Journal of Algebra 635 (2023) 486–526

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

On the maximum number of subgroups of a finite group

Marco Fusari [a], Pablo Spiga [b,*]

[a] *Dipartimento di Matematica "Felice Casorati", University of Pavia, Via Ferrata 5, 27100 Pavia, Italy*
[b] *Dipartimento di Matematica Pura e Applicata, University of Milano-Bicocca, Via Cozzi 55, 20126 Milano, Italy*

ARTICLE INFO

Article history:
Received 27 April 2023
Available online 28 August 2023
Communicated by E.I. Khukhro

MSC:
primary 20D99

Keywords:
Subgroup lattice
Upper bound
Number subgroups

ABSTRACT

Given a finite group R, we let $\mathrm{Sub}(R)$ denote the collection of all subgroups of R. We show that $|\mathrm{Sub}(R)| < c \cdot |R|^{\frac{\log_2(|R|)}{4}}$, where $c < 7.372$ is an explicit absolute constant. This result is asymptotically best possible. Indeed, as $|R|$ tends to infinity and R is an elementary abelian 2-group, the ratio

$$\frac{|\mathrm{Sub}(R)|}{|R|^{\frac{\log_2(|R|)}{4}}}$$

tends to c.

1. Introduction

Let R be a finite group of order r and let

$$\mathrm{Sub}(R)$$

* Corresponding author.
E-mail addresses: lucamarcofusari@gmail.com (M. Fusari), pablo.spiga@unimib.it (P. Spiga).

https://doi.org/10.1016/j.jalgebra.2023.07.047

be the family of subgroups of R. It has been observed several times [1,7–9] that, when R is an elementary abelian p-group, there exist two constants c_p and c'_p depending on p only such that

$$c_p \cdot r^{\frac{\log_p(r)}{4}} \leq |\mathrm{Sub}(R)| \leq c'_p \cdot r^{\frac{\log_p(r)}{4}}.$$

Borovik, Pyber and Shalev [2, Corollary 1.6] have shown that, for an arbitrary finite group R of order r, we have

$$|\mathrm{Sub}(R)| \leq r^{\log_2(r)\left(\frac{1}{4}+o(1)\right)}.$$

Therefore, in the light of the comment on elementary abelian p-groups, this bound is asymptotically best possible.

Besides a natural theoretic interest, there are several practical applications that require an explicit upper bound on $|\mathrm{Sub}(R)|$. In particular, these applications require to replace the "$o(1)$" appearing in the exponent of r with an explicit constant. All applications that we are aware of come from the problem of classifying graphical regular representations of finite groups, see the introductory section of [9] for more details.

Now, let p be a prime number and let

$$c(p) := \prod_{i\geq 1} \frac{1}{1-\frac{1}{p^i}} \left(-1 + 2\sum_{k=0}^{\infty} \frac{1}{p^{k^2}}\right). \tag{1.1}$$

In [9], it was shown that, when R is an elementary abelian p-group, $|\mathrm{Sub}(R)|$ is asymptotic to $c(p)|R|^{\log_p(|R|)/4}$ as $|R|$ tends to infinity. Moreover, using elementary methods, it was shown that, for a fixed prime p, when R is an arbitrary group, $|\mathrm{Sub}(R)| \leq c(2)|R|^{\log_2(|R|)/4+1.5315}$. In this paper, using more sophisticated methods, we improve this result.

Theorem 1.1. *Let R be a finite group and let* $\mathrm{Sub}(R)$ *be the family of all subgroups of R. Then* $|\mathrm{Sub}(R)| < c(2)|R|^{\frac{\log_2(|R|)}{4}}$.

We observe that $c(2)$ is approximately

$$7.37197.$$

2. Preliminaries

Let R be a non-identity finite group and let r be the order of R. Let

$$r = \prod_{i=1}^{\ell} p_i^{a_i}$$

be the prime factorization of r. In particular, $p_1, \dots, p_\ell$ are distinct prime numbers and $a_i \geq 1$ for each $i \in \{1, \dots, \ell\}$. Relabeling the indexed set if necessary, we may suppose that

$$p_1 < p_2 < \cdots < p_\ell.$$

Let H be a subgroup of R. Then H is uniquely determined by a family $(Q_i)_i$ of Sylow p_i-subgroups of H, for each $i \in \{1, \dots, \ell\}$. Each of these subgroups Q_i is contained in a Sylow p_i-subgroup P_i of R. From Sylow's theorems, all Sylow p_i-subgroups of R are conjugate and hence R has at most $r/{p_i}^{a_i}$ Sylow p_i-subgroups. Let n_i be the number of Sylow p_i-subgroups of R. Then

$$n_i = |R : \mathbf{N}_R(P_i)| = \frac{r}{|\mathbf{N}_R(P_i) : P_i| p_i^{a_i}}. \tag{2.1}$$

Therefore, we have

$$\prod_{i=1}^{\ell} \frac{r}{|\mathbf{N}_R(P_i) : P_i| p_i^{a_i}} = r^{\ell-1} \cdot \prod_{i=1}^{\ell} \frac{1}{|\mathbf{N}_R(P_i) : P_i|} \tag{2.2}$$

choices for the ℓ-tuple $(P_i)_i$. When $(P_i)_i$ is given, since Q_i is a subgroup of P_i and since P_i is a p_i-group, we have at most

$$\prod_{i=1}^{\ell} S(p_i, a_i)$$

choices for the ℓ-tuple $(Q_i)_i$, where $S(p_i, a_i)$ is the function defined in [9]. (The function $S(p, a)$ has the property that every p-group of order p^a has at most $S(p, a)$ subgroups, see Lemma 2.1. For not breaking the flow of the argument, we postpone the definition of $S(p, a)$ to (1.1) in Section 2.1.) Thus R has at most

$$r^{\ell-1} \cdot \prod_{i=1}^{\ell} \frac{1}{|\mathbf{N}_R(P_i) : P_i|} \cdot \prod_{i=1}^{\ell} S(p_i, a_i)$$

subgroups.

We are interested in studying when

$$r^{\ell-1} \cdot \prod_{i=1}^{\ell} \frac{1}{|\mathbf{N}_R(P_i) : P_i|} \cdot \prod_{i=1}^{\ell} S(p_i, a_i) < c(2) \cdot r^{\frac{\log_2(r)}{4}} \tag{2.3}$$

holds, because in this case Theorem 1.1 immediately follows.

By taking $\log_r$ on both sides of (2.3), we obtain the equivalent inequality

$$\ell - 1 - \sum_{i=1}^{\ell} \log_r(|\mathbf{N}_R(P_i) : P_i|) + \sum_{i=1}^{\ell} \log_r(S(p_i, a_i)) < \log_r(c(2)) + \sum_{i=1}^{\ell} a_i \frac{\log_2(p_i)}{4}.$$

Finally, this can be rewritten in the following form

$$\ell - 1 - \sum_{i=1}^{\ell} \frac{\log(|\mathbf{N}_R(P_i) : P_i|)}{\log(r)} < \frac{\log(c(2))}{\log(r)} + \sum_{i=1}^{\ell} \left(\frac{a_i \log(p_i)}{4 \log(2)} - \frac{\log(S(p_i, a_i))}{\log(r)} \right). \quad (2.4)$$

2.1. The function $S(p, a)$

Let p be a prime number and let a be a positive integer. We define

$$S(p,a) := \begin{cases} 2 & \text{when } a := 1, \\ p+3 & \text{when } a := 2, \\ 2p^2+2p+4 & \text{when } a := 3, \\ p^4+3p^3+4p^2+3p+5 & \text{when } a := 4, \\ 2p^6+2p^5+6p^4+6p^3+6p^2+4p+6 & \text{when } a := 5, \\ c(p)p^{\frac{a^2}{4}} & \text{when } a \geq 6. \end{cases} \quad (2.5)$$

We observe that in [9], the value of $c(p)$ is slightly different from the value we have defined in (1.1). In general, the value we have set for $c(p)$ in (1.1) is less than or equal to the value of $c(p)$ in [9], and it coincides with the value in [9] when $p = 2$. All the results in [9] remain valid with this slightly improved constant. In particular, we have the following lemma.

Lemma 2.1. *Let R be an elementary abelian p-group of order p^a. Then $|\mathrm{Sub}(R)| \leq S(p,a) < c(2)|R|^{\frac{\log_2(|R|)}{4}}$.*

Proof. The proof follows from Remark 3.1 and Lemma 3.2 in [9]. □

From Lemma 2.1, for the proof of Theorem 1.1, we may suppose that $\ell \geq 2$. Indeed, throughout the rest of this paper, we tacitly assume $\ell \geq 2$. Furthermore, throughout the rest of this paper, we also tacitly assume the notation in this section.

We conclude this section with some numerical information.

Lemma 2.2. *For every positive integer a and for every prime number p, we have $S(p,a) \leq c(p)p^{a^2/4}$.*

Proof. When $a \geq 6$, by (2.5), we have $S(p,a) = c(p)p^{a^2/4}$. When $a \leq 5$, the proof follows from some computations.

From (1.1), we have

$$c(p) > \frac{1}{1-\frac{1}{p}} \cdot \left(-1+2\left(1+\frac{1}{p}\right)\right) = \frac{p+2}{p-1}.$$

Assume $a=1$, that is, $S(p,a)=2$. We have

$$2 \leq \frac{p+2}{p-1} \cdot p^{\frac{1}{4}} < c(p) \cdot p^{\frac{1}{4}} = c(p)p^{\frac{a^2}{4}},$$

for every p (when $p \leq 15$, the first inequality can be verified directly and, when $p \geq 16$, it is clear, because $p^{1/4} \geq 2$). Assume $a=2$, that is, $S(p,a)=p+3$. We have

$$p+3 \leq \frac{p+2}{p-1} \cdot p < c(p) \cdot p = c(p)p^{\frac{a^2}{4}},$$

for every p (the first inequality follows from an easy computation). Assume $a=3$, that is, $S(p,a)=2p^2+2p+4$. We have

$$2p^2+2p+4 \leq \frac{p+2}{p-1} \cdot p^{\frac{9}{4}} < c(p) \cdot p^{\frac{9}{4}} = c(p)p^{\frac{a^2}{4}},$$

for every p (when $p \leq 15$, the first inequality can be verified directly and, when $p \geq 16$, it is clear, because $p^{1/4} \geq 2$ and $p^2+p+2 \leq (p+2)p^2/(p-1)$).

To deal with larger values of a, we need to refine the estimate on $c(p)$. From (1.1), we have

$$c(p) > \frac{1}{\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)} \cdot \left(-1+2\left(1+\frac{1}{p}\right)\right) = \frac{p^3+2p^2}{(p-1)(p^2-1)}.$$

Assume $a=4$, that is, $S(p,a)=p^4+3p^3+4p^2+3p+5$. We have

$$p^4+3p^3+4p^2+3p+5 \leq \frac{p^3+2p^2}{(p-1)(p^2-1)} \cdot p^4 < c(p) \cdot p^4 = c(p)p^{\frac{a^2}{4}},$$

for every p (the first inequality follows from a computation by expanding the two members and manipulating the two polynomials in p). Finally, assume $a=5$, that is, $S(p,a)=2p^6+2p^5+6p^4+6p^3+6p^2+4p+6$. We have

$$2p^6+2p^5+6p^4+6p^3+6p^2+4p+6 \leq \frac{p^3+2p^2}{(p-1)(p^2-1)} \cdot p^{\frac{25}{4}} < c(p) \cdot p^{\frac{25}{4}} = c(p)p^{\frac{a^2}{4}},$$

for every p (when $p \leq 15$, the first inequality can be verified directly and, when $p \geq 16$, it follows with a computation, because $p^{1/4} \geq 2$ and $p^6+p^5+3p^4+3p^3+3p^2+2p+3 \leq (p^3+2p^2)p^6/((p-1)(p^2-1))$). □

2.2. Small groups and computations

To avoid some long arguments for groups having small order, we have checked the veracity of Theorem 1.1 with the computer algebra system `magma` [4], for all groups R with $|R| \leq 2\,000$. Indeed, the library of "small groups" in `magma` has an exhaustive list of all finite groups of order at most $2\,000$.

3. Solvable groups

In this section, we prove the following result.

Theorem 3.1. *If R is solvable, then* $|\mathrm{Sub}(R)| < c(2) \cdot |R|^{\frac{\log_2(|R|)}{4}}$.

We argue by induction on $|R| = r$, where the base case of the induction can be considered Lemma 2.1. Let P_ℓ be a Sylow p_ℓ-subgroup of R. Since R is solvable, R admits a Hall p'_ℓ-subgroup K. Using P_ℓ and K we estimate the number of subgroups of R.

Let H be a subgroup of R. Then $H = H_{p'_\ell} H_{p_\ell}$, where $H_{p'_\ell}$ is a Hall p'_ℓ-subgroup of H and H_{p_ℓ} is a Sylow p_ℓ-subgroup of H. Now, from Hall's theorem, $H_{p'_\ell}$ is conjugate, via an element of P_ℓ, to a subgroup of K and, from Sylow's theorem, H_{p_ℓ} is conjugate, via an element of K, to a subgroup of P_ℓ. In particular, we have at most

$$1 + (|\mathrm{Sub}(K)| - 1)p_\ell^{a_\ell}$$

choices for $H_{p'_\ell}$, because every non-identity subgroup of K as at most $p_\ell^{a_\ell}$ conjugates. Similarly, we have at most

$$1 + (|\mathrm{Sub}(P_\ell)| - 1)\frac{r}{p_\ell^{a_\ell}}$$

choices for H_{p_ℓ}, because every non-identity subgroup of P_ℓ as at most $|K| = r/p_\ell^{a_\ell}$ conjugates. Therefore,

$$|\mathrm{Sub}(R)| \leq (1 + (|\mathrm{Sub}(K)| - 1)p_\ell^{a_\ell}) \cdot \left(1 + (|\mathrm{Sub}(P_\ell)| - 1)\frac{r}{p_\ell^{a_\ell}}\right). \tag{3.1}$$

Thus

$$\begin{aligned} |\mathrm{Sub}(R)| &\leq (1 - p_\ell^{a_\ell} + |\mathrm{Sub}(K)|p_\ell^{a_\ell}) \cdot \left(1 - \frac{r}{p_\ell^{a_\ell}} + |\mathrm{Sub}(P_\ell)|\frac{r}{p_\ell^{a_\ell}}\right) \\ &< |\mathrm{Sub}(K)|p_\ell^{a_\ell} \cdot |\mathrm{Sub}(P_\ell)|\frac{r}{p_\ell^{a_\ell}}. \end{aligned}$$

Using Lemma 2.1, this can be simplified in

$$|\mathrm{Sub}(R)| \leq |\mathrm{Sub}(K)|S(p_\ell, a_\ell)r.$$

As $|K| < r$, by induction we may bound the number of subgroups of K by $c(2)|K|^{\log_2(|K|)/4}$ and hence we obtain

$$|\mathrm{Sub}(R)| < c(2)(r/p_\ell^{a_\ell})^{\frac{\log_2(r/p_\ell^{a_\ell})}{4}} S(p_\ell, a_\ell)r = c(2)r^{\frac{\log_2(r)}{4}} \cdot \frac{S(p_\ell, a_\ell)r}{p_\ell^{\frac{a_\ell \log_2(r/p_\ell^{a_\ell})}{4}} r^{\frac{\log_2(p_\ell^{a_\ell})}{4}}} \quad (3.2)$$

$$= c(2)r^{\frac{\log_2(r)}{4}} \cdot \frac{S(p_\ell, a_\ell)r}{(r^2/p_\ell^{a_\ell})^{\frac{\log_2(p_\ell^{a_\ell})}{4}}}.$$

Proposition 3.2. *Let $r = p_1^{a_1} \cdots p_\ell^{a_\ell}$, with $p_1 < \cdots < p_\ell$, $a_1, \ldots, a_\ell \geq 1$ and $\ell \geq 2$, and let $i \in \{1, \ldots, \ell\}$. Then*

$$\frac{S(p_i, a_i)r}{(r^2/p_i^{a_i})^{a_i \frac{\log_2(p_i)}{4}}} \leq 1, \quad (3.3)$$

except when

(1) $a_i = 1$ and
- *$p_i \in \{2, 3\}$,*
- *$p_i = 5$ and $r/p_i \leq 4\,918$,*
- *$p_i = 7$ and $r/p_i \leq 23$,*
- *$p_i = 11$ and $r = 2 \cdot 11$, $r = 3 \cdot 11$,*
- *$p_i = 13$ and $r = 2 \cdot 13$,*

(2) $a_i = 2$ and
- *$p_i = 2$,*
- *$p_i = 3$ and $r/p_i^2 \leq 46$,*
- *$p_i = 5$ and $r = 50 = 2 \cdot 5^2$, or $r = 75 = 3 \cdot 5^2$,*

(3) $a_i = 3$ and
- *$p_i = 2$ and $r/p_i^3 \leq 723$,*
- *$p_i = 3$ and $r/p_i^3 \leq 7$,*

(4) $a_i = 4$ and
- *$p_i = 2$ and $r/p_i^4 \leq 67$,*
- *$p_i = 3$ and $r = 2 \cdot 3^4 = 162$,*

(5) $a_i = 5$ and
- *$p_i = 2$ and $r/p_i^5 \leq 29$,*
- *$p_i = 3$ and $r = 2 \cdot 3^5 = 486$.*

(6) $a_i \geq 6$, $p_i = 2$ and $r/p_i^{a_i} \leq 21$.

