GENERALIZED EXPONENT OF FINITE GROUPS

A. ABDOLLAHI, B. DAOUD, M. FARROKHI D. G., AND Y. GUERBOUSSA

ABSTRACT. A group G satisfies a positive polynomial identity of length n if there exist elements $g_1, \ldots, g_n \in G$ such that

$$x^{g_1} \ldots x^{g_n} = 1$$

for all $x \in G$. The minimum length of such an identity is called the generalized exponent of G. We compute the generalized exponent of a class of finite groups and apply it to show that every finitely generated solvable group of prime generalized exponent is a finite p-group. Consequently, we show that every finite group of generalized exponent 5 is a 5-group of exponent dividing 25.

1. Introduction

Assume G is an Ω-group, that is, Ω acts on G as a group of automorphisms. Following [6] a *polynomial* of length l on G with respect to Ω is a map $\mathfrak{p} : G \longrightarrow G$ defined as

$$\mathfrak{p}(g) = g^{\epsilon_1 \omega_1} \ldots g^{\epsilon_l \omega_l}$$

for all $g \in G$ in which $\omega_i \in \Omega$ and $\epsilon_i = \pm 1$, for all $i = 1, \ldots, l$. We note that the polynomial $\mathfrak{p}$ is a special case of the generalized words defined in [7]. The polynomial $\mathfrak{p}$ is called positive if $\epsilon_i = 1$, for all $i = 1, \ldots, l$. It is evident that for finite groups the notion of polynomials coincide with that of positive polynomials. The group G satisfies the polynomial $\mathfrak{p}$ if $\mathrm{img}\mathfrak{p} = \{1\}$. Accordingly, the *generalized exponent* of G with respect to Ω is defined as the minimum length of a positive polynomial it satisfies and it is denoted by $\mathrm{gexp}(G, \Omega)$. In the case $\Omega = G$, the number $\mathrm{gexp}(G, \Omega)$ is called the generalized exponent of G and it is denoted by $\mathrm{gexp}(G)$ for convenience. Clearly, the exponent of a group is the minimum length of a nontrivial positive polynomial word it satisfies as a 1-group, that is, $\exp(G) = \mathrm{gexp}(G, 1)$.

The notion of positive polynomials arises naturally in the theory of orderable groups where $g \neq 1$ implies $\mathfrak{p}(g) \neq 1$ for any element g of an orderable group G and any positive polynomial $\mathfrak{p}$ of G (see [3]). Accordingly, an element g of a group G is called *generalized periodic* provided that $\mathfrak{p}(g) = 1$ for some nontrivial positive polynomial $\mathfrak{p}$ of G. Hence an orderable group has no nontrivial generalized periodic elements. However, the converse to this problem is known to be false (see [1]).

Endimioni [2] considers the opposite problem that in which groups all elements are generalized periodic. Indeed, he studies groups having finite generalized exponents and describes those groups whose generalized exponents are small. Obviously, the only group of generalized exponent one is the trivial group. Also, a simple verification shows that the class of groups with generalized exponent two coincide with that of elementary abelian 2-groups. However, the structure of groups with

2000 *Mathematics Subject Classification.* Primary 05C75; Secondary 05C30, 05E18.
Key words and phrases. Generalized exponent, polynomial identity.

generalized exponents exceeding two is not much obvious as it will reveals in the following:

Theorem 1.1 (Endimioni [2]). *Let G be a group of generalized exponent 3. Then*
1. *G is 3-abelian;*
2. *$G^3 \subseteq Z(G)$;*
3. $\exp(G) = 3$ *or* 9*;*
4. *G is nilpotent of class ≤ 3.*

Theorem 1.2 (Endimioni [2]). *Let G be a group of generalized exponent 4. Then*
1. *G^4 is nilpotent of class ≤ 2;*
2. *G^8 is abelian.*

The aim of this paper is to extend the results of Edimioni to those finite groups having generalized exponent 5. To end this, we shall study a more general problem that which finite solvable groups satisfy positive polynomials of prime lengths.

