

RESEARCH

Open Access



Blocks in cycles and k -commuting permutations

Rutilo Moreno¹ and Luis Manuel Rivera^{2,3*}

*Correspondence:

luismanuel.rivera@gmail.com

² Fakultät Für Mathematik,

Universität Wien,

Oskar-Morgenstern-Platz 1,

1090 Wien, Austria

Full list of author information is available at the end of the article

Abstract

We introduce and study k -commuting permutations. One of our main results is a characterization of permutations that k -commute with a given permutation. Using this characterization, we obtain formulas for the number of permutations that k -commute with a permutation β , for some cycle types of β . Our enumerative results are related with integer sequences in “The On-line Encyclopedia of Integer Sequences”, and in some cases provide new interpretations for such sequences.

Keywords: Symmetric group, Hamming metric, Commutation relation, Enumeration

Mathematics Subject Classification: Primary 05A05; Secondary 05A15, 20B30

Background

The symmetric group as a metric space has been studied with different metrics and for different purposes (see, e.g., Deza and Huang 1998; Diaconis 1988; Farahat 1960), and the metric that seems to be more used is the Hamming metric. This metric was introduced by Hamming (1950) for the case of binary strings and in connection with digital communications. For the case of permutations, it was used by Farahat (1960), who studied the symmetries of the metric space (S_n, H) , where S_n denotes the symmetric group on the set $\{1, \dots, n\}$ and H the Hamming metric between permutations. Also, Gorenstein et al. (1962) studied a problem about permutations that almost commute, in the sense of normalized Hamming metric.

Other problems are showed in the survey of Quistorff (2006), about the packing and covering problem, and in the survey of Cameron (2010), about permutation codes. This last problem have turned out to be useful in applications to power line communications, as was showed in Chu et al. (2004).

In this paper, we introduce and study k -commuting permutations. It seems that this is the first time this issued is studied. Shallit (2009) worked in an slightly similar problem but with strings. One of our main results is a characterization of the permutations that k -commute with a given permutation β . This characterization is given in terms of blocks formed by strings of points in cycles in the decomposition of β as a product of disjoint cycles.

Our original motivation to study this type of questions was to develop tools to work with problems related with the stability of the commutator relator in permutations. Recently, Arzhantseva and Păunescu (2015) proved that the equation $xy = yx$ is stable

in permutations. The concept of stability of equations in permutations appears recently in Glebsky and Rivera (2009), in the context of sofic groups, that is a class of groups of growing interest that was defined by Gromov (1999) [details about sofic groups can be consulted in the monograph of Ceccherini-Silberstein and Coornaert (2010) or in the survey of Pestov (2008)].

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 (see, e.g., Friis and Rørdam 1996; Hastings 2009; Lin 1997; Voiculescu 1983; Filonov and Safarov 2011; Glebsky 2010).

In some cases, we need to know upper bounds for the number of permutations that almost commute with a given permutation, as in Păunescu (2016). With this in mind, we work in the problem of determine the number $c(k, \beta)$ of permutations that k -commute with β . In this paper, we present explicit formulas for $c(k, \beta)$, when β is any permutation 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 have worked with several specific types of permutations. Surprisingly, we have found some relations between $c(k, \beta)$ and the following integer sequences in the OEIS database of Sloane (2015): A208529, A208528 and A098916 when β is a transposition, A000757 when β is an n -cycle (this relationship allows us to obtain the binomial transform of sequence A000757), and A053871 when β is a fixed-point free involution.

The relationship between the number $c(k, \beta)$ with some integers sequences in the OEIS database have provided another motivation to studied this problem. Using the techniques developed in this paper, Rivera (2015) showed more such relationship, and also identities between integer sequences in the OEIS database.

We review our results. We present a 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. Also, we present a formula and a bivariate generating function for the number of permutations that k -commute with any n -cycle. We present explicit formulas for the number $c(k, \beta)$, when β is any permutation and $k \leq 4$. Finally, we present formulas for the cases when β is either a transposition or a fixed-point free involution. In all cases, we present relationship between our formulas and sequences in the OEIS database.

Definitions and notation

We first give some definitions and notation used throughout the work. The elements in the set $[n] := \{1, \dots, n\}$ are called *points*. We write $\pi = p_1 p_2 \dots p_n$ for the one-line notation of $\pi \in S_n$, 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 . 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* (Dummit and Foote 2004, Sec. 1.3, p. 29). We say that π has cycle π' or that π' is a cycle of π if π' is a cycle in the disjoint cycle factorization of π . Let $\pi' = (a_1 \dots a_m)$ be a cycle of π , we use $\text{set}(\pi')$ to denote the set $\{a_1, \dots, a_m\}$. We say that a is a point in cycle π' if $a \in \text{set}(\pi')$. The *cycle type* of a permutation β is a vector (c_1, \dots, c_n) such that β has exactly c_i cycles of length i in its cycle decomposition. The *Hamming metric* between permutations $\alpha, \beta \in S_n$, denoted $H(\alpha, \beta)$, is $|\{a \in [n] : \alpha(a) \neq \beta(a)\}|$ [see the

survey of Deza and Huang (1998) for more details about this metric]. It is well-known that this metric is bi-invariant, that not two permutations have Hamming metric equal to 1, and 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 .

Blocks in cycles

Our definition of blocks was motivated by the definitions presented in the work of Christie (1996) and in the work of Bóna and Flynn (2009). A *block* A in a cycle $\pi' = (a_1 a_2 \dots a_m)$ of $\pi \in S_n$ is a consecutive nonempty substring $a_i a_{i+1} \dots a_{i+l}$, of $a_i \dots a_{i-1}$ where $(a_i \dots a_{i-1})$ is one of the m equivalent expressions of π' (the sums are taken modulo m). The *length* $|A|$ of block $A = a_i \dots a_{i+l}$ is the number of elements in the string A , and the points a_i and a_{i+l} are the *first* and the *last* element 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 *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 of π , is defined as the usual concatenation of strings (AB is not necessarily a block in a cycle of π). If $(a_1 \dots a_m)$ is a cycle of π we write $(A_1 \dots A_k)$ to mean that $A_1 \dots A_k = a_i \dots a_{i-1}$, where $(a_i \dots a_{i-1}) = (a_1 \dots a_m)$. A *block partition* of cycle π' is a set $\{A_1, \dots, A_l\}$ of pairwise disjoint blocks in π' such that there exist a block product $A_{i_1} \dots A_{i_l}$ of these blocks such that $\pi' = (A_{i_1} \dots A_{i_l})$. Let $p = J_1 J_2 \dots J_k$ be a block product of k pairwise disjoint blocks, not necessarily from the same cycle of π , and let τ be a permutation in S_k . The *block permutation* $\phi_\tau(P)$ of P , induced by τ , is defined as the block product $J_{\tau(1)} J_{\tau(2)} \dots J_{\tau(k)}$.

