Blocks in cycles and k-commuting permutations

Rutilo Moreno and Luis Manuel Rivera

Abstract

Let k be a nonnegative integer, and let α and β be two permutations of n symbols. We say that α and β k-commute if $H(\alpha\beta, \beta\alpha) = k$, where H denotes the Hamming metric between permutations. In this paper, we consider the problem of finding the permutations that k-commute with a given permutation. Our main result is a characterization of permutations that k-commute with a given permutation β in terms of blocks in cycles in the decomposition of β as a product of disjoint cycles. Using this characterization, we provide formulas for the number of permutations that k-commute with a transposition, a fixed-point free involution and an n-cycle, for any k. Also, we determine the number of permutations that k-commute with any given permutation, for $k \leq 4$.

Keywords: Symmetric group, Hamming metric, conjugate permutations, blocks in cycles.

Contents

1 Introduction

The symmetric group as a metric space has been studied with different metrics and for different purposes, see, for example, [9, 10, 12, 31], and the metric that seems to be more used is the Hamming metric. This metric was introduced in 1950 by R. W. Hamming [25] for the case of binary strings and in connection with digital communications. For the case of permutations it was used in an implicit way by H. K. Farahat [12] who studied the symmetries of the metric space (S_n, H), where S_n denotes the symmetric group on $[n] := \{1, \dots, n\}$ and H the Hamming metric between permutations. Also, D. Gorenstein, R. Sandler and W. H. Mills [20] studied a problem about permutations that almost commute, in the sense of normalized Hamming metric. Other problems studied in this metric space are the packing and covering problem (see, e.g., [29]), and also permutation codes (see, e.g., [4]) which have turned out to be useful in applications to power line communications (see, e.g. [7]).

Our interest in the symmetric group as a metric space, with the Hamming metric, arose from the study of sofic groups, a class of groups of growing interest (see, e.g., [5, 28]) that was first defined by M. Gromov [21] as a common generalization of residually finite groups and of amenable groups. To the best of the author's knowledge it is an open question to determine if all groups are sofic. The following, Theorem 3.5 in [28], shows the importance of the Hamming metric H on the symmetric group. Let $H_n(\alpha, \beta) = H(\alpha, \beta)/n$, for every $\alpha, \beta \in S_n$.

Theorem 1.1. *A group G is sofic if and only if for evey finite $F \subseteq G$ and for each $\varepsilon > 0$, there exist a natural n and a mapping $\theta : F \to S_n$ so that*

1. *if $g, h, gh \in F$, then $H_n(\theta(g)\theta(h), \theta(gh)) < \varepsilon$,*

2. *if the identity e of G belongs to F then $H_n(\theta(e), id) \leq \varepsilon$, and*

3. *for all distinct $g, h \in F$, $H_n(\theta(g), \theta(h)) \geq 1/4$.*

As θ is not necessarily a group homomorphism between G and S_n then permutations $\theta(gh)$ and $\theta(g)\theta(h)$ can be different, and condition (1) in previous theorem ask for a "small" difference between them. Motivated by this, L. Glebsky and the second author defined the concept of stability of a system of equations in permutations [18, Def. 1]. For the convenience of the reader, we remember here some of these definitions. Let $w(x_1, \dots, x_k) = x_{i_1}^{\varepsilon_1} x_{i_2}^{\varepsilon_2} \dots x_{i_l}^{\varepsilon_l}$, $u(x_1, \dots, x_k) = x_{j_1}^{\varepsilon_1'} x_{j_2}^{\varepsilon_2'} \dots x_{j_m}^{\varepsilon_l'}$ be expressions using $x_h \in \{x_1, \dots, x_k\}$ and $\varepsilon_i = \pm 1$, $\varepsilon_j' = \pm 1$ (we may think that w, u are words in $\{x_1, x_1^{-1}, \dots, x_k, x_k^{-1}\}$). We say that permutations $\alpha_1, \dots, \alpha_k$ are an ϵ-*solution* of equation $w(x_1, \dots, x_k) = u(x_1, \dots, x_k)$, if and only if $H_n(w(\alpha_1, \dots, \alpha_k), u(\alpha_1, \dots, \alpha_k)) \leq \epsilon$. We say that permutations $\alpha_1, \dots, \alpha_k$ are an ϵ-*solution* of a system of equations

$$w_i(x_1, \dots, x_k) = u_i(x_1, \dots, x_k), \quad i = 1, \dots, r \tag{1}$$

if and only if $\alpha_1, \dots, \alpha_k$ are an ϵ-solution for each equation of the system. The system of equations (1) is called *stable in permutations* if and only if there exists δ_ϵ, $\lim_{\epsilon \to 0} \delta_\epsilon = 0$, such that for any ϵ-solution $\alpha_1, \dots, \alpha_k \in S_n$ of system (1), there exists an exact solution $\tilde{\alpha}_1, \dots, \tilde{\alpha}_k \in S_n$ of (1) such that $H_n(\alpha_i, \tilde{\alpha}_i) \leq \delta_\epsilon$ for $i = 1, \dots, k$.

Glebsky et. al., [18] showed that the stability in permutations of system (1) is related with the properties of the finitely presented group

$$G = \langle x_1, \ldots, x_k \mid w_i(x_1, \ldots, x_k) = u_i(x_1, \ldots, x_k), i = 1, \ldots, r \rangle. \tag{2}$$

They proved that if G is finite then system (1) is stable in permutations, and if G is sofic but not residually finite then system (1) is unstable in permutations. One question that remains open is to determine if for any finitely presented residually finite group G, with presentation (2), system (1) is stable or not in permutations. As the group $G = \langle x, y \mid xy = yx \rangle$ is an example of a residually finite group we are interested in the following:

Problem 1.2. *To determine if equation $xy = yx$ is or not stable in permutations.*

In an informal way, this problem can be expressed as the following "almost" implies "near" type problem (see, e.g., [1] for more problems of this type): is it true that any pair of almost commuting permutations is closed to a commuting pair of permutations? A problem, which is closely related to problem 1.2 was studied by D. Gorenstein, et al., [20].

The analogous problem about the stability of $xy = yx$ in matrices is a classical problem in linear algebra and operator theory, and has been widely studied for the cases when the distance between matrices are: the operator norm (see, e.g., [16, 22, 26, 27, 36]), the Schatten norm (see, e.g., [15]), and for the normalized Hilbert-Schmidt distance (see, e.g., [14, 17, 23, 24]). On the other hand, the case of rank distance is poorly studied and little understood (see, e.g., [19, Sec. 2.3]).

In order to get insight and to develop tools towards a solution of Problem 1.2, we begin the study of the following problems: let α and β be two permutations, we say that α and β *k-commute* if $H(\alpha\beta, \beta\alpha) = k$.

Problem 1.3. *For given $\beta \in S_n$, to characterize the permutations α that k-commute with β.*

Problem 1.4. *To compute the number $c(k, \beta)$ of permutations that k-commute with β, where β is any permutation and k any nonnegative integer.*

Our main result about Problem 1.3 is a characterization of permutations α that k-commute with a given permutation β. This characterization is given in terms of blocks formed by strings of consecutive points in the cycles of the decomposition of β as a product of disjoint cycles. With respect to Problem 1.4, using our characterization we were able to find explicit formulas for $c(k, \beta)$, for any β and $k \leq 4$. The study of this small cases sheds light of how difficult it can be the problem of computing $c(k, \beta)$ in its generality. So we worked with several specific types of permutations. We have found some relations between $c(k, \beta)$ and the following integer sequences in OEIS [33]: A208529, A208528 and A098916 when β is a transposition, A000757 when β is an n-cycle, and A053871 when β is a fixed-point free involution. The relationship between the number $c(k, \beta)$ with some integers sequences in OEIS have provided another motivation for the authors to studied permutations that k-commute using the Hamming metric. The interested reader in a similar problem but with strings is referred to the work of J. Shallit [32].

The outline of the paper is as it follows. In Section 2 we give some of the definitions and notation used throughout the paper. In Section 3 we present our characterization of permutations that k-commute with a given permutation β. This characterization is given in terms of blocks in cycles in the decomposition of β as a product of disjoint cycles. In Section 4 we present a formula and a bivariate generating function for the number of permutations that k-commute with any n-cycle. Also we present a result about the proportion of even permutations that k-commute with β. In Section 5 we obtain explicit formulas for the number $c(k, \beta)$ when β is any permutation and $k = 3, 4$. In Section 6 we obtain some formulas for the cases when β is a transposition and a fixed-point free involution.

2 Definitions and notation

We first give some definitions and notation used throughout the work. The elements in $[n]$ are called *points* and the elements in S_n are called permutations or n-permutations. For any permutation $\pi \in S_n$, we write $\pi = p_1 p_2 \ldots p_n$ for its one-line notation, i.e., $\pi(i) = p_i$ for every $i \in [n]$. We compute the product $\alpha\beta$ of permutations α and β by first applying β and then α. A permutation $\pi \in S_n$ is called a *cycle* of length m (or m-*cycle*), and it is denoted by $\pi = (a_1 a_2 \ldots a_m)$, if $\pi(a_i) = a_{i+1}$, for $1 \leq i < m$, $\pi(a_m) = a_1$ and $\pi(a) = a$ for every $a \in [n] \setminus \{a_1, \ldots, a_m\}$. It is a known fact that any permutation can be written in essentially one way as a product of disjoint cycles (called its *cycle decomposition*, see, e.g., [11, Sec. 1.3, p. 29]). In this paper, we will denote a cycle in the disjoint cycle decomposition of π by π_j, i.e., π with a subindex $j \in [n]$ that not necessarily means its length, and we will say that π *has cycle* π_j or that π_j is *a cycle of* π. If $\pi_j = (a_1 \ldots a_m)$ is a cycle of π we define $\mathrm{set}(\pi_j) := \{a_1, \ldots, a_m\}$, and we say that a is a point in cycle π_j if $a \in \mathrm{set}(\pi_j)$. The *cycle type* of a permutation β is a vector $(c_1, \ldots, c_n)$ that indicates that β has exactly c_i cycles of length i in its cycle decomposition. The *Hamming metric*, $H(\alpha, \beta)$, between permutations α and β is defined as $H(\alpha, \beta) = |\{a \in [n] : \alpha(a) \neq \beta(a)\}|$. It is well-known (see, e.g., [9]) that this metric is bi-invariant, that not two permutations have Hamming metric equal to 1, and also, that $H(\alpha, \beta) = 2$ if and only if $\alpha\beta^{-1}$ is a transposition. We say that $a \in [n]$ is a *good commuting point* (resp. *bad commuting point*) of α and β if $\alpha\beta(a) = \beta\alpha(a)$ (resp. $\alpha\beta(a) \neq \beta\alpha(a)$). Usually, we abbreviate good commuting points (resp. bad commuting points) with *g.c.p.* (resp. *b.c.p.*). In this work, we use the convention $m \bmod m = m$ for any positive integer m.

