Bounding the maximal size of independent generating sets of finite groups

Andrea Lucchini and Mariapia Moscatiello
Dipartimento di Matematica 'Tullio Levi-Civita', University of Padova, Via Trieste 53, 35121 Padova, Italy (lucchini@math.unipd.it; mariapia.moscatiello@math.unipd.it)

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

Denote by $m(G)$ the largest size of a minimal generating set of a finite group G. We estimate $m(G)$ in terms of $\sum_{p \in \pi(G)} d_p(G)$, where we are denoting by $d_p(G)$ the minimal number of generators of a Sylow p-subgroup of G and by $\pi(G)$ the set of prime numbers dividing the order of G.

1. Introduction

A generating set X of a finite group G is said to be minimal (or independent) if no proper subset of X generates G. We denote by $m(G)$ the largest size of a minimal generating set of G. First steps towards investigating $m(G)$ have been taken in the context of permutation groups. An exhaustive investigation has been done for finite symmetric groups [**2**, **17**], proving that $m(\mathrm{Sym}(n)) = n - 1$ and giving a complete description of the independent generating sets of $\mathrm{Sym}(n)$ having cardinality $n - 1$. Partial results for some families of simple groups are in [**16**]: it turns out that already in the case $G = \mathrm{PSL}(2, q)$, the precise value of $m(G)$ is quite difficult to obtain. Further Apisa and Klopsch [**1**] proposed a natural 'classification problem': given a non-negative integer c, characterize all finite groups G such that $m(G) - d(G) \leqslant c$, where $d(G)$ is the minimal size of a generating set of G. In particular, they classified the finite groups for which the equality $m(G) = d(G)$ holds. During the same period the first author started in [**10**, **11**] a systematic investigation of how $m(G)$ can be estimated for an arbitrary finite group G.

In 1989, Guralnick [**3**] and the first author [**9**] independently proved that, if all the Sylow subgroups of a finite group G can be generated by d elements, then

A. Lucchini, M. Moscatiello and P. Spiga

$d(G) \leqslant d + 1$. One may ask, if minded so, whether a similar result holds also for $m(G)$. More precisely, denote by $d_p(G)$ the minimal number of generators of a Sylow p-subgroup of G.

> *Is it possible to bound $m(G)$ as a function of the numbers $d_p(G)$, with p running through the prime divisors of the order of G?*

As customary, we denote by $\pi(G)$ the set of prime divisors of the order of G. It can be easily seen that, if G is a finite nilpotent group, then $m(G) = \sum_{p \in \pi(G)} d_p(G)$. For simplicity, we let

$$\delta(G) := \sum_{p \in \pi(G)} d_p(G).$$

In a private communication to the first author, Keith Dennis has conjectured that $m(G) \leqslant \delta(G)$, for every finite group G.

This conjecture is true for soluble groups.

THEOREM 1.1. *Let G be a finite soluble group. Then $m(G) \leqslant \delta(G)$.*

Proof. In [**10**], it is proved that $m(G) = \sum_{p \in \pi(G)} \alpha_p(G)$, where $\alpha_p(G)$ denotes the number of complemented factors of p-power order in a chief series of G. Now, an easy inductive argument on the order of G shows that $\alpha_p(G) \leqslant d_p(G)$ (see for example [**12**, lemma 4]). Therefore $m(G) \leqslant \sum_{p \in \pi(G)} d_p(G) = \delta(G)$. □

Despite theorem 1.1, Dennis' conjecture is false if G is a symmetric group. We study the asymptotic behaviour of the function $\delta(\mathrm{Sym}(n))$ in §5. We prove the following theorem.

THEOREM 1.2. *For every $n \geqslant 2$, we have $\delta(\mathrm{Sym}(n)) = \log 2 \cdot n + o(n)$.*

Since $m(\mathrm{Sym}(n)) = n - 1$ by [**17**], the difference $m(\mathrm{Sym}(n)) - \delta(\mathrm{Sym}(n))$ goes to infinity with n and the inequality $m(\mathrm{Sym}(n)) \leqslant \delta(\mathrm{Sym}(n))$ is satisfied by only finitely many values of n. Indeed, using the explicit upper bound on $\delta(\mathrm{Sym}(n))$ in theorem 5.1 and some calculations, we have

$\delta(\mathrm{Sym}(n)) = n - 1$ if and only if $n \in \{1, 2, 3, 4, 5, 8, 10, 11, 16, 17, 18, 19, 25, 30, 31\}$,

$\delta(\mathrm{Sym}(n)) = n$ if and only if $n \in \{6, 7, 12, 13, 20, 26, 42, 43, 48\}$,

$\delta(\mathrm{Sym}(n)) = n + 1$ if and only if $n \in \{14, 21, 44, 45\}$,

$\delta(\mathrm{Sym}(n)) = n + 2$ if and only if $n \in \{15, 22, 23, 24, 46, 47\}$.

For all the other values of n, we have $\delta(\mathrm{Sym}(n)) < n - 1 = m(\mathrm{Sym}(n))$.

The proof of theorem 5.1 is rather technical and uses some explicit bounds on the prime counting function. However, in lemma 4.4 we show by elementary means that, for every positive real number $\eta > 1$, there exists a constant c_η such that $m(\mathrm{Sym}(n)) = n - 1 \leqslant c_\eta (\delta(\mathrm{Sym}(n))^\eta$, for every $n \in \mathbb{N}$.

This motivates the following conjecture, which can be seen as a natural generalization of Dennis' conjecture.

CONJECTURE 1.3. *There exist two constants c and η such that $m(G) \leqslant c \cdot \delta(G)^{\eta}$ for every finite group G.*

Given a normal subgroup N of a finite group G, we let

$$m(G, N) = m(G) - m(G/N).$$

The main result of this paper is the following theorem.

THEOREM 1.4. *Let G be a finite group and assume that there exist two constants $\sigma \geqslant 1$ and $\eta \geqslant 2$ such that $m(X, S) \leqslant \sigma \cdot |\pi(S)|^{\eta}$, for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$. Then $m(G) \leqslant \sigma \cdot \delta(G)^{\eta}$.*

Theorem 1.4 reduces conjecture 1.3 to the following conjecture on finite almost simple groups.

CONJECTURE 1.5. *There exist two constants σ and η such that $m(X, \operatorname{soc} X) \leqslant \sigma \cdot |\pi(\operatorname{soc} X)|^{\eta}$, for every finite almost simple group X.*

Conjecture 1.5 holds true, with $\eta = 2$, when $\operatorname{soc} X$ is an alternating group or a sporadic simple group. Therefore, we have the following corollary.

