On strongly flat p-groups

Min Lin
May 2012
Advisor: Professor R. Keith Dennis

Abstract

In this paper, we provide a survey (both theoretical and computational) of the conditions for determining which finite p-groups are strongly flat. Let $m(G)$ denote the maximum size of an irredundant generating set of a group G. Then, a group G is strongly flat if $m(G)$ is strictly greater than $m(H)$ for all proper subgroups H of G. For example, J. Whiston has shown in his dissertation that all symmetric groups are strongly flat. Here, we shall only consider the simpler case of finite p-groups. We observe that non-abelian powerful p-groups exhibit this property only when p is odd. Meanwhile, computations made using `GAP` show that, in general, the occurrences of strongly flat groups vary greatly between the cases where p is odd and where $p = 2$. When p is odd, there are very few strongly flat p-groups as the group must be nilpotent of class 2 and have exponent p or p^2. When $p = 2$, strongly flat p-groups are fairly common, as both the class and exponent of the group are unbounded. In particular, over $\frac{1}{4}$ of the groups of order 256 are found to be strongly flat. These concepts are of interest in a number of situations: Powerful p-groups are important in the study of profinite groups, and also, many computations of $m(G)$ are aided by knowing that some maximal subgroups are strongly flat. Throughout the paper, we shall mainly be following the notations and definitions of [6].

Acknowledgements

I would like to thank Professor Keith Dennis for giving me the chance to take part in his research seminar. I have always been interested in algebra and group theory in particular, but never knew where to begin with. Through his weekly meetings, Professor Dennis shared materials that provided the necessary mathematical background for this senior thesis. Over the past year, he has been patient with me and is always willing to address my queries, both in the theoretical and the technical aspects. I am also grateful to Dan Collins for sharing his notes on generating sequences. I would also like to thank my parents, and my three sisters, for their continual support throughout my college life.

Contents

1 Introduction

Consider the group $\mathbb{Z}_6$. This group can be generated by either 1 or 2 elements: $\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle = \langle 2, 4 \rangle = \langle 3, 4 \rangle$. This leads us to consider various questions. Which groups can be generated by a single group element? What is the minimum number of elements that are needed to generate a group G? How many elements are needed to generate a proper subgroup of G? In answering these questions, we are better able to classify groups and study their properties in the general form. In this section, we shall begin by going through some key definitions.

Definition 1.1. A *generating set* (of size n) of a finite group G is a finite set $\{ g_1, \ldots, g_n \}$ of elements of G that generate G.

Definition 1.2. We define $r(G)$ as the smallest size of a generating set of G.

Definition 1.3. A generating set $\{ g_1, \ldots, g_n \}$ of G is *irredundant* if no proper subset generates G. A generating set that has a proper subset that generates G is *redundant*.

Definition 1.4. We let *m(G)* be the maximum size of an irredundant generating set of G and *i(G)* be the maximum size of any irredundant set of G. Equivalently,

$$i(G) = \max \{ m(H) : H \leq G \}$$

It follows from the above definitions that $r(G) \leq m(G) \leq i(G)$.

Example 1.5. We have:

$$\begin{aligned} r(G) = 1 \quad &\Longleftrightarrow \quad G \text{ can be generated by a single } g \in G \\ &\Longleftrightarrow \quad G \text{ is cyclic} \end{aligned}$$

Now, for $G = \mathbb{Z}_p$, a cyclic group of prime order, any $g \in G$ (where $g \neq 1$) generates G. Any generating set of more than two elements will then be redundant. Thus, we have $r(G) = m(G) = i(G) = 1$ in this case.

2 Preliminaries

In this section, we will go through some basic definitions of terms that we would use in this paper. We will also work through various relevant propositions and theorems in group theory. Most of them are elementary, and can be found in [6].

2.1 Basic definitions

Definition 2.1. A *non-generating* element of G is an element x in G such that if $x \in X$ and $\langle X \rangle = G$, then $\langle X \setminus \{x\} \rangle = G$. The *Frattini subgroup* $\Phi(G)$ is the set of all non-generating elements of G.

Proposition 2.2. An alternative definition of the Frattini subgroup is given as follows: $\Phi(G) = \bigcap M_i$, where $\{M_i\}$ is the set of all the maximal subgroups of G.

Proof. First, we show that the set of all non-generating elements of G lies in in the intersection of all the maximal subgroups of G. Let x be a non-generating element of G. Suppose $x \notin M_i$, where M_i is a maximal subgroup of G. Then $\langle M_i, x \rangle = G$ since M_i is a maximal subgroup. This implies that $M_i \cup \{x\}$ is a generating set of G. But x is a non-generator means that $\langle M_i \rangle = G$, which is a contradiction since $\langle M_i \rangle = M_i \neq G$. Therefore, $x \in M_i$, for all i. Next, we show the converse is also true. Let x lie in the intersection of all the maximal subgroups of G, and suppose S is a subset such that $S \cup \{x\}$ generates G. Suppose x is a necessary generator, then $\langle S \rangle = H \lneq G$. Since $\langle H, x \rangle = G$, we have $x \notin H$. Since $H \lneq G$, H must lie in some maximal subgroup M_i. But by assumption, $x \in M_i$, so $\langle H, x \rangle \leq M$ and therefore $G \leq M$, which is a contradiction. Thus, x is a non-generator. This shows the equivalence of the two definitions. □

Next, we quote a useful result regarding the Frattini subgroup of a direct product.

Proposition 2.3. Let G and H be finite groups. Then $\Phi(G \times H) = \Phi(G) \times \Phi(H)$.

Proof. This is a standard result, and can be found in many places, including [5]. □

Definition 2.4. Given a group G, the *commutator* of two elements $g, h \in G$ is given as $[g, h] = g^{-1}h^{-1}gh$. Given sets $A, B \subseteq G$, $[A, B]$ is defined as $\langle [a, b] : a \in A, b \in B \rangle$. $[G, G]$ is known as the *commutator subgroup* and is also denoted as G'.

There are many well-known commutator identities which would be useful in our subsequent discussion. Here, we note the following identity: $[ab, c] = [a, c]^b [b, c]$ (where x^y is defined to be $y^{-1}xy$ for $x, y \in G$). This can be proven by expanding both sides of the expression.

Proposition 2.5. G/G' is abelian.

Proof. First, to show that G/G' is well-defined, we prove that $G' \trianglelefteq G$. Let $g \in G$, then:

$$\begin{aligned} g^{-1}G'g &= g^{-1} \langle [x,y] \mid x,y \in G \rangle g \\ &= \left\langle g^{-1}[x,y]g \mid x,y \in G \right\rangle \\ &= \left\langle [g^{-1}xg, g^{-1}yg] \mid x,y \in G \right\rangle \\ &= \langle [x,y] \mid x,y \in G \rangle \end{aligned}$$

Next, to prove that G/G' is abelian, we prove a stronger result that holds for normal subgroups $N \trianglelefteq G$: Let $x,y \in G$. Then:

$$\begin{aligned} (xN)(yN) = (yN)(xN) &\iff (xy)N = (yx)N \\ &\iff (yx)^{-1}(xy) = [x,y] \in N \end{aligned}$$

Since $[x,y] \in G'$ for all $x,y \in G$, therefore G/G' is indeed abelian. $\square$

Definition 2.6. Let p be a prime. A group G is a p-group if it is non-trivial and every element of G has a power of p as its order.

Proposition 2.7. Let G be a finite group. Then, we have the following equivalent relationship: G is a p-group $\iff$ $|G| = p^n$ for some $n > 0$

Proof. Suppose $|G| = p^n$ for some $n > 0$. Then by Lagrange's theorem, for all $g \in G$, $\text{ord}\,(g) \mid p^n$. Therefore, we have $\text{ord}(g) = p^k$, where $k \leq n$. Thus, G is a p-group. Conversely, if G is a p-group with an order not of the form p^n, then there exists a prime $q \neq p$ such that $q \mid |G|$. By Cauchy's theorem, G would have an element of order q, and so G is not a p-group. $\square$

Definition 2.8. An *elementary abelian* p-group is a finite abelian group where every nontrivial element has order p.

Next, we define and list the properties of a nilpotent group. We require the following definitions.

Definition 2.9. The *upper central series* is defined as follows:

$$1 = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \dots$$

with $Z_0(G) = 1$, $Z_1(G) = Z(G)$ and $Z_{i+1}(G)$ is the subgroup of G containing $Z_i(G)$ such that $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$.

