AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **52** (2012), Pages 41–54

On the number of mth roots of permutations

Jesús Leaños

Unidad Académica de Matemáticas
Universidad Autónoma de Zacatecas, Zac., Zacatecas
Mexico
jelema@uaz.edu.mx

Rutilo Moreno

Instituto de Física
Universidad Autónoma de San Luis Potosí
San Luis Potosí, S. L. P.
Mexico
rutilo.moreno@gmail.com

Luis Manuel Rivera-Martínez*

Ingeniería Eléctrica, Jalpa
Universidad Autónoma de Zacatecas, Jalpa, Zacatecas
Mexico
luismanuel.rivera@gmail.com

Abstract

Let m be a fixed positive integer. It is well-known that a permutation σ of $\{1,\dots,n\}$ may have one, many, or no mth roots. In this article we provide an explicit expression and a generating function for the number of mth roots of σ. Let $p_m(n)$ be the probability that a random n-permutation has an mth root. We also include a proof of the fact that $p_m(jq) = p_m(jq+1) = \cdots = p_m(jq+(q-1))$, $j = 0, 1, \dots,$ when m is a power of a prime number q.

1 Introduction and main results

Let S_n be the group of all permutations of the finite set $[n] = \{1,\dots,n\}$. Let m be a fixed positive integer. We say that $\sigma \in S_n$ has an mth root or that σ is an mth power

* Partially supported by PROMEP (SEP), grant UAZ-PTC-103.

if there exists a permutation $\tau \in S_n$ with $\tau^m = \sigma$. For fixed m, not all permutations have an mth root ([15], Theorem 4.8.2); however, Glebsky and Rivera [7] have proved that for sufficiently large n, any permutation has an "almost" mth root (in the sense of the Hamming distance [6]). Now, if we know that a permutation σ has at least one mth root, how many mth roots can σ have? We can find an explicit expression for this quantity in the paper of Pavlov [10]. Also, in the article of Annin, Jansen and Smith [1], there appears a classification of the elements in S_n and A_n that have mth roots, and they propose some problems related with the roots of permutations. In particular, our work is about some questions on Problem 1 in Section 4 of [1].

The main results of this paper are an explicit expression for the number of mth roots of any n-permutation σ (Theorem 1) and a generating function for this number (Theorem 2). In order to obtain our expression we define some sets of non-negative integers that seem interesting by themselves (see Section 2). In particular, such sets provide a simpler expression than the corresponding expression in [10]. Moreover, this new expression allows us to compute the number of mth roots of a permutation in an effective way using a computer algebra system.

Another classical problem consists in estimating the number of permutations in S_n that admit an mth root. Turán [14] gave an upper bound when m is a prime number and Blum [2] gave an asymptotic formula for the case $m = 2$. Recently, Bóna, McLennan and White [4] proved that the probability that a random permutation of length n has an mth root with m prime, is monotonically non-increasing in n. See also the work of Pouyanne [12] for an asymptotic study for any positive integer m, and the work of Bollobás and Pittel [3] who continued the work of Pouyanne and studied the limiting distribution of the root degree of a permutation. This problem can be easily reformulated as the problem about the probability, $p_m(n)$, that an n-permutation chosen uniformly at random has an mth root. For this problem, we give a proof of the fact that when m is a power of a prime q, for all $j \geq 0$, $p_m(jq) = p_m(jq+1) = \cdots = p_m(jq+(q-1))$. For the case m a prime, see the paper of Bóna et al. [4] that includes a combinatorial proof of the equivalent equalities. The paper of Maróti [9], and the bibliography therein, is also recommended for related results about the proportion of ℓ-regular elements in the symmetric group S_n. Another interesting article is due to Pournaki [11], who worked on the problem of determining the number of even permutations with roots.

Before stating our main results, we shall give some notation and definitions. As usual, we denote by $\mathbb{N}$ (respectively $\mathbb{N}_0$) the set of positive (respectively, non-negative) integers. The *cycle type* of an n-permutation is a vector $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ that indicates that the permutation has a_i cycles of length i for every $i \in [n]$. It is an easy exercise to prove that conjugated permutations have the same number of mth roots. Let $m, \ell \in \mathbb{N}$ and $a \in \mathbb{N}_0$. We define the following sets

$$G_m(\ell, a) := \{g \ \in \mathbb{N} : \ g \leq a; \ \gcd(g\ell, m) = g\},$$

and

$$G_m(\ell) := \{g \ \in \mathbb{N} : \ \ \gcd(g\ell, m) = g\}.$$

Clearly $G_m(\ell, a) \subseteq G_m(\ell)$, and both are finite sets. Note that if $a = 0$, then $G_m(\ell, a) = \emptyset$. We will name $(g_1, \dots, g_k)$ the *associate vector* of $G_m(\ell, a)$ if $G_m(\ell, a) = \{g_1, \cdots, g_k\}$ and $g_1 < g_2 < \cdots < g_k$. For every set $G_m(\ell, a)$ of cardinality $k \geq 1$ we define the set of vectors

$$\mathcal{E}_m(\ell, a) := \{\varepsilon \ \in \mathbb{N}_0^k \ : \ \mathbf{g} \cdot \varepsilon = a, \ \text{ with } \mathbf{g} \text{ the associate vector of } G_m(\ell, a)\}.$$

Note that if equation $g_1 x_1 + \cdots + g_k x_k = a$ does not have non-negative integer solutions then $\mathcal{E}_m(\ell, a) = \emptyset$. We use the convention that $\sum_{i \in \mathcal{I}} s_i = 0$ if $\mathcal{I}$ is empty.

