

Document downloaded from:

<http://hdl.handle.net/10251/186784>

This paper must be cited as:

Hauck, P.; Kazarin, LS.; Martínez-Pastor, A.; Pérez-Ramos, MD. (2021). Thompson-like characterization of solubility for products of finite groups. *Annali di Matematica Pura ed Applicata* (1923 -). 200(1):337-362. <https://doi.org/10.1007/s10231-020-00998-z>



The final publication is available at

<https://doi.org/10.1007/s10231-020-00998-z>

Copyright Springer-Verlag

Additional Information

Thompson-like characterization of solubility for products of finite groups

P. Hauck · L. S. Kazarin ·
A. Martínez-Pastor · M. D. Pérez-Ramos

Dedicated to the memory of M. Pilar Gállego (1958-2019)

Abstract A remarkable result of Thompson states that a finite group is soluble if and only if all its two-generated subgroups are soluble. This result has been generalized in numerous ways, and it is in the core of a wide area of research in the theory of groups, aiming for global properties of groups from local properties of two-generated (or more generally, n -generated) subgroups. We contribute an extension of Thompson's theorem from the perspective of factorized groups. More precisely, we study finite groups $G = AB$ with subgroups A, B such that $\langle a, b \rangle$ is soluble for all $a \in A$ and $b \in B$. In this case, the group G is said to be an \mathcal{S} -connected product of the subgroups A and B for the class \mathcal{S} of all finite soluble groups. Our main theorem states that $G = AB$ is \mathcal{S} -connected if and only if $[A, B]$ is soluble. In the course of the proof we derive a result about independent primes regarding the soluble graph of almost simple groups that might be interesting in its own right.

Keywords Solubility · Products of subgroups · Two-generated subgroups · \mathcal{S} -connection · Almost simple groups · Independent primes

Mathematics Subject Classification (2010) 20D40 · 20D10

Research supported by Proyectos PROMETEO/2017/057 from the Generalitat Valenciana (Valencian Community, Spain), and PGC2018-096872-B-I00 from the Ministerio de Ciencia, Innovación y Universidades, Spain, and FEDER, European Union; and second author also by Project VIP-008 of Yaroslavl P. Demidov State University.

P. Hauck

Fachbereich Informatik, Universität Tübingen, Sand 13, 72076 Tübingen, Germany

E-mail: peter.hauck@uni-tuebingen.de

L. S. Kazarin

Department of Mathematics, Yaroslavl P. Demidov State University, Sovetskaya Str 14, 150014 Yaroslavl, Russia. ORCID iD: 0000-0003-1836-0955 E-mail: Kazarin@uniyar.ac.ru

A. Martínez-Pastor

Instituto Universitario de Matemática Pura y Aplicada (IUMPA-UPV), Universitat Politècnica de València, Camino de Vera s/n, 46022 Valencia, Spain. ORCID iD: 0000-0002-0208-4098

E-mail: anamarti@mat.upv.es

M. D. Pérez-Ramos

Departament de Matemàtiques, Universitat de València, C/ Doctor Moliner 50, 46100 Burjassot (València), Spain. ORCID iD: 0000-0003-0173-2759

E-mail: Dolores.Perez@uv.es

1 Introduction

Our work arises from the confluence of two major areas of study in group theory. On the one hand, what we might call local-global theory, and on the other hand, the theory of products of groups.

Regarding the first one, the interest lies in the influence on the global structure of a group of local properties on its elements, either by satisfying explicit relations or formulas or by their generation properties. Classical Burnside problems might be traced to the origin of this theory. We paraphrase here F. Grunewald, B. Kunyavskii and E. Plotkin in [28], which provides a valuable reference on the topic. Widely speaking, one can say that classical Burnside problems ask to what extent finiteness of cyclic subgroups (i.e. generated by one element) determines finiteness of arbitrary finitely generated subgroups of a group. We are interested in the influence of two-generated subgroups on the structure of finite groups. First results in this direction by M. Zorn [41] and R. Baer [6] show that nilpotency and supersolubility, respectively, of a finite group is determined by the same corresponding property of its two-generated subgroups. Undoubtedly one of the most influential results is the one of J. Thompson regarding solubility.

Theorem (Thompson, [39]) *A finite group G is soluble if and only if every two-generated subgroup of G is soluble.*

This result has been generalized and sharpened in various ways. In addition to the above-mentioned reference, we cite for instance [16, 23–27, 37], some of whose results have been applied to prove the results in this paper. As a typical example we mention the following theorem of R. Guralnick, K. Kunyavskii, E. Plotkin and A. Shalev.

Theorem (Guralnick, Kunyavskii, Plotkin, Shalev, [27]) *Let G be a finite group, let $G_{\mathcal{S}}$ denote the soluble radical of G (i.e. the largest soluble normal subgroup of G) and let $x \in G$. Then $x \in G_{\mathcal{S}}$ if and only if the subgroup $\langle x, y \rangle$ is soluble for all $y \in G$.*

In the theory of products of groups, the aim is to seek for information about the structure of a factorized group from the subgroups in the factorization (and vice versa). The well-known theorem by Kegel and Wielandt, about the solubility of a finite group which is the product of nilpotent subgroups, is probably one of the most remarkable results in the area. It is also known that the product of two finite supersoluble subgroups is not necessarily supersoluble, even if the factors are normal subgroups. This fact has motivated the search for conditions to obtain positive results and, at the time, has been the source of a vast line of research on factorized finite groups whose factors are linked by some particular property. Originally M. Asaad and A. Shaalan in [5] introduced totally permutable products of subgroups, which can be seen as extension of central products. A group $G = AB$ is a central product of subgroups A and B if $ab = ba$, for all $a \in A$ and $b \in B$; equivalently, $\langle a, b \rangle$ is abelian, for all $a \in A$ and $b \in B$. The subgroups A and B are said to be totally permutable if every subgroup of A permutes with every subgroup of B ; equivalently, $\langle a \rangle \langle b \rangle = \langle b \rangle \langle a \rangle$, for all $a \in A$ and $b \in B$. R. Maier notes in [36] that for such subgroups, $\langle a, b \rangle = \langle a \rangle \langle b \rangle = \langle b \rangle \langle a \rangle$ is supersoluble, for all $a \in A$ and $b \in B$, which led to the following connection property:

Definition 1 (Carocca, [11]) Let \mathcal{L} be a non-empty class of groups. Subgroups A and B of a group G are \mathcal{L} -connected if $\langle a, b \rangle \in \mathcal{L}$ for all $a \in A$ and $b \in B$.

For the special case when $G = AB = A = B$ this means of course that $\langle a, b \rangle \in \mathcal{L}$ for all $a, b \in G$, and the study of products of \mathcal{L} -connected subgroups provides a more general setting for local-global questions related to two-generated subgroups. We refer to [8, 29, 9] for previous studies for the class $\mathcal{L} = \mathcal{N}$ of finite nilpotent groups, and to [18–21] for \mathcal{L} being the class of finite metanilpotent groups and other relevant classes of groups. For the class $\mathcal{L} = \mathcal{S}$ of finite soluble groups, A. Carocca in [12] proved the solubility of a product of \mathcal{S} -connected soluble subgroups, which provides a first extension of the above-mentioned theorem of Thompson for products of groups (see Corollary 2).

All groups considered in this paper are assumed to be finite. Unless otherwise specified, we shall adhere to the notation used in [15] and we refer also to that book for the basic results on classes of groups. In particular, $G_{\mathcal{S}}$ denotes the soluble radical of a group G as mentioned before. In addition, if n is a positive integer, then $\pi(n)$ denotes the set of primes dividing n ; and $\pi(H) = \pi(|H|)$ for any group H .

The main result in this paper is the following:

Main Theorem. *Let the finite group $G = AB$ be the product of subgroups A and B . Then the following statements are equivalent:*

- (1) A, B are \mathcal{S} -connected.
- (2) For all primes $p \neq q$, all p -elements $a \in A$ and all q -elements $b \in B$, $\langle a, b \rangle$ is soluble.
- (3) $[A, B] \leq G_{\mathcal{S}}$.

The configuration of a minimal counterexample to the Main Theorem is proven to be an almost simple group, i.e. a group G such that $N \trianglelefteq G \leq \text{Aut}(N)$ for some non-abelian simple group N , where $\text{Aut}(N)$ denotes the automorphism group of N . As a major previous result, in Section 2 we prove Theorem 1, which deals with an almost simple group which is the product of subgroups satisfying condition (2) of the Main Theorem. A stronger version of Theorem 1 is stated in Corollary 1 as a consequence of our main theorem. A remarkable result deduced from the checking carried out for the proof of Theorem 1 is stated in Theorem 2 and has to do with the existence of *independent primes* in almost simple groups.

For a group G the Grünberg-Kegel or prime graph $\Gamma(G)$ of G is well-known. It consists of the set of vertices $V(\Gamma(G)) = \pi(G)$ and the set of edges $(p, q) \in \pi(G) \times \pi(G)$ such that there is an element of order pq in G . S. Abe and N. Iiyori introduced in [1] the soluble graph $\Gamma_{\text{sol}}(G)$ which has the same set of vertices as $\Gamma(G)$, but two vertices $p, q \in \pi(G)$ are adjacent if G contains a soluble subgroup of order divisible by pq . Iiyori [33], B. Amberg, A. Carocca and L. Kazarin [2], and Amberg and Kazarin [4] take further the study of the soluble graph specially for non-abelian finite simple groups. In [4] the authors are concerned with subsets $I \subseteq \pi(G)$ such that no pair of vertices in I is adjacent with respect to $\Gamma(G)$ or $\Gamma_{\text{sol}}(G)$, respectively, called *independent sets* of the corresponding graph. This leads to the following main concept for our purposes.

Definition 2 Given a finite group H , we call two prime divisors p and q of $|H|$ *independent* (with respect to H), if H contains no soluble subgroup whose order is divisible by pq .

For an almost simple group $G = AB$ with non-abelian socle N , not contained in either A or B , and except for a few exceptions, we state in Theorem 2, and

in the subsequent Remark, the existence of independent primes with respect to N , one dividing $|A \cap N|$, the other one dividing $|B \cap N|$, derived from the proof of Theorem 1. We also prove that apart from some additional exceptions the existence of such independent primes with respect to $\text{Aut}(N)$ remains true.

It is clear that the Main Theorem extends the above-mentioned theorems of Thompson [39] and Carocca [12]. It also implies the theorem of Guralnick, Kunyavskii, Plotkin and Shalev [27] stated above (with $A = G$, $B = \langle x \rangle$; note that $\langle x \rangle G_{\mathcal{S}}$ is a normal (soluble) subgroup of G by the Main Theorem). However, it is to be emphasized that we make use of this result in the proof of the Main Theorem. Section 3 is devoted to prove our main result and to state some first consequences. In particular, Corollary 2 generalizes Carocca's result via the soluble radical in a product of \mathcal{S} -connected subgroups. In a forthcoming paper [17], our theorem is applied to extend main results known for finite soluble groups in [18–20] to the universe of all finite groups.

2 The case of almost simple groups

The aim of this section is the proof of the following result:

Theorem 1 *Let N be a non-abelian simple group and $N \leq G = AB \leq \text{Aut}(N)$ with subgroups A and B satisfying condition (2) of the Main Theorem, $AN = BN = G$. Then $A = G$ or $B = G$.*

In Corollary 1 we will see, as a consequence of the Main Theorem, that the assumption $AN = BN = G$ in the preceding result is not necessary and that actually $A = 1$ or $B = 1$ holds.

Occasionally, the following lemma will be useful (cf. [3, Lemma 1.3.1]).