The *lower central series* is defined as follows:

$$G = G^0 \geq G^1 \geq G^2 \geq \dots$$

with $G^0 = G$, $G^1 = [G,G]$ and $G^{i+1} = [G, G^i]$

Definition 2.10. A group G is said to be *nilpotent* if the $Z_c(G) = G$ for some $c \in \mathbb{Z}$. The smallest such c is called the *nilpotence class* of G and we denote it as $\mathrm{cl}\,(G) = c$.

Here, we quote a theorem on nilpotent groups. The proof can be found in various texts, including [12], and shall not be included here.

Theorem 2.11. *Let G be a finite group. Then, the following are equivalent:*

1. *G is nilpotent*
2. *$\Phi(G) \geq G'$*
3. *G is a direct product of p-groups*

We end this subsection by introducing the two subgroups $\Omega_i(G)$ (omega) and $\mho_i(G)$ (agemo), and their basic properties:

Definition 2.12. Let G be a finite p-group. Then:

$$\begin{aligned} \Omega_i(G) &= \left\langle \{x \in G \mid x^{p^i} = 1\} \right\rangle \\ \mho_i(G) &= \left\langle \{x^{p^i} \mid x \in G\} \right\rangle \end{aligned}$$

We also introduce another notation, which would be used later in a subsequent section. Let $\mho^1(G) = \mho_1(G), \mho^2(G) = \mho_1(\mho^1(G))$, and so on. In other words, $\mho^n(G) = \mho_1(\mho^{n-1}(G))$, for $n \geq 2$.

Proposition 2.13. The omega and agemo subgroups form two normal series. Let G be a finite p-group with order p^d, then:

$$\begin{aligned} G &= \Omega_d(G) \geq \Omega_{d-1}(G) \geq \cdots \geq \Omega_1(G) \geq \Omega_0(G) = 1 \\ G &= \mho_0(G) \geq \mho_1(G) \geq \cdots \geq \mho_{d-1}(G) \geq \mho_d(G) = 1 \end{aligned}$$

2.2 Properties of p-groups

With the following definitions, we describe some commonly known properties of p-groups, which would be useful for our subsequent discussion. First, we require the following proposition, which holds for finite groups in general.

Proposition 2.14. Let G be a finite group and let $S \subseteq G$. Then S is an irredundant generating set of G if and only if the image of S in $G/\Phi(G)$ is an irredundant generating set of $G/\Phi(G)$.

Proof. Let $S = \{g_1, \ldots, g_n\} \subseteq G$ and let $\bar{S} = \{g_1\Phi(G), \ldots, g_n\Phi(G)\} \subseteq G/\Phi(G)$ be the image of S in $G/\Phi(G)$. Clearly, if S generates G, then $\bar{S}$ generates $G/\Phi(G)$. Now, suppose $\bar{S}$ generates $G/\Phi(G)$ and S does not generate G, then $\langle S \rangle \subseteq M \subsetneq G$, for some maximal subgroup M. In particular, there exists $g \in G$ such that $g \notin M$, so $g \notin \Phi(G)$ and $g\Phi(G) \notin \left\langle \bar{S} \right\rangle$. Therefore, $\bar{S}$ does not generate $G/\Phi(G)$, and we have a contradiction with our initial assumption. Therefore, S generates $G \iff \bar{S}$ generates $G/\Phi(G)$.

Now, suppose S is an irredundant generating set but $\bar{S}$ is a generating set that is redundant. Then, there exists a proper subset $\bar{S}'$ that is generating, and the preimage of $\bar{S}'$ is a proper subset of S that is generating. This would contradict our assumption that S is an irredundant generating set. By a similar argument, if $\bar{S}$ is an irredundant generating set, then S must necessarily be an irredundant generating set. Therefore, S is an irredundant generating set of $G \iff \bar{S}$ is an irredundant generating set of $G/\Phi(G)$. □

Corollary 2.15. Let G be a finite group. Then:

$$r(G) = r(G/\Phi(G))$$
$$m(G) = m(G/\Phi(G))$$

Lemma 2.16. If G is an elementary abelian p-group, then $\Phi(G) = 1$

Proof. Since every element $g \in G$ has order p, therefore $G \simeq \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p = \mathbb{Z}_p^n$. Let $M_i = \mathbb{Z}_p \times \cdots \times 1 \times \cdots \times \mathbb{Z}_p$, where 1 is in the i^{th} coordinate. M_i is a maximal subgroup and

$$\bigcap_{0 \leq i \leq n} M_i = 1$$

Thus, we have $\Phi(G) = 1$ □

Lemma 2.17. Let G be a group. Suppose $N \trianglelefteq G$ and $N \leq \Phi(G)$, then $\Phi(G/N) = \Phi(G)/N$.

Proof. $N \leq \Phi(G)$ implies that N is contained in all the maximal subgroups of G. By the Correspondence Theorem, the maximal subgroups of G/N correspond to the maximal subgroups of G. Therefore, the intersection $\Phi(G/N)$ corresponds to the intersection $\Phi(G)$ of the maximal subgroups of G. □

Lemma 2.18. Let G be a finite p-group. Then $\mho_1(G)G' \leq \Phi(G)$.

Proof. Let $M \leq G$ be a maximal subgroup of G. By Sylow's Theorem, $[G : M] = p$ and so $G/M \simeq \mathbb{Z}_p$, which is abelian. Therefore, $G' \leq M$. Also, $(gM)^p = M$ for all $g \in G$. Therefore, $g^p \in M$ for all $g \in G$ and we have $\mho_1(G) \leq M$. Since G' is a normal subgroup, we have $\mho_1(G)G' \in M$ and thus $\mho_1(G)G' \leq \Phi(G)$. □

With the following lemmas, we can now make the following propositions:

Proposition 2.19. Let G be a finite p-group, then $\mho_1(G)G' = \Phi(G)$.

Proof. From Lemma 2.18, we have $\mho_1(G)G' \leq \Phi(G)$. Now, let $H = \mho_1(G)G'$. Since $\mho_1(G) \trianglelefteq G$, we have $H \trianglelefteq G$. Since $G' \leq H$, therefore G/H is abelian. Also, by Lagrange's theorem, $\mho_1(G) \leq H$ implies that G/H is elementary abelian. Thus, by Lemma 2.16 and 2.17, we have $\Phi(G)/H = \Phi(G/H) = 1$. In other words, $\Phi(G) = H = \mho_1(G)G'$. □

Proposition 2.20. Let G be a finite p-group. Each irredundant generating set of G has d elements, where $|G : \Phi(G)| = p^d$.

Proof. Let $\{ g_1, \ldots, g_n \}$ be an irredundant generating set of G. Then, by Proposition 2.14, we have $\{g_1\Phi(G), \ldots, g_n\Phi(G)\} = G/\Phi(G)$ and therefore $d \leq n$. Suppose that $d < n$. Then, there exists a proper subset of $\{g_1\Phi(G), \ldots, g_n\Phi(G)\}$ which still generates $G/\Phi(G)$. The corresponding proper subset of $\{g_1, \ldots, g_n\}$ generates G. This contradicts the irredundancy of the set $\{g_1, \ldots, g_n\}$. Thus, we have $d = n$. □

Corollary 2.21. Let G be a finite p-group. Then $r(G) = r(G/\Phi(G)) = d = m(G)$, where $|G : \Phi(G)| = p^d$.

Proposition 2.22. Let G be a finite p-group. Then $G/\Phi(G)$ is elementary abelian. Furthermore, if H is another normal subgroup of G such that G/H is elementary abelian, then $\Phi(G) \leq H$.

Proof. From the proof of Lemma 2.18, we have $G' \leq \Phi(G)$ and so $G/\Phi(G)$ is abelian. From the same proof, we have $\mho_1(G) \leq \Phi(G)$. Now, for all $g \in G$, $g\Phi(G)$ has order p, and thus $G/\Phi(G)$ is elementary abelian. Now suppose that G/H is elementary abelian of order p^n. Then G/H is abelian implies that $G' \leq H$. Also, $(gH)^p = 1$ implies that $g^p \in H$ for all $g \in G$, so $\mho_1(G) \leq H$. Thus, $\Phi(G) = \mho_1(G)G' \leq H$. □

Lemma 2.23. Let G be a non-trivial finite p-group. Then $Z(G) \neq 1$.

