ARTICLE IN PRESS

Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Research Paper

Geometric invariants for p-groups of class 2 and exponent p [☆]

E.A. O'Brien [a], Mima Stanojkovski [b,*]

[a] Department of Mathematics, University of Auckland, Private Bag 92019, Auckland, New Zealand
[b] Dipartimento di Matematica, Università di Trento, Italy

ARTICLE INFO

Article history:
Received 28 November 2024
Available online xxxx
Communicated by Colva Roney-Dougal

Dedicated to the memory of our friend Richard Parker

MSC:
20D15
14M12
15A69

Keywords:
Isomorphism testing of finite p-groups
Invariants
Rank loci

ABSTRACT

We introduce geometric invariants for p-groups of class 2 and exponent p. We report on their effectiveness in distinguishing among 5-generator p-groups of this type.

☆ O'Brien was supported by the Marsden Fund of New Zealand Grant 23-UOA-080 and by a Research Award of the Alexander von Humboldt Foundation. Stanojkovski is a member of the Indam group GNSAGA and is funded by the Italian Ministry of Education (the program Rita Levi Montalcini, edition 2020, country Italy). We thank Bettina Eick, Fulvio Gesumundo, Josh Maglione, M.F. Newman, and Christopher Voll for helpful discussions. We thank the referee for helpful guidance on the content and exposition.

* Corresponding author.
E-mail addresses: e.obrien@auckland.ac.nz (E.A. O'Brien), mima.stanojkovski@unitn.it (M. Stanojkovski).

https://doi.org/10.1016/j.jalgebra.2025.08.029
0021-8693/

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

1. Introduction

The problem of deciding whether two presentations present the same group was formulated by Dehn [11]. Adian [1] and Rabin [25] showed that the isomorphism problem for finitely presented groups is undecidable.

A typically easier task is to establish that two groups are non-isomorphic by exhibiting distinguishing invariants. This approach is particularly useful in providing independent evidence that an existing list of groups – perhaps obtained theoretically – is irredundant. But families of finite p-groups, where the prime p is a parameter in the group descriptions, pose particular challenges. It is difficult to find "natural" invariants which distinguish among very similar groups – and it may be impossible to compute their values for moderate values of the prime. For example, power maps are sometimes used to distinguish among the 267 groups of order 2^6.

To set a context for our work, we review the algorithm of O'Brien [21] in a special case: decide isomorphism between two n-generator groups, G and H, of order p^{n+d}, nilpotency class 2 and exponent p. The Frattini quotient of G coincides with that of H, and the automorphism group of this quotient is $\mathrm{GL}(V)$ where $V = \mathbb{F}_p^n$. We write down the action of $\mathrm{GL}(V)$ on the exterior square $\Lambda^2(V)$, a space of dimension $n(n-1)/2$. To each of G and H we associate a d-dimensional subspace of $\Lambda^2(V)$. Now $G \cong H$ if and only if the duals of these two subspaces are in the same $\mathrm{GL}(V)$-orbit. The length of this orbit may prevent its construction. In summary, a complete solution to the isomorphism problem for this family of groups depends on knowledge of the $\mathrm{GL}(V)$-orbits of d-dimensional spaces of $\Lambda^2(V)$. Sun [28] recently announced a new algorithm with running time $m^{O((\log m)^{5/6})}$ to decide isomorphism between two such groups of order m.

Standard group-theoretic invariants for p-groups of class 2 and exponent p often coincide. We introduce invariants from algebraic geometry which apply specifically to these groups. The invariants are extracted from the skew-symmetric matrices of linear forms that these groups determine. We demonstrate that the invariants are discriminating – they sometimes partition a family up to isomorphism – and they can be computed for a range of primes. Our invariants are computed in affine varieties, rather than in the p-group as for many existing invariants, and successful computations seem less dependent on the size of the prime. We plan to investigate the effectiveness of these novel invariants for other related questions.

The structure of the paper is the following. In Section 2.1 we summarise the standard Baer correspondence between p-groups of class 2 and exponent p and skew-symmetric matrices of linear forms over $\mathbb{F}_p$. A consequence is that the rank loci of a skew-symmetric matrix of linear forms over $\mathbb{F}_p$ are determined by the isomorphism class of the corresponding group. Theorem 2.3 lists group invariants attached to the rank ideals. In Section 3 we illustrate how these distinguish up to isomorphism the 4-generator groups of order p^7, class 2, and exponent p. In Section 4, building on work of Brahana [4,5], Copetti [9], and Vaughan-Lee [29], we explore the corresponding 5-generator groups of order dividing p^9. We distinguish these with one exception: two groups of order p^8. In Theorem 4.2 we

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

show that the examples of [17] motivated by Higman's PORC conjecture have minimal order. An explicit discussion of the well-known connection with tensors appears in [23].

2. Geometric invariants associated to groups

Let $K[x_1, \ldots, x_d]$ be the polynomial ring over a field K in the indeterminates $x_1, \ldots, x_d$. We write $\boldsymbol{x} = (x_1, \ldots, x_d)$ and $K[\boldsymbol{x}] = K[x_1, \ldots, x_d]$. Let $K[\boldsymbol{x}]_1$ be the subspace of linear forms of $K[\boldsymbol{x}]$ and let $\mathrm{Mat}_{n\times m}(K[\boldsymbol{x}]_1)$ be the space of $m \times n$ matrices of linear forms in $K[\boldsymbol{x}]$, writing $\mathrm{Mat}_n(K[\boldsymbol{x}]_1)$ if $n = m$. If $X \subset K^d$, then $\langle X\rangle_K$ is the K-span of X. Let $\mathcal{V}_{\mathrm{aff}}(I)$ be the affine variety of a homogeneous ideal I of $K[\boldsymbol{x}]$ in K^d and let $\mathcal{V}_{\mathrm{proj}}(I)$ be the corresponding projective variety in $\mathbb{P}^{d-1}(K)$. See [10, Chap. 1] for standard concepts in algebraic geometry.

