INDEPENDENT SETS OF GENERATORS OF PRIME POWER ORDER

ANDREA LUCCHINI AND PABLO SPIGA

Abstract. A subset X of a finite group G is said to be prime-power-independent if each element in X has prime power order and there is no proper subset Y of X with $\langle Y, \Phi(G)\rangle = \langle X, \Phi(G)\rangle$, where $\Phi(G)$ is the Frattini subgroup of G. A group G is $\mathcal{B}_{pp}$ if all prime-power-independent generating sets for G have the same cardinality. We prove that, if G is $\mathcal{B}_{pp}$, then G is solvable. Pivoting on some recent results of Krempa and Stocka [10, 16], this yields a complete classification of $\mathcal{B}_{pp}$-groups.

1. Introduction

Throughout this paper, all groups are finite. We start this introductory section with some definitions fundamental for our work. Given a group G, an element $g \in G$ is said to be a ***pp-element*** if g has prime power order. A subset X of G is said to be

independent*:** if $\langle X, \Phi(G)\rangle \neq \langle Y, \Phi(G)\rangle$ for every proper subset Y of X (where as customary we denote by $\Phi(G)$ the ***Frattini subgroup of G);

***pp-independent*:** if X is independent and each element in X is a *pp*-element; and

***pp-base*:** if X is a *pp*-independent generating set for G.

Finally, G is said to be a $\mathcal{B}_{pp}$***-group*** if every two *pp*-bases of G have the same cardinality.

The main result of this paper is the following.

Theorem 1.1. *If G is a $\mathcal{B}_{pp}$-group, then G is solvable.*

Theorem 1.1 gives a solution to Question 1 in [10] in a strong sense. In fact, it yields a complete classification of the $\mathcal{B}_{pp}$-groups. Indeed, Krempa and Stocka [10, 16] have obtained an entirely satisfactory classification of solvable $\mathcal{B}_{pp}$-groups and hence Theorem 1.1 together with the work in [10, 16] gives a classification of all $\mathcal{B}_{pp}$-groups. This classification is easier to formulate for Frattini-free groups, that is, for groups G with $\Phi(G) = 1$. (Observe that G is a $\mathcal{B}_{pp}$-group if and only if so is $G/\Phi(G)$.)

Corollary 1.2. *Let G be a group with $\Phi(G) = 1$. Then G is a $\mathcal{B}_{pp}$-group and if only if one of the following holds:*

1. *G is an elementary abelian p-group,*
2. *$G = P \rtimes Q$, where P is an elementary abelian p-group, Q is a non-identity cyclic q-group for distinct prime numbers p and q such that Q acts faithfully on P and the $(\mathbb{Z}/p\mathbb{Z})[Q]$-module P is a direct sum of pair-wise isomorphic simple modules,*
3. *G is a direct product of groups given in (1) or in (2) with pair-wise coprime orders.*

The groups as in (2) are simply refereed to as scalar extensions in [16]. We refer the reader to the work of Krempa and Stocka [10, 16] for various motivations on investigating $\mathcal{B}_{pp}$-groups. Broadly speaking, this motivation is rooted on independent generating sets and on generalizations of the Burnside basis theorem; in turn, these motivations are useful for studying groups satisfying the exchange property for bases which is useful for constructing matroids starting from finite groups.

As a bi-product of the arguments used in the proof of Theorem 1.1, we obtain the following result of independent interest. (See Section 2.1 for undefined terminology.)

Theorem 1.3. *Let G be a group and denote by $m(G)$ the largest cardinality of an independent generating set of G. Then $m(G) \geq a + b$, where a and b are, respectively, the number of non-Frattini and non-abelian factors in a chief series of G.*

We have verified with a computer computation [1] that the bound in Theorem 1.3 is sharp when G is the automorphism group of the alternating group of degree 6: here, $m(G) = 4$, $a = 3$ and $b = 1$. Theorem 1.3 gives a strengthening of the bound $m(G) \geq a$, which was proved in [13]. Here, it was also proved that $m(G) = a$ for every solvable group.

The structure of the paper is straightforward. In Section 2 after establishing some notation, and after a short detour through fixed point ratios and spreads, we give some basic results. In Section 3 after establishing a few rather technical results, we prove Theorem 1.1 and Corollary 1.2. Finally, we prove Theorem 1.3 in Section 4.

2010 *Mathematics Subject Classification.* primary 20D10, secondary 20D60, 20F05.

Key words and phrases. independent sets, generating set, Burnside basis theorem.

2. Preliminaries

2.1. **Notation.** Given a group G, we let $m(G)$ and $m_{pp}(G)$ denote the largest cardinality of an independent generating set of G and of a *pp*-independent generating set for G. Since every *pp*-independent generating set is also an independent generating set, we have $m(G) \geq m_{pp}(G)$. In fact, in Lemma 2.3 we show that $m(G) = m_{pp}(G)$.

Let

$$1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$$

be a chief series for G. A factor G_i/G_{i+1} is said to be a ***non-abelian*** chief factor of G if G_i/G_{i+1} is a non-abelian group; moreover, G_i/G_{i+1} is said to be a ***Frattini*** chief factor of G if $G_i/G_{i+1} \leq \Phi(G/G_{i+1})$.

The ***socle*** of G, denoted by $\operatorname{soc} G$, is the subgroup generated by the minimal normal subgroups of G. In particular, if $\operatorname{soc} G$ is a minimal normal subgroup of G (that is, G has a unique minimal normal subgroup), then G is said to be ***monolithic***.

Let G be a monolithic group with socle N. Following the notation in [14], we define $\mu(G) := m(G) - m(G/N)$.

Given a positive integer n and a group H, we denote by $H \operatorname{wr} \operatorname{Sym}(n)$ the ***wreath product*** of H with the symmetric group $\operatorname{Sym}(n)$ of degree n. We denote the elements of $H \operatorname{wr} \operatorname{Sym}(n)$ with ordered pairs $f\sigma$, where $f \in H^n$ and $\sigma \in \operatorname{Sym}(n)$.

