AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **63(2)** (2015), Pages 226–245

A new inequality related to the Diaconis-Graham inequalities and a new characterisation of the dihedral group

Petros Hadjicostas

School of Mathematics and Statistics
Victoria University of Wellington, PO Box 600
Gate 7, Kelburn Parade, Wellington 6140
New Zealand
petros.hadjicostas@msor.vuw.ac.nz

Chris Monico

Department of Mathematics and Statistics
Texas Tech University, Box 41042
Lubbock, TX 79409-1042
U.S.A.
c.monico@ttu.edu

Abstract

We prove an inequality between three measures of disorder on the symmetric group on n elements. This inequality has been inspired by the well-known Diaconis-Graham inequalities. We also discuss when the inequality is satisfied as equality, and how often this happens. In the case n is odd, the number of permutations that satisfy the equality is a simple function of the Lucas numbers. In addition, we show that a quantity involved in the new inequality (which is a function of the three measures of disorder) can be used to give a new characterization of the dihedral group.

1 Introduction

Throughout the paper, we let $\mathbb{N}^* = \{1, 2, \ldots\}$ be the set of all positive integers (with $\mathbb{N} := \mathbb{N}^* \cup \{0\}$), $\mathbb{Z}$ be the set of all integers, and $\mathbb{R}$ be the set of real numbers. For a finite set A, we let $\#A$ denote the number of elements of A. For $n \in \mathbb{N}^*$, we denote by S_n the symmetric group, i.e., the set of all permutations of the numbers $1, 2, \ldots, n$.

If $n \in \mathbb{N}^*$, $a \in S_n$, and $i \in \{1, \ldots, n\}$, we denote by a_i the i^{th} element of a; that is, if a is considered as a bijection $a : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$, we define $a_i := a(i)$.

Thus we write $a = (a_1, a_2, \dots, a_n)$ to indicate explicitly the elements of permutation $a \in S_n$. For a permutation $a \in S_n$ and $i \in \{1, 2, \dots, n\}$, we define for convenience $a_{jn+i} := a_i$ for all $j \in \mathbb{Z}$, so that in particular, $a_0 := a_n$ and $a_{n+1} := a_1$. To avoid notational ambiguities, we use the nonstandard notation $\langle b_1, b_2, \dots, b_m \rangle$ to denote the cycle: $b_1 \mapsto b_2 \mapsto \cdots \mapsto b_m \mapsto b_1$. We use a^{-1} to denote the inverse permutation of a in the symmetric group S_n equipped with the operation of composition. Finally, we let $e_n := (1, 2, \dots, n)$ be the identity element in S_n.

Several measures of disorder or disarray have been proposed over time to quantify the deviation of a member of S_n from the sorted (in an ascending way) sequence $(1, 2, \dots, n)$; see, for example, references [2]–[8] and [11]. In this paper, we work with three of these measures: If $a = (a_1, a_2, \dots, a_n) \in S_n$, let $I_n(a)$ be the number of inversions in a, i.e., the number of pairs of integers (a_i, a_j) such that $1 \le i < j \le n$ and $a_i > a_j$; let $D_n(a) := \sum_{i=1}^n |i - a_i|$; and finally, let $EX_n(a)$ be the smallest number of exchanges (transpositions) of elements in a needed to leave it sorted. Cayley's result (see [11, Ex. 5.2.2-2, pp. 134 and 628]) states that $EX_n(a)$ equals n minus the number of (disjoint) cycles in the permutation a.

All three measures of disorder are obviously non-negative, and each one equals zero if and only if $a = (1, 2, \dots, n)$. Also, for all $a \in S_n$, $I_n(a) \le n(n-1)/2$, and equality holds if and only if $a = (n, n-1, \dots, 1)$. In addition, for all $a \in S_n$, $D_n(a) \le \lfloor n^2/2 \rfloor$ (where $\lfloor x \rfloor$ is the greatest integer less than or equal to x), and equality holds if and only if $a_i > n/2$ for $i = 1, 2, \dots, n/2$ when n is even; and either $a_i > (n+1)/2$ for $i = 1, 2, \dots, (n-1)/2$ or $a_i \ge (n+1)/2$ for $i = 1, \dots, (n+1)/2$ when n is odd–see [4, p. 266] or [8, Lemma 2.4]. Finally, $EX_n(a) \le n-1$ and equality holds if and only if a has only one cycle (and there are $(n-1)!$ permutations in S_n with exactly one cycle).

The most famous inequalities among these three measures of disorder (in addition to the obvious $EX_n(a) \le I_n(a)$) are the Diaconis-Graham inequalities (see [4]):

$$I_n(a) + EX_n(a) \le D_n(a) \le 2I_n(a) \quad (a \in S_n). \tag{1.1}$$

The proof of the right inequality is quite easy, but the proof of the left one is quite involved. Hadjicostas and Monico [9] provided an alternative proof of the left inequality, which is perhaps more intuitive than the one given by Diaconis and Graham [4]. They also provided some necessary and sufficient conditions for equality to hold (in the left inequality). In particular, if γ_n is the number of permutations $a \in S_n$ such that $I_n(a) + EX_n(a) = D_n(a)$, the two authors have shown that

$$\gamma_n \le 1 + \sum_{k=2}^{n} \left((k-1)! \sum_{l=1}^{k-1} \frac{2}{l} - \sum_{l=1}^{k-1} (l-1)!(k-l-1)! \right),$$

which implies $\gamma_n / n! = \mathcal{O}(\ln n / n)$.

In this paper, we prove another inequality closely related to the above inequalities:

$$D_n(a) \le I_n(a) + EX_n(a) + \left\lfloor \frac{n}{2} \right\rfloor \left(\left\lfloor \frac{n}{2} \right\rfloor - 1 \right) \quad (a \in S_n). \tag{1.2}$$

Note that this bound for $D_n(a)$ is sometimes (but not always) less than $2I_n(a)$ (from the right Diaconis-Graham inequality), as illustrated by the permutation $a = (4, 2, 3, 1) \in S_4$, which has $D_n(a) = 6$, $I_4(a) = 5$ and $EX_4(a) = 1$.

We also give a characterization of the set of permutations in S_n that satisfy (1.2) as equality. When $n \in \{1, 2, 3\}$, equality holds for all $a \in S_n$. When $n = 2k$, where k is an integer greater than or equal to two, equality holds for exactly one permutation:

$$\alpha_n = \alpha_{2k} := (k + 1, k + 2, \dots , 2k, 1, 2, \dots , k). \tag{1.3}$$

When $n = 2k + 1$, where k is an integer greater than or equal to two, equality holds for several permutations that can be obtained from the two permutations

$$\alpha_{1,n} = \alpha_{1,2k+1} := (k + 1, k + 2, \dots , 2k + 1, 1, 2, \dots , k) \tag{1.4}$$

and

$$\alpha_{2,n} = \alpha_{2,2k+1} := (k + 2, k + 3, \dots , 2k + 1, 1, 2, \dots , k + 1) \tag{1.5}$$

through some process that is explained later in the paper: see Lemma 5.1 and the discussion preceding it. See also Theorem 5.3 where we explicitly characterize these permutations that arise from $\alpha_{1,n}$ and $\alpha_{2,n}$ (and satisfy equality in (1.2)) through the disjoint cycle decompositions of the permutations. In addition, when $n = 6m + 3$, where m is an integer greater than or equal to 1, equality holds not only for the above permutations (for odd n), but also for the following two permutations:

$$\beta_{1,n} = \beta_{1,6m+3} := (3m + 1, 3m + 2, \dots , 6m + 3, 1, 2, \dots , 3m) \tag{1.6}$$

and

$$\beta_{2,n} = \beta_{2,6m+3} := (3m + 4, 3m + 5, \dots , 6m + 3, 1, 2, \dots , 3m + 3). \tag{1.7}$$

Unlike $\alpha_{1,n}$ and $\alpha_{2,n}$, each of which has only one cycle (for $n = 2k + 1$), the permutations $\beta_{1,n}$ and $\beta_{2,n}$ (for $n = 6m + 3$) each have three cycles.

If we define

$$K_n(a) := D_n(a) - I_n(a) - EX_n(a) \tag{1.8}$$

for all $a \in S_n$, then the left inequality in (1.1) and inequality (1.2) together are equivalent to

$$0 \le K_n(a) \le \left\lfloor \frac{n}{2} \right\rfloor \left(\left\lfloor \frac{n}{2} \right\rfloor - 1 \right). \tag{1.9}$$

A weaker version of the Diaconis-Graham inequalities [1] (1.1),

$$I_n(a) \le D_n(a) \le 2I_n(a) \quad (a \in S_n),$$

has been generalized in various ways by various authors, most notably in [6] and [7]. As a future research topic, it would be interesting to examine whether these generalizations can be sharpened to include EX_n as well.

[1] Knuth [11, Exercise 5.1.1-28, pp. 22 and 597] gives a simple proof of these inequalities that he attributes to the eminent computer scientist and personal friend Robert W. Floyd in 1983. Knuth (and probably Floyd) calls $D_n(a)$ the *total displacement* of the permutation $a \in S_n$, but he does not cite Diaconis and Graham's paper.

