JCMCC

THE JOURNAL
of
COMBINATORIAL MATHEMATICS
and
COMBINATORIAL COMPUTING

A re-examination of the Diaconis-Graham inequality

Petros Hadjicostas

School of Mathematics, Statistics and Oper. Res.,
Victoria University of Wellington, PO Box 600,
Gate 7, Kelburn Parade
Wellington 6012, New Zealand,
e-mail: *petros.hadjicostas@msor.vuw.ac.nz*

and

Chris Monico

Department of Mathematics and Statistics,
Texas Tech University, Box 41042,
Lubbock, TX 79409-1042, USA,
e-mail: *c.monico@ttu.edu*

Abstract

In this paper we give an alternative and more intuitive proof to one of two classic inequalities given by Diaconis and Graham in 1977. The inequality involves three metrics on the symmetric group, i.e., the set of all permutations of the first n positive integers. Our technique for the proof of the inequality allows us to resolve an open problem posed in that paper: When does equality hold? It also allows us to estimate how often equality holds. In addition, our technique can sometimes be applied for the proof of other inequalities between metrics or pseudo-metrics on the symmetric group.

JCMCC **87** (2013), pp. 275-295

1 Introduction

The distance between any two permutations a and b in the symmetric group S_n on n elements (that is, the set of all permutations of the set $\{1, \ldots, n\}$) can be measured by right-invariant metrics or pseudo-metrics introduced and studied by Diaconis and Graham (1977), Cohen and Deza (1980), Estivill-Castro (1991), and Estivill-Castro *et al.* (1993). The distance between a permutation a in S_n and the identity id $= (1, 2, \ldots, n)$ can be considered as a measure of disorder or disarray of a and quantifies the deviation of the permutation a from the (sorted in ascending way) identity id. Properly standardized, a distance between two permutations a and b in S_n can be transformed into a (non-parametric) rank correlation coefficient between a and b that takes values in the interval $[-1, 1]$.

In this paper, we give an alternative and more intuitive proof to one of two classic inequalities given by Diaconis and Graham (1977). The inequality involves three metrics on the symmetric group – see the left result in (5) below. Our technique for the proof of the inequlity allows us to resolve an open problem posed in that paper: When does equality hold? It also allows us to estimate how often equality holds. Even more, our technique can sometimes be applied for the proof of other inequalities.

We begin the paper with a general introduction to pseudo-metrics and measures of disorder on the symmetric group S_n. We continue with a discussion of the properties of four such pseudo-metrics, and review several inequalities that relate them. In doing so, we provide alternative proofs to some of these inequalities.

A *pseudo-metric* sequence is a list of functions

$$(d_n : S_n \times S_n \to \mathbb{R} | n \in \mathbb{N}^*)$$

satisfying the following properties:

1. For all $n \in \mathbb{N}^*$ and $a, b \in S_n$, $d_n(a, b) \geq 0$, and equality holds if and only if $a = b$.

2. For all $n \in \mathbb{N}^*$ and $a, b \in S_n$, $d_n(a, b) = d_n(b, a)$.

3. There is a constant $M > 0$ such that for all $n \in \mathbb{N}^*$ and all $a, b, c \in S_n$,

$$d_n(a,b) \leq M[d_n(a,c) + d_n(c,b)].$$

In the above definition, we denote by $\mathbb{R}$ the set of real numbers and by $\mathbb{N}^*$ the set of positive integers. If a pseudo-metric sequence satisfies property 3 with $M = 1$, then each function d_n is a *metric* on S_n, and the last property is the usual triangle inequality.

If a pseudo-metric sequence $(d_n : S_n \times S_n \to \mathbb{R} | n \in \mathbb{N}^*)$ satisfies the property

$$d_n(a \circ c) = d_n(b \circ c)$$

for all $n \in \mathbb{N}^*$ and $a, b, c \in S_n$, then it is called *right-invariant*. Here $\circ$ denotes composition between permutations in the same symmetric group. Right-invariance implies that

$$d_n(a,b) = d(a \circ b^{-1}, \mathrm{id}) = d(\mathrm{id}, b \circ a^{-1}) \qquad (1)$$

for $n \in \mathbb{N}^*$ and $a, b \in S_n$. In particular, $d_n(a, id) = d_n(a^{-1}, \mathrm{id})$. (Here a^{-1} is the inverse permutation of a in S_n.) Because of these properties, by abusing notation, we define the *induced measures of disorder* sequence $(d_n : S_n \to \mathbb{R} | \, n \in \mathbb{N}^*)$ by

$$d_n(a) := d_n(a, \mathrm{id})$$

for $n \in \mathbb{N}^*$ and $a \in S_n$.

For all those $n \in \mathbb{N}^*$ for which

$$\max d_n = \max\{d_n(a,b) | \, a, b \in S_n\} > 0,$$

as suggested by Diaconis and Graham (1977), one can define an associated (non-parametric) rank correlation coefficient $r_n : S_n \times S_n \to [-1, 1]$ as follows:

$$r_n(a,b) = 1 - \frac{2\, d_n(a,b)}{\max d_n} \quad (a, b \in S_n).$$

The correlation coefficient equals 1 if and only if $a = b$, and -1 if and only if $d_n(a,b) = \max d_n$.

Over the years several pseudo-metrics, metrics, and measures of disorder or disarray on the symmetric group S_n have been proposed; see, for example, [2], [3], [5], [6], [7], [10], [11], [12], [16], [17], and [18]. In this paper, we work with four of these that are studied in Diaconis and Graham (1977). If $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ are permutations in S_n, we let:

(a) $I_n(a, b)$ = the minimum number of pairwise adjacent transpositions[1] required to bring a^{-1} into b^{-1};

(b) $EX_n(a, b)$ = the minimum number of transpositions needed to bring a into b;

(c) $D_n(a, b) = \sum_{i=1}^{n} |a_i - b_i|$;

(d) $SQ_n(a, b) = \sum_{i=1}^{n} (a_i - b_i)^2$.

