Proc. Indian Acad. Sci. (Math. Sci.) Vol. 125, No. 4, November 2015, pp. 487–499.

n-th Roots in finite polyhedral and centro-polyhedral groups

A SADEGHIEH[1] and K AHMADIDELIR[2,*]

[1]Yazd Branch, Islamic Azad University, Yazd, Iran
[2]Department of Mathematics, Tabriz Branch, Islamic Azad University, Tabriz, Iran
[*]Corresponding author.
E-mail: sadeghieh@iauyazd.ac.ir; kdelir@gmail.com; k_ahmadi@iaut.ac.ir

MS received 25 November 2013; revised 7 July 2014

Abstract. The probability that a randomly chosen element in a non-abelian finite group has a square root, has been investigated by certain authors in recent years. In this paper, this probability will be generalized for the n-th roots when $n \geqslant 2$ and it will be computed for every finite polyhedral group and all of the finite centro-polyhedral groups.

Keywords. Probability in finite groups; roots of elements; polyhedral groups; centro-polyhedral groups.

2010 Mathematics Subject Classification. 20A05, 20B05, 20P05.

1. Introduction

In the past 30 years, and particularly during the last decade, there has been a growing interest in the use of probability in finite groups. In the current article we shall consider one aspect of the way in which probability has been applied to problems in group theory. That is, the probability that a randomly chosen element has an n-th root, for a positive integer n, in some well-known classes of finite groups.

An element g of a finite group G is said to have an n-th root if there exists an element $h \in G$ such that $g = h^n$ (n is a positive integer). Note that g may have at least an n-th root, or it may have none.

Let G^n be the set of all elements of G which have at least one n-th root, i.e.

$$G^n = \{g \in G \mid \exists\ h \in G\ s.t\ g = h^n\}$$

or simply $G^n = \{g^n \mid g \in G\}$. Then $P_n(G) = \frac{|G^n|}{|G|}$ is the probability that a randomly chosen element in G has an n-th root.

The properties of $P_2(S_n)$, where S_n denotes the symmetric group on n letters have been studied by some authors in [2, 3, 9]. Recently, the basic properties of $P_2(G)$ for an arbitrary finite group G have been studied (for example, see [5, 8]). Moreover, $P_2(G)$, in the case in which G is a simple group of Lie type of rank 1 or when G is an alternating group have been calculated by the authors of those articles. Already, in [1], we generalized the probability to p-th root ($p > 2$ is a prime number) and gave some bounds for it. We showed that the set $X = \{P_p(G) \mid G \text{ is a finite group}\}$ is a dense subset of the closed interval [0, 1]. Also, in [10], the n-th roots of the elements of the dihedral groups and the generalized quaternion groups have been calculated by Sadeghieh and Doostie.

The *polyhedral groups* (ℓ, m, n) for $\ell, m, n > 1$ are defined by the presentation

$$\langle x, y, z \mid x^\ell = y^m = z^n = xyz = 1\rangle, \tag{1}$$

or equivalently by the presentation

$$\langle x, y \mid x^\ell = y^m = (xy)^n = 1\rangle \tag{2}$$

and are classic in group theory. They are important both in algebra and geometry. It is known that the polyhedral group (ℓ, m, n) is finite if and only if $\frac{1}{\ell} + \frac{1}{m} + \frac{1}{n} > 1$, and in this case the order of it is obtained by the formula

$$\frac{2\ell mn}{mn + n\ell + \ell m - \ell mn}.$$

Also, if ℓ, m, n are arbitrary integers, then the group presented by (1) is called von-Dyck group and it can be easily shown by Tietze transformations that it is independent of the signs and orders of ℓ, m and n in (ℓ, m, n). For more details, see [4, 7].

Threlfall (1932) considered the larger group $\langle \ell, m, n\rangle$ defined by the presentation:

$$\langle x, y, z \mid x^\ell = y^m = z^n = xyz\rangle. \tag{3}$$

Since (l, m, n) occurs as a factor group, $\langle \ell, m, n\rangle$ is infinite when $\frac{1}{\ell} + \frac{1}{m} + \frac{1}{n} \leqslant 1$. If $\frac{1}{\ell} + \frac{1}{m} + \frac{1}{n} > 1$, it can be shown that the order of $t = xyz$ is 2 and the order of $\langle \ell, m, n\rangle$ is twice that of (ℓ, m, n), namely $\frac{4\ell mn}{mn+n\ell+\ell m-\ell mn}$. In this case, these groups have been called *binary polyhedral groups*. For more information on these groups, see [4].

Also, if in $\langle \ell, m, n\rangle$ we have $\ell, m, n \in \mathbb{Z}$, then the groups presented by (3) and this general condition have been called *centro-polyhedral group*. One can show, in all finite cases that

$$\langle -\ell, m, n\rangle \cong \langle \ell, m, n\rangle \times \mathbb{Z}_r,$$

where $r = \frac{2mn}{mn+n\ell+\ell m-\ell mn} - 1$ and $\mathbb{Z}_r$ is the cyclic group of order r. So, for example, $|(2, 2, n)| = 2n$ and $|\langle 2, 2, n\rangle| = 4n$, but $|\langle -2, 2, n\rangle| = 4n(n - 1)$, where $(n > 0)$. For more information on these groups, see [4].

In this paper we are going to calculate the n-th roots of elements of polyhedral and centro-polyhedral groups and related $P_n(G)$ in all finite cases.

2. Some properties of n-th roots in finite groups

In this section, we give some elementary results about G^n, where G is a finite group. We use (m, n) to denote the highest common factor of the positive integers m and n.

PROPOSITION 2.1

Let G be a finite group with order m. Let n be a positive integer. Then $G^n = G^r$, where r is the remainder of division of n by m $(n = mq + r;\ \ 0 \leqslant r < m)$.