Next, we present our main results about the number of mth roots of permutations.

Theorem 1. *Let m be a fixed positive integer. Let σ be any n-permutation of type $\mathbf{a}$, i.e. for every $\ell \in [n]$, σ has a_ℓ cycles of length ℓ. Let $r^{(m)}(\mathbf{a})$ be the number of mth roots of σ; then*

$$r^{(m)}(\mathbf{a}) = \prod_{\substack{\ell \geq 1 \\ a_\ell \neq 0}} a_\ell! \left(\sum_{\varepsilon \ \in \mathcal{E}_m(\ell, a_\ell)} \ \prod_{i=1}^{k} \frac{\ell^{(g_i - 1)\varepsilon_i}}{g_i{}^{\varepsilon_i} \varepsilon_i!} \right),$$

where $k = |G_m(\ell, a_\ell)|$, and $\mathbf{g} = (g_1, \dots, g_k)$ is the associate vector of $G_m(\ell, a_\ell)$.

Our next theorem provides a generating function for the number of mth roots of permutations.

Theorem 2. *Let m, n be positive integers, and $a_1, \dots, a_n$ be non-negative integers. For $n = a_1 + 2a_2 + \cdots + na_n$, the coefficient of $\frac{t_1^{a_1} \cdots t_n^{a_n}}{a_1! \cdots a_n!}$ in the expansion of*

$$\exp\Big(\sum_{\ell \geq 1} \sum_{g \in G_m(\ell)} \frac{\ell^{g-1}}{g} t_\ell^g \Big),$$

is the number of mth roots of an n-permutation of cycle type $\mathbf{a} = (a_1, \dots, a_n)$.

Note that Theorems 1 and 2 allow us to compute the number of mth roots of a permutation in an effective way using a computer algebra system.

The outline of the paper is as follows. In Section 2 we present some preliminaries results about the sets $G_m(\ell, a)$ and $G_m(\ell)$. In Section 3 we recall how to extract roots of permutations. In Section 4 we give the proofs of Theorem 1 and Theorem 2. Finally, in Section 5 we present a proof of the fact that probability $p_m(n)$ satisfies $p_m(jq) = p_m(jq + 1) = \cdots = p_m(jq + (q - 1))$, where $j = 1, \dots$ and m is a power of a prime number q.

2 Preliminaries

The next notation is standard, and it can be found in several books, for example, in the book of Schoup ([13], Section 1.3). For integer n and prime p we will write $\nu_p(n)$

for the highest power of p that divides n. In this notation the definition of $\gcd(a,b)$ is

$$\gcd(a,b) = \prod_{p\,\in\mathcal{P}} p^{\min(\nu_p(a),\nu_p(b))},$$

where $\mathcal{P}$ is the set of all primes. We use the convention that $\gcd(g) = g$ for every $g \in \mathbb{N}$. If a and b are positive integers then

$$\nu_p(\gcd(a,b)) = \min(\nu_p(a), \nu_p(b)),$$

and

$$\nu_p(a \cdot b) = \nu_p(a) + \nu_p(b).$$

Note that a divides b if and only if $\nu_p(a) \leq \nu_p(b)$ for all primes p. The following definition can be found in the book of Wilf ([15], page 148). For a pair ℓ, m in $\mathbb{N}$, the number $((\ell,m))$ is defined as

$$((\ell,m)) = \prod_{\substack{p\,\mid\,\ell \\ p\,\in\mathcal{P}}} p^{\nu_p(m)}.$$

The number $((\ell,m))$ is very important in the characterization of the permutations that admit mth roots (Theorem 3, Section 3). As the sets $G_m(\ell,a)$ and $G_m(\ell)$ play an important role in our expressions, we first prove some interesting propositions about the elements in these sets. Some of these propositions show the relation between the elements of $G_m(\ell,a)$ and $G_m(\ell)$ with the number $((\ell,m))$.

Proposition 1. *If $a \geq 1$ then $1 \in G_m(\ell,a)$ if and only if* $\gcd(\ell,m) = 1$.

Proof. Because $1 = \gcd(\ell,m) = \gcd(1\cdot\ell,m)$, we have $1 \in G_m(\ell,a)$. The converse follows from the definition of $G_m(\ell,a)$. □

Proposition 2. *Let g, ℓ and m be positive integers. Then $g \in G_m(\ell)$ if and only if conditions 1 and 2 hold:*

1. *Any prime divisor p of g divides m and satisfies one of the following:*
   (a) *If p divides ℓ, then $\nu_p(g) = \nu_p(m)$.*
   (b) *If p does not divide ℓ, then $\nu_p(g) \leq \nu_p(m)$.*
2. *If p is a prime that does not divide g, then p does not divide* $\gcd(\ell,m)$.

