

On Expectation of Generating Certain Finite Nilpotent Groups

Khaled Alajmi

Department of Mathematics, Public Authority for Applied Education and Training, Ardiyah, Kuwait.

How to cite this paper: Khaled Alajmi. (2024) On Expectation of Generating Certain Finite Nilpotent Groups. *Journal of Applied Mathematics and Computation*, 8(2), 113-119.
DOI: 10.26855/jamc.2024.06.003

Received: May 18, 2024

Accepted: June 15, 2024

Published: July 12, 2024

***Corresponding author:** Khaled Alajmi, Department of Mathematics, Public Authority for Applied Education and Training, Ardiyah, Kuwait.

Abstract

Let G be a finite group. Define $E(G)$ to be the expected number of elements of G which have to be drawn at random with replacement from G before a set of generators is found. The purpose of this paper is to compute $E(G)$ for certain nilpotent groups. This paper is divided into six sections. The first section is an introduction. In the second section we present the definition $\lambda_n(G)$ the probability that n elements drawn at random, with replacement from a finite group G generate G , and the definition $E(G)$ the expectation of the group G , that is the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found. In the third section we present some preliminaries and earlier results e.g if G is a group and $\Phi(G)$ is its Frattini subgroup. Then, $\lambda_n(G) = \lambda_n(G/\Phi(G))$. In section four, we computed $E(G)$ for certain nilpotent groups such as \mathbb{Z}_{p^4} , $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$ and $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. In section five, we computed $E(G)$ for a non-trivial example. The last section is a conclusion.

Keywords

Probability, expectation, nilpotent group, p -groups, Euler function

1. Introduction

In [1], V. Acciario computed the probability of generating some common families of finite groups and the function $E(G)$ for some common classes of groups, starting from the p -groups and the groups which are the direct product of groups of coprime order and also analyzed the class of nilpotent groups. The expectation function $E(G)$ is of great importance in describing certain algorithms for testing whether a group G generated by a given set of m permutations of degree n is regular *i.e* if its order and degree are equal. A survey of algorithms and the expected execution time of these algorithms to handle permutation groups has been studied in [2]. In this paper, we compute $E(G)$ for certain nilpotent groups. For more information refer to [3, 5, 7].

2. Definition

The following definitions have been taken from [4].

Definition 1. An ordered set (x_1, \dots, x_n) of n elements of a group G , not necessarily distinct which generates G is called an n -basis of G .

Definition 2. The n -th Eulerian function $\phi_n(G)$ is the number of distinct n -basis of G .

Note 3. If the group G cannot be generated by n elements, then $\phi_n(G) = 0$ and if G is cyclic of order n then $\phi_1(G) = \phi(G)$, where $\phi(n)$ is the ordinary Eulerian function of an integer.

Note 4. Let (g_1, \dots, g_n) be an n -tuple of G . Then either $G = \langle g_1, \dots, g_n \rangle$ or $H = \langle g_1, \dots, g_n \rangle$ where H is a subgroup of G . Hence one has the following fundamental identity

$$|G|^n = \sum_{H \leq G} \phi_n(H).$$

Definition 5. Let $\lambda_n(G)$ denote the probability that n elements drawn at random, with replacement from G generate G . Then one obtains

$$\lambda_n(G) = \frac{\phi_n(G)}{|G|^n}.$$

Definition 6. Let $E(G)$ denote the expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found.

The expectation function

$$E(G) = \sum_{d=1}^{\infty} d(\lambda_d(G) - \lambda_{d-1}(G))$$

where $\lambda_d(G) - \lambda_{d-1}(G)$ is the probability that $G = \langle g_1, \dots, g_d \rangle$ and $G \neq \langle g_1, \dots, g_{d-1} \rangle$.

3. Preliminaries and earlier results

Note 7. The following basic combinatorial identity that we will use to simplify the computation of $E(G)$.

$$\sum_{d=1}^{\infty} x^{d-1} = \left(\frac{x}{x-1}\right)^2,$$

where x is a real number greater than 1.