The first three functions are metrics (and thus pseudo-metrics) on S_n, while the last one is only a pseudo-metric with constant $M = 2$ in property 3. These pseudo-metrics induce the following measures of disorder on S_n: For $a \in S_n$, $I_n(a)$ is the number of inversions in a, i.e., the number of pairs of integers (a_i, a_j) such that $1 \leq i < j \leq n$ and $a_i > a_j$; $EX_n(a)$ is the smallest number of exchanges (transpositions) of elements in a needed to leave it sorted; $D_n(a) = \sum_{i=1}^{n} |i - a_i|$; and $SQ_n(a) = \sum_{i=1}^{n} (i - a_i)^2$. A classical result by Cayley (see [1] and [17, Ex. 5.2.2-2, pp. 134 and 628]) states that $EX_n(a)$ equals n minus the number of cycles in the permutation a.

Because of equations (1) (that follow from right-invariance), for the rest of the paper, we concentrate only on the measures of disorder that the above four pseudo-metrics induce on S_n. For all $a \in S_n$, $I_n(a) \leq n(n-1)/2$ and $SQ_n(a) \leq (n-1)n(n+1)/3$, and each of these inequalities holds as equality if and only if $a = (n, n-1, \ldots, 1)$. In addition, for all $a \in S_n$, $D_n(a) \leq \lfloor n^2/2 \rfloor$ (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 $i = 1, 2, \ldots, n/2$ when n is even; and either $a_i > (n+1)/2$ for $i = 1, 2, \ldots, (n-1)/2$ or $a_i \geq (n+1)/2$ for $i = 1, \ldots, (n+1)/2$ when n is odd–see [7, p. 266] or [14, Lemma 2.4]. Finally, $EX_n(a) \leq n - 1$ 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).

[1] That is, transpositions consisting of adjacent elements.

There are several inequalities among these measures of disorder, and each such inequality can be transformed into an inequality involving corresponding pseudo-metrics using equations (1)[2]. In addition to the obvious $EX_n(a) \leq I_n(a)$, we mention, for example, two inequalities stated in 1984 by Ecker [9]:

$$2I_n(a) \leq SQ_n(a) \leq 2(n-1)I_n(a). \tag{2}$$

Daniels [4] proved the following inequalities:

$$nI_n(a) - \frac{n(n-1)(n-2)}{6} \leq SQ_n(a) \leq nI_n(a). \tag{3}$$

Durbin and Stuart (see [8] or [16, pp. 13 and 29-32]) proved the following classic inequality:

$$SQ_n(a) \geq \frac{4}{3}I_n(a)\left(1 + \frac{I_n(a)}{n}\right).$$

The following two inequalities are found in the last section of a paper by Diaconis and Graham [7]:

$$\frac{SQ_n(a)}{n-1} \leq D_n(a) \leq \min[SQ_n(a), (n\, SQ_n(a))^{1/2}]. \tag{4}$$

In [7], Diaconis and Graham prove the following two inequalities:

$$I_n(a) + EX_n(a) \leq D_n(a) \leq 2I_n(a). \tag{5}$$

The proof of the right inequality is quite easy, but the proof of the left one is quite involved. In this paper we give an alternative and more intuitive proof of the left inequality, and give some necessary and sufficient conditions for equality to hold. According to Diaconis and Graham [7, p. 268] and to the best of our knowledge, this is an open problem.

In Section 2 of the paper we introduce the inversion list $((\lambda_i, \mu_i) : i = 1, \ldots, n)$ of a permutation $a \in S_n$ and give another proof of the right inequality in (5) (which of course was proved by Diaconis and

[2]For example, the inequality $EX_n(a) \leq I_n(a)$ becomes $EX_n(a,b) \leq I_n(a,b)$ for $a, b \in S_n$.

Graham [7] in an equally easy way). In Section 3, we then examine what happens to the inversion list and the above measures of disorder when we switch two elements of a that form an inversion and belong to the same cycle. We show that (under certain conditions) the value of the quantity

$$K_n(a) := D_n(a) - I_n(a) - EX_n(a)$$

decreases or stays the same when we switch two such elements of a. We use this fact to give an alternative proof to the left inequality in (5), and give some necessary and sufficient conditions for equality to hold (see Section 4). The paper concludes with Section 5, where we give some insight on how often equality holds in the left Diaconis-Graham inequality.

For $n \in \mathbb{N}^*$ and $a \in S_n$, and integers i and j with $1 \le i < j \le n$, define $\delta(i,j)$ to be 1 if $(a^{-1})_j < (a^{-1})_i$, and 0 otherwise. Here a^{-1} is the inverse permutation of permutation a. In other words, $\delta(i,j)$ is 1 if rank j preceeds rank i in a. Inequalities (2) both follow from the following Durbin and Stuart's results (see [8] and [9])

$$I_n(a) = \sum_{1 \le i < j \le n} \delta(i,j) \quad \text{and} \quad SQ_n(a) = \sum_{1 \le i < j \le n} 2(j-i)\delta(i,j), \quad (6)$$

and the fact that $1 \le j - i \le n-1$ whenever $1 \le i < j \le n$. We see from the second equation in (6) that $SQ(a)$ can be thought as the number of "weighted" inversions, where each inversion is weighted by twice the distance between the integers comprising the inversion.

Even though inequalities (2) both follow from (6), to illustrate the techniques of this paper, we derive the left inequality in (2) by proving that (under certain conditions) the value of the quantity

$$Q_n(a) := SQ_n(a) - 2I_n(a)$$

decreases or stays the same when we switch two elements of a that form an inversion and belong to the same cycle. Note that the technique of this paper is not always successful. For example, it cannot be used to prove either of Daniels' inequalities in (3) because the value of the quantity

$$R_n(a) := nI_n(a) - SQ_n(a)$$

sometimes increases when we switch two elements of a that form an inversion and belong to the same cycle.