For not breaking the flow of the argument we postpone the proof of Proposition 3.2 to Appendix A.1.

To conclude the proof of Theorem 3.1 we consider various cases, depending on whether $a_\ell = 1$ or $a_\ell \geq 2$.

Lemma 3.3. *If $a_\ell = 1$, then Theorem 3.1 holds true.*

Proof. From Proposition 3.2, Theorem 3.1 follows from (3.2), except when part (1) holds. When $r = |R| \leq 2\,000$, the veracity of this lemma follows from Section 2.2. Therefore, for the rest of the proof, we may suppose that $r > 2\,000$. In particular, either $p_\ell = 3$ and $r = 2^{a_1} \cdot 3$, or $p_\ell = 5$ and $r = r' \cdot 5$ with $400 < r' \leq 4\,918$.

We first need to refine (3.2) (for the cases under consideration). When $a_\ell = 1$, we have $S(p_\ell, a_\ell) = 2$ and hence (3.1) becomes

$$|\mathrm{Sub}(R)| \leq (|\mathrm{Sub}(K)|p_\ell + 1 - p_\ell)\left(\frac{r}{p_\ell} + 1\right).$$

As $|K| < r$, arguing by induction, we deduce

$$\begin{aligned}
|\mathrm{Sub}(R)| &\leq (c(2)(r/p_\ell)^{\frac{\log_2(r/p_\ell)}{4}} p_\ell + 1 - p_\ell)\left(\frac{r}{p_\ell} + 1\right) \\
&< c(2)(r/p_\ell)^{\frac{\log_2(r/p_\ell)}{4}} p_\ell(r/p_\ell + 1) \leq c(2) r^{\frac{\log_2(r)}{4}} \cdot \frac{r + p_\ell}{p_\ell^{\frac{\log_2(r/p_\ell)}{4}} r^{\frac{\log_2(p_\ell)}{4}}} \\
&\leq c(2) r^{\frac{\log_2(r)}{4}} \cdot \frac{r + p_\ell}{2^{\frac{\log_2(p_\ell)\log_2(r/p_\ell)}{4}} r^{\frac{\log_2(p_\ell)}{4}}} = c(2) r^{\frac{\log_2(r)}{4}} \cdot \frac{r + p_\ell}{(r^2/p_\ell)^{\frac{\log_2(p_\ell)}{4}}}.
\end{aligned}$$

(These computations have allowed to replace the numerator $S(p_\ell, a_\ell)r = 2r$ appearing in (3.2) with $r + p_\ell$.) In particular, the lemma follows as long as

$$\frac{r + p_\ell}{(r^2/p_\ell)^{\frac{\log_2(p_\ell)}{4}}} \leq 1. \tag{3.4}$$

Assume $p_\ell = 5$. Since we are assuming $r \geq 2\,000$, we have $r/p_\ell \geq 256 = 2^8$ and hence we obtain

$$\begin{aligned}
\frac{r + p_\ell}{(r^2/p_\ell)^{\frac{\log_2(p_\ell)}{4}}} &= \left(1 + \frac{5}{r}\right) r^{1 - \frac{\log_2(5)}{2}} 5^{\frac{\log_2(5)}{4}} = \left(1 + \frac{5}{r}\right) 5^{1 - \frac{\log_2(5)}{2}} \left(\frac{r}{5}\right)^{1 - \frac{\log_2(5)}{2}} 5^{\frac{\log_2(5)}{4}} \\
&\leq \left(1 + \frac{5}{r}\right) 5^{1 - \frac{\log_2(5)}{4}} 256^{1 - \frac{\log_2(5)}{2}} = \left(1 + \frac{5}{r}\right) 2^{\log_2(5) - \frac{(\log_2(5))^2}{4}} 2^{8 - 4\log_2(5)} \\
&= \left(1 + \frac{5}{r}\right) 2^{8 - 3\log_2(5) - \frac{(\log_2(5))^2}{4}} \leq \left(1 + \frac{5}{r}\right) \cdot 0.81 \leq \left(1 + \frac{1}{256}\right) \cdot 0.81 \\
&< 1.
\end{aligned}$$

Therefore, for the rest of the proof we suppose $p_\ell = 3$. In particular, $\ell = 2$, $p_1 = 2$ and $r = 2^{a_1} \cdot 3$.

Let P be a Sylow 2-subgroup of R and let T be a Sylow 3-subgroup of R. Thus $|P| = 2^{a_1}$ and $|T| = 3$. Let H be an arbitrary subgroup of R. Then $H = \langle Q, S\rangle$, where Q is a Sylow 2-subgroup of H and S is a Sylow 3-subgroup of H. If $S = 1$, then we have at most

$$c(2) \cdot 3 \cdot (2^{a_1})^{\frac{\log_2(2^{a_1})}{4}} = c(2) \cdot 3 \cdot 2^{\frac{a_1^2}{4}} \tag{3.5}$$

choices for $H = Q$, because we have at most 3 Sylow 2-subgroups in R. Assume that $S \neq 1$. Let $\varepsilon \in \{1, 3\}$ be the number of Sylow 2-subgroups of R and let $P_1, \dots, P_\varepsilon$ be the Sylow 2-subgroups of R with $P = P_1$. Now, $Q \leq P_i$ for some $i \in \{1, \dots, \varepsilon\}$. As S acts transitively by conjugation on the set $\{P_1, \dots, P_\varepsilon\}$ of Sylow 2-subgroups of R, replacing Q by a suitable S-conjugate, we may suppose that $Q \leq P_1 = P$.

Let $a \in \{0, \dots, a_1\}$. Corollary 4.2 in [8] shows that the number of subgroups of P having index p^a is at most

$$\begin{bmatrix} a_1 \\ a \end{bmatrix}_2 = \frac{(2^{a_1} - 1) \cdots (2^{a_1 - a + 1} - 1)}{(2^1 - 1) \cdots (2^a - 1)}.$$

(Here, we are denoting with $\begin{bmatrix} a_1 \\ a \end{bmatrix}_2$ the 2-binomial coefficient.) Wince $H = \langle Q, S\rangle = \langle Q, S^x\rangle$, $\forall x \in Q$, we may replace S with any Q-conjugate. We deduce that the number of subgroups of R having order divisible by 3 is at most

$$\sum_{a=0}^{a_1} \begin{bmatrix} a_1 \\ a \end{bmatrix}_2 \cdot 2^a. \tag{3.6}$$

For $a \in \{1, \dots, a_1\}$, we have

$$\begin{bmatrix} a_1 \\ a \end{bmatrix}_2 \cdot 2^a = (2^{a_1} - 1) \begin{bmatrix} a_1 - 1 \\ a - 1 \end{bmatrix}_2 + \begin{bmatrix} a_1 \\ a \end{bmatrix}_2.$$

Therefore, (3.6) becomes

$$1 + (2^{a_1} - 1) \sum_{a=1}^{a_1} \begin{bmatrix} a_1 - 1 \\ a - 1 \end{bmatrix}_2 + \sum_{a=1}^{a_1} \begin{bmatrix} a_1 \\ a \end{bmatrix}_2 = (2^{a_1} - 1) \sum_{a=0}^{a_1 - 1} \begin{bmatrix} a_1 - 1 \\ a \end{bmatrix}_2 + \sum_{a=0}^{a_1} \begin{bmatrix} a_1 \\ a \end{bmatrix}_2. \tag{3.7}$$

Since

$$\sum_{a=0}^{a_1 - 1} \begin{bmatrix} a_1 - 1 \\ a \end{bmatrix}_2 \text{ and } \sum_{a=0}^{a_1} \begin{bmatrix} a_1 \\ a \end{bmatrix}_2$$

count the number of subspaces of a vector space of dimension $a_1 - 1$ and a_1 over the field with 2 elements, from Lemma 2.1, we deduce that (3.6) is at most

$$c(2) \cdot (2^{a_1} - 1)2^{\frac{(a_1-1)^2}{4}} + c(2) \cdot 2^{\frac{a_1^2}{4}}.$$

Summing up, from (3.5) and (3.7), the number of subgroups of R is at most

$$c(2)\cdot 3\cdot 2^{\frac{a_1^2}{4}} + c(2)\cdot(2^{a_1}-1)2^{\frac{(a_1-1)^2}{4}} + c(2)\cdot 2^{\frac{a_1^2}{4}} = c(2)\cdot 2^{\frac{a_1^2}{4}} \cdot \left(4 + 2^{\frac{a_1}{2}+\frac{1}{4}} - 2^{-\frac{a_1}{2}+\frac{1}{4}}\right). \quad (3.8)$$

Assume first $a_1 \geq 12$. Then, from (3.8), we obtain

$$|\mathrm{Sub}(R)| < c(2) \cdot 2^{\frac{a_1^2}{4}} \cdot \left(4 + 2^{\frac{a_1}{2}+\frac{1}{4}}\right) < c(2) \cdot 2^{\frac{a_1^2}{4}} \cdot 2^{\frac{a_1}{2}+\frac{1}{3}} = c(2) \cdot 2^{\frac{a_1^2}{4}+\frac{a_1}{2}+\frac{1}{3}}, \quad (3.9)$$

where the last inequality follows with a computation using $a_1 \geq 12$. On the other hand, we have

$$\begin{aligned} c(2)r^{\frac{\log_2(r)}{4}} = c(2) \cdot (3 \cdot 2^{a_1})^{\frac{\log_2(3\cdot 2^{a_1})}{4}} &\geq c(2) \cdot (2^{a_1+1})^{\frac{\log_2(3\cdot 2^{a_1})}{4}} \\ &= c(2) \cdot 2^{\frac{a_1^2}{4}+a_1\left(\frac{1}{4}+\frac{\log_2(3)}{4}\right)+\frac{\log_2(3)}{4}}. \end{aligned} \quad (3.10)$$

Now, observe

$$\frac{1}{4} + \frac{\log_2(3)}{4} \geq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$

and $\log_2(3)/4 \geq 1/3$. Therefore, when $a_1 \geq 12$, the result follows from (3.9) and (3.10).

When $3 \leq a_1 \leq 11$, we have verified with a calculator that (3.8) is less than or equal to $c(2) \cdot (3 \cdot 2^{a_1})^{\log_2(3\cdot 2^{a_1})/4}$ and hence the result follows also in this case. Finally, when $a_1 \leq 2$, we have $r \leq 12 \leq 2,000$. □

Proof of Theorem 3.1. From Lemma 3.3, we may suppose that $a_\ell \geq 2$. From Proposition 3.2, Theorem 3.1 follows from (3.2), except when one of parts (2)–(6) holds. Observe that we are applying Proposition 3.2 with $i = \ell$ and hence $p_i \neq 2$. Thus $|R| \leq 486$. We have verified the veracity of this lemma with a computation using the database of small groups in the computer algebra system `magma` [4], see Section 2.2. □

4. Notation and arithmetic reductions

4.1. Notation

In the light of Theorem 3.1, for the rest of our argument we may suppose that R is not solvable. In particular, from the Odd Order Theorem, we have

$$p_1 = 2. \tag{4.1}$$

Clearly,

$$a_1 \geq 2 \tag{4.2}$$

because a non-abelian simple group cannot have a cyclic Sylow 2-subgroup. Moreover,

$$\ell \geq 3 \tag{4.3}$$

from the celebrated $p^\alpha q^\beta$ theorem of Burnside.

Recall from Section 2 that, for each prime p_i, P_i is a Sylow p_i-subgroup of R. From [6], we have that, if $p_i \geq 5$, then $|\mathbf{N}_R(P_i) : P_i| \neq 1$. In particular, for each prime $p_i \geq 5$, we have $|\mathbf{N}_R(P_i) : P_i| \geq 2$. From [6], we see that the same conclusion holds when $p_i = 3$, except (possibly) when $\mathrm{PSL}_2(3^{3^a})$ is a composition factor of R for some $a \geq 1$. Hence we may replace (2.4) with the inequality

$$(\ell - 1)\left(1 - \frac{\log(2)}{\log(r)}\right) + \varepsilon\frac{\log(2)}{\log(r)} < \frac{\log(c(2))}{\log(r)} + \sum_{i=1}^{\ell}\left(\frac{a_i \log(p_i)}{4\log(2)} - \frac{\log(S(p_i, a_i))}{\log(r)}\right), \tag{4.4}$$

where $\varepsilon = 0$ when R has no composition factor isomorphic to $\mathrm{PSL}_2(3^{3^a})$ and $\varepsilon = 1$ otherwise.

From (4.4), we are interested in the function

$$f(r) := \frac{\log(c(2))}{\log(r)} + \sum_{i=1}^{\ell}\left(\frac{a_i \log(p_i)}{4\log(2)} - \frac{\log(S(p_i, a_i))}{\log(r)}\right) - (\ell - 1) + (\ell - 2)\frac{\log(2)}{\log(r)}. \tag{4.5}$$

Because of the peculiar behavior of $S(p_i, a_i)$, when $a_i \leq 5$, we consider the auxiliary function

$$\mathcal{S}(p_i, a_i) = c(p_i)p_i^{\frac{a_i^2}{4}}$$

and

$$\mathtt{f}(r) := \frac{\log(c(2))}{\log(r)} + \sum_{i=1}^{\ell}\left(\frac{a_i \log(p_i)}{4\log(2)} - \frac{\log(\mathcal{S}(p_i, a_i))}{\log(r)}\right) - (\ell - 1) + (\ell - 2)\frac{\log(2)}{\log(r)}. \tag{4.6}$$

4.2. Arithmetic reductions

We say that r is good if $f(r) > 0$ and we say that r is `good` if $\mathtt{f}(r) > 0$. From Lemma 2.2, $S(p, a) \leq \mathcal{S}(p, a)$ and hence $f(r) \geq \mathtt{f}(r)$. In particular, if r is `good`, then r is good. Observe that, when $r = |R|$ is good, Theorem 1.1 follows immediately from the discussion in Section 4.1.

We use elementary calculus to deduce some important facts about $f(r)$.

Lemma 4.1. *Assume (4.1), (4.2) and (4.3). Let $i \in \{1, \dots, \ell\}$ and let r' be the positive integer obtained from r, by replacing the prime p_i with a prime number $p > p_i$ and with $p \notin \{p_1, \dots, p_\ell\}$. If r is good, then so is r'.*

Lemma 4.2. *Assume (4.1), (4.2) and (4.3). Let p be a prime number with $p \notin \{p_1, \dots, p_\ell\}$ and $p \geq 17$ and let $r' = r \cdot p$. If r is good, then so is r'.*

Lemma 4.3. *Assume (4.1), (4.2) and (4.3). Let $i \in \{1, \dots, \ell\}$ and let $r' = r \cdot p_i$. If r is* `good`*, then so is r'.*

We prove Lemma 4.1 in Appendix A.2, we prove Lemma 4.2 in Appendix A.3 and we prove Lemma 4.3 in Appendix A.4.

