# LARGE $p$-GROUPS WITHOUT PROPER SUBGROUPS WITH THE SAME DERIVED LENGTH

ELEONORA CRESTANI AND ANDREA LUCCHINI

Abstract. We construct a subgroup $H_d$ of the iterated wreath product $G_d$ of $d$ copies of the cyclic group of order $p$ with the property that the derived length and the smallest cardinality of a generating set of $H_d$ are equal to $d$ while no proper subgroup of $H_d$ has derived length equal to $d$. It turns out that the two groups $H_d$ and $G_d$ are the extreme cases of a more general construction that produces a chain $H_d = K_1 < \cdots < K_{p-1} = G_d$ of subgroups sharing a common recursive structure. For $i \in \{1, \dots, p-1\}$, the subgroup $K_i$ has nilpotency class $(i+1)^{d-1}$.

## 1. Introduction

Certain properties of a finite group can be detected from its 2-generated subgroups. For example, a deep theorem of Thompson says that $G$ is soluble if and only if every 2-generated subgroup of $G$ is soluble. Influenced by these results, one could be tempted to conjecture that there exists a positive integer $c$ with the property that every finite soluble group contains a $c$-generated subgroup with the same derived length. This is false. Consider the iterated wreath product $G_d = C_p \wr \cdots \wr C_p$ of $d$ copies of the cyclic group of order $p$. The derived length of $G_d$ is equal to $d$ and coincides with the smallest cardinality of a generating set. However, if $p = 2$, then every proper subgroup of $G_d$ has derived length smaller than $d$ (see, for example, [2, Lemma 2]), so $d$ elements are really needed to generate a subgroup with derived length equal to $d$. On the other hand, if $p \neq 2$, then $G_d$ contains several proper subgroups with the same derived length and the following questions arise. Does a counterexample to the previous conjecture exist when $p \neq 2$? Does such counterexample appear among the subgroups of $G_d$? The aim of this paper is to answer to the previous two questions.

**Theorem 1.** *For any prime $p$, there exist $d$ elements $x_1, \dots, x_d \in G_d$ such that the subgroup $H_d = \langle x_1, \dots, x_d \rangle$ of $G_d$ generated by these elements has the following properties:*

*(1) the derived length of $H_d$ is $d$;*
*(2) $H_d$ cannot be generated by $d-1$ elements;*
*(3) no proper subgroup of $H_d$ has derived length equal to $d$.*

The interest on $p$-groups without proper subgroups with the same derived length has been related with the problem of bounding the order of a finite $p$-group in terms of its derived length (a long history starting from Burnside's papers, see [5] for more details). Mann [4] showed that if $G$ is a finite $p$-group, then $G^{(d)} \neq 1$ implies

1991 *Mathematics Subject Classification.* 20D15.
*Key words and phrases.* $p$-groups, derived length, generators.

$\log_p |G| > 2^d + 2d - 2$. For primes at least 5, groups of length $d$ and order $p^{2^d-2}$ were constructed in [1], improving previous examples of Hall of order $p^{2^d-1}$ for all odd primes (see [3, III.17.7]). These examples can be generated by 2 elements; our interest goes in a different direction: indeed we want to produce examples of $p$-groups without proper subgroups of the same derived length but with large elementary abelian factors. As a consequence the order of $H_d$ is large with respect to the lower bound proved by Mann (a detailed investigation of the order of $H_d$ is done in section 4). However $H_d$ has other minimality properties. It is well known that if a nilpotent group has derived length $d$, then its nilpotency class is at least $2^{d-1}$. The nilpotency class of $H_d$ is precisely $2^{d-1}$, the smallest possible value. It follows also that no proper factor group of $H_d$ has the same derived length as $H_d$.

Our study of the properties of the group $H_d$ is made possible by a particular choice of the notations: the group $G_d$ acts on the $p^d$-dimensional vector space $V_d$ over the field with $p$-elements and $G_{d+1} = V_d \rtimes G_d$. In section 2 we define a map $\gamma_d : \{0, \dots, p-1\}^d \to V_d$ with the property that the image $\Gamma_d = \gamma_d(\{0, \dots, p-1\}^d)$ is a basis for $V_d$ over $F$. We have $G_d = V_{d-1} \rtimes (V_{d-2} \rtimes \cdots \rtimes V_0)$ and $H_d = \langle x_1, \dots, x_d \rangle$ with $x_i = \gamma_{i-1}(1, \dots, 1) \in V_{i-1}$. An easy formula (see in particular Lemma 3) allows to express, for any $\omega \in \Gamma_d$ and $i \in \{1, \dots, d-1\}$, the commutator $[\omega, x_i]$ as a linear combination of the elements of $\Gamma_d$. In section 5 we discuss a generalization of this construction. For $k \in \{1, \dots, p-1\}$ we can consider the subgroup $X_{k,d} = \langle x_{k,1}, \dots, x_{k,d} \rangle$ of $G_d$ with $x_{k,i} = \gamma_{i-1}(k, \dots, k)$. If $p = 2$, then $H_d = G_d$. Otherwise

$$H_d = X_{1,d} < X_{2,d} < \cdots < X_{p-2,d} < X_{p-1,d} = G_d.$$

This approach allows to study simultaneously the groups $X_{k,d}$ for the different values of $k$: for example the nilpotency class of these groups can be determined with a unified argument: we prove that the nilpotency class of $X_{k,d}$ coincides with $(k+1)^{d-1}$ (see Theorem 30).

## 2. Notations and preliminary results

We fix the following notations: $p$ is a prime number, $F$ is a field with $p$ elements and $V_n = F^{p^n}$ is a vector space over $F$ of dimension $p^n$. For each positive integer $n$, we define a function $\beta_n : V_{n-1} \times \mathbb{N} \to V_n$ as follows: if $v = (a_1, \dots, a_{p^{n-1}})$ then

$$\begin{aligned}\beta_n(v, m) &= (0^m v, 1^m v, \dots, (p-1)^m v)\\ &= (0^m a_1, \dots, 0^m a_{p^{n-1}}, \dots, (p-1)^m a_1, \dots, (p-1)^m a_{p^{n-1}}).\end{aligned}$$

Notice that if $a_1, a_2$ are positive integers and $a_1 \equiv a_2 \mod p-1$, then $\beta_n(v, a_1) = \beta_n(v, a_2)$. However if $t$ is a positive integer, then $\beta_n(v, 0) - \beta_n(v, t(p-1)) = (v, 0, \dots, 0)$. Given $a \in \mathbb{N}$, we define $\overline{a}$ as follows: if $a = 0$, then $\overline{a} = 0$; otherwise $\overline{a}$ is the unique integer with $1 \leq \overline{a} \leq p-1$ and $\overline{a} \equiv a \mod p-1$. With this notation it turns out that $\beta_n(v, a) = \beta_n(v, \overline{a})$ for any $a \in \mathbb{N}$. Now, for every positive integer $n$, we define a function

$$\gamma_n : \mathbb{N}^n \to V_n = F^{p^n}$$

in the following way:

$$\begin{cases}\gamma_1(a) = \beta_1(1, a) = (0^a, 1^a, \dots, (p-1)^a)\\ \gamma_n(a_1, \dots, a_n) = \beta_n(\gamma_{n-1}(a_1, \dots, a_{n-1}), a_n) \text{ if } n > 1.\end{cases}$$

Let $I_p = \{0, \dots, p-1\} \subseteq \mathbb{N}$. Since $\gamma_n(a_1, \dots, a_n) = \gamma_n(\overline{a}_1, \dots, \overline{a}_n)$, we have that $\gamma_n(\mathbb{N}^n) = \gamma_n(I_p^n)$. Notice that for any choice of $(a_1, \dots, a_n)$ in $I_p^n$, $\gamma_n(a_1, \dots, a_n)$ is a non zero vector (for example $\gamma_1(0) = (1, \dots, 1)$). Moreover, a stronger result holds. Indeed we have:

**Lemma 2.** *The set $\Gamma_n = \{\gamma_n(u) \,|\, u \in I_p^n\}$ is a basis for the vector space $V_n$ over $F$.*

*Proof.* We use the fact that any $v \in \Gamma_n$ can be uniquely written in the form $v = \beta_n(w, a)$ with $w \in \Gamma_{n-1}$ and $a \in I_p$. Now, for $w \in \Gamma_{n-1}$ and $a \in I_p$, let $\lambda_{w,a}$ be elements of $F$ such that

$$\sum_{w,a} \lambda_{w,a} \beta_n(w, a) = 0.$$

For $1 \le i \le p$, we have a linear map $\rho_i : V_n \to V_{n-1}$ defined by $\rho_i(a_1, \dots, a_{p^n}) = (a_{1+(i-1)p^{n-1}}, \dots, a_{p^{n-1}+(i-1)p^{n-1}})$. In particular, since $\rho_i(\beta_n(w, a)) = (i-1)^a w$, we get that

$$0 = \rho_i\left(\sum_{w,a} \lambda_{w,a}\beta_n(w,a)\right) = \sum_{w,a} \lambda_{w,a}(i-1)^a w = \sum_{w} \left(\sum_{a} \lambda_{w,a}(i-1)^a\right) w.$$

