

A CLASSIFICATION OF THE FINITE 2-GENERATOR CYCLIC-BY-ABELIAN GROUPS OF PRIME-POWER ORDER

OSNEL BROCHE, DIEGO GARCÍA-LUCAS AND ÁNGEL DEL RÍO

ABSTRACT. We classify the finite 2-generator cyclic-by-abelian groups of prime-power order. We associate to each such group G a list $\text{inv}(G)$ of numerical group invariants which determines the isomorphism type of G . Then we describe the set formed by all the possible values of $\text{inv}(G)$. This allows us to develop practical algorithms to construct all finite non-abelian 2-generator cyclic-by-abelian groups of a given prime-power order, to compute the invariants of such a group, and to decide whether two such groups are isomorphic.

1. INTRODUCTION

Classifying groups up to isomorphism is a fundamental problem in Group Theory, already identified in the seminal work of Cayley on finite groups [Cay78] where he wrote: “The general problem is to find all the groups of a given order”. Unfortunately, an answer to this question is far from attainable unless one restricts to particularly well behaved groups such as, for example, abelian finitely generated groups, or finite metacyclic groups (see e.g. [Hem00, GBR] for the latter case). The special case of groups of prime-power order is particularly difficult as was observed by P. Hall in [Hal40, page 131]: “To put it crudely, there is no apparent limit to the complication of a prime-power group. [...] And it seems unlikely that it will be possible to compass the overwhelming variety of prime-power groups within the bounds of a single finite system of formulae”. This is illustrated, for example, by the 33 pages that Blackburn required to classify the finite p -groups with derived subgroup of order p [Bla99]. A different approach aims at a classification of the p -groups of a given order. This is completed up to p^7 , for p odd, and up to order 2^9 [OVL05, EO99].

Besides the basic interest in classifying, up to isomorphism, the groups of a particular type, such classifications are often vital in addressing other questions. Our initial motivation was trying to solve the Modular Isomorphism Problem for finite 2-generator cyclic-by-abelian p -groups: this paper paved the way to find a negative solution for this problem [GLMR22] for $p = 2$ and has been essential in obtaining some positive results for $p > 2$ [GLdRS22].

A classification of the finite 2-generator cyclic-by-abelian p -groups is available in the literature if p is odd [Mie75, Son13] or if the groups are assumed to be of class 2 [AMM12]. The aim of this paper is to fill this gap. More precisely we give a complete classification of such groups up to isomorphism, by associating to such a group G a tuple of integers

$$\text{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$$

such that if H is another such group then $G \cong H$ if and only if $\text{inv}(G) = \text{inv}(H)$, and describe the possible values of $\text{inv}(G)$. As the classification is known for p odd, the reader may wonder why we do not restrict our treatment to the case $p = 2$. There is no reduction of complexity by considering only the case $p = 2$, and hence for completeness we prefer to present the results in the general case. We followed the approach of Miech because it adapts better to the application we had in mind, namely the Modular Isomorphism Problem. Along the way we fix mistakes in Miech’s classification (see Remark 3.3). While the Miech and Song classifications split into various families depending on parameters with no obvious group theoretical interpretation, we present a unified presentation for the group G in terms of the entries of $\text{inv}(G)$ (see (1.4), (1.1) and (1.3)) and the group theoretical role of each entry of $\text{inv}(G)$ is clear from the definition. This provides a practical algorithm to compute all the groups under consideration and to implement their

2020 *Mathematics Subject Classification.* 20D15.

Key words and phrases. Finite p -groups.

The first author was partially supported by Fundación Séneca of Murcia under a Jiménez de la Espada grant 20598/IV/18. The third author was partially supported by Grant 19880/GERM/15 funded by Fundación Séneca of Murcia. The second and third authors were partially supported by Grant PID2020-113206GB-I00 funded by MCIN/AEI/10.13039/501100011033.

construction in GAP [GAP22]. It also allows us to compute the invariants associated to a given group and hence to decide if two such groups are isomorphic. We have implemented this and, with the help of the GAP package ANUPQ [GNOH22], we have verified that our results agree with the output of the p -group generation algorithm [O'B90] up to orders $2^{12}, 3^{11}, 5^{10}, 7^9, 11^8, 13^7$ and 23^8 .

To present our main result we fix some notation, and at the same time we outline our strategy. Let G be a finite non-abelian 2-generator cyclic-by-abelian group of prime-power order. By the Burnside Basis Theorem [Rob82, 5.3.2], G/G' is 2-generator and non-cyclic, and the first four invariants p, m, n_1 and n_2 of G are given by

$$|G'| = p^m \quad \text{and} \quad G/G' \cong C_{p^{n_1}} \times C_{p^{n_2}}, \quad \text{with } n_1 \geq n_2.$$

A *basis* of G is an ordered pair $b = (b_1, b_2)$ of elements of G satisfying

$$G/G' = \langle b_1 G' \rangle \times \langle b_2 G' \rangle \quad \text{and} \quad |b_i G'| = p^{n_i} \quad (i = 1, 2).$$

Let \mathcal{B} denote the set of bases of G . Each basis determines a list of eight integers, and our strategy selects bases so that the associated lists satisfy an extreme condition with respect to a well order. This provides the remaining eight entries of $\text{inv}(G)$. To define the integers associated to a basis, we first define two maps $\sigma : G \rightarrow \{1, -1\}$ and $o : G \rightarrow \{0, 1, \dots, m-1\}$ as follows:

$$\begin{aligned} \sigma(g) &= \begin{cases} -1, & \text{if } a^g = a^{-1} \neq a \text{ for some } a \in G'; \\ 1, & \text{otherwise.} \end{cases} \\ o(g) &= \begin{cases} 0, & \text{if } a^g = a^{-1} \text{ for every } a \in G'; \\ \log_p |gC_G(G')|, & \text{otherwise.} \end{cases} \end{aligned}$$

So each basis (b_1, b_2) of G yields four integers $\sigma(b_i)$ and $o(b_i)$, $i = 1, 2$ and we use this to define the next four entries of $\text{inv}(G)$ by setting

$$\sigma o = (\sigma_1, \sigma_2, o_1, o_2) = \min_{\text{lex}} \{(\sigma(b_1), \sigma(b_2), o(b_1), o(b_2)) : (b_1, b_2) \in \mathcal{B}\}$$

where \min_{lex} denotes the minimum with respect to the lexicographical order. Let r_1 and r_2 be the unique integers $1 < r_i \leq 1 + p^m$ satisfying

$$(1.1) \quad r_1 \equiv \sigma_1(1 + p^{m-o_1}) \pmod{p^m} \quad \text{and} \quad \begin{cases} r_2 \equiv \sigma_2(1 + p^{m-o_2}) \pmod{p^m}, & \text{if } o_1 o_2 = 0; \\ r_2 \equiv \sigma_2(1 + p^{m-o_1})^{p^{o_1-o_2}} \pmod{p^m}, & \text{otherwise.} \end{cases}$$

Observe that the classes modulo p^m represented by r_i and $\sigma_i + p^{m-o_i}$ generate the same subgroup in the group of units of $\mathbb{Z}/p^m\mathbb{Z}$.

Let

$$\mathcal{B}_r = \{(b_1, b_2) \in \mathcal{B} : a^{b_i} = a^{r_i} \text{ for every } i = 1, 2 \text{ and } a \in G'\}.$$

In Proposition 2.3, we prove that \mathcal{B}_r is not empty. From now on, we only use bases in \mathcal{B}_r and for each $b = (b_1, b_2) \in \mathcal{B}_r$ we denote by $t_1(b)$ and $t_2(b)$ the unique integers satisfying

$$(1.2) \quad 1 \leq t_i(b) \leq p^m \quad \text{and} \quad b_i^{p^{n_i}} = [b_2, b_1]^{t_i(b)} \quad (i = 1, 2).$$

Define $o'(b) = (o'_1(b), o'_2(b))$ and $u(b) = (u_2(b), u_1(b))$ by setting

$$o'_i(b) = \log_p(|b_i|) - n_i \quad \text{and} \quad t_i(b) = u_i(b)p^{m-o'_i(b)}.$$

Observe that $|b_i| = p^{n_i+o'_i(b)}$ and hence $0 \leq o'_i(b) \leq m$ and $p \nmid u_i(b)$. We use this to define the next two entries of $\text{inv}(G)$ by setting

$$(o'_1, o'_2) = \max_{\text{lex}} \{o'(b) : b \in \mathcal{B}_r\}.$$

Then we define

$$\mathcal{B}'_r = \{b \in \mathcal{B}_r : o'(b) = (o'_1, o'_2)\}.$$

The two remaining entries of $\text{inv}(G)$ are given by

$$(u_2, u_1) = \min_{\text{lex}} \{u(b) : b \in \mathcal{B}'_r\}.$$

The “unnatural” order on the u ’s is not a typo but a convenient technicality. Observe that we abuse notation since o'_i, u_i and t_i sometimes denote functions and sometimes integers related to those functions. This does not cause confusion because in the former case the functions always appear with arguments.

Set

$$(1.3) \quad t_i = u_i p^{m-o'_i} \quad (i = 1, 2).$$

Now G is isomorphic to \mathcal{G}_I , where I is an abbreviation for $(p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$ and

$$(1.4) \quad \mathcal{G}_I = \langle b_1, b_2 \mid [b_2, b_1]^{p^m} = 1, \quad [b_2, b_1]^{b_i} = [b_2, b_1]^{r_i}, \quad b_i^{p^{n_i}} = [b_2, b_1]^{t_i}, \quad (i = 1, 2) \rangle,$$

where r_i and t_i are as defined in (1.1) and (1.3).

Hence, G is completely determined up to isomorphism by $\text{inv}(G)$. Therefore, to obtain our classification it only remains to give the list of tuples occurring as $\text{inv}(G)$.

Main Theorem. *The maps $[G] \mapsto \text{inv}(G)$ and $I \mapsto [\mathcal{G}_I]$ define mutually inverse bijections between the set of isomorphism classes of finite non-abelian 2-generator cyclic-by-abelian groups of prime-power order and the set of lists of integers $(p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$ satisfying the following conditions.*

- (1) p is prime and $n_1 \geq n_2 \geq 1$.
- (2) $\sigma_i = \pm 1$, $0 \leq o_i < \min(m, n_i)$ and $p \nmid u_i$ for $i = 1, 2$.
- (3) If $p = 2$ and $m \geq 2$ then $o_i < m - 1$ for $i = 1, 2$.
- (4) $0 \leq o'_i \leq m - o_i$ for $i = 1, 2$ and $o'_1 \leq m - o_2$.
- (5) One of the following conditions holds:
 - (a) $o_1 = 0$.
 - (b) $0 < o_1 = o_2$ and $\sigma_2 = -1$.
 - (c) $o_2 = 0 < o_1$ and $n_2 < n_1$.
 - (d) $0 < o_2 < o_1 < o_2 + n_1 - n_2$.
- (6) Suppose that $\sigma_1 = 1$. Then the following conditions hold:
 - (a) $\sigma_2 = 1$ and $o_2 + o'_1 \leq m \leq n_1$.
 - (b) Either $o_1 + o'_2 \leq m \leq n_2$ or $2m - o_1 - o'_2 = n_2 < m$ and $u_2 \equiv 1 \pmod{p^{m-n_2}}$.
 - (c) If $o_1 = 0$ then either
 - (i) $o'_1 \leq o'_2 \leq o'_1 + o_2 + n_1 - n_2$ and $\max(p - 2, o'_2, n_1 - m) > 0$, or
 - (ii) $p = 2$, $m = n_1$, $o'_2 = 0$ and $o'_1 = 1$.
 - (d) If $o_2 = 0 < o_1$ then $o'_1 + \min(0, n_1 - n_2 - o_1) \leq o'_2 \leq o'_1 + n_1 - n_2$ and $\max(p - 2, o'_1, n_1 - m) > 0$.
 - (e) If $0 < o_2 < o_1$ then $o'_1 \leq o'_2 \leq o'_1 + n_1 - n_2$.
 - (f) $1 \leq u_1 \leq p^{a_1}$, where

$$a_1 = \min(o'_1, o_2, o_2 + n_1 - n_2 + o'_1 - o'_2).$$

- (g) One of the following conditions holds:
 - (i) $1 \leq u_2 \leq p^{a_2}$.
 - (ii) $o_1 o_2 \neq 0$, $n_1 - n_2 + o'_1 - o'_2 = 0 < a_1$, $1 + p^{a_2} \leq u_2 \leq 2p^{a_2}$, and $u_1 \equiv 1 \pmod{p}$, where

$$a_2 = \begin{cases} 0, & \text{if } o_1 = 0; \\ \min(o_1, o'_2, o'_2 - o'_1 + \max(0, o_1 + n_2 - n_1)), & \text{if } o_2 = 0 < o_1; \\ \min(o_1 - o_2, o'_2 - o'_1), & \text{otherwise.} \end{cases}$$

- (7) Suppose that $\sigma_1 = -1$. Then the following conditions hold:
 - (a) $p = 2$, $m \geq 2$, $o'_1 \leq 1$ and $u_1 = 1$.
 - (b) If $\sigma_2 = 1$ then $n_2 < n_1$ and the following conditions hold:
 - (i) If $m \leq n_2$ then $o'_2 \leq 1$, $u_2 = 1$ and either $o'_1 \leq o'_2$ or $o_2 = 0 < n_1 - n_2 < o_1$
 - (ii) If $m > n_2$ then $m + 1 = n_2 + o'_2$, $u_2(1 + 2^{m-o_1-1}) \equiv -1 \pmod{2^{m-n_2}}$, $1 \leq u_2 \leq 2^{m-n_2+1}$, either $o'_1 = 1$ or $o_1 + 1 \neq n_1$, and at least one of the following conditions holds:
 - $o'_1 = 0$ and either $o_1 = 0$ or $o_2 + 1 \neq n_2$.
 - $o'_1 = 1$, $o_2 = 0$ and $n_1 - n_2 < o_1$.
 - $u_2 \leq 2^{m-n_2}$.
 - (c) If $\sigma_2 = -1$ then $o'_2 \leq 1$, $u_2 = 1$ and the following conditions hold:
 - (i) If $o_1 \leq o_2$ and $n_1 > n_2$ then $o'_1 \leq o'_2$.
 - (ii) If $o_1 = o_2$ and $n_1 = n_2$ then $o'_1 \geq o'_2$.
 - (iii) If $o_2 = 0 < o_1 = n_1 - 1$ and $n_2 = 1$ then $o'_1 = 1$ or $o'_2 = 1$.
 - (iv) If $o_2 = 0 < o_1$ and $n_1 \neq o_1 + 1$ or $n_2 \neq 1$ then $o'_1 + \min(0, n_1 - n_2 - o_1) \leq o'_2$.

(v) If $o_1 o_2 \neq 0$ and $o_1 \neq o_2$ then $o'_1 \leq o'_2$.

We now outline the structure of the paper. The goal of Sections 2-5 is to find necessary conditions on a tuple $I = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$ to be realizable as $\text{inv}(G)$ for some finite non-abelian 2-generator cyclic-by-abelian group G of prime-power order. The proof of the Main Theorem concludes in Section 6, where it is shown that the set of conditions we obtain – those described in the Main Theorem – suffices for the realizability of I . To find the necessary conditions we fix a finite non-abelian 2-generator cyclic-by-abelian p -group G with $\text{inv}(G) = I$. Suppose that $b \in \mathcal{B}$. In Lemma 2.2 we find a set of conditions in terms of $p, m, n_1, n_2, \sigma_1(b), \sigma_2(b), o_1(b)$ and $o_2(b)$ equivalent to $(\sigma(b_1), \sigma(b_2), o(b_1), o(b_2)) = (\sigma_1, \sigma_2, o_1, o_2)$. These conditions, substituting $\sigma_i(b)$ and $o_i(b)$ by σ_i and o_i , are added to the set of necessary conditions on I . We close Section 2 with some additional conditions on I . Section 3 is a technical preparation for the next two sections. In Lemmas 4.2, 4.3 and 4.4 we describe, for $b \in \mathcal{B}_r$, a set of conditions, in terms only of the first 8 entries of $\text{inv}(G)$ and of $o'_1(b)$ and $o'_2(b)$, equivalent to $(o'_1, o'_2) = (o'_1(b), o'_2(b))$. These conditions, substituting $o'_i(b)$ by o'_i , are added to our set of necessary conditions. The same is done for $u_i(b)$ and u_i in Lemmas 5.1 and 5.2. We emphasize that in these lemmas we prove equivalences, and not mere implications, because it is useful in the subsequent steps. Moreover, their proofs are the base of an algorithm, implemented in [BCGLdR22], to compute $\text{inv}(G)$ in an apparently efficient way. In Section 7 we discuss our implementation in GAP of our classification and report some experiments which support the correctness of the Main Theorem. In Appendix A we collect technical number theoretical results used frequently in the proofs of Sections 2 and 3.

2. FIXING THE r_i 'S AND CONSTRAINTS ON THE INVARIANTS

In this section we obtain some restrictions on the invariants of our target groups and we prove the existence of a basis (b_1, b_2) such that $[b_2, b_1]^{b_i} = [b_2, b_1]^{r_i}$, where r_i is defined by (1.1).

We start with some notation. If p is a prime integer and n is a non-zero integer then $v_p(n)$ denotes the largest integer m with $p^m \mid n$. We set $v_p(0) = \infty$. If m is an integer coprime to n then $o_m(n)$ denotes the multiplicative order of n modulo m , i.e. the minimum positive integer k such that $n^k \equiv 1 \pmod{m}$. We use \leq_{lex} to denote the lexicographic order on lists of integers of the same length and \min_{lex} and \max_{lex} denote the minimum and maximum with respect to \leq_{lex} , respectively.

We use standard group theoretical notation. For example, the cyclic group of order n is denoted C_n and if G is a group then G' denotes its derived subgroup. For $g, h \in G$

$$g^h = h^{-1}gh, \quad [g, h] = g^{-1}h^{-1}gh, \quad |g| = \text{order of } g.$$

If G' is cyclic and $g \in G$ then $r(g)$ denotes an integer, unique modulo $|G'|$, such that $a^g = a^{r(g)}$ for every $a \in G'$.

Given integers s, t and n with $n \geq 0$ we set

$$\mathcal{S}(s \mid n) = \sum_{i=0}^{n-1} s^i \quad \text{and} \quad \mathcal{T}(s, t \mid n) = \sum_{0 \leq i < j < n} s^i t^j.$$

This notation is motivated by the following lemma whose proof is straightforward. More properties of these operators are included in Appendix A.

Lemma 2.1. *If G is a cyclic-by-abelian group then the following equalities hold:*

$$(2.1) \quad [x_1 \cdots x_n, y_1 \cdots y_m] = \prod_{i=1}^n \prod_{j=1}^m [x_i, y_j]^{x_{i+1} \cdots x_n y_{j+1} \cdots y_m} \quad (x_1, \dots, x_n, y_1, \dots, y_m \in G),$$

$$(2.2) \quad (ga)^n = g^n a^{\mathcal{S}(r(g)|n)} \quad (g \in G, a \in G'),$$

$$(2.3) \quad (gh)^n = g^n h^n [h, g]^{\mathcal{T}(r(g), r(h)|n)} \quad (g, h \in G).$$

In the remainder of the paper G is a finite non-abelian 2-generator cyclic-by-abelian group of prime-power order and

$$\text{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2).$$

Observe that

$$(2.4) \quad \sigma(g) = -1 \quad \text{if and only if} \quad p = 2, m \geq 2 \text{ and } r(g) \equiv -1 \pmod{4}.$$

As $r(g)$ is coprime to p and uniquely determined modulo p^m , we abuse notation by identifying $r(g)$ with an element of \mathcal{U}_{p^m} , the group of units of $\mathbb{Z}/p^m\mathbb{Z}$, and use standard group theoretical notation for the $r(g)$'s. For example, $|r(g)| = o_{p^m}(r(g))$ and $\langle r(g_1), r(g_2), \dots, r(g_k) \rangle$ denotes the group generated by the $r(g_i)$'s in \mathcal{U}_{p^m} , for $g_1, \dots, g_k \in G$. Then $g \mapsto r(g)$ defines a group homomorphism $G \rightarrow \mathcal{U}_{p^m}$ with kernel $C_G(G')$ and image contained in the Sylow p -subgroup of \mathcal{U}_{p^m} . In particular

$$|gC_G(G')| = o_{p^m}(r(g)),$$

and hence

$$(2.5) \quad o(g) = \begin{cases} 0, & \text{if } r(g) \equiv -1 \pmod{p^m}; \\ \log_p(o_{p^m}(r(g))), & \text{otherwise.} \end{cases}$$

Therefore, $|gC_G(G')| = p^e$ with $0 \leq e \leq m-1$ and if $p=2$ and $m \geq 3$ then $e \leq m-2$. Furthermore, if $p=2$, $m=2$ and $e=1$ then $r(g) \equiv -1 \pmod{4}$ and hence $o(g) = 0$. This implies that

$$(2.6) \quad 0 \leq o_i < m \quad \text{and} \quad \text{if } p=2 \text{ and } m \geq 2 \text{ then } o_i \leq m-2.$$

If p is odd or $m \leq 2$ then \mathcal{U}_{p^m} is cyclic and its subgroup of order p^e for $e \leq m-1$ is $\langle 1 + p^{m-e} \rangle$. If $m \geq 3$ then $\mathcal{U}_{2^m} = \langle 5 \rangle \times \langle -1 \rangle$ with $o_{2^m}(5) = 2^{m-2}$ and $o_{2^m}(-1) = 2$. Thus, in this case, \mathcal{U}_{2^m} has exactly three subgroups of order 2, namely $\langle -1 \rangle$, $\langle 1 + 2^{m-1} \rangle$ and $\langle -1 + 2^{m-1} \rangle$, and exactly two cyclic subgroups of order p^e for $e \in \{2, \dots, m-2\}$, namely $\langle 1 + 2^{m-e} \rangle$ and $\langle -1 + 2^{m-e} \rangle$. Hence $\langle r(g) \rangle$ is determined by $o(g)$ and $\sigma(g)$; namely,

$$(2.7) \quad \langle r(g) \rangle = \langle \sigma(g)(1 + p^{m-o(g)}) \rangle = \langle \sigma(g) + p^{m-o(g)} \rangle.$$

Moreover, if $g, h \in G$ and $o(g) \leq o(h)$ then there exists an integer x such that $p \nmid x$ and

$$r(gh^{-xp^{o(h)-o(g)}}) \equiv \pm 1 \pmod{p^m},$$

with negative sign occurring exactly when $p=2$, $m \geq 3$ and either $\sigma(g) = -1$ and $o(h) > o(g)$, or $o(h) = o(g)$ and $\sigma(g) \neq \sigma(h)$. We will use this without specific mention.