Proof. For the "if" part: As any prime divisor p of g satisfies (1) $\nu_p(g) \leq \nu_p(m)$, and therefore $g \mid m$ and $g \mid \gcd(g\ell,m)$. Now we prove that $\gcd(g\ell,m) \mid g$. Let p be any prime divisor of $\gcd(g\ell,m)$, then $p \mid g\ell$ and $p \mid m$. If $p \nmid g$ then $p \mid \ell$ and $p \mid \gcd(\ell,m)$, which implies a contradiction of condition (2), so $p \mid g$. If p divides ℓ then by (1a), $\nu_p(g) = \nu_p(m)$. Thus

$$\nu_p(\gcd(g\ell,m)) = \min(\nu_p(g\ell), \nu_p(g)) = \nu_p(g).$$

If p does not divide ℓ, $\nu_p(\ell)=0$, and by property (1b) $\nu_p(g)\leq\nu_p(m)$. Then

$$\nu_p(\gcd(g\ell,m))=\min(\nu_p(g)+\nu_p(\ell),\nu_p(m))=\nu_p(g).$$

Therefore $\gcd(g\ell,m)\mid g$, and $g\in G_m(\ell)$.

For the converse, let p be any prime divisor of $g\in G_m(\ell)$. By definition $g=\gcd(g\ell,m)$ and then $p\mid m$. We first prove (1a). The hypothesis $p\mid\ell$ implies $\nu_p(\ell)>0$, and $\nu_p(g)=\min(\nu_p(g)+\nu_p(\ell),\nu_p(m))=\nu_p(m)$. Now we prove (1b). As $p\nmid\ell$, $\nu_p(\ell)=0$ and $\nu_p(g)=\min(\nu_p(g)+\nu_p(\ell),\nu_p(m))$, and therefore $\nu_p(g)\leq\nu_p(m)$. Finally, we prove (2), Suppose that there exists a prime p such that $p\nmid g$ and $p\mid\gcd(\ell,m)$. Then $p\mid\gcd(g\ell,m)=g$, which is clearly a contradiction. □

Remark 1. There is another way to build the set $G_m(\ell)$: choose any divisor $d\geq 1$ of m, with d relatively prime to ℓ, and define $g:=m/d$. Thus, we have that $\gcd(\ell g,m)=\gcd(\ell g,gd)=g$, as it is required. Then, the set $G_m(\ell)$ can be defined as the set $\{g=m/d\ :\ d\in\mathbb{N},d\mid m \text{ and} \gcd(d,\ell)=1\}$. It is an easy exercise to show that both sets are the same. To build the set $G_m(\ell,a)$ follow the same procedure only with the condition that $g=m/d\leq a$.

The following proposition shows that $((\ell,m))$ is an element of $G_m(\ell)$.

Proposition 3. *Let ℓ, m, a be positive integers. Then*

1. *$((\ell,m))$ belongs to $G_m(\ell)$;*
2. *if $((\ell,m))$ divides a, then $((\ell,m))\in G_m(\ell,a)$.*

Proof. First we show *1.* The case $\gcd(\ell,m)=1$ follows from Proposition 1. If $\gcd(\ell,m)>1$, for any prime divisor p of $((\ell,m))$, we have that p divides $\gcd(\ell,m)$ and p divides ℓ and m. By definition of $((\ell,m))$, we have $\nu_p\big(((\ell,m))\big)=\nu_p(m)$, and condition (1) in Proposition 2 holds. Let q be a prime that does not divide $((\ell,m))$, if $q\nmid\ell$ clearly $q\nmid\gcd(\ell,m)$ and if $q\mid\ell$, use the hypothesis that $q\nmid((\ell,m))$ and the definition of $((\ell,m))$ to obtain $\nu_q(m)=0$. Therefore, condition (2) in Proposition 2 also holds, and $((\ell,m))\in G_m(\ell)$. Now we show the second part. As a consequence of the first part of this proposition, $((\ell,m))\in G_m(\ell)$. As $((\ell,m))$ divides a, $((\ell,m))\leq a$, and therefore $((\ell,m))\in G_m(\ell,a)$. □

Remark 2. Note that if $k=\gcd(k\ell,m)$ then $\gcd(\ell,m)$ divides k.

Proposition 4. *Let ℓ,m be positive integers. If $G_m(\ell)=\{g_1,\dots,g_h\}$, then* $\gcd(g_1,\dots,g_h)=((\ell,m))$.

Proof. We begin with the case $\gcd(g_1,\dots,g_h)=1$. As a consequence of Remark 2, if $g_i=\gcd(g_i\ell,m)$ then $\gcd(\ell,m)$ divides g_i for any $i\in[h]$, and therefore we have $\gcd(\ell,m)=1$ which implies that $((\ell,m))=1$. Now, for $d:=\gcd(g_1,\dots,g_h)>1$, from part (1) of Proposition 3, $((\ell,m))\in G_m(\ell)$, and therefore d divides $((\ell,m))$. Now we prove that $((\ell,m))$ divides d. As $d>1$ and $d\mid((\ell,m))$ then $((\ell,m))>1$.