COROLLARY 1.6. *There exists a constant σ such that, if G has no composition factor of Lie type, then $m(G) \leqslant \sigma \delta(G)^2$.*

Very little is known about $m(G)$ when G is an almost simple group with socle a simple group of Lie type. Saxl and Whiston in [16] proved that, if $G = \operatorname{PSL}(2, q)$ with $q = p^r$ and with p a prime number, then $m(G) \leqslant \max(6, \tilde{\pi}(r) + 2)$ where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r. It follows from Zsigmondy's Theorem that $\tilde{\pi}(r) \leqslant \tilde{\pi}(q + 1) \leqslant |\pi(\operatorname{PSL}(2, q))|$. Therefore conjecture 1.5 holds true when $G = \operatorname{PSL}(2, q)$. In his PhD thesis [6], P. J. Keen found a good upper bound for $m(\operatorname{SL}(3, q))$, when $q = p^r$ and p is odd. In preparation for this, he also investigated the sizes of independent sets in $\operatorname{SO}(3, q)$ and $\operatorname{SU}(3, q)$, getting in all the cases a linear bound in terms of $\tilde{\pi}(r)$. These partial results lead us to conjecture that, if $\operatorname{soc}(X)$ is a group of Lie type of rank n over the field with $q = p^r$ elements, then $m(X, \operatorname{soc} X)$ is polynomially bounded in terms of n and $\tilde{\pi}(r)$. If this were true, then conjecture 1.5 would also be true.

The proofs of theorem 1.4 and corollary 1.6 are in §4. These proofs require two preliminary results, one concerning the prime divisors of the order of a finite non-abelian simple group and the other about permutation groups, proved respectively in §2 and 3.

2. A result on the order of a finite simple group

For later use we need to recall some definitions and some results concerning Zsigmondy primes.

DEFINITION 2.1. *Let a and n be positive integers. A prime number p is called a primitive prime divisor of $a^n - 1$ if p divides $a^n - 1$ and p does not divide $a^e - 1$*

for every integer $1 \leqslant e \leqslant n - 1$. We denote an arbitrary primitive prime divisors of $a^n - 1$ by a_n.

THEOREM 2.2 Zsigmondy's Theorem [**18**]. *Let a and n be integers greater than 1. There exists a primitive prime divisor of $a^n - 1$ except in one of the following cases:*

(1) $n = 2$, $a = 2^s - 1$ (*i.e. a is a Mersenne prime*), *and $s \geqslant 2$.*

(2) $n = 6$, $a = 2$.

LEMMA 2.3. [**7**, proposition 5.2.15] $a_n \equiv 1 \mod n$.

THEOREM 2.4. *Let S be a simple group of Lie type. There exist two different primes dividing $|S|$ but not $|\mathrm{Out}(S)|$.*

Proof. Let $S = L(q)$ be a simple group of Lie type defined over the field with q elements, where $q = p^t$ and p is a prime number. From Burnside's theorem, $|\pi(S)| \geqslant 3$. From [**4**], if $|\pi(S)| = 3$, then

$$S \in \{A_1(5), A_1(7), A_1(8), A_1(17), A_2(9), A_2(3), {}^2A_2(3), {}^2A_3(2)\},$$

and for these groups the theorem holds by a direct inspection. Therefore, for the rest of the proof we may suppose

$$|\pi(S)| \geqslant 4. \tag{2.1}$$

In particular, the result immediately follows when $|\pi(\mathrm{Out}(S))| \leqslant 2$ and hence we may suppose $|\pi(\mathrm{Out}(S))| \geqslant 3$.

The order of $L(q)$ has the cyclotomic factorization in terms of q:

$$|L(q)| = \frac{1}{d} q^h \prod_{m \in \Lambda} \Phi_m(q)^{r_m},$$

where $\Phi_m(q)$ is the m-th cyclotomic polynomial and Λ, d, h and r_m are listed in tables L.1, C.1 and C.2 of [**8**].

Suppose that $S \neq D_4(q)$ and that S is untwisted. From [**13**, p. 207], if $l \geqslant 2$ and $m \geqslant 1$ are integers such that $l_{m \cdot t}$ is a primitive prime divisor of $(l^t)^m - 1$, then $l_{m \cdot t}$ divides $\Phi_m(l^t)$. From this and from Zsigmondy's theorem, we conclude that, except for the six cases listed below, there exist $i, j \in \Lambda$ with $2 \leqslant i < j$ such that $x := p_{i \cdot t}$ and $y := p_{j \cdot t}$ are distinct primitive prime divisors. In particular, x and y are odd divisors of $|S|$ and are relatively prime to $q - 1$ because $i \geqslant 2$. Moreover, by lemma 2.3, $x \equiv y \equiv 1 \mod t$ and hence x and y are relatively prime to t. In particular, x and y are our required primes. (The case $S = D_4(q)$ is special in this argument because 3 is (potentially) an odd prime divisor of $|\mathrm{Out}(S)|$ not arising from field automorphisms.)

We are going to analyse the groups for which the existence of x and y is not ensured from the previous argument.

(1) $S = A_2(q)$ and q is a Mersenne prime: in this case $|\mathrm{Out}(S)| = 2 \cdot (q - 1, 3)$ is divisible by at most 2 different primes, contradicting $|\pi(\mathrm{Out}(S))| \geqslant 3$.

(2) $S = A_2(4)$: in this case 5 and 7 are the required primes.

(3) $S = A_1(q)$: we may assume $t \geqslant 5$, otherwise $|\pi(\mathrm{Out}S)| \leqslant 2$. Now, the existence of $x = p_t$ and $y = p_{2 \cdot t}$ is ensured by Zsigmondy's Theorem.

(4) $S = B_2(q)$ with q a Mersenne prime: in this case $|\pi(\mathrm{Out}(S))| = 1$, a contradiction.

(5) $S = B_2(8)$: in this case 5 and 7 are the requested primes.

(6) $S = G_2(q)$ with q a Mersenne prime: in this case $|\pi(\mathrm{Out}(S))| \leqslant 2$, a contradiction.

It remains to deal with the case $S = D_4(q)$ and with the twisted groups of Lie type.

Suppose $S = D_4(q)$. Since 3 divides $|\mathrm{Out}(S)|$, the previous argument fails exactly when the primitive prime divisor x or y is 3. The existence of $x = p_{2 \cdot t}$, $y = p_{4 \cdot t}$ and $z = p_{6 \cdot t}$ is ensured when $q \notin \{2, 8\}$ and when q is not a Mersenne prime. When $q = 2$, the result follows since $|\mathrm{Out}(S)| = 6$; when $q = 8$, we have that $t = 3$ does not divide y and z; therefore y and z are prime numbers satisfying our statement. When q is a Mersenne prime, if $q \neq 3$, then q and z are prime numbers satisfying our statement; if $q = 3$, then 5 and 7 are prime numbers satisfying our statement.

Assume $S \in \{{}^2 B_2(q), {}^2 G_2(q), {}^2 F_4(q)\}$. In these cases we have $|\mathrm{Out}(S)| = t$, so we may assume that t is not a prime. Since the existence of $x = p_{i \cdot t}$ and $y = p_{j \cdot t}$ is ensured by Zsigmondy's Theorem, for two different elements i and j of Λ, we are done.

If $S = {}^3 D_4(q)$ and $q \notin \{2, 8\}$ and q is not a Mersenne prime, then we can take $x = p_{2 \cdot t}$ and $y = p_{6 \cdot t}$ (notice that $|\mathrm{Out}\, S|$ divides $3 \cdot t$). When $q = 2$ or $q = 8$ or q is a Mersenne prime, then $|\mathrm{Out}(S)|$ is divisible only by 3, against our assumption.