Another fact that we will use without specific mention is the following: if $(b_1, b_2) \in \mathcal{B}$ then

$$\mathcal{B} = \{(b_1^{x_1} b_2^{y_1} [b_2, b_1]^{z_1}, b_1^{x_2} b_2^{y_2} [b_2, b_1]^{z_2}) : x_i, y_i, z_i \in \mathbb{Z}, \text{ and } p^{n_1-n_2} \mid x_2, \text{ and } x_1 y_2 \not\equiv x_2 y_1 \pmod{p}\}.$$

Our first objective is to characterize the elements b of \mathcal{B} for which $(\sigma(b_1), \sigma(b_2), o(b_1), o(b_2))$ achieves the maximum σo , i.e. the elements of the following set:

$$\mathcal{B}' = \{b \in \mathcal{B} : \sigma o = (\sigma(b_1), \sigma(b_2), o(b_1), o(b_2))\}.$$

Lemma 2.2. *Let $b = (b_1, b_2) \in \mathcal{B}$. Then $b \in \mathcal{B}'$ if and only if the following conditions hold:*

- (1) *If $\sigma(b_1) = 1$ then $\sigma(b_2) = 1$.*
- (2) *If $n_1 = n_2$ then $\sigma(b_1) = \sigma(b_2)$.*
- (3) *One of the following conditions holds:*
 - (a) $o(b_1) = 0$.
 - (b) $0 < o(b_1) = o(b_2)$ and $\sigma(b) = (-1, -1)$.
 - (c) $0 = o(b_2) < o(b_1)$ and $n_2 < n_1$.
 - (d) $0 < o(b_2) < o(b_1) < o(b_2) + n_1 - n_2$. In particular, $n_2 < n_1$.

Proof. Suppose that $b \in \mathcal{B}'$. Our usual approach is the following: if one of the conditions does not hold, then we construct $(\bar{b}_1, \bar{b}_2) \in \mathcal{B}$ with $(\sigma(\bar{b}_1), \sigma(\bar{b}_2), o(\bar{b}_1), o(\bar{b}_2)) >_{\text{lex}} (\sigma(b_1), \sigma(b_2), o(b_1), o(b_2))$.

If $\sigma(b_1) = 1$ and $\sigma(b_2) = -1$ then $\bar{b} = (b_1 b_2, b_2) \in \mathcal{B}$ and $-1 = \sigma(\bar{b}_1) < \sigma(b_1)$ contradicting the minimality. This proves (1).

If $n_1 = n_2$ and $\sigma(b_1) \neq \sigma(b_2)$ then $\sigma(b_1) = -1$ and $\sigma(b_2) = 1$. Then $\bar{b} = (b_1, b_1 b_2) \in \mathcal{B}$ with $\sigma(\bar{b}_1) = \sigma(\bar{b}_2)$ and $\sigma(\bar{b}_2) = -1 < \sigma(b_2)$, contradicting the minimality. This proves (2).

Assume first that $o(b_2) \geq o(b_1)$. Then $r(b_1 b_2^{-xp^{o(b_2)-o(b_1)}}) \equiv \pm 1 \pmod{p^m}$ for some integer x such that $p \nmid x$, with negative sign occurring exactly when $p=2$, $\sigma(b_1) = -1$ and either $\sigma(b_2) = 1$ or $o(b_2) > o(b_1)$. Then $\bar{b} = (b_1 b_2^{-xp^{o(b_2)-o(b_1)}}, b_2) \in \mathcal{B}$ and hence $o(\bar{b}_1) = 0$. If moreover $\sigma(b_1) = 1$ then $\sigma(\bar{b}_1) = \sigma(b_1)$ and hence, since $\sigma(b_2) = \sigma(\bar{b}_2)$, necessarily $o(b_1) = 0$. If $\sigma(b_1) = -1$, and either $\sigma(b_2) = 1$ or $o(b_2) > o(b_1)$ then also $\sigma(\bar{b}_1) = -1$ so $o(b_1) = 0$. Thus in this case either (3a) or (3b) holds.

Now assume that $o(b_1) > o(b_2)$. This implies that $n_2 < n_1$, since otherwise both $\bar{b} = (b_2, b_1)$ and $\hat{b} = (b_1, b_1 b_2)$ belong to \mathcal{B} , and we obtain a contradiction because if $\sigma(b_2) = \sigma(b_1)$ then $\sigma(\bar{b}_1) = \sigma(b_2) = \sigma(b_1)$ and $o(\bar{b}_1) = o(b_2) < o(b_1)$, contradicting the minimality, and if $\sigma(b_1) \neq \sigma(b_2)$ then $\sigma(b_1) = \sigma(\hat{b}_1)$ and $\sigma_2(\hat{b}) = -1 < \sigma(b_2)$. Thus, if $o(b_2) = 0$ then condition (3c) holds. Assume otherwise, so $o(b_2) \neq 0$ and let x be an integer coprime to p such that $r(b_2 b_1^{-x p^{o_1 - o_2}}) \equiv \pm 1 \pmod{p^m}$. If $o(b_2) + n_1 - n_2 \leq o(b_1)$ then $\bar{b} = (b_1, b_1^{-x p^{o(b_1) - o(b_2)}} b_2) \in \mathcal{B}$, $\sigma(\bar{b}_1) = \sigma(b_1)$, $\sigma(\bar{b}_2) = \sigma(b_2)$, $o(\bar{b}_1) = o(b_1)$, and $o(\bar{b}_2) = 0 < o(b_2)$, a contradiction. Thus $o(b_1) < o(b_2) + n_1 - n_2$ and condition (3d) holds.

Conversely, assume that b satisfies conditions (1)-(3) and let $s_i = r(b_i)$ for $i = 1, 2$. By minimality, $(\sigma_1, \sigma_2, o_1, o_2) \leq_{\text{lex}} (\sigma(b_1), \sigma(b_2), o(b_1), o(b_2))$ and we must prove that equality holds. To this end fix $\bar{b} \in \mathcal{B}'$, and take integers x_i and y_i such that $\bar{b}_i G' = b_1^{x_i} b_2^{y_i} G'$ for $i = 1, 2$. Thus $o_i = o_i(\bar{b})$, $\sigma_i = \sigma_i(\bar{b})$ and $r(\bar{b}_i) \equiv s_1^{x_i} s_2^{y_i} \pmod{p^m}$.

Of course, if $\sigma(b_1) = -1$ then $\sigma(b_1) = \sigma_1$. Otherwise, $\sigma(b_1) = \sigma(b_2) = 1$ by condition (1), and hence $\sigma_i(\bar{b}) = 1$ for $i = 1, 2$. This proves that $\sigma(b_1) = \sigma_1$.

If $\sigma(b_2) \neq \sigma_2$ then $\sigma(b_1) = -1 = \sigma_1$ and $\sigma(b_2) = 1$. Then $p = 2$, $n_1 \neq n_2$ by (2), and hence x_2 is even and y_2 is odd, which implies that $\sigma(b_2) = \sigma_2$, a contradiction. Thus $\sigma(b_2) = \sigma_2$.

By means of contradiction suppose that $o_1 < o(b_1)$. In particular $o(b_1) \neq 0$, i.e. b does not satisfy (3a). Suppose that condition (3b) holds. Then $o(b_1) = o(b_2)$ and $\sigma_1 = \sigma(b_1) = \sigma(b_2) = -1$. Thus $p = 2$, $m \geq 2$ and $\langle s_1 \rangle = \langle s_2 \rangle$. Therefore $s_1 \equiv s_2 \pmod{4}$ and hence $s_1^{x_1 + y_1} \equiv s_1^{x_1} s_2^{y_1} \equiv r(\bar{b}_1) \equiv -1 \pmod{4}$. Then $x_1 \not\equiv y_1 \pmod{2}$ and therefore $|\bar{b}_1 C_G(G')| = |b_1 C_G(G')| = 2^{o(b_1)} \neq 2^{o_1}$. Thus, by (2.5), $o_1 = 0$ and $s_1^{x_1} s_2^{y_1} \equiv -1 \pmod{2^m}$. As $o(b_1) = o(b_2) > o_1$ and $x_1 \not\equiv y_1 \pmod{2}$, it follows that $o(b_1) = o(b_2) = 1$, $m \geq 3$ and either $2 \nmid x_1$ and $s_1 \equiv -1 + 2^{m-1} \pmod{2^m}$ or $2 \nmid y_1$ and $s_2 \equiv -1 + 2^{m-1} \pmod{2^m}$. In both cases $-1 \equiv -1 + 2^{m-1} \pmod{2^m}$, a contradiction. This proves that $o(b_2) < o(b_1)$ and $n_2 < n_1$. Therefore $p \mid x_2$, so $p \nmid x_1 y_2$ and $|\bar{b}_1 C_G(G')| = o_{p^m}(s_1^{x_1} s_2^{y_1}) = o_{p^m}(s_1) = p^{o(b_1)} \neq p^{o_1}$. Again this implies that $o_1 = 0$, $\sigma_1 = -1$ and $o(b_1) = 1$, so $o(b_2) = 0$ and $-1 \equiv s_1^{x_1} s_2^{y_1} \equiv \pm s_1 \pmod{2^m}$ which is not possible because $s_1 \notin \langle -1 \rangle$, as $o(b_1) = 1$. This proves that $o_1 = o(b_1)$.

Finally if, $o_2 \neq o(b_2)$ then $o(b_2) \neq 0$. Hence b does not satisfy (3c). If $o_1 = 0$ then $\pm 1 \equiv \pm s_2^{y_1} \pmod{p^m}$ and the signs must agree for otherwise $p = 2$, $m \geq 2$ and $-1 \equiv s_2^{y_1} \pmod{2^m}$ which is only possible if y_1 is odd and $s_2 \equiv -1 \pmod{2^m}$ contradicting $o(b_2) \neq 0$, i.e. b does not satisfy (3a). If $o_1 = o_2$ then $o(b_1) = o_1 = o_2 < o(b_2)$ and hence, by assumption, $o_1 = 0$, which we have just seen is not possible. Thus b does not satisfy (3b) either. Hence, (3d) holds, i.e. $0 < o(b_2) < o(b_1) < o(b_2) + n_1 - n_2$. Thus $p^{o(b_1) - o(b_2) + 1} \mid x_2$ and $p \nmid y_2$. Therefore $p^{o_2} < p^{o(b_2)} = o_{p^m}(s_2) = o_{p^m}(s_1^{x_2} s_2^{y_2}) = o_{p^m}(r(\bar{b}_2))$. Then, by (2.5), $p = 2$, $o_2 = 0$, $o(b_2) = 1$ and $\sigma_2 = -1$, yielding the following contradiction:

$$-1 \equiv r(\bar{b}_2) \equiv s_1^{x_2} s_2^{y_2} \equiv -1 + 2^{m-1} \pmod{2^m}.$$

Hence $o_2 = o(b_2)$. □

Proposition 2.3. *Let p be a prime integer and let G be a non-abelian group with $G' \cong C_{p^m}$ and $G/G' \cong C_{p^{n_1}} \times C_{p^{n_2}}$ with $n_2 \leq n_1$. Let $\sigma o = (\sigma_1, \sigma_2, o_1, o_2)$ and let r_1 and r_2 be given as in (1.1).*

- (1) *If $p \neq 2$ then $\sigma_1 = 1$.*
- (2) *If $\sigma_1 = 1$ then $\sigma_2 = 1$.*
- (3) *If $n_1 = n_2$ then $\sigma_1 = \sigma_2$.*
- (4) *One of the following conditions holds:*
 - (a) $o_1 = 0$.
 - (b) $0 < o_1 = o_2$ and $\sigma_1 = \sigma_2 = -1$.
 - (c) $0 = o_2 < o_1$ and $n_2 < n_1$.
 - (d) $0 < o_2 < o_1 < o_2 + n_1 - n_2$. In particular, $n_2 < n_1$.
- (5) *\mathcal{B} contains an element (b_1, b_2) such that $a^{b_i} = a^{r_i}$ for every $a \in G'$ and $i = 1, 2$.*

Proof. (1) is a direct consequence of (2.4). Statements (2), (3) and (4) follow directly from Lemma 2.2. Fix $(b_1, b_2) \in \mathcal{B}'$. Using (2.7) it easily follows that r_i and $r(b_i)$ generate the same multiplicative group in \mathcal{U}_{p^m} . Thus there are integers x and y with $p \nmid xy$ and $r_i = r(b_i)^{x_i}$. Then $(\bar{b}_1, \bar{b}_2) = (b_1^x, b_2^y) \in \mathcal{B}$ and $r(\bar{b}_i) = r_i$, i.e. $a^{b_i} = a^{r_i}$ for every $a \in G'$. Therefore $(\bar{b}_1, \bar{b}_2) \in \mathcal{B}_r$. □

In Proposition 2.3 we obtained some restrictions on σo . We now obtain some restrictions on the o'_i 's and u_i 's. To this end, we fix $b = (b_1, b_2) \in \mathcal{B}_r$. Recall that $|b_i| = p^{n_i + o'_i(b)}$ and hence

$$(2.8) \quad 0 \leq o'_i(b) = m - v_p(t_i(b)) \leq m, \quad 1 \leq u_i(b) \leq p^{o'_i(b)} \quad \text{and} \quad p \nmid u_i(b) \quad (i = 1, 2).$$

From (1.2) and (2.2) it follows that:

$$(2.9) \quad r_i^{p^{n_i}} \equiv 1 \pmod{p^m},$$

$$(2.10) \quad t_i(b)r_i \equiv t_i(b) \pmod{p^m},$$

$$(2.11) \quad \mathcal{S}(r_1 \mid p^{n_1}) \equiv t_1(b)(1 - r_2) \pmod{p^m},$$

$$(2.12) \quad \mathcal{S}(r_2 \mid p^{n_2}) \equiv t_2(b)(r_1 - 1) \pmod{p^m}.$$

Lemma 2.4. *The following statements hold for every $b \in \mathcal{B}_r$:*

- (1) $o'_i(b) \leq m - o_i$ and if $\sigma_i = -1$ then $o'_i(b) \leq 1$ and $u_i(b) = 1$, for each $i \in \{1, 2\}$.
- (2) $o_i < n_i$, for each $i \in \{1, 2\}$.
- (3) If $\sigma_1 = 1$ then the following conditions hold:
 - (a) $o_2 + o'_1(b) \leq m \leq n_1$ and if $m = n_1$ then $o_1 o_2 = 0$.
 - (b) Either $o_1 + o'_2(b) \leq m \leq n_2$, or $2m - o_1 - o'_2(b) = n_2 < m$ and $u_2(b) \equiv 1 \pmod{p^{m-n_2}}$.
- (4) If $\sigma_1 \neq \sigma_2$ then one of the following conditions hold:
 - (a) $m \leq n_2$ and $o'_2(b) \leq 1$.
 - (b) $m - o'_2(b) + 1 = n_2 < m$, $u_2(b)(1 + 2^{m-o_1-1}) \equiv -1 \pmod{2^{m-n_2}}$ and $1 \leq u_2(b) \leq 2^{m-n_2+1}$.

Proof. For the proof of (1) we fix $i \in \{1, 2\}$. Suppose first that $\sigma_i = -1$. Then $p = 2$, $m \geq 2$ and $r_i \equiv -1 \pmod{4}$, by (2.4). Then $v_2(r_i - 1) = 2$ and from (2.8) and (2.10) it follows that $m - 1 \leq v_2(t_i(b)) = m - o'_i(b)$, so $o'_i(b) \leq 1$ and $o_i + o'_i(b) \leq m - 1$, by (2.6). The former implies that $u_i(b) = 1$. Suppose that $\sigma_i = 1$. Then $v_p(r_i - 1) = m - o_i$ and (2.8) and (2.10) imply that $m \leq v_p(t_i(b)) + v_p(r_i - 1) = 2m - (o_i + o'_i(b))$. This proves (1).

For the proofs of (2), (3) and (4) we consider separately the different values of σ_1 and σ_2 .

Suppose that $\sigma_1 = 1$. Then $\sigma_2 = 1$, by Proposition 2.3 (2). Hence $v_p(r_i - 1) = m - o_i$ and either p is odd or $r_1 \equiv r_2 \equiv 1 \pmod{4}$. Thus $o_{p^m}(r_i) = p^{o_i}$ and $v_p(\mathcal{S}(r_i \mid p^{n_i})) = n_i$, by Lemma A.2 (1). Then $o_i \leq n_i$, by (2.9), and combining this with (2.8), (2.11) and (2.12) we deduce that

$$o_2 + o'_1(b) \leq m \leq n_1 \quad \text{or} \quad n_1 = 2m - o_2 - o'_1(b) < m$$

and

$$o_1 + o'_2(b) \leq m \leq n_2 \quad \text{or} \quad n_2 = 2m - o_1 - o'_2(b) < m.$$

As $n_2 \leq n_1$, if $n_1 < m$ then we obtain a contradiction because

$$2m > n_1 + n_2 = 4m - (o_2 + o'_1(b) + o_1 + o'_2(b)) \geq 2m,$$

by (1). Thus $o_2 + o'_1(b) \leq m \leq n_1$ and hence $o_1 < m \leq n_1$. If $o_2 \geq n_2$ then $n_2 < m$ and hence

$$m \geq o_2 + o'_2(b) \geq n_2 + o'_2(b) = 2m - o_1 > m,$$

a contradiction. This proves (2) in this case. Moreover, if $n_2 < m$ then by (2.12) and Lemma A.1 (3)

$$u_2(b)p^{n_2} \equiv u_2(b)p^{2m-o'_2(b)-o_1} \equiv t_2(b)(r_1 - 1) \equiv \mathcal{S}(r_2 \mid p^{n_2}) \equiv p^{n_2} \pmod{2^m},$$

and hence $u_2(b) \equiv 1 \pmod{p^{m-n_2}}$. Finally assume that $m = n_1$. If $n_2 = n_1$ then $o_1 = 0$, by Proposition 2.3 (4). Otherwise $n_2 < n_1 = m$ and hence $n_2 = 2m - o_1 - o'_2(b)$. Then, by (1),

$$n_1 - n_2 = m - n_2 = -m + o_1 + o'_2(b) \leq o_1 - o_2.$$

Therefore $o_2 = 0$, by Proposition 2.3 (4). This proves (3).

Suppose that $\sigma_2 = -1$. Then $\sigma_1 = -1$, by Proposition 2.3 (2). Hence $p = 2$, $m \geq 2$, $r_i \equiv -1 \pmod{4}$ and $v_2(r_i + 1) = m - o_i$ for $i = 1, 2$. Moreover, $v_p(t_i(b)) = m - o'_i(b) \geq m - 1$, by (1) and therefore $\mathcal{S}(r_i \mid 2^{n_i}) \equiv 0 \pmod{2^m}$ by (2.11) and (2.12). By Lemma A.2 (2)

$$m \leq v_2(\mathcal{S}(r_i \mid 2^{n_i})) = v_2(r_i + 1) + n_i - 1 = m - o_i + n_i - 1,$$

that is $o_i \leq n_i - 1$, proving (2) in this case.

Finally, suppose that $\sigma_1 = -1$ and $\sigma_2 = 1$. Then $p = 2$, $m \geq 2$, $r_1 \equiv -1 \pmod{4}$ and $r_2 \equiv 1 \pmod{4}$. By (1), $o'_1(b) \leq 1$ and hence $v_2(t_1(b)) = m - o'_1(b) \geq m - 1$. Thus $t_1(b)(r_2 - 1) \equiv 0 \pmod{2^m}$ and, by (2.11) and Lemma A.2 (2),

$$m \leq v_2(\mathcal{S}(r_1 | 2^{n_1})) = n_1 + v_2(r_1 + 1) - 1 = n_1 + m - o_1 - 1,$$

i.e. $o_1 \leq n_1 - 1$. Moreover, as $r_2 \equiv 1 \pmod{4}$, by Lemma A.2 (1), $v_2(\mathcal{S}(r_2 | 2^{n_2})) = n_2$ and hence (2.12) implies that either $m \leq n_2$ and $m \leq v_p(t_2(b)) + v_2(r_1 - 1) = m - o'_2(b) + 1$, or $m > n_2 = m - o'_2(b) + 1$. In the former case $o_2 < m \leq n_2$ and $o'_2(b) \leq 1$. In the latter case, by (2.12) and Lemma A.2 (3),

$$u_2(b)2^{n_2}(-1 - 2^{m-o_1-1}) = u_2(b)2^{n_2-1}(-2 - 2^{m-o_1}) = t_2(b)(r_1 - 1) \equiv \mathcal{S}(r_2 | p^{n_2}) \equiv 2^{n_2} \pmod{2^m}.$$

Thus $o_2 \leq m - o'_2(b) < n_2$, which completes the proof of (2), and $u_2(b)(-1 - 2^{m-o_1}) \equiv 1 \pmod{2^{m-n_2}}$, which proves (4). \square

Combining (2.6) and Lemma 2.4 we obtain the following:

Corollary 2.5. *Let G be a finite non-abelian 2-generator cyclic-by-abelian group of prime-power order with $\text{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2)$. Then the following statements hold:*

- (1) $o'_i \leq m - o_i$, $o'_i \leq m - o_2$ and if $\sigma_i = -1$ then $o'_i \leq 1$ and $u_i = 1$.
- (2) $o_i \leq \min(m, n_i) - 1$ and if $p = 2$ and $m \geq 2$ then $o_i \leq m - 2$.
- (3) If $m > n_1$ then $\sigma_1 = -1$.
- (4) If $\sigma_1 = 1$ and $m = n_1$ then $o_1 o_2 = 0$.
- (5) Suppose that $\sigma_1 \neq \sigma_2$.
 - (a) If $m \leq n_2$ then $o'_2 \leq 1$.
 - (b) If $m > n_2$ then $o'_2 = m + 1 - n_2$, $u_2(1 + 2^{m-o_1-1}) \equiv -1 \pmod{2^{m-n_2}}$ and $1 \leq u_2 \leq 2^{m-n_2+1}$.

3. CHANGING BASES WITHIN \mathcal{B}_r

In the previous section we proved that $\mathcal{B}_r \neq \emptyset$. In this section $b = (b_1, b_2) \in \mathcal{B}_r$ and $\bar{b} = (\bar{b}_1, \bar{b}_2)$ with $\bar{b}_i \equiv b_1^{x_i} b_2^{y_i} [b_2, b_1]^{z_i}$, where x_i, y_i and z_i are integers, for $i = 1, 2$.

The next lemma characterizes when \bar{b} belongs to \mathcal{B}_r .

Lemma 3.1. *$\bar{b} \in \mathcal{B}_r$ if and only if the following conditions hold:*

- (1) $p^{n_1-n_2} \mid x_2$ and $x_1 y_2 \not\equiv x_2 y_1 \pmod{p}$.
- (2) If $\sigma_2 = -1$ then $x_1 \not\equiv y_1 \pmod{2}$ and $x_2 \not\equiv y_2 \pmod{2}$.
- (3) (a) If $o_1 = 0$ then $y_1 \equiv y_2 - 1 \equiv 0 \pmod{p^{o_2}}$.
 (b) If $0 < o_1 = o_2$ then $x_1 + y_1 \equiv x_2 + y_2 \equiv 1 \pmod{p^{o_1}}$.
 (c) If $o_2 = 0 < o_1$ then $x_1 - 1 \equiv x_2 \equiv 0 \pmod{p^{o_1}}$.
 (d) If $0 < o_2 < o_1$ then $x_1 + y_1 p^{o_1-o_2} \equiv 1 \pmod{p^{o_1}}$ and $x_2 p^{o_2-o_1} + y_2 \equiv 1 \pmod{p^{o_2}}$. (Observe that $x_2 p^{o_2-o_1} \in \mathbb{Z}$ because $o_1 - o_2 < n_1 - n_2$, by Proposition 2.3 (4).)

