backward-arrow counts

The following tables are auxiliary calculations. The permitted puzzle moves remain L and X.

Write $[a]_n$ for the residue of $a$ in $\{0, \ldots, n-1\}$; for example, $[-2]_7 = 5$ and $[9]_7 = 2$. For each $x$ in that set, put

$$q_x(i) = [p(i) - x]_n .$$

An **arrow** of $q_x$ is $i \to q_x(i)$. It is **backward** if its endpoint is less than its start. Thus $5 \to 1$ is backward, whereas $1 \to 5$ and $i \to i$ are not. A position with $q_x(i) = i$ is a **fixed position of the table**. This describes a table entry; card motion during sorting is counted separately.

Let $H(x)$ be the number of backward arrows in $q_x$, called the table's **height**. For example, take

$$p = (2, 0, 4, 1, 6, 3, 5), \qquad n = 7.$$

Subtracting 2 modulo 7 gives

$$q_2 = (0, 5, 2, 6, 4, 1, 3).$$

Only $5 \to 1$ and $6 \to 3$ are backward, so $H(2) = 2$. All seven heights are

| Subtracted value $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| Height $H(x)$ | 4 | 3 | 2 | 4 | 3 | 2 | 3 |

The original table $q_0 = p$ need not be the table with zero in its first position. Here $H(0) = 4$, whereas $p(0) = 2$ and $q_2$ begins with zero and has height 2.

We call $p_0 = p(0)$ the **initial offset**, and $H(p_0)$ the **initial height**: it is the height of the table whose first entry is zero. The original row itself has height $H(0)$. This example illustrates the calculation and is not assumed to be a counterexample.

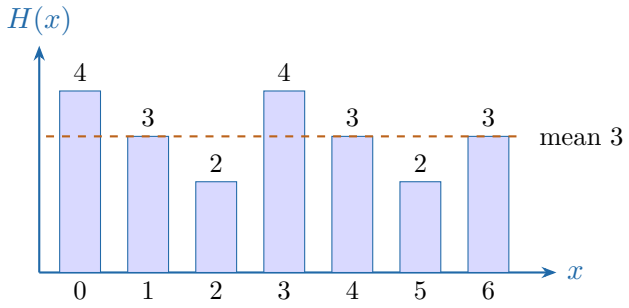



Figure 4: Heights for one row of seven cards. Two heights are 2 and two are 4; the mean, marked by the dashed line, is 3.

## 10 Counting heights, swaps, and shifts

**Rule 1: the sum of all heights is constant.** For a fixed position $i$, the value $[p(i) - x]_n$ runs through every residue once as $x$ does. Exactly $i$ of those values are less than $i$. Thus the arrow starting at $i$ is backward in exactly $i$ tables. Summing,

$$H(0) + H(1) + \cdots + H(n-1) = 0 + 1 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

In the seven-card example the sum is $4 + 3 + 2 + 4 + 3 + 2 + 3 = 21$.

**Rule 2: height decreases by at most one in a single step.** The **offset of position** $i$ is $[p(i) - i]_n$. For instance, the arrow $8 \to 2$ for $n = 11$ has offset $[2 - 8]_{11} = 5$. An offset $x$ occurs at $i$ exactly when $q_x(i) = i$. Let $f(x)$ be its number of occurrences.

Passing from $x$ to $x + 1$ decreases every table entry by one modulo $n$. A fixed arrow $i \to i$ with $i > 0$ becomes backward. The arrow ending at 0, if it starts at a positive position, ceases to be backward when its end wraps to $n - 1$. If 0 is at position 0, both changes are absent: $0 \to 0$ does not become backward, and no backward arrow ending at 0 disappears. In either case,

$$H(x + 1) = H(x) + f(x) - 1.$$

The index is cyclic. Since $f(x) \geq 0$, the decrease is at most one. Two consequences will be used:

1. An absent offset has $f(x) = 0$, so the next height is one lower.
2. A minimum height occurs at an offset that is present; otherwise the next height would be lower than the minimum.

The same rule can be summed over consecutive columns. If $k$ is subtracted modulo $n$ from every entry of a table $q$, let $N_k$ count its relative offsets $[q(i) - i]_n$ that are less than $k$. Then

$$\text{new height} = \text{old height} + N_k - k.$$

In particular, equal heights imply $N_k = k$. For $q_2 = (0, 5, 2, 6, 4, 1, 3)$, the relative offsets are $(0, 4, 0, 3, 0, 3, 4)$. Three are below 2, so subtracting another 2 changes the height from 2 to $2 + 3 - 2 = 3$, taking $H(2)$ to $H(4)$.

For an offset $x$, its **backward gap** is $g = [-x]_n$. This is $n - x$ for $x > 0$ and 0 for $x = 0$. With $n = 7$, offset 5 has gap 2.

### 10.1 From table height to a swap bound

Fix a table $q$ of height $H$. At position $i$, first choose the forward target $q(i)$ if $q(i) \geq i$, and $q(i) + n$ otherwise. Then decrease every target by $H$.

The added turns sum to $nH$, and decreasing $n$ targets by $H$ subtracts $nH$. The resulting displacements are balanced and lie between $-H$ and $n-H-1$. We prove the following bound on the inversion, hence swap, count:

$$\boxed{I \le H(n-H-1).}$$

Let $V$ be the ordinary inversion count of $q$, and let $A$ be the sum of backward-arrow lengths $i-q(i)$ over $q(i)<i$. The quantity $2A$ is Spearman's footrule; comparisons between that statistic and inversion count were studied by Diaconis and Graham [21]. We give the bound needed here explicitly. First,

$$I = H(n-H) + V - 2A.$$

Partition the positions into backward and other positions. There are $H(n-H)$ pairs between the classes. Moving backward targets to the next turn changes each such pair's contribution by one: up if the pair was not an ordinary inversion, down if it was. Pairs within a class are unchanged.

There are exactly $A$ inversions between the classes. To see this, for each backward position $i$, subtract the number of later values less than $q(i)$ from the number of earlier values greater than $q(i)$. The difference is $i-q(i)$, since exactly $q(i)$ values are less than $q(i)$. Sum over backward positions. An inversion between two backward positions cancels, appearing once with each sign. A later nonbackward position $j$ satisfies $q(j) \ge j > i > q(i)$ and contributes no negative term. The remaining terms are exactly the between-class inversions. This proves the identity for $I$.

Next we show $V \le 2A - H$. Temporarily allow swaps of arbitrary positions in the finite row, solely to count $V$. These are not additional puzzle moves. Until the row is increasing, find $i<j$ with $q(i) \ge j$ and $q(j) \le i$. Such a pair exists: take the rightmost $i$ with $q(i) > i$ and follow the values starting at $q(i)$. To the right of $i$, arrows cannot go forward. A fixed position cannot occur along this path, since it would already receive an arrow from a distinct position, contradicting injectivity. The path decreases until it reaches a number at most $i$; its last position before that step can serve as $j$.

Swapping positions $i, j$ brings both cards toward their labelled positions and decreases $A$ by exactly $j-i$. Repeat until the row is increasing. If there are $k$ swaps, their distances sum to the original $A$. A swap at distance $r$ can be implemented with $2r-1$ adjacent swaps, by carrying one card across and restoring the intermediate cards. Thus the construction uses $2A-k$ adjacent swaps. Since their minimum number is $V$, we have $V \le 2A-k$.

Each chosen swap decreases the number of backward positions by at most one. That number starts at $H$ and ends at zero, so $k \ge H$. Hence $V \le 2A-H$, and substitution gives

$$I \le H(n-H) + (2A-H) - 2A = H(n-H-1).$$

Define the nonnegative **reserve**

$$S = H(n-H-1) - I \ge 0.$$

A scan with $\Lambda$ shifts has total length $H(n-H-1) + \Lambda - S$.

### 10.2 What a card's backward-swap count means

For the card initially at $i$, count the cards to its left on the unrolled line whose targets exceed $T_i$, including copies from preceding turns. Call them its **backward predecessors**, and write their number as $b_i$. During the scan, the card must let each predecessor pass by moving one position left. Thus $b_i$ counts its necessary backward swaps and is also called its **depth**. Depth differs from displacement, since the card may also take part in rightward swaps.

A displacement table is **balanced** if its entries sum to zero. For a balanced table with $u_i \ge -H$ for every $i$, all depths satisfy $b_i \le H$. This can be proved without analysing a complete route. Choose a card of maximum depth. If it has a forward crossing with another card, the

other card has strictly greater depth: every larger target that the first card must let pass also exceeds the smaller target of the other card, and the first card itself supplies an additional predecessor. This contradicts maximality. The chosen card therefore has no forward crossings. Its displacement is minus its depth, and the lower bound on displacement bounds that depth by $H$. All other depths are no larger.

For the targets constructed from a table of height $H$, the lower displacement bound is exactly $-H$. Depth $H$ occurs precisely at the fixed positions of $q$. A card of depth $H$ has no forward crossings and therefore displacement $-H$, which in this construction corresponds to a fixed position. Conversely, displacement $-H$ requires at least $H$ backward swaps, and more than $H$ are impossible.

A fixed position here means $q(i) = i$ in the auxiliary table. The card starting there is assigned displacement $-H$ during the scan. The completion estimates distinguish depths $H$, $H-1$, and smaller depths. Encountering the third kind early saves a turn: in Estimate 2 below, $H$ is replaced by $H-1$.

### 10.3 How many shifts the swap queue requires

After the first sweep, the front card has the greatest target among those seen. It has no backward predecessors, so its depth is zero. The other cards form a queue of $n-1$ positions.

Suppose the next card has depth $b$. If $b > 0$, a swap decreases that depth by one and moves the zero-depth card one position forward. After L, the front depth is zero again and the processed card goes to the back of the queue. If $b = 0$, no swap is needed.

Each shift processes one queue position. A card of depth $b$ visits the front of the queue $b$ times, with $n-1$ shifts between visits. If its initial position after the zero-depth front is $i$, its last swap occurs no later than shift

$$i - 1 + (n-1)(b-1).$$

The maximum of these quantities over positive depths bounds completion of the whole queue.

During the first sweep, a card moved left by a comparison loses one unit of depth. If the next target is a new maximum, the old maximum enters the queue with depth equal to the least depth in the prefix already seen. The same comparison count will be used for the initial delay in Section 17.