Proof. We have

$$G^n = \{g^n \mid g \in G\} = \{g^{mq+r} \mid g \in G\} = \{g^r \mid g \in G\} = G^r. \qquad \square$$

Remark 2.2. By the above Proposition, in computing the n-th roots of a finite group G of order m (respectively, computing $P_n(G)$), it suffices to compute the r-th roots only for $0 \leqslant r < m$.

We also have the following result:

PROPOSITION 2.3

Let G be a finite group with order m. Let n be a positive integer. If $d = (m, n)$, then $G^n = G^d$. In particular, n and m are coprime if and only if $G^n = G$ (and so $P_n(G) = 1$).

Proof. By assumption, there are some integers u and v such that $um + vn = d$ and so,

$$G^{vn} = \{g^{vn} \mid g \in G\} = \{g^{d-um} \mid g \in G\} = \{g^d \mid g \in G\} = G^d.$$

Now, $G^{vn} \subseteq G^n$. Therefore, $G^d \subseteq G^n$. On the other hand, since $d \big| n$ then $G^n \subseteq G^d$, and the equality holds. In particular, if n and m are coprime then $G^n = G$.

Conversely, suppose $G^n = G$. Let $(n, m) = d > 1$. Then, there is a prime p such that $p \big| d$. So, $p \big| n$ and therefore $G^n \subseteq G^p \subseteq G$. Hence $G^p = G$. This means that every element in G has a p-th root. If P is a Sylow p-subgroup of G, let p^t be the exponent of P and y an element of P of order p^t. Let $y = x^p$ for some $x \in G$, then, $|x| = p \cdot |y| = p^{t+1}$, contradicting the fact that $\exp(P) = p^t$. So $(|G|, p) = 1$, a contradiction. □

COROLLARY 2.4

For every prime p,

$$P_n(\mathbb{Z}_p) = \begin{cases} \frac{1}{p}, & \text{if } p \big| n, \\ 1, & \text{if } p \nmid n, \end{cases}$$

and, in general,

$$P_n(\mathbb{Z}_{p^k}) = \begin{cases} \frac{1}{p^s}, & \text{if } s = \min\{t, k\}, \text{ where } p^t \big| n \text{ and } p^{t+1} \nmid n, \\ 1, & \text{if } p \nmid n. \end{cases}$$

□

We use the notation $\exp(G)$ for the exponent of a finite group G (the least common multiple of the orders of elements of G). The next propositions reduce the computations of G^n to G^r, where $0 \leq r < \exp(G)$ (cf. with the above results).

PROPOSITION 2.5

Let G be a finite group with exponent $\exp(G) = e$. Let n be a positive integer. Then $G^n = G^r$, where r is the remainder of division of n by e ($n = eq + r$; $0 \leq r < e$).

Proof. We have

$$G^n = \{g^n \mid g \in G\} = \{g^{eq+r} \mid g \in G\} = \{g^r \mid g \in G\} = G^r.$$ □

PROPOSITION 2.6

Let G be a finite group with exponent $\exp(G) = e$. Let n be a positive integer. If $d = (e, n)$, then $G^n = G^d$. In particular, if n and e be coprime then $G^n = G$ (and so $P_n(G) = 1$).

Proof. It is similar to the proof of Proposition 2.3. □

Remark 2.7. By the above propositions, in computing the n-th roots of a finite group G of order m and exponent e (respectively, computing $P_n(G)$), it suffices to compute the r-th roots only for $0 \leq r < e$ (instead of $0 \leq r < m$).

The next result shows that the mapping P_n preserves the direct product of groups.

PROPOSITION 2.8

Let G and H be two finite groups. Then for every positive integer n,

$$P_n(G \times H) = P_n(G) \cdot P_n(H).$$

Proof. Let G and H be two finite groups and $(x, y) \in G \times H$ is an arbitrary element. Then (x, y) is an n-th root of an element of $G \times H$ if and only if x and y are n-th roots of some elements of G and H, respectively. So,

$$P_n(G \times H) = P_n(G) \cdot P_n(H).$$ □

3. Probability of having n-th roots in finite polyhedral and centro-polyhedral groups

We start this section with a lemma about the form of elements of the group $\langle m, 2, -2\rangle$.

Lemma 3.1. *Let $G = \langle m, 2, -2\rangle = \langle x, y, z | x^m = y^2 = z^{-2} = xyz\rangle$. Then,*

(*i*) *every element of G may be presented by $x^i y^j$, where $i = 0, 1, \ldots, 2m(m-1)$ and $j = 0, 1$;*
(*ii*) *$(x^i y)^{2k} = x^{(2i+1)km}$ and $(x^i y)^{2k+1} = x^{i(2km+1)+km} y$, where $k \geq 0$ is an integer.*

Proof.

(i) From $y^2 = xyz$, we have $z = (xy)^{-1} y^2$. So, since $z^2 = y^{-2}$ and $x^m = y^2$, it follows that $xy = yx^{2m-1}$ and $x^i y = yx^{i(2m-1)}$ $(i \geq 0)$. Then we easily get $x^{2m(m-1)} = 1$ and see that $|x| = 2m(m-1)$. On the other hand, we can obtain from the relations that $yx = x^{3m-1} y^{-1}$, and also

$$y^2 = x^m \;\Rightarrow\; x^i y^j = \begin{cases} x^i x^{\frac{1}{2}mj}, & \text{if } j \text{ even}, \\ x^i x^{\frac{j-1}{2}m} y, & \text{if } j \text{ odd}. \end{cases}$$

Now, from the above, we get that for every $g \in G$, $g = x^i y^j$, where $i = 0, 1, \ldots, 2m(m-1)$ and $j = 0, 1$.
(ii) Let $i \geq 0$ be an integer, then by using (i), we have

$$(x^i y)^2 = x^i yx^i y = x^i y^2 x^{i(2m-1)} = x^i x^m x^{i(2m-1)} = x^{(2i+1)m}.$$

Thus we get $(x^i y)^{2k} = x^{(2i+1)km}$ and so $(x^i y)^{2k+1} = x^{(2i+1)km} x^i y = x^{i(2km+1)+km} y$. □

By Tietze transformations, we show in the following proposition that $\langle \ell, m, n\rangle$ is independent of the orders of ℓ, m and n. But, unlike polyhedral groups (von-Dyck groups), it depends on the signs of ℓ, m and n.

