

ENUMERATION OF GROUPS IN SOME SPECIAL VARIETIES OF A -GROUPS

ARUSHI  and GEETHA VENKATARAMAN  

(Received 3 March 2024; accepted 29 April 2024)

Abstract

We find an upper bound for the number of groups of order n up to isomorphism in the variety $\mathfrak{S} = \mathfrak{A}_p\mathfrak{A}_q\mathfrak{A}_r$, where p , q and r are distinct primes. We also find a bound on the orders and on the number of conjugacy classes of subgroups that are maximal amongst the subgroups of the general linear group that are also in the variety $\mathfrak{A}_q\mathfrak{A}_r$.

2020 *Mathematics subject classification*: primary 20E10; secondary 20B15, 20B35, 20D10, 20E45, 20H30.

Keywords and phrases: group enumeration, variety of groups, general linear group, symmetric group, transitive subgroup, primitive subgroup, conjugacy class.

1. Introduction

A group is an A -group if its nilpotent subgroups are abelian. For any class of groups \mathfrak{B} , we denote the number of groups of order n up to isomorphism by $f_{\mathfrak{B}}(n)$. Computing $f(n)$ becomes harder as n gets bigger. Thus, in the area of group enumerations, we attempt to approximate $f(n)$. When counting is restricted to the class of abelian groups, A -groups or groups in general, the asymptotic behaviour of $f(n)$ varies significantly. Let $f_{A,\text{sol}}(n)$ be the number of isomorphism classes of soluble A -groups of order n . Dickenson [2] showed that $f_{A,\text{sol}}(n) \leq n^{c \log n}$ for some constant c . McIver and Neumann [7] showed that the number of nonisomorphic A -groups of order n is at most $n^{\lambda+1}$, where λ is the number of prime divisors of n including multiplicities. In the same paper, they stated the following conjecture based on a result of Higman [4] and Sims [12] on p -group enumerations.

CONJECTURE 1.1. Let $f(n)$ be the number of (isomorphism classes of groups of) order n . Then $f(n) \leq n^{(2/27+\epsilon)\lambda^2}$, where $\epsilon \rightarrow 0$ as $\lambda \rightarrow \infty$.

In 1993, Pyber [9] proved a powerful version of Conjecture 1.1: the number of groups of order n with specified Sylow subgroups is at most $n^{75\mu+16}$, where μ is the

largest integer such that p^μ divides n for some prime p . From the results of Higman and Sims, and Pyber, $f(n) \leq n^{2\mu^2/27+O(\mu^{5/3})}$. In [13], it was shown that $f_{A,sol}(n) \leq n^{7\mu+6}$.

The variety $\mathfrak{A}_u\mathfrak{A}_v$ consists of all groups G with an abelian normal subgroup N of exponent dividing u such that G/N is abelian of exponent dividing v . (For more on varieties, see [8].) Let p, q and r be distinct primes. In this paper, we find a bound for $f_\mathfrak{S}(n)$, where $\mathfrak{S} = \mathfrak{A}_p\mathfrak{A}_q\mathfrak{A}_r$, and $f_\mathfrak{S}(n)$ counts the groups in \mathfrak{S} of order n up to isomorphism. The idea behind studying the variety \mathfrak{S} is that enumerating within the varieties of A -groups might yield a better upper bound for the enumeration function for A -groups. The ‘best’ bounds for A -groups, or even soluble A -groups, still lack the correct leading term. It is believed that a correct leading term for the upper bound of A -groups would lead to the right error term for the enumeration of groups in general.

A few smaller varieties of A -groups have already been studied in [1, Ch. 18]. The class of A -groups for which the ‘best’ bounds exist was obtained by enumerating in such small varieties of A -groups, but this did not narrow the difference between the upper and lower bounds for $f_{A,sol}(n)$ because these groups did not contribute a large enough collection of A -groups. Hence, a good lower bound could not be reached. To reduce the difference, we enumerate in the larger variety \mathfrak{S} of A -groups.

Throughout the paper, p, q, r and t are distinct primes. We assume that s is a power of t . We take logarithms to the base 2, unless stated otherwise, and follow the convention that $0 \in \mathbb{N}$. We use C_m to denote a cyclic group of order m for any positive integer m . Let $O_{p'}(G)$ denote the largest normal p' -subgroup of G . The techniques we use are similar to those in [1, 9, 13].

The main result proved in this paper is the following theorem.

THEOREM 1.2. *Let $n = p^\alpha q^\beta r^\gamma$, where $\alpha, \beta, \gamma \in \mathbb{N}$. Then,*

$$f_\mathfrak{S}(n) \leq p^{6\alpha^2} 2^{\alpha-1+(23/6)\alpha \log \alpha + \alpha \log 6} (6^{1/2})^{(\alpha+\gamma)\beta + (\alpha+\beta)\gamma + \alpha(\alpha-1)/2} n^{\beta+\gamma}.$$

To prove Theorem 1.2, we prove a bound on the number of conjugacy classes of subgroups that are maximal amongst subgroups of $GL(\alpha, s)$ and that are in the variety $\mathfrak{A}_q\mathfrak{A}_r$ or \mathfrak{A}_r . We also prove results about the order of primitive subgroups of S_n that are in the variety $\mathfrak{A}_q\mathfrak{A}_r$, and show that they form a single conjugacy class. These results are stated below.