If $S = {}^2 E_6(q)$, then we can take $x = p_{8 \cdot t}$ and $y = p_{12 \cdot t}$ (notice that $|\mathrm{Out}(S)|$ divides $6 \cdot t$).

If $S = {}^2 D_n(q)$, then $|\mathrm{Out}(S)|$ divides $8 \cdot t$. So, when $q = 2$ or when q is a Mersenne prime, the result holds since $|\mathrm{Out}(S)|$ has only one prime divisor. For the remaining cases, we can take $x = p_{4 \cdot t}$ and $y = p_{6 \cdot t}$.

Finally assume $S = {}^2 A_n(q)$. In this case $|\mathrm{Out}(S)| = 2 \cdot t \cdot (n + 1, q + 1)$. If $n \geqslant 3$ and $q \neq 2$, then we can take $x = p_{4 \cdot t}$ and $y = p_{6 \cdot t}$. When $q = 2$, we have $|\pi(\mathrm{Out}({}^2 A_n(2)))| \leqslant 2$, which is a contradiction. We remain with the case $S = {}^2 A_2(q)$. The group $S = {}^2 A_2(3)$ was already analysed, so we can suppose $q \geqslant 4$. Now $|\mathrm{Out}(S)| = 2 \cdot t \cdot (3, q + 1)$, so we may assume $t \neq 1$. If $(3, q + 1) = 1$, we may assume $t \neq 2$ and we can take $x = p_{2 \cdot t}$ and $y = p_{6 \cdot t}$. Otherwise $(3, q + 1) = 3$, so $(3, q - 1) = 1$ and in particular $x = p_t \neq 3$. It follows that $x = p_t$ and $y = p_{6 \cdot t}$ are the prime we are interested in. $\qquad\square$

3. An auxiliary result

LEMMA 3.1. *Let Q be a p-group, let P be a permutation p-group with domain Δ and let $n_\Delta(P)$ be the number of orbits of P on Δ. Then*

$$d(Q\mathrm{wr}_\Delta P) = d(P) + n_\Delta(P)d(Q).$$

Proof. Let $\Delta_1, \ldots, \Delta_\ell$ be the orbits of P on Δ.

Replacing Q by $Q/\operatorname{Frat}(Q)$ if necessary, we may suppose that Q is an elementary abelian p-group. Let B be the base group of the wreath product $W := Q\operatorname{wr}_\Delta P$.

Using the fact that B is an abelian normal subgroup of W and standard commutator computations, we get $[W, W] = [B, P][P, P]$. Given $\sigma \in P$ and $f \in B$, we have

$$(\sigma f)^p = \sigma^p f^{\sigma^{p-1}} f^{\sigma^{p-2}} \cdots f^\sigma f$$

$$= \sigma^p (f^{\sigma^{p-1}} f^{-1})(f^{\sigma^{p-2}} f^{-1}) \cdots (f^\sigma f^{-1}) \in P^p[B, P]$$

and hence

$$\operatorname{Frat}(W) = [B, P]\operatorname{Frat}(P). \tag{3.1}$$

Consider V, the subspace of B consisting of all functions $g : \Delta \to Q$ with

$$\prod_{\delta \in \Delta_i} g(\delta) = 1, \quad \text{for every } i \in \{1, \ldots, \ell\}.$$

Given $f \in B$, $\sigma \in P$ and $i \in \{1, \ldots, \ell\}$, we have

$$\prod_{\delta \in \Delta_i} [f, \sigma](\delta) = \prod_{\delta \in \Delta_i} (f^\sigma f^{-1})(\delta) = \prod_{\delta \in \Delta_i} f(\delta^{\sigma^{-1}}) f(\delta)^{-1} = \prod_{\delta \in \Delta_i} f(\delta^{\sigma^{-1}}) \prod_{\delta \in \Delta_i} f(\delta)^{-1}$$

$$= \left(\prod_{\delta \in \Delta_i} f(\delta) \right) \left(\prod_{\delta \in \Delta_i} f(\delta) \right)^{-1} = 1.$$

Hence, $[B, P] \leqslant V$. For each $i \in \{1, \ldots, \ell\}$, fix $\bar{\delta}_i \in \Delta_i$ and let $g \in V$. For every $i \in \{1, \ldots, \ell\}$ and $\delta \in \Delta_i \setminus \{\bar{\delta}_i\}$, we let $f_\delta : \Delta \to Q$ and $h_\delta : \Delta \to Q$ be the mappings defined by

$$f_\delta(\delta') = \begin{cases} g(\delta) & \text{if } \delta' = \delta, \\ g(\delta)^{-1} & \text{if } \delta' = \bar{\delta}_i, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta, \bar{\delta}_i\}, \end{cases} \qquad h_\delta(\delta') = \begin{cases} g(\delta)^{-1} & \text{if } \delta' = \delta, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta\}. \end{cases}$$

Since $g \in V$, with a computation, we obtain

$$g = \prod_{\delta \in \Delta \setminus \{\bar{\delta}_1, \ldots, \bar{\delta}_\ell\}} f_\delta.$$

For each $i \in \{1, \ldots, \ell\}$ and $\delta \in \Delta_i \setminus \{\bar{\delta}_i\}$, since δ and $\bar{\delta}_i$ are in the same P-orbit, there exists $\sigma \in P$ with $\delta^\sigma = \bar{\delta}_i$. For each $\delta' \in \Delta$, we have

$$[h_\delta, \sigma](\delta') = h_\delta^{-1}(\delta') h_\delta^\sigma(\delta') = h_\delta(\delta')^{-1} h_\delta(\delta'^{\sigma^{-1}}) = \begin{cases} g(\delta) & \text{if } \delta' = \delta, \\ g(\delta)^{-1} & \text{if } \delta' = \bar{\delta}_i, \\ 1 & \text{if } \delta' \in \Delta \setminus \{\delta, \bar{\delta}_i\}. \end{cases}$$

It follows $f_\delta = [h_\delta, \sigma] \in [B, P]$ and hence $g \in [B, P]$. So, $V \leqslant [B, P]$. Therefore

$$V = [B, P]. \tag{3.2}$$

From (3.1), (3.2) and from the fact that $|B : V| = |Q|^\ell$, we obtain

$$|W : \mathrm{Frat}(W)| = |BP : V\,\mathrm{Frat}(P)| = |P : \mathrm{Frat}(P)||B : V| = p^{d(P)}|Q|^\ell$$
$$= p^{d(P)}p^{d(Q)\ell} = p^{d(P)+n_\Delta(P)d(Q)}. \qquad \square$$

Given a permutation group X on Ω and $\omega \in \Omega$, we let $X_\omega := \{x \in X \mid \omega^x = \omega\}$ the stabilizer of ω in X. Let K be a transitive permutation group on a set Ω and let $\omega \in \Omega$. We define $t_\Omega(K)$ to be the maximum number $t \in \mathbb{N}$ of subgroups $U_1, \ldots, U_t$ of K with

(1) $K_\omega = U_1 \cap \cdots \cap U_t$, and

(2) $K_\omega \neq \bigcap_{j \in J} U_j$, for each proper subset J of $\{1, \ldots, t\}$.