PROPOSITION 3.2

For all $\ell, m, n \in \mathbb{Z}$,

$$\langle \ell, m, n\rangle \cong \langle \ell, n, m\rangle \cong \langle m, \ell, n\rangle \cong \langle m, n, \ell\rangle \cong \langle n, m, \ell\rangle \cong \langle n, \ell, m\rangle.$$

Proof. Using the Tietze transformations, we have the following isomorphisms:

$$\begin{aligned}
\langle \ell, m, n\rangle &= \langle x, y, z \mid x^\ell = y^m = z^n = xyz\rangle \\
&\cong \langle x, y, z \mid x^\ell = y^m = z^n, x^{\ell-1} = yz\rangle \\
&\cong \langle x, y, z \mid x^{-\ell} = y^{-m} = z^{-n},\ x^\ell = yzx\rangle \\
&\cong \langle x, y, z \mid x^{-\ell} = y^{-m} = z^{-n} = x^{-1}z^{-1}y^{-1}\rangle \\
&\cong \langle a, b, c \mid a^\ell = b^n = c^m = abc\rangle \quad (x^{-1} = a,\ z^{-1} = b,\ y^{-1} = c) \\
&= \langle \ell, n, m\rangle.
\end{aligned}$$

$$\begin{aligned}
\langle \ell, m, n\rangle &= \langle x, y, z \mid x^\ell = y^m = z^n = xyz\rangle \\
&\cong \langle x, y, z \mid x^{-\ell} = y^{-m} = z^{-n} = z^{-1}y^{-1}x^{-1}\rangle \\
&\cong \langle x, y, z, a, b, c \mid x^{-\ell} = y^{-m} = z^{-n} = z^{-1}y^{-1}x^{-1}, \\
&\qquad\qquad x^{-1} = c,\ y^{-1} = b,\ z^{-1} = a\rangle \\
&\cong \langle a, b, c \mid a^n = b^m = c^\ell = abc\rangle \\
&= \langle n, m, \ell\rangle.
\end{aligned}$$

Other isomorphisms hold similarly. □

PROPOSITION 3.3

The following isomorphisms hold:

$\langle -2, 3, 3\rangle$	$\cong$	$\langle 2, 3, 3\rangle \times \mathbb{Z}_5$
$\langle 2, -3, l-3\rangle$	$\cong$	$\langle 2, 3, 3\rangle \times \mathbb{Z}_7$
$\langle -2, -3, -3\rangle$	$\cong$	$\langle 2, 3, 3\rangle \times \mathbb{Z}_{13}$
$\langle 2, 3, -4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_5$
$\langle 2, -3, 4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_7$
$\langle -2, 3, 4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_{11}$
$\langle 2, -3, -4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_{13}$
$\langle -2, 3, -4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_{17}$
$\langle -2, -3, 4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_{19}$
$\langle -2, -3, -4\rangle$	$\cong$	$\langle 2, 3, 4\rangle \times \mathbb{Z}_{25}$
$\langle 2, 3, -5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{11}$
$\langle 2, -3, 5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{19}$
$\langle -2, 3, 5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{29}$
$\langle 2, -3, -5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{31}$
$\langle -2, 3, -5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{41}$
$\langle -2, -3, 5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{49}$
$\langle -2, -3, -5\rangle$	$\cong$	$\langle 2, 3, 5\rangle \times \mathbb{Z}_{61}$
$\langle -2, 2, m\rangle$	$\cong$	$\langle 2, 2, m\rangle \times \mathbb{Z}_{m-1}$

Table 1. Finite cases of polyhedral and centro-polyhedral groups.

$\langle n, m, \ell\rangle$	$\lvert\langle n, m, \ell\rangle\rvert$	$\langle n, m, \ell\rangle$	$\lvert\langle n, m, \ell\rangle\rvert$
$\langle 2, 3, 3\rangle$	24	$\langle -2, 3, 3\rangle$	120
$\langle 2, -3, 3\rangle$	72	$\langle -2, -3, 3\rangle$	216
$\langle 2, -3, -3\rangle$	168	$\langle -2, -3, -3\rangle$	312
$\langle 2, 3, 4\rangle$	48	$\langle 2, -3, 4\rangle$	336
$\langle -2, 3, 4\rangle$	528	$\langle 2, 3, -4\rangle$	240
$\langle 2, -3, -4\rangle$	624	$\langle -2, -3, 4\rangle$	912
$\langle -2, 3, -4\rangle$	816	$\langle -2, -3, -4\rangle$	1200
$\langle 2, 3, 5\rangle$	120	$\langle 2, -3, 5\rangle$	2280
$\langle -2, 3, 5\rangle$	3480	$\langle 2, 3, -5\rangle$	1320
$\langle 2, -3, -5\rangle$	3720	$\langle -2, -3, 5\rangle$	5880
$\langle -2, 3, -5\rangle$	4920	$\langle -2, -3, -5\rangle$	7320

Table 2. ($m \geqslant 2$).

Group	Order	Group	Order
$\langle 2, 2, m\rangle$	$4m$	$\langle 2, -2, m\rangle$	$4m(m-1)$
$\langle 2, 2, -m\rangle$	$4m$	$\langle -2, -2, m\rangle$	$4m(2m-1)$
$\langle -2, -2, -m\rangle$	$4m(2m+1)$	$\langle 2, -2, -m\rangle$	$4m(m+1)$

Proof. See pages 67–70 of [4]. □

Also, we get the following propositon about order of some finite cases:

PROPOSITION 3.4

For every positive integer m,

$$|\langle 2, -2, m\rangle| = 4m(m-1),$$

$$|\langle -2, 2, -m\rangle| = |\langle -2, 2, m+1\rangle| = 4m(m+1).$$

Proof. Again, see pages 67–70 of [4]. □

Since the finite cases of polyhedral groups are only $(2, 2, m)$, $(2, 3, 3)$, $(2, 3, 4)$ and $(2, 3, 5)$ (except trivial cases), we can write down all of the corresponding finite cases of centro-polyhedral groups (according to the Introduction and the above results). In tables 1 and 2, we give all finite cases of polyhedral and centro-polyhedral groups (except trivial cases).

