AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **86(2)** (2023), Pages 308–319

On the number of even roots of permutations

Lev Glebsky

Universidad Autónoma de San Luis Potosí
Mexico
glebsky@cactus.iico.uaslp.mx

Melany Licón Luis Manuel Rivera

Universidad Autónoma de Zacatecas
Mexico
mliiqon@gmail.com luismanuel.rivera@gmail.com

Abstract

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

1 Introduction

A classical problem in group theory and combinatorics is the study of problems related to the solution of the equation $x^k = \sigma$ over groups, where k is a fixed positive integer (see, e.g., [6, 8, 14, 15, 16, 21, 24, 25, 30]). One of the most studied situations is the case of the symmetric group S_n. For example, there is a characterization that determines when a given permutation has a kth root in S_n (see, e.g., [1, 3, 7]) and there are several results about the probability that a randomly selected permutation of degree n has a kth root (see, e.g., [2, 5, 16, 17, 22]). In addition, Pavlov [19] gives an explicit formula for the number of solutions in S_n of the equation $x^k = \sigma$, and Leaños et al., [13] give a multivariable exponential generating function. Finally, Roichman [23] gives a formula for such a number expressed as an alternating sum of μ-unimodal kth roots of the identity permutation. For more similar problems, we refer the reader to [9, 10, 12, 20, 27, 28, 29].

ISSN: 2202-3518

In this article, we are interested in the number of even permutations which are kth roots of a given permutation. To our knowledge[1], there are only a few results in this direction and only for the case of the identity permutation. Moser and Wyman [16] study the case of $k = 2$. In OEIS [18] there are only a 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 odd kth roots of the identity permutation, in OEIS we find sequences A001465 ($k = 2$), A061136 ($k = 4$) and A061137 ($k = 6$).

1.1 Basic definitions and main result

In order to formulate our main result, we need some definitions and notation. Let $[n]$ denote the set $\{1, \ldots, n\}$. The *cycle type* of an n-permutation σ is a vector $\mathbf{c} = (c_1, \ldots, c_n)$ such that for every $i \in [n]$, σ has c_i cycles of length i. Sometimes, in order to avoid the cases when $c_i = 0$, we use the following definition: a permutation σ is of *type* $(\ell_1)^{a_1} \ldots (\ell_m)^{a_m}$, 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 any other length. We use $\mathbb{N}$ (respectively $\mathbb{N}_0$) to denote the set of positive (respectively, non-negative) integers. Let $k, \ell \in \mathbb{N}$. Let

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

It is easy to see that if $k = p_1^{a_1} \cdots p_j^{a_j}$, where $p_1, \ldots, p_j$ are distinct primes and $a_i > 0$ for $i \in [j]$, then

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

The main result of this paper is the following.

Theorem 1.1. *Let k, n be positive integers. Let $c_1, \ldots, c_n$ be non-negative integers such that $n = c_1 + 2c_2 + \cdots + nc_n$. Then the coefficient of $\frac{t_1^{c_1} \cdots t_n^{c_n}}{c_1! \cdots c_n!}$ 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 $\mathbf{c} = (c_1, \ldots, c_n)$, 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 $\mathbf{c}$.

[1]After finishing this work, we were aware of the existence of a polynomial generating function which enumerates the even permutations which are kth roots of a given permutation, given in terms of the cycle index of the symmetric group S_n, due to Chernoff [4].

The known result for the identity permutation (see e.g. [11, 16]) is a consequence of this theorem. Another interesting problem, which is out of the scope of this work, is about the asymptotic behavior of the proportion of permutations in A_n that have a k root. Also, it would be interesting to obtain a result similar to Theorem 2 in [19].

The outline of this paper is as follows. In Section 2, we will prove several propositions and lemmas that we use in the proof of our main result. The proof of Theorem 1.1 is at the end of this section. In Section 3, we show a few special cases of Theorem 1.1, which allow some nice simplifications.

2 Auxiliary results and proof of Theorem 1.1

First, we present two known results, which will be used in the proof or our main result.

Proposition 2.1 ([13, Proposition 5]). *A permutation of type $(\ell)^c$ has a kth root if and only if the equation*

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

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

The following result gives a generating function for the number of kth roots of a permutation.

Theorem 2.2 ([13, Theorem 2]). *Let k, n be positive integers. Let $c_1, \ldots, c_n$ be non-negative integers such that $n = c_1 + 2c_2 + \cdots + nc_n$. Then 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 a permutation of cycle type $\mathbf{c} = (c_1, \ldots, c_n)$.