Example 1 Let $\pi = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8\ 9) \in S_9$. Some blocks in cycles of π are $P_1 = 2\ 3\ 4\ 1$ and $P_2 = 1\ 2$, $B_1 = 5\ 6\ 7$, $B_2 = 8$, $B_3 = 9$. The set $\{B_1, B_2, B_3\}$ is a block partition of $(5\ 6\ 7\ 8\ 9)$. The product $B_1 B_2$ is a block in $(5\ 6\ 7\ 8\ 9)$. The product $P_2 B_2 = 128$ is not a block in any cycle of π . Let $\tau = (3\ 1\ 2) \in S_3$, then $\phi_\tau(B_1 B_2 B_3) = B_2 B_3 B_1 = 8\ 9\ 5\ 6\ 7$.

The restriction function of $\pi \in S_n$ to set $X \subseteq [n]$ is denoted by $\pi|_X$. Let $\alpha, \beta \in S_n$. Let $\beta' = (b_1 \dots b_m)$ be a cycle of β . It is well known (Dummit and Foote 2004, Prop. 10, p. 125) that $\alpha\beta'\alpha^{-1} = (\alpha(b_1) \dots \alpha(b_m))$. From this, we use the following matrix notation for $\alpha|_{\text{set}(\beta')}$

$$\alpha|_{\text{set}(\beta')} = \begin{pmatrix} b_1 & \dots & b_m \\ \alpha(b_1) & \dots & \alpha(b_m) \end{pmatrix}. \tag{1}$$

Notice that for a given cycle β' , there are m ways to write $\alpha|_{\text{set}(\beta')}$ in this matrix notation. If $\alpha|_{\text{set}(\beta')}$ is written as in (1), we write

$$\alpha|_{\text{set}(\beta'),k} = \begin{pmatrix} B_1 \dots B_k \\ J_1 \dots J_k \end{pmatrix},$$

to mean that $B_1 \dots B_k = b_1 \dots b_m$ and J_1, \dots, J_k are blocks in cycles of β , where $J_1 \dots J_k = \alpha(b_1) \dots \alpha(b_m)$ and $|J_i| = |B_i|$, for $1 \leq i \leq k$. This notation is called a *block notation* (with respect to β) of $\alpha|_{\text{set}(\beta')}$. This notation depends on the particular selection of one of the m equivalent cyclic expressions of β . Sometimes we omit k in $\alpha|_{\text{set}(\beta'),k}$, when k is clear.

Example 2 Let $\alpha, \beta \in S_6$, where $\alpha = (1\ 3\ 4)(2\ 5\ 6)$ and $\beta = (1\ 2\ 4\ 5)(3\ 6)$. If $\beta' = (1\ 2\ 4\ 5)$, then $\alpha(1\ 2\ 4\ 5)\alpha^{-1} = (3\ 5\ 1\ 6)$, and $\alpha|_{\text{set}(\beta')}$ can be written as

$$\alpha|_{\text{set}(\beta')} = \begin{pmatrix} 1 & 2 & 4 & 5 \\ 3 & 5 & 1 & 6 \end{pmatrix}.$$

Two ways of written $\alpha|_{\text{set}(\beta')}$ in block notation are

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

where the vertical lines denote the limits of the blocks.

Permutations that k -commute with a cycle

In this section, we show the relation between blocks in cycles of β and the permutations that k -commute with β .

Let β' be a cycle of β . Let α be a permutation. If $\alpha\beta'\alpha^{-1}$ is also a cycle of β , then we say that α *transforms* the cycle β' into the cycle $\alpha\beta'\alpha^{-1}$. Let $B = b_1 \dots b_l$ be a block in β' . We say that permutation α *commutes with β on the block B* if $\alpha\beta(b_i) = \beta\alpha(b_i)$, for every $i \in \{1, \dots, l\}$. We say that α *commutes* (resp. do not commute) with β on β' , if $\alpha\beta(b) = \beta\alpha(b)$, for every $b \in \text{set}(\beta')$ (resp. $\alpha\beta(b) \neq \beta\alpha(b)$, for some $b \in \text{set}(\beta')$).

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

Proposition 1 *Let $\alpha, \beta \in S_n$. Let ℓ, m be integers, with $1 \leq \ell < m$. Let $\beta' = (b_1 \dots b_m)$ be a cycle of β . If α commutes with β on the block $b_1 \dots b_\ell$, then $\alpha(b_1) \dots \alpha(b_\ell)\alpha(b_{\ell+1})$ 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 $i \in \{1, \dots, \ell + 1\}$. The proof is by induction on i . 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 , then $\alpha(b_{k+1}) = \alpha(\beta(b_k)) = \beta(\alpha(b_k))$, and by the inductive hypothesis, $\beta(\alpha(b_k)) = \beta(\beta^{k-1}(\alpha(b_1))) = \beta^k(\alpha(b_1))$ as desired. \square

The following result is an easy exercise.

Proposition 2 *Let β' be an m -cycle of β . Then α commutes with β on β' if and only if α transforms β' into an m -cycle of β .*

Let β' be a cycle of β . We say that $\alpha(r, \beta)$ -commutes with β' if there exists exactly r points in β' on which α and β do not commute.

We now present one of our main results.

Theorem 1 *Let β' be an m -cycle of β and k an integer such that $k \geq 1$. Then $\alpha(k, \beta)$ -commutes with β' if and only if $\alpha\beta'\alpha^{-1} = (P_1 \dots P_k)$, where the blocks P_1, \dots, 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, \dots, P_k are k pairwise disjoint blocks, from one or more cycles of β , such that the string $P_i P_{i+1 \bmod k}$ is not a block in any cycle of β , for every $i \in [k]$.

Proof (1) Suppose that $\alpha\beta'\alpha^{-1} = (P_1)$ where P_1 is a proper block in a cycle of β . Without loss of generality assume that $\beta' = (b_1 \dots b_m)$ and $P_1 = \alpha(b_1) \dots \alpha(b_m)$. As P_1 is a block in a cycle of β , then $\beta(\alpha(b_i)) = \alpha(b_{i+1})$, for $i \in \{1, \dots, m-1\}$, which implies that $\beta(\alpha(b_i)) = \alpha(\beta(b_i))$, for $i \in \{1, \dots, m-1\}$. Finally, as P_1 is an improper block in a cycle of β , then $\beta(\alpha(b_m)) \neq \alpha(b_1)$, which implies that $\beta(\alpha(b_m)) \neq \alpha(\beta(b_m))$. Therefore $\alpha(1, \beta)$ -commutes with β' .

