Journal of Integer Sequences, Vol. 20 (2017),
Article 17.10.7

Hultman Numbers and Generalized Commuting Probability in Finite Groups

Yonah Cherniavsky
Department of Mathematics
Ariel University
Israel
yonah@ariel.ac.il

Vadim E. Levit
Department of Computer Sciences
Ariel University
Israel
levitv@ariel.ac.il

Avraham Goldstein
Borough of Manhattan Community College
The City University of New York
USA
avraham.goldstein.nyc@gmail.com

Robert Shwartz
Department of Mathematics
Ariel University
Israel
robertsh@ariel.ac.il

Abstract

Let G be a finite group. We investigate the distribution of the probabilities of the permutation equality

$$a_1 a_2 \cdots a_{n-1} a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n}$$

as π varies over all the permutations in S_n. The probability

$$\Pr_\pi(G) = \Pr(a_1 a_2 \cdots a_{n-1} a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n})$$

is identical to $\Pr_1^\omega(G)$, with

$$\omega = a_1 a_2 \cdots a_{n-1} a_n a_{\pi_n}^{-1} a_{\pi_{n-1}}^{-1} \cdots a_{\pi_2}^{-1} a_{\pi_1}^{-1},$$

which was defined and studied by Das and Nath. The notion of commutativity degree, or the probability of a permutation equality $a_1 a_2 = a_2 a_1$, for which $n = 2$ and $\pi = \langle 2 \ \ 1 \rangle$, was introduced and assessed by Erdős and Turan in 1968 and by Gustafson in 1973. Gustafson established a relation between the probability of $a_1, a_2 \in G$ commuting and the number of conjugacy classes in G. In this work we define several other parameters, which depend only on a certain interplay between the conjugacy classes of

G, and compute probabilities of permutation equalities in terms of these parameters. It turns out that for a permutation π, the probability of its permutation equality depends only on the number $c(\mathrm{Gr}(\pi))$ of alternating cycles in the cycle graph $\mathrm{Gr}(\pi)$ of π. The cycle graph of a permutation was introduced by Bafna and Pevzner, and the number of alternating cycles in it was introduced by Hultman. Hultman numbers are the numbers of different permutations with the same number of alternating cycles in their cycle graphs. We show that the spectrum of probabilities of permutation equalities in a generic finite group, as π varies over all the permutations in S_n, corresponds to partitioning $n!$ as the sum of the corresponding Hultman numbers.

1 Introduction

Study of the (*commuting probability*), i.e., the probability that two random elements in a finite group G commute, is very natural. In 1968 Erdős and Turan [14] proved that

$$\Pr(a_1a_2 = a_2a_1) > \frac{\log(\log|G|)}{|G|}.$$

In the early 1970s, Dixon observed that the commuting probability is $\leq \frac{1}{12}$ for every finite non-Abelian simple group. (This inequality was submitted as an open problem in the Canadian Mathematical Bulletin **13** (1970), with a solution appearing in 1973.) In 1973, Gustafson [16] proved that the commuting probability is equal to $\frac{k(G)}{|G|}$, where $k(G)$ is the number of conjugacy classes in G. Based on that result, Gustafson further obtained the upper bound of the commuting probability in a finite non-Abelian group to be $\frac{5}{8}$. Commuting probability actually attains the upper bound of $\frac{5}{8}$ in many finite groups, including D_8 and Q_8. A significant amount of work has been done in assessing the commuting probability for various special cases of finite groups. For example, Lescot [20] studied the case of dihedral groups. Clifton, Guichard, and Keef [7] studied the case of direct product of dihedral groups. Erovenko and Surg [15] studied the case of wreath products of two Abelian groups. Guralnick and Robinson [17] studied the case of non-solvable groups. Additional information on development of the subject and its applications is found in Dixon [11], Jezernik and Moravec [19], and Lescot, Nguyen, and Yang [21].

Much research concerning probabilistic aspects of finite groups has been done since the introduction of commuting probability. Many of these studies can be regarded as variations of the commuting probability problem. For instance, Erdős and Straus [13] computed the number of ordered k-tuples of elements of a group G that have pairwise commuting elements. Another example is due to Pournakia and Sobhani [24], who determined the probability of the commutator of two random group elements of G being equal to a given element of G. In another example Blackburn, Britnell, and Wildon [2] obtained the probability that two random elements of G are conjugate.

A variation of the commuting probability problem, leading to its generalization, is how to compute the number of balanced G-valued labelings on various finite graphs. Cherniavsky, Goldstein, and Levit [4, 6] computed the number of balanced G-valued labelings on both directed and undirected graphs, when the group G is Abelian. Cherniavsky, Goldstein, Levit, and Shwartz [5] considered a non non-Abelian case.

A different direction in generalization of commuting probability appears in Das and Nath [8, 22]. They studied the probability $\Pr_g^\omega(G)$ of the equality

$$a_1 a_2 \cdots a_{n-1} a_n a_{\pi_n}^{-1} a_{\pi_{n-1}}^{-1} \cdots a_{\pi_2}^{-1} a_{\pi_1}^{-1} = g$$

for a fixed element g in a finite group G. The word

$$a_1 a_2 \cdots a_{n-1} a_n a_{\pi_n}^{-1} a_{\pi_{n-1}}^{-1} \cdots a_{\pi_2}^{-1} a_{\pi_1}^{-1},$$

where ω denotes the product $a_1 a_2 \cdots a_{n-1} a_n$ vary over all the elements of G. Nath [23] generalized the classical study of the commuting probability for which $\omega = a_1 a_2 a_1^{-1} a_2^{-1}$ and $g = 1$.

In this paper we take a slightly different approach in generalizing the commuting probability. Let

$$\pi = \langle \pi_1 \ \ \pi_2 \ \ \ldots \ \ \pi_n \rangle$$

be a permutation in S_n, written in a shortened form of the two-row notation. We define $\Pr_\pi(G)$ as the *permutation probability* of the equality

$$a_1 a_2 \cdots a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n}$$

in G. Notice that $\Pr_{\langle 2 \ 1 \rangle}(G)$ is just the commuting probability in G.

Notice also, that the probability

$$\Pr_\pi(G) = \Pr(a_1 a_2 \cdots a_{n-1} a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n})$$

is identical to $\Pr_1^\omega(G)$, with

$$\omega = a_1 a_2 \cdots a_{n-1} a_n a_{\pi_n}^{-1} a_{\pi_{n-1}}^{-1} \cdots a_{\pi_2}^{-1} a_{\pi_1}^{-1},$$

as Das and Nath [8, 22] have defined it.

In this work we

- obtain a new description of $\Pr_\pi(G)$ in terms of non-negative integers $c_{i_1,\ldots,i_n;j}(G)$. Integer $c_{i_1,\ldots,i_n;j}(G)$ is the number of different ways in which an element from a conjugacy class $\Omega_j \subset G$ can be broken into a product of elements from the conjugacy classes $\Omega_{1_1}, \ldots, \Omega_{i_n} \subset G$.

- prove that $\Pr_\pi(G)$, for a fixed finite group G, depends only on the number of alternating cycles in the cycle graph $\mathrm{Gr}(\pi)$ of the permutation π.

- show that the spectrum of permutation probabilities in a finite non-Abelian group, as π varies over all the elements of S_n, is the partition of $n!$ into a sum of the Hultman numbers A164652.

The following three theorems constitute the main finding of this paper

- Theorem 67: Let G be a finite group. Let $\phi \in S_n$ be a permutation whose cycle graph $\mathrm{Gr}(\phi)$ contains k alternating cycles. Then

$$\Pr_{\phi}(G) = \Pr^{n+1-k}(G) = \Pr(a_1 a_2 \cdots a_{n-k} a_{n+1-k} = a_{n+1-k} a_{n-k} \cdots a_2 a_1).$$

- Theorem 68: Let G be a finite non-Abelian group. Let ϕ and θ be two permutations in S_n. Then, $\Pr_{\phi}(G) = \Pr_{\theta}(G)$ if and only if the number of alternating cycles in the cycle graph $\mathrm{Gr}(\theta)$ equals the number of alternating cycles in the cycle graph of $\mathrm{Gr}(\phi)$. This implies that the spectrum of permutation probabilities in a non-Abelian group G consists of exactly $\left\lfloor \frac{n}{2} \right\rfloor + 1$ different numbers, each number corresponding to its unique Hultman class of permutations in S_n.

- Theorem 69: Let G be a finite group. Then

$$\begin{aligned}
\Pr^{2t}(G) &= \Pr(a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1) \\
&= \Pr(a_1 a_2 a_3 a_4 \cdots a_{2t-1} a_{2t} = a_2 a_1 a_4 a_3 \cdots a_{2t} a_{2t-1}) \\
&= \frac{\sum\limits_{x_1, x_2, \ldots, x_t \in G} |\mathrm{Stab.\,Prod}_n(x_1, x_2, \ldots, x_t))|}{|G|^{2t}} \\
&= \frac{1}{|G|^t} \cdot \sum_{i_1, i_2, \ldots, i_t, j=1}^{c(G)} \frac{|\Omega_j| \cdot c^2_{i_1, i_2, \ldots, i_t; j}(G)}{|\Omega_{i_1}| \cdot |\Omega_{i_2}| \cdot \cdots \cdot |\Omega_{i_t}|}
\end{aligned}$$

1.1 Basic definitions and notation

For a natural number n, S_n denotes the group of all permutations of n. We usually write a permutation $\pi \in S_n$ as

$$\pi = \langle \pi_1 \ \ \pi_2 \ \ \ldots \ \ \pi_n \rangle,$$

which is commonly known as "the shortened way of the two row notation". Sometimes, we also use the cyclic notation for a permutation $\pi \in S_n$, in which case we use parentheses and commas. Thus, for example, $(\theta_1, \theta_2, \theta_3)$ represents the cycle permutation $\theta_1 \mapsto \theta_2 \mapsto \theta_3 \mapsto \theta_1$. We refer to such cycle permutations as "cycles".

We use G to denote a finite group. For a finite set S, we denote the size of S by $|S|$. Two elements $g_1, g_2 \in G$ are called conjugate if there exists $h \in G$ such that $g_2 = h^{-1} g_1 h$. Conjugacy is an equivalence relation in G. As such, it breaks G into conjugacy classes. Let $c(G)$ denotes The number of conjugacy classes in G. Let $\Omega_1, \ldots, \Omega_{c(G)}$ denotes the conjugacy classes. Let$\Omega(g)$ denotes the conjugacy class of g for $g \in G$. The centralizer $C_G(g)$ of an element $g \in G$ is the set of all elements of G that commute with g. Recall that for every all $g \in G$,

$$|G| = |\Omega(g)| \cdot |C_G(g)| \,.$$

Let $C(G)$ denotes the set $\{\Omega_1, \ldots, \Omega_{c(G)}\}$ of all conjugacy classes in G. Let G' denotes the commutator subgroup of G, which is the minimal subgroup of G containing all elements of G of the form $ghg^{-1}h^{-1}$, where $g, h \in G$. We use the notation h^g to denote $g^{-1}hg$. To indicate that that $g, h \in G$ are conjugate in G we write $g \sim h$. The center $Z(G) \subseteq G$ is the subgroup of G, consisting of all elements $h \in G$ for which $h^g = h$ for all $g \in G$.

Let D_{2n} denotes the dihedral group with $2n$ elements, let Q_8 denotes the multiplicative group of unit quaternions, which has 8 elements.

Definition 1. For a sequence $(g_1, g_2, \ldots, g_n)$ of n elements of G, let $\mathrm{Stab.\,Prod}_n(g_1, g_2, \ldots, g_n)$ denotes the set of all the sequences $(a_1, a_2, \ldots, a_n)$ of n elements of G such that

$$a_1^{-1} g_1 a_1 \cdot a_2^{-1} g_2 a_2 \cdot \cdots \cdot a_n^{-1} g_n a_n = g_1 \cdot g_2 \cdot \cdots \cdot g_n.$$

Notice that $\mathrm{Stab.\,Prod}_n(g_1, g_2, \ldots, g_n)$ is a generalization of the notion of the centralizer of an element $g \in G$. Indeed, $\mathrm{Stab.\,Prod}_1(g)$ is just $C_G(g)$.

Definition 2. The nonnegative integer $c_{i_1,\ldots,i_n;j}(G)$ denotes the number of different ways of breaking a fixed element $y \in \Omega_j(G)$ into a product $y = x_1 x_2 \cdots x_n$ of elements $x_1 \in \Omega_{i_1}(G), x_2 \in \Omega_{i_2}(G), \ldots, x_n \in \Omega_{i_n}(G)$.

The number $c_{i_1,\ldots,i_n;j}(G)$ does not depend on the choice of the element $y \in \Omega_j(G)$. Indeed, if we take some other $y' \in \Omega_j(G)$, then there exists some $g \in G$ such that $y' = gyg^{-1}$ and $y = g^{-1}y'g$. Then each product $y = x_1 x_2 \cdots x_n$ corresponds to the product

$$y' = gyg^{-1} = (gx_1g^{-1}) \cdot (gx_2g^{-1}) \cdot \cdots \cdot (gx_ng^{-1}),$$

in which each $x'_t = (gx_tg^{-1})$ belongs to the same conjugacy class $\Omega_{i_t}(G)$ as x_t. Vice versa, each product $y' = x'_1 x'_2 \cdots x'_n$ corresponds back to the product

$$y = g^{-1}y'g = (g^{-1}x'_1g) \cdot (g^{-1}x'_2g) \cdot \cdots \cdot (g^{-1}x'_ng).$$

Thus, we see that the number of such different products is the same for any y and y' in $\Omega_j(G)$.

Notice that $c_{i_1,\ldots,i_n;j}(G)$ can be zero, and that $c_{i;j}(G) = 1$ if $i = j$, and $c_{i;j}(G) = 0$ if $i \neq j$.

Definition 3. Let $L_\pi(G)$ denotes the number of different solutions of the equation

$$a_1 a_2 \cdots a_{n-1} a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n}$$

in G. Clearly, $\mathrm{Pr}_\pi(G) = \frac{L_\pi(G)}{|G|^n}$.

Definition 4. We define $\mathrm{Pr}^n(G)$ as $\mathrm{Pr}_{\langle n \;\; n-1 \;\; \ldots \;\; 2 \;\; 1\rangle}(G)$.

For a permutation $\pi \in S_n$ define $\omega(\pi)$ as a formal expression $a_1 \cdots a_n \cdot a_{\pi_n}^{-1} \cdots a_{\pi_1}^{-1}$. Then $\mathrm{Pr}_\pi(G)$ is identical to $\mathrm{Pr}_1^\omega(G)$, which was defined by Das and Nath [8, 9, 22]. Similarly, $\mathrm{Pr}^n(G)$ is identical to $\mathrm{Pr}_1^n(G)$, as defined by Das and Nath [8, 9, 22]. For further information on calculations, properties, and estimates of $\mathrm{Pr}_1^\omega(G)$ and $\mathrm{Pr}_1^n(G)$ we refer the reader to the papers of Das and Nath [8, 9, 22].

Definition 5. Let $\mathrm{Spec}_n(G)$ denotes the set of all $\Pr_\pi(G)$, as π runs over all the permutations from S_n.

Definition 6. A finite group G is called generic if for two permutations $\pi, \theta \in S_n$, $\Pr_\pi(G) = \Pr_\theta(G)$ only if $\Pr_\pi(H) = \Pr_\theta(H)$ for every finite non-Abelian group H.

Definition 7. Let Part_n denotes the partition of S_n into subsets of permutations, for which the permutation equalities have the same probability for every finite group.

For a generic group G, there is a natural isomorphism between the sets $\mathrm{Spec}_n(G)$ and Part_n. We refer to $\mathrm{Spec}_n(G)$, for a generic group G, as the spectrum of permutation probabilities. Theorem 57 makes use of [10, Thm. 6.8] in order to show that every non-Abelian finite group is generic.

Definition 8. Hall [18] defined two groups G_1 and G_2 to be isoclinic if the following three conditions hold

- There exists an isomorphism α from $G_1/Z(G_1)$ onto $G_2/Z(G_2)$;
- There exists an isomorphism β from the commutator subgroup G_1' to the commutator subgroup G_2';
- If $\alpha(a_1Z(G_1)) = a_2Z(G_2)$ and $\alpha(b_1Z(G_1)) = b_2Z(G_2)$, then

$$\beta(a_1^{-1}b_1^{-1}a_1b_1) = a_2^{-1}b_2^{-1}a_2b_2.$$

For example, every two Abelian groups are isoclinic. The dihedral group D_8 and the quaternion group Q_8 are two non-Abelian groups, which are isoclinic.

Definition 9. Buckley [3] defined two groups G_1 and G_2 to be weakly isoclinic if the first two conditions of Definition 8 hold. Namely, if

- There exists an isomorphism α from $G_1/Z(G_1)$ onto $G_2/Z(G_2)$;
- There exists an isomorphism β from the commutator subgroup G_1' to the commutator subgroup G_2'.

2 Preliminaries

In the Lemmas 10 and 11 we reproduce well-known group theory results, which are fundamental for our work.

Lemma 10. *For any $a, b \in G$ we have $ab \sim ba$.*

Proof. $b(ab)b^{-1} = babb^{-1} = ba$. $\square$

Lemma 11. *For any x and y from the same conjugacy class $\Omega_i \subset G$, there are exactly*

$$\frac{|G|}{|\Omega_i|} = |C_G(x)| = |C_G(y)|$$

different ways to break x into a product $x = ab$ of two elements $a, b \in G$, so that $ba = y$.

Proof. Since $x \sim y$, there exists some $b \in G$ such that $bxb^{-1} = y$. We define $a = xb^{-1}$. Thus, $ab = xb^{-1}b = x$ and $ba = bxb^{-1} = y$. For each pair $a', b' \in G$, such that $a'b' = x$, there exists a unique element $g = b'b^{-1} = (a')^{-1} a$ in G, such that $a' = ag^{-1}$ and $b' = gb$. Now,

$$b'a' = gbag^{-1} = gyg^{-1}.$$

Hence, the pairs (a', b') of elements in G, such that $a'b' = x$ and $b'a' = y$, are in one-to-one correspondence with the elements g from $C_G(Y)$. So, the number of pairs of elements $a', b' \in G$, such that $a'b' = x$ and $b'a' = y$, is equal to $|C_G(y)|$. But

$$|C_G(y)| = \frac{|G|}{|\Omega_i|} = |C_G(x)|.$$

□

The following classical result on commuting probability, which is due to Gustafson [16], follows immediately from Lemmas 10 and 11.

Theorem 12 (Gustafson)**.** $\Pr^2(G) = \Pr(a_1a_2 = a_2a_1) = \frac{c(G)}{|G|}$.

Proof. For each $x \in G$ there are exactly $\frac{|G|}{|\Omega(x)|}$ different ways to write $ab = x = ba$ with $a, b \in G$. Thus, for each Ω_i there are $|G|$ different equations $ab = x = ba$ with $a, b \in G$ and $x \in \Omega(i)$. Indeed, there are $|\Omega(x)|$ different elements x in Ω_i, and for each choice of x, there are $\frac{|G|}{|\Omega(x)|}$ different ways to break that x into a product of commuting elements $a, b \in G$. Thus, $L_{\langle 2\ \ 1\rangle}(G) = |G| \cdot c(G)$ and

$$\Pr^2(G) = \frac{|G| \cdot c(G)}{|G|^2} = \frac{c(G)}{|G|}.$$

□

3 Calculation of $\mathrm{Spec}_3(G)$ and $\mathrm{Spec}_4(G)$

We address the general case of permutational equations in the following sections. In this section we study permutational equations for permutations from S_3 and S_4, which is self-contained and will help to illustrate the general case.

Lemma 13. *For any permutation $\pi \in S_n$, with its inverse $\pi^{-1} \in S_n$, the probability $\Pr_\pi(G) = \Pr_{\pi^{-1}}(G)$.*

Proof. By definition,

$$\Pr_\pi(G) = \Pr(a_1 a_2 \cdots a_{n-1} a_n = a_{\pi_1} a_{\pi_2} \cdots a_{\pi_{n-1}} a_{\pi_n})$$

Let b_1 denotes a_{π_1}, b_2 denotes a_{π_2}, ..., b_n denotes a_{π_n} . Then $a_1 = b_{(\pi^{-1})_1}$, $a_2 = b_{(\pi^{-1})_2}$, ..., $a_n = b_{(\pi^{-1})_n}$. As $a_1, a_2, \ldots, a_n$ run over all the elements of G, so do $b_1, b_2, \ldots, b_n$. Thus,

$$\Pr_{\pi^{-1}}(G) = \Pr(b_{(\pi^{-1})_1} b_{(\pi^{-1})_2} \cdots b_{(\pi^{-1})_{n-1}} b_{(\pi^{-1})_n} = b_1 b_2 \cdots b_{n-1} b_n) = \Pr_\pi(G).$$

□

We continue with Lemma 14, which is a particular case, in which $n = 1$, of a general fact observed by Das and Nath [9] that for

$$\omega_1 = a_1 a_2 \cdots a_{2n} a_1^{-1} a_2^{-1} \cdots a_{2n}^{-1},$$

$$\omega_2 = a_1 a_2 \cdots a_{2n+1} a_1^{-1} a_2^{-1} \cdots a_{2n+1}^{-1},$$

and for any $g \in G$, there is an equality $\Pr_g^{\omega_1}(G) = \Pr_g^{\omega_2}(G)$.