In the next two theorems, we give the $P_n(G)$ for all finite cases of (ℓ, m, n).

Theorem 3.5. *Probabilities of all n-th roots in* $(2, 3, 3)$, $(2, 3, 4)$ *and* $(2, 3, 5)$ *are as in tables* 3–5

Table 3. $G = (2, 3, 3)$ with $\exp(G) = 6$.

n	1	2	3	4	5	6
$P_n(G)$	1	$\frac{3}{4}$	$\frac{1}{3}$	$\frac{3}{4}$	1	$\frac{1}{12}$

Table 4. $G = (2, 3, 4)$ with $\exp(G) = 12$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$P_n(G)$	1	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{3}{8}$	1	$\frac{1}{6}$	1	$\frac{3}{8}$	$\frac{2}{3}$	$\frac{1}{2}$	1	$\frac{1}{24}$

Table 5. $G = (2, 3, 5)$ with $\exp(G) = 30$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_n(G)$	1	$\frac{3}{4}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{3}{5}$	$\frac{5}{12}$	1	$\frac{3}{4}$	$\frac{2}{3}$	$\frac{7}{20}$	1	$\frac{5}{12}$	1	$\frac{3}{4}$	$\frac{4}{15}$
n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$P_n(G)$	$\frac{3}{4}$	1	$\frac{5}{12}$	1	$\frac{7}{20}$	$\frac{2}{3}$	$\frac{3}{4}$	1	$\frac{5}{12}$	$\frac{3}{5}$	$\frac{3}{4}$	$\frac{2}{3}$	$\frac{3}{4}$	1	$\frac{1}{60}$

Proof. We have calculated these tables using GAP codes [6], by considering the propositions and remarks of §2. □

Theorem 3.6. *Let m be an integer, $m \geq 2$. Also, let $G = (2, 2, m)$ and $(|G|, n) = d$. Then*

$$P_n(G) = \begin{cases} \frac{d+1}{2d}, & \text{if } d \text{ is odd,} \\ \frac{1}{2d} + \frac{1}{4m}, & \text{if } m \text{ is odd, } 2 \big| d \text{ and } 4 \nmid d, \\ \frac{1}{2d}, & \text{if } m, d \text{ are even, and } 2 \big| \frac{|G|}{d}, \\ \frac{1}{d}, & \text{otherwise.} \end{cases}$$

Proof. We may assume that $G = (m, 2, 2)$. Note that every element of G may be presented by $x^i y^j$, where $i = 0, 1, \ldots, 2m-1$ and $j = 0, 1$. Also, $|x| = 2m$ and $(xy)^{2k+1} = xy^{2k+1}$.

Consider the sets $A = \{x^i \mid i = 0, 1, \ldots, 2m-1\}$, $B = \{x^i y \mid i = 0, 1, \ldots, 2m-1\}$. It is clear that $G = A \cup B$, $A \cap B = \emptyset$ and $G^n = A^n \cup B^n$. Let $d = (4m, n)$ and m are odd, then n is odd and $d = (m, n)$. There exist integers t and s such that $m = td$ and $n = sd$, where t and s are coprime. We show that $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2t-1\}$. We have $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m-1\}$, but for every integer k, where $2t \leq k \leq 2m-1$, there are positive integers l and r such that $k = 2tl + r$ and $0 \leq r < 2t$. So,

$$x^{kn} = x^{(2tl+r)n} = x^{2tlsd} x^{rn} = (x^{2m})^{ls} x^{rn}.$$

Thus, $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2t-1\}$. If $x^{in} = x^{jn}$ for some i and j, where $0 \leq i < j \leq 2t-1$, then $x^{(j-i)n} = 1$, so $2m \big| (j-i)n$ or $2t \big| (j-i)s$. But $(t, s) = 1$ and s is odd and therefore, $2t \big| (j-i)$. This is impossible and we get $|A^n| = 2m/d$. On the other hand, since $(x^i y)^n = x^i y^n$, we observe that

$$y^{2k+1} = \begin{cases} y, & k \text{ even,} \\ y^3, & k \text{ odd,} \end{cases} \quad \text{and} \quad x^i y^{2k+1} = \begin{cases} x^i, & k \text{ even,} \\ x^{m+i}, & k \text{ odd,} \end{cases}$$

where $k \geq 0$ is an integer. We show that $B^n = B$. For this, if $n = 2k+1$ for some integer k, then $B^n = B^{2k+1} = \{(x^i y)^{2k+1} \mid i = 0, 1, \ldots, 2m-1\} = \{x^i y^{2k+1} \mid i = 0, 1, \ldots, 2m-1\}$, so

$$B^n = \begin{cases} \{x^i y \mid i = 0, 1, \ldots, 2m-1\}, & \text{if } k \text{ is even,} \\ \{x^{m+i} y \mid i = 0, 1, \ldots, 2m-1\}, & \text{if } k \text{ is odd.} \end{cases}$$

If $x^{m+i} = x^{m+j} y$ for some integers i and j, where $0 \leq i < j \leq 2m-1$, then $x^{j-i} = 1$ and we get that $2m|(j-i)$. However $0 < j - i < 2m$. Hence, in each case, $|B^n| = 2m$ and since $B^n \cap A = \emptyset$, thus $B^n = B$. Consequently,

$$P_n(G) = \frac{|G^n|}{|G|} = \frac{|A^n| + |B^n|}{4m} = \frac{2m/d + 2m}{4m} = \frac{d+1}{2d}.$$

The proof of the case that m is even, is similar. So, the first part of the theorem is proved.