2. Generalized exponents

Determining the generalized exponent of a (finite) group is not easy even if the group has small order. Indeed, the most easy cases to be considered are that of abelian groups as well as groups of prime exponents for which generalized exponents coincide with the exponents. We use these facts to compute the generalized exponent of yet another class of groups.

Lemma 2.1. *Assume a normal subset X of a group H satisfies a positive polynomial identity*

$$x^{k_1} \dots x^{k_l} = 1$$

with respect to a group K. Then X also satisfies the positive polynomial identity

$$x^{k_1^k} \dots x^{k_l^k} = 1$$

for all $k \in K$.

Proof. Conjugating the equation $x^{k_1} \dots x^{k_l} = 1$ by k and replacing x by $x^{k^{-1}}$ the result follows. □

Theorem 2.2. *Let $G = H \rtimes K$ be a finite group. Then*

$$\operatorname{gexp}(G) \leq \exp(K) \cdot \operatorname{gexp}(H, K).$$

Proof. Let $m = \exp(K)$ and $n = \operatorname{gexp}(H, K)$. Then there exist elements $k_1, \dots, k_n \in K$ such that

$$h^{k_1} \dots h^{k_n} = 1$$

for all $h \in H$. Since $g^m \in H$ for all $g \in G$, it follows that

$$g^{mk_1} \dots g^{mk_n} = 1$$

for all $g \in G$. Therefore $\operatorname{gexp}(G) \leq mn$, as required. □

Theorem 2.3. *Assume $G = H \rtimes K$ is a finite group, in which H is a minimal normal Sylow p-subgroup and K is a Sylow q-subgroup of G, respectively. Then*

$$\operatorname{gexp}(G) \geq \exp(Z(K)) \cdot \operatorname{gexp}(H, K).$$

Proof. Suppose $\mathrm{gexp}(G) = n$. Then G satisfies a positive polynomial identity

$$g^{g_1} \dots g^{g_n} = 1$$

of length n. Let $g_i = h_i k_i$ for $i = 1, \dots, n$, in which $h_i \in H$ and $k_i \in K$. Clearly, $n = q^e m$ for some $m \geq 1$ in which $q^e = \exp(Z(K))$. Let $y \in Z(K)$ be an element of order q^e. For $x \in H$ and $i = 0, \dots, q^e - 1$, we have

$$(y^i x)^{g_1} \dots (y^i x)^{g_n} = 1,$$

which implies that

$$x^{g_1 y^{ig_2} \dots y^{ig_n}} \dots x^{g_{n-1} y^{ig_n}} x^{g_n} = 1.$$

Since H is abelian and $y \in Z(K)$, it follows that

$$x^{g_1 y^{i(n-1)}} \dots x^{g_{n-1} y^i} x^{g_n} = 1.$$

Writing H additively and looking at y as an operator of H, we observe that $YX = 0$ in which

$$X = \begin{bmatrix} w_1(g_1, \dots, g_n; x) \\ \vdots \\ w_{q^e}(g_1, \dots, g_n; x) \end{bmatrix}, \qquad Y = \begin{bmatrix} 1 & \cdots & 1 & 1 \\ y^{q^e-1} & \cdots & y & 1 \\ \vdots & \ddots & \vdots & \vdots \\ y^{(q^e-1)^2} & \cdots & y^{q^e-1} & 1 \end{bmatrix}$$

and $w_i(g_1, \dots, g_n; x) = x^{g_i} x^{g_{i+q^e}} \dots x^{g_{i+(m-1)q^e}}$, for $i = 1, \dots, q^e$. Let

$$H_i = \langle w_i(g_1^k, \dots, g_n^k; h) : h \in H, k \in K \rangle$$

for $i = 1, \dots, q^e$. By Lemma 2.1, H_i is a normal subgroup of G and hence $H_i = 1$ or H, for $i = 1, \dots, q$. Suppose $H_i = H$ for some i. If Y^* denotes the adjoint of Y, then $\det(Y)X = Y^*YX = 0$ yielding $\det(Y) = 0$ as $h \in H$ and $k \in K$ were arbitrary. On the other hand,

