Publl. Math. Debrecen
85/3-4 (2014), 309–337
DOI: 10.5486/PMD.2014.5938

On the capability of finite groups of class two and prime exponent

By ARTURO MAGIDIN (Lafayette)

Abstract. We consider the capability of p-groups of class two and odd prime exponent. We give a sufficient condition based only on the ranks of $G/Z(G)$ and $[G,G]$, that shows that if $[G,G]$ is sufficiently large relative to $G/Z(G)$, then G is capable.

1. Introduction

In his landmark paper [10] on the classification of finite p-groups, P. Hall remarked:

> The question of what conditions a group G must fulfill in order that it may be the central quotient group of another group H, $G \cong H/Z(H)$, is an interesting one. But while it is easy to write down a number of necessary conditions, it is not so easy to be sure that they are sufficient.

Following M. Hall and Senior [9], we make the following definition:

Definition 1.1. A group G is said to be *capable* if and only if there exists a group H such that $G \cong H/Z(H)$.

Capability of groups was first studied explicitly by R. Baer in [2], where, as a corollary of deeper investigations, he characterized the capable groups that are direct sums of cyclic groups. Capability of groups has received renewed attention in recent years, thanks to results of Beyl, Felgner, and Schmid [3] characterizing the capability of a group in terms of its epicenter; and more recently to

Mathematics Subject Classification: Primary: 20D15; Secondary: 20F12.
Key words and phrases: capability, p-group, 2-nilpotent, prime exponent.

work of Graham Ellis [6] that describes the epicenter in terms of the nonabelian tensor square of the group.

We will consider here the special case of nilpotent groups of class two and exponent an odd prime p. This case was studied in [11], and also addressed elsewhere (e.g., Proposition 9 in [6]). As noted in the final paragraphs of [1], currently available techniques seem insufficient for a characterization of the capable finite p-groups of class 2, but a characterization of the capable finite groups of class 2 and exponent p seems a more modest and possibly attainable goal. The present work is a contribution towards achieving that goal.

The case of class two and exponent p seems tantalizing thanks to known results. For example, it is not hard to use results from [3], [6] to reduce the problem to groups G satisfying $[G,G] = Z(G)$ that are not expressible as a nontrivial direct or central product. Some sufficient conditions for capability are known in this situation (e.g., Proposition 9 in [6]). Nonetheless, the matter is not as straightfoward as it might appear at this point, since every finite group of class two and odd prime exponent can be embedded into groups G_1 and G_2, both of class two and prime exponent and satisfying $[G_i,G_i] = Z(G_i)$, neither expressible as a nontrivial direct or central product, and with G_1 capable and G_2 non-capable [14]. This suggests that a more 'holistic' approach must be taken.

Our main result is a sufficient condition that guarantees that such a group is capable provided that its commutator subgroup is sufficiently large. This result is a nice counterpart to the result of Heineken and Nikolova [11, Theorem 1], which says that if G satisfies $Z(G) = [G,G]$, is capable of exponent p and class two, and the rank of $Z(G)$ is k, then the rank of $G/[G,G]$ is at most $2k + \binom{k}{2}$; we can view this condition as saying that if G is capable, then $[G,G]$ cannot be too small.

In a sense, the general thrust of all of these results (and other known sufficient conditions for capability in this class) suggest that a group is capable if it is "nonabelian enough"; though of course that is not a precise condition.

In the next section we will give basic definitions and our notational conventions, as well as summarize previous results as they relate to the situation we are considering. In Section 3 we we describe a "canonical witness" to the capability of a group G; that is, we show that given a group G of class two and exponent p, there is a group K of class three that is generated by elements of exponent p, which can be described in terms of a presentation of G, and such that G is capable if and only if $K/Z(K) \cong G$. In Section 4 we recast the problem in terms of certain linear transformations. In Section 5 we establish our main result, Theorem 5.28. Section 6 contains our final remarks.

We should mention that the approach of using linear algebra and geometry to study groups of class two and exponent p is hardly new. In particular, the work of Brahana [4], [5] exploits geometry in a striking manner to classify certain groups in this class in terms of equivalence classes of points, lines, planes and subspaces in a projective space under the action of a linear group. We can also relate the work done here, and particularly Corollary 3.3, with work of Graham Ellis [6]. One way to think of the connection is to let F be the relatively free group of class two and exponent p; both the current work and Ellis's work look at $[F,F]\wedge F^{\mathrm{ab}}$, and ask which elements map to a certain subspace of the form $A+B$. In the present work, we attempt to simplify the situation by moding out by B and considering images in the quotient, whereas in [6] the quotient is taken modulo A. We will not go into the details because of length considerations. Likewise, we only mention that our set-up can be used to establish other results, such as those in [6], [11], and [14].

2. Definitions and previous results

Throughout the paper p will be an odd prime, and $\mathbb{F}_p$ will denote the field with p elements. All groups will be written multiplicatively, and the identity element will be denoted by e; if there is danger of ambiguity or confusion, we will use e_G to denote the identity of the group G. The center of G is denoted by $Z(G)$. Recall that if G is a group, and $x,y\in G$, the commutator of x and y is defined to be $[x,y]=x^{-1}y^{-1}xy$; we use x^y to denote the conjugate $y^{-1}xy$. We write commutators left-normed, so that $[x,y,z]=[[x,y],z]$. Given subsets A and B of G we define $[A,B]$ to be the subgroup of G generated by all elements of the form $[a,b]$ with $a\in A$, $b\in B$. The terms of the lower central series of G are defined recursively by letting $G_1=G$, and $G_{n+1}=[G_n,G]$. A group is *nilpotent of class at most c* if and only if $G_{c+1}=\{e\}$, if and only if $G_c\subset Z(G)$. We usually drop the “at most” clause, it being understood. The class of all nilpotent groups of class at most c is denoted by $\mathfrak{N}_c$. Though we will sometimes use indices to denote elements of a family of groups, it will be clear from context that we are not referring to the terms of the lower central series in those cases.

The following commutator identities are well known, and may be verified by direct calculation:

Proposition 2.1. *Let G be any group. Then for all $x,y,z\in G$,*

(a) $[xy,z]=[x,z][x,z,y][y,z]$.

(b) $[x,yz]=[x,z][z,[y,x]][x,y]$.

(c) $[x,y,z][y,z,x][z,x,y] \equiv e \pmod{G_4}$ *(the Hall–Witt identity).*

(d) $[x^r, y^s] \equiv [x,y]^{rs}[x,y,x]^{s\binom{r}{2}}[x,y,y]^{r\binom{s}{2}} \pmod{G_4}$.

(e) $[y^r, x^s] \equiv [x,y]^{-rs}[x,y,x]^{-r\binom{s}{2}}[x,y,y]^{-s\binom{r}{2}} \pmod{G_4}$.

Here, $\binom{n}{2} = \frac{n(n-1)}{2}$ *for all integers* n.

As in [13], our starting tool will be the nilpotent product of groups; specifically the 2-nilpotent and 3-nilpotent product of cyclic groups. We restrict Golovin's original definition [7] to the situation we will consider:

Definition 2.2. Let $A_1, \ldots, A_n$ be nilpotent groups of class at most c. The c-nilpotent product of $A_1, \ldots, A_n$, denoted by $A_1 \amalg^{\mathfrak{N}_c} \cdots \amalg^{\mathfrak{N}_c} A_n$, is defined to be the group $G = F/F_{c+1}$, where F is the free product of the A_i, $F = A_1 * \cdots * A_n$, and F_{c+1} is the $(c+1)$-st term of the lower central series of F.

From the definition it is clear that the c-nilpotent product is the coproduct in the variety $\mathfrak{N}_c$, so it will have the usual universal property. In particular, if $c < p$ (the "small class" case), then the c-nilpotent product of n cyclic groups of order p yields the relatively free group in the variety of c-nilpotent groups of exponent p. Moreover, when $c \leq p$, we may write each element of this nilpotent product uniquely as a product of basic commutators of weight at most c on the generators, as shown in Theorem 3 of [17]; see §12.3 of [8] for the definition of basic commutators which we will use. Our investigation is restricted to the case of odd primes and to the 2-nilpotent and 3-nilpotent product of cyclic groups of order p, so that the normal form in terms of basic commutators applies.

If G is a p-group of exponent p and class exactly two, then we can express G as $G = K \oplus C_p^n$, where C_p is the cyclic group of order p, n is a nonnegative integer, and K is a group satisfying $Z(K) = [K,K]$. It is easy to verify that G is capable if and only if K is nontrivial and capable. Because of this, we may, if convenient, assume that G satisfies $[G,G] = Z(G)$, though in many of the results this condition is not strictly required.

If G is a group (finite or not, p-group or not), the *epicenter of* G, $Z^*(G)$ is the smallest normal subgroup of G with the property that $G/Z^*(G)$ is capable. The epicenter was introduced by Beyl, Felgner, and Schmid [3], as a measure of the obstruction to G being capable. From the definition, it is clear that G is capable if and only if $Z^*(G)$ is trivial; and since $G/Z(G)$ is always capable, we must have $Z^*(G) \subseteq Z(G)$.

3. A canonical witness

Given a group G, we attempt to construct a witness for the capability of G; meaning a group H such that $H/Z(H) \cong G$. The relations among the elements of G force in turn relations among the elements of H. When G is not capable, this will manifest itself as undesired relations among the elements of H, forcing certain elements whose image should not be trivial in G to be central in H. Information about G can be used to deduce information about H; for example, if G is nilpotent of class exactly c, then the potential witness H will necessarily be nilpotent of class exactly $c+1$. Any reductions that can be done in the starting potential witness group H will yield dividens of simplicity later on; this is the main goal of the following result, which holds in full generality for any group G (not necessarily nilpotent, not necessarily finite). The proof that the witness may be chosen to be finite when G is finite comes from Lemma 2.1 of [12], and the argument for condition (ii) appears *en passant* in the proof of Theorem 1 in [11].

Theorem 3.1. *Let G be a group, generated by $g_1, \dots, g_n$. If G is capable, then there exists a group H, such that $H/Z(H) \cong G$, and elements $h_1, \dots, h_n \in H$ which map onto $g_1, \dots, g_n$, respectively, under the isomorphism such that:*

(i) *$H = \langle h_1, \dots, h_n \rangle$, and*

(ii) *The order of h_i is the same as the order of g_i, $i = 1, \dots, n$.*

Moreover, if G is finite, then H can be chosen to be finite as well.

Proof. If G is capable, then there exists a group K such that $K/Z(K) \cong G$. Pick $k_1, \dots, k_n \in K$ mapping to $g_1, \dots, g_n$, respectively, and let M be the subgroup of K generated by $k_1, \dots, k_n$. Since $MZ(K) = K$, it follows that $Z(M) = M \cap Z(K)$, hence $M/Z(M) \cong K/Z(K) \cong G$. Thus, replacing K by M if necessary, we may assume that K is generated by $k_1, \dots, k_n$, mapping onto $g_1, \dots, g_n$, respectively.