Given two positive integers x and n with $x, n \geq 2$, we say that the prime r is a ***primitive prime divisor*** of $x^n - 1$ if r divides $x^n - 1$ and r is relatively prime to $x^i - 1$, for each $i \in \{1, \ldots, n-1\}$. From a celebrated theorem of Zsigmondy [17], either $x^n - 1$ has a primitive prime divisor, or $n = 6$ and $x = 2$, or $n = 2$ and $x + 1$ is a power of 2. In the latter case, when x is a prime power, we deduce that x must be a (Mersenne) prime. We actually need the following refinement. The prime r is said to be a ***large primitive prime divisor*** of $x^n - 1$ if r is a primitive prime divisor of $x^n - 1$ and either $r > n + 1$ or r^2 divides $x^n - 1$. We recall the classical result of Feit [6] on the existence of large primitive prime divisors. (We refer also to [15], for an elementary proof of this result.)

Lemma 2.1. *If x and n are integers greater than 1 there there exists a large primitive prime divisor for $x^n - 1$ except exactly in the following cases:*

1. *$n = 2$ and $x = 2^s 3^t - 1$ for some natural numbers $s \geq 0$ and $t \in \{0, 1\}$ with $s \geq 2$ if $t = 0$,*
2. *$x = 2$ and $n \in \{4, 6, 10, 12, 18\}$,*
3. *$x = 3$ and $n \in \{4, 6\}$,*
4. *$x = 5$ and $n = 6$.*

Our last two definitions are rather technical and (for our application) they only pertain to almost simple groups, but they will prove useful. Given an almost simple group H with socle S and a subgroup K of H with $H = KS$, let

$$t(H, K)$$

be the smallest cardinality of a set X of *pp*-elements in S with $H = \langle K, X \rangle$. Then, define

$$t(H) := \max\{t(H, K) \mid K \leq H \text{ with } H = KS\}.$$

From [9, Theorem 1], S is generated by an involution and by an element of odd prime power order and hence

$$t(H) \leq 2. \tag{2.1}$$

Given a subgroup K of H, we say that a subset Y of H is ***K-generating*** for H if $H = \langle K, Y \rangle$. A K-generating set for H is said to be ***K-independent*** if no proper subset of Y generates H together with K. We denote by

$$m_K(H)$$

the largest cardinality of a K-independent generating set for H.

2.2. **A (short) walk through fixed point ratios and spreads.** Let H be an almost simple group with socle S and let $g, s \in H$. We set

$$P(g, s) := \frac{|\{t \in s^H \mid \langle g, t \rangle \ngeq S\}|}{|s^H|}.$$

This definition is strictly related to the definition of spread and uniform spread in almost simple groups and we refer the reader to [3, 8] for further details.

For any action of H on a set Ω and for any $g \in H$, consider the set $\operatorname{Fix}_\Omega(g) := \{\omega \in \Omega \mid \omega^g = \omega\}$ of fixed points of g on Ω and the ***fixed point ratio***

$$\mu(g, \Omega) := \frac{|\operatorname{Fix}_\Omega(g)|}{|\Omega|}.$$

From [8, Section 2], if $M \backslash H$ denotes the set of right cosets of the subgroup M of H, then

$$\mu(g, M\backslash H) = \frac{|g^H \cap M|}{|g^H|}. \tag{2.2}$$

Let now $\mathcal{M}(H,g)$ be the collection of all maximal subgroups of H containing g and assume that H is almost simple with socle S. Then, from (2.2), we deduce

$$P(g,s) \le \sum_{M\in\mathcal{M}(H,g)} \frac{|\{t\in s^H \mid \langle g,t\rangle \le M\}|}{|s^H|} = \sum_{M\in\mathcal{M}(H,s)} \frac{|\{h\in g^H \mid \langle h,s\rangle \le M\}|}{|g^H|} \le \sum_{M\in\mathcal{M}(H,s)} \mu(g, M\backslash H). \tag{2.3}$$

Eq. (2.3) also appears in [3, (2.4)]. We summarize in the following lemma the main application of fixed point ratios in our context.

Lemma 2.2. *Let H be an almost simple group with socle S. Suppose $H \ne S$. If, for every $g \in H \setminus S$, there exists a pp-element $s_g \in S$ with $P(g,s_g) < 1$, then $t(H) = 1$. In particular, if $\sum_{M\in\mathcal{M}(H,s)} \mu(g,M\backslash H) < 1$ for every $g \in H \setminus S$, then $t(H) = 1$.*

Proof. Let K be a subgroup of H with $H = KS$. For every $g \in K \setminus S$, let s_g be a *pp*-element belonging to S with $P(g,s_g) < 1$. Then by definition of $P(g,s_g)$, there exists $t \in s_g^H$ with $\langle g,t\rangle \ge S$. Thus $H = \langle K,t\rangle$ and hence $t(H,K) = 1$. Since this holds regardless of K, we have $t(H) = 1$. The rest of the proof follows from (2.3). □

2.3. **Basic results.**

Lemma 2.3. *Let G be a group. Then $m(G) = m_{pp}(G)$.*

Proof. As we have observed above, $m(G) \ge m_{pp}(G)$ and hence we only need to show that $m(G) \le m_{pp}(G)$.

Let $X := \{x_1,\dots,x_{m(G)}\}$ be an independent generating set for G of cardinality $m(G)$. For each $i \in \{1,\dots,m(G)\}$, we may write $x_i = y_{1,i}\cdots y_{k_i,i}$, where $y_{1,i},\dots,y_{k_i,i}$ are pair-wise commuting *pp*-elements of G with

$$\langle x_i\rangle = \langle y_{1,i},\dots,y_{k_i,i}\rangle. \tag{2.4}$$

Clearly,

$$\{y_{j,i} \mid 1\le j\le k_i, 1\le i\le m(G)\}$$

is a generating set for G consisting of *pp*-elements and hence it contains a *pp*-base Y.

We claim that, for each $i \in \{1,\dots,m(G)\}$, there exists $j \in \{1,\dots,k_i\}$ with $y_{j,i} \in Y$. Indeed, if for some some $\bar{i}$, Y contains no $y_{j,\bar{i}}$, then

$$G = \langle Y\rangle \le \langle y_{j,i} \mid i \in \{1,\dots,m(G)\}\setminus\{\bar{i}\}, j\in\{1,\dots,k_i\}\rangle \le \langle X\setminus\{x_{\bar{i}}\}\rangle,$$

where in the last inequality we have used (2.4). However, this contradicts the fact that X is independent and hence the claim is proved.