$$\det(Y) = \prod_{0 \leq i < j \leq q^e-1} (y^j - y^i) = y^d \prod_{1 \leq i \leq q^e-1} (y^i - 1)^{q^e-i}$$

for some d, which yields $\prod_{1 \leq i \leq q^e-1} (y^i - 1)^{q^e-i} = 0$ as y is non-singular. Let δ be the least common multiple of all numbers $\leq q^e$ coprime to q. Clearly, the polynomial $\prod_{1 \leq i \leq q^e-1} (t^i - 1)^{q^e-i}$ divides some power of $t^{q^{e-1}\delta} - 1$ so that $y^{q^{e-1}\delta} - 1$ is nilpotent. Being element of $GF(p)\langle y \rangle$, it follows that $y^{q^{e-1}\delta} - 1 = 0$ (see [5, 8.2.1]). Hence $y^{q^{e-1}} = 1$, which is a contradiction. Therefore $H_i = 1$ for all $i = 1, \dots, q^e$, which implies that

$$h^{k_i} h^{k_{i+q^e}} \dots h^{k_{i+(m-1)q^e}} = w_i(k_1, \dots, k_n; h) = 1$$

for $i = 1, \dots, q^e$. Hence $m \geq \mathrm{gexp}(H, K)$ by definition. The proof is complete. □

The above lower and upper bounds yield us the following results:

Corollary 2.4. *Assume $G = H \rtimes K$ is a finite group, in which H is a minimal normal Sylow p-subgroup and K is a Sylow q-subgroup of G, respectively. If, in addition,* $\exp(K) = \exp(Z(K))$ *then*

$$\mathrm{gexp}(G) = \exp(Z(K)) \cdot \mathrm{gexp}(H, K).$$

A Frobenius is said to be *minimal* if it contains no proper Frobenius subgroup.

Corollary 2.5. *Let G be a minimal Frobenius group. Then*

$$\mathrm{gexp}(G) = |H| \cdot \mathrm{gexp}(N, H),$$

in which H and N are a Frobenius complement and the Frobenius kernel of G, respectively. Moreover, $\mathrm{gexp}(N, H)$ *is the minimum coefficient sum among all multiples of the minimal polynomial of a generator of H on N whose coefficients are non-negative integers.*

Proof. Assume H and N are as in the Corollary. Clearly, N is a minimal normal p-subgroup of G and H is a group of prime order $q \neq p$. Hence the equality holds by Corollary 2.4. To complete the proof, let $m = \mathrm{gexp}(N, H)$ and let h be a generator of H. Then there exist integers $0 \leq t_i < q$ such that

$$x^{h^{t_1}} \ldots x^{h^{t_m}} = 1$$

for all $x \in N$. Let $\mathfrak{p}$ be a polynomial defined as $\mathfrak{p}(x) = x^{t_1} + \cdots + x^{t_m}$. Clearly, h acts on N as a linear transformation and that $\mathfrak{p}$ is a multiple of the minimal polynomial of h with positive coefficients. Conversely, any such a polynomial gives rise to a positive polynomial identity for N with respect to H to which N satisfies, as required. □

Example. Utilizing the above corollary, one can verify that $\mathrm{gexp}(A_4) = 6$. This shows that there are groups other than abelian groups and those of prime exponents whose generalized exponents coincide with their exponents. Also, $\mathrm{gexp}(C_7 \rtimes C_3) = 9$, $\mathrm{gexp}(C_{11} \rtimes C_5) = 15$ etc.

3. Groups satisfying a positive polynomial identity of prime length

A well-known result in abstract group theory states that every finite group of prime power exponent is nilpotent. In what follows, we show that the same result holds for finite solvable groups of prime generalized exponent. Utilizing this result, we also show that every finite group of generalized exponent 5 is nilpotent as well.