Lemma 1 *Let $G = AB$ be a group with subgroups A, B satisfying condition (2) of the Main Theorem. If $g, h \in G$, then $G = A^g B^h$ and A^g, B^h also satisfy condition (2) of the Main Theorem.*

Proof Let $g = a_1 b_1$, $h = b_2 a_2$, $b_1 a_2^{-1} = a_3 b_3$ with $a_1, a_2, a_3 \in A$, $b_1, b_2, b_3 \in B$. If $a \in A$ and $b \in B$, then $a^g = (a^{a_1 a_3})^{b_3 a_2}$ and $b^h = (b^{b_2 b_3^{-1}})^{b_3 a_2}$. The assertion follows. \square

Apart from the case of alternating groups our treatment in this section relies heavily on the classification of the maximal factorizations of almost simple groups by Liebeck, Praeger and Saxl [35] (and [30] for the exceptional groups of Lie type). We will also keep to their notation as close as possible.

In order to prove Theorem 1, we assume here that N is neither contained in A nor in B (for otherwise $A = G$ or $B = G$ and we are done). Our aim is to show that for all possible factorizations $G = AB$, with $N \not\leq A$ and $N \not\leq B$, the subgroups A and B do not satisfy condition (2) of the Main Theorem.

Since we have also to consider possibly non-maximal factorizations $G = AB$, we use the following notation:

Notation If $G = AB$ is as above, choose maximal subgroups $\tilde{A} \geq A$ and $\tilde{B} \geq B$, $N \not\leq \tilde{A}$ and $N \not\leq \tilde{B}$. Then $G = \tilde{A}\tilde{B}$ is a factorization of the type considered in [35]. Except for this \sim -notation we use the notation of [35], however with N instead of L .

We need the following simple lemma which follows from elementary order considerations. To formulate it, we denote for a positive integer n and a prime p by n_p the highest p -power dividing n , i.e. $n = n_p m$, $p \nmid m$.

Lemma 2 *Let $G = AB = AN = BN$ as in Theorem 1, p a prime. Then*

$$|A \cap N|_p \geq \frac{|N|_p}{|\tilde{B} \cap N|_p |\text{Out}(N)|_p}$$

and likewise with B and \tilde{A} .

Proof Since $G = \tilde{B}N = \tilde{B}A = AN$, we easily have:

$$\begin{aligned} \frac{|N|}{|\tilde{B} \cap N| |\text{Out}(N)|} &\leq \frac{|N|}{|\tilde{B} \cap N| |G/N|} = \frac{|N|}{|\tilde{B} \cap N| |\tilde{B}/(\tilde{B} \cap N)|} = \frac{|N|}{|\tilde{B}|} \\ &= \frac{|N||A|}{|G||\tilde{B} \cap A|} = \frac{|A \cap N|}{|\tilde{B} \cap A|} \leq |A \cap N|, \end{aligned}$$

and the result follows. \square

We state the outline of the proof of Theorem 1, and explain general arguments and strategies used to carry it out, though usually detailed checking work and easy calculations are omitted.

Strategies (S1) In our treatment of almost simple groups G (especially those of Lie type and the sporadic ones), we will usually determine two primes, one dividing $|A \cap N|$ and the other dividing $|B \cap N|$ that are independent with respect to the simple group N . The divisibility properties follow always from Lemma 2.

We remark that in sections 2.2 - 2.4 independence of primes is always meant with respect to N , even if not explicitly stated.

- (S2) For certain small groups the independency of two primes can be deduced from the subgroup structure given in [10] or [13].
- (S3) The following observation is sometimes helpful: Given a factorization $G = AB$ of the almost simple group G with $A \neq G \neq B$, suppose by way of contradiction that A, B satisfy condition (2) of the Main Theorem. If r and s are distinct primes, $a \in A$ an r -element and $b \in B$ an s -element, we may assume by Lemma 1, and by replacing A by a suitable conjugate, that a and b are contained in a Hall $\{r, s\}$ -subgroup of the soluble group $\langle a, b \rangle$, and so they generate an $\{r, s\}$ -subgroup of G .
- (S4) For infinite families of groups of Lie type, the independency of the specified primes can usually be proved by referring to results about the prime divisors of certain maximal soluble subgroups. One of the primes in question is frequently a primitive prime divisor of $p^k - 1$ for a suitable k , where p is the characteristic of the field over which the group is defined.

We recall this relevant definition:

Definition 3 Let k be a positive integer and p a prime. A *primitive prime divisor* of $p^k - 1$ is a prime r such that $r|p^k - 1$ and $r \nmid p^i - 1$ for every integer i such that $1 \leq i < k$.

The following well-known lemma of Zsigmondy [42] describes when primitive prime divisors exist:

Lemma 3 Let $k \geq 2$ an integer and p a prime.

- a) There exists a primitive prime divisor of $p^k - 1$ unless $k = 2$ and p is a Mersenne prime or $(p, k) = (2, 6)$.
- b) If r is a primitive prime divisor of $p^k - 1$, then $r - 1 \equiv 0 \pmod{k}$. In particular, $r \geq k + 1$.

2.1 Alternating groups

Lemma 4 If n is an integer, $n \geq 5$, $n \neq 10$, then there exists a non-Mersenne prime p such that $\frac{n}{2} < p \leq n$.

Proof By a generalization of the Bertrand-Chebyshev theorem, due to Ramanujan [38], for $n \geq 11$ there exist two primes p_1, p_2 with $\frac{n}{2} < p_1 < p_2 \leq n$. Clearly, not both of them can be Mersenne primes. Hence the assertion holds for $n \geq 11$ and $p = 5$ works for $5 \leq n \leq 9$. \square

Lemma 5 Let H be a soluble permutation group of degree n . If there exists a non-Mersenne prime $p > \frac{n}{2}$ dividing $|H|$, then H is p -closed, i.e. H has a unique Sylow p -subgroup.

Proof p^2 does not divide $|H|$ as $p > \frac{n}{2}$. Hence the assertion is equivalent to $\langle x \rangle$ normal in H for $x \in H$ of order p ; note that x is a p -cycle.

The proof is by induction on n , the case $n = 1$ being trivial. Assume that H is intransitive on $\Omega = \{1, \dots, n\}$ with orbits $\Delta_1, \dots, \Delta_s$. Then $H \leq H^{\Delta_1} \times \dots \times H^{\Delta_s}$ where H^{Δ_i} is the permutation group induced by H on Δ_i . It follows that there exists exactly one j with $|\Delta_j| \geq p$ and p divides $|H^{\Delta_j}|$. By induction, H^{Δ_j} is p -closed and so is H .

Hence we may assume that H is transitive on Ω . Then H is primitive on Ω (see [40, 1.2.(a)]). If $n = p$ then H is 2-transitive or p -closed by a result of Burnside (see [14, Corollary 3.5B]). If $n > p$, then H is 2-transitive by a result of Jordan (see [14, Theorem 7.4A]). So it remains to consider the 2-transitive case.

According to Huppert's classification of soluble 2-transitive permutation groups [31], $n = r^a$ for a prime r and $H \leq AGL_a(r)$ where either H is a group of semilinear mappings over \mathbb{F}_{r^a} with $|H| = r^a(r^a - 1)b$, $b|a$ or $n \in \{3^2, 3^4, 5^2, 7^2, 11^2, 23^2\}$.

It is easily checked that in none of the exceptional cases there exists a prime divisor of $|AGL_a(r)|$ which is larger than $\frac{r^a}{2}$.

In the generic case, $|H| = r^a(r^a - 1)b$, $b|a$. Since $p > \frac{r^a}{2}$, it follows immediately that p does not divide a and if $p|r^a - 1$, then $p = r^a - 1$ and $r = 2$ whence p is a Mersenne prime, contradicting the hypothesis about p . Therefore $p = r$ and $a = 1$. Then $|H| = p(p - 1)$ and H is p -closed by Sylow's theorem. \square

Proposition 1 *Let $N = A_n$ and $n \geq 5$. If $N \leq G = AB \leq \text{Aut}(N)$ with subgroups A and B satisfying condition (2) of the Main Theorem, $AN = BN = G$, then $A = G$ or $B = G$.*

Proof We consider first the case $n = 10$. Suppose 7 divides $|A|$. By [13], a Sylow 5-subgroup and a Sylow 7-subgroup of $N = A_{10}$ generate N . Hence if A contains a Sylow 5-subgroup of N , then $N \leq A$ whence $A = G$. So we may suppose that $5 \nmid |A|$. Again by [13], 5 and 7 are independent, contradicting condition (2) of the Main Theorem for A and B .

Now let $n \neq 10$. By Lemma 4, there exists a non-Mersenne prime p with $\frac{n}{2} < p \leq n$. We may assume that p divides $|A|$. Take P a subgroup of order p in A . If also p divides $|B|$, we may assume by Lemma 1 that $P \leq B$ by replacing B by a suitable conjugate if necessary.

Let $b \in B$ be a q -element for a prime $q \neq p$. By hypothesis, $\langle P, b \rangle$ is soluble. Therefore Lemma 5 implies that $\langle P, b \rangle$ is p -closed. It follows that P is normalized by all p' -elements of B and hence by $O^p(B)$. If p does not divide $|B|$, $B = O^p(B)$; otherwise $B = O^p(B)P$. Therefore B normalizes P . Hence $P \leq A^b$ for all $b \in B$. It follows now from $G = AB$ that $P \leq \bigcap_{b \in B} A^b = \bigcap_{g \in G} A^g$. But then $\text{Core}_G(A) \neq 1$, whence $N \leq A$, $A = G$. \square

Notation for tables in 2.2–2.4.

Sections 2.2–2.4 make essential use of maximal factorizations of almost simple groups whose simple normal subgroup is of Lie type or sporadic as given in [35]. For those factorizations where it is possible to determine independent primes, as described in (S1), the corresponding information is gathered in tables. They appear throughout the proof at the appropriate places.

In all tables the entries in the third and fourth columns are independent primes (with respect to the simple group N) dividing $|A \cap N|$ (third column) and $|B \cap N|$ (fourth column), respectively.

Also, in Tables 1, 3, 5–8, the entries in the second column present subcases of certain factorizations depending on the parameters of the corresponding classical group considered in each case.

In Tables 2, 4, 9–14, the second column describes the subgroups appearing in the possible maximal factorizations of the corresponding almost simple group.

2.2 Classical groups of Lie type

According to our general strategies we proceed here as follows:

- As mentioned in (S1), in the treatment of classical almost simple groups of Lie type, apart from two cases (see Section 2.2.2, case m); Section 2.2.3, case g)) we will always determine two primes, one dividing $|A \cap N|$ and the other dividing $|B \cap N|$ that are independent with respect to the simple group N (cf. Theorem 2).
- Also as said in (S4), for the infinite families of factorizations presented in [35], one of the primes is usually a primitive prime divisor r of $p^k - 1$ for a suitable k , depending on the parameters of the simple groups of Lie type of characteristic p . In this case the independence of r and the other specified prime, say s , can in

general be proved by using results of [2] where necessary conditions for primes dividing the order of a soluble subgroup containing an element of order r are given; we will state them explicitly at the appropriate places but omit the easy calculations needed to show that s is not among the possible primes.

- There are also exceptional factorizations of classical groups with certain small parameters n, q . As mentioned before in (S2), in these cases the independence of the specified primes can be deduced from the subgroup structure given in [10] or [13].
- We also note that many of the independency results can alternatively be inferred from the proof of Theorem 2 in [1] or the one of Theorem 1 in [33].

In the following we use the notation of [35] for the groups of Lie type, especially for the orthogonal groups, and their subgroups. In particular, if \hat{N} is a classical linear group on the vector space V with centre Z such that $N = \hat{N}/Z$ is simple and $\hat{N} \trianglelefteq \hat{G} \leq GL(V)$, for any subgroup X of \hat{G} we denote by \hat{X} the subgroup $(XZ \cap \hat{N})/Z$ of N . Also we use the notation P_i, N_i, N_i^ϵ ($\epsilon = \pm$), for stabilizers of subspaces as described in [35, 2.2.4].