Lemma 8.

1. If G is a group and $\Phi(G)$ is its Frattini subgroup. Then

$$\lambda_n(G) = \lambda_n(G/\Phi(G)).$$

2. If G is a p -group with minimal number of generators d , then

$$\lambda_n(P^n) = \lambda_n(G),$$

where P is an elementary abelian group isomorphic to $G/\Phi(G)$ of order p^d .

3. If G and H are two finite groups of coprime order, then

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

4. If G is nilpotent group of order $p_1^{e_1}, \dots, p_k^{e_k}$, then

$$\lambda_d(G) = \prod_{i=1}^k \lambda_d(G_{p_i}),$$

where G_{p_i} is the p_i -Sylow subgroup of G .

Proof. See [3, problems 8.7, 8.26 and 8.22].

Lemma 9.

i) If G is a p -group with minimal number of generators d , then

(a) $\lambda_d(G) = \prod_{i=1}^d (1 - p^{-i})$

(b) If $k \leq 0$, the $\lambda_{d+k}(G) = \lambda_d(G) \prod_{i=1}^k \frac{p^i - p^{-d}}{p^i - 1}$

ii) If G is a cyclic group of order n , then

$$\lambda_d(G) = \prod_{p|n} \left(1 - \frac{1}{p^d}\right)$$

iii) If G is a p -group of order p^2 , then

$$\lambda_d(G) = \begin{cases} \frac{p^d - 1}{p^d} & \text{if } G \text{ is cyclic} \\ 1 - p^{-d+1} + p^{1-2d} - p^{-d} & \text{if } G \text{ is elementary abelian} \end{cases}$$

iv) If G is a group of order pq with p, q primes and $q < p$, then

$$(a) \lambda_d(G) = \begin{cases} \left(\frac{p^d-1}{p^d}\right)\left(\frac{q^d-1}{q^d}\right) & \text{if } q \nmid p-1 \\ 1 - \frac{1}{p^d} - p^{d-1} + \frac{p^{d-1}}{q^d} & \text{if } q|p-1 \end{cases}$$

Proof. See [1].

Note 7. The following basic combinatorial identity that we will use to simplify the computation of $E(G)$.

$$\sum_{d=1}^{\infty} x^{\frac{d}{x-1}} = \left(\frac{x}{x-1}\right)^2,$$

where x is a real number greater than 1.

Lemma 8.

1. If G is a group and $\Phi(G)$ is its Frattini subgroup. Then

$$\lambda_n(G) = \lambda_n(G/\Phi(G)).$$

2. If G is a p -group with minimal number of generators d , then

$$\lambda_n(P^n) = \lambda_n(G),$$

where P is an elementary abelian group isomorphic to $G/\Phi(G)$ of order p^d .

3. If G and H are two finite groups of coprime order, then

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

4. If G is nilpotent group of order $p_1^{e_1}, \dots, p_k^{e_k}$, then

$$\lambda_d(G) = \prod_{i=1}^k \lambda_d(G_{p_i}),$$

where G_{p_i} is the p_i -Sylow subgroup of G .

Proof. See [[3], problems 8.7, 8.26 and 8.22].

Lemma 9.

i) If G is a p -group with minimal number of generators d , then

$$(a) \lambda_d(G) = \prod_{i=1}^d (1 - p^{-i})$$

$$(b) \text{ If } k \leq 0, \text{ the } \lambda_{d+k}(G) = \lambda_d(G) \prod_{i=1}^k \frac{p^i - p^{-d}}{p^i - 1}$$

ii) If G is a cyclic group of order n , then

$$\lambda_d(G) = \prod_{p|n} \left(1 - \frac{1}{p^d}\right)$$

iii) If G is a p -group of order p^2 , then

$$\lambda_d(G) = \begin{cases} \frac{p^d - 1}{p^d} & \text{if } G \text{ is cyclic} \\ 1 - p^{-d+1} + p^{1-2d} - p^{-d} & \text{if } G \text{ is elementary abelian} \end{cases}$$

iv) If G is a group of order pq with p, q primes and $q < p$, then

$$(a) \lambda_d(G) = \begin{cases} \left(\frac{p^d-1}{p^d}\right)\left(\frac{q^d-1}{q^d}\right) & \text{if } q \nmid p-1 \\ 1 - \frac{1}{p^d} - p^{d-1} + \frac{p^{d-1}}{q^d} & \text{if } q|p-1 \end{cases}$$

Proof. See [1].