2.1. Groups from matrices and back

We briefly review the well-known Baer correspondence [2], a consequence of MacLane's Universal Coefficients Theorem [26, §11.4]. Since we consider only p-groups of class 2 and exponent p, we restrict to odd primes p.

Let n and d be positive integers and let $\mathbb{F}_p$ be the field of p elements. Let $\boldsymbol{y} = (y_1, \ldots, y_d)$ be a vector of independent algebraic variables. Let $\mathrm{B}(\boldsymbol{y}) \in \mathrm{Mat}_n(K[\boldsymbol{y}]_1)$ be a skew-symmetric matrix of linear forms. Write $V = K^n$ and $W = K^d$ and let W have standard basis $(f_1, \ldots, f_d)$. Now B defines the alternating map

$$t : V \times V \longrightarrow W, \quad (v, v') \longmapsto t(v, v') = \sum_{i=1}^{d} v^\top \mathrm{B}(f_i)v' f_i. \tag{2.1}$$

Defining an operation $\star$ on $V \times W$ by

$$(v, w) \star (v', w') = \left(v + v', w + w' + \frac{1}{2}t(v, v')\right)$$

yields a group $\mathrm{G}_\mathrm{B}(K)$. Clearly, a change of basis for V or W does not change the isomorphism class of $\mathrm{G}_\mathrm{B}(K)$. Write

$$\mathrm{B}(\boldsymbol{y}) = \left(\mathrm{B}_{ij}^{(1)}\, y_1 + \ldots + \mathrm{B}_{ij}^{(d)}\, y_d\right)_{ij} \quad \text{with} \quad \mathrm{B}_{ij}^{(\kappa)} \in \mathrm{Mat}_n(K).$$

The *adjoint* of $\mathrm{B}(\boldsymbol{y})$ is

$$\mathrm{B}^\bullet(\boldsymbol{x}) = \left(\sum_{j=1}^{n} \mathrm{B}_{ij}^{(\kappa)}\, x_j\right)_{i\kappa} \in \mathrm{Mat}_{n\times d}(K[x_1, \ldots, x_n]_1). \tag{2.2}$$

In the following, $I_1(\mathrm{B}) \subseteq K[\boldsymbol{y}]$ denotes the ideal generated by the entries of B; define analogously $I_1(\mathrm{B}^\bullet) \subseteq K[\boldsymbol{x}]$. See also Section 2.2.

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Lemma 2.1. *Assume that $K = \mathbb{F}_p$ and write $G = \mathrm{G}_{\mathrm{B}}(\mathbb{F}_p)$.*

(1) *The order of G is p^{n+d}.*
(2) *The class of G is at most 2, where equality holds if and only if* B *is not the zero matrix.*
(3) *The exponent of G is p.*
(4) *The derived group G' of G is an $\mathbb{F}_p$-subspace of $\{0\} \times W$ and has dimension*

$$\dim_{\mathbb{F}_p} G' = d - \dim(\mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B}))).$$

(5) *The centre $\mathrm{Z}(G)$ of G is an $\mathbb{F}_p$-subspace of $V \times W$ containing $\{0\} \times W$ and has dimension*

$$\dim_{\mathbb{F}_p} \mathrm{Z}(G) = d + \dim(\mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B}^\bullet))).$$

Now let G be a p-group of class 2 and exponent p. Assume that $|G'| = p^d$ and $|G| = p^{n+d}$. Clearly $V = G/G'$ and $W = G'$ are $\mathbb{F}_p$-vector spaces of dimension n and d, respectively. Moreover, the commutator map induces an alternating map $t : V \times V \longrightarrow W$. By choosing bases of V and W respectively, we represent t by $\mathrm{B}(\boldsymbol{y}) \in \mathrm{Mat}_n(\mathbb{F}_p[y_1, \ldots, y_d]_1)$, a skew-symmetric matrix of linear forms. The matrix $\mathrm{B}^\bullet$ determines the adjoint operator on V and its rank loci partition the elements of $G \setminus G'$ by centraliser sizes [27, Lem. 4.4]. If also $G' = \mathrm{Z}(G)$, then B and $\mathrm{B}^\bullet$ are respectively the matrices B and A defined in [24, Def. 2.1].

Procedures to construct the Baer-MacLane functor and related tensor invariants are part of the Magma [3] MultilinearAlgebra package of Maglione and Wilson [14,19].

2.2. Varieties and invariants

Let m, n and d be positive integers and write $N = \min\{m, n\}$. Let $\boldsymbol{z} = (z_1, \ldots, z_d)$ be a vector of independent algebraic variables. Let $\mathrm{D}(\boldsymbol{z}) \in \mathrm{Mat}_{m \times n}(K[\boldsymbol{z}]_1)$ be a matrix of linear forms.

- For $k \in \{1, \ldots, N\}$, the *k-th* (*determinantal*) *ideal* of D is the homogeneous ideal $I_k(\mathrm{D})$ of $K[\boldsymbol{z}]$ generated by the $k \times k$ minors of $\mathrm{D}(\boldsymbol{z})$, while the *k-th* (*determinantal*) *variety* of D is $V_k = \mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{D}))$.
- The *ideal rank vector* of D is $\mathrm{irk}(\mathrm{D}) = (\, I_k(\mathrm{D}) : k = 1, \ldots, N\,)$.