The previous paragraph yields $|Y| \ge m(G)$ and hence the lemma follows because $m_{pp}(G) \ge |Y|$. □

We now recall [10, Theorem 6.1 (1)].

Lemma 2.4. *If G is a $\mathcal{B}_{pp}$-group, then every quotient of G is a $\mathcal{B}_{pp}$-group.*

3. Proofs of Theorem 1.1 and Corollary 1.2

3.1. **Technical lemmas.**

Lemma 3.1. *Let q be a prime power with $q \ge 4$ and let H be an almost simple group with socle $S := \mathrm{PSL}_2(q)$ and with $H \ne S$. Then $t(H) = 1$.*

Proof. It suffices to prove that, for every subgroup K of H with $H = KS$, there exists a *pp*-element $x_K \in S$ with $H = \langle K, x_K\rangle$. Write $q := p^f$, where p is a prime number and f is a positive integer.

Let $K \le H$ with $H = KS$ and let $\theta \in K \setminus S$. Assume that $p^{2f}-1$ admits no large primitive prime divisor. From Lemma 2.1, we deduce that either

$$S \in \{\mathrm{PSL}_2(4) = \mathrm{PSL}_2(5), \mathrm{PSL}_2(8), \mathrm{PSL}_2(32), \mathrm{PSL}_2(64), \mathrm{PSL}_2(512), \mathrm{PSL}_2(9), \mathrm{PSL}_2(27), \mathrm{PSL}_2(125)\},$$

or $f = 1$ and $q = p = 2^s3^t - 1$ for some natural numbers $s \ge 0$ and $t \in \{0,1\}$ with $s \ge 2$ if $t = 0$. In the first eight exceptional cases, the result can be established with a direct inspection using, for instance, the assistance of the computer algebra system `magma` [1]. We now consider the case $q = p = 2^s3^t - 1$. Actually, we deal with the more general case that $q = p$ is a prime number. As $H \ne S$, we have $H = \mathrm{PGL}_2(q)$. Clearly, a Sylow p-subgroup of S is cyclic; let $x \in S$ be an element generating a Sylow p-subgroup of S. Observe that we may choose x so that θ does not normalize $\langle x\rangle$. Using the list of the maximal subgroups of S (see for instance [2, Tables 8.1, 8.2]), we see that $S = \langle x, x^\theta\rangle$. Thus $H = \langle K,x\rangle$ and $t(H,K) = 1$.

Assume now that $p^{2f}-1$ admits a large primitive prime divisor r. Observe that, from the previous paragraph, we may suppose that $f > 1$. In particular, either $r > 2f+1 \ge 5$ or r^2 divides $q+1$. Clearly, a Sylow r-subgroup of S is cyclic; let $x \in S$ be an element generating a Sylow r-subgroup of S. Observe that we may choose x so that θ does not normalize $\langle x\rangle$ (this can be easily established by considering the structure of the subgroup lattice of S, see [2, Table 8.1]). Using the list of the maximal subgroups of S (see for instance [2, Tables 8.1, 8.2]), we see that either

- $S = \langle x, x^\theta \rangle$, or
- $r = 5$ and $\langle x, x^\theta \rangle \cong \mathrm{Alt}(5)$, or
- $r = 3$ and $\langle x, x^\theta \rangle$ is isomorphic to either $\mathrm{Alt}(4)$ or $\mathrm{Alt}(5)$.

In the first case, $H = \langle K, x \rangle$ and hence $t(H, K) = 1$. In the last two cases, r is the cardinality of a Sylow r-subgroup of S, because 5 is the cardinality of a Sylow 5-subgroup of $\mathrm{Alt}(5)$ and 3 is the cardinality of a Sylow 3-subgroup of $\mathrm{Sym}(4)$. However, this contradicts the fact that r is a large primitive prime divisor of $p^{2f} - 1$. □

Lemma 3.2. *Let q be a prime power and let H be an almost simple group with socle $S := \mathrm{PSU}_3(q)$ and with $H \neq S$. Then $t(H) = 1$.*

Proof. As $\mathrm{PSU}_3(2)$ is solvable, we have $q > 2$. Here the argument is similar to the proof of Lemma 3.1: we use primitive prime divisors and the structure of the subgroup lattice of S, see [2, Tables 8.5, 8.6]. Write $q := p^f$, where p is a prime number and f is a positive integer.

Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. Assume $p^{6f} - 1$ admits a large primitive prime divisor of r. Clearly, a Sylow r-subgroup of S is cyclic; let $x \in S$ be an element generating a Sylow r-subgroup of S. Observe that we may choose x so that θ does not normalize $\langle x \rangle$. Using the list of the maximal subgroups of S (see [2, Tables 8.5, 8.6]), we see that $S = \langle x, x^\theta \rangle$ (here we are using the fact that r is a large Zsigmondy prime and hence $\langle x, x^\theta \rangle$ cannot be contained in a maximal subgroup in the Aschbacher class $\mathcal{S}$ by [2, Table 8.6]). Thus $H = \langle K, x \rangle$ and $t(H, K) = 1$.

It remains to consider the case that $p^{6f} - 1$ does not admit a large primitive prime divisor. Lemma 2.1 yields $(f, p) \in \{(1, 5), (1, 3), (2, 2), (3, 2)\}$. Here the proof follows with the invaluable help of the computer algebra system `magma` [1]. □

Lemma 3.3. *Let q be a prime power and let H be an almost simple group with socle $S := \mathrm{PSL}_3(q)$ and with $S < H \not\leq \mathrm{P\Gamma L}_3(q)$. Then $t(H) = 1$.*

Proof. As $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, from Lemma 3.1, we may suppose that $q > 2$. Here the argument is similar to the proof of Lemma 3.1: we use primitive prime divisors and the structure of the subgroup lattice of S, see [2, Tables 8.3, 8.4]. Write $q := p^f$, where p is a prime number and f is a positive integer. As $q > 2$, we have $(p, f) \neq (2, 1)$.

Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. From Lemma 2.1, $p^{3f} - 1$ has a large primitive prime divisors, except when $(p, f) \in \{(2, 2), (2, 4), (2, 6), (3, 2), (5, 2)\}$. For these exceptional cases, we have checked the veracity of this lemma with a computer computation. In particular, for the rest of the argument, we let r be a large primitive prime divisor of $p^{3f} - 1$.

A Sylow r-subgroup of S is cyclic; let $x \in S$ be an element generating a Sylow r-subgroup of S. Let $M \in \mathcal{M}(H, x)$. Here we use the information in [2, Tables 8.3, 8.4]. From the list of the maximal subgroups of H and recalling that $S < H \not\leq \mathrm{P\Gamma L}_3(q)$ and r is a large primitive prime divisor, we deduce that either $M = \mathbf{N}_H(\langle x \rangle)$, or f is even, $q = q_0^2$ and $M \cap S \cong \mathrm{SU}_3(q_0)$ (here we are using the fact that r is a large Zsigmondy prime and hence $\langle x, x^\theta \rangle$ cannot be contained in a maximal subgroup in the Aschbacher class $\mathcal{S}$ by [2, Table 8.4]). In particular, when f is odd, we have $\mathcal{M}(H, x) = \{\mathbf{N}_H(\langle x \rangle)\}$. Therefore, we deduce

$$\sum_{M \in \mathcal{M}(H,x)} \mu(\theta, M \backslash H) = \mu(\theta, \mathbf{N}_H(\langle x \rangle) \setminus H) < 1,$$

and hence $t(H, K) = 1$, from Lemma 2.2.

Suppose now that f is even and let $\bar{M} \in \mathcal{M}(H, x) \setminus \{\mathbf{N}_H(\langle x \rangle)\}$. Then $\bar{M} \cap S \cong \mathrm{SU}_3(q_0)$, where $q = q_0^2 = p^{f/2}$. Observe that from the "c" column in [2, Table 8.42], we deduce that the maximal subgroups of H with $\bar{M} \cap S$ isomorphic to $\mathrm{SU}_3(q_0)$ form $\gcd(q_0 - 1, 3)$ S-conjugacy class. Let $\Omega_1 := \{\langle x^g \rangle \mid g \in H\}$. Using the information in [2, Table 8.3], we deduce

$$|\Omega_1| = \frac{q^3(q^3 - 1)(q^2 - 1)}{(q^2 + q + 1)3} = \frac{q^3(q^2 - 1)(q - 1)}{3}.$$

Let $\Omega_2 := \{\bar{M}^g \mid g \in H\}$. Using the information in [2, Table 8.3], we deduce

$$|\Omega_2| = \frac{q^3(q^3 - 1)(q^2 - 1)}{(q_0^3 + 1)q_0^3(q_0^2 - 1)} = q_0^3(q_0^3 - 1)(q_0^2 + 1).$$

How, consider the bipartite graph having vertex set $\Omega_1 \cup \Omega_2$ and having edge set consisting of the pairs $\{A, B\}$ with $A \in \Omega_1$, $B \in \Omega_2$ and $A \leq B$. Fix $B \in \Omega_2$. Using the structure of the unitary group B, we see that the number of $A \in \Omega_1$ with $A \leq B$ is

$$\frac{(q_0^3 + 1)q_0^3(q_0^2 - 1)}{(q_0^2 - q_0 + 1)3} = \frac{q_0^3(q_0^2 - 1)(q_0 + 1)}{3}.$$

In particular, the number of edges of the bipartite graph is

$$|\Omega_2| \frac{q_0^3(q_0^2 - 1)(q_0 + 1)}{3} = \frac{q^3(q^2 - 1)(q_0^3 - 1)(q_0 + 1)}{3}.$$

This shows that the number of elements in Ω_2 containing the element $\bar{M} \in \Omega_1$ is

$$\frac{\frac{q^3(q^2-1)(q_0^3-1)(q_0+1)}{3}}{|\Omega_1|} = q_0^2 + q_0 + 1.$$

Thus

$$|\mathcal{M}(H,x)| = |\{\mathbf{N}_H(\langle x\rangle)\} \cup \{M \in \Omega_2 \mid x \in M\}| = q_0^2 + q_0 + 2.$$

From [5, Lemma 2.10 (ii)], we have $\mu(\theta, M\backslash H) \leq \gcd(3, q-1)/(q_0(q+1))$ for every $M \in \mathcal{M}(\theta, M \setminus H)$ with $M \cap S \cong \mathrm{SU}_3(q_0)$. Moreover, from [12, Theorem 1], we have $\mu(\theta, \mathbf{N}_H(\langle x\rangle)\backslash H) \leq 4/(3q)$. Therefore

$$\sum_{M\in\mathcal{M}(H,x)} \mu(\theta, M\backslash H) \leq \gcd(3, q-1)\frac{q_0^2+q_0+1}{q_0(q+1)} + \frac{4}{3q} < 1,$$

whenever $q \notin \{4, 16\}$. Since we have excluded the case $q = 4$ above, it remains to deal with $q = 16$. This case, yet again, has been dealt with a computer computation. Now Lemma 2.2 shows that $t(H) = 1$. □

Lemma 3.4. *Let e be a positive integer, let $q = 3^{2e+1}$ and let H be an almost simple group with socle $S := {}^2G_2(q)$ and with $H \neq S$. Then $t(H) = 1$.*

Proof. Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. Let r be a primitive prime divisor of $q^6 - 1$. From the structure of the Ree groups ${}^2G_2(q)$, we deduce that the Sylow r-subgroups of S are cyclic. Let $x \in S$ be an element generating a Sylow r-subgroup of S. Using the list of the maximal subgroups of S [2, Tables 8.43], we deduce that $|\mathcal{M}(H,x)| = 1$. Indeed, $\mathcal{M}(H,x) = \{\mathbf{N}_H(\langle x\rangle)\}$. From (2.3), we have $P(\theta, x) \leq \mu(\theta, \mathbf{N}_H(\langle x\rangle)\backslash H) < 1$. Now Lemma 2.2 shows that $t(H) = 1$. □

Lemma 3.5. *Let e be a positive integer, let $q = 2^{2e+1}$ and let H be an almost simple group with socle $S := {}^2B_2(q)$ and with $H \neq S$. Then $t(H) = 1$.*

