On the number of even roots of permutations

Lev Glebsky, Melany Licón, Luis Manuel Rivera

Abstract

Let σ be a permutation on n letters. We say that a permutation τ is an even (resp. odd) kth root of σ if $\tau^k = \sigma$ and τ is an even (resp. odd) permutation. In this article we obtain generating functions for the number of even and odd kth roots of permutations. Our result implies know generating functions of Moser and Wyman and also some generating functions for sequences in The On-line Encyclopedia of Integer Sequences (OEIS).

Keywords: Roots of permutations; even permutations; generating functions.
AMS Subject Classification Numbers: 05A05; 05A15.

1 Introduction

The study of problems related to the solutions of equation $x^k = a$, with k a fixed positive integer, in groups and another structures is a classical problem and has been studied for several year and by different authors (see, e.g., [4, 6, 11, 12, 13, 19, 20, 23]).

One of the most studied cases is when the group is the symmetric group S_n. For example, there are characterizations that said when a given permutation has a kth root in S_n (see, e.g., [1, 3, 7]). Also, there are several results about the probability that a random permutation of length n has a kth root (see, e.g., [2, 5, 13, 14, 15]). For the case of the alternating group, there are a characterization due to Annin, Jansen and Smith [1] about the even permutations that have kth roots in A_n, and it seems that the unique result about the probability that a random even permutation has a kth root in A_n is due to Pournaki [17] for the case $k = 2$.

Another type of problem is about the number of solutions in S_n of the equation $x^k = \sigma$. This problem was studied for several authors and with different points of view. For example Pavlov [16] gave an explicit formula for such a number. Some years later, Leaños, Moreno and the third author of this article gave another explicit formula and a multivariable exponential generating function [10], and Roichman [18] gave a formula expressed as an alternating sum of μ-unimodal kth roots of the identity permutation.

In this article we are interested in the number of even (resp. odd) permutations that are kth roots of a given permutation. To our knowledge, there are only few results in this direction and only for the case of the identity permutation. In OEIS [21] there are only few sequences for the number of even kth roots of the identity permutation: A000704 ($k = 2$), A061129 ($k = 4$), A061130 ($k = 6$), A061131 ($k = 8$) and A061132 ($k = 10$). For the case of the number of odd kth roots of the identity permutation we found sequences A001465 ($k = 2$), A061136 ($k = 4$) and A061137 ($k = 6$). The case $k = 2$ was studied by Moser and Wyman [13].

In order to formulate our main result we need some definitions. The *cycle type* of an n-permutation is a vector $\mathbf{c} = (c_1, \dots, c_n)$ that indicates that the permutation has c_i cycles of length i for every $i \in [n]$, with $c_i \geq 0$. Also, we say that a permutation σ is of *cycle type* $(\ell_1)^{a_1} \dots (\ell_m)^{a_m}$, with $a_i > 0$, if σ has exactly a_i cycles of length ℓ_i in its disjoint cycle factorization and does not have any cycles of another length. Let k, ℓ be positive integers and c a non-negative integer. Let

$$G_k(\ell) = \{g \ \in \mathbb{N} : \operatorname{mcd}(g\ell, k) = g\}.$$

The main result of this paper is the following

Theorem 1.1. *Let n, k be positive integers and let $c_1, \dots, c_n$ be non-negative integers. For $n = c_1 + 2c_2 + \dots + nc_n$, the coefficient of $\frac{t_1^{c_1} \dots t_n^{c_n}}{c_1! \dots c_n!}$ in the expansion of*

$$\frac{1}{2}\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right) + \frac{1}{2}\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)}(-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right)$$

is the number of even kth roots of a permutation of cycle type $\mathbf{c}$, and in the expansion of

$$\frac{1}{2}\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right) - \frac{1}{2}\exp\left(\sum_{\ell\geq 1}\sum_{g\in G_k(\ell)}(-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right).$$

is the number of odd kth roots of a permutation of cycle type $\mathbf{c}$.

This theorem implies the known results for the identity permutation. The outline of this paper is as follows. In Section 2 we present some notation and definitions. Also we present a sketch of the proof of our main result. In Section 3 we prove several propositions and lemas that are used in the proof of our main result. The proof itself is at the end of this section. In Section 4 we present several particular cases of Theorem 1.1 that allows some nice simplifications.