The organization of the paper is as follows. In Section 2 of the paper we state some simple properties of K_n and use these properties to give a new and interesting characterization of the dihedral group Dih_n. In Section 3 we provide a proof of inequality (1.2) (which is equivalent to the right inequality in (1.9)) for the case n is an even positive integer, and (when $n \geq 4$) we prove that equality here is only satisfied for the permutation defined by (1.3). In Section 4 we prove the same inequality for the case n is an odd positive integer.

Finally, in Section 5, for odd $n \geq 5$, we prove our claims made earlier about the equality case in (1.2) and we show in Theorem 5.4 that the number of permutations satisfying the equality case here is a simple function of the Lucas number L_n. When $n = 6m+3$ for $m \in \mathbb{N}^*$, there are exactly $2L_n + 2 - n$ permutations in S_n that satisfy equality in (1.2), while if $n = 6m+1$ or $6m+5$ for $m \in \mathbb{N}$, there are exactly $2L_n - n$ permutations in S_n that satisfy the equality.

2 A new characterization of the dihedral group

In this section of the paper we show how the quantity $K_n(a)$, defined by (1.8) in the introduction, can be used to give a (possibly) new characterization of the *dihedral group* Dih_n, which is the group of rotation and reflection symmetries of a regular polygon with its n vertices labeled clockwise $1, 2, \ldots, n$ (see James and Liebeck [10, Chapter 1]).

Note first that the function $K_n(\cdot) : S_n \to \mathbb{R}$ satisfies

$$K_n(a^{-1}) = K_n(a) \quad \text{for all } a = (a_1, \ldots, a_n) \in S_n.$$

This follows from the well-known properties

$$D_n(a^{-1}) = D_n(a), \quad I_n(a^{-1}) = I_n(a), \quad \text{and} \quad EX_n(a^{-1}) = EX_n(a)$$

for all $a \in S_n$ (e.g., see [4]). If in addition we define

$$\hat{a} := (n+1-a_n, n+1-a_{n-1}, \ldots, n+1-a_1) \in S_n, \tag{2.1}$$

then

$$K_n(\hat{a}) = K_n(a). \tag{2.2}$$

This again follows from the following result:

Lemma 2.1 *For each $a \in S_n$,*

$$D_n(\hat{a}) = D_n(a), \quad I_n(\hat{a}) = I_n(a) \quad \textit{and} \quad EX_n(\hat{a}) = EX_n(a). \tag{2.3}$$

Proof: For $a \in S_n$, the *complement* of a is defined by

$$\overline{a} := (n+1-a_1, n+1-a_2, \ldots, n+1-a_n).$$

For more discussion about this concept see, for example, Section 5 in [8]. For the complement of the identity $\overline{e}_n = (n, n-1, \ldots, 1)$ we observe that $\overline{e}_n^{-1} = \overline{e}_n$. For all $a \in S_n$, we thus have

$$\hat{a} = \overline{e}_n a \overline{e}_n = \overline{e}_n^{-1} a \overline{e}_n = \overline{a}\ \overline{e}_n = \overline{a\overline{e}_n}. \tag{2.4}$$

To prove the first equality in (2.3), observe that, for $a \in S_n$,

$$D_n(\hat{a}) = \sum_{i=1}^{n} |(n+1-a_{n+1-i}) - i| = \sum_{i=1}^{n} |(n+1-i) - a_{n+1-i}| = \sum_{j=1}^{n} |j - a_j| = D_n(a).$$

To show the second equality in (2.3), recall a well-known result about the number of inversions in a permutation $b \in S_n$:

$$I_n(\overline{b}) = \frac{n(n-1)}{2} - I_n(b).$$

Next note that, for $a \in S_n$,

$$I_n(\hat{a}) = I_n(\overline{e}_n a \overline{e}_n) = \frac{n(n-1)}{2} - I_n(a\overline{e}_n) = \frac{n(n-1)}{2} - I_n((a\overline{e}_n)^{-1}).$$

Therefore

$$I_n(\hat{a}) = \frac{n(n-1)}{2} - I_n(\overline{e}_n a^{-1}) = I_n(a^{-1}) = I_n(a).$$

To prove the last equality in (2.3), note that EX_n is a bi-invariant function on S_n, i.e., the cycle structure of a permutation is preserved under conjugation, and so

$$EX_n(a) = EX_n(bab^{-1}) \tag{2.5}$$

for all $a, b \in S_n$. Thus, for $a \in S_n$,

$$EX_n(\hat{a}) = EX_n(\overline{e}_n a \overline{e}_n) = EX_n(\overline{e}_n a \overline{e}_n^{-1}) = EX_n(a).$$

This completes the proof of the lemma. □

Based on the previous remarks and observations, we proceed to state and prove the new characterisation of the dihedral group. For each $n \in \mathbb{N}^*$, define

$$\mathcal{K}_n := \{b \in S_n \,|\, K_n(b^{-1}ab) = K_n(a)\ \forall a \in S_n\}. \tag{2.6}$$

It is easy to prove that the set $\mathcal{K}_n$ is a subgroup of the symmetric group S_n and

$$\mathcal{K}_n = \{b \in S_n \,|\, K_n(ab) = K_n(ba)\ \forall a \in S_n\}.$$

As the Theorem 2.3 below shows, for $n \geq 3$, the function K_n is invariant under conjugation only by members of the dihedral group. One interpretation of this is that the "re-labellings" of $\{1, 2, \ldots, n\}$ under which K_n is invariant are precisely those which are rigid, in the sense that they are in Dih_n. See, for example, Figure 1.

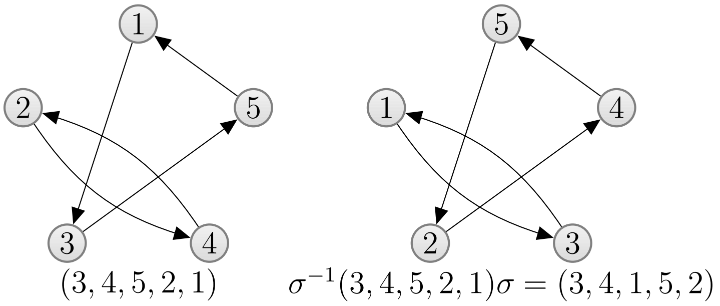

Figure 1: A permutation $a = (3,4,5,2,1) \in S_5$ and its conjugate $\sigma^{-1}a\sigma$, where $\sigma = (2,3,4,5,1) \in \mathrm{Dih}_5$. Here $K_n(a) = K_n(\sigma^{-1}a\sigma) = 2$.

Lemma 2.2 *Assume $n \in \mathbb{N}$ with $n \geq 4$ and let i, j, k be distinct positive integers in $\{2, \dots, n\}$ with $j < k$ and $\sigma = \langle 1, i\rangle\langle j, k\rangle \in S_n$. Then*

$$K_n(\sigma) = \begin{cases} 0 & \text{if } i < j < k \text{ or } j < k < i, \\ 2 & \text{if } j < i < k. \end{cases}$$

Proof: By directly counting the number of inversions, we find that

$$I_n(\sigma) = \begin{cases} 2(i+k-j-2) & \text{if } i < j < k \text{ or } j < k < i, \\ 2(i+k-j-3) & \text{if } j < i < k. \end{cases}$$

Furthermore, $D_n(\sigma) = 2|i-1| + 2|k-j| = 2(i+k-j-1)$, and since σ consists of $n-2$ cycles, $EX_n(\sigma) = 2$, which proves the lemma. □

Theorem 2.3 *We have $\mathcal{K}_1 = S_1$ and $\mathcal{K}_2 = S_2$, while for each $n \geq 3$, we have $\mathcal{K}_n = \mathrm{Dih}_n$.*

Proof: It is easy to show that $\mathcal{K}_1 = S_1$ and $\mathcal{K}_2 = S_2$. Thus, we assume $n \geq 3$. Because of (2.5), it follows that

$$\begin{aligned} \mathcal{K}_n &= \{b \in S_n |\, D_n(b^{-1}ab) - I_n(b^{-1}ab) = D_n(a) - I_n(a)\ \forall a \in S_n\} \\ &= \{b \in S_n |\, D_n(ab) - I_n(ab) = D_n(ba) - I_n(ba)\ \forall a \in S_n\}. \end{aligned}$$

(a) First we prove that $\mathrm{Dih}_n \subseteq \mathcal{K}_n$ for $n \geq 3$. It is well-known that

$$\mathrm{Dih}_n = \langle\langle x, y : x^n = e_n,\, y^2 = e_n,\, y^{-1}xy = x^{-1}\rangle\rangle$$

for some members x and y of the dihedral group. In the above equation, the notation $\langle\langle\cdot\rangle\rangle$ means generation by a number of elements, whereas x^m denotes the composition of x with itself m times.