Conversely, we can assume, without loss of generality, that α commutes with β on block $b_1 \dots b_{m-1}$ of $\beta' = (b_1 \dots b_{m-1} b_m)$ and that does not commute on b_m . By Proposition 1, $\alpha(b_1) \dots \alpha(b_{m-1})\alpha(b_m)$ is a block in a cycle of β and it is a proper block due to Proposition 2.

(2) Suppose that $\alpha\beta'\alpha^{-1} = (P_1 \dots P_k)$, where every $P_i = p_{i1} p_{i2} \dots p_{i\ell_i}$ is a block in a cycle of β and that for every $i \in [k]$, $P_i P_{i+1 \bmod k}$ is not a block in any cycle of β . Without loss of generality we can write the cycle β' as

$$\beta' = (b_{11} \dots b_{1\ell_1} b_{21} \dots b_{2\ell_2} \dots b_{k1} \dots b_{k\ell_k}),$$

with $\alpha(b_{ir}) = p_{ir}$, 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 $r \in \{1, \dots, \ell_i - 1\}$. Therefore, we have, for one side that $p_{i(r+1)} = \beta(p_{ir}) = \beta(\alpha(b_{ir}))$, and for the other side $p_{i(r+1)} = \alpha(b_{i(r+1)}) = \alpha(\beta(b_{ir}))$ which means that α and β commute on b_{ir} , for every $r \in \{1, \dots, \ell_i - 1\}$. We now prove that $\beta(\alpha(b_{i\ell_i})) \neq \alpha(\beta(b_{i\ell_i}))$. 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.

Conversely, if α does not commute with β on exactly k points in $\text{set}(\beta')$, then we can write β' as $(B_1 \dots B_k)$, where $B_i = b_{i1} b_{i2} \dots b_{i\ell_i}$ is a block in a cycle of β , for every $i \in \{1, \dots, k\}$, and in this block, α and β commute on b_{ij} , for $1 \leq j < \ell_i$, and does not commute on $b_{i\ell_i}$. By Proposition 1, we have that $P_i := \alpha(b_{i1})\alpha(b_{i2}) \dots \alpha(b_{i\ell_i})$ 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 a 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 does not commute with β on $b_{i\ell_i}$. □

Remark 1 The function $\alpha|_{\text{set}(\beta'), k}$, using the notation from above, can be written as

$$\alpha|_{\text{set}(\beta'), k} = \left(\begin{array}{c} B_1 \dots B_k \\ P_1 \dots P_k \end{array} \right),$$

with $\beta' = (B_1 \dots B_k)$, $\alpha\beta'\alpha^{-1} = (P_1 \dots P_k)$. Where, for every $i \in \{1, \dots, k\}$, $|B_i| = |P_i| = \ell_i$, $B_i = b_{i1} b_{i2} \dots b_{i\ell_i}$, $P_i = p_{i1} p_{i2} \dots p_{i\ell_i}$ i.e., $\alpha(b_{ir}) = p_{ir}$, with $1 \leq r \leq \ell_i$

and 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 1 we can characterize permutations that k -commute with β .

Corollary 1 *Let $\alpha, \beta \in S_n$. Then α k -commutes with β if and only if there exist h cycles of β , say β_1, \dots, β_h , such that α commutes with β on each cycle of β 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 $k_i \geq 1$, $k = k_1 + \dots + k_h$, 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 $P_r^{(i)}P_{r+1 \bmod k_i}^{(i)}$ is not a block in any cycle of β , for any $r \in [k_i]$.
- 3 $\{P_1^{(1)}, \dots, P_{k_1}^{(1)}, \dots, P_1^{(h)}, \dots, P_{k_h}^{(h)}\}$ is a set of pairwise disjoint blocks from one or more cycles of β .

Example 3 Let $\alpha, \beta \in S_7$, where $\beta = (1\ 2\ 4\ 5\ 3)(7\ 6)$ 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 written as

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

As a first application of Theorem 1, we obtain the following result, that is used in the proof of Theorem 8

Proposition 3 *Let β be a 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' of β , then α commutes with β on β' .*

Proof Suppose that α and β do not commute on the remaining point in β' . By part (1) of Theorem 1, $\alpha\beta'\alpha^{-1} = (P)$, 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 . □

Previous propositions is a generalization of Lemma 2(b) in Gorenstein et al. (1962). The following proposition will be useful in the proofs of some of our results.

Proposition 4 *Let α and β be two permutations that k -commute, $k > 0$. Suppose that α does not commute with β on the cycles β_1, \dots, β_r , of lengths l_1, \dots, l_r , respectively, and that commutes with β on the rest of cycles of β (if any). Then, there exists exactly r cycles of β , say $\beta'_1, \dots, \beta'_r$, of lengths l_1, \dots, l_r , respectively, such that $\alpha(\text{set}(\beta_1) \cup \dots \cup \text{set}(\beta_r)) = \text{set}(\beta'_1) \cup \dots \cup \text{set}(\beta'_r)$. Even more, suppose that α does not commute with β on exactly h_i i -cycles of β and that commutes with β on 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 $\beta_{r+1}, \dots, \beta_s$ the rest of cycles of β of lengths l_{r+1}, \dots, 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 with $r + 1 \leq t \leq s$ (by Proposition 2). Then, there are cycles of β , say $\beta'_{r+1}, \dots, \beta'_s$, of lengths l_{r+1}, \dots, l_s , respectively, such that $\alpha(\text{set}(\beta_{r+1}) \cup \dots \cup \text{set}(\beta_s)) = \text{set}(\beta'_{r+1}) \cup \dots \cup \text{set}(\beta'_s)$, and the result of the first part of the proposition follows because α is a bijection.