The outline of the proof is as follows. First, we work with the difference between the number of even kth roots and the number of odd kth roots of a permutation (Lemma 2.5). The next step is to obtain a multivariable exponential generating function for such a difference (Lemma 2.11). In order to achieve this, first we assign a sign to the number of kth roots, of certain type of permutations all of whose cycles have the same length (Proposition 2.7). Using this, we obtain an exponential generating function for the difference between the number of even kth roots and odd kth roots of permutations all of whose cycles have the same length (Lemma 2.10). Finally, the proof of Theorem 1.1 is obtained as a consequence of Theorem 2.2 and Lemma 2.11.

We need the following easy proposition about groups in general.

Proposition 2.3. *Let G be a group and K be a field. Let $\phi\colon G \to (K,\cdot)$ ($g \mapsto g^{\phi}$) be a homomorphism to the multiplicative group of K and $X, Y \subseteq G$ be finite. Then*

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

Let $\mathrm{re}_k(\sigma)$ (respectively $\mathrm{ro}_k(\sigma)$) denote the number of even (respectively odd) kth roots of permutation σ. The *support* of an n-permutation σ is defined as $\mathrm{supp}(\sigma) = \{a \in [n] : \sigma(a) \neq a\}$.

Proposition 2.4. *Let σ be a permutation such that $\sigma = \sigma_1\sigma_2$ and $\mathrm{supp}(\sigma_1) \cap \mathrm{supp}(\sigma_2) = \emptyset$. Let $\mathrm{re}'_k(\sigma)$ (respectively $\mathrm{ro}'_k(\sigma)$) be the number of even (respectively 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*

$$\mathrm{re}'_k(\sigma) - \mathrm{ro}'_k(\sigma) = (\mathrm{re}_k(\sigma_1) - \mathrm{ro}_k(\sigma_1))\,(\mathrm{re}_k(\sigma_2) - \mathrm{ro}_k(\sigma_2)).$$

Proof. Consider the parity of permutations as a homomorphism $\mathrm{sgn}\colon S_n \to \{-1, 1\}$. Let $X = \{\tau_1 \in S_n \colon \tau_1^k = \sigma_1\}$ and $Y = \{\tau_2 \in S_n \colon \tau_2^k = \sigma_2\}$. Then $\sum_{\tau_1\in X} \tau_1^{\mathrm{sgn}} = \mathrm{re}_k(\sigma_1) - \mathrm{ro}_k(\sigma_1)$ and $\sum_{\tau_2\in Y} \tau_2^{\mathrm{sgn}} = \mathrm{re}_k(\sigma_2) - \mathrm{ro}_k(\sigma_2)$. Therefore, by Proposition 2.3 we have that

$$\sum_{\substack{\tau_1\in X\\ \tau_2\in Y}} (\tau_1\tau_2)^{\mathrm{sgn}} = \mathrm{re}'_k(\sigma) - \mathrm{ro}'_k(\sigma). \qquad \square$$

The following result shows that for a given permutation σ we can obtain the difference $\mathrm{re}_k(\sigma) - \mathrm{ro}_k(\sigma)$ by working with the different lengths in the cycles of σ separately.

Lemma 2.5. *Let σ be an n-permutation that has kth roots. Suppose that the disjoint cycle factorization of σ can be expressed as the product $\sigma_1\sigma_2\cdots\sigma_m$ where σ_i is the product of all the disjoint cycles of length ℓ_i in σ, for every i, with $\ell_i \neq \ell_j$, for $i \neq j$. Then*

$$\mathrm{re}_k(\sigma) - \mathrm{ro}_k(\sigma) = \prod_{i=1}^{m} (\mathrm{re}_k(\sigma_i) - \mathrm{ro}_k(\sigma_i)).$$

Proof. It is well-known 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., [13, §3]). The result follows by Proposition 2.4 and induction. $\square$

Sometimes, we use the following fact: if α is an ℓ-cycle, then α^m is a product of exactly $\gcd(m,\ell)$ disjoint $\ell/\gcd(m,\ell)$-cycles. Let g, k, ℓ be fixed positive integers and s be a fixed non-negative integer. We let $f_{k,\ell,g,s}(c)$ denote the number of permutations of type $(g\ell)^s$ that are kth roots of a permutation of type $(\ell)^c$, $c \in \mathbb{N}_0$. The following proposition has been proven, in essence, by Moreno et al. [13, Proposition 7].