Next we establish the clause on the orders of the generators. Let C be a free abelian group of rank n generated by elements $x_1, \dots, x_n$, and for each i, $1 \leq i \leq n$, let a_i be the order of g_i if g_i is torsion, and $a_i = 0$ if g_i is not a torsion element. Now let $M = (K \times C)/N$, where N is the subgroup of $K \times C$ generated by the elements $(k_i^{a_i}, x_i^{-a_i})$, $i = 1, \dots, n$. Note that since the commutator subgroup of $K \times C$ is $[K,K] \times \{1\}$, we must have that the intersection $N \cap [K \times C, K \times C]$ is trivial (by considering the C-component of an element of N). Therefore, if (k,c) maps to the center of M then $[(k,c), K \times C] \subseteq ([K,K] \times \{1\}) \cap N)$, and so $[(k,c), K \times C]$ is trivial; hence in fact we have $k \in Z(K)$. That is, $Z(M)$ is the image of $Z(K) \times C$ in M; since $k_i^{a_i} \in Z(K)$ owing to the fact that $K/Z(K) \cong G$, it therefore follows that $N \subseteq Z(K)\times C$ and hence

$$\frac{M}{Z(M)} \cong \frac{(K\times C)/N}{(Z(K)\times C)/N} \cong \frac{K\times C}{Z(K)\times C} \cong \frac{K}{Z(K)} \cong G.$$

Note that under the isomorphism, the image of (k_j, x^r) is g_j for all integers r. Now let h_i be the image of (k_i, x_i^{-1}) in M for $i=1,\ldots,n$, and let H be the subgroup of M generated by $h_1,\ldots,h_n$. Then once again we have that $M = HZ(M)$, hence $H/Z(H) \cong M/Z(M) \cong G$, and the map $H \to H/Z(H) \cong G$ maps h_i to g_i. Moreover, the order of h_i is a_i, and so we have obtained a group H with central quotient G, generated by elements $h_1,\ldots,h_n$ that map to $g_1,\ldots,g_n$, and with $o(h_i) = o(g_i)$, as desired.

Finally, if G is finite, then H is finitely generated and $Z(H)$ is of finite index, hence by SCHREIER's theorem [15] $Z(H)$ is finitely generated. We can write $Z(H)$ as $Z_{\rm tor} \oplus F$, where $Z_{\rm tor}$ is the torsion part of $Z(H)$, hence finite, and F is free abelian. We know that $Z(H)/F \subseteq Z(H/F)$; to prove equality, if $[x,H] \subseteq F$, then $[x,h]$ is central for every h. Therefore, from 2.1(b) it follows that the map $h \mapsto [x,h]$ is a group homomorphism from H to F. Now, $Z(H)$ is contained in the kernel of this homomorphism, and since $H/Z(H)$ is finite, then the image is a finite subgroup of a free abelian group, and hence trivial. Thus, $[x,H]$ is trivial, so $x \in Z(H)$, proving that $Z(H/F) = Z(H)/F$. Hence, $(H/F)/Z(H/F) \cong H/Z(H) \cong G$. Note that since G is finite all generators are of finite order, so none of the cyclic subgroups $\langle h_i\rangle$ intersects F, so we may replace H with H/F if necessary to obtain that H may be chosen finite when G is finite without altering the orders of the generators. □

When G is a group of class two, we further know that a potential witness H is of class three, and so we can start from the c-nilpotent product of cyclic groups of appropriate order. In our situation of interest, with G of class two and prime exponent, this now allows us to give a very specific "canonical witness" to the capability of G.

Theorem 3.2. *Let G be a finite noncyclic group of class at most two and exponent an odd prime p. Let $g_1,\ldots,g_n$ be elements of G that project onto a basis for $G/[G,G]$, and let F be the 3-nilpotent product of n cyclic groups of order p generated by $x_1,\ldots,x_n$, respectively. Let N be the kernel of the morphism $\psi: F \to G$ induced by mapping $x_i \mapsto g_i$, $i=1,\ldots,n$. Then G is capable if and only if*

$$G \cong \left(F/[N,F]\right) \Big/ Z\left(F/[N,F]\right).$$

Proof. Sufficiency is immediate. For the necessity, assume that G is capable, and let H be the group guaranteed by Theorem 3.1 such that $G \cong H/Z(H)$. Note that H is of class at most three. Let $\theta : H/Z(H) \to G$ be an isomorphism that maps $h_iZ(H)$ to g_i.

Since $h_1, \dots, h_n$ are of order p, there exists a (unique surjective) morphism $\varphi : F \to H$ induced by mapping x_i to h_i, $i = 1, \dots, n$. If $\pi : H \to H/Z(H)$ is the canonical projection, then we must have $\theta\pi\varphi = \psi$ by the universal property of the coproduct. Thus, $\varphi(N) = \ker(\pi) = Z(H)$, so $[N, F] \subset \ker(\varphi)$, and φ factors through $F/[N, F]$; surjectivity of φ implies that $\varphi(Z(F/[N, F])) \subset Z(H)$, hence $G \cong H/Z(H)$ is a quotient of $(F/[N, F]) \;/\; Z(F/[N, F])$.

On the other hand, $N[N, F] \subseteq Z(F/[N, F])$, so $G \cong F/N = F/N[N, F]$ has $(F/[N, F]) \;/\; Z(F/[N, F])$ as a quotient.

Thus we have that G has $(F/[N, F]) \;/\; Z(F/[N, F])$ as a quotient, which in turn has G as a quotient. Since G is finite, the only possibility is that the central quotient of $F/[N, F]$ is isomorphic to G, as claimed. □

Corollary 3.3. *Let G be a finite noncyclic group of class at most two and exponent an odd prime p. Let $g_1, \dots, g_n$ be elements of G that project onto a basis for $G/[G, G]$, and let F be the 3-nilpotent product of n cyclic groups of order p generated by $x_1, \dots, x_n$, respectively. Let $\psi : F \to G$ be the map induced by sending x_i to g_i, $i = 1, \dots, n$. Finally, let C be the subgroup of F generated by the commutators $[x_j, x_i]$, $1 \leq i < j \leq n$. If X is the subgroup of C such that $\ker(\psi) = X \oplus F_3$, then G is capable if and only if $\{c \in C \mid [c, F] \subset [X, F]\} = X$.*

Proof. Let $N = \ker(\psi)$. By Theorem 3.2, G is capable if and only if G is isomorphic to the central quotient of $F/[N, F]$. Thus, G is capable if and only if the center of $F/[N, F]$ is $N/[N, F]$, and no larger.

An element $h[N, F] \in F/[N, F]$ is in $Z(F/[N, F])$ if and only if $[h, F]$ is contained in $[N, F]$. Since G is of exponent p, $F_3 \subseteq N \subseteq F_2$ and so $[N, F] = [X, F] \subseteq F_3$. In particular, we deduce that if $h[N, F]$ is central, then h must lie in F_2. Write $h = cf$, with $c \in C$ and $f \in F_3$. Then $[h, F] = [c, F]$, so $h[N, F]$ is central if and only if $[c, F] \subset [X, F]$.

If $\{c \in C \mid [c, F] \subset [X, F]\} = X$, then it follows that $h[N, F]$ is central if and only if $h = cf$ with $c \in X$ and $f \in F_3$, which means that $h[N, F]$ is central if and only if $h \in N$. Hence, the center of $F/[N, F]$ is $N/[N, F]$, and G is capable.

Conversely, assume that G is capable. Then the center of $F/[N, F]$ is equal to $N/[N, F]$. Therefore, $X \subseteq \{c \in C \mid [c, f] \subset [X, F]\} \subseteq N \cap C = X$, giving equality. □

One advantage of the description just given is the following: both F_2 and

F_3 are vector spaces over $\mathbb{F}_p$, and the maps $[-,x]: F_2 \to F_3$ are linear transformations for each $x \in F$; hence, the condition just described can be restated in terms of vector spaces, subspaces, and linear transformations. While all the work can still be done at the level of groups and commutators, the author, at any rate, found it easier to think in terms of linear algebra. In addition, once the problem has been cast into linear algebra terms, there is a host of tools (such as geometric arguments) that can be brought to bear on the issue.

We will discuss this translation and more results on capability below, after a brief abstract interlude on linear algebra.

4. Some linear algebra

We set aside groups and capability temporarily to describe the general construction that we will use in our analysis.

Definition 4.1. Let V and W be vector spaces over the same field, and let $\{\ell_i\}_{i\in I}$ be a nonempty family of linear transformations from V to W. Given a subspace X of V, let X^* be the subspace of W defined by:

$$X^* = \operatorname{span}\bigl(\ell_i(X) \mid i \in I\bigr).$$

Given a subspace Y of W, let Y^* be the subspace of V defined by:

$$Y^* = \bigcap_{i\in I} \ell_i^{-1}(Y).$$

It will be clear from context whether we are talking about subspaces of V or W.

It is clear that $X \subset X' \Rightarrow X^* \subset X'^*$ for all subspaces X and X' of V, and likewise $Y \subset Y' \Rightarrow Y^* \subset Y'^*$ for all subspaces Y, Y' of W.

Theorem 4.2. *Let V and W be vector spaces over the same field and let $\{\ell_i\}_{i\in I}$ be a nonempty family of linear transformations from V to W. The operator on subspaces of V defined by $X \mapsto X^{**}$ is a closure operator; that is, it is increasing, isotone, and idempotent. Moreover, $(X^{**})^* = (X^*)^{**} = X^*$ for all subspaces X of V.*

Proof. Since $\ell_i(X) \subseteq X^*$ for all i, it follows that $X \subset X^{**}$, so the operator is increasing. If $X \subset X'$, then $X^* \subset X'^*$, hence $X^{**} \subset X'^{**}$, and the operator is isotone. The equality of $(X^{**})^*$ and $(X^*)^{**}$ is immediate. Since $X \subset X^{**}$, we have $X^* \subset (X^{**})^*$. And by construction $\ell_i(X^{**}) \subset X^*$ for each i, so $(X^{**})^* \subset X^*$ giving equality.

Thus, $(X^{**})^{**} = (X^{***})^* = (X^*)^* = X^{**}$, so the operator is idempotent, finishing the proof. □

It may be worth noting that while this closure operator is algebraic (the closure of a subspace X is the union of the closures of all finitely generated subspaces X' contained in X), it is not topological (in general, the closure of the subspace generated by X and X' is not equal to the subspace generated by X^{**} and X'^{**}).

We note that the dual result holds for subspaces of W, giving an interior operator that is algebraic but not topological.

Given a family of linear transformations $\{\ell_i : V \to W\}_{i\in I}$, we will say a subspace X of V is $\{\ell_i\}_{i\in I}$-*closed* (or simply *closed* if the family is understood from context) if and only if $X = X^{**}$.