By a similar argument, we can show that if α does not commute with β on exactly h_i i -cycles of β and commutes with β on the rest of the i -cycles of β (if any), then there exists exactly h_i i -cycles of β , say $\beta'_1, \dots, \beta'_{h_i}$ such that $\beta'_t \neq \alpha\beta_j\alpha^{-1}$, for every $t \in \{1, \dots, h_i\}$ and every cycle β_j of β . The following claim completes the proof of the second part

Claim 1 *If all the points in an i -cycle β_1 of β are images under α of g.c.p., then there exists an i -cycle β_2 of β such that $\beta_1 = \alpha\beta_2\alpha^{-1}$.*

Proof First, we prove, by contradiction, that if all the points in the i -cycle β_1 are images under α of g.c.p. of α and β , then these g.c.p. belong to exactly one l -cycle, say $\beta_2 = (b_1 \dots b_l)$, of β , with $l \geq i$. Suppose that β_1 contains the images under α of g.c.p. in different cycles of β , then β_2 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 $\alpha(\beta(x)) \neq \alpha(y) = \beta(\alpha(x))$. It is clear that $l \geq i$. Now, we show that $l \leq i$. Suppose that $l > i$, then, and without lost of generality, we have that $\beta_2 = (\alpha(b_1) \dots \alpha(b_i))$, i.e., $\beta(\alpha(b_t)) = \alpha(b_{t+1 \bmod i})$, for every $t \in \{1, \dots, i\}$ (if $\beta(\alpha(b_t)) \neq \alpha(b_{t+1 \bmod i})$, for some t , then b_t will be a b.c.p. of α and β). But this implies that b_i is a b.c.p. because, for one side, $\beta(\alpha(b_i)) = \alpha(b_1)$, and for the other side, $\alpha(b_1) \neq \alpha(b_{i+1}) = \alpha(\beta(b_i))$ (as $l > i$, then $i + 1 \bmod l \neq 1$ and hence $b_1 \neq b_{i+1}$) which is a contradiction. Therefore $l \leq i$, and then $l = i$, i.e., $\beta_1 = \alpha\beta_2\alpha^{-1}$. \square

With this claim, every cycle in $\{\beta'_1, \dots, \beta'_{h_i}\}$ contains at least one point that is the image under α of one b.c.p. of α and β as desired. \square

We finish this subsection with the following result

Theorem 2 *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 Let β_1 be a cycle of β that has exactly one b.c.p of α and β . The proof is by induction on the length l of cycle β_1 . If β_1 is an 1-cycle, then, by Proposition 4, there exists an 1-cycle β_2 of β that fixed a point, say x , such that $x' = \alpha^{-1}(x)$ is a b.c.p. of α and β . From Proposition 2 it follows that x' is a point in a cycle β_3 of β of length greater than one. That is, β_3 is a cycle of the form $(x'B)$, with B a block of length $|B| \geq 1$. Therefore, $\alpha\beta_3\alpha^{-1} = (xB')$, and by Theorem 1, β_3 has at least two b.c.p. of α and β .

Now we consider the case $l > 1$. Let $\beta_1 = (d_1 \dots d_l)$ be a cycle of β with exactly one b.c.p. of α and β . Without lost of generality we can suppose that d_l is such a b.c.p. Assume as induction hypothesis 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 exists). Let \mathcal{C}_l denote the set of all l -cycles of β and $c_l = |\mathcal{C}_l|$. Let

$$\text{set}(C_l) = \bigcup_{\beta' \in C_l} \text{set}(\beta').$$

By Theorem 1, we have that $\alpha\beta_1\alpha^{-1} = (D)$, where $D = \alpha(d_1) \dots \alpha(d_l)$ is a proper block in an s -cycle of β , with $s > l$. As $\alpha(d_1)$ does not belong to an l -cycle of β , then $d_1 \notin \alpha^{-1}(\text{set}(C_l))$, but $d_1 \in \text{set}(C_l)$, so we have that

$$\alpha^{-1}(\text{set}(C_l)) \neq \text{set}(C_l).$$

Therefore, there exist at least one l -cycle, say $\beta_2 = (a_1 \dots a_l)$, of β (with the possibility that $\beta_2 = \beta_1$) with at least one point, says a_1 , which has its preimage under α in one m -cycle, say β_3 , with $m \neq l$. Let r be an integer between 1 and l such that $\alpha^{-1}(a_1) \dots \alpha^{-1}(a_r)$ is a block in cycle $\beta_3 = (b_1 \dots b_m)$, with $b_i = \alpha^{-1}(a_i)$, for $1 \leq i \leq r$, but $\alpha^{-1}(a_1) \dots \alpha^{-1}(a_r)\alpha^{-1}(a_{r+1 \bmod l})$ 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 1).

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

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

Let $\beta \in S_n$ be a fixed permutation and $k \geq 3$ 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_1 , of β , i.e., $m \geq k$ and all the b.c.p. of α and β are in β_1 . From Proposition 4 it follows that there exists exactly one m -cycle, say β_2 , of β such that $\text{set}(\beta_2) = \alpha(\text{set}(\beta_1))$. 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 $\Psi : S_n \rightarrow S_n$ 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 (Bóna 2004, p. 97).

Example 4 Let $\pi \in S_7$ be $(4\ 3\ 1)(6\ 5)(7\ 2)$ (π is written in its canonical cycle notation). Then $\Psi(\pi) = 4316572$.

Algorithm 1 Step 1 Choose two m -cycles, say β_1 and $\beta_2 = (p_1 \dots p_m)$, of β (with the possibility that $\beta_2 = \beta_1$).

Step 2 Choose a k -subset $\{p_{h_1}, \dots, p_{h_k}\}$ of $\text{set}(\beta_2)$. Without lost of generality suppose that $p_{h_k} = p_m$ and that $h_1 < \dots < h_k$. Now, to make a block partition $\{P_1, \dots, P_k\}$ of $P = p_1 \dots p_m$ as follows

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

Notice that p_{h_r} is the last point of $P_r, 1 \leq r \leq k$.
 Step 3 Choose a k -cycle permutation $\tau = (i_1 \dots i_k)$ of $[k] = \{1, \dots, k\}$ such that $\tau(a) \neq a + 1 \pmod k$, for every $a \in [k]$, and make the block permutation

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

Step 4 Construct $\alpha|_{\text{set}(\beta_1)} : \text{set}(\beta_1) \rightarrow \text{set}(\beta_2)$ as it follows:

$$\alpha|_{\text{set}(\beta_1), k} = \begin{pmatrix} B_1 B_2 \dots B_k \\ P_{i_1} P_{i_2} \dots P_{i_k} \end{pmatrix}.$$

where $\beta_1 = (B_1 \dots B_k)$ and $|B_r| = |P_{i_r}|$, for every $r \in \{1, \dots, k\}$.

Step 5 Construct $\alpha|_{[n] \setminus \text{set}(\beta_1)} : [n] \setminus \text{set}(\beta_1) \rightarrow [n] \setminus \text{set}(\beta_2)$ as any bijection that commutes with $\beta|_{[n] \setminus \text{set}(\beta_1)} : [n] \setminus \text{set}(\beta_1) \rightarrow [n] \setminus \text{set}(\beta_2)$.