Theorem 3.1. *Every finitely generated solvable group satisfying a positive polynomial identity of prime length is a finite p-group.*

Proof. Suppose on the contrary that G is a finitely generated solvable group satisfying a positive polynomial identity $\mathfrak{p} = 1$ of prime length p and that G is not a p-group. Clearly, G is not nilpotent. First assume that G is finite and let $\overline{G}$ be a non-nilpotent quotient of G of minimum order. From [5, Excercise 9.2.7], we observe that $\overline{G} = \overline{Q} \rtimes \overline{H}$, in which $\overline{Q}$ is a minimal normal q-subgroup of $\overline{G}$ and $\overline{H}$ is a q'-group acting faithfully on $\overline{Q}$. Since $\overline{G}/\overline{Q}$ is nilpotent, $\overline{H}$ is a p-group. Then, by Theorem 2.3,

$$\mathrm{gexp}(G) \geq \mathrm{gexp}(\overline{G}) \geq p \cdot \mathrm{gexp}(\overline{Q}, \overline{H}) > p,$$

which is a contradiction.

Finally, assume G is infinite. Clearly, $\overline{G} = G/G''$ has the same property as G does. Being a finitely generated abelian group of finite exponent, $\overline{G}/\overline{G}'$ is a finite group, hence $\overline{G}'$ is a finitely generated abelian group. Let q be a prime not dividing $|\overline{G}/\overline{G}'|$. Then $\overline{G}/\overline{G}'^q$ is a finite solvable group satisfying a positive polynomial identity of length p, which is not a p-group, a contradiction. □

Corollary 3.2. *A solvable group satisfying a positive polynomial identity of prime length is a p-group.*

In order to show that a finite group satisfying a positive polynomial identity of prime length is nilpotent, it is now enough to show that it is a solvable group. The following result gives a criterion for the solvability of the corresponding group.

Proposition 3.3. *Assume a finite group G satisfies a positive polynomial identity $x^{g_1}\dots x^{g_p}=1$ of prime length. Then G is solvable if and only if $\langle g_1,\dots,g_p\rangle$ is solvable.*

Proof. Assume $H=\langle g_1,\dots,g_p\rangle$ is solvable. Since H satisfies the positive polynomial identity $x^{g_1}\dots x^{g_p}=1$, it is a p-group by Theorem 3.1. Let P be a Sylow p-subgroup of G containing $g_1,\dots,g_p$. For $g\in N_G(P)$, the solvable group $\langle P,g\rangle$ satisfies the positive polynomial identity $x^{g_1}\dots x^{g_p}=1$ so that it is a p-group and hence $g\in P$. Thus $N_G(P)=P$ and by Guralnick-Malle-Navarro theorem in [4], G is solvable. The converse is obvious. □

Lemma 3.4 ([2]). *Let G be a group satisfying a positive polynomial identity of length n. Then G satisfies the positive polynomial identity*

$$x^2x^{g_1}\dots x^{g_{n-2}}=1$$

for some elements $g_1,\dots,g_{n-2}\in G$.

Theorem 3.5. *Every finite group satisfying a positive polynomial identity of prime length $p\le 5$ is a p-group of exponent dividing p^2.*

Proof. Let G be a group satisfying a positive polynomial identity of prime length $p\le 5$. For $p=2$ the group G is elementary abelian and we are done. Also, by Theorem 1.1, the result holds for $p=3$. Hence assume that $p=5$. We claim that G is a p-group. Indeed, by Theorem 3.1, it is enough to show that G is solvable. Suppose G is a minimal counter-example. Clearly, G has no nontrivial abelian normal subgroup. Then $\mathrm{Soc}(G)$ is a direct product of non-abelian finite simple groups so that $C_G(\mathrm{Soc}(G))=1$. If I is the subgroup of G generated by involutions, then $\mathrm{Soc}(G)\subseteq I$ so that $C_G(I)=1$.

By Lemma 3.4, there exist elements $a,b,c\in G$ such that

$$x^2x^ax^bx^c=1$$

for all $x\in G$. We proceed in some steps.