We choose the rotation $x := (n, 1, 2, \dots, n-1)$ and the reflection $y := \overline{e}_n = (n, n-1, \dots, 2, 1)$ as generators of Dih_n. Obviously $x^n = e_n$ and $y^2 = e_n$. In addition, one can easily verify

$$y^{-1}xy = \hat{x} = (2, 3, \dots, n-1, n, 1) = x^{-1}.$$

Thus, x and y generate Dih_n. Because of (2.3) and (2.4), we conclude that $y \in \mathcal{K}_n$. To finish this part of the proof, we only need show that $x \in \mathcal{K}_n$. Let $a \in S_n$ and define $c := a^{-1}$. Then

$$ax = (a_n, a_1, \ldots, a_{n-1}) \quad \text{and} \quad a^{-1}x^{-1} = (c_2, c_3, \ldots, c_n, c_1).$$

We have:

$$\begin{aligned} I_n(ax) &= I_n(a) - \#\{i \in \mathbb{N}^* \mid 1 \le i \le n-1 \text{ and } a_i > a_n\} \\ &\quad + \#\{i \in \mathbb{N}^* \mid 1 \le i \le n-1 \text{ and } a_i < a_n\} \\ &= I_n(a) - (n - a_n) + (a_n - 1) \\ &= I_n(a) - (n - 2a_n + 1) \end{aligned}$$

and

$$\begin{aligned} I_n(xa) &= I_n((xa)^{-1}) = I_n(a^{-1}x^{-1}) \\ &= I_n(a^{-1}) - (c_1 - 1) + (n - c_1) \\ &= I_n(a) + (n - 2c_1 + 1). \end{aligned}$$

Therefore

$$I_n(xa) = I_n(ax) + 2(n + 1 - a_n - c_1). \tag{2.7}$$

We also have

$$D_n(ax) = |a_n - 1| + \sum_{i=1}^{n-1} |a_i - (i+1)| \tag{2.8}$$

and

$$D_n(xa) = D_n(a^{-1}x^{-1}) = \sum_{j=2}^{n} |c_j - (j-1)| + |c_1 - n| = \sum_{j=1}^{n} |c_j - (j-1)| + n - 2c_1.$$

By considering a as a bijection between the set $\{1, 2, \ldots, n\}$ and itself, and c as its inverse, we can change the order of the terms in the sum $\sum_{j=1}^{n} |c_j - (j-1)|$:

$$j = a_i \Leftrightarrow i = (a^{-1})_j = c_j.$$

We obtain:

$$D_n(xa) = \sum_{i=1}^{n} |i - a_i + 1| + n - 2c_1. \tag{2.9}$$

It follows from equations (2.8) and (2.9) that

$$D_n(xa) = D_n(ax) + 2(n + 1 - a_n - c_1).$$

Using the last equation and equation (2.7) we obtain $D_n(xa) - I_n(xa) = D_n(ax) - I_n(ax)$, from which we conclude that $x \in \mathcal{K}_n$.

(b) If $n = 3$ then part (a) of this proof implies $6 = \#\mathrm{Dih}_3 \le \#\mathcal{K}_3 \le 6$, and hence $S_3 = \mathrm{Dih}_3 = \mathcal{K}_3$. Thus we assume $n \ge 4$. To prove that $\mathcal{K}_n \subseteq \mathrm{Dih}_n$, let $b \in S_n \backslash \mathrm{Dih}_n$.

We will show that $b \notin \mathcal{K}_n$. One can find $\eta \in \mathrm{Dih}_n$ such that $(\eta b)(1) = 1$. Indeed, one may consider the rotation $x = (n, 1, 2, \ldots, n-1)$ from the proof of part (a) of this theorem and let $\eta := x^{b_1 - 1}$.

Since $\mathcal{K}_n$ is a subgroup of S_n and $\eta \in \mathcal{K}_n$ (by part (a) of this proof), it follows that $b \in \mathcal{K}_n$ if and only if $\delta := \eta b$ is in $\mathcal{K}_n$. Thus to finish the proof of the theorem it is enough to show that $\delta \notin \mathcal{K}_n$.

Since $\delta \notin \mathrm{Dih}_n$, there necessarily exists $j \in \{1, 2, \ldots, n\}$ so that $1 < |\delta_{j+1} - \delta_j| < n - 1$ (and this is a consequence of the characterization of Dih_n given in Lemma A.1 in the appendix). Thus, there is an $i \in \{1, \ldots, n\} \backslash \{j, j+1\}$ such that δ_i is between δ_j and δ_{j+1}. Since $\delta_1 = 1$, we must have $i \neq 1$. Thus, we may set

$$\epsilon := \langle 1, \delta_i \rangle \langle \delta_j, \delta_{j+1} \rangle.$$

By Lemma 2.2, $K_n(\epsilon) = 2$. On the other hand, $\delta^{-1} \epsilon \delta = \langle 1, i \rangle \langle j, j+1 \rangle$, and so from Lemma 2.2 again, $K_n(\delta^{-1} \epsilon \delta) = 0 \neq K_n(\epsilon)$. Therefore $\delta \notin \mathcal{K}_n$ and this completes the proof of the theorem. □

Note that for $n = 2k$, where $k \in \mathbb{N}^* - \{1\}$, we have $\alpha_{2k} \in \mathrm{Dih}_{2k}$, and for $n = 2k+1$, where $k \in \mathbb{N}^*$, we have $\alpha_{1,2k+1}, \alpha_{2,2k+1} \in \mathrm{Dih}_{2k+1}$. (Recall that α_{2k} is defined by (1.3) and $\alpha_{1,2k+1}$ and $\alpha_{2,2k+1}$ are defined by (1.4) and (1.5) respectively.) Geometrically, when $n = 2k$, α_{2k} corresponds to a rotation of the regular n-gon by an angle of π radians. On the other hand, for $n = 2k+1$, $\alpha_{1,2k+1}$ corresponds to a clockwise rotation by an angle of $2\pi \left(\frac{k}{2k+1}\right)$, while $\alpha_{2,2k+1}$ corresponds to a clockwise rotation by an angle of $2\pi \left(\frac{k+1}{2k+1}\right)$.

Finally we mention some elementary facts about the operation in (2.1) that will be useful in the next section of the paper. For $n = 2k$, where $k \in \mathbb{N}^*$, $\alpha_{2k}^{-1} = \hat{\alpha}_{2k} = \alpha_{2k}$, while for $n = 2k+1$, with $k \in \mathbb{N}^*$,

$$(\alpha_{1,2k+1})^{-1} = \hat{\alpha}_{1,2k+1} = \alpha_{2,2k+1} \quad \text{and} \quad (\alpha_{2,2k+1})^{-1} = \hat{\alpha}_{2,2k+1} = \alpha_{1,2k+1}.$$

Finally, if $n = 6m+3$ ($m \in \mathbb{N}^*$), then the permutations $\beta_{1,n} = \beta_{1,6m+3}$ and $\beta_{2,n} = \beta_{2,6m+3}$ (defined by (1.6) and (1.7) respectively) satisfy

$$(\beta_{1,6m+3})^{-1} = \hat{\beta}_{1,6m+3} = \beta_{2,6m+3} \quad \text{and} \quad (\beta_{2,6m+3})^{-1} = \hat{\beta}_{2,6m+3} = \beta_{1,6m+3}.$$

3 Proof of the main inequality for the even case

In this section we prove the main result of the paper, inequality (1.2), which is equivalent to the right inequality in (1.9), for the case where n is an even positive integer. First we prove the following lemma, which is used heavily throughout the rest of the paper.

Lemma 3.1 *Let $n \in \mathbb{N}^* \backslash \{1\}$, $a \in S_n$, and $i \in \{1, \ldots, n\}$. Let $\widetilde{a}$ be the permutation* *in S_n obtained from a by switching a_i with a_{i+1}; i.e., $\widetilde{a} = a\langle i, i+1\rangle$. Then*

$$K_n(\widetilde{a}) = K_n(a) + \begin{cases} 1, & \textit{if } a_i, a_{i+1} \textit{ are in the} \\ & \textit{same cycle of } a, \\ -1, & \textit{otherwise,} \end{cases} + \begin{cases} 1, & \textit{if } i < n \textit{ and } a_i \le i < a_{i+1}, \\ & \textit{or } i < n \textit{ and } a_{i+1} < a_i \le i, \\ & \textit{or } i < n \textit{ and } i < a_{i+1} < a_i, \\ & \textit{or } i = n \textit{ and } a_1 < a_n, \\ -1, & \textit{otherwise.} \end{cases}$$

Proof: For $i \in \{1, 2, \ldots, n-1\}$,

$$D_n(\widetilde{a}) = D_n(a) - |i - a_i| - |i + 1 - a_{i+1}| + |i - a_{i+1}| + |i + 1 - a_i|.$$

After some straightforward calculations, it follows that

$$D_n(\widetilde{a}) = D_n(a) + \begin{cases} 2, & \text{if } i < n \text{ and } a_i \le i < a_{i+1}, \\ -2, & \text{if } i < n \text{ and } a_{i+1} \le i < a_i, \\ 2(a_n - a_1), & \text{if } i = n, \\ 0 & \text{otherwise.} \end{cases}$$

In addition,

$$I_n(\widetilde{a}) = I_n(a) + \begin{cases} 1, & \text{if } i < n \text{ and } a_i < a_{i+1}, \\ -1, & \text{if } i < n \text{ and } a_{i+1} < a_i, \\ 2(a_n - a_1) + 1, & \text{if } i = n \text{ and } a_n < a_1, \\ 2(a_n - a_1) - 1, & \text{if } i = n \text{ and } a_1 < a_n. \end{cases}$$

If a_i and a_{i+1} are in the same cycle of a, we have (by Cayley's theorem) $EX_n(\widetilde{a}) = EX_n(a) - 1$ because switching a_i and a_{i+1} increases the number of cycles by one. Similarly, if a_i and a_{i+1} are in different cycles then $EX_n(\widetilde{a}) = EX_n(a) + 1$. The result now follows by applying the definition $K_n(\widetilde{a}) = D_n(\widetilde{a}) - I_n(\widetilde{a}) - EX_n(\widetilde{a})$. □

The following theorem proves inequality (1.2) in the case n is an even positive integer.