Let c_m be the number of m cycles of β . For Step 5, α can be constructed in such a way that it transforms the $c_m - 1$ m -cycles of β different than β_1 (if any) into the $c_m - 1$ m -cycles of β different than β_2 (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 permutations with the desired properties.

Proposition 5 Any permutation α constructed with Algorithm 1 does not commute with β on all points in $\mathcal{A} := \alpha^{-1}(\{p_{h_1}, \dots, p_{h_k}\})$ and commutes with β on all points in $[n] \setminus \mathcal{A}$.

Proof Let β_1 and β_2 be the cycles of β selected in Step 1 of Algorithm 1, and $\{p_{h_1}, \dots, p_{h_k}\}$ the subset of $\text{set}(\beta_2)$ selected in Step 2. By the way in which α is constructed of in Step 3 and 4, $\alpha\beta_1\alpha^{-1} = (P_{i_1} P_{i_2} \dots P_{i_k})$, where $P_{i_r} P_{i_{r+1 \pmod k}}$ is not a block in any cycle of β (by Step 3, $i_{r+1 \pmod k} - i_r \pmod k \neq 1, 1 \leq r \leq k$). From Theorem 1, we have that α does not commute with β on exactly k points in $\text{set}(\beta_1)$. Even more, in the proof of Theorem 1 was showed that α and β do not commute on $\alpha^{-1}(p_{h_r})$, for $r \in \{1, \dots, k\}$ (see Remark 1). Finally, by the construction of α in Step 5, α and β commute on all points in $[n] \setminus \text{set}(\beta_1)$. □

Proposition 6 Let $k \geq 3$. Let α be any permutation that k -commutes with β and such that all the b.c.p. of α and β are in exactly one m -cycle of β . Then α can be obtained with Algorithm 1.

Proof Let β_1 be the m cycle of β that has all the b.c.p. of α and β . From Proposition 4 it follows that there exists exactly one m -cycle, β_2 , of β such that $\alpha(\text{set}(\beta_1)) = \text{set}(\beta_2)$. By Theorem 1, we have that $\alpha\beta_1\alpha^{-1} = (P_1 \dots P_k)$, where P_1, \dots, P_k are k pairwise disjoint blocks in β_2 and $P_r P_{r+1 \pmod k}$ is not a block in any cycle of β , for every $r \in \{1, \dots, k\}$. As $\alpha(\text{set}(\beta_1)) = \text{set}(\beta_2)$, we have that $P_1 \dots P_k$ is a block permutation of $B' = P_{i_1} \dots P_{i_k}$, where $\beta_2 = (B')$. Now, rename the blocks P_{i_s} as B'_s to obtain $B' = B'_1 \dots B'_k$. In this way, $\alpha\beta_1\alpha^{-1} = (B'_1 \dots B'_k)$, with $l_{r+1 \pmod k} - l_r \pmod k \neq 1$, for every $r \in \{1, \dots, k\}$. Indeed, if $l_{r+1 \pmod k} - l_r \pmod k = 1$ for some $r \in \{1, \dots, k\}$, then $B'_{l_r} B'_{l_{r+1 \pmod k}}$ will be a block in β_2 , and hence the number of b.c.p. of α and β will be less than k , which is a contradiction.

As $\alpha\beta_1\alpha^{-1} = (B'_{l_1} \dots B'_{l_k}) = (B'_{l_2} \dots B'_{l_1}) = \dots = (B'_{l_k} \dots B'_{l_{k-1}})$, we can assume without loss of generality that $l_1 = k$ (from these k expressions, choose the one that begins with block B'_k). Then $\alpha|_{\text{set}(\beta_1)}$ can be written as

$$\alpha|_{\text{set}(\beta_1),k} = \begin{pmatrix} B_1 \dots B_k \\ B'_1 \dots B'_k \end{pmatrix},$$

where $\beta_1 = (B_1 \dots B_k)$, and $|B_i| = |B'_i|$, with $1 \leq i \leq k$.

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

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

In this section we present some results about the number $c(k, \beta)$ of permutations that k -commute with β . Let $C_{S_n}(\beta)$ denote the centralizer of β . Let $C(k, \beta)$ be the set $\{\alpha \in S_n : H(\alpha\beta, \beta\alpha) = k\}$, then $c(k, \beta) = |C(k, \beta)|$.

Proposition 7 *Let $\beta \in S_n$ be a permutation of cycle type (c_1, \dots, 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 $c(1, \beta) = 0$. Finally, 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 the even permutation $\alpha\beta\alpha^{-1}\beta^{-1}$ should be a transposition which is a contradiction. □

Now we show that for any nonnegative integer k and any $\beta \in S_m$, the number $c(k, \beta)$ is invariant under conjugation.

Proposition 8 *If $\beta \in S_m$, then $c(k, \tau\beta\tau^{-1}) = c(k, \beta)$, for any $\tau \in S_m$.*

Sketch of the proof For $\tau \in S_m$ 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. Therefore, $|C(k, \beta)| = |\tau C(k, \beta)\tau^{-1}| = |C(k, \tau\beta\tau^{-1})|$. □

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

Proposition 9 *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 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 $\rho \in C(k, \beta)$. The other inclusion is clear. □

On the number $c([k], \beta)$

Let $c([k], \beta)$ denotes the number of permutations α that k -commutes with β which satisfy the extra condition that all the b.c.p. of α and β are in exactly one cycle of β .

Let $f(k)$ be the number of cyclic permutations (k -cycles) of $\{1, \dots, k\}$ with no $i \mapsto i + 1 \pmod k$ (Stanley 1997, exercise 8, p. 88). Sequence $\{f(k)\}$ is labeled as A000757 in the OEIS database.

Theorem 3 *Let $\beta \in S_n$ be a permutation of cycle type (c_1, \dots, c_n) . Let k be an integer, with $3 \leq k \leq n$. Then*

