J. Group Theory, Ahead of Print
DOI 10.1515/jgth-2025-0050

Solvable groups in which every real element has prime power order

Alessandro Giorgi

Communicated by Gareth Tracey

Abstract. We study the finite solvable groups G in which every real element has prime power order. We divide our examination into two parts: the case $\mathbf{O}_2(G) > 1$ and the case $\mathbf{O}_2(G) = 1$. Specifically we prove that if $\mathbf{O}_2(G) > 1$, then G is a $\{2, p\}$-group. Finally, by taking into consideration the examples presented in the analysis of the $\mathbf{O}_2(G) = 1$ case, we deduce some interesting and unexpected results about the connectedness of the real prime graph $\Gamma_{\mathbb{R}}(G)$. In particular, we find that there are groups such that $\Gamma_{\mathbb{R}}(G)$ has 3 or 4 connected components.

1 Introduction

The prime graph $\Gamma(G)$ of a finite group G, also known as the Gruenberg–Kegel graph of G, constitutes an important environment to study the "relations" between the elements of G and more generally to analyze the structure of the group G. The graph is defined in this way: the vertices of $\Gamma(G)$ are the prime divisors of $|G|$ and there is an edge between the vertices p and q if G contains an element of order pq.

Reality is an interesting and useful notion in finite group theory. An element $x \in G$ is said to be *real* if it is G-conjugate to its inverse x^{-1}, i.e. if there exists $g \in G$ with $x^g = x^{-1}$. We can then define, by considering only the real elements of G, the *real prime graph* $\Gamma_{\mathbb{R}}(G)$ analogously to the prime graph: the vertices of $\Gamma_{\mathbb{R}}(G)$ are the primes p for which G contains a real element of order p and the vertices p and q are connected if G contains a real element of order pq.

In this paper, we study the finite solvable groups G for which all the vertices of $\Gamma_{\mathbb{R}}(G)$ are isolated, starting from the results obtained by Dolfi, Gluck and Navarro in [2], where the authors investigated the finite solvable groups for which 2 is an isolated vertex of $\Gamma_{\mathbb{R}}(G)$. Taking into consideration the above definition of $\Gamma_{\mathbb{R}}(G)$, it is clear that the fact that the vertices of $\Gamma_{\mathbb{R}}(G)$ are all isolated is equivalent to the fact that every real element of G has prime power order. The analogous problem for $\Gamma(G)$ was studied in 1957 by Higman in [6], in which he considered both solvable and insolvable groups G for which every element has prime power order. For the solvable case, his main result contained in [6, Theorem 1] tells us that G

must be a p-group (which could be considered as the trivial case for this question) or a $\{p, q\}$-group ([6, Theorem 1] actually says a lot more about the structure of G).

It is easy to see that if G contains a real element other than the identity, then $|G|$ is even. Also, since every involution is a real element, we can conclude that if G has non-trivial real elements, then 2 is a vertex of $\Gamma_{\mathbb{R}}(G)$. So what we initially wanted to prove, following Higman, was that if every real element in G has prime power order, then G must be either a 2-group or a $\{2, p\}$-group. However, as we will see, that is not true in general. Still we have been able to prove it in the case that $\mathbf{O}_2(G) > 1$, where $\mathbf{O}_2(G)$ is the largest normal 2-subgroup of G.

On a more technical side, we note that, since the real elements of G are the real elements of $\mathbf{O}^{2'}(G)$, the smallest normal subgroup of G with odd index, when investigating the real elements of a finite group, we can assume that $G = \mathbf{O}^{2'}(G)$. Moreover, since $\mathbf{O}^{2'}(G)$ has odd index, it contains a Sylow 2-subgroup of G. Therefore, as $\mathbf{O}_2(G)$ is contained in every Sylow 2-subgroup of G, we have

$$\mathbf{O}_2(G) \leq \mathbf{O}_2(\mathbf{O}^{2'}(G)).$$

In particular, if $\mathbf{O}_2(G) > 1$, then also $\mathbf{O}_2(\mathbf{O}^{2'}(G)) > 1$.

With that being said, our first main result is the following.

Theorem A. *Suppose that G is a finite solvable group with $\mathbf{O}^{2'}(G) = G$. Let $N = \mathbf{O}_2(G)$. Suppose also that G is not a 2-group and $N > 1$. Then the following are equivalent:*

(1) *every real element of G has prime power order;*

(2) *G is a $\{2, p\}$-group, with p an odd prime, $G = N \rtimes (K \rtimes Q)$ is a 2-Frobenius group, with K a cyclic p-group and Q a cyclic 2-group. In particular, if $|Q| = 2$, then $K \rtimes Q$ is a dihedral group. In any case, every element of K is real and inverted by z, where z is the only involution of Q;*