2 The inversion list of a permutation

Let $n \in \mathbb{N}^*$ and $a \in S_n$, and for $i = 1, 2, \ldots, n$, define $\lambda_i = \lambda_i(a)$ to be the number of integers a_l such that $1 \leq l < i$ and $a_i < a_l$, and $\mu_i = \mu_i(a)$ to be the number of integers a_m such that $i < m \leq n$ and $a_m < a_i$. Obviously, $0 \leq \lambda_i \leq i-1$, $0 \leq \mu_i \leq n-i$, and

$$I_n(a) = \frac{1}{2}\sum_{i=1}^{n}(\lambda_i + \mu_i) = \sum_{i=1}^{n}\lambda_i = \sum_{i=1}^{n}\mu_i. \tag{7}$$

To the left of a_i there are $i - 1 - \lambda_i$ integers a_l with $1 \leq l < i$ and $a_l < a_i$. Since the total number of a_k's in a less than a_i is $a_i - 1$, we have $\mu_i + (i - 1 - \lambda_i) = a_i - 1$, which implies

$$\mu_i - \lambda_i = a_i - i. \tag{8}$$

It follows that

$$D_n(a) = \sum_{i=1}^{n}|\mu_i - \lambda_i| \quad \text{and} \quad SQ_n(a) = \sum_{i=1}^{n}(\mu_i - \lambda_i)^2. \tag{9}$$

Since $|\mu_i - \lambda_i| \leq \mu_i + \lambda_i$ (with equality if and only if $\mu_i\lambda_i = 0$), we immediately get

$$D_n(a) \leq 2I_n(a) \quad \text{and} \quad SQ_n(a) \leq SQ_n^+(a) := \sum_{i=1}^{n}(\mu_i + \lambda_i)^2. \tag{10}$$

The first inequality is the right inequality in (5) due to Diaconis and Graham [7]. Obviously, in each of the above inequalities, equality holds if and only if $\mu_i\lambda_i = 0$ for all $i \in \{1, \ldots, n\}$. Equalities and inequalities (7)-(10), albeit simple, will be used extensively in the rest of the paper. We call $((\lambda_i, \mu_i) : i = 1, \ldots, n)$ the *inversion list* of the permutation a.

We say that $a \in S_n$ has a 3-inversion if there are three elements a_i, a_j, a_k such that $1 \leq i < j < k \leq n$ and $a_i > a_j > a_k$. Using the notation in the previous paragraph, each of the inequalities

(10) becomes an equality if and only if a has no 3-inversions[3]. This claim (for the first inequality) was made by Diaconis and Graham [7]. They state that Knuth [17, Section 5.1.4] notes that the number of permutations in S_n with no 3-inversions is equal to the n^{th} Catalan number

$$C_n = \frac{1}{2n+1}\binom{2n+1}{n}.$$

The finite sequence $(\lambda_1, \dots, \lambda_n)$ is a permutation of the *inversion table* $(b_1, \dots, b_n)$ of a, which was discussed by Hall [15] and Knuth [17, Section 5.1.1]. The latter is obtained by letting b_k be the number of elements in a to the left of k that are greater than k. In exercises 5.1.1-7 and 8, Knuth [17] introduces another table, $(c_1, \dots, c_n)$, by letting c_k be the number of elements in a to the right of k that are less than k. The finite sequence $(\mu_1, \dots, \mu_n)$ is a permutation of the finite sequence $(c_1, \dots, c_n)$. Actually, in the same exercise he introduces the finite sequences of λ_k's and μ_k's using different notation than ours. He notes that $\lambda_k = b_{a_k}$ and $\mu_k = c_{a_k}$ for $k = 1, \dots, n$ (where a_k is the kth element of permutation $a \in S_n$ used in this section). In the solution to exercise 5.1.1-7 (see [17, p. 592]) he states that the c inversion table was discussed by Rodrigues [20] and the μ inversion table by Rothe in 1800. (We do not use the inversion tables $(b_1, \dots, b_n)$ and $(c_1, \dots, c_n)$ in this paper, and the quantities b_{ij} in the next section have different meaning.)

Since $|\mu_i - \lambda_i| \le \mu_i + \lambda_i \le n - 1$, we have

$$|\mu_i - \lambda_i|^2 \le (n-1)|\mu_i - \lambda_i|$$

for $i = 1, 2, \dots, n$. We immediately get from (9) that $SQ_n(a) \le (n-1)D_n(a)$, which is the left inequality in (4). Equality here holds if and only if $a = (1, 2, \dots, n)$ or $a = (n, 2, 3, \dots, n-1, 1)$. From the Diaconis-Graham inequality $D_n(a) \le 2I_n(a)$ we then get $SQ_n(a) \le 2(n-1)I_n(a)$, which is the right inequality in (2). In the latter inequality, equality holds if and only if $a = (1, 2, \dots, n)$ (unless $n = 2$ in which case equality holds iff $a = (1, 2)$ or $a = (2, 1)$).

[3]Permutations with no 3-inversions are called permutations that avoid the pattern "321." See, for example, [13], [19] and [21].

The quantity $SQ_n^+(a)$ introduced in (10) is obviously nonnegative, and equals zero if and only if $a = (1, 2, \ldots, n)$. Also

$$SQ_n^+(a) \leq n(n-1)^2$$

for all $a \in S_n$, and equality holds if and only if $a = (n, n-1, \ldots, 1)$. It would be interesting to find more inequalities between SQ_n^+, SQ_n and I_n (in addition to the second inequality in (10)).