We use two consequences.

**Estimate 1.** If the front depth is less than $H$ and all depths are at most $H$, the scan finishes by shift $H(n-1)-1$. After the first sweep, every queue depth is at most $H-1$; substitute that bound in the last-swap formula.

**Estimate 2.** Suppose the front depth is less than $H$, all positions of depth $H$ are at most $a$, and some position between 0 and $k$ has depth less than $H-1$. Then completion occurs by shift

$$(H-1)(n-1) + \max(a, k) - 1.$$

After the first sweep, depth $H-1$ can remain only on a former depth-$H$ card or on the card that carried the maximum until the first depth below $H-1$ appeared. The former depth-$H$ cards started at positions at most $a$; the card that carried the maximum started at a position at most $k$. Every other depth is at most $H-2$, so the queue formula gives the estimate.

The last swap may precede the required final marker. To finish at residue $c$, append the necessary shifts. The completion times below are always rounded up to a number with the required residue.

### 10.4 An arrow of almost maximum depth

Let $q$ have height $H$, and let a card at $i$ have depth $H-1$ and relative offset $r$. Its displacement is $r - H$. Displacement equals rightward swaps minus leftward swaps, so its number of rightward

swaps is

$$r - H + (H - 1) = r - 1.$$

At each such swap, a smaller-target card moves left. That card has greater depth, hence depth $H$, and its initial position is fixed in $q$. All these fixed positions lie on the open circular arc from $i$ to $q(i)$. That arc has $r - 1$ positions, exactly the number of rightward swaps. A pair contributes at most one such crossing because all displacements lie in a band of width less than $n$. Therefore **every position passed over by an arrow of depth $H - 1$ is fixed**.

Suppose every depth in an initial segment is at least $H - 1$, with $q(0) \neq 0$ and $H \geq 2$. Every nonfixed arrow in that segment goes forward. Indeed, a backward arrow with nonzero endpoint would pass through position 0 along its circular arc and require $q(0) = 0$. A backward arrow ending at 0 would require all subsequent positions to be fixed. Any earlier backward arrow would then also have to end at 0, contradicting distinct endpoints. Only one backward arrow would remain, contrary to $H \geq 2$.

### 10.5 How many initial positions can be fixed

Let $U$ count unit backward arrows $i \to i - 1$ in $q$. Retain the notation $A$ for total backward length and $V$ for ordinary inversions. Add one modulo $n$ to every entry, and let $j$ be the original position of label $n - 1$. Direct counting gives

$$A' = A + j - H, \qquad V' = V + 2j - (n - 1), \qquad H' \geq H - U.$$

For $A$, each length changes by one and the single label $n - 1$ wraps. For $V$, that label loses $n - 1 - j$ inversions and gains $j$. A backward arrow can cease to be backward only if its length was one, which gives the last inequality.

Use $V' + H' \leq 2A'$, proved above. Substitution cancels $j$ and yields

$$3H \leq n - 1 + 2A - V + U.$$

At a minimum height, $U \leq 1$. The neighbouring-height formula shows that the frequency of the preceding offset is at most one; every unit backward arrow has that offset.

If the first $r$ positions are fixed, remove them and renumber the others from zero. The quantities $H, A, V, U$ are unchanged, and the row length becomes $n - r$. Since $S = 2A - V - H$, we obtain

$$\boxed{r \leq n - 2H + S.}$$

There is a related bound for a prefix of almost maximum depth. If its first $r$ depths are at least $H - 1$ and $q(0) \neq 0$, then (assuming also $H \geq 2$)

$$\boxed{r \leq n - 2H + S + 1.}$$

To prove it, follow arrows starting at 0. Each goes forward and passes over fixed positions only. Replace consecutive links $0 \to b \to q(b)$ by $0 \to q(b)$ and make $b$ fixed. The quantities $A, H, U$ are unchanged, while $V$ increases by one: changes involving intermediate fixed positions cancel, leaving the pair of link endpoints. Thus $2A - V$ does not increase.

Repeat until positions $1, \ldots, r - 1$ are fixed. Move the origin from 0 to 1, changing position numbers and labels together. The quantities $H$ and $2A - V$ are unchanged. The number of unit backward arrows cannot increase except possibly through an arrow from 0 to $n - 1$. Such an arrow would pass over all intermediate positions and, together with the backward arrow ending at 0, give height at most one. The hypothesis $H \geq 2$ excludes it.

There are now $r - 1$ fixed initial positions, so the preceding count gives the second bound. In particular, a depth below $H - 1$ occurs by position $n - 2H + S + 1$.

### 10.6 Which minimum heights remain

In this subsection $H$ is the minimum height, so $H \le (n-1)/2$. An offset attaining that height will be called a **minimum offset**: its height is minimum, not necessarily its numerical value.

If $H > 0$, the first backward position is at most $n - H$, since $H$ backward positions must fit in the remaining row. A backward position has depth below $H$. Move the marker there, run the scan, and finish at the required start. Estimate 1 and the swap bound give at most

$$H(n - H - 1) + (H + 2)(n - 1) - H$$

moves. If $n = 2H + 5 + s$ with $s \ge 0$, the difference between $\frac{3}{4}n^2 - 2n$ and this bound is

$$Hs + \frac{3s^2 + 14s + 3}{4} > 0.$$

Thus $n \ge 2H + 5$ already admits a route within the required bound. If $H = 0$, the auxiliary table is increasing and at most $n - 1$ shifts suffice.

For even $n$, we must also exclude $n = 2H + 4$. Let $g$ be the gap of the chosen offset. Allowing one extra turn, the scan finishes at shift $H(n - 1) + n + g$, giving the total bound

$$\frac{3}{4}n^2 - 2n + g - S.$$

A counterexample therefore requires $g \ge S + 4$. If some position $i \le g + 1$ has depth below $H$, start there and finish at $H(n - 1) + g$ shifts; the length is then less than $B$. Consequently positions $0, \dots, g$ must all be fixed. The fixed-prefix bound gives $g + 1 \le n - 2H + S = 4 + S$, or $g \le S + 3$, a contradiction.

For even $n = 2m$, only $H = m - 1$ remains. For odd $n = 2m + 1$, the possibilities are $H = m - 1$ and $H = m$. In the latter case the minimum equals the mean, so all heights are equal. We handle it next.

### 10.7 Odd size with all heights equal

Let $n = 2m + 1$, $m \ge 3$, and suppose every height equals $m$. The neighbouring-height rule gives $f(x) = 1$ for every $x$: all offsets are distinct. Each auxiliary table has one fixed position, $m$ backward arrows, and $m$ forward arrows.

There is a forward arrow starting at $a > 0$ with length at least $m - 2$ and gap at least 3. Otherwise the $m$ distinct forward lengths could only come from the following possibilities:

- lengths $1, \dots, m - 3$, at most $m - 3$ choices;
- length $n - 2$, at most one choice;
- an arrow starting at 0, at most one choice.

Length $n - 1$ can occur only from 0 and is already included. This gives at most $m - 1$ choices, a contradiction. The chosen arrow has $3 \le g \le m + 3$.

In its table, $q(0) \ne 0$. An arrow of depth $m - 1$ passes over fixed positions only. As there is just one fixed position, its offset is at most 2. Offsets 0, 1, 2 each occur once, so at most three cards have depth at least $m - 1$. Among the first $g + 1 \ge 4$ positions there is a depth below $m - 1$. Estimate 2 gives at most

$$m^2 - S + 2m(m - 1) + g - 1 \le 3m^2 - m + 2 - S$$

moves. If $S \ge 1$, the required bound follows. It remains to treat $S = 0$.

We show that zero reserve makes the starting row a circular reflection. The equality $S = 0$ means $V = 2A - m$. The arbitrary-swap construction above gave $V \le 2A - k$ and $k \ge m$, so $k = m$.

Decompose the arrows of $q$ into cycles. Swapping two positions either joins two cycles or splits one cycle in two, changing the number of cycles by one. Sorting therefore takes at least the number of positions minus the number of cycles. Every nontrivial cycle has at least one forward arrow, so the number of backward arrows is no larger than that same difference.

There is one fixed position and $2m$ nonfixed positions. The equality $k = m$ leaves exactly $m$ nontrivial cycles. Each contains at least two positions, so all are transpositions.

Draw these pairs as arcs above the row. For $a < b < c < d$, their contributions relative to the sum for the individual pairs are

| Pairs | Correction to the inversion count |
|---|---|
| $(a, b)$ and $(c, d)$ | 0 |
| $(a, d)$ and $(b, c)$ | 0 |
| $(a, c)$ and $(b, d)$ | $-2$ |

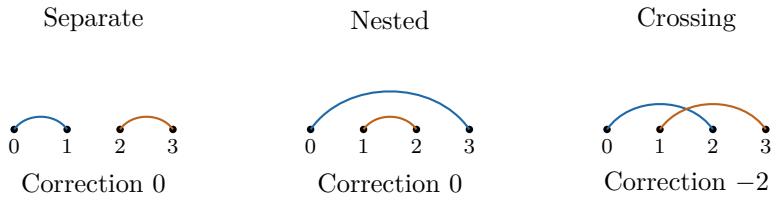



Figure 5: Separate and nested pairs contribute no correction. Crossing pairs reduce the sum of the individual inversion counts by 2.

Comparing the four endpoint values proves the table. For all pairs,

$$V = 2A - m - 2 \cdot \text{number of crossing pairs of arcs.}$$

Thus $V = 2A - m$ excludes crossings.

Cut the circle at its unique fixed position. The remaining positions are joined by noncrossing arcs. If there were two separate groups of nested arcs, each group would contain an innermost arc between adjacent positions. Those two pairs would have the same offset 1, contradicting distinct offsets. The same argument excludes branching within a group. All arcs are therefore nested. The first position after the cut is paired with the last, the second with the next-to-last, and so on. Restoring the original labels gives a reflection $p(i) = [r - i]_n$ for some $r$.

For a reflection, find a forward arrow of length at least $m - 1$ with gap between 3 and $m + 2$. The following starting position $a$ works:

| Value of $r$ | Choice of $a$ |
|---|---|
| $r \geq m + 1$ | 1 |
| $r = m$ | $m + 1$ |
| $r = 0$ | 2 |
| $1 \leq r \leq m - 1$ | $r + 1$ |

Substitution in $p(a) = [r - a]_n$ verifies both conditions. The scan bound is

$$m^2 + 2m(m - 1) + (m + 2) - 1 = 3m^2 - m + 1.$$

Equal heights thus also satisfy the odd bound. Any odd counterexample must have minimum height $h = m - 1$, hence $n = 2h + 3$.