It is easy to verify that the closure operator determined by a nonempty family $\{\ell_i\}_{i\in I}$ of linear transformations is the same as the closure operator determined by the subspace of $\mathcal{L}(V, W)$ (the space of all linear transformations from V to W) spanned by the ℓ_i. Likewise, the following observation is straightforward:

Proposition 4.3. *Let V and W be vector spaces, and X be a subspace of V. Let $\{\ell_i\}_{i\in I}$ be a nonempty family of linear transformations from V to W, and let $\psi \in \mathrm{Aut}(V)$. If we use ** to denote the $\{\ell_i\}_{i\in I}$ closure operator, then the $\{\ell_i\psi^{-1}\}_{i\in I}$-closure of $\psi(X)$ is $\psi(X^{**})$. In particular, X is $\{\ell_i\}$-closed if and only if $\psi(X)$ is $\{\ell_i\psi^{-1}\}$-closed. If $\{\ell_i\}$ and $\{\ell_i\psi^{-1}\}$ span the same subspace of $\mathcal{L}(V, W)$, then X is closed if and only if $\psi(X)$ is closed.*

Back to capability. To tie the construction above back to the problem of capability, we introduce specific vector spaces and linear transformations based on Corollary 3.3. We fix an odd prime p throughout.

Definition 4.4. Let $n > 1$. We let $U(n)$ denote a vector space over $\mathbb{F}_p$ of dimension n. We let $V(n)$ denote the vector space $U(n) \wedge U(n)$ of dimension $\binom{n}{2}$. Finally, we let $W(n)$ be the quotient $(V(n) \otimes U(n))/J$, where J is the subspace spanned by all elements of the form $(\mathbf{a}\wedge\mathbf{b})\otimes\mathbf{c} + (\mathbf{b}\wedge\mathbf{c})\otimes\mathbf{a} + (\mathbf{c}\wedge\mathbf{a})\otimes\mathbf{b}$, with $\mathbf{a}, \mathbf{b}, \mathbf{c} \in U$. The vector space $W(n)$ has dimension $2\binom{n+1}{3}$. If there is no danger of ambiguity and n is understood from context, we will simply write U, V, and W to refer to these vector spaces.

To specify our closure and interior operators on V and W, we define the following family of linear transformations:

Definition 4.5. Let $n > 1$. We embed U into $\mathcal{L}(V, W)$ as follows: given $\mathbf{u} \in U$ and $\mathbf{v} \in V$, we let $\varphi_{\mathbf{u}}(\mathbf{v}) = \overline{\mathbf{v} \otimes \mathbf{u}}$, where $\overline{\mathbf{x}}$ denotes the image in W of a vector $\mathbf{x} \in V \otimes U$. If $x_1, \ldots, x_n$ is a given basis for U and i is an integer, $1 \leq i \leq n$, then we will use φ_i to denote the linear transformation φ_{x_i}.

The closure operator we will consider is given by the family $\{\varphi_{\mathbf{u}} \mid \mathbf{u} \in U\}$. As noted above, if $x_1, \ldots, x_n$ is a basis for U, then this closure operator is also determined by the family $\{\varphi_1, \ldots, \varphi_n\}$.

Going back to the problem of capability, let F be the 3-nilpotent product of cyclic groups of order p generated by $x_1, \ldots, x_n$. We can identify F_2 with $V \oplus W$ by identifying $x_j \wedge x_i$ with $[x_j, x_i]$ and $\overline{(x_j \wedge x_i) \otimes x_k}$ with $[x_j, x_i, x_k]$; this also identifies W with F_3.

Let G be a noncyclic group of class at most two and exponent p, and let $g_1, \ldots, g_n$ be elements of G that project onto a basis for $G/[G, G]$. If we let $\psi : F \to G$ be the map induced by mapping $x_i \mapsto g_i$ and $N = \ker(\psi)$, then as above we can write $N = X \oplus F_3$, where X is a subgroup of

$$C = \langle [x_j, x_i] \mid 1 \leq i < j \leq n \rangle.$$

Thus, we can identify X with a subspace of V by identifying the latter with the subgroup C; abusing notation somewhat, we call this subspace X as well.

Theorem 4.6. *Let G, F, U, V, W, C, and X be as in the preceding paragraphs. Then G is capable if and only if X is $\{\varphi_{\mathbf{u}} \mid \mathbf{u} \in U\}$-closed.*

Proof. We know G is capable if and only if $\{c \in C \mid [c, F] \subset [X, F]\} = X$. Identifying C with V and F_3 with W, note that φ_i is a map from C to F_3, corresponding to $[-, x_i]$. Thus, $X^* \subseteq W$ corresponds to $[X, F] \subseteq F_3$, and X^{**} corresponds to the set $\{c \in C \mid [c, F] \subset [X, F]\}$. Therefore, G is capable if and only if

$$X = \{\mathbf{v} \in V \mid \varphi_{\mathbf{u}}(\mathbf{v}) \in X^* \text{ for all } \mathbf{u} \in U\} = X^{**},$$

as claimed. □

In other words, the closure operator codifies exactly the condition we want to check to test the capability of G. Thus the question *"What n-generated p-groups of class two and exponent p are capable?"* is equivalent to the question *"What subspaces of $V(n)$ are $\{\varphi_{\mathbf{u}} \mid \mathbf{u} \in U\}$-closed?"*

Of course, different subspaces may yield isomorphic groups. In particular, if we let $\mathrm{GL}(n, p)$ act on U, then this action induces an action of $\mathrm{GL}(n, p)$ on $V = U \wedge U$; if X and X' are on the same orbit relative to this action, then the groups G and H that correspond to X and X', respectively, are isomorphic. By Proposition 4.3 the closures of X and X' will also be in the same orbit under the action and G will be capable if and only if H is capable.

Also of interest is the description of the closure of X when G is not capable. It is clear that the quotient of G determined by X^{**} is the largest quotient of G that is capable. That is, X^{**}/X is isomorphic to $Z^*(G)$, the epicenter of G.

5. Dimension counting

In this section, we first obtain some basic consequences of our set-up, before establishing our main result. We will let $x_1, \ldots, x_n$ generated cyclic groups of order p, and let F be the 3-nilpotent product of the cyclic groups $\langle x_1 \rangle$, $\langle x_3 \rangle, \ldots, \langle x_n \rangle$. If $p > 3$, then this will be the relatively free group of class 3 and exponent p. We identify V with the subgroup of F_2 with basis $[x_j, x_i]$, $1 \leq i < j \leq n$, and W with F_3, which has basis given by the commutators $[x_j, x_i, x_k]$ with $1 \leq i < j \leq n$, $i \leq k \leq n$. Our linear maps are $\varphi_k : V \to W$, $k = 1, \ldots, n$, given by $\varphi_k(\mathbf{v}) = \mathbf{v} \wedge x_k = [\mathbf{v}, x_k]$ (identifying V with the corresponding commutator subgroup). Since we are thinking of V and W as vector spaces over $\mathbb{F}_p$, we will use additive notation rather than multiplicative notation for them. Thus, we have

$$\varphi_k([x_j, x_i]) = \begin{cases} [x_j, x_i, x_k] & \text{if } k \geq i, \\ [x_j, x_k, x_i] - [x_i, x_k, x_j] & \text{if } k < i. \end{cases}.$$

Lemma 5.1. *Fix $n > 1$, and let k be an integer, $1 \leq k \leq n$.*

(i) *φ_k is one-to-one, and $W = \langle \varphi_1(V), \ldots, \varphi_n(V) \rangle$.*

(ii) *The trivial and total subspaces of V are closed.*

Definition 5.2. Let i, j, k be integers, $i \leq i < j \leq n$, $i \leq k \leq n$. We let $\pi_{ji} \colon V \to \langle [x_j, x_i] \rangle$ and $\pi_{jik} \colon W \to \langle [x_j, x_i, x_k] \rangle$ be the canonical projections. For $1 \leq i \leq n$, we let Π_i be the canonical projection from V to the subspace spanned by all $[x_i, x_k]$ and $[x_j, x_i]$, with $1 \leq k < i < j \leq n$.

Lemma 5.3. *Let $\mathbf{w} \in \varphi_k(V)$. If $\pi_{rst}(\mathbf{w}) \neq \mathbf{0}$, with $1 \leq s < r \leq n$, $s \leq t \leq n$, then $s \leq k \leq t$, and at most one of the inequalities is strict.*

Proof. It is enough to prove the result for $\mathbf{w}$ an element of a basis of $\varphi_k(V)$. Such a basis is given by the vectors $[x_j, x_i, x_k]$ with $1 \leq i < j \leq n$, $i \leq k \leq n$, and the vectors $[x_j, x_k, x_i] - [x_i, x_k, x_j]$ with $1 \leq i < j \leq n$ and $1 \leq k < i$. Considering these basis vectors, we see that the first class has $r = j$, $s = i$, $t = k$, so $s \leq k = t$. The second class of vectors will yield either $r = j$, $s = k$, $t = i$, with $s = k < t$; or else $r = i$, $s = k$, $t = j$, with $s = k < t$. This proves the lemma. □

Lemma 5.4. *Let i, j be integers, $1 \leq i < j \leq n$, and r an integer such that $1 \leq r \leq n$. For $\mathbf{v} \in V$, $\pi_{jij}(\varphi_r(\mathbf{v})) \neq \mathbf{0}$ if and only if $\pi_{ji}(\mathbf{v}) \neq \mathbf{0}$ and $r = j$. Likewise, $\pi_{jii}(\varphi_r(\mathbf{v})) \neq \mathbf{0}$ if and only if $\pi_{ji}(\mathbf{v}) \neq \mathbf{0}$ and $r = i$.*

Proof. The vectors $[x_j, x_i, x_j]$ occurs in the image of a φ_r exactly when $r = j$ and it is applied a vector with nontrivial π_{ji} projection. Thus, if $\pi_{jij}(\mathbf{v}) \neq \mathbf{0}$ then $\pi_{ji}(\mathbf{v}) \neq \mathbf{0}$. The converse is immediate, and the case of π_{jii} is settled in the same manner. □

Lemma 5.5. *Fix i, j, $1 \leq i < j \leq n$. If $\pi_{ji}(X) = \{\mathbf{0}\}$, then $\pi_{ji}(X^{**}) = \{\mathbf{0}\}$.*

Proof. Since $\pi_{ji}(X) = \{\mathbf{0}\}$, it follows that $\pi_{jii}(X^*) = \{\mathbf{0}\}$ by Lemma 5.3. Therefore, if $\mathbf{v} \in V$ has $\pi_{ji}(\mathbf{v}) \neq \mathbf{0}$ then $\varphi_i(\mathbf{v}) \notin X^*$, hence $\mathbf{v} \notin X^{**}$. □

We will now proceed to establish our main result. The idea is the following: given a subspace X of V, we will find a lower bound for the dimension of X^* in terms of n and the dimension of X. If all subspaces X' of V of dimension strictly larger than that of X yield subspaces X'^* of dimension strictly larger than $\dim(X^*)$, then it will follow that X must be closed since $X^* = (X^{**})^*$. In order to establish these bounds, we will consider the images $\varphi_1(X)$, $\varphi_2(X), \ldots, \varphi_n(X)$; since each φ_i is one-to-one, the dimension of X^* will depend on how much "overlap" there is among these subspaces of W.