By induction, the vectors of $\Gamma_{n-1}$ are linearly independent, so for each $w \in \Gamma_{n-1}$ and each $j \in \{0, \dots, p-1\}$, we have that

$$\sum_{a \in I_p} \lambda_{w,a} j^a = 0.$$

This means that $(\lambda_{w,0}, \dots, \lambda_{w,p-1})$ is a solution of the homogeneous linear system associated to the matrix

$$A := \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 2^2 & \cdots & 2^{p-1} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & p-1 & (p-1)^2 & \cdots & (p-1)^{p-1} \end{pmatrix}.$$

Since $A$ is an invertible matrix, we get that $\lambda_{w,a} = 0$ for each $w \in \Gamma_{n-1}$ and $a \in I_p$. □

We use the previous definition to construct a sequence of vectors $x_n \in V_{n-1}$ :

$$\begin{cases} x_1 = 1 \\ x_{n+1} = \gamma_n(1, \dots, 1) = \beta_n(x_n, 1) \text{ if } n > 0. \end{cases}$$

Now we start to work in the iterated wreath product $G_d = C_p \wr C_p \wr \cdots \wr C_p$, where $C_p$ appears $d$-times. Clearly $G_1 \cong V_0$ while, if $d \ge 1$, then $V_{d-1}$ can be identified with the base subgroup of the wreath product $G_d = C_p \wr G_{d-1} = V_{d-1} \rtimes G_{d-1}$. In particular $x_1, \dots, x_d$ can be viewed as elements of $G_d$.

Our aim is to study the subgroup $H_d = \langle x_1, \dots x_d \rangle$ of $G_d$ generated by these elements. Notice that $V_0 = H_1 = G_1 \cong C_p$ while, if $d \ge 2$, then $H_d = W_{d-1} \rtimes H_{d-1}$, where $W_{d-1}$ is the $H_{d-1}$-submodule of $V_{d-1}$ generated by $x_d$.

**Lemma 3.** *Let $v = \gamma_d(a_1, \dots, a_d) \in V_d$, with and $i \le d$. Consider $k = (d-i)+1$. If $t$ is a positive integer, then*

$$[v, tx_i] = \begin{cases} 0 \ \textit{if } a_k = 0 \\ \sum_{1 \le c \le \overline{a_k}} \binom{\overline{a_k}}{c} (-t)^c \gamma_d(a_1, \dots, a_{k-1}, \overline{a_k} - c, a_{k+1} + c, \dots, a_d + c) \ \textit{otherwise.} \end{cases}$$

*Proof.* Since $\gamma_d(a_1,\dots,a_d)=\gamma_d(\overline{a}_1,\dots,\overline{a}_d)$, we may assume $0\le a_j\le p-1$ for all $j\in\{1,\dots,d\}$. First we prove this lemma for $i=1$. Notice that if $w_1,\dots,w_p\in V_{d-1}$, then

$$(w_1,\dots,w_p)^{x_1}=(w_p,w_1,\dots,w_{p-1}).$$

In our particular case, since $v=\beta_d(w,a)$ for $w=\gamma_{d-1}(a_1,\dots,a_{d-1})$, we get that

$$\begin{aligned}[v,tx_1]=&-(0^{a_d}w,1^{a_d}w,\dots,(p-1)^{a_d}w)+(0^{a_d}w,1^{a_d}w,\dots,(p-1)^{a_d}w)^{tx_1}\\ =&(((-t)^{a_d}-0^{a_d})w,\dots,((i-t)^{a_d}-i^{a_d})w,\dots,((p-1-t)^{a_d}-(p-1)^{a_d})w).\end{aligned}$$

If $a_d=0$, then $[v,tx_1]=0$. Otherwise, since $(i-t)^{a_d}-i^{a_d}=\sum_{0\le b\le a_d-1}\binom{a_d}{b}(-t)^{a_d-b}i^b$, we deduce

$$\begin{aligned}[v,tx_1]&=\sum_{0\le b\le a_d-1}\binom{a_d}{b}(-t)^{a_d-b}\gamma_d(a_1,\dots,a_{d-1},b)\\ &=\sum_{1\le c\le a_d}\binom{a_d}{c}(-t)^{c}\gamma_d(a_1,\dots,a_{d-1},a_d-c).\end{aligned}$$

Now assume $i>1$. Since $v=\beta_d(\gamma_d(a_1,\dots,a_{d-1}),a_d)$ and $tx_i=t\beta(x_{i-1},1)$ we have

$$[v,tx_i]=(w_1,\dots,w_p)$$

with

$$w_j=[(j-1)^{a_d}\gamma_{d-1}(a_1,\dots,a_{d-1}),(t\cdot(j-1))x_{i-1}]\in V_{d-1}.$$

By induction

$$\begin{aligned}w_j=&(j-1)^{a_d}\sum_{1\le c\le a_k}\binom{a_k}{c}(-t(j-1))^c\gamma_{d-1}(a_1,\dots,a_{k-1},a_k-c,a_{k+1}+c,\dots,a_{d-1}+c)\\ =&\sum_{1\le c\le a_k}\binom{a_k}{c}(-t)^c(j-1)^{a_d+c}\gamma_{d-1}(a_1,\dots,a_{k-1},a_k-c,a_{k+1}+c,\dots,a_{d-1}+c).\end{aligned}$$

This implies

$$\begin{aligned}[v,tx_i]=&\sum_{1\le c\le a_k}\binom{a_k}{c}(-t)^c\beta_d(\gamma_{d-1}(a_1,\dots,a_{k-1},a_k-c,a_{k+1}+c,\dots,a_{d-1}+c),a_d+c))\\ =&\sum_{1\le c\le a_k}\binom{a_k}{c}(-t)^c\gamma_d(a_1,\dots,a_{k-1},a_k-c,a_{k+1}+c,\dots,a_{d-1}+c,a_d+c).\end{aligned}$$

This concludes our proof. □

We define a directed graph $\Omega_d$ whose nodes are the elements of $\Gamma_d$ and in which there exists an edge with initial vertex $\omega_1=\gamma(a_1,\dots,a_d)$ and terminal vertex $\omega_2=\gamma(b_1,\dots,b_d)$ if and only if there exists $k\in\{1,\dots,d\}$ such that $a_k\neq 0$ and $\gamma(b_1,\dots,b_d)=\gamma(a_1,\dots,a_{k-1},a_k-1,a_{k+1}+1,\dots,a_d+1)$. Let $\omega=\gamma_d(a_1,\dots,a_d)\in\Omega_d$: we define the height of $\omega$ as follows:

$$\mathrm{ht}(\gamma_d(a_1,\dots,a_d))=2^{d-1}\overline{a_1}+2^{d-2}\overline{a_2}+\dots+2\overline{a_{d-1}}+\overline{a_d}.$$

**Lemma 4.** *If $(\omega_1,\omega_2)$ is an edge in $\Omega_d$, then $\mathrm{ht}(\omega_2)<\mathrm{ht}(\omega_1)$.*

*Proof.* We may assume $\omega_1 = \gamma_d(a_1, \dots, a_d)$ with $0 \leq a_i \leq p-1$ for each $i \in \{1, \dots, d\}$ and that $\omega_2 = \gamma(a_1, \dots, a_{k-1}, a_k - 1, a_{k+1} + 1, \dots, a_d + 1)$ for some $k \in \{1, \dots, d\}$ with $a_k \neq 0$. Since

$$\begin{aligned} \mathrm{ht}(\omega_1) &= 2^{d-1}a_1 + \cdots + a_d \quad \text{ and} \\ \mathrm{ht}(\omega_2) &= 2^{d-1}a_1 + \cdots + 2^{d-k+1}a_{k-1} + 2^{d-k}(a_k - 1) + 2^{d-k-1}\overline{(a_{k+1}+1)} + \cdots + \overline{(a_d+1)} \\ &\leq 2^{d-1}a_1 + \cdots + 2^{d-k+1}a_{k-1} + 2^{d-k}(a_k - 1) + 2^{d-k-1}(a_{k+1}+1) + \cdots + (a_d+1) \end{aligned}$$

we have

$$\mathrm{ht}(\omega_1) - \mathrm{ht}(\omega_2) \geq 2^{d-k} - \sum_{0 \leq j \leq d-k-1} 2^j = 1$$

hence $\mathrm{ht}(\omega_2) < \mathrm{ht}(\omega_1)$. □

Given $\omega \in \Omega_d$ we denote by $\Delta_d(\omega)$ the set of the descendants of $\omega \in \Omega_d$, i.e. the set of the $\omega^* \in \Omega_d$ for which there exists a path in $\Omega_d$ starting from $\omega$ and ending in $\omega^*$.