### 10.8 Finishing a scan at a minimum-height table

Let $n = 2H + 2 + e$, where $e \in \{0, 1\}$. Choose a minimum offset $x$ distinct from the initial offset, and let $a$ be its last occurrence. Put $g = [-x]_n$ and $F = a + [-p(a)]_n$. The terms in $F$ account for the chosen position and the final shifts to the required marker. Only $F = g$ and $F = n + g$ are possible.

If some position $k \le F$ has depth below $H - 1$, Estimate 2 permits completion at

$$(H - 1)(n - 1) + F - 1$$

shifts. This number has the required final residue $g - H$.

First suppose $F = g$. Every fixed position is at most $a \le g$. Start at a depth below $H$ no later than $g + 1$, and finish at $H(n - 1) + g$ shifts. The total is at most $B$ whenever

$$g - S \le 2 + e(H + 1).$$

If this fails, the prefix bound supplies a depth below $H - 1$ by $g$. Use the shorter deadline $(H - 1)(n - 1) + g - 1$. Since $g < n$, the deadline together with the swap bound again gives the desired length.

Thus a last-occurrence arrow $a \to p(a)$ that goes forward or ends at 0 already gives a solution of length at most $B$: these are exactly the arrows for which $F = g$.

If $F = n + g$, a depth below $H - 1$ occurs before $F$, since one exists among the $n$ positions. The length is at most $I + H(n - 1) + g$, so the same condition $g - S \le 2 + e(H + 1)$ suffices.

We obtain a restriction on a counterexample: a minimum offset distinct from the initial one has a backward last-occurrence arrow with nonzero endpoint. Its gap is greater than 2 for even $n$, or greater than $H + 3$ for odd $n$.

## 11 Even size: incompatible values of the second card

Let $n \ge 6$ be even and put

$$B = \frac{3}{4}n^2 - 2n + 3.$$

Assume a row $p$ cannot be sorted in $B$ moves or fewer; call it a **counterexample**. We shall prove the following lemma.

> **First-two-cards lemma.** If a row of even size has no solution of length at most $B$, its first card is 0 and its second card is $n - 1$.

First apply the lemma. Define the reflection $J(i) = [1 - i]_n$, which exchanges 0 and 1. For $n = 6$,

| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $J(i)$ | 1 | 0 | 5 | 4 | 3 | 2 |

The inverse permutation $p^{-1}$ specifies where a labelled card stands; for example, $p^{-1}(1)$ is the position of card 1. Form the new row

$$q(i) = J\big(p^{-1}(J(i))\big).$$

The minimum solution lengths for $p$ and $q$ are equal. Invert a sequence of operations: reverse their order, replace L by a backward shift, and leave X unchanged. Then reflect by $J$. Reflection reverses shift direction, turning the backward shift into the allowed L. It exchanges positions 0 and 1, so X remains the same swap. The sequence length is unchanged. Applying the transformation twice returns to the original row, so it works in both directions.

The row $q$ is also a counterexample, and the lemma gives $q(0) = 0$. Since $J(0) = 1$,

$$q(0) = J(p^{-1}(1)) = 0.$$

Only 1 is mapped to 0 by $J$, so $p^{-1}(1) = 1$, or $p(1) = 1$. But the lemma for $p$ gives $p(1) = n - 1$. These values differ for $n \geq 6$, which is impossible at one position. The lemma therefore proves the even upper bound. With six cards, it would require the second card to be both 1 and 5.

### 11.1 Why the first card must be zero

We now prove the lemma using the height tables. Let $h$ be the minimum height. The scan estimates leave only

$$n = 2h + 2.$$

Let $M$ be the set of minimum offsets. For a counterexample, $|M| \leq h + 1$; if the initial offset $p(0)$ is not minimum, this improves to $|M| \leq h$. Here is the arrow count underlying these bounds.

A minimum offset distinct from 0 and $p(0)$ must be represented by a backward arrow with nonzero endpoint; otherwise the scan ending at its last occurrence is already short enough. Choose the largest minimum offset $t$. Every backward arrow with smaller offset stays backward when $t$ is subtracted from the labels. If $t \neq p(0)$, there is also a backward arrow ending at 0, starting at the position of card $t$.

Indeed, a backward arrow $i \to p(i)$ with smaller offset satisfies

$$n + p(i) - i < t.$$

Thus $p(i) < t$, and its new endpoint is $n + p(i) - t < i$. The additional arrow ending at 0 was not counted: its original endpoint is $t$.

The minimum-height table has only $h$ backward arrows. Count $t$ itself separately and, when necessary, also the initial offset. This gives at most $h + 1$ minimum offsets; if the initial offset is not minimum, the latter exception disappears and the bound is $h$. If 0 is minimum, use the original table for the same count: count offset 0 separately and omit the arrow ending at 0 from the other representatives.

The mean height is $h + \frac{1}{2}$, so the total excess above $h$ is $h + 1$. There are at least $h + 1$ nonminimum columns, each exceeding $h$ by at least one. Hence there are exactly $h + 1$ of each kind and every nonminimum height is $h + 1$. We have proved:

- exactly $h + 1$ offsets have height $h$;
- exactly $h + 1$ offsets have height $h + 1$;
- the initial offset has height $h$, since otherwise there would be at most $h$ minimum columns.

A present offset of height $h + 1$ occurs exactly once: two occurrences would make the next height at least $h + 2$.

Every original backward arrow with nonzero endpoint must have a minimum offset. Suppose one at position $k$ did not. Remove $k$ from the possible representatives of minimum offsets, and also remove the position of card 0 if it is backward. The remaining count is

| Case | Backward positions | Exceptions | Total |
|---|---|---|---|
| $p(0) = 0$ | at most $h - 1$ | 0 only | at most $h$ |
| $p(0) \neq 0$, offset 0 minimum | at most $h - 2$ | 0 and $p(0)$ | at most $h$ |
| $p(0) \neq 0$, offset 0 not minimum | at most $h - 1$ | $p(0)$ only | at most $h$ |

In the first two cases the original height is $h$. In the third it is at most $h + 1$ and two distinct backward positions were removed. This leaves at most $h$ representatives for $h + 1$ minimum offsets, a contradiction.

Consider offset $n-2$, whose gap is 2. A minimum height with gap 1 or 2 would give a solution of length at most $B$. For noninitial offsets this was proved in Section 10. For an initial offset there are at most two fixed positions, since otherwise the next height would exceed $h+1$. A depth below $h$ then occurs by position 2 and Estimate 1 again gives a short enough route. Consequently $H(n-2) = h+1$. Offset $n-2$ is present; otherwise $H(n-1)$ would be minimum with gap 1.

Let $b$ be its unique occurrence. Its original arrow goes forward or ends at 0, since backward arrows with nonzero endpoint have minimum offsets.

Suppose $p(0) \neq 0$. The initial offset is minimum and therefore is neither $n-1$ nor $n-2$, so $1 \leq p(0) \leq n-3$. The table for offset $n-2$ adds 2 to the labels. Its first arrow ends at $p(0)+2 \geq 3$, and it has only one fixed position, $b$.

An arrow of depth $H-1$ passes over fixed positions only. The first arrow would pass over positions 1 and 2 and require at least two fixed positions. Thus the first card has depth at least two below the maximum. This saves a turn. At height $h+1$ and gap 2, the route has at most

$$h(h+1) + h(2h+1) + 1 = 3h^2 + 2h + 1$$

moves. The required bound for $n = 2h+2$ is $3h^2 + 2h + 2$, so this is a contradiction. Therefore $p(0) = 0$.

### 11.2 Why the second card must be $n-1$

Return to position $b$ of offset $n-2$. Its arrow cannot end at 0: card 0 is already at position 0 and $b \neq 0$. Hence $b < p(b)$ and

$$n + b - p(b) = 2.$$

Since $b \geq 1$ and $p(b) \leq n-1$, this requires $b = 1$ and $p(b) = n-1$. The first two cards are indeed $0, n-1$, completing the lemma.

## 12 Restrictions on an odd counterexample

Let $n \geq 7$ be odd. Suppose a row $p$ has no solution of length at most

$$\frac{3}{4}n^2 - 2n + \frac{9}{4}.$$

Let $h$ be the minimum height. The **last occurrence** of an offset is its greatest position index in the original row. For an offset $x$, write $g(x) = [-x]_n$ for its backward gap. Thus $g(x) = n - x$ for $x > 0$ and $g(0) = 0$. For an arrow $i \to p(i)$ this is the forward circular distance from its endpoint $p(i)$ back to its start $i$.

The scan restrictions can be collected as follows.

> **Odd-counterexample lemma.** A counterexample satisfies all of the following conditions.
>
> **A. Three heights.** We have $n = 2h+3$, $h \geq 2$, and every height is $h$, $h+1$, or $h+2$.
>
> **B. The initial card.** We have $p(0) = n-d$ with $d = 1$ or 2, and $H(p(0)) = h+1$. Every present offset of height $h+1$ with positive gap has gap at least $d$.
>
> **C. Minimum height.** If $H(x) = h$, then $g(x) > h+3$. At the last occurrence $i$ of $x$, the original arrow satisfies $0 < p(i) < i$.
>
> **D. One exceptional offset.** Consider a present offset $x \neq p(0)$ with $H(x) = h+1$ and $1 \leq g(x) \leq h+3$. If its last-occurrence arrow goes forward or ends at 0, then $x$ equals a single value $z$.

Such a $z$ exists. For some occurrence $j$ of $z$, put $g = g(z)$ and $k = q_z(0)$. Then

$$0 < k < j \le g \le 4, \qquad k = g - d.$$

The original arrow at $j$ goes forward or ends at 0.

We prove the lemma from the absence of a route of length at most $B$. Sections 13 and 14 will then use A–D to bound one and the same count $N$ both above by $h$ and below by $h+1$.

### 12.1 Why at most one offset is exceptional

Suppose two distinct exceptional offsets have positive gaps $1 \le V < G \le h+3$. Both tables have height $H = h+1$ and a nonzero first entry.