Lemma 5.6. *Fix $n > 1$, and let i and j be integers, $1 \leq i < j \leq n$. Then $\varphi_i(V) \cap \varphi_j(V) = \{\mathbf{0}\}$.*

Proof. Let $\varphi_i(\mathbf{v}) \in \varphi_j(V)$, and assume that $\pi_{sr}(\mathbf{v}) \neq \mathbf{0}$, $1 \leq r < s \leq n$. If $r \leq i$, then $\pi_{sri}(\varphi_i(\mathbf{v})) \neq \mathbf{0}$, and since $\varphi_i(\mathbf{v}) \in \varphi_j(V)$, Lemma 5.3 implies $r \leq j \leq i$, contradicting the choice of i and j. If $i < r$, then $\pi_{sir}(\varphi_i(\mathbf{v})) \neq \mathbf{0}$. By Lemma 5.3, we must have $i < j = r$. We also have $\pi_{ris}(\varphi_i(\mathbf{v})) \neq \mathbf{0}$, and since $\varphi_i(\mathbf{v}) \in \varphi_j(V)$, this time we deduce $i < j = s$. But then we have $j = r = s$, and this is impossible. Thus, $\pi_{sr}(\mathbf{v}) = \mathbf{0}$ for all $1 \leq r < s \leq n$. □

Lemma 5.7. *Fix $n > 1$ and $r \leq n$. Let $i_1, \ldots, i_r$ be pairwise distinct integers, $1 \leq i_1, \ldots, i_r \leq n$. Then $\varphi_{i_1}^{-1}\bigl(\bigl\langle \varphi_{i_2}(V), \ldots, \varphi_{i_r}(V)\bigr\rangle\bigr)$ is of dimension $\binom{r-1}{2}$, with basis given by the vectors $[x_a, x_b]$, with $a, b \in \{i_2, \ldots, i_r\}$, $b < a$. In particular, the intersection $\varphi_{i_1}(V) \cap \bigl\langle \varphi_{i_2}(V), \ldots, \varphi_{i_r}(V)\bigr\rangle$ has a basis made up of* *vectors of the form* $[x_a, x_b, x_{i_1}]$ *with* $a, b \in \{i_2, \ldots, i_r\}$, $b < a$ *and* $b < i_1$*; and vectors of the form* $[x_a, x_{i_1}, x_b] - [x_b, x_{i_1}, x_a]$, *with* $a, b \in \{i_2, \ldots, i_r\}$, $i_1 < b < a$.

Proof. By Proposition 4.3, it is enough to consider the case where $i_1 = 1$. Let A denote the pullback described in the statement.

Given $a, b \in \{i_2, \ldots, i_r\}$, $a > b$, we have $[x_a, x_b] \in A$:

$$\begin{aligned}\varphi_{i_1}([x_a, x_b]) &= [x_a, x_{i_1}, x_b] - [x_b, x_{i_1}, x_a]\\ &= \varphi_b([x_a, x_{i_1}]) - \varphi_a([x_b, x_{i_1}]) \in \langle \varphi_{i_2}(V), \ldots, \varphi_{i_r}(V)\rangle.\end{aligned}$$

Conversely, let $\mathbf{v} \in A$, and a, b be integers, $1 \leq b < a \leq n$, such that $\pi_{ab}(\mathbf{v}) \neq \mathbf{0}$. We can write

$$\varphi_{i_1}(\mathbf{v}) = \varphi_{i_2}(\mathbf{v}_2) + \cdots + \varphi_{i_r}(\mathbf{v}_r).$$

Since $i_1 = 1$, $\pi_{a1b}(\varphi_{i_1}(\mathbf{v})) = -\pi_{b1a}(\varphi_{i_1}(\mathbf{v})) \neq \mathbf{0}$, and therefore we must have $\pi_{a1b}(\varphi_{i_j}(\mathbf{v}_j)) \neq \mathbf{0}$ for some $j \geq 2$. This implies $1 \leq i_j \leq b$, with at most one inequality strict by Lemma 5.3. Since $1 = i_1 \neq i_j$, we have $i_j = b$. Considering π_{b1a} instead, we deduce that $a = i_k$ for some $k \geq 2$, so $a, b \in \{i_2, \ldots, i_r\}$. Therefore, $A \subseteq \langle [x_a, x_b] \mid a, b \in \{i_2, \ldots, i_r\}, a > b\rangle$. This proves equality.

Since the vectors described are linearly independent, they form a basis. Mapping them via φ_{i_1}, which is one-to-one, proves the final clause. □

Corollary 5.8. *Let* $n > 1$, $r \leq n$, *and let* $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ *be integers. Then*

$$\dim\left(\langle \varphi_{i_1}(V), \ldots, \varphi_{i_r}(V)\rangle\right) = r\binom{n}{2} - \binom{r}{3}.$$

Proof. For simplicitly, let $Y = \langle \varphi_{i_1}(V), \ldots, \varphi_{i_r}(V)\rangle$. We have:

$$\begin{aligned}\dim(Y) &= \left(\sum_{k=1}^{r} \dim(\varphi_{i_k}(V))\right) - \left(\sum_{k=2}^{r} \dim\Big(\varphi_{i_k}(V) \cap \big\langle \varphi_{i_1}(V), \ldots, \varphi_{i_{k-1}}(V)\big\rangle\Big)\right)\\ &= r\binom{n}{2} - \left(\sum_{k=2}^{r} \binom{k-1}{2}\right) = r\binom{n}{2} - \binom{r}{3},\end{aligned}$$

as claimed. □

Definition 5.9. Fix $n > 1$. We define $\Phi : V^n \to W$ to be

$$\Phi(\mathbf{v}_1, \ldots, \mathbf{v}_n) = \varphi_1(\mathbf{v}_1) + \cdots + \varphi_n(\mathbf{v}_n).$$

If there is danger of ambiguity, we use Φ_n to denote the map associated to the spaces corresponding to the particular choice of n.

Note that if X is a subspace of V, then $\Phi(X^n) = X^*$.

The following proposition essentially says that the only overlaps in the maps $F_2 \to F_3$ given by $\mathbf{v} \mapsto [\mathbf{v}, \mathbf{u}]$ are consequences of the Hall–Witt identity.

Proposition 5.10. *The kernel of Φ is of dimension $\binom{n}{3}$. A basis for $\ker(\Phi)$ is given as follows: each choice of integers a, b, c, $1 \leq a < b < c \leq n$, gives an element $(\mathbf{v}_1, \ldots, \mathbf{v}_n) \in V^n$ of the basis, with:*

$$\mathbf{v}_i = \begin{cases} [x_c, x_b] & \text{if } i = a, \\ -[x_c, x_a] & \text{if } i = b, \\ [x_b, x_a] & \text{if } i = c, \\ \mathbf{0} & \text{otherwise.} \end{cases}$$

Proof. Denote the element corresponding to $a < b < c$ by $\mathbf{v}_{(abc)}$. Note that $\mathbf{v}_{(abc)}$ is in $\ker(\Phi)$:

$$\begin{aligned} \Phi(\mathbf{v}_{(abc)}) &= \varphi_a([x_c, x_b]) + \varphi_b(-[x_c, x_a]) + \varphi_c([x_b, x_a]) \\ &= [x_c, x_a, x_b] - [x_b, x_a, x_c] - [x_c, x_a, x_b] + [x_b, x_a, x_c] = \mathbf{0}. \end{aligned}$$

Since Φ is surjective, $\dim(W) = n\dim(V) - \dim(\ker(\Phi))$, hence

$$\dim(\ker(\Phi)) = n\binom{n}{2} - 2\binom{n+1}{3} = \binom{n}{3},$$

so the proposition will be established in full if we prove that the elements $\mathbf{v}_{(abc)}$ of V^n are linearly independent.

Let $\sum \beta_{abc}\mathbf{v}_{(abc)} = (\mathbf{0}, \ldots, \mathbf{0})$ be a linear combination equal to zero. If we look at the ith coordinate of these n-tuples, we have:

$$\sum_{1\leq r<s<i\leq n} \beta_{rsi}[x_s, x_r] - \sum_{1\leq r<i<s\leq n} \beta_{ris}[x_s, x_r] + \sum_{1\leq i<r<s\leq n} \beta_{irs}[x_s, x_r] = \mathbf{0}.$$

Each basis vector $[x_s, x_r]$ occurs only once. Thus, if $i \in \{a, b, c\}$, then $\beta_{abc} = 0$. This holds for each choice of i, hence $\beta_{abc} = 0$ for all choices of a, b, c. This proves the $\mathbf{v}_{(abc)}$ are linearly independent. □

Theorem 5.11. *Let $(\mathbf{v}_1, \ldots, \mathbf{v}_n) \in \ker(\Phi)$. Write*

$$\mathbf{v}_k = \sum_{1\leq i<j\leq n} \alpha_{ji}^{(k)}[x_j, x_i], \quad \alpha_{ij}^{(k)} \in \mathbb{F}_p.$$

(i) *If* $i = k$ *or* $j = k$, *then* $\alpha_{ji}^{(k)} = 0$; *i.e.*, $\Pi_k(\mathbf{v}_k) = \mathbf{0}$.

(ii) *If* $1 \leq a < b < c \leq n$, *then* $\alpha_{ba}^{(c)} = \alpha_{cb}^{(a)} = -\alpha_{ca}^{(b)}$.

(iii) *Fix* i, j, $1 \leq i < j \leq n$. *Then*

$$\begin{aligned}
\Pi_i(\mathbf{v}_j) &= \sum_{r=1}^{i-1} \left(-\alpha_{jr}^{(i)}\right)[x_i, x_r] + \sum_{r=i+1}^{j-1} \alpha_{jr}^{(i)}[x_r, x_i] + \sum_{r=j+1}^{n} \left(-\alpha_{rj}^{(i)}\right)[x_r, x_i],\\
\Pi_j(\mathbf{v}_i) &= \sum_{r=1}^{i-1} \left(-\alpha_{ir}^{(j)}\right)[x_j, x_r] + \sum_{r=i+1}^{j-1} \alpha_{ri}^{(j)}[x_j, x_r] + \sum_{r=j+1}^{n} \left(-\alpha_{ri}^{(j)}\right)[x_r, x_j].
\end{aligned}$$

Proof. Part (i) holds for the basis elements described in Proposition 5.10, hence holds for all vectors in the kernel. For (ii), note that if $1 \leq a < b < c \leq n$, then

$$\begin{aligned}
\pi_{bac}\big(\varphi_1(\mathbf{v}_1) + \cdots + \varphi_n(\mathbf{v}_n)\big) &= \left(\alpha_{ba}^{(c)} - \alpha_{cb}^{(a)}\right)[x_b, x_a, x_c],\\
\pi_{cab}\big(\varphi_1(\mathbf{v}_1) + \cdots + \varphi_n(\mathbf{v}_n)\big) &= \left(\alpha_{ca}^{(b)} + \alpha_{cb}^{(a)}\right)[x_c, x_a, x_b].
\end{aligned}$$

Since both are equal to zero, we deduce that $\alpha_{ba}^{(c)} = \alpha_{cb}^{(a)}$ and $\alpha_{ca}^{(b)} = -\alpha_{cb}^{(a)}$. Finally, for (iii), we know that $\Pi_i(\mathbf{v}_i) = \Pi_j(\mathbf{v}_j) = \mathbf{0}$ from (i), so we can write:

$$\begin{aligned}
\Pi_i(\mathbf{v}_j) &= \sum_{r=1}^{i-1} \alpha_{ir}^{(j)}[x_i, x_r] + \sum_{r=i+1}^{j-1} \alpha_{ri}^{(j)}[x_r, x_i] + \sum_{r=j+1}^{n} \alpha_{ri}^{(j)}[x_r, x_i],\\
\Pi_j(\mathbf{v}_i) &= \sum_{r=1}^{i-1} \alpha_{jr}^{(i)}[x_j, x_r] + \sum_{r=i+1}^{j-1} \alpha_{jr}^{(i)}[x_j, x_r] + \sum_{r=j+1}^{n} \alpha_{rj}^{(i)}[x_r, x_j],
\end{aligned}$$

and applying (ii) gives the desired identities. □

Corollary 5.12. *Let* $\mathbf{v} \in \ker(\Phi)$. *If* $\Pi_j(\mathbf{v}_i) = \mathbf{0}$, *then* $\Pi_i(\mathbf{v}_j) = \mathbf{0}$. *In particular, if* $\mathbf{v}_i = \mathbf{0}$, *then* $\Pi_i(\mathbf{v}_j) = \mathbf{0}$ *for all* j.