The measure of disorder SQ_n^+ arises from a right-invariant pseudo-metric

$$SQ_n^+ : S_n \times S_n \to \mathbb{R},$$

which satisfies property 3 with $M = 2$, as follows: For $n \in \mathbb{N}^*$ and $a, h \in S_n$ (by abusing notation) define

$$\mu_i(a,h) := \#\{j \,|\, a_i > a_j \text{ and } h_i < h_j\};$$

$$\lambda_i(a,h) := \#\{j | a_i < a_j \text{ and } h_i > h_j\} = \mu_i(h,a);$$

and

$$SQ_n^+(a,h) := \sum_{i=1}^{n} (\mu_i(a,h) + \lambda_i(a,h))^2.$$

Note that $\mu_i(a, \mathrm{id}) = \mu_i(a)$ and $\lambda_i(a, \mathrm{id}) = \lambda_i(a)$, where $\mu_i(a)$ and $\lambda_i(a)$ are as defined at the beginning of the section. It follows that $SQ_n^+(a) = SQ_n^+(a, \mathrm{id})$. Finally, note that

$$\mu_i(a,h) - \lambda_i(a,h) = a_i - h_i \quad \text{and} \quad I_n(a,h) = \frac{1}{2}\sum_{i=1}^{n}(\mu_i(a,h) + \lambda_i(a,h)).$$

3 An analysis of the first Diaconis-Graham inequality

Let $n \in \mathbb{N}^*$ and $a \in S_n$, and fix integers i and j such that $1 \leq i < j \leq n$ and $a_i > a_j$ (i.e., the pair (a_i, a_j) is an inversion in list a). Define $\tilde{a} \in S_n$ to be the finite sequence obtained from a after exchanging a_i with a_j. Let b_{ij} be the number of integers k with $i < k < j$ and $a_i > a_k > a_j$. In other words, b_{ij} is the number of 3-inversions beginning with a_i and ending with a_j. Since there are

$j - i - 1$ numbers between i and j and $a_i - a_j - 1$ numbers between a_j and a_i, we have

$$b_{ij} \leq \min(a_i - a_j, j - i) - 1. \tag{11}$$

Some of the results in the following lemma are probably well-known. For example, part (i) is due to Knuth [17].

Lemma 3.1 (i) $I_n(\tilde{a}) = I_n(a) - (2b_{ij} + 1) \geq I_n(a) - 2\min(a_i - a_j, j - i) + 1$.

(ii) $SQ_n(\tilde{a}) = SQ_n(a) - 2(j - i)(a_i - a_j)$.

(iii) $D_n(\tilde{a}) = D_n(a) + |j - a_i| + |i - a_j| - |i - a_i| - |j - a_j|$.

Proof: (i) The first equality follows from the statement and solution of problem #5.2.2-1 (pp. 134 and 628) in Knuth [17]. The inequality follows from (11).

(ii) The equality follows from

$$SQ_n(\tilde{a}) = SQ_n(a) + (a_i - j)^2 + (a_j - i)^2 - (a_i - i)^2 - (a_j - j)^2.$$

(iii) It follows from the definition of $\tilde{a}$. □

Corollary 3.2 *If either $i \leq a_j < a_i \leq j$ or $a_j \leq i < j \leq a_i$, then:*

$$D_n(\tilde{a}) - D_n(a) = -2\min(a_i - a_j, j - i).$$

Proof: Assume first $i \leq a_j < a_i \leq j$. In this case $\min(a_i - a_j, j - i) = a_i - a_j$. It follows from Lemma 3.1, part (iii), that

$$D_n(\tilde{a}) - D_n(a) = (j - a_i) + (a_j - i) - (a_i - i) - (j - a_j) = -2(a_i - a_j).$$

The case $a_j \leq i < j \leq a_i$ can be proven in a similar fashion. □

Given $n \in \mathbb{N}^*$, for every permutation $h \in S_n$, define

$$\begin{aligned} K_n(h) &:= D_n(h) - I_n(h) - EX_n(h), \quad \text{and} \\ Q_n(h) &:= SQ_n(h) - 2I_n(h). \end{aligned}$$

Note that i and a_i are in the same cycle. The same holds for j and a_j. If the integers i, a_i, j, and a_j are all in the same cycle, we have the following lemma:

Lemma 3.3 *If the integers i, a_i, j, a_j are in the same cycle, and either $i \leq a_j < a_i \leq j$ or $a_j \leq i < j \leq a_i$, then:*

(i) $K_n(\tilde{a}) - K_n(a) \leq 0$, *and equality holds if and only if* $b_{ij} = \min(a_i - a_j, j - i) - 1$.

(ii) $Q_n(\tilde{a}) - Q_n(a) \leq 0$, *and equality holds if and only* $a_i = j = i + 1 = a_j + 1$.

Proof: Denote by $a^0 := (1, 2, \ldots, n)$, the identity in S_n, and $a^k := a^{k-1} \circ a$ for $k \in \mathbb{N}^*$. Let m denote the length of the cycle containing i, a_i, j, a_j. Obviously, $m \geq 2$. Assume $j = a^\nu(i)$ for some integer ν with $1 \leq \nu \leq m - 1$. Then $a_i = a^1(i)$ and $a_j = a^{\nu+1}(i)$. Switching a_i with a_j breaks the cycle $(i, a^1(i), a^2(i), \ldots, a^{m-1}(i))$ into two cycles,

$$(i, a^{\nu+1}(i), a^{\nu+2}(i), \ldots, a^{m-1}(i))$$

and

$$(a^\nu(i), a^1(i), a^2(i), \ldots, a^{\nu-1}(i)),$$

while it leaves the other cycles unchanged – see the statement and solution of problem #5.2.2-2 (pp. 134 and 628) in Knuth [17]. Therefore $\tilde{a}$ has one more cycle than a, and by Cayley's theorem – see Cayley [1] – we have $EX_n(\tilde{a}) = EX_n(a) - 1$. By Lemma 3.1, Corollary 3.2 and inequality (11),

$$K_n(\tilde{a}) - K_n(a) = 2(1 - \min(a_i - a_j, j - i) + b_{ij}) \leq 0,$$

and equality holds if and only if $b_{ij} = \min(a_i - a_j, j - i) - 1$.