**Proposition 5.** *If $\omega \in \Omega_d$, then $\Delta_d(\omega)$ is a basis for the $H_d$-submodule $U(\omega)$ of $V_d$ generated by $\omega$.*

*Proof.* By Lemma 3, $U(\omega)$ is contained in the subspace of $V_d$ spanned by $\Delta_d(\omega)$. To prove the converse it suffices to show that if $\Omega_n$ contains the edge $(\omega, \omega^*)$ then $\omega^* \in U(\omega)$. Let $\omega = \gamma_d(a_1, \dots, a_d)$. We assume $0 \leq a_i \leq p-1$ for each $i \in \{1, \dots, d\}$. By definition there exists a $k \in \{1, \dots, d\}$ such that $a_k \neq 0$ and

$$\omega^* = \gamma(a_1, \dots, a_{k-1}, a_k - 1, a_{k+1} + 1, \dots, a_d + 1).$$

For $0 \leq c \leq a_k$, let $\omega_c = \gamma_d(a_1, \dots, a_{k-1}, a_k - c, a_{k+1} + c, \dots, a_d + c)$. In particular, $\omega = \omega_0$ and $\omega^* = \omega_1$. By Lemma 3, for $0 \leq c \leq a_k$ there exist $\mu_{c,c+1}, \dots, \mu_{c,k} \in F$ such that

$$[\omega_c, x_i] = \sum_{c+1 \leq j \leq a_k} \mu_{c,j}\omega_j.$$

Moreover $\mu_{c,j} \neq 0$ for each $j \in \{c+1, \dots, a_k\}$. Indeed, since $0 \leq a_k < p-1$,

$$\mu_{c,j} = \binom{a_k - c}{j - c}(-1)^{j-c} \neq 0 \mod p.$$

Now, for $r \in \{0, \dots, a_k - 1\}$ consider

$$\rho_r = [\omega, \underbrace{x_i \dots, x_i}_{r \text{ times}}].$$

We claim that

$$\rho_r = \sum_{r \leq c \leq a_k} \lambda_{r,c}\omega_c, \text{ with } \lambda_{r,c} \in F \text{ and } \lambda_{r,r} \neq 0.$$

If $r = 1$, then $\rho_1 = [\omega_0, x_i]$ and $\lambda_{1,c} = \mu_{0,c}$. Assume $r \neq 1$.

$$\begin{aligned} \rho_r = [\rho_{r-1}, x_i] &= \left[\sum_{r-1 \leq c \leq a_k} \lambda_{r-1,c}\omega_c, x_i\right] = \sum_{r-1 \leq c \leq a_k} [\lambda_{r-1,c}\omega_c, x_i] \\ &= \sum_{r-1 \leq c \leq a_k} \lambda_{r-1,c}\left(\sum_{c+1 \leq j \leq a_k} \mu_{c,j}\omega_j\right) = \sum_{r \leq c \leq a_k} \lambda_{r,c}\omega_c \end{aligned}$$

with

$$\lambda_{r,j} = \sum_{r-1 \leq c \leq j-1} \lambda_{r-1,c}\mu_{c,j}.$$

In particular $\lambda_{r,r} = \lambda_{r-1,r-1}\mu_{r-1,r-1} \neq 0$. Now we can conclude our proof, showing by induction on $a_k - c$ that $\omega_c \in U(\omega)$ for $1 \leq c \leq a_k$. If $a_k - c = 0$, then $\rho_{a_k} = \lambda_{a_k,a_k}\omega_{a_k} \in U$. Since $\rho_{a_k} \in U$ and $\lambda_{a_k,a_k} \neq 0$, we conclude $\omega_{a_k} \in U(\omega)$. Assume $\omega_{c+1}, \dots, \omega_{a_k} \in U(\omega)$. Since $\rho_{c,c} = \sum_{c \leq j \leq a_k} \lambda_{r,j}\omega_j \in U(\omega)$ and $\lambda_{c,c} \neq 0$, we deduce $\omega_c \in U(\omega)$. □

## 3. Derived Length and Nilpotency class of $H_d$

We will denote with $\mathrm{dl}(G)$ the derived length of $G$, if $G$ is a soluble group, and with $\mathrm{nc}(G)$ the nilpotency class of $G$, if $G$ is a nilpotent group.

**Proposition 6.** $\mathrm{dl}(H_d) = d$.

*Proof.* The proof is by induction on $d$. If $d = 1$, then $H_1$ is cyclic of order $p$ and $\mathrm{dl}(H_1) = 1$. Assume $d \geq 2$. We have $H_d' \leq G_d' \leq (G_{d-1})^p$, and so we can consider the projection $\pi_1 : H_d' \to G_{d-1}$. By Lemma 3

$$\begin{aligned}[x_i, x_1] &= [\gamma_{i+1}(1, \dots, 1), x_1] = -\gamma_{i+1}(1, \dots, 1, 0)\\ &= -(\gamma_i(1, \dots, 1), \dots, \gamma_i(1, \dots, 1)) = -(x_{i-1}, \dots, x_{i-1}).\end{aligned}$$

Thus $\pi_1(H_d') \geq \langle x_1, \dots, x_{d-1}\rangle = H_{d-1}$ and by induction

$$d - 1 = \mathrm{dl}(H_{d-1}) \leq \mathrm{dl}(\pi_1(H_d')) \leq \mathrm{dl}(H_d') \leq \mathrm{dl}(G_d') = d - 1.$$

But then, $\mathrm{dl}(H_d') = d - 1$ hence $\mathrm{dl}(H_d) = d$. □

It is well known that $G_d$ is isomorphic to a Sylow $p$-subgroup of $\mathrm{Sym}(p^d)$, hence $H_d$ can be identified with a subgroup of $\mathrm{Sym}(p^d)$.

**Corollary 7.** *$H_d$ is a transitive subgroup of* $\mathrm{Sym}(p^d)$.

*Proof.* Assume that $\Omega_1, \dots, \Omega_r$ are the orbits of $H_d$ on the set $\{1, \dots, p^d\}$. For each $j \in \{1, \dots, r\}$ we have $|\Omega_j| = p^{s_j}$ for some $s_j \in \mathbb{N}$. If $X_j$ is the transitive constituent of $H_d$ corresponding to the orbit $\Omega_j$, then $X_j$ is isomorphic to a subgroup of $G_{s_j}$, since $G_{s_j}$ is a Sylow $p$-subgroup of $\mathrm{Sym}(p^{s_j})$; in particular $\mathrm{dl}(X_j) \leq \mathrm{dl}(G_{s_j}) = s_j$. We deduce that $d = \mathrm{dl}(H_d) \leq \max\{\mathrm{dl}(X_j) \mid 1 \leq j \leq r\} \leq \max\{s_j \mid 1 \leq j \leq r\}$. This is possible only if $r = 1$. □

Define $z_d$ as follows:

$$\begin{cases} z_1 = x_1 & \text{if } d = 1,\\ z_d = \gamma_{d-1}(0, \dots, 0) & \text{otherwise.}\end{cases}$$

It follows immediately from our definitions that $z_d = (1, \dots, 1) \in V_{d-1}$. In particular $\langle z_d\rangle \leq C_{V_{d-1}}(G_{d-1}) \leq C_{V_{d-1}}(H_{d-1})$.