2.1 Blocks in cycles

Let $\pi \in S_n$, a *block* A in a cycle $\pi_j = (a_1 a_2 \ldots a_m)$ of π is a nonempty string $A = a_i a_{i+1} \ldots a_{i+l}$, where $l \leq m$, of consecutive elements in π_j, where the sums on the subindex are taken modulo m. This definition is different from the given in [20], our way of defining a block in a cycle is similar to the definition of block when permutation is written in one-line-notation (see, e.g., ([3, 6]). The *length* of a block A is the number of elements in the block, and is denoted by $|A|$. If we have the block $A = a_1 \ldots a_l$, the elements a_1 and a_l are called the *first* and the *last* elements of the block, respectively. A *proper block* (resp. *improper block*) of an m-cycle is a block of length $l < m$ (resp. $l = m$). Two blocks A and B are said to be *disjoint* if they do

not have points in common. The *product AB* of two disjoint blocks, A and B, not necessarily from the same cycle, is defined by concatenation of strings (this product is not necessarily a block in a cycle of β). If π_j is a cycle, we sometimes write $\pi_j = (A_1 \ldots A_k)$ to mean that one of the m cyclic equivalent ways to write τ is equal (as a block) to $A_1 \ldots A_k$. A *block partition* of a cycle π_j is a set $\{A_1, \ldots, A_l\}$ of pairwise disjoint blocks such that there exist a product $A_{i_1} \ldots A_{i_l}$ of these blocks such that $\pi_j = (A_{i_1} \ldots A_{i_l})$. If $P = J_1 J_2 \ldots J_k$ is a block product of k pairwise disjoint blocks (not necessarily from the same cycle) and α is a permutation in S_k, the *block permutation ϕ_α* induced by α and P is defined as $\phi_\alpha(P) = J_{\alpha(1)} J_{\alpha(2)} \ldots J_{\alpha(k)}$.

Example 2.1. Let $\pi = \pi_1 \pi_2 \in S_9$ with $\pi_1 = (1234), \pi_2 = (56789)$. An improper block in π_1 is 2341 and a proper block is $A = 12$. The blocks $B_1 = 567$, $B_2 = 8$, $B_3 = 9$ are a block partition of π_2. The product $B_1 B_2$ is a block in π_2 and $AB_2 = 128$ is not a block in any cycle of π. Let $\alpha = (321) \in S_3$. The block permutation $\phi_\alpha(B_1 B_2 B_3)$ is $B_3 B_1 B_2 = 95678$.

Let $\alpha, \beta \in S_n$ and $\beta_j = (b_1 \ldots b_m)$ a cycle of β. It is well known (see, e.g., [11, Prop. 10, p. 125]) that $\alpha \beta_j \alpha^{-1} = (\alpha(b_1) \ldots \alpha(b_m))$, i.e., $\alpha \beta_j \alpha^{-1}$ is also an m-cycle, not necessarily of β. Sometimes we write $\alpha|_{\text{set}(\beta_j)}$, the restriction of α to $\text{set}(\beta_j)$, as

$$\alpha|_{\text{set}(\beta_j)} = \begin{pmatrix} b_1 & b_2 & \ldots & b_m \\ \alpha(b_1) & \alpha(b_2) & \ldots & \alpha(b_m) \end{pmatrix}. \tag{3}$$

If $\alpha|_{\text{set}(\beta_j)}$ is written as in (3), we will write

$$\alpha|_{\text{set}(\beta_j),k} = \begin{pmatrix} B_1 B_2 \ldots B_k \\ J_1 J_2 \ldots J_k \end{pmatrix},$$

to mean that if $B_1 \ldots B_k = b_1 \ldots b_m$, then $J_1, \ldots, J_k$ are blocks in cycles of β, with $J_1 \ldots J_k = \alpha(b_1)\alpha(b_2) \ldots \alpha(b_m)$, and $|B_i| = |J_i|$, for $1 \leq i \leq k$ (notice that there are m possibilities for the first point b_1 in the first row). We refer to this notation as the *block notation* (with respect to β) of $\alpha|_{\text{set}(\beta_j)}$. If not required the subindex k in $\alpha|_{\text{set}(\beta_j),k}$ it will be omitted.

Example 2.2. Let $\alpha, \beta \in S_6$ with $\alpha = (1\,3\,4)(2\,5\,6)$ and $\beta = (1\,2\,4\,5)(3\,6)$. If $\beta_j = (1\,2\,4\,5)$, two ways to express $\alpha|_{\text{set}(\beta_j)}$ in block notation are

$$\alpha|_{\text{set}(\beta_j),3} = \left(\left.\begin{array}{c|cc|c} 1 & 2 & 4 & 5 \\ 3 & 5 & 1 & 6 \end{array}\right.\right), \quad \alpha|_{\text{set}(\beta_j),4} = \left(\left.\begin{array}{c|c|c|c} 1 & 2 & 4 & 5 \\ 3 & 5 & 1 & 6 \end{array}\right.\right),$$

where the vertical lines denotes the limits of the blocks.

3 Permutations that k-commute with a cycle of a permutation

In this section we show the relation between blocks in cycles of β and the permutations α that k-commutes with β. First we prove the following.

Proposition 3.1. *Let β be any permutation of cycle type $(c_1, \ldots, c_n)$. Then $c(0, \beta) = \prod_{i=1}^n i^{c_i} c_i!$, and $c(1, \beta) = c(2, \beta) = 0$.*

Proof. When $k = 0$, $c(0, \beta)$ is the size of the centralizer of β. As no two permutations have Hamming metric equal to 1 then $c(1, \beta) = 0$. Now we show case $k = 2$. It is easy to see that $H(\pi, \tau) = 2$ if and only if $\pi\tau^{-1}$ is a transposition. If $H(\alpha\beta, \beta\alpha) = 2$ then $\alpha\beta\alpha^{-1}\beta^{-1}$ should be a transposition, but this lead to a contradiction because $\alpha\beta\alpha^{-1}\beta^{-1}$ is an even permutation. $\square$

If two permutations α and β commute, then $\alpha\beta\alpha^{-1} = \beta$, and we can think that "α rearranges the cycles of β". We will say that α *transforms* the cycle β_j of β into the cycle $\alpha\beta_j\alpha^{-1}$ if $\alpha\beta_j\alpha^{-1}$ is also a cycle in the cycle decomposition of β. Let $B = b_1 \ldots b_l$ be a block in β_j, we say that α *commutes* with β *on the block* B if $\alpha\beta(b_i) = \beta\alpha(b_i)$, for every $i = 1, \ldots, l$, and that *commutes* (resp. do not commute) with β on β_j, or simply (by abusing of notation) that α commutes (resp. do not commute) with β_j, if $\alpha\beta(b) = \beta\alpha(b)$ for every $b \in \text{set}(\beta_j)$ (resp. $\alpha\beta(b) \neq \beta\alpha(b)$ for some $b \in \text{set}(\beta_j)$). The following remark is implicitly used in some of the proofs in this article.

Remark 3.2. Let $\alpha, \beta \in S_n$ and $\{a_1, \ldots, a_l\} \subseteq [n]$. If $\alpha(a_1) \ldots \alpha(a_l)$ is a block in a cycle of β then, by definition of block, it follows that $\beta(\alpha(a_i)) = \alpha(a_{i+1})$, $1 \leq i \leq l - 1$.

The following result is the key to relate commutation and blocks in cycles.

Proposition 3.3. *Let $\alpha, \beta \in S_n$. Let ℓ, m be integers, $1 \leq \ell < m \leq n$. Let $\beta_j = (b_1 \ \ldots \ b_m)$ be a cycle of β. If α commutes with β on the block $b_1 \ldots b_\ell$, then $\alpha(b_1) \ldots \alpha(b_\ell)\alpha(b_{\ell+1})$ is a block in a cycle of β.*

Proof. It is enough to prove that $\alpha(b_i) = \beta^{i-1}(\alpha(b_1))$, for $i = 1, \ldots, \ell + 1$. The proof is by induction on $i \leq \ell + 1$. The base case $i = 1$ is trivial. Assume as inductive hypothesis that the statement is true for every $k < \ell + 1$. As α and β commute on b_k, we have that $\alpha(b_{k+1}) = \alpha(\beta(b_k)) = \beta(\alpha(b_k)) = \beta(\beta^{k-1}(\alpha(b_1))) = \beta^k(\alpha(b_1))$. $\square$

We have the following result.

Proposition 3.4. *Let β_j be an m-cycle of β. Then α commutes with β on β_j if and only if α transforms β_j into an m-cycle of β.*

Proof. If α commutes with β on $\beta_j = (b_1 \ldots b_m)$ then from Proposition 3.3 it follows that $\alpha(b_1) \ldots \alpha(b_{m-1})\alpha(b_m)$ is a block in a cycle of β. Now, as $\beta(\alpha(b_m)) = \alpha(\beta(b_m)) = \alpha(b_1)$ then $\alpha(b_1) \ldots \alpha(b_{m-1})\alpha(b_m)$ is an improper block in an m-cycle, say β_l, of β, i.e., α transforms β_j into β_l. Conversely, if α transform β_j into an m-cycle, say β_l, of β then $\beta_l = \alpha\beta_j\alpha^{-1}$ that is equal to $(\alpha(b_1) \ldots \alpha(b_m))$. Then $\alpha(b_1) \ldots \alpha(b_m)$ is a block in a cycle of β which implies (see Remark 3.2) that $\beta(\alpha(b_i)) = \alpha(b_{i+1 \bmod m})$. As also $\alpha(b_{i+1 \bmod m}) = \alpha(\beta(b_i))$ then $\beta(\alpha(b_i)) = \alpha(\beta(b_i))$, for every $i \in \{1, \ldots, m\}$. $\square$

Corollary 3.5. *Let $\alpha, \beta \in S_n$. Then α and β commute if and only if α transforms all the cycles of β into cycles of β.*

Remark 3.6. Using block notation, Proposition 3.4 can be rewritten as follows: a permutation α commutes with β on $\beta_j = (B)$ if and only if

$$\alpha|_{\text{set}(\beta_j),1} = \begin{pmatrix} B \\ B' \end{pmatrix},$$

where $\beta_l = (B')$ is a cycle of β.

Let β_i be a cycle of β. We say that α (k_i, β)-*commutes* with β_i if there exists exactly k_i points in β_i on which α and β do not commute.

Remark 3.7. Let β be a permutation. Then α k-commutes with β if and only if there exists h cycles, say $\beta_1, \ldots, \beta_h$, of β such that for every $1 \leq i \leq h$, α (k_i, β)-commutes with β_i, $k_i \geq 1$, where $k_1 + \cdots + k_h = k$ and α commutes with β on every cycle not in $\{\beta_1, \ldots, \beta_h\}$.

Now we present one of our main results.

Theorem 3.8. *Let β_j be an m-cycle of β and $k \geq 1$. Then α (k, β)-commutes with β_j if and only if $\alpha\beta_j\alpha^{-1} = (P_1 \ldots P_k)$, where the blocks $P_1, \ldots, P_k$ satisfy the following*

1. *if $k = 1$ then P_1 is a proper block in a cycle of β,*

2. *if $k > 1$ then $P_1, \ldots, P_k$ are k pairwise disjoint blocks, from one or more cycles of β, such that for any $i \in [k]$, the string $P_i P_{i+1 \bmod k}$ is not a block in any cycle of β.*

Proof. (1) ($\Leftarrow$): Suppose that $\alpha\beta_j\alpha^{-1} = (P_1)$ and without lost of generality we can take $\beta_j = (b_1 \ldots b_m)$ such that $P_1 = \alpha(b_1) \ldots \alpha(b_m)$. As, by hypothesis, P_1 is a proper block in a cycle of β then $\beta(\alpha(b_i)) = \alpha(b_{i+1})$, for $i = 1, \ldots, m-1$ (Remark 3.2). As $\alpha(b_{i+1}) = \alpha(\beta(b_i))$, we have that α and β commute on b_i, for every $1 \leq i \leq m-1$. Now we prove that $\beta(\alpha(b_m)) \neq \alpha(\beta(b_m))$ by contradiction. Suppose that $\beta(\alpha(b_m)) = \alpha(\beta(b_m))$, then $\beta(\alpha(b_m)) = \alpha(b_1)$ which implies that P_1 is an improper block in a cycle of β, a contradiction.

($\Rightarrow$): Without lost of generality we can assume that α commutes with β on block $b_1 \ldots b_{m-1}$ of $\beta_j = (b_1 \ldots b_{m-1}b_m)$ and that does not commute on b_m. By Proposition 3.3, $\alpha(b_1) \ldots \alpha(b_{m-1})\alpha(b_m)$ is a block in a cycle of β and is a proper block due to Proposition 3.4 (see also Remark 3.6).