By a similar argument,

$$\begin{aligned} Q_n(\tilde{a}) - Q_n(a) &= -2(j - i)(a_i - a_j) + 2(2b_{ij} + 1) \\ &\leq 2[2\min(a_i - a_j, j - i) \\ &\quad -(j - i)(a_i - a_j) - 1], \end{aligned} \tag{12}$$

and equality holds if and only if $b_{ij} = \min(a_i - a_j, j - i) - 1$. Since $x := j - i \geq 1$ and $y := a_i - a_j \geq 1$, we have $(x-1)(y-1) \geq 0$, which implies

$$xy + 1 \geq x + y \geq 2\min(x, y), \tag{13}$$

where both equalities hold simultaneously if and only if $x = y = 1$. Using (12) and (13), we conclude that $Q_n(\tilde{a}) - Q_n(a) \leq 0$ with equality holding if and only if $j - i = 1 = a_i - a_j$ and $b_{ij} = \min(a_i - a_j, j - i) - 1 = 0$. □

Now we are ready to give an alternative proof to Diaconis and Graham's first inequality. To illustrate the usefulness of our techniques, we also prove the left inequality in (2).

Theorem 3.4 *For each $n \in I\!N^*$ and $h \in S_n$, we have*

(i) $K_n(h) = D_n(h) - I_n(h) - EX_n(h) \geq 0$.

(ii) $Q_n(h) = SQ_n(h) - 2I_n(h) \geq 0$.

Proof: Let $h \in S_n$. If h consists only of cycles of length 1, then $h = (1, 2, \ldots, n)$, and thus $D_n(h) = EX_n(h) = I_n(h) = 0$, and the inequality holds as equality. Assume h has at least one cycle of length greater than or equal to 2. Let i be the smallest integer in h involved in a cycle of length at least 2. Then there is an integer j in h, not equal to i, such that $h_j = i$. The integers $i = h_j, h_i$, and j are in the same cycle, and thus $i < j$ and $h_i > i = h_j$. Let $\tilde{h}$ be the permutation in S_n obtained by switching h_i and $h_j = i$. Since either $h_j = i < j \leq h_i$ or $i = h_j < h_i < j$, by the first part of Lemma 3.3, $K_n(\tilde{h}) \leq K_n(h)$. Also, by Corollary 3.2, $D_n(\tilde{h}) < D_n(h)$. If $\tilde{h} = (1, 2, \ldots, n)$, then $K_n(\tilde{h}) = 0 \leq K_n(h)$. Otherwise, $\tilde{h}$ has at least one cycle of length at least 2, and we can repeat the above procedure to find a permutation $\hat{h} \in S_n$ such that $K_n(\hat{h}) \leq K_n(\tilde{h})$ and $D_n(\hat{h}) < D_n(\tilde{h})$. Since $D_n(g) \geq 0$ for all $g \in S_n$, the procedure has to terminate, and there is a finite sequence $h^{(0)}, h^{(1)}, \ldots, h^{(m)}$ of elements of S_n such that $h^{(0)} = h$,

$$K_n(h^{(0)}) \geq K_n(h^{(1)}) \geq \ldots \geq K_n(h^{(m)}),$$

and

$$D_n(h^{(0)}) > D_n(h^{(1)}) > \ldots > D_n(h^{(m)}) = 0.$$

Thus $h^{(m)} = (1, 2, \ldots, n)$ and $0 = K_n(h^{(m)}) \leq K_n(h)$, and the first part of the theorem has been proven.

The second inequality of the theorem can be proven using exactly the same methodology and the second part of Lemma 3.3. □

4 Analysis of the equality case

In this section of the paper we investigate when does equality hold in the Diaconis-Graham first inequality. In their paper, they have stated that the characterization of permutations in S_n for which equality holds in the first inequality is an open problem. Below we give necessary and sufficient conditions for a list $a \in S_n$ to satisfy $K_n(a) = 0$. These conditions essentially allow for the recursive construction of the set of all such permutations for each $n \in \mathbb{N}^*$. First for $n \geq 2$ and $a \in S_n$, define $a|_1 := (a_n, a_2, \ldots, a_{n-1})$ and $a|_n := (a_1, \ldots, a_{n-2}, a_{n-1})$. When $n \geq 3$ and $i \in \{2, \ldots, n-1\}$ define also

$$a|_i := (a_1, \ldots, a_{i-1}, a_n, a_{i+1}, \ldots, a_{n-1}).$$

Next let $M_1 := S_1$, and for each integer $n \geq 2$ let

$$\begin{aligned} M_{n1} &:= \{a \in S_n \mid \exists\, i \in \{1, \ldots, n-1\} : a_i = n,\ a|_i \in M_{n-1}, \\ &\qquad \text{and} \, [\lambda_i(a|_i) = 0 \, \text{or} \, \mu_i(a|_i) = 0]\}; \\ M_{n2} &:= \{a \in S_n \mid a_n = n \text{ and } a|_n \in M_{n-1}\}; \\ M_n &:= M_{n1} \cup M_{n2}. \end{aligned}$$

In other words, we can construct M_{n1} from M_{n-1} as follows: Take an $\hat{a} \in M_{n-1}$ and an integer i such that $1 \leq i \leq n-1$ and such that either the number of integers in $\hat{a}$ to the left of $\hat{a}_i$ that are greater than $\hat{a}_i$ is zero or the the number of integers in $\hat{a}$ to the right of $\hat{a}_i$ that are less than $\hat{a}_i$ is zero. Replace $\hat{a}_i$ with n and put $\hat{a}_i$ at the end to form an $a \in M_{n1}$. To construct M_{n2} from M_{n-1}, take an $\hat{a} \in M_{n-1}$ and attach n at the end to form an $a \in M_{n2}$. Finally define M_n as the union of M_{n1} and M_{n2}.

Theorem 4.1 *For each $n \in I\!N^*$ and $a \in S_n$, $K_n(a) = 0$ if and only if $a \in M_n$.*

Proof: We prove the theorem by induction on n. For $n = 1$ we have $M_1 = S_1 = \{(1)\}$ and $K_1((1)) = 0$, so the theorem is true in this case. Let $n \geq 2$ and assume the statement of the theorem is true for all integers m with $1 \leq m < n$. Let $a \in S_n$.