2 Preliminares

First some notation and definitions. We use $\mathbb{N}$ (respectively $\mathbb{N}_0$) to denote the set of positive (respectively, non-negative) integers. The elements of S_n are called *permutations* or *n-permutations* and are bijections $\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$. The *support* of an n-permutation σ is defined as $\mathrm{supp}(\sigma) = \{a \in \{1,\dots,n\} : \sigma(a) \neq a\}$. The set $G_k(\ell)$ was defined in [10]. Note that if $k = p_1^{a_1}\cdots p_j^{a_j}$, where $p_1,\dots,p_j$ are distinct primes and $a_i > 0$, for any $i \in \{1,\dots,j\}$, then

$$G_k(\ell) = \left\{p_1^{b_1}\cdots p_j^{b_j} : b_i = a_i \text{ if } p_i|\ell \text{ and } b_i \in \{0,1,\dots,a_i\} \text{ if } p_i \not|\ell\right\}$$

The following observation will be useful in Section 4.

Observation 2.1. *Let k be an even integer.*

1. *if ℓ is even, then $G_k(\ell)$ is a set of even integers,*
2. *if ℓ is odd, then $G_k(\ell)$ can have even and odd integers.*

The importance of the set $G_k(\ell)$ is given by the following proposition that was proved in [10].

Proposition 2.2. *A permutation of cycle type $(\ell)^c$ has a kth root if and only if equation*

$$g_1x_1 + \cdots + g_hx_h = c$$

has non-negative integer solutions, where $G_k(\ell) = \{g_1,\dots,g_h\}$, with $g_1 < \cdots < g_h$.

For the number of kth roots, the following result was obtained by Leaños, Moreno and the third author of this paper.

Theorem 2.3. *Let k,n be positive integers and let $c_1,\dots,c_n$ be non-negative integers. For $n = c_1 + 2c_2 + \cdots + nc_n$, the coefficient of $\frac{t_1^{c_1}\cdots t_n^{c_n}}{c_1!\cdots c_n!}$ in the expansion of*

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

is the number of kth roots of an n-permutation of cycle type $\mathbf{c} = (c_1,\dots,c_n)$.

In the proof of previous theorem the authors used the following well-known result: if a permutation σ has a kth root, then all the roots of σ can by obtained by working with the cycles of different lengths of σ separately (see, e.g., [8] and [10]). However, for the case of even kth roots, the above does not work directly because the product of two permutations of equal parity is an even permutation. We have solve this difficult by working with the difference between the number of even kth roots and the number of odd kth roots of a permutation (Lemma 3.3). The next step was to obtain a multivariable exponential generating function for such a difference (Lemma 3.8). In order to make this, we assign a sign to the number of kth roots, of certain type, of permutations with all its cycles of the same length (Proposition 3.5), and using this we obtain an exponential generating function for the difference between the number of even kth roots and odd kth roots of permutations with all its cycles of the same length (Lemma 3.7). Finally, the proof of Theorem 1.1 is obtained as a consequence of Theorem 2.3 and Lema 3.8.

For the proof of Lemma 3.7 we will use the following result, that is Proposition 5.1.3 in Stanley's book [22]

Theorem 2.4. *Let K be a field of characteristic zero. Fix $m \in \mathbb{N}$ and functions $f_i\colon \mathbb{N} \to K$, $1 \leq i \leq m$. Define a new function $h\colon \mathbb{N}_0 \to K$ by*

$$h(|A|) = \sum f_1(|A_1|) f_2(|A_2|) \cdots f_m(|A_m|),$$

where the sum ranges over all weak partitions $(A_1, \ldots, A_m)$ of A into m blocks, i.e., $A_1, \ldots A_m$ are subsets of A satisfying: (i) $A_i \cap A_j = \emptyset$ if $i \neq j$, and (ii) $A_1 \cup \cdots \cup A_m = A$. Let $F_i(x)$ and $H(x)$ be the exponential generating functions for the series $f_i(n)$ and $h(n)$, respectively. Then

$$H(x) = F_1(x) \ldots F_m(x).$$

3 Proof of the main result

We need the following almost obvious proposition

Proposition 3.1. *Let G be a group and K be a field. Let $\phi\colon G \to (K, \cdot)$ ($g \mapsto \phi^g$) be a homomorphism to the multiplicative group of K and $X, Y \subseteq G$ be finite. Then*

$$\left(\sum_{g \in X} \phi^g \right) \left(\sum_{h \in Y} \phi^h \right) = \sum_{\substack{g \in X \\ h \in Y}} \phi^{gh}.$$

Let $rp_k(\sigma)$ (resp. $ri_k(\sigma)$) denote the number of even (resp. odd) kth roots of permutation σ.