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

Proof As all the b.c.p. of α and β are in one ℓ -cycle, say $\beta_1 = (b_1 \dots b_\ell)$, of β , with $\ell \geq k$, then the images under α of the b.c.p are in exactly one ℓ -cycle, say $\beta_2 = (b'_1 \dots b'_\ell)$, of β (by Proposition 4). There are $\ell \binom{\ell}{k} f(k)$ ways to construct a bijection $\alpha|_{\text{set}(\beta_1)} : \text{set}(\beta_1) \rightarrow \text{set}(\beta_2)$ 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 $B_1 \dots B_k$ in Step 4. Now, let c_ℓ denotes the number of ℓ -cycles in the cycle decomposition of β . There are c_ℓ^2 ways to select the ℓ -cycles β_1 and β_2 , there are $(c_\ell - 1)! \ell^{c_\ell - 1}$ ways to make that α transforms the $c_\ell - 1$ cycles of length ℓ of β different than β_1 into the $c_\ell - 1$ cycles of β of length ℓ different than β_2 . Now for every $t \neq \ell$ there are $t^{c_t} c_t!$ ways to make that α transforms all the c_t t -cycles of β into c_t t -cycles of β and hence there are $\frac{1}{\ell^{c_\ell} c_\ell!} |C_{S_n}(\beta)|$ ways to make that α transforms all the cycles of length $t \neq \ell$ into cycles of length $t \neq \ell$. Finally, we sum over all possible lengths $\ell \geq k$ of cycles of β . Therefore

$$\begin{aligned} c([k], \beta) &= \sum_{\ell \geq k}^n \ell \binom{\ell}{k} f(k) c_\ell^2 (c_\ell - 1)! \ell^{c_\ell - 1} \frac{1}{\ell^{c_\ell} c_\ell!} |C_{S_n}(\beta)| \\ &= |C_{S_n}(\beta)| \sum_{\ell \geq k}^n c_\ell \binom{\ell}{k} f(k). \end{aligned}$$

□

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

Corollary 2 *Let n be a positive integer and k and integer with $0 \leq k \leq n$. Then*

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

The number $T(k, n)$ is now sequence A233440 in the OEIS database. 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 Spivey and Steil (2006), b_n is defined as $\sum_{k=0}^n \binom{n}{k} f(k)$. By Corollary 2, $b_n = \sum_{k=0}^n T(k, n)/n$. As $\sum_{k=0}^n T(k, n) = n!$, then $b_n = (n - 1)!$.

We have the following limit property for $T(k, n)$.

Proposition 10 *Let n be a positive integer and m be a fixed nonnegative integer with $m \neq n$. Then*

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

Proof By direct calculations we have that

$$\frac{T(n - m, n)}{n!} = \frac{f(n - m)}{m!(n - m - 1)!} + \frac{mf(n - m)}{m!(n - m)(n - m - 1)!}.$$

The result follows by using that $\lim_{k \rightarrow \infty} f(k)/(k - 1)! = e^{-1}$ (Stanley 1997, exercise 8-e, p. 88). □

Theorem 4 *Let n, k be positive integers with $k \leq n$. Then*

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

Proof Let $g^{(k)}(z) = \sum_n g_{n,k} \frac{z^n}{n!}$ 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 3. 1, in (Flajolet and Sedgewick 2009, p. 155), and by using the fact that function $f(k)$ is independent of n we have

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

Now, by using Rule (2') in (Wilf 1994, p. 41) we obtain

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

Now

$$\begin{aligned}
 P(z, u) &:= \sum_{k,n} n \binom{n}{k} f(k) \frac{z^n}{n!} u^k \\
 &= \sum_k \left(\sum_n n \binom{n}{k} f(k) \frac{z^n}{n!} \right) u^k \\
 &= \sum_k f(k) z \left(\frac{e^z z^k}{k!} + \frac{e^z z^k k}{zk!} \right) u^k \\
 &= \sum_k f(k) z \frac{e^z z^k}{k!} u^k + \sum_k f(k) z \frac{e^z z^k k}{zk!} u^k \\
 &= ze^z \sum_k f(k) \frac{z^k u^k}{k!} + e^z \sum_k kf(k) \frac{z^k u^k}{k!}.
 \end{aligned}$$

It is known that $\sum_{k \geq 0} f(k) \frac{x^k}{k!} = e^{-x}(1 - \log(1 - x))$ (Stanley 1997, 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 Wilf (1994) to the second term of $P(z, u)$ to obtain

$$e^z \sum_k kf(k) \frac{z^k u^k}{k!} = e^z (zu)e^{-zu} \left(\frac{1}{1 - zu} - (1 - \log(1 - zu)) \right),$$

and the result follows after some algebraic manipulations. □

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, \dots, c_n) and $k = 3, 4$. We use the following notation: Let $[k_1, \dots, k_h]$ denote an integer partition of k , with $k_i \geq 1$. We define a set $C([k_1, \dots, k_h], \beta)$ as follows: $\alpha \in C([k_1, \dots, k_h], \beta)$ if and only if α k -commutes with β , and there are exactly h cycles, says β_1, \dots, β_h in β , such that α (k_1, β) -commutes with β_1 , (k_2, β) -commutes with β_2 , ..., (k_h, β) -commutes with β_h . Let $c([k_1, \dots, k_h], \beta)$ be the cardinality of $C([k_1, \dots, k_h], \beta)$. By Theorem 2, we have that $c([1, \dots, 1], \beta) = 0$, where $[1, \dots, 1]$ denotes the partition of k that consists of k ones.

Theorem 5 *Let β be any n -permutation of cycle type (c_1, \dots, c_n) . Then*

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

Proof The number $c(3, \beta)$ is equal to $c([1, 1, 1], \beta) + c([2, 1], \beta) + c([3], \beta)$. The case $c([3], \beta)$ follows from Theorem 3 and $c([1, 1, 1], \beta) = 0$. 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 4, there exist exactly one ℓ -cycle β'_1 of β and exactly one m -cycle β'_2 of β such that $\alpha(\text{set}(\beta_1) \cup \text{set}(\beta_2)) = \text{set}(\beta'_1) \cup \text{set}(\beta'_2)$. From Theorem 1 we have that

$$\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)} = \begin{pmatrix} A_1 \\ X_1 \end{pmatrix} \begin{pmatrix} B_1 & B_2 \\ X_2 & X_3 \end{pmatrix}; \tag{2}$$

where

- (a) $\beta_1 = (A_1)$, $\beta_2 = (B_1 B_2)$, X_2, X_3 are blocks distributed in β'_1 and β'_2 , and X_1 is a block in a cycle of length greater than A_1 , i.e., X_1 is a block in β'_2 ;
- (b) the strings $X_2 X_3$ and $X_3 X_2$ are not blocks in any cycle of β ,
- (c) The set of all points in the blocks X_1, X_2, X_3 is equal to $\text{set}(\beta'_1) \cup \text{set}(\beta'_2)$.

From condition (a) to condition (c) we have that X_2 and X_3 belongs to different cycles. Without loss of generality we can assume that $\beta'_1 = (X_2)$ and that $\beta'_2 = (X_1 X_3)$. Now we count the number of ways to construct $\alpha|_{\text{set}(\beta_1) \cup \text{set}(\beta_2)}$. 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 $B_1 B_2$. 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).