Proof. The second assertion follows immediately from the first. The first assertion is trivial if $i = j$; and if $i \neq j$, then $\alpha_{jr}^{(i)} = 0$ for all $r < j$ and $\alpha_{rj}^{(i)} = 0$ for $j < r$, so by Theorem 5.11(iii) it follows that $\Pi_i(\mathbf{v}_j) = \mathbf{0}$. □

Corollary 5.13. *Let* $\mathbf{v} \in \ker(\Phi)$, $\mathbf{v} \neq (\mathbf{0}, \ldots, \mathbf{0})$. *If* $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ *then the dimension of* $\langle \mathbf{v}_1, \ldots, \mathbf{v}_n \rangle$ *is at least* 3.

Proof. Write

$$\mathbf{v} = \sum_{1\leq a<b<c\leq n} \beta_{abc}\mathbf{v}_{(abc)}.$$

Fix a, b, c such that $1 \leq a < b < c \leq n$, $\beta_{abc} \neq 0$. We claim that $\mathbf{v}_a$, $\mathbf{v}_b$, and $\mathbf{v}_c$ are linearly independent. Indeed, note that $\Pi_a(\mathbf{v}_a) = \Pi_b(\mathbf{v}_b) = \Pi_c(\mathbf{v}_c) = \mathbf{0}$, and $\pi_{cb}(\mathbf{v}_a) \neq \mathbf{0}$. Therefore, if $\alpha_a\mathbf{v}_a + \alpha_b\mathbf{v}_b + \alpha_c\mathbf{v}_c = \mathbf{0}$, then we must have $\alpha_a = 0$. A symmetric argument looking at π_{ca} shows that $\alpha_b = 0$, and considering π_{ba} shows that $\alpha_c = 0$. □

Corollary 5.14. *Fix $n>1$, and let X be a subspace of V. If $\dim(X)=1$, then $\dim(X^*) = n$; if $\dim(X) = 2$, then $\dim(X^*) = 2n$. That is, if $\dim(X) \leq 2$, then $X^n \cap \ker(\Phi) = \{\mathbf{0}\}$.*

Proof. We prove the contrapositive.

Since $\dim(X^*) = n\dim(X) - \dim(X^n \cap \ker(\Phi))$, if $\dim(X^*) < n\dim(X)$, then $X^n \cap \ker(\Phi) \neq \{\mathbf{0}\}$.

Let $\mathbf{v} = (\mathbf{v}_1, \ldots, \mathbf{v}_n) \in X^n \cap \ker(\Phi)$, $\mathbf{v} \neq \mathbf{0}$. Then $\mathbf{v}_i \in X$ for $i = 1, \ldots, n$, so by Corollary 5.13, $\dim(X) \geq 3$, as claimed. □

We now proceed along the lines outlined above; the first proposition makes the conclusion depend on X, and the second only on $\dim(X)$ (though with a stronger hypothesis).

Proposition 5.15. *Let $X < V$. Assume that for all subspaces Y of V, if Y properly contains X then Y^* properly contains X^*. Then $X = X^{**}$.*

Proof. If X^{**} properly contains X, then X^{***} would properly contain X^*. But $X^{***} = X^*$, a contradiction. □

Proposition 5.16. *Let $n > 1$ and let m be an integer with $0 < m < \binom{m}{2}$. If for every subspaces $X, Y < V(n)$ with $\dim(X) = m$ and $\dim(Y) = m+1$ we have $\dim(X^*) < \dim(Y^*)$, then X is closed.*

We are therefore searching for a function $f(k,n)$, for k with $1 \leq k \leq \binom{n}{2}$, such that for all $Y < V(n)$, if $\dim(Y) = k$ then $\dim(Y^*) \geq nk - f(k,n)$. That is:

$$f(k,n) = \max\bigl\{\dim(X^n \cap \ker(\Phi_n)) \mid X < V,\ \dim(X) = k\bigr\}.$$

Our objective is to find an expression for $f(k,n)$ in terms of k and n; in fact, it turns out that the value is independent of n. The main workhorse in our calculations is Lemma 5.18 below. The idea is to find $\dim(X^n \cap \ker(\Phi_n))$ by examining the "partial intersections"; namely, the intersections of the form

$$\bigl\langle(\mathbf{0}, \ldots \mathbf{0}, \mathbf{v}_i, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) \mid \mathbf{v}_j \in X\bigr\rangle \bigcap \ker(\Phi_n),$$

as i ranges from 1 to $n-2$ (when $i=n-1$ or $i=n$, the intersection is trivial by Corollary 5.13). For a fixed i, we can consider the subspace of X consisting of all vectors $\mathbf{v}_i$ which can be "completed" to an element of $\ker(\Phi)$ by taking and n-tuple with $i-1$ copies of $\mathbf{0}$, followed by $\mathbf{v}_i$, followed by some vectors in X; this is the same as considering the pullbacks $X \cap \varphi_i^{-1}(\langle \varphi_{i+1}(X), \ldots, \varphi_n(X)\rangle)$. It is easy to verify that the sum of the dimensions of these pullbacks is equal to the dimension of $X^n \cap \ker(\Phi_n)$. We will first use the dimension of these pullbacks to establish a lower bound for the dimension of X; then we will turn around and use these calculations to give an upper bound for the dimension of the pullbacks in terms of the dimension of X.

Making the bounds as precise as possible, however, requires one to keep track of a lot of information; this in turn requires the use of multiple indices and subindices in the proof, for which I apologize in advance. To illustrate the ideas and help the reader navigate through the proof, we will first present an illustration. This is not an example in the sense of a specific X, but rather a run-through the main part of the analysis we will perform below, but with specific values for some of the indices and some of the variables to make it more concrete and easier to digest.

Example 5.17. Set $n=6$, and let X be a subspace of V. We will be interested in bounding above the dimension of Z_i in terms of $\dim(X)$, where

$$Z_i = X \cap \varphi_i^{-1}\big(\langle \varphi_{i+1}(X), \ldots, \varphi_6(X)\rangle\big);$$

i.e., Z_i consists of all $\mathbf{v} \in X$ for which there exist $\mathbf{v}_{i+1}, \ldots, \mathbf{v}_6$ in X such that

$$(\mathbf{0}, \ldots, \mathbf{0}, \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_6) \in X^6 \cap \ker(\Phi_6).$$

To do this, we will obtain a lower bound for $\dim(X)$ in terms of $\dim(Z_i)$. To further fix ideas, set $i=2$. Note that by Theorem 5.11(i) and (ii), we must have $\Pi_1(Z_2) = \Pi_2(Z_2) = \mathbf{0}$. Order all pairs (j,i) lexicographically from right to left, so $(j,i) < (b,a)$ if and only if $i<a$, or $i=a$ and $j<b$. Doing Gaussian elimination, we can find a basis $\mathbf{v}_{1,2}$, $\mathbf{v}_{2,2}, \ldots, \mathbf{v}_{k,2}$ for Z_2 (the second index refers to the fact that these vectors are in the second component of an element of $\ker(\Phi_6)$), satisfying that the "leading pair" (smallest nonzero component) of each is strictly smaller than that of its successors, and all other vectors have zero component for that pair. For example, suppose that $\dim(Z_2)=4$, and that the basis has the form:

$$\mathbf{v}_{1,2} = [x_4,x_3] + \alpha_1[x_5,x_3] + \alpha_2[x_6,x_4], \qquad \mathbf{v}_{3,2} = [x_5,x_4] + \gamma[x_6,x_4],$$

$$\mathbf{v}_{2,2} = [x_6, x_3] + \beta[x_6, x_4], \qquad \mathbf{v}_{4,2} = [x_6, x_5],$$

for some coefficients $\alpha_1, \alpha_2, \beta, \gamma \in \mathbb{F}_p$. We know there exist vectors $\mathbf{v}_{i,3}$, $\mathbf{v}_{i,4}$, $\mathbf{v}_{i,5}$, $\mathbf{v}_{i,6}$ such that $(\mathbf{0}, \mathbf{v}_{i,2}, \mathbf{v}_{i,3}, \mathbf{v}_{i,4}, \mathbf{v}_{i,5}, \mathbf{v}_{i,6}) \in X^6 \cap \ker(\Phi_6)$ for $i = 1, 2, 3, 4$. Naturally, X contains all twenty vectors, but there will normally be some linear dependencies between them: some may even be equal to $\mathbf{0}$. We want to extract, in some systematic manner, a subset that we can guarantee is linearly independent. First let us consider the information we can obtain about these vectors from our knowledge of the vectors $\mathbf{v}_{i,2}$.

Since $(\mathbf{0}, \mathbf{v}_{i,2}, \mathbf{v}_{i,3}, \mathbf{v}_{i,4}, \mathbf{v}_{i,5}, \mathbf{v}_{i,6})$ lies in $\ker(\Phi)$, we can use Theorem 5.11(iii) to describe the Π_k-image of each vector $\mathbf{v}_{i,j}$, where $k \leq 2$ and $j > 2$. The Π_1-image must be trivial, and for the Π_2 image we obtain the following:

$$\begin{aligned}
\Pi_2(\mathbf{v}_{1,3}) &= [x_4, x_2] + \alpha_1[x_5, x_2], & \Pi_2(\mathbf{v}_{2,3}) &= [x_6, x_2],\\
\Pi_2(\mathbf{v}_{1,4}) &= -[x_3, x_2] + \alpha_2[x_6, x_2], & \Pi_2(\mathbf{v}_{2,4}) &= \beta[x_6, x_2],\\
\Pi_2(\mathbf{v}_{1,5}) &= -\alpha_1[x_3, x_2], & \Pi_2(\mathbf{v}_{2,5}) &= \mathbf{0},\\
\Pi_2(\mathbf{v}_{1,6}) &= -\alpha_2[x_4, x_2]. & \Pi_2(\mathbf{v}_{2,6}) &= -[x_3, x_2] - \beta[x_4, x_2].
\end{aligned}$$

$$\begin{aligned}
\Pi_2(\mathbf{v}_{3,3}) &= \mathbf{0}, & \Pi_2(\mathbf{v}_{4,3}) &= \mathbf{0},\\
\Pi_2(\mathbf{v}_{3,4}) &= [x_5, x_2] + \gamma[x_6, x_2], & \Pi_2(\mathbf{v}_{4,4}) &= \mathbf{0},\\
\Pi_2(\mathbf{v}_{3,5}) &= -[x_4, x_2], & \Pi_2(\mathbf{v}_{4,5}) &= [x_6, x_2],\\
\Pi_2(\mathbf{v}_{3,6}) &= -\gamma[x_4, x_2] & \Pi_2(\mathbf{v}_{4,6}) &= -[x_5, x_2].
\end{aligned}$$

One way to obtain these without too much confusion is as follows: to find $\Pi_2(\mathbf{v}_{j,k})$, go through the expression for $\mathbf{v}_{j,2}$ replacing all indices k by 2, remembering that $[x_a, x_b] = -[x_b, x_a]$. Any $[x_b, x_a]$ in which neither a nor b are equal to k are simply removed.