(3) *every element of G has prime power order.*

But, as we already mentioned above, it is not generally true that if every real element of G has prime power order, then G must be a 2-group or a $\{2, p\}$-group. As a matter of fact, studying the case $\mathbf{O}_2(G) = 1$, even though we have not been able in this paper to precisely describe the structure of such groups, we did find that there are groups G and H such that every real element has prime power order and $|G|$ and $|H|$ have, respectively, three and four prime divisors, as we will see in Example 4.2. We should now recall that, by [3, Corollary B], since we are assuming G solvable, for every prime p dividing $|G|$, G contains a real element of order p, so p is a vertex of $\Gamma_{\mathbb{R}}(G)$ by definition (and the same holds for H). In the framework of the real prime graph $\Gamma_{\mathbb{R}}(G)$, since every isolated vertex is obviously a connected component, if we write $n(\Gamma)$ to indicate the number of connected components of a graph Γ, then we can state this finding by saying that there exist finite solvable groups G and H with $n(\Gamma_{\mathbb{R}}(G)) = 3$ and $n(\Gamma_{\mathbb{R}}(H)) = 4$.

This fact is somewhat unexpected because it goes against the usual similarity of properties that $\Gamma_{\mathbb{R}}(G)$ has in respect to two other notorious graphs associated to G, the prime graph on real character degrees $\Gamma_{\mathrm{cd},\mathbb{R}}(G)$ and the prime graph on real class sizes $\Gamma_{\mathrm{cs},\mathbb{R}}(G)$, for which it is known that $n(\Gamma_{\mathrm{cd},\mathbb{R}}(G)) \leq 2$ and $n(\Gamma_{\mathrm{cs},\mathbb{R}}(G)) \leq 2$, as we will explain better later.

It could also be an interesting topic of study to investigate how much the number of prime divisors of $|G|$ can be increased while preserving the condition that every real element of G has prime power order, which is closely related, though not equivalent, to the open problem of determining the least upper bound for $n(\Gamma_{\mathbb{R}}(G))$.

2 Preliminary results

We begin by fixing the notation and terminology that will be used throughout the paper. For a group G, $\mathbf{Z}(G)$ denotes its center, G' denotes its derived subgroup, $\mathbf{F}(G)$ denotes its Fitting subgroup, $\Phi(G)$ denotes its Frattini subgroup and G^{∞} denotes its nilpotent residual. An abelian group is said to be homocyclic if it is a direct product of pairwise isomorphic cyclic groups.

For our study, we will need some basic but nevertheless fundamental properties of real elements. Let us start with the following lemma (see [3, Lemma 3.2] for a proof).

Lemma 2.1. *Let G be a finite group.*

(1) *If $x \in G$ is real, then there is a 2-element $y \in G$ with $x^y = x^{-1}$.*

(2) *If $x \in G$ is real, then x^m is real for every integer m.*

(3) *Suppose that $N \trianglelefteq G$ and that $xN \in G/N$ is real. Suppose also that $o(xN)$ is odd. Then there is a real $y \in G$ with $xN = yN$.*

(4) *If Q is a 2-group acting non-trivially on G, then there are $1 \neq x \in G$ and $q \in Q$ with $x^q = x^{-1}$.*

The next lemma will be used in several subsequent proofs to conclude various arguments by contradiction, since it gives us a sufficient condition (actually also a necessary condition, but we only need sufficiency) for the existence of real elements of non-prime power order.

Lemma 2.2. *Let G be a finite group and let $x, y \in G$ be real elements whose orders $o(x) = p$ and $o(y) = q$ are distinct primes. Suppose that x and y are inverted by the same $g \in G$ and that $xy = yx$. Then xy is real inverted by g and $o(xy) = pq$.*

We note that Lemma 2.2 is still valid even if $o(x) = p^\alpha$ and $o(y) = q^\beta$, but it is sufficient to enunciate it in this form, since by Lemma 2.1 (2), we can always consider suitable powers of x and y and get real elements with prime order.

Following [2], we say that a finite group G *satisfies* **R** if every real element has 2-power order or $2'$-order, and we say that G *satisfies* **P** if every real element has prime power order.

We now want to prove that our working hypotheses descend to the quotient. It is well known that solvability does and it is not difficult to verify that if G is a finite group with $\mathbf{O}^{2'}(G) = G$, then, if $N \trianglelefteq G$, we have $\mathbf{O}^{2'}(G/N) = G/N$. Property **P** requires a little bit more work.

Lemma 2.3. *Let G be a finite group and let $N \trianglelefteq G$. If G satisfies* **P***, then G/N satisfies* **P**.

Proof. Since G satisfies **P**, obviously, G satisfies **R**. So, by [2, Lemma 2.2], we have that G/N satisfies **R**, that is, every real element of G/N has 2-power order or odd order. Suppose by contradiction that G/N contains a real element xN of odd non-prime power order. Then, by Lemma 2.1 (3), there exists a real $y \in G$ with $xN = yN$. Then we have $o(xN) \mid o(y)$ and so y is a real element of G with non-prime power order, contradicting our assumptions. □

It is worth noting that Lemma 2.3 could also be proved directly by extending [2, Lemma 2.1] to our case, instead of integrating [2, Lemma 2.2] with Lemma 2.1 (3) as we did above.