**Lemma 8.** $C_{V_{d-1}}(H_{d-1}) = \langle z_d\rangle$.

*Proof.* Let $v = (x_1, \dots, x_{p^{d-1}}) \in C_{V_{d-1}}(H_{d-1})$. Since $H_{d-1}$ is a transitive subgroup of $\mathrm{Sym}(p^{d-1})$ it must be $x_i = x_1$ for all $i \in \{1, \dots, p^{d-1}\}$, hence $v \in \langle z_d\rangle$. □

**Lemma 9.** *Let $d$ be a positive integer. If $a_1 \neq 0$, then $[z_d, \gamma_d(a_1, \dots, a_d)] \neq 0$.*

*Proof.* We prove this statement by induction on $d$. If $d = 1$, then $[z_1, \gamma_1(a_1)] = \gamma_1(a_1 - 1) \neq 0$, by Lemma 3. Otherwise, since $z_d = (z_{d-1}, \dots, z_{d-1})$, we have

$$\begin{aligned}
&[z_d, \gamma_d(a_1, \dots, a_d)] = \\
&\quad = [(z_{d-1}, \dots, z_{d-1}), (0^{a_d}\gamma_{d-1}(a_1, \dots, a_{d-1}), \dots, (p-1)^{a_d}\gamma_{d-1}(a_1, \dots, a_{d-1}))] \\
&\quad = ([z_{d-1}, 0^{a_d}\gamma_{d-1}(a_1, \dots, a_{d-1})], \dots, [z_{d-1}, (p-1)^{a_d}\gamma_{d-1}(a_1, \dots, a_{d-1})]) \neq 0
\end{aligned}$$

since $[z_{d-1}, \gamma_{d-1}(a_1, \dots, a_{d-1})] \neq 0$ by induction. □

**Corollary 10.** *$Z(H_d) = \langle z_d \rangle$ is cyclic of order $p$.*

*Proof.* If $d = 1$ then $Z(H_1) = \langle z_1 \rangle = \langle x_1 \rangle$ is cyclic of order $p$. Assume $d \geq 2$. We have $H_d = W_{d-1} \rtimes H_{d-1}$. By induction, $\langle z_{d-1} \rangle = Z(H_{d-1})$; in particular $z_{d-1}$ is contained in every normal subgroup of $H_{d-1}$ and it follows from Lemma 9 that the action of $H_{d-1}$ on $W_{d-1}$ is faithful. Hence, by Lemma 8, $Z(H_d) \leq C_{W_{d-1}}(H_{d-1}) = \langle z_d \rangle$. □

Let a group $G$ act on another group $A$ via automorphism and suppose that $1 = A_0 \leq \cdots \leq A_m = A$ is a chain of $G$-invariant subgroups: we say that $G$ stabilizes the chain $\{A_i \mid 0 \leq i \leq m\}$ if each right coset of $A_{i-1}$ in $A_i$ is $G$-invariant for all $i$ with $0 < i < m$. The first proof of following result was given by Kaluzhnin.

**Proposition 11.** *Assume that $G$ acts faithfully on $A$ via automorphisms and that $G$ stabilizes a chain $\{A_i \mid 0 \leq i \leq m\}$ of normal subgroups of $A$. Then $A$ is nilpotent of class at most $m - 1$.*

**Lemma 12.** *Let $\omega \in \Omega_d$ with $m = \mathrm{ht}(\omega)$. Define $U_0(\omega) = 0$ and, for any $j \in \{1, \dots, m\}$, let $U_j(\omega) = \langle \omega^* \in \Delta_d(\omega) \mid \mathrm{ht}(\omega^*) \leq j - 1 \rangle$. Then $H_d$ stabilizes the chain $\{U_j(\omega) \mid 0 \leq i \leq m + 1\}$.*

*Proof.* It follows immediately from Lemma 3 and Lemma 4. □

**Lemma 13.** *$H_d$ acts faithfully on the submodule $U_d$ of $W_d$ generated by $\gamma_d(1, 0, \dots, 0)$.*

*Proof.* By Corollary 8, $\langle z_d \rangle$ is contained in all the nontrivial normal subgroups of $H_d$. Now, Lemma 9 guarantees that $[z_d, \gamma_{d+1}(1, 0, \dots, 0)] \neq 0$, and this immediately implies that the action of $H_d$ on $U_d$ is faithfull. □

**Theorem 14.** $\mathrm{nc}(H_d) = 2^{d-1}$.

*Proof.* It is well known that $\mathrm{dl}(G) \leq \log_2(\mathrm{nc}(G)) + 1$ for every nilpotent group. Therefore, from Proposition 6, we deduce that $\mathrm{nc}(G) \geq 2^{d-1}$. On the other hand, by Lemma 13, $H_d$ acts faithfully on the $H_d$-submodule $U_d$ of $W_d$ generated by $\gamma_d(1, 0, \dots, 0)$ and, by Lemma 12, $H_d$ stabilizes a chain of $U_d$ of length at most $\mathrm{ht}(\gamma_d(1, 0, \dots, 0)) + 2 = 2^{d-1} + 2$. Therefore $\mathrm{nc}(H_d) \leq 2^{d-1}$ by Proposition 11. □

Recall that $x_{d+1} = \gamma_d(1, \dots, 1)$ and that $W_d$ is the $H_d$-submodule of $V_d$ generated by $x_{d+1}$. Since $W_d$ is a cyclic $H_d$-module, it contains a unique maximal $H_d$-submodule, say $Y_d$. Let $\Delta_d = \Delta_d(x_{d+1})$ and $\Delta_d^* = \Delta_d \setminus \{x_{d+1}\}$. It follows from Proposition 5 that $\Delta_d$ is a basis for $W_d$ and $\Delta_d^*$ is a basis for $Y_d$. Now let $Z_d$ be the $F$-subspace of $W_d$ spanned by the vectors $\beta_d(w, a)$ with $w \in \Delta_{d-1}^*$ and $a \in I_p$. Again, we can use Proposition 5 to deduce that $Z_d$ is an $H_d$-submodule of $W_d$. More precisely:

**Lemma 15.** *Let $\tilde{x}_{d+1} = \gamma_d(1, \dots, 1, 0)$. The set $\Delta_d \setminus \{x_{d+1}, \tilde{x}_{d+1}\}$ is a basis for $Z_d$. In particular if $\gamma_d(a_1, \dots, a_d) \in Z_d \cap \Delta_d$, then $a_i = 0$ for some $i \in \{1, \dots, d-1\}$.*

*Proof.* Let $\omega = \gamma_d(a_1, \dots, a_d) \in \Delta_d^*$. We have $\sum_{1 \le j \le d} 2^{d-j}\overline{a_j} < \mathrm{ht}(x_{d+1}) = 2^d - 1$ and this is possible only if $a_i = 0$ for some $i \in \{1, \dots, d\}$. If $a_i = 0$ for some $i \in \{1, \dots, d-1\}$ then $w = \gamma_{d-1}(a_1, \dots, a_{d-1}) \in \Delta_{d-1}^*$ and $\omega = \beta_d(w, a_d) \in Z_d$. Otherwise $\omega = \gamma_d(a_1, \dots, a_{d-1}, 0)$ with $a_i \ne 0$ for $1 \le i \le d-1$ : again we deduce from $\mathrm{ht}(\omega) < 2^d - 1$ that $a_1 = \dots = a_{d-1} = 1$, i.e. $\omega = \tilde{x}_{d+1}$. □

Since $Y_n$ is an $H_n$-submodule of $W_n$ for any $n \in \mathbb{N}$, we have $[Y_i, x_j] \le Y_i$ whenever $j \le i$. On the other hand, if $j > i$ then $[Y_i, x_j] \le [Y_i, W_{j-1}] \le [H_i, W_{j-1}] \le Y_{j-1}$. This implies that $F_d = Y_{d-1}Y_{d-2} \cdots Y_1$ is a normal subgroup of $H_d$ and $H_d/F_d$ is an elementary abelian $p$-group of order $p^d$. Since $H_d$ can be generated by the $d$ elements $x_1, \dots, x_d$ we deduce that $F_d = \mathrm{Frat}(H_d) = H_d'$.