When (1) and (2) are satisfied (even if t is not necessarily the maximum), we say that $U_1, \ldots, U_t$ are *independent* subgroups of K. Moreover, let S be a finite non-abelian simple group and let us denote by $\pi^*(S)$ the set of primes dividing $|S|$ but not $|\mathrm{Out}(S)|$.

THEOREM 3.2. *Let K be a transitive permutation group on Ω, let S be a non-abelian simple group and let G be a group with $S\mathrm{wr}_\Omega K \leqslant G \leqslant (\mathrm{Aut}\,S)\mathrm{wr}_\Omega K$. Then*

$$\sum_{p \in \pi^*(S)} d_p(G) > t_\Omega(K).$$

Proof. For every $p \in \pi^*(S)$, we have $d_p(G) = d_p(S\mathrm{wr}_\Omega K)$ and hence, without loss of generality, we may assume $G = S\mathrm{wr}_\Omega K$. For simplicity, we write

$$f(S, \Omega, K) := \sum_{p \in \pi^*(S)} d_p(G).$$

We argue by induction on $t := t_\Omega(K)$. When $t = 1$, from theorem 2.4 we deduce

$$f(S, \Omega, K) \geqslant \pi^*(S) \geqslant 2 > 1 = t.$$

Suppose then $t > 1$. Let $\omega \in \Omega$ and let $U_1, \ldots, U_t$ be t independent subgroups of K with

$$\bigcap_{i=1}^{t} U_i = K_\omega.$$

For each $i \in \{1, \ldots, t\}$, we define

$\bar{U}_i$ to be the intersection $\bigcap_{j \in \{1, \ldots, t\} \setminus \{i\}} U_j$; (as $K_\omega \leqslant \bar{U}_i$, the orbit $\omega^{\bar{U}_i} := \{\omega^x \mid x \in \bar{U}_i\}$ is a block of imprimitivity for the action of K on Ω.)

Ω_i to be the system of imprimitivity determined by the block of imprimitivity $\omega^{\bar{U}_i}$;

$\hat{K}_i$ to be the permutation group induced by K on Ω_i; (we also denote by $\sigma_i : K \to \hat{K}_i$ the natural projection, so $\hat{K}_i = \sigma_i(K)$.)

G_i to be the wreath product $G_i := S\mathrm{wr}_{\Omega_i} \hat{K}_i$.

Let $i \in \{1, \ldots, t\}$. Since the point stabilizer $\sigma_i(\bar{U}_i)$ of $\omega^{\bar{U}_i} \in \Omega_i$ in $\hat{K}_i$ is defined as the intersection of the $t-1$ independent subgroups $\{\sigma_i(U_j) \mid j \in \{1, \ldots, t\} \setminus \{i\}\}$, we have $t_{\Omega_i}(\hat{K}_i) \geqslant t-1$. Moreover, from our inductive argument, we have

$$\sum_{p \in \pi^*(S)} d_p(G_i) = f(S, \Omega_i, \hat{K}_i) > t_{\Omega_i}(\hat{K}_i) \geqslant t-1. \tag{3.3}$$

For each prime $p \in \pi^*(S)$, let Π_p be a Sylow p-subgroup of S and let P be a Sylow p-subgroup of K. In particular, $\hat{P}_i := \sigma_i(P)$ is a Sylow p-subgroup of $\hat{K}_i$. From lemma 3.1, for every $i \in \{1, \ldots, t\}$, we have

$$f(S, \Omega_i, \hat{K}_i) = \sum_{p \in \pi^*(S)} \left(d(\hat{P}_i) + n_{\Omega_i}(\hat{P}_i) d(\Pi_p) \right), \tag{3.4}$$

where $n_{\Omega_i}(\hat{P}_i) = n_{\Omega_i}(P)$ denotes the number of orbits of P on Ω_i. Observe that $d(P) \geqslant d(\hat{P}_i)$.

In particular, using (3.3) and (3.4), we deduce

$$f(S, \Omega, K) > t,$$

unless, for each $i \in \{1, \ldots, t\}$ and for each $p \in \pi^*(S)$,

(a) $d(P) = d(\hat{P}_i)$,

(b) $n_\Omega(P) = n_{\Omega_i}(P)$.

In particular, for the rest of the proof we may assume that (a) and (b) hold.

Since $|\pi^*(S)| \geqslant 2$, we may choose $p \in \pi^*(S)$ and $i \in \{1, \ldots, \ell\}$ such that $|\bar{U}_i : K_\omega|$ is not a power of p. Let $\hat{\delta}_1, \ldots, \hat{\delta}_s$ be a set of representatives of the orbits of P on Ω_i, where $s := n_{\Omega_i}(P)$. In other words, this means that

$$\Omega_i = \bigcup_{j=1}^{s} \{\hat{\delta}_j^x \mid x \in P\}$$

and that this union is disjoint. For each $j \in \{1, \ldots, s\}$, let $\delta_j \in \hat{\delta}_j$. As $\hat{\delta}_j \subseteq \Omega$ is a block of imprimitivity for the action of K on Ω, the union

$$\bigcup_{j=1}^{s} \{\delta_j^x \mid x \in P\} \subseteq \Omega \tag{3.5}$$

is made by pairwise disjoint P-orbits and hence $n_\Omega(P) \geqslant s = n_{\Omega_i}(P)$. Moreover, $n_\Omega(P) = n_{\Omega_i}(P)$ if and only if the equality in (3.5) is attained, which in turn happens, if and only if, for each $j \in \{1, \ldots, s\}$, the points in $\hat{\delta}_j \subseteq \Omega$ are in the same P-orbit.

Since we are assuming that $n_\Omega(P) = n_{\Omega_i}(P)$, the previous paragraph shows that the stabilizer $P_{\hat{\delta}_j}$ of the block $\hat{\delta}_j$ is transitive on the points in $\hat{\delta}_j$. Since P is a p-group, we deduce $|\hat{\delta}_j| = |\bar{U}_i : K_\omega|$ is a power of p, contradicting our choice of i and p. $\qquad\square$

4. Proofs of theorem 1.4 and corollary 1.6

If N is a normal subgroup of a finite group G, we denote by $m(G, N)$ the difference $m(G) - m(G/N)$. We recall in the first part of this section some results proved in [10, 11], estimating the value of $m(G, N)$ when N is a minimal normal subgroup of G.