To extract systematically a set of linearly independent vectors, we proceed in the following manner: consider all the pairs which correspond to leading terms of the basis vectors $\mathbf{v}_{i,2}$; in this case, $(4, 3)$, $(6, 3)$, $(5, 4)$, and $(6, 5)$. The individual indices that occur are 3, 4, 5, and 6. For each of them, we identify the smallest pair in which it occurs. Thus, 3 first occurs in pair number one, as does 4. The index 5 first occurs in pair number three, and 6 first occurs in pair number two.

Since the first pair in which 3 appears is the *first* pair (corresponding to the first basis vectors $\mathbf{v}_{1,2}$), which is $(4, 3)$ where it is paired with 4, we will select the vector $\mathbf{v}_{1,4}$; this vector has first nontrivial term corresponding to $(3, 2)$. The next index is 4, again in the *first* pair, paired with 3; so this time we select $\mathbf{v}_{1,3}$. This has nontrivial $(4,2)$ component, and trivial (j,i) component for all $(j,i) < (4,2)$.

The next index is 5, which first occurs in the third pair (corresponding to $\mathbf{v}_{3,2}$) paired with 4. So we select $\mathbf{v}_{3,4}$, a vector with trivial (j,i) component for all $(j,i) < (5,2)$, and nontrivial $(5,2)$ component. Next we go to the index 6, that first occurs in the second pair together with 3; so we select the vector $\mathbf{v}_{2,3}$, a vector with nontrivial $(6,2)$ component, and trivial (j,i) component for all $(j,i) < (6,2)$.

In summary, we want to consider our original basis vectors $\mathbf{v}_{1,2}$, $\mathbf{v}_{2,2}$, $\mathbf{v}_{3,2}$, and $\mathbf{v}_{4,2}$, plus the vectors we have selected based on the location of the indices, to wit the vectors $\mathbf{v}_{1,4}, \mathbf{v}_{1,3}, \mathbf{v}_{3,4}, \mathbf{v}_{2,3}$ corresponding, respectively, to the indices 3, 4, 5, and 6. The choices we have made ensure that the Π_2-images of these latter four vectors are linearly independent, and so the vectors themselves must be linearly independent. Since $\Pi_2(Z_2) = \mathbf{0}$, the full collection of eight vectors is linearly independent, and so we can conclude that X must have dimension at least 8.

What is more, note that none of the four vectors $\mathbf{v}_{1,4}$, $\mathbf{v}_{1,3}$, $\mathbf{v}_{3,4}$, and $\mathbf{v}_{2,3}$ will occur in a similar analysis involving Z_3 (or more generally Z_k with $k > 2$): when performing a similar analysis, all vectors will have trivial Π_k-image when $k < 3$, and these vectors have nontrivial Π_2-image. Note as well that the number of indices, in this case 4, must satisfy $\dim(Z_2) \leq \binom{4}{2}$, since we need to be able to obtain at least $\dim(Z_2)$ pairs out of the indices that occur.

Thus we have seen that if $\dim(Z_2) = 4$, then $\dim(X) \geq 8$. If we move on to Z_3, we will obtain new vectors that must lie in X; while the vectors in the basis for Z_2 may again occur in that analysis, the vectors $\mathbf{v}_{1,4}$, $\mathbf{v}_{1,3}$, $\mathbf{v}_{3,4}$, and $\mathbf{v}_{2,3}$ will not, and so by keeping track of them we can give an even better lower bound for $\dim(X)$. □

What ensures that this process will work the way we want is how we choose the vectors of the basis and the vectors that "correspond" to each index. The former count towards the value of $\dim(X^n \cap \ker(\Phi_n))$, while the latter may be removed from consideration when we move on to Z_{i+1}. This is all done in generality in the proof of the following promised lemma:

Lemma 5.18. *Fix $n > 1$, and let X be a subspace of V. For each i, $1 \leq i \leq n$, let*

$$Z_i = X \cap \varphi_i^{-1}\bigl(\langle \varphi_{i+1}(X), \ldots, \varphi_n(X)\rangle\bigr);$$

i.e., Z_i consists of all $\mathbf{v} \in X$ for which there exist $\mathbf{v}_{i+1}, \ldots, \mathbf{v}_n$ in X such that

$$(\mathbf{0}, \ldots, \mathbf{0}, \mathbf{v}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n) \in X^n \cap \ker(\Phi).$$

If $\dim\bigl(X \cap \langle [x_s, x_r] \mid i \leq r < s \leq n\rangle\bigr) = d_i$ *and* $\dim(Z_i) = r_i$, *then* $r_i \leq \binom{d_i - r_i}{2}$. *Morevoer, if* s_i *is the smallest positive integer such that* $r_i \leq \binom{s_i}{2}$, *then we must have* $d_{i+1} \leq d_i - s_i$.

Proof. Fix i_0, $1 \leq i_0 \leq n$. For simplicity, write $r = r_{i_0}$. By Theorem 5.11, if $\mathbf{v} \in Z_{i_0}$ then $\Pi_i(\mathbf{v}) = \mathbf{0}$ for all $i \leq i_0$.

Let $\mathbf{v}_{1i_0}, \ldots, \mathbf{v}_{ri_0}$ be a basis for Z_{i_0}. We will modify it as follows:

Order all pairs (j,i), $i_0 < i < j \leq n$ by letting $(j,i) < (b,a)$ if and only if $i < a$ or $i = a$ and $j < b$ (lexicographically from right to left). Let (j_1, i_1) be the smallest pair for which $\pi_{j_1 i_1}(\mathbf{v}_{ki_0}) \neq \mathbf{0}$ for some k, $1 \leq k \leq r$. Reordering if necessary we may assume $k = 1$. Replacing $\mathbf{v}_{1i_0}$ with a scalar multiple of itself and adding adequate multiples to the remaining $\mathbf{v}_{ki_0}$ if necessary we may also assume that

$$\pi_{j_1 i_1}(\mathbf{v}_{ki_0}) = \begin{cases} [x_{j_1}, x_{i_1}] & \text{if } k = 1; \\ \mathbf{0} & \text{if } k \neq 1. \end{cases}$$

Let (j_2, i_2) be the smallest pair for which $\pi_{j_2 i_2}(\mathbf{v}_{ki_0}) \neq \mathbf{0}$ for some k with $2 \leq k \leq r$. Again we may assume $k = 2$, and that

$$\pi_{j_2 i_2}(\mathbf{v}_{ki_0}) = \begin{cases} [x_{j_2}, x_{i_2}] & \text{if } k = 2; \\ \mathbf{0} & \text{if } k \neq 2. \end{cases}$$

Proceeding in the same way for $k = 3, \ldots, r$, we obtain an ordered list of pairs $(j_1, i_1) < (j_2, i_2) < \cdots < (j_r, i_r)$ and a basis $\mathbf{v}_{1i_0}, \ldots, \mathbf{v}_{ri_0}$ such that

$$\pi_{j_\ell i_\ell}(\mathbf{v}_{ki_0}) = \begin{cases} [x_{j_\ell}, x_{i_\ell}] & \text{if } \ell = k, \\ \mathbf{0} & \text{if } \ell \neq k; \end{cases}$$

and such that $\pi_{ba}(\mathbf{v}_{ki_0}) = \mathbf{0}$ for all $(b,a) < (j_k, i_k)$. Write

$$\mathbf{v}_{ki_0} = \sum_{i_0 < i < j \leq n} \alpha_{ji}^{(k,i_0)} [x_j, x_i].$$

From the above we have:

$$\alpha_{ji}^{(k,i_0)} = \begin{cases} 1 & \text{if } (j,i) = (j_k, i_k), \\ 0 & \text{if } (j,i) < (j_k, i_k). \end{cases}$$

For $k = 1, \ldots, r$ and $i = i_0 + 1, \ldots, n$, let $\mathbf{v}_{ki}$ be vectors in X such that

$$(\mathbf{0}, \ldots, \mathbf{0}, \mathbf{v}_{ki_0}, \mathbf{v}_{ki_0+1}, \ldots, \mathbf{v}_{kn}) \in \ker(\Phi) \cap X^n.$$

By Theorem 5.11(iii) we have

$$\Pi_{i_0}\left(\mathbf{v}_{kj}\right) = \sum_{m=i_0+1}^{j-1} \alpha_{jm}^{(k,i_0)}[x_m, x_{i_0}] - \sum_{m=j+1}^{n} \alpha_{mj}^{(k,i_0)}[x_m, x_{i_0}].$$

For simplicity, set $\alpha_{ji}^{(k,i_0)} = -\alpha_{ij}^{(k,i_0)}$, and $\alpha_{jj}^{(k,i_0)} = 0$; then we can rewrite the above expression as:

$$\Pi_{i_0}\left(\mathbf{v}_{kj}\right) = \sum_{m=i_0+1}^{n} \alpha_{jm}^{(k,i_0)}[x_m, x_{i_0}]. \tag{5.19}$$

Let s be the cardinality of the set $\{i_1, j_1, \ldots, i_r, j_r\}$; that is, s is the number of distinct indices that occur in the list $(j_1, i_1), \ldots, (j_r, i_r)$. Note that $r \leq \binom{s}{2}$. Let $a_1 < a_2 < \cdots < a_s$ be the list of these distinct indices. For each ℓ with $1 \leq \ell \leq s$, let $(j_{k(\ell)}, i_{k(\ell)})$ be the smallest pair among $(j_1, i_1), \ldots, (j_r, i_r)$ that has $a_\ell \in \{i_{k(\ell)}, j_{k(\ell)}\}$. If $a_\ell = i_{k(\ell)}$, let $b_\ell = j_{k(\ell)}$; if $a_\ell = j_{k(\ell)}$, let $b_\ell = i_{k(\ell)}$. Consider the following list of vectors from X:

$$\mathbf{v}_{1i_0}, \mathbf{v}_{2i_0}, \ldots, \mathbf{v}_{ri_0}, \mathbf{v}_{k(1)b_1}, \mathbf{v}_{k(2)b_2}, \ldots, \mathbf{v}_{k(s)b_s}.$$

Note that all of these vectors lie in $X \cap \langle [x_j, x_i] \mid i_0 \leq i < j \leq n \rangle$. We will show that these vectors are linearly independent. Since $\mathbf{v}_{1i_0}, \ldots, \mathbf{v}_{ri_0}$ are linearly independent and $\Pi_{i_0}(\mathbf{v}_{ki_0}) = \mathbf{0}$ for $k = 1, \ldots, r$, it suffices to show that $\Pi_{i_0}(\mathbf{v}_{k(1)b_1}), \ldots, \Pi_{i_0}(\mathbf{v}_{k(s)b_s})$ are linearly independent.