Let p be any prime factor of $((\ell, m))$. From the definition of $((\ell, m))$, p divides ℓ and m, thus p divides $\gcd(\ell, m)$. Let g be any element in $G_m(\ell)$. So $g = \gcd(g\ell, m)$. By Remark 1, we know that $\gcd(\ell, m)$ divides $\gcd(g\ell, m)$ and therefore p divides g. By Proposition 2 (1a), the exponent of p in any $g \in G_m(\ell)$ is $\nu_p(m)$, then $\nu_p(d) = \nu_p(m)$. On the other hand, by definition $\nu_p\big(((\ell, m))\big) = \nu_p(m)$, and therefore $\nu_p\big(((\ell, m))\big) = \nu_p(d)$, so we conclude that $((\ell, m))$ divides d. □

A consequence of this proposition is that $((\ell, m))$ is the least element of the set $G_m(\ell)$. We also obtain the following corollary

Corollary 1. *Let a, ℓ, m be positive integers. Let $G_m(\ell, a) = \{g_1, \dots, g_j\}$. Then*

$$\gcd(g_1, \dots, g_j) = ((\ell, m)).$$

Proposition 5. *Let m, ℓ, a be positive integers. Let $G_m(\ell, a) = \{g_1, \dots, g_h\}$. Then $((\ell, m))$ divides a if and only if*

$$g_1x_1 + g_2x_2 + \cdots + g_hx_h = a, \tag{1}$$

has non-negative integer solutions.

Proof. If $h = 1$, then $G_m(\ell, a) = \{((\ell, m))\}$ by Proposition 4, and the result follows. Now, we assume $h > 1$. The if part follows easily because $((\ell, m)) = \gcd(g_1, \dots, g_h)$ (Corollary 1). For the converse, by Proposition 3 part (2), $((\ell, m)) \in \{g_1, \dots, g_h\}$. Now, take $g_i = ((\ell, m))$, $x_i = a/((\ell, m))$ and $x_j = 0$ for any $j \neq i$. □

We conclude this section with one proposition about the elements of $G_m(\ell)$ for the case when ℓ and m are relatively prime.

Proposition 6. *If $\gcd(\ell, m) = 1$, then $G_m(\ell)$ is equal to the set of positive divisors of m.*

Proof. Since $\gcd(\ell, m) = 1$, it follows that $\gcd(g\ell, m) = \gcd(g, m)$. Any g that satisfies the relation $g = \gcd(g\ell, m) = \gcd(g, m)$ is a positive divisor of m. □

3 Roots of permutations

Let σ be an n-permutation and let m be a fixed positive integer. A permutation $\tau \in S_n$ that satisfies $\tau^m = \sigma$ may or may not exist. If such τ exists, it is called an mth root of σ. The following theorem is due to Knopfmacher and Warlimont [15, p. 148, Theorem 4.8.2], and it gives a characterization of the n-permutations that have mth roots.

Theorem 3. *Let m be a positive integer. A permutation σ has an mth root if and only if for every $\ell = 1, 2, \dots$ the number of ℓ-cycles that σ has is divisible by $((\ell, m))$.*

This theorem gives us information about the cycle structure of permutations that admits mth roots. But, if we know that a permutation has mth roots, we need a procedure to get all of its roots (see, for example [8, §3.3]). The first important observation is that we can build any mth root τ of σ if we work with cycles of σ with different lengths separately. Indeed, if τ is an mth root of σ, with $\tau = C_1 \cdots C_s$ its disjoint cycle factorization, then $\sigma = \tau^m = C_1^m \cdots C_s^m$, where C_i^m consists in $\gcd(|C_i|, m)$ cycles of length $|C_i| / \gcd(|C_i|, m)$ each. Let σ_ℓ be the part of σ, that consists in the product of all cycles D_i of length ℓ in σ ($a_\ell \neq 0$, where a_ℓ is the number of cycles of length ℓ in σ). So, we can see permutation σ as a product of parts σ_ℓ, where every part σ_ℓ consist in all the cycles of length ℓ in the disjoint cycle factorization of σ. Let τ_ℓ be the part of τ whose mth power produces the part σ_ℓ

$$\tau_\ell^m = \sigma_\ell = \prod_{|D_i|=\ell} D_i;$$

and we can find τ_ℓ, and therefore τ, working with σ_ℓ independently. This is for every length $\ell \neq 0$ in cycles of σ. Now, we need to find the admissible lengths, $|C_i|$, of cycles in τ_ℓ. We know that for any cycle C_i in τ_ℓ, $|C_i| = \ell \gcd(|C_i|, m)$, and we write $g = \gcd(|C_i|, m)$. We need to find $g \leq a_\ell$, in such a way that $g = \gcd(g\ell, m)$. Note that this number exists because we are assuming that the permutation has mth roots, and by Theorem 3 and Proposition 3 (part 2), $((\ell, m)) \in G_m(\ell, a_\ell)$. Thus, any g cycles of σ_ℓ, $D_{i_1}, \ldots, D_{i_g}$, can be combined in a suitable way (see, for example, proof of Theorem 3 in [1] or proof of Theorem 4.8.2 in [15]) into one $g\ell$-cycle C_i for τ_ℓ with $C_i^m = D_{i_1} \ldots D_{i_g}$.

