REPRESENTING RANDOM PERMUTATIONS AS THE PRODUCT OF TWO INVOLUTIONS

CHARLES BURNETTE AND ERIC SCHMUTZ

Abstract. An involution is a permutation that is its own inverse. Given a permutation σ of $[n]$, let $\mathbf{N}_n(\sigma)$ denote the number of ways to write σ as a product of two involutions of $[n]$. If we endow the symmetric groups S_n with uniform probability measures, then the random variables $\mathbf{N}_n$ are asymptotically lognormal.

The proof is based upon the observation that, for most permutations σ, $\mathbf{N}_n(\sigma)$ can be well-approximated by $\mathbf{B}_n(\sigma)$, the product of the cycle lengths of σ. Asymptotic lognormality of $\mathbf{N}_n$ can therefore be deduced from Erdős and Turán's theorem that $\mathbf{B}_n$ is itself asymptotically lognormal.

1. Introduction

An involution is a permutation that is its own inverse, i.e. a permutation whose cycle lengths are all less than or equal to two. If σ is a permutation of $[n]$, let $\mathbf{N}_n(\sigma)$ be the number of ordered pairs of involutions τ_1, τ_2 of $[n]$ such that $\sigma = \tau_2 \circ \tau_1$. The goal of this paper is to determine the asymptotic distribution of the random variable $\mathbf{N}_n$ for uniform random permutations σ.

Let $\mathcal{T}_n$ be the set of all involutions of $[n]$. The cardinalities $|\mathcal{T}_n|, n = 1, 2, 3, \ldots$ have been extensively investigated and form OEIS Sequence A000085 [23]. See also Amdeberhan and Moll [1] for more recent work. Of particular importance for this paper is an asymptotic formula that was derived by Chowla, Herstein, and Moore [8]:

$$|\mathcal{T}_n| \sim \frac{1}{\sqrt{2}} \left(\frac{n}{e}\right)^{n/2} e^{n^{1/2} - 1/4}. \tag{1.1}$$

Related approximations appear in Moser and Wyman [18], [19].

Vivaldi and Roberts [21] studied the random permutations that are obtained by multiplying random involutions with various restrictions on their fixed points. However the product of two uniformly random involutions is not a uniformly random permutation. For example the identity permutation is generated with probability $\frac{1}{|\mathcal{T}_n|}$, which is much larger than $\frac{1}{n!}$. Thus $\mathbf{N}_n$ is clearly not constant.

Department of Mathematics, Drexel University, Philadelphia, PA 19104-2875, cdb72@drexel.edu.

Department of Mathematics, Drexel University, Philadelphia, PA 19104-2875, Eric.Jonathan.Schmutz@drexel.edu.

Let $I_{\tau_2,\tau_1}(\sigma) = 1$ if $\tau_2 \circ \tau_1 = \sigma$ (and $I_{\tau_2,\tau_1}(\sigma) = 0$ otherwise), so that

$$\mathbf{N}_n = \sum_{\tau_1,\tau_2} I_{\tau_2,\tau_1}. \tag{1.2}$$

Using this representation and Stirling's formula, it is straightforward to estimate the average number of factorizations [16]:

$$\mathbb{E}_n(\mathbf{N}_n) = \frac{1}{n!}\sum_{\tau_1,\tau_2}\sum_{\sigma} I_{\tau_2,\tau_1}(\sigma) = \frac{|\mathcal{T}_n|^2}{n!} \sim \frac{e^{2\sqrt{n}}}{\sqrt{8\pi e n}}. \tag{1.3}$$

Our results show that the average in (1.3) is misleadingly large; if n is large, then for most permutations $\sigma \in S_n$, one has

$$e^{(\frac{1}{2}-\epsilon)\log^2 n} < \mathbf{N}_n(\sigma) < e^{(\frac{1}{2}+\epsilon)\log^2 n}.$$

Another consequence of the sum of indicators representation (1.2) is that $\max_\sigma \mathbf{N}_n(\sigma) = |\mathcal{T}_n|$. The unique permutation that attains the maximum is the identity permutation that fixes all n points. At the other extreme, for $n \geq 2$, $\min_\sigma \mathbf{N}_n(\sigma) = n-1$. The minimum is attained only by the $\frac{n!}{n-1}$ permutations that have a cycle of length $n-1$. These two extremal results are stated on page 161 of Lugo's thesis [16] and are also proved later in [7]. Lugo also conjectured, but did not prove, that $\mathbf{N}_n$ is asymptotically lognormal.