4. Main results

In this section, we compute $E(G)$ for certain abelian groups G of order p^4 namely $G \cong \mathbb{Z}_{p^4}$, $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ and these groups are nilpotent as they are abelian.

Proposition 10. Let $G \cong \mathbb{Z}_{p^4}$. Then $E(G) = \frac{p}{p-1}$.

Proof. By Lemma 9(ii), $\lambda_d(\mathbb{Z}_{p^4}) = \frac{p^d-1}{p^d}$ and hence by Definition 6

$$\begin{aligned} E(\mathbb{Z}_{p^4}) &= \sum_{d=1}^{\infty} d(\lambda_d(G) - \lambda_{d-1}(G)) \\ &= \sum_{d=1}^{\infty} d\left(\frac{p^d-1}{p^d} - \frac{p^{d-1}-1}{p^{d-1}}\right) \\ &= \sum_{d=1}^{\infty} \frac{d}{p^{d-1}}\left(\frac{p^d-1}{p} - p^{d-1} + 1\right) \\ &= \sum_{d=1}^{\infty} \frac{d}{p^{d-1}}\left(\frac{p-1}{p}\right) = \frac{p-1}{p}\left(\frac{p}{p-1}\right)^2, \end{aligned}$$

using the basic combinatorial identity in Note 7

$$= \frac{p}{p-1} \text{ (Compare with 4.11)}$$

Proposition 11. Let $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$, then $E(G) = \frac{2p^2+p}{p^2-1}$.

Proof. By Lemma 9(iv), $\lambda_d(G) = 1 - p^{-d+1} + p^{1-2d} - p^{-d}$ and hence by Definition 6 one has:

$$\begin{aligned} E(G) &= \sum_{d=1}^{\infty} d(1 - p^{-d+1} - p^{-d} + p^{1-2d}) - (1 - p^{-d+1} - p^{-d+1} + p^{3-2d}) \\ &= \sum_{d=1}^{\infty} dp^{-d}(p^2 - 1) + \sum_{d=1}^{\infty} dp^{1-2d}(1 - p^2) \\ &= p^{-1}(p^2 - 1) \sum_{d=1}^{\infty} \frac{d}{p^{d-1}} + p^{-1}(1 - p^2) \sum_{d=1}^{\infty} \left(\frac{d}{p^{2d-2}}\right) \frac{p(p^2 - 1)}{(p - 1)^2} - \frac{p(p^2)}{p^2 - 1} \end{aligned}$$

using the basic combinatorial identity in Note 7

$$= \frac{2p^2 + p}{p^2 - 1}. \text{ (Compare with 4.21)}$$

Proposition 12. Let $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p$, then $E(G) = \frac{2p^2+p}{p^2-1}$.

The group G is a p -group with minimal number of generators equal to two, that is $G \cong \langle b^p, a \rangle$ or $G \cong \langle a^p, a^i b \rangle$, $i = 0, 1, \dots, p - 1$. Therefore, the behavior of these groups is the same as the elementary abelian group $\mathbb{Z}_p \times \mathbb{Z}_p$ of order p^2 . Hence by Proposition 11, the claim follows

Remark 13. The group $G_2 = \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ has the following subgroups:

1. It has $p + 1$ cyclic subgroups of order p namely

$$\begin{aligned} \mathbb{Z}_p &\cong \langle a^p, b^{ip} \rangle, i = 1, 2, \dots, p. \\ \mathbb{Z}_p &\cong \langle b^p \rangle. \end{aligned}$$