Now to obtain all the mth roots of σ, we build the sets $G_m(\ell, a_\ell)$ and $\mathcal{E}_m(\ell, a_\ell)$, for every ℓ with $a_\ell \neq 0$. Theorem 3 and Proposition 5 show that $\mathcal{E}_m(\ell, a_\ell)$ is not empty if and only if $((\ell, m))$ divides a_ℓ. The elements of $\mathcal{E}_m(\ell, a_\ell)$ represent the different ways in which we can group the cycles of σ_ℓ. This is, for $\varepsilon \in \mathcal{E}_m(\ell, a_\ell)$, the coordinates $\varepsilon_1, \varepsilon_2, \ldots$ of ε and the coordinates $g_1, g_2 \ldots$ of the associate vector $\mathbf{g}$ of $G_m(\ell, a_\ell)$ means that τ_ℓ has ε_1 cycles of length $g_1\ell$, ε_2 cycles of length $g_2\ell$, etc.

4 Proof of Theorems 1 and 2

In this section, we present the proofs of two of our main results. Theorem 1 provides an explicit expression for the number of mth roots of permutations of type $\mathbf{a}$, and Theorem 2 provides a generating function for this number. We use the next notation: Let i, j be any positive integers. For an n-permutation of Type $(i)^j$ we mean that this permutation has j cycles of length i, and $n = ij$. First, we prove the following proposition.

Proposition 7. *Let $\ell, m \in \mathbb{N}$ be fixed. Let $g \in G_m(\ell)$ and $p \in \mathbb{N}$. Let σ be any permutation of Type $(\ell)^{gp}$. Then the number of mth roots of σ, τ, of Type $(g\ell)^p$ is*

$$\frac{(gp)!\ell^{p(g-1)}}{g^p p!}.$$

Proof. From the gp cycles, we need to build p cycles of length $g\ell$ for τ. This we make by grouping the cycles in p bundles of g cycles each $(C_1, C_2, \ldots, C_g)$, and then, we build with each bundle, a cycle of length $g\ell$. In how many ways can we group the bundles? As no matter the order of the bundles, this problem is reduced to count the number of unordered partitions of a set of cardinality gp in p equal parts. This number is

$$\frac{(gp)!}{(g!)^p p!}.$$

For each of the p bundles $(C_1, C_2, \ldots, C_g)$, we need to arrange the elements of cycles $C_1, C_2, \ldots, C_g$ in a cycle D that satisfies $D^m = C_1 \cdots C_g$. We can use the procedure in the proof of Theorem 4.8.2 [15, §4.8]), applying it to all the possible combinations of cycles $C_1, C_2, \ldots, C_g$ and their elements in order to obtain all the possible different cycles D. With this procedure we obtain $(g-1)!\ell^{g-1}$ different such cycles. As we have p bundles, with g disjoint cycles each, we have $((g-1)!\ell^{g-1})^p$ different bundles of cycles $(D_1, D_2, \cdots, D_p)$ with which we can build the different mth roots. Therefore the number of mth roots of the required Type is

$$\frac{(gp)!}{(g!)^p p!}((g-1)!\ell^{g-1})^p = \frac{(gp)!\ell^{p(g-1)}}{g^p p!}.$$

□

4.1 Proof of Theorem 1

Let m be a positive integer, let σ be an n-permutation of type $\mathbf{a}$, i.e. σ has a_ℓ cycles of length ℓ for every $\ell \in [n]$. As we see in Section 3, we can build τ from σ working separately with each part σ_ℓ, $a_\ell \neq 0$. For every ℓ-cycle in σ we build the sets $G_m(\ell, a_\ell)$, and $\mathcal{E}_m(\ell, a_\ell)$. By Proposition 5, if σ_ℓ has an mth root, then $\mathcal{E}_m(\ell, a_\ell)$ will be a non-empty set. We will count all the mth roots of σ_ℓ. Take ε in $\mathcal{E}_m(\ell, a_\ell)$, and for every $i \in [h]$, $h = |G_m(\ell, a_\ell)|$, we will build ε_i $g_i\ell$-cycles for τ_ℓ. From the a_ℓ cycles of σ_ℓ, choose h subsets of $g_i\varepsilon_i$ cycles each one, this can be made in

$$\frac{a_\ell!}{\prod_{i=1}^h (g_i\varepsilon_i)!}$$

ways. Now, from every one of the $g_i\varepsilon_i$ cycles, we build ε_i cycles of length $g_i\ell$. By proposition 7 we have

$$\frac{(g_i\varepsilon_i)!}{(g_i!)^{\varepsilon_i}\varepsilon_i!}((g_i-1)!\ell^{g_i-1})^{\varepsilon_i}.$$

As this is for every $i \in [h]$ and all the cycles are disjoint, by the principle of multiplication we have

$$a_\ell! \prod_{i=1}^{h} \frac{1}{(g_i\varepsilon_i)!} \frac{(g_i\varepsilon_i)!}{(g_i!)^{\varepsilon_i}\varepsilon_i!} \left((g_i-1)!\ell^{g_i-1}\right)^{\varepsilon_i}$$

mth roots of σ_ℓ that consist of ε_i cycles of length $g_i\ell$, for every $i \in [h]$. This expression reduces to

$$a_\ell! \prod_{i=1}^{h} \frac{\ell^{(g_i-1)\varepsilon_i}}{g_i^{\varepsilon_i}\varepsilon_i!}.$$

