ON THE $p$-WIDTH OF FINITE SIMPLE GROUPS

BY

ALEXANDER J. MALCOLM

School of Mathematics, University of Bristol
Bristol BS8 1UG, UK
and
The Heilbronn Institute for Mathematical Research, Bristol, UK
e-mail: alex.malcolm@bristol.ac.uk

ABSTRACT

In this paper we measure how efficiently a finite simple group $G$ is generated by its elements of order $p$, where $p$ is a fixed prime. This measure, known as the $p$-width of $G$, is the minimal $k \in \mathbb{N}$ such that any $g \in G$ can be written as a product of at most $k$ elements of order $p$. Using primarily character theoretic methods, we sharply bound the $p$-width of some low rank families of Lie type groups, as well as the simple alternating and sporadic groups.

1. Introduction

The generation of finite simple groups has been a thriving area of research for many years. Since it was established that every finite simple group is generated by a pair of elements (Steinberg [24] and Aschbacher–Guralnick [2]) many interesting refinements have been investigated: for instance, determining the existence of generators with prescribed orders (see [4] and the references therein).

More recently, the notion of width has provided an additional perspective with which to view generation, giving a measure of how efficiently a given subset generates the group. More formally, suppose $G$ is a finite group generated by a subset $S$, and for $g \in G$, let

$$w(g) = \min\{k \mid g = s_1 \cdots s_k, \ s_i \in S\}.$$
Then the width is defined as

$$\text{width}(G, S) = \max_{g \in G} w(g).$$

Equivalently, width$(G, S)$ is the diameter of $\Gamma(G, S)$, the Cayley graph of $G$ with respect to $S$. Now if $G$ is a non-abelian finite simple group, then any nontrivial normal subset $S$ will generate $G$, and a number of interesting cases have been considered in the recent literature. For example, [18] settles the long-standing conjecture of Ore that every element is a commutator (i.e., the commutator width is one). Furthermore, it is shown in [19] that $G$ has width two with respect to its set of squares.

In this work we consider the width of (non-abelian) finite simple groups with respect to elements of a fixed prime order: suppose that a prime $p$ divides $|G|$ and denote the set of order $p$ elements by $I_p(G)$. Then we consider

$$w_p(G) := \text{width}(G, I_p(G))$$

and call this the $p$-width of $G$.

The case where $p = 2$ (also known as the involution width) has received considerable attention in previous work. For example, there exists a classification of the so-called strongly real finite simple groups, i.e., those such that $w_2(G) = 2$ (see [8] and the references therein). In fact $w_2(G) \leq 4$ for all finite simple groups [21, Thm. 1] and one can show that this bound is sharp for a number of infinite families (for example, $PSL_n(q)$ such that $n, q \geq 6$ and $\gcd(n, q - 1) = 1$ [16]).

In contrast, existing work on the $p$-width for odd primes is very limited. In [13], the larger generating set $P$ of all $p$-elements is considered and it is shown that $\text{width}(G, P) \leq 70$ for all finite simple groups $G$ [13, 3.8]. We show that this bound can be reduced significantly in many cases (even on restriction to only prime order elements).

**Theorem 1:** Let $G$ be a finite simple group that is either an alternating, sporadic or rank 1 group of Lie type, and let $p$ be an odd prime dividing $|G|$. Then $w_p(G) \leq 3$.

We give more precise results for almost all groups under consideration. For example, in Sections 3 and 4 we describe the exact $p$-width for all rank 1 groups of Lie type and sporadic groups. In most of these cases, the $p$-width of $G$ is actually 2 (see Propositions 3.4–3.7 and Theorem 4.1). Nonetheless, Theorem 1
is sharp: in Section 2 we describe a family of alternating groups of $p$-width 3, for any prime $p \neq 3$. Furthermore, $w_3(PSU_3(q)) = 3$ if and only if $q \equiv 2 \mod 3$ (see Proposition 3.5 below).

It is interesting to compare Theorem 1 to the case where $p = 2$. Whereas $w_2(G) = 2$ for a sporadic simple group $G$ if and only if $G \in \{J_1, J_2\}$, $w_p(G) = 2$ for almost all pairs of odd $p$ and sporadic $G$. In fact, $w_p(G) \leq w_2(G)$ for all odd primes $p$, and all groups considered in Theorem 1 with the exception of $(G, p) = (PSL_2(2^{2l+1}), 3)$.

In [21], one technique for bounding the involution width of $G$ is to reduce to a collection of Lie-type subgroups of low rank where the result is known. We expect that similar methods will be important in classifying the $p$-width of all finite simple groups, and that Theorem 1 will be useful in this endeavour.

Character-theoretic tools are also important in examining problems of width (see Section 3 below), but complete character tables are unknown for groups of Lie type of rank greater than 7. We expect this to be substantially more restrictive in finding sharp bounds for the $p$-width for odd primes than for $p = 2$.

Now for any prime $p$, there exists a constant $c$ (independent of $p$) such that $w_p(G) \leq c$ for all finite simple groups $G$ with $I_p(G) \neq \emptyset$ [20 Cor. 1.5]. Theorem 1 therefore motivates a number of natural questions:

**Question 1:** For a given odd $p$, do there exist groups of Lie type of unbounded rank and $p$-width three?

**Question 2:** Does there exist any finite simple group $G$ and odd prime $p$ such that $w_p(G) > 3$?

We address the former question in Section 5 where we consider classical groups and a connection with Artin’s conjecture, while the latter question will be examined in future work. Computational evidence and the results of this paper suggest a negative answer to Question 2.