Theorem 3.2 *For $n = 2k$ with $k \in \mathbb{N}^*$ and $a \in S_n$ we have*

$$K_n(a) \le \frac{n}{2}\left(\frac{n}{2} - 1\right) = k^2 - k. \tag{3.1}$$

Equality holds if and only if $a = \alpha_{2k}$, where α_{2k} is given by (1.3), except for $n = 2$, in which case equality holds for all $a \in S_2$.

Proof: If a has fixed points, let i_1 be the smallest fixed point, i.e., $a_{i_1} = i_1$. Let $\widetilde{a}^{(1)}$ be the element of S_n obtained from a by switching a_{i_1} with a_{i_1+1}. By Lemma 3.1, $K_n(\widetilde{a}^{(1)}) = K_n(a)$. Also, $\widetilde{a}^{(1)}$ has one less cycle, and the i_1-th and (i_1+1)-th elements of it are not fixed points. If $\widetilde{a}^{(1)}$ has fixed points, let i_2 be its smallest one. Then $i_2 > i_1 + 1$. Let $\widetilde{a}^{(2)}$ be the element of S_n obtained from $\widetilde{a}^{(1)}$ by switching $\widetilde{a}^{(1)}_{i_2}$ with $\widetilde{a}^{(1)}_{i_2+1}$. Again, by Lemma 3.1,

$$K_n(\widetilde{a}^{(2)}) = K_n(\widetilde{a}^{(1)}) = K_n(a),$$

and $\widetilde{a}^{(2)}$ has one less cycle than $\widetilde{a}^{(1)}$. Continuing this process, we conclude that there is $\widetilde{a} \in S_n$ such that $\widetilde{a}$ has no fixed points, $K_n(\widetilde{a}) = K_n(a)$, and the number of cycles of $\widetilde{a}$ (denoted by $C_n(\widetilde{a})$) is less than or equal to the number of cycles of a. (If a has no fixed points, then $\widetilde{a} = a$.) We shall prove inequality (3.1) for $\widetilde{a}$.

Since $\widetilde{a}$ has no fixed points, each cycle has at least two elements, and thus $n \geq 2C_n(\widetilde{a})$. Since $EX_n(\widetilde{a}) = n - C_n(\widetilde{a})$, we conclude that $2EX_n(\widetilde{a}) \geq n$. From the right Diaconis-Graham inequality (1.1), we have $2I_n(\widetilde{a}) - D_n(\widetilde{a}) \geq 0$. Therefore

$$D_n(\widetilde{a}) - 2K_n(\widetilde{a}) = 2EX_n(\widetilde{a}) + 2I_n(\widetilde{a}) - D_n(\widetilde{a}) \geq n,$$

from which we conclude that

$$K_n(\widetilde{a}) \leq \frac{D_n(\widetilde{a})}{2} - \frac{n}{2} \leq \frac{1}{2}\left\lfloor \frac{n^2}{2} \right\rfloor - \frac{n}{2} = \frac{n}{2}\left(\frac{n}{2} - 1\right) = k^2 - k.$$

In order to have $K_n(\widetilde{a}) = k^2 - k$, it is necessary and sufficient that

$$2EX_n(\widetilde{a}) = n, \quad 2I_n(\widetilde{a}) - D_n(\widetilde{a}) = 0, \quad \text{and} \quad D_n(\widetilde{a}) = \frac{n^2}{2}.$$

The first equality means that $\widetilde{a}$ has exactly $n/2$ cycles of length two. The second equality is equivalent to the condition $\widetilde{a}$ has no 3-inversions (see [4] and [9]), i.e., $\widetilde{a}$ avoids the pattern 321 (see [1, Chapter 4]). We say that $b \in S_n$ has a 3-inversion (b_i, b_j, b_k) if and only if $1 \leq i < j < k \leq n$ and $b_i > b_j > b_k$. The third equality, $D_n(\widetilde{a}) = \frac{n^2}{2}$, is equivalent to saying that $\widetilde{a}_s > n/2$ for $s = 1, 2, \ldots, n/2$ (see again [4] and [8]). It is then clear that $K_n(\widetilde{a}) = k^2 - k$ holds if and only if $\widetilde{a} = \alpha_{2k}$, where α_{2k} is given by (1.3) – even when $n = 2$ (since $\widetilde{a}$ has no fixed points).

If $n = 2$, however, it is possible that either $a = (1, 2)$ or $a = (2, 1)$, both of which give rise to the same $\widetilde{a} = (2, 1)$. In such a case, $K_n(a) = k^2 - k = 1^2 - 1 = 0$ holds for all $a \in S_2$. On the other hand, for n even greater than or equal to 4, it is easy to check that there is no sequence $a \in S_n$ with fixed points that (through the process described above) can give rise to α_{2k} given by (1.3), i.e., $\widetilde{\alpha}_{2k} = \alpha_{2k}$, and equality in (3.1) holds if and only if $a = \alpha_{2k}$. □

4 Proof of the main inequality for the odd case

In this section we prove inequality (1.2) for the case n is an odd positive integer. The idea of the proof is to transform any permutation that maximizes K_n into one that has the form (4.1) in Lemma 4.1 below while keeping the value of K_n the same.

Lemma 4.1 *Let $n = 2k + 1$, where $k \in \mathbb{N}^*\backslash\{1\}$, and $q \in \{1, 2 \ldots, n - 1\}$ and consider the permutation*

$$h := (q + 1, q + 2, \ldots, n, 1, 2, \ldots, q) \in S_n. \tag{4.1}$$

Then $K_n(h) \leq k^2 - k$. Furthermore, equality holds if and only if either $q \in \{k, k+1\}$, or $3 \mid k - 1$ and $q \in \{k - 1, k + 2\}$.

Proof: For all $\theta \in \{1, 2, \ldots, n\}$ we have that $h(\theta) \equiv \theta + q \pmod{n}$. The cycle of h containing a given $\theta_1 \in \{1, 2, \ldots, n\}$ has length s if and only if s is the least positive integer for which $\theta_1 = h^s(\theta_1) \equiv \theta_1 + sq \pmod{n}$, or equivalently $s = n/\gcd(n, q)$. Therefore all cycles of h have the same length, s, and h is composed of $n/s = \gcd(n, q)$ disjoint cycles. It is straightforward to compute $D_n(h) = 2q(n-q)$, $I_n(h) = q(n-q)$, and $EX_n(h) = n - \gcd(n, q)$, so that

$$K_n(h) = q(n-q) - n + \gcd(n, q). \tag{4.2}$$

Because of (2.2), for $u \in \mathbb{N}$ with $1 \le u \le k$, the permutations corresponding to $q = k + u$ and $q = k + 1 - u$ have identical values for K_n, so we may assume without loss of generality that $1 \le q \le k$. In such a case, let $j := k - q \in [0, k-1]$ and $d := \gcd(2k+1, q)$. Then $d \,|\, 2k+1$ and $d \,|\, q$, so $2k+1 \equiv 0 \pmod{d}$ and $k \equiv j \pmod{d}$, and hence $2j+1 \equiv 0 \pmod{d}$. Since $j \ge 0$, it follows that $2j+1 \ge d$ so that $j \ge (d-1)/2$. Now we simply compute

$$\begin{aligned} K_n(h) &= -q^2 + qn - n + \gcd(n, q) \\ &= -(k-j)^2 + (k-j)(2k+1) - (2k+1) + d \\ &= k^2 - k - j^2 - j - 1 + d \\ &\le k^2 - k - 1 - \left(\frac{d-1}{2}\right)^2 - \left(\frac{d-1}{2}\right) + d \\ &= k^2 - k - 1 + \frac{-d^2 + 4d + 1}{4}. \end{aligned}$$

Among all odd positive integers d, $(-d^2 + 4d + 1)/4$ is maximized when $d = 1$ or $d = 3$, and the maximum value is 1, so that $K_n(h) \le k^2 - k$ as desired.