THEOREM 1.3. *Let q and r be distinct primes. Let G be a primitive subgroup of S_n that is in $\mathfrak{A}_q\mathfrak{A}_r$ and let $|G| = q^\beta r^\gamma$, where $\beta, \gamma \in \mathbb{N}$. Let M be a minimal normal subgroup of G .*

- (i) *If $\beta = 0$, then $|M|$ is a power of r and $|G| = n = r$ with $G \cong C_r$.*
- (ii) *If $\beta \geq 1$, then $|M| = q^\beta = n$ with $\beta = \text{order } q \text{ mod } r$. Further, $G \cong M \rtimes C_r$ and $|G| = nr < n^2$.*
- (iii) *If $\gamma = 0$, then $|M|$ is a power of q and $|G| = n = q$ with $G \cong C_q$.*

THEOREM 1.4. *The primitive subgroups of S_n that are in $\mathfrak{A}_q\mathfrak{A}_r$ and of order $q^\beta r^\gamma$, where $\beta, \gamma \in \mathbb{N}$, form a single conjugacy class.*

THEOREM 1.5. *There exist constants b and c such that the number of conjugacy classes of subgroups that are maximal amongst the subgroups of $\mathrm{GL}(\alpha, s)$ that are in $\mathfrak{A}_q\mathfrak{A}_r$ is at most*

$$2^{(b+c)(\alpha^2/\sqrt{\log \alpha})+(5/6)\alpha \log \alpha + \alpha(1+\log 6)} s^{(3+c)\alpha^2},$$

where t, q and r are distinct primes, s is a power of t , and $\alpha > 1$.

Section 2 investigates primitive subgroups of S_n that are in \mathfrak{A}_r or $\mathfrak{A}_q\mathfrak{A}_r$. Sections 3 and 4 deal with subgroups of the general linear group. Theorem 1.2 is proved in Section 5.

2. Primitive subgroups of S_n that are in \mathfrak{A}_r or $\mathfrak{A}_q\mathfrak{A}_r$

In this section, we prove results that give us the structure of the primitive subgroups of S_n that are in \mathfrak{A}_r or $\mathfrak{A}_q\mathfrak{A}_r$. We also show that such subgroups form a single conjugacy class. Both Theorems 1.3 and 1.4 are proved in this section.

Theorem 1.3 provides the order of a primitive subgroup of S_n that is in the variety $\mathfrak{A}_q\mathfrak{A}_r$. By [13, Proposition 2.1], if G is a soluble A -subgroup of S_n , then $|G| \leq (6^{1/2})^{n-1}$. Indeed, this bound is determined primarily by considering primitive soluble A -subgroups of S_n . This bound would clearly hold for any subgroup of S_n that is in the variety $\mathfrak{A}_q\mathfrak{A}_r$. However, we show that when the subgroup is primitive and in the variety $\mathfrak{A}_q\mathfrak{A}_r$, we can do better.

LEMMA 2.1. *S_n has a primitive subgroup in \mathfrak{A}_r if and only if $n = r$. In this case, any primitive subgroup G that is in \mathfrak{A}_r will be cyclic of order r . All primitive subgroups of S_n that are in \mathfrak{A}_r form a single conjugacy class.*

PROOF. Let G be a primitive subgroup of S_n that is in \mathfrak{A}_r . Since G is soluble, M is an elementary abelian r -subgroup. By the O’Nan–Scott theorem [10], $|M| = n = |G|$, so $G = M \cong C_r$ and $n = r$. Conversely, any transitive subgroup G of S_r is primitive [15, Theorem 8.3]. Since n is prime, any subgroup of order n in S_n will be generated by an n -cycle. Further, any two n -cycles are conjugate in S_n . Thus, the primitive subgroups of S_n that are also in \mathfrak{A}_r form a single conjugacy class. \square

PROOF OF THEOREM 1.3. Let G be a subgroup of S_Ω , where $|\Omega| = n$, and let $G \in \mathfrak{A}_q\mathfrak{A}_r$. Then $G = Q \rtimes R$, where Q is an elementary abelian Sylow q -subgroup, R is an elementary abelian Sylow r -subgroup and $|G| = q^\beta r^\gamma$, with $\beta, \gamma \in \mathbb{N}$. Let M be a minimal normal subgroup of G . Then M is an elementary abelian u -group. Clearly, $|M| = u^k$ for some $k > 1$ and for some prime $u \in \{q, r\}$.

Now $F(G)$, the Fitting subgroup of G , is an abelian normal subgroup of G and so, by the O’Nan–Scott theorem, $n = |M| = |F(G)|$. However, $M \leq F(G)$, therefore, $M = F(G)$ and $n = u^k$. If $\beta \geq 1$, then $Q \leq F(G)$ and we have $n = q^\beta = u^k$ and $M = F(G) = Q$. Let $H = G_\alpha$ be the stabiliser of an $\alpha \in \Omega$. By [1, Proposition 6.13], G is a semidirect product of M by H and H acts faithfully by conjugation on M . By Maschke’s theorem,

M is completely reducible. However, M is a minimal normal subgroup of G , so M is a nontrivial irreducible $\mathbb{F}_q H$ -module and H is an abelian group acting faithfully on M . By [14, Corollary 4.1], $H \cong C_r$ and $\beta = \dim M = \text{order } q \text{ mod } r$ and the result follows. If $\gamma = 0$ or $\beta = 0$, then $|G|$ is a power of u , where $u \in \{q, r\}$. Thus, G is a primitive subgroup that is also in \mathfrak{A}_u and the result follows by Lemma 2.1. \square

It is clear from these results that if S_n has a primitive subgroup G of order $q^\beta r^\gamma$ in $\mathfrak{A}_q \mathfrak{A}_r$, then n must be r or q and G is cyclic with $|G| = n$, or $n = q^\beta$ and G is a semi-direct product of an elementary abelian q -group of order q^β by a cyclic group of order r . The limits imposed on n and the structure of such primitive subgroups gives the next result.

PROOF OF THEOREM 1.4. Let G be a primitive subgroup of S_Ω that is in $\mathfrak{A}_q \mathfrak{A}_r$, where $|\Omega| = n$, and let $|G| = q^\beta r^\gamma$. Let M be a minimal normal subgroup of G . As seen in the proof of Theorem 1.3, $M = F(G)$ and $n = |M|$ is either a power of q or r . If $\gamma = 0$ or $\beta = 0$, then $|G|$ is a power of u , where $u \in \{q, r\}$. Thus, G is a primitive subgroup that is also in \mathfrak{A}_u and the result follows by Lemma 2.1.