(2) ($\Leftarrow$): Suppose that $\alpha\beta_j\alpha^{-1} = (P_1 \ldots P_k)$, where every $P_i = p_{i1}p_{i2} \ldots p_{i\ell_i}$ is a block in a cycle of β and that for every $i \in [k]$, $P_i P_{i+1}$ is not a block in any cycle of β. Without lost of generality we assume that $\beta_j = (b_{11} \ldots b_{1\ell_1}b_{21} \ldots b_{2\ell_2} \ldots b_{k1} \ldots b_{k\ell_k})$ such that $\alpha(b_{ir}) = p_{ir}$, for every $i \in [k]$ and $1 \leq r \leq \ell_i$.

As P_i is a block in a cycle of β then $\beta(p_{ir}) = p_{i(r+1)}$, for every $1 \leq r < \ell_i$ (Remark 3.2), then we have for one side that $p_{i(r+1)} = \beta(p_{ir}) = \beta(\alpha(b_{ir}))$ and for the other side $p_{i(r+1)} = \alpha(b_{i(r+1)}) = \alpha(\beta(b_{ir}))$ and hence α and β commute on b_{ir}, for every $1 \leq r < \ell_i$. Now we prove that $\beta(\alpha(b_{i\ell_i})) \neq \alpha(\beta(b_{i\ell_i}))$ by contradiction. Suppose that $\beta(\alpha(b_{i\ell_i})) = \alpha(\beta(b_{i\ell_i}))$, as $\beta(p_{i\ell_i}) = \beta(\alpha(b_{i\ell_i}))$, then $\beta(p_{i\ell_i}) = \alpha(\beta(b_{i\ell_i})) = \alpha(b_{(i+1 \bmod k)1}) = p_{(i+1 \bmod k)1}$, which implies that $P_i P_{i+1 \bmod k}$ is a block in a cycle of β, a contradiction.

($\Rightarrow$): If α does not commute with β on exactly k points in β_j we write $\beta_j = (B_1 \ldots B_k)$, where for every block $B_i = b_{i1}b_{i2} \ldots b_{i\ell_i}$, α and β commute on b_{ij}, for $1 \leq j < \ell_i$, and does not commute on $b_{i\ell_i}$. By Proposition 3.3 we have that $P_i := \alpha(b_{i1})\alpha(b_{i2}) \ldots \alpha(b_{i\ell_i})$ is a block in a cycle of β. Now suppose that for some i, $P_i P_{i+1 \bmod k}$ is a block in any cycle of β, then $\beta(\alpha(b_{i\ell_i})) = \alpha(b_{(i+1 \bmod k)1}) = \alpha(\beta(b_{i\ell_i}))$, contradicting the assumption that α and β do not commute on $b_{i\ell_i}$. $\square$

Remark 3.9. $\alpha|_{\text{set}(\beta_j),k}$ in previous proposition, can be written as

$$\alpha|_{\text{set}(\beta_j),k} = \begin{pmatrix} B_1 \dots B_k \\ P_1 \dots P_k \end{pmatrix},$$

with $\beta_j = (B_1 \dots B_k)$, $\alpha\beta_j\alpha^{-1} = (P_1 \dots P_k)$, where for every $1 \leq i \leq k$, $|B_i| = |P_i| = \ell_i$, $P_i = p_{i1}p_{i2}\dots p_{i\ell_i}$, $B_i = b_{i1}b_{i2}\dots b_{i\ell_i}$, i.e., $\alpha(b_{ir}) = p_{ir}$, $1 \leq r \leq \ell_i$, and where α and β commute on $b_{i1}b_{i2}\dots b_{i(\ell_i-1)}$ and do not commute on $b_{i\ell_i} = \alpha^{-1}(p_{i\ell_i})$ (the last point of B_i).

Using Theorem 3.8 we can characterize permutations that k-commute with β in terms of blocks in cycles of β as follows.

Corollary 3.10. *Let $\alpha, \beta \in S_n$. Then α k-commutes with β if and only if there exist h cycles of β, say $\beta_1, \dots, \beta_h$, such that α commutes with β on each cycle not in $\{\beta_1, \dots, \beta_h\}$ and for every $i \in \{1, \dots, h\}$, $\alpha\beta_i\alpha^{-1} = (P_1^{(i)} \dots P_{k_i}^{(i)})$, with $k_i \geq 1$, $k = k_1 + \dots + k_h$, and where the blocks $P_1^{(i)}, \dots, P_{k_i}^{(i)}$ satisfy the following*

1. *if $k_i = 1$ then $P_1^{(i)}$ is a proper block in a cycle of β,*

2. *if $k_i > 1$ then $P_1^{(i)}, \dots, P_{k_i}^{(i)}$ are k_i pairwise disjoint blocks, from one or more cycles of β, such that for any $r \in [k_i]$, $P_r^{(i)} P_{r+1 \bmod k_i}^{(i)}$ is not a block in any cycle of β,*

3. *$\{P_1^{(1)}, \dots, P_{k_1}^{(1)}, \dots, P_1^{(h)}, \dots, P_{k_h}^{(h)}\}$ is a set of pairwise disjoints blocks from one or more cycles of β.*

Example 3.11. Let $\alpha, \beta \in S_7$, with $\beta = (1\ 2\ 4\ 5\ 3)(7\ 6)$ and $\alpha = (2\ 7)(3\ 6\ 4\ 5)$. By direct calculations we can check that α $(4, \beta)$-commutes with $\beta_1 = (1\ 2\ 4\ 5\ 3)$ (the b.c.p. are $1, 2, 3$ and 5) and $(1, \beta)$-commutes with $\beta_2 = (7\ 6)$ (the b.c.p. is 6). In block notation $\alpha|_{\text{set}(\beta_1)}$ and $\alpha|_{\text{set}(\beta_2)}$ can be expressed as

$$\alpha|_{\text{set}(\beta_1),4} = \begin{pmatrix} 1 & 2 & 4 & 5 & 3 \\ 1 & 7 & 5 & 3 & 6 \end{pmatrix}, \quad \alpha|_{\text{set}(\beta_2),1} = \begin{pmatrix} 7 & 6 \\ 2 & 4 \end{pmatrix}.$$

As a first application of Theorem 3.8 we present the following generalization of Lemma 2(b) in [20] where it was proved only for the case when β is a product of m disjoint l-cycles.

Proposition 3.12. *Let β be any n-permutation whose maximum cycle length in its cycle decomposition is m. If α commutes with β on $m - 1$ points in an m-cycle β_j of β then α commutes with β on β_j.*

Proof. Suppose that α and β do not commute on the remaining point in β_j. By part (1) of Theorem 3.8, $\alpha\beta_j\alpha^{-1} = (P)$, where P is a proper block in an l-cycle of β, i.e., $l > m$, but this is a contradiction because m is the maximum cycle length of cycles in β. $\square$

The following proposition will be useful in the proofs of some of our results.

Proposition 3.13. *Let α and β be two permutations that k-commute, $k > 0$. Suppose that α does not commute with β on the cycles $\beta_1, \ldots, \beta_r$, of lengths $l_1, \ldots l_r$, respectively, and that commutes with the rest of the cycles of β (if any). Then there exists exactly r cycles, say $\beta'_1, \ldots, \beta'_r$, of lengths $l_1, \ldots l_r$, respectively, such that $\alpha\left(\mathrm{set}(\beta_1) \cup \cdots \cup \mathrm{set}(\beta_r)\right) = \mathrm{set}(\beta'_1) \cup \cdots \cup \mathrm{set}(\beta'_r)$. Even more, suppose that α does not commute with exactly h_i i-cycles of β and that commutes with the rest of the i-cycles of β (if any). Then there exists exactly h_i i-cycles of β such that each of them contains at least one point that is the image under α of one b.c.p. of α and β.*

Proof. Let $\beta_{r+1}, \ldots, \beta_s$ the rest of cycles of β of lengths $l_{r+1}, \ldots l_s$, respectively. As α commutes with β on every one of this cycles then α transforms each β_t into an l_t-cycle β'_t, for $r+1 \leq t \leq s$ and then there exists $\beta'_{r+1}, \ldots, \beta'_s$ cycles of β of lengths $l_{r+1}, \ldots, l_s$, respectively such that $\alpha\left(\mathrm{set}(\beta_{r+1}) \cup \cdots \cup \mathrm{set}(\beta_s)\right) = \mathrm{set}(\beta'_{r+1}) \cup \cdots \cup \mathrm{set}(\beta'_s)$ and the result of the first part of the proposition follows because α is a bijection. The previous argument also implies that if α does not commute with exactly h_i i-cycles of β and that commutes with the rest of the i-cycles of β (if any) then there exists exactly h_i i-cycles of β, say $\beta''_1, \ldots, \beta''_{h_i}$, such that $\beta''_t \neq \alpha\beta_j\alpha^{-1}$ for any cycle β_j of β. The following claim completes the proof of the second part

Claim 3.14. *If all the points in an i-cycle $\beta_{j'}$ of β are images under α of g.c.p., then $\beta_{j'} = \alpha\beta_j\alpha^{-1}$ for some i-cycle β_j of β.*

Proof. We first prove that if all the points in the i-cycle $\beta_{j'}$ are images under α of β of g.c.p. of α and β then these g.c.p. belong to exactly one l-cycle $\beta_j = (b_1 \ldots b_l)$. If $\beta_{j'}$ contains the images under α of g.c.p. in different cycles of β, then $\beta_{j'}$ contains the string $\alpha(x)\alpha(y)$ with x and y in different cycles of β, i.e., $\beta(x) \neq y$, but this implies that x is a b.c.p. because $\alpha(\beta(x)) \neq \alpha(y) = \beta(\alpha(x))$. Now we show that $l \leq i$. Suppose that $l > i$ then, and without lost of generality, we have that $\beta'_j = (\alpha(b_1) \ldots \alpha(b_i))$, i.e., $\beta'_j(\alpha(b_t)) = \alpha(b_{t+1 \mod i})$, for every t (if $\beta'_j(\alpha(b_t)) \neq \alpha(b_{t+1 \mod i})$ for some t then b_t will be a b.c.p.). But this implies that b_i is a b.c.p. because $\beta(\alpha(b_i)) = \alpha(b_1) \neq \alpha(b_{i+1}) = \alpha(\beta(b_i))$, which is a contradiction. Therefore $l \leq i$, and this will implies that $l = i$ (by using a similar argument as the previous one), i.e. $\beta_{j'} = \alpha\beta_j\alpha^{-1}$. $\qquad\square$

$\qquad\square$

3.1 Permutations that (k, β)-commute with a cycle of β

Let $k \geq 3$ be a positive integer. Let α be any permutation that k-commutes with β and that (k, β)-commutes with an m-cycle, say β_j, of β, i.e., all the b.c.p. of α and β are in β_j. From Proposition 3.13 it follows that there exist exactly one m-cycle, say $\beta_{j'}$, of β such that $\mathrm{set}(\beta_{j'}) = \alpha(\mathrm{set}(\beta_j))$. Using this fact we present a procedure (Algorithm 1) that allows us to obtain any such permutation α. First we give some definitions. The *canonical cycle notation* of a permutation π is defined as follows: first, write the largest element of each cycle, and then arrange the cycles in increasing order of their first elements. Let π be a permutation written in its canonical cycle notation, the *transition function* of π from canonical cycle notation to one-line notation is the map $\Psi : S_n \to S_n$ that sends π to the permutation $\Psi(\pi)$

written in one-line notation that is obtained from π by omitting all the parentheses. This map is a bijection (see, e.g., [2, p. 96]).