LEMMA 4.1. *If N is an abelian minimal normal subgroup of G, then $m(G, N)$ is either 0 or 1 depending on whether $N \leqslant \mathrm{Frat}(G)$ or not.*

Proof. If follows from [10, lemmas 11 and 12]. $\qquad\square$

LEMMA 4.2. *Assume that N is a non-abelian minimal normal subgroup of a finite group G. There exist a non-abelian simple group S and a positive integer r such that $N = S_1 \times \cdots \times S_r$, with $S \cong S_i$ for each $1 \leqslant i \leqslant r$. Let K be the transitive subgroup of $\mathrm{Sym}(r)$ induced by the conjugacy action of G on the set $\{S_1, \ldots, S_r\}$ of the simple components of N. As in the previous section, let $t(K) := t_{\{1,\ldots,r\}}(K)$ be the largest positive integer t such that the stabilizer in K of a point in $\{1, \ldots, r\}$ can be obtained as an intersection of t independent subgroups. Moreover let X be the subgroup of $\mathrm{Aut}\, S_1$ induced by the conjugation action of $N_G(S_1)$ on the first factor S_1. Then*

$$m(G, N) \leqslant m(X, \mathrm{soc}\, X) + t(K).$$

Proof. If follows from [10, lemma 13] and [11, theorem 1]. $\qquad\square$

LEMMA 4.3. *Let N be a minimal normal subgroup of a finite group G. If $N \not\leqslant \mathrm{Frat}(G)$, then $\delta(G) \geqslant \delta(G/N) + |\pi(N)|$.*

Proof. It suffice to prove that $d_p(G) > d_p(G/N)$ whenever $p \in \pi(N)$. This is clear when N is abelian. Assume that N is non-abelian. Let $p \in \pi(N)$ and let P be a Sylow p-subgroup of G. If $P \cap N \leqslant \mathrm{Frat}(P)$, then Tate's Theorem [5, p. 431] shows that N has a normal p-complement. However, this is impossible because N is a direct product of non-abelian simple groups. Thus $P \cap N \not\leqslant \mathrm{Frat}(P)$, and consequently $d_p(G/N) + 1 \leqslant d_p(G)$. $\qquad\square$

Proof of theorem 1.4. Clearly the statement is true if G is simple. Thus we suppose that S is not a simple group and we proceed by induction on the order of G. We may assume $\mathrm{Frat}(G) = 1$. Let N be a minimal normal subgroup of G. If N is abelian, using lemma 4.3 and the inductive hypotheses, we have

$$m(G) = m(G/N) + 1 \leqslant \sigma\left(\delta(G/N)\right)^\eta + 1 \leqslant \sigma \cdot (\delta(G) - 1)^\eta + 1 \leqslant \sigma \cdot \delta(G)^\eta.$$

(In the last inequality, we used the fact that $\sigma \geqslant 1$ and $\eta \geqslant 2$.) Assume that N is non-abelian. Let K, X and S be as in the statement of lemma 4.2. By theorem 3.2,

we have

$$t(K) < \sum_{p \in \pi^*(S)} d_p(G) \leqslant \delta(G).$$

Combining this with lemmas 4.2 and 4.3, we conclude that

$$\begin{aligned}
m(G) &\leqslant m(G/N) + m(X, S) + t(K) \leqslant \sigma \cdot \delta(G/N)^\eta + \sigma \cdot |\pi(S)|^\eta + \delta(G) \\
&\leqslant \sigma \cdot \delta(G/N)^\eta + \sigma \cdot |\pi(S)|^\eta + \sigma \cdot \delta(G) \leqslant \sigma \left(\delta(G/N)^\eta + |\pi(N)|^\eta + \delta(G) \right) \\
&\leqslant \sigma ((\delta(G/N)^\eta + (\delta(G) - \delta(G/N))^\eta + \delta(G/N) + (\delta(G) - \delta(G/N)))) \\
&\leqslant \sigma \cdot \delta(G)^\eta.
\end{aligned}$$

The last inequality follows from the fact that $x^\eta + y^\eta + x + y \leqslant (x+y)^\eta$, for every positive integers x and y and for every $\eta \geqslant 2$. $\qquad \square$

In order to prove corollary 1.6, we first need the following lemma.

LEMMA 4.4. *For every positive real number $\eta > 1$, there exists a constant c_η such that $n \leqslant c_\eta \pi(n)^\eta$, where $\pi(n)$ is the number of prime numbers less than or equal to n.*

Proof. By [**14**, theorem 29], if $n \geqslant 55$, then $\pi(n) > n/\log n + 2$, so if suffices to notice that $\lim_{n \to \infty} n^{\eta-1}/(\log n + 2)^\eta = \infty$. $\qquad \square$

LEMMA 4.5. *There exists a constant ρ such that, if X is an almost simple group and $S = \mathrm{soc}(X)$ is not a simple group of Lie type, then $m(X, S) \leqslant \rho \cdot |\pi(S)|^2$.*

Proof. First assume that $S = \mathrm{Alt}(n)$. By [**17**, theorem 1], $m(X, S) \leqslant n - 1$. By lemma 4.4, there exists a constant c_2 such that $m(X, S) \leqslant c_2 \pi(n)^2 = c_2 \cdot |\pi(S)|^2$. Clearly there exists a constant c such that $m(X, S) \leqslant c \cdot |\pi(S)|^2$, for every sporadic simple group S. Taking $\rho = \max\{c, c_2\}$, the result follows. $\qquad \square$

Proof of corollary 1.6. It follows from theorem 1.4 and lemma 4.5. $\qquad \square$

5. Estimating $\delta(\mathrm{Sym}(n))$

In this section, we aim to bound, from above and from below, $\delta(\mathrm{Sym}(n))$ as a function of n. By [**17**, theorem 1], $m(\mathrm{Sym}(n)) = n - 1$ while, by Kalužnin's Theorem, if

$$a_{\ell(p,n)} p^{\ell(p,n)} + a_{\ell(p,n)-1} p^{\ell(p,n)-1} + \cdots + a_1 p + a_0$$

is the p-adic expansion of n, then

$$d_p(\mathrm{Sym}(n)) = a_{\ell(p,n)} \ell(p, n) + a_{\ell(p,n)-1}(\ell(p, n) - 1) + \cdots + a_1.$$

In order to make the notation less cumbersome, we set

$$d_p(n) := d_p(\mathrm{Sym}(n)) = a_{\ell(p,n)} \ell(p, n) + a_{\ell(p,n)-1}(\ell(p, n) - 1) + \cdots + a_1$$

and

$$\delta(n) := \sum_{p \text{ prime}} d_p(n) = \delta(\operatorname{Sym}(n)).$$

As in the previous sections we denote by $\pi : \mathbb{R} \to \mathbb{N}$ the prime counting function, that is, $\pi(x)$ is the number of prime numbers less than or equal to x. As $d_p(n) \geqslant 1$ for every prime $p \leqslant n$, we have

$$\pi(n) \leqslant \delta(n).$$

From the Prime Number Theorem, $\pi(n)$ is asymptotic to $n/\log n$ (that is, the ratio $\pi(n)/(n/\log n)$ tends to 1 as n tends to infinity) and hence $n/\log n \in O(\delta(n))$. In this section, we actually prove that $\delta(n)$ is asymptotic to a linear function.

THEOREM 5.1. *For every $n \geqslant 2$, we have*

$$n \log 2 - \frac{12n}{\log n} \leqslant \delta(n) \leqslant n \log 2 + \frac{19n}{2 \log n} + \frac{137n}{2 \log^2 n} + \frac{4\sqrt{n}}{\log n}$$

$$+ \frac{3\sqrt{n}}{2} \log n \leqslant n \log 2 + \frac{112n}{\log n}.$$

In particular, $\delta(n) = n \log 2 + O(n/\log n)$.