Proof. Condition (1) is equivalent to $\bar{b} \in \mathcal{B}$, so we can take it for granted. Under this assumption, $\bar{b} \in \mathcal{B}_r$ if and only if $r_i \equiv r_1^{x_i} r_2^{y_i} \pmod{p^m}$, for $i = 1, 2$. Write $R_i = \sigma_i r_i$. Observe that if $\sigma_i = -1$ then $p = 2$, $m \geq 2$ and $R_i \equiv 1 \pmod{4}$. Therefore $\bar{b} \in \mathcal{B}_r$ if and only if

$$(3.1) \quad \sigma_1^{x_1-1} \sigma_2^{y_1} = \sigma_1^{x_2} \sigma_2^{y_2-1} = 1 \quad \text{and} \quad R_1^{x_1-1} R_2^{y_1} \equiv R_1^{x_2} R_2^{y_2-1} \equiv 1 \pmod{p^m}.$$

By statements (2) and (3) of Proposition 2.3, the equalities on the left side of (3.1) are equivalent to (2). Moreover, $\text{ord}_p(R_i) = p^{o_i}$ and if $o_1 o_2 \neq 0$ then $o_2 \leq o_1$ and $R_2 \equiv R_1^{p^{o_1-o_2}} \pmod{p^m}$, by Proposition 2.3 (4) and (1.1). Hence the congruences on the right side of (3.1) are equivalent to the conditions in (3). \square

In the remainder of the section we assume that $\bar{b} \in \mathcal{B}_r$. We will describe the connection between the $o'_i(b)$'s and $u_i(b)$'s with the $o'_i(\bar{b})$'s and $u_i(\bar{b})$'s. We first obtain a general description and then specialize to three cases depending on the values of σ_1 and σ_2 .

Lemma 3.2. *If $\bar{b} \in \mathcal{B}_r$ then*

$$(3.2) \quad t_1(\bar{b})\alpha \equiv x_1 t_1(b) + y_1 p^{n_1-n_2} t_2(b) + \beta_1 \pmod{p^m},$$

$$(3.3) \quad t_2(\bar{b})\alpha \equiv x_2 t_1(b) p^{n_2-n_1} + y_2 t_2(b) + \beta_2 \pmod{p^m},$$

where

$$(3.4) \quad \alpha = \mathcal{S}(r_1 | x_1) \mathcal{S}(r_2 | y_2) r_2^{y_1} - \mathcal{S}(r_1 | x_2) \mathcal{S}(r_2 | y_1) r_2^{y_2},$$

$$(3.5) \quad \beta_i = \mathcal{S}(r_1 | x_i) \mathcal{S}(r_2 | y_i) \mathcal{S}(r_1^{x_i}, r_2^{y_i} | p^{n_i}) \quad (i = 1, 2).$$

Proof. Let $a = [b_2, b_1]$ and $\bar{a} = [\bar{b}_1, \bar{b}_2]$. Observe that the hypothesis implies that

$$r(b_i) \equiv r(\bar{b}_i) \equiv r_i \equiv r_1^{x_i} r_2^{y_i} \pmod{p^m}.$$

Therefore, by (2.1), for every $v, w \in \mathbb{Z}$

$$(3.6) \quad [a^v, b_i^w] = a^{v(r_i^w - 1)}$$

and

$$(3.7) \quad [b_2^w, b_1^v] = a^{\mathcal{S}(r_1 | v) \mathcal{S}(r_2 | w)}.$$

By (2.1), (3.6) and (3.7)

$$\bar{a} = a^{\alpha + \gamma},$$

where $\gamma = z_2(r_1 - 1) + z_1(1 - r_2)$; by (2.2) and (2.3)

$$(3.8) \quad \bar{b}_i^{p^{n_i}} = b_1^{x_i p^{n_i}} b_2^{y_i p^{n_i}} a^{\beta_i + z_i \mathcal{S}(r_i | p^{n_i})}$$

and as $p^{n_1 - n_2} \mid x_2$

$$\begin{aligned} a^{t_1(\bar{b})(\alpha + \gamma)} &= \bar{a}^{t_1(\bar{b})} = \bar{b}_1^{p^{n_1}} = a^{x_1 t_1(b) + y_1 p^{n_1 - n_2} t_2(b) + \beta_1 + z_1 \mathcal{S}(r_1 | p^{n_1})} \quad \text{and} \\ a^{t_2(\bar{b})(\alpha + \gamma)} &= \bar{a}^{t_2(\bar{b})} = \bar{b}_2^{p^{n_2}} = a^{x_2 t_1(b) p^{n_2 - n_1} + y_2 t_2(b) + \beta_2 + z_2 \mathcal{S}(r_2 | p^{n_2})}. \end{aligned}$$

By (2.10), (2.11) and (2.12) it is clear that $\gamma t_i(\bar{b}) \equiv z_i \mathcal{S}(r_i | p^{n_i}) \pmod{p^m}$ for $i = 1, 2$, so the statement follows. \square

Remark 3.3. An analogue of Lemma 3.2 was stated in the proof of [Mie75, Theorem 9]. Unfortunately, there is a mistake which leads to an incorrect version of condition (3.3). Namely, in our notation, the exponent of a in (3.8) for $i = 2$ appears as $\beta_2 + z_2(r_2 - 1) \mathcal{T}(r_1, r_2 | p^{n_2})$ in [Mie75], rather than $\beta_2 + z_2 \mathcal{S}(r_2 | p^{n_2})$. As a consequence some groups are missing in [Mie75]. A minimal example is provided by the groups G with $\text{inv}(G) = (3, 3, 3, 2, 1, 1, 2, 0, 1, 2, 1, u)$ for $u \in \{1, 4, 7\}$. Only the group with $u = 1$ appears in [Mie75].

Lemma 3.4. *If $\bar{b} \in \mathcal{B}_r$ and $\sigma_1 = 1$ then*

$$(3.9) \quad (x_1 y_2 - x_2 y_1) u_1(\bar{b}) p^{m - o'_1(\bar{b})} \equiv x_1 u_1(b) p^{m - o'_1(b)} + y_1 u_2(b) p^{m - o'_2(b) + n_1 - n_2} + B_1 \pmod{p^m}$$

and

$$(3.10) \quad A + (x_1 y_2 - x_2 y_1) u_2(\bar{b}) p^{m - o'_2(\bar{b})} \equiv x_2 u_1(b) p^{m - o'_1(b) + n_2 - n_1} + y_2 u_2(b) p^{m - o'_2(b)} + B_2 \pmod{p^m},$$

where

$$A = \begin{cases} ((x_1 - 1) y_2 - x_2 y_1) 2^{n_2 - 1}, & \text{if } p = 2 \text{ and } 0 < m - n_2 = o_1 - o_2; \\ 0, & \text{otherwise;} \end{cases}$$

and for $i = 1, 2$

$$B_i = \begin{cases} x_i y_i 2^{n_i - 1}, & \text{if } p = 2 \text{ and } m = n_1; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. By Lemma 3.2, it is enough to prove the following:

$$(3.11) \quad t_1(\bar{b}) \alpha \equiv t_1(\bar{b}) (x_1 y_2 - x_2 y_1) \pmod{p^m},$$

$$(3.12) \quad t_2(\bar{b}) \alpha \equiv A + t_2(\bar{b}) (x_1 y_2 - x_2 y_1) \pmod{p^m},$$

$$(3.13) \quad \beta_i \equiv B_i \pmod{p^m} \quad (i = 1, 2).$$

By Corollary 2.5 (3) and Lemma A.2 (1), $v_p(\mathcal{S}(r_1 | p^{n_1})) = n_1 \geq m$, so using (2.10) and (2.11), it follows that

$$\begin{aligned} t_1(\bar{b}) \alpha &\equiv t_1(\bar{b}) (x_1 y_2 - x_2 y_1) \pmod{p^m}, \\ t_2(\bar{b}) \alpha &\equiv t_2(\bar{b}) (\mathcal{S}(r_1 | x_1) y_2 - \mathcal{S}(r_1 | x_2) y_1) \pmod{p^m}. \end{aligned}$$

This proves (3.11) and reduces the proof of (3.12) to the following:

$$\begin{aligned} t_2(\bar{b})\mathcal{S}(r_1 | x_1) &\equiv \begin{cases} t_2(\bar{b})x_1 + (x_1 - 1)2^{n_2-1} \bmod 2^m, & \text{if } p = 2 \text{ and } 0 < m - n_2 = o_1 - o_2; \\ t_2(\bar{b})x_1 \bmod p^m, & \text{otherwise;} \end{cases} \\ t_2(\bar{b})\mathcal{S}(r_1 | x_2) &\equiv \begin{cases} t_2(\bar{b})x_2 + x_2 2^{n_2-1} \bmod 2^m, & \text{if } p = 2 \text{ and } 0 < m - n_2 = o_1 - o_2; \\ t_2(\bar{b})x_2 \bmod p^m, & \text{otherwise.} \end{cases} \end{aligned}$$

By Lemma 2.4 (3), if $m \leq n_2$ then $v_p(t_2(\bar{b})) + v_p(r_1 - 1) = 2m - o_1 - o'_2(\bar{b}) \geq m$, and hence $t_2(\bar{b})r_i \equiv r_i \bmod p^m$ and $t_2(\bar{b})\mathcal{S}(r_i | x_i) \equiv t_2(\bar{b})x_i \bmod p^m$. Otherwise $2m - o_1 - o'_2(\bar{b}) = n_2 < m$, and since $o'_2(\bar{b}) \leq m$, it follows that $o_1 \neq 0$. By Lemmas 2.4 (1) and 3.1 (3),

$$m - n_2 = o'_2(\bar{b}) + o_1 - m \leq o_1 - o_2 \leq \min(v_p(x_1 - 1), v_p(x_2)).$$

Applying Lemma A.2 (3) we derive that, for $i = 1, 2$,

$$\mathcal{S}(r_i | x_i) \equiv \begin{cases} x_i + 2^{o'_2(\bar{b})-1} \bmod 2^{o'_2(\bar{b})}, & \text{if } p = 2, m - n_2 = o_1 - o_2 \text{ and } x_i \not\equiv 1 \bmod 2^{m-n_2+1}; \\ x_i \bmod p^{o'_2(\bar{b})}, & \text{otherwise.} \end{cases}$$

As $o'_2(\bar{b}) = m - v_p(t_2(\bar{b}))$,

$$t_2(\bar{b})\mathcal{S}(r_i | x_i) \equiv \begin{cases} t_2(\bar{b})x_i + 2^{m-1} \bmod 2^m, & \text{if } p = 2, m - n_2 = o_1 - o_2 \text{ and } x_i \not\equiv 0 \bmod 2^{m-n_2+1}; \\ t_2(\bar{b})x_i \bmod p^m, & \text{otherwise.} \end{cases}$$

Since $0 < m - n_2 \leq \min(v_p(x_2), v_p(x_1 - 1))$ we deduce that

$$\begin{aligned} t_2(\bar{b})\mathcal{S}(r_1 | x_2) &\equiv \begin{cases} t_2(\bar{b})x_2 + x_2 2^{n_2-1} \bmod 2^m, & \text{if } p = 2 \text{ and } m - n_2 = o_1 - o_2; \\ t_2(\bar{b})x_2 \bmod p^m, & \text{otherwise;} \end{cases} \\ t_2(\bar{b})\mathcal{S}(r_1 | x_1) &\equiv \begin{cases} t_2(\bar{b})x_1 + (x_1 - 1)2^{n_2-1} \bmod 2^m, & \text{if } p = 2 \text{ and } m - n_2 = o_1 - o_2; \\ t_2(\bar{b})x_1 \bmod p^m, & \text{otherwise;} \end{cases} \end{aligned}$$

and (3.12) follows.

By Lemma A.3

$$\beta_1 \equiv \begin{cases} \mathcal{S}(r_1 | x_1) \mathcal{S}(r_2 | y_1) 2^{n_1-1} \bmod 2^m, & \text{if } p = 2; \\ 0 \bmod p^m, & \text{otherwise.} \end{cases}$$

This proves (3.13) for $i = 1$ when $p \neq 2$ or $m \neq n_1$. Otherwise, by Lemma A.1 (1),

$$\beta_1 \equiv x_1 y_1 2^{n_1-1} = B_i \bmod 2^m,$$

as desired. Finally, for the proof of (3.13) for $i = 2$, recall that $p^{n_1-n_2} | x_2$, and hence, by Lemma A.2 (1), $p^{n_1-n_2} | \mathcal{S}(r_1 | x_2)$. Moreover, by Lemma A.3, if $p > 2$ then $p^{n_2} | \mathcal{T}(r_1^{x_2}, r_2^{y_2} | p^{n_2})$, so $\beta_2 \equiv 0 \equiv B_2 \bmod p^m$. Assume $p = 2$. Then by the same lemma $\mathcal{T}(r_1^{x_2}, r_2^{y_2} | 2^{n_2}) \equiv 2^{n_2-1} \bmod 2^{n_2}$. Thus

$$\mathcal{S}(r_1 | x_2) \mathcal{T}(r_1^{x_2}, r_2^{y_2} | p^{n_2}) \equiv \mathcal{S}(r_1 | x_2) 2^{n_2-1} \bmod 2^{n_1}.$$

As $v_2(x_2) \geq n_1 - n_2$, if $n_1 > m$ then clearly this expression vanishes modulo 2^m and hence $\beta_2 \equiv B_2 \bmod 2^m$. Otherwise, $m = n_1$ and

$$\mathcal{S}(r_2 | x_2) 2^{n_2-1} \equiv x_2 2^{n_2-1} \bmod 2^m.$$

Thus $\beta_2 \equiv x_2 y_2 2^{n_2-1} = B_2 \bmod 2^m$. This proves (3.13). \square

Lemma 3.5. *If $\bar{b} \in \mathcal{B}_r$, $\sigma_1 = -1$ and $\sigma_2 = 1$ then*

$$\begin{aligned}
t_1(\bar{b})\alpha &\equiv t_1(\bar{b})(x_1y_2 - x_2y_1) \bmod 2^m; \\
t_2(\bar{b})\alpha &\equiv \begin{cases} t_2(\bar{b})(x_1y_2 - x_2y_1) \bmod 2^m, & \text{if } n_2 \geq m; \\ t_2(\bar{b})y_2 + ((x_1 - 1)y_2 - x_2y_1)2^{m-o_1+o_2-1} \bmod 2^m, & \text{if } o_2 + 1 = n_2 < m \text{ and } o_1 > 0; \\ t_2(\bar{b})y_2 \bmod 2^m, & \text{otherwise;} \end{cases} \\
\beta_1 &\equiv y_1 2^{n_1-1} \bmod 2^m; \\
\beta_2 &\equiv \begin{cases} x_2 2^{m-n_1} \bmod 2^m, & \text{if } n_1 = o_1 + 1, \ o_2 = 0 < o_1, \text{ and } n_2 = 1; \\ 0 \bmod 2^m, & \text{otherwise.} \end{cases}
\end{aligned}$$

Proof. Since $\sigma_1 = -1$ and $\sigma_2 = 1$, it follows that $p = 2$, $n_1 > n_2$, $o'_1(\bar{b}) \leq 1$ and $u_1(\bar{b}) = 1$ by Proposition 2.3 and Lemma 2.4 (1). Moreover, $2^{n_1-n_2} \mid x_2$ and $2 \nmid x_1y_2$ by Lemma 3.1, and $t_i(\bar{b})r_i \equiv t_i(\bar{b}) \bmod 2^m$, by (2.10). By (2.11), $t_1(\bar{b})(r_2 - 1) \equiv \mathcal{S}(r_1 \mid 2^{n_1}) \bmod 2^m$ and, by Lemma A.2 (2) and Lemma 2.4 (2), $v_2(\mathcal{S}(r_1 \mid 2^{n_1})) = n_1 + m - o_1 - 1 \geq m$. So the first congruence follows.

Moreover $t_2(\bar{b})\alpha \equiv t_2(\bar{b})(\mathcal{S}(r_1 \mid x_1)y_2 - \mathcal{S}(r_1 \mid x_2)y_1) \bmod 2^m$. If $n_2 \geq m$ then, by (2.12) and Lemma A.2 (1),

$$t_2(\bar{b})(r_1 - 1) \equiv \mathcal{S}(r_2 \mid 2^{n_2}) \equiv 0 \bmod 2^m,$$

so

$$t_2(\bar{b})\alpha \equiv t_2(\bar{b})(x_1y_2 - x_2y_1) \bmod 2^m.$$

Otherwise, $m > n_2 = m - o'_2(\bar{b}) + 1$, by Lemma 2.4 (4). If $o_1 = 0$ then $r_1 \equiv -1 \bmod 2^m$, so $\mathcal{S}(r_1 \mid x_1) \equiv 1 \bmod 2^m$ and $\mathcal{S}(r_1 \mid x_2) \equiv 0 \bmod 2^m$, since $2 \nmid x_1$ and $2 \mid x_2$. Hence $t_2(\bar{b})\alpha \equiv t_2(\bar{b})y_2 \bmod 2^m$. Assume that $o_1 \neq 0$. Then $o_1 > o_2$ by Proposition 2.3 (4), and $x_1 - 1 \equiv x_2 \equiv 0 \bmod 2^{o_1-o_2}$ by Lemma 3.1. So

$$v_2(t_2(\bar{b})\mathcal{S}(r_1 \mid x_2)) = m - o'_2(\bar{b}) + v_2(r_1 + 1) - 1 + v_2(x_2) = 2m - o'_2(\bar{b}) - o_1 - 1 + v_2(x_2) \geq 2m - o'_2(\bar{b}) - o_2 - 1 \geq m - 1,$$

by Lemma 2.4 (1). Moreover, $v_2(t_2(\bar{b})\mathcal{S}(r_1 \mid x_2)) = m - 1$ if and only if $v_2(x_2) = o_1 - o_2$ and $m - o_2 = o'_2(\bar{b})$ if and only if $v_2(x_2) = o_1 - o_2$ and $n_2 = o_2 + 1$ (because $m - o'_2(\bar{b}) + 1 = n_2$). Therefore, if $o_1 \neq 0$ then

$$t_2(\bar{b})\mathcal{S}(r_1 \mid x_2) \equiv \begin{cases} x_2 2^{m+o_2-o_1-1} \bmod 2^m, & \text{if } o_2 + 1 = n_2 < m; \\ 0, & \text{otherwise.} \end{cases}$$

Similar arguments yield

$$t_2(\bar{b})\mathcal{S}(r_1 \mid x_1) = t_2(\bar{b}) + t_2(\bar{b})r_1\mathcal{S}(r_1 \mid x_1 - 1) \equiv \begin{cases} t_2(\bar{b}) + (x_1 - 1)2^{m+o_2-o_1-1} \bmod 2^m, & \text{if } o_2 + 1 = n_2 < m; \\ t_2(\bar{b}) \bmod 2^m, & \text{otherwise.} \end{cases}$$

This proves the second congruence.

As $x_1 - 1$ is even, by Lemma A.2 (2), Lemma A.3 and Lemma 2.4 (2)

$$v_2(\mathcal{S}(r_1 \mid x_1 - 1)\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1})) = v_2(x_1 - 1) + m - o_1 - 1 + n_1 - 1 \geq m - o_1 - 1 + n_1 \geq m.$$

By Lemma A.1, $y_1 + (r_2 - 1)\mathcal{T}(r_2, 1 \mid y_1) = \mathcal{S}(r_2 \mid y_1)$, and by Lemma A.3,

$$v_2((r_2 - 1)\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1})) = m - o_2 + n_1 - 1 \geq m - o_2 + n_2 - 1 \geq m.$$

Thus, using Lemma A.1 (4) and Lemma A.4 we conclude that

$$\begin{aligned}
\beta_1 &\equiv \mathcal{S}(r_1 \mid x_1)\mathcal{S}(r_2 \mid y_1)\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1}) \\
&\equiv (1 + r_1\mathcal{S}(r_1 \mid x_1 - 1))\mathcal{S}(r_2 \mid y_1)\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1}) \\
&\equiv \mathcal{S}(r_2 \mid y_1)\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1}) \\
&\equiv (y_1 + (r_2 - 1)\mathcal{T}(r_2, 1 \mid y_1))\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1}) \\
&\equiv y_1\mathcal{T}(r_1^{x_1}, r_2^{y_1} \mid 2^{n_1}) \\
&\equiv y_1 2^{n_1-1} \bmod 2^m.
\end{aligned}$$

This proves the third congruence.

Lemma A.1 and Lemma 2.4 (2) yield

$$v_2(\beta_2) = v_2(\mathcal{S}(r_1 \mid x_2)\mathcal{S}(r_2 \mid y_2)\mathcal{T}(r_1^{x_2}, r_2^{y_2} \mid 2^{n_2})) = v_2(r_1 + 1) - 1 + v_2(x_2) + n_2 - 1 \geq m - o_1 - 1 + n_1 - 1 \geq m - 1.$$

Therefore $v_2(\beta_2) = m - 1$ if and only if $n_1 = o_1 + 1$ and $v_2(x_2) = n_1 - n_2$. In that case $o_1 > 0$, since $n_1 > n_2$; and $o_2 + n_1 - n_2 = o_2 + o_1 - n_2 + 1 \leq o_1$, by Lemma 2.4 (2). Using Proposition 2.3 (4), we deduce that if $v_2(\beta_2) = m - 1$ then $o_2 = 0 < o_1$, and so $2^{o_1} \mid x_2$, by Lemma 3.1. Then $o_1 + 1 - n_2 = n_1 - n_2 = v_2(x_2) \geq o_1$, which implies $n_2 = 1$. This yields the last congruence. \square

Lemma 3.6. *Suppose that $\bar{b} \in \mathcal{B}_r$, $\sigma_1 = -1$ and $\sigma_2 = 1$.*

(1) *If $m \leq n_2$ then*

- $o'_1(\bar{b}) = o'_1(b) \leq 1$, $o'_2(\bar{b}) \leq 1$, $o'_2(b) \leq 1$, and
- $o'_2(\bar{b}) \neq o'_2(b)$ if and only if $v_2(x_2) = n_1 - n_2$ and $o'_1(b) = 1$.

(2) *If $m > n_2$ then*

- $o'_1(b) \leq 1$, $o'_1(\bar{b}) \leq 1$,
- $o'_1(b) \neq o'_1(\bar{b})$ if and only if $2 \nmid y_1$ and $n_1 = o_1 + 1$, and
- the following congruence holds:

$$(3.14) \quad (u_2(\bar{b}) - u_2(b))2^{n_2-1} + A \equiv x_2 2^{m-o'_1(b)+n_2-n_1} + B \pmod{2^m}$$

where

$$A = \begin{cases} ((x_1 - 1)y_2 - x_2 y_1)2^{m-o_1+o_2-1}, & \text{if } o_2 + 1 = n_2 \text{ and } o_1 > 0; \\ 0, & \text{otherwise;} \end{cases}$$

and

$$B = \begin{cases} x_2 2^{m-n_1}, & \text{if } n_1 = o_1 + 1, \ o_2 = 0 < o_1, \text{ and } n_2 = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. By Proposition 2.3, $p = 2$, $n_1 > n_2$ and hence, by Lemma 3.1 (1), $2 \mid x_2$ and $2 \nmid x_1 y_2$. Moreover, by Lemma 2.4 (1), each of $o'_1(b)$ and $o'_1(\bar{b})$ is at most 1 and $u_1(b) = u_1(\bar{b}) = 1$, so $t_1(b) = 2^{m-o'_1(b)}$ and $t_1(\bar{b}) = 2^{m-o'_1(\bar{b})}$.