Proof. Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. Let r be a primitive prime divisor of $q^4 - 1$. From the structure of the Suzuki groups ${}^2B_2(q)$, we deduce that the Sylow r-subgroups of S are cyclic. Let $x \in S$ be an element generating a Sylow r-subgroup of S. Using the list of the maximal subgroups of S [2, Tables 8.16], we deduce that $|\mathcal{M}(H,x)| = 1$ and $\mathcal{M}(H,x) = \{\mathbf{N}_H(\langle x\rangle)\}$. Now, the proof follows as in the proof of Lemma 3.4. □

Lemma 3.6. *Let e be a positive integer with $e \geq 1$, let $q = 3^e$ and let H be an almost simple group with socle $S := G_2(q)$ and with H containing an outer automorphism which is not a field automorphism. Then $t(H) = 1$.*

Proof. Recall that $|\mathrm{Aut}(S) : S| = 2e$. When $e = 1$, we have checked the veracity of this lemma with the computer algebra system `magma` [1]. Therefore for the rest of the argument we suppose $e \geq 2$.

Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. Let r be a primitive prime divisor of $q^6 - 1$. From the structure of the Lie group $G_2(q)$, we deduce that the Sylow r-subgroups of S are cyclic. Let $x \in S$ be an element generating a Sylow r-subgroup of S. Let $M \in \mathcal{M}(H,x)$. Here we use the information in [2, Table 8.42]. From the list of the maximal subgroups of H and recalling that H does contain an outer automorphism which is not a field automorphism, we deduce that either $M = \mathbf{N}_H(\langle x\rangle)$, or e is odd and $M \cap S \cong {}^2G_2(q)$ (here we are assuming $e \geq 2$). In particular, when e is even, we have $\mathcal{M}(H,x) = \{\mathbf{N}_H(\langle x\rangle)\}$. Therefore, we deduce

$$\sum_{M\in\mathcal{M}(H,x)} \mu(\theta, M\backslash H) = \mu(\theta, \mathbf{N}_H(\langle x\rangle)\backslash H) < 1,$$

and hence $t(H,K) = 1$, from Lemma 2.2.

Suppose now that e is odd and let $\bar{M} \in \mathcal{M}(H,x) \setminus \{\mathbf{N}_H(\langle x\rangle)\}$. Then $\bar{M} \cap S \cong {}^2G_2(q)$. Observe that from the "c" column in [2, Table 8.42], we deduce that the maximal subgroups of H with $\bar{M} \cap S$ isomorphic to ${}^2G_2(q)$ form a unique conjugacy class. Observe that

$$q^6 - 1 = (q^3-1)(q+1)(q+\sqrt{3q}+1)(q-\sqrt{3q}+1).$$

In particular, the primitive prime divisor r of q^6-1 can be chosen so that r divides $q+\sqrt{3q}+1$. Let $\Omega_1 := \{\langle x^g\rangle \mid g \in H\}$. Using the information in [2, Table 8.42], we deduce

$$|\Omega_1| = \frac{q^6(q^6-1)(q^2-1)}{(q^2-q+1)6} = \frac{q^6(q^3-1)(q^2-1)(q+1)}{6}.$$

Let $\Omega_2 := \{\bar{M}^g \mid g \in H\}$. Using the information in [2, Table 8.42], we deduce

$$|\Omega_2| = \frac{q^6(q^6-1)(q^2-1)}{(q^3+1)q^3(q-1)} = q^3(q^3-1)(q+1).$$

Now, consider the bipartite graph having vertex set $\Omega_1 \cup \Omega_2$ and having edge set consisting of the pairs $\{A, B\}$ with $A \in \Omega_1$, $B \in \Omega_2$ and $A \leq B$. Fix $B \in \Omega_2$. Using the structure of the Ree group B, we see that the number of $A \in \Omega_1$ with $A \leq B$ is

$$\frac{(q^3+1)q^3(q-1)}{(q+\sqrt{3q}+1)6} = \frac{(q-\sqrt{3q}+1)q^3(q^2-1)}{6}.$$

In particular, the number of edges of the bipartite graph is

$$|\Omega_2|\frac{(q-\sqrt{3q}+1)q^3(q^2-1)}{6} = \frac{q^6(q^3-1)(q^2-1)(q-\sqrt{3q}+1)(q+1)}{6}.$$

This shows that the number of elements in Ω_2 containing the element $\bar{M} \in \Omega_1$ is

$$\frac{\frac{q^6(q^3-1)(q^2-1)(q-\sqrt{3q}+1)(q+1)}{6}}{|\Omega_1|} = q - \sqrt{3q} + 1.$$

Thus

$$|\mathcal{M}(H,x)| = |\{\mathbf{N}_H(\langle x \rangle)\} \cup \{M \in \Omega_2 \mid x \in M\}| = q - \sqrt{3q} + 2.$$

From [11, Theorem 1], we have $\mu(\theta, M\backslash H) < 1/(q^2-q+1)$ for every $M \in \mathcal{M}(\theta, M \setminus H)$. Therefore

$$\sum_{M \in \mathcal{M}(H,x)} \mu(\theta, M\backslash H) \leq \frac{q-\sqrt{3q}+2}{q^2-q+1} < 1.$$

Now Lemma 2.2 shows that $t(H) = 1$. □

Lemma 3.7. *Let e be a positive integer with $e \geq 2$, let $q = 2^e$ and let H be an almost simple group with socle $S := \mathrm{Sp}_4(q)$ and with H containing an outer automorphism which is not a field automorphism. Then $t(H) = 1$.*

Proof. Recall that $|\mathrm{Aut}(S) : S| = 2e$. Let $K \leq H$ with $H = KS$ and let $\theta \in K \setminus S$. Let r be a primitive prime divisor of $q^4 - 1$. From the structure of the classical group $\mathrm{Sp}_4(q)$, we deduce that the Sylow r-subgroups of S are cyclic. Let $x \in S$ be an element generating a Sylow r-subgroup of S.