Using Lemmas 4.1, 4.2 and 4.3, we are able to reduce the proof of Theorem 1.1 to a very limited number of cases.

Proposition 4.4. *If r satisfies any of the following conditions, then r is good. In particular, if $|R|$ satisfies any of the following conditions, then $|\mathrm{Sub}(R)| < c(2) \cdot |R|^{\log_2(|R|)/4}$.*

(1) $\ell \geq 13$;
(2) $\ell = 4$; *moreover,* $p_\ell \geq 79$, *or* $a_i \geq 5$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 28$;
(3) $\ell = 5$; *moreover,* $p_\ell \geq 173$, *or* $a_i \geq 5$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 15$;
(4) $\ell = 6$; *moreover,* $p_\ell \geq 251$, *or* $a_i \geq 5$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 12$;
(5) $\ell = 7$; *moreover,* $p_\ell \geq 307$, *or* $a_i \geq 5$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 10$;
(6) $\ell = 8$; *moreover,* $p_\ell \geq 277$, *or* $a_i \geq 5$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 9$;
(7) $\ell = 9$; *moreover,* $p_\ell \geq 233$, *or* $a_i \geq 4$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 7$;
(8) $\ell = 10$; *moreover,* $p_\ell \geq 163$, *or* $a_i \geq 3$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 6$;
(9) $\ell = 11$; *moreover,* $p_\ell \geq 89$, *or* $a_i \geq 3$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 4$;
(10) $\ell = 12$; *moreover,* $p_\ell \geq 47$, *or* $a_i \geq 2$ *for some* $i \in \{2, \dots, \ell\}$, *or* $a_1 \geq 3$.

Proof. We have implemented the functions $f(r)$ and $\mathtt{f}(r)$ in (4.5) and in (4.6) in a computer.

We have verified that

$$s = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41$$

is `good`. Observe that s is divisible by the first 13 prime numbers. From Lemmas 4.1, 4.2 and 4.3, we deduce that any positive integer r with $\ell > 12$ is good. This proves (1).

Next, we prove (10). We have verified that

$$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 67,$$
$$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37,$$

$$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37$$

are good. From Lemmas 4.1 and 4.3, we deduce that any positive integer r with $\ell = 12$ and $p_\ell \geq 67$, or with $a_i \geq 2$ for some $i \geq 2$, or with $a_1 \geq 3$ is good. In particular, in all of these cases r is also good. Now, to obtain the refined condition stated in (10), we have computed explicitly the function f in all numbers r of the form $r = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot p_{12}$ with $p_{12} \leq 67$.

All other parts are proved similarly. □

5. The case $\ell = 3$

In this section we prove Theorem 1.1 when $\ell = 3$; this is a case where Proposition 4.4 gives no information.

Lemma 5.1. *Let R be a non-abelian simple group whose order is divisible by at most three distinct primes. Then one of the following holds*

- $R \cong \mathrm{Alt}(5) \cong \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5)$ *and* $|R| = 2^2 \cdot 3 \cdot 5 = 60$,
- $R \cong \mathrm{PSL}_3(2) \cong \mathrm{PSL}_2(7)$ *and* $|R| = 2^3 \cdot 3 \cdot 7 = 168$,
- $R \cong \mathrm{Alt}(6) \cong \mathrm{PSL}_2(9)$ *and* $|R| = 2^3 \cdot 3^2 \cdot 5 = 360$,
- $R \cong \mathrm{PSL}_2(8)$ *and* $|R| = 2^3 \cdot 3^2 \cdot 7 = 504$,
- $R \cong \mathrm{PSL}_2(17)$ *and* $|R| = 2^4 \cdot 3^2 \cdot 17 = 2\,448$,
- $R \cong \mathrm{PSL}_3(3)$ *and* $|R| = 2^4 \cdot 3^3 \cdot 13 = 5\,616$,
- $R \cong \mathrm{PSU}_3(3)$ *and* $|R| = 2^5 \cdot 3^3 \cdot 7 = 6\,048$,
- $R \cong \mathrm{PSU}_4(2) \cong \mathrm{PSp}_4(3)$ *and* $|R| = 2^6 \cdot 3^4 \cdot 5 = 25\,920$.

Proof. This result follows from the contribution of various authors (Brauer, Herzog, Klinger, Leon, Mason, Thompson, and Wales) and we refer to [3] and to the references therein for more details. □

We also need a few rather technical observations.

Lemma 5.2. *Let $r \in \mathbb{N}$ with $r \geq 2\,000$, then*

(1) $4r(r/7)^{\frac{\log_2(r/7)}{4}} + 8r(r/14)^{\frac{\log_2(r/14)}{4}} \leq r^{\frac{\log_2(r)}{4}}$,
(2) $8r(r/28)^{\frac{\log_2(r/28)}{4}} + 6r(r/21)^{\frac{\log_2(r/21)}{4}} + 4r(r/14)^{\frac{\log_2(r/14)}{4}} \leq r^{\frac{\log_2(r)}{4}}$,
(3) $(2r+10)(r/10)^{\frac{\log_2(r/10)}{4}} + (r/5+5)(r/5)^{\frac{\log_2(r/5)}{4}} \leq r^{\frac{\log_2(r)}{4}}$,
(4) $2p(r/p)^{\frac{\log_2(r/p)}{4}} \leq r^{\log_2(r)/4}$, *for every prime $p \geq 3$ with $r \geq 2p$.*

We postpone the proof of Lemma 5.2 to Appendix A.5.

Proof of Theorem 1.1 when $\ell = 3$. From Section 2.2, we have $r = |R| > 2\,000$. Moreover, from Theorem 3.1, R is not solvable and hence R has at least one non-abelian simple section.

From Lemma 5.1, we see that R cannot have a composition factor isomorphic to $\mathrm{PSL}_2(3^{3^a})$, for some $a \geq 1$. Therefore, (4.4) becomes

$$2\left(1 - \frac{\log 2}{\log r}\right) \leq \frac{\log c(2)}{\log r} + \sum_{i=1}^{3}\left(\frac{a_i \log p_i}{4 \log 2} - \frac{\log S(p_i, a_i)}{\log r}\right). \tag{5.1}$$

Moreover, from Lemma 5.1, we have $p_2 = 3$ and $p_3 \in \{5, 7, 13, 17\}$.

Let $f(r)$ be the function defined in (4.5). Suppose $p_3 = 13$ and observe that, from Lemma 5.1, each non-abelian simple section of R is isomorphic to $\mathrm{PSL}_2(13)$. In particular, $|\mathrm{PSL}_3(3)| = 2^4 \cdot 3^3 \cdot 13$ divides r. We have

$$f(2^4 \cdot 3^3 \cdot 13) > 0.46 \geq 0.$$

In particular, from Lemma 4.1 and Lemma 4.3, we deduce r is good.

Suppose $p_3 = 17$. Observe that, from Lemma 5.1, each non-abelian simple section of R is isomorphic to $\mathrm{PSL}_2(17)$. In particular, $|\mathrm{PSL}_2(17)| = 2^4 \cdot 3^2 \cdot 17$ divides r. We have

$$f(2^4 \cdot 3^2 \cdot 17) > 0.3 \geq 0.$$

In particular, from Lemma 4.1 and Lemma 4.3, we deduce r is good.

Case $p_3 = 7$. From Lemma 5.1, each non-abelian simple section of R is isomorphic to $\mathrm{PSL}_2(7)$, or $\mathrm{PSL}_2(8)$ or $\mathrm{PSU}_3(3)$. In particular, we have

$$\begin{aligned} f(2^2 \cdot 3 \cdot 7^3) &> 0.4 \geq 0, \\ f(2^2 \cdot 3^4 \cdot 7) &> 0.1 \geq 0, \\ f(2^3 \cdot 3 \cdot 7^2) &> 0.1 \geq 0, \\ f(2^3 \cdot 3^3 \cdot 7) &> 0.07 \geq 0, \\ f(2^3 \cdot 3^2 \cdot 7^2) &> 0.4 \geq 0, \\ f(2^6 \cdot 3^2 \cdot 7) &> 0.02 \geq 0. \end{aligned}$$

From Lemma 4.1 and Lemma 4.3 and 5.1, we deduce that r is good, as long as r is divisible by an element of

$$\{2^2 \cdot 3 \cdot 7^3, 2^2 \cdot 3^4 \cdot 7, 2^3 \cdot 3 \cdot 7^2, 2^3 \cdot 3^3 \cdot 7, 2^3 \cdot 3^2 \cdot 7^2, 2^6 \cdot 3^2 \cdot 7\}.$$

Therefore, Lemma 5.1 shows that (5.1) is satisfied, except when $r = 2^{a_1} \cdot 3 \cdot 7$ or

$$r \in \{252 = 2^2 \cdot 3^2 \cdot 7, 756 = 2^2 \cdot 3^3 \cdot 7, 504 = 2^3 \cdot 3^2 \cdot 7, 1\,008 = 2^4 \cdot 3^2 \cdot 7, 2\,016 = 2^5 \cdot 3^2 \cdot 7\}.$$

As $r = |R| > 2\,000$, we may exclude the cases $r \in \{252, 756, 504, 1\,008\}$. Assume $|R| = 2\,016 = 2^5 \cdot 3^2 \cdot 7$. From Lemma 5.1, we see that R has a unique non-abelian chief factor, which is isomorphic to either $\mathrm{PSL}_2(7)$ or to $\mathrm{PSL}_2(8)$. Suppose $\mathrm{PSL}_2(8)$ is a chief factor X/Y of R, that is, $X, Y \trianglelefteq R$, $X \geq Y$ and $X/Y \cong \mathrm{PSL}_2(8)$. Let

$$C := \mathbf{C}_R(X/Y).$$

By definition, C is the kernel of the action $R \to \mathrm{Aut}(X/Y)$ of R by conjugation on X/Y. In particular, as $\mathrm{Aut}(\mathrm{PSL}_2(8)) \cong \mathrm{PSL}_2(8) : 3$ and as $3|\mathrm{PSL}_2(8)|$ does not divide $|R|$, we deduce $R/C \cong \mathrm{PSL}_2(8)$ and $|C| = 2\,016/|\mathrm{PSL}_2(8)| = 4$. Since $\mathrm{PSL}_2(8)$ has trivial Schur multiplier (see [5, page 6]), we deduce that R splits over C and hence

$$R \cong \mathrm{PSL}_2(8) \times C_4 \text{ or } R \cong \mathrm{PSL}_2(8) \times C_2 \times C_2.$$

Now, we have checked the veracity of the statement for these two groups with a computer. We postpone the case that R has a composition factor isomorphic to $\mathrm{PSL}_2(7)$ for later.

Assume $r = 2^{a_1} \cdot 3 \cdot 7$, or $r = 2\,016$ and $\mathrm{PSL}_2(7)$ is a composition factor of R. Thus $a_2 = 1$ in the first case and $a_2 = 2$ in the second case. In particular, by Lemma 5.1, R has a unique non-abelian chief factor X/Y and $X/Y \cong \mathrm{PSL}_2(7)$. Let $C := \mathbf{C}_R(X/Y)$. By definition, C is the kernel of the action $R \to \mathrm{Aut}(X/Y)$ of R by conjugation on X/Y. In particular, as $\mathrm{Aut}(\mathrm{PSL}_2(7)) \cong \mathrm{PGL}_2(7)$, we deduce $R/C \cong \mathrm{PSL}_2(7)$ or $R/C \cong \mathrm{PGL}_2(7)$. Assume first $R/C \cong \mathrm{PSL}_2(7)$. Now, $\mathrm{PSL}_2(7)$ has four conjugacy classes of maximal $7'$-subgroups: two of these subgroups have order 24 and two of these subgroups have order 12. Therefore, R has four conjugacy classes (with representatives K_1, K_2, K_3 and K_4, say) of $7'$-subgroups and $|K_1| = |K_2| = 2^{a_1} \cdot 3^{a_2}$, $|K_3| = |K_4| = 2^{a_1-1} \cdot 3^{a_2}$. Therefore, repeating the same argument we have used for solvable groups (but taking in account that R has four conjugacy classes of maximal $7'$-subgroups), we deduce

$$\begin{aligned}
|\mathrm{Sub}(R)| &\leq |\mathrm{Sub}(K_1)|\frac{|R|}{|K_1|}S(7,1)\frac{|R|}{7} + |\mathrm{Sub}(K_2)|\frac{|R|}{|K_2|}S(7,1)\frac{|R|}{7} \\
&\quad + |\mathrm{Sub}(K_3)|\frac{|R|}{|K_3|}S(7,1)\frac{|R|}{7} + |\mathrm{Sub}(K_4)|\frac{|R|}{|K_4|}S(7,1)\frac{|R|}{7} \\
&= 2r(|\mathrm{Sub}(K_1)| + |\mathrm{Sub}(K_2)|) + 4r(|\mathrm{Sub}(K_3)| + |\mathrm{Sub}(K_4)|) \\
&< 4rc(2)(r/7)^{\frac{\log_2(r/7)}{4}} + 8rc(2)(r/14)^{\frac{\log_2(r/14)}{4}},
\end{aligned}$$

where the last inequality follows from Theorem 3.1 and from the fact that K_1, K_2, K_3 and K_4 are solvable. Hence, in this case, Theorem 1.1 follows from Lemma 5.2 (1). Assume next $R/C \cong \mathrm{PGL}_2(7)$. Observe that $a_1 \geq 4$, because a Sylow 2-subgroup of $\mathrm{PGL}_2(7)$ has order 16. Now, $\mathrm{PGL}_2(7)$ has three conjugacy classes of maximal $7'$-subgroups and these groups have order $12, 16$ and 24. Therefore, R has three conjugacy classes (with representatives K_1, K_2 and K_3, say) of $7'$-subgroups and $|K_1| = 2^{a_1-2} \cdot 3^{a_2}$, $|K_2| = 2^{a_1} \cdot 3^{a_2-1}$ and $|K_3| = 2^{a_1-1} \cdot 3^{a_2}$. Therefore, arguing as above, we deduce

$$\begin{aligned}|\mathrm{Sub}(R)| &\leq |\mathrm{Sub}(K_1)|\frac{|R|}{|K_1|}S(7,1)\frac{|R|}{7} + |\mathrm{Sub}(K_2)|\frac{|R|}{|K_2|}S(7,1)\frac{|R|}{7}\\ &\quad + |\mathrm{Sub}(K_3)|\frac{|R|}{|K_3|}S(7,1)\frac{|R|}{7}\\ &= |\mathrm{Sub}(K_1)|S(7,1)4r + |\mathrm{Sub}(K_2)|S(7,1)3r + |\mathrm{Sub}(K_3)|S(7,1)2r\\ &= 8rc(2)(r/28)^{\frac{\log_2(r/28)}{4}} + 6rc(2)(r/21)^{\frac{\log_2(r/21)}{4}} + 4rc(2)(r/14)^{\frac{\log_2(r/14)}{4}}.\end{aligned}$$

Hence, in this case, Theorem 1.1 follows from Lemma 5.2 (2).