We know the structure of G when $\beta \geq 1$ from the proof of Theorem 1.3. Hence, H can be regarded as a soluble r -subgroup of $GL(\beta, q)$ and it is not difficult to show that the conjugacy class of G in S_n is determined by the conjugacy class of H in $GL(\beta, q)$. Let S be a Singer subgroup of $GL(\beta, q)$, so that $|S| = q^\beta - 1$. Now, $|H| = r$ and r divides $|S|$. Further, $\gcd(|GL(\beta, q)|/|S|, r) = 1$ as β is the least positive integer such that $r \mid q^\beta - 1$. From [3, Theorem 2.11], $H^x \leq S$ for some $x \in GL(\beta, q)$. Since all Singer subgroups are conjugate in $GL(\beta, q)$, the result follows. \square

3. Subgroups of $GL(\alpha, s)$ that are in \mathfrak{A}_r

In this section, we prove results that give us a bound on the number of conjugacy classes of the subgroups that are maximal amongst subgroups of $GL(\alpha, s)$ that are in \mathfrak{A}_r . The limits on the structure of such groups ensures that if they exist, they form a single conjugacy class.

LEMMA 3.1. *The number of conjugacy classes of irreducible subgroups of $GL(\alpha, s)$ that are also in \mathfrak{A}_r is at most 1.*

PROOF. Let G be a nontrivial irreducible subgroup of $GL(\alpha, s)$ that is also in \mathfrak{A}_r . Then G is an elementary abelian r -group of order r^γ , say, where $\gamma \in \mathbb{N}$. Since G is a faithful abelian irreducible subgroup of $GL(\alpha, s)$ whose order is coprime to s , it follows that G is cyclic [14, Lemma 4.2]. Thus, $|G| = r$ and $\alpha = d$, where $d = \text{order } s \text{ mod } r$. From [11, Theorem 2.3.3], the irreducible cyclic subgroups of order r in $GL(\alpha, s)$ lie in a single conjugacy class. \square

PROPOSITION 3.2. *The number of conjugacy classes of subgroups that are maximal amongst subgroups of $GL(\alpha, s)$ that are also in \mathfrak{A}_r is at most 1.*

PROOF. Let G be maximal amongst subgroups of $\text{GL}(\alpha, s)$ that are also in \mathfrak{A}_r . Since $\text{char}(\mathbb{F}_p) = t \nmid |G|$, by Maschke's theorem, we can find groups G_i such that $G \leq G_1 \times G_2 \times \cdots \times G_k = \hat{G} \leq \text{GL}(\alpha, s)$, where for each i , the group G_i is a (maximal) irreducible subgroup of $\text{GL}(\alpha_i, s)$ that is also in \mathfrak{A}_r . Further, $\alpha = \alpha_1 + \cdots + \alpha_k$. Clearly, $G_i \cong C_r$ and $\alpha_i = d = \text{order } s \text{ mod } r$ for each i . Thus, we must have $\alpha = dk$ and by the maximality of G , we have $G = \hat{G}$. Further, the conjugacy classes of G_i in $\text{GL}(\alpha_i, s)$ determine the conjugacy class of G in $\text{GL}(\alpha, s)$.

So if d does not divide α , then $\text{GL}(\alpha, s)$ cannot have an elementary abelian r -subgroup. If $d \mid \alpha$, then any G that is maximal amongst subgroups of $\text{GL}(\alpha, s)$ that are also in \mathfrak{A}_r must have order r^k , where $k = \alpha/d$. By Lemma 3.1, all such groups form a single conjugacy class. □

4. Subgroups of $\text{GL}(\alpha, s)$ that are also in $\mathfrak{A}_q \mathfrak{A}_r$

We prove results that give a bound on the order of subgroups of $\text{GL}(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$ and also a bound for the number of conjugacy classes of subgroups that are maximal amongst subgroups of $\text{GL}(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$. Theorem 1.5 is proved in this section.

PROPOSITION 4.1. *Let G be a subgroup of $\text{GL}(\alpha, s)$ that is in $\mathfrak{A}_q \mathfrak{A}_r$.*

- (i) *Let $m = |F(G)|$. If G is primitive, then $|G| \leq cm$, where $c = \text{order } s \text{ mod } m$ and $c \mid \alpha$. Further, m is either r or q or qr .*
- (ii) *$|G| \leq (6^{1/2})^{\alpha-1} d^\alpha$, where $d = \min\{qr, s\}$.*

PROOF. Let $V = (\mathbb{F}_s)^\alpha$. Let G be a primitive subgroup of $\text{GL}(\alpha, s)$ that is in $\mathfrak{A}_q \mathfrak{A}_r$ and let $|G| = q^\beta r^\gamma$, where β and γ are natural numbers. If $\beta = 0$ or $\gamma = 0$, then the result follows from Lemma 3.1. Assume that β and γ are at least 1. Let $F = F(G)$ be the Fitting subgroup of G . Since $G \in \mathfrak{A}_q \mathfrak{A}_r$, it follows that F is abelian and $|F| = q^\beta r^{\gamma_1} = m$, where $\gamma_1 \leq \gamma$. By Clifford's theorem, since G is primitive, $V = X_1 \oplus X_2 \oplus \cdots \oplus X_a$ as an F -module, where the X_i are conjugates of X , an irreducible $\mathbb{F}_s F$ -submodule of V . Note that F acts faithfully on X .

Let E be the subalgebra generated by F in $\text{End}(V)$. The X_i are conjugates of X , so E acts faithfully and irreducibly on X and E is commutative. By [1, Proposition 8.2 and Theorem 8.3], E is a field. Thus, $E \cong \mathbb{F}_{s^c}$ as an $\mathbb{F}_s F$ -module, where $c = \dim(X)$ and $\alpha = ac$. Note that F is an abelian group of order m acting faithfully and irreducibly on X . Consequently, F is cyclic and c is the least positive integer such that $m \mid s^c - 1$. Clearly, $m = q$ or $m = qr$ and so $\beta = 1$. It is not difficult to show that G acts on E by conjugation. Hence, there exists a homomorphism from G to $\text{Gal}_{\mathbb{F}_s}(E)$. Let N be the kernel of this map. Then $N = C_G(E) \leq C_G(F) \leq F$. However, $F \leq N$. Hence, $F = N$. So $G/F \leq \text{Gal}_{\mathbb{F}_s}(E) \cong C_c$ and $|G| \leq cm$.

