Probability of having $n^{th}$-roots and $n$-centrality of two classes of groups

M. Hashemi*, M. Polkouei*

Faculty of Mathematical Sciences, University of Guilan, P.O.Box 41335-19141, Rasht, Iran.

Received 8 December 2015; Revised 28 March 2016; Accepted 15 April 2016.

Abstract. In this paper, we consider the finitely 2-generated groups $K(s, l)$ and $G_m$ as follows;

$K(s, l) = \langle a, b | ab^s = b^l a, ba^s = a^l b \rangle$;

$G_m = \langle a, b | a^m = b^m = 1, [a, b]^n = [a, b], [a, b]^b = [a, b] \rangle$

and find the explicit formulas for the probability of having $n^{th}$-roots for them. Also we investigate integers $n$ for which, these groups are $n$-central.

© 2016 IAUCTB. All rights reserved.

Keywords: Nilpotent groups, $n^{th}$-roots, $n$-central groups

2010 AMS Subject Classification: 20D15, 20P05.

1. Introduction

Let $n > 1$ be an integer. An element $a$ of group $G$ is said to have an $n^{th}$-root $b$ in $G$, if $a = b^n$. The probability that a randomly chosen element in $G$ has an $n^{th}$-root, is given by

$$P_n(G) = \frac{|G^n|}{|G|}$$
where $G^n = \{ a \in G | a = b^m, \text{ for some } b \in G \} = \{ x^n | x \in G \}$. In [5], the probability $P_n(G)$ for Dihedral groups $D_{2n}$ and Quaternion groups $Q_{2n}$ for every integer $m \geq 3$ have been calculated. Also, in [4] the probability that Hamiltonian groups may have $n^{th}$-roots have been calculated. For $n > 1$, a group $G$ is said to be $n$-central if $[x^n, y] = 1$ for all $x, y \in G$. In [6], some aspects of $n$-central groups have been investigated.

First, we state the following Lemma without proof.

**Lemma 1.1** If $G$ is a group and $G' \subseteq Z(G)$, then the following hold for every integer $k$ and $u, v, w \in G$:

(i) $[uv, w] = [u, w][v, w]$ and $[u, vw] = [u, v][u, w]$;

(ii) $[u^k, v] = [u, v]^k = [u, v]^k$;

(iii) $(uv)^k = u^kv^k[u, v]^{k(k-1)/2}$.

Now, we state some lemmas which can be found in [1, 2].

**Lemma 1.2** The groups $K(s, l) = \langle a, b | ab^s = b^l a, ba^s = a^l b \rangle$ where $(s, l) = 1$, have the following properties:

(i) $|K(s, l)| = |l - s|^3$, if $(s, l) = 1$ and is infinite otherwise;

(ii) if $(s, l) = 1$ then $|a| = |b| = (l - s)^2$;

(iii) if $(s, l) = 1$, then $a^{l-s} = b^{s-l}$.

**Lemma 1.3** (i) For every $l \geq 3$, $K(s, l) \cong K(1, 2 - l)$.

(ii) For every $i \geq 2$ and $(s, i) = 1$, $K(s, s + i) \cong K(1, i + 1)$.

Note that if $(s, l) = 1$, then $K(s, l) \cong K(1, l - s + 1)$ which we can write as $K_m$ where $m = l - s + 1$.

**Lemma 1.4** Every element of $K_m$ can be uniquely presented by $x = a^\beta b^\gamma a^{(m-1)\delta}$, where $1 \leq \beta, \gamma, \delta \leq m - 1$.

**Lemma 1.5** In $K_m$, $[a, b] = b^{m-1} \in Z(K_m)$.

The following lemma can be seen in [3].

**Lemma 1.6** Let $G_m = \langle a, b | a^m = b^m = 1, [a, b]^n = [a, b], [a, b]^b = [a, b] \rangle$ where $m \geq 2$, then we have

(i) every element of $G_m$ can be uniquely presented by $a^ib^j[a, b]^t$, where $1 \leq i, j, t \leq m$.