Corollary 3.2. *Let σ be a permutation such that $\sigma = \sigma_1\sigma_2$ and $supp(\sigma_1) \cap supp(\sigma_2) = \emptyset$. Let $rp'_k(\sigma)$ (resp. $ri'_k(\sigma)$) be the number of even (resp. odd) kth roots τ of σ such that $\tau = \tau_1\tau_2$ with $\tau_1^k = \sigma_1$ and $\tau_2^k = \sigma_2$. Then*

$$rp'_k(\sigma) - ri'_k(\sigma) = \left(rp_k(\sigma_1) - ri_k(\sigma_1) \right) \left(rp_k(\sigma_2) - ri_k(\sigma_2) \right).$$

Proof. Consider the parity of permutations as a homomorphism ϕ to $\{-1, 1\}$ and define the sets $X = \{\tau_1 \in S_n \colon \tau_1^k = \sigma_1\}$ and $Y = \{\tau_2 \in S_n \colon \tau_2^k = \sigma_2\}$. Then

$$\sum_{\tau_1 \in X} \phi^{\tau_1} = rp_k(\sigma_1) - ri_k(\sigma_1),$$

$$\sum_{\tau_2 \in Y} \phi^{\tau_2} = rp_k(\sigma_2) - ri_k(\sigma_2)$$

and

$$\sum_{\substack{\tau_1 \in X \\ \tau_2 \in Y}} \phi^{\tau_1 \tau_2} = rp'_k(\sigma) - ri'_k(\sigma).$$

□

The following result shows that for a given permutation σ we can obtain the difference $rp_k(\sigma) - ri_k(\sigma)$ by working with the different lengths in the cycles of σ separately.

Lemma 3.3. *Let σ be a permutation that has kth roots. Suppose that the disjoint cycle factorization of $\sigma \in S_n$ can be expressed as the product $\sigma_1 \sigma_2 \cdots \sigma_m$ where σ_i is the product of all the disjoint ℓ_i-cycles of σ, for every i. Then*

$$rp_k(\sigma) - ri_k(\sigma) = \prod_{i=1}^{m} \left(rp_k(\sigma_i) - ri_k(\sigma_i) \right).$$

Proof. It is well-know that every kth root of σ can be written as $\tau_1 \cdots \tau_m$ with $\tau_i^k = \sigma_i$, for every i (see, e.g., [10, §3]). The proof is by induction on m. The case $m = 1$ is obvious. If $m = 2$, then all the kth roots of σ are of the form $\tau_1\tau_2$, with $\tau_1^k = \sigma_1$ and $\tau_2^k = \sigma_2$, and hence $rp_k(\sigma) = rp'_k(\sigma)$, $ri_k(\sigma) = ri'_k(\sigma)$ and the result follows from Corollary 3.2. Now if $\sigma = \sigma_1 \ldots \sigma_{m-1}\sigma_m$, $m > 2$, then every kth root τ of σ is of the form $\alpha\tau_m$ with $\alpha^k = \sigma_1 \ldots \sigma_{m-1}$ and $\tau_m^k = \sigma_m$. Therefore $rp_k(\sigma) = rp'_k(\sigma)$, $ri_k(\sigma) = ri'_k(\sigma)$. By Corollay 3.2 and by the induction hypothesis we have that

$$\begin{aligned} rp_k(\sigma) - ri_k(\sigma) &= (rp_k(\alpha) - ri_k(\alpha))(rp_k(\tau_m) - ri_k(\tau_m)) \\ &= \prod_{i=1}^{m-1} \left(rp_k(\sigma_i) - ri_k(\sigma_i) \right) \left(rp_k(\tau_m) - ri_k(\tau_m) \right) \\ &= \prod_{i=1}^{m} \left(rp_k(\sigma_i) - ri_k(\sigma_i) \right) \end{aligned}$$

□

Let g, k, ℓ be fixed positive integers and p be a fixed non-negative integer. We use $f_{k,\ell,g,p}(c)$ to denote the number of permutations of cycle type $(g\ell)^p$ that are kth roots of a permutation of cycle type $(\ell)^c, c \in \mathbb{N}_0$. The following proposition was essentially proved in [10].