We now recall [2, Theorem A], which establishes the basis for our work.

Theorem 2.4. *Suppose that G is a finite solvable group with $\mathbf{O}^{2'}(G) = G$. Assume that every real element of G is either a 2-element or a $2'$-element. Let $N = \mathbf{O}_2(G)$ and $Q \in \mathrm{Syl}_2(G)$, and assume that G is not a 2-group. Then*

(1) *G/N has a normal 2-complement K/N and Q/N is cyclic or generalized quaternion. If zN is the unique involution of Q/N, then*

$$C_{K/N}(Q/N) = C_{K/N}(zN).$$

(2) *Suppose that $N > 1$. Then $N = \mathbf{F}(G)$, Q/N is cyclic and G splits over N. If $|Q/N| > 2$, then K/N is cyclic. In any case, K/F_2 is metabelian and F_2/N*

is abelian, where $F_2/N = \mathbf{F}(G/N)$. *If* $|G|$ *is coprime to* 3*, then* K/F_2 *is abelian.*

We are now going to see some lemmas that give us some initial information on the structure of the group G/N described in Theorem 2.4. For the sake of brevity, we are going to write G instead of G/N, K instead of K/N and so on.

Lemma 2.5. *Let* G *be a finite group with* $G = K \rtimes Q$ *and* $\mathbf{O}^{2'}(G) = G$*, where* K *is the normal* 2*-complement and* $Q \in \mathrm{Syl}_2(G)$*. Then we have* $[K, Q] = K$*.*

Proof. Since $K \trianglelefteq G$, then $[K, Q] \leq K$ and we also know that

$$[K, Q] \trianglelefteq \langle K, Q \rangle = G.$$

We can consider $L = [K, Q]Q$. We have $L \trianglelefteq G$, since $[K, Q] \trianglelefteq G$ and

$$Q^g = Q^{qk} = Q^k \subseteq [K, Q]Q \quad \text{for every } g = qk \in G,$$

with $q \in Q$ and $k \in K$. Then L is a normal subgroup of G with odd index and so it must be $L = G$. Then it follows that $[K, Q] = K$. □

Lemma 2.6. *Let* G *be a finite group with* $G = K \rtimes Q$*, where* $Q \in \mathrm{Syl}_2(G)$ *and* K *is the normal* 2*-complement of* G*. Suppose that* $\mathbf{O}^{2'}(G) = G$ *and that* Q *has a unique involution* z*, and assume that* $C_K(z) = C_K(Q)$*. Then* K *is abelian if and only if* $C_K(z) = 1$ *(if and only if* z *inverts every element of* K*).*

Proof. Suppose K is abelian. Since $(|Q|, |K|) = 1$, by the coprime action of Q on K, we have $K = [K, Q] \times C_K(Q)$ (see, for instance, [9, 8.4.2]). But by Lemma 2.5, we know that $[K, Q] = K$ and so $C_K(Q) = 1$. It follows that $C_K(z) = C_K(Q) = 1$.

Conversely, suppose that $C_K(z) = 1$. So z induces an automorphism on K of order 2 with no fixed points. It is a well-known result that z then acts on K as the inversion. Since it is easy to see that a group in which the inversion is an automorphism is abelian, we conclude. □

Let us finish this section with a lemma that contains an idea which will be used several times later on.

Lemma 2.7. *Let* G *be a finite group with* $G = K \rtimes Q$*, where* $Q \in \mathrm{Syl}_2(G)$ *and* K *is the normal* 2*-complement of* G*. Suppose that* $\mathbf{O}^{2'}(G) = G$ *and that* Q *has a unique involution* z*, and assume that* $C_K(z) = C_K(Q)$*. Suppose also that* G *satisfies* $\mathbf{P}$ *and that* K *is nilpotent. Then* K *is a* p*-group for some odd prime* p*.*

Proof. Assume by contradiction that there are at least two odd primes p, q dividing $|K|$, with $p \neq q$. By nilpotence, we have that the p-elements commute with the q-elements. Consider now the actions of z on $\mathbf{O}_p(K)$ and on $\mathbf{O}_q(K)$. If z centralizes, to fix ideas, $\mathbf{O}_p(K)$, then $\mathbf{O}_p(K) \leq C_K(z) = C_K(Q)$. So we would have $Q \leq C_G(\mathbf{O}_p(K))$. In particular, $\mathbf{O}_{p'}(K) \rtimes Q$ would be a normal subgroup of G with odd index, contradicting the fact that $\mathbf{O}^{2'}(G) = G$. The same goes for $\mathbf{O}_q(K)$. So the actions of z on both are not trivial. Then, by Lemma 2.1 (4), there exist real elements $x \in \mathbf{O}_p(K)$ and $y \in \mathbf{O}_q(K)$ inverted by z, respectively of order p and q, that commute. But then, by Lemma 2.2, xy is a real element, inverted by z, of order pq, contradicting **P**. Hence K must be a p-group. □

3 The case $\mathbf{O}_2(G) > 1$

In order to treat this case, it is necessary to repeat some ideas and results introduced in [2].