There are $c_\ell^2 c_m^2$ ways to select the ℓ -cycles and m -cycles β_1, β'_1 and β_2, β'_2 . There are $(c_\ell - 1)! \ell^{c_\ell - 1} (c_m - 1)! m^{c_m - 1}$ ways to make that α transforms the $c_\ell - 1$ cycles of length ℓ of β different than β_1 into the $c_\ell - 1$ cycles of length ℓ of β different than β'_1 and the $c_m - 1$ cycles of length m of β different than β_2 into the $c_m - 1$ cycles of length m of β different than β'_2 . Now, for every $t \notin \{m, \ell\}$ there are $t^{c_t} c_t!$ ways to make that α transforms all the c_t t -cycles of β into c_t t -cycles of β and hence there are $\frac{1}{m^{c_m} c_m! \ell^{c_\ell} c_\ell!} |C_{S_n}(\beta)|$ ways to make that α transforms all the cycles of length different than ℓ and m into cycles of length different than ℓ and m . After summing over all possible values of ℓ and m we have that $c([2, 1], \beta)$ is equal to

$$\begin{aligned} & \sum_{1 \leq \ell < m \leq n} (\ell m)^2 c_\ell^2 c_m^2 (c_\ell - 1)! \ell^{c_\ell - 1} (c_m - 1)! m^{c_m - 1} \frac{1}{m^{c_m} c_m! \ell^{c_\ell} c_\ell!} |C_{S_n}(\beta)| \\ & = \sum_{1 \leq \ell < m \leq n} \ell m c_\ell c_m |C_{S_n}(\beta)|. \end{aligned}$$

□

In a similar way, but with many more cases to consider, we have obtained a formula for $c(4, \beta)$, for any β . In order to avoid an unnecessarily increase in the length of this paper, we have omitted the proof but the interested reader can consult it in the preprint version of this paper (Moreno and Rivera 2014).

Theorem 6 *Let β be any permutation of cycle type (c_1, \dots, 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

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

Transpositions and fixed-point free involutions

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

Proposition 11 *Let $\alpha, \beta \in S_n$ and let $H(\alpha\beta, \beta\alpha) = k$, then $0 \leq k \leq 2|\text{supp}(\beta)|$.*

Proof If α commutes with β , then $k = 0$. If β does not have fixed points then $|\text{supp}(\beta)| = n$ and $k < 2|\text{supp}(\beta)|$. Now, let $x \in \text{fix}(\beta)$. If $\beta\alpha(x) \neq \alpha\beta(x)$ then $\alpha(x) \in \text{supp}(\beta)$ (Theorem 1). Thus, α does not commute with β on at most $|\text{supp}(\beta)|$ fixed points of β and then $k \leq 2|\text{supp}(\beta)|$. □

The following theorem is a consequence of Proposition 7, Theorem 5, Theorem 6 and Proposition 11.

Theorem 7 *Let $\beta \in S_n$ be a 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 $5 \leq k \leq n$.

Formulas (1), (2) and (3) in previous proposition coincide with the number of permutations of n symbols, with $n > 1$, having exactly 2, 3 and 4 points, respectively, on the boundary of their bounding square (that are labeled as sequences A208529, A208528 and A098916 in the OEIS database, respectively). Details about this definitions can be consulted in Deutsch (2012). Therefore, our result provides another interpretation for these sequences in the OEIS database.

Now we give a formula for $c(k, \beta)$ when β is any fixed-point free involution. Let $a(n)$ be the “number of deranged matchings of $2n$ people with partners (of either sex) other than their spouse” (sequence A053871).

Theorem 8 *Let $\beta \in S_{2m}$ be a fixed-point free involution, $m \geq 2$. Then*

- 1 $c(k, \beta) = 0$, for k and odd integer,
- 2 $c(k, \beta) = 2^m m! \binom{m}{j} a(j)$, for $k = 2j, j = 0, 1, 2, \dots$

Proof By hypothesis, the cycle decomposition of β consists of exactly m transpositions. From Proposition 3 we have that if α does not commute on one point in a transposition β_1 of β then α does not commute on the two points in β_1 , therefore any permutation does not commute with β in a even number of points, which implies that $c(k, \beta) = 0$ for k odd. Now, if $k = 2j$, we obtain all the permutations α that k -commutes with β and that do not commute with β on exactly j transpositions, of β . There are $\binom{m}{j}$ ways to select a set, say $\{\beta_1, \dots, \beta_j\}$, of j transpositions of β . Let $X = \bigcup_{i=1}^j \text{set}(\beta_i)$. By Proposition 4, there exists exactly j transpositions, $\beta'_1, \dots, \beta'_j$ of β such that $\alpha(X) = X'$, where $X' = \bigcup_{i=1}^j \text{set}(\beta'_i)$. Given a selection of cycles $\{\beta_1, \dots, \beta_j\}$, there are $\binom{m}{j}$ ways to select a set, $\{\beta'_1, \dots, \beta'_j\}$, of j transpositions of β that will satisfy $\alpha(X) = X'$. We construct $\alpha|_X$ as follows: First, we define the auxiliary bijection from X onto X' as

$$\alpha'|_X = \begin{pmatrix} B_1 \\ B'_1 \end{pmatrix} \cdots \begin{pmatrix} B_j \\ B'_j \end{pmatrix}; \tag{3}$$

where B_l (resp. B'_l) is an improper block of the cycle β_l (resp. β'_l), for every $l \in \{1, \dots, j\}$, and $\{B'_1, \dots, B'_j\} = \{B_1, \dots, B_j\}$. There are 2^j ways to select the first element in each of the blocks B_1, \dots, B_j . There are $j!$ ways to arrange the blocks B'_1, \dots, B'_j in the second row of (3). Until this step $\alpha'|_X$ is a bijection from X onto X' that commutes with β on the cycles β_1, \dots, β_j . We can think that every block B'_i is a partner $B'_i = xy$. We construct $\alpha|_X$ from $\alpha'|_X$ by re-pairing the elements in the blocks B'_1, \dots, B'_j in such a way that every point is paired with a point other than its original partner, this can be made in $a(j)$ ways. Finally, there are $(m - j)! 2^{m-j}$ ways to construct $\alpha|_{[2m] \setminus X}$ in such away that it commutes with β on the $m - j$ transpositions of β not in $\{\beta_1, \dots, \beta_j\}$. Therefore

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

Theorem 9 *Let $\beta \in S_{2m}$ be a fixed-point free involution. Then*

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

Sketch We use the well-known EGF for $a(n)$ [see the formula section of sequence A053871 in Sloane (2015)]

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

and the result follows by using standard techniques of bivariate generating functions similarly as in the proof of Theorem 4. \square

Conclusions

In this paper we give some techniques to work with k -commuting permutations. We present some formulas for the number of permutations that k -commute with β , when β is any permutation and $k \leq 4$. Also we obtain formulas for $c(k, \beta)$ when β is either a transposition, or an n -cycle, or a fixed-point free involution, for any k . These results could be useful when we work in problems related with almost commuting permutations. Even more, these enumerative results could be useful to find relations between integer sequences in the OEIS database, as Rivera (2015) showed.