Proof. The class equation states that:

$$|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(g_i)|$$

where $g_1, \ldots, g_r$ are representatives of the distinct non-central conjugacy classes. By definition, $C_G(g_i) \neq G$ for all i so p divides $|G : C_G(g_i)|$. Since p also divides $|G|$, it follows that p divides $|Z(G)|$ and hence the center of a p-group is non-trivial. □

Corollary 2.24. If $|G| = p^2$ for some prime p, then G is abelian.

Proof. Since $Z(G) \neq 1$, therefore we have $G/Z(G)$ is cyclic. Let $xZ(G)$ be a generator $G/Z(G)$, then every element in G is of the form $x^a z$ for some integer $a \in \mathbb{Z}$ and some element $z \in Z(G)$ Then, G is clearly abelian. □

Proposition 2.25. Let G be a p-group of order p^n. Then G is nilpotent of nilpotence class at most $n-1$ for $n \geq 2$ (and class equal to n when $n = 1$ or 0).

Proof. Now, for each $i \geq 0$, $G/Z_i(G)$ is also a p-group. Thus, if $|G/Z_i(G)| > 1$, then $Z(G/Z_i(G)) \neq 1$. Therefore, if $Z_i(G) \neq G$, we have $Z_{i+1}(G)/Z_i(G) \neq 1$ and thus $|Z_{i+1}(G)| \geq p|Z_i(G)|$. We end up with $|Z_{i+1}(G)| \geq p^{i+1}$. This implies that $|Z_n(G)| \geq p^n$, so $G = Z_n(G)$ and $\mathrm{cl}\,(G) \leq n$. Suppose $\mathrm{cl}(\,G) = n$, then $|Z_i(G)| = p^i$ for all i. However, this would mean that $Z_{n-2}(G)$ would have index p^2 in G and so by Corollary 2.24, $G/Z_{n-2}(G)$ would be abelian. This would then mean that $G/Z_{n-2}(G) = Z(G)$ and $Z_{n-1}(G) = G$, which would be a contradiction. □

Next, we quote a theorem from Laffey [9], which we shall not prove here as it is rather involved:

Theorem 2.26. (T. Laffey) *Let G be a finite p-group, where $p > 2$. Then G has a normal subgroup N such that*

1. $r(G) = r(N)$
2. $\Phi(N) = N' \leq Z(G)$
3. *N' is elementary abelian*

2.3 Extensions to Direct Products

If we were to study the generating sets of a group G, an obvious extension would be to study the sets that generate the direct product $G \times H$.

Definition 2.27. Two groups G and H are *relatively prime* if they do not have any common non-trivial quotient groups.

Proposition 2.28. Let G and H be finite groups such that $|G|$ and $|H|$ are relatively prime integers. Then, G and H are relatively prime groups.

Proof. Let Q be a common quotient group of both G and H. By Lagrange's theorem, $|G|$ and $|H|$ are both divisible by $|Q|$, so we have $|Q| = 1$, and the only common quotient group is the trivial group. □

Theorem 2.29. (D. Collins and K. Dennis) *Let G and H be two relatively prime groups. Then, the following holds:*

1. $r(G \times H) = r(G) + r(H)$
2. $m(G \times H) = m(G) + m(H)$
3. $i(G \times H) = i(G) + i(H)$

Proof. The proof can be found in [4]. In fact, D. Collins and K. Dennis proved a stronger result, showing that (2) and (3) hold for all direct products of finite groups. □

Corollary 2.30. Let $G \simeq \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$, where p_i are distinct primes. Then

$$m(G) = m(\mathbb{Z}_{p_1}^{k_1}) + \cdots + m(\mathbb{Z}_{p_n}^{k_n}) = k_1 + \cdots + k_n$$

2.4 Examples

Before we proceed to the next section, we give several examples here to illustrate the concepts of r, m, i.

Example 2.31. Let $G = \mathbb{Z}_n$, the cyclic group of order n. Then, we have:

$$\begin{aligned} r(\mathbb{Z}_n) &= 1 \\ m(\mathbb{Z}_n) &= \nu(n) \\ i(\mathbb{Z}_n) &= \nu(n) \end{aligned}$$

where $\nu(n)$ is the number of distinct prime divisors of n.

Example 2.32. Let D_{2n} denote the dihedral group of order $2n$. D_{2n} is generated by two elements, R ("rotation") and F ("flip"), that satisfy $R^n = F^2 = 1$ and $RF = FR^{-1}$. We have:

$$\begin{aligned} r(D_{2n}) &= 2 \\ m(D_{2n}) &= 1 + m(\mathbb{Z}_n) \\ i(D_{2n}) &= 1 + m(\mathbb{Z}_n) \end{aligned}$$

Example 2.33. Let A be a finite abelian group. Let

$$A \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$$

for $1 < n_1 | n_2 | \cdots | n_k$ be the unique description of A as a product of cyclic groups, subject to the given conditions. Next, decompose A as a direct product of it Sylow subgroups to express A as a product of cyclic subgroups of prime power order. Let t denote the number of all non-trivial cyclic groups that appear in the second decomposition. Then, we have:

$$\begin{aligned} r(A) &= k \\ m(A) &= t \\ i(A) &= t \end{aligned}$$

3 Flat groups

3.1 Basic definitions

Definition 3.1. Let G be a finite group, then:

1. G is *flat* if $m(H) \leq m(G)$ for all $H \leq G$
2. G is *strongly flat* if $m(H) < m(G)$ for all $H \lneq G$
3. G is *uniformly flat* if $m(K) < m(H)$ for all K $\lneq H \leq G$

Remark 3.2. It is clear from the above definitions that a group G is uniformly flat if every subgroup H of G is strongly flat.

Example 3.3. $\mathbb{Z}_p$ is strongly flat. $\mathbb{Z}_{p^2}$ is flat but not strongly flat.

Proof. Let $G = \mathbb{Z}_p$. Then $m(G) = 1$. However, the only proper subgroup H of G is the trivial group $\langle 1 \rangle$, where $m(H) = 0$. Thus, $\mathbb{Z}_p$ is strongly flat. Now, let $G' = \mathbb{Z}_{p^2}$. Then $m(G') = \nu(G') = 1$. However, $G = \mathbb{Z}_p \lneq G'$ and therefore $\mathbb{Z}_{p^2}$ is not strongly flat. □

In the closing remarks of [14], J. Whiston and J. Saxyl claimed that nilpotent groups are flat. If this were to hold true, then all p-groups would be flat since all p-groups are nilpotent (by Proposition 2.25). We argue that this is in fact false, by showing an example of a p-group that is not flat.

Example 3.4. Let $G = \mathbb{Z}_p^p \rtimes \mathbb{Z}_p$ for p an odd prime. Then G is not flat.

Proof. Let $a = ((1, 0, \ldots, 0); 0)$ and $b = ((0, \ldots, 0); 1)$. Clearly, a and b generate the group G: Denote $(1, 0, \ldots, 0)$ as e_1, $(0, 1, \ldots, 0)$ as e_2, etc. Then we have $a = (e_1; 1)$ and $b = (0; 1)$. Observe that we have:

$$\begin{aligned} bab^{-1} &= (e_2; 0) \\ b(e_2; 0)b^{-1} &= (e_3; 0) \\ &\cdots \\ b(e_i; 0)b^{-1} &= (e_{i+1}; 0) \end{aligned}$$

Therefore, all of $(e_i; 0)$ appear and they form a basis for the vector space $V = \mathbb{Z}_p^p$. Therefore, all of V and $(0, \mathbb{Z}_p)$ appear in $\langle a, b \rangle$ and thus $\langle a, b \rangle$ = G.

Now, since $m(V) = p$ and $V \leq G$, we have $i(G) \geq p$. This leaves us with $i(G) > m(G) = r(G) = 2$, as long as $p > 2$. □

Example 3.5. The symmetric groups S_n are strongly flat.

Proof. The set of transpositions $\{(1,2),(2,3),\ldots,(n-1,n)\}$ forms an independent generating set of S_n and thus $m(S_n) \geq n-1$. In [13], J. Whiston showed that $n-1$ is an upper bound for the size of an independent generating set in S_n and that equality is only achieved when the set generates the whole of S_n In other words, $m(H) < m(S_n)$ for all $H \lneq S_n$ and therefore S_n is strongly flat. □

Lemma 3.6. Let G be a finite abelian p-group. The, the following are equivalent:

1. G is uniformly flat
2. G contains no subgroup isomorphic to $\mathbb{Z}_{p^2}$
3. $G \simeq \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$
4. G is a finite dimensional vector space over $\mathbb{F}_p = \mathbb{Z}_p$
5. $\exp(G) = p$
6. $\Phi(G)$ is trivial
7. G is strongly flat

Proof. First, note that by Remark 3.2 and Example 3.3, (1), (2) and (3) are equivalent. Meanwhile, (3) and (4) are equivalent (by definition of vector space) and they are both equivalent to (5), for G a finite abelian p-group. Also, (5) implies (6) because of Lemma 2.16, while (6) implies (5) because of $\mho_1(G) = 1$ (Proposition 2.19). It remains to prove that (7) implies (1); the converse is trivial.