**Lemma 16.** *$K_d = Z_{d-1}Z_{d-2} \cdots Z_2$ is a normal subgroup of $H_d$.*

*Proof.* Since $Z_i$ is an $H_i$-submodule of $W_i$ for any $i \in \mathbb{N}$, and $H_{i+1} = W_i \rtimes H_i$, we have $[Z_i, x_{j+1}] \le Z_i$ whenever $i \ge j$. So in order to prove our statement, it suffices to prove that if $2 \le i < j$ then $[Z_i, x_{j+1}] \le Z_j$. Recall that $\mathrm{ht}(x_{j+1}) = 2^j - 1$ and let

$$Y_j^* = \langle \omega \in \Delta_j \mid \mathrm{ht}(\omega) \le \mathrm{ht}(x_{j+1}) - 2 = 2^j - 3 \rangle \le Y_j.$$

We have $Y_j = \langle Y_j^*, \tilde{x}_{j+1}, \eta_1, \dots, \eta_j \rangle$ with

$$\begin{aligned} \eta_1 &= \gamma_j(0, 2, 2, \dots, 2), \\ \eta_2 &= \gamma_j(1, 0, 2, \dots, 2), \\ &\dots\dots\dots\dots\dots\dots \\ \eta_{j-1} &= \gamma_j(1, \dots, 1, 0, 2), \\ \eta_j &= \gamma_j(1, \dots, 1, 0) = \tilde{x}_{j+1}. \end{aligned}$$

Now let $h \in Z_i$. Since $h \in Z_i \le H_{i+1} = \langle x_1, \dots, x_{i+1} \rangle$, we have $h = x_{s_1} \dots x_{s_r}$ with $r \in \mathbb{N}$ and $s_1, \dots, s_r \in \{1, \dots, i+1\}$. By Lemma 3, $[W_j, H_j, H_j] = [Y_j, H_j] = Y_j^*$ and

$$[h, x_{j+1}] \equiv \sum_{1 \le t \le r} [x_{s_t}, x_{j+1}] \equiv \sum_{1 \le t \le r} \eta_{j+1-s_t} \mod Y_j^*.$$

Let $l$ be the numbers of $t \in \{1, \dots, r\}$ with $x_{s_t} = x_1$. Since $\eta_k \in Z_j$ if $k \ne j$ and $U_j \le Z_j$ we deduce that $[h, x_{j+1}] \equiv l\tilde{x}_{j+1} \mod Z_j$. On the other hand $h \in Z_i \le W_i \cdots W_2 \trianglelefteq H_i$ and $h \equiv (x_1)^l \mod W_i \cdots W_2$, so it must be $l \equiv 0 \mod p$ and consequently $[h, x_{j+1}] \in Z_j$. □

We are interested in the structure of the factor group $H_d/K_d$. Let

$$\xi_1 = x_1K_d, \xi_2 = x_2K_d, \tilde{\xi}_2 = \tilde{x}_2K_d, \dots, \xi_d = x_dK_d, \tilde{\xi}_d = \tilde{x}_dK_d.$$

**Lemma 17.** *The group $H_d/K_d$ has order $p^{2d-1}$. In particular*

(1) *$\langle \xi_2, \tilde{\xi}_2, \dots, \xi_d, \tilde{\xi}_d \rangle$ is a normal subgroup of $H_d/K_d$ and it is an elementary abelian $p$-group of order $p^{2(d-1)}$.*
(2) *$\langle \tilde{\xi}_2, \dots, \tilde{\xi}_d \rangle$ is a central subgroup of $H_d/K_d$.*
(3) *$[\xi_1, \xi_i] = \tilde{\xi}_i$ for each $i \in \{2, \dots, d\}$.*

**Theorem 18.** *If $T$ is a proper subgroup of $H_d$, then $\mathrm{dl}(T) \le d - 1$.*

*Proof.* We prove the theorem by induction on $d$. It is not restrictive to assume that $T$ is a maximal subgroup of $H_d$. If $W_{d-1} \leq T$, then $T/W_{d-1}$ is a proper subgroup of $H_d/W_{d-1} \cong H_{d-1}$ and by induction $T^{(d-2)} \leq W_{d-1}$. It follows that $T^{(d-1)} = 1$, and so $\mathrm{dl}(T) \leq d-1$. Now assume $W_{d-1} \not\leq T$ : we have $TW_{d-1} = H_{d-1}$ and $T \cap W_{d-1} = Y_{d-1}$, since $Y_{d-1}$ is the unique maximal $H_{d-1}$-submodule of $W_{d-1}$. In particular, there exist $w_1, \ldots, w_{d-1} \in W_{d-1}$ such that

$$T = \langle w_1x_1, \ldots, w_{d-1}x_{d-1}, Y_{d-1}\rangle = \langle w_1x_1, \ldots, w_{d-1}x_{d-1}, \tilde{x}_d, Z_{d-1}\rangle.$$

Since $Y_{d-1} \leq T$ and $W_{d-1} = \langle Y_{d-1}, x_d\rangle$ we may assume $w_i = c_ix_d$ for some $c_i \in \mathbb{N}$. Therefore we have $T = \langle (c_1x_d)x_1, \ldots, (c_{d-1}x_{d-1})x_1, \tilde{x}_d, Z_{d-1}\rangle$ and, since $Z_{d-1} \leq K_d$, it follows

$$TK_d/K_d = \langle (c_1\xi_d)\xi_1, \ldots, (c_{d-1}\xi_d)\xi_{d-1}, \tilde{\xi}_d\rangle.$$

By Lemma 17, $T'K_d/K_d$ is the smallest normal subgroup of $TK_d/Kd$ containing the commutators $[(c_1\xi_d)\xi_1, (c_i\xi_d)\xi_i] = c_1c_i\tilde{\xi}_i$ for $i \in \{2, \ldots, d-1\}$. This means that $T'K_d/K_d \leq \langle \tilde{\xi}_2, \ldots, \tilde{\xi}_{d-1}\rangle$, i.e. $T' \leq \langle \tilde{x}_2, \ldots, \tilde{x}_{d-1}\rangle K_d \leq F_d \leq (H_{d-1})^p$. For $j \in \{1, \ldots, p\}$, let $U_j = \langle \pi_j(\tilde{x}_2), \ldots, \pi_j(\tilde{x}_{d-1})\rangle F_{d-1} \leq H_{d-1}$. Since $d(H_{d-1}) = d-1$ and $F_{d-1} = \mathrm{Frat}\, H_{d-1}$, it must be $U_j \neq H_{d-1}$. By induction $\mathrm{dl}(U_j) \leq d-2$. Moreover, since $\pi_j(K_d) \leq F_{d-1}$, we deduce that $\pi_j(T') \leq U_j$. But then $T' \leq U_1 \times \ldots U_p$ which implies that $\mathrm{dl}(T') \leq \max_j \mathrm{dl}(U_j) \leq d-2$ and consequently that $\mathrm{dl}(T) \leq d-1$. □

**Proposition 19.** *If* $1 \neq N \trianglelefteq H_d$, *then* $\mathrm{dl}(H_d/N) \leq d-1$.

*Proof.* Since by Corollary 10, $Z(H_d)$ is cyclic of order $p$, we have that $Z(H_d) \leq N$. In particular, $\mathrm{nc}(H_d/N) \leq \mathrm{nc}(H_d/Z(H_d)) \leq \mathrm{nc}(H_d) - 1 = 2^{d-1} - 1$ and so $\mathrm{dl}(H_d/N) \leq \log_2(\mathrm{nc}(H_d/N)) - 1 \leq \log_2(2^{d-1} - 1) + 1 < d$. □

## 4. Order of $H_d$

In this section we want to say more about the order of the group $H_d$. If $d = 1$, then $H_1$ is cyclic of order $p$. If $d = 2$, then $W_1$ has a basis over $F$ consisting of the two vectors $\gamma_1(1)$ and $\gamma_1(0)$ so $H_2 = W_1 \rtimes H_1$ is a nonabelian group of order $p^3$. However the order of $H_3$ depends on the choice of the prime $p$: indeed a basis of $W_2$ can be obtained considering the set $\Delta_2$ of the descendants of $x_3 = \gamma_2(1,1)$ in the graph $\Gamma_2$. If $p \neq 2$, then $\Delta_2 = \{\gamma_2(1,1), \gamma_2(1,0), \gamma_2(0,2), \gamma_2(0,1), \gamma_2(0,0)\}$: in this case $|H_2| = |H_1||W_2| = p^3p^5 = p^8$. However for $p$=2 we have $\Delta_2 = \{\gamma_2(1,1), \gamma_2(1,0), \gamma_2(0,1), \gamma_2(0,0)\}$ and $|H_2| = 2^7$.

The dimension of $W_n$ over $F$ is related to the function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ which is uniquely determined by the following rules:

$$f(n,a) = \begin{cases} 1 & \text{if } n = 0 \\ p^n & \text{if } a \geq p \text{ and } n > 0 \\ \sum_{0 \leq j \leq a} f(n-1, a+j) & \text{if } a < p \text{ and } n > 0. \end{cases}$$

It can be easily proved that $f(n, p-1) = p^n$ for any positive integer $n$.

Our aim is to prove that $|W_d| = p^{f(d,1)}$. This requires a more detailed investigation of the properties of the graph $\Omega_n$.

**Lemma 20.** *Let* $\omega = \gamma_d(a_1, \ldots, a_d)$ *with* $a_i \in \{0, \ldots, p-1\}$ *for every* $i \in \{1, \ldots, d\}$. *If* $0 \leq b_i \leq a_i$ *for every* $i \in \{1, \ldots, d\}$, *then* $\gamma_d(b_1, \ldots, b_d) \in \Delta_d(\omega)$.