Proposition 3.4. *Let g, k, ℓ be fixed positive integers and p be a fixed non-negative integer. Let $c \in \mathbb{N}_0$. If $g \in G_k(\ell)$ and $c = gp$, then*

$$f_{k,\ell,g,p}(c) = \frac{(gp)!\ell^{p(g-1)}}{g^p p!},$$

and $f_{k,\ell,g,p}(c) = 0$ *in any other case.*

In view of previous proposition, for $g \in G_k(\ell)$ we define

$$f_{k,\ell,g}(c) = \begin{cases} f_{k,\ell,g,p}(c) & c = gp \\ 0 & \text{other case} \end{cases}$$

Now we assign a sign to the number $f_{k,\ell,g}(c)$ that is useful to known if the roots of cycle type $(g\ell)^p$ of a permutation of cycle type $(\ell)^c$ are even.

Proposition 3.5. *Let* k, ℓ *be fixed positive integers. Let* $g \in G_k(\ell), c \in \mathbb{N}_0$ *and*

$$a(c) = (-1)^{c/g(\ell g+1)} f_{k,\ell,g}(c).$$

If σ *is a permutation of cycle type* $(\ell)^c$ *and* $c = gp$*, then* $a(c) \neq 0$ *and the* k*th roots of* σ *of cycle type* $(g\ell)^p$ *are even permutations if and only if* $a(c) > 0$*.*

Proof. As $c = gp$, we have that $a(c) = (-1)^{p(\ell g+1)} f_{k,\ell,g,p}(c)$ and Proposition 3.4 implies that $a(c) \neq 0$. We have the following cases.

1. p even. In this case the kth roots of σ of cycle type $(\ell g)^p$ are even and by direct calculations we obtain that $a(c) > 0$.

2. p odd.

   2.1. ℓg even. In this case the kth roots of σ of cycle type $(\ell g)^p$ are odd. By direct calculations we obtain $a(c) < 0$.

   2.2. ℓg odd. In this case the kth roots of σ of cycle type $(\ell g)^p$ are even and by direct calculations we obtain that $a(c) > 0$.

□

The exponential generating function, in the variable t_ℓ, for the number $a(c)$ in previous proposition is given in the following result.

Proposition 3.6. *Let* $\ell, k \in \mathbb{N}$*. Let* $g \in G_k(\ell)$ *fixed. Then*

$$\sum_{c \geq 0} (-1)^{c/g(\ell g+1)} f_{k,\ell,g}(c) \frac{t_\ell^c}{c!} = \exp\left((-1)^{\ell g+1} \frac{\ell^{(g-1)}}{g} t_\ell^g \right).$$

Proof. From Proposition 3.4 we have that $f_{k,\ell,g}(c) \neq 0$ if and only if $c = gp$, for some $p \in \mathbb{N}_0$. Therefore

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

□

Let $rp_k(\ell, c)$ (resp. $ri_k(\ell, c)$) denote the number of even (resp. odd) kth-roots of any permutation of cycle type $(\ell)^c$.

Lemma 3.7. *Let $\ell \in \mathbb{N}$. Then*

$$\sum_{c\geq 0}(rp_k(\ell,c) - ri_k(\ell,c))\frac{t_\ell^c}{c!} = \exp\left(\sum_{g\in G_k(\ell)}(-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right).$$

Proof. Let σ be any permutation of cycle type $(\ell)^c$ and S the set of all disjoint cycles in σ. Let $G_k(\ell) = \{g_1, \ldots, g_m\}$, with $g_1 < \cdots < g_m$. By Corollary 2.2 we have that σ has kth roots if and only if the equation