There is an extensive literature on formulas for the number of ways to write a permutation as the product of two or more permutations with various restrictions on the conjugacy classes of the factors of the product. Without trying to review that literature, we refer readers to [13] and [14] as possible starting points. For asymptotic problems, even an explicit formula can be quite useless if it is too complicated. However, as the authors in [13] and [14] point out, formulas with nonnegative terms tend to be more tractable. In this paper, we make use of one such formula:

$$\mathbf{N}_n(\sigma) = \prod_{k=1}^{n} \sum_{j=0}^{\lfloor c_k/2 \rfloor} \frac{k^{c_k-j} c_k!}{2^j j!(c_k-2j)!}, \tag{1.4}$$

where $c_k = c_k(\sigma)$ denotes the number of cycles of length k that σ has. From formula (1.4), one sees that $\mathbf{N}_n(\sigma)$ depends only on the cycle structure of σ. This makes sense because $\mathbf{N}_n(\sigma)$ remains invariant under the conjugacy action of S_n, which follows easily from the fact that the mapping $\tau_1\tau_2 \mapsto (\rho\tau_1\rho^{-1})(\rho\tau_2\rho^{-1})$ is a one-to-one correspondence between the involution factorizations of σ and the involution factorizations of its conjugate $\rho\sigma\rho^{-1}$ for $\rho \in S_n$. As far as we know, the first complete proofs of (1.4) are in Petersen and Tenner [20] and Lugo [15], [16].

We use the formula (1.4) to prove that, for most permutations σ, $\mathbf{N}_n(\sigma)$ can be well-approximated by $\mathbf{B}_n(\sigma) = \prod_k k^{c_k}$, the product of the cycle lengths of σ. The random variable $\mathbf{B}_n$ has been studied by many authors, beginning with the work of Erdös and Turán [10], [11]. Asymptotic lognormality of $\mathbf{N}_n$ will be deduced from the known fact that $\mathbf{B}_n$ is asymptotically lognormal.

2. Factorizations

This section is more or less expository: we discuss the known factorization (1.4). For each integer x, let $\overline{x} = x - n\lfloor \frac{x}{n} \rfloor$ denote the integer remainder when x is divided by n. (The positive integer n will be clear from context.) Yang, Ellis, Mamakani, and Ruskey [24] proved the following lemma.

Lemma 2.1. *There are exactly n ways to factor the n-cycle $\sigma = (0, 1, \ldots, n-1)$ as the product of two involutions of $\{0, 1, 2, \ldots, n-1\}$. The n factorizations are $\sigma = I_k \circ I_{k-1}$, $1 \le k \le n$, where $I_k(x) = \overline{k - x}$ is the integer remainder when $k - x$ is divided by n.*

Our notational preference for modular arithmetic is influenced by page 158 of [12], where the setting is different but the factorization is similar. In [24], the proof of Lemma 2.1 is quite short, elementary, and easy to read. As we show in Proposition 2.4 below, the proof of Lemma 2.1 can be adapted to the product of two m cycles, and therefore can be used as the basis for an alternative proof of (1.4). Corresponding lemmas appear in [16] and [20], but the derivations there are based on a graph theoretical insight and appear to be different from the proof that is presented here.

For any permutation σ, we can apply Lemma 2.1 separately to each of the cycles of σ. Therefore a consequence of Lemma 2.1 is that the product of the cycle lengths is a lower bound:

$$\mathbf{N}_n(\sigma) \ge \mathbf{B}_n(\sigma). \tag{2.1}$$

This inequality is not sharp because, in the factorization $\sigma = \tau_2 \circ \tau_1$, there is no requirement that the cycles of σ are invariant under the involutions τ_1 and τ_2. For example, we can write $\sigma = (1,2,3)(4,5,6)$ as $\tau_2 \circ \tau_1$, where $\tau_2 = (1,4)(2,6)(3,5)$ and $\tau_1 = (1,6)(2,5)(3,4)$. Both involutions "exchange" the elements of $\{1,2,3\}$ with those of $\{4,5,6\}$. The next lemma asserts that there are no other possibilities.