Now, let m be odd, $(4m, n) = d$, $2 \big| d$ and $4 \nmid d$. Then $(m, n) = d/2$, $m = td/2$ and $n = sd/2$ for some integers $t > 0$ and $s > 0$, where $(t, s) = 1$, t is odd and s is even. We get $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m-1\}$. But for every integer k, where $t \leq k \leq 2m-1$, there are integers l and r such that $k = tl + r$ with $0 \leq r < t$, and so

$$x^{kn} = x^{(tl+r)n} = x^{tlsd/2} x^{rn} = (x^{2m})^{ls/2} x^{rn}.$$

Therefore, $A^n = \{x^{in} \mid i = 0, 1, \ldots, t-1\}$. Also, if $x^{in} = x^{jn}$, where $0 \leq i < j \leq t-1$, then $x^{(j-i)n} = 1$. Thus, $2m|(j-i)n$ yields $t|(j-i)$, however, $0 < j - i < t$. This implies that $i = j$ and therefore $|A^n| = t$. On the other hand, we obtain $(x^i y)^n = (x^i y)^{sd/2} = ((x^i y)^s)^{d/2} = (y^s)^{d/2}$, therefore, $B^n = \{y^n\}$ and since $4 \nmid n$, we get $B^n \cap A^n = \emptyset$. Hence, $|G^n| = |A^n| + |B^n|$ and consequently,

$$P_n(G) = \frac{|A^n| + |B^n|}{4m} = \frac{t+1}{4m} = \frac{1}{2d} + \frac{1}{4m}.$$

Now, we prove the third part. Let m and d be even and $2 \big| |G|/d$. Since $(4m, n) = d$, there exist integers $t > 0$ and $s > 0$ such that $4m = td$ and $n = sd$, where $(t, s) = 1$. Note that $2 \big| \frac{4m}{d} = t$. Now, for every integer k, where $t/2 \leq k \leq 2m-1$, there exist integers $l > 0$ and r such that $k = \frac{t}{2} l + r$, where $0 \leq r < t/2$. We get

$$x^{kn} = (x^{\frac{t}{2} l + r})^n = x^{\frac{t}{2} ln} x^{rn} = x^{lsd\frac{t}{2}} x^{rn} = (x^{2m})^{sl} x^{rn}.$$

Hence, $A^n = \{x^{in} \mid i = 0, 1, \ldots, t/2 - 1\}$. On the other hand, for every i and j where $0 \leq i < j \leq t/2 - 1$, we obtain $x^{in} \neq x^{jn}$, as above. Therefore, $|A^n| = t/2$. Now, for every i, where $0 \leq i \leq 2m-1$, we get $(x^i y)^n = x^{msd/2} \in A^n$, so $B^n \subseteq A^n$. Therefore,

$$P_n(G) = \frac{|G^n|}{|G|} = \frac{|A^n|}{4m} = \frac{\frac{t}{2}}{4m} = \frac{1}{2d}.$$

For the proof of the fourth part, we must consider two cases:

(i) m is odd and $4|d$,
(ii) m, d are even and $2 \nmid \frac{|G|}{d}$.

We prove only the case (i), because the proof of the case (ii) is similar. Let m be odd and $4 \big| d$. Then $(m, n) = d/4$ and so $m = td/4$, $n = sd/4$, where t and s are positive

Table 6. $G = \langle 2, 3, 3\rangle$ with $\exp(G) = 12$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$P_n(G)$	1	$\frac{5}{12}$	$\frac{1}{3}$	$\frac{3}{8}$	1	$\frac{1}{12}$	1	$\frac{3}{8}$	$\frac{1}{3}$	$\frac{5}{12}$	1	$\frac{1}{24}$

Table 7. $G = \langle 2, 3, 4\rangle$ with $\exp(G) = 24$.

n	1	2	3	4	5	6	7	8	9	10	11	12
$P_n(G)$	1	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{5}{24}$	1	$\frac{1}{6}$	1	$\frac{3}{16}$	$\frac{2}{3}$	$\frac{1}{3}$	1	$\frac{1}{24}$
n	13	14	15	16	17	18	19	20	21	22	23	24
$P_n(G)$	1	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{3}{16}$	1	$\frac{1}{6}$	1	$\frac{5}{24}$	$\frac{2}{3}$	$\frac{1}{3}$	1	$\frac{1}{48}$

Table 8. $G = \langle 2, 3, 5\rangle$ with $\exp(G) = 60$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_n(G)$	1	$\frac{23}{60}$	$\frac{2}{3}$	$\frac{3}{8}$	$\frac{3}{5}$	$\frac{13}{60}$	1	$\frac{3}{8}$	$\frac{2}{3}$	$\frac{11}{60}$	1	$\frac{5}{24}$	1	$\frac{23}{60}$	$\frac{4}{15}$
n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$P_n(G)$	$\frac{3}{8}$	1	$\frac{13}{60}$	1	$\frac{7}{40}$	$\frac{2}{3}$	$\frac{23}{60}$	1	$\frac{5}{24}$	$\frac{3}{5}$	$\frac{23}{60}$	$\frac{2}{3}$	$\frac{3}{8}$	1	$\frac{1}{60}$
n	31	3 2	33	34	35	36	37	38	39	40	41	42	43	44	45
$P_n(G)$	1	$\frac{3}{8}$	$\frac{2}{3}$	$\frac{23}{60}$	$\frac{3}{5}$	$\frac{5}{24}$	1	$\frac{23}{60}$	$\frac{2}{3}$	$\frac{7}{40}$	1	$\frac{13}{60}$	1	$\frac{3}{8}$	$\frac{4}{15}$
n	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
$P_n(G)$	$\frac{23}{60}$	1	$\frac{5}{24}$	1	$\frac{11}{60}$	$\frac{2}{3}$	$\frac{3}{8}$	1	$\frac{13}{60}$	$\frac{3}{5}$	$\frac{3}{8}$	$\frac{2}{3}$	$\frac{23}{60}$	1	$\frac{1}{120}$

integers such that $(t, s) = 1$. We get $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m-1\} = \{x^{in} \mid i = 0, 1, \ldots, t-1\}$, because, if $t \le k \le 2m-1$, then there are integers $l > 0$ and r such that $k = tl + r$, where $0 \le r < t$, then

$$x^{kn} = (x^{tl+r})^n = x^{tln}x^{rn} = x^{tl\frac{sd}{4}}x^{rn} = (x^{2m})^{\frac{ls}{2}}x^{rn}.$$