Each V_i is an affine variety in K^d and $\{0\} \subseteq V_1 \subseteq V_2 \subseteq \ldots \subseteq V_N \subseteq K^d$. See [8] for a discussion of determinantal ideals and associated varieties.

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Remark 2.2. Let I be a homogeneous ideal in $K[x_1,\dots,x_d]$ and let m be the dimension of $\mathcal{V}_{\mathrm{proj}}(I)$. Following [16, Defs. 12.11 and 12.14], the *degree* of I is the product of $m!$ by the leading coefficient of the Hilbert polynomial of I. If $\mathcal{V}_{\mathrm{proj}}(I)$ is empty, then the degree of I is 0. The Hilbert polynomial is invariant under change of coordinates [16, Rmk. 12.2], thus so is the degree of I. Now I is *primary* if, whenever $ab \in I$ for $a, b \in R$, then $a \in I$, or there exists a positive integer i such that $b^i \in I$. Also I has a *minimal primary decomposition* in the sense of [15, Def. 8.20]. Two minimal decompositions have the same cardinality, and the irreducible components $\mathcal{V}_{\mathrm{proj}}(I_1),\dots,\mathcal{V}_{\mathrm{proj}}(I_r)$ do not depend on the chosen decomposition [15, Prop. 8.27]. For a more detailed treatment, see [13, Chap. 3], [15, §8], and [16, §12].

Theorem 2.3. *Let n and d be positive integers, and let $\boldsymbol{y} = (y_1,\dots,y_d)$ and $\boldsymbol{x} = (x_1,\dots,x_n)$ be vectors of independent algebraic variables. Let $\mathrm{B}(\boldsymbol{y}) \in \mathrm{Mat}_n(\mathbb{F}_p[\boldsymbol{y}]_1)$ be a skew-symmetric matrix of linear forms and let $\mathrm{B}^\bullet(\boldsymbol{x}) \in \mathrm{Mat}_{n\times d}(\mathbb{F}_p[\boldsymbol{x}]_1)$ be its adjoint. Write*

- $\mathrm{irk}(\mathrm{B}) = (I_1,\dots,I_n)$ *for the ideal rank vector of* B, *and*
- $\mathrm{irk}(\mathrm{B}^\bullet) = (J_1,\dots,J_{\min\{n,d\}})$ *for the ideal rank vector of* $\mathrm{B}^\bullet$.

For each $k \in \{1,\dots,n\}$ and $\ell \in \{1,\dots,\min\{n,d\}\}$, the following are invariants of the isomorphism class of $\mathrm{G}_{\mathrm{B}}(\mathbb{F}_p)$:

(1) *the degrees and dimensions of I_k and J_ℓ;*
(2) *the degrees and dimensions of the ideals in a primary decomposition of I_k and J_ℓ;*
(3) *the degrees, the number of rational points, and the number of irreducible components of $\mathcal{V}_{\mathrm{aff}}(I_k)$ and $\mathcal{V}_{\mathrm{aff}}(J_\ell)$;*
(4) *the dimensions of $\langle \mathcal{V}_{\mathrm{aff}}(I_k)\rangle_{\mathbb{F}_p}$ and $\langle \mathcal{V}_{\mathrm{aff}}(J_\ell)\rangle_{\mathbb{F}_p}$.*

Proof. Let $\mathrm{C} \in \mathrm{Mat}_n(\mathbb{F}_p[\boldsymbol{y}]_1)$ be such that $\mathrm{G}_{\mathrm{B}}(\mathbb{F}_p)$ and $\mathrm{G}_{\mathrm{C}}(\mathbb{F}_p)$ are isomorphic, and let X and Z be such that $X\,\mathrm{B}(\boldsymbol{y}Z)X^\top = \mathrm{C}(\boldsymbol{y})$. The existence of X and Z is guaranteed by the Baer-MacLane construction (see [18, Thm. 2.13(2)] for a similar formulation).

Fix $k \in \{1,\dots,n\}$. If $v \in K^d$, then $\mathrm{rk}(\mathrm{B}(v)) = \mathrm{rk}(X\,\mathrm{B}(Zv)X^\top) = \mathrm{rk}(\mathrm{C}(v))$. Hence Z induces a linear isomorphism of varieties $\varphi_Z : \mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{B})) \to \mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{C}))$. Being invariants under isomorphism of varieties, the quantities from (3) are preserved. Since φ_Z is linear, $\dim_{\mathbb{F}_p}\langle \mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{B}))\rangle_{\mathbb{F}_p} = \dim_{\mathbb{F}_p}\langle \mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{C}))\rangle_{\mathbb{F}_p}$, thus (4) holds. Since φ_Z is an isomorphism, the dimensions of the ideals $I_k(\mathrm{B})$ and $I_k(\mathrm{C})$ equal those of the corresponding varieties $\mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{B}))$ and $\mathcal{V}_{\mathrm{aff}}(I_k(\mathrm{C}))$. Moreover, the degrees of $I_k(\mathrm{B})$ and $I_k(\mathrm{C})$ coincide by Remark 2.2 and the linearity of Z. Thus (1) holds. Similarly, we deduce (2). The proof for adjoints is analogous. □

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

3. An illustrative example

Vaughan-Lee [29, §7.4] lists the six isomorphism classes of 4-generator groups of order p^7, class 2, and exponent p. Following Section 2.1, representatives of these isomorphism classes can be constructed over $\mathbb{F}_p$ (with primitive element ω) from the following matrices.

