Enriched Cycle Structures and Roots of Permutations

William Y.C. Chen and Elena L. Wang

Center for Applied Mathematics and KL-AAGDM
Tianjin University
Tianjin 300072, P.R. China

Emails: [1]chenyc@tju.edu.cn, [2]ling_wang2000@tju.edu.cn

Dedicated to Persi Diaconis on the occasion of his 80th birthday

Abstract

This paper is concerned with a duality between r-regular permutations and r-cycle permutations, and a monotone property due to Bóna-McLennan-White on the probability $p_r(n)$ for a random permutation of $\{1,2,\ldots,n\}$ to have an r-th root, where r is a prime. For $r=2$, the duality relates permutations with odd cycles to permutations with even cycles. To handle the general case where $r \geq 2$, we define an r-enriched permutation as a permutation with r-singular cycles colored by one of the colors $1,2,\ldots,r-1$. In this setup, we discover a bijection between r-regular permutations and enriched r-cycle permutations, which in turn yields a stronger version of an inequality of Bóna-McLennan-White. This leads to a fully combinatorial understanding of the monotone property, thereby answering their question. When r is a prime power q^l, we further show that $p_r(n)$ is monotone. In the case that $n+1 \not\equiv 0 \pmod{q}$, the equality $p_r(n) = p_r(n+1)$ has been established by Chernoff.

Keywords: r-regular permutations, nearly r-regular permutations, r-cycle permutations, r-enriched permutations, roots of permutations.

AMS Classification: 05A05, 05A19, 05A20

1 Introduction

This paper is concerned with a duality between r-regular permutations and r-cycle permutations, which are closely related to permutations with an r-th root, see, e.g., [6, 8, 14]. For an integer $r \geq 2$, a cycle is called r-regular if its length is not divisible by r and r-singular otherwise (i.e., if its length is divisible by r). Suppose that permutations are represented in the cycle notation. A permutation is called r-regular provided that all of its cycles are r-regular, and an r-cycle permutation is a permutation where all cycles are r-singular. These terms were introduced by Külshammer, Olsson, and Robinson [14]. As usual, for $n \geq 1$, S_n stands for the set of permutations of $[n] = \{1, 2, \ldots, n\}$. Given a permutation $\sigma \in S_n$, it is said to have an r-th root if there exists a permutation $\pi \in S_n$ such that $\pi^r = \sigma$. Permutations with an r-th root can be characterized in terms of their cycle types [20, p. 158]. For the number of such permutations, one may refer to the sequence A247005 in the OEIS [18]. The exponential generating function for this count was discussed in Bender [2], see also [20, p. 159].

We shall follow the terminology in [14]. Throughout the paper, $\mathrm{Reg}_r(n)$ and $\mathrm{Cyc}_r(n)$ will stand for the set of r-regular permutations of $[n]$ and the set of r-cycle permutations of $[n]$, respectively. Note that $\mathrm{NODIV}_r(n)$ and $\mathrm{PERM}_r(n)$ are used in [8]. For $r \geq 2$ and $n = 0$, set $|\mathrm{Reg}_r(0)| = |\mathrm{Cyc}_r(0)| = 1$. Clearly, $|\mathrm{Cyc}_r(n)| = 0$ whenever $n \not\equiv 0 \pmod{r}$.

The enumeration of r-regular permutations dates back to Erdős and Turán [11]. By using generating functions, they showed that for $n \geq 1$, and r a prime power, the proportion of r-regular permutations in S_n equals

$$\prod_{k=1}^{\lfloor n/r \rfloor} \frac{rk-1}{rk}.$$

It was later observed that the above formula remains true for an arbitrary integer $r \geq 2$, for example, see [17].

There are various ways to count $\mathrm{Reg}_r(n)$ and $\mathrm{Cyc}_r(n)$, see [1, 4, 6, 8, 12, 17, 20]. In particular, for $r \geq 2$, Bóna, McLennan and White [8] presented a bijective argument to deduce the number of r-regular permutations of $[n]$ from the number of r-regular permutations of $[n-1]$. As a consequence, they confirmed the conjecture of Wilf [20] that the probability $p_2(n)$ for a random permutation of $[n]$ to have a square root is monotonically nonincreasing in n. Such permutations have been called square permutations [5]. For example, $(1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$ is a square permutation and it has a square root $(1\ 5\ 2\ 6\ 3\ 7\ 4\ 8)$. Beyond the case $r=2$, they proved that, more generally, for any prime r, the probability $p_r(n)$ that a random permutation of $[n]$ has an r-th root is nonincreasing in n.

Notice that the monotone property does not hold in general. For example, when $r=6$, we have $p_6(4)=1/6$ but $p_6(5)=1/3$. Nonetheless, Bóna, McLennan and White [8] showed that for any $r \geq 2$,

$$p_r(n) \to 0,$$

as $n \to \infty$.

Table 1 exhibits the values of $p_r(n)$ for $r=2,3,5$ and $1 \leq n \leq 12$.

$r \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12
2	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{17}{48}$	$\frac{17}{48}$	$\frac{29}{96}$	$\frac{29}{96}$	$\frac{209}{720}$
3	1	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{9}$	$\frac{5}{9}$	$\frac{5}{9}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{37}{81}$
5	1	1	1	1	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{18}{25}$	$\frac{18}{25}$	$\frac{18}{25}$

Table 1: The values of $p_r(n)$.

As set forth by Bóna, McLennan and White, their proof of the monotone property is mostly combinatorial, and they left the question of seeking a fully combinatorial reasoning, which amounts to a combinatorial understanding of the following inequality

$$\left|\mathrm{Cyc}_{r^2}(mr^2)\right| \leq \left|\mathrm{Reg}_r(mr^2)\right|, \tag{1.1}$$

which we shall call the Bóna-McLennan-White inequality, or the BMW inequality, for short.

Note that for $r = 2$, $\mathrm{Reg}_2(n)$ and $\mathrm{Cyc}_2(n)$ are usually written as $\mathrm{Odd}(n)$ and $\mathrm{Even}(n)$, respectively. In the literature, 2-regular permutations are also known as odd order permutations, which are related to ballot permutations, see, for example, [3, 16, 19]. However, even order permutations are referred as permutations with at least one even cycle. These terms originated from the notion of the order of an element in a group.

It is a known result that $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$ share the same cardinality, $((2n-1)!!)^2$, see A001818 in the OEIS [18]. The equality of their cardinalities entails the existence of a bijection between $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$; however, this mapping is not immediately evident upon first inspection. A specific correspondence was found by Sayag based on the canonical representation of permutations, see Bóna [7, Lemma 6.20]. An intermediate structure, which we call nearly odd order permutations, was introduced in [9]. It induces incremental transforms from a permutation in $\mathrm{Odd}(2n)$ to a permutation in $\mathrm{Even}(2n)$.