Lemma 14. *The probability $\Pr^3(G) = \Pr_{\langle 3\ 2\ 1\rangle}(G) = \Pr(a_1 a_2 a_3 = a_3 a_2 a_1)$ is equal to the probability $\Pr^2(G) = \Pr_{\langle 2\ 1\rangle}(G) = \Pr(a_1 a_2 = a_2 a_1) = \frac{|c(G)|}{|G|}$.*

Proof. For convenience, we rename a_1 to a, a_2 to b, and a_3 to c. Now, from $abc = cba$ we obtain $abcb = cbab$. Thus, the commutator $[cb, ab] = 1$. Therefore, if we choose and fix an element $b \in G$, then the other two elements a and c should be chosen in a such way that $[ab, cb] = 1$.

Hence, for every of choice of an element $a \in G$, we must choose an element $c \in G$ in such a way that $cb \in C_G(ab)$.

Since G is a group, the product ab, as $b \in G$ is fixed and a runs over all the elements of G, produces elements $x \in G$, and each $x \in G$ is produced exactly one time. Similarly, the product cb, as $b \in G$ is fixed and c runs over all the elements of $C_G(ab) \cdot b^{-1}$, produces elements $y \in C_G(ab)$, and each element $y \in C_G(ab)$ is produced exactly one time. Since $b \in G$ runs over all the elements of G, we get

$$L_{\langle 3\ 2\ 1\rangle}(G) = |G| \cdot \sum_{y \in G} |C_G(y)| = |G|^2 \cdot |C(G)|.$$

Dividing Equation 3 by $|G|^3$ gives us

$$\Pr_{\langle 3\ 2\ 1\rangle}(G) = \frac{|C(G)|}{|G|} = \Pr_{\langle 2\ 1\rangle}(G).$$

□

We will now prove that for all five nontrivial permutations in S_3, their probabilities are the same. Notice that these five permutations have two alternating cycles in their cycle graphs, but the identity permutation in S_3 has four alternating cycles in its cycle graph. A detailed explanation of cycle graphs and alternating cycles, followed by a clarification of their relevance to probabilities, will be made in Section 4.

Theorem 15. *For every nontrivial $\pi \in S_3$, the probability* $\Pr(a_1a_2a_3 = a_{\pi_1}a_{\pi_2}a_{\pi_3}) = \frac{c(G)}{|G|}$. *Thus, the spectrum* $\mathrm{Spec}_3(G)$ *is* $\{\frac{c(G)}{|G|}, 1\}$.

Proof. By Lemma 14, $\Pr(a_1a_2a_3 = a_3a_2a_1) = \frac{c(G)}{|G|}$. Clearly,

$$\Pr(a_1a_2a_3 = a_2a_1a_3) = \Pr(a_1a_2 = a_2a_1) = \frac{c(G)}{|G|}$$

and

$$\Pr(a_1a_2a_3 = a_1a_3a_2) = \Pr(a_2a_3 = a_3a_2) = \frac{c(G)}{|G|}.$$

To compute $\Pr(a_1a_2a_3 = a_3a_1a_2)$, notice that if g denotes the product a_1a_2. Then, as a_1 and a_2 run over all the elements of G, their product g will also run over all the elements of G, becoming equal to every element of G exactly $|G|$ times. Thus, the number $L(a_1a_2a_3 = a_3a_1a_2)$ of different solutions of the equation $a_1a_2a_3 = a_3a_1a_2$ in G is $|G|$ times the number of different solutions of the equation $ga_3 = a_3g$ in G. Hence,

$$\Pr(a_1a_2a_3 = a_3a_1a_2) = \frac{|G| \cdot |G| \cdot c(G)}{|G|^3} = \frac{c(G)}{|G|}.$$

By Lemma 13, we get

$$\Pr(a_1a_2a_3 = a_2a_3a_1) = \Pr(a_1a_2a_3 = a_3a_1a_2) = \frac{c(G)}{|G|}.$$

Obviously, $\Pr(a_1a_2a_3 = a_1a_2a_3) = 1$. $\square$

We now investigate permutation probabilities for S_4.

Lemma 16. *For any nontrivial permutation $\pi \in S_4$, if $\pi_1 = 1$ or $\pi_4 = 4$, then* $\Pr_\pi(G) = \frac{c(G)}{|G|}$.

Proof. If $\pi_1 = 1$, then the equation $a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$ is equivalent to the equation $a_2a_3a_4 = a_{\pi_2}a_{\pi_3}a_{\pi_4}$. By Theorem 15, there are $|G|^2 \cdot c(G)$ different equations $a_2a_3a_4 = a_{\pi_2}a_{\pi_3}a_{\pi_4}$ in G. Each of these equations corresponds exactly to $|G|$ different equations of the form $a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$ (since a_1 can be any element of G). Thus $L_\pi(G) = |G|^3 \cdot c(G)$ and $\Pr_\pi(G) = \frac{c(G)}{|G|}$. The same argument, but with a_4 instead of a_1, is applied for $\pi_4 = 4$. $\square$

Lemma 17. *For all nontrivial permutations $\pi \in S_4$, such that $\pi_{i+1} = \pi_i + 1$ for some $1 \leq i \leq 3$, the probability* $\Pr_\pi(G) = \frac{c(G)}{|G|}$.

Proof. The condition $\pi_{i+1} = \pi_i + 1$ implies that the permutation π keeps two consecutive numbers π_i and $\pi_i + 1$ in their consecutive order. Such are, for example, the permutations $\langle 4 \;\; 3 \;\; 1 \;\; 2 \rangle$, $\langle 3 \;\; 4 \;\; 1 \;\; 2 \rangle$, $\langle 2 \;\; 3 \;\; 4 \;\; 1 \rangle$, and $\langle 4 \;\; 2 \;\; 3 \;\; 1 \rangle, \langle 4 \;\; 1 \;\; 2 \;\; 3 \rangle$. Let g denotes the product $a_{\pi_i} a_{\pi_{i+1}}$. Then, as a_{π_i} and $a_{\pi_{i+1}}$ run over all the elements of G, their product g also runs over all the elements of G, becoming equal to each element of G exactly $|G|$ times. By Theorem 14, the equation $a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$, in which we change $a_{\pi_i}a_{\pi_{i+1}}$, on both sides, to g, has exactly $|G|^2 \cdot c(G)$ solutions. But these solutions naturally correspond to $|G|$ different solutions of the equation $a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$. Thus $L_\pi(G) = |G|^3 \cdot c(G)$ and $\Pr_\pi(G) = \frac{c(G)}{|G|}$. ☐

Lemmas 16 and 17 establish that for fifteen different permutations π in S_4, their probabilities equal $\Pr_\pi(G) = \frac{c(G)}{|G|}$. Notice that these fifteen permutations have exactly three alternating cycles in their cycle graphs $\mathrm{Gr}(\pi)$ (see Bafna and Pevzner [1]; Doignon and Labarre [12]). For the identity permutation, which has five alternating cycles in its cycle graph, the probability of the corresponding trivial permutation equation is 1.

The remaining eight permutations in S_4 have one alternating cycle in their cycle graphs. We will now show that for these eight permutations, the corresponding permutations have the same probability, which, in a generic group, is different both from 1 and from $\frac{c(G)}{|G|}$.

Theorem 18. *For any finite group G we have*

$$\begin{aligned}
\Pr{}^4(G) &= \Pr(a_1a_2a_3a_4 = a_4a_3a_2a_1) = \Pr(a_1a_2a_3a_4 = a_2a_1a_4a_3) \\
&= \frac{\sum\limits_{x,y\in G} |\mathrm{Stab.\,Prod}_2(x,y)|}{|G|^4} = \frac{1}{|G|^2} \cdot \sum_{i,k,j=1}^{c(G)} \frac{|\Omega_j| \cdot c^2_{i,k;j}(G)}{|\Omega_i| \cdot |\Omega_k|} \\
&= \frac{1}{|G|^2} \cdot \sum_{i,k,j=1}^{c(G)} \frac{|\Omega_j| \cdot c_{i,k;j}(G) \cdot c_{k,i;j}(G)}{|\Omega_i| \cdot |\Omega_k|}.
\end{aligned}$$

Proof. Notice that for any $x, y \in G$, the set $\mathrm{Stab.\,Prod}_2(x,y)$ of all ordered pairs (g,h) of elements of G, such that $xy = g^{-1}xgh^{-1}yh$, has an alternative description as the set of all the ordered pairs $(g \in G, f^{-1} \in G)$, such that $gxyf = xgfy$. Indeed, by setting $f = h^{-1}$, the equation $xy = g^{-1}xgh^{-1}yh$ becomes $xy = g^{-1}xgfyf^{-1}$. Multiplying the right by g and the left by f gives us $gxyf = xgfy$.

Thus, for each fixed ordered pair (x,y) of elements in G, there are exactly $|\mathrm{Stab.\,Prod}_2(x,y)|$ different equations $gxyf = xgfy$ with $g,h \in G$. As x and y run over all the elements of G, we obtain that the total number of different equations $gxyf = xgfy$ in G is $\sum\limits_{x,y\in G} |\mathrm{Stab.\,Prod}_2(x,y)|$.

Dividing the total number of different equations $gxyf = xgfy$ in G by $|G|^4$ gives us

$$\Pr(a_1a_2a_3a_4 = a_2a_1a_4a_3) = \frac{\sum\limits_{x,y\in G} |\mathrm{Stab.\,Prod}_2(x,y)|}{|G|^4}.$$

Next, consider the equation $a_1a_2a_3a_4 = a_4a_3a_2a_1$. Let x denotes the product a_1a_2, x' denotes the product a_2a_1, y denotes the product a_3a_4, and y' denotes the product a_4a_3. The equation $a_1a_2a_3a_4 = a_4a_3a_2a_1$ becomes $xy = y'x'$. By Lemma 10, we have $x \sim x'$ and $y \sim y'$.

Now consider any $x, x', y, y' \in G$, such that $x \sim x\prime$, $y \sim y'$, and $xy = y'x'$. By Lemma 11, there are $\frac{|G|}{|\Omega(x)|} = |C_G(x)|$ different ways of breaking x into a product a_1a_2 in such a way that $x' = a_2a_1$. Again, by Lemma 11, there are $\frac{|G|}{|\Omega(y)|} = |C_G(y)|$ different ways of breaking y into a product a_3a_4 in such a way that $y' = a_4a_3$. Thus, to each fixed equation $xy = y'x'$ correspond $|C_G(x)| \cdot |C_G(y)|$ different equations $a_1a_2a_3a_4 = a_4a_3a_2a_1$.

Next, for each fixed $x, y \in G$, we count the number of different equations $xy = y'x'$, where $x \sim x\prime$ and $y \sim y'$. Define $x'' = (y^{-1}xy)$. Thus, we get an equation $xy = y(y^{-1}xy) = yx''$. Now, for each equation $xy = y'x'$, as above, there exist some $g, h \in G$ such that $y' = g^{-1}yg$ and $x' = h^{-1}x''h$. But, for each fixed $x, y \in G$ we have $|\mathrm{Stab.\,Prod}_2(y, x'')|$ different elements $g, h \in G$, such that $xy = yx'' = g^{-1}ygh^{-1}x''h$. For each fixed pair $g, h \in G$, such that $yx'' = g^{-1}ygh^{-1}x''h$, a pair $g', h' \in G$ satisfies $(g')^{-1}yg' = g^{-1}yg$ and $(h')^{-1}x''h' = h^{-1}x''h$, if, and only if, $g'g^{-1} \in C_G(y)$ and $h'h^{-1} \in C_G(x'')$. Thus, for each fixed $x, y \in G$, there are exactly

$$\frac{|\mathrm{Stab.\,Prod}_2(y, x'')|}{|C_G(y)| \cdot |C_G(x'')|}$$

different equations $xy = y'x'$, in which $x' \sim x$ and $y' \sim y$. But, $|C_G(x'')| = |C_G(x)|$. Thus, for each fixed ordered pair (x, y) of elements of G, we have

$$\frac{|\mathrm{Stab.\,Prod}_2(y, (y^{-1}xy))|}{|C_G(y)| \cdot |C_G(x)|}$$

different equations $xy = y'x'$. As we showed above, to each of these equations correspond $|C_G(x)| \cdot |C_G(y)|$ different equations $a_1a_2a_3a_4 = a_4a_3a_2a_1$, in which $a_1a_2 = x$, $a_3a_4 = y$, $a_2a_1 = x'$, and $a_4a_3 = y'$. Thus, to each ordered pair (x, y) of elements of G correspond $|\mathrm{Stab.\,Prod}_2(y, (y^{-1}xy))|$ different equations $a_1a_2a_3a_4 = a_4a_3a_2a_1$, in which $a_1a_2 = x$ and $a_3a_4 = y$.

Thus, to find $\Pr(a_1a_2a_3a_4 = a_4a_3a_2a_1)$ we need to sum $|\mathrm{Stab.\,Prod}_2(y, (y^{-1}xy))|$ over all $x, y \in G$, and then divide that sum by $|G|^4$. For each fixed y, the product $v = y^{-1}xy$ runs over all the elements of G when x runs over all the elements of G. Thus, summing $|\mathrm{Stab.\,Prod2}(y, (y^{-1}xy))|$ over all $x, y \in G$ is the same as summing $|\mathrm{Stab.\,Prod}_2(y, v)|$ over all $y, v \in G$. Thus, we obtain

$$L_{\langle 4\ 3\ 2\ 1\rangle}(G) = \sum_{y,v\in G} |\mathrm{Stab.\,Prod}_2(x,y)|,$$

and

$$\begin{aligned}\Pr^4(G) &= \Pr(a_1a_2a_3a_4 = a_4a_3a_2a_1)\\ &= \frac{\sum\limits_{x,y\in G} |\mathrm{Stab.\,Prod}_2(x,y)|}{|G|^4} = \Pr(a_1a_2a_3a_4 = a_2a_1a_4a_3).\end{aligned}$$

Now, fix an element z in some equivalence class Ω_j in G. For each equation $xy = z = x'y'$ we have exactly

$$|C_G(x)| \cdot |C_G(y)| = \frac{|G|^2}{|\Omega(x)| \cdot |\Omega(y)|}$$

different equations

$$(a_1a_2)(a_3a_4) = xy = z = x'y' = (a_2a_1)(a_4a_3).$$

Indeed, there are $|C_G(x)|$ different ways to break x into a product a_1a_2 so that $a_2a_1 = x'$, and there are $|C_G(y)|$ different ways to break y into a product a_3a_4 so that $a_4a_3 = y'$.

Now, there are $c_{i,k;j}(G)$ different ways to break z as a product xy so that $x \in \Omega_i$ and $y \in \Omega_k$. For each of these $c_{i,k;j}(G)$ different ways, there are $c_{i,k;j}(G)$ different ways to break z as a product $x'y'$. Thus, for each ordered pair (Ω_i, Ω_k) of conjugacy classes in G, there are $c^2_{i,k;j}(G)$ different equations $xy = z = x'y'$ with $x, x' \in \Omega_i$ and $y, y' \in \Omega_k$. The number of different equations $xy = z = x'y'$ with $x, x' \in \Omega_i$ and $y, y' \in \Omega_k$ is the same for all $z \in \Omega_j$.

Taking the sum of the number of different equations $a_1a_2a_3a_4 = z = a_2a_1a_4a_3$, as z runs over all the elements of G, and dividing it by $|G|^4$, gives us

$$\Pr(a_1a_2a_3a_4 = a_2a_1a_4a_3) = \frac{1}{|G|^2} \cdot \sum_{i,k,j=1}^{c(G)} \frac{|\Omega_j| \cdot c^2_{i,k;j}(G)}{|\Omega_i| \cdot |\Omega_k|}.$$

Finally, fix an element z in some equivalence class Ω_j in G. For each equation $xy = z = y'x'$ we have exactly

$$|C_G(x)| \cdot |C_G(y)| = \frac{|G|^2}{|\Omega(x)| \cdot |\Omega(y)|}$$

different equations

$$(a_1a_2)(a_3a_4) = xy = z = y'x' = (a_4a_3)(a_2a_1).$$

Now, there are $c_{i,k;j}(G)$ different ways to break z as a product xy so that $x \in \Omega_i$ and $y \in \Omega_k$. For each of these $c_{k,i;j}(G)$ different ways, there are $c_{i,k;j}(G)$ different ways to break z as a product $x'y'$. Thus, for each ordered pair (Ω_i, Ω_k) of conjugacy classes in G, there are there are $c_{i,k;j}(G) \cdot c_{k,i;j}(G)$ different equations $xy = z = y'x'$ with $x, x' \in \Omega_i$ and $y, y' \in \Omega_k$.

Taking the sum of the number of different equations $a_1a_2a_3a_4 = z = a_4a_3a_2a_1$, as z runs over all the elements of G, and dividing it by $|G|^4$, gives us

$$\Pr(a_1a_2a_3a_4 = a_4a_3a_2a_1) = \frac{1}{|G|^2} \cdot \sum_{i,k,j=1}^{c(G)} \frac{|\Omega_j| \cdot c_{i,k;j}(G) \cdot c_{k,i;j}(G)}{|\Omega_i| \cdot |\Omega_k|}.$$

$\square$

To study the other four permutations in S_4, we first prove a lemma that is a particular case of Theorem 43.

Lemma 19. *Let $\pi \in S_4$ be a permutation such that $\pi_4 + 1 = \pi_3 = 2$ or $\pi_4 + 1 = \pi_3 = 3$. Then the equations*

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4},$$

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_3}a_{\pi_4}a_{\pi_2}$$

have the same number of solutions.

Proof. First, consider the case $\pi_4 + 1 = \pi_3 = 2$.

Rewrite the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_2a_1$$

as

$$a_1a_{\pi_2}^{-1}a_{\pi_2}a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_2a_1.$$

Let a denotes $a_{\pi_2}a_2$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_2a_1$$

becomes

$$a_1a_{\pi_2}^{-1}aa_3a_4 = a_{\pi_1}aa_1, \tag{1}$$

in which the variable $a_{\pi_2}^{-1}$ runs over all the elements of G, and for each fixed value of $a_{\pi_2}^{-1}$, the variable a runs over all the elements of G.

Rewrite the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_2a_1a_{\pi_2}$$

as

$$a_1a_{\pi_2}a_{\pi_2}^{-1}a_2a_3a_4 = a_{\pi_1}a_2a_1a_{\pi_2}.$$

Let a denotes $a_1a_{\pi_2}$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_2a_1a_{\pi_2}$$

becomes

$$aa_{\pi_2}^{-1}a_2a_3a_4 = a_{\pi_1}a_2a, \tag{2}$$

in which the variable $a_{\pi_2}^{-1}$ runs over all the elements of G, and for each fixed value of $a_{\pi_2}^{-1}$, the variable a runs over all the elements of G.

Now, Equation 1 is obtained from Equation 2 by renaming a to a_1 and renaming a_2 to a. Thus, they have the same number of solutions.

Finally, consider the case $\pi_4 + 1 = \pi_3 = 3$.

Rewrite the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_3a_2$$

as

$$a_1a_2a_{\pi_2}^{-1}a_{\pi_2}a_3a_4 = a_{\pi_1}a_{\pi_2}a_3a_2.$$

Let a denotes $a_{\pi_2}a_3$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_3a_2$$

becomes

$$a_1a_2a_{\pi_2}^{-1}aa_4 = a_{\pi_1}aa_2, \tag{3}$$

in which the variable $a_{\pi_2}^{-1}$ runs over all the elements of G, and for each fixed value of $a_{\pi_2}^{-1}$, the variable a runs over all the elements of G.

Rewrite the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_3a_2a_{\pi_2}$$

as

$$a_1a_2a_{\pi_2}a_{\pi_2}^{-1}a_3a_4 = a_{\pi_1}a_3a_2a_{\pi_2}.$$

Let a denotes $a_2a_{\pi_2}$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_3a_2a_{\pi_2}$$

becomes

$$a_1aa_{\pi_2}^{-1}a_3a_4 = a_{\pi_1}a_3a, \tag{4}$$

in which the variable $a_{\pi_2}^{-1}$ runs over all the elements of G, and for each fixed value of $a_{\pi_2}^{-1}$, the variable a runs over all the elements of G.