$$g_1x_1 + \cdots + g_mx_m = c$$

has non-negative integer solutions, where a solution $(p_1, \ldots, p_m)$ of previos equation means that σ has kth roots of cycle type $(g_1\ell)^{p_1} \ldots (g_m\ell)^{p_m}$. We can obtain all these roots by running over all the weak ordered partitions $(A_1, \ldots, A_m)$ of S. Indeed, if $(A_1, \ldots, A_m)$ is such a partition, the number of kth of roots associated to this partition is given by $f_{k,\ell,g_1}(|A_1|)\cdots f_{k,\ell,g_m}(|A_m|)$, where this product is different to cero if $|A_i|$ is a multiple of g_i, for every i. Let $\mathcal{A}$ be the set of all weak ordered partitions of S into m blocks. The number of all kth roots of σ is equal to

$$\sum_{(A_1,\ldots,A_m)\in\mathcal{A}} f_{k,\ell,g_1}(|A_1|)\cdots f_{k,\ell,g_m}(|A_m|).$$

Now, for a given partition $(A_1, \dots, A_m)$ with

$$f_{k,\ell,g_1}(|A_1|) \cdots f_{k,\ell,g_m}(|A_m|) \neq 0,$$

the sign of

$$(-1)^{|A_1|/g_1(\ell g_1+1)} f_{k,\ell,g_1}(|A_1|) \cdots (-1)^{|A_m|/g_m(\ell g_m+1)} f_{k,\ell,g_m}(|A_m|),$$

determine the parity of the kth roots of σ of cycle type $(g_1\ell)^{p_1} \dots (g_m\ell)^{p_m}$, where $p_i = |A_i|/g_i$. Therefore, the number $rp_k(\ell, c) - ri_k(\ell, c)$ is equal to

$$\sum_{(A_1,\dots,A_m)\in\mathcal{A}} (-1)^{|A_1|/g_1(\ell g_1+1)} f_{k,\ell,g_1}(|A_1|) \cdots (-1)^{|A_m|/g_m(\ell g_m+1)} f_{k,\ell,g_m}(|A_m|),$$

and the desired exponential generating function is obtained by Theorem 2.4 and Proposition 3.6. □

Let $rp_k(\mathbf{c})$ (resp. $rp_k(\mathbf{c})$) denote the number of even (resp. odd) kth roots of a permutation of cycle type $\mathbf{c}$. The following multivariable exponential generating function, in the variables $t_1, t_2, \dots$, for the difference between the number of even kth roots and the number of odd kth roots of permutations of any cycle type follows from Lemmas 3.3 and 3.7.

Lemma 3.8. *Let n, k be a positive integers and let $c_1, \dots, c_n$ be non-negative integers. For $n = c_1 + 2c_2 + \cdots + nc_n$, the coefficient of $\frac{t_1^{c_1}\dots t_n^{c_n}}{c_1!\dots c_n!}$ in the expansion of*

$$\exp\left(\sum_{\ell\geq 1} \sum_{g\in G_k(\ell)} (-1)^{\ell g+1} \frac{\ell^{g-1}}{g} t_\ell^g\right)$$

is equal to the number $rp_k(\mathbf{c}) - ri_k(\mathbf{c})$.

Proof of Theorem 1.1.

Let $r_k(\sigma)$ denote the number of kth roots of a permutation σ. For any permutation σ, we have that

$$\begin{aligned} 2rp_k(\sigma) &= rp_k(\sigma) + ri_k(\sigma) + rp_k(\sigma) - ri_k(\sigma) \\ &= r_k(\sigma) + (rp_k(\sigma) - ri_k(\sigma)). \end{aligned}$$

Similarly

$$2ri_k(\sigma) = r_k(\sigma) - (rp_k(\sigma) - ri_k(\sigma)).$$

Therefore, Theorem 1.1 follows immediately from Theorem 2.3 and Lemma 3.8.

4 Particular cases

If k is odd, then any solution of equation $x^k = \sigma$ should have the same parity that σ, and hence the generating function is the same that the given in Theorem 2.3. Therefore in this section k is a fixed even integer.

Permutations of cycle type $(\ell)^c$

For a fixed positive integers ℓ, the exponential generating function for the number of even kth roots of permutations of cycle type $(\ell)^c$, $c \in \mathbb{N}$, becomes

$$\sum_{c\geq 0} rp_k(\ell,c)\frac{t_\ell^c}{c!} = \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g}t_\ell^g\right) + \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)} (-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right) \tag{1}$$

and

$$\sum_{c\geq 0} ri_k(\ell,c)\frac{t_\ell^c}{c!} = \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g}t_\ell^g\right) - \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)} (-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right). \tag{2}$$

With this expressions, we can obtain the exponential generating functions that appear in the following sequences in OEIS: A000704, A061129, A061130, A061131, A061132, A001465, A061136 and A061137.