*Proof.* We prove by induction on $d-j$ that if $b_i \leq a_i$ for every $i \in \{j,\dots,d\}$ then $\gamma_d(a_1,\dots,a_{j-1},b_j,\dots,b_d) \in \Delta_d(\omega)$. This is certainly true if $d-j=0$, since $\Omega_d$ contains the edge $(\gamma_d(a_1,\dots,a_{d-1},y_d),\gamma_d(a_1,\dots,a_{d-1},y_d-1))$ whenever $1 \leq y_d \leq a_d$. Now assume that we have proved our statement for a $j \neq 1$, assume that $a_{j-1} \neq 0$ and consider $\omega_1 = \gamma_d(a_1,\dots,a_{j-1},a_j^*,\dots,a_d^*)$ with $a_k^* = a_k - 1$ if $a_k > 0$ and $a_k^* = 0$ otherwise. By induction $\omega_1 \in \Delta_d(\omega)$. Moreover $\Omega_d$ contains the edge $(\omega_1,\omega_2)$ for $\omega_2 = \gamma_d(a_1,\dots,a_{j-1}-1,a_j^*+1,\dots,a_d^*+1)$. By induction

$$\gamma_d(a_1,\dots,a_{j-1}-1,b_j,\dots,b_d) \in \Delta_d(\omega_1) \subseteq \Delta_d(\omega)$$

if $b_i \leq a_i^*+1$ for every $i \in \{j,\dots,d\}$. Since $a_i \leq a_i^*+1$, we deduce

$$\gamma_d(a_1,\dots,a_{j-1}-1,b_j,\dots,b_d) \in \Delta_d(\omega)$$

if $b_i \leq a_i$ for every $i \in \{j,\dots,d\}$. Repeating this argument, we can conclude $\gamma_d(a_1,\dots,b_{j-1},b_j,\dots,b_d) \in \Delta_d(\omega)$ if $b_i \leq a_i$ for every $i \in \{j-1,\dots,d\}$. □

**Lemma 21.** *If $\omega = \gamma_d(a_1,\dots,a_d)$, $a_{i-1} \neq 0$ and $a_i = p-1$, then*

$$\gamma_d(a_1,\dots,a_{i-1}-1,b,a_{i+1}+1,\dots,a_d+1) \in \Delta_d(\omega)$$

*for every $b \in \{0,\dots,p-1\}$.*

*Proof.* By Lemma 20, $\omega_1 = \gamma_d(a_1,\dots,a_{i-1},p-2,a_{i+1},\dots,a_d) \in \Delta_d(\omega)$ and consequently $\omega_2 = \gamma_d(a_1,\dots,a_{i-1}-1,p-1,a_{i+1}+1,\dots,a_d+1) \in \Delta_d(\omega_1) \subseteq \Delta_d(\omega)$. Again by Lemma 20, $\gamma_d(a_1,\dots,a_{i-1}-1,b,a_{i+1}+1,\dots,a_d+1) \in \Delta_d(\omega_2) \subseteq \Delta_d(\omega)$ for every $b \in \{0,\dots,p-1\}$. □

We define a new graph $\tilde{\Omega}_d$ with the same vertices as $\Omega_d$ but with a different set of edges: let $\omega_1 = \gamma_d(a_1,\dots,a_d)$ and $\omega_2 = \gamma_d(b_1,\dots,b_d)$ with $0 \leq a_i, b_j \leq p-1$ : $(\omega_1,\omega_2)$ is an edge in $\tilde{\Omega}_d$ if and only if there exists $k \in \{1,\dots,d\}$ such that: $a_k \neq 0$, $b_i = a_i$ if $i < k$, $b_k = a_k - 1$, $b_i = \min\{a_i+1,p-1\}$ if $i > k$. We denote by $\tilde{\Delta}_d(\omega)$ the set of the descendants of $\omega \in \Gamma_d$. It follows immediately from Lemma 21 that:

**Lemma 22.** *For every $\omega \in \Gamma_d$ we have $\tilde{\Delta}_d(\omega) = \Delta_d(\omega)$.*

**Lemma 23.** *Let $\omega = \gamma_d(b,\dots,b)$ with $0 \leq b \leq p-1$. Then $|\tilde{\Delta}_d(\omega)| = f(d,b)$.*

*Proof.* We prove the statement by induction on $d$. It follows immediately from the definition that $\tilde{\Delta}_1(\gamma_1(b)) = \{\gamma_1(b),\gamma_1(b-1),\dots,\gamma_1(0)\}$ has cardinality $b+1 = f(1,b)$.

Let $(\omega_1,\omega_2)$ be an edge in the graph $\tilde{\Omega}_d$. We say that $(\omega_1,\omega_2)$ is a $k$-edge if

$$\omega_1 = \gamma_d(a_1,\dots,a_d) \text{ with } a_1,\dots,a_d \in \{0,\dots,p-1\}, a_k \neq 0 \text{ and}$$
$$\omega_2 = \gamma_d(a_1,\dots,a_{k-1},a_k-1,\min\{a_{k+1}+1,p-1\},\dots,\min\{a_d+1,p-1\}).$$

Now let $\omega = \gamma_d(b,\dots,b)$ with $b \in \{0,\dots,p-1\}$ and let $\omega^* \in \tilde{\Delta}_d(\omega)$. The number of 1-edges in a path connecting $\omega$ to $\omega^*$ is at most $b$. For $j \in \{0,\dots,b\}$ let $\tilde{\Delta}_d(\omega,j)$ be the subset of $\tilde{\Delta}_d(\omega)$ consisting of the descendants of $\omega$ connected to $\omega$ by a path which contains exactly $j$ 1-edges. Notice that if $\omega^* = \gamma_d(a_1,\dots,a_d) \in \tilde{\Delta}_d(\omega,j)$, then $a_1 = b-j$ and consequently $\tilde{\Delta}_d(\omega)$ is the disjoint union of the subsets $\tilde{\Delta}_d(\omega,j)$, $0 \leq j \leq b$, and $|\tilde{\Delta}_d(\omega)| = \sum_{0 \leq j \leq b} |\tilde{\Delta}_d(\omega,j)|$.

Clearly $\omega^* = \gamma_d(a_1,\dots,a_p) \in \tilde{\Delta}_d(\omega,0)$ if and only if $\omega^* = \gamma_d(b,b_1,\dots,b_{p-1})$ with $\gamma_{d-1}(b_1,\dots,b_{d-1}) \in \tilde{\Delta}_{d-1}(\gamma_{d-1}(b,\dots,b))$ so, by induction, $|\tilde{\Delta}_d(\omega_0)| = f(d-1,b)$.

Now suppose that there is a path

$$\omega_0 = \omega, \omega_1, \dots, \omega_{k+1} = \omega^*$$

where $(\omega_j, \omega_{j+1})$ is an 1-edge if and only if $j = k$. We claim that if $k \neq 0$, then there exist $r < k$ and a path

$$\tilde{\omega}_0 = \omega, \tilde{\omega}_1, \dots, \tilde{\omega}_{s+1} = \omega^*$$

with $s \geq r$ and where $(\omega_j, \omega_{j+1})$ is a 1-edge if and only if $j = r$. Let $\omega_{k-1} = \gamma_d(a_1, \dots, a_d)$ with $a_1, \dots, a_d \in \{0, \dots, p-1\}$ and assume that $(\omega_{k-1}, \omega_k)$ is an $i$-edge. Hence,

$$\begin{aligned} \omega_k &= \gamma_d(a_1, \dots, a_{i-1}, a_i - 1, \min\{a_{i+1}+1, p-1\}, \dots, \min\{a_d+1, p-1\}) \\ \omega_{k+1} &= \gamma_d(a_1 - 1, \min\{a_2+1, p-1\}, \dots, \min\{a_{i-1}+1, p-1\}, \\ &\qquad a_i, \min\{a_{i+1}+2, p-1\}, \dots, \min\{a_d+2, p-1\}). \end{aligned}$$

Now, the graph $\tilde{\Delta}_d(\omega)$ contains also the 1-edge $(\omega_{k-1}, \omega_k^*)$ and the $i$-edge $(\omega_k^*, \omega_{k+1}^*)$ with

$$\begin{aligned} \omega_k^* &= \gamma_d(a_1 - 1, \min\{a_2+1, p-1\}, \dots, \{a_d+2, p-1\}) \\ \omega_{k+1}^* &= \gamma_d(a_1 - 1, \min\{a_2+1, p-1\}, \dots, \min\{a_{i-1}+1, p-1\}, \min\{a_i+1, p-1\} - 1, \\ &\qquad \min\{a_{i+1}+2, p-1\}, \dots, \min\{a_d+2, p-1\}). \end{aligned}$$

