r-Enriched Permutations and an Inequality of Bóna-McLennan-White

William Y.C. Chen and Elena L. Wang

Center for Applied Mathematics
Tianjin University
Tianjin 300072, P.R. China

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

Dedicated to Persi W. 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. In general, given $r \geq 2$, we define an r-enriched permutation to be a permutation with r-singular cycles colored by one of the colors $1,2,\ldots,r-1$. In this setup, we discover a duality between r-regular permutations and enriched r-cycle permutations, which yields a stronger version of an inequality of Bóna-McLennan-White. This answers their question of seeking a fully combinatorial understanding of the monotone property. When r is a prime power q^l, we further show that $p_r(n)$ is monotone without using generating functions. In the case $n+1 \not\equiv 0 \pmod{q}$, 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 related to permutations with an r-th root, see, e.g., [6, 8, 14]. For an integer $r \geq 2$, we call a cycle r-regular if its length is not divisible by r and call a cycle r-singular if its length is divisible by r. Suppose that permutations are represented in the cycle notation. A permutation is called r-regular if all of its cycles are r-regular, and an r-cycle permutation is referred to a permutation with r-singular cycles. These terms were coined by Külshammer, Olsson, and Robinson [14]. As is customary, 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 the cycle lengths [21, p. 158]. The set of permutations of $[n]$ with an r-th root is denoted by S_n^r. The exponential generating function of $|S_n^r|$ has been derived by Bender [2], see also [21, p. 159]. When r is a prime power, the characterization takes a simpler form.

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

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 realized later that the above formula holds naturally for an arbitrary integer $r \geq 2$, for example, see [17].

There are various ways to count $\text{Reg}_r(n)$ and $\text{Cyc}_r(n)$, see [1, 4, 6, 8, 12, 17, 21]. 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 permutation of $[n-1]$. As a consequence, they confirmed the conjecture of Wilf [21] 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 $(1\ 5\ 2\ 6\ 3\ 7\ 4\ 8)$. In a larger sense, for any prime r, they [8] proved that 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 always hold in general. For example, when $r = 6$, we have $p_6(4) = 1/6$ but $p_6(5) = 1/3$. One may consult the sequence A247005 in OEIS [19] for the number of permutations of $[n]$ with an r-th root. Nonetheless, Bóna, McLennan and White showed that for any $r \geq 2$,

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

as $n \to \infty$.

The table below 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: Values for $p_r(n)$.

As set forth by Bóna, McLennan and White, their proof of the monotone property is mostly combinatorial, and they left a question of searching for 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.

The case $r = 2$ deserves a special mention. The sets $\mathrm{Reg}_2(2n)$ and $\mathrm{Cyc}_2(2n)$ often appear as $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$, respectively. Both of them are enumerated by $((2n-1)!!)^2$, see A001818 in OEIS [19]. In the literature, 2-regular permutations are also known as odd order permutations, which are related to ballot permutations, see, for example, [3, 16, 20]. However, even order permutations are referred to permutations with at least one even cycle. These terms originated from the notion of the order of an element in a group.

There is a bijection between $\mathrm{Odd}(2n)$ and $\mathrm{Even}(2n)$, which does not seem to be as obvious as it looks at first glance. A correspondence has been found by Sayag based on the first fundamental transformation or 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 $\mathrm{Even}(2n)$.

Can these incremental transformations be carried over to the general case $r \geq 2$? An intuitive trial does not seem to work as indicated by small examples. The objective of this paper is to introduce the structure of r-enriched permutations, from which a suitable notion with regard to the duality comes into being. In this setting, 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. So we have provided an answer to the question of Bóna, McLennan and White for any prime $r \geq 3$. For the case $r = 2$, we fill up with some discussions for the sake of completeness.

Resorting to the 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 Knopfmacher and Warlimont [21, p. 158], we take a step further to show that for any prime power $r = q^l$, $p_r(n)$ is monotone, being aware that Chernoff [10] established the equality $p_r(n) = p_r(n+1)$ in the case $n+1 \not\equiv 0 \pmod{q}$, and

Leaños, Moreno and Rivera–Martínez [15] presented two approaches, with one using generating functions, and the other being combinatorial. Our approach to the monotone property may be considered combinatorial, at least in the sense that no generating functions played no roles.

2 r-Enriched permutations

The aim of this section is to establish a duality 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 enriched we mean that each r-singular cycle is colored by one of $r-1$ colors. Bear in mind that r-regular cycles is never colored.