It is natural to ask whether the correspondence between $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$ can be extended to any $r \geq 2$? In this paper, we introduce the structure of enriched permutations, and we find a bijection between r-regular permutations of $[rn]$ and enriched r-cycle permutations of $[rn]$. As an immediate consequence, we achieve a combinatorial comprehension of the BMW inequality, or a stronger version, strictly speaking. This answers the question of Bóna, McLennan and White for any prime $r \geq 3$. As for the case $r = 2$, we fill up with some discussions for the sake of completeness.

While the monotone property of $p_r(n)$ does not hold for general r, we show that it is valid for prime powers $r = q^l$. The proof relies on a stronger version of the Bóna-McLennan-White inequality and the characterization of permutations with an r-th root, for a prime power r, due to A. Knopfmacher and R. Warlimont [20, p. 158].

2 r-Enriched permutations

The aim of this section is to provide a bijection between r-regular permutations of $[rn]$ and enriched r-singular permutations of $[rn]$, for $r \geq 2$ and $n \geq 1$. Given $r \geq 2$, by saying that a permutation is r-enriched we mean that each r-singular cycle is colored by one of the $r-1$ colors in the set $\{1, 2, \ldots, r-1\}$. Later, we simply call such a permutation enriched. Bear in mind that r-regular cycles are never colored.

Given $r \geq 2$, we shall use the symbol $*$ to signify the enriched structure. For example, $\mathrm{Cyc}_r^*(rn)$ denotes the set of enriched r-cycle permutations of $[rn]$. Throughout, we represent each permutation in cycle notation, where each cycle is written as a linear order starting with its smallest element, and the cycles are arranged in increasing order of their minima. We use the subscript of a cycle to denote the color assigned to it. For example, for $r = 3$, $(1\ 2\ 4)_2\,(3)\,(5\ 6)$ represents an 3-enriched permutation for which the 3-singular cycle $(1\ 2\ 4)$ is colored by 2.

To transform an r-regular permutation of $[rn]$ to an enriched r-singular permutation of $[rn]$, we introduce an intermediate structure like nearly odd permutations emerging in [9]. For $n \geq 1$, we say that a permutation σ of $[n]$ is nearly r-regular if its cycles are all r-regular except that the one containing 1 is r-singular. The notation $\mathrm{NReg}_r(n)$ stands for the set of all nearly r-regular permutations of $[n]$. For example, $(1\ 2\ 4)\,(3)\,(5\ 6)$ is a nearly 3-regular permutation.

Enriched nearly r-regular permutations serve as an intermediate structure linking r-regular and enriched r-cycle permutations. More precisely, we manipulate the cycle structures to construct a bijection between $\mathrm{Reg}_r(rn)$ and $\mathrm{Cyc}_r^*(rn)$. For $r = 2$, it reduces to a bijection between $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$.

Theorem 2.1. *For any $r \geq 2$, there is a bijection Φ from $\mathrm{Reg}_r(rn)$ to $\mathrm{Cyc}_r^*(rn)$. Moreover, if $\sigma \in \mathrm{Reg}_r(rn)$ and the cycle containing 1 in σ has length $l = rk + i$, $1 \leq i \leq r-1$, then $\Phi(\sigma) \in \mathrm{Cyc}_r^*(rn)$, where the cycle containing 1 in $\Phi(\sigma)$ has length $rk + r$.*

To prove the theorem, let $Q_{r,k}(n)$ denote the set of permutations of $[n]$ for which the length of the cycle containing 1 is k, and the other cycles are r-regular.

We first build a bijection between $Q_{r,k}(n)$ and $Q_{r,k+1}(n)$ by applying an elegant bijection of Bóna, McLennan and White in [8, Lemma 2.1], which is a paradigm of a recursive algorithm.

Lemma 2.2. *For all* $r \geq 2$ *and* $n+1 \not\equiv 0 \pmod{r}$*, there is a bijection* Ψ *from* $\mathrm{Reg}_r(n) \times [n+1]$ *to* $\mathrm{Reg}_r(n+1)$.

Practically, to make use of the bijection, it is unnecessary to adjust the elements of the underlying sets to fit in the above canonical form. It seems to be convenient to harness the following more generic formulation, and it might be informative to reproduce the proof as such. For a nonempty set S, we use $\mathrm{Reg}_r(S)$ to denote the set of r-regular permutations of S.

Lemma 2.3. *Let S be a nonempty finite set and r an integer such that $r \geq 2$. If* $|S| \not\equiv 0 \pmod{r}$*, then there is a bijection* Δ *from* $\mathrm{Reg}_r(S)$ *to the set of pairs* (x, π) *such that* $x \in S$ *and* π *is in* $\mathrm{Reg}_r(S \setminus \{x\})$.

Proof. Assume that σ belongs to $\mathrm{Reg}_r(S)$ and $|S| \not\equiv 0 \pmod{r}$. From now on, we shall use $|\sigma|$ to denote the number of elements of σ. Let D_1 denote the first cycle of σ, l be its length, x be the last entry in D_1, and let $\tilde{\sigma}$ be σ with D_1 being removed. In effect, the map Δ will remove x in D_1 and turn it into a distinguished element. We encounter three cases.

Case 1: $l = 1$. Then set $\Delta(\sigma) = (x, \tilde{\sigma})$. By construction, the element x is smaller than every element of $\tilde{\sigma}$.

Case 2: $l \not\equiv 1 \pmod{r}$. Then remove x from D_1 to get C_1 and set $\Delta(\sigma) = (x, C_1\,\tilde{\sigma})$. Contrary to the previous case, the element x is greater than the smallest element of $C_1\,\tilde{\sigma}$. Since $l \not\equiv 0, 1 \pmod{r}$, we have $|C_1| = l - 1 \not\equiv -1, 0 \pmod{r}$, which ensures that the resulting permutation is r-regular.

Case 3: $l \equiv 1 \pmod{r}$ and $l \neq 1$. Let $\tilde{x}$ be the second-to-last element in D_1 and C_1 be the cycle obtained from D_1 by removing x and $\tilde{x}$. Since $|\tilde{\sigma}| + 1 = |\sigma| - l + 1 \not\equiv 0 \pmod{r}$, we can apply Δ^{-1} to $(\tilde{x}, \tilde{\sigma})$ to get $\tilde{\pi}$. Then set $\Delta(\sigma) = (x, C_1\,\tilde{\pi})$. In this situation, the element x is greater than the smallest element of $C_1\,\tilde{\pi}$ and $|C_1| = l - 2 \equiv -1 \pmod{r}$.