Lemma 2.2. *Suppose $\mathcal{O}$ is the set of points on a cycle of σ, and that $\sigma = \tau_2 \circ \tau_1$ is a factorization of σ into two involutions. Then $\tau_1(\mathcal{O}) = \tau_2(\mathcal{O})$, and $\tau_1(\mathcal{O})$ is the set of points on a cycle of σ of length $|\mathcal{O}|$.*

Proof. Because each τ_i is a bijection, it is clear that $|\tau_1(\mathcal{O})| = |\tau_2(\mathcal{O})| = |\mathcal{O}|$.

Suppose y_1, y_2 are points in $\tau_1(\mathcal{O})$. We need to verify that y_1 and y_2 are on the same cycle of σ. Let x_1, x_2 be their preimages in $\mathcal{O}$, that is, $\tau_1(x_i) = y_i$, $i = 1, 2$. Because x_1 and x_2 are on the same cycle $\mathcal{O}$, we have $x_2 = \sigma^\ell(x_1)$ for some ℓ. But then $y_2 = \tau_1(\sigma^\ell(x_1)) = \tau_1 \circ (\tau_2 \circ \tau_1)^\ell(x_1) = (\tau_1 \circ \tau_2)^\ell \circ \tau_1(x_1) = \sigma^{-\ell}(y_1)$. Thus y_1 and y_2 are on the same cycle, and $\tau_1(\mathcal{O})$ is a single cycle of length $|\mathcal{O}|$.

Finally, note that $\tau_2 = \sigma \circ \tau_1$. If $x \in \mathcal{O}$, then the set of points on the cycle of σ that contains $\tau_2(x)$ is $\{v : v = \sigma^t \circ \tau_2(x) \text{ for some } t \in \mathbb{Z}\} = \{v : v = \sigma^{t+1} \circ \tau_1(x) \text{ for some } t \in \mathbb{Z}\}$, and the latter set is the set of points on the cycle of σ that contains $\tau_1(x)$. This proves that $\tau_1(\mathcal{O}) = \tau_2(\mathcal{O})$; the two involutions both map $\mathcal{O}$ to the same cycle. □

Definition 2.3. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be two distinct sets of points on cycles of σ. Two involutions τ_1 and τ_2 *exchange* $\mathcal{O}_1$ and $\mathcal{O}_2$ provided that $\sigma = \tau_2 \circ \tau_1$ and $\tau_1(\mathcal{O}_1) = \tau_2(\mathcal{O}_1) = \mathcal{O}_2$.

Lemma 2.4. *If $\sigma = (0,1,2,\ldots,n-1)(n,n+1,n+2,\ldots,2n-1)$, then there are precisely n ways to write σ as a product of two involutions of $\{0,1,\ldots,2n-1\}$ that exchange the two cycles of σ.*

EXAMPLE: If $n = 5$, then one of the five factorizations is $(0,1,2,3,4)(5,6,7,8,9) = J_3 \circ J_2$,
where $J_3 = (0,8)(1,7)(2,6)(3,5)(4,9)$ and $J_2 = (0,7)(1,6)(2,5)(3,9)(4,8)$.

Proof. Let $X = \{0,1,\ldots,2n-1\}$. For integral k, define J_k to be the involution whose n transpositions are $(x, n+\overline{k-x})$, $x = 0,1,2,\ldots,n-1$. Note that $J_k(x) = J_{k\pm n}(x)$, so we are free to calculate the index k modulo n. Also note that if $y = n+\overline{k-x}$, then $J_k(y) = \overline{x}$. Hence it is straightforward to verify that, for any integer k, $\sigma = J_k \circ J_{k-1}$. Since there are n choices for $\overline{k}$, this proves that there *at least* n of the factorizations.

Now suppose $\sigma = S \circ T$ for some involutions S and T on X, and suppose S and T exchange the two cycles of σ. Because S exchanges the cycles of σ, there must be some k for which $S(0) = n+\overline{k}$. To prove the lemma, it suffices to prove that $S = J_k$ and $T = J_{k-1}$. We use induction to show that, for $0 \le i < n$, $S(i) = n+\overline{k-i}$ and $T(i) = n+\overline{k-1-i}$.