2.2.1 Linear groups

$N = L_n(q)$, $n \geq 2$, $q = p^e$, p prime.

We will proceed by considering the possible maximal factorizations according to [35, Tables 1,3]. Using the notation of [35], in general $X_{\tilde{A}} = \tilde{A} \cap N$ and likewise for \tilde{B} as can be seen from chapters 2 and 3 of [35]; in the exceptional cases, we give information about $|(\tilde{A} \cap N) : X_{\tilde{A}}|$ or $|(\tilde{B} \cap N) : X_{\tilde{B}}|$, respectively. Then:

- In all cases we determine independent primes, one dividing $|A \cap N|$, the other one dividing $|B \cap N|$.
- The independency of the given primes can be proved as explained at the beginning of Section 2.2.
- In addition, in case of $N = L_2(q)$ the independence of the given primes is always a consequence of Dickson's list of subgroups of $L_2(q)$ as presented for instance in [32, Theorem II.8.27].

In order to deal with infinite families of factorizations we introduce primes r, s, t , depending on the parameters (n, p, e) of the linear group $N = L_n(q)$, $q = p^e$, p prime, in each considered case, as we explain below in Notation 1. The next remark considers the restrictions for their existence with the consequence that for one type of factorization (type a) below) the treatment has to be split into subcases.

- Remark** • If $(n, p, e) \neq (2, \text{Mersenne prime}, 1), (2, 2, 3), (3, 2, 2), (6, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{en} - 1$.
- If $(n, p, e) \neq (2, p, 1), (2, \text{Mersenne prime}, 2), (2, 2, 6), (4, 2, 2), (7, 2, 1), (3, \text{Mersenne prime}, 1), (3, 2, 3)$, then by Lemma 3 there exists a primitive prime divisor of $p^{e(n-1)} - 1$.
 - If $(n, p, e) \neq (4, \text{Mersenne prime}, 1), (4, 2, 3), (5, 2, 2), (8, 2, 1)$, $n \geq 4$, then by Lemma 3 there exists a primitive prime divisor of $p^{e(n-2)} - 1$.

Notation 1 In those cases where they exist, we denote primes r, s, t for linear groups as follows:

- r a primitive prime divisor of $p^{en} - 1$.
- s a primitive prime divisor of $p^{e(n-1)} - 1$.
- t a primitive prime divisor of $p^{e(n-2)} - 1$.

It follows from Lemma 3 that such primes r, s, t do not divide $|\text{Out}(N)|$.

For the mentioned use of [2], the result that is needed is the following:

Lemma 6 ([2, Lemma 2.5]) *With the previous notation, let the prime r be as above. If H is a maximal soluble subgroup of $GL_n(q)$, $n \geq 2$, whose order is divisible by r , then one of the following holds:*

- (1) $\pi(H) = \pi(n) \cup \pi(q^n - 1)$;
- (2) $\pi(H) \subseteq \pi(q - 1) \cup \pi(l) \cup \{2, r\}$, where $n = 2^l$, $r = n + 1$ and $q = p$ is a prime.

This result is sufficient for the subsequent treatment, but for some cases Lemma 2.6 of [2] can be used alternatively.

We consider now the possible maximal factorizations for linear groups according to [35, Tables 1,3], as mentioned above at the beginning of subsection 2.2.1.

a) $\tilde{A} \cap N = \tilde{GL}_a(q^b).b$, $ab = n$, b prime, $\tilde{B} \cap N = P_1$ or P_{n-1} , $(n, q) \neq (4, 2)$:

In this case there are independent primes (with respect to N) dividing $|A \cap N|$ and $|B \cap N|$, respectively, listed in Table 1. Here r, s, t are the primes in Notation 1, unless otherwise specified. There are eight subcases depending on the parameters (n, p, e) .

a1)	$n \geq 3, (n, p, e) \neq (3, \text{Mersenne prime}, 1), (3, 2, 3), (7, 2, 1), e > 1$ or $s \neq n$ (r as above or $r = 7$ if $(n, p, e) = (3, 2, 2)$ or $(6, 2, 1)$, s as above or $s = 7$ if $(n, p, e) = (4, 2, 2)$)	r	s
a2)	$n \geq 4, e = 1, n = s$ (s as above or $s = 7$ if $(n, p, e) = (7, 2, 1)$)	r	t
a3)	$(n, p, e) = (3, p, 1), p \neq 3$	r	p
a4)	$(n, p, e) = (3, 3, 1)$	13	2
a5)	$(n, p, e) = (3, 2, 3)$	73	7
a6)	$(n, p, e) = (2, p, e), e \geq 2,$ $(n, p, e) \neq (2, \text{Mersenne prime}, 2)$	r (3 if $p = 2$ and $e = 3$)	s (7 if $p = 2$ and $e = 6$)
a7)	$(n, p, e) = (2, \text{Mersenne prime}, 2), p > 3$	r	p
a8)	$(n, p, e) = (2, p, 1), p > 3$	largest prime divisor of $p + 1$	p

Table 1

We show details for the proof of the existence of independent primes listed in Table 1, corresponding to the case **a1)**, as model of the arguments and strategies used along the present proof of Theorem 1.

Case a1) We aim to prove under the conditions of **a1)** that r divides $|A \cap N|$, s divides $|B \cap N|$, and r and s are independent primes with respect to N .

We first notice that, attending Notation 1, in the present case there exists a primitive prime divisor r of $p^{en} - 1$, except when $(n, p, e) = (3, 2, 2)$ or $(6, 2, 1)$, and there exists a primitive prime divisor s of $p^{e(n-1)} - 1$, except when $(n, p, e) = (4, 2, 2)$, in which case we take $s = 7$.

Assume first that $(n, p, e) \neq (3, 2, 2), (6, 2, 1)$, and take primes r, s as mentioned. Then we can use Lemma 6 to prove the independency of r and s .

We claim that $s \notin \pi(n) \cup \pi(q^n - 1)$, and $s \notin \pi(q - 1) \cup \pi(l) \cup \{2, r\}$ when $n = 2^l$, $r = n + 1$, $q = p$. This will imply that r and s are independent by Lemma 6.

This is easily checked if $(n, p, e) = (4, 2, 2)$ and $s = 7$. Otherwise, s is a primitive prime divisor of $p^{e(n-1)} - 1$. By Lemma 3 we have that $s \geq e(n - 1) + 1$. If $s \in \pi(n)$, then $e = 1$ and $s = n$, which is not the case. Then $s \notin \pi(n)$. On the other hand, if $s \in \pi(q^n - 1)$, then s divides $(q^{n-1} - 1, q^n - 1) = q - 1$, which is not the case by the definition of s and the fact that $n - 1 \geq 2$. Thus $s \notin \pi(q^n - 1) \supseteq \pi(q - 1)$. It is also clear that $s \neq r, 2$. Finally, if $n = 2^l$, since $s \geq n > l$, we have that $s \notin \pi(l)$, and the claim is proven.

We use Lemma 2 to prove that r divides $|A \cap N|$ and s divides $|B \cap N|$.

In the present case, one checks that r does not divide $|\tilde{B} \cap N| |\text{Out}(N)|$ but divides $|N|$, which implies that r divides $|A \cap N|$ by Lemma 2. Analogously, s divides $|B \cap N|$ as it does not divide $|\tilde{A} \cap N| |\text{Out}(N)|$ and divides $|N|$.

Finally we consider the cases $(n, p, e) = (3, 2, 2)$ or $(6, 2, 1)$.

Here we take $r = 7$ and notice that for the case $(n, p, e) = (3, 2, 2)$, $s = 5$ is primitive prime divisor of $p^{e(n-1)} - 1 = 2^4 - 1$, whereas for the case $(n, p, e) = (6, 2, 1)$, $s = 31$ is primitive prime divisor of $p^{e(n-1)} - 1 = 2^5 - 1$.

In the case $(n, p, e) = (6, 2, 1)$, 7^2 does not divide $|\tilde{B} \cap N|$ but divides $|N|$, and 7 does not divide $|\text{Out}(N)|$. Then Lemma 2 implies that 7 divides $|A \cap N|$.

In the case $(n, p, e) = (3, 2, 2)$, 7 does not divide $|\tilde{B} \cap N| |\text{Out}(N)|$ but divides $|N|$, which implies again that 7 divides $|A \cap N|$.

Regarding s , in the both cases $(n, p, e) = (3, 2, 2)$ or $(6, 2, 1)$, s does not divide $|\tilde{A} \cap N| |\text{Out}(N)|$ but divides $|N|$, and Lemma 2 implies again that s divides $|B \cap N|$.

In order to prove the independency of r and s in the cases $(n, p, e) = (3, 2, 2)$ or $(6, 2, 1)$, we notice that a soluble subgroup of N whose order is divisible by rs , would contain an $\{r, s\}$ -subgroup with order also divisible by rs . It is easily checked, for instance using [13], that N contains no such $\{r, s\}$ -subgroup.

- b)** $X_{\tilde{A}} = PSp_n(q)$, $\tilde{B} \cap N = P_1$ or P_{n-1} , n even, $n \geq 4$:

(Note that $|\tilde{A} \cap N| : X_{\tilde{A}} = 1$ or 2 since $PSp_n(q)$ or $PSp_n(q).2$ is a maximal subgroup of N , depending on n and q ; see [10] and [34].)

This case is handled exactly as **a1)**. All other cases in **a)** do not occur here since $n \geq 4$ is even.

- c)** $X_{\tilde{A}} = PSp_n(q)$, $\tilde{B} \cap N = \text{Stab}(V_1 \oplus V_{n-1})$, n even, $n \geq 4$:

This case is handled exactly as **a1)**.

- d)** $\tilde{A} \cap N = \gamma GL_{n/2}(q^2).2$, $\tilde{B} \cap N = \text{Stab}(V_1 \oplus V_{n-1})$, $q = 2, 4$, n even, $n \geq 4$:

This case is handled exactly as **a1)**.

We treat now all exceptional factorizations of N corresponding to [35, Table 3]. We gather the different cases occurring and the corresponding independent

primes in Table 2. Recall that in the second column we also include $\tilde{A} \cap N$ and $\tilde{B} \cap N$.

e)	$N = L_2(11), \tilde{A} \cap N = P_1, \tilde{B} \cap N = A_5$	11	3
f)	$N = L_2(19), \tilde{A} \cap N = P_1, \tilde{B} \cap N = A_5$	11	5
g)	$N = L_2(29), \tilde{A} \cap N = P_1, \tilde{B} \cap N = A_5$	29	5
h)	$N = L_2(59), \tilde{A} \cap N = P_1, \tilde{B} \cap N = A_5$	59	5
i)	$N = L_2(7), \tilde{A} \cap N = P_1, \tilde{B} \cap N = S_4$	7	2
j)	$N = L_2(23), \tilde{A} \cap N = P_1, \tilde{B} \cap N = S_4$	23	3
k)	$N = L_2(11), \tilde{A} \cap N = P_1, \tilde{B} \cap N = A_4$	11	3
l)	$N = L_2(16), \tilde{A} \cap N = D_{34}, \tilde{B} \cap N = L_2(4)$	17	5
m)	$N = L_3(4), \tilde{A} \cap N = L_2(7), \tilde{B} \cap N = A_6$	7	5
n)	$N = L_5(2), \tilde{A} \cap N = 31.5, \tilde{B} \cap N = P_2 \text{ or } P_3$	31	7

Table 2

2.2.2 Unitary groups

$N = U_n(q)$, $n \geq 3$, $q = p^e$, p prime.