Standard Hypotheses. Suppose that $G = KQ$, where $K > 1$ is normal of odd order, $Q \in \mathrm{Syl}_2(G)$ is cyclic or generalized quaternion and $C_K(Q) = C_K(z)$, with z the unique involution of Q. Suppose also that $\mathbf{O}^{2'}(G) = G$. Assume that G acts on a 2-group V and that $C_G(v)$ has a normal Sylow 2-subgroup for all $1 \neq v \in V$. In this case, we say that G satisfies the Standard Hypotheses with respect to V.

The following theorem (see [2, Theorem 3.1]) explains the introduction of such hypotheses.

Theorem 3.1. *Suppose G is a finite solvable group with $\mathbf{O}^{2'}(G) = G$. Assume that G satisfies* **R** *and that $G > N = \mathbf{O}_2(G) > 1$. Then there exists a subgroup H of G such that $G = NH$, with $N \cap H = 1$, and H satisfies the Standard Hypotheses with respect to N. Moreover, $\mathbf{O}_{2'}(G) \leq \mathbf{Z}(G)$.*

Conversely, if $H = K \rtimes Q$, with $Q \in \mathrm{Syl}_2(H)$, satisfies the Standard Hypotheses with respect to V, then $G = V \rtimes H$ satisfies **R**.

We would like now to have a set of assumptions that descend to quotients. Recall that, in a group action of Q on K, A/B is a *Q-invariant p-section*, for a prime p, if A, B are Q-invariant subgroups of K, $B \trianglelefteq A$ and A/B is a p-group.

Hypotheses H2. Let G be a group with a cyclic Sylow 2-subgroup $Q > 1$ and a normal 2-complement K. Suppose that $\mathbf{O}^{2'}(G) = G$ and $C_K(Q) = C_K(z)$, where z is the unique involution of Q. Assume also that, for every prime p and for every Q-invariant p-section A/B of K, $[A/B, Q]$ is cyclic. In this case, we say that G satisfies (H2).

Then we have that Hypotheses H2 descend to quotients on $N \trianglelefteq G$, $N \leq K$ (see [2, Lemma 3.2]).

Lemma 3.2. *Suppose that G satisfies (H2) and let $N \trianglelefteq G$, $N \leq K$. Then G/N also satisfies (H2).*

The following proposition clarifies the connection between the Standard Hypotheses and (H2) (see [2, Proposition 3.4]).

Proposition 3.3. *If $G = KQ$ satisfies the Standard Hypotheses, then G satisfies (H2).*

Before we can start with our own investigation, we need two other results from [2], which describe the chief factors and the structure of the Sylow subgroups of a group G satisfying (H2) (see respectively [2, Proposition 3.7] and [2, Theorem 3.9]).

Proposition 3.4. *Let G satisfy (H2). Let p be a prime dividing $|K|$ and let $P = \mathbf{O}_p(G)$, $R = \Phi(G) \cap P$ and $X = P/R$. If $X \neq 1$, then X is a noncentral chief factor of G, $P \in \mathrm{Syl}_p(G)$ and $R = \Phi(P)$.*

Theorem 3.5. *Let G satisfy (H2) with $K > 1$. Let p be a prime dividing $|K|$ and $P \in \mathrm{Syl}_p(G)$. Then P is homocyclic abelian of rank at most 3. Also, we have $\mathbf{Z}(G) = 1$. If p divides $|K/K'|$, then P is cyclic.*

The first consequence that we deduce is the following.

Proposition 3.6. *Let G satisfy (H2) and* **P** *and suppose that G is not a 2-group. Then $\mathbf{F}(G) = \mathbf{F}(K)$ and $\mathbf{F}(G) \in \mathrm{Syl}_p(G)$, for p an (odd) prime.*

Proof. Let us start by proving that $\mathbf{F}(G) = \mathbf{F}(K)$. To do so, it is sufficient to show that $\mathbf{F}(G)$ has odd order. Indeed, in that case, $\mathbf{F}(G) \leq K$ and so $\mathbf{F}(G) \leq \mathbf{F}(K)$. The other inclusion is trivial. Suppose then by contradiction that $\mathbf{F}(G)$ has even order. Then it must be $\mathbf{O}_2(G) > 1$, so $z \in \mathbf{O}_2(G)$, where z is the unique involution of Q. Therefore, z commutes with $\mathbf{O}_{2'}(G) = K$, that is, $K = C_K(z) = C_K(Q)$. Then $Q \trianglelefteq G$ and $G = K \times Q$. Since $\mathbf{O}^{2'}(G) = G$, we have $G = Q$ and $K = 1$, contradicting the assumptions.