Let $M \in \mathcal{M}(H, x)$. Here we use the information in [2, Table 8.14]. From the list of the maximal subgroups of H and recalling that H does contain an outer automorphism which is not a field automorphism, we deduce that either $M = \mathbf{N}_H(\langle x \rangle)$, or e is odd and $M \cap S \cong {}^2B_2(q)$. In particular, when e is even, we have $\mathcal{M}(H, x) = \{\mathbf{N}_H(\langle x \rangle)\}$. Therefore, we deduce

$$\sum_{M \in \mathcal{M}(H,x)} \mu(\theta, M\backslash H) = \mu(\theta, \mathbf{N}_H(\langle x \rangle)\backslash H) < 1,$$

and hence $t(H, K) = 1$, from Lemma 2.2.

Suppose now that e is odd and let $\bar{M} \in \mathcal{M}(H, x) \setminus \{\mathbf{N}_H(\langle x \rangle)\}$. Then $\bar{M} \cap S \cong {}^2B_2(q)$. Observe that from the "c" column in [2, Table 8.14], we deduce that the maximal subgroups of H with $\bar{M} \cap S$ isomorphic to ${}^2B_2(q)$ form a unique conjugacy class. Observe that

$$q^4 - 1 = (q^2-1)(q+\sqrt{2q}+1)(q-\sqrt{2q}+1).$$

In particular, the primitive prime divisor r of q^4-1 can be chosen so that r divides $q+\sqrt{2q}+1$. Let $\Omega_1 := \{\langle x^g \rangle \mid g \in H\}$. Using the information in [2, Table 8.14], we deduce

$$|\Omega_1| = \frac{q^4(q^4-1)(q^2-1)}{(q^2+1)4} = \frac{q^4(q^2-1)^2}{4}.$$

Let $\Omega_2 := \{\bar{M}^g \mid g \in H\}$. Using the information in [2, Table 8.14], we deduce

$$|\Omega_2| = \frac{q^4(q^4-1)(q^2-1)}{(q^2+1)q^2(q-1)} = q^2(q^2-1)(q+1).$$

How, consider the bipartite graph having vertex set $\Omega_1 \cup \Omega_2$ and having edge set consisting of the pairs $\{A, B\}$ with $A \in \Omega_1$, $B \in \Omega_2$ and $A \leq B$. Fix $B \in \Omega_2$. Using the structure of the Suzuki group B, we see that the number of $A \in \Omega_1$ with $A \leq B$ is

$$\frac{(q^2+1)q^2(q-1)}{(q+\sqrt{2q}+1)4} = \frac{(q-\sqrt{2q}+1)q^2(q-1)}{4}.$$

In particular, the number of edges of the bipartite graph is

$$|\Omega_2|\frac{(q-\sqrt{2q}+1)q^2(q-1)}{4} = \frac{q^4(q^2-1)^2(q-\sqrt{2q}+1)}{4}.$$

This shows that the number of elements in Ω_2 containing the element $\bar{M} \in \Omega_1$ is

$$\frac{\frac{q^4(q^2-1)^2(q-\sqrt{2q}+1)}{4}}{|\Omega_1|} = q - \sqrt{2q} + 1.$$

Thus
$$|\mathcal{M}(H,x)| = |\{\mathbf{N}_H(\langle x\rangle)\} \cup \{M \in \Omega_2 \mid x \in M\}| = q - \sqrt{2q} + 2.$$

Now, [4, Theorem 1] yields $\mu(\theta, M\backslash H) \leq |\theta^H|^{-\frac{1}{4}} = |H : \mathbf{C}_H(\theta)|^{-\frac{1}{4}}$ for every $M \in \mathcal{M}(H,x)$. As θ is an outer automorphism which is not a field automorphism and as e is odd, replacing θ with a suitable power, we may suppose that θ is an involution and that θ is a graph-field automorphism. From [7], we deduce that $\mathbf{C}_S(\theta) \cong {}^2B_2(q)$ and hence
$$|\theta^H| = \frac{q^4(q^4-1)(q^2-1)}{(q^2+1)q^2(q-1)} = q^2(q^2+1)(q+1).$$

Therefore
$$\sum_{M\in\mathcal{M}(M,x)} \mu(\theta, M\backslash H) \leq \frac{q-\sqrt{2q}+2}{(q^2(q^2+1)(q+1))^{1/4}} < 1,$$
where the last inequality follows with a computation. Now Lemma 2.2 shows that $t(H) = 1$. □

Lemma 3.8. *Let H be an almost simple group with socle S. Then there exists a subgroup K of H with $H = KS$ and with $m_K(H) > t(H)$.*

Proof. Suppose first $H = S$. Choose $K := 1$. Then $m_K(H) = m(H) \geq 3$, because we can generate $H = S$ with conjugated involutions. Therefore, the proof follows from (2.1). Thus, for the rest of the argument, we suppose $H \neq S$. Now, we use the Classification of Finite Simple Groups and we divide our proof depending on the type of S.

Alternating groups: Suppose S is an alternating group $\mathrm{Alt}(n)$ of degree $n \geq 5$. Assume first $n \neq 6$, or $n = 6$ and $H = \mathrm{Sym}(6)$. Then $H = \mathrm{Sym}(n)$. Choose $K := \langle(1,2)\rangle$ and let
$$\Lambda := \{(1,2,3), (1,2)(3,4), (1,2)(3,5), \ldots, (1,2)(3,n)\}.$$
It is readily seen that Λ is a K-independent generating set for H. Therefore, $m_K(H) \geq |\Lambda| = n-2 \geq 3$ and the proof follows again from (2.1).

As $\mathrm{Alt}(6) \cong \mathrm{PSL}_2(9)$, we postpone the proof of the case $n = 6$ and $H \neq \mathrm{Sym}(6)$, when we deal with groups of Lie type.

Sporadic groups: Suppose S is a sporadic simple group. As $H \neq S$, we deduce $H = \mathrm{Aut}\, S$ and S is one of the following groups
$$Fi_{22}, Fi_{24}, HN, J_3, M_{22}, O'N, HS, J_2, McL, He, M_{12}, Suz.$$

If $S \in \{Fi_{22}, Fi_{24}, HN, J_3, M_{22}, O'N\}$, then it follows from [3, Table 9] that $t(H) = 1$. However, if we choose α an involution from $H \setminus S$ and we set $K := \langle\alpha\rangle$, then $m_K(H) \geq 2$, because we can generated H with α and a suitable number (at least 2) of involutions from S.