(1) Suppose first that $m \leq n_2$. Then $n_1 > n_2 \geq m > o_1$, and hence, by Lemma 3.5, $\beta_1 \equiv \beta_2 \equiv 0 \pmod{2^m}$. By (2.12) and Lemma A.1 (1) also $t_2(\bar{b})(r_1 - 1) \equiv \mathcal{S}(r_2 \mid p^{n_2}) \equiv 0 \pmod{p^m}$, therefore

$$m \leq v_2(t_2(\bar{b})) + v_2(r_1 - 1) = m - o'_2(\bar{b}) + 1,$$

and consequently $o'_2(\bar{b}) \leq 1$, $t_2(\bar{b}) = p^{m-o'_2(\bar{b})}$ and $t_2(b)2^{n_1-n_2} \equiv 0 \pmod{2^m}$. Then Lemmas 3.2 and 3.5 imply $o'_1(\bar{b}) = o'_1(b)$ and

$$2^{m-o'_2(\bar{b})} \equiv x_2 2^{m-o'_1(b)+n_2-n_1} + 2^{m-o'_2(b)} \pmod{2^m}.$$

As both $o'_2(\bar{b})$ and $o'_2(b)$ are at most 1 and $2^{n_1-n_2} \mid x_2$, it follows that $o'_2(\bar{b}) \neq o'_2(b)$ if and only if $v_2(x_2) = n_1 - n_2 + o'_1(b) - 1$ if and only if $v_2(x_2) = n_1 - n_2$ and $o'_1(b) = 1$.

(2) Suppose now that $m > n_2$. Then $o'_2(\bar{b}) = o'_2(b) = m - n_2 + 1 > 1$, by Lemma 2.4 (4). Thus Lemma 3.5 yields that (3.3) takes the form of (3.14).

We claim that

$$(3.15) \quad y_1 t_2(b) 2^{n_1-n_2} + y_1 2^{n_1-1} \equiv \begin{cases} y_1 2^{m-1} \pmod{2^m}, & \text{if } n_1 = o_1 + 1; \\ 0 \pmod{2^m}, & \text{otherwise.} \end{cases}$$

Indeed,

$$y_1 t_2(b) 2^{n_1-n_2} + y_1 2^{n_1-1} \equiv y_1 2^{n_1-1} (u_2(b) + 1) \pmod{2^m}$$

and, by Lemma 2.4 (4), $u_2(b)(-1 + 2^{m-o_1-1}) \pmod{2^{m-n_2}}$. Thus $v_2(u_2(b) + 1) \geq \min(m - n_2, m - o_1 - 1)$. Moreover $n_1 > n_2$, and therefore $n_1 - 1 + m - n_2 \geq m$ and $n_1 - 1 + m - o_1 - 1 \geq m - 1$. Hence, from Lemma 2.4 (2), it follows that $n_1 - 1 + v_2(u_2(b) + 1) = m - 1$ if and only if $n_1 = o_1 + 1$. Therefore (3.15) follows.

By (3.2) and Lemma 3.5, and recalling that each of $o'_1(b)$ and $o'_1(\bar{b})$ is at most 1 and $2 \nmid x_1 y_2$ and $2 \mid x_2$, we deduce that the left-hand side of (3.15) is congruent modulo 2^m to $2^{m-o'_1(\bar{b})} - 2^{m-o'_1(b)}$. Hence, $o'_1(b) \neq o'_1(\bar{b})$ if and only if $n_1 = o_1 + 1$ and $2 \nmid y_1$, as desired. \square

Lemma 3.7. *If $\bar{b} \in \mathcal{B}_r$ and $\sigma_2 = -1$ then*

$$(3.16) \quad 2^{m-o'_1(\bar{b})} \equiv x_1 2^{m-o'_1(b)} + y_1 2^{m-o'_2(b)+n_1-n_2} \pmod{2^m},$$

$$(3.17) \quad 2^{m-o'_2(\bar{b})} \equiv x_2 2^{m-o'_1(b)+n_2-n_1} + y_2 2^{m-o'_2(b)} + B \pmod{2^m},$$

where B is as in Lemma 3.6.

Proof. Since $\sigma_2 = -1$, by Proposition 2.3, Lemma 2.4 (1) and Lemma 3.1, $p = 2$, $\sigma_1 = -1$, $x_1 \equiv y_2 \pmod{2}$, $x_1 \not\equiv x_2 \pmod{2}$, $x_2 \equiv y_1 \pmod{2}$, and, for $i \in \{1, 2\}$, $u_i(b) = u_i(\bar{b}) = 1$ and each of $o'_i(b)$ and $o'_i(\bar{b})$ is at most 1. Then

$$t_i(\bar{b})(r_i - 1) \equiv t_i(\bar{b})(r_2 - 1) \equiv t_2(\bar{b})(r_1 - 1) \equiv 0 \pmod{2^m},$$

so

$$t_i(\bar{b})\alpha \equiv (x_1 y_2 - x_2 y_1) 2^{m-o'_i(\bar{b})} \equiv 2^{m-o'_i(\bar{b})} \pmod{2^m}$$

and $t_i(b) = 2^{m-o'_i(b)}$. Thus, by Lemma 3.2 it suffices to prove that $\beta_1 \equiv 0 \pmod{2^m}$ and $\beta_2 \equiv B \pmod{2^m}$.

By Lemma A.2 (2) and Lemma A.3

$$v_2(\beta_1) \equiv \begin{cases} v_2(r_1 + 1) + v_2(x_1) + n_1 - 2 = m - o_1 + v_2(x_1) + n_1 - 2 \geq m + v_2(x_1) - 1, & \text{if } 2 \mid x_1; \\ v_2(r_2 + 1) + v_2(y_1) + n_1 - 2 = m - o_2 + v_2(y_1) + n_1 - 2 \geq m + v_2(y_1) - 1, & \text{otherwise.} \end{cases}$$

In both cases $v_2(\beta_1) \geq m$, so $\beta_1 \equiv 0 \pmod{2^m}$.

Arguing similarly, in combination with Lemma 3.1, we obtain

$$v_2(\beta_2) \equiv \begin{cases} m - o_1 + v_2(x_2) + n_2 - 2 \geq m - o_1 + n_1 - 2 \geq m - 1, & \text{if } 2 \mid x_2; \\ m - o_2 + v_2(y_2) + n_2 - 2 \geq m + v_2(y_2) - 1 \geq m, & \text{otherwise.} \end{cases}$$

Thus either $\beta_2 \equiv 0 \pmod{2^m}$ or $\beta_2 \equiv 2^{m-1} \pmod{2^m}$, $v_2(x_2) = n_1 - n_2 > 0$ and $n_1 = o_1 + 1$. In the latter case $o_2 < o_2 + n_1 - n_2 = o_2 + o_1 + 1 - n_2 \leq o_1$, by Corollary 2.5 (2). Hence $o_2 = 0 < o_1$, by Proposition 2.3 (4), and $o_1 + 1 - n_2 = n_1 - n_2 = v_2(x_2) \geq o_1$, by Lemma 3.1, so $n_2 = 1$. Thus $\beta_2 \equiv 2^{m-1} \pmod{2^m}$ if and only if $n_1 = o_1 + 1$, $o_2 = 0 < o_1 = v_2(x_2)$ and $n_2 = 1$. This proves that $\beta_2 \equiv B \pmod{2^m}$. \square

4. DESCRIPTION OF \mathcal{B}'_r AND CONDITIONS ON o'_1 AND o'_2

Recall that \mathcal{B}'_r is formed by the basis $b = (b_1, b_2) \in \mathcal{B}_r$ such that $o'(b) = (o'_1, o'_2)$, or equivalently $(|b_1|, |b_2|) \geq_{\text{lex}} (|\bar{b}_1|, |\bar{b}_2|)$ for every $\bar{b} \in \mathcal{B}_r$. In this section $b = (b_1, b_2)$ is a fixed element of \mathcal{B}_r and the goal is to obtain necessary and sufficient conditions for $b \in \mathcal{B}'_r$ in terms of conditions on the entries of $o'(b) = (o'_1(b), o'_2(b))$. The arguments in the proof of Lemma 4.2, 4.3 and 4.4 are repetitive, so with the aim of avoiding repetitions we explain now the structure of the proofs. In all cases we must prove that $b \in \mathcal{B}'_r$ if and only if $o'(b)$ satisfies certain conditions. We have a generic element $\bar{b} = (b_1^{x_1} b_2^{y_1} [b_2, b_1]^{z_1}, b_1^{x_2} b_2^{y_2} [b_2, b_1]^{z_2})$ in \mathcal{B}_r and we compare $o'(b)$ and $o'(\bar{b})$ using the results of the previous section. For the direct implication we assume that $b \in \mathcal{B}'_r$ and select several $\bar{b} \in \mathcal{B}_r$ to deduce the conditions on $o'(b)$ from the inequality $o'(b) \geq_{\text{lex}} o'(\bar{b})$. For the reverse implication we assume that $b \notin \mathcal{B}'_r$ and $\bar{b} \in \mathcal{B}'_r$ and deduce from $o'(b) < o'(\bar{b})$ that $o'(b)$ does not satisfy the given conditions. In both cases it is important to recall Lemma 3.1 because it establishes when \bar{b} belongs to \mathcal{B}_r . Moreover, A , B and the B_i 's are as in Lemmas 3.4, 3.6 or 3.7, depending on the case considered, and always relative to the \bar{b} used in each case.

The following straightforward observation is often used.

Remark 4.1. Let X , Y , Z , W and T be integers.

(1) If $v_p(X), v_p(Y) \leq m$ and $Y \equiv XW + Z \pmod{p^m}$ then

$$v_p(X) \leq v_p(Y) \quad \text{if and only if} \quad v_p(X) \leq v_p(Z)$$

(2) If $v_2(X), v_2(Y) \leq m$ and $Y \equiv XW + Z + T2^{m-1} \pmod{2^m}$ then

$$v_2(X) \leq v_2(Y) \quad \text{if and only if} \quad \text{one of the following holds:} \quad \begin{cases} 2 \mid T \text{ and } v_2(X) \leq v_2(Z); \\ 2 \nmid T, v_2(X) \leq m - 1 \text{ and } v_2(X) \leq v_2(Z); \\ 2 \nmid T, v_2(X) = m \text{ and } v_2(Z) = m - 1. \end{cases}$$

Lemma 4.2. *Suppose that $\sigma_1 = 1$ and $b \in \mathcal{B}_r$. Then $b \in \mathcal{B}'_r$ if and only if the following conditions hold:*

(1) *If $o_1 = 0$ then either*

- (a) $o'_1(b) \leq o'_2(b) \leq o'_1(b) + o_2 + n_1 - n_2$ and $\max(p-2, o'_2(b), n_1 - m) > 0$, or
 (b) $p = 2$, $m = n_1$, $o'_2(b) = 0$ and $o'_1(b) = 1$.
 (2) If $o_2 = 0 < o_1$ then $\max(p-2, o'_1(b), n_1 - m) > 0$ and

$$o'_1(b) + \min(0, n_1 - n_2 - o_1) \leq o'_2(b) \leq o'_1(b) + n_1 - n_2.$$

- (3) If $o_1 o_2 \neq 0$ then $o'_1(b) \leq o'_2(b) \leq o'_1(b) + n_1 - n_2$.

Proof. By Proposition 2.3 (2) $\sigma_2 = 1$, and by Lemma 3.4 the congruences (3.9) and (3.10) hold for each $\bar{b} \in \mathcal{B}_r$. We will use this without explicit mention. We consider separately three cases.

Case (i). Suppose that if $p = 2$ then $m \neq n_1$ and either $m \leq n_2$ or $m - n_2 \neq o_1 - o_2$. Then $A = B_1 = B_2 = 0$. We now apply Remark 4.1 (1) to (3.9), with

$$Y = (x_1 y_2 - x_2 y_1) u_1(\bar{b}) p^{m-o'_1(\bar{b})}, \quad X = u_1(b) p^{m-o'_1(b)} \quad \text{and} \quad Z = y_1 u_2(b) p^{m-o'_2(b)+n_1-n_2},$$

and to (3.10), with

$$Y = (x_1 y_2 - x_2 y_1) u_2(\bar{b}) p^{m-o'_2(\bar{b})}, \quad X = u_2(b) p^{m-o'_2(b)} \quad \text{and} \quad Z = x_2 u_1(b) p^{m-o'_1(b)+n_2-n_1}.$$

It follows that $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if

$$(4.1) \quad o'_2(b) \leq v_2(y_1) + n_1 - n_2 + o'_1(b)$$

and

$$(4.2) \quad \text{if } o'_1(b) = o'_1(\bar{b}) \text{ then } o'_1(b) \leq v_2(x_2) + n_2 - n_1 + o'_2(b).$$

Suppose that $b \in \mathcal{B}'_r$ and consider several $\bar{b} \in \mathcal{B}_r$. If $o_1 = 0$ then we take $\bar{b} = (b_1 b_2^{p^{o_2}}, b_2) \in \mathcal{B}_r$, so (4.1) takes the form $o'_2(b) \leq o_2 + n_1 - n_2 + o'_1(b)$ and then we take $\bar{b} = (b_1, b_1^{p^{n_1-n_2}} b_2) \in \mathcal{B}_r$, so (4.2) yields $o'_1(b) \leq o'_2(b)$. Thus condition (1) holds. If $o_2 = 0 < o_1$ then we take $\bar{b} = (b_1 b_2, b_2) \in \mathcal{B}_r$, so (4.1) yields $o'_2(b) \leq n_1 - n_2 + o'_1(b)$, and then we take $\bar{b} = (b_1, b_1^{p^{\max(n_1-n_2, o_1)}} b_2) \in \mathcal{B}_r$ which using (4.2) yields $o'_1(b) \leq \max(0, o_1 - n_1 + n_2) + o'_2(b)$. Thus condition (2) holds. Finally, if $o_1 o_2 \neq 0$ then $o_2 < o_1 < o_2 + n_1 - n_2$ by Proposition 2.3 (4). In this case we take $\bar{b} = (b_1^{1-p^{o_1-o_2}} b_2, b_2) \in \mathcal{B}_r$, and (4.1) yields $o'_2(b) \leq n_1 - n_2 + o'_1(b)$, and then we take $\bar{b} = (b_1, b_1^{p^{n_1-n_2}} b_2^{1-p^{n_1-n_2-o_1+o_2}}) \in \mathcal{B}_r$ so (4.2) implies $o'_1(b) \leq o'_2(b)$. Hence condition (3) holds.

Conversely assume $b \notin \mathcal{B}'_r$ and suppose that our generic element \bar{b} belongs to \mathcal{B}'_r , so $o'(b) < o'(\bar{b})$. Thus either (4.1) or (4.2) fails. If (4.1) fails then

$$o'_2(b) > v_2(y_1) + n_1 - n_2 + o'_1(b) \geq n_1 - n_2 + o'_1(b)$$

and hence b satisfies neither the consequent of (2) nor the consequent of (3). Thus we may assume that $o_1 = 0$. By Lemma 3.1, $2^{o_2} \mid y_1$, so $o'_2(b) > o_2 + n_1 - n_2 + o'_1(b)$, and hence b does not satisfy (1a). As $p > 2$ or $m \neq n_1$, it follows that b does not satisfy (1b) either. Thus, b does not satisfy (1). Suppose otherwise that (4.1) holds but (4.2) does not. Thus $o'_1(b) = o'_1(\bar{b})$ and $o'_1(b) > v_2(x_2) + n_2 - n_1 + o'_2(b)$. By Lemma 3.1, $v_2(x_2) \geq n_1 - n_2$ and hence $o'_1(b) > v_2(x_2) + n_2 - n_1 + o'_2(b) \geq o'_2(b)$. In particular, as we are assuming that if $p = 2$ then $m \neq n_1$, necessarily b satisfies neither the consequent of (1) nor the consequent of (3). Thus we may assume that $o_2 = 0 < o_1$. Then $2^{\max(n_1-n_2, o_1)} \mid x_2$, by Lemma 3.1, so $o'_1(b) > \max(0, o_1 + n_2 - n_1) + o'_2(b)$. Hence b does not satisfy (2).

Case (ii). Suppose that $p = 2$ and $0 < m - n_2 = o_1 - o_2$. In particular, $o_1 \neq 0$. By Lemma 2.4 (3), $o'_2(b) = o'_2(\bar{b}) = 2m - n_2 - o_1 = m - o_2 \geq o'_1(\bar{b})$ for every $\bar{b} \in \mathcal{B}_r$. Therefore the first inequality in (3) holds and if $o_2 = 0$ then $o_1 = m - n_2 \leq n_1 - n_2$ and hence $o'_1(b) + \min(0, n_1 - n_2 - o_1) \leq o'_2(b)$. Moreover, $o'(\bar{b}) \geq o'(b)$ if and only if $o'_1(\bar{b}) \geq o'_1(b)$.

Assume $n_1 > m$, so $B_i = 0$. In this case we must prove that $b \in \mathcal{B}'_r$ if and only if $o'_2(b) \leq o'_1(b) + n_1 - n_2$. Indeed, applying Remark 4.1 to (3.9), with suitable X, Y and Z , we deduce that $o'_1(\bar{b}) \geq o'_1(b)$ if and only if (4.1) holds. If $b \in \mathcal{B}'_r$ then, taking $\bar{b} = (b_1^{1-p^{o_1-o_2}} b_2, b_2) \in \mathcal{B}_r$, we deduce that $o'_2(b) \leq o'_1(b) + n_1 - n_2$. Conversely if $b \notin \mathcal{B}'_r$ and $\bar{b} \in \mathcal{B}'_r$ then $o'_1(\bar{b}) > o'_1(b)$ and hence

$$o'_2(b) > v_2(y_1) + n_1 - n_2 + o'_1(b) \geq n_1 - n_2 + o'_1(b),$$

as desired.

If $n_1 \leq m$ then $n_1 = m$, by Lemma 2.4 (3). In particular $o_2 = 0$, by Corollary 2.5 (4). Moreover, applying Remark 4.1 to (3.9), $o'_1(\bar{b}) \leq o'_1(b)$ if and only if

$$(4.3) \quad \text{one of the following conditions holds} \quad \begin{cases} 2 \mid x_1 y_1 \text{ and } o'_2(b) \leq v_2(y_1) + n_1 - n_2 + o'_1(b); \\ 2 \nmid x_1 y_1, \ 1 \leq o'_1(b) \text{ and } o'_2(b) \leq n_1 - n_2 + o'_1(b); \\ 2 \nmid x_1 y_1, \ o'_1(b) = 0 \text{ and } 1 + n_1 - n_2 = o'_2(b). \end{cases}$$

However, the assumption $n_1 = m > n_2$ implies that $2 \nmid x_1$ by Lemma 3.1, and $2 \leq m - o_1 = n_2 - m + o'_2$, by Lemma 2.4 (2) and since $p = 2$. Thus the last case of (4.3) does not hold and $2 \mid x_1 y_1$ if and only if $2 \mid y_1$.

Assume $b \in \mathcal{B}'_r$. Then, taking $\bar{b} = (b_1 b_2, b_2) \in \mathcal{B}_r$, condition (4.3) implies that $1 \leq o'_1(b)$ and $o'_2(b) \leq n_1 - n_2 + o'_1(b)$. Thus condition (2) holds. Conversely, if $b \notin \mathcal{B}'_r$ and $\bar{b} \in \mathcal{B}'_r$ then $o'_1(\bar{b}) > o'_1(b)$ so (4.3) does not hold. If $2 \mid y_1$ then

$$o'_2(b) > v_2(y_1) + n_1 - n_2 + o'_1(b) \geq 1 + n_1 - n_2 + o'_1(b),$$

so (2) does not hold. Similarly, if $2 \nmid y_1$ and $1 \leq o'_1(b)$ then $o'_2(b) > n_1 - n_2 + o'_1(b)$, so again (2) does not hold.

Case (iii). Finally suppose that $p = 2$ and $m = n_1$ and either $m \leq n_2$ or $m - n_2 \neq o_1 - o_2$. Then for every $\bar{b} \in \mathcal{B}_r$, $A = 0$ and by Lemma 2.4 (3), $o_1 o_2 = 0$.

Assume first that $n_2 \geq m$. Then $n_2 = m = n_1$, so $o_1 = 0$ by Proposition 2.3 (4), and $B_i = x_i y_i 2^{m-1}$ for every $\bar{b} \in \mathcal{B}_r$. By Lemma 3.1, $y_1 \equiv y_2 - 1 \equiv 0 \pmod{p^{o_2}}$, and Remark 4.1 yields $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if one of the conditions in (4.3) holds and

$$(4.4) \quad \text{if } o'_1(b) = o'_1(\bar{b}) \quad \text{then one of the following holds} \quad \begin{cases} 2 \mid x_2 y_2 \text{ and } o'_1(b) \leq v_2(x_2) + o'_2(b); \\ 2 \nmid x_2 y_2, \ 1 \leq o'_2(b) \text{ and } o'_1(b) \leq o'_2(b); \\ 2 \nmid x_2 y_2, \ o'_2(b) = 0 \text{ and } 1 = o'_1(b). \end{cases}$$

We must prove that $b \in \mathcal{B}'_r$ if and only if condition (1) holds. Suppose $b \in \mathcal{B}'_r$. If $o_2 = 0$ then we can take $\bar{b} = (b_2, b_1) \in \mathcal{B}_r$, so (4.3) implies $o'_2(b) \leq o'_1(b) + o_2$; and if $o_2 > 0$ then, taking $(b_1 b_2^{2^{o_2}}, b_2) \in \mathcal{B}_r$, (4.3) implies $o'_2(b) \leq o'_1(b) + o_2$. Moreover taking $\bar{b} = (b_1, b_1 b_2) \in \mathcal{B}_r$ and using (4.4) we obtain that either $1 \leq o'_2(b)$ and $o'_1(b) \leq o'_2(b)$ or $o'_2(b) = 0$ and $o'_1(b) = 1$. Thus condition (1) holds. Conversely, suppose $b \notin \mathcal{B}'_r$ and take $\bar{b} \in \mathcal{B}'_r$ such that $o'(\bar{b}) > o'(b)$. Thus one of (4.3) or (4.4) does not hold. Suppose that (4.3) does not hold. If $2 \mid x_1 y_1$ then $o'_2(b) > v_2(y_1) + o'_1(b) \geq o'_1(b) + o_2 + n_1 - n_2$, so (1) does not hold. If $2 \nmid x_1 y_1$ then either $o'_2(b) > o'_1(b)$, or $o'_1(b) = 0$ and $1 + n_1 - n_2 \neq o'_2(b)$. In any case condition (1) does not hold. Suppose that (4.4) does not hold. Therefore $o'_1(\bar{b}) = o'_1(b)$ and the three conditions on the right part of (4.4) fail. If $2 \nmid x_2 y_2$ then $o'(b) \neq (0, 1)$ and hence (1b) fails; and moreover $o'_2(b) = 0$ or $o'_1(b) > o'_2(b)$, so (1a) fails too. Suppose that $2 \mid x_2 y_2$. Then $o'_1(b) > v_2(x_2) + o'_2(b) \geq o'_2(b)$ and hence (1a) fails. If moreover $2 \mid x_2$ then $o'_1(b) > v_2(x_2) + o'_2(b) > o'_2(b) \geq 0$, so (1b) fails too. So we assume that $2 \nmid x_2$ and hence $2 \mid y_2$. Then $2 \nmid y_1$ by Lemma 3.1. If (1b) holds then (3.9) yields the following contradiction $2^{m-1} \equiv x_1(1 + y_1)2^{m-1} \equiv 0 \pmod{2^m}$. This completes the case $m \leq n_2$.