(ii) $|G_m| = m^3$.

In this paper, we consider the groups $K_m$ and $G_m$ which are nilpotent groups of nilpotency class two. In section 2, we compute the probability of having $n^{th}$-root of $K_m$ and $G_m$. Section 3 is devoted to finding integers $n$ for which, $K_m$ and $G_m$ are $n$-central.

2. The probability of having $n^{th}$-roots

In this section we consider groups $K_m$ and $G_m$ and find the probability of having $n^{th}$-roots. Here for $m \in \mathbb{Z}$, by $m^*$ we mean the arithmetic inverse of $m$.

**Proposition 2.1** For integers $m, n \geq 2$;

(1) If $G = K_m$ and $x \in G$, then we have

$$x^n = a^{\beta n} b^{n\gamma} a^{(m-1)(n\delta + \frac{n(n-1)\beta\gamma}{2})},$$
(2) If $G = G_m$ and $x \in G$, then we have
\[ x^n = a^{n^2 b^m} a^{(m-1)(n\delta + \frac{n(n-1)}{2} \beta \gamma)}. \]

**Proof.** We use an induction method on $n$. By Lemma 1.4, the assertion holds for $n = 1$. Now, let
\[ x^n = a^{n\beta} b^{n\gamma} a^{(m-1)(n\delta + \frac{n(n-1)}{2} \beta \gamma)}. \]
Then
\[ x^{n+1} = a^{n\beta} b^{n\gamma} a^{(m-1)(n\delta + \frac{n(n-1)}{2} \beta \gamma)} = a^{(n+1)\beta} b^{(n+1)\gamma} a^{(m-1)((n+1)\delta + \frac{n(n+1)}{2} \beta \gamma)}. \]

By Lemma 1.2, $a^{(m-1)\delta} = b^{(1-m)\delta}$. So
\[ x^{n+1} = a^{(n+1)\beta} b^{(n+1)\gamma} a^{(m-1)((n+1)\delta + \frac{n(n+1)}{2} \beta \gamma)}. \]
Since $K_m$ is a group of nilpotency class two, $G' \subseteq Z(G)$. Hence by Lemma 1.1 we have
\[ x^{n+1} = a^{(n+1)\beta} b^{(n+1)\gamma} a^{(m-1)((n+1)\delta + \frac{n(n+1)}{2} \beta \gamma)}. \]
The second part can be proved similarly. $\blacksquare$

**Theorem 2.2** Let $G = K_m$, where $m \geq 2$. Then
\[ P_n(G) = \begin{cases} \frac{d}{2} & \text{if } n \text{ be even, } \left( \frac{n}{2}, m-1 \right) = \frac{d}{2} \text{ and } \frac{m-1}{d} \text{ be odd;} \\ \frac{d}{2} & \text{otherwise,} \end{cases} \]
where $(n, m-1) = d$.

**Proof.** Let $a^{\beta} b^{\gamma} a^{(m-1)\delta}$ be an element of $G^n$ where $1 \leq \beta, \gamma, \delta \leq m-1$. If $x = (x_1)^n$ when $a^{\beta_1} b^{\gamma_1} a^{(m-1)\delta_1} \in G$, $1 \leq \beta_1, \gamma_1, \delta_1 \leq m-1$, then by Proposition 2.1 we have
\[ a^{\beta} b^{\gamma} a^{(m-1)\delta} = (a^{\beta_1} b^{\gamma_1} a^{(m-1)\delta_1})^n = a^{n\beta_1} b^{n\gamma_1} a^{(m-1)(n\delta_1 + \frac{n(n-1)}{2} \beta_1 \gamma_1)}. \]