**Remarks on notation and structure of the paper.** Throughout, $p$ will denote a fixed prime divisor of $|G|$. The $p$-width of an element $g \in G$, denoted $w_p(g)$, is then the minimal $k \in \mathbb{N}$ such that

$$g \in I_p(G)^k = \{x_1 \cdots x_k \mid x_i \in I_p(G)\}.$$ 

It follows that $w_p(G) = \max_{g \in G} w_p(g)$. Lastly, we denote the $G$-conjugacy class of an element $g$ by $g^G$. 
In Section 2, we bound the p-width of the alternating groups $A_n$, using existing work of Dvir [6] and Bertram [3], as well as a careful consideration of the case $p = 3$ (see Lemma 2.3). Furthermore, for fixed $p$ and increasing $n$, we examine the asymptotic behaviour of $w_p(A_n)$ using work of Larsen and Shalev [17]. The bulk of this paper is then dedicated to the rank 1 Lie type groups and the sporadic groups, in Sections 3 and 4 respectively. Here we translate a study of products of conjugacy classes in $I_p(G)$ into a question concerning irreducible characters via a classical result of Frobenius (see Theorem 3.2). We then utilise known character tables of these groups to sharply bound the p-width. Finally, in Section 5 we remark on groups of Lie type of unbounded rank.

2. Alternating groups

In this Section we consider the simple alternating groups $A_n, n \geq 5$. Our first result, Theorem 2.1, bounds the p-width for any choice of $n$ and $p$. However for a fixed odd prime $p$, we also study the asymptotic behaviour of the p-width, showing in Theorem 2.7 that $w_p(A_n) = 2$ for all but finitely many values of $n$.

**Theorem 2.1:** Fix a prime $p$. The p-width of $A_n, (n \geq p)$ is at most three.

The bound in Theorem 2.1 is sharp for each choice of $p \neq 3$: for example, if $p = 2$ then all but the strongly real groups $A_5, A_6, A_{10}, A_{14}$ have 2-width three [21, 2.3]. Furthermore, if $p \geq 5$ then [3 Thm. 1 and 2] imply that $A_n \neq I_p(A_n)^2$ for the non-empty range $(4p + 3)/3 < n < 2p$. The case $p = 3$ is an interesting exception which we examine separately in Lemma 2.3.

As remarked earlier, the involution width of finite simple groups is well understood and [21, 2.3] proves Theorem 2.1 in the case $p = 2$. We therefore restrict our attention to odd primes. But we note that this has also appeared in the literature before: the p-width of the alternating groups is studied by this author in the unpublished note [22], and Theorem 2.1 is proved there by direct combinatorial methods. Here we present a greatly simplified proof of Theorem 2.1 using existing work of Dvir [6].

First let us establish some notation.
**Definition 2.2:** Let \( g \in S_n \). Denote the support of \( g \) by \( \mu(g) \), the number of non-trivial cycles in the decomposition of \( g \) by \( c^*(g) \) and the number of fixed points by \( \text{fix}(g) \). Lastly, set 
\[
    r(g) := |\mu(g)| - c^*(g).
\]

This notation extends naturally to conjugacy classes.

Before considering the general case, we restrict our attention to \( p = 3 \).

**Lemma 2.3:** The 3-width of \( A_n, n \geq 5 \) is two.

**Proof.** Firstly observe that we can decompose an \( l \)-cycle \( (l \geq 4) \), into a product of a 3-cycle and an \( (l - 2) \)-cycle, in the following two ways:

\[
    (1, \ldots, l) = (1, 2, 3)(4, \ldots, l, 1),
\]

\[
    (1, \ldots, l) = (l - 2, 1, 2, \ldots, l - 3)(1, l - 1, l).
\]

We refer to the decomposition (1) as “breaking and permuting left” as we have broken off a 3-cycle from our initial \( l \)-cycle, and then permuted the entries in the remaining \( (l - 2) \)-cycle one step to the left. Similarly, we refer to (2) as “breaking and permuting right”. In particular, after breaking and permuting left and then right we produce

\[
    (1, \ldots, l) = (1, 2, 3) \cdot (l - 1, 4, \ldots, l - 2) \cdot (4, l, 1).
\]

Now suppose that \( l \geq 5 \) is odd. It is clear from the above that we can write \( g = (1, \ldots, l) \) as a product in \( I_3(G)^2 \) by progressively breaking and permuting left then right, and collecting the product of disjoint 3-cycles on either side. As \( l \) is odd, the middle cycle will reduce in length by 2 at each step, reducing to a 3-cycle itself. In particular, letting \( m = \lceil (l - 1)/2 \rceil \), we write \( g \) as the following product of \( m \) 3-cycles:

\[
    (1, \ldots, l) = \prod_{i=0}^{\lfloor m/2 \rfloor - 1} (l + 1 - 2i, 2i + 2, 2i + 3) \cdot \prod_{i=0}^{\lfloor m/2 \rfloor - 1} (4 + 2i, l - 2i, l - 2i + 1),
\]

where \( l + 1 \) is to be read as 1. We denote this product by \( (1, \ldots, l) = x \cdot y \).

For example, if \( l = 11 \), then breaking and permuting three times to the left and twice to the right yields

\[
    (1, \ldots, 11) = (1, 2, 3) \cdot (10, 4, \ldots, 9) \cdot (4, 11, 1)
\]

\[
    = (1, 2, 3)(10, 4, 5)(8, 6, 7) \cdot (6, 9, 10)(4, 11, 1).
\]
To check that \( x \in I_3(G) \) it suffices to show that \( |\mu(x)| = 3[m/2] \). Well suppose for a contradiction that there exists \( i \leq j \leq \lceil m/2 \rceil - 1 \) such that \( l + 1 - 2i = 2j + 3 \). Rearranging then gives that \( l \leq 4j + 2 \). But
\[
4j + 2 \leq 4([m/2] - 1) + 2 \leq 2m \leq l - 1,
\]
giving us our contradiction. The remaining case follows similarly, as does the proof that \( y \in I_3(G) \). Hence any cycle of odd length \( l \geq 5 \) has 3-width two.

