

PERMUTATIONS WITH ROOTS

MIKLÓS BÓNA, ANDREW MCLENNAN, AND DENNIS WHITE

ABSTRACT. We prove that the probability $p_2(n)$ that a random permutation of length n has a square root is monotonically nonincreasing in n . More generally, we prove that the probability $p_r(n)$ that a random permutation of length n has an r th root, r prime, is monotonically nonincreasing in n . We also show for all $r \geq 2$ that $p_r(n) \rightarrow 0$ as $n \rightarrow \infty$. While doing this, we combinatorially prove that $p_r(n) = p_r(n+1)$ for r prime and for all n not congruent to $-1 \pmod r$, and we construct several bijections for sets of permutations defined by modular class restrictions on the cycle lengths. We also include a simple probabilistic proof that, for $r \geq 2$, $p_r(n) \rightarrow 0$ as $n \rightarrow \infty$.

1. INTRODUCTION

Let $\sigma \in S_n$ be a permutation of length n . If there exists another permutation $\gamma \in S_n$ so that $\gamma^2 = \sigma$, then we say that σ has a *square root*. Certainly, σ may have one, or many square roots, or it may have none. Let $POWER_2(n)$ be the set of permutations of length n , or, in what follows, n -permutations, that have at least one square root, and let $p_2(n) = |POWER_2(n)|/n!$. In other words, $p_2(n)$ is the probability that a random permutation of length n has a square root. Asymptotic properties of $p_2(n)$ were studied in [1] and [3]. In this paper we prove the conjecture of Wilf [8] that $p_2(n)$ is monotonically nonincreasing in n .

More generally, let $\sigma \in S_n$ be a permutation of length n . If there exists another permutation $\gamma \in S_n$ so that $\gamma^r = \sigma$, then we say that σ has an *r th root* and that σ is an *r th power*. Let $POWER_r(n)$ be the set of n -permutations that have at least one r th root, and let $p_r(n) = |POWER_r(n)|/n!$. We prove that $p_r(n)$ is monotonically nonincreasing in n for r prime. We also show that $\lim_{n \rightarrow \infty} p_r(n) = 0$ for all r . Our proof that $p_r(n)$ is monotonic for r prime is mostly combinatorial. We give two proofs of the limit theorem for r prime. One uses the bounds we obtain in our proof of monotonicity. The other is probabilistic. The limit theorem for general r follows easily from the prime case.

The outline of this paper will be as follows. In Section 2 we construct several bijections that show how fast the number of n -permutations satisfying some relevant cycle length restrictions grows when n grows. In Section 3 we characterize permutations that have r th roots, r prime, in terms of their cycle lengths. This characterization leads us to the notion of a pseudopower to extend results to composite numbers. We then use the results of Section 2 to describe combinatorially how the probability of an r th power grows. We are required to make special arguments when the permutation has length a multiple of r^2 . We conclude that the

Date: August 17, 1999.

This paper was written while the first author's stay at the Institute was supported by Trustee Ladislaus von Hoffmann, the Arcana Foundation.

probability of an r th power tends to zero as n tends to infinity. Finally in Section 4 we give a probabilistic proof of this limit theorem.

2. PERMUTATIONS WITH CYCLE LENGTHS OF A GIVEN MODULAR CLASS

Permutations which have r th roots, r prime, have certain restrictions on the cycles of lengths which are multiples of r , as we shall see in the next section. In this section, we investigate the combinatorics of permutations whose cycles of lengths rk have been specified. Throughout this paper, we will write our permutations in the following canonical way. In each cycle, we will write the largest entry first, and we will write the cycles in increasing order of their first entry, such as in $(4\ 1\ 2)(6)(7\ 5\ 3)(8)$. Basic facts about the cycle decomposition of permutations can be found in [6].

For any permutation $\pi \in S_n$, the *type* of π is the partition given by its cycle lengths. So the type of $(4\ 1\ 2)(5\ 3)(6)(8\ 7)(9)$ is $(3, 2, 2, 1, 1)$. The type of π is an integer partition of n .