Infinite families of factorizations of N described in [35, Table 1] exist only for even n . So we assume first that $n = 2m \geq 4$. Then:

- In all cases we determine independent primes, one dividing $|A \cap N|$, the other one dividing $|B \cap N|$.
- The divisibility properties and the independency are proved as described at the beginning of Section 2.2.

We introduce primes r, s depending on (n, p, e) , as explained next, where the remark considers the restrictions for their existence:

- Remark**
- If $(n, p, e) \neq (4, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{2e(n-1)} - 1$.
 - If $(n, p, e) \neq (6, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor s of $p^{en} - 1$.

Notation 2 In those cases where they exist, we denote primes r, s for unitary groups as follows:

- r a primitive prime divisor of $p^{2e(n-1)} - 1$.
- s a primitive prime divisor of $p^{en} - 1$.

It follows from Lemma 3 that such primes r, s do not divide $|\text{Out}(N)|$.

We make use of the following result in [2]:

Lemma 7 ([2, Lemma 2.8(1)]) *With the previous notation, let the prime r be as above. If H is a maximal soluble subgroup of $U_n(q)$, $n = 2m \geq 4$, with $r \mid |H|$, then $\pi(H) \subseteq \pi(n-1) \cup \pi(q^{n-1} + 1)$.*

We consider first the possible maximal factorizations for unitary groups according to [35, Table 1].

a) $\tilde{A} \cap N = N_1$, $\tilde{B} \cap N = P_m$:

We have to consider two subcases, presented in Table 3.

a1)	$(n, p, e) \neq (4, 2, 1)$	r	s (s as above or $s = 7$ if $(n, p, e) = (6, 2, 1)$)
a2)	$(n, p, e) = (4, 2, 1)$	3	5

Table 3

This case is proven by using analogous arguments to those for linear groups, in Section 2.2.1, case **a1)**, but with corresponding primes r , s as in Notation 2 or as specified, and Lemma 7 for the proof of the independence.

b) $\tilde{A} \cap N = N_1$, $X_{\tilde{B}} = PSp_n(q)$:

Note that $|(\tilde{B} \cap N) : X_{\tilde{B}}| = 1$ or 2 since $PSp_n(q)$ or $PSp_n(q).2$ is a maximal subgroup of N (depending on q and n ; cf. [34] and [10]).

This case is handled exactly as **a)**.

c) $N = U_n(2)$, $m \geq 3$, $\tilde{A} \cap N = N_1$, $X_{\tilde{B}} = \hat{SL}_m(4).2$:

This case is handled exactly as **a1)**.

d) $N = U_n(4)$, $\tilde{A} \cap N = N_1$, $X_{\tilde{B}} = \hat{SL}_m(16).3.2$:

This case is handled exactly as **a1)**.

We treat now the exceptional factorizations as given in [35, Table 3].

Here we have:

- Apart from one case ($N = U_4(3)$) there are independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, summarized in Table 4.
- The divisibility of $|A \cap N|$ and $|B \cap N|$ by the specified primes follows from Lemma 2.

e)	$N = U_3(3)$, $\tilde{A} \cap N = L_2(7)$, $\tilde{B} \cap N = P_1$	7	2
f)	$N = U_3(5)$, $\tilde{A} \cap N = A_7$, $\tilde{B} \cap N = P_1$	7	5
g)	$N = U_3(8)$, $\tilde{A} \cap N = 19.3$, $\tilde{B} \cap N = P_1$	19	7
h)	$N = U_4(2)$, $\tilde{A} \cap N = 3^3.S_4$, $\tilde{B} \cap N = P_2$	3	5
i)	$N = U_6(2)$, $\tilde{A} \cap N = N_1$, $\tilde{B} \cap N = U_4(3).2$	11	7
j)	$N = U_6(2)$, $\tilde{A} \cap N = N_1$, $\tilde{B} \cap N = M_{22}$	11	7
k)	$N = U_9(2)$, $\tilde{A} \cap N = J_3$, $\tilde{B} \cap N = P_1$	19	43
l)	$N = U_{12}(2)$, $\tilde{A} \cap N = Suz$, $\tilde{B} \cap N = N_1$	13	683

Table 4

For case j) we have to explain why 11 divides $|A \cap N|$. If not, this would lead to a non-trivial factorization $A(\tilde{A} \cap \tilde{B})$ of \tilde{A} , \tilde{A} an almost simple group with socle $N_1 \cong U_5(2)$. This is impossible by [35, Tables 1,3].

It remains to consider the exceptional factorizations for the case $N = U_4(3)$ according to [35, Table 3].

m) $N = U_4(3)$, $\tilde{A} \cap N = L_3(4)$, $\tilde{B} \cap N = P_1$ or $PSp_4(3)$ or P_2 :

It follows from Lemma 2 that in all three cases 7 divides $|A \cap N|$ and 3^4 divides $|B \cap N|$.

Suppose that A and B satisfy condition (2) of the Main Theorem. Note that 7 is a primitive prime divisor of $3^6 - 1$. Let $y \in A \cap N$ of order 7. By [13], $|N_N(\langle y \rangle)| = 7 \cdot 3$. This and Lemma 7 imply that $N_N(\langle y \rangle)$ is the only maximal soluble subgroup of N containing y . Therefore $\langle x, y \rangle = N_N(\langle y \rangle)$ for all non-trivial 3-elements x of $B \cap N$, a contradiction.

(We note that in case $G = N$ the primes 2 and 7 are independent and 2 divides $|B \cap N|$. But this need not be the case if $G \geq N.2$, see Theorem 2.)

2.2.3 Symplectic groups

$N = PSp_{2m}(q)$, $m \geq 2$, $q = p^e$, p prime.

For arguments like in the previous cases, we introduce primes r, s, t , depending on (m, p, e) , as explained next:

Remark • If $(m, p, e) \neq (3, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{2em} - 1$.

- If $(m, p, e) \neq (2, \text{Mersenne prime}, 1), (2, 2, 3), (3, 2, 2), (6, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{em} - 1$.
- If $(m, p, e) \neq (2, \text{Mersenne prime}, 1), (2, 2, 3), (4, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{2e(m-1)} - 1$.

Notation 3 In those cases where they exist, we denote primes r, s for symplectic groups as follows:

- r a primitive prime divisor of $p^{2em} - 1$.
- s a primitive prime divisor of $p^{em} - 1$.
- t a primitive prime divisor of $p^{2e(m-1)} - 1$.

It follows from Lemma 3 that such primes r, s, t do not divide $|\text{Out}(N)|$.

We first consider the possible maximal factorizations according to [35, Table 1]. Then:

- In all but one case ($N = PSp_6(2)$) there exist independent primes with respect to N , one dividing $|A \cap N|$, the other one dividing $|B \cap N|$.
- The independency of the given primes can be proved as mentioned at the beginning of Section 2.2.

The result that is needed from [2] is the following. For later use in Sections 2.2.4 and 2.2.5 we formulate it already in a way that also includes orthogonal groups in odd dimension and of - type in even dimension.

Lemma 8 ([2, Lemma 2.8(2)]) *With the previous notation, let the prime r be as above. If H is a maximal soluble subgroup of $PSp_{2m}(q)$, $m \geq 2$, $P\Omega_{2m+1}(q)$, $m \geq 3$ and q odd, or $P\Omega_{2m}^-(q)$, $m \geq 4$, whose order is divisible by r , then one of the following holds:*

- (1) $\pi(H) \subseteq \pi(m) \cup \pi(q^m + 1) \cup \{2\}$;
(2) $\pi(H) \subseteq \pi(q - 1) \cup \pi(l + 1) \cup \{2, r\}$, where $m = 2^l$, $r = 2m + 1$ and $q = p$ is a prime.

The possible maximal factorizations are as follows.

- a) $\tilde{A} \cap N = PSp_{2a}(q^b).b$, $ab = m$, b prime, $\tilde{B} \cap N = P_1$:

In this case there are always independent primes (with respect to N) dividing $|A \cap N|$ and $|B \cap N|$, respectively. They are specified in Table 5. The primes r and t are as in Notation 3.

a1)	$(m, p, e) \neq (2, \text{Mersenne prime}, 1)$ $(r = 7 \text{ if } (m, p, e) = (3, 2, 1),$ $t = 7 \text{ if } (m, p, e) = (2, 2, 3) \text{ or } (4, 2, 1))$	r	t
a2)	$(m, p, e) = (2, \text{Mersenne prime}, 1)$	r	p

Table 5

- b) $q = 2^e$, $\tilde{A} \cap N = Sp_{2a}(q^b).b$, $ab = m$, b prime, $\tilde{B} \cap N = O_{2m}^+(q)$:

(Note that $X_{\tilde{B}} = \tilde{B} \cap N$ since $O_{2m}^+(q)$ is a maximal subgroup of $N = Sp_{2m}(q)$, see [34] and [10].)

There are always independent primes (with respect to N) dividing $|A \cap N|$ and $|B \cap N|$, respectively. They are specified in Table 6 for all subcases to be considered. The meaning of r and t is as above in Notation 3.

b1)	$(m, e) \neq (2, 3), (3, 1), (4, 1)$	r	t
b2)	$(m, e) = (2, 3)$	13	7
b3)	$(m, e) = (3, 1)$	7	5
b4)	$(m, e) = (4, 1)$	17	7

Table 6

In **b3)** we have to justify why 7 divides $|A|$ (note that $|\text{Out}(N)| = 1$). Since 2^2 and 3^2 divide $|A|$, this follows from the fact that there is no subgroup of $Sp_2(8).3$ whose order is divisible by 36, but not by 7.

- c) $q = 2^e$, $\tilde{A} \cap N = Sp_{2a}(q^b).b$, $ab = m$, b prime, $\tilde{B} \cap N = O_{2m}^-(q)$:

(Note that $X_{\tilde{B}} = \tilde{B} \cap N$ since $O_{2m}^-(q)$ is a maximal subgroup of $N = Sp_{2m}(q)$, see [34] and [10].)

Again there are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively. They are presented in Table 7 where the meaning of r , s and t is as above in Notation 3.

c1	$(m, e) \neq (2, 3), (3, 1), (4, 1), r \mid A \cap N $	r	t
c2	$(m, e) \neq (2, 3), (3, 1), (3, 2), (6, 1), r \nmid A \cap N $	s	r
c3	$(m, e) = (2, 3), r = 13 \mid A \cap N $	13	7
c4	$(m, e) = (2, 3), r = 13 \nmid A \cap N $	7	13
c5	$(m, e) = (3, 1)$	7	5
c6	$(m, e) = (4, 1)$	17	7
c7	$(m, e) = (3, 2)$ or $(6, 1), r = 13 \nmid A \cap N $	7	13

Table 7

d) $q = 2^e$, $\tilde{A} \cap N = O_{2m}^-(q)$, $\tilde{B} \cap N = P_m$:

Here there are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively. They are presented in Table 8 where the meaning of r and s is as above in Notation 3.

d1	$(m, e) \neq (2, 3), (3, 1)$ $(s = 7 \text{ for } (m, e) = (3, 2) \text{ or } (6, 1))$	r	s
d2	$(m, e) = (2, 3)$	13	7
d3	$(m, e) = (3, 1)$	5	7

Table 8

e) $q = 2^e$, m even, $\tilde{A} \cap N = O_{2m}^-(q)$, $\tilde{B} \cap N = Sp_m(q) \text{ wr } S_2$:

This case case is handled exactly like **d**).

f) $q = 2$, m even, $\tilde{A} = Sp_m(2).2$, $\tilde{B} = N_2$ (note that $|\text{Out}(N)| = 1$):

One can assume that $m \geq 4$ since $Sp_4(2)' = L_2(9)$. Then r divides $|A \cap N|$ and t divides $|B \cap N|$ where r and t are as in Notation 3, or $t = 7$ if $m = 4$. r and t are independent.

g) $q = 2$, $\tilde{A} = O_{2m}^-(2)$, $\tilde{B} = O_{2m}^+(2)$ (note that $|\text{Out}(N)| = 1$):

If $m \neq 3$, let r and s as above in Notation 3, or $s = 7$ for $m = 6$. Then r divides $|A|$ and s divides $|B|$. r and s are independent.