Next consider the product of two disjoint cycles \( g_1g_2 \) of even lengths \( l_1 \) and \( l_2 \). Firstly we apply the same process as above to \( g_1 \), breaking and permuting on the left then right until we have broken off \( (l_1/2 - 1) \) 3-cycles and a 2-cycle remains in the middle. In particular, letting \( m_1/l_1/2 – 1 = m_1 \) then
\[
(1, \ldots, l_1) = \prod_{i=0}^{[m_1/2] - 1} (l_1 + 1 - 2i, 2i + 2, 2i + 3)
\times (2[(m_1 + 1)/2] + 2, 2[(m_1 + 1)/2] + 3)
\times \prod_{i=0}^{[m_1/2] - 1} (4 + 2i, l_1 - 2i, l_1 - 2i + 1).
\]
For ease we relabel this product
\[
(1, \ldots, l_1) = x_1 \cdot (a_1, a_1 + 1) \cdot y_1
\]
and note that if \( m_1 \) is odd, then \( a_1 \notin \mu(x_1) \cup \mu(y_1) \) but \( a_1 + 1 \in \mu(x_1) \setminus \mu(y_1) \). On the other hand, when \( m_1 \) is even, \( a_1 + 1 \notin \mu(x_1) \cup \mu(y_1) \) but \( a_1 \in \mu(y_1) \setminus \mu(x_1) \). In other words, the set \( \{a_1, a_1 + 1\} \) intersects non-trivially with the support of exactly one of \( x_1 \) or \( y_1 \) and this intersection has size one. Furthermore, the non-trivial intersection is determined by whether our final step was to break and permute to the left or to the right (determined by the parity of \( m_1 \)).

Now we constructed this decomposition of \( (1, \ldots, l_1) \) by breaking to the left as the first step. But alternatively, breaking right first would produce a similar decomposition
\[
(1, \ldots, l_1) = x'_1 (a'_1, a'_1 + 1) y'_1
\]
such that \( x'_1, y'_1 \in I_3(G) \)—we leave the details of this to the reader. Crucially, this would then reverse which of \( x'_1 \) on the left, or \( y'_1 \) on the right, intersects non-trivially with the central 2-cycle.
Applying this process to $g_1g_2$ (and recalling that $\mu(g_1) \cap \mu(g_2) = \emptyset$) yields

$$g_1g_2 = x_1(a_1, a_1 + 1)y_1 \cdot x_2(a_2, a_2 + 1)y_2$$

$$= x_1x_2 \cdot (a_1, a_1 + 1)(a_2, a_2 + 1) \cdot y_1y_2,$$

chosen such that $a_1, a_2, a_2 + 1 \notin \mu(x_1x_2)$ and $a_1, a_1 + 1, a_2 + 1 \notin \mu(y_1y_2)$. But

$$(a_1, a_1 + 1)(a_2, a_2 + 1) = (a_1, a_2 + 1, a_2)(a_1, a_2 + 1, a_1 + 1).$$

Hence $x_1x_2(a_1, a_2 + 1, a_2)$ and $(a_1, a_2 + 1, a_1 + 1)y_1y_2$ are elements of order 3, and $w_3(g_1g_2) = 2$ as required.

So we have shown that $w_3(g) = 2$ for $g \in A_n$ which is either a single cycle of odd length at least 5, or a pair of even-length cycles. But any $h \in A_n$ can be written as a disjoint product of such elements plus a number of 3-cycles and so the Lemma follows.  

Let us return to the general case of any odd prime $p$. The crucial result of Dvir is the following:

**Theorem 2.4 ([6, Thm. 10.2]):** Let $C \subset A_n$ be a conjugacy class not containing $2^k$-cycles for $k > 1$ and such that $r(C) \geq \frac{1}{2}(n-1)$. Then

$$C^3 = A_n.$$  

**Corollary 2.5:** Fix a prime $p \geq 3$ and suppose that $n \geq kp$ for some $k \in \mathbb{N}$. Let $C \subset A_n$ be a conjugacy class of elements of cycle type $(p^k, 1^{n-kp})$. If $C^3 \neq A_n$, then

$$n \geq (k+1)p.$$  

**Proof.** Firstly note that $r(C) = k(p-1)$. So if $k = 1$ then (by Theorem 2.1) the assumption that $C^3 \neq A_n$ implies that $(n-1)/2 > p - 1$, which holds if and only if $n > 2p - 1$. Now assume that $k \geq 2$ and suppose for a contradiction that $n < (k+1)p$. Well again by Theorem 2.4 the assumption that $C^3 \neq A_n$ implies that $(n-1)/2 > k(p-1)$. Hence

$$\frac{(k+1)p-1}{2} > k(p-1),$$

and this reduces to $2k-1 > p(k-1)$. But as $p \geq 3$, it follows that $p(k-1) \geq 3k-3$ and we have a contradiction.  

**Proof of Theorem 2.1 for $p \geq 3$.** This is immediate from Corollary 2.5 as $n$ is finite.  

Now that we have bounded the $p$-width of $A_n$, it is interesting to ask whether this bound is sharp asymptotically. Similar asymptotic problems in symmetric groups have been considered by Larsen and Shalev [17]. In particular, the following result will be useful.