So $A^n = \{x^{in} \mid i = 0, 1, \ldots, t-1\}$. Now, $x^{in} \neq x^{jn}$ for every i and j, where $0 \le i < j \le t-1$, as above. Hence $|A^n| = t$. On the other hand, $(x^i y)^n = ((x^i y)^4)^{s/4)(d/4)} = 1$, and so $B^n = \{1\}$ yields $G^n = A^n$. Consequently,

$$P_n(G) = \frac{|A^n|}{4m} = \frac{t}{td} = \frac{1}{d}. \qquad \square$$

Finally, in the following theorems, we give $P_n(G)$ for all finite cases of $\langle \ell, m, n\rangle$.

Theorem 3.7. *Probabilities of all n-th roots in* $\langle 2, 3, 3\rangle$, $\langle 2, 3, 4\rangle$ *and* $\langle 2, 3, 5\rangle$ *are as in tables* 6–8

Proof. We have calculated these tables using GAP [6] codes, by considering the propositions and remarks of §2. $\square$

Now, one may use the propositions in the previous section and table 1 to compute $P_n(G)$ for all finite cases of $\langle \ell, m, n\rangle$, where $\ell = \pm 2$, $m = \pm 3$ and $n = \pm 3, \pm 4, \pm 5$.

Theorem 3.8. *Let m be an integer, $m \geqslant 2$ and G be one of the groups $\langle 2, 2, m\rangle$, $\langle 2, 2, -m\rangle$, $\langle 2, -2, m\rangle$, $\langle 2, -2, -m\rangle$, $\langle -2, -2, m\rangle$ or $\langle -2, -2, -m\rangle$ and also $(|G|, n) = d$. Then*

$$P_n(G) = \begin{cases} \frac{1}{2d}, & m \text{ even, } d \text{ even and } 2\big|\frac{|G|}{d}, \\ \frac{(m,d)+1}{2d}, & d \text{ odd and } (m,d) \neq 1, \\ \frac{1}{2d} + \frac{1}{2dm}, & m \text{ odd, } d \text{ even and } 2m\big|\frac{|G|}{d}, \\ \frac{1}{d} + \frac{1}{4m(m-1)}, & m \text{ odd, } 2m \nmid \frac{|G|}{d},\ m\big|\frac{|G|}{d} \text{ and } m \neq \frac{|G|}{d}, \\ \frac{1}{2d} + \frac{1}{2d(m,\frac{|G|}{d})}, & m \text{ odd, } d \text{ even, } (m, \frac{|G|}{d}) \neq m \text{ and } 2\big|\frac{|G|}{d}, \\ \frac{2}{d}, & m \text{ odd, } d \text{ even, } (m, \frac{|G|}{d}) = 1 \text{ and } 2 \nmid \frac{|G|}{d}, \\ \frac{1}{d}, & \text{otherwise.} \end{cases}$$

Proof. We prove the theorem only for the case $G = \langle m, 2, -2\rangle$. The proofs of the other cases are similar.

By assumption, there exist positive integers s and t such that $4m(m-1) = sd$ and $n = td$, where s and t are coprime. Consider the sets

$$A = \{x^i \mid i = 0, 1, \ldots, 2m(m-1)-1\},\ B = \{x^i y \mid i = 0, 1, \ldots, 2m(m-1)-1\}.$$

It is clear that $G = A \cup B$, $A \cap B = \emptyset$ and $G^n = A^n \cup B^n$. Let m and d be even, and $2\big|\frac{|G|}{d}$. We have $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m(m-1)-1\}$. But for every integer k where $s/2 \leq k \leq 2m(m-1)-1$, there are integers $l > 0$ and r such that $k = \frac{s}{2}l + r$ and $0 \leq r < s/2$. So

$$x^{kn} = x^{(\frac{s}{2}l+r)n} = x^{\frac{s}{2}ltd}x^{rn} = (x^{2m(m-1)})^{lt}x^{rn} = x^{rn}.$$

Thus $A^n = \{x^{in} \mid i = 0, 1, \ldots, s/2-1\}$. If $x^{in} = x^{jn}$ for some i and j where $0 \leq i < j \leq s/2-1$, then $x^{(j-i)n} = 1$, and we get $s/2\big|(j-i)$, but this is impossible and we obtain $|A^n| = s/2$. On the other hand, by Lemma 3.1, $(x^i y)^n = x^{(2i+1)\frac{n}{2}m}$, where $i = 0, 1, \ldots, 2m(m-1)$. Since m is even, $x^{(2i+1)m/2} \in A$ and so $x^{(2i+1)\frac{n}{2}m} \in A^n$, hence $B^n \subseteq A^n$. Therefore,

$$P_n(G) = \frac{|G^n|}{|G|} = \frac{|A^n|}{4m(m-1)} = \frac{s/2}{sd} = \frac{1}{2d}.$$

This completes the proof of the first part.