Let $m = 3$. By Lemma 2, 3^2 divides $|A|$ and 7 divides $|B|$. If 5 divides $|A|$, we are done since 5 and 7 are independent. Otherwise 5 divides $|B|$. Using [10] or [13], the only maximal soluble subgroups of N whose order is divisible by 15 are the normalizers of subgroups of order 5, isomorphic to $(5 \times S_3) : 4$. Suppose A and B satisfy condition (2) of the Main Theorem. It follows that if $y \in B$ is of order 5, then $\langle x_1, y \rangle = \langle x_2, y \rangle$ of order 15 for all non-trivial 3-elements $x_1, x_2 \in A$, a contradiction.

(We note that in case $m = 3$ there need not be independent primes dividing $|A|$ and $|B|$, respectively. See Theorem 2.)

It remains to consider the three cases **h**), **i**), **j**) summarized in Table 9.

Note in case **j**) that $X_{\tilde{B}} = \tilde{B} \cap N$ by [35, 3.2.4(d)].

h)	$q = 4, \tilde{A} \cap N = O_{2m}^-(4), \tilde{B} \cap N = O_{2m}^+(4)$	r	s ($s = 7$ if $m = 3$)
i)	$q = 4, m$ even, $\tilde{A} \cap N = Sp_m(16).2, \tilde{B} \cap N = N_2$	r	t
j)	$q = 4, 16, \tilde{A} \cap N = O_{2m}^-(q), \tilde{B} \cap N = Sp_{2m}(q^{1/2})$	r	s

Table 9

We now consider the possible maximal factorizations according to [35, Table 2]. Here:

- There are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, as specified next.

k) $m = 2, q = 2^e, e$ odd, $e \geq 3, \tilde{A} \cap N = Sz(q), \tilde{B} \cap N = O_4^+(q)$:

r divides $|A \cap N|$, s divides $|B \cap N|$, r and s are independent.

l) $m = 3, q = 2^e, \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = O_6^+(q)$:

If $e > 1$, then r divides $|A \cap N|$, t divides $|B \cap N|$, r and t are independent. If $e = 1$, then $G = N$. Clearly 5 divides $|B|$. Since $N = A\tilde{B}$, it follows that $G_2(2) \cong \tilde{A} = A(\tilde{A}\tilde{B})$. But according to [35, Table 5], $G_2(2)$ has only trivial factorizations, whence $A = \tilde{A}$ and 7 divides $|A|$. 7 and 5 are independent.

m) $m = 3, q = 2^e, \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = O_6^-(q)$:

Assume first the $e > 1$. t divides $|B \cap N|$. If r divides $|A \cap N|$, we choose the independent primes r and t . If r does not divide $|A \cap N|$, then r divides $|B \cap N|$. As s divides $|A \cap N|$ ($s = 7$ if $e = 2$), we choose the independent primes s and r .

If $e = 1$, 7 divides $|A \cap N|$ and 5 divides $|B \cap N|$. 7 and 5 are independent.

n) $m = 3, q = 2^e, \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = P_1$ or N_2 :

This follows exactly like case **l**).

We now consider the exceptional maximal factorizations according to [35, Table 3]. Here:

- There are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, specified in Table 10.

Note that $\text{Out}(N) = 1$ in **q**) and **r**).

o)	$N = PSp_4(3), \tilde{A} \cap N = 2^4.A_5, \tilde{B} \cap N = P_1$ or P_2	5	3
p)	$N = PSp_6(3), \tilde{A} \cap N = L_2(13), \tilde{B} \cap N = P_1$	7	5
q)	$N = Sp_8(2), \tilde{A} = O_8^-(2), \tilde{B} = S_{10}$	17	5
r)	$N = Sp_8(2), \tilde{A} = L_2(17), \tilde{B} = O_8^+(2)$	17	5

Table 10

2.2.4 Orthogonal groups in odd dimension

$N = P\Omega_{2m+1}(q)$ ($= \Omega_{2m+1}(q)$), $m \geq 3$, $q = p^e$ odd, p prime.

We consider the maximal factorizations according to [35, Tables 1,2,3]. Then:

- There are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, specified in Table 11.

In order to prove it, we consider primes as follows, and Lemma 8.

Notation 4 We denote primes r, s, t for orthogonal groups in odd dimension, as in Notation 3.

Note that they exist in this case without any restriction since $m \geq 3$ and $p \neq 2$. Note that none of r, s, t divides $|\text{Out}(N)|$.

a)	$\tilde{A} \cap N = N_1^-, \tilde{B} \cap N = P_m$	r	s
b)	$N = \Omega_7(q), \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = P_1$	r	t
c)	$N = \Omega_7(q), \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = N_1^+$	r	t
d)	$N = \Omega_7(q), \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = N_1^-, r \mid A \cap N $	r	t
e)	$N = \Omega_7(q), \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = N_1^-, r \nmid A \cap N $	s	r
f)	$N = \Omega_7(q), \tilde{A} \cap N = G_2(q), \tilde{B} \cap N = N_2^\epsilon, \epsilon = +, -$	r	t
g)	$N = \Omega_{13}(3^e), \tilde{A} \cap N = PSp_6(3^e).a, a \leq 2, \tilde{B} \cap N = N_1^-$	r	s
h)	$N = \Omega_{25}(3^e), \tilde{A} \cap N = F_4(3^e), \tilde{B} \cap N = N_1^-$	s	r
i)	$N = \Omega_7(3), \tilde{A} \cap N = G_2(3), \tilde{B} \cap N = Sp_6(2)$ or $S_9, 7 \mid A \cap N $	7	5
j)	$N = \Omega_7(3), \tilde{A} \cap N = G_2(3), \tilde{B} \cap N = Sp_6(2)$ or $S_9, 7 \nmid A \cap N $	13	7
k)	$N = \Omega_7(3), \tilde{A} \cap N = S_9, \tilde{B} \cap N = N_1^+$ or P_3	7	13
l)	$N = \Omega_7(3), \tilde{A} \cap N = Sp_6(2), \tilde{B} \cap N = N_1^+$ or P_3	7	13
m)	$N = \Omega_7(3), \tilde{A} \cap N = 2^6.A_7, \tilde{B} \cap N = P_3$	7	13

Table 11

2.2.5 Orthogonal groups of $-$ type in even dimension

$N = P\Omega_{2m}^-(q)$, $m \geq 4$, $q = p^e$, p prime.

We now consider the maximal factorizations according to [35, Tables 1,3]. Here:

- There are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, specified in Table 12.

In order to prove it, we again consider primes as follows, and Lemma 8.

Notation 5 In those cases where they exist, we denote primes r, t for orthogonal groups of $-$ type in even dimension as in Notation 3.

Note that they exist in this case with the only restriction $(m, p, e) \neq (4, 2, 1)$ to ensure the existence of t . Note that both r and t do not divide $|\text{Out}(N)|$.

a)	$\tilde{A} \cap N = P_1$ or $N_1, \tilde{B} \cap N = GU_m(q), m$ odd	t	r
b)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \Omega_m^-(q^2).2, q = 2, 4, m$ even	t ($t = 7$ for $(m, q) = (4, 2)$)	r
c)	$\tilde{A} \cap N = N_2^+, \tilde{B} \cap N = GU_m(4), q = 4, m$ odd	t	r
d)	$N = P\Omega_{10}^-(2), \tilde{A} \cap N = A_{12}, \tilde{B} \cap N = P_1$	11	17

Table 12

2.2.6 Orthogonal groups of + type in even dimension

$N = P\Omega_{2m}^+(q), m \geq 4, q = p^e, p$ prime.

We will consider below the maximal factorizations according to [35], Tables 1, 2, 3 (case $m \geq 5$) and Table 4 (case $m = 4$).

For arguments like in previous cases, we introduce primes r, s, t , depending on (m, p, e) , as explained next:

- Remark** • If $(m, p, e) \neq (4, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{2e(m-1)} - 1$.
- If $(m, p, e) \neq (6, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{em} - 1$.
 - If $(m, p, e) \neq (4, 2, 2), (7, 2, 1)$, then by Lemma 3 there exists a primitive prime divisor of $p^{e(m-1)} - 1$.

Notation 6 In those cases where they exist, we denote primes r, s, t for orthogonal groups of + type in even dimension as follows:

- r a primitive prime divisor of $p^{2e(m-1)} - 1$.
- s a primitive prime divisor of $p^{em} - 1$.
- t a primitive prime divisor of $p^{e(m-1)} - 1$.

It follows from Lemma 3 that such primes r, s, t do not divide $|\text{Out}(N)|$. Moreover, r, s, t are pairwise distinct.

For independency proofs we will need the following result of [2] (with a corrected misprint there):

Lemma 9 ([2, Lemma 2.8(3)]) *With the previous notation, let the prime r be as above. If H is a maximal soluble subgroup of $N = P\Omega_{2m}^+(q), m \geq 4$, whose order is divisible by r , then one of the following holds:*

- (1) $\pi(H) \subseteq \pi(m-1) \cup \pi(q^{m-1}+1) \cup \pi(q+1) \cup \{2\}$;
- (2) $\pi(H) \subseteq \pi(q^2-1) \cup \pi(l+1) \cup \{2, r\}$, where $m-1 = 2^l, r = 2m-1$ and $q = p$ is a prime;
- (3) $\pi(H) \subseteq \pi(q-1) \cup \pi(l+1) \cup \{2, r\}$, where $m = 2^l, r = 2m-1$ and $q = p$ is a prime.

We assume first that $m \geq 5$ and consider the maximal factorizations according to [35, Tables 1,2,3]. Then:

- There are always independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively, specified in Table 13.

We note in part **d)** that $X_{\tilde{B}} = PSp_2(q) \otimes PSp_m(q)$ has index 1 or 2 in $\tilde{B} \cap N$; cf. [34, Table 3.5.E, Prop. 4.4.12].

a)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = P_m \text{ or } P_{m-1}$	r	s
b)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \mathcal{C}GU_m(q).2,$ $m \text{ even}, r \mid A \cap N $	r	s
c)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \mathcal{C}GU_m(q).2,$ $m \text{ even}, r \nmid A \cap N $	t	r
d)	$\tilde{A} \cap N = N_1, X_{\tilde{B}} = PSp_2(q) \otimes PSp_m(q),$ $m \text{ even}, q > 2$	r	s
e)	$\tilde{A} \cap N = N_2^-, \tilde{B} \cap N = P_m \text{ or } P_{m-1}$	r	s $(s = 7 \text{ for } (m, q) = (6, 2))$
f)	$\tilde{A} \cap N = P_1, \tilde{B} \cap N = \mathcal{C}GU_m(q).2, m \text{ even}$	t	r
g)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \mathcal{C}GL_m(q).2$	r	s $(s = 7 \text{ for } (m, q) = (6, 2))$
h)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \Omega_m^+(4).2^2, q = 2,$ $m \text{ even}$	r	s $(s = 7 \text{ for } (m, q) = (6, 2))$
i)	$\tilde{A} \cap N = N_1, \tilde{B} \cap N = \Omega_m^+(16).2^2, q = 4,$ $m \text{ even}$	r	s
j)	$\tilde{A} \cap N = N_2^-, \tilde{B} \cap N = \mathcal{C}GL_m(2).2, q = 2$	r	s $(s = 7 \text{ for } (m, q) = (6, 2))$
k)	$\tilde{A} \cap N = N_2^-, \tilde{B} \cap N = \mathcal{C}GL_m(4).2, q = 4$	r	s
l)	$\tilde{A} \cap N = N_2^+, \tilde{B} \cap N = \mathcal{C}GU_m(4).2, q = 4,$ $m \text{ even}$	t	r
m)	$\tilde{A} \cap N = \Omega_9(q).a, \tilde{B} \cap N = N_1, a \leq 2, m = 8$	s	r
n)	$N = \Omega_{24}^+(2), \tilde{A} \cap N = Co_1, \tilde{B} \cap N = N_1$	13	683

Table 13

We treat now the case $m = 4$ and consider the maximal factorizations according to [35, Table 4]. Here:

- The primes r and s ($r = 7$ if $q = 2$) are independent.