Working by contradiction, assume now that $\mathbf{F}(G)$ is not a p-group. Then there exist distinct primes p, q, with $\mathbf{O}_p(G), \mathbf{O}_q(G) > 1$. Let us consider the action of z on $\mathbf{O}_j(G)$, for $j = p, q$. If the action is trivial, then, as in Lemma 2.7, we have $Q \leq C_G(\mathbf{O}_j(G))$. So $C_G(\mathbf{O}_j(G))$ is a normal subgroup with odd index. Therefore, since $\mathbf{O}^{2'}(G) = G$, we have $C_G(\mathbf{O}_j(G)) = G$, that is, $\mathbf{O}_j(G) \leq \mathbf{Z}(G)$, whereas $\mathbf{Z}(G) = 1$ by Theorem 3.5. So both those actions are not trivial. Thus, by Lemma 2.1 (4), there exist a non-trivial real p-element x and a non-trivial real q-element y both inverted by z, and they commute. Then, by Lemma 2.2, xy is a real element of order pq, contradicting property **P**. So $\mathbf{F}(G) = \mathbf{O}_p(G)$ for some (odd) prime p.

Finally, we note that a group satisfying (H2) is solvable by the Feit–Thompson theorem. It is well known that, in a finite non-trivial solvable group, $\mathbf{F}(G) > 1$ and $\mathbf{F}(G) > \Phi(G)$. Then, since $R = \mathbf{F}(G) \cap \Phi(G) = \Phi(G)$, we have

$$\mathbf{F}(G)/R = \mathbf{F}(G)/\Phi(G) > 1.$$

Therefore, by Proposition 3.4, we conclude that $\mathbf{F}(G) \in \mathrm{Syl}_p(G)$. □

We are almost ready to prove the main theorem of this paper. We just need to simplify our work with one last observation. Suppose G is a finite solvable group, with $\mathbf{O}^{2'}(G) = G$, $G > N = \mathbf{O}_2(G) > 1$ and assume that G satisfies **P**. In particular, we can apply Theorem 2.4 to G. Since we are assuming $N > 1$, if we also suppose $|Q/N| > 2$, where $Q \in \mathrm{Syl}_2(G)$, then by Theorem 2.4 (2), we have that K/N is cyclic. Therefore, by Lemma 2.7, or even with little more work by Lemma 2.6, we know that K/N is a p-group.

So it suffices to consider the case $|Q/N| = 2$. We begin with an auxiliary result that will play a key role in the proof of the main theorem.

Proposition 3.7. *Let $H = KQ$ satisfy* (H2) *and* **P**, *with $|Q| = 2$. Suppose that K is not nilpotent and that $K/\mathbf{F}(H)$ is abelian. Then H is 2-Frobenius with lower kernel a homocyclic abelian q-group of rank 2, upper complement of order 2 and lower complement a cyclic p-group, with $p \neq q$.*

Proof. Firstly, let us consider H/K'. We note that H/K' still satisfies (H2) and **P** and therefore its normal 2-complement K/K' is a p-group by Lemma 2.7. Also, by Lemma 2.5, we have $[K/K', QK'/K'] = K/K'$. Then $K/K' = [K/K', Q]$, which is cyclic since H satisfies (H2).

We have $\mathbf{F}(H) = \mathbf{F}(K)$ by Proposition 3.6. Thus $K/\mathbf{F}(K)$ is abelian and therefore $K' \leq \mathbf{F}(K)$. Furthermore, by Proposition 3.6, $\mathbf{F}(K)$ is a q-group, for some prime q dividing $|K|$. Since we are assuming that K is not nilpotent, it must be that $p \neq q$. Then it must also be that $K' = \mathbf{F}(K)$; otherwise, we would have $p \mid |\mathbf{F}(K)|$. For convenience, let $L = K' = \mathbf{F}(K)$. We note that $L \in \mathrm{Syl}_q(H)$, so by Theorem 3.5, L is homocyclic of rank at most 3. From what has been said so far, we have $K = L \rtimes P$, where $P \in \mathrm{Syl}_p(K)$. Moreover, up to conjugacy, we can assume that $z \in N_H(P)$, where z is such that $Q = \langle z \rangle$. Indeed, by the Frattini argument, we have $H = KN_H(P)$ and so

$$2|K| = |H| = |KN_H(P)| = \frac{|K||N_H(P)|}{|K \cap N_H(P)|} = \frac{|K||N_H(P)|}{|N_K(P)|},$$

so that $|N_H(P)| = 2|N_K(P)|$. Then we can assume that z acts on P. We now prove that $P\langle z\rangle$ is dihedral. Indeed, since P is a cyclic p-group and p is odd, we know that $\mathrm{Aut}(P)$ is cyclic and hence it has a unique element of order 2, namely the inversion map. Therefore, either $C_P(z) = P$ or z acts on P as the inversion. So $P\langle z\rangle$ is either abelian or dihedral. But $\mathbf{O}^{2'}(P\langle z\rangle) = P\langle z\rangle$ and so $P\langle z\rangle$ is not abelian. Then $P\langle z\rangle$ is dihedral, and in particular, it is a Frobenius group.