Example 3.15. Let $\pi \in S_7$ be $(431)(65)(72)$ (π is written in its canonical cycle notation). Then $\Psi(\pi) = 4316572$.

Algorithm 1.

Step 1. Choose m-cycles β_j and $\beta_{j'}$ of β (with the possibility that $\beta_{j'} = \beta_j$), and with $m \geq k$.

Step 2 Choose a subset of k points of $\mathrm{set}(\beta_{j'})$. Let $P = p_1 p_2 \ldots p_m$ be any improper block of $\beta_{j'}$ such that p_m is one of the selected points. Let $p_{h_1}, p_{h_2}, \ldots, p_{h_k} = p_m$ the k selected points whit $h_1 < \cdots < h_k$. Now partition the improper block P into k blocks, $P_1, P_2, \ldots, P_k$, as follows

$$\underbrace{p_1 \cdots p_{h_1}}_{P_1} \underbrace{p_{h_1+1} \cdots p_{h_2}}_{P_2} \cdots \underbrace{p_{h_{k-1}+1} \cdots p_{h_k}}_{P_k},$$

i.e., $P = P_1 P_2 \ldots P_k$, and where p_{h_r} is the last point of P_r, $1 \leq r \leq k$.

Step 3 Choose any k-cycle τ of $[k] = \{1, \ldots, k\}$ with $\tau(a) \neq a+1 \bmod k$, for every $a \in [k]$, and make the block permutation

$$P' := P_{\Psi(\tau)(1)} P_{\Psi(\tau)(2)} \ldots P_{\Psi(\tau)(k)} = P_{i_1} P_{i_2} \ldots P_{i_k},$$

where $\Psi(\tau)$ is the transition function of the canonical cycle notation of τ to one-line notation (notice that τ in its canonical cycle notation is equal to $(i_1 \ldots i_k)$).

Step 4 Construct $\alpha|_{\mathrm{set}(\beta_j)} : \mathrm{set}(\beta_j) \to \mathrm{set}(\beta_{j'})$ in block notation as it follows:

$$\alpha|_{\mathrm{set}(\beta_j),k} = \begin{pmatrix} B_1 & B_2 & \ldots & B_k \\ P_{i_1} & P_{i_2} & \ldots & P_{i_k} \end{pmatrix}.$$

where $\beta_j = (B_1 \ldots B_k)$ and $|B_r| = |P_{i_r}|$, $1 \leq r \leq k$.

Step 5. Construct $\alpha|_{[n]\setminus\mathrm{set}(\beta_j)} : [n] \setminus \mathrm{set}(\beta_j) \to [n] \setminus \mathrm{set}(\beta_{j'})$ as any bijection that commutes with $\beta|_{[n]\setminus\mathrm{set}(\beta_j)} : [n] \setminus \mathrm{set}(\beta_j) \to [n] \setminus \mathrm{set}(\beta_{j'})$.

Notice that Step 5 is possible because α can be constructed in such a way that it transforms the $c_m - 1$ m-cycles of β different than β_j (if any) into the $c_m - 1$ m-cycles of β different than $\beta_{j'}$ (if any), and that transforms the l-cycles of β (if any), with $l \neq m$, into l-cycles of β (if any). The following two propositions shows that Algorithm 1 produces all the permutation α with the desired properties.

Proposition 3.16. *Permutation α constructed with Algorithm 1 does not commute with β on all points in $\mathcal{A} := \alpha^{-1}(\{p_{h_1}, \ldots, p_{h_k}\})$ and commutes with β on all points in $[n] \setminus \mathcal{A}$.*

Proof. Let β_j and $\beta_{j'}$ be the cycles of β selected in Step 1 of Algorithm 1, and $\{p_{h_1}, \ldots, p_{h_k}\}$ the subset of $\mathrm{set}(\beta_{j'})$ selected in Step 2. By the way in which α is constructed of in Step 3 and 4, $\alpha\beta_j\alpha^{-1}$ has $P_{i_1}P_{i_2}\ldots P_{i_k}$ as an improper block, where $P_{i_r}P_{i_{r+1 \bmod k}}$, $1 \le r \le k$, is not a block in any cycle of β (by Step 3, $i_{r+1 \bmod k} - i_r \bmod k \ne 1$). From Theorem 3.8, we have that α does not commute with β on exactly k points in $\mathrm{set}(\beta_j)$. Even more, in the proof of Theorem 3.8 was showed that α and β do not commute on $\alpha^{-1}(p_{h_r})$, $1 \le r \le k$ (see Remark 3.9). Finally, by the construction of α in Step 5, α and β commute on all points in $[n] \setminus \mathrm{set}(\beta_j)$. $\qquad\square$

Proposition 3.17. *Let $k \ge 3$. Any permutation α that k-commutes with β and such that all the b.c.p. of α and β are in one cycle of β can be obtained with Algorithm 1.*

Proof. Let α be any permutation that k-commutes with β and such that all the b.c.p. are in exactly one m-cycle, say β_j, of β. From Proposition 3.13 it follows that there exists exactly one m-cycle, say $\beta_{j'}$, of β such that $\alpha(\mathrm{set}(\beta_j)) = \mathrm{set}(\beta_{j'})$. By Theorem 3.8, we have that $\alpha\beta_j\alpha^{-1} = (P_1 \ldots P_k)$, where $P_1, \ldots, P_k$ are k pairwise disjoint blocks in $\beta_{j'}$ and $P_r P_{r+1 \bmod k}$ is not a block in any cycle of β, $1 \le r \le k$. As $\alpha(\mathrm{set}(\beta_j)) = \mathrm{set}(\beta_{j'})$, we have that $P_1 \ldots P_k$ is a block permutation of $B' = P_{i_1} \ldots P_{i_k}$, where $\beta_{j'} = (B')$. Now, rename the blocks P_{i_s} as B'_s to obtain $B' = B'_1 \ldots B'_k$. In this way, $\alpha\beta_j\alpha^{-1} = (B'_{l_1} \ldots B'_{l_k})$ with $l_{r+1 \bmod k} - l_r \bmod k \ne 1$, $1 \le r \le k$. Indeed, if $l_{r+1 \bmod k} - l_r \bmod k = 1$ for some $r \in \{1, \ldots, k\}$, then $B'_{l_r}B'_{l_{r+1 \bmod k}}$ will be a block in $\beta_{j'}$, and hence the number of b.c.p. of α and β will be less than k, which is a contradiction.

As $\alpha\beta_j\alpha^{-1} = (B'_{l_1} \ldots B'_{l_k}) = (B'_{l_2} \ldots B'_{l_1}) = \cdots = (B'_{l_k} \ldots B'_{l_{k-1}})$, we can assume without lost of generality that $l_1 = k$ (from these k expressions, choose the one that begins with block B'_k). Then $\alpha|_{\mathrm{set}(\beta_j)}$ can be written as

$$\alpha|_{\mathrm{set}(\beta_j),k} = \begin{pmatrix} B_1 & \ldots & B_k \\ B'_{l_1} & \ldots & B'_{l_k} \end{pmatrix},$$

where $\beta_j = (B_1 \ldots B_k)$, and $|B_i| = |B'_{h_i}|$, $1 \le i \le k$.

Now, we consider $l_1 l_2 \ldots l_k$ as a permutation, named π, of $\{1, \ldots, k\}$ in one-line notation. As l_1 (that is equal to k) is the greatest element in $\{l_1, \ldots, l_k\}$, then $\tau := \Psi^{-1}(\pi) = (l_1 \ldots l_k)$, where Ψ is the transition function of the canonical cycle notation to one-line notation. Notice that τ is a k-cycle in S_k such that $\tau(a) \ne a + 1$, for any $a \in [k]$. Thus we conclude that $\alpha|_{\mathrm{set}(\beta_j)}$ can be obtained by Steps 1 to 4 of Algorithm 1. Now as α commutes with β on all different cycles from β_j, $\alpha|_{[n]\setminus\mathrm{set}(\beta_j)}$ can be obtained with Step 5 of Algorithm 1. $\qquad\square$

4 On the number $c(k, \beta)$

In this section we present some results about the number $c(k, \beta)$. First we show that for any nonnegative integer k and any $\beta \in S_n$, the number $c(k, \beta)$ is invariant under conjugation. Let $C(k, \beta) = \{\alpha \in S_n : H(\alpha\beta, \beta\alpha) = k\}$ (so that $c(k, \beta) = |C(k, \beta)|$)

Proposition 4.1. *Let $\beta \in S_n$. Then $c(k, \tau\beta\tau^{-1}) = c(k, \beta)$ for any $\tau \in S_n$.*

Proof. (*Sketch*) For $\tau \in S_n$, let $\tau C(k, \beta) \tau^{-1} := \{\tau \alpha \tau^{-1} : \alpha \in C(k, \beta)\}$. By the bi-invariance of the Hamming metric is straightforward to show that $C(k, \tau \beta \tau^{-1}) = \tau C(k, \beta) \tau^{-1}$. Now, it is easy to check that the function $\phi : C(k, \beta) \rightarrow \tau C(k, \beta) \tau^{-1}$ given by $\sigma \mapsto \tau \sigma \tau^{-1}$ is a bijection, so we have that $|C(k, \beta)| = |\tau C(k, \beta) \tau^{-1}| = |C(k, \tau \beta \tau^{-1})|$.
$\square$

Remark 4.2. If β and β' are conjugate permutations it is not always true that $C(k, \beta) = C(k, \beta')$. For example, let $\beta = (12345) \in S_5$ and $\beta' = (23145)$. If $\alpha = (14)(25)$ then $H(\alpha\beta, \beta\alpha) = 3$ and $H(\alpha\beta', \beta'\alpha) = 5$, which implies that $C(3, \beta) \neq C(3, \beta')$.

The following result shows that $c(k, \beta)$ is a multiple of $|C_{S_n}(\beta)|$.

Proposition 4.3. *Let $\beta \in S_n$. Suppose that $C(k, \beta)$ is a non-empty set. Then*

$$C(k, \beta) = \bigcup_{\alpha \in C(k, \beta)} C_{S_n}(\beta) \alpha.$$

Proof. The inclusion $C(k, \beta) \subseteq \bigcup_{\alpha \in C(k, \beta)} C_{S_n}(\beta) \alpha$ is clear. Now, let $\rho \in \bigcup_{\alpha \in C(k, \beta)} C_{S_n}(\beta) \alpha$, then $\rho = \tau \alpha$ for some $\tau \in C_{S_n}(\beta)$ and some $\alpha \in C(k, \beta)$. So we have that $H(\rho\beta, \beta\rho) = H(\tau\alpha\beta, \beta\tau\alpha) = H(\tau\alpha\beta, \tau\beta\alpha) = H(\alpha\beta, \beta\alpha) = k$, and then $\rho \in C(k, \beta)$.
$\square$

Corollary 4.4. *Let $\beta \in S_n$ and let k be any non-negative integer. Then $c(k, \beta)$ is a multiple of $|C_{S_n}(\beta)|$.*

4.1 Number of even permutations in $C(k, \beta)$

One interesting application of Proposition 4.3 is that for β of some special cycle type we can find the proportion of even permutations in $C(k, \beta)$. We say that a permutation is a *cdoi-permutation* if its cycle type consist of distinct odd integers. We need the following propositions.

Proposition 4.5. *[11, exercise 21, p. 131.] The permutation $\sigma \in S_n$ does not commute with any odd permutation if and only if the cycle type of σ consist of distinct odd integers.*

Proposition 4.6. *[30, exercise 3.22, p. 51.] If $G \leq S_n$ contains an odd permutation, then $|G|$ is even, and exactly half of the elements in G are odd permutations.*

We are ready to prove the following.