For all maximal factorizations $G = \tilde{A}\tilde{B}$ with $\Omega_8^+(q) \leq G \leq \text{Aut}(\Omega_8^+(q))$ listed in [35, Table 4], r divides $|A \cap N|$ and s divides $|B \cap N|$, or vice versa.

2.3 Exceptional groups of Lie type

For the exceptional groups of Lie type all factorizations (not only the maximal ones) have been determined in [30]; see also [35, Table 5].

- a)** $N = G_2(q)$, $q = 3^e$, $A \cap N = SL_3(q)$ or $SL_3(q).2$, $B \cap N = SU_3(q)$ or $SU_3(q).2$:
By [1, Table 3] (with corrected misprint), there exist independent prime divisors r of $q^2 + q + 1 \mid |A \cap N|$ and s of $q^2 - q + 1 \mid |B \cap N|$.
- b)** $N = G_2(q)$, $q = 3^e$, e odd, $A \cap N = SL_3(q)$ or $SL_3(q).2$, $B \cap N = {}^2G_2(q)$:
This case is handled as in **a**).
- c)** $N = G_2(4)$, $A \cap N = J_2$, $B \cap N = SU_3(4)$ or $SU_3(4).2$:
7 divides $|A \cap N|$ and 13 divides $|B \cap N|$. 7 and 13 are independent.
- d)** $N = G_2(4)$, $A \cap N = (G_2(2) \times 2) \cap N$, $B \cap N = (SU_3(4).4) \cap N$:
This case is handled as in **c**).
- e)** $N = F_4(q)$, $q = 2^e$, $A \cap N = Sp_8(q)$, $B \cap N = {}^3D_4(q)$ or ${}^3D_4(q).3$:
By [1, Table 3], there exist independent prime divisors r of $q^4 + 1 \mid |A \cap N|$ and s of $q^4 - q^2 + 1 \mid |B \cap N|$.

2.4 Sporadic groups

We use the list of maximal factorizations in [35, Table 6].

- In all cases there are independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively. They are presented in Table 14.

Note that $\text{Out}(N) = 1$ for $N \cong M_{11}, M_{23}, M_{24}, Ru, Co_1$ (see for instance [13]).

a)	$N = M_{11}, \tilde{A} = L_2(11), \tilde{B} = M_{10}$ or $M_9.2$	11	3
b)	$N = M_{12}, \tilde{A} \cap N = M_{11}, \tilde{B} \cap N = M_{11}, L_2(11), 11 \nmid A \cap N $	3	11
c)	$N = M_{12}, \tilde{A} \cap N = M_{11}, \tilde{B} \cap N = M_{11}, L_2(11), 11 \mid A \cap N $	11	3
d)	$N = M_{12}, \tilde{A} \cap N = M_{11}, \tilde{B} \cap N = M_{10}.2, M_9.S_3, 2 \times S_5,$ $4^2 \times D_{12}$ or $A_4 \times S_3$	11	3
e)	$N = M_{12}, \tilde{A} \cap N = L_2(11), \tilde{B} \cap N = M_{10}.2$ or $M_9.S_3$	11	3
f)	$N = M_{22}, \tilde{A} \cap N = L_2(11).2 \cap N, \tilde{B} \cap N = L_3(4).2 \cap N$	11	7
g)	$N = M_{23}, \tilde{A} = 23.11, \tilde{B} = M_{22}, M_{21}.2$ or $2^4.A_7$	23	7
h)	$N = M_{24}, \tilde{A} = M_{23}, \tilde{B} = L_2(23), 23 \mid A $	23	2
i)	$N = M_{24}, \tilde{A} = M_{23}, \tilde{B} = L_2(23), 23 \nmid A $	2	23
j)	$N = M_{24}, \tilde{A} = M_{23}, \tilde{B} = M_{12}.2, 2^6.3.S_6, L_2(7)$ or $2^6(L_3(2) \times S_3)$	23	2
k)	$N = M_{24}, \tilde{A} = L_2(23), \tilde{B} = M_{22}.2, 2^4.A_8$ or $L_3(4).S_3$	23	2
l)	$N = J_2, \tilde{A} \cap N = U_3(3), \tilde{B} \cap N = A_5 \times D_{10}$	7	5
m)	$N = J_2, \tilde{A} \cap N = U_3(3).2 \cap N, \tilde{B} \cap N = 5^2(4 \times S_3) \cap N$	7	5

Table 14

n)	$N = HS, \tilde{A} \cap N = M_{22}, \tilde{B} \cap N = U_3(5).2, 7 \mid A \cap N $	7	5
o)	$N = HS, \tilde{A} \cap N = M_{22}, \tilde{B} \cap N = U_3(5).2, 7 \nmid A \cap N $	11	7
p)	$N = HS, \tilde{A} \cap N = M_{22}.2 \cap N, \tilde{B} \cap N = 5^{1+2}.2^5 \cap N$	7	5
q)	$N = He, \tilde{A} \cap N = Sp_4(4).2, \tilde{B} \cap N = 7^2.SL_2(7)$	17	7
r)	$N = He, \tilde{A} \cap N = Sp_4(4).4 \cap N, \tilde{B} \cap N = 7^{1+2}(S_3 \times 6) \cap N$	17	7
s)	$N = Ru, \tilde{A} = L_2(29), \tilde{B} = {}^2F_4(2)$	29	13
t)	$N = Suz, \tilde{A} \cap N = G_2(4) \cap N, \tilde{B} \cap N = U_5(2) \text{ or } 3^5.M_{11}$	13	11
u)	$N = Fi_{22}, \tilde{A} \cap N = {}^2F_4(2)', \tilde{B} \cap N = 2.U_6(2)$	13	11
v)	$N = Co_1, \tilde{A} = Co_2 \text{ or } Co_3, \tilde{B} \cap N = 3.Suz.2 \text{ or } (A_4 \times G_2(4)).2$	23	13

Table 14 (contd.)

This completes the proof of Theorem 1.

As a consequence of the proof we state the following result:

Theorem 2 *Let N be a simple group of Lie type (classical or exceptional) or a sporadic simple group.*

Let $G = AB$ be a factorized almost simple group with socle N , i.e. $N \leq G \leq \text{Aut}(N)$, $A \leq G$, $B \leq G$ with $N \not\leq A$, $N \not\leq B$.

- a) *If $N \cong PSp_6(2)$ and $U_4(3)$, there exist independent primes with respect to N , one dividing $|A \cap N|$, the other one dividing $|B \cap N|$.*

If $N \cong PSp_6(2) \cong \Omega_7(2)$, there exists a (non-maximal) factorization $N = AB$ of type g), Section 2.2.3, such that there are no independent primes dividing $|A|$ and $|B|$, respectively.

If $N \cong U_4(3) \cong P\Omega_6^-(2)$, then for each of the three factorization types in m), Section 2.2.2, there exists a (non-maximal) factorization $G = AB$ with $|G : N| = 2$ such that there are no independent primes dividing $|A \cap N|$ and $|B \cap N|$, respectively.

- b) *If in addition to the two exceptional cases in a) $N \cong L_2(8)$, $L_2(p)$, p Mersenne prime, $L_3(3)$, $L_4(2)$, and $U_3(3)$, then there exist primes dividing $|A \cap N|$ and $|B \cap N|$ that are independent with respect to $\text{Aut}(N)$.*

For $N \cong L_2(8)$, $L_2(p)$, p Mersenne prime, $L_3(3)$, or $U_3(3)$, all pairs of primes dividing $|N|$ are not independent with respect to $\text{Aut}(N)$.

For $N \cong L_4(2)$ there exist factorizations $G = AB$ without primes independent with respect to $\text{Aut}(N)$ dividing $|A \cap N|$ and $|B \cap N|$, respectively.

Proof a) We mention that we can replace G by $AN \cap BN = (A \cap BN)(B \cap AN)$ to satisfy the condition $G = AN = BN$ in Theorem 1; since $N \not\leq A$ and $N \not\leq B$, none of the factors $(A \cap BN)$ and $(B \cap AN)$ equals $AN \cap BN$.

The first assertion follows now from an inspection of the proof of Theorem 1. Note however that in [35] the group $N = L_4(2) \cong A_8$ is treated as alternating group. Here the primes 2 and 7 are independent with respect to N , and any pair of a Sylow 2-subgroup with a Sylow 7-subgroup generates N . This proves the assertion for $L_4(2)$.

By [35, Table 1] there is a factorization $PSp_6(2) = \tilde{A}\tilde{B}$ with $\tilde{A} = O_6^-(2) = U_4(2) : 2$, $\tilde{B} = O_6^+(2)$ and $\tilde{A} \cap \tilde{B} = S_6 \times 2$ is maximal in \tilde{A} and \tilde{B} . We infer from [35, Table 1] again that there is a factorization $\tilde{A} = A(\tilde{A} \cap \tilde{B})$ with $A = GU_3(2)$ of order $2^3 \cdot 3^4$. It follows that $PSp_6(2) = A\tilde{B}$. Since a subgroup of order 5 in $PSp_6(2)$ is normalized by $S_3 \cdot 4$ and a subgroup of order 7 by a cyclic group of order 6, none of the prime divisors of $|A|$ is independent of the prime divisors of $|\tilde{B}|$.

Therefore the exceptional case $PSp_6(2)$ does actually occur.

Let $G = N\langle x \rangle$ with $N = U_4(3)$ and x the square of the diagonal automorphism. There are two conjugacy classes of involutions, represented by 2B and 2C in [13], such that $G = N\langle s \rangle = N\langle t \rangle$, s of type 2B, t of type 2C. There exists a subgroup $A_0 \cong L_3(4)$ in N normalized by s and a Sylow 3-subgroup D of N normalized by t such that st generates together with a Sylow 2-subgroup of A_0 a Sylow 2-subgroup of N . Setting $A = A_0\langle s \rangle$ and $B = D\langle t \rangle$, then $G = AB$, $A \cap N = A_0$, $B \cap N = D$. The prime 3 is not independent of the other prime divisors of $|N|$: the normalizer of a subgroup of order 7 has order 21 and there is a subgroup of order 3^4 normalized by A_6 , so in particular by elements of order 5 and 2.

Therefore the exceptional case $N = U_4(3)$ with $|G : N| \geq 2$ does actually occur.

The presented factorization of G has been constructed and verified using [13] and GAP [22].

b) For $N = L_4(2)$ a factorization $N = AB$ with $A \cong A_7$ and B a Sylow 2-subgroup provides an example: 2 is not independent of any other prime with respect to $\text{Aut}(N)$.

For all other groups, apart from those already treated as exceptions in a), only such cases in the proof of Theorem 1 have to be considered where one of the independent primes divides $|\text{Out}(N)|$. This leads to the groups $N \cong L_2(8), L_2(p)$, p Mersenne prime, $L_3(3), U_3(3)$. It is easily checked that all pairs of primes dividing $|N|$ are not independent with respect to $\text{Aut}(N)$. \square

Remark We have excluded the alternating groups from consideration in Theorem 2 and add some remarks about them here.