(i) Suppose first that $a \in M_n$. If $a \in M_{n2}$, then $a_n = n$ and $a|_n = (a_1, \ldots, a_{n-2}, a_{n-1}) \in M_{n-1}$ and $D_n(a) = D_{n-1}(a|_n)$, $I_n(a) = I_{n-1}(a|_n)$, and $EX_n(a) = EX_{n-1}(a|_n)$. Therefore $K_n(a) = K_{n-1}(a|_n) = 0$, where the latter equality follows from the induction hypothesis.

Assume now that $a \in M_{n1}$. Then there is $i \in \{1, \ldots, n-1\}$ such that $a_i = n$, $a|_i \in M_{n-1}$ and either $\lambda_i(a|_i) = 0$ or $\mu_i(a|_i) = 0$. Hence $\min[\lambda_i(a|_i), \mu_i(a|_i)] = 0$. By the induction hypothesis, $K_{n-1}(a|_i) = 0$. Since the i^{th} element of $a|_i$ is a_n, by (8),

$$a_n - i = \mu_i(a|_i) - \lambda_i(a|_i). \tag{14}$$

The latter equality implies $\lambda_i(a|_i) = \mu_i(a|_i) - (a_n - i)$, and hence $\min(\mu_i(a|_i) - (a_n - i), \mu_i(a|_i)) = 0$. It follows that

$$\mu_i = \mu_i(a|_i) = \max(0, a_n - i). \tag{15}$$

Note also μ_i is the number of integers among $a_{i+1}, \ldots, a_{n-1}$ that are less than a_n, and hence $n-1-i-\mu_i$ is the number of integers among $a_{i+1}, \ldots, a_{n-1}$ that are greater than a_n. (If $i = n-1$, then $\mu_i = 0$ and $n - 1 - i - \mu_i = 0$.)

Define $\tilde{a} = (a|_i, n)$, i.e., $\tilde{a}$ is created by attaching n at the end of $a|_i$. Since $i < n$, note that $\tilde{a}$ can be obtained from a by switching a_i and a_n. Note also that either $i \leq a_n < a_i = n$ or $a_n < i < n = a_i$ and the numbers i, a_n $a_i = n$ are in the same cycle of a. Also

$$\begin{aligned} b_{in}(a) &= \#\{k \mid i+1 \leq k \leq n-1 \text{ and } a_i = n > a_k > a_n\} \\ &= n - i - 1 - \mu_i(a|_i). \end{aligned} \tag{16}$$

(Here $\#A$ denotes the number of elements in the finite set A.) Using (15) we obtain

$$\begin{aligned} b_{in}(a) &= n - 1 - i - \max(0, a_n - i) \\ &= \min(n - i, n - a_n) - 1 = \min(n - i, a_i - a_n) - 1. \end{aligned}$$

By Lemma 3.3 we have $K_n(a) = K_n(\tilde{a}) = K_{n-1}(a|_i) = 0$.

(ii) Conversely, assume $K_n(a) = 0$. If $a_n = n$, then

$$a|_n = (a_1, \ldots, a_{n-2}, a_{n-1})$$

and $D_n(a) = D_{n-1}(a|_n)$, $I_n(a) = I_{n-1}(a|_n)$, and $EX_n(a) = EX_{n-1}(a|_n)$. Thus $K_{n-1}(a|_n) = K_n(a) = 0$. By the induction hypothesis $a|_n \in M_{n-1}$. Hence $a \in M_{n2} \subseteq M_n$.

Assume now $a_n \neq n$, in which case there is $i \in \{1, \ldots, n-1\}$ such that $a_i = n$ and $a|_i = (a_1, \ldots, a_{i-1}, a_n, a_{i+1}, \ldots, a_{n-1})$. Define $\tilde{a} = (a|_i, n)$, and note that $\tilde{a}$ can be obtained from a by switching a_n with $a_i = n$. Since either $i \leq a_n < a_i = n$ or $a_n < i < n = a_i$ and the numbers $i, a_n\ a_i = n$ are in the same cycle, by Lemma 3.3, $K_n(\tilde{a}) \leq K_n(a) = 0$ (by assumption). By the first Diaconis-Graham inequality (Theorem 3.4), $K_n(\tilde{a}) \geq 0$, and thus $K_n(\tilde{a}) = 0$. But $K_{n-1}(a|_i) = K_n(\tilde{a}) = 0$, and by the induction hypothesis $a|_i \in M_{n-1}$. Since $K_n(\tilde{a}) - K_n(a) = 0$, by Lemma 3.3, $b_{in}(a) = \min(n-i, a_i - a_n) - 1$. Using the last equation and equations (14) and (16), we conclude that $\min[\mu_i(a|_i), \lambda_i(a|_i)] = 0$. Therefore, $a \in M_{n1} \subseteq M_n$, and the induction step is complete. □

5 How often does equality hold?

In this section we give some insight on how often the equality holds in the first Diaconis-Graham inequality. First note that $M_1 = S_1$, $M_2 = S_2$, $M_3 = S_3$, and $M_4 = S_4 - \{(3,4,1,2)\}$. Also,

$$\begin{aligned} M_5 = S_5 - \{&(1,4,5,2,3),(2,4,5,1,3),(3,4,1,2,5),(3,4,1,5,2),\\ &(3,4,5,1,2),(3,4,5,2,1),(3,5,1,2,4),(3,5,1,4,2),\\ &(3,5,4,1,2),(4,1,5,2,3),(4,2,5,1,3),(4,3,5,1,2),\\ &(4,5,1,2,3),(4,5,1,3,2),(4,5,2,1,3),(4,5,3,1,2),\\ &(5,4,1,2,3)\}. \end{aligned}$$

For each $n \in \mathbb{N}^*$, let $\gamma_n := \#M_n$. Then $\gamma_1 = 1$, $\gamma_2 = 2$, $\gamma_3 = 6$, $\gamma_4 = 23$, $\gamma_5 = 103$, $\gamma_6 = 511$, $\gamma_7 = 2719$, $\gamma_8 = 15205$, $\gamma_9 = 88197$,

$\gamma_{10} = 526018$, $\gamma_{11} = 3206206$, $\gamma_{12} = 19885911$, $\gamma_{13} = 125107063$, and $\gamma_{14} = 796453594$.