For the base case $i = 0$, we already have $S(0) = n+\overline{k}$. Note that $T(n+\overline{k-1}) = S^2 \circ T(n+\overline{k-1}) = S \circ \sigma(n+\overline{k-1}) = S(n+\overline{k}) = 0$. Therefore $T(0) = n+\overline{k-1}$. This completes the base case $i = 0$.

Now let $0 < i < n-1$, and assume the inductive hypothesis. Since $i = \sigma(i-1) = ST(i-1)$, we have

$$S(i) = S^2 \circ T(i-1) = T(i-1) \underbrace{=}_{\text{ind.hypoth.}} n+\overline{k-1-(i-1)} = n+\overline{k-i}.$$

Similarly

$$T(n+\overline{k-i-1}) = S^2 \circ T(n+\overline{k-i-1}) = S \circ \sigma(n+\overline{k-i-1}) = S(n+\overline{k-i}) = i.$$

Therefore

$$T(i) = n+\overline{k-1-i}.$$

□

For nonnegative integers m and k define

$$V_m(k) = \sum_{j=0}^{\lfloor m/2 \rfloor} \frac{k^{-j} m!}{2^j j!(m-2j)!} = \frac{He_m\left(i\sqrt{k}\right)}{\left(i\sqrt{k}\right)^m}, \tag{2.2}$$

where He_m is the "probabilists' Hermite polynomial" $He_m(x) = m! \sum_{r=0}^{\lfloor m/2 \rfloor} \frac{(-1)^r}{r!(m-2r)!} \frac{x^{m-2r}}{2^r}$. We thank Victor Moll for pointing out this connection with the Hermite polynomials. A less general version appears as equation 2 of Moser and Wyman [18].

Theorem 2.5. *(Lugo, Petersen,Tenner) If $c_k(\sigma)$ denotes the number of k-cycles that $\sigma \in S_n$ has, then*

$$\mathbf{N}_n(\sigma) = \mathbf{B}_n(\sigma) \prod_{k=1}^{n} V_{c_k}(k).$$

Proof. By Lemma 2.2, any involution factorization of σ exchanges some number of pairs of cycles of the same size, and leaves the rest fixed. For each $j \leq \lfloor c_k/2 \rfloor$, there are precisely $\frac{c_k!}{2^j j!(c_k-2j)!}$ ways to match j pairs of k-cycles for swapping, leaving the remaining $c_k - 2j$ k-cycles to be fixed. Once the j pairs have been specified, Lemmas 2.1 and 2.4 show that there are $k^j \cdot k^{c_k-2j}$ ways to factor the k-cycles. Hence, the total number of factorizations of σ is $\prod_{k=1}^{n} \sum_{j=0}^{\lfloor c_k/2 \rfloor} \frac{k^{c_k-j} c_k!}{2^j j!(c_k-2j)!} = \prod_{k=1}^{n} k^{c_k} V_{c_k}(k)$. □

3. Approximation by $\mathbf{B}_n$

Let $\mathbf{T}_n(\sigma)$ be the order of σ as an element of the symmetric group, i.e. the least common multiple of the cycle lengths. The asymptotic distribution of $\mathbf{T}_n$ was deduced from that of $\mathbf{B}_n$. (See equation 14.4 of [10], section 7 of [6], and Lemma 2 of [4].) A similar strategy is used in this paper. The goal of this section is to prove that $\mathbf{B}_n$ can serve as a proxy for $\mathbf{N}_n$.

The following deterministic lemma supplies a sufficient condition on σ that, when satisfied, imposes a bound on the error of the approximation.

Lemma 3.1. *Suppose $\xi \geq 1$ and that, for every integer $k > \xi$, we have $c_k(\sigma) \leq 1$. Also assume that, for every positive integer k, $c_k(\sigma) \leq \xi$. Then there is a constant $c > 0$, not dependent on σ nor ξ, such that $\mathbf{B}_n(\sigma) \leq \mathbf{N}_n(\sigma) \leq \mathbf{B}_n(\sigma) \cdot \left(c\xi^{\xi}\right)^{\xi}$.*