Now, Equation 3 is obtained from Equation 4 by renaming a into a_2 and renaming a_3 into a. Thus, they have the same number of solutions. □

The following corollary of Lemma 19 provides examples of the $x--y$ exchange operation, which will be introduced in Definition 33. It also illustrates the notion of the $x--y$ exchange orbit, which will be introduced in Definition 42, and demonstrates how the $3-\mathit{cycle}$ of Proposition 38 works.

Corollary 20. *The equations*

$$a_1a_2a_3a_4 = a_4a_3a_2a_1,$$

$$a_1a_2a_3a_4 = a_4a_2a_1a_3,$$

$$a_1a_2a_3a_4 = a_4a_1a_3a_2$$

have the same number of solutions.

Proof. For permutation $\pi = \langle 4\ \ 3\ \ 2\ \ 1\rangle$ we have $\pi_4 + 1 = \pi_3 = 2$. Thus, by Lemma 19, the permutation equation of the permutation $\langle 4\ \ 2\ \ 1\ \ 3\rangle$ has the same number of solutions as the permutation equation of π.

For permutation $\theta = \langle 4\ \ 1\ \ 3\ \ 2\rangle$ we have $\pi_4 + 1 = \pi_3 = 3$. Thus, by Lemma 19, the permutation equation of the permutation $\langle 4\ \ 3\ \ 2\ \ 1\rangle$ has the same number of solutions as the permutation equation of θ. □

The following corollary is based on Lemma 13, since $\langle 4 \ \ 2 \ \ 1 \ \ 3\rangle^{-1} = \langle 3 \ \ 2 \ \ 1 \ \ 4\rangle$ and $\langle 4 \ \ 1 \ \ 3 \ \ 2\rangle^{-1} = \langle 2 \ \ 4 \ \ 3 \ \ 1\rangle$.

Corollary 21. *(i) The equations*

$$a_1a_2a_3a_4 = a_4a_2a_1a_3,$$

$$a_1a_2a_3a_4 = a_3a_2a_1a_4$$

have the same number of solutions.

(ii) The equations

$$a_1a_2a_3a_4 = a_4a_1a_3a_2,$$

$$a_1a_2a_3a_4 = a_2a_4a_3a_1$$

have the same number of solutions.

To study the remaining two permutation in S_4, we first prove the following.

Lemma 22. *Let $\pi \in S_4$ be a permutation such that for some $i \in \{1, 2\}$, $\pi_i + 1 = \pi_{i+2}$ and $\pi_{i+1} = \pi_i - 2$. Let $j \in \{1, 2, 3, 4\}$ be such an integer that $pi_j = \pi_i - 1$. Let $\theta \in S_4$ be obtained from π by interchanging π_i and π_j. Then the equations*

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4},$$

$$a_1a_2a_3a_4 = a_{\theta_1}a_{\theta_2}a_{\theta_3}a_{\theta_4}$$

have the same number of solutions.

Proof. First, for permutations in S_4, the only option for the integer j is a unique element in $\{1, 2, 3, 4\}$, which is different from all three integers $i, i + 1, i + 2$. Similarly, the only option for the value p_i, for $\pi \in S_4$, is 3, and for the value p_j is 2.

For simplicity of dealing with the indices, we will consider the cases $j = 1, i = 2$, and $j = 4, i = 1$ separately. Even though the permutation $\pi \in S_4$ is uniquely determined in each of these two cases, we will use the notation $\pi_i = x$, $\pi_{i+1} = y$, $\pi_{i+2} = x+1$, and $\pi_j = y+1$. This is done to illustrate both the $x - -y$ cyclic operation, which will be introduced in Definition 44, and the proof of the Theorem 52. Additionally, this proof, in which the $x, y, x + 1, y + 1$ notation is used, can be adopted for a more general case of substrings in a longer string, which is the case for certain permutations in S_n with $n > 4$. An example of a substring of that type in a longer string, for which this proof works, will be provided at the end of the proof.

First, let $j = 4, i = 1$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$$

can be written as

$$a_ya_{y+1}a_xa_{x+1} = a_xa_ya_{x+1}a_{y+1} \tag{5}$$

Similarly, the equation

$$a_1a_2a_3a_4 = a_{\theta_1}a_{\theta_2}a_{\theta_3}a_{\theta_4}$$

can be written as

$$a_ya_{y+1}a_xa_{x+1} = a_{y+1}a_ya_{x+1}a_x \tag{6}$$

Now, define $c = a_xa_{x+1}$ and $d = a_ya_x^{-1}$, and insert them into Equation 5 as follows

$$da_xa_{y+1}c = a_xdca_{y+1} \tag{7}$$

Notice that as random variables a_y, a_x, a_{x+1} run over all the elements of G, so do random variables a_x, c, d. Similarly, as random variables a_x, c, d run over all the elements of G, so do random variables a_y, a_x, a_{x+1}. Thus, there is a one-to-one correspondence between the solutions of Equation 5 and the solutions of Equation 7. But Equation 7 is obtained from Equation 6 by renaming a_y to d and a_{x+1} to c. Thus, Equation 7 and Equation 6, after renaming the variables, have the same solutions.

Second, let $j = 1, i = 2$. Then the equation

$$a_1a_2a_3a_4 = a_{\pi_1}a_{\pi_2}a_{\pi_3}a_{\pi_4}$$

can be written as

$$a_ya_{y+1}a_xa_{x+1} = a_{y+1}a_xa_ya_{x+1} \tag{8}$$

Similarly, the equation

$$a_1a_2a_3a_4 = a_{\theta_1}a_{\theta_2}a_{\theta_3}a_{\theta_4}$$

can be written as

$$a_ya_{y+1}a_xa_{x+1} = a_xa_{y+1}a_ya_{x+1} \tag{9}$$

Now, define $c = a_xa_{x+1}$ and $d = a_ya_x^{-1}$, and insert them into Equation 8 as follows

$$da_xa_{y+1}c = a_xa_{y+1}dc \tag{10}$$

Again, there is a one-to-one correspondence between the solutions of Equation 8 and the solutions of Equation 10, but Equation 10 is obtained from Equation 9 by renaming a_y to d and a_{x+1} to c. Thus, Equation 10 and Equation 9, after renaming the variables, have the same solutions.

Obviously, for our purpose in this section, the case $j = 1, i = 2$ is of no interest, since multiplication of Equation 8 by a_{x+1}^{-1} on the right reduces it to a permutational equation for a permutation in S_3. However, it illustrates how the $x - -y$ cyclic operation works, when $a_ya_{y+1}a_xa_{x+1}$ and $a_{y+1}a_xa_ya_{x+1}$ are just substrings in a longer string, which is the case for certain permutations in S_n with $n > 4$. For example, the proof we provided here adapts to show that the equations $a_1(a_2a_3a_4a_5)a_6 = a_6(a_3a_4a_2a_5)a_1$ and $a_1(a_2a_3a_4a_5)a_6 = a_6(a_4a_3a_2a_5)a_1$ have the same number of solutions. □

Corollary 23. *(i) The equations*

$$a_1a_2a_3a_4 = a_2a_1a_4a_3,$$

$$a_1a_2a_3a_4 = a_3a_1a_4a_2$$

have the same number of solutions.

(ii) The equations

$$a_1a_2a_3a_4 = a_2a_1a_4a_3,$$

$$a_1a_2a_3a_4 = a_2a_4a_1a_3$$

have the same number of solutions.

Proof. The case of $j = 4, i = 1$ in Lemma 22 corresponds to $y = 1, y + 1 = 2$, $x = 3, x+1 = 4$. Thus, the equations of the permutations $\pi = \langle 3 \ \ 1 \ \ 4 \ \ 2\rangle$ and $\theta = \langle 2 \ \ 1 \ \ 4 \ \ 3\rangle$ have the same number of solutions. Specifically, Equation 5 is

$$a_1a_2a_3a_4 = a_3a_1a_4a_2$$

and Equation 6 is

$$a_1a_2a_3a_4 = a_2a_1a_4a_3.$$

By Lemma 22, they have the same number of solutions.

Since $\langle 2 \ \ 4 \ \ 1 \ \ 3\rangle = \langle 3 \ \ 1 \ \ 4 \ \ 2\rangle^{-1}$, the equations

$$a_1a_2a_3a_4 = a_3a_1a_4a_2,$$

$$a_1a_2a_3a_4 = a_2a_4a_1a_3$$

have, by Lemma 13, the same number of solutions. □

Thus, we obtain the following.

Theorem 24. *The permutations*

$$\langle 4 \ \ 3 \ \ 2 \ \ 1\rangle, \langle 2 \ \ 1 \ \ 4 \ \ 3\rangle, \langle 4 \ \ 2 \ \ 1 \ \ 3\rangle, \langle 4 \ \ 1 \ \ 3 \ \ 2\rangle, \langle 3 \ \ 2 \ \ 1 \ \ 4\rangle, \langle 2 \ \ 4 \ \ 3 \ \ 1\rangle,$$

$$\langle 3 \ \ 1 \ \ 4 \ \ 2\rangle, \langle 2 \ \ 4 \ \ 1 \ \ 3\rangle$$

in S_4 have the same probabilities.

Proof. This theorem follows from Theorem 18 and Corollaries 20, 21, and 23. □

In Theorem 57 we will show that every finite non-Abelian group is generic. Thus,

$$\Pr(a_1a_2a_3a_4 = a_2a_1a_3a_4) \neq \Pr(a_1a_2a_3a_4 = a_4a_3a_2a_1) \tag{11}$$

for every finite non-Abelian group G. Since both probabilities, appearing in Equation 11, cannot be equal to 1 in a non-Abelian group, it will Imply that the spectrum of probabilities, for permutations in S_4, consists of three different values. But now, in the Example 25, we explicitly compute $\Pr(a_1a_2a_3a_4 = a_2a_1a_3a_4) = \Pr^2(G)$ and $\Pr(a_1a_2a_3a_4 = a_2a_1a_4a_3) = \Pr^4(G)$ for the groups $G = D_8$ and $G = Q_8$. These probabilities, for both $G = D_8$ and $G = Q_8$, are different. This permits us to avoid using Theorem 57 in establishing Lemma 26. In Example 58 we will perform the same calculations for the general case of $\Pr^{2n}(G)$. Results, similar to our calculations of $\Pr^2(G)$ and $\Pr^4(G)$ for $G = D_8$ and $G = Q_8$, but in a much more general form and for a larger variety of groups, were obtained in [8, 22].

Example 25. Both $G = D_8$ and $G = Q_8$ have five conjugacy classes.
Thus, $\Pr^2(G) = \frac{5}{8}$ for both of these groups. For both D_8 and Q_8, the center consists of the identity 1 and another element c, such that $c^2 = 1$. For both of these groups, the factor of the group by its center is the Abelian group $K_4 = Z_2 \times Z_2$. This means that if for some $x, y \in G$, $xy \neq yx$, then $xy = cyx$. Hence, the equation $a_1a_2a_3a_4 = a_2a_1a_4a_3$ is satisfied either if $a_1a_2 = a_2a_1$ and $a_3a_4 = a_4a_3$, or if $a_1a_2 = ca_2a_1$ and $a_3a_4 = ca_4a_3$. The first option has the probability $\frac{5}{8} \cdot \frac{5}{8} = \frac{25}{64}$. The second option has the probability $\frac{3}{8} \cdot \frac{3}{8} = \frac{9}{64}$. Thus, $\Pr^4(G) = \frac{25}{64} + \frac{9}{64} = \frac{17}{32}$. Notice that $\Pr^4(G) < \Pr^2(G)$.

Now we may conclude with the following.

Theorem 26. *For a generic finite non-Abelian group G, the spectrum of permutation probabilities over S_4 consists of only three probabilities*

$$\mathrm{Spec}_4(G) = \{1, \Pr^2(G) = \frac{|c(G)|}{|G|}, \Pr^4(G)\}$$

Notice that the calculations for $G = D_8$ and $G = Q_8$ show that the three probabilities belonging to $\mathrm{Spec}_4(G)$ are pairwise different for these two groups.

From the results of this section it is evident that permutational equalities of any two permutations from S_2, S_3, or S_4 have the same probability if they have the same number of alternating cycles in their cycle graphs. Consequently, the number of different permutations, corresponding to each probability in $\mathrm{Spec}_2(G)$, $\mathrm{Spec}_3(G)$, or $\mathrm{Spec}_4(G)$, is precisely the Hultman number $S_H(n, k)$, where $n = 2, 3, 4$ and k is the number of alternating cycles in the cycle graphs of these permutations. In the following sections we extend the observations and calculations of this section to S_n.

4 Probabilities of permutation equations, number of alternating cycles, and Hultman decomposition

For the information on cycle graphs, decomposition to alternating cycles, and Hultman numbers, as well as many other related definitions and notions, we refer to Doignon and Labarre [12] and the On-Line Encyclopedia of Integer Sequences [25]. Here we briefly review these notions.

Definition 27. The cycle graph $\mathrm{Gr}(\phi)$ of a permutation $\phi \in S_n$ is the bi-colored directed graph with $n+1$ vertices $\phi_0 = 0, \phi_1, \ldots, \phi_n$, whose edge set consists of

- black edges $\phi_n \to \phi_{n-1}$, $\phi_{n-1} \to \phi_{n-2}$, …, $\phi_1 \to \phi_0$, $\phi_0 \to \phi_n$, and
- grey edges $0 \dashrightarrow 1$, $1 \dashrightarrow 2$, …, $(n-1) \dashrightarrow n$, $n \dashrightarrow 0$.

The set of black and grey edges is decomposed in a unique way into edge-disjoint alternating cycles in which the black and the grey edges alternate. It is called the decomposition of $\mathrm{Gr}(\phi)$ into alternating cycles.

Definition 28. The Hultman number $S_H(n,k)$ is a nonnegative integer that counts the number of permutations in S_n, whose cycle graph decomposes into k alternating cycles.

Let $S(1+n)$ denotes the group of all permutations of the set $\{0,1,2,\ldots,n\}$.

Definition 29. Let $\phi^\bullet$ denotes the $n+1$-cycle in a permutation $\phi \in S_n$.

$$\phi_n \to \phi_{n-1} \to \phi_{n-2} \to \cdots \to \phi_1 \to \phi_0 \to \phi_n$$

in $S(1+n)$, which is the $n+1$-cycle, composed of the black arrows of $\mathrm{Gr}(\phi)$.

We will use the cyclic notation $(\phi_0, \phi_n, \phi_{n-1}, \ldots, \phi_2, \phi_1)$ for $\phi^\bullet$. Notice that there is a trivial one-to-one correspondence between all the permutations of S_n and all the $n+1$-cycles in $S(1+n)$. Namely, the entries of a $n+1$-cycle, starting from the one after 0, are interpreted as the entries of the permutation, but read backwards, written in the shortened way of the two-row notation. Thus, for any $n+1$-cycle C in $S(1+n)$, we can easily obtain the unique permutation $\phi \in S_n$, for which the $n+1$-cycle C is its black cycle $\phi^\bullet$.

Definition 30. For a permutation $\phi \in S_n$ we define the corresponding permutation $\phi^\circ \in S(1+n)$ to be $\phi^\bullet \cdot (0,1,\ldots,n)$.

Notice that ϕ° cannot contain $m \mapsto (m+1)$ for any $m = 0,1,\ldots,n$, since $m \mapsto (m+1)$ is $i \dashrightarrow (i+1) \to (i+1)$, but an $(n+1)$-cycle $\phi^\bullet$ cannot contain $(i+1) \to (i+1)$.

Theorem 31 (Doignon and Labarre's theorem 8)**.** *There is a natural one-to-one correspondence between the cycles in the cycle decomposition of the permutation ϕ° and the alternating cycles in* $\mathrm{Gr}(\phi)$*.*

Therefore, there is a unique way to decompose a permutation into alternating cycles.

Definition 32. We define $H(S_n)$ as a partition of S_n into pairwise disjoint sets containing permutations with the same number of alternating cycles in their cycle graph.

Now we are going to introduce two operations, $x--y$ exchange operation in Definition 33 and $x--y$ cyclic operation in Definition 44, which transform permutations in S_n. Next, we show that these two operations do not change the number of alternative cycles in the cycle graph of a permutation. After that, we demonstrate that these two operations do not change the probabilities of the permutation equations. Finally, we prove that any two permutations that have the same number of alternating cycles in their cycles graphs, can be connected to each-other by performing a finite number of these operations. This establishes that any two permutations with the same number of alternating cycles in their cycle graphs, have the same probabilities of their permutation equalities.

4.1 Exchange operation

Let $\phi \in S_n$ be a permutation. We augment ϕ by defining $\phi_0 = 0$.

Definition 33. Let $0 \le x = \phi_j, y = \phi_i, w, z \le n$, for some $0 \le i, j \le n$, be four integers, such that

$$z \to x \dashrightarrow x+1 \to y$$

and

$$y \to w$$

appear in some alternating cycles of $\mathrm{Gr}(\phi)$. The black arrow $x+1 \to y$ implies that $x+1 = \phi_{i+1}$. The black arrow $z \to x$ implies that $z = \phi_{j+1}$. The black arrow $y \to w$ implies that $w = \phi_{i-1}$. All the arithmetic is performed modulo $n+1$. The $x--y$ exchange operation is defined as follows (compare it to Lemma 19)

- if $x = w$ or if $y = z$, then the $x--y$ exchange operation does not change ϕ;
- if $y = \phi_0 = 0$, then the $x--y$ exchange operation changes

  $$\langle \phi_1 = (x+1) \ \ \dots \ \ \phi_{j-1} \ \ \phi_j = x \ \ \phi_{j+1} = z \ \ \dots \ \ \phi_n = w \rangle$$

  to

  $$\langle \phi_{j+1} = z \ \ \phi_{j+2} \ \ \dots \phi_n = w \ \ \phi_1 = (x+1) \ \ \dots \ \ \phi_{j-1} \ \ \phi_j = x \rangle;$$

- if $x = \phi_0 = 0$, then the $x--y$ exchange operation changes

  $$\langle \phi_1 = z \ \ \dots \ \ \phi_{i-1} = w \ \ \phi_i = y \ \ \phi_{i+1} = 1 \ \ \dots \ \ \phi_n \rangle$$

  to

  $$\langle \phi_i = y \ \ \phi_1 = z \ \ \dots \ \ \phi_{i-1} = w \ \ \phi_{i+1} = 1 \ \ \dots \ \ \phi_n \rangle;$$

- if $1 < i+1 < j$, then the $x--y$ exchange operation changes

  $$\langle \phi_1 \ \ \dots \ \ \phi_{i-1} = w \ \ \phi_i = y \ \ \phi_{i+1} = (x+1) \ \ \dots \ \ \phi_j = x \ \ \phi_{j+1} = z \ \ \dots \ \ \phi_n \rangle$$

  to

  $$\langle \phi_1 \ \ \dots \ \ \phi_{i-1} = w \ \ \phi_{i+1} = (x+1) \ \ \dots \ \ \phi_j = x \ \ \phi_i = y \ \ \phi_{j+1} = z \ \ \dots \ \ \phi_n \rangle;$$

- if $0 < j < i$, then the $x - -y$ exchange operation changes

$$\langle \phi_1 \ \ \ldots \ \ \phi_j = x \ \ \phi_{j+1} = z \ \ \ldots \ \ \phi_{i-1} = w \ \ \phi_i = y \ \ \phi_{i+1} = (x+1) \ \ \ldots \ \ \phi_n \rangle$$

to

$$\langle \phi_1 \ \ \ldots \ \ \phi_j = x \ \ \phi_i = y \ \ \phi_{j+1} = z \ \ \ldots \ \ \phi_{i-1} = w \ \ \phi_{i+1} = (x+1) \ \ \ldots \ \ \phi_n \rangle.$$

Let us consider several examples of the $x - -y$ exchange operation.

Example 34. Let $\phi = \langle 4 \ 1 \ 6 \ 2 \ 5 \ 7 \ 3 \rangle$. We perform the $5 - -1$ exchange operation on ϕ. Here $x = 5 = \phi_5$ and $y = 1 = \phi_2$. Hence, $z = \phi_6 = 7$ and $w = \phi_1 = 4$. The fact that $x + 1 = 6 = \phi_3$ causes the condition $x + 1 \to y$ to be satisfied. The condition $x + 1 \to y$ is what makes the $x - -y$ exchange operation possible. Now, $i = 2$ and $j = 5$. Thus, $1 < i + 1 < j$ and we get that the $5 - -1$ exchange operation changes ϕ to $\langle 4 \ 6 \ 2 \ 5 \ 1 \ 7 \ 3 \rangle$.