For example, sequence A061131 in OEIS correspond to the number of even 8th roots of the identity permutation. In this case $\ell = 1$ and $G_8(1) = \{1,2,4,8\}$. Therefore

$$\begin{aligned}\sum_{c\geq 0} rp_8(1,c)\frac{x^c}{c!} &= \frac{1}{2}\exp\left(x+\frac{1}{2}x^2+\frac{1}{4}x^4+\frac{1}{8}x^8\right) + \frac{1}{2}\exp\left(x-\frac{1}{2}x^2-\frac{1}{4}x^4-\frac{1}{8}x^8\right)\\ &= \exp(x)\cosh\left(\frac{1}{2}x^2+\frac{1}{4}x^4+\frac{1}{8}x^8\right).\end{aligned}$$

For another example, sequence A061132 is the number of even 10th root of the identity permutation. In this case, $G_{10}(1) = \{1,2,5,10\}$ and hence

$$\begin{aligned}\sum_{c\geq 0} rp_{10}(1,c)\frac{x^c}{c!} &= \frac{1}{2}\exp\left(x+\frac{1}{2}x^2+\frac{1}{5}x^5+\frac{1}{10}x^{10}\right) + \frac{1}{2}\exp\left(x-\frac{1}{2}x^2+\frac{1}{5}x^5-\frac{1}{10}x^{10}\right)\\ &= \exp\left(x+\frac{1}{5}x^5\right)\cosh\left(\frac{1}{2}x^2+\frac{1}{10}x^{10}\right).\end{aligned}$$

This examples shows that we can make further simplifications to equations (1) and (2).

First we consider the case when ℓ is even. By Observation 2.1 we have that

$$\sum_{c\geq 0} rp_k(\ell,c)\frac{t_\ell^c}{c!} \;=\; \cosh\left(\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right)$$

and

$$\sum_{c\geq 0} ri_k(\ell,c)\frac{t_\ell^c}{c!} \;=\; \sinh\left(\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right).$$

For ℓ odd, let $G_k(\ell)' = \{g \in G_k(\ell)\colon g \text{ is odd }\}$ and $G_k(\ell)'' = G_k(\ell) - G_k(\ell)'$. Then

$$\begin{aligned}
\sum_{c\geq 0} rp_k(\ell,c)\frac{t_\ell^c}{c!} &= \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right)+\frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)}(-1)^{\ell g+1}\frac{\ell^{g-1}}{g}t_\ell^g\right),\\
&= \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right)+\frac{1}{2}\exp\left(\sum_{g\in G'_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g-\sum_{g\in G''_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right),\\
&= \exp\left(\sum_{g\in G'_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right)\cosh\left(\sum_{g\in G''_k(1)}\frac{\ell^{g-1}}{g}t_\ell^g\right).
\end{aligned}$$

Similarly, for the case of odd kth roots we obtain

$$\sum_{c\geq 0} ri_k(\ell,c)\frac{x^c}{c!} \;=\; \exp\left(\sum_{g\in G'_k(\ell)}\frac{\ell^{g-1}}{g}t_\ell^g\right)\sinh\left(\sum_{g\in G''_k(1)}\frac{\ell^{g-1}}{g}t_\ell^g\right).$$

For the case $k=2$ and permutations of cycle type $(\ell)^c$ we have the following

Corollary 4.1. *Let ℓ be a fixed positive integer. Then*

$$\sum_{c\geq 0} rp_2(\ell,c)\frac{t_\ell^c}{c!} = \exp\left((\ell \bmod 2)t_\ell\right)\cosh\left(\frac{\ell}{2}t_\ell^2\right)$$

and

$$\sum_{c\geq 0} ri_2(\ell,c)\frac{t_\ell^c}{c!} = \exp\left((\ell \bmod 2)t_\ell\right)\sinh\left(\frac{\ell}{2}t_\ell^2\right).$$