Take the table $q$ of gap $G$. All its fixed positions are at most $G$: its last fixed position $a$ satisfies $a \le G$. If a depth below $H-1$ occurred between 0 and $G$, Estimate 2 would give at most

$$H(n-H-1) + (H-1)(n-1) + G - 1 \le 3h^2 + 5h + 3$$

moves, the required odd bound for $n = 2h+3$. All those depths are therefore at least $H-1$. Their nonfixed arrows go forward and pass over fixed positions only.

Put $t = G - V > 0$. Subtracting $t$ from the entries of $q$ gives the table of gap $V$ with the same height, so exactly $t$ relative offsets of $q$ are below $t$.

For each $i \in \{V+1, \dots, G\}$, its arrow cannot end after $G+1$; otherwise position $G+1$ would have to be fixed. Its offset is therefore at most

$$G + 1 - i \le G - V = t.$$

Equality is impossible, since it would make $i$ fixed in the gap-$V$ table, whose last fixed position is at most $V$. All $t$ positions $V+1, \dots, G$ therefore have offsets below $t$, and they exhaust all such offsets.

The offset at 0 is at least $t$ and cannot equal $t$, since the other table also has a nonzero first entry. The first arrow ends after $t$, hence at least at 2, making position 1 fixed. Its offset is zero, below $t$, but $1 \le V$ excludes it from the $t$ positions already counted. This contradiction proves uniqueness.

### 12.2 A preliminary window count without a height bound

For now, heights may exceed $h+2$. Call a column high if its height is at least $h+2$. Let $P$ count high columns, $Z$ count minimum columns, and $E$ be the sum of the excesses above $h+2$. The total-height identity gives

$$Z = P + E.$$

The minimum-offset count from Section 11 gives $Z \le h+1$. That count used minimum-height scan bounds and did not depend on parity.

Let $W$ be the window of offsets with gaps from 1 to $h+3$; it has $h+3$ elements. A minimum offset in this window can only be the initial offset $p_0 = p(0)$, since all other short minimum gaps have been excluded.

If $p_0$ is minimum and belongs to the window, let its gap be $d$ and its frequency be $F$. If $F \le d+1$, a depth below $h$ would appear by $d+1$ and a scan would fit within $B$. Thus $F \ge d+2$. On passing from $p_0$ to offset 0, at least $F$ zero relative offsets are counted and $d$ is subtracted, so $H(0) \ge h+2$.

Thus the minimum-offset set can meet the window only in $p_0$. At the same time, the high column at offset 0 lies outside their union. The overlap on the left of a count can be cancelled against this extra high column on the right.

An offset in the window falls into one of the following categories:

1. height at least $h + 2$;
2. the initial offset $p_0$;
3. the preceding offset $p_0 - 1$ modulo $n$, when the initial height is minimum;
4. the unique exceptional offset $z$ of height $h + 1$, if it exists;
5. a backward arrow with nonzero endpoint and height $h + 1$.

To check completeness, a minimum height must be $p_0$. For a present offset of height $h + 1$, take its last occurrence. It is initial, exceptional if the arrow goes forward or ends at 0, or in the last category. An absent offset has next height one lower, hence minimum. The next gap lies between 0 and $h + 2$, so the next offset is $p_0$ and the absent one is $p_0 - 1$.

Define three events:

- $T$: the initial height is minimum, or is $h + 1$ with positive initial gap in the window;
- $K$: the initial height is minimum and $p_0 - 1$ belongs to the window;
- $Q$: an exceptional offset exists, and another offset of the same height $h + 1$ has a smaller positive gap.

An event has indicator 1 when it holds and 0 otherwise. We claim

$$\boxed{E + 2 \le \mathbf{1}_T + \mathbf{1}_K + \mathbf{1}_Q.}$$

First suppose a present height-$(h+1)$ offset lies in the window. Choose one with smallest positive gap and call its offset $t$. Every other window offset of that height is numerically less than $t$. Noninitial minimum offsets are also less than $t$, since their gaps exceed the entire window.

Select backward arrows whose offsets are below $t$. They remain backward after subtracting $t$. If $t \neq p_0$, the new table also has a backward arrow ending at 0. Hence at most $h + 1 - \delta$ arrows were selected, where $\delta = 1$ if $t \neq p_0$ and $\delta = 0$ otherwise.

Count $t$ separately. Together with the initial offset, it requires at most $\mathbf{1}_T + \delta$ places; a coincident $t = p_0$ needs no second place. The preceding offset requires at most $\mathbf{1}_K$ places. The exceptional offset needs an additional place only if its gap exceeds the smallest chosen gap, which is exactly event $Q$; at equality it is already $t$. Including the overlap cancellation gives

$$Z + h + 3 \le P + (h + 1 - \delta) + (\mathbf{1}_T + \delta) + \mathbf{1}_K + \mathbf{1}_Q.$$

Use $Z - P = E$ to obtain the claim.

If no present height-$(h + 1)$ offset lies in the window, high columns and the initial and preceding offsets cover the window. Then $h + 3 \le P + \mathbf{1}_T + \mathbf{1}_K$. Since $P = Z - E \le h + 1 - E$, the same claim follows, with $Q$ absent.

### 12.3 Excluding heights above $h + 2$

The preliminary bound gives $E \le 1$. If $E > 0$, then $E = 1$ and all three events $T, K, Q$ hold. In particular, the initial height is minimum and its gap $d$ lies between 0 and $h + 3$. Gap 0 means $p_0 = 0$. We show that under these conditions $E = 0$.

Take threshold $t = p_0 - 1$ modulo $n$. If $d > 0$, the absence of a short scan gives $F \ge d + 2$, where $F$ is the frequency of $p_0$. Since every height is at most $h + 3$, the next-height formula gives $F \le 4$, hence $d \le 2$.

The height at $t$ is at most $h + 1$, since the next column is the initial minimum $h$. It cannot be $h$: it is noninitial and has gap $d + 1 \le 3$, whereas noninitial minimum gaps exceed $h + 3$. Thus $H(t) = h + 1$, and $t$ is absent.

Every present height-$(h + 1)$ offset is strictly below $t$. Indeed, between $p_0$ and the end of the scale there are fewer than $d$ offsets. Passing to any of them counts at least $F$ offsets and

subtracts fewer than $d$, giving height at least $h+3$. The offset $p_0$ has height $h$, and $t$ is absent. If $d=0$, take $t=n-1$; the neighbouring-height argument again gives height $h+1$ and absence, and all present offsets are below $t$ numerically.

Repeat the window count at this threshold. At most $h$ selected backward arrows have offsets below $t$, since the height-$(h+1)$ table also has an arrow ending at 0. Count $p_0$, $t$, and a possible exceptional $z$ separately, with the same high-column cancellation. Then

$$Z + h + 3 \le P + h + 2 + \mathbf{1}_{z \text{ exists}},$$

so $E+1 \le \mathbf{1}_{z \text{ exists}} \le 1$. This gives $E=0$, contradicting $E=1$. The only possible heights are $h, h+1, h+2$.

### 12.4 Geometry of an exceptional table

For an exceptional table $q=q_z$, let $F$ be its number of fixed positions, $g$ its gap, and $k=q(0)$. Its height is $h+1$, so

$$H(z+1) = h+1+F-1 = h+F.$$

The maximum height $h+2$ gives $F \le 2$. At least one fixed position exists, namely the last occurrence $j$ of $z$, so $1 \le F \le 2$.

A depth below $h$ by position $g$ would give a short scan by Estimate 2. Thus every depth in $0,\dots,g$ is at least $h=H-1$. A depth-$(H-1)$ arrow contains as many fixed positions as its offset minus one, so that offset is at most $F+1$. Depth-$H$ cards are fixed and have offset zero. All these prefix offsets are therefore below $F+2$.

Subtracting $F+2$ from the labels increases height by at most one, from $h+1$ to at most $h+2$. The height rule gives at most $F+3$ offsets below $F+2$. The prefix supplies $g+1$ such positions, whence $g \le F+2$.

The first arrow $0 \to k$ contains $k-1$ fixed positions, so $1 \le k \le F+1$. All $F$ fixed positions lie between 1 and $j \le g$, so $F \le g$. We have proved

$$1 \le F \le 2, \qquad F \le g \le F+2, \qquad 1 \le k \le F+1.$$

In particular $g \le 4$. No assumption about the initial height being $h+1$ was needed.

### 12.5 Excluding a minimum initial height

First exclude event $K$. Under $K$, the initial height is minimum and $d=0$ or 1: for $d>0$, combine $F \ge d+2$ with $F \le 3$; for $d=0$, $p_0=0$. Thus $p_0$ is either 0 or $n-1$.

The repeated threshold count at $p_0-1$, now with $E=0$, shows that an exceptional $z$ exists. Take its table $q$, gap $g$, first target $k$, and fixed-position count $F$.

Suppose the initial height is minimum. Subtracting $k$ from $q$ takes height $h+1$ to $h$, so exactly $k-1$ offsets of $q$ are below $k$. All $F$ fixed positions are counted, and every position $1,\dots,k-1$ is fixed because the first arrow passes over it. Consequently

$$F = k-1,$$

and there are no other offsets below $k$.

If $k \le g$, position $k$ belongs to the high-depth prefix and is nonfixed, since it receives the arrow from 0. All fixed positions are less than $k$, so its arrow must go to $k+1$. This supplies offset 1 below $k$, contradicting the completed count. Thus $g<k$. But $F \le g$ and $k \le F+1$, so $g=F=k-1$ and the original first label is $[k-g]_n = 1$. This contradicts $p_0 \in \{0, n-1\}$. Event $K$ is impossible.

With $E=0$, the preliminary count now gives $2 \le \mathbf{1}_T + \mathbf{1}_Q$, so both $T$ and $Q$ hold. If the initial height were still minimum, the geometry just proved would give $F=g$. Event $Q$ supplies

another height-$(h+1)$ offset with positive gap $v < g$. Between these equal heights, exactly $g - v$ relative offsets are below $g - v$. But all $F = g$ zero offsets are already counted, so $g \le g - v$, contrary to $v > 0$.

The initial height is therefore $h + 1$ and its positive gap lies in the window.