Proposition 4.7. *Let $\beta \in S_n$ be a permutation that is not a cdoi-permutation. Then exactly one half of the permutations in $C(k, \beta)$ are odd.*

Proof. As the cycle type of β does not consist only of distinct odd integers, then from Proposition 4.5 it follows that β commutes with an odd permutation, i.e., $C_{S_n}(\beta)$ contains at least one odd permutation. By Proposition 4.6 we have that exactly one half of the elements in $C_{S_n}(\beta)$ are odd permutations. Then, for any α in $C(k, \beta)$, the number of odd permutations in $C_{S_n}(\beta)\alpha$ remains one half. Finally, as $C(k, \beta) = \bigcup_{\alpha \in C(k, \beta)} C_{S_n}(\beta)\alpha$ (by Proposition 4.3), we have that exactly one half permutations in $C(k, \beta)$ are odd.
$\square$

Corollary 4.8. *If β is not a cdoi-permutation then $c(k, \beta)$ is even.*

Question 4.9. *Let β be a cdoi-permutation, what is the number of even permutations that k-commute with β?*

4.2 On the number $c(\lambda_{k^{(1)}}, \beta)$

We use the following notation: Let $\lambda_k = [k_1, \ldots, k_h]$ denotes an integer partition of k, with $k_i \geq 1$. If $\lambda_k = [k_1, \ldots, k_h]$ is an integer partition of k, we use $C(\lambda_k, \beta)$, or $C([k_1, \ldots, k_h], \beta)$, to denote the set of permutations that k-commutes with β such that for every $\alpha \in C([k_1, \ldots, k_h], \beta)$ there exists exactly h cycles, says $\beta_1, \ldots, \beta_h$, in the cycle decomposition of β, where α (k_1, β)-commutes with β_1, (k_2, β)-commutes with β_2, ..., (k_h, β)-commutes with β_h. We will use $c(\lambda_k, \beta)$ or $c([k_1, \ldots, k_h], \beta)$ to denote the cardinality of $C(\lambda_k, \beta)$. We will use the notation $c(\lambda_{k^{(1)}}, \beta)$ and $c(\lambda_{k^{(k)}}, \beta)$ instead of $c([k_1], \beta)$ and $c([1, \ldots, 1], \beta)$, respectively.

Example 4.10. Let $\alpha, \beta \in S_{14}$, with $\beta = (1\ 2)(3\ 4\ 5)(6\ 7\ 8)(9\ 10\ 11\ 12)(13\ 14)$ and $\alpha = (1\ 3\ 9\ 6)(2\ 4\ 10\ 7)(5\ 11\ 8)$. We have that α 6-commutes with β in the following way: α $(1, \beta)$-commutes with $(1\ 2)$, $(1, \beta)$-commutes with $(3\ 4\ 5)$, $(2, \beta)$-commutes with $(6\ 7\ 8)$, $(2, \beta)$-commutes with $(9\ 10\ 11\ 12)$ and commutes with β on $(13\ 14)$.

Remark 4.11. We are considering unordered partitions, for example $[2, 2, 1] = [2, 1, 2]$.

Let $L(\beta)$ denotes the set of cycle lengths in the cycle decomposition of β including 1-cycles. Let $\mathcal{C}_l(\beta)$ be the set of all l-cycles in the cycle decomposition of β. Let $\mathcal{S}(\beta)$ be a subset of the set of all the cycles in β. Suppose that we want to construct a permutation α that will not commute with β on all the cycles in $\mathcal{S}(\beta)$ (for every cycle $\beta_j \in \mathcal{S}(\beta)$, α and β will not commute on at least one point in β_j) and that commutes on every point of the remaining (if any) cycles of β. Let $L_\mathcal{S}$ be the set of lengths of cycles in $\mathcal{S}(\beta)$ and let $\mathcal{S}_l$ be the set of all cycles of length l in $\mathcal{S}(\beta)$. From Proposition 3.13 it follows that we can construct α by obtaining two bijections $\alpha|_R : R \to R'$ and $\alpha|_{\overline{R}} : \overline{R} \to \overline{R'}$, where $R = \bigcup_{\beta_j \in \mathcal{S}(\beta)} \text{set}(\beta_j)$, $\overline{R} = [n] \setminus R$, with the following steps (R' and $\overline{R'}$ are defined in Step 2 below).

Algorithm 2.

Step 1 For every $l \in L_\mathcal{S}$, select a subset $\mathcal{S}'_l(\beta) \subseteq \mathcal{C}_l(\beta)$ of cardinality $h_l := |\mathcal{S}_l(\beta)|$ and obtain $\mathcal{S}'(\beta) := \bigcup_{l \in L_\mathcal{S}} \mathcal{S}'_l(\beta)$ (the cycles in $\mathcal{S}'(\beta)$ will contain the images under α of points in cycles in $\mathcal{S}(\beta)$).

Step 2 Construct a bijection $\alpha|_R : R \to R'$, where $R' = \bigcup_{\beta_j \in \mathcal{S}'(\beta)} \text{set}(\beta_j)$, in such a way that $\alpha|_R$ and $\beta|_R$ will not commute on the desired points.

Step 3 Construct a bijection $\alpha|_{\overline{R}} : \overline{R} \to \overline{R'}$, where $\overline{R'} = [n] \setminus R'$, as any bijection that commutes with $\beta|_{\overline{R}}$.

The construction in Step 3 can be done as follows: for every $l \in L_\mathcal{S}$ (resp. $l \notin L_\mathcal{S}$), construct $\alpha|_{\overline{R}}$ in such a way that α transforms cycles in $\mathcal{C}_l(\beta) \setminus \mathcal{S}_l(\beta)$ into cycles in $\mathcal{C}_l(\beta) \setminus \mathcal{S}'_l(\beta)$ (resp. that transforms cycles in $\mathcal{C}_l(\beta)$ into cycles in $\mathcal{C}_l(\beta)$). The more difficult part is to obtain all bijections $\alpha|_R$ in Step 2. Let r_0 denotes the number of ways to construct $\alpha|_R$ in Step 2 of Algorithm 2. The following technical proposition will be useful to simplify some of the calculations in some of the enumerative results in this paper (and also shows that the main enumerative problem is to find r_0).

Proposition 4.12. *Let $H = \{\ell_1, \ldots, \ell_i\}$ be a subset of $L(\beta)$. The number of permutations α that does not commute with β on exactly h_{ℓ_1} ℓ_1-cycles of β, h_{ℓ_2} ℓ_2-cycles of β, $\ldots$, h_{ℓ_i} ℓ_i-cycles of β and that commutes with the rest of cycles of β is equal to*

$$r_0 |C_{S_n}(\beta)| \prod_{\ell \in H} \frac{1}{h_\ell! \ell^{h_\ell}} \binom{c_\ell}{h_\ell}.$$

Proof. We will count the number of ways to select the set $\mathcal{S}(\beta)$ of all cycles of β where α and β will not commute and the set $\mathcal{S}'(\beta)$ in Step 1 of Algorithm 2. Let c_ℓ denotes the number of ℓ-cycles in the cycle decomposition of β. For every $\ell \in H$, there are $\binom{c_\ell}{h_\ell}$ ways to select the ℓ-cycles that will belong to $\mathcal{S}(\beta)$ and $\binom{c_\ell}{h_\ell}$ ways to select the ℓ-cycles that will belong to $\mathcal{S}'(\beta)$. Now we enumerate all bijections $\alpha|_{\overline{R}}$ that can be obtained as in Step 3 of Algorithm 2. Once we have selected $\mathcal{S}(\beta)$ and $\mathcal{S}'(\beta)$, for every $l \in H$, there are $(c_\ell - h_\ell)! l^{c_\ell - h_\ell}$ ways to make that α transforms the $c_\ell - h_\ell$ cycles of length ℓ of β not belonging to $\mathcal{S}(\beta)$ into the $c_\ell - h_\ell$ cycles of length ℓ of β not belonging to $\mathcal{S}'(\beta)$. For $l \notin H$, there are $|C_{S_n}(\beta)| \prod_{l \in H} \frac{1}{l^{c_\ell} c_\ell!}$ ways to make that α transforms the c_ℓ ℓ-cycles of β into c_ℓ ℓ-cycles of β. Then we have that the number of permutations α that satisfies the desired conditions is equal to

$$r_0 \prod_{l \in H} \binom{c_\ell}{h_\ell}^2 \prod_{l \in H} (c_\ell - h_\ell)! l^{c_\ell - h_\ell} \left(|C_{S_n}(\beta)| \prod_{l \in H} \frac{1}{l^{c_\ell} c_\ell!} \right) = r_0 |C_{S_n}(\beta)| \prod_{l \in H} \frac{1}{h_\ell! l^{h_\ell}} \binom{c_\ell}{h_\ell}.$$

$\square$

Let $f(k)$ be the number of cyclic permutations (k-cycles) of $\{1, \ldots, k\}$ with no $i \mapsto i + 1 \mod k$ (see, e.g., [35, exercise 8, p. 88] or sequence A000757 in OEIS [33]).

Theorem 4.13. *Let $\beta \in S_n$ be of type $(c_1, \ldots, c_n)$. Let k be an integer, $3 \leq k \leq n$. Then*

$$c(\lambda_{k^{(1)}}, \beta) = |C_{S_n}(\beta)| \sum_{\ell \geq k} c_\ell \binom{\ell}{k} f(k).$$

Proof. As all the b.c.p. of α and β are in one ℓ-cycle $\beta_j = (b_1 \ b_2 \ \ldots \ b_\ell)$ of β, then the images under α of the b.c.p are in exactly one ℓ-cycle $\beta_{j'} = (b'_1 \ b'_2 \ \ldots \ b'_\ell)$ of β (by Proposition 3.13). There are $\ell \binom{\ell}{k} f(k)$ ways to construct a bijection $\alpha|_{\text{set}(\beta_j)} : \text{set}(\beta_j) \to \text{set}(\beta_{j'})$ with steps 2 to 4 in Algorithm 1. Indeed, there are $\binom{\ell}{k}$ ways to choose the subset in Step 2; there are $f(k)$ ways to select the permutation τ in Step 3, and there are ℓ ways to select the first point in block $B_1 \ldots B_k$ in Step 4. By using Proposition 4.12 (with $H = \{\ell\}$, $h_\ell = 1$ and $r_0 = \ell \binom{\ell}{k} f(k)$) and after summing over all possible lengths $\ell \geq k$ of cycles of β we have

$$c(\lambda_{k^{(1)}}, \beta) = \sum_{\ell \geq k} \ell \binom{\ell}{k} f(k) \frac{1}{\ell} c_\ell |C_{S_n}(\beta)| = |C_{S_n}(\beta)| \sum_{\ell \geq k} c_\ell \binom{\ell}{k} f(k).$$

$\square$

Let $T(k, n)$ denote the number of permutations that k-commute with an n-cycle.

Corollary 4.14. *Let n be a positive integer and k and integer with $0 \le k \le n$. Then*

$$T(k, n) = n \binom{n}{k} f(k).$$

The number $T(k, n)$ is now sequence A233440 in [33]. With this corollary we can obtain in an easy way the binomial transform of sequence A000757. Let $A = \{f(0), f(1), \dots\}$ be sequence A000757, and let $B = \{b_0, b_1, \dots\}$ be the binomial transform of A. In [34] b_n is defined as $\sum_{k=0}^{n} \binom{n}{k} f(k)$ that is equal to $\sum_{k=0}^{n} T(k, n)/n$ by Corollary 4.14. Then we have that $b_n = (n-1)!$ because $\sum_{k=0}^{n} T(k, n) = n!$. No we present the following limit property for $T(k, n)$.