Let G be an irreducible imprimitive subgroup of $\text{GL}(\alpha, s)$ that is also in $\mathfrak{A}_q \mathfrak{A}_r$. Then $G \leq G_1 \text{ wr } G_2 \leq \text{GL}(\alpha, s)$, where G_1 is a primitive subgroup of $\text{GL}(\alpha_1, s)$ that is in $\mathfrak{A}_q \mathfrak{A}_r$, and the group G_2 can be regarded as a transitive subgroup of S_k that is in

$\mathfrak{A}_q \mathfrak{A}_r$. Further, $\alpha = \alpha_1 k$. By the previous part, $|G_1| \leq c' m'$, where $c' = \text{order } s \text{ mod } m'$ and $m' = |F(G_1)|$ is either r or q or qr . Also $c' \mid \alpha_1$. By [13, Proposition 2.1], $|G_2| \leq (6^{1/2})^{k-1}$. Using $c' \leq 2^{c'-1} \leq (6^{1/2})^{c'-1}$, we see that $|G| \leq (6^{1/2})^{\alpha-1} (m')^k$. Since $m' \mid p^{c'} - 1$, we have $(m')^k \leq d^\alpha$, where $d = \min\{qr, s\}$.

Since t does not divide q or r , by Maschke's theorem, any subgroup G of $\text{GL}(\alpha, s)$ that is in $\mathfrak{A}_q \mathfrak{A}_r$ will be completely reducible. Thus, $G \leq G_1 \times \dots \times G_k \leq \text{GL}(\alpha, s)$, where the G_i are irreducible subgroups of $\text{GL}(\alpha_i, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$ and $\alpha = \alpha_1 + \dots + \alpha_k$. Hence, $|G| \leq (6^{1/2})^{\alpha-1} d^\alpha$, where $d = \min\{qr, s\}$. \square

PROPOSITION 4.2. *There exist constants b and c such that the number of conjugacy classes of subgroups that are maximal amongst irreducible subgroups of $\text{GL}(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$ is at most $2^{(b+c)(\alpha^2/\sqrt{\log \alpha} + (5/6)\log \alpha + \log 6)s^{(3+c)\alpha^2}}$ provided $\alpha > 1$.*

PROOF. Let G be a subgroup of $\text{GL}(\alpha, s)$ that is maximal amongst irreducible subgroups of $\text{GL}(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$. Let $|G| = q^\beta r^\gamma$, where β and γ are natural numbers. If $\beta = 0$ or $\gamma = 0$, then the result follows from Lemma 3.1. Assume that β and γ are at least 1. Let $V = (\mathbb{F}_s)^\alpha$ and $F = F(G)$, the Fitting subgroup of G . Then $F = Q \times R_1$, where Q is the unique Sylow q -subgroup of G and $R_1 \leq R$, where R is a Sylow r -subgroup of G . So F is abelian and $|F| = q^{\beta} r^{\gamma_1} = m$, where $\gamma_1 \leq \gamma$.

From Clifford's theorem, regarding V as an $\mathbb{F}_s F$ -module, $V = Y_1 \oplus Y_2 \oplus \dots \oplus Y_l$, where $Y_i = kX_i$ for all i , and X_1, \dots, X_l are irreducible $\mathbb{F}_s F$ -submodules of V . Further, for each i, j , there exists $g_{ij} \in G$ such that $g_{ij} X_i = X_j$ and, for $i = 1, \dots, l$, the X_i form a maximal set of pairwise nonisomorphic conjugates. Also, the action of G on the Y_i is transitive. It is not difficult to check that $C_F(Y_i) = C_F(X_i) = K_i$, say. Thus, F/K_i acts faithfully on Y_i and when its action is restricted to X_i , it acts faithfully and irreducibly on X_i . Since X_i is a nontrivial irreducible faithful $\mathbb{F}_s F/K_i$ -module, and t is coprime to q and r , it follows that F/K_i is cyclic and $\dim_{\mathbb{F}_s}(X_i) = d_i$, where d_i is the least positive integer such that m_i divides $s^{d_i} - 1$, and where m_i is the order of F/K_i . Since the X_i are conjugate, $\dim_{\mathbb{F}_s}(X_i) = d_i = d$ for all i .

Let E_i be the subalgebra generated by F/K_i in $\text{End}_{\mathbb{F}_s}(Y_i)$. Note that E_i is commutative as F/K_i is abelian. Further, X_i is a faithful irreducible E_i -module. So E_i is simple and becomes a field such that $E_i \cong \mathbb{F}_{s^{d_i}}$. We also observe that $\alpha = kld$.

Let k, l, d be fixed such that $\alpha = kld$. Next we find the number of choices for F up to conjugacy in $\text{GL}(V)$. Clearly,

$$\begin{aligned} F &\leq F/K_1 \times F/K_2 \times \dots \times F/K_l \leq E_1^* \times E_2^* \times \dots \times E_l^* \\ &\leq \text{GL}(Y_1) \times \text{GL}(Y_2) \times \dots \times \text{GL}(Y_l) \leq \text{GL}(V), \end{aligned}$$

where E_i^* denotes the multiplicative group of the field E_i . Let $E = E_1^* \times E_2^* \times \dots \times E_l^*$. Then $|E| = (s^d - 1)^l$. Regarding V as an $\mathbb{F}_s E$ -module, $V = kX_1 \oplus kX_2 \oplus \dots \oplus kX_l$, where E_i^* acts faithfully and irreducibly on X_i and $\dim_{E_i}(X_i) = 1$ for all i . Further, for $i \neq j$, E_i^* acts trivially on X_j . It is not difficult to show that there is only one conjugacy class of subgroups of type E in $\text{GL}(V)$.

So once k, l and d are chosen such that $\alpha = kld$, up to conjugacy, there is only one choice for E . Since E is a direct product of l isomorphic cyclic groups, any subgroup of E can be generated by l elements. In particular, F can be generated by l elements. So the number of choices for F as a subgroup of E is at most $|E|^l = (s^d - 1)^l$.