Given $r \geq 2$, we shall use the symbol $*$ to signify an r-enriched structure. For example, $\mathrm{Cyc}_r^*(rn)$ denotes the set of enriched r-cycle permutations of $[rn]$. Throughout, we assume that a permutation is represented in the cycle notation, with each cycle being treated as a linear order with the minimum element placed at the beginning, and assume that the cycles of a permutation are listed in the increasing order of their minimum elements. 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, for $r = 3$, $(1\,2\,4)\,(3)\,(5\,6)$ is a nearly 3-regular permutation.

As an intermediate structure, enriched nearly r-regular permutations lead to a bridge between r-regular permutations and enriched r-cycle permutations. By iteration, we discover a duality between $\mathrm{Reg}_r(rn)$ and $\mathrm{Cyc}_r^*(rn)$. For $r = 2$, it reduces to a duality 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 $[n]$, where the length of the cycle containing 1 is k, and the other cycles are r-regular. We first construct 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 (Bóna, Mclennan and White [8])**.** *For all $r \geq 2$ and $n+1 \not\equiv 0 \pmod r$, there is a bijection Ψ from $\mathrm{Reg}_r(n) \times [n+1]$ onto $\mathrm{Reg}_r(n+1)$.*

To employ the bijection, we do not really have to adjust the elements of the underlying sets to fit in the above decorated form. It seems to be more convenient to harness the following raw version, and it might be informative to reproduce the proof. For any nonempty set S, we use $\mathrm{Reg}_r(S)$ to denote the set of r-regular permutations of S.

Lemma 2.3 (A Reformulation)**.** *Let S be a nonempty finite set. For any $r \geq 2$, 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), where $x \in S$ and π is in $\mathrm{Reg}_r(S \setminus \{x\})$.*

Proof. Assume that σ is in $\mathrm{Reg}_r(S)$ 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, $\tilde{\sigma} = \sigma - D_1$ and let x be the last entry in D_1. 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 $\Delta(\sigma) = (x, \tilde{\sigma})$. In this case, 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 $\Delta(\sigma) = (x, C_1\,\tilde{\sigma})$. In this case, the element x is bigger than the smallest element of $C_1\,\tilde{\sigma}$. Since $l \not\equiv 0, 1 \pmod r$, we have $|C_1| = l - 1 \not\equiv -1, 0 \pmod r$.

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 case, the element x is bigger 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 $\tilde{\pi} = \pi - C_1$. Conversely, the map Δ^{-1} will place x as the last entry in the first cycle of $\Delta^{-1}(x, \pi)$. Accordingly, we face with 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 bigger 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 bigger 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 $|\pi - C_1| = |\pi| - l \not\equiv 0 \pmod r$. Thus we can apply Δ to $\pi - C_1$ 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 $|D_1| \neq 1$. This completes the proof. ∎

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

Lemma 2.4. *For all $r \geq 2$ and $k \geq 1$, if $n-k \not\equiv 0 \pmod r$. 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 $Q_{r,k+1}(n)$ with the help of the above bijection Δ. Assume that $n-k \not\equiv 0 \pmod r$ and $k \geq 1$. Given

$\sigma \in Q_{r,k}(n)$, let $\tilde{\sigma} = \sigma - C_1$, where C_1 is the first cycle in σ, that is, $\tilde{\sigma}$ is the permutation obtained from σ by removing the cycle containing 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 clearly in $Q_{r,k+1}(n)$.

Conversely, let us construct 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 $\tilde{\pi} = \pi - C_1$. 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 both are inverses to each other. Thus φ is a bijection. ∎

Writing $n-k = mr+d$ with $0 < d < r$, it is known that, see [1, 4, 6, 8, 12, 17, 21],

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

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 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 $k \geq 1$, there is a bijection φ between $A_{2n,2k-1}$ and $P_{2n,2k}$, and there is 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

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

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 establish the following incremental transformation Λ by taking into account the length of the first cycle.

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 in regard with the length of the first cycle of π.

If π is in $\mathrm{NReg}_r(rn)$, that is, $i = r-1$, in this case, we get an enriched permutation in $\mathrm{NReg}_r^*(rn)$, whose first cycle has color $r-1$. Set it to be $\Lambda(\sigma)$. If π is still 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 goes on until we obtain a permutation π in $\mathrm{NReg}_r(rn)$. Finally, we obtain an enriched permutation in $\mathrm{NReg}_r^*(rn)$ whose first cycle has color i. We set it to be $\Lambda(\sigma)$. Clearly, it takes $r-i$ steps to reach this point.