Proof. We already have the lower bound (See equation 2.1). Observe that $V_0(k) = 1$ and $V_1(k) = 1$ for all $k \in [n]$. For $2 \leq m < \xi$ and $1 \leq k \leq \xi$, a very crude bound for $V_m(k)$ suffices. For example, by Stirling's formula we see that for $2 \leq m < \xi$,

$$V_m(k) \leq m! \sum_{j=0}^{\lfloor m/2 \rfloor} \frac{1}{(2k)^j j!} \leq m! e^{\frac{1}{2k}} < c m^m,$$

where c is a positive constant independent of k and m. By assumption $c_k(\sigma) \leq \xi$ for all $k \leq \xi$. Therefore

$$\mathbf{N}_n(\sigma) \leq \mathbf{B}_n(\sigma) \cdot \left(\prod_{1 \leq k \leq \xi} V_{c_k(\sigma)}(k) \right) \leq \mathbf{B}_n(\sigma) \cdot \left(c\xi^{\xi}\right)^{\xi}.$$

□

Clearly $\mathbf{B}_n(\sigma)$ is not *always* a good approximation for $\mathbf{N}_n(\sigma)$. For example, if σ is the identity permutation with n cycles of length one, then $\log \mathbf{B}_n(\sigma) = 0$ and $\log \mathbf{N}_n(\sigma) \sim \frac{n}{2} \log n$. There is a tradeoff when applying Lemma 3.1. The parameter $\xi = \xi(n)$ must

be sufficiently large so that most permutations satisfy the hypotheses. However the larger ξ is, the cruder the bound. The next two lemmas make this precise.

Lemma 3.2. *If $\xi = \xi(n) \to \infty$ as $n \to \infty$, and if $\mathbb{P}_n$ is the uniform probability measure on S_n, then $\mathbb{P}_n(c_k \geq 2$ for some $k \geq \xi) = O(\frac{1}{\xi})$.*

Proof. For any choice of ξ, Boole's inequality implies that

(3.1)
$$\mathbb{P}_n(c_k \geq 2 \text{ for some } k \geq \xi) \leq \sum_{k \geq \xi} \mathbb{P}_n(c_k \geq 2) = \sum_{k=\lceil \xi \rceil}^{\lfloor \frac{n}{2} \rfloor} \left[1 - \mathbb{P}_n(c_k = 0) - \mathbb{P}_n(c_k = 1)\right].$$

It is well known that the probabilities $\mathbb{P}_n(c_k = j)$ can be calculated using the Principle of Inclusion Exclusion, and that the alternating inequalities yield upper and lower bounds. (See also chapter 5 of Sachkov [22] for the "generatingfunctionological"approach). Thus

$$\mathbb{P}_n(c_k = 0) = \sum_{j=0}^{\lfloor \frac{n}{k} \rfloor} (-1)^j \frac{1}{j! k^j} \geq 1 - \frac{1}{k}, \tag{3.2}$$

and

$$\mathbb{P}_n(c_k = 1) = \frac{1}{k} \sum_{j=0}^{\lfloor n/k - 1 \rfloor} (-1)^j \frac{1}{j! k^j} \geq \frac{1}{k} \left(1 - \frac{1}{k}\right). \tag{3.3}$$

Putting (3.2) and (3.3) into (3.1), we get

$$\mathbb{P}_n(c_k \geq 2 \text{ for some } k \geq \xi) \leq \sum_{k=\lceil \xi \rceil}^{\lfloor \frac{n}{2} \rfloor} \left[1 - \left(1 - \frac{1}{k}\right) - \frac{1}{k}\left(1 - \frac{1}{k}\right)\right] = \sum_{k=\lceil \xi \rceil}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{k^2} = O\left(\frac{1}{\xi}\right).$$

□

The second hypothesis is even more likely to hold.

Lemma 3.3. *If $\xi = \xi(n) \to \infty$, then $\mathbb{P}_n(c_k \geq \xi$ for some $k \leq \xi) = O((\frac{\xi}{e^\xi} + \frac{\xi}{n}))$.*

Proof. Let $\mathbf{Z}_k$, $\xi \leq k \leq n$ be a sequence of independent Poisson$(1/k)$ random variables. By Theorem 4 of [5], $\mathbb{P}_n(c_k \leq \xi \text{ for all } k \leq \xi) = \Pr(\mathbf{Z}_k \leq \xi \text{ for all } k \leq \xi) + O(\frac{\xi}{n})$. Standard estimates using Markov's inequality and moment generating functions shows that this probability is small:

$$\begin{aligned} \Pr(\mathbf{Z}_k \geq \xi) &= \Pr(e^{\mathbf{Z}_k} \geq e^\xi) \\ &\leq \frac{\mathbb{E}(e^{\mathbf{Z}_k})}{e^\xi} = \frac{e^{\frac{1}{k}(e-1)}}{e^\xi} < \frac{8}{e^\xi}. \end{aligned}$$