Since we have been unable to find a closed-form formula for γ_n, we seek an upper bound on its value for each n, and study its asymptotic behaviour. Let $f_n(k,m)$ be the number of permutations $a = (a_1,\ldots,a_n) \in S_n$ such that $a_k = n$, $a_n = m$ and either $\lambda_k(\alpha|_k) = 0$ or $\mu_k(\alpha|_k) = 0$. Our immediate goal is to determine $f_n(k,m)$, from which we can determine an upper bound on $\gamma_n = \#M_n$. The reason is that

$$M_{n1} \subseteq \bigcup_{k=1}^{n-1}\bigcup_{m=1}^{n-1}\{a \in S_n \mid a_k = n,\ a_n = m,\ \text{and}\ [\lambda_k(a|_k) = 0 \,\text{or}\, \mu_k(a|_k) = 0]\},$$

and there is an obvious bijection between M_{n-1} and M_{n2}, from which we conclude that

$$\gamma_n = \#M_{n1} + \#M_{n2} \leq \gamma_{n-1} + \sum_{k=1}^{n-1}\sum_{m=1}^{n-1} f_n(k,m). \qquad (17)$$

Using this inequality, we can prove the following theorem:

Theorem 5.1 *For each $N \in \mathbb{N}^*$ we have*

$$\gamma_N \leq 1 + \sum_{n=2}^{N}\left((n-1)!\sum_{k=1}^{n-1}\frac{2}{k} - \sum_{k=1}^{n-1}(k-1)!(n-k-1)!\right). \qquad (18)$$

Proof: We first count the number of $a = (a_1,\ldots,a_n) \in S_n$ with $a_k = n$, $a_n = m$ and $\lambda_k(a|_k) = 0$. Clearly a is such a permutation if and only if

$$\{a_1,\ldots,a_{k-1}\} \subseteq \{1,\ldots,m-1\}$$

and

$$\{a_{k+1},\ldots,a_{n-1}\} \subseteq \{1,\ldots,n-1\} \setminus \{m,a_1,\ldots,a_{k-1}\}.$$

Such a permutation exists if and only if for the three positive integers n,k,m we have $k \leq m \leq n-1$. The number of such permutations is

$(n-k-1)!(m-1)(m-2)\cdots(m-k+1)$ (where an empty product is by definition equal to one).

Similarly, the number of $a=(a_1,\ldots,a_n)\in S_n$ with $a_k=n$, $a_n=m$ and $\mu_k(a|_k)=0$ is $(k-1)!(n-m-1)(n-m-2)\cdots(k+1-m)$, and such permutations exist if and only if the three positive integers n,k,m we have $m\le k\le n-1$. Finally, the number of $a\in S_n$ with $a_k=n$, $a_n=m$, and $\lambda_k(a|_k)=\mu_k(a|_k)=0$ is $(m-1)!(n-m-1)!\delta_{m,k}$, where $\delta_{m,k}=1$ if $m=k$, and zero otherwise. It follows that

$$f_n(k,m)=\begin{cases}\frac{(n-k-1)!(m-1)!}{(m-k)!} & \text{if } k\le m\le n-1,\\ \frac{(k-1)!(n-m-1)!}{(k-m)!} & \text{if } m\le k\le n-1,\end{cases}$$

and $f_n(m,m)=(m-1)!(n-m-1)!$.

Now we have from inequality (17) and the fact that $\gamma_1=1$ that for $N\in\mathbb{N}^*$,

$$\begin{aligned}\gamma_N &= \gamma_1+\sum_{n=2}^{N}(\gamma_n-\gamma_{n-1})\le 1+\sum_{n=2}^{N}\sum_{k=1}^{n-1}\sum_{m=1}^{n-1}f_n(k,m)\\ &= 1+\sum_{n=2}^{N}\sum_{k=1}^{n-1}\left((n-k-1)!\sum_{m=k}^{n-1}\frac{(m-1)!}{(m-k)!}\right.\\ &\qquad\left.+(k-1)!\sum_{m=1}^{k}\frac{(n-m-1)!}{(k-m)!}-(k-1)!(n-k-1)!\right).\end{aligned}$$

Using standard combinatorial arguments, one can show that

$$(n-k-1)!\sum_{m=k}^{n-1}\frac{(m-1)!}{(m-k)!}=\frac{(n-1)!}{k}$$

and

$$(k-1)!\sum_{m=1}^{k}\frac{(n-m-1)!}{(k-m)!}=\frac{(n-1)!}{n-k}.$$

Since also $\sum_{k=1}^{n-1}\frac{1}{k}=\sum_{k=1}^{n-1}\frac{1}{n-k}$, we obtain inequality (18). □

We now have the following result.

Theorem 5.2 *We have* $\gamma_N/N! = \mathcal{O}(\ln N/N)$. *In particular,* $\lim_{N\to\infty}\gamma_N/N! = 0$.