Now, let G be a finite abelian p-group. By the Fundamental theorem of finite abelian groups, $G \simeq \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_n}}$. Let $H \simeq \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p = \mathbb{Z}_p^n$. Now, we have $H \leq G$ with $m(H) = m(G) = n$. Since G is strongly flat, therefore $H = G$. Thus, we have (7) implies (3) and thus (1). □

We can also extend the above lemma to finite abelian groups in general, with the following modifications:

Lemma 3.7. Let G be a finite abelian group. Then, the following are equivalent:

1. G is uniformly flat
2. G contains no subgroup isomorphic to $\mathbb{Z}_{p^2}$ for any prime p
3. Every Sylow p-subgroup is uniformly flat

4. $\exp(G)$ is square-free

5. $\Phi(G)$ is trivial

6. G is strongly flat

Proof. From Lemma 3.6, (2) and (3) are equivalent. (1) implies (2) from Example 3.3. The converse is true because of Proposition 2.29 and Lemma 3.6: $G \simeq \mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}$. Suppose we have $K \lneq H$, then we have $K \simeq \mathbb{Z}_{p_1}^{a_1} \times \cdots \times \mathbb{Z}_{p_n}^{a_n}$ and $H \simeq \mathbb{Z}_{p_1}^{b_1} \times \cdots \times \mathbb{Z}_{p_n}^{b_n}$ with $a_i \leq b_i$ for all i (with equality not holding for at least one i). Thus, we have:

$$m(K) = \sum_{i=1}^{n} a_i < \sum_{i=1}^{n} b_i = m(H)$$

Now, (2) and (4) are equivalent since $\exp(\mathbb{Z}_{p_1}^{k_1} \times \cdots \times \mathbb{Z}_{p_n}^{k_n}) = p_1 \cdot \cdots \cdot p_n$ is square-free. Meanwhile, to show that (2) and (5) are equivalent, we know from Proposition 2.3 and Lemma 3.6 that $\Phi(G) = \Phi(\mathbb{Z}_{p_1}^{k_1}) \times \cdots \times \Phi(\mathbb{Z}_{p_n}^{k_n}) = 1$. It remains to prove that (6) implies (1); the converse is trivial.

Let G be a finite abelian group. By the Fundamental theorem of finite abelian groups, $G \simeq \mathbb{Z}_{p_1^{k_1}}^{j_1} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}^{j_n}$, where p_i and p_j are not necessarily distinct primes. Let $H \simeq \mathbb{Z}_{p_1}^{j_1} \times \cdots \times \mathbb{Z}_{p_n}^{j_n}$. Now we have $H \leq G$ with

$$m(G) = \sum_{i=1}^{n} j_i = m(H)$$

Since G is strongly flat, therefore we have $H = G$. We have (6) implies (2) and thus (1). □

3.2 Strongly flat p-groups

Definition 3.8. Let G be a finite p-group. Then G is *r-maximal* if $r(H) < r(G)$ for all proper subgroups H of G.

The properties of r-maximal groups have been studied in various papers [3, 11]. Here, we make the following observation: If G is a finite p-group, then $r(G) = m(G)$. In other words, G is r-maximal is equivalent to saying G is strongly flat. In this sub-section, we will work through the proof of the following theorem from Chin[3].

Theorem 3.9. (A. Chin) *Let G be a strongly flat p-group. If $p > 2$, then G has exponent p or p^2. If $p = 2$, then G has exponent 4 if any one of the following conditions is satisfied:*

1. $|\Phi(G)| \leq 2^3$.
2. $\Phi(G)$ *is elementary abelian.*
3. $r(G) \leq 3$.

Before we start on the proof, we need the following lemma (Kahn, [8]) and a few propositions.

Lemma 3.10. If G is a strongly flat p-group and $N \trianglelefteq G$ with $N \subseteq \Phi(G)$, then G/N is strongly flat.

Proof. Let $K/N \lneq G/N$. In other words, $N \leq K \lneq G$ with $N \trianglelefteq K$. Since the standard projection of K on K/N is clearly onto, the minimal generating set of K is at least as big as K/N. Thus, we have $r(K/N) \leq r(K)$. Similarly, $N \subseteq \Phi(G)$ implies that $r(G/\Phi(G)) \leq r(G/N)$.

$$\begin{aligned} r(K/N) &\leq r(K) \\ &= m(K) \text{ (K is a p-group)} \\ &< m(G) \text{ (G is strongly flat)} \\ &= r(G) \\ &= r(G/\Phi(G)) \text{ (by Corollary 2.21)} \\ &\leq r(G/N) \end{aligned}$$

Thus, G/N is strongly flat. □

Proposition 3.11. If G is a strongly flat p-group, then $\Phi(G) = G'$.

Proof. Since G is strongly flat and $G' \subseteq \Phi(G)$, it follows from Lemma 3.10 that G/G' is strongly flat. Also, we know from Proposition 2.5 that G/G' is abelian. It follows from Lemma 3.6 that $\exp(G/G') = p$ and thus G/G' is in fact elementary abelian. From Proposition 2.22, we have $\Phi(G) \leq G'$, and thus $\Phi(G) = G'$. □

Proposition 3.12. Let x, y be elements of a group G and let n be a positive integer. Then $(x[x,y])^n = x^n[y,x^n]^{-1}$. In particular, if $G' \subseteq Z(G)$, then $[x,y]^n = [y,x^n]^{-1} = [x^n, y]$.

Proof.

$$\begin{aligned}
(x[x,y])^n &= (xx^{-1}y^{-1}xy)^n \\
&= (y^{-1}xy)^n \\
&= y^{-1}x^ny \\
&= x^nx^{-n}y^{-1}x^ny \\
&= x^n[x^n, y] \\
&= x^n[y, x^n]^{-1}
\end{aligned}$$

Suppose $G' \subseteq Z(G)$, then we can collect the x terms on the left hand side of the expression above and it follows that $[x,y]^n = [y,x^n]^{-1}$. Meanwhile, $[x,y]^n = [x^n, y]$ can be derived from the expansion of terms. □

We now proceed to prove Theorem 3.9:

Proof. For the case of G being abelian, we have already shown earlier that $\exp(G) = p$ for G to be strongly flat. Now, let G be a non-abelian strongly flat p-group. Then, the nilpotency class of G is 2 [2, 9, 11]. Thus, we have $G' \leq Z(G)$. From Proposition 3.11, we have:

$$\mho_1(G) \leq \Phi(G) = G' \leq Z(G)$$

Suppose that $\exp(G) > p$. Let x, y be arbitrary elements of G. Since G' is contained in the center of G and $\mho_1(G) \leq Z(G)$ implies that $[\mho_1(G), G] = 1$, we have by Proposition 3.12 that $[x,y]^p = [x^p, y] = 1$. Thus, $\exp(G') = p$. We now have:

$$\mho_2(G) \subseteq (\mho_1(G))^p \subseteq (G')^p = 1$$

Therefore, $\exp(G) = p^2$.

For the case of $p = 2$, Chin noted that any group with at least two distinct elements of order 2 contains a dihedral subgroup, and thus has exponent at least 4. □

A direct consequence of the theorem by Chin is that it allows us to rule out p-groups that are not strongly flat.

Corollary 3.13. Let G be a non-abelian p-group with exponent $\geq p^3$. Then G is not strongly flat if any one of the following conditions is satisfied:

1. p is odd
2. $p = 2$ and $|\Phi(G)| \leq 2^3$
3. $p = 2$ and $\Phi(G)$ is elementary abelian
4. $p = 2$ and $r(G) \leq 3$

Aother observation by Chin is that we can put a lower bound for $r(G)$ when G is strongly flat:

Proposition 3.14. Let G be a non-abelian strongly flat p-group. Then $r(G) \geq 3$, except when $G = Q_8$.