If $a_i \neq p-1$, then $\omega_{k+1}^* = \omega_{k+1}$ so $\omega_0, \dots, \omega_{k-1}, \omega_k^*, \omega_{k+1}$ is the path we are looking for. On the other hand, if $a_i = p-1$ then $\min\{a_i+1, p-1\} - 1 = p-2$ so this case requires a different argument. We may label the path $\omega_0, \dots, \omega_{k-1}$ with the sequence $(i_1, \dots, i_{k-1})$ meaning that $(\omega_{j-1}, \omega_j)$ is an $i_j$-edge for any $j \in \{1, \dots, k-1\}$. Now we consider the sequence $(i_1^*, \dots, j_t^*)$ obtained from $(i_1, \dots, i_k)$ by removing the entries $i_j$ whenever $i_j > i$ and let $\omega_0, \omega_1^*, \dots, \omega_t^*$ be the unique path starting from $\omega_0$ and labeled by the sequence $(i_1^*, \dots, j_t^*)$. It is not difficult to see that

$$\omega_t^* = \gamma_d(a_1 \dots, a_{i-1}, p-1, \dots, p-1).$$

Now we can continue the previous path adding the 1-edge $(\omega_t^*, \omega_{t+1}^*)$ with

$$\omega_{t+1}^* = (a_1 - 1, \min\{a_2+1, p-1\}, \dots, \min\{a_{i-1}+1, p-1\}, p-1, \dots, p-1\}).$$

By Lemma 20, there is a path $\omega_{t+1}^*, \dots, \omega_u^* = \omega_{k+1}$, involving only $j$-edges with $j \geq i$. In particular $\omega_0, \omega_1^*, \dots, \omega_u^*$ is the path we are looking for.

This completes the proof of our claim. Iterated applications of this remark allow to conclude that if $\omega^* \in \tilde{\Delta}_d(\omega, 1)$ then

$$\omega^* \in \tilde{\Delta}_d(\gamma_d(b-1, \min\{b+1, p-1\}, \dots, \min\{b+1, p-1\})).$$

In particular

$$|\tilde{\Delta}_d(\omega, 1)| = |\tilde{\Delta}_{d-1}(\gamma_{d-1}(\min\{b+1, p-1\}, \dots, \min\{b+1, p-1\})|.$$

If $b+1 = p$, then $|\tilde{\Delta}_d(\omega, 1)| = |\tilde{\Delta}_{d-1}(\gamma_{d-1}(p-1, \dots, p-1))| = p^{d-1} = f(d-1, b-1)$ by Lemma 20. If $b+1 < p$, then $|\tilde{\Delta}_d(\omega, 1)| = |\tilde{\Delta}_{d-1}(\gamma_{d-1}(b-1, \dots, b-1))| = f(d-1, b-1)$ by induction.

A similar argument allows us to conclude that for any $j \in \{0, \dots, b\}$ we have

$$|\tilde{\Delta}_d(\omega, j)| = |\tilde{\Delta}_{d-j}(\gamma_{d-j}(\min\{b+j, p-1\}, \dots, \min\{b+j, p-1\}) = f(d-j, b+j).$$

But then $|\tilde{\Delta}_d(\omega)| = \sum_{0 \leq j \leq b} |\tilde{\Delta}_d(\omega, j)| = \sum_{0 \leq j \leq b} f(d-j, b+1) = f(d, b)$. □

**Corollary 24.** $\dim_F W_d = f(d, 1)$ *and* $\log_p |H_d| = \sum_{0 \leq i \leq d-1} f(i, 1)$.

*Proof.* By the previous Lemma, $\dim_F W_d = |\tilde{\Delta}_d(\gamma_d(1,\dots,1))| = f(d,1)$ □

**Corollary 25.** *If $p = 2$, then $H_d = G_d = C_2 \wr \cdots \wr C_2$.*

*Proof.* For any positive integer $n$, we have that $\dim W_n = f(n,1) = f(n-1,1) + f(n-1,2) = 2^{n-1} + 2^{n-1} = 2^n = \dim V_n$, hence $W_n = V_n$ and $H_d = W_{d-1} \cdots W_0 = V_{d-1} \cdots V_0 = G_d$. □

On the other hand, if $p > 2$ then $|H_d|$ is much smaller then $|G_d|$. Indeed we have

**Proposition 26.** $\log_p |H_d| \le \frac{1}{p-1}\left(\frac{p^d-1}{p-1} + (p-2)d\right) = \frac{1}{p-1}\left(\log_p |G_d| + (p-2)d\right).$

*Proof.* First we prove by induction that $f(n,1) \le 1 + (p^n - 1)/(p-1)$ for each $n \in \mathbb{N}$. This is clearly true if $n = 0$ since $f(0,1) = 1$. On the other hand, if $n > 0$ then

$$f(n,1) = f(n-1,1) + f(n-1,2) \le 1 + \frac{p^{n-1}-1}{p-1} + p^{n-1} = 1 + \frac{p^n-1}{p-1} \tag{4.1}$$

since $f(n-1,2) = \dim_F(\gamma_{n-1}(2,\dots,2)) \le \dim_F V_{n-1} = p^{n-1}$. In particular

$$\log_p |H_d| = \log_p |W_0 \cdots W_{d-1}| = \sum_{0 \le i \le p} \log_p |W_i|$$
$$\le \sum_{0 \le i \le d-1} 1 + \frac{p^i - 1}{p-1} = \frac{1}{p-1}\left(\frac{p^d-1}{p-1} + (p-2)d\right).$$

To conclude it suffices to recall that $G_d = C_p \wr \cdots \wr C_p$ has order $(p^d - 1)/(p-1)$. □

If $p = 3$, then it follows from Lemma 20 that $f(m,2) = 3^m$ for every positive integer $m$ and (4.1) is indeed an equality: hence

$$|H_d| = \frac{1}{2}\left(\frac{3^d-1}{2} + d\right) \text{ if } p = 3.$$

However if $p \ne 3$, then $\gamma_m(i, a_2, \dots, a_m) \notin \Delta_m(\gamma_m(2,\dots,2))$ whenever $i \ge 3$ and this implies $f(m,2) \le p^m - (p-3)p^{m-1} = 3p^{m-1}$. In particular if $p \ge 5$ then the bound given in Proposition 26 can still be improved. The following table describes the behavior of $|H_d|$ when $d \in \{3,4,5\}$ and $p \in \{3,5,7\}$.

| | $p=3$ | $p=5$ | $p=7$ |
|---|---|---|---|
| $\dim_F W_2$ | 5 | 5 | 5 |
| $\dim_F W_3$ | 14 | 17 | 17 |
| $\dim_F W_4$ | 41 | 73 | 83 |
| $\log_p \lvert H_3\rvert$ | 8 | 8 | 8 |
| $\log_p \lvert H_4\rvert$ | 22 | 25 | 25 |
| $\log_p \lvert H_5\rvert$ | 63 | 98 | 108 |

## 5. A generalization

In this section we introduce a more general construction. it turns out that the two groups $H_d$ and $G_d$ are particular examples of the groups that can be obtained with this method; in particular, such groups can be studied simultaneously and share some properties.

We fix an integer $k \in \{1, \dots, p-1\}$ and we define recursively a sequence of vectors $x_{k,n} \in V_{n-1}$ :

$$\begin{cases} x_{k,1} = k \\ x_{k,n+1} = \gamma_n(k, \dots, k) = \beta_n(x_{k,n}, k) \text{ if } n > 1. \end{cases}$$

Let $X_{k,d}$ be the subgroup of $G_d$ generated by $x_{k,1}, \dots, x_{k,d}$.

**Lemma 27.** *If $k_1 \leq k_2$ then $X_{k_1,d} \leq X_{k_2,d}$. Moreover $X_{1,d} = H_d$ and $X_{p-1,d} = G_d$.*

*Proof.* We make induction on $d$. Clearly if $d = 1$, then $X_{k,1} = X_{1,1} = \langle x_1 \rangle \cong C_p$. So we may assume $d \geq 2$. By induction $H_{d-1} \leq X_{k_1,d-1} \leq X_{k_2,d-1}$. In particular $X_{k_2,d}$ contains the $(H_{d-1})$-submodule of $V_{d-1}$ generated by $x_{k_2,d} = \gamma_{d-1}(k_2, \dots, k_2)$. By Proposition 5 and Lemma 20, $x_{k_1,d} = \gamma_{d-1}(k_1, \dots, k_1)$ belongs to this submodule. Hence $X_{k_1,d} = \langle x_{k_1,d}, X_{k_1-1,d-1} \rangle \leq X_{k_2,d}$. In the particular case when $k_2 = p-1$, the $H_{d-1}$ submodule of $V_{d-1}$ generated by $x_{p-1,d} = \gamma_{d-1}(p-1, \dots, p-1)$ coincides with $V_{d-1}$ and the previous argument allows to conclude that $X_{p-1,d} = G_d$. □

We may generalize Lemma 3 to the general case.