Let $NODIV_r(n)$ be the set of n -permutations with no cycle lengths a multiple of r . We first construct a bijection Ψ from $NODIV_r(n) \times [n+1]$ onto $NODIV_r(n+1)$, where $n+1$ is not a multiple of r . Our construction will be recursive.

Let $\pi \in NODIV_r(n)$, and let $k \leq n+1$ be a positive integer. First, adjust π so that k is not a letter in π by simply increasing all values $\geq k$ in π by 1. Now define $\Psi(\pi, k)$ as follows. With π written in canonical form, let c denote the last cycle of π and let l be its length. If $k = n+1$, then create the singleton cycle $(n+1)$. If $k \neq n+1$ and $l \not\equiv -1 \pmod{r}$, then place k at the end of c .

Finally, if $k \neq n+1$ and $l \equiv -1 \pmod{r}$, then apply Ψ^{-1} to $\tilde{\pi} = \pi - c$. Call the resulting pair $(\tilde{\sigma}, \tilde{k})$. Note that this is allowed since $\tilde{\pi} \in NODIV_r(n-l)$ and $n-l = n+1 \pmod{r}$. The result of Ψ applied to (π, k) is given by $\tilde{\sigma}$ with the cycle \tilde{c} adjoined, where \tilde{c} is c with $\tilde{k}k$ attached to the end.

Lemma 2.1. *For all $r \geq 2$ and $n+1$ not a multiple of r , the map Ψ is a bijection from $NODIV_r(n) \times [n+1]$ onto $NODIV_r(n+1)$.*

Proof. To find the inverse of Ψ , take $\sigma \in NODIV_r(n+1)$ in canonical form and let k be the last letter in σ and let c be the last cycle (whose length is l) in σ . If $l = 1$, then remove $k = n+1$ from σ to form π . If $l \not\equiv 1 \pmod{r}$, again remove k from c to form π . Finally, if $l \equiv 1 \pmod{r}$ and $l \neq 1$, then let \tilde{k} be the next-to-last letter in c , let $\tilde{\sigma}$ be σ with c removed and let $\tilde{\pi} = \Psi(\tilde{\sigma}, \tilde{k})$. Then let \tilde{c} be c with k and \tilde{k} removed, and π is $\tilde{\pi}$ with \tilde{c} adjoined. \square

Example 2.2. If $r = 3$ and $(\pi, k) = ((6\ 1\ 2\ 5\ 3)(7), 4)$, then we get $\Psi(\pi, k) = (6\ 1\ 2\ 5\ 3)(7\ 4)$.

Example 2.3. If $r = 3$ and $(\pi, k) = ((6\ 1\ 2\ 5)(7\ 3), 4)$, we first compute

$$\Psi^{-1}((6\ 1\ 2\ 5)) = ((2)(6\ 1), 5).$$

Then we get $\Psi(\pi, k) = (2)(6\ 1)(7\ 3\ 5\ 4)$.

Remark 2.4. Lemma 2.1 may be refined somewhat to reflect what happens to the length of the last cycle.

Let $nodiv_r(n)$ be the probability that a random n -permutation has no cycles of length a multiple of r , that is, $nodiv_r(n) = |NODIV_r(n)|/n!$.

Corollary 2.5. *If $n + 1$ is not a multiple of r , then $\text{nodiv}_r(n) = \text{nodiv}_r(n + 1)$.*

The case where $n + 1$ is a multiple of r is somewhat similar. The bijection Φ will map $\text{NODIV}_r(n) \times [n]$ onto $\text{NODIV}_r(n + 1)$. Take a pair $(\pi, k) \in \text{NODIV}_r(n) \times [n]$, and let c be the cycle of π containing k . Let l be the length of c and let $\tilde{\pi}$ be π with c removed. Now let $\sigma = \Psi(\tilde{\pi}, k)$. Note that this is allowed since $\tilde{\pi} \in \text{NODIV}_r(n - l)$ and $n - l + 1 \not\equiv 0 \pmod{r}$. Finally, replace k in c with $n + 1$ to form \tilde{c} . The image of (π, k) under Φ is then σ with \tilde{c} adjoined.