Proposition 2.6. *Let g, k, ℓ be fixed positive integers and s be a fixed non-negative integer. Let $c \in \mathbb{N}_0$. If $g \in G_k(\ell)$ and $c = gs$, then*

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

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

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

$$f_{k,\ell,g}(c) = \begin{cases} f_{k,\ell,g,s}(c) & c = gs \\ 0 & \text{otherwise.} \end{cases}$$

Now, we assign a sign to the number $f_{k,\ell,g}(c)$, which helps to know whether the roots of type $(g\ell)^s$ of a permutation of type $(\ell)^c$ are even.

Proposition 2.7. *Let k, ℓ be fixed positive integers. Let $g \in G_k(\ell), c \in \mathbb{N}_0$ and*

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

If σ is a permutation of type $(\ell)^c$ and $c = gs$, then $a(c) \neq 0$. In addition, the kth roots of type $(g\ell)^s$ of σ are even permutations if and only if $a(c) > 0$.

Proof. As $c = gs$, we have that $a(c) = (-1)^{s(\ell g+1)} f_{k,\ell,g,s}(c)$, and Proposition 2.6 implies that $a(c) \neq 0$. The result follows because the sign of a q-cycle is $(-1)^{q+1}$ and hence the sign of the product of s cycles of length (ℓg) is $(-1)^{s(\ell g+1)}$. □

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

Proposition 2.8. *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 2.6 we have that $f_{k,\ell,g}(c) \neq 0$ if and only if $c = gs$, for some $s \in \mathbb{N}_0$. Therefore

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

□

Let $\mathrm{re}_k(\ell, c)$ (respectively $\mathrm{ro}_k(\ell, c)$) denote the number of even (respectively odd) kth roots of any permutation of type $(\ell)^c$.

In the proof of Lemma 2.10 we need the following result that is Proposition 5.1.3 in Stanley's book [26].

Proposition 2.9. *Let K be a field of characteristic zero. Fix $m \in \mathbb{N}$ and functions $\phi_i \colon \mathbb{N} \to K$, $1 \leq i \leq m$. Define a new function $\varphi \colon \mathbb{N}_0 \to K$ by*

$$\varphi(|A|) = \sum \phi_1(|A_1|)\phi_2(|A_2|) \cdots \phi_m(|A_m|),$$

where the sum ranges over all weak partitions $(A_1, \dots, A_m)$ of A into m blocks, i.e., $A_1, \dots, A_m$ 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 $\phi_i(n)$ and $\varphi(n)$, respectively. Then

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

Lemma 2.10. *Let $\ell \in \mathbb{N}$. Then*

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

Proof. Let σ be any permutation of type $(\ell)^c$ and let A be the set of all disjoint cycles in σ. Let $G_k(\ell) = \{g_1, \dots, g_m\}$, with $g_1 < \cdots < g_m$. By Proposition 2.1, σ has kth roots if and only if the equation

$$g_1 x_1 + \cdots + g_m x_m = c$$

has non-negative integer solutions, where a solution $(s_1, \dots, s_m)$ of the previous equation means that σ has kth roots of type $(g_1\ell)^{s_1} \dots (g_m\ell)^{s_m}$. We can obtain all these roots by running over all the weak ordered partitions $(A_1, \dots, A_m)$ of A. Indeed, if $(A_1, \dots, A_m)$ is such a partition, the number of kth 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 from 0 if $|A_i|$ is a multiple of g_i, for every i. Let $\mathcal{A}$ be the set of all weak ordered partitions of A into m blocks. The number of kth roots of σ is equal to

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

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

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

determines the parity of the kth roots of σ of type $(g_1\ell)^{s_1}\dots(g_m\ell)^{s_m}$, where $s_i = |A_i|/g_i$. Therefore, the number $\mathrm{re}_k\,(\ell,c) - \mathrm{ro}_k\,(\ell,c)$ 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 Propositions 2.8 and 2.9. $\square$

Let $\mathrm{re}_k(\mathbf{c})$ (respectively $\mathrm{ro}_k(\mathbf{c})$) denote the number of even (respectively 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 2.5 and 2.10.

Lemma 2.11. *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*

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

is equal to the number $\mathrm{re}_k(\mathbf{c}) - \mathrm{ro}_k(\mathbf{c})$, with $\mathbf{c} = (c_1, \dots, c_n)$.