Let m be even, d be odd and $(m,d) \neq 1$. Let $(m,d) = q$, then there exist integers u and v such that $m = uq$ and $d = vq$, where $(u,v) = 1$. Since $2m\big|\frac{s}{2}d$, thus $2u\big|\frac{s}{2}v$. But $(u,v) = 1$ and v is odd, so $u\big|s/4$. We show that $A^n = \{x^{in} \mid 0 \leq i \leq s/2-1\}$. We have $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m(m-1)\}$, but for every integer k where $s/2 \leq k \leq 2m(m-1)$, there are integers $l > 0$ and r such that $k = \frac{s}{2}l + r$ and $0 \leq r < s/2$. So

$$x^{kn} = x^{\frac{s}{2}ltd}x^{rn} = (x^{2m(m-1)})^{lt}x^{rn} = x^{rn}.$$

Also, for every i and j, where $0 \leq i < j \leq s/2-1$, $x^{in} \neq x^{jn}$, just as above. Hence $|A^n| = s/2$. On the other hand, $B^n = \{(x^i y)^n \mid i = 0, 1, \ldots, 2m(m-1)-1\}$. But for

every integer k, where $\frac{s}{2}q \leq k \leq 2m(m-1)-1$, there are integers $l > 0$ and r such that $k = \frac{s}{2}ql + r$ and $0 \leq r \leq \frac{s}{2}q$. Therefore, by Lemma 3.1,

$$\begin{aligned}(x^k y)^n &= x^{(\frac{s}{2}ql+r)((n-1)m+1)+\frac{n-1}{2}m}y \\ &= x^{\frac{s}{2}qlnm}x^{-\frac{s}{2}ql(m-1)}x^{r((n-1)m+1)+\frac{n-1}{2}m}y \\ &= x^{\frac{s}{2}qltdm}(x^{2uq(m-1)})^{-\frac{s}{4u}l}x^{r((n-1)m+1)+\frac{n-1}{2}m}y \\ &= (x^{2m(2m-1)})^{qltm}(x^{2m(m-1)})^{-\frac{s}{4u}l}x^{r((n-1)m+1)+\frac{n-1}{2}m}y \\ &= x^{r((n-1)m+1)+\frac{n-1}{2}m}y.\end{aligned}$$

So $B^n = \{(x^i y)^n | i = 0, 1, \ldots, \frac{s}{2}q - 1\}$. Now, if $(x^i y)^n = (x^j y)^n$ for some i and j, where $0 \leq i < j \leq \frac{s}{2}q - 1$, then we get a contradiction. Consequently, $|B^n| = \frac{s}{2}q$. It is clear that $A^n \cap B^n = \emptyset$. Therefore,

$$P_n(G) = \frac{|A^n| + |B^n|}{4m(m-1)} = \frac{\frac{s}{2} + \frac{s}{2}q}{sd} = \frac{(m,d)+1}{2d}.$$

Now, we start to prove the third part and let m be odd, d be even and $2m\big|\frac{|G|}{d}$. Then $2m\big|s$, and s is even. We have $A^n = \{x^{in} \mid i = 0, 1, \ldots, 2m(m-1)-1\}$, but for every integer k, where $s/2 \leq k \leq 2m(m-1)-1$, there exist integers $l > 0$ and r such that $k = \frac{s}{2}l + r$ and $0 \leq r < s/2$, so

$$x^{kn} = x^{(\frac{s}{2}l+r)n} = x^{\frac{s}{2}ltd}x^{rn} = (x^{2m(m-1)})^{lt}x^{rn} = x^{rn}.$$

Also, as before, $x^{in} \neq x^{jn}$ for every i and j, where $0 \leq i < j \leq s/2 - 1$. Hence $|A^n| = s/2$. On the other hand, $B^n = \{(x^i y)^n \mid 0 \leq i \leq 2m(m-1)-1\}$. But for every integer k, where $\frac{s}{2m} \leq k \leq 2m(m-1)-1$, there are integers $l > 0$ and r such that $k = \frac{s}{2m}l + r$ and $0 \leq r < \frac{s}{2m}$. So, by Lemma 3.1 (note that n is even),

$$\begin{aligned}(x^k y)^n &= (x^{\frac{s}{2m}l+r}y)^n = x^{(2(\frac{s}{2m}l+r)+1)\frac{n}{2}m} = x^{\frac{s}{2}ln}x^{(2r+1)\frac{n}{2}m} \\ &= x^{\frac{s}{2}ltd}x^{(2r+1)\frac{n}{2}m} = (x^{2m(m-1)})^{lt}(x^r y)^n = (x^r y)^n.\end{aligned}$$

Thus $B^n = \{(x^i y)^n \mid 0 \leq i \leq \frac{s}{2m} - 1\}$. If $(x^i y)^n = (x^j y)^n$, for some i and j where $0 \leq i < j \leq \frac{s}{2m} - 1$, then we again get a contradiction. Consequently, $|B^n| = \frac{s}{2m}$. We get $A^n \cap B^n = \emptyset$ (for, if $(x^i y)^n = x^{jn}$ for some integers i and j where $0 \leq i \leq \frac{s}{2m} - 1$ and $0 \leq j \leq s/2$, then $x^{(2i+1)\frac{n}{2}m} = x^{jn} \Rightarrow x^{(2j-2im-m)n/2} = 1 \Rightarrow 2m(m-1)\big|(2j - 2im - m)n/2 \Rightarrow \frac{s}{2}d\big|(2j - 2im - m)td/2 \Rightarrow s\big|(2j - 2im - m)t$, since $(s,t) = 1$, thus $s\big|(2j - 2im - m)$. This is impossible and hence,

$$P_n(G) = \frac{|G^n|}{|G|} = \frac{|A^n| + |B^n|}{4m(m-1)} = \frac{\frac{s}{2} + \frac{s}{2m}}{sd} = \frac{1}{2d} + \frac{1}{2dm}.$$