Proposition 4.15. *Let n be a positive integer and m be a fixed nonnegative integer with $m \ne n$. Then*

$$\lim_{n \to \infty} \frac{T(n-m, \ n)}{n!} = \frac{e^{-1}}{m!}.$$

Proof.

$$
\begin{aligned}
T(n-m, n)/n! &= n \binom{n}{n-m} f(n-m)/n! \\
&= \frac{n}{m!(n-m)!} f(n-m) \\
&= \frac{n}{m!} \frac{f(n-m)}{(n-m)(n-m-1)!} \\
&= \frac{f(n-m)}{m!(n-m-1)!} + \frac{m f(n-m)}{m!(n-m)(n-m-1)!}.
\end{aligned}
$$

And the result follows by using that $\lim_{k \to \infty} f(k)/(k-1)! = e^{-1}$ ([35, exercise 8-e, p. 88]). $\square$

If $m = 0$ we have $\lim_{n \to \infty} \frac{T(n,\ n)}{n!} = e^{-1}$. Now we present a bivariate generating function for $T(k, n)$.

Theorem 4.16. *Let n, k be positive integers with $k \le n$. Then*

$$\sum_{n,k} T(k, n) \frac{z^n}{n!} u^k = z e^{z(1-u)} \left(\left(1 - \log(1 - zu)\right)\left(1 - u\right) + \frac{u}{1 - zu} \right)$$

Proof. Let $g^{\langle k \rangle}(z) = \sum_n g_{n,k} \frac{z^n}{n!}$ denotes the vertical generating function (exponential case) of the sequence $\{g_{n,k}\}$. Let $c_{n,k} = T(k, n)/n = \binom{n}{k} f(k)$. From Example III. 1, in [13, p. 155], and by using the fact that function $f(k)$ is independent of n we have

$$c^{\langle k \rangle}(z) = \sum_n \binom{n}{k} f(k) \frac{z^n}{n!} = f(k) \frac{e^z z^k}{k!}$$

Now, by using Rule (2') in [37, p. 41] we obtain

$$\sum_n n \binom{n}{k} f(k) \frac{z^n}{n!} = f(k) z \left(\frac{e^z z^k}{k!} + \frac{e^z z^k k}{zk!} \right)$$

15

Now

$$P(z, u) \;:=\; \sum_{k,n} n \binom{n}{k} f(k) \frac{z^n}{n!} u^k$$

$$= \sum_{k} \Big(\sum_{n} n \binom{n}{k} f(k) \frac{z^n}{n!} \Big) u^k$$

$$= \sum_{k} f(k) z \Big(\frac{e^z z^k}{k!} + \frac{e^z z^k k}{zk!} \Big) u^k$$

$$= \sum_{k} f(k) z \Big(\frac{e^z z^k}{k!} \Big) u^k + \sum_{k} f(k) z \frac{e^z z^k k}{zk!} u^k$$

$$= ze^z \sum_{k} f(k) \frac{z^k u^k}{k!} + e^z \sum_{k} k f(k) \frac{z^k u^k}{k!}.$$

It is known that $\sum_{k \geq 0} f(k) \frac{x^k}{k!} = e^{-x}(1 - \log(1 - x))$ (see, e.g., [35, exercise 8, p. 88]), then

$$ze^z \sum_{k} f(k) \frac{z^k u^k}{k!} = ze^z (e^{-zu}(1 - \log(1 - zu)).$$

Now, we apply Rule (2') in [37] to the second term of $P(z, u)$ to obtain

$$e^z \sum_{k} k f(k) \frac{z^k u^k}{k!} = e^z (zu) e^{-zu} \Big(\frac{1}{1 - zu} - (1 - \log(1 - zu)) \Big),$$

and the result follows after some algebraic manipulations. $\qquad\square$

4.3 On the number $c(\lambda_{k^{(k)}}, \beta)$

In some cases, the number $c(\lambda_k, \beta)$ can be zero as shows the following

Proposition 4.17. *Let $\beta \in S_n$ and k be a positive integer. Then $c(\lambda_{k^{(k)}}, \beta) = 0$.*

This result is a direct consequence of the following.

Proposition 4.18. *Let $\alpha, \beta \in S_n$. If one cycle of β has exactly one b.c.p. of α and β, then there exist a cycle of β that contains at least two b.c.p. of α and β.*

Proof. The proof is by induction on the length l of the cycle β_1 of β which contains exactly one b.c.p of α and β. First we prove the case $l = 1$. By hypothesis, β has a fixed point that is a b.c.p. of α and β and then, by Proposition 3.13, there exists one fixed point, say x', of β whose preimage under α, $\alpha^{-1}(x')$, is a b.c.p. From Proposition 3.4 it follows that $\alpha^{-1}(x')$ is a point in a cycle β_j of β of length greater than one. Then $\beta_j = (\alpha^{-1}(x')B)$ with B a block of length $|B| \geq 1$. Therefore, $\alpha\beta_j\alpha^{-1} = (x'B')$, and, by Theorem 3.8, β_j has at least two b.c.p. of α and β.

Now we prove the case $l > 1$. Let $\beta_1 = (d_1 \ldots d_l)$ be a cycle of β with exactly one b.c.p. of α and β, that without lost of generality we can suppose that is d_l. Assume by induction that the statement of the proposition is true for r-cycles of β which contains exactly one b.c.p of α and β with $r < l$ (notice that in general, it could be the case that no such cycles in β exist).

Let $\text{set}(\mathcal{C}_l(\beta)) = \bigcup_{\beta_j \in \mathcal{C}_l(\beta)} \text{set}(\beta_j)$. Let c_l denote the number of l-cycles of β. By Theorem 3.8 we have that $\alpha\beta_1\alpha^{-1} = (D)$ where $D = \alpha(d_1)\ldots\alpha(d_l)$ is a proper block in an s-cycle of β, with $s > l$, which implies that $\alpha^{-1}\big(\text{set}(\mathcal{C}_l(\beta))\big) \neq \text{set}(\mathcal{C}_l(\beta))$. Then, there exist at least one l-cycle $\beta_2 = (a_1 \ldots a_l)$ of β (with the possibility that $\beta_2 = \beta_1$) which contains at least one point, says a_1, which has its preimage under α in one m-cycle, say β_3, of length different than l. Let r be an integer between 1 and l such that $\alpha^{-1}(a_1)\ldots\alpha^{-1}(a_r)$ is a block $b_1 \ldots b_r$ in $\beta_3 = (b_1 \ldots b_m)$ of β, with $b_i = \alpha^{-1}(a_i)$, for $1 \leq i \leq r$, and such that $\alpha^{-1}(a_1)\ldots\alpha^{-1}(a_r)\alpha^{-1}(a_{r+1 \bmod l})$ is not a block in β_3. We have the following cases:

Case I. If $m > r$, then β_3 has at least two b.c.p. of α and β (by Theorem 3.8).

Case II. If $m = r$ then $r < l$ (because $m \neq l$ and $1 \leq r \leq l$) and $\alpha\beta_3\alpha^{-1} = (a_1 \ldots a_m)$. As $a_1 \ldots a_m$ is a proper block in β_2 then β_3 has exactly one b.c.p. of α and β (by Theorem 3.8). And it follows from the inductive hypothesis that β has a cycle with at least two b.c.p. of α and β. $\square$

5 The number $c(k, \beta)$ for $k = 3, 4$

In this section we present formulas for the number $c(k, \beta)$, when β is any permutation of cycle type $(c_1, \ldots, c_n)$ and $k = 3, 4$.

Theorem 5.1. *Let β be any n-permutation of type $(c_1, \ldots, c_n)$. Then*

$$c(3, \beta) = \left(\sum_{\ell \geq 3}^{n} c_\ell \binom{\ell}{3} + \sum_{1 \leq \ell < m \leq n} \ell m c_\ell c_m \right) |C_{S_n}(\beta)|.$$

Proof. By Proposition 4.17 we have that $c(\lambda_{3^{(3)}}, \beta) = 0$. Then $c(3, \beta) = c(\lambda_{3^{(1)}}, \beta) + c([2, 1], \beta)$. The case $c(\lambda_{3^{(1)}}, \beta)$ follows from Lemma 4.13. In order to obtain $c([2, 1], \beta)$, we construct all permutations α that 3-commute with β and such that β has a unique ℓ-cycle (resp. m-cycle), say β_1 (resp. β_2), where α $(1, \beta)$-commutes with β_1 (resp. $(2, \beta)$-commutes with β_2). By Proposition 3.13 there exist exactly one ℓ-cycle β_1' and exactly one m-cycle β_2' such that $\alpha\left(\text{set}(\beta_1) \cup \text{set}(\beta_2)\right) = \text{set}(\beta_1') \cup \text{set}(\beta_2')$. From Theorem 3.8 we have that

$$\alpha|_{\text{set}(\beta_1)\cup\text{set}(\beta_2)} = \begin{pmatrix} A_1 \\ X_1 \end{pmatrix} \begin{pmatrix} B_1 & B_2 \\ X_2 & X_3 \end{pmatrix}, \tag{4}$$

where

a) $\beta_1 = (A_1)$, $\beta_2 = (B_1 B_2)$, and X_1, X_2, X_3 are blocks in β_1' and β_2'.

b) The strings $X_2 X_3$ and $X_3 X_2$ are not blocks in any cycle of β, and X_1 is a block in a cycle of length greater that A_1, i.e., X_1 is not a block in β_1'.

c) The set of all points in X_1, X_2, X_3 should be equal to $\mathrm{set}(\beta_1') \cup \mathrm{set}(\beta_2')$.

From conditions a) to c) above we have that X_2 and X_3 belongs to different cycles. Without lost of generality we can assume that $\beta_1' = (X_2)$ and that $\beta_2' = (X_1 X3)$. Now we count the number of ways to construct $\alpha|_{\mathrm{set}(\beta_1) \cup \mathrm{set}(\beta_2)}$ using notation (4). There are ℓ ways to select the first point of block A_1 and there are m ways to select the first point of block $B_1 B2$. There are ℓ ways to select the first point of block X_2 and there are m ways to select the first point of block X_1 (after this selection the first point of block X_3 is uniquely determined). Now by Proposition 4.12 (with $H = \{\ell, m\}$, $h_\ell = 1$, $h_m = 1$, $r_0 = (\ell m)^2$) we have $\ell m c_\ell c_m |C_{S_n}(\beta)|$ for this ℓ and m. The result is obtained after we sum over all possible values of ℓ and m. $\qquad\square$

Theorem 5.2. *Let β be any permutation of cycle type $(c_1, \ldots, c_n)$. Then*

$$c(4, \beta) = c(\lambda_{4^{(1)}}, \beta) + c([3, 1], \beta) + c([2, 2], \beta) + c([2, 1, 1], \beta),$$

where

$$
\begin{aligned}
c(\lambda_{4^{(1)}}, \beta) &= |C_{S_n}(\beta)| \sum_{i \geq 4} c_i \binom{i}{4}; \\
c([3, 1], \beta) &= |C_{S_n}(\beta)| \sum_{i \geq 1, j \geq i+2} ij(j - i - 1) c_i c_j; \\
c([2, 2], \beta) &= |C_{S_n}(\beta)| \left(\sum_{i \geq 2} i \binom{i}{2} \binom{c_i}{2} + \sum_{j > i \geq 2} i(i - 1) j c_i c_j \right); \\
c([2, 1, 1], \beta) &= |C_{S_n}(\beta)| \left(\sum_{i \geq 1} i^3 c_{2i} \binom{c_i}{2} + \sum_{j > i \geq 1} ij(i + j) c_i c_j c_{i+j} \right).
\end{aligned}
$$

Proof. From Proposition 4.17 it follows that $c(\lambda_{4^{(4)}}, \beta) = 0$ and $c(\lambda_{4^{(1)}}, \beta)$ is obtained by Theorem 4.13. We divide the rest of the proof into three parts.