Example 35. Let $\phi = \langle 4 \ 1 \ 6 \ 2 \ 5 \ 7 \ 3 \rangle$. We perform the $4 - -2$ exchange operation on ϕ. Here $x = 4 = \phi_1$ and $y = 2 = \phi_4$. Hence, $z = \phi_2 = 1$ and $w = \phi_3 = 6$. The fact that $x + 1 = 5 = \phi_5$ causes the condition $x + 1 \to y$ to be satisfied. The condition $x + 1 \to y$ is what makes the $x - -y$ exchange operation possible. Now, $i = 4$ and $j = 1$. Thus, $0 < j < i$ and we get that the $4 - -2$ exchange operation changes ϕ to $\langle 4 \ 2 \ 1 \ 6 \ 5 \ 7 \ 3 \rangle$.

Example 36. Let $\phi = \langle 4 \ 6 \ 1 \ 2 \ 5 \ 7 \ 3 \rangle$. We perform the $0 - -6$ exchange operation on ϕ. Here $x = 0 = \phi_0$ and $y = 6 = \phi_2$. Hence, $z = \phi_1 = 4$ and $w = \phi_5 = 5$. The fact that $x+1 = 1 = \phi_3$ causes the condition $x+1 \to y$ to be satisfied. The condition $x+1 \to y$ is what makes the $x - -y$ exchange operation possible. Now, $i = 2$ and $j = 0$. Since $x = \phi_0 = 0$, we get that the $0 - -6$ exchange operation changes ϕ to $\langle 6 \ 4 \ 1 \ 2 \ 5 \ 7 \ 3 \rangle$.

Example 37. Let $\phi = \langle 4 \ 1 \ 6 \ 3 \ 5 \ 7 \ 2 \rangle$. We perform the $3 - -0$ exchange operation on ϕ. Here $x = 3 = \phi_4$ and $y = 0 = \phi_0$. Hence, $z = \phi_5 = 5$ and $w = \phi_7 = 2$. The fact that $x+1 = 4 = \phi_1$ causes the condition $x+1 \to y$ to be satisfied. The condition $x+1 \to y$ is what makes the $x - -y$ exchange operation possible. Now, $i = 0$ and $j = 4$. Since $y = \phi_0 = 0$, we get that the $3 - -0$ exchange operation changes ϕ to $\langle 5 \ 7 \ 2 \ 4 \ 1 \ 6 \ 3 \rangle$.

Notice that after completing the $x - -y$ exchange operation on ϕ, $y \to x \dashrightarrow x + 1 \to w$ and $z \to y$ will appear in the alternating cycles of the cycle graph of the new permutation.

Proposition 38. *Let ϕ and θ be two different permutations in S_n, such that θ is obtained from ϕ by an $x - -y$ exchange operation. Then $\theta^\bullet$ is obtained from $\phi^\bullet$ by multiplying $\phi^\bullet$ on the left by the $3-$cycle $(x, y, w) \in S(1 + n)$. Namely,*

$$\theta^\bullet = (x, y, w) \cdot \phi^\bullet.$$

Proof. Since the $x--y$ exchange operation was permissible on ϕ, and since this operation changed ϕ, the cycle $\phi^\bullet$ must be of the form $(x+1, y, w, \ldots, z, x, \ldots)$. Indeed, $(x+1) \to y \to w$ and $z \to x$ cannot intersect, since $\theta \neq \phi$. Here we are using the cyclic notation, in which the cycles can be written starting from any entry. Now,

$$(x, y, w) \cdot \phi^\bullet = (x+1, w, \ldots, z, y, x, \ldots).$$

To construct θ we need to rewrite the cycle $(x+1, w, \ldots, z, y, x, \ldots)$, starting from 0. Then the cycle will become $(0, \theta_n, \ldots, \theta_1)$, which permits us to obtain $\theta = \langle \theta_1 \ \ \ldots \ \ \theta_n \rangle$. When we rewrite the cycle $(x+1, w, \ldots, z, y, x, \ldots)$, starting from 0, we can have four different cases

- if $y = 0$, then the cycle, after rewriting, becomes $(y = 0, x, \ldots, x+1, w, \ldots, z)$;
- if $x = 0$, then the cycle, after rewriting, becomes $(x = 0, \ldots, x+1 = 1, w, \ldots, z, y)$;
- if $1 < i+1 < j$, then the cycle, after rewriting, becomes $(0, \ldots, z, y, x, \ldots, x+1, w, \ldots)$;
- if $1 < j < i$, then the cycle, after rewriting, becomes $(0, \ldots, x+1, w, \ldots, z, y, x, \ldots)$.

In all these four cases we obtain the exact θ, which is described in Definition 33 as the result of the $x--y$ exchange operation. □

Notice that the inverse of an $x--y$ exchange operation is not, in general, an $x--y$ exchange operation. Indeed, $\theta^\bullet$ might not contain $(w+1) \to y \to x$, which is required to perform a $w--x$ exchange operation on θ and obtain ϕ.

Proposition 39. *Let $\theta \neq \phi$ be a permutation obtained from ϕ by some $x--y$ exchange operation. Then the cyclic presentation of θ° is obtained from the cyclic presentation of ϕ° by relocating x from the place after $(z-1)$ and before y to the place after $(y-1)$ and before w; i.e., the cycle of ϕ° of the form $(\ldots, z-1, x, y, \ldots)$ becomes $(\ldots, z-1, y, \ldots)$, and the cycle of ϕ° of the form $(\ldots, y-1, w, \ldots)$ becomes $(\ldots, y-1, x, w, \ldots)$. This, in particular, implies that θ° and ϕ° have the same number of cycles in their cyclic decompositions.*

Proof. By Proposition 38, $\theta^\bullet = (x, y, w) \cdot \phi^\bullet$. This implies that

$$\theta^\circ = \theta^\bullet \cdot (0, 1, \ldots, n) = (x, y, w) \cdot \phi^\bullet \cdot (0, 1, \ldots, n) = (x, y, w) \cdot \phi^\circ$$

Now, multiplication of ϕ° on the left by (x, y, w) removes x from the cycle $(\ldots, z-1, x, y, \ldots)$ and places it in the cycle $(\ldots, y-1, w, \ldots)$ between $y-1$ and w. Thus, $z-1$, instead of going to x, now goes to y. And x, instead of going to y, now goes to w. And $y-1$, instead of going to w, now goes to x. No other changes are done by multiplication of ϕ° from the left by 3−cycle (x, y, w). □

Recall that Bafna and Pevzner [1], for $1 \le i < j < k \le n+1$, defined the permutation $\rho(i,j,k)$ to be

$$\rho(i,j,k) = \langle 1 \ \ \ldots \ \ (i-1) \ \ j \ \ \ldots \ \ (k-1) \ \ i \ \ \ldots \ \ (j-1); \ k \ \ \ldots \ \ n \rangle. \tag{12}$$

Next, for a permutation $\phi \in S_n$, Bafna and Pevzner defined a block-transposition, which exchanges places of the blocks $i \ \ \ldots \ \ (j-1)$ and $j \ \ \ldots \ \ (k-1)$ inside ϕ, to be $\phi \cdot \rho(i,j,k)$. For any three pairwise different integers $1 \le i,j,k \le n$ one can define

$$\rho(i,j,k) = \rho(i,k,j) = \rho(j,i,k) = \rho(j,k,i) = \rho(k,i,j) = \rho(k,j,i).$$

Since in one of these six expressions, i,j,k are placed in the increasing order, which makes that expression well-defined by Equation 12, all six expressions are now well-defined and represent the same permutation $\rho(i,j,k)$. Finally, if two or more of the three integers $1 \le i,j,k \le n+1$ are equal, $\rho(i,j,k)$ is defined as an identity permutation. Now $\rho(i,j,k)$ is defined for any three integers $1 \le i,j,k \le n+1$ and represents an appropriate block-transposition. Clearly, if two or more of the three integers $1 \le i,j,k \le n$ are equal, at least one of the blocks is empty, which corresponds to no change performed to ϕ. Now we can relate our $x--y$ exchange operation to the block-transpositions.

Remark 40. Let ϕ be a permutation in S_n, extended by $\phi_0 = 0$, such that for some $0 \le \phi_j = x, \phi_i = y \le n$, $\phi_{i+1} = x+1$. Then performing the $x--y$ exchange operation is a block-transposition, for which the permutation ρ is selected as follows

- if $x = j = 0$, then select $\rho(1, i, i+1)$;
- if $y = i = 0$, then select $\rho(1, j+1, n+1)$;
- in all other cases select $\rho(i, i+1, j+1)$.

Lemma 2.1 in Bafna and Pevzner's work [1] asserts that a block-transformation can either increase by two, or decrease by two, or keep unchanged the number of alternating cycles in the cycle graph of a permutation. We now show that an $x--y$ exchange operation does not change the number of alternating cycles in the cycle graph of a permutation.

Lemma 41. *Let a permutation $\theta \in S_n$ be obtained from a permutation $\phi \in S_n$ by an $x--y$ exchange operation. Then θ and ϕ have the same number of alternating cycles in their cycle graphs* $\mathrm{Gr}(\theta)$ *and* $\mathrm{Gr}(\phi)$.

Proof. The lemma directly follows from Proposition 39 and Theorem 31. However, we produce an alternative proof, based on Bafna and Pevzner's analysis of block-transformations.

Notice that the edges, which appear in $\mathrm{Gr}(\phi)$ and which do not appear in $\mathrm{Gr}(\theta)$, are precisely the three black edges $\phi_i = y \to w = \phi_{i-1}$, $\phi_{i+1} = x+1 \to y = \phi_i$, and $\phi_{j+1} = z \to x = \phi_j$.

Similarly, the edges, which appear in $\mathrm{Gr}(\theta)$ and which do not appear in $\mathrm{Gr}(\phi)$, are precisely the three black edges $\phi_{i+1} = x+1 \to w = \phi_{i-1}$, $\phi_{j+1} = z \to y = \phi_i$, and $\phi_i = y \to x = \phi_j$.

Since the black edges $\phi_{i+1} = x+1 \to y = \phi_i$ and $\phi_{j+1} = z \to x = \phi_j$ belong to the same alternating cycle in $\mathrm{Gr}(\phi)$, the above-mentioned three black edges $y \to w$, $x+1 \to y$, and $z \to x$ belong to, at most, two alternating cycles in $\mathrm{Gr}(\phi)$. Similarly, since the black edges $\phi_{i+1} = x+1 \to w = \phi_{i-1}$ and $\phi_i = y \to x = \phi_j$ belong to the same alternating cycle in $\mathrm{Gr}(\theta)$, the above-mentioned three black edges $x+1 \to w$, $z \to y$, and $y \to x$ belong to, at most, two alternating cycles in $\mathrm{Gr}(\phi)$.

In the proof of Lemma 2.1 in Bafna and Pevzner's work [1],it is shown that if $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ differ by exactly three black edges, which in both graphs $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ belong to one or two alternating cycles, then $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ have the same number of alternating cycles. $\square$

Definition 42. We say that the permutations $\phi, \theta \in S_n$ are in the same "$x--y$ exchange orbit" if there exist some permutations $\tau_1, \ldots, \tau_k \in S_n$ such that $\tau_1 = \phi$, $\tau_k = \theta$, and, for each $i = 1, \ldots, k-1$, either τ_i can be obtained from τ_{i+1} by an $x--y$ exchange operation, or τ_{i+1} can be obtained from τ_i by an $x--y$ exchange operation.

Notice that according to Definition 42, $\phi, \theta \in S_n$ can be in the same $x--y$ exchange orbit, while neither of them can be obtained from the other by performing $x--y$ exchange operations.

Theorem 43. *Let $\phi, \theta \in S_n$ be two permutations such that θ is obtained from ϕ by an $x--y$ exchange operation. Then*

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Proof. Compare this proof with the proof of Lemma 19 above. If $x = y$ then $\theta = \phi$ and the theorem follows. Hence, we assume that $x \neq y$.

First, we consider the case when $x, x+1, w, y, z$ are all different than 0. In that case, the requirement that $z \to x \dashrightarrow x+1 \to y$ and $y \to w$ are present in $\mathrm{Gr}(\phi)$ implies that the product $a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$ contains sub-products $a_w a_y a_{x+1}$ and $a_x a_z$. These two sub-products $a_w a_y a_{x+1}$ and $a_x a_z$ can "overlap" if and only if $z = w$. By overlapping we mean that they have a common piece. For example, if $z = w$ then $a_z = a_w$ is the overlap of these two products.

If the sub-product $a_w a_y a_{x+1}$ appears in the product $a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$ before the sub-product $a_x a_z$, then $z \neq w$. In that case, we rewrite the equation

$$a_1 \cdots a_x a_{x+1} a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-2}} a_w a_y a_{x+1} a_{\phi_{i+2}} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots a_{\phi_n}$$

as

$$a_1 \cdots a_x a_y^{-1} (a_y a_{x+1}) a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-2}} a_w (a_y a_{x+1}) a_{\phi_{i+2}} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots\ a_{\phi_n} \quad (13)$$

Similarly, the fact that $y \to x \dashrightarrow x+1 \to w$ and $z \to y$ are present in $\mathrm{Gr}(\theta)$, implies that the product $a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}$ contains sub-products $a_x a_y a_z$ and $a_w a_{x+1}$. These two sub-products can "overlap" if and only if either $x = w$ or $z = x+1$. But $\phi_{j+1} = z = x+1 = \phi_{i+1}$ would imply $i = j$ and $\phi_j = x = y = \phi_i$. Thus, $\theta = \phi$. If $x = w$, then $\theta = \phi$ by Definition 33. So, we can assume that $a_w a_y a_{x+1}$ and $a_x a_z$ do not overlap. Again, we rewrite the equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\theta_1} \cdots a_{\theta_{i-2}} a_w a_{x+1} a_{\theta_{i+1}} \cdots a_{\theta_{j-2}} a_x a_y a_z a_{\theta_{j+2}} \cdots a_{\theta_n}$$

as

$$a_1 \cdots a_{x-1} (a_x a_y) a_y^{-1} a_{x+1} \cdots a_n = a_{\theta_1} \cdots a_{\theta_{i-2}} a_w a_{x+1} a_{\theta_{i+1}} \cdots a_{\theta_{j-2}} (a_x a_y) a_z a_{\theta_{j+2}} \cdots a_{\theta_n} . \quad (14)$$

Notice that as the random variable a_y runs over all the elements of G, so does its inverse a_y^{-1}. Also, for each choice of a_y, as the random variable a_x runs over all the elements of G, so does the random variable $b = (a_x a_y)$. Similarly, for each choice of $a = a_y^{-1}$, as the random variable a_{x+1} runs over all the elements of G, so does the random variable $c = (a_y a_{x+1})$.

We show now that Equations 13 and 14, up to renaming variables, are identical. We regard $b = (a_x a_y)$ as one variable. Similarly, we regard $c = (a_y a_{x+1})$ as one variable. Notice that the left sides of Equations 13 and 14 have $n+1$ variables in each, and their right sides have $n-1$ variables in each. Both left sides have the variables $a_1, \ldots, a_{x-1}$ in place of $1, \ldots, x-1$, respectively, and the variables $a_{x+2}, \ldots, a_n$ in place of $x+3, \ldots, n+1$, respectively.

Notice that for all $1 \le r \le i-1$, $\phi_r = \theta_r$ and $a_{\phi_r} = a_{\theta_r}$. Similarly, for all $j+1 \le r \le n$, $\phi_r = \theta_r$ and $a_{\phi_r} = a_{\theta_r}$. For $i+1 \le r \le j-2$, $\phi_{r+1} = \theta_r$ and $a_{\phi_{r+1}} = a_{\theta_r}$. Thus, the right sides of Equations 13 and 14 carry the same variables in place of $1, \ldots, i-1$ and $i+1, \ldots, j-2$ and $j, \ldots, n-1$.

The random variable a_x appears in the x-th place on the left side of Equation 13 and in the $(j-1)$-th place on its right side. Similarly, the random variable $b = (a_x a_y)$ appears in the x-th place on the left side of Equation 14 and in the $(j-1)$-th place on its right side.

The inverse a_y^{-1} of the random variable a_y appears in the $(x+1)$-th place on the left side of Equation 13 and does not appear on its right side. Similarly, the inverse a_y^{-1} of the random variable a_y appears in the $(x+1)$-th place on the left side of Equation 14 and does not appear its right side. The random variable a_y cannot appear in the x-th, $(x+1)$-th, or $(x+2)$-th place on the left side of Equation 13 or of Equation 14. Since the rest of the places of the left sides of Equations 13 and 14 carry the same variables, a_y must appear in the same place in both left sides. The right sides of Equations 13 and 14 do not contain a_y.

The random variable $c = (a_y a_{x+1})$ appears in the $(x+2)$-th place on the left side of Equation 13 and on the i-th place on its right side. Similarly, the random variable a_{x+1} appears in the $(x+2)$-th place on the left side of Equation 14 and in the i-th place on its right side.

Thus, Equations 13 and 14, up to renaming variables, are identical. This implies that they have the same number of solutions. This, in its turn, implies that

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Now, assume that the sub-product $a_x a_z$ appears in the product $a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$ before the sub-product $a_w a_y a_{x+1}$. Then, if $z = w$, then a_z is the same as a_w, and we have the sub-product $a_x a_w a_y a_{x+1}$ inside the product $a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$. In that case, the $x - -y$ exchange operation only exchanges the places of a_w and a_y. We rewrite the equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-3}} a_x a_w a_y a_{x+1} a_{\phi_{i+2}} \cdots a_{\phi_n}$$

as

$$a_1 \cdots a_{x-1} a_x a_y^{-1} (a_y a_{x+1}) a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-3}} a_x a_w (a_y a_{x+1}) a_{\phi_{i+2}} \cdots a_{\phi_n}. \tag{15}$$

The equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\theta_1} \cdots a_{\theta_{i-3}} a_x a_y a_w a_{x+1} a_{\theta_{i+2}} \cdots a_{\theta_n}$$

is identical to the equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-3}} a_x a_y a_w a_{x+1} a_{\phi_{i+2}} \cdots a_{\phi_n},$$

which we rewrite as

$$a_1 \cdots a_{x-1} (a_x a_y) a_y^{-1} a_{x+1} a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{i-3}} (a_x a_y) a_w a_{x+1} a_{\phi_{i+2}} \cdots a_{\phi_n}. \tag{16}$$

Again, the random variable a_y and its inverse a_y^{-1} appear in the same places in both Equations 15 and 16. The random variable $c = (a_x a_y)$ in Equation 16 plays the role of the random variable a_x in the Equation 15. The random variable a_{x+1} in Equation 16 plays the role of the random variable $b = (a_y a_{x+1})$ in Equation 15. Thus, Equations 15 and 16, up to renaming variables, are identical. This implies that they have the same number of solutions. This, in its turn, implies that

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

If $z \neq w$, then we rewrite the equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots a_w a_y a_{x+1} a_{\phi_{i+2}} \cdots a_{\phi_n}$$

as

$$a_1 \cdots a_{x-1} a_x a_y^{-1} (a_y a_{x+1}) a_{x+2} \cdots a_n = a_{\phi_1} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots a_w (a_y a_{x+1}) a_{\phi_{i+2}} \cdots a_{\phi_n}\,. \tag{17}$$

Similarly, we rewrite the equation

$$a_1 \cdots a_{x-1} a_x a_{x+1} a_{x+2} \cdots a_n = a_{\theta_1} \cdots a_{\theta_{j-1}} a_x a_y a_z a_{\theta_{j+3}} \cdots a_w a_{x+1} a_{\theta_{i+2}} \cdots a_{\theta_n}$$

as

$$a_1 \cdots a_{x-1} (a_x a_y) a_y^{-1} a_{x+1} a_{x+2} \cdots a_n = a_{\theta_1} \cdots a_{\theta_{j-1}} (a_x a_y) a_z a_{\theta_{j+3}} \cdots a_w a_{x+1} a_{\theta_{i+2}} \cdots a_{\theta_n}\,. \tag{18}$$

Comparison of Equations 17 and 18, shows that, similarly to Equations 13 and 14, and Equations 15 and 16, which we compared in detail above, a certain renaming of variables in Equation 18 transforms it into Equation 17. Thus, again

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Now, we consider the case when $x = \phi_0 = \theta_0 = 0$. In this case $y = \phi_i = \theta_1$, $z = \phi_1 = \theta_2$, $\phi_2 = \theta_3, \ldots, \phi_{i-1} = \theta_i = w$, $x + 1 = \phi_{i+1} = \theta_{i+1} = 1$, and $\phi_{i+2} = \theta_{i+2}, \ldots, \phi_n = \theta_n$. We rewrite the equation

$$a_1 a_2 \cdots a_n = a_z a_{\phi_2} \cdots a_{\phi_{i-2}} a_w a_y a_1 a_{\phi_{i+2}} \cdots a_{\phi_n}$$

as

$$(a_y a_1) a_2 \cdots a_n = a_y a_z a_{\phi_2} \cdots a_{\phi_{i-2}} a_w (a_y a_1) a_{\phi_{i+2}} \cdots a_{\phi_n}, \tag{19}$$

in which the random variable a_1 is omitted, and for each fixed value of a_y, as a_1 runs over all the elements of G, so does the random variable $b = (a_y a_1)$.