Case $p_3 = 5$. From Lemma 5.1, each non-abelian simple section of R is isomorphic to $\mathrm{Alt}(5)$, or $\mathrm{Alt}(6)$ or $\mathrm{PSU}_4(2)$. We have

$$\begin{aligned}f(2^2\cdot 3\cdot 5^3) &> 0.12 \geq 0,\\ f(2^2\cdot 3^2\cdot 5^2) &> 0.04 \geq 0,\\ f(2^2\cdot 3^5\cdot 5) &> 0.17 \geq 0,\\ f(2^3\cdot 3^4\cdot 5) &> 0.15 \geq 0,\\ f(2^4\cdot 3^3\cdot 5) &> 0.04 \geq 0,\\ f(2^5\cdot 3\cdot 5^2) &> 0.03 \geq 0,\\ f(2^9\cdot 3^2\cdot 5) &> 0.04 \geq 0.\end{aligned}$$

From Lemma 4.1 and Lemma 4.3 and 5.1, we deduce that $f(r) \geq 0$ and hence r is good, as long as r is divisible by an element of

$$\{2^2\cdot 3\cdot 5^3, 2^2\cdot 3^2\cdot 5^2, 2^2\cdot 3^5\cdot 5, 2^3\cdot 3^4\cdot 5, 2^4\cdot 3^3\cdot 5, 2^5\cdot 3\cdot 5^2, 2^9\cdot 3^2\cdot 5\}.$$

Therefore, Lemma 5.1 shows that (5.1) is satisfied, except when $r = 2^{a_1}\cdot 3\cdot 5$ or

$$\begin{aligned}r \in \{&300 = 2^2\cdot 3\cdot 5^2, 600 = 2^3\cdot 3\cdot 5^2, 1\,200 = 2^4\cdot 3\cdot 5^2,\\ &1\,620 = 2^2\cdot 3^4\cdot 5, 540 = 2^2\cdot 3^3\cdot 5, 1\,080 = 2^3\cdot 3^3\cdot 5,\\ &180 = 2^2\cdot 3^2\cdot 5, 360 = 2^3\cdot 3^2\cdot 5, 720 = 2^4\cdot 3^2\cdot 5, 1\,440 = 2^5\cdot 3^2\cdot 5,\\ &2\,880 = 2^6\cdot 3^2\cdot 5, 5\,760 = 2^7\cdot 3^2\cdot 5, 11\,520 = 2^8\cdot 3^2\cdot 5\}.\end{aligned}$$

As $r = |R| > 2,000$, we may exclude the cases $r \in \{180, 300, 360, 540, 600, 720, 1\,080, 1\,200, 1\,440, 1\,620\}$. Assume $r \in \{2\,880, 5\,760, 11\,520\}$. Thus $r = 2^{a_1}\cdot 3^2\cdot 5$, with $a_1 \in \{6, 7, 8\}$. From Lemma 5.1, we see that R has a unique non-abelian composition factors, which is isomorphic to either $\mathrm{Alt}(5)$ or to $\mathrm{Alt}(6)$. Suppose $\mathrm{Alt}(6)$ is a composition factor X/Y of R. Let $C := \mathbf{C}_R(X/Y)$. By definition, C is the kernel of the action $R \to \mathrm{Aut}(X/Y)$ of R by conjugation on X/Y. In particular, as $\mathrm{Aut}(\mathrm{Alt}(6)) \cong \mathrm{P\Gamma L}_2(9)$, we deduce

- $R/C \cong \mathrm{Alt}(6)$ and $|C| = 2^{a_1-3}$, or
- $R/C \cong \mathrm{PGL}_2(9)$ and $|C| = 2^{a_1-4}$, or
- $R/C \cong M_{10}$ and $|C| = 2^{a_1-4}$, or
- $R/C \cong \mathrm{P\Sigma L}_2(9)$ and $|C| = 2^{a_1-4}$, or
- $R/C \cong \mathrm{P\Gamma L}_2(9)$ and $|C| = 2^{a_1-5}$.

Since $\mathrm{Alt}(6)$ has Schur multiplier of order 6 (see [5, page 6]) and since C is a 2-group, we deduce that either R splits over C and hence $R \cong R/C \times C$, or $R \cong R/C \circ C$. Using this information we recover the various isomorphism classes of R and check the veracity of Theorem 1.1 in each case. For instance, when $R/C \cong \mathrm{Alt}(6)$, $R \cong R/C \times C$ and $a_1 = 6$, we have that R is isomorphic to one of the following five groups

$$\mathrm{Alt}(6) \times C_2^3,\ \mathrm{Alt}(6) \times C_2 \times C_4,\ \mathrm{Alt}(6) \times C_8,\ \mathrm{Alt}(6) \times D_4,\ \mathrm{Alt}(6) \times Q_8.$$

Assume $r = 2^{a_1} \cdot 3 \cdot 5$, or $r \in \{2\,880, 5\,760, 11\,520\}$ and $\mathrm{Alt}(5)$ is a composition factor of R. Thus $a_2 = 1$ in the first case and $a_2 = 2$ in the second case. In particular, by Lemma 5.1, R has a unique non-abelian chief factor X/Y and $X/Y \cong \mathrm{Alt}(5)$. Let $C := \mathbf{C}_R(X/Y)$. By definition, C is the kernel of the action $R \to \mathrm{Aut}(X/Y)$ of R by conjugation on X/Y. In particular, as $\mathrm{Aut}(\mathrm{Alt}(5)) \cong \mathrm{Sym}(5)$, we deduce $R/C \cong \mathrm{Alt}(5)$ or $R/C \cong \mathrm{Sym}(5)$. Here we need to argue slightly differently from the case in the previous paragraph, because otherwise we end up with too many cases to be checked with a computer. Now $\mathrm{Alt}(5)$ and $\mathrm{Sym}(5)$ both have two conjugacy classes of maximal $5'$-subgroups and these subgroups have order 6 and 12 in $\mathrm{Alt}(5)$ and have order 12 and 24 in $\mathrm{Sym}(5)$. Therefore, R has two conjugacy classes (with representatives K_1 and K_2, say) of $5'$-subgroups and $|K_1| = 2^{a_1-1} \cdot 3^{a_2}$ and $|K_2| = 2^{a_1} \cdot 3^{a_2}$. Let us call a the number of subgroups of R having order relatively prime to 5 and let us call b the number of subgroups of R having order divisible by 5. Since K_1 has 10 conjugates in R and since K_2 has 5 conjugates in R, we deduce

$$a \leq 10|\mathrm{Sub}(K_1)| + 5|\mathrm{Sub}(K_2)| \leq 10c(2)(r/10)^{\frac{\log_2(r/10)}{4}} + 5c(2)(r/5)^{\frac{\log_2(r/5)}{4}}. \quad (5.2)$$

Now, let H be an arbitrary subgroup of R having order divisible by 5. Then $H = \langle A, B\rangle$, where A is a $5'$-subgroup of H and B is a Sylow 5-subgroup of H. Now, A is contained in one of the 15 maximal $5'$-subgroups of R. However, since B acts transitively on the five conjugates of K_2, we may assume (replacing A with a suitable B-conjugate if necessary) that either A is contained in one of the 10 conjugates of K_1 or $A \leq K_2$. Taking this in account, we have

$$b \leq 10|\mathrm{Sub}(K_1)|\frac{r}{5} + |\mathrm{Sub}(K_2)|\frac{r}{5} \leq c(2) \cdot 2r \cdot (r/10)^{\frac{\log_2(r/10)}{4}} + c(2) \cdot \frac{r}{5} \cdot (r/5)^{\frac{\log_2(r/5)}{4}}. \quad (5.3)$$

Clearly, $|\mathrm{Sub}(R)| = a + b$. Using (5.2) and (5.3), we obtain $a + b \leq c(2)r^{\log_2 r/4}$, except when $a_1 = 2$. Therefore, in this case, Theorem 1.1 immediately follows from Lemma 5.2 (3). □

6. The final cases

Before dealing with the remaining cases, we need three general results.

Lemma 6.1. *Let R be a counterexample of minimal order to Theorem 1.1. Then R has no normal non-identity Sylow p-subgroup.*

Proof. We argue by contradiction and we let R be a counterexample of minimal order to Theorem 1.1 admitting a normal non-identity Sylow p-subgroup P. From the Schur-Zassenhaus theorem, let K be a complement of P in R. Thus $p \geq 3$.

If $p = 2$, then from the Odd Order Theorem P and R/P are solvable, and hence so is R. However, this contradicts Theorem 3.1.

From Section 2.2, we may suppose that $|R| > 2\,000$ and, from Section 5, we may suppose that $\ell \geq 4$.

Let H be a subgroup of R. Then, from the Schur-Zassenhaus theorem, $H = H_{p'}H_p$, where $H_{p'}$ is a Hall p'-subgroup of H and H_p is a Sylow p-subgroup of H. Now, from the Schur-Zassenhaus theorem, $H_{p'}$ is conjugate, via an element of P, to a subgroup of K and, from Sylow's theorem, H_p is conjugate, via an element of K, to a subgroup of P. In particular, we have at most $1 + (|\mathrm{Sub}(K)| - 1)|P|$ choices for $H_{p'}$, because every non-identity subgroup of K as at most $|P|$ conjugates. Similarly, we have at most $1 + (|\mathrm{Sub}(P)| - 1)|K|$ choices for H_p, because every non-identity subgroup of P as at most $|K| = |R|/|P|$ conjugates. Write $|P| = p^a$ and $r = |R|$. Therefore,

$$|\mathrm{Sub}(R)| \leq (1 + (|\mathrm{Sub}(K)| - 1)p^a) \cdot \left(1 + (|\mathrm{Sub}(P)| - 1)\frac{r}{p^a}\right). \tag{6.1}$$

Using Lemma 2.1, this can be simplified in

$$|\mathrm{Sub}(R)| \leq |\mathrm{Sub}(K)|p^a \cdot |\mathrm{Sub}(P)|\frac{r}{p^a} \leq |\mathrm{Sub}(K)|S(p,a)r.$$

As $K < R$, K is not a counterexample to Theorem 1.1 and hence

$$|\mathrm{Sub}(R)| < c(2)(r/p^a)^{\frac{\log_2(r/p^a)}{4}} S(p,a)r = c(2)r^{\frac{\log_2 r}{4}} \cdot \frac{S(p,a)r}{p^{\frac{a\log_2(r/p^a)}{4}} r^{\frac{\log_2(p^a)}{4}}}$$

$$= c(2)r^{\frac{\log_2 r}{4}} \cdot \frac{S(p,a)r}{(r^2/p^a)^{\frac{\log_2(p^a)}{4}}}.$$

As R is a counterexample to Theorem 1.1, we have

$$\frac{S(p,a)r}{(r^2/p^a)^{\frac{\log_2(p^a)}{4}}} > 1.$$

From Proposition 3.2, we obtain that one of (1)–(6) is satisfied. As $r > 2\,000$, we deduce $p \in \{3,5\}$ and $a = 1$.

When $a = 1$, 1 and P are the only p-subgroups of R and hence we may refine (6.1) with

$$|\mathrm{Sub}(R)| \leq (1 + (|\mathrm{Sub}(K)| - 1)p^a) \cdot 2 \leq 2p|\mathrm{Sub}(K)| < 2pc(2)(r/p)^{\frac{\log_2(r/p)}{4}}.$$

Now, the proof follows from Lemma 5.2 (4). □

Lemma 6.2. *Let C be a solvable group and let p be a prime divisor of $|C|$ with the property that, for each prime power divisor q of $|C|$ with $q > 1$ and $p \nmid q$, p is relatively prime to $q - 1$. Then C has a normal Sylow p-subgroup.*

Proof. We argue by contradiction and we let C be a counterexample of minimal order. Let N be a minimal normal subgroup of C. As C is solvable, N has order a prime power $q > 1$. We adopt the "bar" notation for $\bar{C} = C/N$. If p is relatively prime to $|\bar{C}|$, then N is a normal Sylow p-subgroup of C, contradicting the fact that C is a counterexample to the statement of this lemma. Thus $p \mid |\bar{C}|$. As $|\bar{C}| < |C|$, $\bar{C}$ has a normal Sylow p-subgroup $\bar{P}$. Thus $\bar{P} = NP/N$, where P is a Sylow p-subgroup of C. As $\bar{P} \trianglelefteq \bar{C}$, we have $NP \trianglelefteq C$ and hence the minimality of C gives $C = NP$. Now the action of P by conjugation on N endows N of the structure of module for P. As N is a minimal normal subgroup of C, P acts irreducibly on N and hence p divides $|N| - 1 = q - 1$, which is a contradiction. □

6.1. An algorithm: step 1

In view of Proposition 4.4, there is only a finite number of counterexamples to Theorem 1.1 and our task is to show that actually there is no counterexample. We now describe an algorithm that greatly reduces the number of exceptions we need to analyze in detail.

The first step in our algorithm is to refine even further the functions (4.5) and (4.6). The input in the first step of our algorithm is a positive integer r satisfying none of the conditions in Proposition 4.4. The output of our algorithm is "yes" if a finite group of order r satisfies Theorem 1.1 and is "unknown" if our procedure cannot exclude the existence of a counterexample to Theorem 1.1.

First, as usual, we write $r = p_1^{a_1} \cdots p_\ell^{a_\ell}$, where $p_1 < \cdots < p_\ell$. Next, for each $i \in \{1, \dots, \ell\}$,

- when $p_i = 2$, we let $n_i = r/p_i^{a_i}$,

Table 6.1
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 10$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 59$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 29 \cdot 31$

Table 6.2
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 9$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 53$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 59$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 47$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 37$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29$

- when $p_i = 3$ and r is divisible by the order of $\mathrm{PSL}_2(3^{3^f})$ for some $f \geq 0$, we let n_i be the largest divisor of $r/p_i^{a_i}$ with $n_i \equiv 1 \mod p_i$ and with $n_i \leq r/p_i^{a_i}$, otherwise
- we let n_i be the largest divisor of $r/p_i^{a_i}$ with $n_i \equiv 1 \mod p_i$ and with $n_i < r/p_i^{a_i}$.

Observe that, by [6], n_i is an upper bound on the number of Sylow p_i-subgroups of a non-solvable finite group of order r. From Section 2, for every non-solvable group R of order r, we have

$$|\mathrm{Sub}(R)| \leq \prod_{i=1}^{\ell} n_i S(p_i, a_i). \tag{6.2}$$

We have computed $n_1, \ldots, n_\ell$ and we have computed the right hand side of this inequality. When $n_i = 1$ for some i or when this number is less than $c(2) r^{\log_2 r/4}$, we return "yes" otherwise we return "unknown". The list of positive integers r where this procedure returns "unknown" is reported in Tables 6.1–6.7. From Lemma 6.1 and from (6.2), when the procedure returns "yes", finite groups of order r satisfy Theorem 1.1. Therefore, the cardinalities that require further considerations are in Tables 6.1–6.7.

Using the order of the non-abelian simple groups (via the Classification of Finite Simple Groups), we are able to verify two important facts in our second procedure.

Fact 1: Let T be a non-abelian simple group whose order divides r. Then T appears in Table 6.8. Observe that the order of the outer automorphism group of T is not divisible by primes larger than 3.

Fact 2: Let $\kappa \geq 2$ and let $T_1, \ldots, T_\kappa$ be non-abelian simple groups with r divisible by $|T_1| \cdot |T_2| \cdots |T_\kappa|$. Then $\kappa = 2$ and $T_1 \times T_2$ is isomorphic to either

Table 6.3
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 8$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 37$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 37$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 41$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 53$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 53$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 61$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 67$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 73$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 23$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 43$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 53$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 59$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 61$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 47$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23 \cdot 83$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 37$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 41$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 59$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29 \cdot 61$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 41$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 47$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 61$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 41$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23 \cdot 43$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23 \cdot 37$
$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31$			

Table 6.4
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 7$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$
$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$
$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 41$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 43$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 53$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 67$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 43$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 47$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 59$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 61$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot 79$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 19 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23$
$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 31$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 53$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 \cdot 61$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 29$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 43$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 53$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19 \cdot 23$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 23 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 37$
$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \cdot 41$	$2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$

$$\mathrm{Alt}(5) \times \mathrm{PSL}_2(7), \text{ or } \mathrm{Alt}(5) \times \mathrm{PSL}_2(13), \text{ or } \mathrm{PSL}_2(11) \times \mathrm{PSL}_2(13).$$

In particular, a non-solvable group R of order r (where the previous procedure has returned "unknown") has at most two non-abelian simple sections, and if R has two non-abelian simple sections, then these two sections are not isomorphic.

6.2. An algorithm: step 2

We are now ready to describe our second procedure that needs to be applied to all cases where the previous procedure returns "unknown", that is, to each positive integer in Tables 6.1–6.7.

The input of the second procedure is a positive integer r. First, we determine the set $\mathcal{D}$ all the divisors d of r, with the property that d is the order of a direct product of non-abelian simple groups. (The number d represents the product of the cardinalities of the non-abelian simple sections in a non-solvable group of order r.) Clearly, in this step, we may use the information in Table 6.8.