It remains to verify that Δ is a bijection. Given a pair (x,π) where $x\in S$ and π is an r-regular permutation of $S\setminus\{x\}$ with $|\pi|+1\not\equiv 0 \pmod r$. Let C_1 denote the first cycle of π, l be its length and let $\tilde{\pi}$ be permutation π with C_1 being removed. Conversely, the map Δ^{-1} will place x as the last entry in the first cycle of $\Delta^{-1}(x,\pi)$. Accordingly, we face three possibilities.

Case 1: The element x is smaller than every element of π. Then set $\Delta^{-1}(x,\pi)=(x)\,\pi$. In this case, $|D_1|$=1.

Case 2: The element x is greater than the smallest element of π and $l\not\equiv -1 \pmod r$. Let D_1 be C_1 with x appended to the end of C_1. Then set $\Delta^{-1}(x,\pi)=D_1\,\tilde{\pi}$. Notice that $l\not\equiv -1,0 \pmod r$, and so $|D_1|=l+1\not\equiv 0,1 \pmod r$.

Case 3: The element x is greater than the smallest element of π and $l\equiv -1 \pmod r$. Under the conditions $|\pi|-l\equiv|\pi|+1 \pmod r$ and $|\pi|+1\not\equiv 0 \pmod r$, we have $|\tilde{\pi}|=|\pi|-l\not\equiv 0 \pmod r$. Thus we can apply Δ to $\tilde{\pi}$ to get $(\tilde{x},\tilde{\sigma})$. Let D_1 be C_1 with $\tilde{x}x$ appended to the end. Then set $\Delta^{-1}(x,\pi)=D_1\,\tilde{\sigma}$. Notice that in this case $|D_1|=l+2\equiv 1 \pmod r$ and $|D_1|\neq 1$, completing the proof. ∎

For example, when $r=3$, consider

$$\sigma=(1\ 8\ 2\ 5)\,(3)\,(4)\,(6\ 7).$$

Since the length of the first cycle is congruent to $1 \pmod 3$, we are in Case 3. Hence,

$$\Delta(\sigma)=(5,(1\ 8)\,\tilde{\pi}),$$

where

$$\tilde{\pi}=\Delta^{-1}(2,(3)\,(4)\,(6\ 7)).$$

Because the element 2 is smaller than every element in $\tilde{\pi}$, we are in Case 1 of Δ^{-1}. Therefore,

$$\Delta^{-1}\,(2,(3)\,(4)\,(6\ 7))=(2)\,(3)\,(4)\,(6\ 7).$$

Consequently,

$$\Delta(\sigma)=(5,(1\ 8)\,(2)\,(3)\,(4)\,(6\ 7)).$$

We now turn to the description of the bijection φ. The following lemma is the building block of the correspondence between r-regular permutations and enriched r-cycle permutations. It rests on the Lemma of Bóna, McLennan and White, as restated in Lemma 2.3.

Lemma 2.4. *Let n,r,k be integers such that $n \geq 0, r \geq 2, k \geq 1$ and $n-k \not\equiv 0 \pmod{r}$. Then there is a bijection φ from $Q_{r,k}(n)$ to $Q_{r,k+1}(n)$.*

Proof. We proceed to construct a map φ from $Q_{r,k}(n)$ to $Q_{r,k+1}(n)$ by employing the above bijection Δ. Assume that $n-k \not\equiv 0 \pmod{r}$ and $k \geq 1$. Let $\sigma \in Q_{r,k}(n)$, and denote by C_1 the cycle containing 1. Define $\tilde{\sigma} = \sigma - C_1$, by which we mean the permutation obtained from σ by removing C_1. Since $|\tilde{\sigma}| = n-k \not\equiv 0 \pmod{r}$ and $\tilde{\sigma}$ is an r-regular permutation, applying the map of Δ, we get $\Delta(\tilde{\sigma}) = (x, \tilde{\pi})$. Now, let D denote the cycle obtained from C_1 with x attached at the end. Set $\varphi(\sigma) = D\tilde{\pi}$, which is readily seen to lie in $Q_{r,k+1}(n)$.

Conversely, let us define a map α from $Q_{r,k+1}(n)$ to $Q_{r,k}(n)$. Given $\pi \in Q_{r,k+1}(n)$, where $n-k \not\equiv 0 \pmod{r}$ and $k \geq 1$, let C_1 be the first cycle of π, and let D be the cycle obtained from C_1 by removing its last entry x. Define $\tilde{\pi}$ be π with C_1 being removed. Note that $|\tilde{\pi}|+1 = n-k \not\equiv 0 \pmod{r}$ and $\tilde{\pi}$ is an r-regular permutation. Then set

$$\alpha(\pi) = D\Delta^{-1}(x, \tilde{\pi}),$$

which belongs to $Q_{r,k}(n)$.

It is straightforward to verify that the maps φ and α are well-defined and are inverses of each other. Thus φ is a bijection. ∎

For example, if $r=3$, then $\varphi((3)\,(5\,6)) = (3\,6)\,(5)$ and $\varphi((3\,6)\,(5)) = (3\,6\,5)$.

Writing $n-k = mr+d$ with $0 < d < r$, it is known that, see [1, 4, 6, 8, 12, 17, 20],

$$|\mathrm{Reg}_r(n-k)| = (n-k)!\,\frac{(r-1)\,(2r-1)\cdots(mr-1)}{r^m m!},$$

from which we deduce that

$$\left|Q_{r,k}(n)\right| = \left|Q_{r,k+1}(n)\right| = (n-1)!\,\frac{(r-1)\,(2r-1)\cdots(mr-1)}{r^m m!}. \tag{2.1}$$

For $k \geq 1$, let $A_{n,2k-1}$ denote the set of permutations of $[n]$ with only odd cycles for which the element 1 appears in a cycle of length $2k-1$, and let $P_{n,2k}$ denote the set of permutations of $[n]$ with odd cycles except that the element 1 is contained in an even cycle of length $2k$. When $r = 2$, we come to the following correspondence. Notice that the construction in [9] by way of breaking cycles does not possess this refined property.

Corollary 2.5. *For $k \geq 1$, the map φ defined in Lemma 2.4 gives a bijection between $A_{2n,2k-1}$ and $P_{2n,2k}$, as well as a bijection between $P_{2n+1,2k}$ and $A_{2n+1,2k+1}$.*

For example, when $r = 2$, given $\sigma = (1\ 2\ 3\ 4\ 6)\,(5\ 10\ 8)\,(7)\,(9) \in A_{10,5}$, we have

$$\Delta((5\ 10\ 8)\,(7)\,(9)) = (8, (5)\,(7\ 9\ 10)).$$

Thus

$$\varphi(\sigma) = (1\ 2\ 3\ 4\ 6\ 8)\,(5)\,(7\ 9\ 10) \in P_{10,6}.$$

Below are the explicit formulas:

$$\left|A_{2n,2k-1}\right| = \left|P_{2n,2k}\right| = \frac{(2n-1)!}{(2n-2k)!}\left((2n-2k-1))!!\right)^2, \tag{2.2}$$

$$\left|P_{2n+1,2k}\right| = \left|A_{2n+1,2k+1}\right| = \frac{(2n)!}{(2n-2k)!}\left((2n-2k-1))!!\right)^2. \tag{2.3}$$

Exploiting the bijection φ, we are led to the following incremental transformation Λ.