(1) $[\beta\alpha^{-1},\gamma\alpha^{-1}]=1$ when $\{\alpha,\beta,\gamma\}=\{a,b,c\}$.

To end this, choose any involution $x\in G$. We observe that $x^ax^bx^c=1$ so that $xx^ux^v=1$ in which $u=ba^{-1}$ and $v=ca^{-1}$. By Lemma 2.1, we obtain $xx^ux^{v^u}=1$, which implies that $x^v=x^{v^u}$. Hence $[u,v^{-1}]\in C_G(x)$. Since this is hold for all involutions x, it follows that $[u,v^{-1}]\in C_G(I)=1$, as required. The other two cases are proved analogously.

(2) $[ca,bc^{-3}]=[ca,a^2b^{-1}a]=1$.

We use the proof of [2, Lemma 2.2]. Write the equality $x^2x^ax^bx^c=1$ as

$$x^2a^{-1}xab^{-1}xbc^{-1}xc=1.$$

Applying the transformation $x\mapsto c^{-1}x$ yields

$$x^2c^{-1}xa^{-1}c^{-1}xab^{-1}c^{-1}xbc^{-2}=1,$$

which simplifies to

$$x^2x^cx^{cac}x^{bc^{-2}} = 1.$$

Hence $[ca, bc^{-3}] = [cac \cdot c^{-1}, bc^{-2} \cdot c^{-1}] = 1$ by (1). In the same way, by applying the transformation $x \mapsto ax$, one gets

$$x^2ab^{-1}axbc^{-1}axcaxa = 1,$$

which simplifies to

$$x^2x^{a^{-1}ba^{-1}}x^{ca^2}x^a = 1.$$

Thus $[ca, a^{-1}ba^{-2}] = [ca^2 \cdot a^{-1}, a^{-1}ba^{-1} \cdot a^{-1}] = 1$ by (1) so that $[ca, a^2b^{-1}a] = 1$.

(3) $\langle a, b, c\rangle$ is an elementary abelian 5-group.

One can verify that the group

$$\langle \alpha, \beta, \gamma : \alpha^2\alpha^\alpha\alpha^\beta\alpha^\gamma = \beta^2\beta^\alpha\beta^\beta\beta^\gamma = \gamma^2\gamma^\alpha\gamma^\beta\gamma^\gamma = [\beta\alpha^{-1}, \gamma\alpha^{-1}] = [\gamma\alpha, \beta\gamma^{-3}] = [\gamma\alpha, \alpha^2\beta^{-1}\alpha] = 1\rangle$$

is elementary abelian of order 5^3. As a quotient of $\langle \alpha, \beta, \gamma\rangle$, the group $\langle a, b, c\rangle$ is an elementary abelian 5-group, as required.

Now, by Proposition 3.3, the group G is solvable, which contradicts the assumption. Therefore G is a p-group. To prove $\exp(G)$ divides 25, we use the NQ package of GAP [8]. The following codes show that the largest nilpotent quotient $\overline{H}$ of the group $H = \langle a, b, c, x; g : g^2g^ag^bg^c = 1\rangle$ of generalized exponent 5 is a finite 5-group, in which the element $\overline{x} = x\overline{H}$ has order 25. This shows that every element of G has order dividing 25. The proof is complete. □

```
LoadPackage("nq");
F:=FreeGroup(5);
g:=F.1;a:=F.2;b:=F.3;c:=F.4;x:=F.5;
T:=F/[g^a*g^b*g^c*g^2];
H:=NilpotentQuotient(G,[g]);
Order(H.4);
25
```

The results obtained in this section suggest us to pose the following conjecture.

Conjecture 3.6. *Every nontrivial finite group satisfying a positive polynomial identity of prime length is nilpotent.*

Notice that a nilpotent group satisfying a positive polynomial identity of prime length is always a p-group. Here we pose another conjecture describing the exponent of such groups.