In the case that there is no such divisor d, that is $\mathcal{D} = \emptyset$, we stop our algorithm and we return "yes": this represents the fact that a finite group of order r is solvable because r is not divisible by the order of a non-abelian simple group. For instance, when $r = 2^2 \cdot 3 \cdot 7 \cdot 11 = 924$ from Table 6.7, we have $\mathcal{D} = \emptyset$, because no non-abelian simple group has order a divisor of 924.

Table 6.5
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 6$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$
$2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 17$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 17$
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 19$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11 \cdot 23$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$
$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29$
$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 29$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 31$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 31$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 31$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 41$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 41$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 41$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 71$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 73$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$
$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 23$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 31$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 31$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 31$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 37$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 41$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 41$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 43$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 53$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 59$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 23$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 41$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 43$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 83$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 29$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 19 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 29$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$
$2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 13 \cdot 17$	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$	$2^6 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19$
$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 43$	$2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 17 \cdot 19$
$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 17$	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 23$

Table 6.6
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 5$.

$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 11$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	$2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$2^9 \cdot 3 \cdot 5 \cdot 7 \cdot 11$
$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$2^2 \cdot 3 \cdot 5 \cdot 7^2 \cdot 13$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 13$
$2^5 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17$	$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 17$
$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	$2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	$2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 17$	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 17$
$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 19$
$2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 19$	$2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 23$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23$
$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	$2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 31$
$2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 37$	$2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	$2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 43$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 13$
$2^5 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	$2^3 \cdot 3 \cdot 5 \cdot 11 \cdot 17$	$2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 17$	$2^2 \cdot 3^2 \cdot 5 \cdot 11 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 29$
$2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 47$	$2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 17$	$2^3 \cdot 3 \cdot 5 \cdot 13 \cdot 19$	$2^2 \cdot 3 \cdot 5 \cdot 13 \cdot 37$	$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 13$
$2^2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 13$	$2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 13$	$2^4 \cdot 3 \cdot 7 \cdot 11 \cdot 13$	$2^6 \cdot 3 \cdot 7 \cdot 11 \cdot 13$	$2^4 \cdot 3 \cdot 7 \cdot 11 \cdot 17$
$2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 19$	$2^3 \cdot 3 \cdot 7 \cdot 11 \cdot 23$	$2^2 \cdot 3 \cdot 7 \cdot 17 \cdot 31$		

Let κ be the number of non-abelian factors in a composition series of a non-solvable group R of order r. From Fact 2, $\kappa \leq 2$ and, in the case $\kappa = 2$, the two non-abelian factors are non-isomorphic. Let $X_1/Y_1, \dots, X_\kappa/Y_\kappa$ be the non-abelian simple sections of R and let $d = |X_1/Y_1| \cdots |X_\kappa/Y_\kappa|$. When $\kappa = 1$, by taking a suitable chief series, we may suppose that X_1 and Y_1 are normal subgroups of R. Similarly, when $\kappa = 2$, as $X_1/Y_1 \ncong X_2/Y_2$, by taking a suitable chief series, we may suppose that X_1, X_2, Y_1, Y_2 are normal subgroups of R. Let $C = \mathbf{C}_R(X_1/Y_1)$ when $\kappa = 1$ and let $C = \mathbf{C}_R(X_1/Y_1) \cap \mathbf{C}_R(X_2/Y_2)$ when $\kappa = 2$. Now, C is the kernel of the action of R by conjugation on X_1/Y_1 (when

Table 6.7
Positive integers returning "unknown" in the step 1 of the algorithm with $\ell = 4$.

$2^2 \cdot 3 \cdot 5 \cdot 7$	$2^2 \cdot 3 \cdot 5 \cdot 7^2$	$2^2 \cdot 3 \cdot 5^2 \cdot 7$	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	$2^2 \cdot 3^4 \cdot 5 \cdot 7$
$2^3 \cdot 3 \cdot 5 \cdot 7$	$2^3 \cdot 3 \cdot 5^2 \cdot 7$	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	$2^3 \cdot 3^3 \cdot 5 \cdot 7$	$2^4 \cdot 3 \cdot 5 \cdot 7$
$2^4 \cdot 3 \cdot 5 \cdot 7^2$	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	$2^5 \cdot 3 \cdot 5 \cdot 7$	$2^6 \cdot 3 \cdot 5 \cdot 7$	$2^6 \cdot 3^2 \cdot 5 \cdot 7$
$2^7 \cdot 3 \cdot 5 \cdot 7$	$2^8 \cdot 3 \cdot 5 \cdot 7$	$2^9 \cdot 3 \cdot 5 \cdot 7$	$2^{10} \cdot 3 \cdot 5 \cdot 7$	$2^{11} \cdot 3 \cdot 5 \cdot 7$
$2^{12} \cdot 3 \cdot 5 \cdot 7$	$2^{13} \cdot 3 \cdot 5 \cdot 7$	$2^{14} \cdot 3 \cdot 5 \cdot 7$	$2^{16} \cdot 3 \cdot 5 \cdot 7$	$2^{17} \cdot 3 \cdot 5 \cdot 7$
$2^{19} \cdot 3 \cdot 5 \cdot 7$	$2^{22} \cdot 3 \cdot 5 \cdot 7$	$2^2 \cdot 3 \cdot 5 \cdot 11$	$2^2 \cdot 3 \cdot 5^2 \cdot 11$	$2^2 \cdot 3^2 \cdot 5 \cdot 11$
$2^3 \cdot 3 \cdot 5 \cdot 11$	$2^3 \cdot 3^2 \cdot 5 \cdot 11$	$2^4 \cdot 3 \cdot 5 \cdot 11$	$2^6 \cdot 3 \cdot 5 \cdot 11$	$2^7 \cdot 3 \cdot 5 \cdot 11$
$2^9 \cdot 3 \cdot 5 \cdot 11$	$2^3 \cdot 3 \cdot 5 \cdot 13$	$2^3 \cdot 3 \cdot 5^2 \cdot 13$	$2^4 \cdot 3 \cdot 5 \cdot 13$	$2^4 \cdot 3 \cdot 5 \cdot 17$
$2^5 \cdot 3 \cdot 5 \cdot 17$	$2^2 \cdot 3 \cdot 5 \cdot 19$	$2^4 \cdot 3 \cdot 5 \cdot 19$	$2^3 \cdot 3 \cdot 5 \cdot 23$	$2^2 \cdot 3 \cdot 5 \cdot 29$
$2^2 \cdot 3 \cdot 7 \cdot 11$	$2^3 \cdot 3 \cdot 7 \cdot 11$	$2^4 \cdot 3 \cdot 7 \cdot 11$	$2^6 \cdot 3 \cdot 7 \cdot 11$	$2^2 \cdot 3 \cdot 7 \cdot 13$
$2^3 \cdot 3 \cdot 7 \cdot 13$	$2^2 \cdot 3 \cdot 7 \cdot 41$	$2^2 \cdot 3 \cdot 11 \cdot 13$		

Table 6.8
Putative non-abelian simple sections in a counterexample to Theorem 1.1.

Group	Order	Order of outer Automorphism
Alt(5)	$60 = 2^2 \cdot 3 \cdot 5$	2
$\mathrm{PSL}_2(7)$	$168 = 2^3 \cdot 3 \cdot 7$	2
Alt(6)	$360 = 2^3 \cdot 3^2 \cdot 5$	4
$\mathrm{PSL}_2(8)$	$504 = 2^3 \cdot 3^2 \cdot 7$	3
$\mathrm{PSL}_2(11)$	$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	2
$\mathrm{PSL}_2(13)$	$1\,092 = 2^2 \cdot 3 \cdot 7 \cdot 13$	2
$\mathrm{PSL}_2(17)$	$2\,448 = 2^4 \cdot 3^2 \cdot 17$	2
Alt(7)	$2\,520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	2
$\mathrm{PSL}_2(19)$	$3\,420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$	2
$\mathrm{PSL}_2(16)$	$4\,080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	4
$\mathrm{PSL}_3(3)$	$5\,616 = 2^4 \cdot 3^3 \cdot 13$	2
$\mathrm{PSL}_2(23)$	$6\,072 = 2^3 \cdot 3 \cdot 11 \cdot 23$	2
$\mathrm{PSL}_2(25)$	$7\,800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$	4
M_{11}	$7\,920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$	1
$\mathrm{PSL}_2(27)$	$9\,828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$	6
$\mathrm{PSL}_2(29)$	$12\,180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	2
Alt(8)	$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	2
$\mathrm{PSL}_3(4)$	$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	12
Suz(8)	$29\,120 = 2^6 \cdot 5 \cdot 7 \cdot 13$	3
$\mathrm{PSL}_2(41)$	$34\,440 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$	2
$\mathrm{PSL}_2(43)$	$39\,732 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$	2
$\mathrm{PSL}_2(67)$	$150\,348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$	2
J_1	$175\,560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	1

$\kappa = 1$) and on $X_1/Y_1 \times X_2/Y_2$ (when $\kappa = 2$). When $\kappa = 1$, R/C is almost simple with socle X_1/Y_1 and C is solvable. When $\kappa = 2$, R/C is isomorphic to a subgroup of $\mathrm{Aut}(X_1/Y_1) \times \mathrm{Aut}(X_2/Y_2)$ and C is solvable.

The order of C divides r/d. Now, we select all prime divisor $p \geq 5$ of r/d with

- $p \nmid d$, and
- for each divisor q of r/d with $q > 1$ and with q a prime power, p is relatively prime to $q - 1$.

If there is at least one such prime, we stop the computations and we return "yes"; indeed, by Lemma 6.1 and 6.2, r is not the order of a minimal counterexample to Theorem 1.1.

The only positive integers r where this produce did not return "yes" are recorded in Tables 6.9, 6.10 and 6.11. In particular, observe that $\ell \in \{4, 5, 6\}$ and hence there are no counterexamples to Theorem 1.1 with $\ell > 6$.

We give an example. Suppose $r = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$ from Table 6.1. We have

$$\mathcal{D} = \{60, 168, 660, 1\,092, 12\,180\}.$$

In particular, a non-solvable group R of order r has a unique non-abelian composition factor X/Y. Moreover, X/Y is isomorphic to one of the following groups

$$\mathrm{Alt}(5), \mathrm{PSL}_2(7), \mathrm{PSL}_2(11), \mathrm{PSL}_2(13), \mathrm{PSL}_2(29).$$

Therefore $\kappa = 1$ in this case. Let $C = \mathbf{C}_R(X/Y)$. As the outer automorphism group of each of these groups has order 2 and as $2^3 \nmid r$, we have $R/C \cong X/Y$. Then C is solvable and the order of C is an element of

$$\{r/d \mid d \in \mathcal{D}\} = \{7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29, 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29,$$
$$7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29, 5 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 29, 11 \cdot 17 \cdot 19 \cdot 23\}.$$

Just to give an example, let us say $|C| = 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29$. From Lemma 6.2, we see that a Sylow 29-subgroup of C is normal in C and hence also normal in R. Therefore, from Lemma 6.1, R is not a counterexample of minimal order to Theorem 1.1.

A direct inspection in Tables 6.9, 6.10 and 6.11 shows that, except when $|R| = 20\,160$ and $\mathrm{Alt}(5) \times \mathrm{PSL}_2(7)$ is a section of R, R has a unique non-abelian composition factor. Suppose that $|R| = 20\,160$ and $\mathrm{Alt}(5) \times \mathrm{PSL}_2(7)$ is a section of R. As $|\mathrm{Alt}(5) \times \mathrm{PSL}_2(7)| = 10\,080$, we deduce that R has a normal subgroup N such that either

- $|R : N| = 2$ and $N \cong \mathrm{Alt}(5) \times \mathrm{PSL}_2(7)$, or
- $|N| = 2$ and $R/N \cong \mathrm{Alt}(5) \times \mathrm{PSL}_2(7)$.

Taking in account that the Schur multiplier and the outer automorphism group of $\mathrm{Alt}(5)$ and $\mathrm{PSL}_2(7)$ have order 2, we deduce that R is isomorphic to

$$\mathrm{Sym}(5) \times \mathrm{PSL}_2(7),\ \mathrm{Alt}(5) \times \mathrm{PGL}_2(7),\ (\mathrm{Alt}(5) \times \mathrm{PSL}_2(7)).2,$$

or to

$$C_2 \times \mathrm{Alt}(5) \times \mathrm{PSL}_2(7),\ \mathrm{SL}_2(5) \times \mathrm{PSL}_2(7),\ \mathrm{Alt}(5) \times \mathrm{SL}_2(7),\ \mathrm{SL}_2(5) \circ \mathrm{SL}_2(7).$$

The veracity of Theorem 1.1 for these seven groups can be verified with a computer. Therefore, for the rest of our argument, we may suppose that R has a unique non-abelian simple factor T. Therefore, R has a normal solvable subgroup C with R/C almost simple with socle T.

Table 6.9
Exceptions with $\ell = 6$.

$r = \lvert R\rvert$	non-abelian sections	$\lvert R\rvert/\lvert T\rvert$
$175\,560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	J_1	1
$351\,120 = 2^4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	J_1	2
$702\,240 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	J_1	4

Table 6.10
Exceptions with $\ell = 5$.

$r = \lvert R\rvert$	non-abelian sections	$\lvert R\rvert/\lvert T\rvert$
$36\,960 = 2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$\mathrm{PSL}_2(11)$	56
$73\,920 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$\mathrm{PSL}_2(11)$	112
$147\,840 = 2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$\mathrm{PSL}_2(11)$	224
$295\,680 = 2^8 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$\mathrm{PSL}_2(11)$	448
$591\,360 = 2^9 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	$\mathrm{PSL}_2(11)$	896
$87\,360 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$\mathrm{PSL}_2(13)$	80
$12\,180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$\mathrm{PSL}_2(29)$	1
$24\,360 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29$	$\mathrm{PSL}_2(29)$	2

6.3. The case $\ell = 6$

From Table 6.9, we have $T = J_1$. Since J_1 has trivial Schur multiplier and trivial outer automorphism group, we deduce $R = T \times C$. As $|C| \in \{1, 2, 4\}$, we get that R is isomorphic to one of the following groups

$$J_1,\ C_2 \times J_1,\ C_4 \times J_1,\ C_2 \times C_2 \times J_1.$$

Now, the veracity of Theorem 1.1 for these groups can be verified with a computer.

6.4. The case $\ell = 5$

We use the information from Table 6.10. When $T = \mathrm{PSL}_2(29)$, we have $|C| \leq 2$ and hence we deduce that $R \in \{\mathrm{PSL}_2(29), \mathrm{SL}_2(29), \mathrm{PGL}_2(29)\}$. Here, we check Theorem 1.1 with a computer.

Suppose now $T = \mathrm{PSL}_2(p)$, with $p \in \{11, 13\}$. Thus $R/C \cong \mathrm{PSL}_2(p)$ or $R/C \cong \mathrm{PGL}_2(p)$. Observe that p is relatively prime to $|C|$. We adopt the "bar" notation for the projection of R onto $\bar{R} = R/C$. Let $\bar{H}_1, \dots, \bar{H}_\kappa$ be representatives for the $\bar{R}$-conjugacy classes of the maximal p'-subgroups of $\bar{R}$. Then the preimages $H_1, \dots, H_\kappa$ are representatives for the R-conjugacy classes of the maximal p'-subgroups of R. Since the Sylow p-subgroups of R are cyclic of order p and since R has at most r/p Sylow p-subgroups, we deduce

$$|\mathrm{Sub}(R)| \leq \sum_{i=1}^{\kappa} |\mathrm{Sub}(H_i)| \cdot \frac{r}{|H_i|} \cdot 2 \cdot \frac{r}{p} \leq \frac{2r^2 c(2)}{p} \sum_{i=1}^{\kappa} |H_i|^{\frac{\log_2 |H_i|}{4} - 1}.$$

Table 6.11
Exceptions with $\ell = 4$.