**Theorem 2.6 ([17] Thm. 1.10):** For all $\epsilon > 0$ there exists $N_0$ such that for all $n \geq N_0$, if $g \in S_n$ satisfies both

1. $c^*(g) + \text{fix}(g) < \left(\frac{1}{4} - \epsilon\right)n$ and
2. $\text{fix}(g^2) < n^{1/4 - \epsilon},$

then $(g^{S_n})^2 = A_n$.

**Theorem 2.7:** Fix $p \geq 3$. There exists $N$ such that for all $n > N$,

$$w_p(A_n) = 2.$$  

**Proof.** As the case where $p = 3$ is immediate from Lemma [2.3], we restrict our attention to $p \geq 5$. Fix $\epsilon = 1/p^2$ and let $N_0$ be the constant given by Theorem [2.6]. It suffices to show that for sufficiently large $n \geq N_0$, there exists an element $g \in I_p(A_n)$ satisfying conditions (1) and (2) of Theorem [2.6].

Well clearly if $n \geq p$ then $I_p(A_n) \neq \emptyset$, so assuming this, let $g \in I_p(A_n)$ be any element consisting of $\lfloor n/p \rfloor$ disjoint $p$-cycles. Evidently

$$c^*(g) + \text{fix}(g) \leq n/p + (p - 1).$$

It then follows that if

$$n > N_1 := \frac{4p^3 - 4p^2}{p^2 - 4p - 4},$$

then

$$c^*(g) + \text{fix}(g) < \left(\frac{1}{4} - \frac{1}{p^2}\right)n.$$  

Next we note that $\text{fix}(g^2) = \text{fix}(g) \leq p - 1$ and that $n^{1/4 - 1/p^2}$ is strictly increasing in $n$. Hence there exists $N_2$ such that $\text{fix}(g^2) < n^{1/4 - 1/p^2}$ for all $n > N_2$. So letting

$$N := \max\{N_0, N_1, N_2\}$$

it is clear that for all $n > N$, our chosen element $g$ satisfies conditions (1) and (2) and we are done by Theorem [2.6].
3. Low rank groups of Lie type

In this section we consider the \( p \)-width of low-rank groups of Lie type. This includes an examination of all groups of (twisted) rank 1. We recall that the case where \( p = 2 \) is investigated in [21] and so we restrict our attention to odd primes.

Let \( A := \{ \text{PSL}_2(q), \text{PSL}_3^e(q), 2B_2(2^{2n+1}), 2G_2(3^{2n+1}), n \geq 1 \} \).

**Theorem 3.1:** Let \( G \in A \) and let \( p \) be an odd prime dividing \( |G| \). Then \( w_p(G) \leq 3 \).

Width questions are often reduced to studying the product of a given collection of conjugacy classes and that is our general strategy here: given \( g \in G \), we show that \( g \in C_1 \cdots C_k \) for some collection of classes \( C_1, \ldots, C_k \subseteq I_p(G) \). From this it is then immediate that \( w_p(g) \leq k \). The character theory of \( G \) plays an important role via the following well-known result.

**Theorem 3.2** ([I, §1, Thm. 10.1]): Let \( G \) be a finite group, \( C_1, \ldots, C_k \) be conjugacy classes of \( G \) with representatives \( g_1, \ldots, g_k \), and let \( g \in G \). Then \( g \in C_1 \cdots C_k \) if and only if

\[
\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_k) \chi(g^{-1})}{\chi(1)^{k-1}} \neq 0.
\]

The sum in (3) is known as the **normalised structure constant** and we denote it by \( \kappa(C_1, \ldots, C_k, g^G) \). Often the summand for the trivial character is dominant, and to show that \( \kappa \neq 0 \) it suffices to accurately bound character ratios for \( \chi \in \text{Irr}(G) \setminus \{1_G\} \) (for example, see Proposition [3.7] below).

Existing work of Guralnick and Malle [11] will also be useful in the proof of Theorem 3.1. In particular, we use some cases covered by the following result.

**Theorem 3.3** ([II 7.1]): Let \( G \) be a rank 1 finite simple group of Lie type. Let \( C \) be the conjugacy class of an element \( g \) of order \( o(g) > 2 \). Assume that one of the following holds:

1. \( G = \text{PSL}_2(q) \) with \( q \) odd and \( g \) not unipotent;
2. \( G = \text{PSL}_2(q) \) with \( q \) even and \( o(g) \) not divisible by \( q + 1 \);
3. \( G = 2G_2(3^{2n+1}), n \geq 1 \) and \( o(g) \) not divisible by 3;
136 A. J. MALCOLM Isr. J. Math.

(4) \( G = 2B_2(2^{2n+1}), n \geq 1; \) or

(5) \( G = PSU_3(q) \) and \( g \) is regular of order \((q^2 - q + 1)/d \) or \((q^2 - 1)/d \) with \( d = \gcd(3, q + 1) \).

Then \( G \{1\} \subseteq C^2 \).

We consider each of the families listed in Theorem 3.1 individually. For ease of reference we adopt the notation of [1, 23, 15] for the groups \( PSL_2(q), PSL^c(q) \) and \( 2G_2(q^2) \), respectively.

**Proposition 3.4:** Let \( G = PSL_2(q), q \geq 4 \) and let \( p \) be an odd prime dividing \(|G|\). If \( q = 2^{2n+1} \geq 8 \) and \( p = 3 \) then \( w_p(G) = 3 \). Otherwise \( w_p(G) = 2 \).