Lemma 2.6. *The map Φ is a bijection from $\text{NODIV}_r(n) \times [n]$ onto $\text{NODIV}_r(n + 1)$.*

Proof. To get the unique preimage of $\sigma \in \text{NODIV}_r(n + 1)$ under Φ , let c be the cycle (of length l) containing $n + 1$ and let $\tilde{\sigma}$ be σ with c removed. Run $\tilde{\sigma}$ through Ψ^{-1} to get $(\tilde{\pi}, k)$. This is allowed since $\tilde{\sigma} \in \text{NODIV}_r(n + 1 - l)$ and $n + 1 - l \not\equiv 0 \pmod{r}$. Now replace $n + 1$ in c with k to get \tilde{c} and adjoin \tilde{c} to $\tilde{\pi}$ to get π . The preimage is then (π, k) . \square

Example 2.7. If $r = 3$ and $(\pi, k) = ((6\ 1\ 2\ 4\ 5)(7\ 3)(8), 5)$, we first compute $\Psi((7\ 3)(8), 5) = (7\ 3)(8\ 5)$. Then we get $\Phi(\pi, k) = (7\ 3)(8\ 5)(9\ 6\ 1\ 2\ 4)$.

Example 2.8. If $r = 3$ and $(\pi, k) = ((6\ 3)(7)(8\ 1\ 2\ 4\ 5), 7)$, we first compute $\Psi((6\ 3)(8\ 1\ 2\ 4\ 5), 7) = (6)(8\ 1\ 2\ 4\ 5\ 3\ 7)$. Then we get $\Phi(\pi, k) = (6)(8\ 1\ 2\ 4\ 5\ 3\ 7)(9)$.

Corollary 2.9. *If $n + 1$ is a multiple of r , then $\text{nodiv}_r(n + 1) = \text{nodiv}_r(n) \cdot \frac{n}{n+1} < \text{nodiv}_r(n)$.*

The bijection Ψ can be extended to n -permutations with cycles of length kr specified. Let $\text{DIV}_{\rho,r}(n)$ be the set of n -permutations whose cycles of length a multiple of r have type ρ . For instance, $\text{DIV}_{(9,9,3),3}(30)$ is the set of permutations of $[30]$ with two 9-cycles, one 3-cycle, and no other cycles whose lengths are multiples of 3. Notice that $\text{DIV}_{\emptyset,r}(n) = \text{NODIV}_r(n)$.

For $\pi \in \text{DIV}_{\rho,r}(n)$, let $\pi_{(r)}$ denote the part of π consisting of the cycles of lengths which are multiples of r and let $\pi_{(\sim r)}$ denote the part of π consisting of cycles of lengths which are not multiples of r . For example, if

$$\pi = (7\ 3)(10\ 6\ 9\ 1)(11)(13\ 5\ 2\ 8)(14\ 12\ 4),$$

then $\pi_{(2)} = (7\ 3)(10\ 6\ 9\ 1)(13\ 5\ 2\ 8)$ and $\pi_{(\sim 2)} = (11)(14\ 12\ 4)$.

Now define the bijection Ψ from $\text{DIV}_{\rho,r}(n) \times [n + 1]$ onto $\text{DIV}_{\rho,r}(n + 1)$, where $n + 1$ is not a multiple of r , as follows. Let π be an n -permutation and $k \leq n + 1$. As before, adjust the letters of π by adding one to all letters k or larger. Now apply Ψ to $(\pi_{(\sim r)}, k)$ to get $\sigma_{(\sim r)}$ and let $\sigma_{(r)} = \pi_{(r)}$.

Lemma 2.10. *The map Ψ is a bijection from $\text{DIV}_{\rho,r}(n) \times [n + 1]$ onto $\text{DIV}_{\rho,r}(n + 1)$, where $n + 1$ is not a multiple of r .*

Proof. To form the preimage of $\sigma \in \text{DIV}_{\rho,r}(n + 1)$, apply Ψ^{-1} to $\sigma_{(\sim r)}$ to get $(\pi_{(\sim r)}, k)$ and let $\pi_{(r)} = \sigma_{(r)}$. \square

Example 2.11. If $r = 3$ and $(\pi, k) = ((5\ 2)(6\ 1\ 4)(8\ 3), 7)$, we first compute $\Psi((5\ 2)(8\ 3), 7) = 3D(5)(8\ 3\ 2\ 7)$. Then we get $\Psi(\pi, k) = (5)(6\ 1\ 4)(8\ 3\ 2\ 7)$.