Theorem 2.6. *For all $r \geq 2$, there is a bijection Λ from $\mathrm{Reg}_r(rn)$ to $\mathrm{NReg}_r^*(rn)$. Moreover, if $\sigma \in \mathrm{Reg}_r(rn)$ and the cycle containing 1 in σ has length $l = rk+i$, $1 \leq i \leq r-1$, then $\Lambda(\sigma) \in \mathrm{NReg}_r^*(rn)$, where the cycle containing 1 in $\Lambda(\sigma)$ has length $rk+r$.*

Proof. Let σ in $\mathrm{Reg}_r(rn)$. Assume that its first cycle length is $rk+i$, where $1 \leq i \leq r-1$. Since $rn \not\equiv rk+i \pmod{r}$, we can apply the bijection φ in Lemma

2.4 to σ to get a permutation π. There are two possibilities with regard to the length of the first cycle of π.

If π is in $\mathrm{NReg}_r(rn)$, in which case, $i+1=r$, we color its first cycle with $r-1$ to obtain $\Lambda(\sigma)\in\mathrm{NReg}_r^*(rn)$.

If π stays in $\mathrm{Reg}_r(rn)$ with the length of the first cycle increased by 1 in comparison with σ, that is, the length of the first cycle of π equals $rk+i+1$ with $rk+i+1\not\equiv 0 \pmod r$. Again, since $rn\not\equiv rk+i+1 \pmod r$, we may move on to apply the bijection φ once more. The procedure continues until we obtain a permutation π in $\mathrm{NReg}_r(rn)$. Color π's first cycle with i and define the resulting enriched permutation to be $\Lambda(\sigma)$, which lies in $\mathrm{NReg}_r^*(rn)$. Apparently, it takes $r-i$ steps to reach this point.

As an example, for $r=3$, we have

$$\Lambda((3)\,(5\;6))=(3\;6\;5)_1$$

and

$$\Lambda((1\;2)\,(3\;4)\,(5\;6))=(1\;2\;4)_2\,(3)\,(5\;6).$$

It is readily seen that the process is reversible because the color of the r-singular cycle keeps track of the number of times that the map φ is applied. Thus Λ is a bijection. ∎

Proof of Theorem 2.1. We proceed to define a map Φ from $\mathrm{Reg}_r(rn)$ to $\mathrm{Cyc}_r^*(rn)$ by successively applying the map Λ in Theorem 2.6.

Given an r-regular permutation σ, our goal is to create a sequence of colored r-singular cycles C_i^*. At the first step, applying the bijection Λ to σ, we get

$$\Lambda(\sigma)=C_1^*\,\sigma_1,$$

where C_1^* is a colored r-singular cycle and σ_1 is an r-regular permutation (possibly empty), and $C_1^*\sigma_1$ stands for the permutation obtained by putting together the colored cycle C_1^* and the cycles in σ_1. If σ_1 is empty, then we set $\Phi(\sigma)=C_1^*$; otherwise, applying Λ again to σ_1 gives

$$\Lambda(\sigma_1)=C_2^*\,\sigma_2.$$

If σ_2 is empty, we define $\Phi(\sigma) = C_1^* C_2^*$; otherwise, we may apply Λ to σ_2.

We may iterate the procedure as follows. Assume that we have obtained a nonempty permutation σ_i for some i. Applying Λ to σ_i yields

$$\Lambda(\sigma_i) = C_{i+1}^* \sigma_{i+1},$$

where C_{i+1}^* is a colored r-singular cycle and σ_{i+1} is an r-regular permutation (possibly empty). If σ_{i+1} is not empty, we apply Λ again; otherwise, we stop. Clearly, the above process will terminate at some point when σ_{i+1} is empty. Now define

$$\Phi(\sigma) = C_1^* \cdots C_{i+1}^*.$$

Since Λ is bijective, so is Φ. ∎

For example, for $r = 3$, given

$$\sigma = (1\ 2)\,(3\ 4)\,(5\ 6).$$

Applying Λ to σ yields

$$\Lambda\left((1\ 2)\,(3\ 4)\,(5\ 6)\right) = (1\ 2\ 4)_2\,(3)\,(5\ 6);$$

at this stage, the permutation still contains r-regular cycles (3) and $(5\ 6)$, so we need to repeat the above procedure. One more round of iteration gives

$$\Lambda\left((3)\,(5\ 6)\right) = (3\ 6\ 5)_1,$$

thus we finally obtain

$$\Phi\left((1\ 2)\,(3\ 4)\,(5\ 6)\right) = (1\ 2\ 4)_2\,(3\ 6\ 5)_1.$$

3 The Bóna-McLennan-White inequality

In the proof of the following monotone property, there is an inequality that demands a combinatorial explanation. As will be seen, the structure of enriched cycle permutations entails a combinatorial interpretation of this inequality. Recall that $p_r(n)$ is the probability for a random permutation of $[n]$ to have an r-th root.

Theorem 3.1 (Bóna, McLennan and White [8]). *For all positive integers n and all primes r, we have,*

$$p_r(n) \geq p_r(n+1).$$

The above assertion consists of three circumstances contingent to modulo conditions on $n+1$.

Theorem 3.2 (Bóna, McLennan and White [8]). *Let r be a prime. Then we have the following.*

(i) *If $n+1 \not\equiv 0 \pmod{r}$, then $p_r(n) = p_r(n+1)$.*

(ii) *If $n+1 \equiv 0 \pmod{r}$ but $n+1 \not\equiv 0 \pmod{r^2}$, then*

$$p_r(n) \geq \frac{n+1}{n} p_r(n+1)$$

with equality only when $n+1 = kr$, where $k = 1, 2, \ldots, r-1$.

(iii) *If $n+1 \equiv 0 \pmod{r^2}$, then $p_r(n) \geq p_r(n+1)$ with equality only when $r = 2$ and $n = 3$.*

The proof of the above theorem builds upon a special case of the characterization of permutations with an r-th root, due to Knopfmacher and Warlimont, see [20, p. 158]. In particular, when r is prime, a permutation has an r-th root if and only if for any positive integer i, the number of cycles of length ir is a multiple of r. Making use of the bijection Ψ as restated in Lemma 2.3, Bóna, McLennan and White gave an entirely combinatorial proof of (i) and (ii). However, in order to have a fully combinatorial understanding of (iii), one needs a combinatorial interpretation of the following inequality, see [8, Lemma 3.3], which we call the Bóna-McLennan-White inequality, or the BMW inequality, for short.