$$\mathrm{B}_1(x,y,z) = \begin{pmatrix} 0 & x & y & z \\ -x & 0 & 0 & 0 \\ -y & 0 & 0 & 0 \\ -z & 0 & 0 & 0 \end{pmatrix}, \qquad \mathrm{B}_2(x,y,z) = \begin{pmatrix} 0 & x & y & 0 \\ -x & 0 & z & 0 \\ -y & -z & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\mathrm{B}_3(x,y,z) = \begin{pmatrix} 0 & x & y & 0 \\ -x & 0 & 0 & z \\ -y & 0 & 0 & 0 \\ 0 & -z & 0 & 0 \end{pmatrix}, \qquad \mathrm{B}_4(x,y,z) = \begin{pmatrix} 0 & x & y & z \\ -x & 0 & z & 0 \\ -y & -z & 0 & 0 \\ -z & 0 & 0 & 0 \end{pmatrix},$$

$$\mathrm{B}_5(x,y,z) = \begin{pmatrix} 0 & x & 0 & y \\ -x & 0 & y & 0 \\ 0 & -y & 0 & z \\ -y & 0 & -z & 0 \end{pmatrix}, \quad \mathrm{B}_6(x,y,z) = \begin{pmatrix} 0 & x & y & z \\ -x & 0 & 0 & \omega y \\ -y & 0 & 0 & x \\ -z & -\omega y & -x & 0 \end{pmatrix}.$$

Since $\dim \mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B})) = 0$ for $\mathrm{B} \in \{\mathrm{B}_1, \ldots, \mathrm{B}_6\}$, Lemma 2.1 confirms that these define groups of the claimed type. The adjoint matrices of $\mathrm{B}_1, \ldots, \mathrm{B}_6$ are:

$$\mathrm{B}_1^{\bullet}(x,y,z,w) = \begin{pmatrix} y & z & w \\ -x & 0 & 0 \\ 0 & -x & 0 \\ 0 & 0 & -x \end{pmatrix}, \quad \mathrm{B}_2^{\bullet}(x,y,z,w) = \begin{pmatrix} y & z & 0 \\ -x & 0 & z \\ -0 & -x & -y \\ 0 & 0 & 0 \end{pmatrix},$$

$$\mathrm{B}_3^{\bullet}(x,y,z,w) = \begin{pmatrix} y & z & 0 \\ -x & 0 & w \\ 0 & -x & 0 \\ 0 & 0 & -y \end{pmatrix}, \quad \mathrm{B}_4^{\bullet}(x,y,z,w) = \begin{pmatrix} y & z & w \\ -x & 0 & z \\ 0 & -x & -y \\ 0 & 0 & -x \end{pmatrix},$$

$$\mathrm{B}_5^{\bullet}(x,y,z,w) = \begin{pmatrix} y & w & 0 \\ -x & z & 0 \\ 0 & -y & w \\ 0 & -x & -z \end{pmatrix}, \quad \mathrm{B}_6^{\bullet}(x,y,z,w) = \begin{pmatrix} y & z & w \\ -x & \omega w & 0 \\ w & -x & 0 \\ -z & -\omega y & -x \end{pmatrix}.$$

Let $n_p(I)$ denote the number of $\mathbb{F}_p$-rational points of $\mathcal{V}_{\mathrm{aff}}(I)$. The invariants summarised in Table 1 separate the groups up to isomorphism.

4. The 5-generator p-groups of class 2 and exponent p

Brahana [4,5] used concepts from projective geometry to study some of the 5-generator groups of class 2 and exponent p: in particular, commutators in such a group arise as solutions of a system of homogeneous quadratic equations called Plücker relations; cf. [9, §4.2]. As in other treatments, his construction of the groups up to isomorphism reduces to an orbit problem. Copetti [9] presents a modern and highly accessible treatment of his

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Table 1
Invariants of $B_1, \ldots, B_6$.

B	B_1	B_2	B_3	B_4	B_5	B_6
$n_p(I_4(B))$	p^3	p^3	$2p^2 - p$	p^2	p^2	p
$n_p(I_3(B^\bullet))$	p^3	p^4	$2p^3 - p^2$	p^3	$p^3 + p^2 - p$	p^2

work. Vaughan-Lee [29] used an approach similar to the p-group generation algorithm [20] to determine the groups of order dividing p^8 having class 2 and exponent p.

A 5-generator p-group of class 2 and exponent p has order p^{5+d} where $1 \leqslant d \leqslant 10$. Recall from the introduction that we consider the action of $\mathrm{GL}(V)$, where $V = \mathbb{F}_p^5$, on the exterior square $\Lambda^2(V)$, a space of dimension 10. Two groups of order p^{5+d} are isomorphic if and only if the duals of their associated d-dimensional spaces of $\Lambda^2(V)$ are in the same $\mathrm{GL}(V)$-orbit. For $V = \mathbb{F}_p^n$, there are $\lfloor n/2 \rfloor$ orbits of 1-dimensional spaces on $\Lambda^2(V)$: each orbit is determined by the rank of the associated form [9, Thm. 3.5]. Brooksbank, Maglione, and Wilson [7] give a polynomial-time algorithm to decide isomorphism between two such groups of order p^{n+2}. Hence, by exploiting well-known properties of duality (cf. for example [9, Chap. 2]), we consider only $d \in \{3, 4, 5\}$.

4.1. Derived groups of order p^3

Copetti [9] and Vaughan-Lee [29] showed that there are 22 isomorphism classes of 5-generator groups of order p^8, class 2, and exponent p. Case (j) of [9, Thm. 7.22] corresponds via the Lazard Correspondence to Group 8.5.j of [29, §8.5].