Let $\text{div}_{\rho,r}(n)$ denote the probability that a random n -permutation has only cycles with lengths multiples of r given by ρ , that is, $\text{div}_{\rho,r}(n) = |\text{DIV}_{\rho,r}(n)|/n!$.

Corollary 2.12. *If $n + 1$ is not a multiple of r then $div_{\rho,r}(n) = div_{\rho,r}(n + 1)$.*

The bijection Φ cannot be extended in the same way. Since the bijection Ψ used $k \in [n + 1]$ as an additional letter, it could also be used as an additional letter in the part of the permutation not containing cycles of lengths $\equiv 0 \pmod r$. However, the bijection Φ used $k \in [n]$ as one of the letters of the permutation. Difficulties emerge when this letter is in a cycle of length $\equiv 0 \pmod r$. Nevertheless, Φ can be extended in a slightly different way.

Suppose $n + 1$ is a multiple of r and ρ is a partition of $m < n$ with all parts multiples of r . We will define a bijection Γ from $DIV_{\rho,r}(n + 1) \times [n + 1 - m]$ onto $DIV_{\rho,r}(n) \times [n - m] \times [n + 1]$.

Let $\pi \in DIV_{\rho,r}(n + 1)$ and let k be a letter in $\pi_{(\sim=r)}$. Thus, $(\pi, k) \in DIV_{\rho,r}(n + 1) \times [n + 1 - m]$.

Now let $\sigma \in DIV_{\rho,r}(n)$. Let $j \leq n + 1$ and add one to all the letters in σ which are at least j . Let l be a letter in $\sigma_{(\sim=r)}$. Thus, $(\sigma, l, j) \in DIV_{\rho,r}(n) \times [n - m] \times [n + 1]$.

We now define $\Gamma(\pi, k)$ to be (σ, l, j) where the parameters are related as follows. First, $j = k$. Second, replace k in $\pi_{(\sim=r)}$ by $N > n + 1$, creating $\widetilde{\pi_{(\sim=r)}}$. Apply Φ^{-1} to $\widetilde{\pi_{(\sim=r)}}$. The result is $(\sigma_{(\sim=r)}, l)$. Finally, let $\sigma_{(r)} = \pi_{(r)}$.

Lemma 2.13. *The map Γ is a bijection from $DIV_{\rho,r}(n + 1) \times [n + 1 - m]$ onto $DIV_{\rho,r}(n) \times [n - m] \times [n + 1]$, where $n + 1$ is a multiple of r and ρ is a partition of m with all parts a multiple of r .*

Proof. To reverse Γ , begin with $(\sigma, l, j) \in DIV_{\rho,r}(n) \times [n - m] \times [n + 1]$. Let $k = j$ and $\pi_{(r)} = \sigma_{(r)}$. Run $(\sigma_{(\sim=r)}, l)$ through Φ , using $N > n + 1$ as the new added letter, creating the permutation $\tilde{\pi}$. Form $\pi_{(\sim=r)}$ by replacing N with k in $\tilde{\pi}$. \square

Example 2.14. If $r = 3$, $\rho = (3)$, $n = 11$, $\pi = (7\ 6\ 2)(8)(10\ 4\ 1\ 9\ 5)(11)(12\ 3)$ and $k = 9$, then apply Φ^{-1} to $(8)(11)(12\ 3)(N\ 5\ 10\ 4\ 1)$ to get $(8)(10\ 4\ 1\ 3\ 5)(11)(12)$ with $l = 3$. Thus $\sigma = (7\ 6\ 2)(8)(10\ 4\ 1\ 3\ 5)(11)(12)$.