By uniqueness of presentation of $G$, we obtain
\[ \begin{cases} n\beta_1 \equiv \beta \pmod{m-1} \\ n\gamma_1 \equiv \gamma \pmod{m-1} \\ n\delta_1 + \frac{n(n-1)}{2} \beta_1 \gamma_1 \equiv \delta \pmod{m-1} \end{cases} \quad (1) \]
Now let $(n, m-1) = d$. The first congruence of the system (1) has the solution
\[ \beta_1 \equiv \left( \frac{n}{d} \right)^* \left( \frac{\beta}{d} \right) \pmod{\frac{m-1}{d}}. \]
if and only if $d \mid \beta$. Then
\[
\beta \in \{d, 2d, \ldots, \frac{m-1}{d} \times d\}.
\]
This means that $\beta$ has $\frac{m-1}{d}$ choices. Similarly, by second equation of System (1) we get
\[
\gamma \in \{d, 2d, \ldots, \frac{m-1}{d} \times d\}.
\]
So $\gamma$ admits $\frac{m-1}{d}$ values.

Now for finding the number of values of $\delta$, we consider two cases, where $n$ is odd or even.

First let $n$ be an odd integer. Then
\[
n(\delta_1 + \frac{n(n-1)}{2} \beta_1 \gamma_1) \equiv \delta \pmod{m-1}.
\]
Since $(n, m-1) = d$, we get
\[
\delta_1 \equiv (\frac{n}{d})^* \frac{\delta}{d} - \frac{n(n-1)}{2} \beta_1 \gamma_1 \pmod{\frac{m-1}{d}}
\]
provided that $d \mid \delta$. So
\[
\delta \in \{d, 2d, \ldots, \frac{m-1}{d} \times d\}.
\]
Therefore in this case we have $\frac{m-1}{d}$ choices for $\delta$. By the above facts, we have
\[
|G^n| = |\{a^\beta b^\gamma d^{(m-1)\delta} \mid \beta \in \{d, \ldots, \frac{m-1}{d} \times d\}, \gamma \in \{d, \ldots, \frac{m-1}{d} \times d\}, \delta \in \{d, \ldots, \frac{m-1}{d} \times d\}\}|
\]
\[
= |\{\beta, \gamma, \delta \mid \beta \in \{d, \ldots, \frac{m-1}{d} \times d\}, \gamma \in \{d, \ldots, \frac{m-1}{d} \times d\}, \delta \in \{d, \ldots, \frac{m-1}{d} \times d\}\}|
\]
\[
= \frac{m-1}{d} \times \frac{m-1}{d} \times \frac{m-1}{d} = (\frac{m-1}{d})^3.
\]

So
\[
P_n(G) = \frac{|G^n|}{|G|} = \frac{(m-1/d)^3}{(m-1)^3} = \frac{1}{d^3}.
\]

Now suppose $n$ be an even integer. Then $(\frac{n}{2}, m-1) = d$ or $(\frac{n}{2}, m-1) = \frac{d}{2}$.

Case 1. Let $(\frac{n}{2}, m-1) = d$. Then
\[
\frac{n}{2}(2\delta_1 + (n-1)\beta_1 \gamma_1) \equiv \delta \pmod{m-1}.
\]

So
\[
2\delta_1 \equiv \frac{n}{2d} \frac{\delta}{d} - (n-1)\beta_1 \gamma_1 \pmod{\frac{m-1}{d}}.
\]
Since \((\frac{n}{2}, m-1) = d\), \(\frac{m-1}{d}, 2 \Rightarrow 1\). Hence, the above congruence holds if and only if 
\(d \mid \delta\). Therefore

\[
\delta \in \{d, 2d, \ldots, \frac{m-1}{d} \times d\}.
\]

So

\[
|G^n| = |\{(\beta, \gamma, \delta) | \{\beta \in \{d, \ldots, \frac{m-1}{d} d\}, \gamma \in \{d, \ldots, \frac{m-1}{d} d\}, \delta \in \{d, \ldots, \frac{m-1}{d} d\}\}|
\]

\[
= \left(\frac{m-1}{d}\right)^3
\]

and consequently

\[
P_n(G) = \frac{1}{d^3}
\]