Part A: The number $c([2, 1, 1], \beta)$

Let l_1, l_2, l_3 denote the lengths of the cycles $\beta_1, \beta_2, \beta_3$ of β, respectively, that contains exactly two b.c.p. of α and β, exactly one b.c.p., and exactly one b.c.p., respectively. By Proposition 3.13 β has exactly three cycles, say $\beta_1', \beta_2', \beta_3'$, with $|\beta_i'| = |\beta_i|$, for $i = 1, 2, 3$, such that $\alpha\,(\mathrm{set}(\beta_1) \cup \mathrm{set}(\beta_2) \cup \mathrm{set}(\beta_3)) = \mathrm{set}(\beta_1') \cup \mathrm{set}(\beta_2') \cup \mathrm{set}(\beta_3')$. From Theorem 3.8 we have

$$
\alpha|_{\mathrm{set}(\beta_1) \cup \mathrm{set}(\beta_2) \cup \mathrm{set}(\beta_3)} = \begin{pmatrix} A_1 & A_2 \\ X_1 & X_2 \end{pmatrix} \begin{pmatrix} B \\ X_3 \end{pmatrix} \begin{pmatrix} C \\ X_4 \end{pmatrix}, \tag{5}
$$

where

a) $\beta_1 = (A_1 A_2)$, $\beta_2 = (B)$, $\beta_3 = (C)$, and the blocks X_1, X_2, X_3, X_4 came from β_1', β_2' and β_3' (not necessarily in this order),

b) The strings $X_1 X_2$ and $X_2 X_1$ are not blocks in any cycle of β and the cycle that contains X_3 (resp. X_4) is of length grater that l_2 (resp. l_3).

c) The set of all points in X_1, X_2, X_3, X_4 should be equal to $\mathrm{set}(\beta_1') \cup \mathrm{set}(\beta_2') \cup \mathrm{set}(\beta_3')$.

18

From conditions a) to c) above follows that the blocks X_3 and X_4 are blocks in β_1' (which implies that $l_1 = l_2 + l_3$) and that X_1 and X_2 are improper blocks in β_2' and β_3' (not necessarily in this order). We have two cases:

Claim 5.3. *1. If $l_2 = l_3$ then the number of permutations in $C([2,1,1], \beta)$ satisfying this extra condition is*

$$|C_{S_n}(\beta)| \sum_{l_2 \geq 1} l_2{}^3 c_{2l_2} \binom{c_{l_2}}{2}.$$

2. If $l_2 \neq l_3$ then the number of permutations in $C([2,1,1], \beta)$ satisfying this extra condition is

$$|C_{S_n}(\beta)| \sum_{l_3 > l_2 \geq 1} (l_2 + l_3) l_2 l_3 c_{l_2 + l_3} c_{l_2} c_{l_3},$$

where we are assuming, without lost of generality, that $l_3 > l_2$.

Proof. 1). As $|\beta_2'| = |\beta_3'|$ then it follows that $l_1 = 2l_2$. Now we count all bijections using matrix notation 5. There are l_1, l_2, and l_2 ways to select the points that will be the first points of the blocks $A_1 A_2, B, C$, respectively. There are l_2 and l_2 ways to select the first element of the block X_1 and X_2, respectively. There are l_1 ways to select the first point of the block X_3. Once the first point of X_3 is selected the first point of the block X_4 is uniquely determined. From Proposition 4.12 (with $H = \{l_1, l_2\}, h_{l_1} = 1, h_{l_2} = 2, r_0 = l_1^2 l_2^4$) we have that the number of permutations α that satisfies the desired conditions is $l_2^3 c_{2l_2} \binom{c_{l_2}}{2} |C_{S_n}(\beta)|$. Finally, the result follows by summing over all possible lengths of cycles $\beta_1, \beta_2, \beta_3$ *Proof of 2).* $l_2 \neq l_3$. Without lost of generality we can assume that $l_3 > l_2$. The enumeration of all bijections as in equation 5 is similar to the previous case. Then, from Proposition 4.12 (with $H = \{l_1, l_2, l_3\}, h_{l_i} = 1$, for every i, and $r_0 = l_1^2 l_2^2 l_3^2$) we have that the desired number is $(l_2 + l_3) l_2 l_3 c_{l_2 + l_3} c_{l_2} c_{l_3} |C_{S_n}(\beta)|$ and the result follows by summing over all possible lengths of cycles $\beta_1, \beta_2, \beta_3$. $\qquad\square$

Part B: The number $c([2,2], \beta)$

Let β_1 and β_2 the cycles of β of lengths l_1, l_2, respectively, that will contains 2 b.c.p of α and β every one. By Proposition 3.13, there exist exactly two cycles β_1' and β_2' such that $\alpha(\text{set}(\beta_1) \cup \text{set}(\beta_2)) = \text{set}(\beta_1') \cup \text{set}(\beta_2')$, with $|\beta_1'| = |\beta_1|$ and $|\beta_2'| = |\beta_2|$. By Theorem 3.8) we have that

$$\alpha\big|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)} = \begin{pmatrix} A_1 & A_2 \\ X_1 & X_2 \end{pmatrix} \begin{pmatrix} B_1 & B_2 \\ X_3 & X_4 \end{pmatrix}, \tag{6}$$

where

a) $\beta_1 = (A_1 A_2)$, $\beta_2 = (B_1 B_2)$, and X_1, X_2, X_3, X_4 are blocks in β_1' and β_2'.

b) The strings $X_1 X_2$ (resp. $X_3 X_4$) and $X_2 X_1$ (resp. $X_4 X_3$) are not blocks in any cycle of β.

c) The set of all points in X_1, X_2, X_3, X_4 should be equal to $\text{set}(\beta_1') \cup \text{set}(\beta_2') \cup \text{set}(\beta_3')$.

From points a) to c) above we have that X_1 and X_2 (resp. X_3 and X_4) belongs to different cycles. Without lost of generality we can assume that $\beta_1' = (X_1 X_3)$ and that $\beta_2' = (X_2 X4)$.

Claim 5.4.   *1. If $l_1 = l_2$, then the number $c([2,2], \beta)$ with this extra condition is*

$$|C_{S_n}(\beta)| \sum_{l_1 \geq 2} l_1 \binom{l_1}{2} \binom{c_{l_1}}{2}.$$

2. If $l_1 \neq l_2$, then the number $c([2,2], \beta)$ with this extra condition is

$$|C_{S_n}(\beta)| \sum_{l_2 > l_1 \geq 2} l_1(l_1 - 1)l_2 c_{l_1} c_{l_2}.$$

Proof of Claim 5.4. (1) $l_1 = l_2$: We count all possible bijections $\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)}$. There are l_1 and l_1 ways to select the first point of block $A_1 A_2$ and $B_1 B_2$, respectively. There are l_1 ways to select the point that will be the first point of X_1 and $l_1 - 1$ ways to select the first point of X_3. After that, the lengths of blocks A_1 and B_1 are unique determined (and hence also the lengths of blocks A_2 and B_2). There are l_1 ways to select the first point of X_2 and the first point of X_4 is uniquely determined. Then from Proposition 4.12 (with $H = \{l_1\}, h_{l_1} = 2$ and $r_0 = l_1^4(l_1 - 1)$) it follows that the number of permutations α satisfying the desired conditions is $l_1 \binom{c_{l_1}}{2} \binom{l_1}{2} |C_{S_n}(\beta)|$. Finally, the result follows by summing over all possible values of l_1.
    (2) $l_1 \neq l_2$: without lost of generality we can assume that $l_2 > l_1$. Notice that $l_1 \geq 2$. We make the enumeration of all possible bijections $\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)}$. There are l_1, l_2 ways to select the first points of $A_1 A_2$ and $B_1 B_2$, respectively. There are l_1 ways to select the point that will be the first point of block X_1 and $l_1 - 1$ ways to select the first point of block X_3. After that, the lengths of the blocks X_2 and X_4 are uniquely determined, so that it is enough to select the first point of block X_2 (in l_2 ways). From Proposition 4.12 (with $H = \{l_1, l_2\}, h_{l_1} = h_{l_2} = 1$ and $r_0 = l_1^2(l_1 - 1)l_2^2$) we have that the number of permutations with the desired characteristics is $l_1(l_1 - 1)l_2 c_{l_1} c_{l_2} |C_{S_n}(\beta)|$. The result follows after summing over all possible values of the cycle lengths. $\square$

Part C:
$$c([3,1], \beta) = |C_{S_n}(\beta)| \sum_{i \geq 1, j \geq i+2} ij(j - i - 1) c_i c_j.$$

Let α be any permutation that 4-commutes with β and such that $(3, \beta)$-commutes with an l_1-cycle, say β_1, of β and that $(1, \beta)$-commutes with an l_2-cycle, say β_2, of β. By Proposition 3.13, there exist exactly two cycles β_1' and β_2' such that $\alpha(\text{set}(\beta_1) \cup \text{set}(\beta_2)) = \text{set}(\beta_1') \cup \text{set}(\beta_2')$, with $|\beta_1'| = |\beta_1|$ and $|\beta_2'| = |\beta_2|$. From Theorem 3.8, and without lost of generality, we have

$$\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)} = \begin{pmatrix} A_1 & A_2 & A_3 \\ X_1 & X_2 & X_3 \end{pmatrix} \begin{pmatrix} B \\ Y \end{pmatrix}, \tag{7}$$

where $\beta_1 = (A_1 A_2 A_3)$, $\beta_2 = (B)$, Y is a block in β_1' (because $|Y| = l_2$) and X_1, X_2, X_3 are blocks in β_1' and β_2' such that $X_i X_{i+1}$ is not a block in any cycle of β. Without lost of generality we can assume that $\beta_1' = (Y X_1 X_3)$ which implies that $\beta_2' = (X_2)$. Notice that $l_1 \geq l_2 + 2$. Now we make the enumeration of all possible bijections in equation 7. There are l_1, l_2 ways to select the points that will be the first points of blocks $A_1 A_2 A_3$ and B, respectively. There are l_1 ways to select the point that will be the first point of

20

Y. After that, the first point of X_1 is uniquely determined (because $|Y| = |B|$). There are $l_1 - l_2 - 1$ ways to select the first point for the block X_3. There are l_2 ways to select the first point of the block X_2. Then by Proposition 4.12 we have that the desired number is $l_1 l_2 (l_1 - l_2 - 1) c_{l_1} c_{l_2} |C_{S_n}(\beta)|$. Finally we obtain our result by summing over all possible lengths.

With this last case the proof of theorem is completed. $\qquad\square$

6 Fixed-point free involutions

In this section we show formulas for $c(k, \beta)$ when β is a transposition and also when it is a fixed-point free involution. First we prove the following proposition. Let $\mathrm{fix}(\beta)$ denotes the set of fixed points of β and $\mathrm{supp}(\beta) = [\mathrm{n}] \setminus \mathrm{fix}(\beta)$.

Proposition 6.1. *Let* $\alpha, \beta \in S_n$ *and let* $H(\alpha\beta, \beta\alpha) = k$, *then* $0 \le k \le 2|\mathrm{supp}(\beta)|$.

Proof. If α and β commute then $k = 0$. If β does not have fixed points then $|\mathrm{supp}(\beta)| = $ n and $k < 2|\mathrm{supp}(\beta)|$. Now, let $x \in \mathrm{fix}(\beta)$. If $\beta\alpha(x) \ne \alpha\beta(x)$ then $\alpha(x) \in \mathrm{supp}(\beta)$ (Theorem 3.8). Thus, α does not commute with β on at most $|\mathrm{supp}(\beta)|$ fixed points of β and then $k \le 2|\mathrm{supp}(\beta)|$. $\qquad\square$

The following proposition is a consequence of Proposition 3.1, Theorem 5.1, Theorem 5.2 and Proposition 6.1.

Proposition 6.2. *Let* $\beta \in S_n$ *be any transposition. Then*

1. $c(0, \beta) = 2(n-2)!$, $n > 1$.