Proof. Since G is non-abelian, $r(G) \neq 1$. Suppose $r(G) = 2$, then G is strongly flat implies that $r(H) = 1$ for any subgroup $H \lneq G$ (Recall that $r(P) = m(P)$ for a p-group P). This implies that every proper subgroup of G is cyclic. In particular, G would have a cyclic maximal subgroup. Checking through the list (from [7]) of p-groups which have a cyclic maximal subgroup, none of those groups are strongly flat, except for $G = Q_8$. □

Search for strongly flat groups amongst non-abelian p-groups

Order	**Conditions**	**Primes** $(p =)$				
		3	5	7	11	13
p	(0)	1	1	1	1	1
	(1)	0	0	0	0	0
p^2	(0)	2	2	2	2	2
	(1)	0	0	0	0	0
p^3	(0)	5	5	5	5	5
	(1)	2	2	2	2	2
	(2)	2	2	2	2	2
	(3)	2	2	2	2	2
p^4	(0)	15	15	15	15	15
	(1)	10	10	10	10	10
	(2)	9	9	9	9	9
	(3)	5	5	5	5	5

Table 1: Table showing how the conditions help to restrict the number of cases we have to consider in our search for strongly flat groups amongst the non-abelian p-groups (for p odd), using Corollary 3.13. (0) denotes the number of groups of that order. (1) denotes the number of groups that is non-abelian. (2) denotes the number of groups left after imposing the second condition that the exponent of the group is at most p^2. (3) denotes the number of groups left after imposing the third condition that the group is of nilpotency class 2. Notice here that there are no differences amongst the p-groups here up to the order of p^4.

(Continued)

Order	**Conditions**	**Primes** ($p =$)				
		3	5	7	11	13
p^5	(0)	67	77	83	87	97
	(1)	60	70	76	80	90
	(2)	50	60	66	70	80
	(3)	22	24	26	30	32
p^6	(0)	504	684	860	1192	1476
	(1)	493	673	849	1181	1465
	(2)	405	580	744	1060	1328
	(3)	101	115	129	157	171
p^7	(0)	9310	34297	113147	750735	
	(1)	9295	34282	113132	750720	
	(2)	8315	33091	111577	748745	
	(3)	1563	6849	26463	204373	

Table 2: A continuation of the previous table. Once again, (0) denotes the number of groups of that order. (1) denotes the number of groups that are non-abelian. (2) denotes the number of groups left after imposing the second condition that the exponent of the group is at most p^2. (3) denotes the number of groups left after imposing the third condition that the group is of nilpotency class 2. Note that the computations here are done using `GAP` and the SmallGroups library in `GAP` only contains groups of order up to p^6 for p = 13.

4 Powerful p-groups

In the study of profinite groups, the concept of powerful p-groups play an important role. These groups were introduced in 1987 by Lubotzky and Mann [10], where a number of applications are given. Here, we follow closely to [1, 10].

4.1 Basic definitions

Definition 4.1. Let G be a finite p-group. Then G is *powerful* if p is odd and $G/\mho_1(G)$ is abelian, or if $p = 2$ and $G/\mho_2(G)$ is abelian.

Recall in the proof of Proposition 2.5 that G/N is abelian if and only if $G' \leq N$. Thus, the above definition is equivalent to saying that G is *powerful* if p is odd and $G' \leq \mho_1(G)$, or if $p = 2$ and $G' \leq \mho_2(G)$. This is an alternative definition of a powerful group. Here, we note that if G is a 2-group, then $G' \leq \mho_1(G)$ and thus we need a different definition from the general case. While this makes the proofs regarding powerful groups slightly trickier (having to consider both cases separately), this can usually be resolved by direct substitution of the definitions for the two cases.

Meanwhile, the condition $G' \leq \mho_1(G)$ implies that $\mho_1(G) = G'\mho_1(G) = \Phi(G)$

Definition 4.2. A subgroup $N \leq G$ is *powerfully embedded* in G if p is odd and $[N, G] \leq \mho_1(N)$, or $p = 2$ and $[N, G] \leq \mho_2(N)$.

From the above definitions, we note the following: if G is powerful, then G is powerfully embedded in itself; if N is powerfully embedded in G, then $N \trianglelefteq G$ and N is powerful.

Example 4.3. Since all quotient groups of an abelian group are also abelian, every finite abelian p-group is powerful. Furthermore, their subgroups are all powerfully embedded.

We observe that the conditions for a group N to be powerfully embedded in a p-group G are different for p odd and p even. For the next three lemmas, we prove the case for p odd. The proofs for $p = 2$ are similar - simply apply direct substitutions of the definitions.

Lemma 4.4. If N is powerfully embedded in G and $K \triangleleft G$, then NK/K is powerfully embedded in G/K.

Proof. Let ϕ be the natural epimorphism $G \to G/K$ Then, we have $\phi(N) = NK/K$, $\phi(\mho_1(N)) = \mho_1(\phi(N))$. Since $[N, G] \leq \mho_1(N)$, by applying ϕ to both sides of the expression, we obtain $[\phi(N), \phi(G)] \leq \mho_1(\phi(N))$ □

Lemma 4.5. Let $K, N \trianglelefteq G$ and $K \leq \mho_1(N)$. Then N is powerfully embedded in G if and only if N/K is powerfully embedded in G/K.

Proof. It remains to prove the converse. Suppose $[N/K, G/K] \leq \mho_1(N/K)$. Since $\mho_1(N/K) = \mho_1(N)/K$, we have $[N, G] \leq \mho_1(N)$. □

Lemma 4.6. Let N be powerfully embedded in G and $x \in G$. Then $H = \langle N, x \rangle$ is powerful.

Proof. We have $N/\mho_1(N) \leq Z(H/\mho_1(N)$. Since H/N is cyclic, we have $H/\mho_1(N)$ is abelian. Then, $\mho_1(H) \geq \mho_1(N) \geq H'$ implies that H is powerful. □

Proposition 4.7. Let G be a powerful p-group. Then $\mho_j(\mho_i(G)) = \mho_{i+j}(G)$ for any integers $i, j \geq 0$.

Proof. We start by proving that $\mho_1(\mho_j(G)) = \mho_{j+1}(G)$. Since $\mho_{j+1}(G) \subseteq \mho_1(\mho_j(G))$, we assume $\mho_{j+1}(G) = 1$. Otherwise, by Lemma 4.5, we can pass G to the quotient $G/\mho_{j+1}(G)$. We then attempt to show that $\mho_1(\mho_j(G)) = 1$.

We first consider the case for p odd: Let N be a minimal normal subgroup contained in $\mho_j(G)$. By induction, $\mho_1(\mho_j(G)) \subseteq N$. Since $\mho_j(G)$ is powerful, therefore $\mho_j(G)/N$ is abelian, while $N \subseteq Z(G)$ (since N is minimal normal), and so $\mathrm{cl}(\mho_j(G)) \leq 2$. Since $\mho_{j+1} = 1$, $\mho_j(G)$ is generated by elements of order p, and thus we have $\mho_1(\mho_j(G)) = 1$.

Next, we consider the case for $p = 2$: Again, let N be a minimal normal subgroup contained in $\mho_j(G)$. By induction, $\mho_1(\mho_j(G)) \subseteq N$, and hence $\mho_2(\mho_j(G)) = 1$. But since $\mho_j(G)$ is powerfully embedded, so $[\mho_j(G), G] = 1$, and therefore $\mho_j(G)$ is abelian. By our assumption that $\mho_{j+1}(G) = 1$, $\mho_j(G)$ is generated by elements of order 2, and thus has exponent 2. Therefore, $\mho_1(\mho_j(G)) = 1$.

For both cases of p, we have shown that $\mho_1(\mho_j(G)) = 1$. By induction on i, we have:

$$\begin{aligned}
\mho_{i+1}(\mho_j(G)) &= \mho_1(\mho_i(\mho_j(G))) \\
&= \mho_1(\mho_{i+j}(G)) \\
&= \mho_{i+j+1}(G)
\end{aligned}$$

□

4.2 Flatness of powerful p-groups

In this subsection, we will work through various propositions and lemmas, to show that all powerful p-groups are flat. The proofs here are for the case when p is odd, but the proof for the case when $p = 2$ is similar. We follow closely [1, 10].

Proposition 4.8. If G is a finite p-group, and N is powerfully embedded in G, then $\mho_1(N)$ is powerfully embedded in G.