First, from (5.19) we have $\pi_{a_\ell i_0}(\mathbf{v}_{k(m)b_m}) = \alpha_{b_m a_\ell}^{(k(m),i_0)}$. We claim that if $\ell < m$, then $\alpha_{b_m a_\ell}^{(k(m),i_0)} = 0$. By construction, this claim will follow if we can show that either $a_\ell = b_m$, or else the pair made up of b_m and a_ℓ is strictly smaller than the pair made up of a_m and b_m (which is equal to $(j_{k(m)}, i_{k(m)})$); the claim will then follow because $\alpha_{ba}^{(k,i_0)} = 0$ whenever $(b, a) < (j_k, i_k)$. Indeed, we know that $a_\ell < a_m$. If $a_m = i_{k(m)}$ and $b_m = j_{k(m)}$, then replacing a_m in the pair (b_m, a_m) with something smaller (namely a_ℓ) gives a smaller pair: $(b_m, a_\ell) < (b_m, a_m)$. If, on the other hand, we have $a_m = j_{k(m)}$ and $b_m = i_{k(m)}$, then if $a_\ell > b_m$ we have $(a_\ell, b_m) < (a_m, b_m)$, and if $a_\ell < b_m$ then we also have $(b_m, a_\ell) < (a_m, b_m)$. The only remaining possibility is $a_\ell = b_m$, which is of course no trouble.

Thus, we conclude that $\alpha_{b_m a_\ell}^{k(m),i_0} = 0$ whenever $\ell < m$. To see that the vectors $\Pi_2(\mathbf{v}_{k(1)b_1}), \ldots, \Pi_2(\mathbf{v}_{k(s)b_s})$ are linearly independent, note that

$$\pi_{a_\ell i_0}\left(\mathbf{v}_{k(m)b_m}\right) = \alpha_{b_m a_\ell}^{(k(m),i_0)}[x_{a_\ell}, x_{i_0}] = \begin{cases} \mathbf{0} & \text{if } \ \ell < m, \\ [x_{b_\ell}, x_{a_\ell}] & \text{if } \ m = \ell. \end{cases}$$

Therefore, if $\beta_1\Pi_{i_0}(\mathbf{v}_{k(1)b_1}) + \cdots + \beta_s\Pi_{i_0}(\mathbf{v}_{k(s)b_s}) = \mathbf{0}$, then $\beta_1 = 0$ since the only vector with nontrivial (a_1, i_0)-component is $\Pi_{i_0}(\mathbf{v}_{k(1)b_1})$. Hence $\beta_2 = 0$, because the only remaining vector with nontrivial (a_2, i_0)-component is $\Pi_{i_0}(\mathbf{v}_{k(2)b_2})$; and continuing this way we conclude $\beta_j = 0$ for all j. So the vectors are indeed linearly independent. Thus we have established that

$$\mathbf{v}_{1i_0}, \mathbf{v}_{2i_0}, \ldots, \mathbf{v}_{ri_0}, \mathbf{v}_{k(1)b_1}, \mathbf{v}_{k(2)b_2}, \ldots, \mathbf{v}_{k(s)b_s}$$

is a collection of linearly independent vectors in $X \cap \langle [x_s, x_r] \mid i_0 \leq r < s \leq n\rangle$.

Thus we conclude that $d_{i_0} \geq r + s$. Since $r \leq \binom{s}{2}$, it follows that

$$r \leq \binom{s}{2} \leq \binom{d_{i_0} - r}{2},$$

as claimed.

To complete the proof, it only remains to establish the upper bound on d_{i_0+1}. We have $d_{i_0} = d_{i_0+1} + \dim(\langle [x_j, x_i] \mid i_0 \leq i < j \leq n\rangle \cap \{\mathbf{v} \in X \mid \Pi_{i_0}(\mathbf{v}) \neq \mathbf{0}\})$. Since the vectors $\mathbf{v}_{k(1)b_1}, \ldots, \mathbf{v}_{k(s)b_s}$ are linearly independent, have nontrivial Π_{i_0} projection, and lie in $X \cap \langle [x_j, x_i] \mid i_0 \leq i < j \leq n\rangle$, we have $d_{i_0} \geq d_{i_0+1} + s$. Moreover, since $r \leq \binom{s}{2}$, we also have $s_{i_0} \leq s$; therefore, $d_{i_0+1} \leq d_{i_0} - s \leq d_{i_0} - s_{i_0}$, as desired. □

Note that Z_{n-1} and Z_n are always trivial. To match the computations above, we want to define $r(d)$, depending on d, to be the largest nonnegative integer such that $r(d) \leq d$ and $r(d) \leq \binom{d-r(d)}{2}$. Adding $r - r(d)$ to both sides of the latter inequality leads to the following definition:

Definition 5.20. Let d be a nonnegative integer. We define $r(d)$ to be the largest integer such that $r(d) \leq d \leq \binom{d-r(d)+1}{2}$.

The definition above makes it somewhat difficult to compute the function $r(d)$. After computing the first few values by hand, I consulted the On-line encyclopedia of integer sequences [16] and discovered that it was related to sequence A083920. This readily gives the following alternative descriptions, which are easy to establish:

Proposition 5.21 (cf. sequence A083920 in [16]). *Let d be a positive integer. Then $r(d)$ is the number of nontriangular numbers strictly less than d. Equivalently, if we write $d = \binom{t}{2} + s$, with $0 < s \leq t$, then $r(d) = \binom{t-1}{2} + (s-1)$; alternatively,*

$$r(d) = d - \left\lceil \frac{-1 + \sqrt{8d+1}}{2} \right\rceil$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x.

Definition 5.22. For $n > 0$ and integer m, $0 \leq m \leq \binom{n}{2}$, we let $f(m,n)$ denote the largest possible value of $\sum \dim(Z_k)$ for a subspace X of V with $\dim(X) = m$; equivalently,

$$f(m,n) = \max\bigl\{\dim(X^n \cap \ker(\Phi_n)) \mid X < V(n),\ \dim(X) = m\bigr\}.$$

Remark 5.23. As we will see below, the value of $f(m,n)$ does not depend on n; meaning that if $m \leq \binom{n}{2}$ and $n \leq N$, then $f(m,n) = f(m,N)$. It is easy to verify that $f(m,n) \leq f(m,N)$: if X is a subspace of $V(n)$ of dimension m, we can also consider it as a subspace of $V(N)$. If the dimension of X^* with respect to $\{\varphi_i\}_{i=1}^{n}$ is $nm - r$, then the dimension of X^* with respect to $\{\varphi_i\}_{i=1}^{N}$ is $Nm - r$; so we have

$$\dim(X^n \cap \ker(\Phi_n)) = \dim(X^N \cap \ker(\Phi_N)).$$

Intuitively, the reason the reverse inequality also holds is that the largest value of $f(m,n)$ occurs when the vectors in Z_i use fewer indices rather than more. Because more indices means a larger value of s in the proof of Lemma 5.18, which means more vectors are "taken out of circulation" for Z_{i+1}, which in turn yields a smaller possible value for $X \cap \langle v_{rs} \mid i < r < s < n\rangle$. So the "best" strategy for larger intersection with $\ker(\Phi_n)$ is to keep X confined to as small a number of indices as possible. The proof below will formalize this intuition, and show that indeed the value of f depends only on m.

Theorem 5.24. *Let $m > 0$, and write $m = \binom{T}{2} + s$, $0 \leq s \leq T$. If $m \leq \binom{n}{2}$, then*

$$f(m,n) = \binom{T}{3} + \binom{s}{2}.$$

Remark 5.25. Although there is some ambiguity in the expression for m, since $\binom{T}{2} + T = \binom{T+1}{2}$, note that the values $\binom{T}{3} + \binom{T}{2}$ and $\binom{T+1}{3} + \binom{0}{2}$ are equal, so the given value of $f(m)$ is well-defined.

Proof. By replacing $\binom{T+1}{2}$ with $\binom{T}{2} + T$ if necessary, we may assume $s > 0$. Note that we must have $T < n$. First we show that $f(m,n) \geq \binom{T}{3} + \binom{s}{2}$.

Let X be the m-dimensional coordinate subspace of $V(n)$ generated by all $[x_j, x_i]$ with $1 \leq i < j \leq T$, and the vectors $[x_{T+1}, x_1], \ldots, [x_{T+1}, x_s]$. Then X^* is the coordinate subspace of $W(n)$ generated by all vectors of the form $[x_j, x_i, x_k]$ with $1 \leq i < j \leq T$, $i \leq k \leq n$; plus the vectors of the form $[x_{T+1}, x_i, x_k]$ with $1 \leq i \leq s$, $i \leq k \leq n$. There are $2\binom{T+1}{2} + (n-T)\binom{n}{2}$ vectors of the first kind, and

$$n + (n-1) + (n-2) + \cdots + n - (s-1) = sn - \binom{s}{2}$$

of the second kind. Thus $\dim(X^*) = 2\binom{T+1}{2} + (n-T)\binom{T}{2} + sn - \binom{s}{2}$; and we have:

$$\begin{aligned} n\dim(X) - \dim(X^*) &= T\binom{T}{2} - 2\binom{T+1}{3} + \binom{s}{2} \\ &= (T-2)\binom{T}{2} - 2\binom{T}{3} + \binom{s}{2} = \binom{T}{3} + \binom{s}{2}. \end{aligned}$$

Therefore, $f(m,n) \geq \binom{T}{3} + \binom{s}{2}$.

For the reverse inequality, we will apply induction. Assume the result for any subspace X' of $V(n)$ with $\dim(X') < m$. Write $m = \binom{T}{2} + s$ with $0 < s \leq T$, and $T < n$, and let X be a subspace of V of dimension m. We want to show that $\sum \dim(Z_i)$ is bounded above by $\binom{T}{3} + \binom{s}{2}$. If all Z_i are trivial, this follows. Otherwise, assume i is the smallest index with nontrivial Z_i, and $\dim(Z_i) = k > 0$. Then $k \leq r(m)$, and if ℓ is the smallest positive integer such that $k \leq \binom{\ell}{2}$ then

$$\dim\bigl(X \cap \langle [x_s, x_r] \mid i < r < s \leq n \rangle\bigr) \leq m - \ell.$$

So the sum of the dimensions of the Z_j with $j > i$ is at most $f(m-\ell, n)$; that is, the sum over all k is bounded:

$$\sum \dim(Z_k) \leq k + f(m-\ell, n).$$

We want to show that $k + f(m-\ell,n) \leq \binom{T}{3} + \binom{s}{2}$ for all k and ℓ that satisfy the relevant conditions. It is easy to show that for $m = 1,2,3,4,$ and 5, all values of the form $k + f(m-\ell,n)$, $k \leq r(m)$ and ℓ as above are less than or equal to $\binom{T}{3} + \binom{s}{2}$.