**Proof.** Firstly assume that \( q = 2^{2n+1} \geq 8 \). Products of conjugacy classes in \( PSL_2(q) \) are considered in [1] and, in particular, the proof of [1, §4, Thm. 4.2] shows that \( C^2 = G \) for all non-trivial conjugacy classes except \( C = R_j, 1 \leq j \leq q/2 \) (see [1] for notation). Note here that \( R_j = (b^j)^G \) for \( b \in G \) an element of order \( q+1 \), and in fact \( R_j^2 \) contains all but the unipotent elements of \( G \).

Now if \( p \mid q - 1 \), it is clear from the conjugacy class descriptions [1, §4] that there exists a class \( C \subset I_p(G) \) such that \( C \neq R_j \). Hence \( w_p(G) = 2 \) by the above. If instead \( 3 \neq p \mid q + 1 \), then \( R_{(q+1)/p} \neq R_{2(q+1)/p} \) are distinct classes in \( I_p(G) \). Furthermore, calculating structure constants explicitly in CHEVIE [10] shows that \( R_{(q+1)/p} \cdot R_{2(q+1)/p} \) contains \( C_2 \), the unique unipotent class, and so again \( w_p(G) = 2 \). It remains to consider the case where \( p = 3 \): well as \( q = 2^{2n+1}, \) it follows that \( 3 \nmid q - 1 \) and that \( R_{(q+1)/3} \) is the unique class of order 3 elements. As remarked above, \( R_{(q+1)/3}^2 \neq G \) and so \( w_3(G) \geq 3 \). But \( C^3 = G \) for all non-trivial classes [1, §4, Thm. 4.2] and so we conclude that \( w_3(G) = 3 \). For other values of \( q \), the proof follows in a very similar manner so we omit the details, but to summarise: Theorem 3.3 gives a reduction to the case where \( p \mid q \) and then any other necessary structure constants can be checked in CHEVIE [10]. 

**Proposition 3.5:** Let \( G = PSU_3(q), q \geq 3 \) and let \( p \) be an odd prime dividing \(|G|\). If \( q \equiv 2 \mod 3 \) and \( p = 3 \), then \( w_p(G) = 3 \), otherwise \( w_p(G) = 2 \).

**Proof.** The proposition is easily checked for \( q \leq 7 \) using the available character tables in GAP [9] and we therefore assume that \( q \geq 8 \). Now products of conjugacy classes in \( G \) (and similarly in \( PSL_3(q) \)) are examined extensively in [23], where structure constants are computed using the generic character tables available in [7]. We use this work to pick appropriate classes in \( I_p(G) \) and bound the \( p \)-width.
Firstly assume that \( q \not\equiv 2 \mod 3 \): here \([23, \text{Thm 1.3 and Table 2}]\) detail exactly when \( 1 \not\in C_a C_b C_c \) for any non-central conjugacy classes \( C_i \subset SU_3(q) \). Recall that

\[
|SU_3(q)| = q^3(q^2 - q + 1)(q + 1)^2(q - 1).
\]

The conjugacy classes of \( SU_3(q) \) are divided into 8 families with representatives given in \([23, \text{Table 1}]\). For example, suppose that \( p \) divides \( q^2 - q + 1 \). If \( p \) also divides \( q + 1 \) then it follows that \( p = 3 \), a contradiction against our earlier assumption. Similarly \( p \mid q - 1 \) and we see that \( C := C_{8\frac{(q^2+1)}{p}} \) is a class of order \( p \) elements in the 8th family of \([23, \text{Table 1}]\). We then check using \([23, \text{Thm 1.3 and Table 2}]\) that \( C_2 \) contains all non-central classes of \( SU_3(q) \), and as \( SU_3(q) = PSU_3(q) = G \) it follows that \( w_p(G) = 2 \). The result follows similarly when \( p \) divides \( q \) or \( q - 1 \). In particular, we find classes in \( I_p(G) \) denoted \( C_3^{(q+1)} \) or \( C_7^{(q+1),(q^2-1)/p} \) respectively (see \([23]\) for notation), and the squares of these classes contain all non-central elements.

The final case to consider is when \( 3 \neq p \) divides \( q + 1 \): here we see from \([23, \text{Table 1}]\) that there exists a collection of prime order classes (which we denote \( \mathcal{C} \)) in the 4th and 6th families. These are

\[
\mathcal{C} = \left\{ C_6^{(\alpha,2\alpha, \frac{(p-3)\alpha}{2})}, C_6^{(\alpha,\beta, \frac{(p-\beta)\alpha}{2})} \mid \alpha := \frac{q+1}{p}, 1 \leq \beta \leq \frac{p-1}{2} \right\} \quad \text{when } p \geq 7;
\]

\[
\mathcal{C} = \left\{ C_4^{(\alpha,\beta, \frac{(5-2\beta)\alpha}{2})}, C_6^{(\alpha,4\alpha,5\alpha)}, C_6^{(2\alpha,3\alpha,5\alpha)} \mid \alpha := \frac{q+1}{5}, 1 \leq \beta \leq 4 \right\} \quad \text{when } p = 5.
\]

Now in general \( G \setminus \{1\} \not\subset C^2 \) for a single \( C \in \mathcal{C} \). However, clearly \( |\mathcal{C}| \geq 3 \) and checking the technical conditions given in \([23, \text{Thm 1.3 and Table 2}]\) (these concern the eigenvalues of the three classes in question) we see that

\[
G \setminus \{1\} \subseteq \bigcup_{C,C' \in \mathcal{C}} CC'.
\]

It then follows again that \( w_p(G) = 2 \).