We recall that $A_5 \cong L_2(5)$, $A_6 \cong L_2(9)$ and $A_8 \cong L_4(2)$.

More generally, there are many examples of alternating groups A_n that possess a factorization $A_n = AB$ without independent primes dividing $|A|$ and $|B|$, respectively. For instance, if $n = 2^m$ and $2^m - 1$ not prime, then let $A = A_{n-1}$ and B a Sylow 2-subgroup of A_n . If p is a prime and $2 < p < n$, then a subgroup generated by a p -cycle is normalized by a suitable involution in A_n , because $2^n - 1$ is not prime and hence $p < n - 2$. We argue similarly if $n = 3^m$, $m \geq 2$, A is as above and B is a Sylow 3-subgroup of A_n : If $n - 2$ is not a prime, then a suitable 3-cycle centralizes a p -cycle (if p is odd) or a product of two disjoint transpositions (if $p = 2$). If $q := n - 2$ is a prime, then 3 divides $n - 3 = q - 1$ and therefore we find a 3-cycle that normalizes a subgroup generated by a q -cycle.

On the other hand, if $p \geq 5$ is a prime, then every non-trivial factorization $A_p = AB$ yields independent primes dividing the order of the factors. This can be seen as follows: In A_5 the primes 3 and 5 are independent and a Sylow 3-subgroup together with a Sylow 5-subgroup generate the whole group; the same is true in A_7 with the primes 5 and 7. This proves the assertion for $p = 5, 7$. For $p \geq 11$ there exists a prime q with $\frac{p}{2} \leq q \leq p - 4$; one can choose $q = 7$ for $p = 11$ or 13 and for

$p \geq 17$ this follows from [38]. By [35, Theorem D], we may assume that a p -cycle is contained in B and that $A_{p-4} \leq A$ since there exists no 5-transitive group of prime degree p other than A_p or S_p . Then a q -cycle is contained in B . As q does not divide $p-1$, p and q are independent.

There are also other examples for both situations. But it is an open problem to determine all alternating groups where every non-trivial factorization yields independent primes dividing the order of the factors.

3 The general case

Proof of Main Theorem

That (1) implies (2) is trivial. Also that (3) implies (1) is obvious: If $G = AB$ with $[A, B] \leq G_S$, then $\langle a, b \rangle' \leq G_S$ whence $\langle a, b \rangle$ is soluble for all $a \in A$ and $b \in B$.

It remains to prove that (2) implies (3). Suppose not and let G be a minimal counterexample. The proof proceeds in several steps.

(i) G has a unique minimal normal subgroup N , N is non-abelian, $C_G(N) = 1$ (in particular, $G_S = 1$), $N \leq [A, B] \leq R$ where $R/N = (G/N)_S$.

If N is a minimal normal subgroup of G , then one verifies easily that also $G/N = AN/N \cdot BN/N$ satisfies (2). G/N is not a counterexample whence $[A, B] \leq R$ with $R/N = (G/N)_S$. Since $[A, B] \trianglelefteq G$ and $[A, B] \neq 1$ (G being a counterexample), $N \leq [A, B]$. Clearly N is non-abelian, for otherwise R and hence $[A, B]$ would be soluble.

Suppose there are two distinct minimal normal subgroups N_1, N_2 of G . Let $R_i/N_i = (G/N_i)_S$, $i = 1, 2$. Choose d such that $R_i^{(d)} = N_i$, $i = 1, 2$ (d -th derived subgroup).

Then $[A, B]^{(d)} \leq R_1^{(d)} \cap R_2^{(d)} = N_1 \cap N_2 = 1$ and $[A, B]$ is soluble, contradiction.

Therefore G has a unique minimal normal subgroup N . As N is non-abelian, $N \cap C_G(N) = 1$, and it follows from $C_G(N) \trianglelefteq G$ that $C_G(N) = 1$.

(ii) $N \not\leq A$ and $N \not\leq B$.

Suppose that $N \leq A$. Since $B \neq 1$, we can choose $b \in B$ of prime order, say p . Then $N\langle b \rangle = (A \cap N\langle b \rangle)\langle b \rangle$ satisfies (2). If $N\langle b \rangle < G$, then $[N, \langle b \rangle] \leq (N\langle b \rangle)_S \leq C_{N\langle b \rangle}(N) = 1$ by (i). Therefore $b \leq C_G(N) = 1$, contradiction. Hence $N\langle b \rangle = G$.

Suppose first that N is simple. If $G = A$, then Theorems 1 and 2 of [26] imply that $b \in G_S = 1$, contradiction. If $G = A\langle b \rangle > A = N$, let $1 \neq g \in G$ be a q -element for a prime $q \neq p$. Then $g \in N = A$ and $\langle b, g \rangle$ is soluble by (2). Again the same theorems as before imply that $b \in G_S = 1$, a contradiction.

Hence N is not simple and in particular $b \notin N$. Consequently, N is the direct product of p copies of a non-abelian simple group L , permuted transitively by b . Therefore we can assume w.l.o.g. that there are automorphisms α_i of L , $1, \dots, p$, such that $(l_1, \dots, l_p)^b = (\alpha_2(l_2), \dots, \alpha_p(l_p), \alpha_1(l_1))$ for all $(l_1, \dots, l_p) \in N$.

Assume first that $p = 2$. Let $q \geq 5$ be a prime divisor of $|L|$. Since $G_S = 1$, by [23, Theorem 1.4] (see also [24], [25]), there exist (conjugate) elements $m_1, m_2 \in L$ of order q such that $\langle m_1, m_2 \rangle$ is not soluble. Set $n = (m_1, \alpha_2^{-1}(m_2))$. Then n is of order q and $\langle n, b \rangle \geq \langle n, n^b \rangle = \langle (m_1, \alpha_2^{-1}(m_2)), (m_2, \alpha_1(m_1)) \rangle$ is not soluble, contradicting (2).

Now let $p \geq 3$. By [37, Theorem A] there exist three involutions m_1, m_2, m_3 in L such that $\langle m_1, m_2, m_3 \rangle$ is not soluble unless $L = U_3(3)$. In the latter case we let

m_1, m_2 be elements of order 8 that generate a parabolic maximal subgroup $3^{1+2} : 8$ of L ([10, Table 8.5]) and choose m_3 as a 2-element outside this maximal subgroup. Setting $l_1 = m_1$, $l_2 = \alpha_2^{-1}(m_2)$, $l_3 = \alpha_3^{-1}\alpha_2^{-1}(m_3)$ and $l_i = 1$ for $3 < i \leq p$ in case $p \geq 5$, the element $n = (l_1, \dots, l_p) \in N$ is a 2-element. Then conjugating n with b , b^2 , it follows as above that $\langle n, b \rangle$ is not soluble, contradicting (2).

Hence $N \not\leq A$ and analogously $N \not\leq B$.

(iii) $AN = BN = G$ and G/N is soluble.

Suppose $AN = A(AN \cap B) < G$. Then $[A, AN \cap B] \leq (AN)_S \leq C_G(N) = 1$. It follows that $AN \cap B$ is normal in AN and that $N \cap B$ is normalized by B and centralized by A , whence $N \cap B = 1$ or $N \cap B = N$. The latter is impossible by (ii). Then $[N, AN \cap B] \leq N \cap AN \cap B = N \cap B = 1$ whence $AN \cap B \leq C_G(N) = 1$. This implies $AN = A$, contradicting (ii).

This shows that $AN = G$ and analogously $BN = G$.

Because of $AN = BN = AB = G$ and the fact that A and B satisfy (2) it follows that all for all primes $p \neq q$ every p -element and every q -element of G/N generate a soluble group. Then by [16, Theorem B] (applied to a hypothetical non-cyclic composition factor of G/N) or likewise by Theorems 1 and 2 of [26] it follows that G/N is soluble.

(iv) Let N be the direct product of k copies of a non-abelian simple group L . We denote the i -th component by L_i . Since G is a counterexample, it follows from (i), (ii), (iii) and Theorem 1 that $k \geq 2$.

To conclude the proof we have to show that $k \geq 2$ is not possible in a minimal counterexample. To this end, after introducing some notation, we define below groups $V_{i,X}$ whose crucial property is proved in (v). This property, together with a well-known result about the size of soluble subgroups of symmetric groups, will lead to the final contradiction.

Let $M_i = \text{Aut}(L_i) \cong \text{Aut}(L)$ and identify L_i with $\text{Inn}(L_i)$ whence $L_i \leq M_i$, $i = 1, \dots, k$. Then $N = L_1 \times \dots \times L_k \leq G \leq (M_1 \times \dots \times M_k)T \cong \text{Aut}(L) \text{ wr } S_k$ where $T \cong S_k$, the symmetric group of degree k (see e.g. [15, Proposition A.18.14]). Set $M = M_1 \times \dots \times M_k$. By slight abuse of notation we denote the elements of T by permutations t and conjugation of elements in $M_1 \times \dots \times M_k$ by any $t \in T$ inside the semidirect product $(M_1 \times \dots \times M_k)T$ is given by $(m_1, \dots, m_k)^t = (m_{1t^{-1}}, \dots, m_{kt^{-1}})$. Let ρ_i denote the projection of M onto M_i , $1 \leq i \leq k$.

For $X = G, A, B$ and $1 \leq i \leq k$ set

$$W_{i,X} = \{(m_1, \dots, m_k)t \in X \mid m_j \in M_j \text{ and } t \in T \text{ fixes } i\} \text{ and}$$

$$V_{i,X} = \{m_i \in M_i \mid \text{there exists } (m_1, \dots, m_k)t \in W_{i,X}\}.$$

It is clear that $W_{i,X}$ is a subgroup of X and $X \cap M \leq W_{i,X}$. Also $V_{i,X}$ is a subgroup of M_i , $\rho_i(X \cap M) \leq V_{i,X}$.

We claim:

(v) For each $1 \leq i \leq k$, $V_{i,G} = V_{i,A}$ and $V_{i,B} = 1$ or vice versa.

It suffices to prove the assertion for $i = 1$ (the other cases being analogous) and we set V_X and W_X for $V_{1,X}$ and $W_{1,X}$, respectively.

Let $l_1 \in L_1$ be arbitrary. There exist $a \in A$ and $b \in B$ with $(l_1, 1, \dots, 1) = ab$.

Let $a = (m_1, \dots, m_k)t$ and assume w.l.o.g. that in the decomposition of t in disjoint cycles the cycle containing 1 is just $(1, \dots, d)$ for some $1 \leq d \leq k$. Clearly, $b = t^{-1}(m_1^{-1}l_1, m_2^{-1}, \dots, m_k^{-1})$.

Set $m = (m_1, \dots, m_k)$ and $m' = (m_1^{-1}l_1, m_2^{-1}, \dots, m_k^{-1})$.

Then $a^d = m \cdot m^{t^{-1}} \cdots m^{t^{-(d-1)}} t^d = (m_1 m_2 \cdots m_d, *, \dots, *) t^d \in W_A$ and $b^d = m^t \cdots m^{t^d} t^{-d} = (m_d^{-1} m_{d-1}^{-1} \cdots m_2^{-1} m_1^{-1} l_1, *, \dots, *) t^{-d} \in W_B$.

It follows that $(l_1, *, \dots, *) = a^d b^d \in W_A W_B$. Therefore, $l_1 \in V_A V_B$, whence $L_1 \subseteq V_A V_B$. (Since we are only interested in the first component of the $M_1 \times \cdots \times M_k$ -parts of a^d , b^d and $a^d b^d$, we have denoted the other components by $*$ to avoid superfluous notation.)