Therefore

$$\Pr(\mathbf{Z}_k \leq \xi \text{ for all } k \leq \xi) \geq \left(1 - \frac{8}{e^\xi}\right)^\xi = 1 - O\left(\frac{\xi}{e^\xi}\right).$$

□

4. The Asymptotic Lognormality of $\mathbf{N}_n$

It is well known that $\mathbf{B}_n$ is asymptotically lognormal.

Lemma 4.1. *(Erdös and Turán) For any real number x,*

$$\lim_{n\to\infty} \mathbb{P}_n(\log \mathbf{B}_n(\sigma) \leq \mu_n + x\sigma_n) = \Phi(x)$$

where $\mu_n = \sum_{k=1}^{n} \frac{\log k}{k} \sim \frac{1}{2}\log^2 n$, $\sigma_n^2 = \sum_{k=1}^{n} \frac{\log^2 k}{k} \sim \frac{1}{3}\log^3 n$, *and* $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2}\, dt$.

Remark 4.2. The first proof Lemma 4.1 is in the work of Erdös and Turán [11]. Alternative proofs, as well as stronger and more general results have been proved using quite varied techniques. See, for example, [2], [3], [4], [9], [17].

Theorem 4.3. $\mathbb{P}_n(\log \mathbf{N}_n(\sigma) \leq \mu_n + x\sigma_n) = \Phi(x) + o(1)$.

Proof. Because $\mathbf{N}_n(\sigma) \geq \mathbf{B}_n(\sigma)$ for all $\sigma \in S_n$, one direction is an immediate consequence of Lemma 4.1.

$$\mathbb{P}_n(\log \mathbf{N}_n \leq \mu_n + x\sigma_n) \leq \mathbb{P}_n(\log \mathbf{B}_n \leq \mu_n + x\sigma_n) = \Phi(x) + o(1). \tag{4.1}$$

For the other direction, we use the continuity of Φ and the bound $\mathbf{N}_n(\sigma) \leq (c\xi^{\xi})^{\xi}\mathbf{B}_n(\sigma)$ from Lemma 3.1, which, due to Lemma 3.2 and Lemma 3.3, holds with probability $1 - O(\frac{1}{\xi} + \frac{\xi}{n} + \frac{\xi}{e^{\xi}})$.

In more detail, let $\epsilon > 0$ be a fixed but arbitrarily small positive number. We can choose $\delta > 0$ so that $|\Phi(x) - \Phi(a)| < \epsilon$ whenever $|x - a| < \delta$. If we choose $\xi = \sqrt{\log n}$, then we have $\log\big((c\xi^{\xi})^{\xi}\big) = o(\sigma_n)$. Therefore we can choose N_ϵ so that, for all $n \geq N_\epsilon$, $\log\big((c\xi^{\xi})^{\xi}\big) < \frac{\delta\sigma_n}{2}$. But then

$$\mathbb{P}_n(\log \mathbf{N}_n(\sigma) \leq \mu_n + x\sigma_n) \geq \mathbb{P}_n\Big(\log \mathbf{B}_n(\sigma) + \log\Big((c\xi^{\xi})^{\xi}\Big) \leq \mu_n + x\sigma_n\Big) \tag{4.2}$$

$$\geq \mathbb{P}_n\left(\log \mathbf{B}_n(\sigma) + \frac{\delta\sigma_n}{2} \leq \mu_n + x\sigma_n\right) \tag{4.3}$$

$$= \mathbb{P}_n\left(\log \mathbf{B}_n(\sigma) \leq \mu_n + \left(x - \frac{\delta}{2}\right)\sigma_n\right) \tag{4.4}$$

$$= \Phi\left(x - \frac{\delta}{2}\right) + o(1) > \Phi(x) - \epsilon + o(1). \tag{4.5}$$

Yet $\epsilon > 0$ was arbitrary, and so $\mathbb{P}_n(\log \mathbf{N}_n(\sigma) \leq \mu_n + x\sigma_n) \geq \Phi(x) + o(1)$. □

References

[1] Amdeberhan, Tewodros and Moll, Victor H., Involutions and their progenies, *J. Comb.*, **6**, (2015), no. 4, 483–508.