The matrices $B \in \mathrm{Mat}_5(\mathbb{F}_p[y_1, y_2, y_3]_1)$, extracted from [29, §8.5] and described as in Section 2.1, are available at [22]. Since B is skew-symmetric, $I_5(B)$ is necessarily the zero ideal, and no information on the isomorphism class of $G_B(\mathbb{F}_p)$ is gained from the rank 5 locus of B.

For $p \in \{3, \ldots, 37\}$, Table 2 records the values of invariants from Theorem 2.3 for these 22 groups. There, $\deg(I)$ denotes the degree of an ideal I and $\mathrm{degprim}(I)$ records the degrees of the ideals in a minimal primary decomposition of I. By comparing Tables 1 and 2, we observe that groups (1)–(6) are direct products of the six groups from Section 3 with a group of order p. Twenty of the 22 isomorphism classes are identified using just three of the invariants associated with the rank 4 locus of B and the rank 3 locus of $B^\bullet$. The invariants from Theorem 2.3 do not distinguish between (14) and (15). Yet, Vaughan-Lee [29, §8.5] showed that the automorphism groups of $G_{B_{14}}(\mathbb{F}_p)$ and $G_{B_{15}}(\mathbb{F}_p)$ have orders $2(p-1)(p^2-1)p^{17}$ and $2(p-1)^3p^{17}$ respectively.

4.2. Quasi-polynomiality

Motivated by Higman's PORC conjecture, Lee [17] constructed a family $\mathcal{L}$ of groups of order p^9 for all primes $p \geqslant 5$, and showed that its cardinality is not determined by a quasi-

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Table 2
Invariants for 5-generator groups with derived group of order p^3.

Case	$n_p(I_4(\mathrm{B}))$	$\deg(I_4(\mathrm{B}))$	$n_p(I_3(\mathrm{B}^\bullet))$	$\mathrm{degprim}(I_3(\mathrm{B}^\bullet))$
(1)	p^3	1	p^4	$(2,3)$
(2)	p^3	1	p^5	(1)
(3)	$2p^2-p$	4	$2p^4-p^3$	$(1,1,4)$
(4)	p^2	4	p^4	$(2,3)$
(5)	p^2	4	$p^4+p^3-p^2$	$(2,4)$
(6)	p	4	p^3	$(2,3)$
(7)	1	9	p^3	$(1,3)$
(8)	1	6	p^3-p^2+p	$(2,2)$
(9)	1	0	p^3	(4)
(10)	p	10	p^3	(4)
(11)	p	9	$2p^3-p^2$	$(1,3)$
(12)	p	6	$2p^3-p^2$	$(2,2)$
(13)	p	9	$2p^3-p^2$	$(1,1,2)$
(14)	p	3	$2p^3-p$	$(1,3)$
(15)	p	3	$2p^3-p$	$(1,3)$
(16)	$2p-1$	9	$3p^3-2p^2$	$(1,1,2)$
(17)	$2p-1$	6	$3p^3-p^2-p$	$(1,1,2)$
(18)	$3p-2$	9	$4p^3-3p^2$	$(1,1,1,1)$
(19)	p^2+p-1	2	$p^4+p^3-p^2$	$(1,1,2)$
(20)	p^2	2	p^4	$(1,2,4)$
(21)	p^2	2	$p^4+p^3-p^2$	$(1,1,6)$
(22)	p^2	2	$p^4+p^3-p^2$	$(1,1,2)$

polynomial function in p. We briefly review his construction. Let $\mathrm{B} \in \mathrm{Mat}_5(\mathbb{Z}[y_1, y_2, y_3])$ where

$$\mathrm{B} = \begin{pmatrix} 0 & 0 & 0 & y_1 & y_2 \\ 0 & 0 & 0 & y_3 & y_1 \\ 0 & 0 & 0 & 2y_2 & y_3 \\ -y_1 & -y_3 & -2y_2 & 0 & 0 \\ -y_2 & -y_1 & -y_3 & 0 & 0 \end{pmatrix}.$$

The group $\mathrm{G}_\mathrm{B}(\mathbb{F}_p)$ has order $p^{5+3} = p^8$. Its isomorphism type is one of (7), (13) and (18); their projective varieties $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}))$ have respectively 0, 1, and 3 points in $\mathbb{P}^2(\mathbb{F}_p)$. The isomorphism type depends on p, each occurs infinitely often, and the function

$$\mathcal{P} = \{\text{primes}\} \longrightarrow \mathbb{N}, \quad p \longmapsto |\operatorname{Aut}(\mathrm{G}_\mathrm{B}(\mathbb{F}_p))| \tag{4.1}$$

is *not* quasi-polynomial. The groups in $\mathcal{L}$ are *immediate descendants* [20] of $\mathrm{G}_\mathrm{B}(\mathbb{F}_p)$: they have order p^9, class 3, and exponent p. They are determined by orbit representatives for the action of $\operatorname{Aut}(\mathrm{G}_\mathrm{B}(\mathbb{F}_p))$ on the duals of 1-spaces in $\mathbb{F}_p^{13}$; the number of orbits, or equivalently the cardinality of $\mathcal{L}$, varies according to $|\operatorname{Aut}(\mathrm{G}_\mathrm{B}(\mathbb{F}_p))|$, and so it is also not quasi-polynomial. We show that the groups in $\mathcal{L}$ have minimal order.