The case of the identity permutation

Now, we can do more simplifications for the case of the identity permutation ($\ell = 1$). Let $k = 2^{a_1} \cdots p_j^{a_j}$, where $2, p_2, \ldots, p_j$ are distinct primes and $a_i > 0$, for any $i \in \{1, \ldots, j\}$. Then

$$G_k(1) = \{m \colon m | k\}$$

and hence

$$\sum_{c \geq 0} rp_k(1, c) \frac{x^c}{c!} = \frac{1}{2} \exp\left(\sum_{d|k} \frac{x^d}{d}\right) + \frac{1}{2} \exp\left(\sum_{d|k} (-1)^{d-1} \frac{x^d}{d}\right).$$

For the case $k = 2^m$, we have

$$\sum_{c \geq 0} rp_{2^m}(1, c) \frac{x^c}{c!} = \frac{1}{2} \exp\left(\sum_{i=0}^{m} \frac{1}{2^i} x^{2^i}\right) + \frac{1}{2} \exp\left(x - \sum_{i=1}^{m} \frac{1}{2^i} x^{2^i}\right).$$

This generating function was used in the work of Koda, Sato and Tskegahara [9]. For the case of odd roots

$$\sum_{c \geq 0} ri_{2^m}(1, c) \frac{x^c}{c!} = \exp(x) \sinh\left(\frac{1}{2} x^2 + \cdots + \frac{1}{2^m} x^{2^m}\right)$$

Square roots of any permutation

For the case of even square roots we have the following

Corollary 4.2. *The coefficient of $t_1^{c_1} \ldots t_n^{c_n} / (c_1! \ldots c_n!)$ in the expansion of*

$$\prod_{j \geq 1} \exp\left(t_{2j-1}\right) \cosh\left(\sum_{j \geq 1} \left(\frac{2j-1}{2} t_{2j-1}^2 + j t_{2j}^2\right)\right)$$

is the number of even square roots of any permutation of cycle type $\mathbf{c} = (c_1, \ldots, c_n)$.

Proof. We rewrite Theorem 1.1 for the case of even square roots. When $k = 2$, $G_2(\ell) \subseteq \{1, 2\}$. Now we work with the parity of ℓ. If $\ell = 2j - 1$, for some integer $j \geq 1$, then $G_2(2j - 1) = \{1, 2\}$ and hence

$$\sum_{g \in G_k(\ell)} (-1)^{\ell g + 1} \frac{\ell^{g-1}}{g} t_\ell^g = t_{2j-1} - \frac{2j-1}{2} t_{2j-1}^2$$

and

$$\sum_{g \in G_k(\ell)} \frac{\ell^{g-1}}{g} t_\ell^g = t_{2j-1} + \frac{2j-1}{2} t_{2j-1}^2.$$

If $\ell = 2j$, for some integer$j \geq 1$, then $G_2(2j) = \{2\}$ and hence

$$\sum_{g \in G_k(\ell)} (-1)^{\ell g+1} \frac{\ell^{g-1}}{g} t_\ell^g = -jt_{2j}^2$$

and

$$\sum_{g \in G_k(\ell)} \frac{\ell^{g-1}}{g} t_\ell^g = jt_{2j}^2.$$

Therefore, the exponential generating for the number of even square roots of permutations becomes

$$\frac{1}{2}\left(\exp\left(\sum_{j\geq 1}\left(t_{2j-1} + \frac{2j-1}{2}t_{2j-1}^2 + jt_{2j}^2\right)\right) + \exp\left(\sum_{j\geq 1}\left(t_{2j-1} - \frac{2j-1}{2}t_{2j-1}^2 - jt_{2j}^2\right)\right)\right),$$

from which we obtain

$$\frac{1}{2}\prod_{j\geq 1}\exp\left(t_{2j-1}\right)\left(\prod_{j\geq 1}\exp\left(\frac{2j-1}{2}t_{2j-1}^2 + jt_{2j}^2\right) + \prod_{j\geq 1}\exp\left(-\frac{2j-1}{2}t_{2j-1}^2 - jt_{2j}^2\right)\right),$$

that is equal to

$$\prod_{j\geq 1}\exp\left(t_{2j-1}\right)\cosh\left(\sum_{j\geq 1}\left(\frac{2j-1}{2}t_{2j-1}^2 + jt_{2j}^2\right)\right)$$

□

In a similar way we obtain the following

Corollary 4.3. *The coefficient of $t_1^{c_1} \dots t_n^{c_n}/(c_1! \dots c_n!)$ in the expansion of*

$$\prod_{j\geq 1}\exp\left(t_{2j-1}\right)\sinh\left(\sum_{j\geq 1}\left(\frac{2j-1}{2}t_{2j-1}^2 + jt_{2j}^2\right)\right)$$

is the number of odd square roots of any permutation of cycle type $c = (c_1, \dots, c_n)$.