2. $c(3, \beta) = 4(n-2)(n-2)!$, $n > 1$.

3. $c(4, \beta) = (n-2)(n-3)(n-2)!$, $n > 2$.

4. $c(k, \beta) = 0$, *for* $5 \le k \le n$.

We have noted that formulas (1), (2) and (3) in previous proposition coincide with the number of permutations of $n > 1$ having exactly 2, 3 and 4 points, respectively, on the boundary of their bounding square [8] (A208529, A208528 and A098916 in [33], respectively).

Now we give a formula for $c(k, \beta)$ when β is any fixed-point free involution. Let $a(n)$ be the "number of derarenged matchings of $2n$ people with partners (of either sex) other than their spouse" (taken from the Comments for A053871 in [33]).

Theorem 6.3. *Let* $\beta \in S_{2m}$ *be a fixed-point free involution, $m \ge 2$. Then*

1. $c(k, \beta) = 0$, *for* k *and odd integer,*

2. $c(k, \beta) = 2^m m! \binom{m}{j} a(j)$, *for* $k = 2j$, $j = 0, 1, 2, \ldots$

Proof. From Proposition 3.12 we have that if α does not commute on one point in cycle β_i of β then α does not commute on the two points in β_i, then if k is odd we obtain the desired result. Now we will obtain all the permutations α that k-commutes with β and that do not commute on j 2-cycles, $\beta_1, \beta_2, \ldots, \beta_j$, of β. By Proposition 3.13 there exists exactly j 2-cycles, $\beta_1', \beta_2', \ldots, \beta_j'$ of β such that $\alpha(\bigcup_{i=1}^{j} \operatorname{set}(\beta_i)) = \bigcup_{i=1}^{j} \operatorname{set}(\beta_i')$. We construct $\alpha|_{\bigcup_{i=1}^{j} \operatorname{set}(\beta_i)}$ as follows: First put

$$
\alpha'|_{\bigcup_{i=1}^{j} \operatorname{set}(b_i)} = \begin{pmatrix} B_1 \\ B_{i_1'} \end{pmatrix} \begin{pmatrix} B_2 \\ B_{i_2'} \end{pmatrix} \cdots \begin{pmatrix} B_j \\ B_{i_j'} \end{pmatrix},
$$

where B_i is an improper block of the cycle β_i and B_i' is an improper block of β_i', for every i, and where $B_{i_1'} B_{i_2'} \ldots B_{i_j'}$ is any block permutation of the j improper blocks of $\beta_1', \ldots, \beta_k'$ (there are $j!$ such permutations). Until this step $\alpha'|_{\bigcup_{i=1}^{j} \operatorname{set}(b_i)}$ is a permutation that commutes with β on the cycles $\beta_1, \ldots, \beta_n$. Now we can see every block B_i' as a partner $B_i' = xy$, and we finish the construction of $\alpha|_{\bigcup_{i=1}^{j} \operatorname{set}(b_i)}$ by re-paired the elements in the blocks $B_{i_1'}, B_{i_2'}, \ldots, B_{i_j'}$ in such a way that no point is with its original partner, this can be made in $a(j)$ ways. As there are 2^j ways to select the first element in the blocks $B_1, \ldots, B_j$, we have that $r_0 = 2^j j! a(j)$. Finally, by Proposition 4.12 (with $\ell = 2$, $c_\ell = m$, $h_\ell = j$ and $|C_{S_n}(\beta)| = 2^m m!$) we obtain

$$
2^j j! a(j) \binom{m}{j}^2 \frac{(m-j)!}{2^j m!} 2^m m! = 2^m m! \binom{m}{j} a(j).
$$

$\square$

Theorem 6.4. *Let $\beta \in S_{2m}$ be a fixed-point free involution. Then*

$$
\sum_{m,j \geq 0} c(2j, \beta) \frac{z^m}{m!} \frac{u^j}{j!} = \left((1 - 2z) \sqrt{1 - 4 \frac{zu}{1 - 2z}} \exp\left(\frac{2zu}{1 - 2z} \right) \right)^{-1}.
$$

Proof. (Sketch) We use the well-known EGF for $a(n)$ (A053871 in [33])

$$
\sum_{n \geq 0} a(n) \frac{x^n}{n!} = \left(\exp(x) \sqrt{1 - 2x} \right)^{-1},
$$

and the result follows by using standard techniques of bivariate generating functions similarly as in the proof of Theorem 4.16. $\square$

7 Final comments

As we have seen in previous sections, the problem of computing in an exact way the number $c(k, \beta)$ can be a difficult task. This is because we have that the number of cases can be equal to the number of partitions $[k_1, \ldots, k_h]$ of k, with $k_i \geq 1$. Even more, once we have selected a partition of k, it can be difficult to compute in exact way all the permutations with the desired properties. For example, if we have that β has at least two cycles β_1 and β_2 of lengths l and m, respectively, and we look for all the permutations that k-commute with

β and that (k_1, β)-commutes with β_1 and that (k_2, β)-commutes with β_2 then $\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)}$ must look like

$$\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)} = \left(\begin{array}{ccc} A_1 & \ldots & A_{k_1} \\ X'_1 & \ldots & X'_{k_1} \end{array} \right) \left(\begin{array}{ccc} B_1 & \ldots & B_{k_2} \\ Y'_1 & \ldots & Y'_{k_2} \end{array} \right),$$

where we can have many possibilities for the selection of blocks $X'_1, \ldots, X'_{k_1}, Y'_1, \ldots, Y'_{k_2}$, that depends of the lengths of the cycles β_1, β_2. And after we have selected these blocks, we have the problem of the number of ways in which we can arranged it. However, it is possible that for some specific cycle type of permutations, the problem can be managed. We leave as an open problem to find another technique, or a refinement of the presented in this article, to compute $c(k, \beta)$ in exact way, or at least to obtain non trivial upper and lower bounds for this number.

8   Acknowledgements

References

[1] R. M. Anderson, "Almost" implies "near", *Trans. Amer. Math. Soc.,* **296** (1986), 229–237.

[2] M. Bóna, *Combinatorics of Permutations*, Chapman & Hall/CRC, Boca Raton, FL, 2004.

[3] M. Bóna and R. Flynn, The average number of block interchanges needed to sort a permutation and a recent result of Stanley, *Inform. Process. Lett.,* **109** (2009), 927–931.

[4] P. J. Cameron, Permutation codes, *European J. Combin.,* **31** (2010), 482–490.

[5] T. Ceccherini-Silberstein and M. Coornaert, *Cellular Automata and Groups*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2010.

[6] D. A. Christie, Sorting permutations by block interchanges, *Inform. Process. Lett.,* **60** (1996), 165–169.

[7] W. Chu, C. Colbourn, and P. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.,* **32** (2004), 51–64.

[8] E. Deutsch, Permutations and their bounding squares, *Math. Mag.,* **85**(1) (2012), p. 63.

[9] M. Deza and T. Huang, Metrics on permutations, a survey, *J. Comb. Inf. Sys. Sci.,* **23** (1998), 173–185.

[10] P. Diaconis, *Group Representations in Probability and Statistics*, Institute of Mathematical Statistics Lecture Notes–Monograph Series, 11, Institute of Mathematical Statistics, Hayward, CA, 1988.

[11] D. S. Dummit and R. M. Foote, *Abstract Algebra*, third ed., John Wiley & Sons, Inc., 2004.

[12] H. K. Farahat, The symmetric group as metric space, *J. London Math. Soc.,* **35** (1960), 215–220.

[13] P. Flajolet and R. Sedgewick, *Analytic Combinatorics*, Cambridge University Press, Cambridge, 2009.

[14] N. Filonov and I. Kachkovskiy, A Hilbert-Schmidt analog of Huaxin Lin's theorem, preprint, `http://arxiv.org/abs/1008.4002` (2010).

[15] N. Filonov and Y. Safarov, On the relation between an operator and its self-commutator, *J. Funct. Anal.,* **260** (2011), 2902–2932.

[16] P. Friis and M. Rørdam, Almost commuting self-adjoint matrices –a short proof of Huaxin Lin's theorem–, *J. Reine Angew. Math.,* **479** (1996), 121–131.

[17] L. Glebsky, Almost commuting matrices with respect to normalized Hilbert-Schmidt norm, preprint `http://arxiv.org/abs/1002.3082` (2010).

[18] L. Glebsky and L. M. Rivera, Almost solutions of equations in permutations, *Taiwanese J. Math.,* **13**, (2009), 493–500.

[19] L. Glebsky and L. M. Rivera, On low rank perturbations of complex matrices and some discrete metric spaces, *Electron. J. Linear Algebra,* **18** (2009), 302–316.

[20] D. Gorenstein, R. Sandler, and W. H. Mills, On almost-commuting permutations, *Pacific J. of Math.,* **12** (1962), 913–923.

[21] M. Gromov, Endomorphisms of symbolic algebraic varieties, *J. Eur. Math. Soc.,* **1** (1999), 109–197.

[22] M. B. Hastings, Making almost commuting matrices commute, *Comm. Math. Phys.,* **291** (2009), 321–345.

[23] D. Hadwin, Free entropy and approximate equivalence in von Neumann algebras, *Operator algebras and operator theory*, (Shanghai 1997) 111–131, *Contemp. Math.,* **228** Amer. Math. Soc. Providence, RI (1998).

[24] D. Hadwin and W. Li, A note on approximate liftings, *Oper. Matrices,* **3** (2009), 125–143.

[25] R. W. Hamming, Error detecting and error correcting codes, *Bell System Tech. J.,* **26** (2), (1950) 147–160.

[26] H. Lin, Almost commuting self-adjoint matrices and applications, in *Operator algebras and their applications* (Waterloo, ON, 1994/1995), *Fields Inst. Commun.,* **13** Amer. Math. Soc. Providence, RI (1997), 193–233.

[27] T. J. Osborne, Almost commuting unitaries with spectral gap are near commuting unitaries, *Proc. Amer. Math. Soc.,* **137** (2009), 4043–4048.

[28] V. G. Pestov, Hyperlinear and sofic groups: a brief guide, *Bull. Symbolic Logic,* **14** (2008), 449–480.

[29] J. Quistorff, A survey on packing and covering problems in the Hamming permutation Space, *Electron. J. Combin.,* **13** (2006), A1.

[30] J. J. Rotman, *An Introduction to the Theory of Groups*, Springer-Verlag, fourth ed. 1995.

[31] T. Schiavinotto, T. Stützle, A review of metrics on permutations for search landscape analysis, *Comput. Oper. Res.,* **34** (2007), 3143–3153.

[32] J. Shallit, Hamming distance for conjugates, *Discrete Math.,* **309** (2009), 4197–4199.

[33] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

[34] M. Z. Spivey and L. L. Steil, The k-binomial transforms and the Hankel transform, *J. Integer Seq.,* **9**, Article 06.1.1 (2006).

[35] R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Cambridge University Press, 1997.

[36] D. Voiculescu, Asymptotically commuting finite rank unitary operators without commuting approximants, *Acta Sci. Math. (Szeged),* **45** (1983), 429–431.

[37] H. S. Wilf, *Generatingfunctionology*, second ed., Academic Press, San Diego, 1994.

UNIDAD ACADÉMICA MULTIDISCIPLINARIA ZONA MEDIA & INSTITUTO DE FÍSICA, UNIVERSIDAD AUTÓNOMA DE SAN LUIS POTOSÍ, MEXICO.
E-mail: rutilo.moreno@gmail.com.

FAKULTÄT FÜR MATHEMATIK, UNIVERSITÄT WIEN, AUSTRIA &
UAIE & UAM, UNIVERSIDAD AUTÓNOMA DE ZACATECAS*, MEXICO.
E-mail: luismanuel.rivera@gmail.com.
*current affiliation.