For equality, consider first the case when $1 = d = \gcd(2k+1, q)$ (for a general $q \in \{1, 2, \ldots, n-1\}$). Then (4.2) implies that $k^2 - k = q(2k+1-q) - 2k$ so that $q^2 - q(2k+1) + k^2 + k = 0$. Solving for q we find that $q = k$ or $q = k+1$. Since $\gcd(2k+1, k) = \gcd(2k+1, k+1) = 1$, they are both indeed solutions.

The remaining case has $3 = d = \gcd(2k+1, q)$ (for a general $q \in \{1, 2, \ldots, n-1\}$). Here it follows from (4.2) that

$$k^2 - k = q(2k+1-q) - 2k + 2,$$

that is, $q^2 - q(2k+1) + k^2 + k - 2 = 0$, and so $q = k-1$ or $q = k+2$. However, $\gcd(2k+1, k-1) = \gcd(3, k-1)$, so $3 = \gcd(2k+1, k-1)$ iff $3 \,|\, k-1$. Similarly, since $k \ge 2$, we find that $3 = \gcd(2k+1, k+2)$ iff $3 \,|\, k-1$. Therefore, $q = k-1, k+2$ are also solutions of the equation $K_n(h) = k^2 - k$ iff $n = 2k+1 = 6m+3$ for some $m \in \mathbb{N}^*$. □

Finally, in the next theorem we prove (1.2) for the case n is an odd positive integer. The theorem also contains an auxiliary result which will be used in Section 5. A permutation $a \in S_n$ is called *maximal* if $K_n(a) = \max\{K_n(c) | c \in S_n\}$.

Theorem 4.2 *Let $n = 2k+1$ with $k \in \mathbb{N}$ and $a \in S_n$. Then $K_n(a) \leq k^2 - k$. Furthermore, if $K_n(a)$ is maximal, then there is a sequence $a = a^{(0)}, a^{(1)}, \ldots, a^{(t)}$ of permutations in S_n such that* (i) *$a^{(j)} = a^{(j-1)}\langle i_j, i_j+1\rangle$ for $1 \leq j \leq t$ and for some i_j with $a^{(j-1)}_{i_j}$ and $a^{(j-1)}_{i_j+1}$ in different cycles of $a^{(j-1)}$, and* (ii) *$a^{(t)}$ is maximal and has the form described in Lemma 4.1.*

Proof: For $n = 1$ the inequality is obvious, so we assume $n \geq 3$ (i.e., $k \geq 1$). Suppose that $a \in S_n$ and $K_n(a)$ is maximal. Consider the following algorithm applied to a:

1. Set $a^{(0)} \leftarrow a$ and $j \leftarrow 1$.
2. If there is an $i \in \{1, 2, \ldots, n\}$ for which $a^{(j-1)}_i = i$, choose such an i arbitrarily, set $a^{(j)} \leftarrow a^{(j-1)}\langle i, i+1\rangle$, $j \leftarrow j+1$, and go to Step 2 (i.e., repeat this step).
3. If there is an $i \in \{1, 2, \ldots, n-1\}$ for which $a^{(j-1)}_i < i < a^{(j-1)}_{i+1}$, then choose one such i arbitrarily, set $a^{(j)} \leftarrow a^{(j-1)}\langle i, i+1\rangle$, $j \leftarrow j+1$, and go to Step 2.
4. Output $\widetilde{a} = a^{(j-1)}$ and terminate.

We first claim that this algorithm must terminate. For an arbitrary permutation $b \in S_n$ define $M_n(b) := \sum_{m=1}^{n} m \operatorname{sgn}(m - b_m)$. Trivially we have that $-n(n+1)/2 \leq M_n(b) \leq n(n+1)/2$ for all $b \in S_n$. Each time a swap is performed with $i < n$ in Step 2 or Step 3, we have

$$\begin{aligned} M_n(a^{(j)}) &= \sum_{m=1}^{n} m \operatorname{sgn}(m - a^{(j)}_m) \\ &= M_n(a^{(j-1)}) - i \operatorname{sgn}(i - a^{(j-1)}_i) - (i+1)\operatorname{sgn}(i+1-a^{(j-1)}_{i+1}) \\ &\qquad + i \operatorname{sgn}(i - a^{(j-1)}_{i+1}) + (i+1)\operatorname{sgn}(i+1-a^{(j-1)}_i) \\ &= M_n(a^{(j-1)}) + i\Big(\operatorname{sgn}(i - a^{(j-1)}_{i+1}) - \operatorname{sgn}(i - a^{(j-1)}_i)\Big) \\ &\qquad + (i+1)\Big(\operatorname{sgn}(i+1-a^{(j-1)}_i) - \operatorname{sgn}(i+1-a^{(j-1)}_{i+1})\Big). \end{aligned}$$

Each time a swap is performed in Step 2 with $i < n$ we therefore have that

$$M_n(a^{(j)}) = M_n(a^{(j-1)}) + \begin{cases} i, & \text{if } a^{(j-1)}_{i+1} < i, \\ 1, & \text{if } a^{(j-1)}_{i+1} = i+1, \\ i+2, & \text{if } a^{(j-1)}_{i+1} > i+1. \end{cases}$$

Each time a swap is performed in Step 2 with $i = n$, we have that

$$M_n(a^{(j)}) = M_n(a^{(j-1)}) + \begin{cases} n-1, & \text{if } a^{(j-1)}_1 = 1, \\ n, & \text{if } a^{(j-1)}_1 > 1. \end{cases}$$

Finally, each time a swap is performed in Step 3 we must have that $a^{(j-1)}_{i+1} \neq i+1$, so that $a^{(j-1)}_{i+1} > i+1$, and it follows that $M_n(a^{(j)}) = M_n(a^{(j-1)}) + 2$. In any case, we have $M_n(a^{(j)}) \geq 1 + M_n(a^{(j-1)})$ whenever both $a^{(j)}$ and $a^{(j-1)}$ are defined, and so the algorithm must terminate.

By Lemma 3.1, $K_n(\widetilde{a}) \geq K_n(a)$, but since $K_n(a)$ was maximal, we must have $K_n(\widetilde{a}) = K_n(a)$. It follows also that each time a swap is performed in Step 2 or Step 3, $a_i^{(j-1)}$ and $a_{i+1}^{(j-1)}$ are in different cycles of $a^{(j-1)}$, otherwise it would be the case that $K_n(a^{(j)}) > K_n(a^{(j-1)})$.

Consider the finite sequence $(\delta_i : i = 1, \ldots, n)$ given by $\delta_i := \widetilde{a}_i - i$. Since $\widetilde{a}$ has no fixed points, $\delta_1 > 0$ and $\delta_n < 0$, so there is at least one sign change from positive to negative in this sequence. If there were two or more such sign changes, then there would have to also be at least one sign change from negative to positive, say $\delta_\nu < 0$ and $\delta_{\nu+1} > 0$ for some $\nu \in \{1, 2, \ldots, n-2\}$. But this gives $\widetilde{a}_\nu < \nu < \widetilde{a}_{\nu+1}$ and the algorithm could not have terminated with this $\widetilde{a}$. Thus, the sequence $\delta_1, \ldots, \delta_n$ has exactly one sign change. So there is an $r \in \{1, \ldots, n-1\}$ such that $\widetilde{a}_j > j$ for all $j \in \{1, \ldots, r\}$ and $\widetilde{a}_j < j$ for $j \in \{r+1, \ldots, n\}$. Appealing again to Lemma 3.1, we may, without changing the value of K_n, sort the first r entries and the last $n - r$ entries to be ascending, using a bubble sort which swaps only entries of the form $\widetilde{a}_i, \widetilde{a}_{i+1}$ with $\widetilde{a}_i > \widetilde{a}_{i+1}$. [It follows from Lemma 3.1 that for any inversion of $\widetilde{a}$ of the form $j < \widetilde{a}_{j+1} < \widetilde{a}_j$ (for $j \in \{1, \ldots, r-1\}$) or of the form $\widetilde{a}_{j+1} < \widetilde{a}_j < j$ (for $j \in \{r+1, \ldots, n-1\}$) we can switch $\widetilde{a}_j$ with $\widetilde{a}_{j+1}$ and still keep K_n maximal.] Again, each time such a swap is performed, we must have that $\widetilde{a}_i$ and $\widetilde{a}_{i+1}$ are in different cycles since $K_n(\widetilde{a})$ is maximal. After such a sort, we obtain an $f \in S_n$ with

$$1 < f_1 < f_2 < \cdots < f_r \quad \text{and} \quad f_{r+1} < f_{r+2} < \cdots < f_n.$$

Now if $f_n > f_1$, we again invoke Lemma 3.1 to swap f_n and f_1 (which must again be in different cycles of f since $K_n(f)$ is maximal) and then re-sort the left and right halves. Repeating this as necessary, we obtain a $g \in S_n$ with $K_n(g) = K_n(f) = K_n(\widetilde{a})$ and such that

$$1 < g_1 < g_2 < \cdots < g_r, \quad g_{r+1} < g_{r+2} < \cdots < g_n, \quad \text{and } g_n < g_1.$$

This $g \in S_n$ therefore has the form described in Lemma 4.1, which proves the result. □

5 The equality case when n is odd

In this section of the paper we investigate when equality holds in (1.2) (or equivalently in the right inequality in (1.9)) when $n = 2k+1$ for some $k \in \mathbb{N}^* \backslash \{1\}$. Recall that we call any permutation in S_n that satisfies equality in (1.2) as *maximal.* We show that the number of permutations in S_n that satisfy the equality is a function of the Lucas number L_n: when $n = 6m + 3$ for $m \in \mathbb{N}^*$, there are exactly $2L_n + 2 - n$ maximal permutations in S_n, while if $n = 6m + 1$ or $6m + 5$ for $m \in \mathbb{N}$, there are exactly $2L_n - n$ maximal permutations in S_n. (For $m = 0$ and $n = 1$ the last statement is trivially true.)