Theorem 4.1. *Assume that $n+d \leqslant 7$ and let $\mathrm{B} \in \mathrm{Mat}_n(\mathbb{Z}[y_1, \ldots, y_d]_1)$ be skew-symmetric. The function $\mathcal{P} \longrightarrow \mathbb{N}$, defined by $p \mapsto |\operatorname{Aut}(\mathrm{G}_\mathrm{B}(\mathbb{F}_p))|$, is quasi-polynomial.*

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Proof. Assume that $d \leqslant 2$. Let $G = \mathrm{G_B}(\mathbb{Q})$ and $G_p = \mathrm{G_B}(\mathbb{F}_p)$. If $\mathrm{Z}(G) \neq G'$, then we replace n by a smaller value, so we assume without loss of generality that $\mathrm{Z}(G) = G'$. The number of primes p for which $\mathrm{Z}(G_p) \neq G'_p$ is finite, since the reduction modulo p of $\mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B}))$ or $\mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B}^\bullet))$ now has positive dimension (instead of 0); cf. Lemma 2.1. These primes do not impact on quasi-polynomiality. By requiring that $\mathrm{Z}(G_p) = G'_p$ and comparing with [29], we deduce that, for $(n, d) \neq (4, 2), (5, 2)$, the function $p \mapsto |\operatorname{Aut}(\mathrm{G_B}(\mathbb{F}_p))|$ is constant. For the two remaining cases, the list in [29] demonstrates that variation over the primes is determined either by the dimension of $\mathcal{V}_{\mathrm{aff}}(I_1(\mathrm{B}))$, or by a given integer being a square modulo a prime. Both conditions are quasi-polynomial.

We now assume that $d \geqslant 3$, so the only possible parameters are $(n, d) \in \{(3, 3), (4, 3)\}$. If $(n, d) = (3, 3)$ then (4.1) is quasi-polynomial. Consider $(n, d) = (4, 3)$. Now $I_4(\mathrm{B})$ is principal, generated by the square of a homogeneous quadratic polynomial $f \in \mathbb{Z}[y_1, y_2, y_3]$. Using the notation of Section 3, the projective varieties given by the zero locus of f are the following:

- $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_1))$ and $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_2))$ equal $\mathbb{P}^2(\mathbb{Q})$;
- $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_3))$ is a union of two lines in $\mathbb{P}^2(\mathbb{Q})$;
- $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_4))$ is a line in $\mathbb{P}^2(\mathbb{Q})$;
- $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_5))$ is an ellipse in $\mathbb{P}^2(\mathbb{Q})$;
- $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}_6))$ is a point in $\mathbb{P}^2(\mathbb{Q})$.

If $f = 0$, then $\mathrm{G_B}(\mathbb{F}_p)$ is isomorphic to either $\mathrm{G_{B_1}}(\mathbb{F}_p)$ or $\mathrm{G_{B_2}}(\mathbb{F}_p)$. By [29, §7.4], their automorphism groups have the same order, and so (4.1) is quasi-polynomial. Assume that $f \neq 0$. Since the coefficients of f have a finite number of common prime divisors, we can ignore B_1 and B_2. Assume that $\mathrm{G_B}(\mathbb{F}_p) \cong \mathrm{G_{B_5}}(\mathbb{F}_p)$ for some prime p. Now f is necessarily smooth over $\mathbb{Z}$, and there are only finitely many primes r (of bad reduction) such that $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}))$ is a point, a line, or a union of two lines in $\mathbb{P}^2(\mathbb{F}_r)$. By multiplying the bad primes r into the modulus, and using the automorphism group orders from [29, §7.4], we deduce that (4.1) is quasi-polynomial. Consider the splitting behaviour of f in the three remaining cases. Let r be an odd prime. One of the following holds:

(0) $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}))$ is a point in $\mathbb{P}^2(\mathbb{F}_r)$ if and only if f mod r is (equivalent to) an irreducible polynomial in two variables;
(1) $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}))$ is a line in $\mathbb{P}^2(\mathbb{F}_r)$ if and only if f mod r is (a scalar multiple of) a square;
(2) $\mathcal{V}_{\mathrm{proj}}(I_4(\mathrm{B}))$ is a union of two lines in $\mathbb{P}^2(\mathbb{F}_r)$ if and only if f mod r is reducible but not (a scalar multiple of) a square.

If f is a polynomial in three indeterminates, then (0) can occur only for a finite number of primes, and so can be ignored. So either f is a square, as is every reduction mod r, or (1) occurs for only finitely many primes. In either case, the formulae from [29, §7.4] show that (4.1) is quasi-polynomial. If f is a polynomial in two indeterminates, then the

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

splitting of f modulo r is determined by a quasi-polynomial condition, again implying that (4.1) is quasi-polynomial. $\square$

4.3. Derived groups of order p^4

Brahana [4,5] identified 59 4-dimensional subspaces of the 10-dimensional commutator space as orbit representatives. Copetti [9] showed that the spaces he labelled 29 and 31 are in the same orbit. In unpublished work from 2001, M.F. Newman and O'Brien found two additional redundancies.

- Spaces 50 and 51 are in the same orbit.
- Space 35 is in the orbit of 30 when $p = 5$; it is in the orbit of 29 when $p \equiv \pm 1 \bmod 5$; and it is in the orbit of 32 when $p \equiv \pm 2 \bmod 5$.

They also identified one missing orbit representative. Independently, Eick and Vaughan-Lee [12] showed that the number of these groups is 57. We summarise the outcome.