2. It has $p^2 + p$ cyclic subgroups of order p^2 namely:

$$\begin{aligned} \mathbb{Z}_p^2 &\cong \langle ab^i \rangle, i = 1, 2, \dots, p^2. \\ \mathbb{Z}_p^2 &\cong \langle a^p b^j \rangle, j = 1, \dots, p - 1. \\ \mathbb{Z}_p^2 &\cong \langle b \rangle \end{aligned}$$

and one elementary abelian group of order p^2 that is $\mathbb{Z}_p \times \mathbb{Z}_p = \langle a^p b^p \rangle$

3. It has $p + 1$ subgroups of order p^3 of the form

$$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \cong \langle a^p, a^i b \rangle, i = 0, 1, \dots, p - 1.$$

$$\mathbb{Z}_{p^2} \times \mathbb{Z}_p \cong \langle b^p, a \rangle.$$

4. It has also two trivial subgroups.

For the above remark, see [3].

Proposition 14. Let $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p^2$, then

$$\lambda_d(G) = 1 - p^{-4d} [1 - (p + 1)(p^d - 1) - (p^{2+d} - p^{d+1})(p^d - 1) - (p + 2)(p^{2d} - p^{d+1} - p^d + p)].$$

Proof. By applying the identity $|G|^d = \sum_{H \leq G} \phi_d(G)$ in Note 4, Remark 13 and Lemma 9, one obtains

$$\phi_d(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}) = p^{4d} - 1 - (p + 1)(p^d - 1) - (p^2 + p)(p^d)(p^d - 1) - (p^{2d} - p^{d+1} - p^d + p) - (p + 1)(p^{2d} - p^{d+1} - p^d + p)$$

which implies

$$\lambda_d(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}) = \frac{\phi_d(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})}{p^{4d}}$$

and hence the claim.

Theorem 15. Let $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$. Then

$$E(G) = (p^2 + p - 1 - \frac{1}{p^2} - \frac{1}{p^3}) (\frac{p^4}{p^4 - 1})^2 + (3 - \frac{2}{p^2} + 2p + p^2) (\frac{p^2}{p^2 - 1})^2 + (\frac{5}{p^2} + \frac{2}{p} + 3 + 4p) (\frac{p^3}{p^3 - 1})^2$$

Proof. Apply Definition 6 and Proposition 14, one has

$$\begin{aligned} E(G) &= \sum_{d=1}^{\infty} d [(1 - p^{-4d} - p^{-4d}(p + 1)(p^d - 1) - p^{-4d}(p^{2+d} + p^{d+1})(p^d - 1) \\ &\quad - (p + 2)(p^{2d} - p^{d+1} - p^d + p)p^{-4d}) - (1 - p^{-4d+4} - p^{-4d+4}(p + 1)(p^{d-1} - 1) \\ &\quad - p^{-4d}(p^{2d} + p^{d+1})(p^d - 1) - (p + 2)(p^{2d} - p^{d+1} - p^d + p)p^{-4d}] \\ &= \sum_{d=1}^{\infty} dp^{-4d}(p^4 - 1) - \sum_{d=1}^{\infty} dp^{-3d}(p + 1) + \sum_{d=1}^{\infty} d(p + 1)p^{-4d} - \\ &\quad \sum_{d=1}^{\infty} dp^{-2d}(p^2 + p) + \sum_{d=1}^{\infty} dp^{-3d}(p^2 + p) - \sum_{d=1}^{\infty} d(p + 2)p^{-2d} + \\ &\quad \sum_{d=1}^{\infty} d(p + 2)p^{-3d+1} + \sum_{d=1}^{\infty} d(p + 2)p^{-3d} - \sum_{d=1}^{\infty} d(p + 2)p^{-4d+1} + \\ &\quad \sum_{d=1}^{\infty} d(p + 1)p^{-3d+3} - \sum_{d=1}^{\infty} d(p + 1)p^{-4d+4} + \sum_{d=1}^{\infty} d(p + 1)p^{-2d+3} - \\ &\quad \sum_{d=1}^{\infty} d(p + 1)p^{-4d+4} + \sum_{d=1}^{\infty} d(p + 2)p^{-2d+2} - \sum_{d=1}^{\infty} d(p + 2)p^{-3d+4} + \\ &\quad \sum_{d=1}^{\infty} d(p + 2)p^{-2d+2} - \sum_{d=1}^{\infty} d(p + 2)p^{-3d+4} - \sum_{d=1}^{\infty} d(p + 2)p^{-3d+3} + \\ &\quad \sum_{d=1}^{\infty} d(p + 2)p^{-4d+5} = A \sum_{d=1}^{\infty} dp^{-4d} + B \sum_{d=1}^{\infty} dp^{-2d} + C \sum_{d=1}^{\infty} dp^{-3d} \end{aligned}$$