If $S \in \{HS, J_2, McL, He, M_{12}, Suz\}$, we have verified that $m_K(H) \geq 3$ using `magma`: in all cases there exists $\alpha \in H \setminus S$ with $|\alpha| = 2$ and three conjugated involutions in S such that $\{\alpha, t_1, t_2, t_3\}$ is a $\langle\alpha\rangle$-independent generating set for H.

Groups of Lie type: Here we use the information and the notation in [7, Section 2.4]. The simple group of Lie type S is generated by root elements $x_{\pm\hat{\alpha}}(t)$, where $\alpha \in \Pi$, Π is a fundamental system for the root system Σ of S, and t lies in a suitable finite field $\mathbb{F}$. As $x_{\hat{\alpha}}(t)$ is unipotent, $x_{\hat{\alpha}}(t)$ has prime order and hence it is a *pp*-element.

The action of the automorphism group of S on the root elements $x_{\pm\hat{\alpha}}(t)$ is described in [7, Section 2.5] and again we use the information and the notation therein. The outer automorphisms of S are divided in inner-diagonal, field and graph automorphisms. These can be chosen so that inner-diagonal and field automorphisms normalize each root subgroup $\langle x_{\hat{\alpha}}(t) \mid t \in \mathbb{F}\rangle$; whereas, graph automorphisms permute the root subgroups according to the action of the graph automorphism on the nodes of the Dynkin diagram. In particular, we may choose a supplement K of S in H so that the elements in K consist of inner-diagonal, field and graph automorphisms, with respect to the choice of the root system Σ. Now, let $\tilde{\Pi} \subseteq \Pi$ be a set of representatives of the orbits for the action of K on Π. Then
$$H = \langle K, x_{\hat{\alpha}}(t) \mid \alpha \in \pm\tilde{\Pi}, t \in \mathbb{F}\rangle$$
and hence from the set $\{x_{\hat{\alpha}}(t) \mid \alpha \in \pm\tilde{\Pi}, t \in \mathbb{F}\}$ we may extract a K-independent generating set Y for H consisting of *pp*-elements. For each $\beta \in \pm\Pi$, define $S_\beta := \langle x_{\hat{\alpha}}(t) \mid \alpha \in \pm\Pi \setminus \{\beta\}, t \in \mathbb{F}\rangle$. Observe that S_β is contained in a proper parabolic subgroup of S normalized by K. This implies $|Y| \geq 2|\tilde{\Pi}|$. A direct inspection on the various root systems gives that one of the following holds:

(1) $|\tilde{\Pi}| \geq 2$, or
(2) S is a simple group of Lie type of Lie rank 1, that is, $S \in \{A_1(q) = \mathrm{PSL}_2(q),\ {}^2A_2(q) = \mathrm{PSU}_3(q),\ {}^2B_2(q),\ {}^2G_2(q)\}$, or
(3) $S = A_2(q) = \mathrm{PSL}_3(q)$ and $H \nleq \mathrm{P\Gamma L}_3(q)$,
(4) $S = B_2(q) = \mathrm{PSp}_4(q)$, $q = 2^e$ for some $e \geq 1$ and H contains an outer automorphism which is not a field automorphism,
(5) $S = G_2(q)$, $q = 3^e$ for some $e \geq 1$, and H contains an outer automorphism which is not a field automorphism.

If (1) holds, then the proof follows from (2.1). In the remaining cases, we have shown in Lemmas 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 and 3.7 that $t(H) = 1$. Using this slight refinement on the value of $t(H)$ and repeating the argument above for the remaining groups we deduce $m_K(H) \geq 2 > 1 = t(H)$. □

3.2. **Pulling the threads of the argument.**

Proof of Theorem 1.1. We argue by contradiction and among all non-soluble $\mathcal{B}_{pp}$-groups we choose G having minimal order.

Let N be a minimal normal subgroup of G. From Lemma 2.4, G/N is a $\mathcal{B}_{pp}$-group and hence, from our minimal choice of G, we deduce that

$$G/N \text{ is solvable.} \tag{3.1}$$

Suppose that G has two distinct minimal normal subgroups N_1 and N_2. Since $N_1 \cap N_2 = 1$, G embeds into the cartesian product $G/N_1 \times G/N_2$. As G/N_1 and G/N_2 are both solvable, we deduce that G is solvable, which is a contradiction. Therefore, G has a unique minimal normal subgroup N, that is, G is monolithic.

If N is abelian, then G is solvable by (3.1), which is a contradiction. Therefore, N is non-abelian and hence $N \cong S^n$, for some non-abelian simple group S. Write $N := S_1 \times \cdots \times S_n$, where $S_1, \ldots, S_n$ are the simple direct factors of N. Let H be the subgroup of $\mathrm{Aut}(S)$ induced by the conjugacy action of $\mathbf{N}_G(S_1)$ on S. Clearly, H is an almost simple group with socle S. Moreover, since G is monolithic, G embeds into the wreath product $H \wr \mathrm{Sym}(n)$ and hence, without loss of generality, we may assume that G is a subgroup of $H \,\mathrm{wr}\, \mathrm{Sym}(n)$ with $S^n \leq G$ and with

$$\pi : \mathbf{N}_G(S_1) \to H$$

projecting onto H. In particular, we may write the elements of G as ordered pairs $f\sigma$, with $f \in H^n$ and $\sigma \in \mathrm{Sym}(n)$.

Let

$$m_1 = m(G/N).$$

Let

$$Y = \{g_1, \ldots, g_{m_1}\}$$

be a set of *pp*-elements of G with $\{g_1N, \ldots, g_{m_1}N\}$ a *pp*-base for G/N.

Let

$$K := \pi(\mathbf{N}_{\langle Y\rangle}(S_1)).$$

As $G = \langle Y\rangle N$, from the modular law we get

$$\mathbf{N}_G(S_1) = \mathbf{N}_G(S_1) \cap G = (\mathbf{N}_G(S_1) \cap \langle Y\rangle)N = \mathbf{N}_{\langle Y\rangle}(S_1)N.$$

Thus

$$H = \pi(\mathbf{N}_G(S_1)) = \pi(\mathbf{N}_{\langle Y\rangle}(S_1))\pi(N) = KS.$$

Let X be a set of *pp*-elements in S with $H = \langle X, K\rangle$ and having cardinality $t(H, K)$. Let

$$\tilde{X} := \{(x, \underbrace{1, \ldots, 1}_{n-1 \text{ times}}) \in N \mid x \in X\}$$

and observe that $\tilde{X} \subseteq S^n = N \leq G \leq H \,\mathrm{wr}\, \mathrm{Sym}(n)$.