Proof of Theorem 1.1. Let $r_k(\sigma)$ denote the number of kth roots of the permutation σ. We have that

$$2\,\mathrm{re}_k(\sigma) = \mathrm{re}_k(\sigma) + \mathrm{ro}_k(\sigma) + \mathrm{re}_k(\sigma) - \mathrm{ro}_k(\sigma) = r_k(\sigma) + (\mathrm{re}_k(\sigma) - \mathrm{ro}_k(\sigma)).$$

Similarly $2\,\mathrm{ro}_k(\sigma) = r_k(\sigma) - (\mathrm{re}_k(\sigma) - \mathrm{ro}_k(\sigma))$. Therefore, the result follows immediately from Theorem 2.2 and Lemma 2.11. $\square$

3 Particular cases

If k is odd, then any solution of the equation $x^k = \sigma$ has the same parity as σ, so the generating function is the same as the one given in Theorem 2.2. Therefore, in this section k is a fixed even integer.

In some examples, we use, without explicit mention, the following observation.

Observation 3.1. *Let k be an even integer. If ℓ is even, then $G_k(\ell)$ is a set of even integers.*

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

For a fixed positive integer ℓ, we have that

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

and

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

With these expressions, we can obtain the generating functions of the following sequences in OEIS: A000704, A061129, A061130, A061131, A061132, A001465, A061136 and A061137. For example, sequence A061131 corresponds 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

$$\begin{aligned}\sum_{c\geq 0} re_8(1,c)\frac{t^c}{c!} &= \frac{1}{2}\exp\left(t+\frac{1}{2}t^2+\frac{1}{4}t^4+\frac{1}{8}t^8\right) + \frac{1}{2}\exp\left(t-\frac{1}{2}t^2-\frac{1}{4}t^4-\frac{1}{8}t^8\right)\\ &= \exp(t)\cosh\left(\frac{1}{2}t^2+\frac{1}{4}t^4+\frac{1}{8}t^8\right).\end{aligned}$$

We can make further simplifications of equations (1) and (2). First, we consider the case when ℓ is even. By Observation 3.1 we have that

$$\sum_{c\geq 0} \mathrm{re}_k(\ell,c)\frac{t^c}{c!} = \cosh\left(\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right)$$

and

$$\sum_{c\geq 0} \mathrm{ro}_k(\ell,c)\frac{t^c}{c!} = \sinh\left(\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right).$$

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

$$\begin{aligned}\sum_{c\geq 0} \mathrm{re}_k(\ell,c)\frac{t^c}{c!} &= \frac{1}{2}\exp\left(\sum_{g\in G_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right) + \frac{1}{2}\exp\left(\sum_{g\in GO_k(\ell)} \frac{\ell^{g-1}}{g}t^g - \sum_{g\in GE_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right),\\ &= \exp\left(\sum_{g\in GO_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right)\cosh\left(\sum_{g\in GE_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right).\end{aligned}$$

Similarly, for the case of odd kth roots we have

$$\sum_{c\geq 0} \mathrm{ro}_k(\ell,c)\frac{t^c}{c!} = \exp\left(\sum_{g\in GO_k(\ell)} \frac{\ell^{g-1}}{g}t^g\right)\sinh\left(\sum_{g\in GE_k(1)} \frac{\ell^{g-1}}{g}t^g\right).$$

For the case of the identity permutation ($\ell = 1$) we have that $G_k(1) = \{m\colon m|k\}$. Therefore,

$$\sum_{c\geq 0} \mathrm{re}_k(1,c)\frac{t^c}{c!} = \exp\left(\sum_{\substack{g|k\\ g \text{ odd}}} \frac{1}{g}t^g\right)\cosh\left(\sum_{\substack{g|k\\ g \text{ even}}} \frac{1}{g}t^g\right),$$

and

$$\sum_{c\geq 0} \mathrm{ro}_k(1,c)\frac{t^c}{c!} = \exp\left(\sum_{\substack{g|k\\ g \text{ odd}}} \frac{1}{g}t^g\right)\sinh\left(\sum_{\substack{g|k\\ g \text{ even}}} \frac{1}{g}t^g\right).$$

In particular, for the case $k = 2^m$, we have

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

This generating function was used in the work of Koda, Sato and Tskegahara [11]. For the case of odd roots we have

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

3.2 Square roots of permutations

For the case of even square roots we have the following consequence of Theorem 1.1.