### 12.6 Why the initial gap is 1 or 2

The exceptional-table bounds imply

$$-3 \le k - g \le 1, \qquad p(0) = [k - g]_n \,.$$

The value $p(0) = 0$ would give $d = 0$, and $p(0) = 1$ would give $d = n - 1 > h + 3$. Both are excluded. Hence $k - g$ is $-1, -2$, or $-3$, so $d = g - k > 0$ and $d < g$.

We refine the bound on $F$. Since

$$k = g - d,$$

subtracting $k$ from $q$ gives the initial table with the same height. Exactly $k$ relative offsets of $q$ are below $k$. All $F$ fixed positions are counted, and the first arrow fixes $1, \ldots, k - 1$, so

$$k - 1 \le F \le k.$$

If $F = k - 1$, those are all the fixed positions. The next two prefix arrows must be $k \to k + 1$ and $k + 1 \to k + 2$, since longer arrows would contain additional fixed positions. Since $F \ge 1$, we have $k \ge 2$. The two unit arrows have offset 1 below $k$; together with the $k - 1$ zero offsets, they give at least $k + 1$ offsets below $k$, a contradiction. Therefore $F = k$, and $g \le F + 2 = k + 2$ gives

$$1 \le d = g - k \le 2.$$

There are $k - 1$ fixed positions before $k$, while $k$ itself is nonfixed, as it receives the arrow from 0. The last, $k$th fixed position $j$ is therefore after $k$. Thus

$$0 < k < j \le g \le 4.$$

### 12.7 Why the initial gap is smallest at height $h + 1$

For $d = 1$, no smaller positive integer gap exists. Suppose $d = 2$. Then $g = k + 2$ and the last fixed position $j$ is $k + 1$ or $k + 2$; all other fixed positions are $1, \ldots, k - 1$.

If $j = k + 1$, the arrow at $k + 2$ goes to $k + 3$. If $j = k + 2$, the arrow at $k$ goes to $k + 1$. Either case supplies an offset 1. If $k \ge 2$, this offset together with the $k$ zero offsets would give more than $k$ offsets below $k$. Hence $k = 1$.

Offset 1 now occurs at least twice: on the first arrow and on the unit arrow just found. There is also one fixed position with offset 0, so at least three offsets are below 2. Gap 1 corresponds to subtracting 2 from this table's entries and would have height

$$h + 1 - 2 + \text{number of offsets below } 2 \;\ge\; h + 2.$$

Thus no gap 1 has height $h + 1$; the initial gap 2 is indeed smallest among positive gaps of that height.

Conditions A, B, and D of the lemma are proved. Condition C follows from the minimum-height scan bound in Section 10. The initial height is larger than the minimum, so there is no initial exception: every minimum gap exceeds $h + 3$, and its last arrow is backward with nonzero endpoint. This completes the structural lemma.

Let $Z$ count offsets of height $h$ and $P$ those of height $h+2$. The mean height is $(n-1)/2 = h+1$. Each minimum column is one below that mean, each height-$(h + 2)$ column is one above, and all others equal it. Therefore

$$\boxed{Z = P.}$$

## 13 Selecting positions: an upper bound on their number

Write $p_0 = p(0) = n - d$. Select positions $i$ satisfying both

- $0 < p(i) < i$: the original arrow is backward with nonzero endpoint;
- the offset at $i$ is less than $p_0$.

Let $N$ be the number selected. For example, with $n = 11$ and $p_0 = 9$, the arrow $8 \to 2$ qualifies, since its offset is $5 < 9$. The arrow $2 \to 0$ does not qualify, since it ends at 0.

We prove $N \le h$. A selected position satisfies

$$n + p(i) - i < n - d, \qquad p(i) + d < i.$$

The table $q_{p_0}$ adds $d$ modulo $n$ to the labels. There is no wrap at a selected position because $p(i) + d < i < n$, so

$$q_{p_0}(i) = p(i) + d < i.$$

Each selected position therefore gives a backward arrow in $q_{p_0}$, whose height is $h+1$ by condition B.

There is one more backward arrow not in the selection. Take $j$ from condition D. Its offset $z$ implies $[p(j) + g]_n = j$, so

$$q_{p_0}(j) = [p(j) + d]_n = [j - g + d]_n = [j - k]_n .$$

Since $0 < k < j < n$, the residue is already $j - k$, and

$$q_{p_0}(j) = j - k < j.$$

The position $j$ was not selected: its original arrow went forward or ended at 0.

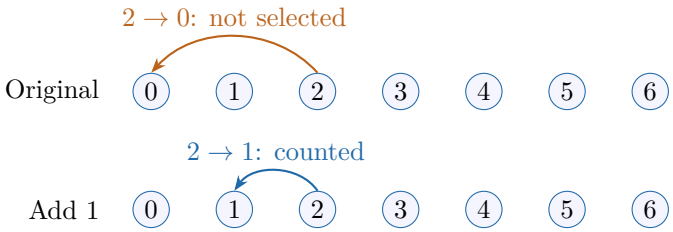



Figure 6: How an additional backward arrow can appear. An arrow ending at 0 is excluded from the original selection; after adding 1, $2 \to 1$ contributes to the height. This illustrates a local step, not a complete counterexample.

The $N$ selected positions and $j$ yield at least $N + 1$ backward arrows, but the height is $h + 1$. Therefore

$$N + 1 \le h + 1, \qquad \boxed{N \le h.}$$

## 14 Counting offsets: the opposite bound

Now count distinct *values* of offsets. Multiple occurrences of one value count only once. Take two sets:

- $M$, the $Z$ offsets of height $h$;
- $W = \{n - (h + 3), \ldots, n - 1\}$, the last $h + 3$ nonzero residues.

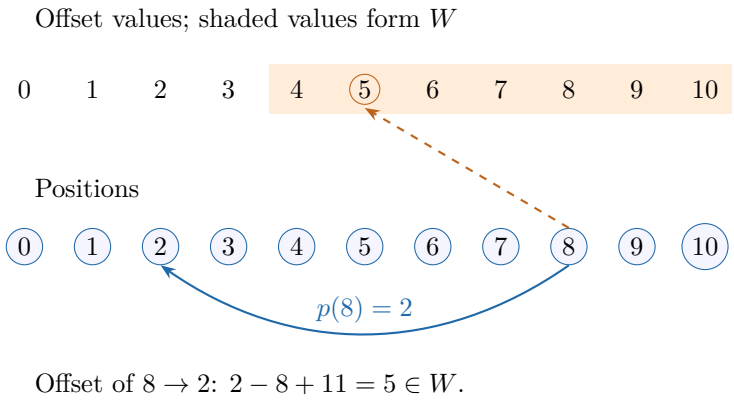



Figure 7: Offset values and position numbers are different sets of indices. The arrow from position 8 to position 2 has offset 5.

Call $W$ the window. For $n = 11$, $h = 4$, it consists of the seven values $4, 5, 6, 7, 8, 9, 10$.

Window gaps lie from 1 to $h + 3$, while minimum gaps exceed $h + 3$ by condition C. Thus $M$ and $W$ are disjoint, with altogether

$$Z + h + 3$$

distinct values. We cover them by categories whose sizes can be bounded.

**Minimum offsets are represented by selected positions.** By C, the last occurrence has a backward arrow with nonzero endpoint. Its gap exceeds $h + 3$, hence exceeds $d$, so its offset is $n - g(x) < n - d = p_0$. Both selection conditions hold.

**Window offsets of height $h + 2$.** There are at most $P$, since there are only $P$ such values in the entire height table.

**Window offsets of height $h + 1$.** First suppose $x$ is present and take its last occurrence.

- If $x = p_0$, count one exception.
- If $x \neq p_0$ and its arrow goes forward or ends at 0, condition D gives $x = z$, a second exception.
- Otherwise the arrow is backward with nonzero endpoint. By B its gap is at least $d$. Equality would give $x = p_0$, already counted. Hence the gap exceeds $d$, the offset is below $p_0$, and the position is selected.

If a window value $x$ is absent, Rule 2 gives next height $h$ and next gap between 0 and $h + 2$. Condition C excludes such a minimum height, including the cyclic transition from $x = n - 1$ to $x = 0$. Height $h$ is itself impossible in the window. The categories are complete.

| Category | Number of values |
|---|---|
| Height $h + 2$ | at most $P$ |
| Initial offset $p_0$ | at most 1 |
| Exceptional offset $z$ | at most 1 |
| Offsets of selected positions | at most $N$ |

The last entry is an upper bound because different selected positions can share an offset. Therefore

$$Z + h + 3 \leq P + 2 + N.$$

Since $Z = P$,

$$h + 3 \leq 2 + N, \qquad \boxed{N \geq h + 1.}$$

Section 13 gave $N \leq h$ for the same set of positions. The two bounds are incompatible. For example, $h = 4$ would require at most four and at least five positions.

The odd-counterexample lemma therefore proves the odd upper bound. The finite case $n = 5$ was handled in Section 5.

## 15 Permutations that attain the bound

Computational examples of extremal rows appear in [15]. For each $n \geq 6$, we now construct a row whose every solution has length at least $B$ and prove that lower bound uniformly. Start with the reflected row

$$1,\ 0,\ n-1,\ n-2, \ldots,\ 2.$$

For **even** $n$, exchange positions 1 and 2. For $n = 6$ this gives

$$(1, 5, 0, 4, 3, 2).$$

For **odd** $n = 2m + 1$, take the reflected row's card at position $m + 1$ and put it at position 2, moving the intervening cards at positions $2, \ldots, m$ one place right. This defines a starting row; it is not claimed to be an allowed puzzle move. For $n = 7$, $m = 3$, the row $(1, 0, 6, 5, 4, 3, 2)$ becomes

$$(1, 0, 4, 6, 5, 3, 2).$$

We separately bound swaps and shifts from below. Swaps are counted by pairs whose order must change. Shifts are counted by repeated leftward moves of a card, between which the marker must travel almost a full turn.

## 16 Counting swaps with two colours

Let $\rho(i)$ be the original position in the reflected row from which the card now at $i$ was taken. Its label is

$$s(i) = [1 - \rho(i)]_n .$$

For even size, $\rho$ just exchanges 1 and 2. For odd size, it puts index $m + 1$ at position 2.