Now, compare Equation 19 with the equation

$$a_1 a_2 \cdots a_n = a_y a_z a_{\theta_3} \cdots a_{\theta_{i-1}} a_w a_1 a_{\theta_{i+2}} \cdots a_{\theta_n}. \tag{20}$$

Clearly, renaming $b = (a_y a_1)$ to a_1 turns Equation 19 to Equation 20. Thus, again

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Now we consider the case when $x = n$. In that case $x + 1 = 0 = \phi_0 = \theta_0$, $y = \phi_n$ and $w = \phi_{n-1} = \theta_n$. Observe, that in that case the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

is

$$a_1 a_2 \cdots a_n = a_{\phi_1} \cdots a_{\phi_{j-1}} a_n a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-2}} a_w a_y. \tag{21}$$

Similarly, the equation

$$a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}$$

in that case becomes

$$a_1 a_2 \cdots a_n = a_{\phi_1} \cdots a_{\phi_{j-1}} a_n a_y a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-2}} a_w,$$

which we rewrite as

$$a_1 a_2 \cdots (a_n a_y) = a_{\phi_1} \cdots a_{\phi_{j-1}} (a_n a_y) a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-2}} a_w a_y. \tag{22}$$

Again, the random variable $b = (a_n a_y)$ in Equation 22 plays the role of the random variable a_n in Equation 21. Thus, again

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Finally, we consider the case when $y = 0 = \phi_0 = \theta_0$. In this case $x+1 = \phi_1$ and $w = \phi_n$. Thus, the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

becomes

$$a_1 a_2 \cdots a_n = a_{x+1} a_{\phi_2} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-1}} a_w.$$

On the other hand, the equation

$$a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}$$

becomes

$$a_1 a_2 \cdots a_n = a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-1}} a_w a_{x+1} a_{\phi_2} \cdots a_{\phi_{j-1}} a_x.$$

Let

$$r = a_x, s = a_{x+1}, A = a_1 \cdots a_{x-1}, B = a_{x+2} a_{x+3} \cdots a_n, P = a_{\phi_2} \cdots a_{\phi_{j-1}},$$

and $Q = a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-1}} a_w$. Then

$$a_1 a_2 \cdots a_n = a_{x+1} a_{\phi_2} \cdots a_{\phi_{j-1}} a_x a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-1}} a_w$$

becomes

$$ArsB = sPrQ,$$

and

$$a_1 a_2 \cdots a_n = a_z a_{\phi_{j+2}} \cdots a_{\phi_{n-1}} a_w a_{x+1} a_{\phi_2} \cdots a_{\phi_{j-1}} a_x$$

becomes

$$ArsB = QsPr.$$

But $\Pr(ArsB = sPrQ)$ is the same as $\Pr(rArsB = rsPrQ)$, which is the same as $\Pr(\gamma A\theta B = \theta P\gamma Q)$, where $\gamma = r, \theta = rs$, which, in its turn, is the same as $\Pr(\gamma A\theta BQ^{-1}\gamma^{-1} = \theta P)$. Notice that since the random element s does not appear in the last equation, we regard $\theta = rs$ as a random element from G. And $\gamma A\theta BQ^{-1}\gamma^{-1} = \theta P$ is equivalent to saying that $A\theta BQ^{-1}$ is conjugate to θP.

Similarly, $\Pr(ArsB = QsPr)$ is the same as $\Pr(ArsBs = QsPrs)$, which is the same as $\Pr(A\theta B\gamma = Q\gamma P\theta)$, where $\gamma = s, \theta = rs$, which, in turn, is the same as $\Pr(\gamma^{-1}Q^{-1}A\theta B\gamma = P\theta)$. Again, we regard $\theta = rs$ as a random element from G. And $\gamma^{-1}Q^{-1}A\theta B\gamma = P\theta$ is equivalent to saying that $Q^{-1}A\theta B$ is conjugate to $P\theta$.

Finally, notice that $\theta P = \theta(P\theta)\theta^{-1}$ is conjugate to $P\theta$, and $A\theta BQ^{-1} = Q(Q^{-1}A\theta B)Q{-}1$ is conjugate to $Q^{-1}A\theta B$. Thus, $A\theta BQ^{-1}$ is conjugate to θP if and only if $Q^{-1}A\theta B$ is conjugate to $P\theta$. Thus,

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

$\square$

4.2 Cyclic operation

Now we define and discuss $x--y$ cyclic operation. This material is illustrated by Lemma 22 above. Let $\phi \in S_n$ be a permutation such that $\phi^\bullet \in S(1+n)$ contains some $(x+1) \to y \to x$. In other words, for some $0 \le i \le n$, we have $\phi_i = x$, $\phi_{i+1} = y$, and $\phi_{i+2} = y$. Notice that if $x = n$, the condition $(x+1) \to y \to x$ becomes
$0 = \phi_0 \to y = \phi_n \to n = \phi_{n-1}$.

Definition 44. The $x--y$ cyclic operation on the permutation ϕ is defined as follows

- If $y = x+2$, then the $x--y$ cyclic operation does not do anything to ϕ;
- If $y > x+2$, then in the long cycle $\phi^\bullet$ we replace $x+1$ by $y-1$ and replace each $t = x+2, \ldots, y-1$ by $t-1$. In other words, the $x--y$ cyclic operation changes $\phi^\bullet$ to
$$(y-1, y-2, \ldots, x+2, x+1)^{-1} \cdot \phi^\bullet \cdot (y-1, y-2, \ldots, x+2, x+1) = \phi^{\bullet(y-1,y-2,\ldots,x+2,x+1)};$$
- If $y = x-1$, then the $x--y$ cyclic operation does not do anything to ϕ;
- If $y < x-1$, then in the long cycle $\phi^\bullet$ we replace x by $y+1$ and replace each $t = y+1, \ldots, x-1$ by $t+1$. In other words, the $x--y$ cyclic operation changes $\phi^\bullet$ to
$$(y+1, y+2, \ldots, x-1, x)^{-1} \cdot \phi^\bullet \cdot (y+1, y+2, \ldots, x-1, x) = \phi^{\bullet(y+1,y+2,\ldots,x-1,x)}.$$

Since we can easily restore any permutation $\theta \in S_n$ from its corresponding long cycle $\theta^\bullet \in S(1+n)$, Definition 44 unambiguously describes what an $x--y$ cyclic operation does to a permutation $\phi \in S_n$. The fact that an $x--y$ cyclic operation always produces a long cycle in $S(1+n)$, is straightforward from the definition.

The requirement that $\phi^\bullet \in S(1+n)$ must contain $(x+1) \to y \to x$, implies that the permutation $\phi^\circ = \phi^\bullet \cdot (0, 1, \ldots, n)$ has a cycle that contains
$(x \mapsto y) = (x \dashrightarrow x+1 \to y)$, and a cycle that contains $(y-1 \mapsto x) = (y-1 \dashrightarrow y \to x)$. Thus, ϕ° has a cycle, which contains $y-1 \mapsto x \mapsto y$.

Let us consider several examples of $x--y$ cyclic operations.

Example 45. Let $\phi = \langle 6\ \ 5\ \ 3\ \ 1\ \ 4\ \ 2 \rangle$. Then $\phi^\bullet = (0, 2, 4, 1, 3, 5, 6)$. We can perform a $1--4$ cyclic operation on ϕ to obtain a new permutation θ. Since $y = 4 > x+1 = 2$, we get $\theta^\bullet = (0, 3, 4, 1, 2, 5, 6)$. Hence, $\theta = \langle 6\ \ 5\ \ 2\ \ 1\ \ 4\ \ 3 \rangle$.

Example 46. Let $\phi = \langle 4\ \ 1\ \ 5\ \ 2\ \ 6\ \ 3 \rangle$. Then $\phi^\bullet = (0, 3, 6, 2, 5, 1, 4)$. We can perform a $5--2$ cyclic operation on ϕ to obtain a new permutation θ. Since $y = 2 < x = 5$, we get $\theta^\bullet = (0, 4, 6, 2, 3, 1, 5)$. Hence, $\theta = \langle 5\ \ 1\ \ 3\ \ 2\ \ 6\ \ 4 \rangle$.

Example 47. Let $\phi = \langle 4\ \ 1\ \ 5\ \ 2\ \ 6\ \ 3 \rangle$. Then $\phi^\bullet = (0, 3, 6, 2, 5, 1, 4)$. We can perform a $0--4$ cyclic operation on ϕ to obtain a new permutation θ. Since $y = 4 > x+1 = 1$, we get $\theta^\bullet = (0, 2, 6, 1, 5, 3, 4)$. Hence, $\theta = \langle 4\ \ 3\ \ 5\ \ 1\ \ 6\ \ 2 \rangle$.

Example 48. Let $\phi = \langle 4 \ \ 1 \ \ 5 \ \ 2 \ \ 6 \ \ 3 \rangle$. Then $\phi^\bullet = (0, 3, 6, 2, 5, 1, 4)$. We can perform a $6 - -3$ cyclic operation on ϕ to obtain a new permutation θ. Since $y = 3 < x = 6$, we get $\theta^\bullet = (0, 3, 4, 2, 6, 1, 5)$. Hence, $\theta = \langle 4 \ \ 3 \ \ 5 \ \ 1 \ \ 6 \ \ 2 \rangle$.

Example 49. Let $\phi = \langle 4 \ \ 1 \ \ 5 \ \ 2 \ \ 6 \ \ 3 \rangle$. Then $\phi^\bullet = (0, 3, 6, 2, 5, 1, 4)$. We can perform a $3 - -0$ cyclic operation on ϕ to obtain a new permutation θ. Since $y = 0 < x = 3$, we get $\theta^\bullet = (0, 1, 6, 3, 5, 2, 4)$. Hence, $\theta = \langle 4 \ \ 2 \ \ 5 \ \ 3 \ \ 6 \ \ 1 \rangle$.

We now describe the transformation of ϕ° under an $x - -y$ cyclic operation. First, write ϕ° in the cyclic notation. Let ϕ° consist of k cycles $C_1, \ldots, C_k$ of lengths $h_1, \ldots, h_k$, respectively. We think of these cycles as consisting of boxes

$$C_1 = B_{1,1} \mapsto B_{1,2} \mapsto \cdots B_{1,h_1} \mapsto B_{1,1}, \ldots, C_k = B_{k,1} \mapsto B_{k,2} \mapsto \cdots B_{k,h_k} \mapsto B_{k,1}.$$

Each box in each cycle contains inside it one element of ϕ°. Let $B_{k(z),h(z)}$ denotes the box that contains it for every element $z \in \phi^\circ$. The requirement that $\phi^\bullet$ contains $(x+1) \to y \to x$, asserts that $k(y-1) = k(x) = k(y)$ and $h(y-1) + 2 = h(x) + 1 = h(y)$. Let $|B_{i,j}|$ denote its content for each box $B_{i,j}$. We now fix the labeling of the boxes and start transforming their contents. At any stage of the transformation, we permit the boxes to contain a single element, two elements $z_1 \mapsto z_2$ with an arrow between them, or no elements. The last case, namely that of a box with no elements in it, we permit only in a cycle in which at least one of its remaining boxes is not empty. When we read a cycle, we treat an empty box as if it, together with the arrow following it, are deleted. Thus, we regard a cycle containing an empty box as if the arrow $\mapsto$ goes directly from the content of the first nonempty box before the empty one, to the content of the first nonempty box following the empty one.

Lemma 50. *Let $\theta \in S_n$ be obtained from $\phi \in S_n$ by an $x - -y$ cyclic operation. Then the $x - -y$ cyclic operation transforms ϕ° to θ° as follows*

- *If $y = x + 2$ or $y = x - 1$, then $\theta^\circ = \phi^\circ$;*
- *If $y > x + 2$, then perform the following steps*
  1. *Inside the box $B_{k(x+1),h(x+1)}$ replace $x + 1$ by $y - 1 \mapsto x$. In other words, in the cycle $C_{k(x+1)}$, the piece $|B_{k(x+1),h(x+1)-1}| \mapsto x + 1 \mapsto |B_{k(x+1),h(x+1)+1}|$ becomes $|B_{k(x+1),h(x+1)-1}| \mapsto y - 1 \mapsto x \mapsto |B_{k(x+1),h(x+1)+1}|$;*
  2. *Inside each box $B_{k(t),h(t)}$, for all $t = x + 2, \ldots, y - 1$, replace t by $t - 1$;*
  3. *Delete the element x from the box $B_{k(x),h(x)}$. The box $B_{k(x),h(x)}$ is now empty. Notice that the box before $B_{k(x),h(x)}$ is $B_{k(y-1),h(y-1)}$, and it now contains $y-2$. The box after $B_{k(x),h(x)}$ is $B_{k(y),h(y)}$, and it still contains y. Thus, we obtain $y - 2 \mapsto y$ in the cycle $C_{k(x)}$.*
- *If $y < x - 1$, then perform the following steps*

1. *Inside the box* $B_{k(x-1),h(x-1)}$ *replace* $x-1$ *by* $x \mapsto y$. *In other words, in the cycle* $C_{k(x-1)}$, *the piece* $|B_{k(x-1),h(x-1)-1}| \mapsto x-1 \mapsto |B_{k(x-1),h(x-1)+1}|$ *becomes* $|B_{k(x-1),h(x-1)-1}| \mapsto x \mapsto y \mapsto |B_{k(x-1),h(x-1)+1}|$;
2. *Inside each box* $B_{k(t),h(t)}$, *for all* $t = y, \ldots, x-2$, *replace* t *by* $t+1$;
3. *Delete the element* x *from the box* $B_{k(x),h(x)}$. *The box* $B_{k(x),h(x)}$ *is now empty. Notice that the box before* $B_{k(x),h(x)}$ *is* $B_{k(y-1),h(y-1)}$, *and it still contains* $y-1$. *The box after* $B_{k(x),h(x)}$ *is* $B_{k(y),h(y)}$, *and it now contains* $y+1$. *Thus, we obtain* $y-1 \mapsto y+1$ *in the cycle* $C_{k(x)}$.

In particular, the number of cycles in the cyclic decompositions of θ° *and of* ϕ° *is the same.*

Proof. We start by investigating the effect of replacements of elements in $\phi^\bullet$ on ϕ°. First, notice that when in a piece $c \to a \to d$ we replace an element a by an element b, b replaces a in two black arrows – in the beginning of the black arrow $a \to d$, and also the end of the black arrow $c \to a$. We study these two replacements separately.

- The replacement of a by b in the end of the black arrow $\to a$ transforms $(c-1) \dashrightarrow c \to a$, which, in ϕ°, is the arrow $(c-1) \mapsto a$, to $(c-1) \dashrightarrow c \to b$, which is $(c-1) \mapsto b$. To indicate that b element of ϕ° is post the replacement of a by b in $\to a$, we mark it as $\acute{b}$. Thus, we say that the replacement of $c \to a$ by $c \to \acute{b}$ transforms $(c-1) \dashrightarrow c \to a$, which is $(c-1) \mapsto a$ to $(c-1) \dashrightarrow c \to \acute{b}$, which is $(c-1) \mapsto \acute{b}$. From $\acute{b}$ we draw a grey arrow $\acute{b} \dashrightarrow (b+1)$. If, at this point, the original element b of $\phi^\bullet$ is still not replaced in $\to b$, we regard that original b as deleted, and do not use it in any further replacements, marking, or arrow-drawing, except the future replacement of b in $\to b$, which eliminates that original b;

- The replacement of a by b in the beginning of the black arrow $a \to$ transforms $(a-1) \dashrightarrow a \to d$, which, in ϕ°, is the arrow $(a-1) \mapsto d$, to $(b-1) \dashrightarrow b \to d$, which is $(b-1) \mapsto d$. To indicate that b element of ϕ° is post the replacement of a by b in $a \to$, we mark it as $\ddot{b}$. Since this replacement replaces $(a-1)$ in $(a-1) \mapsto$ of ϕ° by $(b-1)$, we also mark $(b-1)$ as $(\grave{b-1})$. Thus, we say that the replacement of $a \to d$ by $\ddot{b} \to d$ transforms $(a-1) \dashrightarrow a \to d$, which is $(a-1) \mapsto d$, to $(\grave{b-1}) \dashrightarrow \ddot{b} \to d$, which is $(\grave{b-1}) \mapsto d$. If, at this point, the original element b of $\phi^\bullet$ is still not replaced in $b \to$, we regard that original b as deleted, and do not use it in any further replacements, marking, or arrow-drawing, except the future replacement of b in $b \to$, which eliminates that original b;

- If we need to mark b as both $\acute{b}$ and $\grave{b}$, we write $\hat{b}$;

- If we need to mark b as both $\acute{b}$ and $\ddot{b}$, we write $\vec{b}$;

- If we need to mark b as both $\grave{b}$ and $\ddot{b}$, we write $\tilde{b}$;

- If we need to mark b as $\acute{b}$ and $\grave{b}$ and $\ddot{b}$, we write $\breve{b}$.

Notice that our notation permits us to study the effect of replacements of elements in $\phi^\bullet$ on ϕ° in several steps. Namely, if we have to replace elements $a_1, \ldots, a_m$ by elements $b_1, \ldots, b_m$, we do not have to perform all the $2m$ replacements in the black arrows at once. Instead, we can perform these $2m$ replacements in several steps, each time marking the elements as described above. The final ϕ°, after we perform all the $2m$ replacements, will be the same, regardless of the selection of intermediate steps. Now we are ready to start our investigation

If $y > x+2$, then the $x--y$ cyclic operation, applied to $\phi^\bullet$, replaces $x+1$ by $y-1$, and replaces each t, for $t = x+2, \ldots, y-1$, by $t-1$. Thus, $y \to x$ remains untouched by the $x--y$ cyclic operation. This implies that θ° contains $y-1 \mapsto x$. Notice that our marking notation implies that after all the replacements in $\phi^\bullet$, $\phi^\bullet$ will contain $\grave{x}$ instead of x and $\breve{t}$ instead of t, for all $t = x+1, \ldots, y-2$, and $(y \vec{-} 1)$ instead of $(y-1)$. Altogether, we need to perform $2(y-x-1)$ replacements in the black arrows of $\phi^\bullet$.

At the first step, we perform the following four replacements

1. Replacement of $(x+2)$ by $(x \ddot{+} 1)$ in the black arrow $(x+2) \to$. This changes x to $\grave{x}$;
2. Replacement of $(x+1)$ by $(y \vec{-} 1)$ in the black arrows $\to (x+1)$ and $(x+1) \to$. This changes $(y-2)$ to $(y \grave{-} 2)$;
3. Replacement of $(y-1)$ by $(y \hat{-} 2)$ in the arrow $\to (y-1)$.

If ϕ° contains $(x+1) \mapsto (y-1)$, then, according to our notation, the original $\phi^\bullet$ takes $u = |B_{k(x+1),h(x+1)-1}| + 1$ to $x+1$. Indeed, in the original ϕ° we must have an alternating path

$$(u-1) \dashrightarrow u \to (x+1) \dashrightarrow (x+2) \to (y-1) \dashrightarrow y \to x \dashrightarrow (x+1) \to y, \qquad (23)$$

which is

$$(u-1) \mapsto (x+1) \mapsto (y-1) \mapsto x \mapsto y.$$

The four replacements of our first step transform Equation 23 to

$$(u-1) \dashrightarrow u \to (y \vec{-} 1) \dashrightarrow y \to \grave{x} \dashrightarrow (x \ddot{+} 1) \to (y \hat{-} 2) \dashrightarrow (y \vec{-} 1) \to y, \qquad (24)$$

which is

$$(u-1) \mapsto (y \vec{-} 1) \mapsto \grave{x} \mapsto (y \hat{-} 2) \mapsto y.$$

Notice that all four replacements in the black arrows appear in path 24. Thus, these four replacements correspond to the replacement of $x+1$ by $(y \vec{-} 1) \mapsto \grave{x}$ inside the box $B_{k(x+1),h(x+1)}$, deletion of x from the box $B_{k(x),h(x)}$, and replacement of $y-1$ by $(y \hat{-} 2)$ in the box $B_{k(y-1),h(y-1)}$.