Now, let m is odd, $2m \nmid \frac{|G|}{d}$, $m\big|\frac{|G|}{d}$ and $m \neq \frac{|G|}{d}$. Since $2m \nmid s$ and $m\big|s$, thus s is odd (m is odd) and d is even. We have $A^n = \{x^{in} \mid 0 \leq i \leq 2m(m-1)-1\}$. But for every integer k, where $s \leq k \leq 2m(m-1)$, there exist integers $l > 0$ and r such that $k = sl + r$ and $0 \leq r < s$, so

$$x^{kn} = x^{sltd}x^{rn} = (x^{2m(m-1)})^{2lt}x^{rn} = x^{rn}.$$

Again, $x^{in} \neq x^{jn}$ for all i and j where $0 \leq i < j \leq s-1$. Hence $|A^n| = s$. On the other hand, for every i, where $0 \leq i \leq 2m(m-1)-1$, we get $(x^i y)^n = x^{(2i+1)\frac{n}{2}m} = x^{(2i+1)\frac{td}{2}m}$. If $i \geq 1$, then $2m(m-1)|(2i+1)\frac{n}{2}m$ and so $(x^i y)^n = 1$ and if $i = 0$, then $(x^i y)^n = x^{n/2m}$, which does not belong to A^n. Therefore, $|B^n| = 2$ and $1 \in B^n$, so $|A^n \cap B^n| = 1$, thus $|A^n \cup B^n| = |A^n| + 1$. Consequently,

$$P_n(G) = \frac{|A^n|+1}{4m(m-1)} = \frac{s+1}{sd} = \frac{1}{d} + \frac{1}{4m(m-1)}.$$

For the next part, suppose that m is odd, d is even, $(m, |G|/d) \neq m, 1$, and $2\big||G|/d$. Let $(m, s) = u \neq 1$, then there exist integers k_1 and k_2 such that $s = k_1 u$, $m = k_2 u$ and $(k_1, k_2) = 1$, so $(s/u, k_2) = 1$. It is easy that see that $|A^n| = s/2$. On the other hand, $B^n = \{(x^i y)^n \mid i = 0, 1, \ldots, 2m(m-1)-1\}$. But for every integer k, where $\frac{s}{2u} \leq k \leq 2m(m-1)$ (note that $2\big|s$ and u is odd, so $2u\big|s$), there are integers $l > 0$ and r such that $k = \frac{s}{2u}l + r$ and $0 \leq r < \frac{s}{2u}$. So,

$$\begin{aligned}(x^k y)^n &= (x^{\frac{s}{2u}l+r} y)^n = x^{(2(\frac{s}{2u}l+r)+1)\frac{n}{2}m} = x^{\frac{s}{2u}lnm} x^{(2r+1)\frac{n}{2}m} \\ &= x^{\frac{s}{2}tdl\frac{m}{u}} x^{(2r+1)\frac{n}{2}m} = (x^{2m(m-1)})^{tl\frac{m}{u}} (x^r y)^n = (x^r y)^n.\end{aligned}$$

Hence $B^n = \{(x^i y)^n | 0 \leq i \leq \frac{s}{2u} - 1\}$. Again, one can easily see that $(x^i y)^n \neq (x^j y)^n$ for all i and j, where $0 \leq i < j \leq \frac{s}{2u} - 1$. Hence $|B^n| = \frac{s}{2u}$. We get $A^n \cap B^n = \emptyset$, therefore,

$$P_n(G) = \frac{|A^n| + |B^n|}{4m(m-1)} = \frac{\frac{s}{2} + \frac{s}{2u}}{sd} = \frac{u+1}{2ud} = \frac{1}{2d} + \frac{1}{2d(m, |G|/d)}.$$

For the proof of the last part, we must consider the five cases:

(i) m, d are even and $2 \nmid s$,
(ii) m is even, d is odd and $(m, d) = 1$,
(iii) m, d are odd and $(m, d) = 1$,
(iv) m is odd, d is even and $m = |G|/d$,
(v) m is odd, d is even, $(m, |G|/d) = 1$ and $2\big||G|/d$.

We prove only part (i) for, the proof of the other cases are similar. Let m, d are even and $2 \nmid s$. Then $A^n = \{x^{in} | i = 0, 1, \ldots, s-1\}$, because for every integer k, where $s \leq k \leq 2m(m-1)$, there are integers $l > 0$ and r such that $k = sl + r$ and $0 \leq r < s$. So,

$$x^{kn} = x^{sltd} x^{rn} = (x^{2m(m-1)})^{2lt} x^{rn} = x^{rn}.$$

Again, for all i and j where $0 \leq i < j \leq s-1$ we get $x^{in} \neq x^{jn}$. Hence $|A^n| = s$. On the other hand, $B^n \subseteq A^n$ (its proof is similar to the proof of that in the first part). Therefore,

$$P_n(G) = \frac{|A^n|}{4m(m-1)} = \frac{s}{sd} = \frac{1}{d}. \qquad \square$$

Acknowledgements

The authors would like to express their deep gratitute to the referee for his invaluable comments and suggestions which improved the paper. The first author would like to thank

Yazd Branch, Islamic Azad University for the financial support, which is based on a research project contract.

References

[1] Ahmadidelir K, Doostie H and Sadeghieh A, Probability that an element of a finite group has an nth root, *unpublished*
[2] Blum J, Enumeration of the square permutations in S_n, *J. Combinatorial Theory, (Ser. A)* **17** (1974) 156–161
[3] Bona M, Mclennan A and White D, Permupations with roots, *Random Structures Algorithms* **17(2)** (2000) 157–167
[4] Coxeter H S M and Moser W O J, Generators and relations for discrete groups (1984) (Berlin Heidelberg, New York: Springer-Verlag)
[5] Das A K, On groups elements having square roots, *Bull. Iranian Math. Soc.* **31(2)** (2005) 33–36
[6] The GAP Group, *GAP – Groups, Algorithms and Programming*, Version 4.4.12 Aachen, St Andrews (2010) (http://www.gap-system.org)
[7] Johnson D L, Presentations of Groups (1990) (Cambridge University Press)
[8] Lucido M S and Pournaki M R, Elements with square roots in finite groups, *Algebra Colloquium* **12(4)** (2005) 677–690
[9] Pouyanne N, On the number of permutations admiting an m-th root, *Electron. J. Combin.* **9(1)** (2002), Research Paper 3, 12 pages (electronic)
[10] Sadeghieh A and Doostie H, The nth roots of elements in finite groups, *Mathematical Sciences* **2** (2008) 347–356

COMMUNICATING EDITOR: Parameswaran Sankaran