Example 2.15. If $r = 4$, $\rho = (4)$, $n = 11$, $\sigma = (7\ 2)(10\ 1\ 8\ 3)(11\ 9\ 4)(12\ 6)$, $j = 5$ and $l = 9$, then apply Φ to $(7\ 2)(11\ 9\ 4)(12\ 6)$ and 9 to get $\tilde{\pi} = (7\ 2)(12\ 6\ 9)(N\ 4\ 11)$. Thus $\pi = (7\ 2)(10\ 1\ 8\ 3)(11\ 5\ 4)(12\ 6\ 9)$ and $k = 5$.

Corollary 2.16. *If $n + 1$ is a multiple of r and ρ is a partition of m with all parts a multiple of r , then*

$$|DIV_{\rho,r}(n + 1)| = (n + 1) \frac{n - m}{n - m + 1} \cdot |DIV_{\rho,r}(n)| \leq n \cdot |DIV_{\rho,r}(n)|$$

and

$$div_{\rho,r}(n + 1) = div_{\rho,r}(n) \cdot \frac{n - m}{n - m + 1} \leq div_{\rho,r}(n) \cdot \frac{n}{n + 1},$$

where the inequalities are equalities if and only if $\rho = \emptyset$.

3. PERMUTATIONS WHICH ARE POWERS AND PSEUDOPOWERS

We now apply the results of the previous section to permutations which have r th roots. The following Proposition characterizes such permutations, for prime r , in terms of their cycle lengths. It will be our basic tool throughout this section.

Proposition 3.1. *(cf. [8]) A permutation σ has an r th root, r prime, if and only if, for every integer k , the number of cycles of σ of length kr is a multiple of r .*

Proof. When taking the r th power of a permutation γ , each cycle of γ of length relatively prime to r will contribute a cycle of that same length to γ^r . Also each cycle of γ of length kr will contribute r cycles of length k to γ^r . Therefore, if k is a multiple of r , a k -cycle in $\sigma = \gamma^r$ can only be the result of the splitting of a cycle of length rk in γ into r cycles, = so the number of k -cycles of σ is a multiple of r .

Conversely, suppose that σ has this property. We can then create an r th root γ of σ as follows. For cycles in σ whose length is relatively prime to r , (a_1, a_2, \dots, a_k) , write $(b_1, b_2, b_3, \dots, b_k)$ in γ , where $b_1 = a_1, b_{1+r} = a_2, b_{1+2r} = 3Da_3, \dots$, where the subscript arithmetic is done mod k .

For cycles in σ of length $m = kr$, group r m -cycles together:

$$\begin{aligned} &(a_1^1, a_2^1, \dots, a_m^1), \\ &(a_1^2, a_2^2, \dots, a_m^2), \\ &\vdots \\ &(a_1^r, a_2^r, \dots, a_m^r), \end{aligned}$$

and thread them together to form an mr -cycle:

$$= (a_1^1, a_1^2, \dots, a_1^r, a_2^1, a_2^2, \dots, a_2^r, \dots, a_m^1, a_m^2, \dots, a_m^r).$$

Carrying out these respective operations for all cycles of σ we get a permutation γ whose r th power is σ . □

Proposition 3.1 motivates us to define an n -permutation as a r *pseudopower* if the number of cycles of length kr is a multiple of r . If r is prime, then pseudopowers are permutations with roots. Many of our combinatorial results hold for pseudopowers.

As was mentioned in Section 1, let $POWER_r(n)$ be the set of n -permutations that have at least one r th root, and let $p_r(n) = |POWER_r(n)|/n!$. Furthermore, let $PPOWER_r(n)$ be the set of n -permutations which are r pseudopowers and let $pp_r(n) = |PPOWER_r(n)|/n!$. Note that $PPOWER_r$ and pp_r agree with $POWER_r$ and p_r , respectively, when r is prime.

If we examine the first few values of $p_2(n)$ for $n = 1, 2, \dots$ we see that they are equal to 1, 1/2, 1/2, 1/2, 1/2, 3/8, 3/8, 7/20, 7/20, \dots , giving rise to two natural conjectures. The first one is that $p_2(2n) = p_2(2n + 1)$ for all n . This has been proved by Wilf [8] by exponential generating functions and also follows from Corollary 2.12.

The other one is that $p_2(n)$ is nonincreasing. In this section we prove that $pp_r(n)$ is nonincreasing, which, in view of Corollary 2.12, amounts to proving that $pp_r(n) \geq pp_r(n + 1)$ when $n + 1$ is a multiple of r .