If ϕ° does not contain $(x+1) \mapsto (y-1)$ then, according to our notation, the original $\phi^\bullet$ takes $u = \left|B_{k(x+1),h(x+1)-1}\right| + 1$ to $x+1$, takes $x+2$ to $v = |B_{k(x+1),h(x+1)+1}|$, and takes $p = \left|B_{k(y-1),h(y-1)-1} + 1\right|$ to $(y-1)$. Indeed, in the original ϕ° we must have an alternating path

$$(u-1) \dashrightarrow u \to (x+1) \dashrightarrow (x+2) \to v, \tag{25}$$

which is

$$(u-1) \mapsto (x+1) \mapsto v,$$

and an alternative path

$$(p-1) \dashrightarrow p \to\to (y-1) \dashrightarrow y \to x \dashrightarrow (x+1) \to y, \tag{26}$$

which is

$$(p-1) \mapsto (y-1) \mapsto x \mapsto y.$$

The four replacements of the first step transform path 25 to

$$(u-1) \dashrightarrow u \to (y \vec{-} 1) \dashrightarrow y \to \grave{x} \dashrightarrow (x \ddot{+} 1) \to v, \tag{27}$$

which is

$$(u-1) \mapsto (y \vec{-} 1) \mapsto \grave{x} \mapsto v,$$

and transforms path 26 to

$$(p-1) \dashrightarrow p \to (y \hat{-} 2) \dashrightarrow (y \vec{-} 1) \to y, \tag{28}$$

which is

$$(p-1) \mapsto (y \hat{-} 2) \mapsto y.$$

Notice that all four replacements in the black arrows appear in paths 27 and 28. Thus, these four replacements correspond to the replacement of $x+1$ by $y \vec{-} 1 \mapsto \grave{x}$ inside the box $B_{k(x+1),h(x+1)}$, deletion of x from the box $B_{k(x),h(x)}$, and replacement of $y-1$ by $(y \hat{-} 2)$ in the box $B_{k(y-1),h(y-1)}$.

At the second step, we perform the following two replacements

1. Replacement of $(x+2)$ by $(x \vec{+} 1)$ in the black arrow $\to (x+2)$;

2. Replacement of $(x+3)$ by $(x \ddot{+} 2)$ in the black arrow $(x+3) \to$. This changes $(x \vec{+} 1)$ to $(x \check{+} 1)$;

According to our notation, $\phi^\bullet$, modified by the first step, takes $u = |B_{k(x+2),h(x+2)-1}| + 1$ to $x+2$ and takes $x+2$ to $v = |B_{k(x+2),h(x+2)+1}|$. Indeed, after the first step, in ϕ° we must have an alternating path

$$(u-1) \dashrightarrow u \to (x+2) \dashrightarrow (x+3) \to v, \tag{29}$$

which is
$$(u-1) \mapsto (x+2) \mapsto v.$$

The two replacements of the second step transform path 29 to
$$(u-1) \dashrightarrow u \rightarrow (x \check{+} 1) \dashrightarrow (x \ddot{+} 2) \rightarrow v, \tag{30}$$
which is
$$(u-1) \mapsto (x \check{+} 1) \mapsto v.$$

Notice that both replacements in the black arrows appear in path 30. Thus, these two replacements correspond to the replacement of $x+2$ by $(x \check{+} 1)$ inside the box $B_{k(x+2),h(x+2)}$.

At the third step, we perform the following two replacements

1. Replacement of $(x+3)$ by $(x \vec{+} 2)$ in the black arrow $\rightarrow (x+3)$;

2. Replacement of $(x+4)$ by $(x \ddot{+} 3)$ in the black arrow $(x+4) \rightarrow$. This changes $(x \vec{+} 2)$ to $(x \check{+} 2)$;

According to our notation, $\phi^{\bullet}$, modified by the first and second steps, takes $u = |B_{k(x+3),h(x+3)-1}| + 1$ to $x+3$ and takes $x+3$ to $v = |B_{k(x+3),h(x+3)+1}|$. Indeed, after the second step, in ϕ° we must have an alternating path
$$(u-1) \dashrightarrow u \rightarrow (x+3) \dashrightarrow (x+4) \rightarrow v, \tag{31}$$
which is
$$(u-1) \mapsto (x+3) \mapsto v.$$

The two replacements of the third step transform path 31 to
$$(u-1) \dashrightarrow u \rightarrow (x \check{+} 2) \dashrightarrow (x \ddot{+} 3) \rightarrow v, \tag{32}$$
which is
$$(u-1) \mapsto (x \check{+} 2) \mapsto v.$$

Notice that both replacements in the black arrows appear in path 32. Thus, these two replacements correspond to the replacement of $x+3$ by $(x \check{+} 2)$ inside the box $B_{k(x+3),h(x+3)}$.

We continue that way until **at the last step** we perform the following two replacements

1. Replacement of $(y \grave{-} 2)$ by $(y \vec{-} 3)$ in the black arrow $\rightarrow (y-2)$;

2. Replacement of $(y-1)$ by $(y \check{-} 2)$ in the black arrow $(y-1) \rightarrow$. This changes $(y \vec{-} 3)$ to $y \check{-} 3)$;

According to our notation, $\phi^{\bullet}$, modified by all the previous steps, takes $u = |B_{k(y-2),h(y-2)-1}| + 1$ to $(y \grave{-} 2)$ and takes $y-1$ to $v = |B_{k(y-2),h(y-2)+1}|$. Indeed, after the previous step, in ϕ° we must have an alternating path

$$(u-1) \dashrightarrow u \rightarrow (y \grave{-} 2) \dashrightarrow (y-1) \rightarrow v, \tag{33}$$

which is

$$(u-1) \mapsto (y \grave{-} 2) \mapsto v.$$

The two replacements of the last step transform path 33 to

$$(u-1) \dashrightarrow u \rightarrow (y \check{-} 3) \dashrightarrow (y \check{-} 2) \rightarrow v, \tag{34}$$

which is

$$(u-1) \mapsto (y \check{-} 3) \mapsto v.$$

Notice that both replacements in the black arrows appear in path 34. Thus, these two replacements correspond to the replacement of $y \grave{-} 2$ by $y \check{-} 3$ inside the box $B_{k(y-2),h(y-2)}$, and to change of $(y \hat{-} 2)$ in the box $B_{k(y-1),h(y-1)}$ to $(y \check{-} 2)$.

At this point, we performed all the $2(y-x-1)$ replacements in the black arrows of $\phi^{\bullet}$. Our marking notation makes it easy to verify that all the required replacements in $\phi^{\bullet}$ were performed correctly. Thus the lemma is proved for $y > x+2$. The proof for $y < x-1$ is done in a similar way, by using the same marking notation and performing the replacements in steps. $\square$

Definition 51. We say that the permutations $\phi, \theta \in S_n$ are in the same "$x--y$ cyclic orbit" if there exist some permutations $\tau_1, \ldots, \tau_k \in S_n$ such that $\tau_1 = \phi$, $\tau_k = \theta$, and, for each $i = 1, \ldots, k-1$, either τ_i can be obtained from τ_{i+1} by an $x--y$ cyclic operation or τ_{i+1} can be obtained from τ_i by an $x--y$ cyclic operation.

Notice that according to Definition 51, $\phi, \theta \in S_n$ can be in the same $x--y$ exchange orbit, while neither of them can be obtained from the other one by performing $x--y$ cyclic operations.

Theorem 52. *Let $\phi, \theta \in S_n$ be two permutations such that θ is obtained from ϕ by an $x--y$ cyclic operation. Then*

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Proof. We consider four different possible cases, and prove the theorem for each of them

Case 1 is when $x \neq 0, n$ and $y \neq 0$. In this case, there exists some k, $1 \leq k \leq n-2$, such that $\phi_k = x$, $\phi_{k+1} = y$, and $\phi_{k+2} = x+1$. Hence, the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

is of the form

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_{k-1}} a_x a_y a_{x+1} a_{\phi_{k+3}} \cdots a_{\phi_n} \tag{35}$$

If $y > x$, then Equation 35 is equivalent to

$$a_1 \cdots (a_x a_{x+1}) \cdots a_y \cdots a_n = a_{\phi_1} \cdots a_{\phi_{k-1}} (a_x a_{x+1})(a_{x+1}^{-1} a_y a_{x+1}) a_{\phi_{k+3}} \cdots a_{\phi_n}. \tag{36}$$

We define

- $b_t = a_t$ for all $t < x$ and $t > y$;
- $b_x = a_x a_{x+1}$;
- $b_t = a_{t+1}$ for all $x + 1 < t < y - 1$;
- $b_{y-1} = a_{x+1}$;
- $b_y = a_{x+1}^{-1} a_y$.

Next, $b_{y-1} = a_{x+1}$ and $b_y = a_{x+1}^{-1} a_y$ imply

- $b_{y-1} b_y = a_y$;
- $b_y b_{y-1} = a_{x+1}^{-1} a_y a_{x+1}$.

As random variables $a_1, \ldots, a_n$ run over all elements of G, so do random elements $b_1, \ldots, b_n$. Now, the Equation 36 is equivalent to the equation

$$b_1 b_2 \cdots b_n = b_{\theta_1} b_{\theta_2} \cdots b_{\theta_{k-1}} b_x b_y b_{y-1} b_{\theta_{k+3}} \cdots b_{\theta_n}, \tag{37}$$

where

- $\theta_t = \phi_t$ for all such t, for which $1 \le \phi_t \le x$ or $y \le \phi_t \le n$;
- $\theta_t = y - 1$ for the t, for which $\phi_t = x + 1$;
- $\theta_t = \phi_t - 1$ for all such t, for which $x + 1 < \phi_t < y$.

This proves the theorem for the subcase $y > x$ of the first case.

If $y < x$, then Equation 35 is equivalent to

$$a_1 \cdots a_y \cdots (a_x a_{x+1}) \cdots a_n = a_{\phi_1} \cdots a_{\phi_{k-1}} (a_x a_y a_x^{-1})(a_x a_{x+1}) a_{\phi_{k+3}} \cdots a_{\phi_n}. \tag{38}$$

We define

- $b_t = a_t$ for all $t < y$ and $t > x + 1$;
- $b_{x+1} = a_x a_{x+1}$;
- $b_t = a_{t-1}$ for all $y + 1 < t < x$;

- $b_{y+1} = a_x$;
- $b_y = a_y a_{x+1}^{-1}$.

Next, $b_{y+1} = a_x$ and $b_y = a_y a_{x+1}^{-1}$ imply

- $b_y b_{y+1} = a_y$;
- $b_{y+1} b_y = a_x a_y a_x^{-1}$.

As random variables $a_1, \ldots, a_n$ run over all elements of G, so do random elements $b_1, \ldots, b_n$. Now, Equation 38 is equivalent to the equation

$$b_1 b_2 \cdots b_n = b_{\theta_1} b_{\theta_2} \cdots b_{\theta_{k-1}} b_{y+1} b_y b_{x+1} b_{\theta_{k+3}} \cdots b_{\theta_n}, \tag{39}$$

where

- $\theta_t = \phi_t$ for all such t, for which $1 \leq \phi_t \leq x$ or $x+1 \leq \phi_t \leq n$;
- $\theta_t = y+1$ for the t, for which $\phi_t = x$;
- $\theta_t = \phi_t + 1$ for all such t, for which $y < \phi_t < x$.

This proves the theorem for the subcase $y < x$ of the first case.

Case 2 is when $x = 0 = \phi_0$. In this case, $\phi_1 = y$ and $\phi_2 = 1$. Hence, the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

is of the form

$$a_1 a_2 \cdots a_n = a_y a_1 a_{\phi_3} \cdots a_{\phi_n} \tag{40}$$

Multiplying Equation 40 from the left by a_1^{-1} gives us

$$a_2 \cdots a_n = (a_1^{-1} a_y a_1) a_{\phi_3} \cdots a_{\phi_n} \tag{41}$$

We define

- $b_t = a_t$ for all $t > y$;
- $b_t = a_{t+1}$ for all $1 \leq t < y-1$;
- $b_{y-1} = a_1$;
- $b_y = a_1^{-1} a_y$.

Next, $b_{y-1} = a_1$ and $b_y = a_1^{-1} a_y$ imply

- $b_{y-1} b_y = a_y$;

- $b_y b_{y-1} = a_1^{-1} a_y a_1$.

As random variables $a_1, \ldots, a_n$ run over all elements of G, so do random elements $b_1, \ldots, b_n$.

Now, Equation 41 is equivalent to the equation

$$b_1 \cdots b_n = b_y b_{y-1} b_{\theta_3} \cdots b_{\theta_n}, \tag{42}$$

where

- $\theta_t = \phi_t$ for all such t, for which $\phi_t \geq y$;
- $\theta_t = y - 1$ for the t, for which $\phi_t = 1$;
- $\theta_t = \phi_t - 1$ for all such t, for which $2 \leq \phi_t \leq y - 1$.

This proves the theorem for the second case.

Case 3 is when $x = n$. In this case, $x + 1 = 0 = \phi_0$, $\phi_n = y$ and $\phi_{n-1} = x = n$. Hence, the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

is of the form

$$a_1 a_2 \cdots a_n = a_{\phi_1} \cdots a_{\phi_{n-2}} a_n a_y \tag{43}$$

We apply the inverse map $inv(g) = g^{-1}$ to both sides of Equation 43 and obtain

$$a_n^{-1} a_{n-1}^{-1} \cdots a_1^{-1} = a_y^{-1} a_n^{-1} a_{\phi_{n-2}}^{-1} \cdots a_{\phi_1}^{-1} \tag{44}$$

Define $c_{n+1-i} = a_i^{-1}$ and $\phi'_i = n + 1 - \phi_{n+1-i}$, for all $i = 1, \ldots, n$. Define $x' = 0$ and $y' = n + 1 - y$. Then Equation 44 becomes

$$c_1 c_2 \cdots c_n = c_{\phi'_1} c_{\phi'_2} \cdots c_{\phi'_n}, \tag{45}$$

in which $\phi'_1 = y'$ and $\phi'_2 = 1$. We apply $x' - -y'$ cyclic operation to ϕ'. In the study of Case 2, above, we showed that Equation 45 is equivalent to the equation

$$b_1 \cdots b_n = b_{y'} b_{y'-1} b_{\theta'_3} \cdots b_{\theta'_n}, \tag{46}$$

where

- $\theta'_t = \phi'_t = n + 1 - \phi_{n+1-t}$ for all such t, for which $n + 1 - \phi_{n+1-t} = \phi'_t \geq y' = n + 1 - y$;
- $\theta'_t = y' - 1 = n - y$ for the t, for which $n + 1 - \phi_{n+1-t} = \phi'_t = 1$;
- $\theta'_t = \phi'_t - 1 = n - \phi_{n+1-t}$ for all such t, for which $2 \leq n + 1 - \phi_{n+1-t} = \phi'_t \leq y' - 1 = n - y$.

Next, we apply the inverse map $inv(g) = g^{-1}$ to both sides of the Equation 46 and obtain

$$b_n^{-1} \cdots b_1^{-1} = b_{\theta'_n}^{-1} \cdots \theta'_3 - 1 b_{y'-1}^{-1} b_{y'}^{-1}. \tag{47}$$

Define $d_{n+1-i} = b_i^{-1}$ and $\theta_i = n + 1 - \theta'_{n+1-i}$, for all $i = 1, \ldots, n$. Then the Equation 47 becomes

$$d_1 \cdots d_n = d_{\theta_1} b_{\theta_2} \cdots d_{\theta_{n-2}}, d_{y-1} d_y. \tag{48}$$

Here

- $\theta_t = n+1-\theta'_{n+1-t} = n+1-\phi'_{n+1-t} = \phi_t$ for all such t, for which $\phi_t = n+1-\phi'_{n+1-t} \leq n+1-y' = y$;
- $\theta_t = n+1-\theta'_{n+1-t} = n+1-(n-y) = y+1$ the t, for which $\phi_t = n+1-\phi'_{n+1-t} = n+1-1 = n$;
- $\theta_t = n+1-\theta'_{n+1-t} = n+1-(\phi'_{n+1-t}-1) = \phi_t+1$ for $y+1 = n+1-(n-y) \leq \phi_t = n+1-\phi'_{n+1-t} \leq n+1-2 = n-1$.

This proves the theorem for Case 3.

Case 4 is when $y = 0 = \phi_0$. In this case, $\phi_1 = x+1$ and $\phi_n = x$. Hence, the equation

$$a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}$$

is of the form

$$a_1 a_2 \cdots a_n = a_{x+1} a_{\phi_2} \cdots a_{\phi_{n-1}} a_x \tag{49}$$

Multiplying Equation 49 on the left by a_x gives us

$$a_x a_1 a_2 \cdots a_{x-1} (a_x a_{x+1}) \cdots a_n = (a_x a_{x+1}) a_{\phi_2} \cdots a_{\phi_{n-1}} a_x \tag{50}$$

We define

- $b_t = a_t$ for all $t > x+1$;
- $b_{x+1} = a_x a_{x+1}$
- $b_t = a_{t-1}$ for all $1 < t \leq x$;
- $b_1 = a_x$.

As random variables $a_1, \ldots, a_n$ run over all elements of G, so do random elements $b_1, \ldots, b_n$. Finally, the Equation 50 is equivalent to the equation

$$b_1 \cdots b_n = b_{x+1} b_{\theta_2} \cdots b_{\theta_{n-1}} b_1, \tag{51}$$

where

- $\theta_t = \phi_t$ for all such t, for which $\phi_t > x$;
- $\theta_t = 1$ for the t, for which $\phi_t = x$;
- $\theta_t = \phi_t + 1$ for all such t, for which $1 \leq \phi_t < x$.

This proves our theorem for Case 4. $\square$

4.3 Main results

Definition 53. Two permutations $\phi, \theta \in S_n$ are called "$x - -y$ equivalent" if there exist some permutations $\phi = \tau_1, \ldots, \theta = \tau_k \in S_n$ such that τ_i and τ_{i+1}, for each $i = 1, \ldots, k-1$, are in the same $x - -y$ exchange orbit or in the same $x - -y$ cyclic orbit.

Theorem 54. *If θ and ϕ are $x - -y$ equivalent, then $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ have the same number of alternating cycles.*

Proof. Since θ and ϕ are $x - -y$ equivalent, there exist some permutations $\phi = \tau_1, \ldots, \theta = \tau_k \in S_n$ such that τ_i and τ_{i+1}, for each $i = 1, \ldots, k-1$, are in the same $x - -y$ exchange orbit or in the same $x - -y$ cyclic orbit. For each $t = 1, \ldots, k-1$, if τ_i and τ_{i+1} are in the same $x - -y$ exchange orbit, then, by Lemma 41, $\mathrm{Gr}(\tau_i)$ and $\mathrm{Gr}(\tau_{i+1})$ have the same number of alternating cycles. Else, if τ_i and τ_{i+1} are in the same $x - -y$ cyclic orbit, then, by Lemma 41, τ_i° and τ_{i+1}° have the same number of cycles in their cyclic decompositions. Now, Theorem 31 asserts, that $\mathrm{Gr}(\tau_i)$ and $\mathrm{Gr}(\tau_{i+1})$ have the same number of alternating cycles. Hence, $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ have the same number of alternating cycles. $\square$

Theorem 55. *If θ and ϕ are $x - -y$ equivalent, then*

$$\Pr(a_1 a_2 \cdots a_n = a_{\phi_1} a_{\phi_2} \cdots a_{\phi_n}) = \Pr(a_1 a_2 \cdots a_n = a_{\theta_1} a_{\theta_2} \cdots a_{\theta_n}).$$

Proof. Since θ and ϕ are $x - -y$ equivalent, there exist some permutations $\phi = \tau_1, \ldots, \theta = \tau_k \in S_n$ such that τ_i and τ_{i+1}, for each $i = 1, \ldots, k-1$, are in the same $x - -y$ exchange orbit or in the same $x - -y$ cyclic orbit. For each $t = 1, \ldots, k-1$, if τ_i and τ_{i+1} are in the same $x - -y$ exchange orbit, then, by Theorem 43, $\Pr_{\tau_i}(G) = \Pr_{\tau_{i+1}}(G)$. Else, if τ_i and τ_{i+1} are in the same $x - -y$ cyclic orbit, then, by Theorem 52, $\Pr_{\tau_i}(G) = \Pr_{\tau_{i+1}}(G)$. $\square$

At this point, we proceed to show that in a finite non-Abelian group G two permutation equalities have the same probability if, and only if, their permutations have the same number of alternating cycles. The "only if" part implies that every finite non-Abelian group G is generic. This part immediately follows from a stronger result, stated in Theorem 6.8 due to Das and Nath [10].

Theorem 56 (Theorem 6.8 of Das and Nath)**.** *For any finite non-Abelian group G, $\Pr^{2n+2}(G) < \Pr^{2n}(G)$.*

Theorem 57. *Every finite non-Abelian group is generic.*

Proof. Let $\phi \in S_n$ have k alternating cycles in its cycle graph $\mathrm{Gr}(\phi)$, and $\theta \in S_n$ have t alternating cycles in its cycle graph $\mathrm{Gr}(\theta)$. Then, by Theorem 67, $\Pr_\phi(G) = \Pr^{2k}(G)$ and $\Pr_\theta(G) = \Pr^{2t}(G)$. Thus, by Theorem 56, $\Pr_\phi(G) = \Pr_\theta(G)$ only if $k = t$. $\square$

We illustrate Theorem 57 by the following example, which is a generalization of Example 25.