For example, if $r=3$, then $\Lambda((3)\,(5\ 6)) = (3\ 6\ 5)_1$. It is readily seen that the process is reversible because the color of the r-singular cycle keeps a record of the number of times that the map φ is applied. Thus Λ is a bijection. ∎

Below is an example for $r=3$:

$$(1\ 2)\,(3\ 4)\,(5\ 6) \longleftrightarrow (1\ 2\ 4)_2\,(3)\,(5\ 6).$$

The bijection Φ in Theorem 2.1 can be constructed with the aid of the bijection Λ from $\mathrm{Reg}_r(rn)$ to $\mathrm{NReg}_r^*(rn)$. For example, for $r=3$, we have

$$(1\ 2)\,(3\ 4)\,(5\ 6) \longleftrightarrow (1\ 2\ 4)_2\,(3\ 6\ 5)_1.$$

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 is what is needed to serve the purpose. 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 is constituted 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 holds 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 holds 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 [21, 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 2.2, 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 account 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 (Bóna, Mclennan and White [8])**.** *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 has been proved in [8] by means of generating functions. In fact, we observe that a stronger version of (3.1) holds, which can be deduced from the following known formulas, see [1, 4, 6, 8, 12, 17, 21]. 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 the colors of r-singular cycles 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 completes 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 $n+1 \equiv 0 \pmod{r^2}$.

Consider the case $r = 2$. As defined before, $|\mathrm{Reg}_r(0)| = 1$ and $|\mathrm{Cyc}_r(0)| = 1$. Once the Lemma 2.2 is established, it is easy to get the following recurrence of $|\mathrm{Reg}_r(rm)|$. For details, one can 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, 18]. In [1], it has been shown that

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

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

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

This proves (3.6).

Similarly, the following recurrence relation for $\mathrm{Cyc}_r(rm)$ holds. We can prove this also using the recursive generation of permutations in the cycle notation.

Lemma 3.6. *For all $r \geq 2$ and $m \geq 1$, 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

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

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 lead to 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. The case $r = 2$ requires a special treatment.

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

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

Proof. For $m \geq 1$, applying 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 $m_0 = 4$. ∎

Owing to the relation (3.8), the proof in [8] for $r = 2$ can be recast in combinatorial terms. More precisely, it can be shown that we have $p_2(n+1) < p_2(n)$ whenever $n+1 \equiv 0 \pmod 4$, with the only exceptions for $n = 3, 7, 11$. For these three special cases, we can look up the data given in [8] or the sequence A247005 in OEIS [19]. By inspection, 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 all primes $r \geq 2$, a combinatorial analysis is accomplished, assuming that the use of data for special cases is allowed. At any rate, the bottom line is that generating functions play no role here.

4 The monotone property for prime powers

Prompted by numerical evidence, we find that the monotone property remains valid for prime powers. Below is the table of $p_r(n)$ for $r = 4, 8, 9$ and $1 \leq n \leq 12$.

Theorem 4.1. *For all positive integers n and all $r = q^l$, where q is a prime and $l \geq 1$, we have $p_r(n) \geq p_r(n+1)$.*

Like the case for primes, the monotone property stands on the following cases subject to modulo conditions on $n+1$. First, we recall an equality of Chernoff [10].

$r \backslash n$	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: Values for $p_r(n)$.

Theorem 4.2 (Chernoff)**.** *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.

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

(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 holds 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 holds only when $r = 2$ and $n = 3$.

To prove the above theorem, it is necessary to employ some auxiliary inequalities. Even though these estimates can be considerably improved, we will be content with coarse lower bounds in order to keep the proofs brief. First, let us recall a characterization of permutations of $[n]$ with an r-th root, for a prime power r. In full generality, a criterion was given by Knopfmacher and Warlimont, see Wilf [21, p. 158].

Definition 4.4. *Let ρ be a partition, and let q, r be positive integers. We say that ρ is q-divisible if all its parts are divisible by q, and we say that (q, r)-divisible,* *denoted $(q,r) \mid \rho$, if it is q-divisible, and for any i, the number of occurrences of the part iq is a multiple of r. We assume that $(q,r) \mid \emptyset$, where $\emptyset$ denote the empty partition.*

For a permutation σ of $[n]$, we may partition the set of its cycles into two kinds. Use $R_q(\sigma)$ to denote the corresponding permutation consisting of its q-regular cycles and $S_q(\sigma)$ to denote the permutation consisting of its q-singular cycles, in lieu of $\sigma_{(\sim q)}$ and $\sigma_{(q)}$ as used in [8]. We say that a permutation σ is of q-singular cycle type ρ if $S_q(\sigma)$ is of type ρ. Let $S_{\rho,q}(n)$, in place of $\mathrm{DIV}_{\rho,q}(n)$ as used in [8], denote the set of permutations of $[n]$ with q-singular cycle type ρ. For example, given $q=2$ and $r=2$, $(1\ 2)(3\ 4)(5\ 9\ 7\ 8)(6\ 10\ 11\ 13)(12)$ is of 2-singular type $(4^2,2^2)$, and its 2-singular type is $(2,2)$-divisible. For the special case $\rho=\emptyset$, $S_{\rho,q}(n)$ becomes the set of permutations of $[n]$ with q-regular cycles, i.e., $\mathrm{Reg}_q(n)$.