Lastly, assume that \( q \equiv 2 \mod 3 \). Provided \( p \neq 3 \) then the result follows by picking the same classes as above and considering their images \( \tilde{C} \) in \( PSU_3(q) \). If however \( p = 3 \), then

\[
\tilde{C}_2^{(0)} \not\subset \tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})} = \tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})},
\]
by \textbf{[23]} Cor. 1.8. But $\tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})}$ is the unique class of order three elements and hence $w_3(G) \geq 3$ (in particular, $w_3(g) \geq 3$ for $(J_2, J_1)$-unipotent elements $g \in \tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})}$). But $G = (\tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})})^3$ by \textbf{[23]} Cor. 1.9 and so the 3-width is exactly three.

\textbf{Remark}: The above result demonstrates interesting differences in the behaviour of $w_p(PSU_3(q))$ depending on whether $p$ is odd or even: if $q \equiv 2 \mod 3$ then $w_2(PSU_3(q)) = 3$ but otherwise $w_2(PSU_3(q)) = 4$ \textbf{[21]} Lem. 6.9. Further families of groups where $w_2(G) \geq w_p(G)$ (for all odd $p$) are given in Proposition \textbf{3.7} and Section \textbf{4}.

\textbf{PROPOSITION 3.6}: Let $G = PSL_3(q)$ and let $p$ be an odd prime dividing $|G|$. Then $w_p(g) = 2$.

\textbf{Proof}. Here the proof follows almost exactly as for $PSU_3(q)$ and so we omit the details. To summarise, for each $p$ dividing $q^2 + q + 1$, $q$, $q + 1$ and $q - 1$ we identify a collection of conjugacy classes $C_p$ from the 8th, 3rd, 7th and 6th families respectively (see \textbf{[23]} for notation) such that $C_p \subset I_p(G)$. Examining the conditions given in \textbf{[23]} Thm 1.3 and Table 2] we see that $G \setminus \{1\} \subseteq \bigcup_{C, C' \in C_p} CC'$ for each choice of $p$, and hence $w_p(G) = 2$. Note that despite there being a unique class of order 3 elements (namely $\tilde{C}_6^{(0, \frac{q+1}{3}, \frac{2(q+1)}{3})}$) when $q \equiv 1 \mod 3$, the square of said class does contain the unipotent class $\tilde{C}_2^{(0)}$, unlike the unitary case.

\textbf{PROPOSITION 3.7}: Let $G = 2G_2(q^2)$, $q^2 \geq 27$ and let $p$ be an odd prime dividing $|G|$. Then $w_p(G) = 2$.

\textbf{Proof}. By Theorem \textbf{3.3} it suffices to consider the case $p = 3$. Now the unipotent elements of order 3 fall into three conjugacy classes which we denote $C_3^0$, $C_3^+$ and $C_3^-$—we refer the reader to \textbf{[15]} for a comprehensive description of the classes in $G$ and notation. In particular, $C_3^+$ is a class of non-real elements of order 3, with representative $T$ such that $|C_G(T)| = 2q^4$. Using CHEVIE \textbf{[10]} it is straightforward to confirm that $(C_3^+)^2$ contains all elements of orders 2, 6 and 9. For each remaining element of $G \setminus I_3(G)$, a conjugate is contained in $A_i \cup JA_i$, where $J$ is a representative of the single class of involutions, and $A_i, 0 \leq i \leq 3$ are cyclic Hall subgroups of the following orders:

$|A_0| = \frac{1}{2}(q^2 - 1)$, $|A_1| = \frac{1}{4}(q^2 + 1)$, $|A_2| = q^2 - \sqrt{3}q + 1$, $|A_3| = q^2 + \sqrt{3}q + 1$. 


We check that $G \backslash I_3(G) \subset (C_3^+)^2$ using Theorem 3.2 and the character tables in [26]: for example, consider a cyclic subgroup $A_1$. Non-identity elements in $A_1$ are denoted by $S^a$, and if $\chi \in \text{Irr}(G)$ is such that $\chi(T)^2 \chi(S^{-a}) \neq 0$, then either $\chi \in \{1_G, \xi_2, \xi_5, \xi_6, \xi_7, \xi_8\}$ or $\chi$ is one of a $(q^2 - 3)/6$ characters denoted $\eta_1$ or $\eta'_1$ (see [26]). Here

$$
\begin{align*}
\xi_5(1) &= \xi_7(1) = \frac{q}{2\sqrt{3}}(q^2 - 1)(q^2 + \sqrt{3}q + 1); \\
\xi_6(1) &= \xi_8(1) = \frac{q}{2\sqrt{3}}(q^2 - 1)(q^2 - \sqrt{3}q + 1); \\
\xi_2(1) &= (q^6 - 2q^4 + 2q^2 - 1)/(q^2 - 1); \\
\eta_1(1) &= \eta'_1(1) = q^6 - 2q^4 + 2q^2 - 1.
\end{align*}
$$

Note that $\xi_5(T) = \xi_6(T)$, but $\xi_5(S^{-a}) = -\xi_6(S^{-a})$ and so the corresponding summands in the structure constant formula (see Theorem 3.2) sum to zero. Similarly, the summands for $\xi_7$ and $\xi_8$ sum to zero giving

$$
\kappa(T^G, T^G, (S^a)^G) = 1 + \sum_{\chi \in \{\xi_2\} \cup \{\eta_1 \cup \eta'_1\}} \frac{\chi(T)^2 \chi(S^a)}{\chi(1)}.
$$