[2] Arratia, Richard and Barbour, A. D. and Tavaré, Simon, Logarithmic combinatorial structures: a probabilistic approach, *EMS Monographs in Mathematics*, (2003) ISBN 3-03719-000-0.

[3] Arratia, R. and Barbour, A. D. and Tavaré, S., Limits of logarithmic combinatorial structures, *Ann. Probab.*, **28**, (2000), no.4, 1620–1644.

[4] Arratia, Richard and Tavaré, Simon, Limit theorems for combinatorial structures via discrete process approximations, *Random Structures Algorithms*, **3**, (1992), no. 3, 321–345.

[5] Arratia, Richard and Tavaré, Simon, The cycle structure of random permutations, *Ann. Probab.*, **20**,(1992), no.3, 1567–1591.

[6] Best, M. R., The distribution of some variables on symmetric groups, *Nederl. Akad. Wetensch. Proc. Ser. A* **73**=*Indag. Math.*, **32**, (1970), 385–402.

[7] Burnette, Charles, Drexel University Doctoral Dissertation, in. prep.

[8] Chowla, S. and Herstein, I. N. and Moore, W. K., On recursions connected with symmetric groups. I, *Canadian J. Math.*, **3** (1951), 328-334.

[9] DeLaurentis, J. M. and Pittel, B. G., Random permutations and Brownian motion, *Pacific J. Math.*, **119**, (1985), no. 2, 287–301.

[10] Erdős, P. and Turán, P., On some problems of a statistical group-theory. I, *Z. Wahrscheinlichkeitstheorie und Verw. Gebiete*, **4**, (1965), 175-186.

[11] Erdős, P. and Turán, P., On some problems of a statistical group-theory. III, *Acta Math. Acad. Sci. Hungar.*, **18**, (1967), 309-320.

[12] Gustafson, W. H. and Halmos, P. R. and Radjavi, H., Products of Involutions, *Linear Algebra and Appl.*, **13**, (1976), no. 1/2, 157-162.

[13] Goupil, Alain and Schaeffer, Gilles, Factoring n-cycles and counting maps of given genus, *European J. Combin.*, **19**, 1998, no. 7, 819–834.

[14] Irving, John, On the number of factorizations of a full cycle, *J. Combin. Theory Ser. A*, **113**, 2006, no. 7, 1549–1554.

[15] Lugo, Michael T., The cycle structure of compositions of random involutions, (2009), arXiv:0911.3604 [math.CO].

[16] Lugo, Michael T., Profiles of large combinatorial structures, Thesis (Ph.D.)–University of Pennsylvania, ProQuest LLC, Ann Arbor, MI, 2010, ISBN = 978-1124-31808-0.

[17] Manstavičius, E., The Berry-Esseen bound in the theory of random permutations, Ramanujan J., **2**, (1998), no. 1-2, 185–199.

[18] Moser, Leo and Wyman, Max, On solutions of $x^d = 1$ in symmetric groups, Canad. J. Math., **7**, (1955) 159–168.

[19] Moser, Leo and Wyman, Max, Asymptotic expansions, *Canad. J. Math.*, **8**, 1956, 225–233.

[20] Petersen, T. Kyle and Tenner, Bridget Eileen, How to write a permutation as a product of involutions (and why you might care),*Integers*,**13**, (2013), Paper No. A63, 20.

[21] Roberts, John A. G. and Vivaldi, Franco, A combinatorial model for reversible rational maps over finite fields, *Nonlinearity*, **22**, 2009, no. 8, 1965–1982.

[22] Sachkov, Vladimir N., Probabilistic methods in combinatorial analysis, *Encyclopedia of Mathematics and its Applications*, **56**, Cambridge University Press, Cambridge, 1997, ISBN 0-521-45512-X.

[23] OEIS Sequence A000085, Number of self-inverse permutations on n letters, also known as involutions; number of Young tableaux with n cells, (Formerly M1221 N0469), *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://oeis.org.

[24] Yang, Qingxuan and Ellis, John and Mamakani, Khalegh and Ruskey, Frank, In-place permuting and perfect shuffling using involutions, *Inform. Process. Lett.*, **113** (2013), no. 10-11, 386–391.