Case 2. Let \((\frac{n}{2}, m-1) = \frac{d}{2}\). Then

\[
\frac{n}{d}(2\delta_1 + (n-1)\beta_1 \gamma_1) \equiv \frac{2\delta}{d} \pmod{\frac{2(m-1)}{d}}.
\]

Hence

\[
2\delta_1 \equiv \frac{n}{d} \frac{2\delta}{d} - (n-1)\beta_1 \gamma_1 \pmod{\frac{2(m-1)}{d}}. \quad (2)
\]

So, we must have \(2 \mid \beta_1 \gamma_1\). Suppose \(2 \mid \gamma_1\). Now by congruence

\[
\gamma_1 \equiv \left(\frac{n}{d}\right)^* \frac{\gamma}{d} \pmod{\frac{m-1}{d}} \quad (3)
\]

we consider two subcases:

Subcase 2.a. Let \(\frac{(m-1)}{d}\) be an even integer. Now since

\[
\frac{n}{d}\left(\frac{n}{d}\right)^* \equiv 1 \pmod{\frac{m-1}{d}},
\]

both \(\frac{n}{d}\) and \(\left(\frac{n}{d}\right)^*\) are odd. Since \(2 \mid \gamma_1\), By congruence \((3)\) we get \(2 \mid \frac{\gamma}{d}\). It means that

\[
\gamma \in \{2d, 4d, \ldots, \frac{m-1}{2d} \times 2d\}.
\]

Hence the number of values of \(\gamma\) is \(\frac{m-1}{2d}\). On the other hand according to congruence \((2)\),
\(\frac{d}{2} \mid \delta\). Therefore

\[
\delta \in \left\{\frac{d}{2}, d, \ldots, \frac{2(m-1)}{d} \times \frac{d}{2}\right\}.
\]
So \( \delta \) admits \( \frac{2(m-1)}{d} \) values. Consequently
\[
|G^n| = \frac{m-1}{d} \times \frac{m-1}{2d} \times \frac{2(m-1)}{d} = \left( \frac{m-1}{d} \right)^3
\]
and
\[
P_n(G) = \frac{1}{d^3}.
\]

Case 2.b. Let \( \frac{m-1}{d} \) be an odd integer and \( \gamma \in \{d, 2d, \ldots, \frac{m-1}{d}d\} \). If \( \gamma_1 \equiv \frac{n}{d} (mod \frac{m-1}{d}) \) and \( \gamma_1 \) be an even integer, then we get the desired result. Otherwise, instead of \( \gamma_1 \), we put \( \gamma_1 + \frac{m-1}{d} \). So for each
\[
\gamma \in \{d, 2d, \ldots, \frac{m-1}{d} \times d\},
\]
the congruence holds. It means that the number of choices for \( \gamma \) is equal to \( \frac{m-1}{d} \). Finally, we get
\[
|G^n| = \frac{m-1}{d} \times \frac{m-1}{d} \times \frac{2(m-1)}{d} = 2\left( \frac{m-1}{d} \right)^3
\]
and
\[
P_n(G) = \frac{2}{d^3}.
\]

**Theorem 2.3** Let \( G = G_m \), where \( m \geq 2 \). Then
\[
P_n(G) = \begin{cases} 
\frac{2}{d^3} & \text{if } n \text{ be even, } \left( \frac{n}{2}, m \right) = \frac{d}{2} \text{ and } \frac{m}{d} \text{ be odd;} \\
\frac{1}{d^3} & \text{otherwise},
\end{cases}
\]
where \( (n, m) = d \).