Finally suppose that $m > n_2$. By assumption $0 < m - n_2 \neq o_1 - o_2$. In particular $o_1 \geq o_1 + o'_2 - m = m - n_2 > 0$, thus $o_2 = 0$. So we must prove that $b \in \mathcal{B}'_r$ if and only if condition (2) holds. Moreover, by Lemma 2.4 (3), $o'_2(\bar{b}) = 2m - n_2 - o_1$ for each $\bar{b} \in \mathcal{B}_r$. Then

$$n_1 - n_2 - o_1 = m - n_2 - o_1 = o'_2(\bar{b}) - m \leq 0$$

and hence

$$o'_1(b) + \min(0, n_1 - n_2 - o_1) = o'_1(b) + o'_2(b) - m \leq o'_2(b).$$

As in the previous case, the third condition of (4.3) does not hold. Therefore $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if $o'_1(\bar{b}) \leq o'_1(b)$ if and only if one of the first two conditions in (4.3) holds. Suppose $b \in \mathcal{B}'_r$. Then taking $\bar{b} = (b_1 b_2, b_2) \in \mathcal{B}'_r$ from (4.3) we obtain that condition (2) holds. Conversely, if $b \notin \mathcal{B}'_r$ and $\bar{b} \in \mathcal{B}'_r$ then $o'_1(\bar{b}) > o'_1(b)$ and consequently none of the conditions in (4.3) hold. If $2 \mid x_1 y_1$ then $2 \mid y_1$ and $o'_2(b) > 1 + n_1 - n_2 + o'_1(b)$, so condition (2) fails. Otherwise either $o'_1(b) = 0$ or $o'_2 > n_1 - n_2 + o'_1$. In all cases condition (2) fails. \square

Lemma 4.3. Suppose $\sigma_1 = -1$, $\sigma_2 = 1$ and let $b \in \mathcal{B}_r$. Then $b \in \mathcal{B}'_r$ if and only if the following conditions hold:

- (1) If $m \leq n_2$ then $o'_1(b) \leq o'_2(b)$ or $o_2 = 0 < n_1 - n_2 < o_1$.
 (2) If $m > n_2$ then $o'_1(b) = 1$ or $o_1 + 1 \neq n_1$.

Proof. By Proposition 2.3, $p = 2$ and $n_1 > n_2$, and by Lemma 2.4 each of $o'_1(b)$ and $o'_1(\bar{b})$ is at most 1.

(1) Assume that $m \leq n_2$. By Lemma 3.6, $o'_1(b) = o'_1(\bar{b})$, $o'_2(b) \leq 1$ and $o'_2(\bar{b}) \leq 1$. Moreover $o'_2(b) \neq o'_2(\bar{b})$ if and only if $v_2(x_2) = n_1 - n_2$ and $o'_1(b) = 1$. This implies that if $o'_1(b) \leq o'_2(b)$ then $b \in \mathcal{B}'_r$ because if $o'_1(b) = 1$ then $o'_2(b) = 1$ and otherwise $o'_2(b) = o'_2(\bar{b})$ for every $\bar{b} \in \mathcal{B}_r$. It also implies, in combination with Lemma 3.1, that if $o_2 = 0$ and $n_1 - n_2 < o_1$ then $o'_2(b) = o'_2(\bar{b})$, so again $b \in \mathcal{B}'_r$. Suppose otherwise that $o'_2(b) < o'_1(b)$ and either $o_2 \neq 0$ or $o_1 \leq n_1 - n_2$. Then $o'_1(b) = 1$, $o'_2(b) = 0$, $\bar{b} = (b_1, b_1^{2^{n_1-n_2}} b_2) \in \mathcal{B}_r$ and $o'_2(\bar{b}) > o'_2(b)$. Thus $b \notin \mathcal{B}'_r$.

(2) Assume that $m > n_2$. Then $o'_2(b) = o'_2(\bar{b}) = m - n_2 + 1$ by Lemma 2.4 (4). Moreover, by Lemma 3.6, $o'_1(b) \neq o'_1(\bar{b})$ if and only if $2 \nmid y_1$ and $n_1 = o_1 + 1$. This implies that if $o'_1(b) = 1$ then $b \in \mathcal{B}'_r$. If $o_1 + 1 \neq n_1$ then $o'_1(b) = o'_1(\bar{b})$ and as $o'_2(b) = o'_2(\bar{b})$, in this case $\mathcal{B}_r = \mathcal{B}'_r$ and in particular $b \in \mathcal{B}'_r$. Finally, if $o'_1(b) \neq 1$ and $o_1 + 1 = n_1$ then, taking $\bar{b} = (b_1^{1-2^{o_1-o_2}} b_2, b_2) \in \mathcal{B}_r$, we obtain that $o'_1(\bar{b}) > o'_1(b) = 0$. Therefore $b \notin \mathcal{B}'_r$. \square

Lemma 4.4. Suppose that $\sigma_2 = -1$ and let $b \in \mathcal{B}_r$. Then $b \in \mathcal{B}'_r$ if and only if the following conditions hold:

- (1) If $o_1 \leq o_2$ and $n_1 > n_2$ then $o'_1(b) \leq o'_2(b)$.
 (2) If $o_1 = o_2$ and $n_1 = n_2$ then $o'_1(b) \geq o'_2(b)$.
 (3) If $o_2 = 0 < o_1 = n_1 - 1$ and $n_2 = 1$ then $o'_1(b) = 1$ or $o'_2(b) = 1$.
 (4) If $o_2 = 0 < o_1$ and either $n_1 \neq o_1 + 1$ or $n_2 \neq 1$, then $o'_1(b) + \min(0, n_1 - n_2 - o_1) \leq o'_2(b)$.
 (5) If $o_1 o_2 \neq 0$ and $o_1 \neq o_2$ then $o'_1(b) \leq o'_2(b)$.

Proof. By Proposition 2.3 and Lemma 2.4 (1), $p = 2$, $\sigma_1 = -1$ and for $i = 1, 2$ each of $o'_i(b)$ and $o'_i(\bar{b})$ is at most 1. Moreover, (3.16) and (3.17) hold. We consider separately two cases.

Case (i). Suppose that $o_1 + 1 = n_1$, $o_2 = 0 < o_1$ and $n_2 = 1$. Then the summand B in (3.17) is $x_2 2^{m-n_1} = T 2^{m-n_1}$ with $T = x_2 2^{n_2-n_1} \in \mathbb{Z}$. Applying Remark 4.1 to the congruences (3.16) and (3.17), and recalling that $o'_i(b) \leq 1$, we obtain that $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if

$$(4.5) \quad o'_2(b) \leq v_2(y_1) + n_1 - n_2 + o'_1(b);$$

and

$$(4.6) \quad \text{if } o'_1(b) = o'_1(\bar{b}) \text{ and } v_2(x_2) = n_1 - n_2 \text{ then } o'_1(b) = 1 \text{ or } o'_2(b) = 1.$$

Observe that (4.5) always holds because

$$v_2(y_2) + n_1 - n_2 + o'_1(b) \geq n_1 - n_2 = o_1 \geq 1 \geq o'_2(b).$$

Thus $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if (4.6) holds. Moreover, by the assumptions, none of the antecedents in (1), (2), (4) and (5) holds, while the antecedent of (3) holds. So we must prove that $b \in \mathcal{B}'_r$ if and only if $o'_1(b) = 1$ or $o'_2(b) = 1$. Indeed, if $b \in \mathcal{B}'_r$ then taking $\bar{b} = (b_1, b_1^{2^{o_1}} b_2) \in \mathcal{B}_r$ we obtain that $o'_1(b) = 1$ or $o'_2(b) = 1$ by (4.6). Conversely, if $b \notin \mathcal{B}'_r$ and $\bar{b} \in \mathcal{B}_r$ then (4.6) fails, so $o'_1(b) = o'_2(b) = 0$ and hence condition (3) fails. This proves the lemma in Case (i).

Case (ii). Assume that at least one of the following conditions holds: $o_1 + 1 \neq n_1$, $o_2 \neq 0$, $o_1 = 0$ or $n_2 \neq 1$.

Then the summand B in (3.17) is 0 and by Remark 4.1, $o'(\bar{b}) \leq_{\text{lex}} o'(b)$ if and only if (4.5) holds and

$$(4.7) \quad \text{if } o'_1(b) = o'_1(\bar{b}) \text{ then } o'_1(b) \leq v_2(x_2) + n_2 - n_1 + o'_2(b).$$

By hypothesis, the antecedent of (3) does not hold in this case. So we must prove that $b \in \mathcal{B}'_r$ if and only if the conditions (1), (2), (4) and (5) hold.

Suppose that $b \in \mathcal{B}'_r$. Assume $o_1 \leq o_2$ and $n_1 > n_2$. Then either $o_1 = 0$ or $0 < o_1 = o_2$ by Proposition 2.3 (4). In the first case take $\bar{b} = (b_1, b_1^{2^{n_1-n_2}} b_2) \in \mathcal{B}_r$, and in the second take $\bar{b} = (b_1, b_1^{2^{n_1-n_2}} b_2^{1-2^{n_1-n_2}}) \in \mathcal{B}_r$. In both cases $o'_1(b) \leq o'_2(b)$ by (4.7). Thus condition (1) holds. If $o_1 = o_2$ and $n_1 = n_2$ then, taking $\bar{b} = (b_2, b_1)$, (4.5) yields $o'_1(b) \geq o'_2(b)$. Hence condition (2) holds. If $o_2 = 0 < o_1$ then, taking $\bar{b} = (b_1, b_1^{2^{\max(n_1-n_2, o_1)}} b_2) \in \mathcal{B}_r$, (4.7) yields $o'_1(b) + \min(0, n_1 - n_2 - o_1) \leq o'_2(b)$. Thus condition (4) holds. If $o_1 o_2 \neq 0$ and $o_1 \neq o_2$ then $o_2 < o_1 < o_2 + n_1 - n_2$, by Proposition 2.3 (4). Taking $\bar{b} = (b_1, b_1^{2^{n_1-n_2}} b_2^{1-2^{n_1-n_2+o_2-o_1}}) \in \mathcal{B}_r$, (4.7) yields $o'_1(b) \leq o'_2(b)$.

Conversely, suppose that b satisfies (1), (2), (4) and (5) and $b \notin \mathcal{B}'_r$. Take $\bar{b} \in \mathcal{B}'_r$. Then either (4.5) or (4.7) fails. If (4.5) fails then

$$1 \geq o'_2(b) > v_2(y_1) + n_1 - n_2 + o'_1(b),$$

so necessarily $o'_2(b) = 1$ and $v_2(y_1) = o'_1(b) = n_1 - n_2 = 0$. Then either $o_1 = 0$ or $o_1 = o_2 > 0$ by Proposition 2.3 (4). If $o_1 = 0$ then $o_2 \leq v_2(y_1) = 0$ by Lemma 3.1. Hence in both cases $o_1 = o_2$ and condition (2) yields the contradiction $0 = o'_1(b) \geq o'_2(b) = 1$. Suppose that (4.7) does not hold. Then $o'_1(b) = o'_1(\bar{b})$ and

$$1 \geq o'_1(b) > v_2(x_2) + n_2 - n_1 + o'_2(b) \geq 0.$$

Therefore $o'_1(b) = 1$, $o'_2(b) = 0$ and $v_2(x_2) = n_1 - n_2$. If $o_1 \leq o_2$ then $n_1 = n_2$ by condition (1), hence $2 \nmid x_2 y_1$ and $2 \mid x_1, y_2$ by Lemma 3.1 (2), therefore Lemma 3.7 yields the contradiction $0 = o'_2(b) = o'_1(\bar{b}) = o'_1(b) = 1$. Thus $o_2 < o_1$. By condition (5), $o_1 o_2 = 0$, so necessarily $o_2 = 0 < o_1$. Then $n_1 - n_2 = v_2(x_2) \geq o_1$ by Lemma 3.1, and consequently $\min(0, n_1 - n_2 - o_1) + o'_1(b) = o'_1(b) > o'_2(b)$ contradicting condition (4). \square

5. CONDITIONS ON u_1 AND u_2 : THE SET \mathcal{B}_{rt}

In this section, the roles of \mathcal{B}_r and \mathcal{B}'_r from Section 4 are now played respectively by \mathcal{B}'_r and

$$\mathcal{B}_{rt} = \{b \in \mathcal{B}'_r : u(b) = (u_2, u_1)\}.$$

Let $b = (b_1, b_2)$ be a fixed element of \mathcal{B}'_r . The goal is to obtain necessary and sufficient conditions for $b \in \mathcal{B}_{rt}$ in terms of conditions on the entries of $u(b) = (u_2(b), u_1(b))$. Observe that if $b = (b_1, b_2) \in \mathcal{B}$ then $b \in \mathcal{B}_{rt}$ if and only if

$$[b_2, b_1]^{b_i} = [b_2, b_1]^{r_i} \quad \text{and} \quad b_i^{p^{n_i}} = [b_2, b_1]^{t_i}, \quad \text{for } i \in \{1, 2\}.$$

We consider separately the cases $\sigma_1 = 1$ and $\sigma_1 = -1$ and use the following notation from the Main Theorem:

$$\begin{aligned} a_1 &= \min(o'_1, o_2, o_2 + n_1 - n_2 + o'_1 - o'_2), \\ a_2 &= \begin{cases} 0, & \text{if } o_1 = 0; \\ \min(o_1, o'_2, o'_2 - o'_1 + \max(0, o_1 + n_2 - n_1)), & \text{if } o_2 = 0 < o_1; \\ \min(o_1 - o_2, o'_2 - o'_1), & \text{otherwise.} \end{cases} \end{aligned}$$

Lemma 5.1. *Assume $\sigma_1 = 1$ and let $b \in \mathcal{B}'_r$. Then $b \in \mathcal{B}_{rt}$ if and only if $u_1(b) \leq p^{a_1}$ and one of the following holds:*

- (1) $u_2(b) \leq p^{a_2}$;
- (2) $o_1 o_2 \neq 0$, $n_1 - n_2 + o'_1 - o'_2 = 0 < a_1$, $1 + p^{a_2} \leq u_2(b) \leq 2p^{a_2}$, and $u_1(b) \equiv 1 \pmod{p}$.

Proof. By Lemma 2.4 (3), $o_2 + o'_1 \leq m \leq n_1$ and if $m = n_1$ then $o_1 o_2 = 0$. Moreover, either $o_1 + o'_2(\bar{b}) \leq m \leq n_2$ or $2m - o_1 - o'_2(\bar{b}) = n_2 < m$ for every $\bar{b} \in \mathcal{B}_r$. We will use this without specific mention. Let $\tilde{\mathcal{B}}_{rt}$ denote the set of the elements in \mathcal{B}'_r which satisfy $u_1(b) \leq p^{a_1}$ and either (1) or (2).

It suffices to prove the following:

- (i) $\tilde{\mathcal{B}}_{rt} \neq \emptyset$.
- (ii) If $b \in \tilde{\mathcal{B}}_{rt}$ and $\bar{b} \in \mathcal{B}'_r$ and $u(\bar{b}) \leq_{\text{lex}} u(b)$ then $u(b) = u(\bar{b})$.

Proof of (i). Start with $b = (b_1, b_2) \in \mathcal{B}'_r$. We construct another element $\bar{b} = (b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2})$ with x_1, x_2, y_1 and y_2 selected as in the Tables 1, 2 or 3, depending on the values of o_1 and o_2 . The reader may verify that the conditions of Lemma 3.1 hold, so $\bar{b} \in \mathcal{B}_r$. Using congruences (3.9) and (3.10) we verify that in all cases $o'_i(\bar{b}) = o'_i$, which guarantees that $\bar{b} \in \mathcal{B}'_r$, and that $u_1(\bar{b}) \leq p^{a_1}$ and $u(\bar{b})$ satisfies either (1) or (2) in each case, i.e. $\bar{b} \in \tilde{\mathcal{B}}_{rt}$.

(a) Suppose first that $o_1 = 0$. Write $u_1(b) = \rho + qp^{a_1}$ with $1 \leq \rho \leq p^{a_1}$. Observe that $p \nmid \rho$, since $p \nmid u_1(b)$ and if $a_1 = 0$ then $\rho = 1$. Let ρ' be an integer with $\rho\rho' \equiv 1 \pmod{p^m}$. We take x_1, x_2, y_1 and y_2 as in Table 1.

We verify now that $o'(\bar{b}) = o'$, $u_1(\bar{b}) = \rho$ and $u_2(\bar{b}) = 1$, which imply that $\bar{b} \in \tilde{\mathcal{B}}_{rt}$, as desired. Indeed, in all cases $p \nmid y_2$. Moreover (3.10) takes the form

$$y_2 u_2(b) u_2(\bar{b}) p^{m-o'_2(\bar{b})} \equiv y_2 u_2(b) p^{m-o'_2} \pmod{p^m},$$

hence $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) = 1$. Now we use (3.9). If $o'_1 = a_1$ then

$$u_2(b) u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv u_2(b) u_1(b) p^{m-o'_1} \pmod{p^m}$$

$o_1 = 0$	x_1	y_1	x_2	y_2
$a_1 = o'_1$	$u_2(b)$	0	0	1
$a_1 = o_2$	$u_2(b)$	0	0	$\rho' u_1(b)$
$a_1 = o_2 + n_1 - n_2 + o'_1 - o'_2 < o_2$	$u_2(b)$	$-qp^{o_2}$	0	1

TABLE 1. Values of x_i and y_i such that $\bar{b} = (b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2}) \in \tilde{\mathcal{B}}_{rt}$, when $o_1 = 0$

and hence $o'_1(\bar{b}) = o'_1$ and $u_1(\bar{b}) = u_1(b) \leq p^{o'_1} = p^{a_1}$, so $u_1(\bar{b}) = \rho$. Suppose that $a_1 = o_2$. Then

$$u_2(b) \rho' u_1(b) u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv u_2(b) u_1(b) p^{m-o'_1} \pmod{p^m}.$$

Thus $o'_1(\bar{b}) = o'_1$ and $u_1(\bar{b}) \equiv \rho \pmod{p^{o'_1}}$. Since $1 \leq \rho \leq p^{o'_1}$ and $1 \leq u_1(\bar{b}) \leq p^{o'_1}$, we deduce that $u_1(\bar{b}) = \rho$. Finally, assume that $a_1 = o_2 + n_1 - n_2 + o'_1 - o'_2 < o_2$. Then $o'_2 > o'_1 + n_1 - n_2$ and hence $o_2 \neq 0$, by Lemma 4.2 (1). So $p \mid y_1$ and thus $B_1 \equiv 0 \pmod{p^m}$. Hence

$$\begin{aligned} u_2(b) u_1(\bar{b}) p^{m-o'_1(\bar{b})} &\equiv u_2(b) u_1(b) p^{m-o'_1} - q u_2(b) p^{m-o'_2+o_2+n_1-n_2} \\ &\equiv u_2(b) p^{m-o'_1} (u_1(b) - q p^{a_1}) \\ &\equiv u_2(b) p^{m-o'_1} \rho \pmod{p^m}. \end{aligned}$$

Therefore $o'_1(\bar{b}) = o'_1$ and, arguing as in the previous case, we deduce again that $u_1(\bar{b}) = \rho$.

(b) Suppose now that $o_2 = 0 < o_1$. In this case we write $u_2(b) = \rho + q p^{a_2}$ with $1 \leq \rho \leq p^{a_2}$. Again $p \nmid \rho$ and we choose an integer ρ' with $\rho \rho' \equiv 1 \pmod{p^m}$. Moreover let

$$\delta = \begin{cases} 1, & \text{if } p = 2 \text{ and } m - n_2 = o_1; \\ 0, & \text{otherwise.} \end{cases}$$

Then we take x_1, x_2, y_1 and y_2 as in Table 2. We verify now that $o'(\bar{b}) = o'$, $u_1(\bar{b}) = 1$ and $u_2(\bar{b}) = \rho$, so again $\bar{b} \in \tilde{\mathcal{B}}_{rt}$.

$o_2 = 0 < o_1$	x_1	y_1	x_2	y_2
$a_2 = o'_2$	1	0	0	$u_1(b)$
$a_2 = o'_2 - o'_1 + \max(0, o_1 + n_2 - n_1) < o_1$	1	0	$-q p^{\max(n_1 - n_2, o_1)}$	$u_1(b)$
$a_2 = o_1$	$\rho' u_2(b) + \delta q 2^{m-1}$	0	0	$u_1(b)$

TABLE 2. Values of x_i and y_i such that $\bar{b} = (b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2}) \in \tilde{\mathcal{B}}_{rt}$, when $o_2 = 0 < o_1$

By (2.6), $m - 1 \geq o_1 > 0$ and therefore in all cases $x_1 \equiv 1 \pmod{p^{o_1}}$, so the conditions in Lemma 3.1 hold. By (3.9),

$$x_1 u_1(b) u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv x_1 u_1(b) p^{m-o'_1} \pmod{p^m},$$

so $o'_1 = o'_1(\bar{b})$ and $u_1(\bar{b}) = 1$. Next we use (3.10). If $a_2 = o'_2$ then

$$u_1(b) u_2(\bar{b}) p^{m-o'_2(\bar{b})} \equiv u_1(b) u_2(b) p^{m-o'_2} \pmod{p^m},$$

so $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) = u_2(b) = \rho$. If $a_2 = o'_2 - o'_1 + \max(0, o_1 + n_2 - n_1) < o_1$ then $n_1 > m$, since otherwise $m = n_1 > n_2 = 2m - o_1 - o'_2$, so

$$o_1 \leq m - o'_1 = o'_2 - o'_1 + o_1 + n_2 - n_1 = a_2 < o_1.$$

Thus $B_2 = 0$ and hence

$$\begin{aligned} u_1(b) u_2(\bar{b}) p^{m-o'_2(\bar{b})} &\equiv -q p^{\max(0, o_1 + n_2 - n_1)} u_1(b) p^{m-o'_1} + u_1(b) u_2(b) p^{m-o'_2} \\ &\equiv u_1(b) (-q p^{a_2} + u_2(b)) p^{m-o'_2} \\ &\equiv u_1(b) \rho p^{m-o'_2} \pmod{p^m}, \end{aligned}$$

so once more $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) = \rho$. Now assume $a_2 = o_1$. If $p = 2$ and $m - n_2 = o_1$ then, recalling that $1 < v_2(r_1 - 1) = m - o_1 = n_2$, we deduce that $A \equiv q2^{m-1} \pmod{2^m}$. Moreover, $o'_2 = o'_2(\bar{b}) = 2m - n_2 - o_1 = m$. Thus

$$u_2(\bar{b})\rho'u_2(b)u_1(b) \equiv q2^{m-1} + u_2(\bar{b})(\rho'u_2(b) + q2^{m-1})u_1(b) \equiv u_1(b)u_2(b) \pmod{2^m}.$$

Otherwise $\delta = A = 0$ and again

$$\rho'u_2(b)u_1(b)u_2(\bar{b})p^{m-o'_2(\bar{b})} \equiv u_1(b)u_2(b)p^{m-o'_2} \pmod{p^m}.$$

In both cases $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) = \rho$, as desired.