Example 58. Let the group G be D_8 or Q_8. Then

$$\Pr(a_1a_2a_3a_4\cdots a_{2k-1}a_{2k}a_{2k+1}a_{2k+2}\cdots a_{2n} = a_2a_1a_4a_3\cdots a_{2k}a_{2k-1}a_{2k+1}a_{2k+2}\cdots a_n)$$

is equal to

$$\left(\frac{5}{8}\right)^k + \frac{k!}{2!(k-2)!}\left(\frac{5}{8}\right)^{k-2}\left(\frac{3}{8}\right)^2 + \frac{k!}{4!(k-4)!}\left(\frac{5}{8}\right)^{k-4}\left(\frac{3}{8}\right)^4 + \dots. \tag{52}$$

The last summand in the sum 52 is $\left(\frac{3}{8}\right)^k$, for even k, or $\left(\frac{5}{8}\right)k\left(\frac{3}{8}\right)^{k-1}$, for odd k. Indeed, in order for the equation

$$a_1a_2a_3a_4\cdots a_{2k-1}a_{2k}a_{2k+1}a_{2k+2}\cdots a_n = a_2a_1a_4a_3\cdots a_{2k}a_{2k-1}a_{2k+1}a_{2k+2}\cdots a_n$$

to hold, an even number of the inverted pairs $a_{j+1}a_j$ must be equal to ca_ja_{j+1}, where c is the nontrivial element from the center of G. All the other inverted pairs $a_{j+1}a_j$ must be equal to a_ja_{j+1}. But, for each $2t$ where $0 \le 2t \le k$, there are $\frac{k!}{(2t)!(k-2t)!}$ different choices of $2t$ inverted pairs, for which $a_{j+1}a_j = ca_ja_{j+1}$. Now, $\Pr(a_{j+1}a_j = a_ja_{j+1}) = \frac{5}{8}$ and $\Pr(a_{j+1}a_j = ca_ja_{j+1}) = 1 - \frac{5}{8} = \frac{3}{8}$. This justifies the sum 52. A direct computation now shows that for different values of k we get different probabilities for the corresponding permutation equalities.

Next, we prove Theorem 66, which, for even n, asserts the opposite direction of the statement of Theorem 54. This, in turn, permits us to prove Theorem 67, in which the "if" part of the above statement is asserted. In order to prove Theorem 66, we need the following several technical lemmas.

Definition 59. Let ϕ be a permutation in S_n. Let i be any nonnegative integer smaller than $n+1$. We define the permutation $\phi +_i 2 \in S_{n+2}$ as follows

- $\mu_t = \phi_t$ for $t = 1, \dots, i$;
- $\mu_{i+1} = n+2$;
- $\mu_{i+2} = n+1$;
- $\mu_t = \phi_{t-2}$ for $t = i+3, \dots, n+2$.

Notice that for $i = n$, our definition implies $\phi +_i 2 = \langle \phi_1 \ \dots \ \phi_n \ n+2 \ n+1 \rangle$, and, for $i = 0$, it implies $\phi +_i 2 = \langle n+2 \ n+1 \ \phi_1 \ \dots \ \phi_n \rangle$. Observe that for all $0 \le i \le n$,

$$(\phi +_i 2)^\bullet = (\phi_i, n+1, n+2) \cdot \phi^\bullet = (\phi_i, \phi_{i-1}, \dots, \phi_0, \phi_n, \dots, \phi_{i+1}, n+1, n+2).$$

Lemma 60. *Let ϕ be a permutation in S_n, $i \le n$ be a nonnegative integer, and $\mu = \phi +_i 2 \in S_{n+2}$. Then $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\mu)$ have the same number of alternating cycles.*

Proof. From $\mu^\bullet = (\phi_i, n+1, n+2) \cdot \phi^\bullet$ we obtain

$$\mu^\circ = \mu^\bullet \cdot (0, 1, \ldots, n, n+1, n+2) = (\phi_i, n+1, n+2) \cdot \phi^\bullet \cdot (0, n+1, n+2) \cdot (0, 1, \ldots, n)$$

Now, ϕ° always contains $(\phi_{i+1} - 1) \mapsto \phi_i$ and $n \mapsto \phi_n$. When $\phi_{i+1} = 0 = \phi_0$, $i = n$ and $\phi_{i+1} - 1 = n$. Thus, $(\phi_{i+1} - 1) \mapsto \phi_i$ is identical to $n \mapsto \phi_n$. With regard to μ°, the following holds

- If $\phi_{i+1} \neq 0$ then μ° contains $(\phi_{i+1} - 1) \mapsto (n+1) \mapsto \phi_i$ and $n \mapsto (n+2) \mapsto \phi_n$. For all $j \neq \phi_{i+1} - 1, n, n+1, andn + 2$, the piece $\mu_j \mapsto \mu_k$ of μ° is identical to the piece $\phi_j \mapsto \phi_k$ of ϕ°;
- If $\phi_{i+1} = 0$ then μ° contains $(\phi_{i+1} - 1) = n \mapsto (n+2) \mapsto (n+1) \mapsto \phi_i = \phi_n$. For all $j \neq n, n+1, andn + 2$, the piece $\mu_j \mapsto \mu_k$ of μ° is identical to the piece $\phi_j \mapsto \phi_k$ of ϕ°.

This shows that μ° and ϕ° have the same number of cycles in their cyclic decomposition. Hence, by Theorem 31, $\mathrm{Gr}(\mu)$ and $\mathrm{Gr}(\phi)$ have the same number of alternating cycles. □

Lemma 61. *Let ϕ be a permutation in S_n. Let $i \leq n$ and $j \leq n$ be two nonnegative integers. Let $\mu = \phi +_i 2 \in S_{n+2}$ and $\tau = \phi +_j 2 \in S_{n+2}$. Then the permutations τ and μ in S_{n+2} are $x - -y$ equivalent.*

Proof. If $i = j$ then $\tau = \mu$ and our lemma trivially follows. If $i \neq j$, we can assume that $i > j$. Since $\mu^\bullet = (\phi_i, n+1, n+2) \cdot \phi^\bullet$, the $x - -y$ exchange operation, where $x = n+1$ and $y = \phi_i$, by Proposition 38, produces a permutation $\theta \in S_{n+2}$, for which

$$\begin{aligned}\theta^\bullet &= (n+1, \phi_i, \phi_{i-1}) \cdot (\phi_i, n+1, n+2) \cdot \phi^\bullet \\ &= (\phi_{i-1}, n+1, n+2) \cdot \phi^\bullet = (\phi_{i-1}, \phi_{i-2}, \ldots, \phi_0, \phi_n, \ldots, \phi_i, n+1, n+2).\end{aligned}$$

Thus, consecutively performing on μ $i - j$ $x - -y$ exchange operations, in which $x = n+1$ and $y = \phi_i, \phi_{i+1}, \ldots, \phi_{j-1}$, produces the permutation τ. □

Lemma 62. *Let ϕ, θ be $x - -y$ equivalent permutations in S_{2t}. Then any two permutations $\mu = \phi +_i 2 \in S_{2t+2}$ and $\tau = \theta +_j 2 \in S_{2t+2}$ are $x - -y$ equivalent in $S(2t+2)$.*

Proof. It is sufficient to prove that for any permutation $\theta \in S_{2t}$, which is obtained from $\phi \in S_{2t}$ by one $x - -y$ exchange operation or one $x - -y$ cyclic operation, there exist some nonnegative integers q and k, such that the permutation $\mu = \phi +_q 2 \in S_{2t+2}$ is $x - -y$ equivalent to the permutation $\tau = \theta +_k 2 \in S_{2t+2}$. Indeed, our lemma then follows, based on Definition 53 and Lemma 61.

We start by considering the situation when θ was obtained from ϕ by one $x - -y$ exchange operation. In this case, we set q to be equal to k. An $x - -y$ exchange operation on ϕ, by Proposition 38, produces θ, such that $\theta^\bullet = (x, y, z) \cdot \phi^\bullet$.

If $t = 1$ then $\phi = \theta$ and our lemma follows from Lemma 61 . If $t \geq 2$ we select any k such that $\phi_k \notin \{x, y, z\}$. Then the sets $\{x, y, z\}$ and $\{\phi_k, 2t+1, 2t+2\}$ do not intersect. Then applying the same $x--y$ exchange operation on μ produces a permutation τ, such that

$$\begin{aligned}\tau^{\bullet} &= (x, y, z) \cdot \mu^{\bullet} = (x, y, z) \cdot (\phi_k, 2t+1, 2t+2) \cdot \phi^{\bullet} \\ &= (\phi_k, 2t+1, 2t+2) \cdot (x, y, z) \cdot \cdot \phi^{\bullet} = (\phi_k, 2t+1, 2t+2) \cdot \theta^{\bullet}.\end{aligned}$$

The cycles (x, y, z) and $(\phi_{2t}, 2t+1, 2t+2)$ in the equation commute, because the sets $\{x, y, z\}$ and $\{\phi_{2t}, 2t+1, 2t+2\}$ do not intersect. Thus, τ is exactly $\theta +_k 2 \in S_{2t+2}$.

We conclude by considering the situation when θ was obtained from ϕ by one $x--y$ cyclic operation. It is evident from Definition 44, that the $x--y$ cyclic operation, applied on θ, does not affect the $(2t+1) \rightarrow (2t+2)$ piece in the $(2t+3)$-cycle $\mu^{\bullet}$, since both $2t+1$ and $2t+2$ are strictly greater than x and greater than y. Thus, performing an $x--y$ cyclic operation on $\mu = \phi +_q 2 \in S_{2t+2}$ produces a $(2t+3)$-cycle $\tau^{\bullet}$, which contains some $\theta_{k+1} \rightarrow (2t+1) \rightarrow (2t+2) \rightarrow \theta_k$. This Shows that $\tau = \theta +_k 2 \in S_{2t+2}$. $\square$

Let ϕ be a permutation in S_{2t}, with $\phi_{2t} = 2t-1$ and $\phi_{2t-1} = 2t$. Let a be a nonnegative integer, smaller than $2t+1$. Let $\theta \in S_{2t}$ be defined by $\theta_{\chi+i} = (\phi_i + a) \mod (2t+1)$, where χ is such that $\phi_\chi = -a$. For $a = 0$ we have $\theta = \phi$. Notice that

$$\phi^{\bullet} = (\phi_{2t-2}, \phi_{2t-3}, \ldots, \phi_1, \phi_0 = 0, 2t-1, 2t)$$

and

$$\theta^{\bullet} = (\phi_{2t-2} + a, \phi_{2t-3} + a, \ldots, \phi_1 + a, \phi_0 + a = a, 2t-1+a = a-2, 2t+a = a-1).$$

Here all indices and all elements are modulo $2t+1$.

Lemma 63. *The permutations ϕ and θ are $x--y$ equivalent.*

Proof. The lemma is trivial for $a = 0$. Assume, by induction hypothesis, that the lemma holds for a. We prove our lemma for $a+2$. This, by induction, implies our lemma for all $a+2, a+4, a+6, \ldots$. Since $a+1 = a+2t+2$ modulo $2t+1$, this implies our lemma for $a+1$.

For all $q = 1, \ldots, 2t-2$, let j_q be such that $\phi_{j_q} = 2t-1-q$. Since $\theta^{\bullet}$ contains $(a-2) \rightarrow (a-1)$, we can perform the $(a-3)--(a-1)$ exchange operation on θ. Recall that all the calculations are carried modulo $2t+1$. Thus, for example, $-1 = 2t$, $-2 = 2t-1$, and $-3 = 2t-2$. This $(a-3)--(a-1)$ exchange operation produces the permutation $\rho[1]$ such that

$$\rho[1]^{\bullet} = (\phi_{2t-2} + a, \phi_{2t-3} + a, \ldots, \phi_{j_1 - 1} + a, 2t+a = a-1, \phi_{j_1} + a = a-3, \ldots,$$

$$\ldots, \phi_1 + a, \phi_0 + a = a, 2t-1+a = a-2).$$

Since $\rho[1]^\bullet$ contains $(a-1) \to (a-3)$, we can perform the $(a-2)--(a-3)$ exchange operation on $\rho[1]$. This $(a-2)--(a-3)$ exchange operation produces the permutation $\varrho[1]$ such that

$$\varrho[1]^\bullet = (\phi_{2t-2}+a, \phi_{2t-3}+a, \dots, \phi_{j_1-1}+a, 2t+a = a-1, \phi_{j_1+1}+a, \dots,$$

$$\dots, \phi_1+a, \phi_0+a = a, \phi_{j_1}+a = a-3, 2t-1+a = a-2).$$

Since $\varrho[1]^\bullet$ contains $(a-3) \to (a-2)$, we can perform the $(a-4)--(a-2)$ exchange operation on $\varrho[1]$. This $(a-4)--(a-2)$ exchange operation produces the permutation $\rho[2]$ such that $\rho[2]^\bullet$ contains $(a-2) \to (a-4)$. Thus, we perform an $(a-3)--(a-4)$ exchange operation on $\rho[2]$ and obtain $\varrho[2]$. Notice that $\varrho[1]^\bullet$ is obtained from

$$\theta^\bullet = (\phi_{2t-2}+a, \phi_{2t-3}+a, \dots, \phi_1+a, \phi_0+a = a, 2t-1+a = a-2, 2t+a = a-1)$$

by adding 2 to $\theta_{\chi+j_1} = \phi_{j_1}+a = a-3$ and to $\theta_{\chi+j_2} = \phi_{j_2}+a = a-4$, and subtracting 2 from $2t-1+a = a-2$ and $2t+a = a-1$. Continuing this way, we produce permutations $\varrho[3], \dots, \varrho[2t-2]$. Now,

$$\begin{aligned}\varrho[2t-2]^\bullet = (&\phi_{2t-2}+a+2, \phi_{2t-3}+a+2, \dots, \phi_1+a+2, \phi_0+a \\ &= a, 2t-1+a-[2t-2] \\ &= a+1, 2t+a-[2t-2] \\ &= a+2).\end{aligned}$$

Finally, we perform an $a--(a+2)$ exchange operation on $\varrho[2t-2]$ and obtain the permutation ζ, for which

$$\begin{aligned}\zeta^\bullet = (&\phi_{2t-2}+a+2, \phi_{2t-3}+a+2, \dots, \phi_1+a+2, \phi_0+a+2 \\ &= a+2, 2t-1+a+2 \\ &= a, 2t+a+2 \\ &= a+1).\end{aligned}$$

Thus, we proved the lemma for $a+2$. □

Lemma 64. *Any permutation $\phi \in S_{2t}$, such that $\phi^\bullet = (\dots, a, b, a-1, \dots)$, where a and b are between 0 and $2t$, is $x--y$ equivalent to some permutation $\theta \in S_{2t}$, such that*

$$\theta^\bullet = (\theta_{2t-2}, \theta_{2t-3}, \dots, \theta_1, \theta_0 = 0, 2t-1, 2t).$$

Proof. First, we show, that ϕ is $x--y$ equivalent to some $\rho \in S_{2t}$, such that $\rho^\bullet$ contains some $k \to k+1$. Indeed, if $b = a+1$, then we let $k = b$. Otherwise, if $b > a+1$, then an $(a-1)--b$ cyclic operation on ϕ produces permutation ρ, such that $\rho^\bullet = (\dots, b-1, b, a-1, \dots)$. Thus, we set $k = b-1$. And if $b < a-1$, then an $(a-1)--b$ cyclic operation on ϕ produces permutation ρ, such that $\rho^\bullet = (\dots, a, b, b+1, \dots)$. Thus, we set $k = b$.

Next, let i, j be such that, in $\rho^\bullet$, $\rho_i \to k$ and $\rho_j = k+2$. If $i = j$, then we set $\varrho = \rho$. Otherwise, a consecutive performance of $k - -\rho_i$, $k - -\rho_{i+1}$, …, $k - -\rho_j$ exchange operations, just like in the proof of Lemma 61, produces a permutation $\varrho = (\ldots, k+2, k, k+1, \ldots)$.

Lemma 63 now establishes that ϱ, and, hence, ϕ, is $x - -y$ equivalent to θ. □

Lemma 65. *Let $\phi \in S_{2t}$ be a permutation, different than the identity. Then ϕ is $x - -y$ equivalent to some permutation $\theta \in S_{2t}$, such that*

$$\theta^\bullet = (\theta_{2t-2}, \theta_{2t-3}, \ldots, \theta_0, 2t-1, 2t).$$

Proof. There exists some number a between 0 and $2t$, such that $\phi^\bullet$ does not contain $a \to (a-1)$. Otherwise, ϕ is the identity permutation. Now, let $\phi^\bullet$ contain some path

$$a \to b_1 \to b_2 \to \cdots \to b_k \to (a-1), \tag{53}$$

where $k \geq 1$. First, assume that $k \geq 2$. Then we look for $b(i)$,
where $1 \leq i \leq k-1$, such that $(b(i)-1) \notin \{b(1), \ldots, b(k)\}$. If we find such a $b(i)$, we perform the $(b(i)-1) - -b_{i+1}$ exchange operation on ϕ, which shortens the path 53 to

$$a \to b_1 \to \cdots \to b_i \to b_{i+2} \to \cdots \to b_k \to (a-1).$$

If we do not find such a $b(i)$, then $(b(k)-1) \notin \{b(1), \ldots, b(k)\}$. In this case, we perform the $(a-1) - -b(1)$ exchange operation on ϕ, which changes the path 53 to

$$a \to b_2 \to \cdots \to b_k \to b_1 \to (a-1).$$

Now we perform the $(b(k)-1) - -b_1$ exchange operation, which shortens the path 53 to

$$a \to b_2 \to \cdots \to b_{k-1} \to b_1 \to (a-1).$$

By repeating the argument of shortening the path 53, we can assume that $k = 1$. The lemma now follows from Lemma 64. □

Theorem 66. *If two permutations ϕ and θ in S_{2t} have the same number of alternating cycles in their cycle graphs $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$, then they are $x - -y$ equivalent.*

Proof. We prove the theorem by induction on t.

Basic step. For $t = 1$ we only have one permutation $\langle 2 \;\; 1 \rangle \in S_2$ with one alternating cycle in its cycle graph, and one permutation $\langle 1 \;\; 2 \rangle \in S_2$ with two alternating cycles in its cycle graph. Hence, the proof is completed for $t = 1$.

Induction. Assume that the induction hypothesis is true for t. We will now prove it for $t + 1$.

If $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$ have only one alternating cycle, then $\phi = \theta$ is the identity permutation, and the proof is finished.

Otherwise, by Lemma 65, there exist permutations μ and τ in S_{2t+2} such that

$$\mu^\bullet = (\mu_{2t}, \mu_{2t-1}, \ldots, \mu_0, 2t+1, 2t+2),$$

$$\tau^\bullet = (\tau_{2t}, \tau_{2t-1}, \ldots, \tau_0, 2t+1, 2t+2),$$

and μ is $x--y$ equivalent to ϕ, τ is $x--y$ equivalent to θ.

By Lemma 60, the permutations $\rho = \langle \mu_1 \;\; \mu_2 \;\; \ldots \;\; \mu_{2t-1} \;\; \mu_{2t} \rangle$ and $\varrho = \langle \tau_1 \;\; \tau_2 \;\; \ldots \;\; \tau_{2t-1} \;\; \tau_{2t} \rangle$ in S_{2t} have the same number of alternating cycles in their cycle graphs as the permutations μ and τ, which, in turn, by Theorem 54, have the same number of alternating cycles in their cycle graphs as the permutations ϕ and θ. Now we apply the induction hypothesis to obtain that ρ and ϱ are $x--y$ equivalent in S_{2t}. This, by Lemma 62, establishes that μ and τ are $x--y$ equivalent in S_{2t+2}. Thus, ϕ and θ are $x--y$ equivalent in S_{2t+2}, which completes the proof. $\square$

At this point we are ready to state and prove the two main findings. They generalize the observation, made at the end of the previous section, that the probability of a permutation equality in a fixed finite group G depends only on the number of the alternating cycles in the cycle graph of the permutation.

Theorem 67. *Let $\phi \in S_n$ be a permutation such that $\mathrm{Gr}(\phi)$ contains k alternating cycles. Then, for all positive $k \leq n$,*

$$\Pr_\phi(G) = \Pr^{n+1-k}(G) = \Pr(a_1 a_2 \cdots a_{n-k} a_{n+1-k} = a_{n+1-k} a_{n-k} \cdots a_2 a_1)$$

Since, as shown in [12], $n-k$ must be an odd number, $k \leq n$ implies $k \leq n-1$. If $k > n$ then $k = n+1$ and ϕ is the identity permutation, which implies $\Pr_\phi(G) = 1$.

Proof. If n is an even number then, by Theorem 66, the permutations ϕ and $\langle a_{n+1-k} \;\; \ldots \;\; a_1 \;\; a_{n+2-k} \;\; \ldots \;\; a_n \rangle$, both having k alternating cycles in their cycle graphs, are $x--y$ equivalent in S_n. Next, Theorem 55 asserts that $\Pr_\phi(G) = \Pr^{n+1-k}(G)$.