**Lemma 28.** *Let $v = \gamma_d(a_1, \dots, a_d) \in V_d$, and $i \leq d$. Consider $k = (d-i)+1$. Then*

$$[v, tx_{r,i}] = \begin{cases} 0 \ \textit{if } a_k = 0 \\ \sum_{1 \leq c \leq \overline{a_k}} \binom{\overline{a_k}}{c} (-tr)^c \gamma_d(a_1, \dots, \overline{a_k} - c, a_{k+1} + cr, \dots, a_d + cr) \ \textit{otherwise.} \end{cases}$$

*Proof.* We may assume $0 \leq a_j \leq p-1$ for all $j \in \{1, \dots, p-1\}$. Suppose $i = 1$. If $a_d = 0$, then $[v, tx_1] = 0$; otherwise, by Lemma 3,

$$[v, tx_{r,1}] = [v, trx_1] = \sum_{1 \leq c \leq a_d} \binom{a_d}{c} (-tr)^c \gamma_d(a_1, \dots, a_{d-1}, a_d - c).$$

Now assume $i > 1$. Since $v = \beta(\gamma_{d-1}(a_1, \dots, a_{d-1}), a_d)$ and $tx_{r,i} = t\beta(x_{r,i-1}, r)$ we have

$$[v, tx_{r,i}] = (w_1, \dots, w_p)$$

with

$$w_j = [(j-1)^{a_d} \gamma_{d-1}(a_1, \dots, a_{d-1}), (t(j-1)^r) x_{r,i-1}] \in V_{d-1}.$$

By induction

$$\begin{aligned} w_j &= (j-1)^{a_d} \sum_{1 \leq c \leq a_k} \binom{a_k}{c} (-tr(j-1)^r)^c \gamma_{d-1}(a_1, \dots, a_k - c, a_{k+1} + cr, \dots, a_{d-1} + cr) \\ &= \sum_{1 \leq c \leq a_k} \binom{a_k}{c} (-tr)^c (j-1)^{a_d + cr} \gamma_{d-1}(a_1, \dots, a_k - c, a_{k+1} + cr, \dots, a_{d-1} + cr). \end{aligned}$$

This implies

$$\begin{aligned} [v, tx_{r,i}] &= \sum_{1 \leq c \leq a_k} \binom{a_k}{c} (-tr)^c \beta_d(\gamma_{d-1}(a_1, \dots, a_k - c, a_{k+1} + cr, \dots, a_{d-1} + cr), a_d + cr)) \\ &= \sum_{1 \leq c \leq a_k} \binom{a_k}{c} (-tr)^c \gamma_d(a_1, \dots, a_k - c, a_{k+1} + cr, \dots, a_{d-1} + cr, a_d + cr). \end{aligned}$$

This concludes our proof. □

We recall that $\Gamma_d = \{\gamma_d(a_1, \dots, a_d) | 0 \leq a_i \leq p-1 \text{ for every i } \in \{1, \dots, d\}\}$ is a basis of $V_d$ over $F$. For each $k \in \{1, \dots, p-1\}$, we define the $k$-height of $\omega = \gamma_d(a_1, \dots, a_d)$ as follows:

$$\mathrm{ht}_k(\gamma_d(a_1, \dots, a_d)) = (k+1)^{d-1}a_1 + (k+1)^{d-2}a_2 + \cdots + (k+1)a_{d-1} + a_d.$$

For $v = \sum_{\omega \in \Gamma_d} \lambda_\omega \omega \neq 0 \in V_d$ we define $\mathrm{supp}(v) = \{\omega \mid \lambda_\omega \neq 0\}$ and $\mathrm{ht}_k(v) = \max\{\mathrm{ht}_k(\omega) \mid \omega \in \mathrm{supp}(v)\}$. We set $\mathrm{ht}_k(v) = -1$ if $v = 0$. For $n \in \{0, \dots, (k+1)^d\}$, let $V_{k,d,n} = \{v \mid \mathrm{ht}_k(\omega) \leq n-1\}$. It follows immediately from Lemma 28 that, for each $n \in \{0, \dots, (k+1)^d - 1\}$, $[G_d, V_{k,d,n+1}] \leq V_{k,d,n}$. A more precise result can be proved.

**Lemma 29.** *Suppose $v \in V_d$. If $\mathrm{ht}_k(v) = r > 0$, then there exists $(j_1, \dots, j_r) \in \{1, \dots, d\}^r$ such that $[v, x_{k,j_1}, \dots, x_{k,j_r}] \neq 0$.*

*Proof.* We may work by induction on $r$ so it suffices to prove that there exists $i \in \{1, \dots, d\}$ such that $\mathrm{ht}_k([v, x_{k,i}]) = r-1$. Since $\mathrm{ht}_k(v) = r$, there exist $i \in \{1, \dots, d\}$ and $\overline{\omega} = \gamma(b_1, \dots, b_d) \in \mathrm{supp}(v)$ with $\mathrm{ht}_k(\overline{\omega}) = r$, $b_i \neq 0$ and $b_j = 0$ if $j > i$. Let

$$\Lambda = \{\omega = \gamma_d(a_1, \dots, a_d) \in \mathrm{supp}(v) \mid a_i \neq 0 \text{ and } \mathrm{ht}_k(\omega) = r\}.$$

For $\omega = \gamma_d(a_1, \dots, a_d) \in \Lambda$, define $\omega^* = \gamma_d(a_1, \dots, a_i - 1, a_{i+1} + k, \dots, a_d + k)$. Notice that $\mathrm{ht}_k(\overline{\omega}^*) = r-1$, that $\mathrm{ht}_k(\omega^*) \leq r-1$ for every $\omega \in \Lambda$ and that $\omega_1^* \neq \omega_2^*$ if $\omega_1 \neq \omega_2$. If follows from Lemma 28 that

$$[v, x_{k,i}] \equiv \sum_{\omega \in \Lambda} \lambda_\omega \omega^* \mod V_{k,d,r-1}$$

and consequently $\mathrm{ht}_k([v, x_{k,i}]) = r-1$. □

**Theorem 30.** $\mathrm{nc}(X_{k,d}) = (k+1)^{d-1}$.

*Proof.* Notice that

$$\mathrm{ht}_k(x_{k,d}) = \mathrm{ht}_k(\gamma_{d-1}(k, \dots, k)) = k(1 + (k+1) + \cdots + (k+1)^{d-2}) = (k+1)^{d-1} - 1.$$

Therefore if follows from Lemma 29 that $\mathrm{nc}(X_{k,d}) \geq (k+1)^{d-1}$. On the other hand, by Lemma 13, $X_{k,d}$ acts faithfully on the submodule $U_d$ of $V_d$ generated by $\gamma_d(1, 0, \dots, 0)$. We have $\mathrm{ht}_k(\gamma_d(1, 0, \dots, 0)) = (k+1)^{d-1}$ so $U_d \leq V_{k,d,(k+1)^{d-1}+1}$. For $i \in \{0, \dots, (k+1)^{d-1} + 1\}$ let $U_{d,i} = V_{k,d,i} \cap U_d$. It follows from Lemma 28 that $X_{k,d}$ stabilizes the chain $0 = U_{d,0} \leq \cdots \leq U_{d,(k+1)^{d-1}+1} = U_d$. Therefore $\mathrm{nc}(H_d) \leq (k+1)^{d-1}$ by Proposition 11. □

## References


1. Susan Evans-Riley, M. F. Newman, and Csaba Schneider, *On the soluble length of groups with prime-power order*, Bull. Austral. Math. Soc. **59** (1999), no. 2, 343–346.
2. S. P. Glasby, *The shape of solvable groups with odd order*, Groups St. Andrews 2005. Vol. 2, London Math. Soc. Lecture Note Ser., vol. 340, Cambridge Univ. Press, Cambridge, 2007, pp. 432–437.
3. B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967.
4. Avinoam Mann, *The derived length of p-groups*, J. Algebra **224** (2000), no. 2, 263–267.
5. Csaba Schneider, *The derived series of a finite p-group*, J. Algebra **307** (2007), no. 1, 136–152.

Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy.
*E-mail address*: crestani@math.unipd.it

Dipartimento di Matematica, Via Trieste 63, 35121 Padova, Italy.
*E-mail address*: lucchini@math.unipd.it