Take any solution of $s$ and retain every card's unrolled target. For some common integer $C$, the targets have the form

$$T_i = C - \rho(i) + nk_i,$$

where $k_i$ specifies the copy of the final position occupied by the card initially at $i$. Colour $i$ blue if $k_i$ is even and orange if $k_i$ is odd.

Suppose $i < j$ have the same colour and $\rho(i) < \rho(j)$. Then $k_j - k_i$ is even and

$$T_j - T_i = n(k_j - k_i) - (\rho(j) - \rho(i)).$$

The parenthesized difference is between 1 and $n - 1$, so $\lfloor (T_j - T_i)/n \rfloor = k_j - k_i - 1$ is odd and nonzero. This pair contributes at least one periodic inversion.

As in Section 8, a pair $i < j$ contributes

$$\left| \left\lfloor \frac{T_j - T_i}{n} \right\rfloor \right|.$$

This counts order violations including periodic copies. Each adjacent swap changes the total by one, up or down. Eliminating all violations requires at least the initial inversion count in swaps.

If $a$ positions are blue, the number of same-colour pairs is

$$\frac{a(a-1)}{2} + \frac{(n-a)(n-a-1)}{2}.$$

Exceptions can occur only at ordinary inversions of $\rho$, where $\rho(i) > \rho(j)$. There is one such pair for even size and $m - 1$ for odd size, since the relocated card crosses $m - 1$ cards.

Same-colour pairs are fewest when the colour classes are as equal as possible. For $n = 2m$ the minimum is $m(m - 1)$; for $n = 2m + 1$ it is $m^2$. For six positions, a split into three of each colour gives $3 + 3 = 6$ pairs. Subtracting the possible exceptions gives

| Number of cards | Necessary swaps |
|---|---|
| $n = 2m$ | at least $m^2 - m - 1$ |
| $n = 2m + 1$ | at least $m^2 - m + 1$ |

This applies to every choice of turns $k_i$. It does not assume that cards use the nearest copies of their target positions.

## 17 A lower bound on shifts

Follow a card that must move left. After a swap moving it one place left, the marker is at the card's new position. To move the same card left again, the marker must reach the preceding circular position. As it only advances, this takes $n - 1$ shifts.

For an arbitrary route, count the first time the card reaches each new position to the left of its start. Extra rightward motion does not remove the need to cross those positions. The same count therefore bounds routes with backtracking.

For example, a card going from position 3 to coordinate 0 must cross $3 \to 2$, $2 \to 1$, and $1 \to 0$. With $n = 7$, the marker can be at the starts of these successive crossings no earlier than unrolled coordinates 2, 8, and 14. A final shift may still be needed for the required start.

Let $\Lambda$ be the total number of shifts. If the card initially at $i$ ends at $T_i < i$, counting leftward crossings and the final marker gives

$$\Lambda \geq n \max(i - 1, 0) - (n - 1)T_i + [-s(i)]_n .$$

The last term is the number of shifts from the last crossing under consideration to the nearest allowed final marker; it depends on the card's label $s(i)$.

For the nearly reflected rows, apply this to cards with the smallest displacements. Sometimes two cards give the same bound, so changing the turns of one leaves a restriction supplied by the other. The exact constants require an additional analysis of initial swaps and all possible turns. We prove the following lemma.

> **Move-count lemma for nearly reflected rows.** Every solution of the rows in Section 15 uses at least
>
> $$3m^2 - 4m + 3 \quad (n = 2m), \qquad 3m^2 - m + 1 \quad (n = 2m + 1)$$
>
> moves in total.

We first state the bounds for individual cases, then prove them and check that all possible targets are covered.

For even size, potentially short routes reduce to two cases:

| Targets | Swaps at least | Shifts at least | Total at least |
|---|---|---|---|
| Ordinary | $m^2 - m - 1$ | $2m^2 - 3m + 4$ | $3m^2 - 4m + 3$ |
| Exceptional | $m^2 - m$ | $2m^2 - 3m + 3$ | $3m^2 - 4m + 3$ |

The exceptional case requires one more swap but permits one fewer shift; the total is unchanged. For $n = 6$, these are $5 + 13 = 18$ and $6 + 12 = 18$.

For odd $n = 2m + 1$, $m \geq 3$, the residue $c$ of the total shifts must be considered. Each case gives at least $3m^2 - m + 1$ moves. For example, if $2 \leq c \leq m + 1$ and $\varepsilon = (c + m) \bmod 2$, one target case gives

$$\text{swaps} \geq m^2 + 1 - c + \varepsilon, \qquad \text{shifts} \geq 2m^2 + m + c - (2m + 1)\varepsilon.$$

Consequently

$$\text{moves} \geq 3m^2 + m + 1 - 2m\varepsilon.$$

For $\varepsilon = 1$ this is the desired $3m^2 - m + 1$; for $\varepsilon = 0$ it is larger by $2m$. The other target cases give at least the same bound, as we now prove. The case $n = 5$ already follows from Section 5.

### 17.1 Which turns are possible in a solution shorter than $B$

Start with any purported solution shorter than the bound. Keep each card's unrolled displacement $u_i$, and let $c$ be the total shifts modulo $n$. Then

$$u_i \equiv s(i) + c - i \pmod{n}, \qquad \sum_i u_i = 0.$$

If some $u_i \leq -m - 1$, its repeated leftward crossings alone require at least $m(n - 1)$ shifts. Together with the two-colour swap bound, this reaches the required total. A shorter solution must therefore satisfy

$$u_i \geq -m \quad \text{for every } i.$$

For each $c$, choose the least displacement in each residue class that is at least $-m$. For our rows the resulting table is

$$v_i = [c + 1 - \rho(i) - i + m]_n - m.$$

Each $v_i$ lies in $n$ consecutive integers starting at $-m$, so every other admissible displacement is

$$u_i = v_i + na_i, \qquad a_i \geq 0,$$

with integer $a_i$. Balance gives

$$0 = \sum_i v_i + n \sum_i a_i.$$

For the nearly reflected rows, $\sum_i v_i \geq -n$. Only two balanced possibilities remain:

- $\sum_i v_i = 0$, and every $a_i = 0$;
- $\sum_i v_i = -n$, and exactly one $a_i = 1$.

If the sum is positive, balance is impossible. It suffices to check the base table and, when its sum is $-n$, tables obtained by adding $n$ to one coordinate. This restriction follows from the assumption of a short solution; it is not imposed in advance.

For example, with $n = 7$, $m = 3$, $c = 3$,

$$v = (-3, 2, -2, -1, -3, 1, -1).$$

The sum is $-7$, so exactly one coordinate must receive 7. Adding 14 to one coordinate or 7 to two coordinates would give sum 7 instead of 0.

To prove the sum bound, first use the unmodified reflection, replacing $\rho(i)$ by $i$. Its table is

$$e_i = [c + 1 - 2i + m]_n - m.$$

For odd $n$, step 2 visits every residue, so $-m, \ldots, m$ each occur once and $\sum_i e_i = 0$.

Modifying the reflection decreases the expression at position 2 by $m - 1$ and increases those at $3, \ldots, m + 1$ by one. These changes sum to zero, so only wraps at the ends of the chosen band affect the total:

- position 2 receives $n$ if $e_2 \le -2$;
- a position in $3, \dots, m+1$ loses $n$ if $e_i = m$. There is at most one such position, since the values of $e$ are distinct.

Thus $\sum_i v_i \ge -n$. More precisely, with $\varepsilon = (c+m) \bmod 2$,

| Values of $c$ | $\sum_i v_i$ |
|---|---|
| 0 and 1 | $n\varepsilon$ |
| $2 \le c \le m+1$ | $n(\varepsilon - 1)$ |
| $m+2$ | 0 |
| $m+3 \le c \le 2m$ | $n(1-\varepsilon)$ |

In the middle range, for instance, $e_2 = c - 3 \ge -1$, so no $n$ is added. The value $e_j = m$ occurs in the modified segment only when $c+m$ is even, at $j = (c+m+2)/2 \in \{3, \dots, m+1\}$. The sum is then $-n$; otherwise it is 0.

For even $n = 2m$, the unmodified reflection visits every residue of the appropriate parity twice. Its sum is $-n\varepsilon$. Swapping positions 1 and 2 decreases one expression by one and increases the other by one. The lower-end wrap adds $n$ only at $c = m+1$, and the upper-end wrap subtracts $n$ only at $c = m+2$. Hence

$$\sum_i v_i = -n\varepsilon + n\mathbf{1}_{c=m+1} - n\mathbf{1}_{c=m+2}.$$

In the case subtracting $n$, $\varepsilon = 0$, so the sum is again at least $-n$.

### 17.2 What changes when one turn is added

Adding $n$ to one target affects only the $n-1$ pairs containing that card. Each contribution changes by $+1$ or $-1$. If $b$ decrease, then

$$\Delta I = (n - 1 - b) - b = n - 1 - 2b.$$

Here $b$ equals the card's backward-crossing count before the added turn. For a balanced table with every displacement at least $-H$, Section 10 bounds this count by $H$.

If $v$ has sum $-n$, first add one to every displacement. The result is balanced, and target differences and inversion count are unchanged. All displacements are at least $1-m$, so take $H = m-1$. Adding a turn to any one coordinate therefore increases the inversion count by at least one for $n = 2m$, and at least two for $n = 2m+1$.

### 17.3 Even size: excluding the bottom of the band

Let $n = 2m$ and suppose a displacement is $-m$. At a position $i \ge 3$, the label is $1 - i$ modulo $n$. Substitute $T_i = i - m$ in the shift bound:

$$\Lambda \ge (2m-1)m + 2i - 2m - 1.$$

Combining with $I \ge m^2 - m - 1$ gives

$$I + \Lambda \ge 3m^2 - 4m + 2i - 2 \ge 3m^2 - 4m + 4,$$

which exceeds the desired $3m^2 - 4m + 3$. Position 0 also gives a sufficient bound. In a purported shorter route, $-m$ can therefore occur only at position 1 or 2.