We want now to verify that $C_L(P) = 1$, which, since L is abelian, follows easily once we prove that $\mathbf{Z}(K) = 1$. Assume by contradiction that $1 \neq \mathbf{Z}(K)$. Obviously, $\mathbf{Z}(K) \trianglelefteq H$. Consider then the action of z on $\mathbf{Z}(K)$. This action is not trivial; otherwise, we would have $1 \neq \mathbf{Z}(K) \leq \mathbf{Z}(H)$, contradicting the fact that $\mathbf{Z}(H) = 1$ by Theorem 3.5. So, by Lemma 2.1 (4), there is a real element $1 \neq x \in \mathbf{Z}(K)$, $x = ly$, $l \in L$, $y \in P$, inverted by z. If $l \neq 1$, then an appropriate power of x would be a real q-element inverted by z that commutes with every element of P. Recalling that every element of P is a real p-element inverted by z, by Lemma 2.2, we would get a real element of non-prime power order, contradicting **P**. So $l = 1$ and x is a real p-element inverted by z that commutes with every element of L. But z acts non-trivially on L. Otherwise we would have $z \in C_H(L)$. Since we also have $C_H(L) \trianglelefteq H$ and $\mathbf{O}^{2'}(H) = H$, we would get $1 < L \leq \mathbf{Z}(H)$, contradicting Theorem 3.5. So L contains at least one non-trivial real q-element inverted by z by Lemma 2.1 (4). As before, that goes against **P**.

We can now prove that L has precisely rank 2. We have $\Phi(L) \trianglelefteq H$ (actually, by Proposition 3.4, $\Phi(L) = \Phi(H)$). So $P\langle z\rangle$ acts on $\Phi(L)$. Let us consider the quotient $L/\Phi(L)$. Using the bar notation, we have that $\overline{L}$ is a $\mathbb{Z}_q$-vector space of dimension at most 3, by Theorem 3.5. By the coprime action of P on L, we have $C_{\overline{L}}(P) = \overline{C_L(P)} = 1$ (see, for instance, [9, 8.2.2]). Recall also that $P\langle z\rangle$ is a Frobenius group, with kernel P and complement $\langle z\rangle$. So, considering $\overline{L}$ as a $\mathbb{Z}_q[P\langle z\rangle]$-module, by [7, Theorem 15.16], we deduce

$$\dim_{\mathbb{Z}_q}(\overline{L}) = |\langle z\rangle| \dim_{\mathbb{Z}_q}(C_{\overline{L}}(\langle z\rangle)).$$

In particular, $2 \mid \dim_{\mathbb{Z}_q}(\overline{L})$ and $\dim_{\mathbb{Z}_q}(\overline{L}) \leq 3$, so it must be $\dim_{\mathbb{Z}_q}(\overline{L}) = 2$. Then L has rank 2.

At this point, it remains to prove that $K = L \rtimes P$ is a Frobenius group. Considering the quotient $L/\Phi(L)$, we can assume that $\Phi(L) = 1$. By Proposition 3.4, we then have that L is minimal normal in H. Also, if we write $\mathbb{F} = \mathbb{Z}_q$, we have seen above that L is an $\mathbb{F}$-vector space of dimension 2. So L is an irreducible $\mathbb{F}[H]$-module. Since $K \trianglelefteq H$, by Clifford's theorem, we know that L is completely reducible as an $\mathbb{F}[K]$-module (which we write as L_K). If L_K is irreducible, then it is a faithful and irreducible $\mathbb{F}[P]$-module, and P is cyclic. It is well known that P then acts fixed-point free on L. Suppose therefore that $L_K = L_1 \oplus L_2$, with L_1, L_2 irreducible $\mathbb{F}[K]$-modules. We want to verify that the irreducible components L_1, L_2 have the same kernel. If L_K is homogeneous, then it is obvious, since $L_1 \cong L_2$ as $\mathbb{F}[K]$-modules. Assume that L_K is not homogeneous. By Clifford's theorem, we know that $H/K \cong \langle z \rangle$ acts transitively on the set of homogeneous components, in this case $\{L_1, L_2\}$. Thus $L_1^z = L_2$ and therefore $C_K(L_1)^z = C_K(L_1^z) = C_K(L_2)$, that is, the kernels are z-conjugate. But $C_K(L_1) = LX$ for some $X \leq P$, and so $C_K(L_2) = C_K(L_1)^z = L^z X^z = LX$, since $L \trianglelefteq H$ and z normalizes every subgroup of P. In any case, we have proved that $C_K(L_1) = C_K(L_2)$. We observe that $C_K(L) = L$, since it is well known that the Fitting subgroup of a solvable group is self-centralizing and L is abelian. Then we have