Theorem 4.2. *For every prime $p \geqslant 3$, there are 57 isomorphism classes of 5-generator groups of order p^9, class 2, and exponent p.*

The matrices $\mathrm{B} \in \mathrm{Mat}_5(\mathbb{F}_p[y_1, y_2, y_3]_1)$ for the groups determined by the duals of the 60 4-dimensional subspaces are available at [22]. For $p \in \{3, \dots, 37\}$, we investigated the values of invariants from Theorem 2.3 for these groups; the resulting 57 distinct sets of invariants support the amendments to Brahana's list. Table 3 records the values of some distinguishing invariants for the 57 cases. We retain our earlier notation; also $\mathrm{rad}(I)$ denotes the radical of an ideal I, and $\mathrm{irr}_a(I)$ is the number of irreducible components of $\mathcal{V}_{\mathrm{aff}}(I)$, and $\#\,\mathrm{prim}(I)$ is the number of ideals in a minimal primary decomposition of I.

We label as (55) the missed representative, otherwise we use Brahana's labels [4,5]; we omit cases (31), (35), and (51). For compactness, we write $I_4 = I_4(\mathrm{B})$ and $I_3^\bullet = I_3(\mathrm{B}^\bullet)$. For $p = 3$ the value $\#\,\mathrm{prim}(I_3^\bullet)$ for (26) is 3, not 4.

4.4. Derived groups of order p^5

Eick and Vaughan-Lee [12] showed that the number of these groups is $63 + 3p + 2\gcd(p, 2) + \gcd(p, 3) + 2\gcd(p-1, 3) + \gcd(p-1, 4)$. No listing of isomorphism types is known. Brahana [6] considered 11-groups of this type, listing eight isomorphism types. We report just one computation: by generating "random" 5×5 skew-symmetric matrices in five indeterminates over $\mathbb{F}_5$ and partitioning them using the invariants of Theorem 2.3, we identified 60 of the 87 isomorphism types.

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Table 3
Invariants for 5-generator groups with derived group of order p^4.

Case	$n_p(I_4)$	deg(rad(I_4))	irr$_a(I_4)$	# prim(I_4)	$n_p(I_3^\bullet)$	deg(rad($I_3^\bullet$))	irr$_a(I_3^\bullet)$	# prim($I_3^\bullet$)
(0)	p^4	1	1	1	p^4	1	1	2
(1)	p^3+p^2-p	2	1	1	$2p^3-p$	2	2	3
(2)	p^3-p^2+p	2	1	1	p	2	1	2
(3)	p^3	2	1	1	p^3	1	1	2
(4)	$2p^2-p$	3	2	2	p^3+p^2-p	1	2	4
(5)	p^2+p-1	2	2	3	p^2+p-1	2	2	3
(6)	p^2	2	1	3	p^2	2	1	3
(7)	$2p^3-p^2$	2	2	2	p^4	1	1	3
(8)	p^3+p^2-p	1	2	2	p^4	1	1	4
(9)	p^3	1	1	2	p^4	1	1	3
(9′)	p^3	1	1	2	p^4	1	1	4
(10)	p^3+p-1	1	2	2	p^3+p^2-1	1	2	2
(11)	p^3	1	1	2	p^3	1	1	2
(12)	$3p^2-2p$	3	3	3	p^3+2p^2-2p	1	3	6
(13)	$3p^2-2p$	3	3	4	p^3	1	1	5
(14)	$2p^2-1$	2	3	4	$4p^2-2p-1$	4	4	6
(15)	$2p^2-p$	2	2	2	p^3+p^2-p	1	2	4
(16)	$2p^2-p$	2	2	4	$2p^2-p$	2	2	4
(17)	$2p^2-p$	2	2	4	$3p^2-2p$	3	3	5
(18)	$2p^2-p$	2	2	3	p^3	1	1	5
(19)	p^2+2p-2	1	3	4	$3p^2+p-3$	3	4	5
(20)	p^2+p-1	1	2	3	$2p^2+p-2$	2	3	4
(20′)	p^2+p-1	1	2	3	$2p^2-1$	2	2	4
(20″)	p^2+p-1	1	2	4	$3p^2-p-1$	3	3	6
(21)	p^2	3	2	3	p^3	1	1	4
(21′)	p^2	1	1	2	p^3	1	1	4
(22)	p^2	3	2	2	p^3	1	2	4
(23)	p^2	1	1	3	p^2	1	1	3
(24)	p^2	1	2	3	p^2+p-1	3	3	4
(25)	p^2	1	1	3	$2p^2-p$	2	2	5
(26)	p^2	1	1	3	$2p^2-p$	2	2	4
(27)	p^2	1	1	4	$3p^2-2p$	3	3	4
(28)	p^2	3	1	1	p^3	1	1	2
(29)	$5p-4$	5	5	5	$10p-9$	10	10	11
(30)	$4p-3$	4	4	4	$7p-6$	7	7	8
(32)	$3p-2$	5	4	4	$4p-3$	10	7	8
(33)	$3p-2$	3	3	3	$4p-3$	4	4	5
(34)	$3p-2$	3	3	3	$5p-4$	5	5	6
(36)	$2p-1$	5	3	3	p	10	4	5
(37)	$2p-1$	4	3	3	$3p-2$	7	5	6
(38)	$2p-1$	2	2	2	$3p-2$	3	3	4
(39)	$2p-1$	2	2	3	$2p-1$	4	2	4
(40)	$2p-1$	2	2	2	$2p-1$	2	2	3
(41)	$2p-1$	2	2	2	p^2+p-1	2	2	5
(42)	$2p-1$	2	2	2	p^2+p-1	2	2	4
(43)	p	3	1	2	p^3	1	1	3
(44)	p	1	1	1	p^2	2	1	3
(45)	p	2	1	3	p	2	1	3
(46)	p	3	2	2	$2p-1$	4	3	4
(47)	p	1	1	1	p	1	1	2
(48)	p	4	2	2	p	7	3	4
(49)	p	3	2	2	p	5	3	4
(50)	p	5	3	3	$2p-1$	10	6	7
(52)	p	5	2	2	1	10	3	4
(53)	1	5	2	2	p	10	3	4
(54)	1	5	1	1	1	10	2	3
(55)	p^2	1	1	3	p^2	3	2	3