$r = \lvert R\rvert$	non-abelian sections	$\lvert R\rvert/\lvert T\rvert$
$2\,520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(7)$	1
$5\,040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(7)$	2
$7\,560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$	$\mathrm{Alt}(7)$	3
$3\,360 = 2^5 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	56
$6\,720 = 2^6 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	112
$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	336
$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(6)$	56
$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(7)$	8
$20\,160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(8)$ or $\mathrm{PSL}_3(4)$	1
$20\,160 = 2^5 \cdot 3^2 \cdot 5 \cdot 7$	$\mathrm{Alt}(5) \times \mathrm{PSL}_2(7)$	2
$13\,440 = 2^7 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	224
$13\,440 = 2^7 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	80
$26\,880 = 2^8 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	448
$26\,880 = 2^8 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	160
$53\,760 = 2^9 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	896
$53\,760 = 2^9 \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	320
$107\,520 = 2^{10} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	1 792
$107\,520 = 2^{10} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	640
$215\,040 = 2^{11} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	3 584
$215\,040 = 2^{11} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	1 280
$430\,080 = 2^{12} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{Alt}(5)$	7 168
$430\,080 = 2^{12} \cdot 3 \cdot 5 \cdot 7$	$\mathrm{PSL}_2(7)$	2 560
$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	1
$1\,320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	2
$1\,980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	3
$2\,640 = 2^4 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	4
$3\,300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$	$\mathrm{PSL}_2(11)$	5
$3\,960 = 2^3 \cdot 3^2 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	6
$10\,560 = 2^6 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	16
$21\,120 = 2^7 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	32
$84\,480 = 2^9 \cdot 3 \cdot 5 \cdot 11$	$\mathrm{PSL}_2(11)$	128
$7\,800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$	$\mathrm{PSL}_2(25)$	1
$4\,080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	$\mathrm{PSL}_2(16)$	1
$8\,160 = 2^5 \cdot 3 \cdot 5 \cdot 17$	$\mathrm{PSL}_2(16)$	2
$1\,092 = 2^2 \cdot 3 \cdot 7 \cdot 13$	$\mathrm{PSL}_2(13)$	1
$2\,184 = 2^3 \cdot 3 \cdot 7 \cdot 13$	$\mathrm{PSL}_2(13)$	2

We have implemented this function using the information on $\bar{R}$ and in all cases this bound is less than $c(2)|R|^{\log_2 |R|/4}$.

6.5. The case $\ell = 4$

We omit the analysis of this case. All groups can be checked with arguments analogous to the methods used in Section 6.4.

Data availability

Data will be made available on request.

Appendix A

A.1. Proof of Proposition 3.2

We consider various cases depending on the value of a_i.

Case $a_i = 1$. We have $S(p_i, a_i) = 2$. As $\ell \geq 2$, we have $r/p_i \geq p_1 \cdots p_{i-1} \cdot p_{i+1} \cdots p_\ell \geq 2$. Hence, we have

$$\begin{aligned}\frac{S(p_i,a_i)r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} &= \frac{2r}{(r^2/p_i)^{\frac{\log_2(p_i)}{4}}} = 2p_i^{\frac{\log_2(p_i)}{4}} r^{1-\frac{\log_2(p_i)}{2}} \\ &= 2p_i^{\frac{\log_2(p_i)}{4}} p_i^{1-\frac{\log_2(p_i)}{2}} \left(\frac{r}{p_i}\right)^{1-\frac{\log_2(p_i)}{2}} \qquad \text{(A.1)} \\ &\leq 2p_i^{1-\frac{\log_2(p_i)}{4}} 2^{1-\frac{\log_2(p_i)}{2}} = 2^{2-\frac{\log_2(p_i)}{2}} p_i^{1-\frac{\log_2(p_i)}{4}} = 2^{2+\frac{\log_2(p_i)}{2}-\frac{(\log_2(p_i))^2}{4}}.\end{aligned}$$

Set $x := \log_2(p_i)$. Now, the expression

$$2 + \frac{x}{2} - \frac{x^2}{4}$$

is a parabola and it can be verified that it is negative when $x > 4$, that is, $p_i > 16$. In particular, (3.3) follows from (A.1) when $p_i > 16$.

Suppose $p_i \leq 16$, that is, $p_i \leq 13$ because p_i is a prime number. Set $y = \log_2(r/p_i)$. By following the same computations as in (A.1), we obtain

$$\frac{S(p_i,a_i)r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} = 2p_i^{1-\frac{\log_2(p_i)}{4}} 2^{\left(1-\frac{\log_2(p_i)}{2}\right)y} = 2^{1+\log_2(p_i)-\frac{(\log_2(p_i))^2}{4}+\left(1-\frac{\log_2(p_i)}{2}\right)y}.$$

Now, the expression

$$1 + \log_2(p_i) - \frac{(\log_2(p_i))^2}{4} + \left(1 - \frac{\log_2(p_i)}{2}\right) y$$

is linear in y. When $p_i \geq 5$, we have $1 - \log_2(p_i)/2 < 0$ and hence this linear expression is negative for

$$y > \frac{\frac{(\log_2(p_i))^2}{4} - \log_2(p_i) - 1}{1 - \frac{\log_2(p_i)}{2}}.$$

When $p_i = 13$, we find $r/p_i = 2^y > 2.8$ and hence (3.3) is satisfied as long as $r/p_i > 2.8$. Thus, the only exceptions arising with $p_i = 13$ are in (1). All other cases are dealt with similarly, considering all primes $p_i \leq 13$.

Case $a_i = 2$. We have $S(p_i, a_i) = p_i + 3$. When $p_i = 2$, we have the exceptions in (2). Therefore, for the rest of the argument we suppose $p_i \geq 3$. In particular, $p_i + 3 \leq 2p_i$. As $\ell \geq 2$, we have $r/p_i^{a_i} \geq 2$. Hence, we have

$$\begin{aligned}\frac{(p_i+3)r}{(r^2/p_i^2)^{\frac{\log_2(p_i)}{2}}} &\leq \frac{2p_i \cdot r}{(r^2/p_i^2)^{\frac{\log_2(p_i)}{2}}} \\ &= 2p_i^{1+\log_2(p_i)} r^{1-\log_2(p_i)} = 2p_i^{1+\log_2(p_i)} p_i^{2-2\log_2(p_i)} \left(\frac{r}{p_i^2}\right)^{1-\log_2(p_i)} \\ &= 2p_i^{3-\log_2(p_i)} \left(\frac{r}{p_i^2}\right)^{1-\log_2(p_i)} \leq 2p_i^{3-\log_2(p_i)} 2^{1-\log_2(p_i)} \\ &= 2^{2-\log_2(p_i)} p_i^{3-\log_2(p_i)}.\end{aligned} \tag{A.2}$$

When $p_i \geq 7$, we have $2^{2-\log_2(p_i)} p_i^{3-\log_2(p_i)} < 1$ and hence (3.3) is satisfied.

Assume $p_i = 5$. If $r/p_i^2 \geq 4$, then we may follow step by step the computations in (A.2) and replace r/p_i^2 with 4 (rather than 2); thus we obtain

$$\frac{(p_i+3)r}{(r^2/p_i^{a_i})^{a_i \frac{\log_2(p_i)}{4}}} \leq 2^{3-2\log_2(p_i)} p_i^{3-\log_2(p_i)} < 1.$$

If $r/p_i^2 < 4$, then $r = 2 \cdot p_i^2 = 50$ or $r = 3 \cdot p_i^2 = 75$ and we obtain the exceptions in (2).

Assume $p_i = 3$. If $r/p_i^2 \geq 64$, as above, we may follow step by step the computations in (A.2) and replace r/p_i^2 with $64 = 2^6$; thus we obtain

$$\frac{(p_i+3)r}{(r^2/p_i^{a_i})^{a_i \frac{\log_2(p_i)}{4}}} \leq 2^{7-6\log_2(p_i)} p_i^{3-\log_2(p_i)} = 0.83 < 1.$$

When $r/p_i^2 < 64$, we have computed explicitly the value on the left hand side of (3.3) and we have verified that the only exceptions arise with $r/p_i^2 \leq 46$, that is, we obtain the exceptions in (2).

Case $a_i = 3$. We have $S(p_i, a_i) = 2p_i^2 + 2p_i + 4$. Moreover, we have

$$\begin{aligned}\frac{(2p_i^2+2p_i+4)r}{(r^2/p_i^3)^{3\frac{\log_2(p_i)}{4}}} &\leq \frac{4p_i^2 \cdot r}{(r^2/p_i^3)^{3\frac{\log_2(p_i)}{4}}} = 2^2 p_i^{2+9\frac{\log_2(p_i)}{4}} r^{1-3\frac{\log_2(p_i)}{2}} \\ &= 2^2 p_i^{2+9\frac{\log_2(p_i)}{4}} p_i^{3-9\frac{\log_2(p_i)}{2}} \left(\frac{r}{p_i^3}\right)^{1-3\frac{\log_2(p_i)}{2}} \\ &= 2^2 p_i^{5-9\frac{\log_2(p_i)}{4}} \left(\frac{r}{p_i^3}\right)^{1-3\frac{\log_2(p_i)}{2}} \leq 2^2 p_i^{5-9\frac{\log_2(p_i)}{4}} 2^{1-3\frac{\log_2(p_i)}{2}} \\ &= 2^{3-3\frac{\log_2(p_i)}{2}} p_i^{5-9\frac{\log_2(p_i)}{4}}\end{aligned}$$

$$= 2^{3+7\frac{\log_2(p_i)}{2}-9\frac{(\log_2(p_i))^2}{4}}.$$

This number is less than 1 for each $p_i > 3$ and hence (3.3) is satisfied in these cases.

Assume $p_i = 3$. If $r/p_i^2 \geq 16$, as usual, we may follow the computations above but replacing r/p_i^3 with $16 = 2^4$; thus we obtain

$$\frac{(2p_i^2+2p_i+4)r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} \leq 2^2 p_i^{5-9\frac{\log_2(p_i)}{4}} 2^{4-6\log_2(p_i)} = 0.42 < 1.$$

When $r/p_i^3 < 16$, we have computed explicitly the value on the left hand side of (3.3) and we have verified that the only exceptions arise with $r/p_i^3 \leq 7$, that is, we obtain the exceptions in (3).

Assume $p_i = 2$. We obtain

$$\frac{(2p_i^2+2p_i+4)r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} = \frac{16r}{(r^2/8)^{3/4}} = \frac{2^{25/4}}{r^{1/2}}.$$

This expression is less than 1 when $r \geq 5\,800$, therefore the only exceptions arise when $r/p_i^3 \leq 723$, that is, we obtain the exceptions in (3).

Case $a_i \in \{4,5\}$. These values of a_i are checked similarly; indeed, for $a_i \in \{4,5\}$, (3.3) is satisfied, except for the cases listed in (4) and (5).

Case $a_i \geq 6$. We have $S(p_i,a_i) = c(p_i)p_i^{a_i^2/4}$. Assume $p_i \geq 3$. Using $c(p_i) \leq c(3) < 4$, we have

$$\begin{aligned}\frac{c(p_i)p_i^{\frac{a_i^2}{4}}r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} &= c(p_i)p_i^{\frac{a_i^2}{4}+\frac{a_i^2\log_2(p_i)}{4}} r^{1-\frac{a_i\log_2(p_i)}{2}} \\ &= c(p_i)p_i^{\frac{a_i^2}{4}+\frac{a_i^2\log_2(p_i)}{4}+a_i-\frac{a_i^2\log_2(p_i)}{2}} \left(\frac{r}{p_i^{a_i}}\right)^{1-\frac{a_i\log_2(p_i)}{2}} \\ &< c(3)p_i^{\frac{a_i^2}{4}-\frac{a_i^2\log_2(p_i)}{4}+a_i} 2^{1-\frac{a_i\log_2(p_i)}{2}} = 2^{3-\frac{a_i\log_2(p_i)}{2}} p_i^{\frac{a_i^2}{4}-\frac{a_i^2\log_2(p_i)}{4}+a_i}.\end{aligned}$$

Summing up,

$$\frac{S(p_i,a_i)r}{(r^2/p_i^{a_i})^{a_i\frac{\log_2(p_i)}{4}}} \leq 2^{3-\frac{a_i\log_2(p_i)}{2}} p_i^{\frac{a_i^2}{4}-\frac{a_i^2\log_2(p_i)}{4}+a_i}. \tag{A.3}$$

Now,

$$3-\frac{a_i\log_2(p_i)}{2} \leq 3-\frac{a_i\log_2(3)}{2} \leq 3-\frac{6\cdot\log_2(3)}{2} < 0.$$

Similarly, for $(a_i,p_i) \neq (6,3)$, one can check that

$$\frac{a_i^2}{4} - \frac{a_i^2 \log_2(p_i)}{4} + a_i < 0.$$

Therefore, for $(a_i, p_i) \neq (6, 3)$, (3.3) follows from (A.3). Finally, when $(a_i, p_i) = (6, 3)$, we have

$$2^{3 - \frac{a_i \log_2(p_i)}{2}} p_i^{\frac{a_i^2}{4} - \frac{a_i^2 \log_2(p_i)}{4} + a_i} = 0.6646 < 1$$

and hence (3.3) follows again from (A.3).

Finally, assume $p_i = 2$ and set $r' = r/p_i^{a_i}$. We have

$$\begin{aligned}\frac{c(p_i) p_i^{\frac{a_i^2}{4}} r}{(r^2/p_i^{a_i})^{a_i \frac{\log_2(p_i)}{4}}} &= c(2) 2^{\frac{a_i^2}{4} + \frac{a_i^2}{4}} r^{1 - \frac{a_i}{2}} = c(2) 2^{\frac{a_i^2}{2}} r^{1 - \frac{a_i}{2}} = c(2) 2^{\frac{a_i^2}{2}} 2^{a_i - \frac{a_i^2}{2}} r'^{1 - \frac{a_i}{2}} \\ &= c(2) 2^{a_i} r'^{1 - \frac{a_i}{2}} = c(2) 2^{a_i} 2^{(1 - a_i/2) \log_2 r'} < 2^{3 + a_i + (1 - a_i/2) \log_2(r')}.\end{aligned}$$

Now, consider the function $g(a_i, r') = 3 + a_i + (1 - a_i/2) \log_2(r')$, where we think of a_i and r' as continuous variables. We have $\partial g / \partial a_i = 1 - \log_2(r')/2 \leq 0$. Therefore,

$$g(a_i, r') \leq 3 + 6 + (1 - 6/2) \log_2(r') = 9 - 2 \log_2(r').$$

Now, $9 - 2 \log_2(r') \leq 0$, when $\log_2(r') \geq 9/2$, that is, $r' \geq 22$. In particular, the only exceptions to (3.3) arise when $r/p_i^{a_i} = r' \leq 21$, as stated in (6).

A.2. Directional monotonicity of $f(r)$ and proof of Lemma 4.1

Let $i \in \{1, \dots, \ell\}$. By considering the discrete variable p_i as continue, we find

$$\frac{\partial f(r)}{\partial p_i} = -\frac{a_i \log c(2)}{p_i (\log r)^2} + \frac{a_i}{4 p_i \log 2} - \frac{\partial S(p_i, a_i)/\partial p_i}{S(p_i, a_i) \log r} + \frac{a_i \log S(p_i, a_i)}{p_i (\log r)^2} - \frac{(\ell - 2) a_i \log 2}{p_i (\log r)^2}.$$

We are interested in showing $\partial f(r)/\partial p_i \geq 0$, $\forall p_i \geq 2$, where $f(r) = f(p_1, \dots, p_\ell)$ is thought as a function in $p_1, \dots, p_\ell$ with $a_1, \dots, a_\ell$ being fixed. From this, the proof of Lemma 4.1 immediately follows.

Multiplying by $p_i (\log r)^2$, we obtain

$$\begin{aligned}p_i (\log r)^2 \frac{\partial f(r)}{\partial p_i} = -a_i \log c(2) + \frac{a_i (\log r)^2}{4 \log 2} - \frac{p_i \partial S(p_i, a_i)/\partial p_i}{S(p_i, a_i)} \log r \\ + a_i \log S(p_i, a_i) - (\ell - 2) a_i \log 2.\end{aligned} \tag{A.4}$$

We now distinguish various cases depending on a_i.