Let $g \in W_G$ be arbitrary. By (iii) and (iv) $g = an$, $a = (m_1, \dots, m_k)t \in W_A$, $n = (l_1, \dots, l_k) \in N$. By what we have proved before, $m_1 l_1 \in V_A V_B$, whence $V_G = V_A V_B$.

We claim that V_A and V_B satisfy (2) in V_G . Since W_A and W_B satisfy (2), it suffices to show that for every prime p and every p -element $m \in V_X$ there exists a p -element $(m', m_2, \dots, m_k)t \in W_X$ ($X = A, B$) with $\langle m \rangle = \langle m' \rangle$. This follows easily: Choose $y = (m, m'_2, \dots, m'_k)\tilde{t} \in W_X$. Let the order of y be $p^a \cdot r$ where p does not divide r . Then $y^r = (m^r, *, \dots, *)\tilde{t}^r$ since \tilde{t} fixes position 1. The assertion follows with $m' = m^r$.

Minimality of G (recall that $k \geq 2$) now yields that $[V_A, V_B] \leq (V_G)_S$.

Since $L_1 \leq V_G \leq M_1$ and since L_1 is the unique minimal normal subgroup of M_1 , it follows that $[V_A, V_B] = 1$. This means that one of V_A and V_B contains L_1 and the other is trivial. Hence (v) holds.

(vi) $G \cap M = N$; moreover with appropriate choice of notation $B \cap M = 1$ and $\rho_i(A \cap N) = L_i$ for $1 \leq i \leq k$.

By (v) we may assume that $V_{1,G} \times \cdots \times V_{k,G} = V_{1,A} \times \cdots \times V_{h,A} \times V_{h+1,B} \times \cdots \times V_{k,B}$ and $V_{1,B} = \cdots = V_{h,B} = V_{h+1,A} = \cdots = V_{k,A} = 1$ for some $0 \leq h \leq k$. W.l.o.g. assume that $h \geq 1$. Then $L_1 \leq V_{1,G} = V_{1,A}$.

By (iii) G/N is soluble. Then $A/(A \cap N)$ is soluble and taking iterated derived groups, it follows that $L_1 \leq \rho_1(A \cap N)$. Since $G = AN$ by (iii), A acts transitively on $\{L_1, \dots, L_k\}$. As $A \cap N$ is normal in A , $N \leq \rho_1(A \cap N) \times \cdots \times \rho_k(A \cap N)$. Moreover, $B \cap M = 1$. Since $BN = G$ by (iii), the latter implies $G \cap M = N$.

(vii) Final contradiction.

It is well known (see for instance [7, Proposition 1.1.39]) that because of (vi) there is a partition of $\{1, \dots, k\}$ into subsets J_1, \dots, J_d such that $A \cap N = \times_{i=1}^d A_i$ where $A_i = A \cap \times_{j \in J_i} L_j$ and $|A_i| = |L|$, $1 \leq i \leq d$.

Suppose that $A \cap L_i = 1$ for all $1 \leq i \leq k$. Then $d \leq k/2$ (note that $k \geq 2$, see (iv)), whence $|A \cap N| \leq |L|^{k/2}$. Since $G = AN$, $|G| = |A||N|/|A \cap N| \geq |A||L|^{k/2}$. Since $B \cap N = 1$ by (5), B is isomorphic to a soluble subgroup of S_k and hence $|B| \leq 3^{k-1}$ by a result of Dixon (see [14, Theorem 5.8B]). Therefore $|G| \leq |A||B| \leq |A| \cdot 3^{k-1}$. It follows that $|L|^{k/2} \leq 3^{k-1} < 9^{k/2}$, whence $|L| < 9$, a contradiction.

Therefore we may assume that $A \cap L_1 \neq 1$. If $(l, 1, \dots, 1) \in A \cap L_1$ with $l \neq 1$, then because of $\rho_1(A \cap N) = L_1 (\cong L)$ all $([l, l'], 1, \dots, 1)$, $l' \in L$ are in $A \cap L_1$. But the elements $[l, l']$ generate L , whence $A \cap L_1 = L_1$.

As A acts transitively on $\{L_1, \dots, L_k\}$, it follows that $N \leq A$ which contradicts (ii). \square

Corollary 1 *Let N be a non-abelian simple group and $N \leq G = AB \leq \text{Aut}(N)$ with subgroups A and B satisfying (2) of the Main Theorem, then $A = 1$ or $B = 1$.*

Proof By the Main Theorem, $[A, B] \leq G_S = 1$. Therefore A and B are normal in G , whence $A = 1$ or $B = 1$ or $N \leq A \cap B$. But the latter implies $N = N' \leq [A, B] = 1$, a contradiction. \square

There is another corollary to the Main Theorem that generalizes a result of Carocca [12] on the solubility of \mathcal{S} -connected products of finite soluble groups:

Corollary 2 *Let $G = AB$ be a finite group with \mathcal{S} -connected subgroups A, B . Then $A_{\mathcal{S}} = A \cap G_{\mathcal{S}}$ and $B_{\mathcal{S}} = B \cap G_{\mathcal{S}}$.*

In particular, if A and B are soluble then G is soluble.

Proof By the Main Theorem, $A_{\mathcal{S}}G_{\mathcal{S}}$ is a normal subgroup of G . Since $A_{\mathcal{S}}G_{\mathcal{S}}/G_{\mathcal{S}}$ is soluble, $A_{\mathcal{S}}G_{\mathcal{S}}$ is soluble. Consequently, $A_{\mathcal{S}} \leq G_{\mathcal{S}}$ whence $A_{\mathcal{S}} = A \cap G_{\mathcal{S}}$. \square

References

1. S. Abe, N. Iiyori, A generalization of prime graphs of finite groups. *Hokkaido Math. J.* 29 (2000) 391-407.
2. B. Amberg, A. Carocca, L. Kazarin, Criteria for the solubility and non-simplicity of finite groups. *J. Algebra* 285 (2005) 58-72.
3. B. Amberg, S. Franciosi, F. de Giovanni, *Products of groups*. Clarendon Press (1992).
4. B. Amberg, L. Kazarin, On the soluble graph of a finite simple group. *Comm. Algebra* 41 (2013) 2297-2309.
5. M. Asaad and A. Shaalan, On the supersolvability of finite groups. *Arch. Math.* 53 (1989) 318-326.
6. R. Baer, Supersoluble immersion. *Canad. J. Math.* 11 (1959) 353-369.
7. A. Ballester-Bolinches, L. M. Ezquerro, *Classes of finite groups*. Springer (2006).
8. A. Ballester-Bolinches, M. C. Pedraza-Aguilera, On finite soluble products of \mathcal{N} -connected groups. *J. Group Theory* 2 (1999) 291-299.
9. J. Beidleman and H. Heineken, Pairwise \mathcal{N} -connected products of certain classes of finite groups. *Comm. Algebra* 32 (2004) 4741-4752.
10. J. N. Bray, D. F. Holt, C. M. Roney-Dougal, *The maximal subgroups of the low-dimensional finite classical groups*. Cambridge University Press (2013).
11. A. Carocca, A note on the product of \mathcal{F} -subgroups in a finite group. *Proc. Edinburgh Math. Soc.* (2) 39 (1996) 37-42.
12. A. Carocca, Solvability of factorized finite groups. *Glasgow Math. J.* 42 (2000) 271-274.
13. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups*. Clarendon Press (1985).
14. J. D. Dixon, B. Mortimer, *Permutation groups*. Springer (1996).
15. K. Doerk, T. Hawkes, *Finite soluble groups*. Walter de Gruyter (1992).
16. S. Dolfi, R. M. Guralnick, M. Herzog, C. E. Praeger, A new solvability criterion for finite groups. *J. London Math. Soc.* 85 (2012) 269-281.
17. M. P. Gállego, P. Hauck, L. S. Kazarin, A. Martínez-Pastor, M. D. Pérez-Ramos, Products of finite connected subgroups. Preprint. <http://arxiv.org/abs/1908.03347>
18. M. P. Gállego, P. Hauck, M. D. Pérez-Ramos, Soluble products of connected subgroups. *Rev. Mat. Iberoamericana* 24 (2008) 433-461.
19. M. P. Gállego, P. Hauck, M. D. Pérez-Ramos, On 2-generated subgroups and products of groups. *J. Group Theory* 11 (2008) 851-867.
20. M. P. Gállego, P. Hauck, M. D. Pérez-Ramos, Saturated formations and products of connected subgroups. *J. Algebra* 333 (2011) 105-119.
21. M. P. Gállego, P. Hauck, M. D. Pérez-Ramos, 2-Engel relations between subgroups. *J. Algebra* 447 (2016) 31-55.
22. The GAP Group, GAP – Groups, Algorithms, and Programming, <http://www.gap-system.org>, Version 4.10.2, 2019.
23. N. Gordeev, F. Grunewald, B. Kunyavskii, E. Plotkin, Baer-Suzuki theorem for the solvable radical of a finite group. *C. R. Acad. Sci. Paris Sr. I* 347 (2009) 217-222.
24. N. Gordeev, F. Grunewald, B. Kunyavskii, E. Plotkin, From Thompson to Baer-Suzuki: A sharp characterization of the solvable radical. *J. Algebra* 323 (2010) 2888-2904.
25. S. Guest, A solvable version of the Baer-Suzuki theorem. *Trans. Amer. Math. Soc.* 362 (2010) 5909-5946.
26. S. Guest, D. Levy, Criteria for solvable radical membership via p -elements. *J. Algebra* 415 (2014) 88-111.

27. R. Guralnick, B. Kunyavskii, E. Plotkin, A. Shalev, Thompson-like characterizations of the solvable radical. *J. Algebra* 300 (2006) 363-375.
28. F. Grunewald, B. Kunyavskii, E. Plotkin, Characterization of solvable groups and solvable radical. *Internat. J. Algebra Comput.* 23 (2013) 1011-1062.
29. P. Hauck, A. Martínez-Pastor, M. D. Pérez-Ramos, Products of \mathcal{N} -connected groups. *Illinois J. Math.* 47 (2003) 1033-1045.
30. C. Hering, M. W. Liebeck, J. Saxl, The factorizations of the finite exceptional groups of Lie type. *J. Algebra* 106 (1987) 517-527.
31. B. Huppert, Zweifach transitive, auflösbare Permutationsgruppen. *Math. Z.* 68 (1957) 126-150.
32. B. Huppert, *Endliche Gruppen I*. Springer (1967).
33. N. Iiyory, p -Solvability and a generalization of prime graphs of finite groups. *Comm. Algebra* 30 (2002) 1679-1691.
34. P. Kleidman, M. Liebeck, *The subgroup structure of the finite classical groups*. Cambridge University Press (1990).
35. M. W. Liebeck, C. E. Praeger, J. Saxl, The maximal factorizations of the finite simple groups and their automorphism groups. *Memoirs AMS* 86, no. 432 (1990).
36. R. Maier, A completeness property of certain formations. *Bull. London Math. Soc.* 24 (1992) 540-544.
37. G. Malle, J. Saxl, T. Weigel, Generation of classical groups. *Geom. Dedicata* 49 (1994) 85-116.
38. S. Ramanujan, A proof of Bertrand's postulate. *J. Indian Math. Soc.* 11 (1919) 181-182.
39. J. Thompson, Nonsolvable finite groups all of whose local subgroups are solvable. *Bull. Amer. Math. Soc.* 74 (1968) 383-437.
40. J. Wiegold, A. G. Williamson, The factorisation of the alternating and symmetric groups. *Math. Z.* 175 (1980) 171-179.
41. M. Zorn, Nilpotency of finite groups. *Bull. Amer. Math. Soc.* 42 (1936) 485-486.
42. K. Zsigmondy, Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* 3 (1892) 265-284.