(c) Suppose that $o_1 o_2 \neq 0$ and let

$$a'_1 = n_1 - n_2 - \max(o_1 - o_2, o'_2 - o'_1).$$

Then $m < n_1$, by Lemma 2.4 (3); $n_2 < n_1$, by Proposition 2.3 (4); $a_1 = \min(o'_1, o_2)$, by Lemma 4.2 (3); and $0 \leq \min(a'_1, a_2)$ by the combination of Proposition 2.3 (4) and Lemma 4.2 (3). Moreover, $a'_1 = 0$ if and only if $n_1 - n_2 = o'_2 - o'_1$ and, in that case, $a_2 = o_1 - o_2 > 0$. Similarly, $a_2 = 0$ if and only if $o'_2 = o'_1$ and, in that case, $a'_1 = n_1 - n_2 - o_1 + o_2 > 0$.

Let ρ and q be integers such that

$$1 \leq \rho \leq p^{a_2} \quad \text{and} \quad u_2(b) = \rho + qp^{a_2}.$$

Define

$$(R_2, q_2) = \begin{cases} (\rho + p^{a_2}, q - 1), & \text{if } u_1(b) \equiv qp^{a'_1} \pmod{p} \text{ and } 0 < a_1; \\ (\rho, q), & \text{otherwise;} \end{cases}$$

and

$$R = u_1(b) - q_2 p^{a'_1}.$$

Finally, let R_1 and q_1 be integers such that

$$1 \leq R_1 \leq p^{a_1} \quad \text{and} \quad R = R_1 + q_1 p^{a_1}.$$

As in the previous cases $p \nmid \rho$.

Claim: $p \nmid R_i$ for $i = 1, 2$ and if $p \mid R$ then $a'_1 = o'_1 = 0$.

Indeed, as $p \nmid u_1(b)$, if $p \mid R$ then $a'_1 = 0$ and hence $u_1(b) \equiv q_2 \pmod{p}$. Then $a_1 = 0$ by the definition of q_2 and thus $o'_1 = 0$. This proves the last statement of the claim. If $p \mid R_1$ then $a_1 > 0$ and hence $p \mid R$, so also $a'_1 = 0$, and therefore $u_1(b) \equiv q_2 \pmod{p}$, contradicting the definition of q_2 . Finally, if $p \mid R_2$ then $u_1(b) \equiv qp^{a'_1} \pmod{p}$, $a_1 > 0$ and $a_2 = 0$, so $a'_1 > 0$ and hence $p \mid u_1(b)$, yielding a contradiction. This proves the claim.

Therefore there are integers R'_1, R'_2 with $R_i R'_i \equiv 1 \pmod{p^m}$, for $i = 1, 2$ and if $a'_1 \neq 0$ or $o'_1 \neq 0$ then there is another integer R' such that $RR' \equiv 1 \pmod{p^m}$. Observe that $u_2(b) = R_2 + q_2 p^{a_2}$ and hence $R'_2 u_2(b) \equiv 1 + R'_2 q_2 p^{a_2} \pmod{p^m}$.

We take x_1, x_2, y_1 and y_2 as in Table 3 with

$$\delta = \begin{cases} 1, & \text{if } p = 2 \text{ and } m - n_2 = o_1 - o_2; \\ 0, & \text{otherwise.} \end{cases}$$

In all cases it is straightforward that the conditions of Lemma 3.1 hold and that $p \nmid y_2$. We will prove that $o'(\bar{b}) = o'$ and $u_i(\bar{b}) = R_i$ for $i = 1, 2$. It is then straightforward to verify that $\bar{b} \in \tilde{\mathcal{B}}_{rt}$, because if $R_2 > p^{a_2}$ then $u_1(b) \equiv qp^{a'_1} \pmod{p}$, $0 < a_1$, $q_2 = q - 1$ and $1 + p^{a_2} \leq R_2 = \rho + p^{a_2} \leq 2p^{a_2}$. Hence $a'_1 = 0$, so $u_1(b) \equiv q \pmod{p}$, and therefore $R_1 = u_1(b) - (q - 1) \equiv 1 \pmod{p}$.

$o_1 o_2 \neq 0$	x_1	y_1	x_2	y_2
$a_2 = o'_2 - o'_1, a_1 = o_2$	1	0	$-R'_1 q_2 p^{n_1 - n_2}$	$R'_1 u_1(b)$
$a_2 = o'_2 - o'_1, a_1 = o'_1$	1	0	$-R'_1 q_2 p^{n_1 - n_2}$	$R'_1 u_1(b)$
$a_2 \neq o'_2 - o'_1, a_1 = o_2$	$R'_2 u_2(b) + \delta q_2 2^{o'_2 - 1}$	$-R'_2 q_2 - \delta q_2 2^{o'_2 - 1 - o_1 + o_2}$	0	$R'_1 R$
$a_2 \neq o'_2 - o'_1, a_1 = o'_1$	$R'_2 u_2(b) + \delta q_2 2^{o'_2 - 1}$	$-R'_2 q_2 - \delta q_2 2^{o'_2 - 1 - o_1 + o_2}$	0	1

TABLE 3. Values of x_i and y_i such that $\bar{b} = (b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2}) \in \tilde{\mathcal{B}}_{rt}$, when $o_1 o_2 \neq 0$

Observe that $B_1 = B_2 = 0$ because $m < n_1$.

Assume that $a_2 = o'_2 - o'_1$. Then $a'_1 = n_1 - n_2 + o_2 - o_1 > 0$. Hence $u_1(b) \not\equiv q_2 p^{a'_1} \pmod{p}$, so $R_2 = \rho$ and $q_2 = q$. Then $y_2 \equiv R'_1 u_1(b) \pmod{p^{o'_1}}$. By (3.9), $y_2 u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv u_1(b) p^{m-o'_1} \pmod{p^m}$, thus $o'_1(\bar{b}) = o'_1$ and $R'_1 u_1(b) u_1(\bar{b}) \equiv u_1(b) \pmod{p^{o'_1}}$. This implies that $R_1 \equiv u_1(\bar{b}) \pmod{p^{o'_1}}$. Hence, as $1 \leq R_1 \leq p^{o'_1}$ and $1 \leq u_1(\bar{b}) \leq p^{o'_1}$, we deduce that $u_1(\bar{b}) = R_1$. Moreover, by (3.10),

$$y_2 u_2(\bar{b}) p^{m-o'_2(\bar{b})} \equiv x_2 u_1(b) p^{m-o'_1+n_2-n_1} + y_2 u_2(b) p^{m-o'_2} \pmod{p^m}.$$

Substituting x_2 and y_2 by their values in Table 3, and multiplying both sides by R_1 if $a_1 = o_2$ and by R if $a_1 = o'_1$, we obtain that

$$u_1(b) u_2(\bar{b}) 2^{m-o'_2(\bar{b})} \equiv -q_2 u_1(b) p^{m-o'_1} + u_2(b) u_1(b) p^{m-o'_2} \pmod{p^m},$$

that is,

$$u_2(\bar{b}) p^{m-o'_2(\bar{b})} \equiv (-q_2 p^{a_2} + u_2(b)) p^{m-o'_2} = R_2 p^{m-o'_2} \pmod{p^m}.$$

Therefore $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) = R_2$.

Otherwise $0 < a_2 = o_1 - o_2 < o'_2 - o'_1$ and $a'_1 = n_1 - n_2 + o'_1 - o'_2$. In particular, $a_2 < o'_2$ and $o'_1 < o'_2 - 1$. Thus $\delta 2^{m-o'_1+o'_2-1} \equiv 0 \pmod{p^m}$. We consider separately the two options for δ .

Suppose that $\delta = 0$. Then $A = 0$ and by (3.10)

$$y_2 R'_2 u_2(b) u_2(\bar{b}) p^{m-o'_2(\bar{b})} \equiv y_2 u_2(b) p^{m-o'_2} \pmod{p^m}.$$

Hence $o'_2(\bar{b}) = o'_2$ and $u_2(\bar{b}) \equiv R_2 \pmod{p^{o'_2}}$. Moreover $1 \leq R_2 \leq 2p^{a_2} \leq p^{o'_2}$ and $1 \leq u_2(\bar{b}) \leq p^{o'_2}$, so $u_2(\bar{b}) = R_2$. Furthermore, by (3.9),

$$R'_2 u_2(b) y_2 u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv R'_2 u_2(b) u_1(b) p^{m-o'_1} - R'_2 q_2 u_2(b) p^{m-o'_2+n_1-n_2} \pmod{p^m},$$

hence

$$(5.1) \quad y_2 u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv (u_1(b) - q_2 p^{a'_1}) p^{m-o'_1} \equiv R p^{m-o'_1} \pmod{p^m}.$$

If $a_1 = o_2$ then $o'_1 \geq o_2 > 0$, so $p \nmid R$, by the Claim. Then (5.1) takes the form

$$R'_1 R u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv R p^{m-o'_1} \pmod{p^m}.$$

If $a_1 = o'_1$ then $R = R_1 + q_1 p^{o'_1}$, so (5.1) takes the form

$$u_1(\bar{b}) p^{m-o'_1(\bar{b})} \equiv R_1 p^{m-o'_1} \pmod{p^m}.$$

In either case $o_1(\bar{b}) = o'_1$ and $u_1(\bar{b}) \equiv R_1 \pmod{p^{o'_1}}$; thus, as $R_1 \leq p^{a_1} \leq p^{o'_1}$ and $u_1(\bar{b}) \leq p^{o'_1}$, we conclude that $u_1(\bar{b}) = R_1$.

Finally assume $\delta = 1$, i.e., $p = 2$ and $m - n_2 = o_1 - o_2$. Then $n_2 = 2m - o_1 - o'_2 = 2m - o_1 - o'_2(\bar{b})$, by Lemma 2.4 (3), so $o'_2 = o'_2(\bar{b}) = m - o_2$. Since $0 < o_1 - o_2 < o'_2 - o'_1$, $m - o'_1 + o'_2 - 1 > m$. Furthermore, by Proposition 2.3 (4), $m - 1 - o_1 + o_2 + n_1 - n_2 \geq m$. Thus congruence (3.9) implies

$$\begin{aligned} R'_2 u_2(b) y_2 u_1(\bar{b}) 2^{m-o'_1(\bar{b})} &\equiv R'_2 u_2(b) u_1(b) 2^{m-o'_1} - R'_2 q_2 u_2(b) 2^{m-o'_2+n_1-n_2} \\ &\equiv R'_2 u_2(b) 2^{m-o'_1} (u_1(b) - q_2 2^{a'_1}) \\ &\equiv R'_2 R u_2(b) 2^{m-o'_1} \pmod{2^m}. \end{aligned}$$

Hence $y_2 u_1(\bar{b}) 2^{m-o'_2(\bar{b})} \equiv R 2^{m-o'_1} \pmod{2^m}$, and arguing as in the previous paragraph we obtain again that $o'_1 = o'_1(\bar{b})$ and $u_1(\bar{b}) = R_1$. On the other hand $a_2 + n_2 - 1 = m - 1$ and, as $p = 2$ and $m \geq 2$, by Corollary 2.5 (2), $n_2 + o'_2 - 2 = 2m - o_1 - 2 \geq m$. Thus

$$\begin{aligned} A &\equiv (R'_2 u_2(b) + q_2 2^{o'_2-1} - 1) y_2 2^{n_2-1} \\ &\equiv (R'_2 q_2 2^{a_2} + q_2 2^{o'_2-1}) y_2 2^{n_2-1} \\ &\equiv y_2 R'_2 q_2 2^{a_2+n_2-1} + y_2 q_2 2^{n_2+o'_2-2} \\ &\equiv q_2 2^{m-1} \pmod{2^m}. \end{aligned}$$

Moreover $y_2 \delta q_2 2^{o'_2-1} 2^{m-o'_2} \equiv q_2 2^{m-1} \pmod{2^m}$. Hence, by (3.10),

$$R'_2 u_2(b) y_2 u_2(\bar{b}) 2^{m-o'_2} \equiv q_2 2^{m-1} + x_1 y_2 u_2(\bar{b}) 2^{m-o'_2(b)} \equiv y_2 u_2(b) 2^{m-o'_2} \pmod{2^m}.$$

So arguing as in the previous case one obtains that $u_2(\bar{b}) = R_2$. This proves (i).

Proof of (ii). Take $b \in \tilde{\mathcal{B}}_{rt}$ and $\bar{b} \in \mathcal{B}'_r$ such that $u(\bar{b}) \leq u(b)$. Then $o'_i(b) = o'_i(\bar{b})$ and $\bar{b}_i = b_1^{x_i} b_2^{y_i} [b_2, b_1]^{z_i}$ for some integers x_i, y_i, z_i satisfying the conditions in Lemma 3.1 and congruences (3.9) and (3.10), for $i = 1, 2$. We will prove that $u(\bar{b}) = u(b)$ by considering three cases.

(1) Suppose first that $o_1 = 0$. Then $a_2 = 0$ and $u_i(b) \leq p^{a_i}$. Thus $1 = u_2(b) = u_2(\bar{b})$ and $1 \leq u_1(\bar{b}) \leq u_1(b) \leq p^{a_1}$. If $a_1 = 0$ then $1 = u_1(b) = u_1(\bar{b})$. Assume otherwise. As $a_1 \leq o_2$, Lemma 3.1 yields $y_1 \equiv y_2 - 1 \equiv 0 \pmod{p^{a_1}}$, so $B_1 \equiv 0 \pmod{p^{a_1+n_1-1}}$. In particular, $B_1 \equiv 0 \pmod{p^m}$, and hence (3.9) implies $u_1(\bar{b})x_1 \equiv x_1u_1(b) \pmod{p^{a_1}}$, while $x_1 \equiv x_1y_2 - x_2y_1 \not\equiv 0 \pmod{p}$, so $u_1(\bar{b}) \equiv u_1(b) \pmod{p^{a_1}}$. Therefore $u_1(\bar{b}) = u_1(b)$.

(2) Assume now that $o_2 = 0 < o_1$. Then $a_1 = 0$ and $n_2 < n_1$ by Proposition 2.3 (4). Moreover, $(u_2(\bar{b}), u_1(\bar{b})) \leq_{\text{lex}} (u_2(b), u_1(b))$, $u_2(b) \leq p^{a_2}$ and $u_1(b) = 1$. Hence it suffices to prove that $u_2(b) = u_2(\bar{b})$. Moreover $p^{\max(o_1, n_1-n_2)} \mid x_2$. We assert that $A \equiv B_2 \equiv 0 \pmod{p^m}$ or $a_2 < o'_2$. Otherwise, $p = 2$ and, by the definition of a_2 , we conclude that $o'_2 \leq o_1$. If $A \not\equiv 0 \pmod{2^m}$ then $0 < o_1 = m - n_2 = -m + o_1 + o'_2$, by Lemma 2.4 (3), so $o_1 < m = o'_2 \leq o_1$, a contradiction. If $B_2 \not\equiv 0 \pmod{2^m}$ then $m = n_1$ and $0 < o_1 \leq v_2(x_2) \leq n_1 - n_2$, by Lemma 3.1. Thus, again by Lemma 2.4 (3), $o_1 \leq m - n_2 = -m + o_1 + o'_2$, yielding the contradiction $m \leq o'_2 \leq o_1 < m$. This proves the assertion. If $A \equiv B_2 \equiv 0 \pmod{p^m}$ then dividing by $p^{m-o'_2}$ in (3.10), with the help of Lemmas 3.1 and 4.2, the reader may verify that $u_2(\bar{b})y_2 \equiv y_2u_2(b) \pmod{p^{o'_2}}$ and hence also $u_2(\bar{b})y_2 \equiv y_2u_2(b) \pmod{p^{a_2}}$. Otherwise, $p = 2$ and $0 \leq a_2 < o'_2$ and hence $m - o'_2 \leq \min(v_2(A), v_2(B_2))$. Thus the same argument shows that $u_2(\bar{b})y_2 \equiv y_2u_2(b) \pmod{p^{a_2}}$. Since $y_2 \equiv x_1y_2 - x_2y_1 \not\equiv 0 \pmod{p}$, $u_2(\bar{b}) \equiv u_2(b) \pmod{p^{a_2}}$, so $u_2(b) = u_2(\bar{b})$ as desired.

(3) Assume that $o_1o_2 \neq 0$. By Lemma 3.1,

$$x_1 = 1 + x'_1p^{o_1-o_2}, \quad x_2 = x'_2p^{n_1-n_2}, \quad y_1 = -x'_1 - y'_1p^{o_1}, \quad y_2 = 1 - x'_2p^{n_1-n_2+o_2-o_1} + y'_2p^{o_2},$$

for some integers x'_1, x'_2, y'_1 and y'_2 . By Proposition 2.3 (4),

$$0 < \min(o_2, o_1 - o_2, n_1 - n_2 + o_2 - o_1),$$

so clearly $p \nmid x_1y_2$ and, by Lemma 4.2 (3), $a_1 = \min(o'_1, o_2)$. Moreover, by Corollary 2.5 (4), $m < n_1$, so $B_1 = B_2 = 0$. Thus (3.9) and (3.10) take the forms

$$\begin{aligned} u_1(\bar{b}) (x_1(1 + y'_2p^{o_2}) + x'_2p^{n_1-n_2-o_1+o_2}(y'_1p^{o_1} - 1)) &\equiv x_1u_1(b) - (x'_1 + y'_1p^{o_2})u_2(b)p^{n_1-n_2+o'_1-o'_2} \pmod{p^{o'_1}} \\ Ap^{o'_2-m} + u_2(\bar{b}) (y_2 + x'_1p^{o_1-o_2}(1 + y'_2p^{o_2}) + x'_2y'_1p^{n_1-n_2+o_2}) &\equiv u_1(b)x'_2p^{o'_2-o'_1} + u_2(b)y_2 \pmod{p^{o'_2}}. \end{aligned}$$

The congruences imply respectively that

$$\begin{aligned} u_1(b) &\equiv u_1(\bar{b}) \pmod{p^{\min(a_1, a'_1)}}, \\ Ap^{o'_2-m} + y_2u_2(\bar{b}) &\equiv y_2u_2(b) \pmod{p^{a_2}}. \end{aligned}$$

Suppose that $u_2(\bar{b}) \not\equiv u_2(b) \pmod{p^{a_2}}$. Then $p^{a_2} \nmid Ap^{o'_2-m}$ and hence $p = 2$ and $m - n_2 = o_1 - o_2 > 0$. Thus $2m - o_1 - o'_2 = n_2$, by Lemma 2.4 (3), so $o_2 + o'_2 = m$ and hence

$$a_2 \leq o_1 - o_2 \leq m - 1 - o_2 = o'_2 - 1.$$

As $2^{m-1} \mid A$, it follows that $2^{a_2} \mid A2^{o'_2-m}$, a contradiction. Therefore, $u_2(b) \equiv u_2(\bar{b}) \pmod{p^{a_2}}$. If $a_1 \leq a'_1$ then $n_1 - n_2 + o'_1 - o'_2 \neq 0$ or $a_1 = 0$ and hence $1 \leq u_i(b) \leq p^{a_i}$. Therefore $u_2(\bar{b}) = u_2(b)$ and $u_1(\bar{b}) = u_1(b)$, and we are done.

So we can assume $a'_1 < a_1$. Fix integers λ_1 and λ_2 such that $u_1(b) = u_1(\bar{b}) + \lambda_1p^{a'_1}$ and $u_2(b) = u_2(\bar{b}) + \lambda_2p^{a_2}$. So the congruences above can be rewritten as

$$u_1(\bar{b}) (x'_2p^{n_1-n_2-o_1+o_2-a'_1}(y'_1p^{o_1} - 1) + x_1y'_2p^{o_2-a'_1}) \equiv x_1\lambda_1 - (x'_1 + y'_1p^{o_2})u_2(b)p^{n_1-n_2+o'_1-o'_2-a'_1} \pmod{p^{o'_1-a'_1}},$$

and

$$Ap^{o'_2-m-a_2} + u_2(\bar{b}) (x'_1p^{o_1-o_2-a_2}(1 + y'_2p^{o_2}) + x'_2y'_1p^{n_1-n_2+o_2-a_2}) \equiv u_1(b)x'_2p^{o'_2-o'_1-a_2} + y_2\lambda_2 \pmod{p^{o'_2-a_2}}.$$

Note that $o'_1 - a'_1 < o'_2 - a_2$, since $a'_1 - a_2 = n_1 - n_2 + o_2 - o_1 + o'_1 - o'_2 > o'_1 - o'_2$. This, together with $a'_1 < a_1 = \min(o_2, o'_1)$, $o_1 - a_2 \geq o_2$ and $n_1 - n_2 - a_2 = n_1 - n_2 - \min(o_1 - o_2, o'_2 - o'_1) \geq a'_1 \geq 0$ implies that

$$\begin{aligned} -u_1(\bar{b})x'_2p^{n_1-n_2-o_1+o_2-a'_1} &\equiv (1+x'_1p^{o_1-o_2})\lambda_1 - x'_1u_2(b)p^{n_1-n_2+o'_1-o'_2-a'_1} \pmod{p^{a_1-a'_1}}, \\ u_2(\bar{b})x'_1p^{o_1-o_2-a_2} &\equiv u_1(b)x'_2p^{o'_2-o'_1-a_2} + (1-x'_2p^{n_1-n_2+o_2-o_1})\lambda_2 \pmod{p^{a_1-a'_1}}. \end{aligned}$$

If $a_2 = o_1 - o_2$, then $a'_1 = n_1 - n_2 + o'_1 - o'_2$, and

$$\begin{aligned} -u_1(\bar{b})x'_2p^{o'_2-o'_1-o_1+o_2} &\equiv (1+x'_1p^{o_1-o_2})\lambda_1 - x'_1u_2(b) \pmod{p^{a_1-a'_1}}, \\ u_2(\bar{b})x'_1 &\equiv u_1(b)x'_2p^{o'_2-o'_1-o_1+o_2} + (1-x'_2p^{n_1-n_2+o_2-o_1})\lambda_2 \pmod{p^{a_1-a'_1}}. \end{aligned}$$

By subtracting the second congruence from the first and simplifying, we obtain that

$$0 \equiv (\lambda_1 - \lambda_2)(1 + x'_1p^{o_1-o_2} - x'_2p^{n_1-n_2-o_1+o_2}) \pmod{p^{a_1-a'_1}}.$$

Similarly, if $a_2 = o'_2 - o'_1$ then $a'_1 = n_1 - n_2 + o_2 - o_1$, so

$$\begin{aligned} -u_1(\bar{b})x'_2 &\equiv (1+x'_1p^{o_1-o_2})\lambda_1 - x'_1u_2(b)p^{o_1-o_2+o'_1-o'_2} \pmod{p^{a_1-a'_1}}, \\ u_2(\bar{b})x'_1p^{o_1-o_2-o'_2+o'_1} &\equiv u_1(b)x'_2 + (1-x'_2p^{n_1-n_2+o_2-o_1})\lambda_2 \pmod{p^{a_1-a'_1}}, \end{aligned}$$

and consequently once again

$$0 \equiv (\lambda_1 - \lambda_2)(1 + x'_1p^{o_1-o_2} - x'_2p^{n_1-n_2-o_1+o_2}) \pmod{p^{a_1-a'_1}}.$$

In either case $\lambda_1 \equiv \lambda_2 \pmod{p^{a_1-a'_1}}$. Fix an integer q_1 such that $\lambda_1 = \lambda_2 + q_1p^{a_1-a'_1}$.