We finish this paper by showing the case of even and odd square roots of involutions.

Corollary 4.4. *Let $rp_2(c_1, c_2)$ (resp. $rp_2(c_1, c_2)$) denote the number of even (resp. odd) square roots of an involution with exactly c_1 cycles of length 1 and exactly c_2 cycles of length 2. Then*

$$\sum_{c_1,c_2\geq 0} rp_2(c_1, c_2)\frac{t_1^{c_1}t_2^{c_2}}{c_1!c_2!} = \exp\left(t_1\right)\cosh\left(\frac{t_1^2 + 2t_2^2}{2}\right)$$

and

$$\sum_{c_1,c_2\geq 0} ri_2(c_1,c_2)\frac{t_1^{c_1}t_2^{c_2}}{c_1!c_2!} = \exp{(t_1)}\sinh\left(\frac{t_1^2+2t_2^2}{2}\right).$$

Acknowledgments

L.M.R. was partially supported by PROFOCIE grant 2018-2019 through UAZ-CA-169.

References

[1] S. Annin, T. Jansen and C. Smith, On kth roots in the symmetric and alternating groups, *Pi Mu Epsilon Journal*, **12** (10) (2009), 581–589.

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

[3] I. Z. Bouwer, W. W. Chernoff, Solutions to $x^r = \alpha$ in the symmetric group, *Ars. Combin.* **20** (1985) 83–88.

[4] W.W. Chernoff, Solutions to $x^r = \alpha$ in the alternating group, *Ars Combin.* **29**(C), (1990), 226–227 (Twelfth British Combinatorial Conference, Norwich, 1989).

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

[6] N. Chigira, The solutions of $x^d = 1$ in finite groups, *J. Algebra* **180** (1996), 653–661.

[7] I. S. Chowla, I. N. Herstein, W. R. Scott, The solution of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh., Trondheim* **25**, No. 2, (1952), 29-31,

[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] T. Koda, M. Sato, Y. Tskegahara, 2-adic properties for the numbers of involutions in the alternating groups, *J. Algebra Appl.* **14**(4) (2015), 1550052.

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

[11] M. S. Lucido and M. R. Pournaki, Elements with square roots in finite groups *Algebra Colloq.* **12** (4) (2005), 677–690.

[12] M. S. Lucido and M. R. Pournaki, Probability that an element of a finite group has a square root, *Colloq. Math.* **112** (2008), 147–155.

[13] L. Moser and M. Wyman, On the solutions of $x^d = 1$ in symmetric groups. *Canad. J. Math.* **7**(2) (1955), 159–168.

[14] A. C. Niemeyer and C.E. Praeger, On permutations of order dividing a given integer *J. Algebr. Comb.* **26** (2007), 125–142.

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

[16] 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).

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

[18] Y. Roichman, A note on the number of k-roots in S_n, *Sem. Lothar. Combin.* **70** (2014), Article B70i, 5pp.

[19] A. Sadeghieh, K. Ahmadidelir, n-th Roots in finite polyhedral and centro-polyhedral groups, *Proc Math Sci.* **125**(4) (2015), 125–487.

[20] A. Sadeghieh, H. Dostie, The nth roots of elements in finite groups, *Mathematical Sciences,* **2** (2008), 347–356.

[21] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://oeis.org.

[22] R. P. Stanley, Enumerative Combinatorics Vol 2, 1999.

[23] C. W. York, Enumerating kth roots in the Symmetric Inverse Monoid, *J. Combin. Math. Combin. Comput.* **108** (2019), 147–159.

L. G., UNIVERSIDAD AUTÓNOMA DE SAN LUIS POTOSÍ, MEXICO.
E-mail: glebsky@cactus.iico.uaslp.mx.

M. L. and L.M.R., UNIVERSIDAD AUTÓNOMA DE ZACATECAS, MEXICO.
E-mail: mliiqon@gmail.com and luismanuel.rivera@gmail.com.