Since, G acts transitively on $\{Y_1, \dots, Y_l\}$, there exists a homomorphism ϕ from G into S_l . Let $N = \ker(\phi) = \{g \in G \mid gY_i = Y_i \text{ for all } i\}$. Clearly, $F \leq N$ and G/N is a transitive subgroup of S_l that is in \mathfrak{A}_r . If $g \in N$, then $gE_i g^{-1} = E_i$. Thus, there exists a homomorphism $\psi_i : N \rightarrow \text{Gal}_{\mathbb{F}_s}(E_i)$. This induces a homomorphism ψ from N to $\text{Gal}_{\mathbb{F}_s}(E_1) \times \text{Gal}_{\mathbb{F}_s}(E_2) \times \dots \times \text{Gal}_{\mathbb{F}_s}(E_l)$ such that $\ker(\psi) = \bigcap_{i=1}^l N_i = F$, where $N_i = \ker(\psi_i) = C_N(E_i)$. So N/F is isomorphic to a subgroup of $\text{Gal}_{\mathbb{F}_s}(E_1) \times \text{Gal}_{\mathbb{F}_s}(E_2) \times \dots \times \text{Gal}_{\mathbb{F}_s}(E_l)$. Since $\text{Gal}_{\mathbb{F}_s}(E_i) \cong C_d$ for every i , it follows that N/F can be generated by l elements.

Let $T = \text{GL}(\alpha, s)$. Let $\hat{N} = \{x \in N_T(F) \mid xY_i = Y_i \text{ for all } i\}$. Then $F \leq N \leq \hat{N} \leq N_T(F)$. We will find the number of choices for N as a subgroup of \hat{N} , given that F has been chosen. The group \hat{N} acts by conjugation on E_i and fixes the elements of \mathbb{F}_s . So we have a homomorphism $\rho_i : \hat{N} \rightarrow \text{Gal}_{\mathbb{F}_s}(E_i)$ with kernel $C_{\hat{N}}(E_i)$. Define $C = \bigcap_{i=1}^l C_{\hat{N}}(E_i)$. Note that $N \cap C = F$. Also, \hat{N}/C is isomorphic to a subgroup of $\text{Gal}_{\mathbb{F}_s}(E_1) \times \text{Gal}_{\mathbb{F}_s}(E_2) \times \dots \times \text{Gal}_{\mathbb{F}_s}(E_l)$, where each $\text{Gal}_{\mathbb{F}_s}(E_i)$ is isomorphic to C_d . So $|\hat{N}/C| \leq d^l$. Clearly, C centralises E_i for each i . Therefore, there exists a homomorphism from C into $\text{GL}_{E_i}(Y_i)$ for each i . Hence, C is isomorphic to a subgroup of $\text{GL}_{E_1}(Y_1) \times \text{GL}_{E_2}(Y_2) \times \dots \times \text{GL}_{E_l}(Y_l)$. As $\dim_{\mathbb{F}_i}(Y_i) = k$ and $E_i \cong \mathbb{F}_{s^d}$ for all i , it follows that $|C| \leq s^{dk^2l}$. Hence, $|\hat{N}| \leq d^l s^{dk^2l}$.

Now $NC/C \cong N/(N \cap C) = N/F$. So NC/C can be generated by l elements since N/F can be generated by l elements. However, $|\hat{N}/C| \leq d^l$, therefore, there are at most d^l choices for NC/C as a subgroup of \hat{N}/C . Once we make a choice for NC/C as a subgroup of \hat{N}/C , we choose a set of l generators for NC/C . As $N \cap C = F$, we see that N is determined as a subgroup of \hat{N} by F and l other elements that map to the chosen generating set of NC/C . We have $|C|$ choices for an element of \hat{N} that maps to any fixed element of \hat{N}/C . Thus, there are at most $|C|^l$ choices for N as a subgroup of \hat{N} once NC/C has been chosen. So we have at most $d^{l^2} (s^{dk^2l})^l = d^{l^2} s^{dk^2l^2}$ choices for N as a subgroup of \hat{N} , once F is fixed.

Next we find the number of choices for G given that F and N are fixed as subgroups of T and $\hat{N} \leq T$, respectively. Let $\hat{Y} = \{y \in N_T(F) \mid y \text{ permutes the } Y_i\}$. Then $F \leq G \leq \hat{Y} \leq N_T(F) \leq \text{GL}(V)$. Also there exists a homomorphism from \hat{Y} to S_l with kernel $\{y \in \hat{Y} \mid yY_i = Y_i \text{ for all } i\} = \hat{N}$. Thus, \hat{Y}/\hat{N} may be regarded as a subgroup of S_l . However, $G \cap \hat{N} = N$. Thus, $G/N = G/(G \cap \hat{N}) \cong G\hat{N}/\hat{N}$. So $G/N \cong G\hat{N}/\hat{N} \leq \hat{Y}/\hat{N} \leq S_l$. Note that G/N is a transitive subgroup of S_l that is in \mathfrak{A}_r . By [5, Theorem 1], there exists a constant b such that S_l has at most $2^{b l^2 / \sqrt{\log l}}$ transitive subgroups for $l > 1$. Hence, the number of choices for $G\hat{N}/\hat{N}$ as a subgroup of \hat{Y}/\hat{N} is at most $2^{b l^2 / \sqrt{\log l}}$.