As N is a minimal normal subgroup of G, G acts transitively by conjugation on the set $\{S_1, \ldots, S_n\}$ of simple direct factors of N. From this, it follows that $Y \cup \tilde{X}$ is a generating set for G. As $Y \cup \tilde{X}$ consists of *pp*-elements and as all *pp*-bases of G have the same cardinality, we get $m_{pp}(G) \leq m_1 + t(H, K) \leq m_1 + t(H)$. Thus

$$m(G) \leq m_1 + t(H), \tag{3.2}$$

by Lemma 2.3.

Recall the definition of $\mu(G)$ and $\mu(S)$ in Section 2.1. In [14, page 403, inequality (1)] and in [13, Proposition 4], it is proved that $\mu(G) \geq \mu(H)$. Moreover, by [13, Lemma 7], we have $\mu(H) \geq m_K(H)$, for every subgroup K of H with $H = KS$. In particular, combining these two results, we deduce $\mu(G) \geq m_K(H)$. From (3.2), we get

$$t(H) \geq m(G) - m_1 = m(G) - m(G/N) = \mu(G) \geq m_K(H),$$

for every subgroup K of H with $H = KS$. However, this contradicts Lemma 3.8. □

Proof of Corollary 1.2. Let G be a $\mathcal{B}_{pp}$-group with $\Phi(G) = 1$. From Theorem 1.1, G is solvable and hence the proof now follows from [16, Theorem 1.2]. □

4. Proof of Theorem 1.3

Let G be a finite group. Take a chief series

$$1 = G_t \trianglelefteq \cdots \trianglelefteq G_0 = G$$

and consider the non-negative integers $\mu_i = m(G/G_{i+1}) - m(G/G_i)$. Clearly

$$m(G) = \sum_{0\leq i\leq t-1} \mu_i. \tag{4.1}$$

Information on the values of μ_i have been obtained in [13], where is it proved in particular:

- if G_i/G_{i+1} is abelian, then $\mu_i = 0$ if $G_{i+1}/G_i \leq \Phi(G/G_{i+1})$, $\mu_i = 1$ otherwise;
- if G_i/G_{i+1} is non-abelian, then $\mu_i = \mu_i(L_i) = m(L_i) - m(L_i/\operatorname{soc} L_i)$, where $L_i = G/C_G(G_i/G_{i+1})$.

In the second case, L_i is a monolithic group and $\operatorname{soc} L_i = S_i^{n_i}$ where n_i is a positive integer and S_i is a finite non-abelian simple group. As we already recalled in the previous section, by [14, page 403, inequality (1)] and [13, Proposition 4], there exists an almost simple group H_i such that $\operatorname{soc} H_i = S_i$ and $\mu_i = \mu(L_i) \geq \mu(H_i)$. Moreover, by [13, Lemma 7], we have $\mu(H_i) \geq m_{K_i}(H_i)$, for every subgroup K_i of H_i with $H_i = K_iS_i$. By the results in Section 3, for every choice of H_i there exists K_i such that $K_iS_i = H_i$ and $m_{K_i}(H_i) \geq 2$. So $\mu_i \geq 2$ whenever G_i/G_{i+1} is non-abelian, and therefore the statement of Theorem 1.3 follows from (4.1).

References

[1] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (3-4) (1997), 235–265.
[2] J. H. Bray, D. F. Holt, C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*, London Mathematical Society, Lecture Note Series **407**, Cambridge University Press, 2013.
[3] T. Breuer, R. M. Guralnick and W. M. Kantor, Probabilistic generation of finite simple groups, II, *J. Algebra* **320** (2008), 443–494.
[4] T. C. Burness, Fixed point ratios in actions of finite classical groups. I, *J. Algebra* **309** (2007), 69–79.
[5] T. C. Burness, S. Guest, On the uniform spread of almost simple linear groups, *Nagoya Math. J.* **209** (2013), 35–109.
[6] W. Feit, On large Zsigmondy primes, *Proc. Amer. Math. Soc.* **102** (1988), 26–36.
[7] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups. number 3. part I. chapter A*, **40** (1998), xvi+419.
[8] R. M. Guralnick, W. M. Kantor, Probabilistic generation of finite simple groups, *J. Algebra* **234** (2000), 743–792.
[9] C. S. H. King, Generation of finite simple groups by an involution and an element of prime order, *J. Algebra* **478** (2017), 153–173.
[10] J. Krempa, A. Stocka, On some sets of generators of finite groups, *J. Algebra* **405** (2014), 122–134.
[11] R. Lawther, M. W. Liebeck, G. M. Seitz, Fixed point ratios in actions of finite exceptional groups of Lie type, *Pacific J. Math.* **205** (2002), 393–464.
[12] M. W. Liebeck, J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of Riemann surfaces, *Proc. London Math. Soc. (3)* **63** (1991) 266–314.
[13] A. Lucchini, The largest size of a minimal generating set of a finite group, *Arch. Math.* (Basel) **101** (2013), no. 1, 1–8.
[14] A. Lucchini, Minimal generating sets of maximal size in finite monolithic groups, *Arch. Math.* (Basel) **101** (2013), no. 5, 401–410.
[15] M. Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997), 1913–1919.
[16] A. Stocka, Sets of prime power order generators of finite groups, *Algebra and Discrete Mathematics* **29** (2020), 129–138.
[17] K. Zsigmondy, Zur Theorie der Potenzreste, *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284.

Andrea Lucchini, Dipartimento di Matematica "Tullio Levi-Civita",
University of Padova, Via Trieste 63, 35121 Padova, Italy
Email address: lucchini@math.unipd.it

Pablo Spiga, Dipartimento di Matematica Pura e Applicata,
University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy
Email address: pablo.spiga@unimib.it