Moreover $1 \leq u_2(\bar{b}) \leq u_2(b) \leq 2p^{a_2}$ and, as $u_2(b) = u_2(\bar{b}) + \lambda_2p^{a_2}$ it follows that $\lambda_2 \in \{0, 1\}$. We claim that $\lambda_2 = 0$. Otherwise $1 + p^{a_2} \leq u_2(b) \leq 2p^{a_2}$, $1 \leq u_2(\bar{b}) \leq p^{a_2}$, $\lambda_2 = 1$ and $u_1(b) \equiv 1 \pmod{p}$. Therefore condition (2) holds, and hence $u_1(b) = u_1(\bar{b}) + \lambda_2 + q_1p^{a_1} \equiv u_1(\bar{b}) + 1 \pmod{p}$. Therefore $u_1(\bar{b}) \equiv 0 \pmod{p}$, contradicting $p \nmid u_1(\bar{b})$. Therefore $\lambda_2 = 0$, so $u_2(b) = u_2(\bar{b})$, $p^{a_1-a'_1} \mid \lambda_1$ and $u_1(b) \equiv u_1(\bar{b}) \pmod{p^{a_1}}$, which implies that $u_1(b) = u_1(\bar{b})$ because $1 \leq u_1(\bar{b}) \leq u_1(b) \leq p^{a_1}$. \square

Lemma 5.2. *Suppose that $\sigma_1 = -1$ and let $b \in \mathcal{B}'_r$. Then $b \in \mathcal{B}_{rt}$ if and only if at least one of the following conditions holds:*

- (1) $\sigma_2 = -1$ or $m \leq n_2$.
- (2) $o'_1 = 0$ and either $o_1 = 0$ or $o_2 + 1 \neq n_2$.
- (3) $o'_1 = 1$, $o_2 = 0$ and $n_1 - n_2 < o_1$.
- (4) $u_2(b) \leq 2^{m-n_2}$.

Proof. By Proposition 2.3 (1) and Lemma 2.4 (4), $o'_1 \leq 1$ and $u_1(b) = 1$ for each $b \in \mathcal{B}'_r$. Also by Lemma 2.4 (4), if $\sigma_2 = -1$ or $m \leq n_2$ then $o'_2 \leq 1$ and $u_2(b) = 1$ for each $b \in \mathcal{B}'_r$. In that case $\mathcal{B}'_r = \mathcal{B}_{rt}$, so we shall assume otherwise, i.e., $\sigma_2 = 1$ and $n_2 < m$. Then, once more by Lemma 2.4 (4), $n_2 = m - o'_2 + 1 < m$ and $u_2(b) \in \{v, v + 2^{m-n_2}\}$, where v is the unique integer satisfying $1 \leq v \leq 2^{m-n_2}$ and $v(1 + 2^{m-o_1-1}) \equiv -1 \pmod{2^{m-n_2}}$.

We argue as in the proofs in Section 4: we use several $\bar{b} = (b_1^{x_1}b_2^{y_1}[b_2, b_1]^{z_1}, b_1^{x_2}b_2^{y_2}[b_2, b_1]^{z_2}) \in \mathcal{B}'_r$ to compare $u(b)$ and $u(\bar{b})$ with the help of (3.14). We use Lemmas 3.1 and 4.3 to verify that the different \bar{b} constructed belong to \mathcal{B}'_r . Moreover, $b \in \mathcal{B}_{rt}$ if and only if $u_2(b) \leq u_2(\bar{b})$ for every $\bar{b} \in \mathcal{B}'_r$. Observe that (4) is equivalent to $u_2(b) = v$ and in that case obviously $u_2(b) \leq u_2(\bar{b})$. Thus we may assume that $u_2(b) \neq v$ and we must prove that $u_2(b) = u_2(\bar{b})$ for every $\bar{b} \in \mathcal{B}'_r$ if and only if either (2) or (3) holds.

Suppose that $u_2(b) = u_2(\bar{b})$ for every $\bar{b} \in \mathcal{B}'_r$. We consider separately the two possible values of o'_1 . Firstly assume that $o'_1 = 1$. If $o_2 = 0 < o_1$, $n_1 = o_1 + 1$ and $n_2 = 1$ and we take $\bar{b} = (b_1^{1-2^{o_1}}, b_1^{2^{o_1}}b_2) \in \mathcal{B}_r$ then $o'_1(\bar{b}) = o'_1(b)$, by Lemma 3.6 (2), so $\bar{b} \in \mathcal{B}'_r$ by Lemma 4.3 (2), and (3.14) yields the contradiction $2^{m-1} \equiv 0 \pmod{2^m}$, since $A = B = 2^{m-1}$. Therefore $o_1 + 1 < n_1$, $0 < o_2$, $o_1 = 0$ or $1 < n_2$. Then $B = 0$. If $o_1 = 0$ then take $\bar{b} = (b_1, b_1^{2^{n_1-n_2}}b_2)$; if $o_2 = 0 < o_1 \leq n_1 - n_2$ then take $\bar{b} = (b_1, b_1^{2^{n_1-n_2}}b_2)$, and if $o_1o_2 \neq 0$ then take $\bar{b} = (b_1, b_1^{2^{n_1-n_2}}b_2^{1-2^{n_1-n_2-o_1+o_2}})$. In each case $\bar{b} \in \mathcal{B}'_r$ by Lemma 3.6 (2) and Lemma 4.3 (2) and $A \equiv 0 \pmod{2^m}$, so congruence (3.14) yields again the contradiction that $2^{m-1} \equiv 0 \pmod{2^m}$. Therefore $o_2 = 0$ and $n_1 - n_2 < o_1$, so condition (3) holds. Next suppose $o'_1 = 0$. Then $o_1 + 1 \neq n_1$ and $\mathcal{B}_r = \mathcal{B}'_r$ by Lemma 4.3. The former implies that $B = 0$. Suppose that $o_2 + 1 = n_2$ and $o_1 > 0$ and take $\bar{b} = (b_1^{1-2^{o_1-o_2}}b_2, b_2)$. By

Proposition 2.3, $o_1 \neq o_2$ and hence $\bar{b} \in \mathcal{B}'_r$. Moreover, $A = 2^{m-1}$, so (3.14) yields once more the contradiction that $2^{m-1} \equiv 0 \pmod{2^m}$. Therefore $o_1 = 0$ or $o_2 + 1 \neq n_2$, so condition (2) holds.

Conversely, assume $u_2(b) \neq u_2(\bar{b})$ for some $\bar{b} \in \mathcal{B}_{rt}$. Therefore $u_2(b) - u_2(\bar{b}) = 2^{m-n_2}$ and we must prove that neither (2) nor (3) holds. Suppose that $o'_1 = 1$, $o_2 = 0$ and $n_1 - n_2 < o_1$. In particular $1 < n_2$, by Corollary 2.5 (2), and $2^{n_1-n_2+1} \mid x_2$, by Lemma 3.1, so $A = B = 0$. Moreover, $n_1 - n_2 + 1 \leq o_1 \leq v_2(x_2)$, by Lemma 3.1, and therefore $x_2 2^{m-o'_1+n_2-n_1} \equiv 0 \pmod{2^m}$. Thus (3.14) yields the contradiction $2^{m-1} \equiv 0 \pmod{2^m}$. Suppose that $o'_1 = 0$, and either $o_2 + 1 < n_2$ or $o_1 = 0$. This implies that $A = 0$. Since $o'_1 = 0$ and $m > n_2$, Lemma 4.3 yields $o_1 + 1 \neq n_1$. Thus $B = 0$. Hence once more (3.14) implies the contradiction that $2^{m-1} \equiv 0 \pmod{2^m}$. \square

6. PROOF OF THE MAIN THEOREM

By the arguments given in the introduction, the map associating $\text{inv}(G)$ to the isomorphism class of a finite non-abelian 2-generator cyclic-by-abelian group G of prime-power order is well defined and injective. So to prove our main result it is enough to show that the image of this map is formed by the lists satisfying the conditions in the Main Theorem.

We first prove that if G is a finite non-abelian 2-generator cyclic-by-abelian group of prime-power order and

$$\text{inv}(G) = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o'_1, o'_2, u_1, u_2),$$

then the conditions in the Main Theorem hold. Condition (1) follows from the definition of p, m, n_1 and n_2 . Conditions (2), (3) and (4) follow from the definitions of σ_i and u_i and from (2.6) and Corollary 2.5. Condition (5) is a consequence of Proposition 2.3.

To prove (6) and (7) we fix $b \in \mathcal{B}_{rt}$, which exists by Proposition 2.3 (5) and the definition of \mathcal{B}_{rt} . Then $o'_i = o'_i(b)$, $u_i = u_i(b)$. Suppose that $\sigma_1 = 1$. Then (6a) follows from Proposition 2.3 (2) and Corollary 2.5 (3), and (6b) from Lemma 2.4 (3). Furthermore, (6c), (6d) and (6e) follow from Lemma 4.2, and (6f) and (6g) from Lemma 5.1. This proves condition (6). Suppose now that $\sigma_1 = -1$. Then (7a) follows from the definition of σ_1 and Corollary 2.5 (1). Suppose that $\sigma_2 = 1$. Then $n_2 < n_1$, by Proposition 2.3 (2). Therefore (7(b)i) follows from Corollary 2.5 (5a) and Lemma 4.3 (1); and (7(b)ii) follows from Corollary 2.5 (5b), Lemma 4.3 (2) and Lemma 5.2. Finally, (7c) follows from Corollary 2.5 (1) and Lemma 4.4. This proves condition (7).

To complete the proof we need the following lemma, where for integers m and n with $n > 0$, $\lfloor \frac{m}{n} \rfloor$ and $[m]_n$ denote, respectively, the quotient and the remainder of m divided by n .

Lemma 6.1. *Let $M, N_1, N_2, r_1, r_2, t_1, t_2$ be positive integers satisfying the following conditions:*

$$(6.1) \quad r_i^{N_i} \equiv 1 \pmod{M},$$

$$(6.2) \quad t_i r_i \equiv t_i \pmod{M},$$

$$(6.3) \quad \mathcal{S}(r_1 \mid N_1) \equiv t_1(1 - r_2) \pmod{M},$$

$$(6.4) \quad \mathcal{S}(r_2 \mid N_2) \equiv t_2(r_1 - 1) \pmod{M}.$$

Consider the groups $A = \langle a \rangle$ and $B = \langle b_1 \rangle \times \langle b_2 \rangle$ with $|a| = M$ and $|b_i| = N_i$ for $i = 1, 2$. Then there is a group homomorphism $\sigma : B \rightarrow \text{Aut}(A)$ given by $a^{\sigma(b_i)} = a^{r_i}$ and a 2-cocycle $\rho : B \times B \rightarrow A$ given by

$$\rho(b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2}) = a^{r_2^{y_2} \mathcal{S}(r_1 \mid x_2) \mathcal{S}(r_2 \mid y_1) + t_1 r_2^{y_1+y_2} \lfloor \frac{x_1+x_2}{N_1} \rfloor + t_2 \lfloor \frac{y_1+y_2}{N_2} \rfloor}$$

for $b_1^{x_i} b_2^{y_i} \in B$ with $0 \leq x_i < N_1$ and $0 \leq y_i < N_2$, for $i = 1, 2$.

Proof. The only non-obvious statement is that ρ satisfies the cocycle condition: namely,

$$(6.5) \quad \rho(b_1^{x_1} b_2^{y_1}, b_1^{x_2+x_3} b_2^{y_2+y_3}) \cdot \rho(b_1^{x_2} b_2^{y_2}, b_1^{x_3} b_2^{y_3}) = \rho(b_1^{x_1+x_2} b_2^{y_1+y_2}, b_1^{x_3} b_2^{y_3}) \cdot \rho(b_1^{x_1} b_2^{y_1}, b_1^{x_2} b_2^{y_2})^{\sigma(b_1^{x_3} b_2^{y_3})}$$

for $b_1^{x_i} b_2^{y_i} \in B$ with $0 \leq x_i < N_1$ and $0 \leq y_i < N_2$ for $i = 1, 2, 3$. To prove (6.5) we first make several observations.

Let n be a non-negative integer. A case-by-case argument shows that if $0 \leq z_i < n$ for $i \in \{1, 2, 3\}$ then

$$(6.6) \quad \left\lfloor \frac{[z_1 + z_2]_n + z_3}{n} \right\rfloor + \left\lfloor \frac{z_1 + z_2}{n} \right\rfloor = \left\lfloor \frac{z_1 + [z_2 + z_3]_n}{n} \right\rfloor + \left\lfloor \frac{z_2 + z_3}{n} \right\rfloor.$$

We also observe that

$$\mathcal{S}(r_i | n) = \sum_{j=0}^{\lfloor \frac{n}{N_i} \rfloor - 1} r_i^{jN_i} \sum_{k=0}^{N_i-1} r_i^k + r_i^{N_i \lfloor \frac{n}{N_i} \rfloor} \sum_{k=0}^{[n]_{N_i}} r_i^k$$

and hence from (6.1)

$$(6.7) \quad \mathcal{S}(r_i | n) \equiv \left\lfloor \frac{n}{N_i} \right\rfloor \mathcal{S}(r_i | N_i) + \mathcal{S}(r_i | [n]_{N_i}) \pmod{M}.$$

Arguing by induction on n , congruences (6.3) and (6.4) generalize to

$$(6.8) \quad t_1 \equiv t_1 r_2^n + \mathcal{S}(r_2 | n) \mathcal{S}(r_1 | N_1) \pmod{M},$$

$$(6.9) \quad t_2 \equiv t_2 r_1^n - \mathcal{S}(r_1 | n) \mathcal{S}(r_2 | N_2) \pmod{M}.$$

Let

$$\begin{aligned} R &= r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_2) + r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | [x_2 + x_3]_{N_1}), \\ R' &= r_1^{x_3} r_2^{y_2+y_3} \mathcal{S}(r_1 | x_2) \mathcal{S}(r_2 | y_1) + r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | [y_1 + y_2]_{N_2}), \\ T_1 &= t_1 r_2^{y_2+y_3} \left(r_2^{y_1} \left\lfloor \frac{x_1 + [x_2 + x_3]_{N_1}}{N_1} \right\rfloor + \left\lfloor \frac{x_2 + x_3}{N_1} \right\rfloor \right), \\ T_1' &= t_1 r_2^{y_1+y_2+y_3} \left(\left\lfloor \frac{[x_1 + x_2]_{N_1} + x_3}{N_1} \right\rfloor + \left\lfloor \frac{x_1 + x_2}{N_1} \right\rfloor \right), \\ T_2 &= t_2 \left(\left\lfloor \frac{y_1 + [y_2 + y_3]_{N_2}}{N_2} \right\rfloor + \left\lfloor \frac{y_2 + y_3}{N_2} \right\rfloor \right), \\ T_2' &= t_2 \left(\left\lfloor \frac{[y_1 + y_2]_{N_2} + y_3}{N_2} \right\rfloor + r_1^{x_3} \left\lfloor \frac{y_1 + y_2}{N_2} \right\rfloor \right). \end{aligned}$$

Then (6.6), (6.8) and (6.7) imply

$$\begin{aligned} T_1' &\equiv t_1 r_2^{y_1+y_2+y_3} \left(\left\lfloor \frac{x_1 + [x_2 + x_3]_{N_1}}{N_1} \right\rfloor + \left\lfloor \frac{x_2 + x_3}{N_1} \right\rfloor \right) \\ &\equiv T_1 + t_1 r_2^{y_2+y_3} (r_2^{y_1} - 1) \left\lfloor \frac{x_2 + x_3}{N_1} \right\rfloor \\ &\equiv T_1 - r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | N_1) \left\lfloor \frac{x_2 + x_3}{N_1} \right\rfloor \\ &\equiv T_1 - r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | x_2 + x_3) + r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | [x_2 + x_3]_{N_1}) \pmod{M}. \end{aligned}$$

Similarly, (6.6), (6.9) and (6.7) imply

$$T_2' \equiv T_2 + r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_1 + y_2) - r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | [y_1 + y_2]_{N_2}) \pmod{M}.$$

Therefore

$$\begin{aligned} T_1' + T_2' + R' - R &\equiv T_1 - r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | x_2 + x_3) + T_2 + r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_1 + y_2) \\ &\quad + r_1^{x_3} r_2^{y_2+y_3} \mathcal{S}(r_1 | x_2) \mathcal{S}(r_2 | y_1) - r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_2) \\ &\equiv T_1 - r_2^{y_2+y_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | x_3) - r_2^{y_2+y_3} r_1^{x_3} \mathcal{S}(r_2 | y_1) \mathcal{S}(r_1 | x_2) \\ &\quad + T_2 + r_2^{y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_2) + r_2^{y_2+y_3} \mathcal{S}(r_1 | x_3) \mathcal{S}(r_2 | y_1) \\ &\quad + r_1^{x_3} r_2^{y_2+y_3} \mathcal{S}(r_1 | x_2) \mathcal{S}(r_2 | y_1) - r_2^{y_2} \mathcal{S}(r_1 | x_2) \mathcal{S}(r_2 | y_3) \\ &\equiv T_1 + T_2 \pmod{M}, \end{aligned}$$

which implies (6.5). \square

We are ready to finish the proof of the Main Theorem. Let $I = (p, m, n_1, n_2, \sigma_1, \sigma_2, o_1, o_2, o_1', o_2', u_1, u_2)$ satisfy conditions (1)-(7) in the Main Theorem. We prove that $I = \text{inv}(G)$ for some finite non-abelian 2-generator cyclic-by-abelian group G of prime-power order. Let r_1, r_2 be as in (1.1) and $t_i = u_i p^{m-o_i'}$ for

$i = 1, 2$. Then, by conditions (2), (4), (6b) and (7), the congruences (6.1)-(6.4) hold for $M = p^m$ and $N_i = p^{n_i}$. Using the notation of Lemma 6.1, consider the group extension

$$1 \rightarrow A \rightarrow G \rightarrow B \rightarrow 1$$

realizing the action σ and the 2-cocycle ρ . That is, G is generated by a, b_1 and b_2 , and these generators satisfy the relations $a^{b_i} = a^{r_i}$, $[b_2, b_1] = a$ and $b_i^{p^{n_i}} = a^{t_i}$, because $\rho(b_2, b_1) = a$, $\rho(b_i, b_i^{k-1}) = 1$ if $k < p^{n_i}$ and $\rho(b_i, b_i^{p^{n_i}-1}) = a^{t_i}$. This implies that G is the group given by the presentation in (1.4). From now on, the notation for \mathcal{B} and its variants refers to this group. Observe that $b = (b_1, b_2) \in \mathcal{B}$, $\sigma(b_i) = \sigma_i$ and $o(b_i) = o_i$ for $i = 1, 2$ by the definition of the r_i 's. Moreover, $o'(b) = (o'_1, o'_2)$ and $u(b) = (u_2, u_1)$, by the definition of the t_i 's. Also, b satisfies the conditions in Lemma 2.2, as the parameters satisfy conditions (6a), (7b) and (5). Then $b \in \mathcal{B}'$ and therefore $\sigma o(G) = (\sigma_1, \sigma_2, o_1, o_2)$. Hence $b \in \mathcal{B}_r$ by the definitions of r_i and t_i . Using Lemma 4.2 if $\sigma_1 = 1$, or Lemmas 4.3 and 4.4 if $\sigma_1 = -1$, it follows that $b \in \mathcal{B}'_r$, since the parameters satisfy conditions (6c), (6d) and (6e) if $\sigma_1 = 1$, and otherwise they satisfy conditions (7b) and (7c). Finally, Lemmas 5.1 and 5.2 yield $b \in \mathcal{B}_{rt}$, since the parameters satisfy conditions (6f), (6g), (7b) and (7c). Therefore $\text{inv}(G) = I$, as desired.

7. IMPLEMENTATION OF OUR CLASSIFICATION

In this section we present some GAP [GAP22] functions dealing with finite non-abelian 2-generator cyclic-by-abelian p -groups. The related code is available at [BCGLdR22].