Lemma 3.3. *For all $r \geq 2$ and $m \geq 1$,*

$$\left|\mathrm{Cyc}_{r^2}(mr^2)\right| < \left|\mathrm{Reg}_r(mr^2)\right|. \tag{3.1}$$

The BMW-inequality was proved in [8] by means of generating functions. In fact, we observe that a stronger version of (3.1), i.e., Theorem 3.4, holds, which can be deduced from the following known formulas, see [1, 4, 6, 8, 12, 17, 20]. For $r \geq 2$ and $m \geq 1$,

$$|\mathrm{Cyc}_r(rm)| = (rm)!\frac{(1+r)\,(1+2r)\cdots(1+(m-1)r)}{r^m m!}, \tag{3.2}$$

$$|\mathrm{Reg}_r(rm)| = (rm)!\frac{(r-1)\,(2r-1)\cdots(mr-1)}{r^m m!}. \tag{3.3}$$

On the other hand, it is transparent from a combinatorial point of view.

Theorem 3.4. *For $r \geq 2$ and $n \geq 1$,*

$$|\mathrm{Cyc}_r(n)| \leq |\mathrm{Reg}_r(n)|, \tag{3.4}$$

where the equality holds only when $r = 2$ and n is even.

Proof. When $n \not\equiv 0 \pmod{r}$, we have $|\mathrm{Cyc}_r(n)| = 0$, nothing needs to be done. When $n = rm$, by restricting to only one color, we see that

$$|\mathrm{Cyc}_r(rm)| \leq |\mathrm{Cyc}^*_r(rm)|. \tag{3.5}$$

But Theorem 2.1 says that $|\mathrm{Reg}_r(rm)| = |\mathrm{Cyc}^*_r(rm)|$, and so (3.4) follows. The equality holds only when $r = 2$ and n is even. This concludes the proof. ∎

To see that the BMW inequality (3.1) stems from (3.4), just observe that for $r \geq 2$,

$$\mathrm{Cyc}_{r^2}(mr^2) \subset \mathrm{Cyc}_r(mr^2).$$

This inequality, together with the combinatorial reasoning in [8] gives rise to the conclusion that $p_r(n) > p_r(n+1)$ for any prime $r \geq 3$ and $n+1 \equiv 0 \pmod{r^2}$.

As defined before, $|\mathrm{Reg}_r(0)| = 1$ and $|\mathrm{Cyc}_r(0)| = 1$. With Lemma 2.2 in hand, it is easy to get the following recurrence of $|\mathrm{Reg}_r(rm)|$. For details, we refer to Lemma 2.1 and Lemma 2.6 in [8].

Lemma 3.5. *For all $r \geq 2$ and $m \geq 1$, we have*

$$|\mathrm{Reg}_r(rm)| = (rm-1)\,(rm-1)_{r-1}\,|\mathrm{Reg}_r(rm-r)|, \tag{3.6}$$

where $(x)_m$ stands for the lower factorial $x(x-1)\cdots(x-m+1)$.

The above relation can also be deduced inductively by using the recursive generation of permutations in the cycle notation, see, for example, [1, 13]. In [1], it has been shown that

$$|\mathrm{Reg}_r(rm)| = \sum_{1\le l\le r-1} (rm-1)_{l-1}\, |\mathrm{Reg}_r(rm-l)| \\ + (rm-1)_r\, |\mathrm{Reg}_r(rm-r)|\,,$$

and by an easy induction on n, it can be shown that

$$|\mathrm{Reg}_r(rm-l)| = (rm-l)_{r-l}\, |\mathrm{Reg}_r(rm-r)|\,, \; 1\le l\le r-1.$$

This proves (3.6).

Similarly, we have the following recurrence relation for $\mathrm{Cyc}_r(rm)$.

Lemma 3.6. *For all $r\ge 2$ and $m\ge 1$, we have*

$$|\mathrm{Cyc}_r(rm)| = (rm-1)_{r-1}(rm-r+1)\, |\mathrm{Cyc}_r(rm-r)|\,. \tag{3.7}$$

Proof. Let σ be a permutation in $\mathrm{Cyc}_r(rm)$. Let l be the length of the first cycle of σ. If $l=r$, then there are $(rm-1)_{r-1}$ choices to form the first cycle. If the first cycle contains more than r elements, say $(1\ \cdots\ j_r\ j_{r+1}\ \cdots)$, then there are $(rm-1)_r\, |\mathrm{Cyc}_r(rm-r)|$ choices. We can break the first cycle into two segments $1\ \cdots\ j_r$ and $j_{r+1}\ \cdots$. The second segment can be viewed as a cycle with a distinguished element j_{r+1}. Combining this cycle with a distinguished element and other cycles, we see a permutation in $\mathrm{Cyc}_r(rm-r)$ with a distinguished element. There are $(rm-1)_{r-1}$ for the first segment $1\ \cdots\ j_r$ and there are there are $rm-r$ choices for the distinguished element j_{r+1}. Hence

$$|\mathrm{Cyc}_r(rm)| = (rm-1)_{r-1}\, |\mathrm{Cyc}_r(rm-r)| \\ + (rm-1)_{r-1}(rm-r)\, |\mathrm{Cyc}_r(rm-r)|\,,$$

which gives (3.7). ∎

As per the recurrence relations (3.6) and (3.7), one can derive the formulas for $|\mathrm{Reg}_r(rm)|$ and $|\mathrm{Cyc}_r(rm)|$, which result in the stronger version of the BMW inequality, i.e., (3.4). Thus, for a prime $r \geq 3$, we obtain another combinatorial explanation of the monotone property.

As noted in [8], the case $r = 2$ requires a stronger inequality, which they justify using generating functions.