where

$$\begin{aligned}
 A &= p^6 + p^5 - p^4 - p^2 - p \\
 B &= 3p^2 + 2p^3 + p^4 - 2 \\
 C &= p^5 + 4p^4 + 3p^3 + 2p^2 + 5p + 2
 \end{aligned}$$

Hence

$$\begin{aligned}
 E(G) &= Ap^{-4} \sum_{d=1}^{\infty} \frac{d}{(p^4)^{d-1}} + Bp^{-2} \sum_{d=1}^{\infty} \frac{d}{(p^2)^{d-1}} + Cp^{-3} \sum_{d=1}^{\infty} \frac{d}{(p^3)^{d-1}} \\
 &= Ap^{-4} \left(\frac{p^4}{p^4 - 1}\right)^2 + Bp^{-2} \left(\frac{p^2}{p^2 - 1}\right)^2 + Cp^{-3} \left(\frac{p^3}{p^3 - 1}\right)^2,
 \end{aligned}$$

using the basic combinatorial identity in Note 7. Hence the claim follows.

Remark 16. The abelian group $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_p$ has $3p + 5$ subgroups and these are $p + 1$ cyclic groups \mathbb{Z}_p of order p . There are $p + 1$ p -subgroups \mathbb{Z}_{p^2} or $\mathbb{Z}_p \times \mathbb{Z}_p$, $p + 1$ subgroups of type \mathbb{Z}_{p^3} or $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ and the trivial two subgroups G itself and the identity $\{e\}$. The computation $E(G)$ is similar to that of $E(\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2})$ in Theorem 15, as $\lambda_d(H)$ for the subgroup H of $G \cong \mathbb{Z}_{p^3} \times \mathbb{Z}_p$ is similar to that of $G \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, except the subgroup $\mathbb{Z}_{p^3} \times \mathbb{Z}_p$ which is a p -group with minimal number of generators is 3 , hence its behavior is the same as \mathbb{Z}_{p^3} [by Lemma 8 (ii), (iii)].

5. A non-trivial example

We conclude this paper with the computation of $E(G)$, where G is a nilpotent group, $G \cong G_{p_1} \times G_{p_2} \times G_{p_3}$, G_{p_i} is a p_i -Sylow subgroup of G . So