A more careful analysis of the above data also shows that while $p_2(6)/p_2(5) = 3/4$, in the next step we get $p_2(8)/p_2(7) = 14/15$, and so we might suspect that the decrease of $pp_r(n)$ slows down. However, we will show that $pp_r(n)$ converges to 0, and still show some explanation of the described phenomenon.

Let $PERM_k(n)$ be the set of n permutations whose cycle lengths are all multiples of k and let $PERM_{k,l}(n)$ be the set of n permutations whose cycle lengths are all multiples of k and each cycle length is repeated a multiple of l times.

Our interest will be in $|PERM_{r,r}(mr^2)|$. Notice that the r th power of any permutation in $PERM_{r^2}(mr^2)$ is a permutation in $PERM_{r,r}(mr^2)$. Also notice that if the cycle length kr^2 appears in $\pi \in PERM_{r^2}(mr^2)$ j times, then the cycle length kr appears in π^r jr times. We exploit this in the proof of the next lemma.

Lemma 3.2. *For all $m \geq 1$, we have*

$$\frac{|PERM_{r^2}(mr^2)|}{|PERM_{r,r}(mr^2)|} > (mr)^{r-1}.$$

Proof. Although this bound may be proved directly from the formula for the number of permutations of a given cycle type, in keeping with the spirit of this paper we give a combinatorial proof.

Let the type ρ of $\pi \in PERM_{r,r}(mr^2)$ consist of rj_i cycles of length ri . For each ri , take the ri cycles in groups of r , and consider the r th roots of π each of whose cycles has the same elements as one of these groups. One way to form such a root is to place the first ri cycle in every r th position, then choose a starting value for the second such ri cycle and place it in every position following one of the elements of the first cycle. Evidently there are $\prod_i (ri)^{(r-1)j_i}$ ways to do this, each producing a different r th root. Therefore there are at least $\prod_i (ri)^{(r-1)j_i}$ such roots, so the result follows if we can show that this product is minimized when $j_m = 1$ and $j_i = 3D0$ for all other i . But this follows easily from the fact that $st \geq s + t$ for all integers $s, t \geq 2$. \square

Lemma 3.3. *For all $m \geq 1$ and $r \geq 2$, except for $m = 1$ and $r = 2$, we have*

$$\frac{|NODIV_r(mr^2)|}{|PERM_{r,r}(mr^2)|} > mr^2.$$

Proof. Using exponential generating functions, it is not difficult to show [8] that

$$(1) \quad |PERM_{r^2}(mr^2)| = (mr^2)! \frac{1 \cdot (1+r^2) \cdot \dots \cdot (1+(m-1)r^2)}{r^2 \cdot 2r^2 \cdot \dots \cdot mr^2}.$$

A similar calculation shows that

$$(2) \quad |NODIV_r(mr^2)| = (mr^2)! \frac{(r-1) \cdot (2r-1) \cdot \dots \cdot (mr^2-1)}{r \cdot 2r \cdot \dots \cdot mr^2}.$$

Taking the ratio of Equation 1 and Equation 2, we have

$$\frac{|NODIV_r(mr^2)|}{|PERM_{r^2}(mr^2)|} = \left(\frac{r-1}{1} \cdot \frac{r^2+r-1}{r^2+1} \cdot \dots \cdot \frac{(m-1)r^2+r-1}{(m-1)r^2+1} \right) \times \left(\frac{(2r-1)}{r} \cdot \frac{(3r-1)}{2r} \cdot \dots \right) > 1.$$

The inequality follows since each factor is at least 1 and at least one factor is > 1 . Thus, the bound for $r \geq 3$ and $m \geq 1$ follows from Lemma 3.2. For $r = 2$ and for $m \geq 4$ we have

$$\frac{|NODIV_2(4m)|}{|PERM_4(4m)|} = \frac{3}{2} \cdot \frac{5}{4} \cdot \dots \cdot \frac{4m-1}{4m-2} \geq \frac{33}{16} > 2.$$