5.1 Neighboring maximal permutations

For each $a \in S_n$ with $n \geq 2$ define $\mathcal{C}_n(a)$ to be the set of all $b \in S_n$ such that b can be obtained from a by switching two consecutive elements a_i and a_{i+1} of a (where $i \in \{1, 2, \ldots, n\}$) that are in the same cycle. In this definition, we assume that $n+1 := 1$, i.e., a_n and a_1 are assumed to be consecutive elements of a. For example, if $n = 4$ and $a = (4, 3, 2, 1)$, then

$$\mathcal{C}_4(a) = \{(1, 3, 2, 4), (4, 2, 3, 1)\}$$

because a has two cycles (1 with 4 and 2 with 3).

Next, we define $\mathcal{I}_n(a)$ to be the set of all $b \in S_n$ for which there is $m \in \mathbb{N}^*$ and a finite sequence $b^{(1)}, \ldots, b^{(m)}$ in S_n such that $b^{(1)} = a$, $b^{(m)} = b$, and

$$b^{(j+1)} \in \mathcal{C}_n(b^{(j)}) \quad \text{for } j = 1, 2, \ldots, m-1.$$

(If $b = a$, then $m = 1$ and the last condition holds vacuously. In other words, $\mathcal{I}_n(a)$ always contains the permutation a.) In our previous example, with $n = 4$ and $a = (4, 3, 2, 1)$, we have

$$\mathcal{I}_4(a) = \{(4, 3, 2, 1), (1, 3, 2, 4), (4, 2, 3, 1), (1, 2, 3, 4)\}.$$

Note that if $a = e_n$, then $\mathcal{I}_n(a) = \{e_n\}$.

Lemma 5.1 *Let $n \geq 5$ be an odd positive integer and $a \in S_n$. If $n \not\equiv 3 \pmod 6$, then a is maximal if and only if $a \in \mathcal{I}_n(\alpha_{1,n}) \cup \mathcal{I}_n(\alpha_{2,n})$. If $n \equiv 3 \pmod 6$, then a is maximal if and only if $a \in \mathcal{I}_n(\alpha_{1,n}) \cup \mathcal{I}_n(\alpha_{2,n}) \cup \{\beta_{1,n}, \beta_{2,n}\}$.*

Proof: If $a \in S_n$ is maximal then by Theorem 4.2 there is a sequence $a = a^{(0)}, a^{(1)}, \ldots, a^{(t)}$ of permutations in S_n such that $a^{(j)} = a^{(j-1)}\langle i_j, i_j + 1\rangle$ and $a^{(j-1)}_{i_j}$, $a^{(j-1)}_{i_j+1}$ are in different cycles of $a^{(j-1)}$, and $a^{(t)}$ is maximal with the form described in Lemma 4.1. It follows that $a^{(j-1)} \in \mathcal{C}_n(a^{(j)})$ for $1 \leq j \leq t$, so that $a = a^{(0)} \in \mathcal{I}_n(a^{(t)})$.

Conversely, if α is a maximal permutation of the form described in Lemma 4.1 and $a \in \mathcal{I}_n(\alpha)$, then by Lemma 3.1, $K_n(a) \geq K_n(\alpha)$, and so a is maximal as well.

Finally, suppose that $n \equiv 3 \pmod 6$ and $n = 2k + 1$. Then $k \equiv 1 \pmod 3$ and $\beta_{1,n}(i) \equiv i + k - 1 \pmod n$, so $\beta_{1,n}(i) \equiv i \pmod 3$. In particular, no two consecutive elements $\beta_{1,n}(i), \beta_{1,n}(i+1)$ are in the same cycle of $\beta_{1,n}$. Therefore $\mathcal{I}_n(\beta_{1,n}) = \{\beta_{1,n}\}$. Similarly, since $\beta_{2,n}(i) \equiv i + k + 2 \pmod n$, it follows that $\beta_{2,n}(i) \equiv i \pmod 3$ and so $\mathcal{I}_n(\beta_{2,n}) = \{\beta_{2,n}\}$. □

5.2 Maximal permutations and Lucas numbers

We count the number of maximal permutations by characterizing elements of $\mathcal{I}_n(\alpha_{\ell,n})$ (for each $\ell \in \{1, 2\}$) in terms of their cycle structure. For the remainder of this section, we assume $n = 2k + 1 \geq 5$.

Definition 5.2 *Let $\gamma = \langle g_1, \ldots, g_m \rangle \in S_n$ and $i \in \{1, 2, \ldots, m\}$. The cycle obtained from γ by deleting g_i is defined to be*

$$\gamma - \{g_i\} := \langle g_1, \ldots, g_{i-1}, g_{i+1}, \ldots, g_m \rangle.$$

The cycle obtained from γ by deleting $g_{i_1}, \ldots, g_{i_t}$ is inductively defined by

$$\gamma - \{g_{i_1}, \ldots, g_{i_t}\} := \Big(\gamma - \{g_{i_1}, \ldots, g_{i_{t-1}}\}\Big) - \{g_{i_t}\}.$$

For example, $\langle 1, 4, 7, 3, 6, 2, 5 \rangle - \{3, 6\} = \langle 1, 4, 7, 2, 5 \rangle$; this example is valid in S_n for all $n \geq 7$.

Theorem 5.3 *Let $\ell \in \{1, 2\}$ and $\alpha_{\ell,n} = \langle a_1, \ldots, a_n \rangle$. A permutation $\beta \in S_n$ is in $\mathcal{I}_n(\alpha_{\ell,n})$ if and only if β has a disjoint cycle decomposition of the form*

$$\beta = \langle a_{i_1}, a_{i_1+1} \rangle \cdots \langle a_{i_t}, a_{i_t+1} \rangle \Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_t}, a_{i_t+1}\}\Big).$$

Proof: Suppose first that $\beta \in \mathcal{I}_n(\alpha_{\ell,n})$. Then there is a sequence $b^{(0)}, b^{(1)}, \ldots, b^{(t)}$ of permutations in S_n such that $b^{(0)} = \alpha_{\ell,n}$, $b^{(t)} = \beta$, and $b^{(j+1)} \in \mathcal{C}_n(b^{(j)})$ for $0 \leq j < t$. We use mathematical induction on j to prove that the permutations in this sequence have a disjoint cycle decomposition as claimed in the statement of the theorem. For $j = 0$, note that $b^{(0)}$ trivially has such a decomposition (with no 2-cycles).

Suppose $j \in \{0, 1, \ldots, t-1\}$ and $b^{(j)}$ has a disjoint cycle decomposition of the form

$$b^{(j)} = \langle a_{i_1}, a_{i_1+1} \rangle \cdots \langle a_{i_j}, a_{i_j+1} \rangle \widetilde{b},$$

where $\widetilde{b} = \Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_j}, a_{i_j+1}\}\Big)$. Further suppose that $b^{(j+1)} \in \mathcal{C}_n(b^{(j)})$, so that there exists an i for which $b_i^{(j)}$ and $b_{i+1}^{(j)}$ are in the same cycle of $b^{(j)}$ and $b^{(j+1)} = b^{(j)}\langle i, i+1 \rangle$.