Proof. We consider here the case when p is odd. Since N is powerfully embedded in G, we have $[N, G] \leq \mho_1(N)$ Thus, it suffices to show that $[\mho_1(N), G] \leq \mho_1([N, G])$. Without loss of generality, we assume that $\mho_1([N, G]) = 1$. Otherwise, by Lemma 4.5, we can pass G to the quotient $G/\mho_1([N, G])$. Since G is nilpotent, $[K, G] \lneq K$ for every non-trivial normal subgroup $K \trianglelefteq G$. Hence, we can further assume that $[[\mho_1(N), G], G] = 1$. This implies that $[[N, G], G] \leq [\mho_1(N), G] \leq Z(G)$.

Let $x \in N$ and $g \in G$. Then $[[x, g], x^i] \in Z(G)$ for $i \in \{0, \ldots, p-1\}$, and

$$\prod_{i=0}^{p-1}[[x,g],x^i] = \prod_{i=0}^{p-1}[[x,g],x]^i = [[x,g],x^i]^{p(p-1)/2}$$

Since p is odd and $\mho_1([N, G]) = 1$, we have

$$\begin{aligned}
[x^p, g] &= [x,g]^{x^{p-1}}[x,g]^{x^{p-2}}\ldots[x,g] \quad \text{(using the identity } [ab,c]=[a,c]^b[b,c]) \\
&= \prod_{j=p-1}^{0}[x,g][[x,g],x^j] \\
&= [x,g]^p\prod_{j=0}^{p-1}[[x,g],x^j] \qquad\qquad ([[x,g],x^i] \in Z(G)) \\
&= [x,g]^p[[x,g],x]^{p(p-1)/2} \\
&= 1
\end{aligned}$$

Therefore, we have $[\mho_1(N), G] = 1$ □

The lower p-series of a group G is the descending series

$$G = P_1(G) \geq P_2(G) \geq \ldots, \text{where } P_{i+1}(G) = \mho_1(P_i(G))[P_i(G), G]$$

Then, for a p-group, we have $P_2(G) = \mho_1(P_1(G))[P_1(G), G] = \mho_1(G)[G, G] = \Phi(G)$.

Lemma 4.9. Let G be a powerful p-group. Then:

1. For each $i \geq 1$, $P_i(G)$ is powerfully embedded in G and $P_{i+1}(G) = \mho_1(P_i(G)) = \Phi(P_i(G))$.

2. For each $i \geq 1$, the map $x \mapsto x^p$ induces a homomorphism from $P_i(G)/P_{i+1}(G)$ onto $P_{i+1}(G)/P_{i+2}(G)$

Proof. (1.) $P_1(G) = G$ is powerfully embedded in G. Suppose that $P_i(G)$ is powerfully embedded in G for some $i \geq 1$, then:

$$P_{i+1}(G) = \mho_1(P_i(G))[P_i(G), G] \leq \mho_1(P_i(G))\mho_1(P_i(G)) = \mho_1(P_i(G)) \leq P_{i+1}(G)$$

This implies that $P_{i+1}(G) = \mho_1(P_i(G))$. By Proposition 4.8, $P_{i+1}(G)$ is powerfully embedded in G. Therefore, $P_{i+1}(G) = \mho_1(P_i(G)) = \Phi(P_i(G))$.
(2.) We know from the proof above that $P_i(G)$ is powerful and $P_{i+1}(G) = \Phi(P_i(G)) = P_2(P_i(G))$. Also, $P_{i+2}(G) = \mho_1(\mho_1(P_i(G))) = P_3(P_i(G))$. By changing notation if necessary, we can assume that $i = 1$, and $P_3(G) = 1$ (by replacing G with G/P_3). Then, $G' \leq \Phi(G) = P_2(G) \leq Z(G)$, so for $x, y \in G$, we have $(xy)^p = x^p y^p [y, x]^{p(p-1)/2}$ (This identity holds for G if $\mathrm{cl}(G) = 2$). Since $p > 2$, we get $[y, x]^{p(p-1)/2} \in \mho_1(P_2(G)) = P_3(G) = 1$, and thus $(xy)^p = x^p y^p$. Since $\mho_1(P_2(G)) = P_3(G) = 1$ and $\mho_1(G) = P_2(G)$, this shows that $x \mapsto x^p$ induces a homomorphism from $G/P_2(G)$ onto $P_2(G)/P_3(G)$. □

Lemma 4.10. If a powerful p-group $G = \langle a_1, \ldots, a_d \rangle$, then $\mho_1(G) = \langle a_1^p, \ldots, a_d^p \rangle$.

Proof. Let $\phi : G/P_2(G) \to P_2(G)/P_3(G)$ be the homomorphism given in the previous lemma. Then:

$$\begin{aligned} P_2(G)/P_3(G) &= \phi(G/P_2(G)) \\ &= \langle \phi(a_1 P_2(G)), \ldots, \phi(a_d P_2(G)) \rangle \\ &= \langle a_1^p, \ldots, a_d^p \rangle P_3(G) \end{aligned}$$

Since $P_3(G) = \Phi(P_2(G))$, we get $\mho_1(G) = \langle a_1^p, \ldots, a_d^p \rangle$. □

Proposition 4.11. If G is a powerful p-group, then every element of $\mho_1(G)$ is a p-th power.

Proof. We proceed by induction on $|G|$. Let $g \in \mho_1(G) = P_2(G)$. By Lemma 4.9, there exists $x \in G$ and $y \in P_3(G)$ such that $g = x^p y$. Let $H = \langle \mho_1(G), x \rangle$. Since $\mho_1(G) = P_2(G)$ is powerfully embedded in G (by Lemma 4.9), it follows from Lemma 4.6 that H is powerful. Also, $g \in \mho_1(G)$ since $y \in P_3(G) = \mho_1(\mho_1(G)) \leq \mho_1(H)$. Assuming that G is not cyclic, then $H < G$. Then g is a p-th power in H, by induction. □

Remark 4.12. Let G be a powerful p-group. Then $\mho_1(G) = \{x^p \mid x \in G\}$, by the previous proposition. By Proposition 4.8, $\mho_1(G)$ is also powerful. Thus, we get $\mho^2(G) = \mho_1(\mho^1(G)) = \mho_1(\mho_1(G)) = \{y^p \mid y \in \mho_1(G)\} = \{x^{p^2} \mid x \in G\}$, and so on. We thus have $\mho^k(G) = \{x^{p^k} \mid x \in G\}$.

We can now summarize the results that we have on powerful p-groups as follows:

Theorem 4.13. *Let $G = \langle a_1, \ldots, a_d \rangle$ be a powerful p-group. Then,*

1. *$P_i(G)$ is powerfully embedded in G*
2. *$P_i(G) = \mho_{i-1}(G) = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle$*
3. *$P_{i+k}(G) = P_{k+1}(P_i(G)) = \mho_k(P_i(G))$ for each $k \geq 0$*
4. *The map $x \mapsto x^{p^k}$ induces a surjective homomorphism $P_i(G)/P_{i+1}(G) \to P_{i+k}(G)/P_{i+k+1}(G)$ for each i and k*

Proof. (1) is exactly part (1) of Lemma 4.9. We also observed from the same lemma that $P_{i+1}(G) = \mho_1(P_i(G)) = P_2(P_i(G))$. It thus follows from Proposition 4.11 that $P_{i+1}(G) = \{x^p \mid x \in P_i(G)\}$ and by induction, $P_i(G) = \{x^p \mid x \in P_{i-1}(G)\}$. But Remark 4.12 and (1.) implies that $P_{i-1}(G) = \{x^{p^{i-2}} \mid x \in G\}$, and thus, we have $P_i(G) = \{x^{p^{i-1}} \mid x \in G\}$. Since $P_i(G) < G$, this means that $P_i(G) = \mho_{i-1}(G)$. Meanwhile, repeated application of Lemma 4.10 shows that $P_i(G) = \left\langle a_1^{p^{i-1}}, \ldots, a_d^{p^{i-1}} \right\rangle$, and thus (2) is proven. Then, if we were to replace G with $P_i(G)$ and i with $k+1$ (where $k \geq 0$), then (2) would translate to (3):

$$\begin{aligned} P_{k+1}(P_i(G)) &= \mho_k(P_i(G)) \\ &= \{x^{p^k} \mid x \in P_i(G)\} \\ &= \{y^{p^{i-1+k}} \mid y \in G\} \\ &= P_{i+k}(G) \end{aligned}$$

Meanwhile, (4) is exactly part (2) of Lemma 4.9.

□

Theorem 4.14. *Let G be a powerful p-group. Then G is flat.*

Proof. For this theorem, we will show both the proofs for p odd and $p = 2$.