**Proof.** Let \( a^i b^j [a, b]^t \) be an element of \( G^n \) where \( 1 \leq i, j, t \leq m \). If \( x = (x_1)^n \) when \( a^{i_1} b^{j_1} [a, b]^{t_1} \in G, 1 \leq i_1, j_1, t_1 \leq m \), then by Proposition 2.1 we have
\[
a^i b^j [a, b]^t = (a^{i_1} b^{j_1} [a, b]^{t_1})^n
= a^{ni_1} b^{nj_1} [a, b]^{nt_1 - \frac{n(n-1)}{2} i_1 j_1}.
\]
By uniqueness of presentation of \( G \), we obtain
\[
\begin{align*}
ni_1 & \equiv i \pmod{m} \\
nj_1 & \equiv j \pmod{m} \\
nt_1 - \frac{n(n-1)}{2} i_1 j_1 & \equiv t \pmod{m}.
\end{align*}
\]
The obtained congruence system is exactly similar to System (1). So it can be solve, similarly.

3. \textit{n}-centrality

In this section, we again consider groups $K_m, G_m$ and investigate \textit{n}-centrality for them.

**Theorem 3.1** Let $G = K_m$, where $m \geq 2$. Then for $n > 1$, the group $G$ is \textit{n}-central if and only if $m - 1 | n$.

**Proof.** By Proposition 2.1 and Lemma 1.1, we get

$$x^n y = a^{n\delta_1 + \beta_1 b^{\gamma_1} + \gamma_2} a^{(m-1)(n\delta_1 + \delta_2 + \frac{n(n-1)}{2}\beta_1 \gamma_1 + n\beta_2 \gamma_1)}.$$

Also we obtain

$$yx^n = a^{n\delta_1 + \beta_2 b^{\gamma_1} + \gamma_2} a^{(m-1)(n\delta_1 + \delta_2 + \frac{n(n-1)}{2}\beta_1 \gamma_1 + n\beta_1 \gamma_2)}.$$

We know that $G$ is \textit{n}-central if and only if $x^n y = yx^n$, for all $x, y \in G$. Furthermore by uniqueness of presentation of $x^n y$ and $yx^n$, we see that $x^n y = yx^n$ if and only if

$$n\delta_1 + \delta_2 + \frac{n(n-1)}{2}\beta_1 \gamma_1 + n\beta_2 \gamma_1 \equiv n\delta_1 + \delta_2 + \frac{n(n-1)}{2}\beta_1 \gamma_1 + n\beta_1 \gamma_2 \pmod{m - 1}.$$

This is equivalent to

$$n(\beta_1 \gamma_2 - \beta_2 \gamma_1) \equiv 0 \pmod{m - 1}.$$

Now since this holds for all $x, y \in G$, $m - 1 | n$.

**Theorem 3.2** Let $G = G_m$, where $m \geq 2$. Then for $n > 1$, the group $G$ is \textit{n}-central if and only if $m | n$.

**Proof.** By Proposition 2.1 and Lemma 1.1, we get

$$x^n y = a^{ni_1 + i_2 b^{nj_1 + j_2}} [a, b]^{nt_1 + t_2 - \frac{n(n-1)}{2}i_1 j_1 - ni_1 j_1}.$$

Also we obtain

$$yx^n = a^{ni_1 + i_2 b^{nj_1 + j_2}} [a, b]^{nt_1 + t_2 - \frac{n(n-1)}{2}i_2 j_2 - ni_2 j_2}.$$

We know that $G$ is \textit{n}-central if and only if $x^n y = yx^n$, for all $x, y \in G$. Furthermore by uniqueness of presentation of $x^n y$ and $yx^n$, we see that $x^n y = yx^n$ if and only if

$$nt_1 + t_2 - \frac{n(n-1)}{2}i_1 j_1 - ni_1 j_1 \equiv nt_1 + t_2 - \frac{n(n-1)}{2}i_2 j_2 - ni_2 j_2 \pmod{m}.$$

This is equivalent to

$$n(i_1 j_2 - i_2 j_1) \equiv 0 \pmod{m}.$$

Now since this holds for all $x, y \in G$, $m | n$. 

References