If $\ell = T = m - r(m)$, then since $k \leq r(m)$ we have

$$\begin{aligned} k + f(m-\ell,n) &\leq r(m) + f(r(m),n) \\ &= \binom{T-1}{2} + (s-1) + f\left(\binom{T-1}{2} + (s-1), n\right) \\ &= \binom{T-1}{2} + (s-1) + \binom{T-1}{3} + \binom{s-1}{2} = \binom{T}{3} + \binom{s}{2}; \end{aligned}$$

If $\ell < T$, since $k \leq \binom{\ell}{2}$, it is enough to to show that for $1 < \ell < T$,

$$\binom{\ell}{2} + f(m-\ell,n) \leq \binom{T}{3} + \binom{s}{2}.$$

If $2 \leq \ell \leq s$, then:

$$\begin{aligned}\binom{\ell}{2} + f(m-\ell, n) &= \binom{\ell}{2} + f\left(\binom{T}{2} + (s-\ell), n\right)\\ &= \binom{\ell}{2} + \binom{T}{3} + \binom{s-\ell}{2} \leq \binom{T}{3} + \binom{s}{2}.\end{aligned}$$

The last inequality follows since $\binom{\ell}{2} + \binom{s-\ell}{2}$ is the number of two element subsets of $\{1, \ldots, s\}$, where either both elements are less than or equal to ℓ, or both strictly larger than ℓ.

If $s < \ell < T$, then write $\ell = s + a$, $a > 0$. We then have

$$m - \ell = \binom{T}{2} + s - (s+a) = \binom{T-1}{2} + (T-1-a),$$

so

$$\binom{\ell}{2} + f(m-\ell, n) = \binom{\ell}{2} + \binom{T-1}{3} + \binom{T-1-a}{2}.$$

Since $\ell + 1 - T \leq 0$ and $a > 0$, we must have

$$6a(s + a + 1 - T) \leq 0.$$

Rewriting and introducing suitable terms we have:

$$6as + 3a^2 - 3a - 3T^2 + 9T - 6 + 3T^2 - 9T - 6aT + 9a + 3a^2 + 6 \leq 0$$

In turn, this can be rewritten as

$$6as + 3a^2 - 3a - 3(T-1)(T-2) + 3(T-a-1)(T-a-2) \leq 0.$$

This gives:

$$3(s^2 + 2as + a^2 - s - a) - 3(T-1)(T-2) + 3(T-a-1)(T-a-2) \leq 3(s^2 - s),$$

and so

$$3((s+a)^2 - (s+a)) - 3(T-1)(T-2) + 3(T-a-1)(T-a-2) \leq 3(s^2 - s).$$

Substituting ℓ for $s + a$ and adding $T(T-1)(T-2)$ to both sides we have

$$3(\ell^2 - \ell) + (T-3)(T-2)(T-1) + 3(T-a-1)(T-a-2) \leq T(T-1)(T-2) + 3(s^2 - s);$$

dividing through by 6 yields the desired inequality:

$$\binom{\ell}{2} + f(m-\ell, n) \leq \binom{\ell}{2} + \binom{T-1}{3} + \binom{T-1-a}{2} \leq \binom{T}{3} + \binom{s}{2}.$$

We therefore conclude that $f(m,n) \leq \binom{T}{3} + \binom{s}{2}$, which completes the proof. Note that indeed, the value of n is not relevant to the value of $f(m,n)$, so long as n is large enough to satisfy $m \leq \binom{n}{2}$. □

Since the value of $f(m,n)$ does not depend on n, we drop the second argument and simply call this function $f(m)$. It is not hard to verify that $T = \left\lfloor \frac{1+\sqrt{1+8m}}{2}\right\rfloor$, where $\lfloor x\rfloor$ is the largest integer greater than or equal to x, so that $f(m) \sim \frac{\sqrt{2}}{3}m^{3/2}$ asymptotically (or more precisely, $\frac{m}{12}(4\sqrt{2m+1}-9) \leq f(m) \leq \frac{m}{6}(\sqrt{8m+1}-3)$ for all m). The value of T can be used to obtain a (rather complicated) explicit expression for $f(m)$ in terms of m. The sequence of values of $f(m)$ is sequence A111138 in [16].

The result above implies:

Theorem 5.26. *Fix $n > 1$ and let X be a subspace of V. Write $\dim(X) = \binom{T}{2} + s$, $0 \leq s \leq T$. Then*

$$n\dim(X) - \binom{T}{3} - \binom{s}{2} \leq \dim(X^*) \leq \min\left\{ n\dim(X),\ 2\binom{n+1}{3}\right\}.$$

Corollary 5.27. *Fix $n > 1$ and let X be a subspace of V with $\dim(X) = m$. If $\dim(X^*) = nm - t$ and $n + t > f(m+1)$, then X is closed.*

Proof. Suppose X is as in the statement, and let Y be any subspace of V of dimension $m+1$. From the definition of f we know that

$$\dim(Y^*) \geq n(m+1) - f(m+1),$$

so $\dim(Y^*) - \dim(X^*) \geq n + t - f(m+1) > 0$. Therefore every Y strictly larger than X must have $\dim(X^*) < \dim(Y^*)$, which shows that X is closed by Proposition 5.15. □

In terms of groups, we conclude:

Theorem 5.28. *Fix $n > 1$. Let G is a group of class two and exponent p, where p is an odd prime, such that $|G/Z(G)| = p^n$, and let r be the largest integer such that $f(r) < n$; finally, let $m = \binom{n}{2} - r$. If $|[G,G]| \geq p^m$, then G is capable.*

We can think of m as a "co-rank" condition on the commutator subgroup of G: the commutator subgroup is of order at most $p^{\binom{n}{2}}$, and r measures how much smaller than this $[G,G]$ can be and still guarantee capability of G.

Table 1 combines Theorem 5.28 with the necessary condition given in Prop. 9 of [11] for the first few values of n. If G is a group with $|G/Z(G)| = p^n$, then $|[G,G]| \geq p^k$ is necessary for the capability of G, and $|[G,G]| \geq p^m$ is sufficient for the capability of G. Note that for $|G/Z(G)| = p^3$, we cannot have $|[G,G]| = p$; however, if $|G/[G,G]| = p^3$, then $|[G,G]| = p$ still yields a capable group; this explains why the necessary conditions seems more restrictive than the sufficient one on the table for $n = 3$.

n	k	m	n	k	m	n	k	m
2	1	1	7	3	14	12	4	55
3	2	1	8	3	20	13	4	67
4	2	2	9	3	28	14	4	79
5	2	4	10	4	37	15	5	93
6	3	8	11	4	45	16	5	108

Table 1. If $|G/Z(G)| = p^n$, $|[G,G]| \geq p^k$ is necessary and $|[G,G]| \geq p^m$ is sufficient for the capability of G; we always have $|[G,G]| \leq p^{\binom{n}{2}}$.

6. Final remarks

In the case where G is 5-generated (that is, it can be generated by 5 elements, though it may require fewer), there is nontrivial work of Brahana [4] classifying the corresponding p-groups that yield a very satisfying result when combined with Theorem 5.28. By combining the conditions we have derived on the rank of $[G,G]$, and considering the different possible subspaces Brahana lists, we may obtain the following result. We note that the exceptions to capability have long been known; the interesting content of the result is that these are in fact the only exceptions at least as far as the 5-generated groups are concerned:

Theorem 6.1. *Let G be a 5-generated group of class at most 2 and exponent p. Then G is one and only one of the following:*

(i) *Nontrivial cyclic; or*

(ii) *A nontrivial central product AB, with $[A,A] \cap [B,B] \cong C_p$; or*

(iii) *Capable.*

Unfortunately, as is evident from Table 1, proceeding along these lines becomes ever more problematic, as more and more cases need to be considered individually to determine if the corresponding group is capable. And for $k \geq 6$, I am not aware of any work like Brahana's that classifies the corresponding p-groups.

Aknowledgements. In addition to the theorems from [4], the work of Brahana helped to clarify many notions with which I had been playing; I thank Prof. Mike Newman very much for bringing the work of Brahana to my attention and other helpful references. I also thank Michael Bush for his help with some geometric considerations and in using the work of Brahana. I especially thank David McKinnon for many stimulating conversations, and for his help in finding a formula for the function $f(m)$. Thanks to users in MathOverflow for comments on bounds for $f(m)$. I also thank the anonymous referees for pointing out some errors in the presentation, and for suggestions that improved the clarity of several proofs. Part of this work was conducted while the author was on a brief visit to the University of Waterloo at the invitation of Prof. McKinnon; I am very grateful to him for the invitation, and to the Department of Pure Mathematics and the University of Waterloo for the great hospitality I received there. The work was begun while the author was at the University of Montana, and finished at the University of Louisiana in Lafayette.

References

[1] Michael R. Bacon and Luise-Charlotte Kappe, On capable p-groups of nilpotency class two, *Illinois J. Math.* **47** (2003), 49–62.

[2] Reinhold Baer, Groups with preassigned central and central quotient group, *Trans. Amer. Math. Soc.* **44** (1938), 387–412.

[3] F. Rudolf Beyl, Ulrich Felgner and Peter Schmid, On groups occurring as central factor groups, *J. Algebra* **61** (1979), 161–177.

[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, Finite metabelian groups and the Plücker line-coordinates, *Amer. J. Math.* **62** (1940), 365–379.

[6] Graham Ellis, On the capability of groups, *Proc. Edinburgh Math. Soc. (2)* **41** (1998), 487–495.

[7] O. N. Golovin, Nilpotent products of groups, *Amer. Math. Soc. Transl. Ser. 2* **2** (1956), 89–115.

[8] Marshall Hall, Jr., The theory of groups, *Mac Millan and Company*, 1959.

[9] M. Hall and J. K. Senior, The groups of order 2^n $(n \leq 6)$, *Mac Millan and Company*, 1964.

[10] Philip Hall, The classification of prime-power groups, *J. Reine Angew. Math.* **182** (1940), 130–141.

[11] Hermann Heineken and Daniela Nikolova, Class two nilpotent capable groups, *Bull. Austral. Math. Soc.* **54** (1996), 347–352.

[12] I. M. Isaacs, Derived subgroups and centers of capable groups, *Proc. Amer. Math. Soc.* **129** (2001), 2853–2859.

[13] Arturo Magidin, Capability of nilpotent products of cyclic groups, *J. Group Theory* **8** (2005), 431–452.

[14] Arturo Magidin, Embedding groups of class two and prime exponent in capable and noncapable groups, *Bull. Aust. Math. Soc.* **79** (2009), 303–308.

[15] Otto Schreier, Die Untergruppen der freien Gruppen, *Abh. Math. Sem. Univ. Hamburg* **5** (1927), 161–183.

[16] N. J. A. Sloane, *On-line encyclopedia of integer sequences*, 2005, `http://oeis.org`.

[17] Ruth Rebekka Struik, On nilpotent products of cyclic groups, *Canad. J. Math.* **12** (1960), 447–462.

ARTURO MAGIDIN
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF LOUISIANA AT LAFAYETTE
217 MAXIM DOUCET HALL
P.O. BOX 41010
LAFAYETTE LA 70504-1010
USA

E-mail: magidin@member.ams.org

(Received July 27, 2013; revised February 6, 2014)