Case $a_i = 1$. Then $S(p_i, a_i) = 2$ and, from (A.4), we obtain

$$p_i (\log r)^2 \frac{\partial f(r)}{\partial p_i} = \log(8/c(2)) + \frac{(\log r)^2}{4 \log 2} - \ell \log 2. \tag{A.5}$$

We have

$$\ell \leq \log_2 r = \frac{\log r}{\log 2}, \tag{A.6}$$

because ℓ is the number of prime factors of r. From (A.5) and (A.6) and from $c(2) < 8$, we have

$$p_i(\log r)^2 \frac{\partial f(r)}{\partial p_i} \geq \log(8/c(2)) + \frac{(\log r)^2}{4\log 2} - \log r \geq \frac{(\log r)^2}{4\log 2} - \log r.$$

The formula appearing on the right hand side of $p_i(\log r)^2 \partial f(r)/\partial p_i$ is positive for $\log r \geq 4\log 2$, that is, $r \geq 16$. In particular, $\partial f(r)/\partial p_i \geq 0$, for each r with $r \geq 16$. Recalling that $\ell \geq 3$, the condition $r \geq 16$ is automatically satisfied.

Case $a_i = 2$. Then $S(p_i, a_i) = p_i + 3$ and $\partial S(p_i, a_i)/\partial p_i = 1$ and, from (A.4), we obtain

$$p_i(\log r)^2 \frac{\partial f(r)}{\partial p_i} = -2\log c(2) + \frac{(\log r)^2}{2\log 2} - \log r \frac{p_i}{p_i + 3} + 2\log(p_i + 3) - 2(\ell - 2)\log 2.$$

As above, by using $p_i \geq 2$ in the first inequality, by using $\log(16/c(2)^2) + 2\log(5) \geq 1.99$ in the second inequality and by using (A.6) in the last inequality, we deduce

$$\begin{aligned} p_i(\log r)^2 \frac{\partial f(r)}{\partial p_i} &= \log(16/c(2)^2) + \frac{(\log r)^2}{2\log 2} - \log r \frac{p_i}{p_i + 3} + 2\log(p_i + 3) - 2\ell \log 2 \\ &\geq \log(16/c(2)^2) + \frac{(\log r)^2}{2\log 2} - \log r + 2\log(5) - 2\ell \log 2 \\ &\geq \frac{(\log r)^2}{2\log 2} - \log r - 2\ell \log 2 + 1.99 \\ &\geq \frac{(\log r)^2}{2\log 2} - \log r - 2\log r + 1.99 = \frac{(\log r)^2}{2\log 2} - 3\log r + 1.99. \end{aligned}$$

The formula appearing on the right hand side of $p_i(\log r)^2 \partial f(r)/\partial p_i$ is quadratic in $\log r$ and it can be verified that it is positive for $r \geq 28$. As $\ell \geq 3$ by (4.3), we have $r \geq 2 \cdot 3 \cdot 5 = 30$ and hence the condition $r \geq 28$ is automatically satisfied. Thus $\partial f(r)/\partial p_i \geq 0$, $\forall p_i \geq 2$.

Case $a_i = 3$. Then $S(p_i, a_i) = 2p_i^2 + 2p_i + 4$ and $\partial S(p_i, a_2)/\partial p_i = 4p_i + 2$ and, from (A.4), we obtain

$$\begin{aligned} p_i(\log r)^2 \frac{\partial f(r)}{\partial p_i} = -3\log c(2) + \frac{3(\log r)^2}{4\log 2} - \frac{4p_i^2 + 2p_i}{2p_i^2 + 2p_i + 4} \log r \\ + 3\log(2p_i^2 + 2p_i + 4) - 3(\ell - 2)\log 2. \end{aligned}$$

We deduce

$$\begin{aligned} p_i(\log r)^2\frac{\partial f(r)}{\partial p_i} &\geq -3\log c(2)+\frac{3(\log r)^2}{4\log 2}-2\log r+3\log(2p_i^2+2p_i+4)-3(\ell-2)\log 2\\ &\geq -3\log c(2)+\frac{3(\log r)^2}{4\log 2}-2\log r+3\log(16)-3(\ell-2)\log 2\\ &= -3\log c(2)+\frac{3(\log r)^2}{4\log 2}-2\log r+18\log(2)-3\ell\log 2\\ &\geq -3\log c(2)+\frac{3(\log r)^2}{4\log 2}-2\log r+18\log(2)-3\log r\\ &= -3\log c(2)+\frac{3(\log r)^2}{4\log 2}-5\log r+18\log(2). \end{aligned}$$

Now, using this expression, it can be verified that $\partial f(r)/\partial p_i$ is always positive.

Case $a_i \in \{4,5\}$. These cases are analogous and their proof is omitted.

Case $a_i \geq 6$. Then $S(p_i,a_i)=c(p_i)p_i^{\frac{a_i^2}{4}}$ and

$$\frac{\partial S(p_i,a_i)}{\partial p_i}=c(p_i)\frac{a_i^2}{4}p_i^{\frac{a_i^2}{4}-1}+\frac{\partial c(p_i)}{\partial p_i}p_i^{\frac{a_i^2}{4}}\leq c(p_i)\frac{a_i^2}{4}p_i^{\frac{a_i^2}{4}-1},$$

because $c(p_i)$ is a strictly decreasing function. Thus, from (A.4), we deduce

$$p_i(\log r)^2\frac{\partial f(r)}{\partial p_i}\geq -a_i\log c(2)+\frac{a_i(\log r)^2}{4\log 2}-\frac{a_i^2}{4}\log r+a_i\log S(p_i,a_i)-(\ell-2)a_i\log 2.$$

Using (A.6), we deduce

$$\begin{aligned} p_i(\log r)^2\frac{\partial f(r)}{\partial p_i} &\geq -a_i\log(c(2)/4)+\frac{a_i(\log r)^2}{4\log 2}-\frac{a_i^2}{4}\log r+a_i\log S(p_i,a_i)-a_i\log r \qquad (A.7)\\ &\geq \frac{a_i(\log r)^2}{4\log 2}-\frac{a_i^2}{4}\log r-a_i\log r, \end{aligned}$$

where in the last inequality we are using $S(p_i,a_i)\geq S(2,6)\geq 2^9$ and hence $\log S(p_i,a_i)\geq \log(c(2)/4)$. Therefore,

$$\frac{p_i\log r}{a_i}\frac{\partial f(r)}{\partial p_i}\geq \frac{\log r}{4\log 2}-\frac{a_i}{4}-1. \qquad (A.8)$$

When $p_i\geq 3$, we have $r\geq 3^{a_i}\cdot 2\cdot 5$, because $\ell\geq 3$. Hence $\log r\geq a_i\log 3+\log 10$. Therefore,

$$\frac{\log r}{4\log 2}\geq \frac{a_i\log 3}{4\log 2}+\frac{\log 10}{4\log 2}.$$

This inequality and the fact that $a_i \geq 6$ show that (A.8) is satisfied and hence $\partial f(r)/\partial p_i \geq 0$. Assume then $p_i = 2$. When $r/2^{a_i} > 15$, we have $\log r \geq a_i \log 3 + \log 16$. Therefore,

$$\frac{\log r}{4\log 2} \geq \frac{a_i}{4} + \frac{\log 16}{4\log 2} = \frac{a_i}{4} + 1$$

and hence (A.8) shows that $\partial f(r)/\partial p_i \geq 0$. Finally, when $p_i = 2$ and $r/2^{a_i} < 16$, we must have $r = 2^{a_i} \cdot 3 \cdot 5$, because $\ell \geq 3$. In this particular case, we may refine the computations in (A.7). Indeed, by repeating the same steps except by replacing $S(p_i, a_i)$ with $c(2)2^{a_i^2/4}$, we have

$$\begin{aligned} p_i(\log r)^2 \frac{\partial f(r)}{\partial p_i} &\geq -a_i \log c(2) + \frac{a_i(\log r)^2}{4\log 2} - \frac{a_i^2}{4}\log r + a_i \log S(p_i, a_i) - (\ell - 2)a_i \log 2 \\ &\geq -a_i \log c(2) + \frac{a_i(\log r)^2}{4\log 2} - \frac{a_i^2}{4}\log r + a_i \log c(2) \\ &\quad + \frac{a_i^3}{4}\log 2 - a_i \log r + 4\log 2 \\ &\geq \frac{a_i(\log r)^2}{4\log 2} + \frac{a_i^3}{4}\log 2 - \frac{a_i^2}{4}\log r - a_i \log r. \end{aligned} \tag{A.9}$$

Therefore,

$$\frac{p_i \log r}{a_i}\frac{\partial f(r)}{\partial p_i} \geq \frac{\log r}{4\log 2} + \frac{a_i^2}{4}\frac{\log 2}{\log r} - \frac{a_i}{4} - 1.$$

It is now clear that also in this case $\partial f(r)/\partial p_i \geq 0$.

Proof of Lemma 4.1. We have proved that the directional derivative $\partial/\partial p_i$ of $f(r)$ is positive. Since r is good, we have $f(r) > 0$. Therefore, as $p' > p_i$, $f(r') \geq f(r) > 0$ and r' is also good. □

A.3. Increasing the number of prime factors and proof of Lemma 4.2

Let p be a prime number with $p \notin \{p_1, \dots, p_\ell\}$ and let $r' = r \cdot p$. Observe that r has ℓ distinct prime factors, whereas r' has $\ell + 1$ distinct prime factors. We have

$$\begin{aligned} f(r') - f(r) &= \log c(2)\left(\frac{1}{\log r'} - \frac{1}{\log r}\right) + \frac{\log p}{4\log 2} - \frac{\log 2}{\log r'} \\ &\quad - \sum_{i=1}^{\ell} \log S(p_i, a_i)\left(\frac{1}{\log r'} - \frac{1}{\log r}\right) - 1 + (\ell - 1)\frac{\log 2}{\log r'} - (\ell - 2)\frac{\log 2}{\log r} \\ &= -\frac{\log c(2)\log p}{\log r \log r'} + \frac{\log p}{4\log 2} - \sum_{i=1}^{\ell} \log S(p_i, a_i)\left(\frac{1}{\log r'} - \frac{1}{\log r}\right) \end{aligned}$$

$$\begin{aligned}
&\quad -1+(\ell-2)\frac{\log 2}{\log r'}-(\ell-2)\frac{\log 2}{\log r}\\
&=-\frac{\log c(2)\log p}{\log r\log r'}+\frac{\log p}{4\log 2}+\left(\sum_{i=1}^{\ell}\log S(p_i,a_i)\right)\frac{\log p}{\log r\log r'}\\
&\quad -1-(\ell-2)\frac{\log 2\log p}{\log r\log r'}.
\end{aligned}$$

Now, when $i\geq 2$, we have $S(p_i,a_i)\geq 2$ and hence $\log S(p_i,a_i)\geq \log 2$. Similarly, when $i=1$, we have $p_1=2$ and $a_1\geq 2$ by (4.2); hence $S(p_i,a_i)\geq S(2,2)=5\geq 4$; thus $\log S(p_i,a_i)\geq 2\log 2$. Taking this into account, we obtain

$$\begin{aligned}
f(r')-f(r)&\geq -\frac{\log c(2)\log p}{\log r\log r'}+\frac{\log p}{4\log 2}+\frac{(\ell+1)\log 2\log p}{\log r\log r'}-1-(\ell-2)\frac{\log 2\log p}{\log r\log r'}\\
&=-\frac{\log c(2)\log p}{\log r\log r'}+\frac{\log p}{4\log 2}+\frac{3\log 2\log p}{\log r\log r'}-1\geq\frac{\log p}{4\log 2}-1,
\end{aligned}$$

where in the last inequality we have used $8>c(2)$, that is, $3\log 2\geq\log c(2)$.

Proof of Lemma 4.2. As $p\geq 17$, we have $\log p/(4\log 2)-1\geq 0$. Therefore, $f(r')-f(r)\geq \log p/(4\log 2)-1\geq 0$. Since r is good, we have $f(r)>0$. Thus $f(r')>0$ and r' is good. □

A.4. Increasing the multiplicity of a prime

Let $i\in\{1,\dots,\ell\}$. We think of a_i as a continuous variable and we compute $\partial\mathtt{f}(r)/\partial a_i$. We are interested in showing $\partial\mathtt{f}(r)/\partial a_i\geq 0$, where $f(r)=f(a_1,\dots,a_\ell)$ is thought as a function of $a_1,\dots,a_\ell$ with $p_1,\dots,p_\ell$ being fixed. From this Lemma 4.3 immediately follows.

We have

$$\begin{aligned}
\frac{\partial\mathtt{f}(r)}{\partial a_i}&=-\frac{\log p_i\log c(2)}{(\log r)^2}+\frac{\log p_i}{4\log 2}-\frac{a_i\log p_i}{2\log r}\\
&\quad+\frac{\log p_i\log(c(p_i)p_i^{a_i^2/4})}{(\log r)^2}-(\ell-2)\frac{\log 2\log p_i}{(\log r)^2}.
\end{aligned}$$

Multiplying this by $(\log r)^2$, we obtain

$$\begin{aligned}
(\log r)^2\frac{\partial\mathtt{f}(r)}{\partial a_i}&=-\log p_i\log c(2)+\frac{\log p_i}{4\log 2}(\log r)^2-\frac{a_i\log p_i}{2}\log r\\
&\quad+\log p_i\log(c(p_i)p_i^{a_i^2/4})-(\ell-2)\log 2\log p_i.
\end{aligned}\tag{A.10}$$

In particular, using (A.6) and $c(p_i)\geq 1$, we get

$$\frac{(\log r)^2}{\log p_i}\frac{\partial \mathtt{f}(r)}{\partial a_i} \geq -\log(c(2)/4) + \frac{(\log r)^2}{4\log 2} - \frac{a_i}{2}\log r + \frac{a_i^2 \log p_i}{4} - \log r. \tag{A.11}$$

Write $r = p_i^{a_i} r'$. Replacing r in (A.11) with $p_i^{a_i} r'$, we obtain

$$\begin{aligned}\frac{(\log r)^2}{\log p_i}\frac{\partial \mathtt{f}(r)}{\partial a_i} &\geq -\log(c(2)/4) + \frac{a_i^2(\log p_i)^2}{4\log 2} + \frac{(\log r')^2}{4\log 2} + \frac{a_i \log p_i \log r'}{2\log 2} \\ &\quad - \frac{a_i^2 \log p_i}{2} - \frac{a_i \log r'}{2} + \frac{a_i^2 \log p_i}{4} - a_i \log p_i - \log r' \\ &= \left(-\log(c(2)/4) + \frac{(\log r')^2}{4\log 2} - \log r'\right) + \left(\frac{a_i^2(\log p_i)^2}{4\log 2} - \frac{a_i^2 \log p_i}{4}\right) \\ &\quad + \frac{a_i \log p_i \log r'}{2\log 2} - \frac{a_i \log r'}{2} - a_i \log p_i.\end{aligned}$$

Now, $\log p_i \geq \log 2$ and hence

$$\frac{a_i^2(\log p_i)^2}{4\log 2} - \frac{a_i^2 \log p_i}{2} + \frac{a_i^2 \log p_i}{4} \geq 0.$$

Assume, for the time being, $p_i \geq 3$ and $r' \geq 27$. If we set $x := \log r'$, then

$$-\log(c(2)/4) + \frac{(\log r')^2}{4\log 2} - \log r' = -\log(c(2)/4) + \frac{x^2}{4\log 2} - x$$

is a parabola and it is not hard to verify that it is positive when $r' \geq 27$. Furthermore,

$$\frac{a_i \log p_i \log r'}{2\log 2} - \frac{a_i \log r'}{2} - a_i \log p_i \geq a_i \left(\frac{\log 3 \log r'}{2\log 2} - \frac{r'}{2} - \log 3\right) \geq 0,$$

where in the last inequality we are using again $r' \geq 27$. In particular, we have shown that $\partial \mathtt{f}(r)/\partial a_i \geq 0$, provided that $r' \geq 27$ and $p_i \geq 3$.