Proof. We start by collecting some basic inequalities that we use throughout this proof. From theorems 1 and 2 in [**15**], we have

$$\pi(x) \leqslant \frac{x}{\log x} \left(1 + \frac{3}{2 \log x}\right), \quad \forall x > 1, \tag{5.1}$$

$$\pi(x) \geqslant \frac{x}{\log x - 1/2}, \quad \forall x \geqslant 67. \tag{5.2}$$

Given a prime number p with $p \leqslant n$, $\ell(p,n) \leqslant \lfloor \log_p n \rfloor$ and hence

$$d_p(n) \leqslant (p-1)(\ell(p,n) + (\ell(p,n) - 1) + \cdots + 2 + 1)$$

$$= (p-1)\frac{\ell(p,n)(\ell(p,n)+1)}{2} \leqslant (p-1)\frac{\log_p n(\log_p n + 1)}{2}. \tag{5.3}$$

We define the two auxiliary functions

$$d'(n) := \sum_{p \leqslant \sqrt{n}} d_p(n); \quad d''(n) := \sum_{\sqrt{n} < p \leqslant n} d_p(n).$$

We aim to obtain explicit bounds on $d'(n)$ and $d''(n)$ as functions of n. We start with $d'(n)$.

From (5.3), we get

$$d'(n) \leqslant \frac{\log^2 n}{2} \sum_{p \leqslant \sqrt{n}} \frac{p-1}{\log^2 p} + \frac{\log n}{2} \sum_{p \leqslant \sqrt{n}} \frac{p-1}{\log p}. \tag{5.4}$$

For every $k \in \mathbb{N}$ with $k \geqslant 1$, we denote by p_k the kth prime number. Using [**15**, corollary, p. 69], we have

$$k \log k < p_k < k(\log k + \log \log k),$$

where the first inequality is valid for every $k \geqslant 1$ and the second inequality is valid for every $k \geqslant 6$.

This shows that, for every $k \geqslant 6$,

$$\frac{p_k - 1}{\log p_k} \leqslant \frac{k(\log k + \log \log k)}{\log(k \log k)} = k. \tag{5.5}$$

An explicit computation yields that (5.5) is also valid when $k \in \{2, 3, 4, 5\}$.

Therefore, for $n \geqslant 11$, (5.1) and (5.5) yield:

$$\sum_{p \leqslant \sqrt{n}} \frac{p-1}{\log p} = \frac{1}{\log 2} + \sum_{2 < p \leqslant \sqrt{n}} \frac{p-1}{\log p} = \frac{1}{\log 2} + \sum_{k=2}^{\pi(\sqrt{n})} \frac{p_k - 1}{\log p_k} \leqslant \frac{1}{\log 2} + \sum_{k=2}^{\pi(\sqrt{n})} k$$

$$= \frac{1}{\log 2} + \frac{\pi(\sqrt{n})(\pi(\sqrt{n}) + 1)}{2} - 1 = \frac{1}{\log 2} - 1 + \frac{\pi(\sqrt{n})^2}{2} + \frac{\pi(\sqrt{n})}{2}$$

$$\leqslant -1 + \frac{1}{\log 2} + \frac{1}{2} \left(\frac{\sqrt{n}}{\log \sqrt{n}} \left(1 + \frac{3}{2 \log \sqrt{n}} \right) \right)^2$$

$$+ \frac{\sqrt{n}}{2 \log \sqrt{n}} \left(1 + \frac{3}{2 \log \sqrt{n}} \right)$$

$$= -1 + \frac{1}{\log 2} + \frac{1}{2} \left(\frac{4n}{\log^2 n} + \frac{36n}{\log^4 n} + \frac{24n}{\log^3 n} \right) + \frac{\sqrt{n}}{\log n} + \frac{3\sqrt{n}}{\log^2 n}$$

$$\leqslant \frac{2n}{\log^2 n} + \frac{24n}{\log^3 n}.$$

In fact, we only require n to be at least 11 for the last inequality above. Thus, using this, together with direct inspection for the cases $2 \leqslant n \leqslant 10$, we have:

$$\sum_{p \leqslant \sqrt{n}} \frac{p-1}{\log p} \leqslant \frac{2n}{\log^2 n} + \frac{24n}{\log^3 n}, \tag{5.6}$$

for every $n > 1$.

Arguing in a similar manner, for every $k \geqslant 6$, we obtain

$$\frac{p_k - 1}{\log^2 p_k} \leqslant \frac{k(\log k + \log \log k)}{\log^2(k \log k)} = \frac{k}{\log k + \log \log k}. \tag{5.7}$$

An explicit computation yields that (5.7) is also valid when $k \in \{2, 3, 4, 5\}$. Therefore, using (5.7), we have

$$\sum_{p \leqslant \sqrt{n}} \frac{p - 1}{\log^2(p)} \leqslant \frac{1}{\log^2(2)} + \sum_{k=2}^{\pi(\sqrt{n})} \frac{k}{\log k + \log \log k}.$$

For every $t \in \mathbb{N}$ with $t \geqslant 2$, write $f(t) := \sum_{k=2}^{t} k/(\log k + \log \log k)$. When $k > 2$, we have $k/(\log k + \log \log k) \leqslant k$. Moreover, when $k \geqslant \sqrt{t}$, we have

$$\frac{k}{\log k + \log \log k} \leqslant \frac{k}{\log \sqrt{t} + \log \log(\sqrt{t})} = \frac{k}{\log t/2 + \log(\log t) - \log 2}$$

$$\leqslant \frac{2k}{\log t},$$

where the last inequality holds for $t \geqslant 8$. Therefore, for every $t \geqslant 8$, we have

$$f(t) = \frac{2}{\log 2 + \log \log 2} + \sum_{2 < k \leqslant \sqrt{t}} \frac{k}{\log k + \log \log k} + \sum_{\sqrt{t} < k \leqslant t} \frac{k}{\log k + \log \log k}$$

$$\leqslant \frac{2}{\log 2 + \log \log 2} + \sum_{2 < k \leqslant \sqrt{t}} k + \sum_{\sqrt{t} < k \leqslant t} \frac{2k}{\log t}$$

$$\leqslant \frac{2}{\log 2 + \log \log 2} + \frac{\sqrt{t}(\sqrt{t} + 1)}{2} - 3 + \frac{t(t+1)}{\log t} \leqslant \frac{t^2}{\log t} + t,$$

where the last inequality follows with some elementary computations. A direct computation with $2 \leqslant t < 8$ shows that the same upper bound for $f(t)$ holds. Therefore, applying this upper bound with $t := \pi(\sqrt{n})$, we get

$$\sum_{p \leqslant \sqrt{n}} \frac{p - 1}{\log^2(p)} \leqslant \frac{1}{\log^2 2} + f(\pi(\sqrt{n})) \leqslant \frac{1}{\log^2 2} + \frac{\pi(\sqrt{n})^2}{\log \pi(\sqrt{n})} + \pi(\sqrt{n}). \tag{5.8}$$

Now, for every $n \geqslant 67^2$, using (5.1) and (5.2), we see that the right-hand side of (5.8) is bounded above by

$$\frac{1}{\log^2 2} + \frac{\left(\frac{\sqrt{n}}{\log \sqrt{n}} \left(1 + \frac{3}{2 \log \sqrt{n}}\right)\right)^2}{\log\left(\frac{\sqrt{n}}{\log \sqrt{n} - 1/2}\right)} + \frac{\sqrt{n}}{\log \sqrt{n}} \left(1 + \frac{3}{2 \log \sqrt{n}}\right). \tag{5.9}$$