By [6, Theorem 2], there exists a constant c such that any transitive permutation group of finite degree greater than 1 can be generated by $\lfloor cl / \sqrt{\log l} \rfloor$ generators. Thus, $G\hat{N}/\hat{N}$ can be generated by $\lfloor cl / \sqrt{\log l} \rfloor$ generators for $l > 1$. Once a choice for $G\hat{N}/\hat{N}$

is made as a subgroup of \hat{Y}/\hat{N} and $\lfloor cl/\sqrt{\log l} \rfloor$ generators are chosen for $G\hat{N}/\hat{N}$ in \hat{Y}/\hat{N} , then G is determined as a subgroup of \hat{Y} by \hat{N} and the elements of \hat{Y} that map to the $\lfloor cl/\sqrt{\log l} \rfloor$ generators chosen for $G\hat{N}/\hat{N}$. So we have at most $|\hat{N}|^{\lfloor cl/\sqrt{\log l} \rfloor}$ choices for G as a subgroup of \hat{Y} once a choice of $G\hat{N}/\hat{N}$ in \hat{Y}/\hat{N} is fixed. Hence, there are

$$2^{bl^2/\sqrt{\log l}} (d^l s^{dk^2l})^{\lfloor cl/\sqrt{\log l} \rfloor} \leq 2^{bl^2/\sqrt{\log l}} d^{cl^2/\sqrt{\log l}} s^{cdk^2l^2/\sqrt{\log l}}$$

choices for G as a subgroup of \hat{Y} assuming that choices for F and N have been made. Putting together all these estimates, the number of conjugacy classes of subgroups that are maximal amongst irreducible subgroups of $GL(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$ is at most

$$\sum_{(k,l,d)} (s^d - 1)^l d^{l^2} s^{dk^2l^2} 2^{bl^2/\sqrt{\log l}} d^{cl^2/\sqrt{\log l}} s^{cdk^2l^2/\sqrt{\log l}},$$

where (k, l, d) ranges over ordered triples of natural numbers which satisfy $\alpha = kld$ and $l > 1$. We simplify the above expression as follows. Writing $\alpha = kld$,

$$(s^d - 1)^l d^{l^2} s^{dk^2l^2} s^{cdk^2l^2/\sqrt{\log l}} \leq s^{(3+c)\alpha^2}.$$

Since $x/\sqrt{\log x}$ is increasing for $x > e^{1/2}$, we have $l/\sqrt{\log l} \leq \alpha/\sqrt{\log \alpha}$ for $l \geq 2$. Thus, $2^{bl^2/\sqrt{\log l}} d^{cl^2/\sqrt{\log l}} \leq 2^{(b+c)\alpha^2/\sqrt{\log \alpha}}$.

There are at most $2^{(5/6)\log \alpha + \log 6}$ choices for (k, l, d) . Thus, there exist constants b and c such that the number of conjugacy classes of subgroups that are maximal amongst irreducible subgroups of $GL(\alpha, s)$ that are in $\mathfrak{A}_q \mathfrak{A}_r$ is at most

$$2^{(b+c)(\alpha^2/\sqrt{\log \alpha}) + (5/6)\log \alpha + \log 6} s^{(3+c)\alpha^2}$$

provided $\alpha > 1$. □

Theorem 1.5 follows as a corollary to Proposition 4.2.

PROOF OF THEOREM 1.5. Let G be maximal amongst subgroups of $GL(\alpha, s)$ that are also in $\mathfrak{A}_q \mathfrak{A}_r$. As the characteristic of $\mathbb{F}_s = t$ and $t \nmid |G|$, by Maschke’s theorem, $G \leq \hat{G}_1 \times \dots \times \hat{G}_k \leq GL(\alpha, s)$, where the \hat{G}_i are maximal among irreducible subgroups of $GL(\alpha_i, p)$ that are also in $\mathfrak{A}_q \mathfrak{A}_r$, and where $\alpha = \alpha_1 + \dots + \alpha_k$. By the maximality of G , we have $G = \hat{G}_1 \times \dots \times \hat{G}_k$.

The conjugacy classes of $\hat{G}_i \in GL(\alpha_i, s)$ determine the conjugacy class of $G \in GL(\alpha, s)$. So by Proposition 4.2, the number of conjugacy classes of subgroups that are maximal amongst the subgroups of $GL(\alpha, s)$ that are also in $\mathfrak{A}_q \mathfrak{A}_r$ is at most

$$\sum_{(\alpha)} \prod_{i=1}^k 2^{(b+c)(\alpha_i^2/\sqrt{\log \alpha_i}) + (5/6)\log \alpha_i + \log 6} s^{(3+c)\alpha_i^2},$$

where the sum is over all unordered partitions $\alpha_1, \dots, \alpha_k$ of α . We assume that if $\alpha_i = 1$ for some i , then the part of the expression corresponding to it in the product is 1. Since $x/\sqrt{\log x}$ is increasing for $x > e^{1/2}$ and $\alpha = \alpha_1 + \dots + \alpha_k$,

$$\prod_{i=1}^k 2^{(b+c)(\alpha_i^2/\sqrt{\log \alpha_i})+(5/6)\log \alpha_i+\log 6} \leq 2^{(b+c)(\alpha^2/\sqrt{\log \alpha})+(5/6)\alpha \log \alpha+\alpha \log 6}.$$

It is not difficult to show that the number of unordered partitions of α is at most $2^{\alpha-1}$. So the number of conjugacy classes of subgroups that are maximal amongst the subgroups of $\text{GL}(\alpha, s)$ that are also in $\mathfrak{A}_q\mathfrak{A}_r$ is at most

$$2^{(b+c)(\alpha^2/\sqrt{\log \alpha})+(5/6)\alpha \log \alpha+\alpha(1+\log 6)} 5^{(3+c)\alpha^2}$$

provided $\alpha > 1$. □

We end this section with the following remark that provides an alternative bound.

REMARK 4.3. We do not have an estimate for the constants b and c occurring in Theorem 1.5. If we use a weaker fact that any subgroup of S_n can be generated by $\lfloor n/2 \rfloor$ elements for all $n \geq 3$, then we get a weaker result that the number of transitive subgroups of S_n that are in $\mathfrak{A}_q\mathfrak{A}_r$ is at most $6^{n(n-1)/4} 2^{(n+2)\log n}$. Using this in the proof of Theorem 1.5 shows that the number of conjugacy classes of subgroups that are maximal amongst the subgroups of $\text{GL}(\alpha, s)$ that are also in $\mathfrak{A}_q\mathfrak{A}_r$ is at most

$$s^{5\alpha^2} 6^{\alpha(\alpha-1)/4} 2^{\alpha-1+(23/6)\alpha \log \alpha+\alpha \log 6},$$

where t, q and r are distinct primes, s is a power of t , and $\alpha \in \mathbb{N}$.