Corollary 3.2. *The coefficient of $t_1^{c_1}\dots t_n^{c_n}/(c_1!\dots c_n!)$ in the expansion of*

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

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

Proof. We rewrite Theorem 1.1 for the case of even square roots. When $k = 2$, $G_2(\ell) \subseteq \{1, 2\}$. We have two cases depending on the parity of ℓ. If $\ell = 2j - 1$, with $j \in \mathbb{N}$, then $G_2(2j - 1) = \{1, 2\}$. Thus

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

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 $\ell = 2j$, with $j \in \mathbb{N}$, then $G_2(2j) = \{2\}$. Therefore,

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

and

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

Therefore, the exponential generating function in Theorem 1.1 becomes

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

From this we obtain

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

which is equal to

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

The proof for the case of odd square roots is similar. $\square$

Acknowledgments

The authors would like to thank the reviewers for their valuable comments and suggestions. L.M.R. was partially supported by PROFOCIE grant 2018-2021, 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 J.* **12**(10) (2009), 581–589.

[2] M. Bóna, A. McLennan and D. White, Permutations with roots, *Random Structures & Algorithms* **17**(2) (2000), 157–167.

[3] I. Z. Bouwer and 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, Twelfth British Combin. Conf. (Norwich 1989), *Ars Combin.* **29**(C) (1990), 226–227.

[5] W. W. Chernoff, Permutations with p^lth roots, 13th British Combin. Conf. (Guildford, 1991), *Discrete Math.* **125** (1994), 123–127.

[6] N. Chigira, The solutions of $x^d = 1$ in finite groups, *J. Algebra* **180**(3) (1996), 653–661.

[7] S. Chowla, I. N. Herstein and W. R. Scott, The solution of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk. Forh., Trondheim* **25** (1952), 29–31.

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

[9] O. Gruder, Zur Theorie der Zerlegung von Permutationen in Zyklen, *Arkiv für Matematik*, Band 2 no. 20, (1952), 385–414.

[10] E. Jacobsthal, Sur le nombre d'elements du groupe symetrique S_n dont l'ordre est un nombre premier, *Norske Vid. Selsk.* **21**(12) (1949), 49–51.

[11] T. Koda, M. Sato and Y. Takegahara, 2-adic properties for the numbers of involutions in the alternating groups, *J. Algebra Appl.* **14**(4) (2015), 1550052, 21 pp.

[12] A. V. Kolchin, Equations that contain an unknown permutation, *Diskret. Mat.* **6**(1) (1994), 100–115.

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

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

[15] 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.

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

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

[18] OEIS Foundation Inc. (2020), The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

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

[20] A. I. Pavlov, An equation in a symmetric semigroup, *Trudy Mat. Inst. Steklov.* **177** (1986), 114121, 208, Proc. Steklov Inst. Math. 1988, no. 4, 121–129, Probabilistic problems of discrete mathematics.

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

[22] N. Pouyanne, On the number of permutations admitting an m-th root, *Electron. J. Combin.* **9** (2002), #R3, 12 pp.

[23] Y. Roichman, A note on the number of k-roots in S_n, *Sém. Lothar. Combin.* **70** (2013), Art. B70i, 5 pp.

[24] A. Sadeghieh and K. Ahmadidelir, n-th roots in finite polyhedral and centro-polyhedral groups, *Proc. Indian Acad. Sci. Math Sci.* **125**(4) (2015), 487–499.

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

[26] R. P. Stanley, Enumerative Combinatorics Vol. 2, Cambridge Univ. Press, 1999.

[27] L. M. Volynets, The number of solutions of the equation $x^s = e$ in a symmetric group, *Mat. Zametki* **40**(2) (1986), 155–160.

[28] R. Warlimont, Uber die Anzahl der Losungen von $x^n = 1$ in der symmetrischen Gruppe S_n, *Arch. Math. (Basel)* **30**(6) (1978), 591–594.

[29] H. S. Wilf, The asymptotics of $e^P(z)$ and the number of elements of each order in S_n, *Bull. Amer. Math. Soc. (N.S.)* **15**(2) (1986), 228–232.

[30] C. W. York, Enumerating kth roots in the symmetric inverse monoid, *J. Combin. Math. Combin. Comput.* **108** (2019), 147–159.

(Received 23 Nov 2021; revised 10 Oct 2022, 4 Apr 2023)