Finally, we sum over all the elements in $\mathcal{E}_m(\ell, a_\ell)$. Repeat the process for every cycle length ℓ in σ with $a_\ell \neq 0$. So we have that the number of mth roots of a permutation of type $\mathbf{a}$ is

$$r^{(m)}(\mathbf{a}) = \prod_{\substack{\ell \geq 1 \\ a_\ell \neq 0}} a_\ell! \left(\sum_{\varepsilon\ \in \mathcal{E}_m(\ell, a_\ell)} \prod_{i=1}^{h} \frac{\ell^{(g_i-1)\varepsilon_i}}{{g_i}^{\varepsilon_i}\varepsilon_i!} \right).$$

Note that $r^{(m)}(\mathbf{a})$ is zero if and only if $\mathcal{E}_m(\ell, a_\ell)$ is an empty set for some ℓ, i.e. if a_ℓ is not a multiple of $((\ell, m))$.

4.2 A generating function: Proof of Theorem 2

First we obtain a generating function for permutations of Type $(\ell)^{gp}$.

Proposition 8. *Let ℓ, m be fixed positive integers. Let $g \in G_m(\ell)$. Let $p \in \mathbb{N}_0$. Let σ be any permutation of Type $(\ell)^{gp}$. Let $f(gp)$ be the number of mth roots of Type $(g\ell)^p$ of σ. Then*

$$\sum_{p \geq 0} f(gp) \frac{t_\ell^{gp}}{(gp)!} \ = \ \exp\left(\frac{\ell^{(g-1)}}{g} t_\ell^g\right).$$

Proof. Use Proposition 7 to obtain

$$\begin{aligned} \sum_{p \geq 0} f(gp) \frac{t_\ell^{gp}}{(gp)!} \ &= \ \sum_{p \geq 0} \frac{(gp)!\ell^{p(g-1)}}{g^p p!} \frac{t_\ell^{gp}}{(gp)!} \\ &= \ \sum_{p \geq 0} \frac{\ell^{p(g-1)}}{g^p} \frac{t_\ell^{gp}}{(p)!} \\ &= \ \exp\left(\frac{\ell^{(g-1)}}{g} t_\ell^g\right). \end{aligned}$$

□

Note that if $p = 0$, $f(gp) = 1$, but $p = 0$ does not have sense in this context, we use it only for technical purposes. Now, we give a generating function for the number of mth roots of a permutation of type $\mathbf{a}$, for m fixed.

Theorem 2. *For $n = a_1 + 2a_2 + \cdots + na_n$, the coefficient of $\dfrac{t_1^{a_1}\cdots t_n^{a_n}}{a_1!\cdots a_n!}$ in the expansion of*

$$\exp\Big(\sum_{\ell\geq 1}\sum_{g\in G_m(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\Big) \tag{2}$$

is the number of mth roots of an n-permutation of type $\mathbf{a} = (a_1, \ldots, a_n)$.

Proof. We expand equation (2) and we look for the coefficients of our interest. First note that for any ℓ the only factors that contribute to exponent of $t_\ell^{a_\ell}$ ($a_\ell \neq 0$) are the factors in

$$\prod_{g\in G_m(\ell)} e^{\frac{\ell^{g-1}}{g}t_\ell^g} = \prod_{g\in G_m(\ell)}\Big(\sum_{j\geq 0}\frac{\ell^{(g-1)j}}{g^j}t_\ell^{gj}\Big)\frac{1}{j!},$$

with $a_\ell = g_1j_1+\cdots+g_kj_k$, where $k = |G_m(\ell)|$, $\mathbf{g} = (g_i, \ldots, g_k)$ is the associate vector of $G_m(\ell)$ and $j_1, \ldots, j_k$ is any non negative solution of equation $g_1x_1+\cdots+g_kx_k = a_\ell$. The coefficient of any $t_\ell^{a_\ell}$ is

$$\sum_{g_1j_1+\cdots+g_kj_k=a_\ell}\prod_{i=1}^{k}\frac{\ell^{(g_i-1)j_i}}{g_i^{j_i}}\frac{1}{j_i!}.$$

For the coefficient of $t_\ell^{a_\ell}/a_\ell!$ multiply the previous expression by $a_\ell!$. Clearly the coefficient of $\frac{t_1^{a_1}\cdots t_n^{a_n}}{a_1!\cdots a_n!}$ comes from equation (2) when we take ℓ from 1 to n and this coefficient is

$$\prod_{\substack{\ell\geq 1\\ a_\ell\neq 0}} a_\ell! \sum_{g_1j_1+\cdots+g_kj_k=a_\ell}\prod_{i=1}^{k}\frac{\ell^{(g_i-1)j_i}}{g_i^{j_i}}\frac{1}{j_i!}.$$

Note that this expression is equivalent to the right hand side of equation in Theorem 1 by changing $g_1j_1 + \cdots + g_kj_k = a_\ell$ in the index of summation by $\varepsilon \in \mathcal{E}_m(\ell, a_\ell)$, where $\varepsilon = (j_1, \ldots, j_k) \in \mathcal{E}_m(\ell, a_\ell) = \{\varepsilon \in \mathbb{N}_0^k \ : \ g_1j_1 + \cdots + g_kj_k = a_\ell\}$. □

Another proof can be obtained using Proposition 8. For fixed length ℓ, we build the set $G_m(\ell)$, and for fixed $g \in G_m(\ell)$ we can obtain the generating function as in Proposition 8. Then we use properties of generating functions to obtain $\prod_{g\in G_m(\ell)} e^{\frac{\ell^{g-1}}{g}t_\ell^g}$. As for different ℓ, the variables t_ℓ are different, then we can obtain the desired generating function as the product $\prod_{\ell\geq 1}\prod_{g\in G_m(\ell)} e^{\frac{\ell^{g-1}}{g}t_\ell^g}$.