The function `CbA2GenByOrder(p,n)` constructs the list of all 12-tuples $\text{inv}(G)$ with G a finite non-abelian 2-generator cyclic-by-abelian group of order p^n . For example, there are exactly 273 and 100 isomorphism classes of such groups of order 2^{10} and 3^{10} , respectively.

```
gap> l1:=CbA2GenByOrder(2,10);;l2:=CbA2GenByOrder(3,10);;
gap> Length(l1);Length(l2);
273
100
```

We select the groups G and H with the following invariants:

```
gap> l1[210];l2[92];
[ 2, 5, 3, 2, -1, 1, 0, 1, 1, 4, 1, 7 ]
[ 3, 3, 5, 2, 1, 1, 2, 1, 1, 2, 2, 1 ]
```

By (1.1), (1.3) and (1.4)

$$G = \langle b_1, b_2 \mid a = [b_2, b_1], a^{2^5} = 1, a^{b_1} = a^{-1}, a^{b_2} = a^{1+2^4}, b_1^{2^3} = a^{2^4}, b_2^{2^2} = a^{7 \cdot 2} \rangle$$

and

$$H = \langle b_1, b_2 \mid a = [b_2, b_1], a^{3^3} = 1, a^{b_1} = a^{1+3}, a^{b_2} = a^{1^2}, b_1^{3^5} = a^{2 \cdot 3^2}, b_2^{3^2} = a^{2 \cdot 3} \rangle.$$

`CbA2GenPcp(x)` constructs a power-conjugate presentation [HEO05, Section 9.4.1] for the group G with $x = \text{inv}(G)$.

```
gap> G:=CbA2GenPcp(l1[210]);DG:=DerivedSubgroup(G);;Order(DG);
<pc group of size 1024 with 10 generators>
32
gap> AbelianInvariants(G);NilpotencyClassOfGroup(G);
[ 4, 8 ]
6
gap> H:=CbA2GenPcp(l2[92]);DH:=DerivedSubgroup(H);;Order(DH);
<pc group of size 59049 with 10 generators>
27
gap> AbelianInvariants(H);NilpotencyClassOfGroup(H);
[ 9, 243 ]
4
gap> StructureDescription(G);
"C8 . ((C32 x C2) : C2) = C32 . (C8 x C4)"
```

```
gap> StructureDescription(H);
"C81 . (C27 : C27) = C27 . (C243 x C9)"
```

`InvariantsAndBasis(G)` takes as input a finite non-abelian 2-generator cyclic-by-abelian p -group G and outputs a pair $(\text{inv}(G), [b_1, b_2])$ where $[b_1, b_2]$ is an element of the set \mathcal{B}_{rt} of G , so $G = \langle b_1, b_2 \rangle$ and b_1 and b_2 satisfy the relations of (1.4). The function `Invariants(G)` only outputs $\text{inv}(G)$.

```
gap> ib:=InvariantsAndBasis(G);
[ [ 2, 5, 3, 2, -1, 1, 0, 1, 1, 4, 1, 7 ], [ f1*f3*f5, f4 ] ]
gap> b1:=ib[2][1];; b2:=ib[2][2];; a := Comm(b2,b1);;
gap> Order(a);
32
gap> a^b1=a^-1 and a^b2=a^(1+2^4) and b1^(2^3)=a^(2^4) and b2^(2^2)=a^(7*2);
true
gap> Invariants(H);
[ 3, 3, 5, 2, 1, 1, 2, 1, 1, 2, 2, 1 ]
```

`AreIsomorphicGroups(G,H)` decides whether two finite non-abelian 2-generator cyclic-by-abelian p -groups G and H are isomorphic by comparing $\text{inv}(G)$ and $\text{inv}(H)$. If so then `IsomorphismCbAGroups(G,H)` returns an explicit isomorphism.

```
gap> G:=SmallGroup(2^8,465);
<pc group of size 256 with 8 generators>
gap> inv:=Invariants(G);
[ 2, 4, 2, 2, -1, -1, 0, 1, 0, 0, 1, 1 ]
gap> H:=CbA2GenPcp(inv);
<pc group of size 256 with 8 generators>
gap> AreIsomorphicGroups(G,H);
true
gap> IsomorphismCbAGroups(G,H);
[ f1, f1*f2 ] -> [ f1, f3 ]
gap> K:=SmallGroup(2^8,532);
<pc group of size 256 with 8 generators>
gap> AreIsomorphicGroups(K,H);
false
gap> Invariants(K);
[ 2, 2, 5, 1, -1, 1, 0, 0, 1, 2, 1, 1 ]
```

`DescendantsCbA2Gen(p,n)` computes representatives of the isomorphism classes of finite non-abelian 2-generator cyclic-by-abelian groups of order p^n , using the p -group generation algorithm [O'B90] as implemented for GAP in [GNOH22].

```
gap> x:=DescendantsCbA2Gen(2,10);;
gap> Length(x);
273
```

`CheckNumber(p,n)` and `CheckIsoClasses(p,n)` compare the outputs of `CbA2GenByOrder(p,n)` and `DescendantsCbA2Gen(p,n)`, returning `true` if they agree. More precisely, `CheckNumber(p,n)` returns `true` if the outputs of `CbA2GenByOrder(p,n)` and `DescendantsCbA2Gen(p,n)` have the same cardinality. The output of `CheckIsoClasses(p,n)` is `true` when the list obtained by applying `Invariants` to the list of groups given by `DescendantsCbA2Gen(p,n)` coincides, possibly up to reordering, with the output of `CbA2GenByOrder(n,p)`.

The following calculation demonstrates the correctness of the Main Theorem for a certain range of values. It is a costly calculation, which for large values requires 8Gb of memory. We have verified that the output is `true` up to the following orders: $2^{12}, 3^{11}, 5^{10}, 7^9, 11^8, 13^7$ and 23^8 .

```

gap> CheckIsoClasses(2,12);
true
gap> CheckIsoClasses(3,10);
true

```

APPENDIX A. THE OPERATORS $\mathcal{S}(-|-)$ AND $\mathcal{T}(-,-|-)$

Here we prove some useful properties of the operators $\mathcal{S}(-|-)$ and $\mathcal{T}(-,-|-)$ defined at the beginning of Section 2.

Lemma A.1. *Let x and y be integers and let a, b, c and d be positive integers.*

- (1) $\mathcal{S}(x|a) = \begin{cases} a, & \text{if } x = 1; \\ \frac{x^a - 1}{x - 1}, & \text{otherwise.} \end{cases}$
- (2) $\mathcal{S}(x|1+a) = 1 + x\mathcal{S}(x|a)$.
- (3) $\mathcal{S}(x|ab) = \mathcal{S}(x|a)\mathcal{S}(x^a|b)$.
- (4) $(x-1)\mathcal{T}(x, 1|a) = \mathcal{S}(x|a) - a$.

Proof. The first three properties are obvious. The fourth holds since

$$(x-1)\mathcal{T}(x, 1|a) = (x-1) \sum_{j=1}^{a-1} \sum_{i=0}^{j-1} x^i = \sum_{j=1}^{a-1} (x^j - 1) = \mathcal{S}(x|a) - a. \quad \square$$

Lemma A.2. *Let p be a prime integer and let s and n be integers with $n > 0$ and $s \equiv 1 \pmod{p}$.*

- (1) *If p is odd, or $p = 2$ and $s \equiv 1 \pmod{4}$, then $v_p(s^n - 1) = v_p(s - 1) + v_p(n)$. Therefore $v_p(\mathcal{S}(s|n)) = v_p(n)$ and $o_{p^n}(s) = p^{\max(0, n - v_p(s-1))}$.*
- (2) *If $p = 2$ and $s \equiv -1 \pmod{4}$ then*

$$\begin{aligned} v_2(s^n - 1) &= \begin{cases} 1, & \text{if } 2 \nmid n; \\ v_2(s+1) + v_2(n), & \text{otherwise;} \end{cases} \\ v_2(\mathcal{S}(s|n)) &= \begin{cases} 0, & \text{if } 2 \nmid n; \\ v_2(s+1) + v_2(n) - 1, & \text{otherwise;} \end{cases} \end{aligned}$$

and if $n \geq 2$ then $o_{2^n}(s) = 2^{\max(1, n - v_2(s+1))}$.

- (3) *If $v_p(s-1) = a$ and either n or $n-1$ is a multiple of p^{m-a} then*

$$\mathcal{S}(s|n) \equiv \begin{cases} 0 \pmod{2^m}, & \text{if } p = 2, a = 1 < m, \text{ and } n \equiv 0 \pmod{2^{m-1}}; \\ 1 \pmod{2^m}, & \text{if } p = 2, a = 1 < m, \text{ and } n \equiv 1 \pmod{2^{m-1}}; \\ n + 2^{m-1} \pmod{2^m}, & \text{if } p = 2, 2 \leq a < m \text{ and } n \not\equiv 0, 1 \pmod{2^{m-a+1}}; \\ n \pmod{p^m}, & \text{otherwise.} \end{cases}$$

Proof. (1) is clear if $s = 1$ (with the convention that $\infty + n = \infty$ and $n - \infty = -\infty < 0$) so suppose that $s \neq 1$. Then $\mathcal{S}(s|n) = \frac{s^n - 1}{s - 1}$, and hence $v_p(\mathcal{S}(s|n)) = v_p(s^n - 1) - v_p(s - 1)$. Thus, to prove (1) by induction on $v_p(n)$, it is enough to show that if $p \nmid n$ then $v_p(s^n - 1) = v_p(s - 1)$ and $v_p(s^p - 1) = v_p(s - 1) + 1$. Let $a = v_p(s - 1)$. So $s = 1 + kp^a$ with $p \nmid k$. Then

$$s^n = 1 + knp^a + \sum_{i=2}^n \binom{n}{i} k^i p^{ia} \equiv 1 + knp^a \pmod{p^{a+1}}.$$

Thus, if $p \nmid n$ then $v_p(s^n - 1) = a$. Moreover $s^p = 1 + kp^{a+1} + \sum_{i=2}^p \binom{p}{i} k^i p^{ia}$. If $2 \leq i < p$ then $v_p(\binom{p}{i} p^{ia}) = 1 + ap \geq a + 2$. In particular, if $p \neq 2$ then $v_p(s^p - 1) = a + 1$. If $p = 2$ then $s \equiv 1 \pmod{4}$, by hypothesis. Therefore $a \geq 2$ and hence $2a > a + 1$ and $s^2 = 1 + k2^{a+1} + k^2 2^{2a} \equiv 1 + k2^{a+1} \pmod{2^{a+2}}$. So, in both cases $v_p(s^p - 1) = a + 1$, as desired.

The hypothesis $s \equiv 1 \pmod{p}$ implies that $o_{p^n}(s) = p^m$ for

$$\begin{aligned} m &= \min\{i \geq 0 : s^{p^i} \equiv 1 \pmod{p^n}\} = \min\{i \geq 0 : v_p(s^{p^i} - 1) \geq n\} \\ &= \min\{i \geq 0 : i + v_p(s - 1) \geq n\} = \max(0, n - v_p(s - 1)). \end{aligned}$$

(2) The argument above shows that in general $v_p(s^n - 1) = v_p(s - 1)$ if $p \nmid n$. In particular if $2 \nmid n$ then $v_2(s^n - 1) = v_2(s - 1) = 1$, and consequently $v_2(\mathcal{S}(s \mid n)) = v_2(s^n - 1) - v_2(s - 1) = 0$, because by assumption $s \equiv -1 \pmod{4}$. Since $s^2 \equiv 1 \pmod{4}$, if $2 \mid n$ then (1) yields

$$v_2(s^n - 1) = v_2((s^2)^{\frac{n}{2}} - 1) = v_2(s^2 + 1) + v_2\left(\frac{n}{2}\right) = v_2(s + 1) + v_2(s - 1) + v_2(n) - 1 = v_2(s + 1) + v_2(n).$$

The assertions about $v_2(\mathcal{S}(s \mid n))$ and $o_{2^n}(s)$ follow as in the proof of (1).

(3) The statement is clear if $a \geq m$ so we assume that $a < m$.

Suppose first that either p is odd or $a \geq 2$. In that case, by (1), $o_{p^m}(s) = p^{m-a}$ and thus the multiplicative group $\langle s \rangle$ generated by s in $\mathbb{Z}/p^m\mathbb{Z}$ is formed by the classes represented by the integers of the form $1 + ip^a$ with $0 \leq i < p^{m-a}$. Thus

$$\begin{aligned} \mathcal{S}(s \mid p^{m-a}) &\equiv \sum_{i=0}^{p^{m-a}-1} (1 + ip^a) = p^{m-a} + p^a \sum_{i=0}^{p^{m-a}-1} i \\ &\equiv p^{m-a} + p^a \frac{(p^{m-a} - 1)p^{m-a}}{2} \\ &\equiv p^{m-a} + \frac{(p^{m-a} - 1)p^m}{2} \\ &\equiv \begin{cases} p^{m-a} \pmod{p^m}, & \text{if } p \neq 2; \\ 2^{m-a} + 2^{m-1} \pmod{2^m}, & \text{otherwise.} \end{cases} \end{aligned}$$

Recall that $s^i \equiv s^j \pmod{p^m}$ if $i \equiv j \pmod{p^{m-a}}$. Thus $\mathcal{S}(s \mid bp^{m-a}) \equiv b\mathcal{S}(s \mid p^{m-a}) \pmod{p^m}$ for each integer b . Therefore, if p^{m-a} divides n then

$$\mathcal{S}(s \mid n) \equiv \frac{n}{p^{m-a}} \mathcal{S}(s \mid p^{m-a}) \equiv \begin{cases} n \pmod{p^m}, & \text{if } p \neq 2; \\ n + \frac{n}{2^{m-a}} 2^{m-1} \pmod{2^m}, & \text{if } p = 2; \end{cases}$$

equivalently

$$\mathcal{S}(s \mid n) \equiv \begin{cases} n + 2^{m-1} \pmod{2^m}, & \text{if } p = 2 \text{ and } n \not\equiv 0 \pmod{2^{m-a+1}}; \\ n \pmod{p^m}, & \text{otherwise.} \end{cases}$$

If $n \equiv 1 \pmod{p^{m-a}}$ then $s^{n-1} \equiv 1 \pmod{p^m}$, and the previous statement for $n - 1$ yields

$$\mathcal{S}(s \mid n) = \mathcal{S}(s \mid n - 1) + s^{n-1} \equiv \begin{cases} n + 2^{m-1} \pmod{2^m}, & \text{if } p = 2 \text{ and } n \not\equiv 1 \pmod{2^{m-a+1}}; \\ n \pmod{p^m}, & \text{otherwise.} \end{cases}$$

Now consider the case $p = 2$ and $a = 1$. If $m \geq 2$ then $\mathcal{S}(s \mid 2^{m-1}) = (1 + s)\mathcal{S}(s^2 \mid 2^{m-2})$. Let $b = v_2(s + 1)$. As $a = 1$, $b \geq 2$ and $v_2(s^2 - 1) = b + 1 \geq 3$. Applying the results above for s^2 and 2^{m-2} in the roles of s and n respectively, we deduce that $\mathcal{S}(s^2 \mid 2^{m-2}) \equiv 2^{m-2} \pmod{2^m}$. In particular, 2^{m-2} divides $\mathcal{S}(s^2 \mid 2^{m-2})$. As $4 \mid (s + 1)$ we deduce that $\mathcal{S}(s \mid 2^{m-1}) \equiv 0 \pmod{2^m}$. Arguing as above, we deduce that if 2^{m-1} divides n then $\mathcal{S}(s \mid n) \equiv 0 \pmod{2^m}$. Applying this to $n - 1$ we deduce that if $n \equiv 1 \pmod{2^{m-1}}$ then $s^{n-1} \equiv 1 \pmod{2^m}$ and $\mathcal{S}(s \mid n - 1) \equiv 0 \pmod{2^m}$. Hence

$$\mathcal{S}(s \mid n) = \mathcal{S}(s \mid n - 1) + s^{n-1} \equiv 1 \pmod{2^m}.$$

□

In the proof of the following two lemmas we will use the following equality:

$$\begin{aligned}
 \mathcal{T}(s, t \mid p^{n+1}) &= \sum_{0 \leq i < j < p^{n+1}} s^i t^j = \sum_{k=0}^{p-1} \sum_{\substack{k p^n \leq i < (k+1)p^n, \\ i < j < p^{n+1}}} s^i t^j \\
 (A.1) \quad &= \sum_{k=0}^{p-1} \left(\sum_{k p^n \leq i < j < (k+1)p^n} s^i t^j + \sum_{\substack{k p^n \leq i < (k+1)p^n, \\ (k+1)p^n \leq j < p^{n+1}}} s^i t^j \right) \\
 &= \sum_{k=0}^{p-1} \left(s^{k p^n} t^{k p^n} \sum_{0 \leq i < j < p^n} s^i t^j + s^{k p^n} t^{(k+1)p^n} \sum_{0 \leq i < p^n, 0 \leq j < p^n(p-k-1)} s^i t^j \right) \\
 &= \mathcal{S}(s^{p^n} t^{p^n} \mid p) \mathcal{T}(s, t \mid p^n) + t^{p^n} \mathcal{S}(s \mid p^n) \sum_{k=0}^{p-1} s^{k p^n} t^{k p^n} \mathcal{S}(t \mid p^n(p-k-1)).
 \end{aligned}$$

Lemma A.3. *Suppose that $s \equiv t \equiv 1 \pmod p$ and n is a positive integer. Then*

$$\mathcal{T}(s, t \mid p^n) \equiv \begin{cases} 0 \pmod{p^n}, & \text{if } p \neq 2; \\ 2^{n-1} \pmod{2^n}, & \text{if } p = 2. \end{cases}$$

Proof. We argue by induction on n with the case $n = 1$ being obvious. Suppose that the statement holds for n . Observe that $s^{p^n} \equiv t^{p^n} \equiv 1 \pmod{p^{n+1}}$. Moreover, by Lemma A.2 (3), $\mathcal{S}(s \mid p^n) \equiv \mathcal{S}(t \mid p^n) \equiv 0 \pmod{p^n}$. Hence, by (A.1), $\mathcal{T}(s, t \mid p^{n+1}) \equiv p \mathcal{T}(s, t \mid p^n) \pmod{p^{n+1}}$. By the induction hypothesis, if $p \neq 2$ then $\mathcal{T}(s, t \mid p^n)$ is a multiple of p^n and hence $\mathcal{T}(s, t \mid p^{n+1}) \equiv 0 \pmod{p^{n+1}}$. If $p = 2$ then $\mathcal{T}(s, t \mid 2^n) = 2^{n-1} + a 2^n$ for some integer a and hence $\mathcal{T}(s, t \mid 2^{n+1}) \equiv 2^n \pmod{2^{n+1}}$. \square

Lemma A.4. *Let m be a positive integer, and let s_1, s_2 be integers such that $s_1 \equiv -1 \pmod 4$ and $s_2 \equiv 1 \pmod 2$. Denote $o_1 = \max(0, m - v_2(s_1 + 1))$ and $o_2 = \max(0, m - v_2(s_2 - 1))$. If n is a positive integer such that $\max(o_1, o_2) \leq n - 1$ then $\mathcal{T}(s_1, s_2 \mid 2^n) \equiv 2^{n-1} \pmod{2^m}$.*

Proof. We proceed by double induction, first on m and then on n . As $s_1 \equiv s_2 \equiv 1 \pmod 2$,

$$\mathcal{T}(s_1, s_2 \mid 2^n) \equiv \mathcal{T}(1, 1 \mid 2^n) \equiv 2^{n-1} \pmod 2$$

for every n . Now assume that both $m \geq 2$ and the induction hypothesis holds for $m - 1$ and proceed by induction on n . If $n = 1$ then $o_1 = o_2 = 0$, so $s_1 \equiv -1 \pmod{2^m}$ and $s_2 \equiv 1 \pmod{2^m}$, and hence $\mathcal{T}(s_1, s_2 \mid 2) \equiv \mathcal{T}(-1, 1 \mid 2) = 1 \pmod{2^m}$. Assume that both $n \geq 2$ and the induction hypothesis holds for $n - 1$. Observe that the hypothesis $\max(o_1, o_2) \leq n - 1$, combined with Lemma A.2, implies that $s_1^{2^{n-1}} \equiv s_2^{2^{n-1}} \equiv 1 \pmod{2^m}$. This and (A.1) yield

$$\mathcal{T}(s_1, s_2 \mid 2^n) \equiv 2 \mathcal{T}(s_1, s_2 \mid 2^{n-1}) + \mathcal{S}(s_1 \mid 2^{n-1}) \mathcal{S}(s_2 \mid 2^{n-1}) \pmod{2^m}.$$

By Lemma A.2,

$$v_2(\mathcal{S}(s_1 \mid 2^{n-1}) \mathcal{S}(s_2 \mid 2^{n-1})) \geq v_2(\mathcal{S}(s_1 \mid 2^{n-1})) + 1 = n - 1 + v_2(s_1 + 1) \geq n - 1 + m - o_1,$$

which is at least m by hypothesis. Hence $\mathcal{T}(s_1, s_2 \mid 2^n) \equiv 2 \mathcal{T}(s_1, s_2 \mid 2^{n-1}) \pmod{2^m}$. If $\max(o_1, o_2) < n - 1$ then we can apply the induction hypothesis (on n) to deduce that $\mathcal{T}(s_1, s_2 \mid 2^{n-1}) \equiv 2^{n-2} \pmod{2^m}$, and the result follows. Thus we can assume $\max(o_1, o_2) = n - 1$. Write $\tilde{m} = m - 1$,

$$\tilde{o}_1 = \max(0, \tilde{m} - v_2(s_1 + 1)) = \max(0, o_1 - 1)$$

and

$$\tilde{o}_2 = \max(0, \tilde{m} - v_2(s_2 - 1)) = \max(0, o_2 - 1).$$

As $\max(o_1, o_2) = n - 1 \geq 1$, $\max(\tilde{o}_1, \tilde{o}_2) = n - 2$, so by the induction hypothesis (on m) $\mathcal{T}(s_1, s_2 \mid 2^{n-1}) \equiv 2^{n-2} \pmod{2^{m-1}}$. Hence $\mathcal{T}(s_1, s_2 \mid 2^n) \equiv 2 \mathcal{T}(s_1, s_2 \mid 2^{n-1}) \equiv 2^{n-1} \pmod{2^m}$. \square

Acknowledgments. The authors are grateful to the referee for many helpful comments which helped to improve the paper.

REFERENCES

- [AMM12] A. Ahmad, A. Magidin, and R. F. Morse, *Two generator p -groups of nilpotency class 2 and their conjugacy classes*, Publ. Math. Debrecen **81** (2012), no. 1-2, 145–166.
- [BCGLdR22] O. Broche-Cristo, D. García-Lucas, and Á. del Río, *CbA2Gen. A classification of 2-generated cyclic-by-abelian finite p -groups*, <https://github.com/angeldelriomateos/CbA2Gen>, 2022.
- [Bla99] S. R. Blackburn, *Groups of prime power order with derived subgroup of prime order*, J. Algebra **219** (1999), 625–657.
- [Cay78] A. Cayley, *Desiderata and suggestions. No. 1.—The theory of groups*, Amer. J. Math. **1** (1878), no. 1, 50–52.
- [EO99] B. Eick and E. A. O’Brien, *Enumerating p -groups*, J. Austral. Math. Soc. **67** (1999), 191–205.
- [GAP22] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.
- [GBR] À. García-Blázquez and Á. del Río, *A classification of metacyclic groups by group invariants*, Preprint: <http://arxiv.org/abs/2301.08683>.
- [GLdRS22] D. García-Lucas, Á. del Río, and M. Stanojkowski, *On group invariants determined by modular group algebras: even versus odd characteristic*, Algebr. Represent. Theory. <https://doi.org/10.1007/s10468-022-10182-x> (2022).
- [GLMR22] D. García-Lucas, L. Margolis, and Á. del Río, *Non-isomorphic 2-groups with isomorphic modular group algebras*, J. Reine Angew. Math. **154** (2022), no. 783, 269–274.
- [GNOH22] G. Gamble, W. Nickel, E. O’Brien, and M. Horn, *ANUPQ, ANU p -Quotient, Version 3.2.6*, 2022.
- [Hal40] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141.
- [Hem00] C. E. Hempel, *Metacyclic groups*, Comm. Algebra **28** (2000), no. 8, 3865–3897.
- [HEO05] D. F. Holt, B. Eick, and E. A. O’Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005.
- [Mie75] R. J. Miech, *On p -groups with a cyclic commutator subgroup*, J. Austral. Math. Soc. **20** (1975), no. 2, 178–198.
- [O’B90] E. A. O’Brien, *The p -group generation algorithm*, J. Symbolic Comput. **9** (1990), no. 5-6, 677–698.
- [OVL05] E. A. O’Brien and M. R. Vaughan-Lee, *The groups of order p^7 for odd prime p* , J. Algebra **292** (2005).
- [Rob82] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics, vol. 80, Springer-Verlag, New York, 1982.
- [Son13] Q. Song, *Finite two-generator p -subgroups with cyclic derived group*, Comm. Algebra **41** (2013), no. 4, 1499–1513.

O. BROCHE: DEPARTAMENTO DE MATEMÁTICA E MATEMÁTICA APLICADA, UNIVERSIDADE FEDERAL DE LAVRAS, CAIXA POSTAL 3037, 37200-000, LAVRAS, BRAZIL. osnel@ufla.br

D. GARCÍA-LUCAS, Á. DEL RÍO: DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE MURCIA, 30100, MURCIA, SPAIN. diego.garcial@um.es, adelrio@um.es