Conjecture 3.7. *The exponent of a nontrivial finite p-group satisfying a positive polynomial identity of length p is bounded above by p^2.*

While it seems the groups satisfying a positive polynomial identity of prime length are restricted in structure, the situation is completely different for those groups satisfying a positive polynomial identities of non-prime lengths. To see this, let $\mathfrak{B}_n$ denote the class of all groups satisfying a positive polynomial identity of length n.

Theorem 3.8. *The class $\mathfrak{B}_{n^2}$ contains an infinite finitely generated solvable group for every natural number n.*

Proof. It is known that the $(n-1)\times(n-1)$ matrix

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & -1 \\ 1 & 0 & \cdots & 0 & -1 \\ 0 & 1 & \cdots & 0 & -1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -1 \end{bmatrix}$$

satisfies the equation $A^{n-1} + \cdots + A + I = 0$ so that $A^n = I$. Consider the group $G = \mathbb{Z}^{n-1} \rtimes \langle A \rangle$ in which A acts on $\mathbb{Z}^{n-1}$ in the natural way. A simple verification shows that G is an infinite finitely generated metabelian group satisfying the identity

$$x^{nA^{n-1}} \dots x^{nA} x^n = 1$$

of length n^2. Hence $G \in \mathfrak{B}_{n^2}$, as required. □

Corollary 3.9. *The class $\mathfrak{B}_{n^2}$ contains a finite solvable group of exponent divisible by any given number for every natural number n.*

Proof. Let $G = \mathbb{Z}^{n-1} \rtimes \langle A \rangle$ be the group defined in Theorem 3.8. Then $G/m\mathbb{Z}^{n-1} \in \mathfrak{B}_{n^2}$ is a finite group of exponent mn for any m, as required. □

Acknowledgment

The research of the first author was in part supported by a grant (No. 94050219) from School of Mathematics, Institute for Research in Fundamental Sciences (IPM). The research of the first author is also financially supported by the Center of Excellence for Mathematics, University of Isfahan. The second author would like to thank IPM-Isfahan for kind hospitality during his stay in the Institute of Mathematics in Isfahan.

References

[1] V. V. Bludov, An example of an unorderable group with strictly isolated identity, *Algebra Logic* **11** (1972), 341–349.
[2] G. Endimioni, On certain classes of generalized periodic groups, *Ischia Group Theory* (2006), 93–102, World Sci. Publ., Hackensack, NJ, 2007.
[3] L. Fuchs, *Partially Ordered Algebraic Systems*, Pergamon Press, London, 1963.
[4] R. M. Guralnick, G. Malle and G. Navarro, Self-normalizing Sylow subgroups, *Proc. Amer. Math. Soc.* **132**(4) (2004), 973–979.
[5] D. J. S. Robinson, *A Course in the Theory of Groups*, Second Edition, Springer-Verlag, 1996.
[6] D. Schweigert, Polynomautomorphismen auf endlichen Gruppen, *Arch. Math.* **29** (1977), 34–38.
[7] D. Segal, *Words: Notes on Verbal Width in Groups*, London Mathematical Society Lecture Note Series, Cambridge University Press, Cambridge, 2009.
[8] The GAP Group, *GAP-Groups, Algorithms and Programming, Version 4.7.9, 2015* (http://www.gap-system.org/).

Department of Mathematics, University of Isfahan, Isfahan 81746-73441, Iran and School of Mathematics, Institute for Research in Fundamental Sciences (IPM), P. O. Box 19395-5746, Tehran, Iran
E-mail address: a.abdollahi@math.ui.ac.ir

Department of Mathematics, Laboratory of Fundamental and Numerical Mathematics, Ferhat Abbas University, Setif 1, Algeria
E-mail address: boun_daoud@yahoo.fr

Mathematical Science Research Unit, College of Liberal Arts, Muroran Institute of Technology, 27-1, Mizumoto, Muroran 050-8585, Hokkaido, Japan
E-mail address: m.farrokhi.d.g@gmail.com

Department of Mathematics, University Kasdi Merbah Ouargla, Ouargla, Algeria
E-mail address: yassine_guer@hotmail.fr