$$L = C_K(L) = C_K(L_1 \oplus L_2) = C_K(L_1) \cap C_K(L_2) = C_K(L_i)$$

for $i = 1, 2$. So it follows that L_1 and L_2 are faithful and irreducible $\mathbb{F}[P]$-modules. Then, again since P is cyclic, P acts fixed-point free on L_1 and L_2 and therefore P acts fixed-point free on L. So what we have actually proved is that P acts fixed-point free on the section $L/\Phi(L)$. We can also demonstrate that L is $P\langle z \rangle$-indecomposable. Assume by contradiction that it is not true. Then there are $1 \neq L_1, L_2 \leq L$ such that L_1, L_2 are $P\langle z \rangle$-invariant (so $L_1, L_2 \trianglelefteq H$) and $L = L_1 \times L_2$. Then $L/\Phi(L) = L_1/\Phi(L_1) \times L_2/\Phi(L_2)$, contradicting the fact that $L/\Phi(L)$ is minimal normal in $H/\Phi(L)$ by Proposition 3.4. Therefore, L is $P\langle z \rangle$-indecomposable and $P\langle z \rangle$ acts coprimely on L. Then, by [5, Corollary 1], if $\exp(L) = q^n$, there exists a normal $P\langle z \rangle$-series

$$L = \Omega_n(L) \trianglerighteq \Omega_{n-1}(L) \trianglerighteq \cdots \trianglerighteq \Omega_0(L) = 1$$

in which every factor $\Omega_{n-i}(L)/\Omega_{n-i-1}(L)$ is $P\langle z \rangle$-isomorphic to $L/\Phi(L)$ for every $i = 1, \ldots, n-1$. Also, since L is a homocyclic q-group, it is known that $\Omega_n(L)/\Omega_{n-1}(L) = L/\Phi(L)$. We already know that P acts fixed-point free on this factor, so we conclude that the series is a normal P-series such that P acts fixed-point free on every section. Then it follows that P acts fixed-point free on L, that is, $K = L \rtimes P$ is a Frobenius group. □

Now we are finally able to prove the main theorem.

Theorem 3.8. *Let G be a finite solvable group, with $\mathbf{O}^{2'}(G) = G$, and suppose that G satisfies* **P**. *Let $N = \mathbf{O}_2(G)$ and $Q \in \mathrm{Syl}_2(G)$. Assume that G is not a 2-group, $N > 1$ and $|Q/N| = 2$. Then we have $G = N \rtimes H$, $H = K \rtimes \langle z \rangle$, with*

$\langle z\rangle \in \mathrm{Syl}_2(H)$ and $o(z) = 2$, and K is a cyclic p-group for some (odd) prime p. Moreover, H is a dihedral group. In particular, every element of K is real in H, inverted by z.

Proof. Since every hypothesis descends to quotients on $M \trianglelefteq G$, $M < N$, we may assume that N is minimal normal in G, so that it is an elementary abelian 2-group. Therefore, all its elements are involutions and real elements of G, and $[N, N] = 1$.

By Theorem 3.1, we know that there exists $H \leq G$ such that $G = N \rtimes H$ and H satisfies the Standard Hypotheses with respect to N. So $H = K \rtimes Q_0$, with $K > 1$ the normal 2-complement of H and $Q_0 \in \mathrm{Syl}_2(H)$. But $H \cong G/N$; therefore, $|Q_0| = 2$. So $H = K \rtimes \langle z\rangle$, with z involution. Furthermore, by Proposition 3.3, we have that H satisfies (H2).

Working by contradiction, assume that K is not a p-group. Then K is not nilpotent, since otherwise, as in Lemma 2.7, K would be a p-group. Let us consider K^∞ the residual nilpotent of K, which for a finite group is the last term of the lower central series and the smallest normal subgroup for which the quotient is nilpotent. We have K^∞ char K and so $K^\infty \trianglelefteq H$. Moreover, $K^\infty \neq 1$. Thus H/K^∞ has the normal 2-complement K/K^∞, which is nilpotent, and so K/K^∞ is a p-group by Lemma 2.7. Also, by Lemma 2.5, we have $[K/K^\infty, \langle z\rangle K^\infty/K^\infty] = K/K^\infty$. Then $K/K^\infty = [K/K^\infty, z]$, which is cyclic since H satisfies (H2). In particular, K/K^∞ is abelian; therefore, $K' \leq K^\infty$ and we conclude $K' = K^\infty$.

At this point, by the results in Theorem 2.4 (2), it is natural to split the proof into two parts: the case where $K/\mathbf{F}(H)$ is abelian, which will be part (a), and the case where $K/\mathbf{F}(H)$ is (strictly) metabelian, which will be part (b).