The next corollary is for the special case when m is equal to a prime number p. Note that by Propositions 2 and 6, we have that if $\gcd(\ell, p) = 1$ then $G_p(\ell) = \{1, p\}$ and for $\gcd(\ell, p) = p$, $G_p(\ell) = \{p\}$.

Corollary 2. *Let p be a fixed prime number. For $n = a_1 + 2a_2 + \cdots + na_n$, the coefficient of $\frac{t_1^{a_1}\cdots t_n^{a_n}}{a_1!\cdots a_n!}$ in the expansion of*

$$\exp\Big(\sum_{i\geq 1}\frac{i^{p-1}}{p}t_i^p + \sum_{\substack{j\geq 1\\ \gcd(j,p)=1}} t_j\Big)$$

is the number of p-th roots of an n-permutation of type $\mathbf{a} = (a_1, \dots, a_n)$.

5 A property of the probability $p_m(n)$

Let m be a power of a prime number p. In this section we include a proof of an interesting property about the probability, $p_m(n)$, that an n-permutation chosen at random has an mth root. In the work of Bóna et al. [4], there are a combinatorial proof of the identity $p_m(n) = p_m(n+1)$, with m a prime number, and for all n not congruent to -1 mod m. We prove the analogous result for the case when m is a power of prime number q, first by using the generating function of the number of permutations that admit an mth root (see [5] for a different proof). We use the terminology in [15]. For $q \geq 1$, let $\exp_q(x)$ denote the formal series defined by

$$\exp_q(x) = \sum_{i \geq 0} \frac{x^{iq}}{(iq)!}.$$

The following statement can be found as Theorem 4.8.3 in H. Wilf's generatingfunctionology (p. 149, [15])

Theorem 4. *Let $r(n,m)$ be the number of n-permutations that have an mth root. Then*

$$\sum_{n=0}^{\infty} r(n,m) \frac{x^n}{n!} = \prod_{\ell=1}^{\infty} \exp_{((\ell,m))}\left(\frac{x^\ell}{\ell}\right).$$

Remark 3. Note that if m is a prime power, $m = p^r$, then for any $l \in \mathbb{N}$

$$((l,m)) = \begin{cases} 1 & \text{if } \gcd(l,p) = 1 \\ m & \text{otherwise} \end{cases}$$

The next proposition gives one property of $p_m(n)$.

Proposition 9. *Let p be a prime. Let $p_m(n)$ be the probability that an n-permutation chosen uniformly at random has an mth root. If $m = p^r$, $r \in \mathbb{N}$, then for all $j \in \mathbb{N}_0$ we have*

$$p_m(jp) = p_m(jp+1) = \cdots = p_m(jp + (p-1))$$

Proof. By Remark 3 the generating function in Theorem 4 can be written as

$$\prod_{l\, \in\, \mathbb{N}} \exp_{((l,m))}\left(\frac{x^l}{l}\right) = \prod_{\substack{l\, \in\, \mathbb{N} \\ \gcd(l,m)=1}} \exp\left(\frac{x^l}{l}\right) \prod_{j=1}^{\infty} \exp_m\left(\frac{x^{jp}}{jp}\right)$$

which can be written in the form

$$\prod_{j=1}^{\infty} \exp\left(\frac{x^j}{j}\right) \prod_{j=1}^{\infty} \exp\left(-\frac{x^{jp}}{jp}\right) \prod_{j=1}^{\infty} \exp_m\left(\frac{x^{jp}}{jp}\right),$$

or

$$\frac{1}{(1-x)} \left(1-x^p\right)^{1/p} \prod_{j=1}^{\infty} \exp_m\left(\frac{x^{jp}}{jp}\right).$$

Notice that, due to the fact that $m = p^r$, we can write $\left(1-x^p\right)^{1/p} \prod_{j=1}^{\infty} \exp_m\left(\frac{x^{jp}}{jp}\right)$ as a function of the form $G(x) = \sum_{j=0}^{\infty} b_j x^{pj}$, for any adequate election of b_j. Now $\frac{1}{(1-x)} G(x)$, where $G(x) := \left(1-x^p\right)^{1/p} \prod_{j=1}^{\infty} \exp_m\left(x^{jp}/jp\right)$ is the power series of some function in the variable x^p. Note that $p_m(n)$ is the coefficient of x^n in the expansion of

$$\sum_{n=0}^{\infty} r(n,m) \frac{x^n}{n!} = \frac{1}{(1-x)} G(x) = \frac{1}{(1-x)} \sum_{k=0}^{\infty} b_k x^{kp}$$