At both positions, $i + \rho(i) = 3$. The residue condition for $-m$ gives $c \equiv m+2 \pmod{2m}$. The base sum is then $-n$, so one turn must be added to one coordinate. Its base inversion count is $m^2 - m$, and adding a turn increases it by at least one:

$$I \ge m^2 - m + 1.$$

The card at position 1 or 2 gives

$$\Lambda \geq (2m-1)m - 2m + 2 = 2m^2 - 3m + 2.$$

Together these yield

$$I + \Lambda \geq 3m^2 - 4m + 3.$$

Thus a shorter route has no displacement $-m$, leaving the narrower band

$$u_i \geq 1 - m.$$

### 17.4 Even size: ordinary and exceptional final markers

Choose residue representatives from $1 - m$ to $m$:

$$w_i = [c + 1 - \rho(i) - i + m - 1]_{2m} - (m - 1).$$

Their sum is nonnegative. Balance permits no added turns, so necessarily $u = w$.

For the unmodified reflection, the expressions $c + 1 - 2i$ decrease by two, visiting each residue of the required parity twice. Their representatives in this band sum to $2m$ if $c + m$ is odd and to 0 if it is even. The swap at positions 1 and 2 changes only two terms; it can decrease the sum by a full period only at $c \equiv m + 3 \pmod{2m}$. Precisely,

$$\sum_i w_i = n\varepsilon + n\mathbf{1}_{c=m+2} - n\mathbf{1}_{c=[m+3]_n},$$

where $\varepsilon = (c + m) \bmod 2$. The positive correction is the wrap of modified position 1 through the lower end, and the negative one is the wrap of position 2 through the upper end.

Residue $c = m + 2$ gives positive sum and is excluded. All others allow only two cases:

1. $c$ and $m$ have the same parity;
2. $c \equiv m + 3 \pmod{2m}$.

In the first case, displacement $1 - m$ occurs at position 0 or at a position $j \geq m + 2$. To verify this, solve

$$c + 1 - \rho(j) - j \equiv 1 - m \pmod{2m}.$$

At unchanged positions $\rho(j) = j$, so $2j \equiv c + m \pmod{2m}$. The two solutions differ by $m$. If one lies at a modified position 1 or 2, the other remains near the end; the boundary case gives position 0.

For $j \geq m + 2$, the shift bound gives

$$\Lambda \geq (2m-1)(m-1) + 2j - 2m - 1 \geq 2m^2 - 3m + 4.$$

Position 0 gives at least as much. Adding $I \geq m^2 - m - 1$ yields

$$I + \Lambda \geq 3m^2 - 4m + 3.$$

In the second case the displacement table is explicit:

| Position | Displacement |
|---|---|
| 0 | $4 - m$ |
| 1 and 2 | $1 - m$ |
| $3 \leq i \leq m + 1$ | $m + 4 - 2i$ |
| $m + 2 \leq i \leq 2m - 1$ | $3m + 4 - 2i$ |

Here $I \geq m^2 - m$. The first three cards delay the subsequent swap queue. Counting that delay gives at least $(n-1)(m-2)+2$ shifts before the swaps finish. Yet the total shift count must have residue $m+3$. The preceding number $(n-1)(m-2)+1$ already has that residue but is one too small. The next allowed count adds $n$:

$$\Lambda \geq (n-1)(m-2) + 1 + n = 2m^2 - 3m + 3.$$

Again $I + \Lambda \geq 3m^2 - 4m + 3$. The required final residue turns a shortage of one shift into the need for an extra full turn.

For $n = 6$, the table is $(1, -2, -2, 1, -1, 3)$. Finishing the swaps requires at least seven shifts. The final residue is 0, so the next admissible shift count is 12; with six swaps this gives 18 moves.

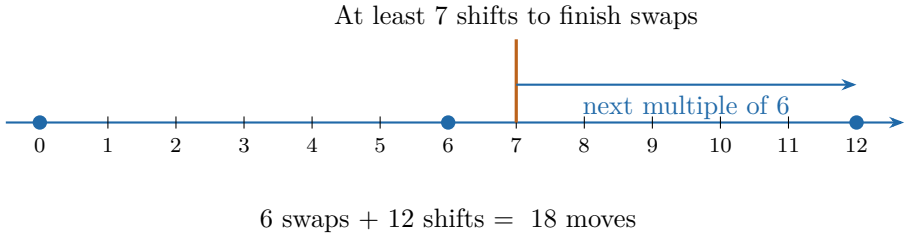



Figure 8: For six cards, six shifts cannot suffice, since the swaps require at least seven. The final marker requires a multiple of six, so at least twelve shifts are necessary.

### 17.5 Odd size: all final residues

Let $n = 2m + 1$, $m \geq 3$. The base table remains

$$v_i = [c + 1 - \rho(i) - i + m]_{2m+1} - m.$$

Partition the possible $c$ into three disjoint ranges:

- outer: $c = 0, 1$ or $m + 3 \leq c \leq 2m$;
- middle: $2 \leq c \leq m + 1$;
- the remaining value $c = m + 2$.

In the outer range balance permits only the base table. For $c \leq 1$, $c + m$ must be even; for $c \geq m + 3$, it must be odd. In either case, a position $t \geq m + 2$ has displacement $-m$:

$$t = \frac{c + 3m + 2}{2} \quad (c \leq 1), \qquad t = \frac{c + m + 1}{2} \quad (c \geq m + 3).$$

Substitution in the shift bound gives $\Lambda \geq 2m^2 + 2$. Thus

$$I + \Lambda \geq (m^2 - m + 1) + (2m^2 + 2) = 3m^2 - m + 3,$$

two moves above the required bound.

In the middle range put $\varepsilon = (c + m) \bmod 2$. The base inversion count satisfies

$$I(v) \geq m^2 + 1 - c + \varepsilon.$$

To obtain the improvement over the general two-colour bound, observe that position 2 has turn number zero in the base table. Each position $j$ with

$$\left\lfloor \frac{c + m + 2}{2} \right\rfloor < j \leq m + 1$$

has turn number 1: the expression $c + m + 2 - 2j$ is negative but greater than $-n$, so taking its residue adds exactly $n$. There are

$$K = \left\lfloor \frac{m - c + 1}{2} \right\rfloor$$

such positions.

Each pair $(2, j)$ is reversed by the modification of the reflection, since $\rho(2) = m + 1 > j - 1 = \rho(j)$. These positions have different colours, with turns 0 and 1. The coarse bound subtracted one for every reversed pair, even a different-colour pair that had contributed zero before subtraction. Here the actual contribution is at least one: for opposite colours and reversed order, the floor of the target difference divided by $n$ is an odd integer. We can replace the coarse contribution $-1$ by $+1$, an improvement of two for each of the $K$ pairs. Hence

$$I(v) \geq m^2 - m + 1 + 2K = m^2 + 1 - c + \varepsilon.$$

The equality $2K = m - c + \varepsilon$ follows by checking the two parities of $c + m$.

There are two distinct positions with displacement $\varepsilon - m$. One is in the modified segment:

$$j = \frac{c + m + 2 - \varepsilon}{2}.$$

The other is $j + m$ if $j + m < n$, and position 0 in the boundary case. Both follow by substituting into $v$.

If no turn is added, the second position gives

$$\Lambda \geq 2m^2 + m + c - (2m + 1)\varepsilon.$$

The total is at least

$$3m^2 + m + 1 - 2m\varepsilon \geq 3m^2 - m + 1.$$

If a turn is added, balance is possible only for $\varepsilon = 0$. The swap count increases by at least two:

$$I \geq m^2 + 3 - c.$$

Only one coordinate receives the turn, so at least one of the two coordinates just found is unchanged. Even the weaker shift bound gives

$$\Lambda \geq 2m^2 + c - m - 1,$$

and therefore

$$I + \Lambda \geq 3m^2 - m + 2.$$

Finally, at $c = m + 2$, the base table is balanced:

| Position | Displacement |
|---|---|
| 0 | $2 - m$ |
| 1 | $-m$ |
| 2 | 0 |
| $3 \leq i \leq m + 1$ | $m + 4 - 2i$ |
| $m + 2 \leq i \leq 2m$ | $3m + 4 - 2i$ |

No turn can be added, since it would make the sum positive. The first two cards give a delay of at least $(n - 1)(m - 1) + 1$ shifts before the swaps finish. The preceding count $(n - 1)(m - 1)$ already has the required residue $m + 2$. Another full period is needed:

$$\Lambda \geq (n - 1)(m - 1) + n = 2m^2 + 1.$$

Together with $I \geq m^2 - m + 1$ this gives $3m^2 - m + 2$. All final residues have now been covered.

### 17.6 Why the first cards delay the entire scan

Consider the first $r$ cards, initially at $0, \ldots, r-1$, and suppose each needs at least $q$ backward swaps (we assume $q \geq 1$). Assume the next target, at position $r$, exceeds all the preceding targets. We prove that the scan cannot finish before shift

$$q(n-1) + r - 1.$$

During the first sweep, the scan carries the largest target seen so far to the right. Call its card the carried card. After inspecting the first $r$ cards, the carried card's remaining backward count is the minimum of those cards' initial backward counts.

This is checked one comparison at a time. If the next target is smaller, the carried card moves right and the smaller card performs one backward swap. The carried card's backward count is unchanged. If the next target is greater, its card becomes the carried card. A card with the greater adjacent target has no more backward predecessors. Each step therefore preserves the minimum of the counts seen so far.

At the boundary before $r$, the next target exceeds all preceding ones. The old carried card remains at $r-1$ and still needs at least $q$ leftward swaps. The marker is already at $r-1$, comparing with the right neighbour. To perform the first leftward swap, it must reach the previous circular position, taking $n-1$ shifts. Each further backward swap costs at least another $n-1$ shifts. This gives $(r-1) + q(n-1)$.

Backtracking or skipped swaps cannot produce earlier completion, because Section 8 compares the scan with every schedule for the same targets.

Apply this to the two exceptional tables. In the even case take $r = 3$, $q = m-2$. Cards 1 and 2 have displacement $1-m$, so each needs at least $m-1$ backward swaps. Card 0 has at least $m-2$ backward predecessors, supplied by copies of the last $m-2$ targets from the preceding turn. The target at position 3 exceeds the first three. The delay is $(n-1)(m-2)+2$.

In the odd case take $r = 2$, $q = m-1$. Card 1 has displacement $-m$. Card 0 has at least $m-1$ backward predecessors from copies of the last $m-1$ targets on the preceding turn. The target at position 2 is 2 and exceeds the first two. The delay is $(n-1)(m-1)+1$.