We begin by considering the case for p odd. Here, (1) to (4) refers to the respective parts of the previous theorem. For the proof, we use induction on $|G|$. Let $H \leq G$ and let $r = r(G), r_2 = r(P_2(G))$. By (1), we know that $P_2(G)$ is powerful, so by induction,

$r(K) \leq r_2$, where $K = H \cap P_2(G)$. By (4), the map $\theta : G/P_2(G) \to P_2(G)/P_3(G)$, induced by $x \mapsto x^p$, is an epimorphism. By considering $G/P_2(G)$ as a vector space over $\mathbb{F}_p$, we get $\dim(\ker(\theta)) = r - r_2$. Therefore, $\dim(\ker(\theta) \cap HP_2(G)/P_2(G)) \leq r - r_2$. Denoting $e = \dim(HP_2(G)/P_2(G))$, we get:

$$\begin{aligned}
\dim(\theta(HP_2(G)/P_2(G))) &= \dim(HP_2(G)/P_2(G)) - \dim(\ker(\theta) \cap HP_2(G)/P_2(G) \\
&\geq \dim(HP_2(G)/P_2(G)) - (r - r_2) \\
&= e - (r - r_2) \\
&= r_2 - (r - e)
\end{aligned}$$

Now, let $h_1, \ldots, h_e \in H$ be such that $HP_2(G) = \langle h_1, \ldots, h_e \rangle P_2(G)$. Since $\Phi(K) = \Phi(H \cap \Phi(G)) \leq \Phi(\Phi(G)) = P_3(G)$, therefore the subspace of $K/\Phi(K)$ spanned by the cosets of $h_1^p, \ldots, h_e^p$ has dimension at least $\dim(\theta(HP_2(G)/P_2(G))) \geq r_2 - (r - e)$. Since $\dim(K/\Phi(K)) = d(K) \leq r_2$, we can find $r - e$ elements $y_i, \ldots, y_{r-e} \in K$ such that

$$K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{r-e} \rangle \Phi(K) = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{r-e} \rangle$$

Then, by the modular law, we have

$$\begin{aligned}
H &= H \cap \langle h_1, \ldots, h_e \rangle P_2(G) \\
&= \langle h_1, \ldots, h_e \rangle (H \cap P_2(G)) \\
&= \langle h_1, \ldots, h_e \rangle K \\
&= \langle h_1, \ldots, h_e, y_1, \ldots, y_{r-e} \rangle
\end{aligned}$$

Thus, we have $r(H) \leq r = r(G)$. But H and G are both p-groups and thus we have $m(H) = r(H) \leq r = r(G) = m(G)$, implying that G is flat.

We then consider the case for $p = 2$. Again, we use induction on $|G|$. The map $\theta : G/\mho_1(G) \to \mho_1(G)/\mho_2(G)$, induced by $x \mapsto x^2$, is an epimorphism. Since G is a powerful 2-group, $G/\mho_2(G)$ is abelian by definition. Therefore, for $x, y \in G$, we have $(xy)^2 \equiv x^2y^2 \pmod{\mho_2(G)}$. Also, $G = \langle a_1, \ldots, a_d \rangle$ implies that $\mho_1(G) = \langle a_1^2, \ldots, a_d^2 \rangle$, by Lemma 4.10. Let $r = r(G)$ and set $r_1 = r(\mho_1(G))$ so that $r_2 \leq r$. Since $\mho_1(G)$ is powerful, therefore by induction, $r(K) \leq r_1$, where $K = H \cap \mho_1(G)$ By considering $G/\mho_1(G)$ as a vector space over $\mathbb{F}_p$, we get $\dim(\ker(\theta)) = r - r_1$. Therefore, $\dim(\ker(\theta) \cap H\mho_1(G)/\mho_1(G)) \leq r - r_1$. Denoting $e = \dim(H\mho_1(G)/\mho_1(G))$, we get:

$$\begin{aligned}
\dim(\theta(H\mho_1(G)/\mho_1(G))) &= \dim(H\mho_1(G)/\mho_1 G)) - \dim(\ker(\theta) \cap H\mho_1(G)/\mho_1(G) \\
&\geq \dim(H\mho_1(G)/\mho_1(G)) - (r - r_1) \\
&= e - (r - r_1) \\
&= r_1 - (r - e)
\end{aligned}$$

Now, let $h_1, \ldots, h_e \in H$ be such that $H\mho_1(G) = \langle h_1, \ldots, h_e \rangle \mho_1(G)$. Thus, $\langle h_1, \ldots, h_e \rangle$ covers H/K. Since $\Phi(K) = \Phi(H \cap \mho_1(G)) \leq \mho_1(\mho_1(G)) = \mho_2(G)$, therefore the subspace of $K/\Phi(K)$, spanned by the cosets of $h_1^2, \ldots, h_e^2$ has dimension at least $\dim(\theta(H\mho_1(G)/\mho_1(G))) \geq r_1 - (r-e)$. Since $r(K) \leq r_1$, we can find $r-e$ elements $y_i, \ldots, y_{r-e} \in K$ such that

$$K = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{r-e} \rangle \Phi(K) = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{r-e} \rangle$$

Recall that $\langle h_1, \ldots, h_e \rangle$ covers H/K and thus $H = \langle h_1^p, \ldots, h_e^p, y_1, \ldots, y_{r-e} \rangle$. Thus, we have $m(H) = r(H) \leq r = r(G) = m(G)$, implying that G is flat. □

4.3 Strongly flat powerful p-groups

Given that all powerful p-groups are flat, it remains to study which powerful p-groups exhibit the property of being strongly flat. Here, we quote a theorem from [3].

Theorem 4.15. *Let G be a non-abelian powerful 2-group. Then G is not strongly flat.*

Proof. From Theorem 4.14, $r(H) \leq r(G)$ for any subgroup H of G. Suppose that G is strongly flat, then $\Phi(G) = G'$ (Proposition 3.11). Since $\Phi(G) = \mho_1(G)G'$, it follows that $\mho_1(G) \leq G'$. Meanwhile, G is a powerful 2-group implies that $G' \leq \mho_2(G)$. Then, we get $\mho_1(G) \leq G' \leq \mho_2(G) \leq \mho_1(G)$, which gives us $G' = \mho_2(G) = \mho_1(G)$. By Proposition 4.7 and induction, we obtain $G' = \mho_1(G) = \mho_2(G) = \cdots = \mho_n(G) = \cdots$. Since G has exponent 2^k for some k, thus $G^{2^k} = \{1\}$, which means that G is abelian. This is a contradiction, and hence G is not strongly flat. □

Corollary 4.16. The only possible non-abelian powerful p-groups which are strongly flat are the ones with exponent p^2 where p is odd.

Proof. The above theorem implies that a non-abelian powerful 2-group would not be strongly flat. We then consider the case where p is odd. A non-abelian powerful p-group has exponent $\geq p^2$. By Corollary 3.13, we know that any non-abelian p-group of exponent $\geq p^3$ cannot be strongly flat. This leave us with groups of exponent p^2 to consider, where p is odd. □

Non strongly flat powerful 2-groups

Order	Conditions	Number of groups
$2^1 = 2$	(0)	1
	(1)	1
	(2)	0
$2^2 = 4$	(0)	2
	(1)	2
	(2)	0
$2^3 = 8$	(0)	5
	(1)	3
	(2)	0
$2^4 = 16$	(0)	14
	(1)	6
	(2)	1
$2^5 = 32$	(0)	51
	(1)	11
	(2)	4
$2^6 = 64$	(0)	267
	(1)	23
	(2)	12
$2^7 = 128$	(0)	2328
	(1)	51
	(2)	36
$2^8 = 256$	(0)	56092
	(1)	139
	(2)	117

Table 3: Table showing the number of 2-groups with various conditions. (0) denotes the total number of 2-groups of that order. (1) denotes the number of powerful 2-groups of that order. (2) denotes the number of non-abelian powerful 2-groups. These groups are not strongly flat.

Possible strongly flat powerful 2-groups

Order	**Conditions**	**Primes** ($p =$)				
		3	5	7	11	13
p^2	(0)	2	2	2	2	2
	(1)	2	2	2	2	2
	(2)	0	0	0	0	0
	(3)	0	0	0	0	0
p^3	(0)	5	5	5	5	5
	(1)	4	4	4	4	4
	(2)	1	1	1	1	1
	(3)	1	1	1	1	1
p^4	(0)	15	15	15	15	15
	(1)	9	9	9	9	9
	(2)	4	4	4	4	4
	(3)	3	3	3	3	3

Table 4: Table showing how the conditions help to restrict the number of cases we have to consider in our search for strongly flat groups amongst the powerful p-groups. (0) denotes the number of groups of that order. (1) denotes the number of groups that are powerful. (2) denotes the number of groups that are powerful and non-abelian. (3) denotes the number of groups that are powerful, non-abelian and have exponent p^2. These are the only powerful non-abelian p-groups that might be strongly flat.