Now, if we take $n = kp$, for any $k = 0, 1, \ldots$ we have that

$$\begin{aligned} p_m(kp) &= b_0 + b_1 + b_2 + \cdots + b_k \\ p_m(kp+1) &= b_0 + b_1 + b_2 + \cdots + b_k \\ &\vdots \\ p_m(kp+(p-1)) &= b_0 + b_1 + b_2 + \cdots + b_k. \end{aligned}$$

□

5.1 A second proof of Proposition 9

In this section, we give a second proof of Proposition 9. Here we deduce Proposition 9 from Corollary 2.12 in [4]. We start by recalling some notation and definitions used in [4]. Let $POWER_m(n)$ be the set of n-permutations that have at least one mth root. Let $DIV_{\rho,m}(n)$ denote the set of n-permutations whose cycles of length a multiple of m have type ρ and let $div_{\rho,m}(n) = |DIV_{\rho,m}(n)|/n!$. For $\pi \in DIV_{\rho,m}(n)$, we denote with $\pi_{(m)}$ (respectively $\pi_{(\sim m)}$) the part of π consisting of the cycles of lengths which are (respectively not are) multiples of m. By Theorem 3 and Remark 3, if $m = p^r$ is a power of a prime p, then the set $POWER_{p^r}(n)$ consist of all n-permutations whose number of cycles of length a multiple of p is divisible by p^r. Corollary 2.12 in [4] says that if p does not divide $n+1$ then $div_{\rho,p}(n) = div_{\rho,m}(n+1)$. So in order to prove Proposition 9 we only need to show that if $n+1$ is not a multiple of

p then the only possible cycle types for $\pi_{(p)}$ are the same for $POWER_m(n)$ as for $POWER_m(n+1)$. We will prove that this is the case. Let ρ be any cycle type of $\pi_{(p)}$ with $\pi \in POWER_m(n)$ then, clearly, ρ is a cycle type of $\pi'_{(p)}$ for some π' in $POWER_m(n+1)$. Let $\pi \in POWER_m(n+1)$. Since p does not divide $n+1$, then $\pi_{(\sim p)}$ cannot be empty. Then the n-permutation π' with $\pi'_{(p)} = \pi_{(p)}$ and with the part $\pi'_{(\sim p)}$ (possible empty) containing as fixed points all the elements (different that $n+1$) in $\pi_{(\sim p)}$, has p^rth root and hence ρ is also the cycle type of a permutation π' in $POWER_m(n)$.

Acknowledgements

The authors would like to thank E. Ugalde and L. Glebsky for many useful comments. Also the authors would like to thank the anonymous referees for their careful reading and valuable comments and suggestions. Section 5.1 was not present in the original version. Its addition was inspired by a referee's thoughtful question. Part of this work was made when R. Moreno was staying at Campus Jalpa, UAZ. The final version was written while Rivera-Martínez was a postdoctoral fellow at the University of Vienna, supported by the European Research Council (ERC) grant of Goulnara Arzhantseva, grant agreement no. 259527.

References

[1] S. Annin, T. Jansen and C. Smith, On kth roots in the symmetric and alternating groups, *Pi Mu Epsilon Journal* **12** No. 10 (2009), 581–589.

[2] J. Blum, Enumeration of the square permutations in $\mathfrak{S}_n$, *J. Combin. Theory Ser. A* **17**, (1974), 156–161.

[3] B. Bollobás and B. Pittel, The distribution of the root degree of a random permutation, *Combinatorica* **29** (2) (2009), 131–151.

[4] M. Bóna, A. McLennan and D. White, Permutations with roots, *Random Structures & algorithms* **17** (2000), No. 2, 157–167.

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

[6] M. Deza and T. Huang, Metrics on Permutations, a survey, *J. Combin. Inf. Sys. Sci.* **23** (1998), 173–185.

[7] L. Glebsky and L. M. Rivera, Almost solutions of equations in permutations, *Taiwanese J. Math.* **13** (2009), No. 2A, 493–500.

[8] A. Groch, D. Hofheinz, and R. Steinwandt, A practical attack on the root problem in braid groups, *Contemporary Math.* **418** (2006), 121–132.

[9] A. Maróti, Symmetric functions, generalized blocks, and permutations with restricted cycle structure, *European J. Combin.* **28** (2007), No. 3, 942–963.

[10] A. I. Pavlov, On the number of solutions of the equation $x^k = a$ in the symmetric group S_n, *Mat. Sb.* **112(154)** (1980), 380–395; English transl. *Math. USSR Sb.*, **40** (1981).

[11] M. R. Pournaki, On the number of even permutations with roots, *Australas. J. Combin.* **45** (2009), 37–42.

[12] N. Pouyanne, On the number of permutations admitting an mth root, *Electron. J. Combin.* **9** (2002), #R3., 1–12.

[13] V. Schoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2nd edition, (2008)

[14] P. Turán, On some connections between combinatorics and group theory, *Colloq. Math. Soc. János Bolyai*, P. Erdös, A. Rényi and V. T. Sós, eds., North Holland, Amsterdan (1970), 1055–1082.

[15] H. S. Wilf, *Generatingfunctionology*, Academic Press, San Diego, 2nd edition, (1994).

(Received 20 June 2010; revised 2 Sep 2011)