Proof: Set

$$g(N) := \frac{1}{N!}\sum_{n=2}^{N}(n-1)!\sum_{k=1}^{n-1}\frac{2}{k}. \tag{19}$$

The result in Theorem 5.1 shows that $\gamma_N/N! \le g(N)$ for $N \ge 2$, so it suffices to show that $g(N) = \mathcal{O}(\ln N/N)$. Notice that

$$\begin{aligned} g(N) - g(N-1) &= \frac{(N-1)!}{N!}\sum_{k=1}^{N-1}\frac{2}{k} \\ &\quad + \sum_{n=2}^{N-1}\left(\frac{(n-1)!}{N!} - \frac{(n-1)!}{(N-1)!}\right)\sum_{k=1}^{n-1}\frac{2}{k} \\ &= \frac{2}{N}\sum_{k=1}^{N-1}\frac{1}{k} - \frac{N-1}{N}g(N-1), \end{aligned}$$

so that

$$g(N) = \frac{2}{N}\sum_{k=1}^{N-1}\frac{1}{k} + \frac{g(N-1)}{N}. \tag{20}$$

Since

$$\sum_{k=1}^{n}\frac{1}{k} < 1 + \ln n$$

for all $n \in \mathbb{N}^*$, it follows from (19) that for each $N \ge 2$,

$$g(N) \le \frac{1}{N!}\sum_{n=2}^{N}(N-1)!\,2(1+\ln N) \le 2 + 2\ln N.$$

If follows from (20) that, for $N \ge 2$,

$$g(N) \le \frac{2}{N}(1+\ln(N-1)) + \frac{2}{N} + \frac{2\ln(N-1)}{N} = \mathcal{O}\left(\frac{\ln N}{N}\right),$$

as desired. □

We finish the paper by discussing when both of the Diaconis-Graham inequalities hold as equalities simultaneously. For given $n \in \mathbb{N}^*$, this occurs for those permutations $a \in S_n$ for which $I_n(a) = EX_n(a)$, which happens if and only if $a \in M_n$ and a has no 3-inversions. Diaconis and Graham [7] mention that the number of such permutations is the Fibonacci number F_{2n-1} defined by $F_0 = 0$, $F_1 = 1$ and $F_{m+2} = F_{m+1} + F_m$ for $m \geq 0$. Below we characterize those permutations. Let $\Pi_1 := S_1$, and for each integer $n \geq 2$ let

$$\begin{aligned} \Pi_{n1} &:= \{a \in S_n \mid \exists i \in \{1, \ldots, n-2\} : a_i = n,\ a_n = n-1, \\ &\qquad\qquad a|_i \in \Pi_{n-1}\}; \\ \Pi_{n2} &:= \{a \in S_n \mid a_n = n \text{ and } a|_n \in \Pi_{n-1}\}; \\ \Pi_{n3} &:= \{a \in S_n \mid a_{n-1} = n \text{ and } a|_{n-1} \in \Pi_{n-1}\}; \\ \Pi_n &:= \Pi_{n1} \cup \Pi_{n2} \cup \Pi_{n3}. \end{aligned}$$

It can be proved by induction on n that $a \in \Pi_n$ if and only $a \in M_n$ and a has no 3-inversions. It can also be proved by induction that $\#\Pi_{n2} = F_{2n-3} = \#\Pi_{n3}$ and

$$\begin{aligned} \#\Pi_{n1} = \#\Pi_{n-1} - \#\Pi_{(n-1)2} &= \#\Pi_{n-1} - \#\Pi_{n-2} \\ &= F_{2n-3} - F_{2n-5} = F_{2n-4}. \end{aligned}$$

In such a case,

$$\#\Pi_n = F_{2n-4} + F_{2n-3} + F_{2n-3} = F_{2n-2} + F_{2n-3} = F_{2n-1}.$$

We omit the proofs of the above claims.

Acknowledgements

We would like to thank two anonymous scientists whose comments helped improve the presentation of the paper.

References

[1] A. Cayley, Note on the theory of permutations. *Philosophical Mag.* 34(1849), 527-529.

[2] G. Cohen and M. Deza, Some metrical problems on S_n. *Ann. Discrete Math.* 8(1980), 211-216.

[3] D. E. Critchlow, *Metric methods for analyzing partially ranked data*, Lecture Notes in Statistics (Springer-Verlag, Berlin, Germany, 1985).

[4] H. E. Daniels (1950). Rank correlation and population models (with discussion). *J. R. Stat. Soc. Ser. B Stat. Methodol.* 12(1950), 171-191.

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

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

[7] 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.

[8] J. Durbin and A. Stuart, Inversions and rank correlation coefficients. *J. R. Stat. Soc. Ser. B Stat. Methodol.* 13(1951), 303-309.

[9] A. Ecker, Time-division multiplexing scramblers: Selecting permutations and testing the system, *Proceedings of Eurocrypt '84*; in: *Advances in Cryptology 1981-1997: Electronic Proceedings of the Crypto and Eurocrypt Conferences 1981-1997*, edited by K. S. McCurley and C. D. Ziegler, Lecture Notes in Computer Science, Springer-Verlag (1998), pp. 399-415.

[10] V. Estivill-Castro, Sorting and measures of disorder, *Ph.D. thesis* (University of Waterloo, Waterloo, Ontario, Canada, 1991).

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

[12] V. Estivill-Castro, H. Mannila, and D. Wood, Right invariant metrics and measures of presortedness. *Discrete Appl. Math.* 42(1993), 1-16.

[13] O. Guibert and E. Pergola, Enumeration of vexillary involutions which are equal to their mirror/complement. *Discrete Math.* 224(2000), 281-287.

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

[15] M. Hall, *Proceedings of the Symposium on Pure Mathematics*, American Mathematical Society, Providence, RI, 6(1956), p. 203 and following.

[16] M. Kendall, *Rank Correlation Methods,* 4th edition, 2nd impression (Oxford University Press, New York, NY, 1975).

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

[18] H. Mannila, Measures of presortedness and optimal sorting algorithms. *IEEE Trans. Comp.* 34(1985), 318-325.

[19] J. Noonan and D. Zeilberger, The enumeration of permutations with a prescribed number of "forbidden" patterns. *Adv. in Appl. Math.* 17(1996), 381-407.

[20] O. Rodrigues, Note sur les inversions, ou derangements produits dans les permutations, *Journal de Mathematiques* 4(1839), 236–240.

[21] R. Simion and F. W. Schmidt, Restricted permutations. *European J. Combin.* 6(1985), 383-406.