### 17.7 Counting inversions in the exceptional tables

For even size the targets form three blocks:

- the first three are $4-m,\ 2-m,\ 3-m$;
- the next $m-1$ decrease from $m+1$ to 3 in steps of one;
- the last $m-2$ decrease from $2m+2$ to $m+5$ in steps of one.

The first block has two inversions. Every pair within either decreasing block is an inversion. Every pair from the first and last blocks has target difference at least $n$ and less than $2n$, contributing one. All other between-block pairs contribute zero. Thus

$$I = 2 + \frac{(m-1)(m-2)}{2} + \frac{(m-2)(m-3)}{2} + 3(m-2) = m^2 - m.$$

For odd size the first targets are $2-m,\ 1-m,\ 2$, followed by two decreasing blocks of $m-1$ cards each. Contributions come from one inversion among the first three, all within-block pairs, and pairs of the first two targets with the last block:

$$I = 1 + 2 \cdot \frac{(m-1)(m-2)}{2} + 2(m-1) = m^2 - m + 1.$$

For the even boundary table $c = m+2$, every displacement is one less than in the exceptional table. A common shift leaves target differences unchanged, so its inversion count is also $m^2 - m$.

### 17.8 A complete seven-card example

For the row $(1, 0, 4, 6, 5, 3, 2)$ we have $m = 3$. The seven possible final residues give the following cases:

| $c$ | Displacements | Moves at least |
|---|---|---|
| 0 | Balance impossible in the chosen band | – |
| 1 | Base table | 27 |
| 2 | Base table | 25 |
| 3 | One coordinate increased by 7 | 26 |
| 4 | Base table | 25 |
| 5 | Exceptional table | 26 |
| 6 | Base table | 27 |

"Balance impossible" does not prohibit sorting with that final residue. It means that such a route has already been excluded from the class of putative solutions shorter than 25 moves. Every route therefore uses at least 25 moves.

In each case the swap and shift bounds apply to the same target table, so their sum bounds the length of that solution.

## 18 Combining the bounds

For even $n = 2m$, the upper bound from Section 11 and the lower bound from Section 17 agree:

$$D(2m) = 3m^2 - 4m + 3.$$

Substituting $m = n/2$ gives

$$D(n) = \frac{3}{4}n^2 - 2n + 3.$$

For odd $n = 2m + 1$, Sections 12–14 and the lower bound give

$$D(2m + 1) = 3m^2 - m + 1.$$

Substituting $m = (n - 1)/2$ gives

$$D(n) = \frac{3}{4}n^2 - 2n + \frac{9}{4}.$$

The upper bound applies to every starting row. The lower bound applies to every solution of the rows in Section 15. Their agreement proves the diameter formula for every $n \geq 6$. Section 5 supplies $n = 5$.

## 19 Formalization and computational provenance

An accompanying code [23] in Lean 4[24], using Mathlib [25], proves the exact directed diameter. The source version cited here is commit

`9e04062fc06c6c1009295a8047e0ca52dd017456`.

Its toolchain is Lean 4.34.0 with Mathlib v4.34.0.

The public entry point is `LX/SharpDiameterAll.lean`. The commands

```
lake build LX
lake env lean VerifyLXExact.lean
```

check the development and the full public theorem types. The axiom audit at this commit checks 4593 project theorems, including generated auxiliary declarations, and permits only `propext`, `Classical.choice`, and `Quot.sound`.

## 20 Acknowledgements

We thank the members of the CayleyPy collaboration for useful related discussions. F.L.-M. also thanks A. Guerrieri for discussions. The work of F.L.-M. was supported by the STFC grants APP69281 and ST/C004225/1. F.L.-M. is grateful to Anthropic for access to their models through the Claude Team plan for scientists. I. L. thanks V. Kirova for computations using equipment of the National Research Nuclear University MEPhI high-performance computing cluster.

## References


[1] V. M. Glushkov. Completeness of a system of operations in digital computers. *Cybernetics*, 4(2):1–4, 1968. English translation of Kibernetika **4**(2) (1968), 1–5. doi:10.1007/BF01073731.

[2] A. Chervov, D. Fedoriaka, E. Konstantinova, et al. CayleyPy Growth: Efficient growth computations and hundreds of new conjectures on Cayley graphs (Brief version), 2025. Version 2, 1 April 2026. Section 4.1, Conjecture 11. URL: https://arxiv.org/abs/2509.19162v2, arXiv:2509.19162.

[3] L. Babai and Á. Seress. On the diameter of Cayley graphs of the symmetric group. *Journal of Combinatorial Theory, Series A*, 49(1):175–179, 1988. doi:10.1016/0097-3165(88)90033-7.

[4] L. Babai and Á. Seress. On the diameter of permutation groups. *European Journal of Combinatorics*, 13(4):231–243, 1992. doi:10.1016/S0195-6698(05)80029-0.

[5] L. Babai, R. Beals, and Á. Seress. On the diameter of the symmetric group: polynomial bounds. In *Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2004)*, pages 1108–1112. SIAM, 2004.

[6] E. Breuillard, B. Green, and T. Tao. Approximate subgroups of linear groups. *Geometric and Functional Analysis*, 21(4):774–819, 2011. doi:10.1007/s00039-011-0122-y.

[7] H. A. Helfgott and Á. Seress. On the diameter of permutation groups. *Annals of Mathematics*, 179(2):611–658, 2014. doi:10.4007/annals.2014.179.2.4.

[8] A. Chervov, F. Levkovich-Maslyuk, A. Smolensky, et al. CayleyPy-4: AI-holography. Towards analogs of holographic string dualities for AI tasks, 2026. URL: https://arxiv.org/abs/2603.22195, arXiv:2603.22195.

[9] M. M. Glukhov and A. Yu. Zubov. On the lengths of symmetric and alternating permutation groups in various generating systems (a survey). In *Matematicheskie Voprosy Kibernetiki*, volume 8, pages 5–32. Nauka, Moscow, 1999. In Russian. URL: https://keldysh.ru/papers/1999/mvk/mvk1999_5.pdf.

[10] B. A. Pogorelov. On a problem of V. M. Glushkov. *Kibernetika*, (5):141–143, 1973. In Russian. English translation: *A problem of V. M. Glushkov*, Cybernetics **9** (1973), 895–899, doi:10.1007/BF01069732. Historical results and this bibliographic record are also given in [9, pp. 20–21 and reference 48].

[11] A. Yu. Zubov. On the diameter of the group $S_N$ with respect to a system of generators consisting of a complete cycle and a transposition. In *Trudy po Diskretnoi Matematike*, volume 2, pages 112–150. TVP, Moscow, 1998. In Russian. URL: https://www.mathnet.ru/eng/tdm22.

[12] A. Yu. Zubov. On the representation of substitutions as products of a transposition and a full cycle. *Journal of Mathematical Sciences*, 166(6):710–724, 2010. Russian original: Fundamentalnaya i Prikladnaya Matematika **15**(1) (2009), 31–51. doi:10.1007/s10958-010-9887-z.

[13] A. Yu. Zubov. Circular inversions of permutations and their use in sorting problems. *Prikladnaya Diskretnaya Matematika*, (1(31)):13–31, 2016. In Russian. URL: https://www.mathnet.ru/eng/pdm540, doi:10.17223/20710410/31/2.

[14] D. desJardins and contributors. A039745: Diameter of symmetric group $S_n$ when generated by $(1, 2)$ and $(1, 2, 3, \ldots, n)$. The On-Line Encyclopedia of Integer Sequences. Accessed 29 October 2026. URL: https://oeis.org/A039745.

[15] K. Ryde and contributors. A378881: Irregular triangle listing permutations of $\{1, \ldots, m\}$ which are at maximum distance from the identity permutation under steps rotate left (L) or exchange first two elements (E). The On-Line Encyclopedia of Integer Sequences, 2024. Accessed 29 October 2026. URL: https://oeis.org/A378881.

[16] A. Chervov, A. Soibelman, S. Lytkin, et al. CayleyPy RL: Pathfinding and reinforcement learning on Cayley graphs, 2025. Version 3, 15 May 2026. URL: https://arxiv.org/abs/2502.18663v3, arXiv:2502.18663.

[17] S. S. Kuppili and B. Chitturi. Exact upper bound for sorting $R_n$ with LE. *Discrete Mathematics, Algorithms and Applications*, 12(3):2050033, 2020. 12 pp. Author-hosted manuscript: https://bpb-us-e2.wpmucdn.com/sites.utdallas.edu/dist/f/1052/files/2023/03/LE.pdf. doi:10.1142/S1793830920500330.

[18] A. Williams. Hamiltonicity of the Cayley digraph on the symmetric group generated by $\sigma = (1\ 2\ \cdots\ n)$ and $\tau = (1\ 2)$, 2013. Version 3, 6 July 2017. URL: https://arxiv.org/abs/1307.2549v3, arXiv:1307.2549.

[19] J. Sawada and A. Williams. Solving the Sigma-Tau problem. *ACM Transactions on Algorithms*, 16(1):11:1–11:17, 2020. Article 11; published online 15 November 2019. doi:10.1145/3359589.

[20] R. M. Adin, N. Alon, and Y. Roichman. Circular sorting, 2025. Version 2, 6 August 2025. URL: https://arxiv.org/abs/2502.14398v2, arXiv:2502.14398.

[21] P. Diaconis and R. L. Graham. Spearman's footrule as a measure of disarray. *Journal of the Royal Statistical Society, Series B*, 39(2):262–268, 1977. doi:10.1111/j.2517-6161.1977.tb01624.x.

[22] Andrea Guerrieri. In preparation.

[23] S. Uskov, A. Chervov, F. Levkovich-Maslyuk, I. Litvak, A. Smolensky, and A. Soibelman. Exact directed L/X diameter in Lean 4. https://github.com/snow-ghost/glushkov-lx-lean/releases/tag/v1.0.0, November 2026. Lean 4 formalization, version v1.0.0, commit `9e04062`.

[24] L. de Moura and S. Ullrich. The Lean 4 theorem prover and programming language. In *Automated Deduction – CADE 28*, volume 12699 of *Lecture Notes in Computer Science*, pages 625–635. Springer, 2021. doi:10.1007/978-3-030-79876-5_37.

[25] The mathlib Community. The Lean mathematical library. In *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020)*, pages 367–381. ACM, 2020. doi:10.1145/3372885.3373824.