Furthermore,

$$
|\xi_2(T)| = |\eta_1(T)| = |\eta'_1(T)| = 1,
$$

whereas $|\xi_2(S^a)| \leq 3$ and $|\eta_1(S^a)| = |\eta'_1(S^a)| \leq 6$. These bounds give

$$
\left| \sum_{\chi \in \{\xi_2\} \cup \{\eta_1 \cup \eta'_1\}} \frac{\chi(T)^2 \chi(S^a)}{\chi(1)} \right| \leq \frac{3(q^2 - 1)}{q^6 - 2q^4 + 2q^2 - 1} + \frac{q^2 - 3}{q^6 - 2q^4 + 2q^2 - 1} = \frac{4q^2 - 6}{q^6 - 2q^4 + 2q^2 - 1} < \frac{4}{q^4 - 2q^2} < 1.
$$

It follows that $\kappa(T^G, T^G, (S^a)^G) \neq 0$ and so $A_1 \subset (C_3^+)^2$. The remaining cases follow similarly, giving $G = I_3(G) \cup (C_3^+)^2$ and hence $w_3(G) = 2$.  

Remark: We note that each class of order 3 elements is a genuine exception to Theorem 3.3 as $C_3^0 \not\subset (C_3^+)^2$ and $C_3^\pm \not\subset (C_3^0)^2$.

Proof of Theorem 3.1: If $G = 2B_2(2^{2n+1})$, $n \geq 1$ then the result is immediate from Theorem 3.3. The remaining cases then follow from Propositions 3.4–3.7.
4. Sporadic groups

Lastly let us consider the sporadic finite simple groups. Again, we find that the width is typically smaller for odd primes than in the case of involutions: whereas $w_2(G) = 2$ for sporadic $G$ only if $G \in \{J_1, J_2\}$ [25, Thm. 1.6], $w_p(G) = 2$ for $p \geq 3$ in almost all cases.

Theorem 4.1: Let $(G, p)$ be a pair consisting of a sporadic finite simple group $G$ and an odd prime $p$, dividing $|G|$. Then $w_p(G) = 2$, unless it is one of the exceptions listed in Table 1, where $w_p(G) = 3$.

Table 1. Sporadic groups with $p$-width 3

| Group | Prime | Width-three Classes       |
|-------|-------|---------------------------|
| HS    | 3     | 4A, 6A                    |
| Co₂   | 3     | 4A                        |
| Co₃   | 3     | 2A                        |
| Fi₂₂  | 3, 5  | 2A, 4A, 6AB, 12D (p = 3); 2A (p = 5) |
| Fi₂₃  | 3, 5  | 2A (p = 3, 5)             |
| BM    | 3     | 2A                        |

Proof. The character tables of the sporadic simple groups are available in GAP [9] and it is easy to calculate the relevant structure constants using Theorem 3.2. We remark that in most cases $G \setminus \{1\} \subseteq C^2$ where $C$ is (one of) the largest conjugacy classes in $I_p(G)$. Exactly which classes are not contained in $I_p(G)^2$ are given in Table 1.

5. Lie type groups of larger rank

In Section 3 we saw that typically the $p$-width is two, for all odd prime divisors of a given low-rank group of Lie type. In particular, the upper bound in Theorem 3.1 is only reached when $p = 3$. However, we do not necessarily expect that this will remain true for groups of arbitrarily large rank, as the following example illustrates.

Proposition 5.1: Let $p \neq l$ be primes such that $p$ is odd and $l$ is a primitive root modulo $p$. Then $G \in \{SL_{p−1}(l), Sp_{p−1}(l)\}$ has $p$-width at least 3.
Proof. Let $\Lambda$ denote the set of non-trivial $p$th roots of unity in $\mathbb{F}_{l(p-1)}$ and let $\sigma : \Lambda \to \Lambda$ be the permutation
\[
\sigma : \lambda \mapsto \lambda^l.
\]
Recall that $l$ primitive modulo $p$ implies that $p$ divides $l^{p-1} - 1$ but not $l^k - 1$ for any $k < p - 1$. It follows that $\sigma$ is transitive on $\Lambda = \Lambda^{-1}$ and so there exists a unique $G$-class, denoted $C$, of elements of order $p$ [5 Sect. 3.2–3.4]. In particular, $C = C^{-1}$ and elements $x \in C$ act irreducibly on $V = \mathbb{F}_l^{p-1}$. Now consider a transvection $t \in G$. As transvections have order $l$, it suffices for the proposition to show that $w_p(t) \neq 2$.

Assuming that $w_p(t) = 2$ for a contradiction, it follows that $t = x_1x_2$ for some $x_i \in C$.

As $x_2$ is conjugate to $x_1^{-1}$ we may write this as a commutator $t = [x_1, y]$ for some $y \in G$, and applying [12 Thm. 9] we see that $H = \langle x_1, y \rangle$ is contained in a Borel subgroup of $G$. It follows that the derived subgroup $H'$ is unipotent and in particular, $H'$ is a non-trivial $l$-group acting naturally on $V$. Considering the fixed points of this action, it is an easy consequence of the orbit-stabiliser theorem that $|V^{H'}| \equiv |V| \equiv 0 \mod l$. But of course $V^{H'}$ contains the zero vector, so in fact $V^{H'}$ is a non-trivial subspace of $V$, which is invariant under $H$. This is clearly a contradiction as $H$ contains irreducible elements from $C$.