Assume now $p_i = 2$. Thus $i = 1$ and $r = 2^{a_1} r'$. By specializing (A.10) with $p_i = 2$ and by using $\log r = a_1 \log 2 + \log r'$, we obtain

$$\begin{aligned}\frac{(\log r)^2}{\log 2}\frac{\partial \mathtt{f}(r)}{\partial a_i} &= -\log c(2) + \frac{(\log r)^2}{4\log 2} - \frac{a_i \log r}{2} + \log c(2) + \frac{a_i^2 \log 2}{4} - (\ell - 2)\log 2 \\ &= \frac{(\log r)^2}{4\log 2} - \frac{a_i \log r}{2} + \frac{a_i^2 \log 2}{4} - (\ell - 2)\log 2 \\ &= \frac{a_1^2 \log 2}{4} + \frac{(\log r')^2}{4\log 2} + \frac{a_1 \log r'}{2} - \frac{a_1^2 \log 2}{2} - \frac{a_1 \log r'}{2} \\ &\quad + \frac{a_1^2 \log 2}{4} - (\ell - 2)\log 2 \\ &= \frac{(\log r')^2}{4\log 2} - (\ell - 2)\log 2.\end{aligned}$$

Now, $r' = p_2^{a_2} \cdots p_\ell^{a_\ell}$ with $p_2, \dots, p_\ell \geq 3$ and hence $\log r' \geq \ell - 1$. We deduce

$$\frac{(\log r)^2}{\log 2} \frac{\partial \mathtt{f}(r)}{\partial a_i} \geq \frac{(\log r')^2}{4 \log 2} - (\log r' - 1) \log 2.$$

The expression appearing on the right hand side is a parabola in $x := \log r'$ and it is not hard to verify that it is positive. Therefore, $\partial \mathtt{f}(r)/\partial a_i \geq 0$ also in this case.

Finally, suppose $p_i \geq 3$ and $r' < 27$. Since the product of three distinct primes is at least 30, we deduce $\ell = 3$. Assume, $r' \geq 10$. By specializing (A.10) with $\ell = 3$ and by using

$$a_i \log p_i + \log 10 \leq \log r = a_i \log p_i + \log r' \leq a_i \log p_i + \log 26,$$

we obtain

$$\begin{aligned}
\frac{(\log r)^2}{\log p_i} \frac{\partial \mathtt{f}(r)}{\partial a_i} &= -\log c(2) + \frac{(\log r)^2}{4 \log 2} - \frac{a_i \log r}{2} + \frac{a_i^2 \log p_i}{4} - \log 2 \\
&= -\log(c(2)/2) + \frac{(\log r)^2}{4 \log 2} - \frac{a_i \log r}{2} + \frac{a_i^2 \log p_i}{4} \\
&\geq -\log(c(2)/2) + \frac{a_i^2 (\log p_i)^2}{4 \log 2} + \frac{(\log 10)^2}{4 \log 2} + \frac{a_i \log p_i \log 10}{2 \log 2} \\
&\quad - \frac{a_i^2 \log p_i}{2} - \frac{a_i \log 26}{2} + \frac{a_i^2 \log p_i}{4} \\
&= -\log(c(2)/2) + \frac{a_i^2 (\log p_i)^2}{4 \log 2} + \frac{(\log 10)^2}{4 \log 2} + \frac{a_i \log p_i \log 10}{2 \log 2} \\
&\quad - \frac{a_i^2 \log p_i}{4} - \frac{a_i \log 26}{2} \\
&\geq \frac{a_i^2 (\log p_i)^2}{4 \log 2} + \frac{a_i \log p_i \log 10}{2 \log 2} - \frac{a_i^2 \log p_i}{4} - \frac{a_i \log 26}{2},
\end{aligned}$$

where the last inequality follows because $-\log(c(2)/2) + (\log 10)^2/(4 \log 2) > 0$. Observe that

$$\frac{a_i^2 (\log p_i)^2}{4 \log 2} - \frac{a_i^2 \log p_i}{4} = \frac{a_i^2 \log p_i}{4} \left(\frac{\log p_i}{\log 2} - 1 \right) \geq 0,$$

because $p_i \geq 3$. Observe also that

$$\frac{a_i \log p_i \log 10}{2 \log 2} - \frac{a_i \log 26}{2} = \frac{a_i}{2} \left(\frac{\log p_i \log 10}{\log 2} - \log 26 \right) \geq 0,$$

because $p_i \geq 3$. Therefore $\partial \mathtt{f}(r)/\partial a_i \geq 0$ in this case. It remains to consider the case $r' < 10$. Since $\ell = 3$, r' is the product of two distinct primes and hence $r' = 6$. In other

words, $i = \ell = 3$ and $r = 2 \cdot 3 \cdot p_i^{a_i}$. By repeating the computations above with this value of r and r', we obtain

$$\begin{aligned}\frac{(\log r)^2}{\log p_i}\frac{\partial \mathtt{f}(r)}{\partial a_i} &= -\log(c(2)/2) + \frac{(\log r)^2}{4\log 2} - \frac{a_i \log r}{2} + \frac{a_i^2 \log p_i}{4} \\ &\geq -\log(c(2)/2) + \frac{a_i^2(\log p_i)^2}{4\log 2} + \frac{(\log 6)^2}{4\log 2} + \frac{a_i \log p_i \log 6}{2\log 2} \\ &\quad - \frac{a_i^2 \log p_i}{2} - \frac{a_i \log 6}{2} + \frac{a_i^2 \log p_i}{4} \\ &= -\log(c(2)/2) + \frac{a_i^2(\log p_i)^2}{4\log 2} + \frac{(\log 6)^2}{4\log 2} + \frac{a_i \log p_i \log 6}{2\log 2} \\ &\quad - \frac{a_i^2 \log p_i}{4} - \frac{a_i \log 6}{2}.\end{aligned}$$

Now, using $a_i \geq 1$ and $p_i \geq 5$, we have

$$\frac{a_i \log p_i \log 6}{2\log 2} - \frac{a_i \log 6}{2} = \frac{a_i \log 6}{2}\left(\frac{\log p_i}{\log 2} - 1\right) \geq \frac{a_i \log 6}{2} \geq \frac{\log 6}{2}.$$

Therefore,

$$\begin{aligned}\frac{(\log r)^2}{\log p_i}\frac{\partial \mathtt{f}(r)}{\partial a_i} &\geq -\log(c(2)/2) + \frac{\log 6}{2} + \frac{(\log 6)^2}{4\log 2} + \frac{a_i^2(\log p_i)^2}{4\log 2} - \frac{a_i^2 \log p_i}{4} \\ &\geq \frac{a_i^2(\log p_i)^2}{4\log 2} - \frac{a_i^2 \log p_i}{4} = \frac{a_i^2 \log p_i}{4}\left(\frac{\log p_i}{\log 2} - 1\right) \geq 0,\end{aligned}$$

where the second inequality follows with a calculation and the third inequality follows because $p_i \geq 5$.

Proof of Lemma 4.3. From above $\partial \mathtt{f}/\partial a_i \geq 0$. Thus if $\mathtt{f}(r) > 0$, then $\mathtt{f}(r') = \mathtt{f}(r \cdot p_i) \geq \mathtt{f}(r) > 0$ and hence r' is `good`. □

A.5. Proof of Lemma 5.2

We start by proving part (1). As $r \geq 2\,000$, we have

$$\begin{aligned}(r/14)^{\frac{\log_2(r/14)}{4}} &= 2^{-\frac{\log_2(r/14)}{4}}(r/7)^{\frac{\log_2(r/14)}{4}} \leq 2^{-\frac{\log_2(2\,000/14)}{4}}(r/7)^{\frac{\log_2(r/14)}{4}} \\ &= 2^{-\frac{\log_2(2\,000/14)}{4}}(r/7)^{-\frac{1}{4}}(r/7)^{\frac{\log_2(r/7)}{4}} \\ &\leq 2^{-\frac{\log_2(2\,000/14)}{4}}(2\,000/7)^{-\frac{1}{4}}(r/7)^{\frac{\log_2(r/7)}{4}} \\ &\leq 2^{-3}(r/7)^{\frac{\log_2(r/7)}{4}},\end{aligned}$$

where the last inequality follows with a computation. Therefore,

$$\begin{aligned} 4r(r/7)^{\frac{\log_2(r/7)}{4}} + 8r(r/14)^{\frac{\log_2(r/14)}{4}} &\leq 5r(r/7)^{\frac{\log_2(r/7)}{4}} < 5 \cdot 2^{\log_2(r)} \cdot 2^{\frac{(\log_2(r/7))^2}{4}} \\ &= 2^{\frac{(\log_2(r/7))^2}{4} + \log_2(r) + \log_2(5)}. \end{aligned}$$

Similarly, $r^{\log_2(r)/4} = 2^{(\log_2(r))^2/4}$. We show that

$$\frac{(\log_2(r/7))^2}{4} + \log_2(r) + \log_2(5) \leq \frac{(\log_2(r))^2}{4}, \tag{A.12}$$

from which (1) immediately follows. Rearranging the summands in (A.12) and using $\log_2(r/7) = \log_2(r) - \log_2(7)$, we obtain the equivalent inequality

$$\left(\frac{\log_2(7)}{2} - 1\right) \log_2(r) \geq \log_2(5) + \frac{(\log_2(7))^2}{4},$$

that is,

$$\log_2(r) \geq \frac{\log_2(5) + \frac{(\log_2(7))^2}{4}}{\frac{\log_2(7)}{2} - 1} = 10.63. \tag{A.13}$$

As $r \geq 2\,000$, we have $\log_2(r) \geq 10.96$ and hence (A.13) is satisfied.

We prove part (2). We have

$$\begin{aligned} 8r(r/28)^{\frac{\log_2(r/28)}{4}} + 6r(r/21)^{\frac{\log_2(r/21)}{4}} + 4r(r/14)^{\frac{\log_2(r/14)}{4}} &\leq 8r(r/14)^{\frac{\log_2(r/14)}{4}} \\ &\quad + 6r(r/14)^{\frac{\log_2(r/14)}{4}} \\ &\quad + 4r(r/14)^{\frac{\log_2(r/14)}{4}} \\ &= 18r(r/14)^{\frac{\log_2(r/14)}{4}} \\ &= 2^{\frac{(\log_2(r/14))^2}{4} + \log_2(r) + \log_2(18)}. \end{aligned}$$

As above, we use the fact that $r^{\log_2(r)/4} = 2^{(\log_2(r))^2/4}$. We show that

$$\frac{(\log_2(r/14))^2}{4} + \log_2(r) + \log_2(18) \leq \frac{(\log_2(r))^2}{4}, \tag{A.14}$$

from which (2) immediately follows. Rearranging the summands in (A.14) and using $\log_2(r/14) = \log_2(r) - \log_2(14)$, we obtain the equivalent inequality

$$\left(\frac{\log_2(14)}{2} - 1\right) \log_2(r) \geq \log_2(18) + \frac{(\log_2(14))^2}{4},$$

that is,

$$\log_2(r) \geq \frac{\log_2(18) + \frac{(\log_2(14))^2}{4}}{\frac{\log_2(14)}{2} - 1} = 8.62. \tag{A.15}$$

As $\log_2(r) \geq 10.96$, (A.15) is satisfied.

We prove part (3). As $r \geq 2\,000$, we have

$$\begin{aligned}(r/10)^{\frac{\log_2(r/10)}{4}} &= 2^{-\frac{\log_2(r/10)}{4}}(r/5)^{\frac{\log_2(r/10)}{4}} \leq 2^{-\frac{\log_2(2\,000/10)}{4}}(r/5)^{\frac{\log_2(r/10)}{4}} \\ &= 2^{-\frac{\log_2(200)}{4}}(r/5)^{-\frac{1}{4}}(r/5)^{\frac{\log_2(r/5)}{4}} \leq 2^{-\frac{\log_2(200)}{4}}(2\,000/5)^{-\frac{1}{4}}(r/5)^{\frac{\log_2(r/5)}{4}} \\ &\leq 2^{-4}(r/5)^{\frac{\log_2(r/5)}{4}},\end{aligned}$$

where the last inequality follows with a computation. Therefore,

$$\begin{aligned}(2r+10)(r/10)^{\frac{\log_2(r/10)}{4}} + (r/5+5)(r/5)^{\frac{\log_2(r/5)}{4}} &\leq \left(\frac{13}{40}r + \frac{45}{8}\right)(r/5)^{\frac{\log_2(r/5)}{4}} \\ &\leq 2^{-1}r(r/5)^{\frac{\log_2(r/5)}{4}}.\end{aligned}$$

Recall $r^{\log_2(r)/4} = 2^{(\log_2(r))^2/4}$. We show that

$$-1 + \log_2(r) + \frac{(\log_2(r/5))^2}{4} \leq \frac{(\log_2(r))^2}{4}, \tag{A.16}$$

from which (3) immediately follows. Rearranging the summands in (A.16) and using $\log_2(r/5) = \log_2(r) - \log_2(5)$, we obtain the equivalent inequality

$$\left(\frac{\log_2(5)}{2} - 1\right)\log_2(r) \geq \frac{(\log_2(5))^2}{4} - 1,$$

that is,

$$\log_2(r) \geq \frac{-1 + \frac{(\log_2(5))^2}{4}}{-1 + \frac{\log_2(5)}{2}} = \frac{\log_2(5)}{2} + 1 = 2.16. \tag{A.17}$$

As $r \geq 2\,000$, we have $\log_2(r) \geq 10.96$ and hence (A.17) is satisfied.

We prove part (4). We have

$$2p(r/p)^{\log_2(r/p)} = 2^{1+\log_2(p)+\frac{(\log_2(r/p))^2}{4}} = 2^{1+\log_2(r)+\frac{(\log_2(r))^2}{4}+\frac{(\log_2(p))^2}{4}-\frac{\log_2(p)\log_2(r)}{2}}.$$

Therefore, (4) is equivalent to the inequality

$$1 + \log_2(r) + \frac{(\log_2(r))^2}{4} + \frac{(\log_2(p))^2}{4} - \frac{\log_2(p)\log_2(r)}{2} \leq \frac{(\log_2(r))^2}{4}.$$

In turn, this is equivalent to

$$\left(\frac{\log_2(p)}{2} - 1\right) \log_2(r) \geq \frac{(\log_2(p))^2}{4} + 1,$$

that is,

$$\log_2(r) \geq \frac{1 + \frac{(\log_2(p))^2}{4}}{-1 + \frac{\log_2(p)}{2}} \geq \frac{\log_2(p)}{2} + 1. \tag{A.18}$$

As $r \geq 2p$, we have $\log_2(r) \geq \log_2(p) + 1$ and hence (A.18) is satisfied.

References

[1] A. Ballester-Bolinches, R. Esteban-Romero, P. Jimènez-Seral, Bounds on the number of maximal subgroups of finite groups: applications, Mathematics 10 (2022) 1–25.
[2] A.V. Borovik, L. Pyber, A. Shalev, Maximal subgroups in finite and profinite groups, Trans. Am. Math. Soc. 348 (1996) 3745–3761.
[3] Y. Bugeaud, Z. Cao Zhenfu, M. Mignotte, On simple K_4-groups, J. Algebra 241 (2001) 658–668.
[4] C. Bosma, J. Cannon, C. Playoust, The magma algebra system. I. The user language, J. Symb. Comput. 24 (1997) 235–265.
[5] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, An ATLAS of Finite Groups, Oxford University Press, Eynsham, 1985.
[6] R.M. Guralnick, G. Malle, G. Navarro, Self-normalizing Sylow subgroups, Proc. Am. Math. Soc. 132 (4) (2004) 973–979.
[7] M.W. Liebeck, L. Pyber, A. Shalev, On a conjecture of G. E. Wall, J. Algebra 317 (2007) 184–197.
[8] A. Shalev, Growth functions, p-adic analytic groups, and groups of finite coclass, J. Lond. Math. Soc. (2) 46 (1992) 111–122.
[9] P. Spiga, An explicit upper bound on the number of subgroups of a finite group, J. Pure Appl. Algebra 227 (2023), https://doi.org/10.1016/j.jpaa.2022.107312.