Lemma 3.7. *For $m \geq 4$, we have*

$$2\,|\mathrm{Cyc}_4(4m)| < |\mathrm{Reg}_2(4m)|\,. \tag{3.8}$$

Proof. For $m \geq 1$, by Lemmas 3.5 and 3.6, we obtain that

$$|\mathrm{Reg}_2(4m)| = (4m-1)^2\,(4m-3)^2\,|\mathrm{Reg}_2(4m-4)|\,, \tag{3.9}$$

$$|\mathrm{Cyc}_4(4m)| = (4m-1)\,(4m-2)\,(4m-3)^2\,|\mathrm{Cyc}_4(4m-4)|\,. \tag{3.10}$$

In fact, the proofs of Lemmas 3.5 and 3.6 reveal that there is a bijection from $\mathrm{Reg}_2(4m)$ to $[4m-1]^2 \times [4m-3]^2 \times \mathrm{Reg}_2(4m-4)$, and there is also a bijection from $\mathrm{Cyc}_4(4m)$ to $[4m-1] \times [4m-2] \times [4m-3]^2 \times \mathrm{Cyc}_4(4m-4)$. Clearly, the coefficient in (3.9) is greater than that in (3.10), and it is just a matter of formality to make this comparison in combinatorial terms. Consequently, if

$$2\,|\mathrm{Cyc}_4(4m)| < |\mathrm{Reg}_2(4m)|$$

holds for some value m_0, then it holds for all $m \geq m_0$. It is easily verified that we can choose $m_0 = 4$, since from (3.9) and (3.10), we have

$$\frac{|\mathrm{Reg}_2(4m_0)|}{|\mathrm{Cyc}_4(4m_0)|} = \frac{15}{14} \cdot \frac{11}{10} \cdot \frac{7}{6} \cdot \frac{3}{2} \cdot \frac{|\mathrm{Reg}_4(0)|}{|\mathrm{Cyc}_2(0)|} = \frac{33}{16} > 2.$$

So the Lemma is proved. ∎

In view of the above argument, inequality (3.8) admits a combinatorial interpretation. Appealing to this inequality, we deduce that $p_2(n+1) < p_2(n)$ whenever $n+1 \equiv 0 \pmod 4$, with the only exceptions for $n = 3, 7, 11$, see [8]. For these three special cases, we can look up the data in [8] or the sequence A247005 in the OEIS [18]. The values of $p_2(n)$ for $n = 3, 4, 7, 8, 11, 12$ are given as follows

$$\frac{1}{2}, \frac{1}{2}, \frac{3}{8}, \frac{17}{48}, \frac{29}{96}, \frac{209}{720}.$$

Thus for $n = 3, 7, 11$, the inequality $p_2(n+1) \leq p_2(n)$ is valid with equality attained only when $n = 3$. Therefore, for any prime r, a full combinatorial analysis is achieved.

4 The monotone property for prime powers

Whereas the monotone property of $p_r(n)$ does not hold in general, numerical evidence raises hopes that it might hold for prime powers, as indicated in Table 2 for $r = 4, 8, 9$ and $1 \leq n \leq 12$.

$r \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12
4	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{53}{192}$	$\frac{53}{192}$	$\frac{95}{384}$	$\frac{95}{384}$	$\frac{29}{128}$
8	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{5}{16}$	$\frac{35}{128}$	$\frac{35}{128}$	$\frac{63}{256}$	$\frac{63}{256}$	$\frac{231}{1024}$
9	1	1	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{5}{9}$	$\frac{5}{9}$	$\frac{5}{9}$	$\frac{40}{81}$	$\frac{40}{81}$	$\frac{40}{81}$	$\frac{110}{243}$

Table 2: The values of $p_r(n)$.

The main result of this section is as follows.

Theorem 4.1. *Let n be a positive integer and $r = q^l$, where q is a prime, and $l \geq 1$, then $p_r(n) \geq p_r(n+1)$.*

Like the case for primes, this monotone property stands on the following cases subject to modulo conditions on $n+1$. First, we recall an equality concerning $p_r(n)$ when r is a prime power. Chernoff [10] established the following equality, and Leaños, Moreno and Rivera-Martínez [15] presented two proofs, with one using generating functions and the other being combinatorial.

Theorem 4.2. *Let q be a prime and $r = q^l$, $l \geq 1$. If $n+1 \not\equiv 0 \pmod{q}$, then $p_r(n) = p_r(n+1)$.*

For the remaining cases, we obtain the following relations.

Theorem 4.3. *Let q be a prime, and $r = q^l$, $l \geq 1$.*

(i) *If* $n+1 \equiv 0 \pmod{q}$ *but* $n+1 \not\equiv 0 \pmod{qr}$*, then*

$$p_r(n) \geq \frac{n+1}{n} p_r(n+1), \tag{4.1}$$

with equality only when $n+1 = kq$*, where* $k = 1, 2, \ldots, r-1$*.*

(ii) *If* $n+1 \equiv 0 \pmod{qr}$*, then* $p_r(n) \geq p_r(n+1)$ *with equality only when* $r = 2$ *and* $n = 3$*.*

To prove the above theorem, it is helpful to prepare some auxiliary inequalities. Even though these estimates can be considerably improved, we will be content with the coarse lower bounds in order to keep the proofs brief. Recall that for any r, permutations with an r-th root can be characterized in terms of the cycle type by Knopfmacher and Warlimont, see Wilf [20, p. 158]. In particular, we need the following criterion when r is a prime power.

Proposition 4.4. *If* $r = q^l$ *with* q *being a prime number and* $l \geq 1$*, then a permutation has an* r*-th root if and only if for any integer* i*, the number of cycles of length* iq *is a multiple of* r*.*

Next, we show that the two inequalities in Lemma 3.2 and Lemma 3.3 in [8] for a prime r can be extended to a prime power. With the common notation S_n^r for the set of permutations of $[n]$ with an r-th root, by Proposition 4.4, we have for a prime power $r = q^l$,

$$\mathrm{Reg}_q(n) \subseteq S_n^r. \tag{4.2}$$

Let $\mathrm{Cyc}_{q,r}(n)$ denote the set of permutations such that each cycle length is a multiple of q and each cycle length occurs a multiple of r times. The following relation is an extension of Lemma 3.2 in [8].

Lemma 4.5. *For any* $m \geq 1$*, let* $r = q^l$*, where* $q \geq 2$ *(not necessarily a prime) and* $l \geq 1$*, we have*

$$\frac{\left|\mathrm{Cyc}_{qr}(mqr)\right|}{\left|\mathrm{Cyc}_{q,r}(mqr)\right|} \geq (mq)^{r-1}. \tag{4.3}$$

Proof. Let $\pi \in \mathrm{Cyc}_{q,r}(mqr)$. By definition, we assume that π contains $k_i r$ cycles of length iq, where $k_i \geq 0$. For each i with $k_i \neq 0$, partition the cycles of length iq into k_i classes with each class containing r cycles. For each class F of r cycles of length iq, we proceed to generate a cycle of length iqr out of the elements in F. Running over all such classes F, we obtain permutations in $\mathrm{Cyc}_{qr}(mqr)$.

First, let $A_1, A_2, \ldots, A_r$ be the cycles in F, where every cycle has length iq, that is, arrange the cycles in F in any specific linear order. To form a cycle of length iqr, we represent A_1 with the minimum element at the beginning. Then break the cycles $A_2, A_2, \ldots, A_r$ into linear orders by starting with any element. There are iq ways to break a cycle of length iq into a linear order. Assume that $A_2', A_3', \ldots, A_r'$ are in linear orders by breaking the cycles $A_2, A_3, \ldots, A_r$, respectively. Now we can form a cycle of length iqr by adjoining $A_2', A_3', \ldots, A_r'$ successively at the end of A_1. Evidently, the cycles formed in this way are all distinct, and there are $(iq)^{r-1}$ of them that can be generated in this manner.