It is clear that Proposition 5.1 provides new examples of groups with $p$-width 3, for odd primes $p \neq 3$: for example, $l = 2$ is primitive modulo 5, 11, 13, 19, ... Furthermore, Proposition 5.1 provides an interesting link between the $p$-width of finite groups and the famed conjecture of Artin that any integer $l$ that is neither $\pm 1$ nor a perfect square is a primitive root modulo infinitely many primes [14]:

**Corollary 5.2:** Assume that Artin’s conjecture is true. Then for any prime $l$, there exist groups of Lie type $G(l)$ of arbitrarily large rank and characteristic $l$, such that $w_p(G) \geq 3$ for at least one prime divisor $p$ of $|G|$.

**Proof.** Fix $l$ and let $\{p_i\}_{i \in \mathbb{N}}$ be the primes guaranteed by Artin’s conjecture. Then for $G \in \{SL_{(p_i-1)}(l), Sp_{(p_i-1)}(l)\}_{i \in \mathbb{N}},$
\[
w_{p_i}(G) \geq 3
\]
by Proposition 5.1.

$\blacksquare$
Remark: In particular, Artin’s conjecture asserts that $l = 2$ is primitive modulo infinitely many primes, and so Corollary 5.2 yields two families of simple groups of width at least 3.

Acknowledgements. The author is very grateful to Tim Burness for providing detailed feedback on a previous version of this paper, and to Bob Guralnick for sharing his expertise in a number of helpful conversations.

References

[1] Z. Arad and M. Herzog (eds.), Products of Conjugacy Classes in Groups, Lecture Notes in Mathematics, Vol. 1112, Springer, Berlin, 1985.

[2] M. Aschbacher and R. Guralnick, Some applications of the first cohomology group, Journal of Algebra 90 (1984), 446–460.

[3] E. Bertram, Even permutations as a product of two conjugate cycles, Journal of Combinatorial Theory. Series A 12 (1972), 368–380.

[4] T. C. Burness, Simple groups, generation and probabilistic methods, in Groups St Andrews 2017, London Mathematical Society Lecture Note Series, Vol. 455, Cambridge University Press, Cambridge, 2019, pp. 200-229.

[5] T. C. Burness and M. Giudici, Classical Groups, Derangements and Primes, Australian Mathematical Society Lecture Series, Vol. 25, Cambridge University Press, Cambridge, 2016.

[6] Y. Dvir, Covering properties of permutation groups, in Products of Conjugacy Classes in Groups, Lecture Notes in Mathematics, Vol. 1112, Springer, Berlin, 1985, pp. 197–221.

[7] J. S. Frame and W. A. Simpson, The character tables for $SL_3(q)$, $SU_3(q^2)$, $PSL_3(q)$, $PSU_3(q^2)$, Canadian Journal of Mathematics 25 (1973), 486–494.

[8] A. A. Gal’t and E. P. Vdovin, Strong reality of finite simple groups, Siberian Mathematical Journal 51 (2010), 610–615.

[9] The GAP Group, GAP—Groups, Algorithms, and Programming, Version 4.7.7, http://www.gap-system.org.

[10] M. Geck, G. Hiss, F. Lübeck, G. Malle and G. Pfeiffer, CHEVIE—A system for computing and processing generic character tables for finite groups of Lie Type, Weyl groups and Hecke algebras, Applicable Algebra in Engineering, Communication and Computing 7 (1996), 175–210.

[11] R. Guralnick and G. Malle, Products of conjugacy classes and fixed point spaces, Journal of the American Mathematical Society 25 (2012), 77–121.

[12] R. Guralnick and G. Malle, Products and commutators of classes in algebraic groups, Mathematische Annalen 362 (2015), 743–771.

[13] R. M. Guralnick and P. H. Tiep, Effective results on the Waring problem for finite simple groups, American Journal of Mathematics 137 (2015), 1401–1430.

[14] C. Hooley, On Artin’s conjecture, Journal für die Reine und Angewandte Mathematik 225 (1967), 209–220.

[15] G. A. Jones, Ree groups and Riemann surfaces, Journal of Algebra 165 (1994), 41–62.
[16] F. Knüppel and K. Nielsen, $SL(V)$ is 4-reflectional, Geometriae Dedicata 38 (1991), 301–308.
[17] M. Larsen and A. Shalev, Characters of symmetric groups: sharp bounds and applications, Inventiones Mathematicae 174 (2008), 645–687.
[18] M. W. Liebeck, E. A. O’Brien, A. Shalev and P. H. Tiep, The Ore conjecture, Journal of the European Mathematical Society 12 (2010), 939–1008.
[19] M. W. Liebeck, E. A. O’Brien, A. Shalev and P. H. Tiep, Products of squares in finite simple groups, Proceedings of the American Mathematical Society 140 (2012), 21–33.
[20] M. W. Liebeck and A. Shalev, Diameters of finite simple groups: sharp bounds and applications, Annals of Mathematics 154 (2001), 383–406.
[21] A. J. Malcolm, The involution width of finite simple groups, Journal of Algebra 493 (2018), 297–340.
[22] A. J. Malcolm, The $p$-width of the alternating groups, https://arxiv.org/abs/1710.04972
[23] S. Orevkov, Products of conjugacy classes in finite unitary groups $GU_3(q^2)$ and $SU_3(q^2)$, Annales de la Faculté des Sciences de Toulouse. Mathématiques 22 (2013), 219–251.
[24] R. Steinberg, Generators for simple groups, Canadian Journal of Mathematics 14 (1962), 277–283.
[25] I. Suleiman, Strongly real elements in alternating and sporadic groups, Jordan Journal of Mathematics and Statistics 1 (2008), 97–103.
[26] H. N. Ward, On Ree’s series of simple groups, Transactions of the American Mathematical Society 121 (1966), 62–89.