The second summand of (5.9) is at most

$$\frac{\frac{4n}{\log^2 n} \left(1 + \frac{3}{\log n}\right)^2}{\log(\sqrt{n}/\log \sqrt{n})}.$$

Now, we have $\log(\sqrt{n}/\log\sqrt{n}) > \log n/4$. Thus the second summand of (5.9) is at most

$$\frac{16n}{\log^3 n} + \frac{96n}{\log^4 n} + \frac{144n}{\log^5 n} \leqslant \frac{16n}{\log^3 n} + \frac{114n}{\log^4 n},$$

where the last inequality follows with a computation using the fact that $n \geqslant 67^2$. For the first and third summand of (5.9), we have

$$\frac{1}{\log^2(2)} + \frac{2\sqrt{n}}{\log(n)} + \frac{6\sqrt{n}}{\log^2(n)} < \frac{3\sqrt{n}}{\log(n)},$$

where this inequality follows again with some elementary computations using the fact that $n \geqslant 67^2$. Summing up, for every $n \geqslant 67^2$, we have

$$\sum_{p \leqslant \sqrt{n}} \frac{p-1}{\log^2 p} \leqslant \frac{16n}{\log^3 n} + \frac{114n}{\log^4 n} + \frac{3\sqrt{n}}{\log n}. \tag{5.10}$$

A direct inspection shows that this bound is also valid for the natural numbers n with $n \leqslant 67^2$.

Summing up, from (5.4), (5.6) and (5.10), we get

$$d'(n) \leqslant \frac{8n}{\log n} + \frac{57n}{\log^2 n} + \frac{3}{2}\sqrt{n}\log(n) + \frac{n}{\log n} + \frac{12n}{\log^2 n}$$

$$= \frac{9n}{\log n} + \frac{69n}{\log^2 n} + \frac{3}{2}\sqrt{n}\log n. \tag{5.11}$$

We now start working on the function $d''(n) = \sum_{\sqrt{n}<p\leqslant n} d_p(n)$. Here we are interested in a lower bound and in an upper bound for $d''(n)$. First we obtain an upper bound for $d''(n)$. As $p > \sqrt{n}$, the p-adic expansion of n is simply $n := a_1(p,n)p + a_0$ and hence $d_p(n) = a_1(p,n)$. Now we refine further $d''(n)$. For every $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor - 1\}$, we let

$$g_i(n) := \sum_{n/(i+1)<p\leqslant n/i} a_1(p,n)$$

and we let

$$g_{\lfloor\sqrt{n}\rfloor}(n) := \sum_{\sqrt{n}<p\leqslant n/\lfloor\sqrt{n}\rfloor} a_1(p,n).$$

When $i \in \{1, \ldots, \lfloor\sqrt{n}\rfloor\}$, we have $a_1(p,n) = i$ and hence $g_i(n)$ equals i times the number of prime numbers in the interval $(n/(i+1), n/i]$. Therefore, when

$i \in \{1, \ldots, \lfloor \sqrt{n} \rfloor - 1\}$,

$$g_i(n) = i(\pi(n/i) - \pi(n/(i+1)))$$

and

$$g_{\lfloor \sqrt{n} \rfloor}(n) = \lfloor \sqrt{n} \rfloor (\pi(n/\lfloor \sqrt{n} \rfloor) - \pi(\sqrt{n})).$$

Since every prime p, with $\sqrt{n} < p \leqslant n$, lies in one of the intervals $(n/(i+1), n/i]$, for some $i \in \{1, \ldots, \lfloor \sqrt{n} \rfloor - 1\}$, or in the interval $(\sqrt{n}, n/\lfloor \sqrt{n} \rfloor]$, we have

$$d''(n) = \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} g_i(n) = \sum_{i=1}^{\lfloor \sqrt{n} \rfloor - 1} i(\pi(n/i) - \pi(n/(i+1))) + \lfloor \sqrt{n} \rfloor (\pi(n/\lfloor \sqrt{n} \rfloor) - \pi(\sqrt{n}))$$

$$= \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \pi(n/i) - \lfloor \sqrt{n} \rfloor \pi(\sqrt{n}). \tag{5.12}$$

Using (5.1), we have

$$\sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \pi(n/i) \leqslant \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log(n/i)} \left(1 + \frac{3}{2 \log(n/i)} \right)$$

$$= \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log(n/i)} + \frac{3}{2} \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log^2(n/i)}. \tag{5.13}$$

The function $x \mapsto (n/x)/\log(n/x)$ is decreasing in the interval $(0, \lfloor \sqrt{n} \rfloor]$ and hence we obtain for the first summand the estimate

$$\sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log(n/i)} = \frac{n}{\log n} + \sum_{i=2}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log(n/i)} \leqslant \frac{n}{\log n} + \int_1^{\lfloor \sqrt{n} \rfloor} \frac{n/x}{\log(n/x)} \, \mathrm{d}x$$

$$= \frac{n}{\log n} + [-n \log(\log(n/x))]_1^{\lfloor \sqrt{n} \rfloor}$$

$$= \frac{n}{\log n} - n \log \log(n/\lfloor \sqrt{n} \rfloor) + n \log(\log n). \tag{5.14}$$

For the second summand observe that the function $x \mapsto (n/x)/\log^2(n/x)$ is decreasing in the interval $(0, \lfloor \sqrt{n} \rfloor]$ and hence we obtain the estimate

$$\frac{3}{2} \sum_{i=1}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log^2(n/i)} = \frac{3n}{2 \log^2 n} + \frac{3}{2} \sum_{i=2}^{\lfloor \sqrt{n} \rfloor} \frac{n/i}{\log^2(n/i)}$$

$$\leqslant \frac{3n}{2 \log^2 n} + \frac{3}{2} \int_1^{\lfloor \sqrt{n} \rfloor} \frac{n/x}{\log^2(n/x)} \, \mathrm{d}x$$

$$= \frac{3n}{2 \log^2(n)} + \frac{3}{2} \left[\frac{n}{\log(n/x)} \right]_1^{\lfloor \sqrt{n} \rfloor}$$

$$= \frac{3n}{2 \log^2(n)} + \frac{3n}{2 \log(n/\lfloor \sqrt{n} \rfloor)} - \frac{3n}{2 \log n}. \tag{5.15}$$

Further, for $n \geqslant 67^2$, we get

$$
\begin{aligned}
\lfloor \sqrt{n} \rfloor \pi(\sqrt{n}) &\geqslant (\sqrt{n} - 1)\frac{\sqrt{n}}{\log \sqrt{n} - 1/2} = \frac{2n}{\log n - 1} - \frac{2\sqrt{n}}{\log n - 1} \\
&= \frac{2n}{\log n} + 2n\left(\frac{1}{\log n - 1} - \frac{1}{\log n}\right) - \frac{2\sqrt{n}}{\log n - 1} \\
&\geqslant \frac{2n}{\log n} + \frac{2n}{\log n(\log n - 1)} - \frac{2\sqrt{n}}{\log n/2} \\
&\geqslant \frac{2n}{\log n} + \frac{2n}{\log^2 n} - \frac{4\sqrt{n}}{\log n}.
\end{aligned}
\tag{5.16}
$$