$$\begin{aligned}
 \lambda_d(G) &= \prod_{i=1}^3 \lambda_d(G_{p_i}) = \prod_{i=1}^3 \left(1 - \frac{1}{p_i^d}\right) = 1 - \sum_{d=1}^3 \frac{1}{p_i^d} + \sum_{1 \leq i < j \leq 3} \frac{1}{p_i^d p_j^d} - \frac{1}{p_1^d p_2^d p_3^d} \\
 E(G) &= \sum_{d=1}^{\infty} d(\lambda_d(G) - \lambda_{d-1}(G)) \\
 &= \sum_{d=1}^{\infty} d \left(\left(1 - \sum_{d=1}^3 \frac{1}{p_i^d} + \sum_{1 \leq i < j \leq 3} \frac{1}{p_i^d p_j^d} - \frac{1}{p_1^d p_2^d p_3^d}\right) - \left(1 - \sum_{d=1}^3 \frac{1}{p_i^{d-1}} + \sum_{1 \leq i < j \leq 3} \frac{1}{p_i^{d-1} p_j^{d-1}} - \frac{1}{p_1^{d-1} p_2^{d-1} p_3^{d-1}}\right) \right) \\
 &= \sum_{i=1}^3 \left(\sum_{d=1}^{\infty} \frac{d}{p_i^{d-1}} \left(1 - \frac{1}{p_i}\right) \right) - \sum_{1 \leq i < j \leq 3} \left(\sum_{d=1}^{\infty} \frac{d}{p_i^{d-1} p_j^{d-1}} \left(1 - \frac{1}{p_i p_j}\right) \right) + \left(\sum_{d=1}^{\infty} \frac{d}{p_1^{d-1} p_2^{d-1} p_3^{d-1}} \left(1 - \frac{1}{p_1 p_2 p_3}\right) \right) \\
 &= \sum_{i=1}^3 \left(1 - \frac{1}{p_i}\right) \left(\frac{p_i}{p_i - 1}\right)^2 - \sum_{1 \leq i < j \leq 3} \left(1 - \frac{1}{p_i p_j}\right) \left(\frac{p_i p_j}{1 - p_i p_j}\right)^2 + \left(1 - \frac{1}{p_1 p_2 p_3}\right) \left(\frac{p_1 p_2 p_3}{1 - p_1 p_2 p_3}\right)^2.
 \end{aligned}$$

So, if $|G| = 30$, then $G = G_2 \times G_3 \times G_5$ and

$$\begin{aligned}
 E(G) &= \left(1 - \frac{1}{2}\right)(4)^2 + \left(1 - \frac{1}{3}\right)\left(\frac{3}{2}\right)^2 + \left(1 - \frac{1}{5}\right)\left(\frac{5}{4}\right)^2 - \left(1 - \frac{1}{6}\right)\left(\frac{6}{5}\right)^2 - \left(1 - \frac{1}{10}\right)\left(\frac{10}{9}\right)^2 - \left(1 - \frac{1}{15}\right)\left(\frac{15}{14}\right)^2 + \left(1 - \frac{1}{30}\right)\left(\frac{30}{29}\right)^2 \\
 &\approx 1.470.
 \end{aligned}$$

6. Conclusion

This study shows that the methodology we have used to compute $E(G)$ is mainly, based on the the work of Acciaro, Eulerian function $\phi(G)$ and the basic combinatorial identity

$$\sum_{d=1}^{\infty} \frac{d}{x^{d-1}} = \left(\frac{x}{x - 1}\right)^2$$

Also, this study shows that the computations $E(G)$ for nilpotent groups requires to have good information about the

subgroup constructions of these groups in order to compute their Eulerian functions and then their $\lambda_n(G)$ and $E(G)$.

Acknowledgements

The author would like to thank PAAET for supporting this project No BE-23-07, and Professor Mashhour Bani-Ata for his helpful discussion and valuable remarks.

References

- [1] Acciaro, V. (1996). The probability of generating some common families of finite groups. *Utilitas Mathematica*, 49, 243-253.
- [2] Alhasanat, B. (2022). On classification of groups of order p^4 , p odd prime, *International Journal of Mathematics and Computer Science*, 17 no 4, 1564-1593.
- [3] Alhasanat, B. (2022). Some probabilistic approaches on finite groups, *International Journal of Applied Mathematics*, 35 NO.6, 827-838.
- [4] Atkinson, M. (1990). A survey of algorithms for handling permutation group. School of Computer Science Technical report SCS-TR-164, Carlton University, Ottawa, January.
- [5] Eberhard, S, Shumyatsky, P. (2023). Probabilistically nilpotent groups of class 2. *Mathematische Annalen*, doi.org 10.1007/500208-023-02567-0- accepted and to appear.
- [6] Hall, P. (1936). The Eulerian functions of a group. *Quart. J.Math., Ox. Series*, 7, 134-151.
- [7] Madadi, H. (2023). An upper bound for the probability of generating a finite nilpotent group, *Kyungpook Math. J.*, 63, 167-173.