Proposition 4.5 (Knopfmacher and Warlimont)**.** *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 its q-singular cycle type is (q,r)-divisible.*

We take up the common notation

$$S_n^r = \{\sigma^r \mid \sigma \in S_n\}$$

for the set of permutations of $[n]$ with an r-th root. In connection with regular permutations, the above characterization implies that for a prime power $r=q^l$ with q prime and $l \geq 1$, and $n \geq 1$,

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

Given any $q \geq 2$, not necessarily a prime, let $r=q^l$, $l \geq 1$, and let $\mathrm{Cyc}_{q,r}(n)$ denote the set of permutations of $[n]$ such that each cycle length is a multiple of q and each cycle length occurs a multiple of r times. In other words, $\mathrm{Cyc}_{q,r}(n)$ is the set of permutations of $[n]$ whose cycle type is (q,r)-divisible. The following relation is parallel to Lemma 3.2 in [8]. The construction in the proof is reminiscent of the argument in the proof of Lemma 3.6.

Lemma 4.6. *For any $m \geq 1$, let $r = q^l$, where $q \geq 2$ 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 construct 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 then produce certain permutations in $\mathrm{Cyc}_{qr}(mqr)$. The number of permutations one can generate 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

$$\sum_i iqk_ir = mqr.$$

This completes the proof. ∎

The following lemma is analogous to Lemma 3.3 in [8].

Lemma 4.7. *Let $r = q^l$, where $q \geq 2$ and $l \geq 1$. For any $m \geq 1$, 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 be used in the proof of Theorem 4.3.

Lemma 4.8. *Let $r = q^l$ with $q = 2$ and $l \geq 2$, or with any prime $q \geq 3$ and $l \geq 1$, we have for $m \geq 1$,*

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

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

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

By (4.2), that is, $\mathrm{Reg}_q(mqr) \subseteq S^r_{mqr}$, we get

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

as claimed. ∎

Recall that S^r_n denote the set of permutations of $[n]$ with an r-th root. The proof of Theorem 4.3 also relies on Corollary 2.16 in [8], which reads as follows, where for a partition ρ, we write $|\rho|$ for the sum of parts of ρ.

Proposition 4.9 (Bóna, Mclennan and White [8]). *Let $q \geq 2$, $n \geq 1$, and let ρ be a q-divisible partition such that $|\rho| \leq n$. If $n+1$ is a multiple of q, then*

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

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

In the case $\rho = \emptyset$, the equality says 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 is a consequence of the bijection from $\mathrm{Reg}_q(n) \times [n]$ to $\mathrm{Reg}_q(n+1)$ due to Bóna, Mclennan and White, see Lemma 2.6 in [8]. It is easily seen that for $n \geq 1$ and $q \geq 2$, if a permutation σ of $[n]$ is of q-singular cycle type ρ, then the permutation σ' of $[n+1]$ by adjoining the singleton cycle $(n+1)$ to σ is also of q-singular cycle type ρ.

We are now ready to prove Theorem 4.3.

Proof of Theorem 4.3. Given that r is a prime power q^l, by Proposition 4.5, we see that a permutation of $[n]$ is in S^r_n if and only if its q-singular cycle type is (q,r)-divisible. So we can write

$$S^r_n = \bigcup_{\substack{|\rho| \leq n, \\ (q,r)\,|\,\rho}} S_{\rho,q}(n).$$

Hence

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

Again, by Proposition 4.5, 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 partition ρ with $|\rho| \le n$ and $(q,r) \mid \rho$, Proposition 4.9 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,

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

Consequently,

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

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 partition 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

$$n\,|S_n^r| \geq \left|S_{n+1}^r\right|,$$

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

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

Substituting (4.12) into (4.10), we obtain

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

Expressing (4.6) as

$$\frac{1}{mqr}\left|S_{mqr}^r\right| > \left|\mathrm{Cyc}_{q,r}(mqr)\right|,$$

and invoking (4.13), we obtain that

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

It follows that

$$mqr\left|S_{mqr-1}^r\right| > \left|S_{mqr}^r\right|.$$

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 the equalities are attained in (i) and (ii) can be easily discerned. This completes the proof. ∎

Acknowledgment. This work was supported by the National Science Foundation of China.

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] E. Munarini and D. Torri, Cayley continuants, Theoret. Comput. Sci., 347 (2005) 353–369.

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

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

[21] H.S. Wilf, Generatingfunctionology: Third Edition, CRC Press, 2005.