5. Enumeration of groups in $\mathfrak{A}_p\mathfrak{A}_q\mathfrak{A}_r$

In this section, we prove Theorem 1.2, namely,

$$f_{\in}(n) \leq p^{6\alpha^2} 2^{\alpha-1+(23/6)\alpha \log \alpha+\alpha \log 6} (6^{1/2})^{(\alpha+\gamma)\beta+(\alpha+\beta)\gamma+\alpha(\alpha-1)/2} n^{\beta+\gamma},$$

where $n = p^\alpha q^\beta r^\gamma$ and $\alpha, \beta, \gamma \in \mathbb{N}$. We use techniques adapted from [9, 13, 14].

PROOF OF THEOREM 1.2. Let G be a group of order $n = p^\alpha q^\beta r^\gamma$ in $\mathfrak{A}_p\mathfrak{A}_q\mathfrak{A}_r$. Then $G = P \rtimes H$, where P is the unique Sylow p -subgroup of G and $H \in \mathfrak{A}_q\mathfrak{A}_r$. So we can write $H = Q \rtimes R$, where $|Q| = q^\beta$ and $|R| = r^\gamma$. Let $G_1 = G/O_{p'}(G)$, $G_2 = G/O_{q'}(G)$ and $G_3 = G/O_{r'}(G)$. Clearly, each G_i is a soluble A -group and $G \leq G_1 \times G_2 \times G_3$ as a subdirect product. Further, $O_{p'}(G_1) = 1 = O_{q'}(G_2) = O_{r'}(G_3)$.

Since $G_1 = G/O_{p'}(G)$, we see that $G_1 \in \mathfrak{A}_p\mathfrak{A}_q\mathfrak{A}_r$ and if P_1 is the Sylow p -subgroup of G_1 , then $P_1 \cong P$. Thus, $|G_1| = p^\alpha q^{\beta_1} r^{\gamma_1}$ and we can write $G_1 = P_1 \rtimes H_1$, where $H_1 \in \mathfrak{A}_q\mathfrak{A}_r$. So $H_1 = Q_1 \rtimes R_1$, where $Q_1 \in \mathfrak{A}_q$ and $|Q_1| = q^{\beta_1}$, $R_1 \in \mathfrak{A}_r$ and $|R_1| = r^{\gamma_1}$. Further, H_1 acts faithfully on P_1 . Hence, we can regard $H_1 \leq \text{Aut}(P_1) \cong \text{GL}(\alpha, p)$. Let M_1 be a subgroup that is maximal amongst p' - A -subgroups of $\text{GL}(\alpha, p)$ that are also in $\mathfrak{A}_q\mathfrak{A}_r$ and such that $H_1 \leq M_1$. Let $\hat{G}_1 = P_1 M_1$. The number of conjugacy classes of the M_1 in $\text{GL}(\alpha, p)$ is at most $p^{5\alpha^2} 6^{\alpha(\alpha-1)/4} 2^{\alpha-1+(23/6)\alpha \log \alpha+\alpha \log 6}$ by Remark 4.3.

Since $G_2 = G/O_{q'}(G)$, we see that $G_2 \in \mathfrak{A}_q\mathfrak{A}_r$ and if Q_2 is the Sylow q -subgroup of G_2 , then $Q_2 \cong Q$. Thus, $|G_2| = q^\beta r^{\gamma_2}$ and we can write $G_2 = Q_2 \rtimes H_2$, where

$H_2 \in \mathfrak{A}_r$. So $|H_2| = r^{\gamma_2}$. Also, $H_2 \leq \text{Aut}(Q_2) \cong \text{GL}(\beta, q)$. Let M_2 be a subgroup that is maximal amongst q' - A -subgroups of $\text{GL}(\beta, q)$ that are also in \mathfrak{A}_r and such that $H_2 \leq M_2$. Let $\hat{G}_2 = Q_2 M_2$. The number of conjugacy classes of M_2 in $\text{GL}(\beta, q)$ is at most 1 by Proposition 3.2.

Since $G_3 = G/O_{r'}(G)$, we see that $G_3 \in \mathfrak{A}_r \mathfrak{A}_q$ and if R_3 is the Sylow r -subgroup of G_3 , then $R_3 \cong R$. Thus, $|G_3| = q^{\beta_3} r^{\gamma}$ and we can write $G_3 = R_3 \rtimes H_3$, where $H_3 \in \mathfrak{A}_r$. So $|H_3| = q^{\beta_3}$. Also, $H_3 \leq \text{Aut}(R_3) \cong \text{GL}(\gamma, r)$. Let M_3 be a subgroup that is maximal amongst r' - A -subgroups of $\text{GL}(\gamma, r)$ that are also in \mathfrak{A}_q and such that $H_3 \leq M_3$. Let $\hat{G}_3 = R_3 M_3$. The number of conjugacy classes of the M_3 in $\text{GL}(\gamma, r)$ is at most 1 by Proposition 3.2.

Let $\hat{G} = \hat{G}_1 \times \hat{G}_2 \times \hat{G}_3$. Then $G \leq \hat{G}$. The choices for P_1, Q_2 and R_3 are unique, up to isomorphism. We enumerate the possibilities for \hat{G} up to isomorphism and then find the number of subgroups of \hat{G} of order n up to isomorphism. For the former, we count the number of \hat{G}_i up to isomorphism which depends on the conjugacy class of the M_i . Hence, the number of choices for \hat{G} up to isomorphism is $\prod_{i=1}^3 \{\text{number of choices for } \hat{G}_i \text{ up to isomorphism}\}$. Now we estimate the choices for G as a subgroup of \hat{G} using a method of ‘Sylow systems’ introduced by Pyber in [9].