Case I: Suppose $\ell = 1$. Since i and $i+1$ are in the same cycle as $b_i^{(j)}$ and $b_{i+1}^{(j)}$ and $a_{m+1} \equiv a_m + k \pmod{n}$, they cannot be in any of the transpositions, so they are all contained in the cycle $\widetilde{b}$. If $i + 1 = a_r$ then $a_{r+2} = i$. Since $\widetilde{b}$ is obtained by deleting consecutive pairs of elements from $\alpha_{1,n}$, it follows that a_{r+1} was not deleted, so $b_{i+1}^{(j)} = a_{r+1}$. Observe now that

$$\widetilde{b} = \langle \ldots, a_r = i+1,\ a_{r+1} = b_{i+1}^{(j)},\ a_{r+2} = i,\ b_i^{(j)}, \ldots \rangle.$$

Therefore,

$$\begin{aligned} \widetilde{b}\langle i, i+1 \rangle &= \langle i, b_{i+1}^{(j)} \rangle (\widetilde{b} - \{i, b_{i+1}^{(j)}\}) \\ &= \langle a_{r+2}, a_{r+1} \rangle (\widetilde{b} - \{a_{r+2}, a_{r+1}\}) \\ &= \langle a_{r+1}, a_{r+2} \rangle (\widetilde{b} - \{a_{r+1}, a_{r+2}\}). \end{aligned}$$

Hence $b^{(j+1)} = b^{(j)}\langle i, i+1\rangle$ has the disjoint cycle decomposition $b^{(j+1)} =$

$$\langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_j}, a_{i_j+1}\rangle\langle a_{r+1}, a_{r+2}\rangle\Big(\alpha_{1,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_j}, a_{i_j+1}, a_{r+1}, a_{r+2}\}\Big).$$

Case II: Suppose $\ell = 2$. Since $i, i+1, b_i^{(j)}, b_{i+1}^{(j)}$ are in the same cycle and $a_{m+1} \equiv a_m + k + 1 \pmod{n}$, it follows as above that they are in the cycle $\widetilde{b}$. If $i = a_r$, then $a_{r+2} = i+1$ and as above we must have that $a_{r+1} = b_i^{(j)}$, and so

$$\widetilde{b} = \langle \ldots, a_r = i,\ a_{r+1} = b_i^{(j)},\ a_{r+2} = i+1,\ b_{i+1}^{(j)}, \ldots\rangle.$$

Again, it follows that

$$\begin{aligned}\widetilde{b}\langle i, i+1\rangle &= \langle i+1, b_i^{(j)}\rangle(\widetilde{b} - \{i+1, b_i^{(j)}\})\\ &= \langle a_{r+1}, a_{r+2}\rangle(\widetilde{b} - \{a_{r+1}, a_{r+2}\}).\end{aligned}$$

Therefore $b^{(j+1)}$ has the disjoint cycle decomposition $b^{(j+1)} =$

$$\langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_j}, a_{i_j+1}\rangle\langle a_{r+1}, a_{r+2}\rangle\Big(\alpha_{1,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_j}, a_{i_j+1}, a_{r+1}, a_{r+2}\}\Big)$$

and this completes the mathematical induction of this part of the proof.

For the converse, consider the collection $\mathcal{B}_{\ell,n,t}$ of permutations in S_n whose disjoint cycle decomposition is of the form

$$\beta = \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_t}, a_{i_t+1}\rangle\Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_t}, a_{i_t+1}\}\Big),$$

and has exactly t cycles of length 2 (and one cycle of length $n-2t$). By induction on t, we shall show that $\mathcal{B}_{\ell,n,t} \subseteq \mathcal{I}_n(\alpha_{\ell,n})$ for $t \in \{0, 1, \ldots, k\}$. If $t = 0$, then $\mathcal{B}_{\ell,n,0} = \{\alpha_{\ell,n}\}$ and $\alpha_{\ell,n} \in \mathcal{I}_n(\alpha_{\ell,n})$, so assume that $k \geq T \geq 1$ and $\mathcal{B}_{\ell,n,T-1} \subseteq \mathcal{I}_n(\alpha_{\ell,n})$.

Let $\gamma \in \mathcal{B}_{\ell,n,T}$ have a disjoint cycle decomposition

$$\gamma = \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_T}, a_{i_T+1}\rangle\Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_T}, a_{i_T+1}\}\Big).$$

Let $r \in \{1, 2, \ldots, n\}$ be such that a_r is in the cycle $\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_T}, a_{i_T+1}\}$ but a_{r+1} and a_{r+2} are not. Then $r+1 = i_j$ for some j; without loss of generality, assume $r+1 = i_T$. Define

$$b := \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_{T-1}}, a_{i_{T-1}+1}\rangle\widetilde{b},$$

where $\widetilde{b} := \alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_{T-1}}, a_{i_{T-1}+1}\}$ (and we assume this is the disjoint cycle decomposition of b). Then $\widetilde{b} = \langle \ldots, a_r, a_{r+1}, a_{r+2}, \ldots\rangle$. Note also that, by the induction hypothesis, $b \in \mathcal{B}_{\ell,n,T-1} \subseteq \mathcal{I}_n(\alpha_{\ell,n})$.

Case I: Suppose $\ell = 1$. Let $i = a_{r+2}$ so that $a_r \equiv i+1 \pmod{n}$. Since both i and $i+1$ are in the cycle $\widetilde{b}$ of b, so are b_i and b_{i+1}. Furthermore, $\widetilde{b}\langle i, i+1\rangle = \widetilde{b}\langle a_{r+2}, a_r\rangle = \langle a_{r+1}, a_{r+2}\rangle\Big(\widetilde{b} - \{a_{r+1}, a_{r+2}\}\Big)$, and so

$$\begin{aligned}b\langle i, i+1\rangle &= \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_{T-1}}, a_{i_{T-1}+1}\rangle\widetilde{b}\langle i, i+1\rangle\\ &= \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_{T-1}}, a_{i_{T-1}+1}\rangle\langle a_{r+1}, a_{r+2}\rangle\Big(\widetilde{b} - \{a_{r+1}, a_{r+2}\}\Big)\\ &= \gamma\end{aligned}$$

because $r+1 = i_T$. Therefore, $\gamma \in \mathcal{C}_n(b) \subseteq \mathcal{I}_n(\alpha_{1,n})$, and so $\mathcal{B}_{1,n,T} \subseteq \mathcal{I}_n(\alpha_{1,n})$.

Case II: Suppose $\ell = 2$. Let $i = a_r$, so that $a_{r+2} \equiv i+1 \pmod{n}$. Since both i and $i+1$ are in the cycle $\widetilde{b}$ of b, so are b_i and b_{i+1}. As above, we have that $\widetilde{b}\langle i, i+1\rangle = \langle a_{r+1}, a_{r+2}\rangle\Big(\widetilde{b} - \{a_{r+1}, a_{r+2}\}\Big)$, from which it again follows that $b\langle i, i+1\rangle = \gamma$. Thus, $\gamma \in \mathcal{C}_n(b) \subseteq \mathcal{I}_n(\alpha_{2,n})$, so that $\mathcal{B}_{2,n,T} \subseteq \mathcal{I}_n(\alpha_{2,n})$. □

Let F_m be the m-th Fibonacci number with $F_0 := 0$, $F_1 := 1$ and $F_{m+2} := F_{m+1} + F_m$. Let L_m be the m-th Lucas number with $L_0 := 2$, $L_1 := 1$ and $L_{m+2} := L_{m+1} + L_m$. Then we have the following result:

Theorem 5.4 *Let $n \geq 5$ be an odd positive integer. Then $\#\Big(\mathcal{I}_n(\alpha_{1,n}) \cup \mathcal{I}_n(\alpha_{2,n})\Big) = 2L_n - n$.*

Proof: Let $\ell \in \{1,2\}$. We first show that $\#\mathcal{I}_n(\alpha_{\ell,n}) = L_n$. Let $\alpha_{\ell,n} = \langle a_1, a_2, \ldots, a_n\rangle$. For $j \in \{0,1,\ldots,n\}$ (and fixed $\ell \in \{1,2\}$), let $\mathcal{D}_{n,j}$ be the set of permutations in S_n having a disjoint cycle decomposition of the form

$$\left\{\begin{array}{l} \langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_t}, a_{i_t+1}\rangle\Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_t}, a_{i_t+1}\}\Big), \\ \text{with } 1 \leq i_1 < i_1+1 < i_2 < \cdots < i_t < i_t+1 \leq j \text{ (for some } t \in \{0,1,\ldots,k\}). \end{array}\right. \tag{5.1}$$

Let also $f_n(j) = \#\mathcal{D}_{n,j}$. Clearly $f_n(0) = f_n(1) = 1$. For $j = n$, the number of permutations of the form (5.1) with $t \in \{1,2,\ldots,k\}$ and $i_t = n-1$ is $f_n(n-2)$. More generally, for each fixed $j \geq m+1$, the number of permutations of the form (5.1) with $t \geq 1$ and $i_t = m$ is $f_n(m-1)$ for $1 \leq m \leq n-1$. (This is because, for each $j \geq m+1$, there is an obvious bijection between $\mathcal{D}_{n,m-1}$ and the subset of permutations in $\mathcal{D}_{n,j}$ that have $i_t = m$.) There is one permutation of the form (5.1) which has $t = 0$; namely $\alpha_{\ell,n}$ itself. For $2 \leq m \leq n$, we may determine $f_n(m)$ by successively counting permutations whose "largest" transposition (i.e., the transposition with the maximal subscripts) is $\langle a_{m-1}, a_m\rangle, \langle a_{m-2}, a_{m-1}\rangle, \ldots, \langle a_1, a_2\rangle$. Counting in this way, and using the conditions $f_n(0) = f_n(1) = 1$, we find that

$$\begin{aligned} f_n(m) &= f_n(m-2) + f_n(m-3) + \cdots + f_n(0) + 1 \\ &= f_n(m-2) + f_n(m-1) \\ &= F_{m+1}. \end{aligned}$$