Thus, from (5.12), (5.13), (5.14), (5.15) and (5.16), for every $n \geqslant 67^2$, we have that

$$
d''(n) \leqslant n\log(\log n) - n\log(\log(n/\lfloor \sqrt{n} \rfloor)) - \frac{n}{2\log n} + \frac{3n}{2\log^2 n} + \frac{3n}{2\log(n/\lfloor \sqrt{n} \rfloor)}
$$
$$
- \frac{2n}{\log n} - \frac{2n}{\log^2 n} + \frac{4\sqrt{n}}{\log n}.
$$

First of all, as $n/\lfloor \sqrt{n} \rfloor \geqslant \sqrt{n}$, we get $\log(n/\lfloor \sqrt{n} \rfloor) \geqslant \log \sqrt{n} = \log(n)/2$ and hence

$$
-\frac{n}{2\log n} + \frac{3n}{2\log(n/\lfloor \sqrt{n} \rfloor)} - \frac{2n}{\log n} \leqslant \left(-\frac{1}{2} + 3 - 2\right)\frac{n}{\log n} = \frac{n}{2\log n}.
$$

Moreover,

$$
\begin{aligned}
n\log(\log n) - n\log(\log(n/\lfloor \sqrt{n} \rfloor)) &\leqslant n\log\log n - n\log\log(\sqrt{n}) \\
&= n\log\left(\frac{\log n}{\log \sqrt{n}}\right) = n\log 2.
\end{aligned}
$$

Summing up, for every $n \geqslant 67^2$,

$$
d''(n) \leqslant n\log 2 + \frac{n}{2\log n} - \frac{n}{2\log^2 n} + \frac{4\sqrt{n}}{\log n}.
\tag{5.17}
$$

An explicit computation with the positive integers n with $2 \leqslant n < 67^2$ shows that the same upper bound remains true when $n \leqslant 67^2$.

Using the upper bounds (5.11) and (5.17), for every $n \geqslant 2$, we deduce

$$
\delta(n) = d'(n) + d''(n) \leqslant n\log 2 + \frac{19n}{2\log n} + \frac{137n}{2\log^2 n} + \frac{4\sqrt{n}}{\log n}
$$
$$
+ \frac{3\sqrt{n}}{2}\log n \leqslant n\log 2 + \frac{112n}{\log n},
$$

where the last inequality follows with some computation.

Now, we use the argument above to obtain also a lower bound for $d''(n)$ and hence for $d''(n)$. Using (5.2) and (5.12), we have

$$d''(n) = \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \pi(n/i) - \lfloor\sqrt{n}\rfloor\pi(\sqrt{n}) \geqslant \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log(n/i) - 1/2} - \lfloor\sqrt{n}\rfloor\pi(\sqrt{n})$$

$$\geqslant \sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log(n/i)} - \sqrt{n}\pi(\sqrt{n}).$$

The function $x \mapsto (n/x)/\log(n/x)$ is decreasing in the interval $(0, \lfloor\sqrt{n}\rfloor]$ and hence we obtain the estimate

$$\sum_{i=1}^{\lfloor\sqrt{n}\rfloor} \frac{n/i}{\log(n/i)} \geqslant \int_1^{\lfloor\sqrt{n}\rfloor} \frac{n/x}{\log(n/x)}\,\mathrm{d}x = [-n\log(\log(n/x))]_1^{\lfloor\sqrt{n}\rfloor}$$

$$= -n\log\log(n/\lfloor\sqrt{n}\rfloor) + n\log(\log n) = n\log\left(\frac{\log n}{\log(n/\lfloor\sqrt{n}\rfloor)}\right)$$

$$= n\log\left(\frac{\log n}{\log n - \log(\lfloor\sqrt{n}\rfloor)}\right)$$

$$= n\log\left(\frac{\log n}{\log n - \log\sqrt{n} - \log(\lfloor\sqrt{n}\rfloor/\sqrt{n})}\right)$$

$$= n\log\left(\frac{\log n}{(\log n)/2 - \log(\lfloor\sqrt{n}\rfloor/\sqrt{n})}\right) \geqslant n\log 2,$$

where in the last inequality we used the fact that $\lfloor\sqrt{n}\rfloor/\sqrt{n} \leqslant 1$ and hence $\log(\lfloor\sqrt{n}\rfloor/\sqrt{n}) \leqslant 0$. Furthermore, from (5.1), we have

$$\sqrt{n}\pi(\sqrt{n}) \leqslant \frac{n}{\log\sqrt{n}}\left(1 + \frac{3}{2\log\sqrt{n}}\right) = \frac{2n}{\log n}\left(1 + \frac{3}{\log n}\right) \leqslant \frac{12n}{\log n},$$

where the last inequality follows from an easy computation. Summing up,

$$\delta(n) = d'(n) + d''(n) \geqslant d''(n) \geqslant n\log 2 - \frac{12n}{\log n}. \qquad \square$$

References

1   P. Apisa and B. Klopsch. A generalization of the Burnside basis theorem. *J. Algebra* **400** (2014), 8–16.

2   P. Cameron and P. Cara. Independent generating sets and geometries for symmetric groups. *J. Algebra* **258** (2002), 641–650.

3   R. Guralnick. On the number of generators of a finite group. *Arch. Math.* **53** (1989), 521–523.

4   M. Herzog. On finite simple groups of order divisible by three primes only. *J. Algebra* **10** (1968), 383–388.

5   B. Huppert. *Endliche Gruppen*. I. (German) Die Grundlehren der Mathematischen Wissenschaften, Band 134 (Springer-Verlag, Berlin-New York, 1967).

6   P. J. Keen, Independent sets in some classical groups of dimension three, Ph.D. Thesis. University of Birmingham, 2012.

7   P. Kleidman and M. Liebeck. *The subgroup structure of the finite classical groups*. London Mathematical Society Lecture Note Series, vol. 129 (Cambridge: Cambridge University Press, 1990).

8   W. Kimmerle, R. Lyons, R. Sandling and D. N. Teague. Composition factors from the group ring and Artin's theorem on orders of simple groups. *Proc. London Math. Soc.* **60** (1990), 89–122.

9   A. Lucchini. A bound on the number of generators of a finite group. *Arch. Math.* **53** (1989), 313–317.

10 A. Lucchini. The largest size of a minimal generating set of a finite group. *Arch. Math.* **101** (2013), 1–8.

11 A. Lucchini. Minimal generating sets of maximal size in finite monolithic groups. *Arch. Math.* **101** (2013), 401–410.

12 A. Lucchini. A bound on the expected number of random elements to generate a finite group all of whose Sylow subgroups are d-generated. *Arch. Math.* **107** (2016), 1–8.

13 P. Ribenboin. *The book of prime number records*, 2nd edn. (New York: Springer-Verlag, 1989).

14 B. Rosser. Explicit bounds for some functions of prime numbers. *Amer. J. Math.* **63** (1941), 211–232.

15 J. K. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962), 64–94.

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

17 J. Whiston. Maximal independent generating sets of the symmetric group. *J. Algebra* **232** (2000), 255–268.

18 K. Zsigmondy. Zur Theorie der Potenzreste. *Monatsch. Math. Phys.* **3** (1892), 265–284.