Combining this with Lemma 3.2 gives our result. Finally, for $m = 2, 3$ and $r = 2$, we find directly that

$$\begin{aligned} |NODIV_2(8)| &= 11025, \\ |PERM_{2,2}(8)| &= 1365, \\ |NODIV_2(12)| &= 108056025 \quad \text{and} \\ |PERM_{2,2}(12)| &= 8534295. \end{aligned}$$

\square

Theorem 3.4. *Let $r \geq 2$. Then*

1. *If $n + 1 \not\equiv 0 \pmod r$ then $pp_r(n + 1) = pp_r(n)$.*
2. *If $n + 1 \equiv 0 \pmod r$ but $n + 1 \not\equiv 0 \pmod{r^2}$ then $pp_r(n + 1) < pp_r(n) \frac{n}{n+1}$.*
3. *If $n + 1 \equiv 0 \pmod{r^2}$ then $pp_r(n + 1) < pp_r(n)$ with equality only when $r = 2$ and $n = 3$.*

Proof. By Proposition 3.1, the only possible cycle types for $\pi_{(r)}$ will be the same for $PPOWER_r(n)$ as for $PPOWER_r(n + 1)$ as long as $n + 1$ is not a multiple of r^2 . Therefore, the first statement follows from Corollary 2.12 and the second statement follows from Corollary 2.16.

The third statement will require an examination of permutations in $PERM_{r,r}(n + 1)$, since the cycle types of permutations in $PERM_{r,r}(n + 1)$ will not appear in $PPOWER_r(n)$. Lemma 3.3 shows that the number of such permutations will be small compared to the total number of pseudopowers.

We have from Corollary 2.16 and Proposition 3.1

$$|PPOWER_r(mr^2)| - |PERM_{r,r}(mr^2)| \leq (mr^2 - 1) \cdot |PPOWER_r(mr^2 - 1)|.$$

But for $m > 1$ or $r > 2$, Lemma 3.3, implies the following upper bound on $|PERM_{r,r}(mr^2)|$:

$$|PERM_{r,r}(mr^2)| < \frac{|NODIV_r(mr^2)|}{mr^2} \leq \frac{|PPOWER_r(mr^2)|}{mr^2}.$$

(Here we are using $NODIV_r(mr^2) \subseteq PPOWER_r(mr^2)$, which is a simple implication of Proposition 3.1.) Therefore,

$$|PPOWER_r(mr^2)| \cdot \left(1 - \frac{1}{mr^2}\right) < (mr^2 - 1) \cdot |PPOWER_r(mr^2 - 1)|,$$

which implies that $|PPOWER_r(mr^2)| < (mr^2) \cdot |PPOWER_r(mr^2 - 1)|$. For $m = 1$ and $r = 2$, we can verify the truth of our statement using the numerical data given at the beginning of this section. \square

Theorem 3.4 yields the main results of this paper.

Corollary 3.5. *For all positive integers n and all $r \geq 2$, we have $pp_r(n) \geq pp_r(n + 1)$.*

Corollary 3.6. *For all positive integers n and all $r \geq 2$, we have,*

$$\lim_{n \rightarrow \infty} pp_r(n) = 0.$$

Proof. This result follows from Corollary 3.5, the bound in the second part of Theorem 3.4 and a routine calculation. \square

Corollary 3.7. *For all positive integers n and all $r \geq 2$, we have,*

$$\lim_{n \rightarrow \infty} p_r(n) = 0.$$

Proof. If a permutation has an r th root, it has a q th root for any prime q that divides r , so the probability of an r th root is not greater than the minimum of the probabilities of q th roots for primes q that divide r . \square

4. A PROBABILISTIC PROOF

We now give an independent probabilistic proof of Corollary 3.6 in the following more general setting.

Let $r \geq 2$, let \mathbf{E} be the set of positive integers divisible by r , and let $V = (\mathbf{Z}_r)^{\mathbf{E}}$, where \mathbf{Z}_r are the integers mod r . So the elements of V are infinite strings $\mathbf{v} = (v_r, v_{2r}, v_{3r}, \dots)$. We say that a permutation $\pi \in S_n$ *satisfies* \mathbf{v} if, for each $k = r, 2r, 3r, \dots$ the number of k -cycles in π is congruent to v_k mod r . Let $P_n(\mathbf{v})$ be the probability that a random permutation in S_n satisfies \mathbf{v} , and let

$$M_n = \max_{\mathbf{v} \in V} P_n(\mathbf{v}).$$

Theorem 4.1. $\limsup M_n = 0$.