Taking into account all classes F, we may produce certain permutations in $\mathrm{Cyc}_{qr}(mqr)$. The number of permutations generated this way equals $\prod_i (iq)^{(r-1)k_i}$. Moreover, the range of i in $\prod_i (iq)^{(r-1)k_i}$ can be restricted to those such that $k_i \geq 1$. Given that $q \geq 2$, for any $k_i \geq 1$, we have $(iq)^{k_i} \geq iqk_i$ and

$$\prod_i iqk_i \geq \sum_i iqk_i.$$

Thus we see that

$$\prod_i (iq)^{(r-1)k_i} \geq \left(\sum_i iqk_i \right)^{r-1} = (mq)^{r-1},$$

where we have used the relation

$$\sum_i iqk_i = mq,$$

because

$$\sum_i iqk_i r = mqr.$$

So the Lemma is proved. ∎

The following lemma is an extension of Lemma 3.3 in [8].

Lemma 4.6. *Let $r = q^l$, where $q \geq 2$ (not necessarily a prime) and $l \geq 1$. Then, for any integer $m \geq 1$, we have*

$$\frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_{q,r}(mqr)\right|} > (mq)^{r-1}. \tag{4.4}$$

Proof. By definition, we have

$$\mathrm{Cyc}_{qr}(mqr) \subset \mathrm{Cyc}_q(mqr),$$

and hence $\left|\mathrm{Cyc}_{qr}(mqr)\right| < \left|\mathrm{Cyc}_q(mqr)\right|$. In light of the stronger version of the BMW inequality (3.4), we see that

$$\frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_{qr}(mqr)\right|} = \frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_q(mqr)\right|} \cdot \frac{\left|\mathrm{Cyc}_q(mqr)\right|}{\left|\mathrm{Cyc}_{qr}(mqr)\right|} > 1. \tag{4.5}$$

Comparing with (4.3) shows that

$$\frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_{q,r}(mqr)\right|} = \frac{\left|\mathrm{Cyc}_{qr}(mqr)\right|}{\left|\mathrm{Cyc}_{q,r}(mqr)\right|} \cdot \frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_{qr}(mqr)\right|} > (mq)^{r-1},$$

as required. ∎

The following lower bound of $\left|S^r_{mqr}\right|$ will also be needed in the proof of Theorem 4.3.

Lemma 4.7. *Let $r = q^l$ be a prime power greater than 2. For any $m \geq 1$, we have*

$$\left|S^r_{mqr}\right| > mqr\left|\mathrm{Cyc}_{q,r}(mqr)\right|. \tag{4.6}$$

Proof. For the conditions stated in the lemma, we obtain

$$r - 1 = q^l - 1 \geq l + 1,$$

thus, $(mq)^{r-1} \geq mq^{l+1}$. Thanks to (4.4), we find that

$$\frac{\left|\mathrm{Reg}_q(mqr)\right|}{\left|\mathrm{Cyc}_{q,r}(mqr)\right|} > (mq)^{r-1} \geq mq^{l+1} = mqr.$$

Recalling (4.2), we get

$$\left|S^r_{mqr}\right| \geq \left|\mathrm{Reg}_q(mqr)\right| > mqr\left|\mathrm{Cyc}_{q,r}(mqr)\right|,$$

as claimed. ∎

For now, we still need one more inequality, that is, Corollary 2.16 in [8]. Given a permutation σ, we may partition its set of cycles into two classes. Let $R_q(\sigma)$ and $S_q(\sigma)$ denote the permutation consisting of the q-regular cycles and the permutation consisting of the q-singular cycles of σ, respectively, in lieu of $\sigma_{(\sim q)}$ and $\sigma_{(q)}$ as used in [8]. We refer to $R_q(\sigma)$ and $S_q(\sigma)$ as the q-regular part and q-singular part of σ, respectively.

The cycle type ρ of a permutation is defined to be the multiset of its cycle lengths, often denoted by $1^{k_1}2^{k_2}\cdots n^{k_n}$, meaning that there are k_i cycles of length i for $1 \le i \le n$. We write $|\rho|$ for the sum of the cycle lengths in ρ.

Let $S_{\rho,q}(n)$, in place of $\mathrm{DIV}_{\rho,q}(n)$ as used in [8], denote the set of permutations of $[n]$ whose q-singular part has cycle type ρ. In particular, $S_{\emptyset,q}(n)$ is the set of q-regular permutations, i.e., $\mathrm{Reg}_q(n)$. For instance, the permutation $\sigma = (1\ 2)\,(3\ 4)\,(5\ 9\ 7\ 8)\,(6\ 10\ 11\ 13)\,(12)$ belongs to $S_{2^24^2,2}(13)$.

The inequality in [8] can be restated as follows.

Proposition 4.8. *Let $n \ge 1$, $q \ge 2$ (not necessarily a prime), and let ρ be a cycle type with $|\rho| \le n$. If $n+1$ is a multiple of q, then*

$$\left|S_{\rho,q}(n)\right| \ge \frac{1}{n}\left|S_{\rho,q}(n+1)\right|,$$

where equality is attained if and only if $\rho = \emptyset$.

In the event that $\rho = \emptyset$, the equality states that if $n+1$ is a multiple of q, then

$$n\left|\mathrm{Reg}_q(n)\right| = \left|\mathrm{Reg}_q(n+1)\right|,$$

which follows from the bijection between $\mathrm{Reg}_q(n) \times [n]$ and $\mathrm{Reg}_q(n+1)$ constructed by Bóna, McLennan and White, see Lemma 2.6 in [8].

We are now ready to prove Theorem 4.3.

Proof of Theorem 4.3. Let us first introduce a notation. Given positive integers q,r, we say that a cycle type ρ is (q,r)-divisible, denoted by $(q,r) \mid \rho$, if every cycle length in ρ is divisible by q, and for any integer i, the number of cycles of length iq is a multiple of r. We also set $(q,r) \mid \emptyset$ by convention.