5. Providing access to our results

The lists of skew-symmetric matrices defining groups of order p^{4+3}, p^{5+3} and p^{5+4} are available at [22]. We provide MAGMA functions to construct from a group of class 2 and exponent p the matrices B and $\mathrm{B}^\bullet$ and vice versa; and the invariants listed in Theorem 2.3. Our machinery relies on Gröbner basis computations, but typically has good practical performance. Using MAGMA 2.28-15 on a 2.6GHz machine, Tables 2 and 3 were constructed in 17 and 124 minutes of CPU time respectively. The most expensive calculation is the primary decomposition of an ideal; it can be omitted, as was done in the calculations reported in Section 4.4.

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

Data availability

Link to Github page collecting the code used is listed in the references.

References

[1] S. Adian, On algorithmic problems in effectively complete classes of groups, Dokl. Akad. Nauk SSSR 123 (1958) 13–16.

[2] R. Baer, Groups with abelian central quotient group, Trans. Amer. Math. Soc. 44 (3) (1938) 357–386.

[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (3–4) (1997) 235–265.

[4] H.R. Brahana, Finite metabelian groups and the lines of a projective four-space, Amer. J. Math. 73 (1951) 539–555.

[5] H.R. Brahana, Metabelian p-groups with five generators and orders p^{12} and p^{11}, Ill. J. Math. 2 (1958) 641–717.

[6] H.R. Brahana, On metabelian groups of order p^{10} with five generators, Rend. Circ. Mat. Palermo 2 (9) (1960) 97–113.

[7] P.A. Brooksbank, J. Maglione, J.B. Wilson, A fast isomorphism test for groups whose Lie algebra has genus 2, J. Algebra 473 (2017) 545–590.

[8] W. Bruns, U. Vetter, Determinantal Rings, Monogr. Mat. Instituto de Matemática Pura e Aplicada, vol. 45, IMPA, Rio de Janeiro, 1988.

[9] A. Copetti, Finite-dimensional Lie algebras of nilpotency class 2, Master's thesis, Australian National University, 2004, https://openresearch-repository.anu.edu.au/handle/1885/150852.

[10] D.A. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4th edition, Undergrad. Texts Math., Springer, Cham, 2015.

[11] M. Dehn, Über unendliche diskontinuierliche gruppen, Math. Ann. 71 (1911) 116–144.

[12] B. Eick, M.R. Vaughan-Lee, Counting p-groups and Lie algebras using PORC formulae, J. Algebra 545 (2020) 198–212.

[13] D. Eisenbud, Commutative Algebra. With a View Toward Algebraic Geometry, Grad. Texts in Math., vol. 150, Springer-Verlag, New York, 1995.

[14] U. First, J. Maglione, J.B. Wilson, A spectral theory for transverse tensor operators, https://arxiv.org/abs/1911.02518, 2019.

[15] A. Gathmann, Commutative Algebra, Class Notes TU Kaiserslautern, 2013, https://agag-gathmann.math.rptu.de/class/commalg-2013/commalg-2013.pdf.

[16] A. Gathmann, Algebraic Geometry, Class Notes TU Kaiserslautern, 2014, https://agag-gathmann.math.rptu.de/class/alggeom-2014/alggeom-2014.pdf.

[17] S. Lee, A class of descendant p-groups of order p^9 and Higman's PORC conjecture, J. Algebra 468 (2016) 440–447.

[18] J. Maglione, M. Stanojkovski, Smooth cuboids in group theory, Algebra Number Theory 19 (5) (2025) 967–1006.

[19] J. Maglione, J.B. Wilson, Tensorspace, version 2.3, Contributions from Peter A. Brooksbank, 2020, https://github.com/thetensor-space/TensorSpace.

[20] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (1990) 677–698.

[21] E.A. O'Brien, Isomorphism testing for p-groups, J. Symbolic Comput. 17 (1994) 133–147.

[22] E.A. O'Brien, M. Stanojkovski, Geometric invariants for finite p-groups, https://github.com/eamonnaobrien/Invariants-class2-pgroups.

[23] E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, https://arxiv.org/abs/2411.19555, 2024.

[24] E.A. O'Brien, C. Voll, Enumerating classes and characters of p-groups, Trans. Amer. Math. Soc. 367 (11) (2015) 7775–7796.

[25] M. Rabin, Recursive unsolvability of group theoretic problems, Ann. Math. 67 (1958) 172–194.

[26] D.J.S. Robinson, A Course in the Theory of Groups, second edition, Grad. Texts in Math., vol. 80, Springer-Verlag, New York, 1996.

[27] M. Stanojkovski, C. Voll, Hessian matrices, automorphisms of p-groups, and torsion points of elliptic curves, Math. Ann. 381 (1–2) (2021) 593–629.

Please cite this article in press as: E.A. O'Brien, M. Stanojkovski, Geometric invariants for p-groups of class 2 and exponent p, J. Algebra (2025), https://doi.org/10.1016/j.jalgebra.2025.08.029

[28] X. Sun, Faster isomorphism testing for p-groups of class 2 and exponent p, in: STOC'23–Proceedings of the 55th Annual ACM Symposium on Theory of Computing, 2023, pp. 433–440.

[29] M. Vaughan-Lee, The automorphisms of class two groups of prime exponent, https://arxiv.org/abs/1501.00678, 2015.