Proof. Consider the following method of generating a random permutation $\pi \in S_n$. Choose $\pi(1)$ equiprobably from $\{1, \dots, n\}$, choose $\pi(\pi(1))$ equiprobably from $\{1, \dots, n\} - \pi(1)$, and so forth until a cycle is achieved. Then repeat the process beginning with the smallest element of $\{1, \dots, n\}$ that is not in the first cycle, continuing in this fashion until the permutation is complete. It is easy to show ([5], Exercise 3.3) that for any $k = 1, \dots, n$, the first cycle has length k with probability $1/n$, so

$$P_n(\mathbf{v}) = \frac{1}{n} \cdot \left(\sum_{k \not\equiv 0 \pmod r} P_{n-k}(\mathbf{v}) + \sum_{k \equiv 3D0 \pmod r} P_{n-k}(\mathbf{v}'_k) \right),$$

where \mathbf{v}'_k is obtained from \mathbf{v} by subtracting $1 \pmod r$ from v_k . Observe that there is at most one $k > [n/2]$ such that $P_{n-k}(\mathbf{v}'_k) > 0$, for an n -permutation cannot have more than one cycle longer than $[n/2]$. Therefore,

$$(3) \quad M_n \leq \frac{1}{n} \cdot \left(1 + \sum_{k \not\equiv 0 \pmod r} M_{n-k} + \sum_{\substack{k \leq [n/2] \\ k \equiv 0 \pmod r}} M_{n-k} \right).$$

Let $L = \limsup M_n$. Then (3) implies, by routine computations, that $L \leq \frac{2r-1}{2r} \cdot L$, so $L = 0$. \square

Corollary 3.6 now follows because

$$0 \leq \liminf pp_r(n) \leq \limsup pp_r(n) \leq \limsup M_n = 0.$$

5. FURTHER DIRECTIONS

Most of the results of Section 2 have simple generating function proofs. Simply note that the exponential generating function for permutations in $NODIV_r(n)$ is given by

$$\frac{(1-t^r)^{1/r}}{1-t}.$$

Our approach has been to give combinatorial proofs wherever possible. To this end, it would be interesting to find an injective proof of the third part of Theorem 3.4.

ACKNOWLEDGMENT

We are grateful to Richard Stanley, Dennis Stanton and Herb Wilf for helpful remarks.

REFERENCES

- [1] E. A. Bender, Asymptotic methods in Enumeration, *SIAM Rev.* **16** (1974), 485–515. Errata: *SIAM Rev.* = **18** (1976), 292.
- [2] E. A. Bertram, B. Gordon, Counting special permutations. *European J. Combin.* **10** (1989), no. 3, 221–226.
- [3] J. Blum, Enumeration of the square permutations in S_n . *J. Combinatorial Theory*, Series A, **17** (1974), 156–161.
- [4] E. D. Bolker, A. M. Gleason, Counting permutations. *J. Combin. Theory Ser. A* **29** (1980), no. 2, 236–242.
- [5] L. Lovász, **Combinatorial Problems and Exercises**, Akadémiai Kiadó, Budapest, Hungary, second edition, 1993.
- [6] R. Stanley, **Enumerative Combinatorics**, Volume I, Cambridge University Press, Cambridge, UK, second edition, 1997.
- [7] R. Stanley, **Enumerative Combinatorics**, Volume II, Cambridge University Press, Cambridge, UK, 1999.
- [8] H. Wilf, **Generatingfunctionology**, Academic Press, San Diego, second edition, 1994.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NJ 08540
E-mail address: bona@IAS.EDU

DEPARTMENT OF ECONOMICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455
E-mail address: mclennan@icarus.socsci.umn.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MINNESOTA, MINNEAPOLIS, MN 55455
E-mail address: white@math.umn.edu