Since r is a prime power q^l, Proposition 4.4 implies that a permutation of $[n]$ belongs to S_n^r if and only if the cycle type of its q-singular part is (q,r)-divisible. So we have

$$S_n^r = \bigcup_{\substack{|\rho|\le n\\ (q,r)\,|\,\rho}} S_{\rho,q}(n).$$

Hence

$$|S_n^r| = \sum_{\substack{|\rho|\le n\\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n)\right|. \tag{4.7}$$

Again, by Proposition 4.4, a permutation of $[n+1]$ is in S_{n+1}^r if and only if its q-singular cycle type is (q,r)-divisible, namely,

$$S_{n+1}^r = \bigcup_{\substack{|\rho|\le n+1\\ (q,r)\,|\,\rho}} S_{\rho,q}(n+1).$$

Considering the range of ρ, we get

$$\left|S_{n+1}^r\right| = \sum_{\substack{|\rho|\le n\\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n+1)\right| + \sum_{\substack{|\rho|=n+1\\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n+1)\right|. \tag{4.8}$$

Concerning the terms in (4.7) and in the first sum in (4.8), given any cycle type ρ with $|\rho| \le n$ and $(q,r) \mid \rho$, Proposition 4.8 asserts that if $n+1$ is a multiple of q, then

$$\left|S_{\rho,q}(n)\right| \ge \frac{1}{n}\left|S_{\rho,q}(n+1)\right|, \tag{4.9}$$

where equality is attained if and only if $\rho = \emptyset$. Therefore,

$$\begin{aligned}
|S_n^r| &= \sum_{\substack{|\rho|\le n\\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n)\right| \\
&\ge \frac{1}{n} \sum_{\substack{|\rho|\le n\\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n+1)\right|
\end{aligned}$$

$$= \frac{1}{n}\left(\left|S^r_{n+1}\right| - \sum_{\substack{|\rho|=n+1 \\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n+1)\right| \right).$$

Consequently,

$$n\,|S^r_n| \geq \left|S^r_{n+1}\right| - \sum_{\substack{|\rho|=n+1 \\ (q,r)\,|\,\rho}} \left|S_{\rho,q}(n+1)\right|. \tag{4.10}$$

We now proceed to prove (i). Assume that $n+1$ is a multiple of q but not a multiple of qr. We claim that for a cycle type ρ with $|\rho| = n+1$ and $(q,r) \mid \rho$,

$$S_{\rho,q}(n+1) = \emptyset. \tag{4.11}$$

Suppose to the contrary that there exists a permutation in $S_{\rho,q}(n+1)$. Under the condition that ρ is (q,r)-divisible, we have $|\rho|$ is a multiple of qr, but we also have $|\rho| = n+1$, which contradicts the condition that $n+1$ is not a multiple of qr. Utilizing the property (4.11) and the relation (4.10), we get

$$n\,|S^r_n| \geq \left|S^r_{n+1}\right|,$$

which is equivalent to (4.1). This proves (i).

To prove (ii), assume that $n+1 = mqr$. We shall proceed in the same fashion as the argument given in [8] when r is a prime. The case $r = 2$ has been taken care of in the preceding section. So we may set our mind on the case when r is a prime power greater than 2.

In the notation $(q,r) \mid \rho$, we can write

$$\mathrm{Cyc}_{q,r}(mqr) = \bigcup_{\substack{|\rho|=mqr \\ (q,r)\,|\,\rho}} S_{\rho,q}(mqr). \tag{4.12}$$

Inserting (4.12) into (4.10) yields

$$(mqr-1)\left|S^r_{mqr-1}\right| \geq \left|S^r_{mqr}\right| - \left|\mathrm{Cyc}_{q,r}(mqr)\right|. \tag{4.13}$$

Putting (4.6) into (4.13) yields

$$(mqr-1)\left|S^r_{mqr-1}\right| > \left(1 - \frac{1}{mqr}\right)\left|S^r_{mqr}\right|.$$

It follows that

$$mqr \left| S^r_{mqr-1} \right| > \left| S^r_{mqr} \right| .$$

Thus we conclude that $p_r(n) > p_r(n+1)$ when $n+1 \equiv 0 \pmod{qr}$. This proves (ii).

The conditions under which equality holds in (i) and (ii) are readily discerned, and so the theorem is proved. ∎

To conclude, we note that the monotonicity of $p_r(n)$ for prime powers r, as stated in Theorem 4.1, is immediate from Theorems 4.2 and 4.3.

Acknowledgments. We are deeply indebted to the referees for their close scrutiny of the manuscript and for their constructive suggestions.

References

[1] R. Beals, C.R. Leedham-Green, A.C. Niemeyer, C.E. Praeger and Á. Seress, Permutations with restricted cycle structure and an algorithmic application, Combin. Probab. Comput., 11 (2002) 447–464.

[2] E.A. Bender, Asymptotic methods in enumeration, SIAM Rev., 16 (1974) 485–515.

[3] O. Bernardi, B. Duplantier, and P. Nadeau, A bijection between well-labelled positive paths and matchings, Sém. Lothar. Combin., 63 (2010) B63e.

[4] E.A. Bertram and B. Gordon, Counting special permutations, European J. Combin., 10 (1989) 221–226.

[5] J. Blum, Enumeration of the square permutations in S_n, J. Combin. Theory Ser. A, 17 (1974) 156–161.

[6] E.D. Bolker and A.M. Gleason, Counting permutations, J. Combin. Theory Ser. A, 29 (1980) 236–242.

[7] M. Bóna, A Walk Through Combinatorics, World Scientific, 2005.

[8] M. Bóna, A. McLennan and D. White, Permutations with roots, Random Struct. Algor., 17 (2000) 157–167.

[9] W.Y.C. Chen, Breaking cycles, the odd versus the even, Enumer. Comb. Appl., 4 (2024) #S2R17.

[10] W.W. Chernoff, Permutations with p^l-th roots, Discrete Math., 125 (1994) 123–127.

[11] P. Erdős and P. Turán, On some problems of a statistical group-theory. II, Acta Math. Acad. Sci. Hungar., 18 (1967) 151–163.

[12] S.P. Glasby, Using recurrence relations to count certain elements in symmetric groups, European J. Combin., 22 (2001) 497–501.

[13] R.B. Herrera, The number of elements of given period in finite symmetric groups, Am. Math. Monthly, 64 (1957) 488–490.

[14] B. Külshammer, J.B. Olsson and G.R. Robinson, Generalized blocks for symmetric groups, Invent. Math., 151 (2003) 513–552.

[15] J. Leaños, R. Moreno and L.M. Rivera–Martínez, On the number of mth roots of permutations, Australas. J. Combin., 52 (2012) 41–54.

[16] Z.C. Lin, D.G.L. Wang and T.Y. Zhao, A decomposition of ballot permutations, pattern avoidance and Gessel walks, J. Combin. Theory Ser. A, 191 (2022) 105644.

[17] A. Maróti, Symmetric functions, generalized blocks, and permutations with restricted cycle structure, European J. Combin., 28 (2007) 942–963.

[18] The OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, `https://oeis.org`.

[19] S. Spiro, Ballot permutations and odd order permutations, Discrete Math., 343 (2020) 111869.

[20] H.S. Wilf, generatingfunctionology, 3rd Ed., CRC Press, 2005.