Let \hat{G} be fixed. We count the number of choices for G as a subgroup of \hat{G} . Let $\mathcal{S} = \{S_1, S_2, S_3\}$ be a Sylow system for G , where S_1 is the Sylow p -subgroup of G , S_2 is a Sylow q -subgroup of G and S_3 is a Sylow r -subgroup of G such that $S_i S_j = S_j S_i$ for all $i, j = 1, 2, 3$. Then $G = S_1 S_2 S_3$. By [1, Theorem 6.2, page 49], there exists $\mathcal{B} = \{B_1, B_2, B_3\}$, a Sylow system for \hat{G} such that $S_i \leq B_i$, where B_1 is the Sylow p -subgroup of \hat{G} , B_2 is a Sylow q -subgroup of \hat{G} and B_3 is a Sylow r -subgroup of \hat{G} . Note that $|B_1| = p^\alpha$. Further, any two Sylow systems for \hat{G} are conjugate. Hence, the number of choices for G as a subgroup of \hat{G} and up to conjugacy is at most

$$|\{S_1, S_2, S_3 \mid S_i \leq B_i, |S_1| = p^\alpha, |S_2| = q^\beta, |S_3| = r^\gamma\}| \leq |B_1|^\alpha |B_2|^\beta |B_3|^\gamma.$$

We observe that $B_2 = T_{21} \times T_{22} \times T_{23}$, where T_{2i} are Sylow q -subgroups of \hat{G}_i for $i = 1, 2, 3$. From [13, Proposition 3.1], $|T_{21}| \leq |M_1| \leq (6^{1/2})^{\alpha-1} p^\alpha$ and $|T_{23}| = |M_3| \leq (6^{1/2})^{\gamma-1} r^\gamma$. Further, $|T_{22}| = |Q_2| = q^\beta$. Hence, $|B_2| \leq (6^{1/2})^{\alpha+\gamma-2} p^\alpha q^\beta r^\gamma \leq (6^{1/2})^{\alpha+\gamma} n$ and so $|B_2|^\beta \leq (6^{1/2})^{(\alpha+\gamma)\beta} n^\beta$. Similarly, we can show that $|B_3| \leq (6^{1/2})^{\alpha+\beta-2} p^\alpha q^\beta r^\gamma$. So $|B_3|^\gamma \leq (6^{1/2})^{(\alpha+\beta)\gamma} n^\gamma$. Putting all the estimates together, the number of choices for G as a subgroup of \hat{G} up to conjugacy is at most $|B_1|^\alpha |B_2|^\beta |B_3|^\gamma$, which is at most

$$p^{\alpha^2} (6^{1/2})^{(\alpha+\gamma)\beta} n^\beta (6^{1/2})^{(\alpha+\beta)\gamma} n^\gamma \leq p^{\alpha^2} (6^{1/2})^{(\alpha+\gamma)\beta+(\alpha+\beta)\gamma} n^{\beta+\gamma}.$$

Therefore, the number of groups of order $p^\alpha q^\beta r^\gamma$ in $\mathfrak{A}_p \mathfrak{A}_q \mathfrak{A}_r$ up to isomorphism is at most

$$\begin{aligned} & p^{5\alpha^2} 6^{\alpha(\alpha-1)/4} 2^{\alpha-1+(23/6)\alpha \log \alpha + \alpha \log 6} p^{\alpha^2} (6^{1/2})^{(\alpha+\gamma)\beta+(\alpha+\beta)\gamma} n^{\beta+\gamma} \\ &= p^{6\alpha^2} 2^{\alpha-1+(23/6)\alpha \log \alpha + \alpha \log 6} (6^{1/2})^{(\alpha+\gamma)\beta+(\alpha+\beta)\gamma+\alpha(\alpha-1)/2} n^{\beta+\gamma}. \quad \square \end{aligned}$$

References

- [1] S. R. Blackburn, P. M. Neumann and G. Venkataraman, *Enumeration of Finite Groups* (Cambridge University Press, Cambridge, 2007).
- [2] G. Dickenson, 'On the enumeration of certain classes of soluble groups', *Q. J. Math.* **20**(1) (1969), 383–394.
- [3] M. D. Hestenes, 'Singer groups', *Canad. J. Math.* **22**(3) (1970), 492–513.
- [4] G. Higman, 'Enumerating p -groups. I: Inequalities', *Proc. Lond. Math. Soc. (3)* **10**(3) (1960), 24–30.
- [5] A. Lucchini, 'Enumerating transitive finite permutation groups', *Bull. Lond. Math. Soc.* **30**(6) (1998), 569–577.
- [6] A. Lucchini, F. Menegazzo and M. Morigi, 'Asymptotic results for transitive permutation groups', *Bull. Lond. Math. Soc.* **32**(2) (2000), 191–195.
- [7] A. McIver and P. M. Neumann, 'Enumerating finite groups', *Q. J. Math.* **38**(2) (1987), 473–488.
- [8] H. Neumann, *Varieties of Groups* (Springer-Verlag, Berlin–Heidelberg, 1967).
- [9] L. Pyber, 'Enumerating finite groups of given order', *Ann. of Math. (2)* **137**(1) (1993), 203–220.
- [10] L. Scott, 'Representations in characteristic p ', in: *The Santa Cruz Conference on Finite Groups*, Proceedings of Symposia in Pure Mathematics, 37 (eds. B. Cooperstein and G. Mason) (American Mathematical Society, Providence, RI, 1981).
- [11] M. W. Short, *The Primitive Soluble Permutation Groups of Degree Less than 256* (Springer, Berlin–Heidelberg, 1992).
- [12] C. C. Sims, 'Enumerating p -groups', *Proc. Lond. Math. Soc. (3)* **15**(3) (1965), 151–166.
- [13] G. Venkataraman, 'Enumeration of finite soluble groups with Abelian Sylow subgroups', *Q. J. Math.* **48**(1) (1997), 107–125.
- [14] G. Venkataraman, *Enumeration of Finite Soluble Groups in Small Varieties of A -groups and Associated Topics*, Tech. Report, Centre for Mathematical Sciences, St. Stephen's College (University of Delhi, Delhi, 1999).
- [15] H. Wielandt, *Finite Permutation Groups* (Academic Press, London, 1964), translated from German by R. Bercov.

ARUSHI, School of Liberal Studies (Mathematics),
Dr. B. R. Ambedkar University Delhi, Delhi 110006, India
e-mail: arushi.18@stu.aud.ac.in, arushi.garvita@gmail.com

GEETHA VENKATARAMAN, School of Liberal Studies (Mathematics),
Dr. B. R. Ambedkar University Delhi, Delhi 110006, India
e-mail: geetha@aud.ac.in, geevenkat@gmail.com