If n is odd then define $\rho \in S_{n+1}$ by $\rho = \langle \phi_1 \;\; \ldots \;\; \phi_n \;\; (n+1) \rangle$. Notice that $\mathrm{Gr}(\rho)$ contains the same k alternating cycles as $\mathrm{Gr}(\phi)$ plus one additional alternating cycle $(n+1) \dashrightarrow 0 \to (n+1)$, which is $(n+1) \mapsto (n+1)$. Since $n+1$ is even, $\Pr_\phi(G) = \Pr_\rho(G) = \Pr^{n+2-(k+1)}(G) = \Pr^{n+1-k}(G)$. $\square$

Theorem 68. *Let G be a finite non-Abelian group. Let ϕ and θ be two permutations in S_n. Then, $\Pr_\phi(G) = \Pr_\theta(G)$ if, and only if, the number of the alternating cycles in the cycle graph $\mathrm{Gr}(\phi)$ equals the number of alternating cycles in the cycle graph $\mathrm{Gr}(\theta)$. Thus, the spectrum of probabilities of permutation equalities for permutations from S_n in a finite non-Abelian group G consisting of exactly $\left\lfloor \frac{n}{2} \right\rfloor + 1$ different numbers, each number corresponding to its unique Hultman class of permutations in S_n.*

Proof. This theorem follows trivially from Theorem 67 and Theorem 57. $\square$

5 Two explicit formulae for $\mathrm{Pr}^{2t}(G)$

We provide two explicit formulae for $\mathrm{Pr}^{2t}(G)$. Our first formula expresses $\mathrm{Pr}^{2t}(G)$ in terms of $\mathrm{Stab.\,Prod}_t(x_1, x_2, \ldots, x_t)$. Our second formula expresses $\mathrm{Pr}^{2t}(G)$ in terms of $c_{i_1,\ldots,i_t;j}(G)$. These results constitute a generalization of what was shown in Theorem 18 for permutations in S_4.

Theorem 69. *Let G be a finite group. Then*

$$\Pr(a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1) = \frac{\sum\limits_{x_1,x_2,\ldots,x_t \in G} |\mathrm{Stab.\,Prod}_t(x_1, x_2, \ldots, x_t)|}{|G|^{2t}} \tag{54}$$

$$\Pr(a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1) = \frac{1}{|G|^t} \cdot \sum_{i_1,i_2,\ldots,i_t,j=1}^{c(G)} \frac{|\Omega_j| \cdot c^2_{i_1,i_2,\ldots,i_t;j}(G)}{|\Omega_{i_1}| \cdot |\Omega_{i_2}| \cdot \cdots \cdot |\Omega_{i_t}|} \tag{55}$$

Proof. Let us consider a generic equation

$$a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1.$$

Let x_i denotes the product $a_{2i-1}a_{2i}$ for all $i = 1, \ldots, t$. Let x'_i denotes the product $a_{2i}a_{2i-1}$. Notice that by Lemma 10, we have $x_i \sim x'_i$.

The equation

$$a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1$$

then becomes

$$x_1 x_2 \cdots x_t = x'_t x'_{t-1} \cdots x'_1.$$

Now, consider any equation

$$x_1, \ldots, x_n, x'_1, \ldots, x'_n \in G,$$

such that $x_i \sim x'_i$ for all $i = 1, \ldots, t$. Then, by Lemma 11, there are exactly $\frac{|G|}{|\Omega_{x_i}|} = |C_G(x_i)|$ different ways to break each x_i into a product $a_{2i-1}a_{2i}$ in such a way that $x'_i = a_{2i}a_{2i-1}$. Thus, to each fixed equation

$$x_1 x_2 \cdots x_t = x'_t x'_{t-1} \cdots x'_1$$

corresponds to

$$|C_G(x_1)| \cdot |C_G(x_2)| \cdot \cdots \cdot |C_G(x_t)|$$

different equations

$$a_1 a_2 \cdots a_{2t} = a_{2t} a_{2t-1} \cdots a_1.$$

Notice that for any fixed elements $x_1, x_2, \ldots, x_t \in G$, we can define an element

$$x''_1 = (x_2 x_3 \cdots x_t)^{-1} x_1 (x_2 x_3 \cdots x_t) = x_t^{-1} \cdots x_3^{-1} x_2^{-1} x_1 x_2 x_3 \cdots x_t$$

and obtain an equation

$$x_1x_2\cdots x_t = x_tx_{t-1}\cdots x_2x_1''.$$

Now, for any general equation

$$x_1x_2\cdots x_t = x_t'x_{t-1}'\cdots x_1',$$

in which $x_i \sim x_i'$ for all i, there exist some elements $g_1, g_2, \ldots, g_t \in G$, such that $x_1' = g_1x_1''g_1^{-1}$ and, for all $i = 2, 3, \ldots, t$, $x_i' = g_ix_ig_i^{-1}$.

Thus, if we select and fix elements $x_1, x_2, \ldots, x_t \in G$, we will have

$$\frac{|\mathrm{Stab.\,Prod}_t(x_t, \ldots, x_2, x_1'')|}{|C_G(x_t)|\cdot\cdots\cdot|C_G(x_2)|\cdot|C_G(x_1'')|}$$

different equations

$$x_1x_2\cdots x_t = x_t'x_{t-1}'\cdots x_1',$$

in which $x_i' \sim x_i$ and for all i. Indeed, every ordered t-tuple

$$(g_t, g_{t-1}, \ldots, g_2, g_1'') \in \mathrm{Stab.\,Prod}_t(x_t, \ldots, x_2, x_1''),$$

by setting $x_i' = g_ix_ig_i^{-1}$, for all $i = t, \ldots, 2$, and $x\prime_1 = g_1x_1''g_1^{-1}$, produces an equation

$$x_1x_2\cdots x_t = x_t'x_{t-1}'\cdots x_1'.$$

And any two of these equations produced from the equation $x_1x_2\cdots x_t = x_tx_{t-1}\cdots x_2x_1''$ are identical if, and only if, $g_i \in C_G(x_i)$, for all $i = t, \ldots, 2$ and $g_1 \in C_G(x'')$. Now, $|C_G(x_1'')| = |C_G(x_1)|$. Thus, for each fixed ordered t-tuple $(x_1, x_2, \ldots, x_t)$ of elements of G we have

$$\frac{|\mathrm{Stab.\,Prod}_t(x_t, \ldots, x_2, x_1'')|}{|C_G(x_t)|\cdot\cdots\cdot|C_G(x_2)|\cdot|C_G(x_1)|}$$

different equations

$$x_1x_2\cdots x_t = x_t'x_{t-1}'\cdots x_1'.$$

As we showed above, to each of these equations correspond

$$|C_G(x_1)|\cdot|C_G(x_2)|\cdot\cdots\cdot|C_G(x_t)|$$

different equations

$$a_1a_2\cdots a_{2t} = a_{2t}a_{2t-1}\cdots a_1.$$

Thus to each ordered t-tuple $(x_1, x_2, \ldots, x_t)$ of elements of G correspond $|\mathrm{Stab.\,Prod}_t(x_t, \ldots, x_2, x_1'')|$ different equations

$$a_1a_2\cdots a_{2t} = a_{2t}a_{2t-1}\cdots a_1.$$

Hence, to find

$$\Pr(a_1a_2\cdots a_{2t} = a_{2t}a_{2t-1}\cdots a_1)$$

we need to sum $|\mathrm{Stab.\,Prod}_t(x_t, x_{t-1}, \ldots x_2, x_1'')|$, as $x_1, x_2, \ldots, x_t$ run over all elements of G.

Since $x_1, x_2, \ldots, x_n$ run over all the elements of G, and for each fixed $x_1, \ldots, x_{n-1}$ there is a one-to-one correspondence between x_1'' and x_1, the sum remains the same if we sum $|\mathrm{Stab.\,Prod}_t(x_t, x_{t-1}, \ldots, x_2, x_1)|$, as $x_1, x_2, \ldots, x_t$ run over all elements of G. That proves Equation 54.

Now, select and fix an element z in an equivalence class Ω_j of G.
Let $x_1, \ldots, x_t, x_1', \ldots, x_t' \in G$ be such, that $x_i \sim x_i'$ for all i, and

$$x_1 x_2 \cdots x_t = z = x_1' x_2' \cdots x_t'. \tag{56}$$

For each $i = 1, \ldots, t$, there are $|C_G(x_i)|$ different ways to break x_i into a product $a_{2i-1}a_{2i}$ so that $a_{2i}a_{2i-1} = x_i'$. Hence, for each (fixed) Equation 56 we have exactly $|C_G(x_1)| \cdot |C_G(x_2)| \cdot \cdots \cdot |C_G(x_t)|$ different equations

$$\begin{aligned}(a_1a_2)(a_3a_4)\cdots(a_{2t-1}a_{2t}) &= x_1x_2\cdots x_t \\ &= z = x_1'x_2'\cdots x_t' = (a_2a_1)(a_4a_3)\cdots(a_{2t}a_{2t-1}).\end{aligned}$$

But,

$$|C_G(x_1)| \cdot |C_G(x_2)| \cdot \cdots \cdot |C_G(x_t)| = \frac{|G|^t}{|\Omega(x_1)| \cdot |\Omega(x_2)| \cdot \cdots \cdot |\Omega(x_t)|}.$$

Now, for $z \in \Omega_j$ there are $c_{i_1,i_2,\ldots,i_t;j}(G)$ different ways to write z as a product $x_1x_2\cdots x_t$, where $x_i \in \Omega_i$ for all $i = 1, \ldots, t$, and $c_{i_1,i_2,\ldots,i_t;j}(G)$ different ways to write z as a product $x_1'x_2'\cdots x_t'$, where $x_i' \in \Omega_i$ for all $i = 1, \ldots, t$. Thus, for each $z \in \Omega_j$ there are $c^2_{i_1,i_2,\ldots,i_t;j}(G)$ different equations of the form

$$x_1x_2\cdots x_t = z = x_1'x_2'\cdots x_t',$$

in which $x_i, x_i' \in \Omega_i$ for all $i = 1, \ldots, t$. Thus, for each $z \in \Omega_j$ there are

$$|G|^t \cdot \sum_{i_1,i_2,\ldots,i_t=1}^{c(G)} \frac{c^2_{i_1,i_2,\ldots,i_t;j}(G)}{|\Omega_{i_1}| \cdot |\Omega_{i_2}| \cdot \cdots \cdot |\Omega_{i_t}|}$$

different equations of the form

$$(a_1a_2)(a_3a_4)\cdots(a_{2t-1}a_{2t}) = z = (a_2a_1)(a_4a_3)\cdots(a_{2t}a_{2t-1}).$$

We make z run over all the elements of G and obtain

$$\Pr(a_1a_2\cdots a_{2t-1}a_{2t} = a_2a_1\cdots a_{2t}a_{2t-1}) = \frac{1}{|G|^t} \cdot \sum_{i_1,i_2,\ldots,i_t,j=1}^{c(G)} \frac{|\Omega_j| \cdot c^2_{i_1,i_2,\ldots,i_t;j}(G)}{|\Omega_{i_1}| \cdot |\Omega_{i_2}| \cdot \cdots \cdot |\Omega_{i_t}|}.$$

Since both permutations $\phi = \langle 2t \;\; 2t-1 \;\; \ldots \;\; 1\rangle$ and $\theta = \langle 2 \;\; 1 \;\; 4 \;\; 3 \;\; \ldots \;\; 2t \;\; 2t-1\rangle$ have exactly one alternating cycle in their cycle graphs $\mathrm{Gr}(\phi)$ and $\mathrm{Gr}(\theta)$, Equation 55 follows from Theorem 68. $\square$

6 Conclusion

In conclusion, we recall two known results. The first result relates $\mathrm{Pr}^{2t}(G)$ to the commutator subgroup G' and the quotient group $G/Z(G)$, and the second result relates $\mathrm{Pr}^{2t}(G)$ to the notion of isoclinism of groups. We give a counter-example to the opposite direction of the second result. We conjecture a weaker form of the opposite direction of the second result. Finally, we give an example, demonstrating that the isoclinism in the second result cannot be replaced by weak isoclinism. From that it follows that the opposite direction of our conjecture is false.

Theorem 70. *The first result, established by Das and Nath [9], is*

$$\lim_{t\to\infty} \mathrm{Pr}^{2t}(G) = \frac{1}{|G'|}.$$

Theorem 71. *The second result, established by Das and Nath [9] If two finite groups G_1 and G_2 are isoclinic, then $\mathrm{Pr}^{2t}(G_1) = \mathrm{Pr}^{2t}(G_2)$ for all $t = 1, 2, \ldots$.*

For example, every two Abelian groups are isoclinic. Clearly, $\mathrm{Pr}^{2t}(G) = 1$ for all t, for every Abelian group. The dihedral group D_8 and the quaternion group Q_8, both of order 8, are isoclinic. As we showed in Example 58, $\mathrm{Pr}^{2t}(D_8) = \mathrm{Pr}^{2t}(Q_8)$ for every $t \geq 1$.

Now, notice that the opposite direction of the second result is not true. Two finite groups G_1 and G_2, for which $\mathrm{Pr}^{2t}(G_1) = \mathrm{Pr}^{2t}(G_2)$ for all $t = 1, 2, \ldots$, do not have to be isoclinic. For example, the groups

$$\begin{aligned}G_1 = &\langle a_1, a_2, a_3, a_4, a_5, a_6 \ : \ a_1^2 = a_4, a_4^2 = a_6, a_2^2 = a_3^2 = a_5^2 = a_6^2 = 1,\\ &[a_1, a_2] = a_3, [a_1, a_3] = [a_2, a_4] = a_5,\\ &[a_1, a_5] = [a_2, a_5] = [a_3, a_5] = [a_2, a_3] = [a_3, a_4] = [a_2, a_6] = [a_3, a_6] = 1\rangle\end{aligned}$$

and

$$\begin{aligned}G_2 = &\langle a_1, a_2, a_3, a_4, a_5, a_6 \ : \ a_1^2 = a_2^2 = a_3^2 = a_4^2 = a_5^2 = a_6^2 = 1,\\ &[a_1, a_2] = a_6, [a_1, a_3] = [a_2, a_4] = a_5,\\ &[a_1, a_4] = [a_1, a_5] = [a_1, a_6] = [a_2, a_3] = [a_2, a_5] = [a_2, a_6]\\ &= [a_3, a_4] = [a_3, a_5] = [a_3, a_6] = [a_4, a_5] = [a_4, a_6] = [a_5, a_6] = 1\rangle,\end{aligned}$$

both of the order 64, are not isoclinic, not even weakly isoclinic. Indeed, $G_1/Z(G_1)$ is a non-Abelian group of order 16, while $G_2/Z(G_2)$ is an Abelian group of order 16. The fact that $\mathrm{Pr}^{2t}(G_1) = \mathrm{Pr}^{2t}(G_2)$, for every $t \geq 1$, is verifiable by a direct calculation.

From Theorem 70 it follows that, if for two finite groups G_1 and G_2 we have $\mathrm{Pr}^{2t}(G_1) = \mathrm{Pr}^{2t}(G_2)$ for every $t \geq 1$, then $|G_1'| = |G_2'|$. That motivates the following conjecture, which, together with $|G_1'| = |G_2'|$, is a weaker form of the opposite direction of the second result.

Conjecture 72. Let G_1 and G_2 are two finite groups, such that $\mathrm{Pr}^{2t}(G_1) = \mathrm{Pr}^{2t}(G_2)$ for every $t \geq 1$. Then $|G_1/Z(G_1)| = |G_2/Z(G_2)|$.

The groups G_2 and $G_3 = D_8 \times D_8$ give a counterexample to the opposite direction of Conjecture 72. Moreover, G_2' is isomorphic to $G_3'|$, and $G_2/Z(G_2)$ is isomorphic to $G_3/Z(G_3)|$. Thus, G_2 and G_3 are weakly isoclinic. However,
$\mathrm{Pr}^2(G_2) = \frac{22}{64} \neq \frac{25}{64} = \mathrm{Pr}^2(G_3)$. Hence, by Theorem 71, G_2 and G_3 are not isoclinic.

7 Acknowledgments

We thank both referees for their helpful remarks that gave us an opportunity to significantly improve the presentation of the paper. Our special gratitude is to the referee that paid attention to fruitful connections between block transpositions due to Bafna and Pevzner [1] and the $x - -y$ exchange operation defined in this paper.

References

[1] V. Bafna and P. A. Pevzner, Sorting by transpositions, *SIAM J. Discrete Math.* **11** (1998) 224–240.

[2] S. R. Blackburn, J. R. Britnell, and M. Wildon, The probability that a pair of elements of a finite group are conjugate, *J. Lond. Math. Soc.* **86** (2012) 755–778.

[3] S. M. Buckley, Isoclinism and weak isoclinism invariants, preprint, http://archive.maths.nuim.ie/staff/sbuckley/Papers/gp_isoc.pdf, 2014.

[4] Y. Cherniavsky, A. Goldstein, and V. E. Levit, Groups of balanced labelings on graphs, *Discrete Math.* **320** (2014) 15–25.

[5] Y. Cherniavsky, A. Goldstein, V. E. Levit, and R. Shwartz, Enumeration of balanced finite group valued functions on directed graphs, *Inform. Process. Lett.* **116** (2016) 484–488.

[6] Y. Cherniavsky, A. Goldstein, and V. E. Levit, Balanced Abelian group-valued functions on directed graphs, *Ars Math. Contemporanea* **13** (2017) 307–315.

[7] C. Clifton, D. Guichard, and P. Keef, How commutative are direct products of dihedral groups?, *Math. Mag.* **84** (2011) 137–140.

[8] A. K. Das and R. K. Nath, A generalization of commutativity degree of finite groups, *Comm. Algebra* **40** (2012) 1974–1981.

[9] A. K. Das and R. K. Nath, A survey on the estimation of commutativity in finite groups, *Southeast Asian Bull. Math.* **37** (2013) 161–180.

[10] A. K. Das and R. K. Nath, On generalized commutativity degree of a finite group, *Rocky Mountain J. Math.* **41** (2011) 1987–2000.

[11] J. Dixon, Probabilistic group theory, *C. R. Math. Acad. Sci. Soc. R. Can.* **24** (2002) 1–15.

[12] J. P. Doignon and A. Labarre, On Hultman numbers, *J. Integer Seq.* **10** (2007), Article 07.6.2.

[13] P. Erdős and E. G. Straus, How abelian is a finite group?, *Linear Multilinear Algebra* **3** (1976) 307–312.

[14] P. Erdős and P. Turan, On some problems of statistical group theory, *Acta Math. Acad. Sci. Hungar.* **19** (1968) 413–435.

[15] I. V. Erovenko and B. Surg, Commutativity degrees of wreath products of finite abelian groups, *Bull. Aust. Math. Soc.* **77** (2008) 31–36.

[16] W. H. Gustafson, What is the probability that two group elements commute?, *Amer. Math. Monthly* **80** (1973) 1031–1034.

[17] R. M. Guralnick and G. R. Robinson, On the commuting probability in finite groups, *J. Algebra* **300** (2006) 509–528.

[18] P. Hall, The classification of prime-power groups, *J. Reine Angew. Math.* **182** (1940) 130–141.

[19] U. Jezernik and P. Moravec, Universal commutator relations, Bogomolov multipliers, and commuting probability, *J. Algebra* **428** (2015) 1–25.

[20] P. Lescot, Central extensions and commutativity degrees, *Comm. Algebra* **29** (2001) 4451–4460.

[21] P. Lescot, H. N. Nguyen, and Y. Yang, On the commuting probability and supersolvability of finite groups, *Monatsh. Math.* 174 (2014) 567–576.

[22] R. K. Nath and A. K. Das, On generalized commutativity degree of a finite group, *Rocky Mountain J. Math.* **41** (2011) 1987–2000.

[23] R. K. Nath, *Some New Directions in Commutativity Degree of Finite Groups: Recent Developments*, *Lambert Academic Publishing*, 2011.

[24] M. R. Pournakia and R. Sobhani, Probability that the commutator of two group elements is equal to a given element, *J. Pure Appl. Algebra* **212** (2008) 727–734.

[25] N. J. A. Sloane, *The On-line Encyclopedia of Integer Sequences*, `http://www.oeis.org`.

2010 *Mathematics Subject Classification*: Primary 20P05; Secondary 20F12, 20B05, 05A05, 20D60.
Keywords: commuting probability, Hultman number, cycle graph of a permutation, isoclinism, finite group.

(Concerned with the sequence A164652.)

Received December 17 2015; revised versions received March 29 2017; October 31 2017. Published in *Journal of Integer Sequences*, November 22 2017.

Return to Journal of Integer Sequences home page.