The problem of computing in an exact way the number $c(k, \beta)$ could be a difficult task. 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.

Authors' contributions

This work was carried out by the two authors, in collaboration. LMR designed research; RM and LMR performed research; and RM and LMR wrote the paper. Both authors read and approved the final manuscript.

Author details

¹ Instituto de Física, Universidad Autónoma de San Luis Potosí, San Luis Potosí, Mexico. ² Fakultät Für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, 1090 Wien, Austria. ³ Present Address: UAIE and UAM, Universidad Autónoma de Zacatecas, Calzada Solidaridad entronque Paseo a la Bufa, 98000 Zacatecas, Mexico.

Acknowledgements

The authors would like to thank L. Glebsky for very useful suggestions and comments. The authors also would like to thank Jesús Leañós for his careful reading of the paper and his very valuable suggestions. Also, the authors would like to thank the anonymous reviewer for his/her suggestions. The second author was supported by the European Research Council (ERC) Grant of Goulmara Arzhantseva, Grant Agreement No. 259527 and by PROMEP (SEP, México) Grant UAZ-PTC-103 (No. 103.5/09/4144 and No. 103.5/11/3795).

Competing interests

The authors declare that they have no competing interests.

Received: 27 November 2015 Accepted: 2 November 2016

Published online: 10 November 2016

References

- Arzhantseva G, Păunescu L (2015) Almost commuting permutations are near commuting permutations. *J Funct Anal* 269(3):745–757
- Bóna M (2004) Combinatorics of permutations. *Discrete mathematics and its applications* (Boca Raton). Chapman & Hall/CRC, Boca Raton, Florida, p 383. With a foreword by Richard Stanley
- Bóna M, Flynn R (2009) The average number of block interchanges needed to sort a permutation and a recent result of Stanley. *Inf Process Lett* 109(16):927–931
- Cameron PJ (2010) Permutation codes. *Eur J Comb* 31(2):482–490
- Ceccherini-Silberstein T, Coornaert M (2010) Cellular automata and groups. *Springer monographs in mathematics*. Springer, Berlin, p 439
- Christie DA (1996) Sorting permutations by block-interchanges. *Inf Process Lett* 60(4):165–169
- Chu W, Colbourn CJ, Dukes P (2004) Constructions for permutation codes in powerline communications. *Des Codes Cryptogr* 32(1–3):51–64
- Deutsch E (2012) Permutations and their bounding squares. *Math Mag* 85(1):63
- Deza M, Huang T (1998) Metrics on permutations, a survey. *J Comb Inf Syst Sci* 23(1–4):173–185. J. N. Srivastava: felicitation volume
- Diaconis P (1988) Group representations in probability and statistics. *Institute of mathematical statistics lecture notes—monograph series*, 11. Institute of Mathematical Statistics, Hayward, CA, p 198
- Dummit DS, Foote RM (2004) *Abstract algebra*, 3rd edn. Wiley, Hoboken, NJ
- Farahat HK (1960) The symmetric group as metric space. *J Lond Math Soc* 35:215–220
- Filonov N, Safarov Y (2011) On the relation between an operator and its self-commutator. *J Funct Anal* 260(10):2902–2932

- Flajolet P, Sedgewick R (2009) *Analytic combinatorics*. Cambridge University Press, Cambridge
- Friis P, Rørdam M (1996) Almost commuting self-adjoint matrices—a short proof of huaxin lin’s theorem. *J Reine Angew Math* 479:121–131
- Glebsky L (2010) Almost commuting matrices with respect to normalized Hilbert–Schmidt norm. [arXiv:1002.3082](https://arxiv.org/abs/1002.3082)
- Glebsky L, Rivera LM (2009) Almost solutions of equations in permutations. *Taiwan J Math* 13(2A):493–500
- Gorenstein D, Sandler R, Mills WH (1962) On almost-commuting permutations. *Pac J Math* 12:913–923
- Gromov M (1999) Endomorphisms of symbolic algebraic varieties. *J Eur Math Soc (JEMS)* 1(2):109–197
- Hamming RW (1950) Error detecting and error correcting codes. *Bell Syst Tech J* 29:147–160
- Hastings MB (2009) Making almost commuting matrices commute. *Commun Math Phys* 291(2):321–345
- Lin H (1997) Almost commuting selfadjoint matrices and applications. In: *Operator algebras and their applications* (Waterloo, ON, 1994/1995). *Fields Institute Communications*, vol 13. American Mathematical Society, Providence, RI, pp 193–233
- Moreno R, Rivera LM (2014) Blocks in cycles and k -commuting permutations. [arXiv:1306.5708](https://arxiv.org/abs/1306.5708), 1–25
- Păunescu L (2016) Convex structures revisited. *Ergod Theory Dyn Syst* 36(5):1596–1615
- Pestov VG (2008) Hyperlinear and sofic groups: a brief guide. *Bull Symb Logic* 14(4):449–480
- Quistorff J (2006) A survey on packing and covering problems in the hamming permutation space. *Electron J Comb* 13(1):1–13
- Rivera LM (2015) Integer sequences and k -commuting permutations. *Integers* 15(A46):1–22
- Shallit J (2009) Hamming distance for conjugates. *Discret Math* 309(12):4197–4199
- Sloane NJA (2015) The on-line encyclopedia of integer sequences
- Spivey MZ, Steil LL (2006) The k -binomial transforms and the Hankel transform. *J Integer Seq* 9(1):06–1119
- Stanley RP (1997) *enumerative combinatorics*. Vol. 1. *Cambridge studies in advanced mathematics*, vol 49. Cambridge University Press, Cambridge, p 325. With a foreword by Gian-Carlo Rota, Corrected reprint of the 1986 original
- Voiculescu D (1983) Asymptotically commuting finite rank unitary operators without commuting approximants. *Acta Sci Math (Szeged)* 45(1–4):429–431
- Wilf HS (1994) *Generatingfunctionology*, 2nd edn. Academic Press Inc, Boston, MA, p 228

Submit your manuscript to a SpringerOpen[®] journal and benefit from:

- Convenient online submission
- Rigorous peer review
- Immediate publication on acceptance
- Open access: articles freely available online
- High visibility within the field
- Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com