(Continued)

Order	Conditions	Primes ($p =$)				
		3	5	7	11	13
p^5	(0)	67	77	83	87	97
	(1)	26	28	30	34	36
	(2)	19	21	23	27	29
	(3)	13	15	17	21	23
p^6	(0)	504	684	860	1192	1476
	(1)	99	113	127	155	169
	(2)	88	102	116	144	158
	(3)	57	69	81	105	117
p^7	(0)	9310	34297	113147	750735	
	(1)	1300	6349	25561	201973	
	(2)	1285	6334	25546	201958	
	(3)	1081	6084	25250	201570	

Table 5: A continuation of the previous table. (0) denotes the number of groups of that order. (1) denotes the number of groups that are powerful. (2) denotes the number of groups that are powerful and non-abelian. (3) denotes the number of groups that are powerful, non-abelian and have exponent p^2. These are the only powerful non-abelian p-groups that might be strongly flat. Again, note that the computations here are done using `GAP` and the SmallGroups library in `GAP` only contains groups of order up to p^6 for p = 13,

5 Computations of strongly flat p-groups

The computations here are done using `GAP`. The SmallGroups library in `GAP` contains all groups of certain small order. This includes groups of order p^n, which goes up to $n = 7$ for $p = 3, 5, 7, 11$ and up to $n = 6$ for $p = 13$. The identification numbers allow us a systematic way to check through the entire list of the groups of that particular order. Since the conditions for a p-group to be strongly flat are different for $p = 2$ and for p odd, we consider them under different subsections.

5.1 2-groups

Strongly flat 2-groups

Order	**Conditions**	**Number of groups**	exp = 2	exp = 4
$2^1 = 2$	(0)	1		
	(1)	1	1	
$2^2 = 4$	(0)	2		
	(1)	1	1	
$2^3 = 8$	(0)	5		
	(1)	2	1	1
$2^4 = 16$	(0)	14		
	(1)	3	1	2
$2^5 = 32$	(0)	51		
	(1)	6	1	5
$2^6 = 64$	(0)	267		
	(1)	25	1	24
$2^7 = 128$	(0)	2328		
	(1)	131	1	130

Table 6: Table showing the number of 2-groups with various conditions. (0) denotes the total number of 2-groups of that order. (1) denotes the number of strongly flat 2-groups. They are split up into groups of exponent 2 and exponent 4. Up to the groups of order 2^7, there is only 1 strongly flat 2-group with exponent 2 in each order, which is the group C_2^n (for groups of order 2^n).

Professor Dennis's program for searching strongly flat 2-groups of order $2^8 = 256$ is still ongoing, but most of the strongly flat 2-groups have exponent 4. Listed below, however, are two examples that have exponent 8.

Group ID: $[256, 22218]$
Group Structure: $C_4.((C_4 \times D_8) : C_2) = (C_4 \times C_2 \times C_2).(C_2 \times C_2 \times C_2 \times C_2)$
$\Phi(G) : [16, 10]$
$\Phi(G)$ Group Structure: $C4 \times C2 \times C2$
Exponent: 8
m: 4
i: 4

Group ID: $[256, 22219]$
Group Structure: $C_4.((C_4 \times D_8) : C_2) = (C_4 \times C_2 \times C_2).(C_2 \times C_2 \times C_2 \times C_2)$
$\Phi(G) : [16, 10]$
$\Phi(G)$ Group Structure: $C_4 \times C_2 \times C_2$
Exponent: 8
m: 4
i: 4

Since these computations were made using `GAP`, we use their notation C_n for a cyclic group of order n here rather than the $\mathbb{Z}_n$ that we used earlier. We will continue to use the C_n notation for results that we attain from `GAP`.

5.2 p-groups, where p is odd

Strongly flat 3-groups

Order	**Conditions**	**Number of groups**	exp = 3	exp = 9
$3^1 = 3$	(0)	1		
	(1)	1	1	
$3^2 = 9$	(0)	2		
	(1)	1	1	
$3^3 = 27$	(0)	5		
	(1)	2	1	1
$3^4 = 81$	(0)	15		
	(1)	2	1	1
$3^5 = 243$	(0)	67		
	(1)	4	2	2
$3^6 = 729$	(0)	504		
	(1)	12	2	10

Table 7: Table showing the number of 3-groups with various conditions. (0) denotes the total number of 3-groups of that order. (1) denotes the number of strongly flat 2-groups. (2) denotes the number of strongly flat 3-groups with exponent 3, and with exponent 9.

We continued computations for p-groups of order $5, 7, 11$ and 13 and find that a similar pattern follows up to the order of p^5.

Strongly flat p-groups

Order	**Conditions**	**Number of groups**	exp $= p$	exp $= p^2$
p^1	(0)	1		
	(1)	1	1	
p^2	(0)	2		
	(1)	1	1	
p^3	(0)	5		
	(1)	2	1	1
p^4	(0)	15		
	(1)	2	1	1
p^5	(0)	*		
	(1)	4	2	2

Table 8: Table showing the number of p-groups with various conditions. (0) denotes the total number of p-groups of that order. (1) denotes the number of strongly flat p-groups. (2) denotes the number of strongly flat p-groups with exponent p, and with exponent p^2. Note: * $= 77, 83, 87, 97$ for $p = 5, 7, 11$ and 13.

6 Concluding remarks

In this paper, we have provided a survey of the strongly flat p-groups. Through the computations, we find that the behavior for $p = 2$ and p odd vary rather markedly. For example, for $n = 5$, 11.8% of the groups of order 2^n are strongly flat while just 6.0% of the groups of order 3^n are strongly flat. Meanwhile, the p-groups for with $p = 5, 7, 11$ and 13 display a similar pattern as the case for $p = 3$.

Another observation is that amongst the 2-groups, up to the order of $2^8 = 512$, there exists only 1 strongly flat group with exponent 2. For groups of order 2^n, this particular group would be C_2^n. In contrast, groups of order 3^5 have 2 strongly flat groups with exponent 2, of which one is not abelian $((C_3 \times ((C_3 \times C_3) : C_3)) : C_3)$.

A. Chin's theorem provides a suggestion why the behavior may vary. For p odd, G must have exponent at most p^2, and be nilpotent of class 2. These conditions, restrict the possible choices to consider, and also simply our search for strongly flat p-groups for odd p. For $p = 2$, there is no upper bound on our exponent. Though few in comparison, groups of exponent 8 showed up as examples of strongly flat p-groups for groups of order 256.

References

[1] Y. Berkovich, *Groups of prime power order, Vol. 1*, Walter de Gruyter, 2008.

[2] N. Blackburn, *Generalizations of certain elementary theorems on p-groups*, Proc. London Math. Soc. (3) **11** (1961), 1-22.

[3] A. Chin, *On d-Maximal Groups*, Rend. Sem. Mat. Univ. Pol. Torino **67** (2009), 15-21.

[4] D. Collins, *Generating Sequence of Finite Groups*, Notes, 2012.

[5] D. Collins, *Group Theory*, Notes, 2012.

[6] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley and Sons, Inc, 2004.

[7] M. Hall, *The theory of groups*, The Macmillan Co., 1959.

[8] B. Kahn, *The total Stiefel-Whitney class of a regular representation*, J. Algebra **144** (1999), 214-247.

[9] T. J. Laffey, *The minimum number of generators of a finite p-group*, Bull. London. Math. Soc. **5** (1973), 288-290.

[10] A. Lubotzky and A. Mann, *Powerful p-groups. I. Finite Groups*, J. Algebra **105** (1987), 484-505.

[11] P. A. Minh, *d-maximal p-groups and Stiefel-Whitney classes of a regular representation*, J. Algebra **179** (1996), 483500.

[12] M. Quick, Nilpotent groups, `http://www-groups.mcs.st-andrews.ac.uk/~martyn/teaching/5824/5824nilpotent.pdf`.

[13] J. Whiston, *Maximal independent generating sets of the symmetric group*, J. Algebra **232** (2000), 255-268.

[14] J. Whiston and J. Saxl, *On the maximal size of independent generating sets of $PSL_2(q)$*, J. Algebra **258** (2002), 651-657.