Every disjoint cycle decomposition of the form in Theorem 5.3 either has the form (5.1) or

$$\langle a_{i_1}, a_{i_1+1}\rangle \cdots \langle a_{i_t}, a_{i_t+1}\rangle\langle a_n, a_1\rangle\Big(\alpha_{\ell,n} - \{a_{i_1}, a_{i_1+1}, \ldots, a_{i_t}, a_{i_t+1}, a_n, a_1\}\Big)$$

for some $t \in \{0,1,2,\ldots,k-1\}$. By a re-indexing of the a_i's, it is easily seen that there are precisely $f_n(n-2)$ permutations of the latter form, and so

$$\#\mathcal{I}_n(\alpha_{\ell,n}) = \#\mathcal{D}_{n,n} + f_n(n-2) = F_{n+1} + f_n(n-2) = F_{n+1} + F_{n-1} = L_n.$$

We now show that $\#\Big(\mathcal{I}_n(\alpha_{1,n}) \cap \mathcal{I}_n(\alpha_{2,n})\Big) = n$, which will complete the proof. Suppose $\beta \in \mathcal{I}_n(\alpha_{1,n}) \cap \mathcal{I}_n(\alpha_{2,n})$. Writing $\alpha_{1,n} = \langle a_1, \ldots, a_n \rangle$, we have that $\alpha_{2,n} = \alpha_{1,n}^{-1} = \langle a_n, a_{n-1}, \ldots, a_1 \rangle$. It follows immediately that β cannot contain a cycle of length 3 or more, and hence it has a fixed point. For each $1 \leq j \leq n$, $\beta \in \mathcal{I}_n(\alpha_{1,n})$ has the fixed point a_j if and only if

$$\beta = \langle a_{j+1}, a_{j+2} \rangle \langle a_{j+3}, a_{j+4} \rangle \cdots \langle a_{j+2k-1}, a_{j+2k} \rangle \langle a_j \rangle.$$

On the other hand, such a β can also be written as

$$\beta = \langle a_{j-1}, a_{j-2} \rangle \langle a_{j-3}, a_{j-4} \rangle \cdots \langle a_{j-2k+1}, a_{j-2k} \rangle \langle a_j \rangle,$$

so that every such permutation is also in $\mathcal{I}_n(\alpha_{2,n})$, which completes the proof. □

A Appendix

A.1 A simple characterization of the dihedral group

Here we prove a simple property of the dihedral group that is needed in the proof of Theorem 2.3. Letting $b_{n+1} := b_1$, we define the following sets for each integer $n \geq 3$:

$$\begin{aligned}
\Omega_{n1} &:= \{b \in S_n \,|\, [b_{i+1} - b_i \in \{1, 1-n\} \text{ for } i = 1, \ldots, n]\}; \\
\Omega_{n2} &:= \{b \in S_n \,|\, [b_{i+1} - b_i \in \{-1, n-1\} \text{ for } i = 1, \ldots, n]\}; \\
\Omega_n &:= \Omega_{n1} \cup \Omega_{n2}; \quad \text{and} \\
\widetilde{\Omega}_n &:= \{b \in S_n \,|\, |b_{i+1} - b_i| \in \{1, n-1\} \text{ for } i = 1, 2, \ldots, n\}.
\end{aligned}$$

We then have the following result:

Lemma A.1 *For $n \geq 3$ we have* $\mathrm{Dih}_n = \Omega_n = \widetilde{\Omega}_n$.

Proof: Observe that $e_n \in \Omega_n$. Let $z, w \in \Omega_n$. If $z_{i+1} - z_i$ and $w_{i+1} - w_i$ are both in $\{1, 1-n\}$ for $i = 1, \ldots, n$, or $z_{i+1} - z_i$ and $w_{i+1} - w_i$ are both in $\{-1, n-1\}$ for $i = 1, \ldots, n$, then

$$z(w(i+1)) - z(w(i)) \in \{1, 1-n\} \quad \text{for} \quad i = 1, \ldots, n.$$

On the other hand, if $z_{i+1} - z_i$ is in $\{1, 1-n\}$ for $i = 1, \ldots, n$ and $w_{i+1} - w_i$ is in $\{-1, n-1\}$ for $i = 1, \ldots, n$, or vice versa, then

$$z(w(i+1)) - z(w(i)) \in \{-1, n-1\} \quad \text{for} \quad i = 1, \ldots, n.$$

Therefore $zw \in \Omega_n$. Finally, let $b \in S_n$, and assume $b_{i+1} - b_i \in \{1, 1-n\}$ for $i = 1, \ldots, n$. Then (by letting $i := b^{-1}(j)$) we get

$$b(b^{-1}(j+1)) = j + 1 = b(b^{-1}(j)) + 1 = b(b^{-1}(j) + 1),$$

with the understanding that $b^{-1}(j) + 1 := 1$ when $b^{-1}(j) = n$. Thus $(b^{-1})_{j+1} = (b^{-1})_j + 1$ for $j = 1, \ldots, n$, and $b^{-1} \in \Omega_n$. If $b_{i+1} - b_i \in \{-1, -1+n\}$ for $i = 1, \ldots, n$, we can prove in a similar way that $b^{-1} \in \Omega_n$ (by letting $i := b^{-1}(j+1)$). Therefore Ω_n is a subgroup of S_n.

One can easily check that $\mathrm{Dih}_n \subseteq \Omega_n$: a rotation b satisfies $b_{i+1} - b_i \in \{1, 1-n\}$ for $i = 1, \ldots, n$, while a reflection b satisfies $b_{i+1} - b_i \in \{-1, n-1\}$ for $i = 1, \ldots, n$. Also, an element b of Ω_n is uniquely determined by the value of b_1 and whether we assume b satisfies the first condition or the second condition, i.e., $\#\Omega_n = 2n$. It follows that $\Omega_n = \mathrm{Dih}_n$.

It is clear that $\Omega_n \subseteq \widetilde{\Omega}_n$. To show that $\widetilde{\Omega}_n \subseteq \Omega_n$, let $b \in \widetilde{\Omega}_n$. Assume $b_j = n$ for some $j \in \{1, 2, \ldots, n\}$. Since $|n - b_{j-1}| \in \{1, n-1\}$ and $|b_{j+1} - n| \in \{1, n-1\}$ (where we define $1 - 1 := n$ and $n + 1 := 1$), we have $\{b_{j-1}, b_{j+1}\} = \{1, n-1\}$.

Assume first $b_{j-1} = 1$, in which case $b_{j+1} = n - 1$. If $n = 3$ then clearly $b \in \Omega_3$, otherwise assume $n \geq 4$ and note that $|1 - b_{j-2}| \in \{1, n-1\}$. We find that $b_{j-2} = 2$. If $n = 4$, then clearly $b \in \Omega_4$, otherwise we assume $n \geq 5$ and continue this line of thought. Essentially, this argument shows that $b_{i+1} - b_i \in \{-1, n-1\}$ for $i = 1, 2, \ldots, n$, which shows that $b \in \Omega_n$.

If, however, $b_{j-1} = n - 1$, then $b_{j+1} = 1$, and using a similar argument as above we can show that $b_{i+1} - b_i \in \{1, 1-n\}$ for $i = 1, \ldots, n$, and hence $b \in \Omega_n$. This completes the proof of the lemma. □

References

[1] M. Bóna, *Combinatorics of permutations*, 2nd ed., CRC Press (Boca Raton, 2012).

[2] M. Deza and T. Huang, Metrics on permutations, a survey, *J. Combin. Inform. System Sci.* 23 (1998), 173–185.

[3] P. Diaconis. *Group representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes–Monograph Series, Vol. 11 (Hayward, California, 1988).

[4] P. Diaconis and R. L. Graham, Spearman's footrule as a measure of disarray, *J. R. Stat. Soc. Ser. B Stat. Methodol.* 39 (1977), 262–268.

[5] V. Estivill-Castro, Generating nearly sorted sequences – The use of measures of disorder, *Electron. Notes Theor. Comput. Sci.* 91 (2004), 56–95.

[6] R. Fagin, R. Kumar, M. Mahdian, D. Sivakumar and E. Vee, Comparing partial rankings, *SIAM J. Discrete Math.* 20 (2006), 628–648.

[7] R. Fagin, R. Kumar and D. Sivakumar, Comparing top k lists, *SIAM J. Discrete Math.* 17 (2003), 134–160.

[8] P. Hadjicostas and K. B. Lakshmanan, Measures of disorder and straight insertion sort with erroneous comparisons, *Ars Combin.* 98 (2011), 259–288.

[9] P. Hadjicostas and C. Monico, A re-examination of the Diaconis-Graham inequality, *J. Combin. Math. Combin. Comput.* 87 (2013), 275–295.

[10] G. James and M. Liebeck, *Representations and characters of groups*, 2nd edition, Cambridge University Press (Cambridge, UK, 2001).

[11] D. E. Knuth, *The art of computer programming, Vol. 3: Sorting and Searching*, 2nd ed., Addison-Wesley (Reading, MA, 1998).

(Received 28 June 2014; revised 28 Aug 2015)