(a) Suppose that $K/\mathbf{F}(H)$ is abelian. Then, by Proposition 3.7, we get that H is 2-Frobenius with lower kernel a homocyclic abelian q-group of rank 2, upper complement of order 2 and lower complement a cyclic p-group, with $p \neq q$. Let L denote the lower kernel and let P be a Sylow p-subgroup of H. Note also that $L = K' = \mathbf{F}(K)$ and that we can assume that z acts on P, as in the proof of Proposition 3.7.

Therefore, we can conclude part (a). We recall $H \cong G/N$ and so $NL \trianglelefteq G$. We now prove that $[N, L] \trianglelefteq G$. Indeed, if $n \in N$, $l \in L$ and $g \in G$, then there are $n_1 \in N$ and $l_1 \in L$ for which $l^g = n_1 l_1$, since $N \trianglelefteq G$ and $NL \trianglelefteq G$. Then $[n, l]^g = [n^g, n_1 l_1] = [n^g, l_1] \in [N, L]$. Therefore, $[N, L] \trianglelefteq G$. Suppose by contradiction that $[N, L] = 1$. Then every element of N commutes with every element of L. Considering the action of z on $N - \{1\}$, we see that there is a fixed point $1 \neq x \in N$ with $x^z = x = x^{-1}$, since N is elementary abelian. That is, x is a real 2-element inverted by z. Since L contains a real non-trivial q-element inverted by z, we would get by Lemma 2.2 a real element of non-prime power order, contradicting **P**. So $1 \neq [N, L] \trianglelefteq N$ and the minimality of N means that

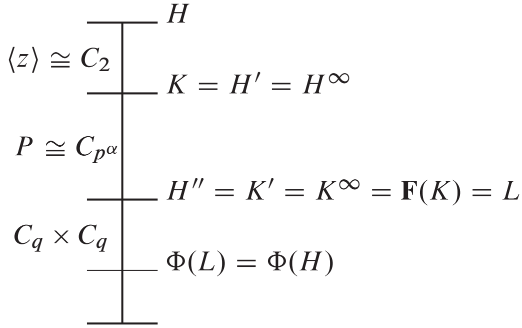

Figure 1. Structure of group H in part (a)

$[N, L] = N$. By the Fitting decomposition (see, for instance, [9, 8.4.2]), we have $N = [N, L] \times C_N(L)$, and thus $C_N(L) = 1$. So, applying [7, Theorem 15.16] to the $\mathbb{Z}_2[K]$-module N, we get that $C_N(P) > 1$. Also,

$$C_N(P)^z = C_{N^z}(P^z) = C_N(P)$$

and so $z \in N_G(C_N(P))$. Considering then the action of z on $C_N(P) - \{1\}$, we see that there exists a fixed point $1 \neq x \in C_N(P)$ with $x^z = x = x^{-1}$, i.e. x is real inverted by z and commutes with every element of P. But also every element of P is real inverted by z, and so, as usual, this contradicts **P**. Therefore, if $K/\mathbf{F}(H)$ is abelian, then K is a p-group.

(b) Let $K/\mathbf{F}(H)$ be metabelian. Obviously, we still have $\mathbf{F}(H) = \mathbf{F}(K)$, $\mathbf{F}(K)$ is an abelian q-group and $\mathbf{F}(K) \in \mathrm{Syl}_q(H)$ by Proposition 3.6. We write again $L = \mathbf{F}(K)$.

Assume by contradiction that $L \not\leq K'$. Then $q \mid |K : K'|$ and, by Theorem 3.5, L is cyclic. But L is abelian and, being the Fitting subgroup of a solvable group, L is self-centralizing. So $C_H(L) = L$ and therefore $H/L \lesssim \mathrm{Aut}(L) \cong \mathrm{Aut}(C_{q^a})$; thus H/L is abelian. Since $\mathbf{O}^{2'}(H/L) = H/L$, we have that H/L is a 2-group, that is, $H/L \cong \langle z\rangle$ and $L = K$. So K would be a q-group, contradicting the assumptions. Then $L \leq K'$. Since K/L is metabelian, we have that $K'/L = (K/L)'$ is abelian and so $K'' \leq L$. We note that we can assume that $K'/L \neq 1$; otherwise, we are in the case of part (a). Now we prove $K'' = L$. Suppose by contradiction that $K'' < L$. Then $L/K'' = \mathbf{F}(H/K'')$ by Proposition 3.6, since L/K'' is a normal Sylow q-subgroup of H/K'' and H/K'' satisfies (H2) and **P**. We then have, since K'/K'' is abelian, that $K'/K'' \leq C_{H/K''}(L/K'')$, contradicting the fact that the Fitting subgroup is self-centralizing and $L < K'$.

Now we want to verify that K'/L is a Sylow t-subgroup of H/L for some (odd) prime t dividing $|K|$. Let us consider H/L. It is easy to see that $H' = K$ and so

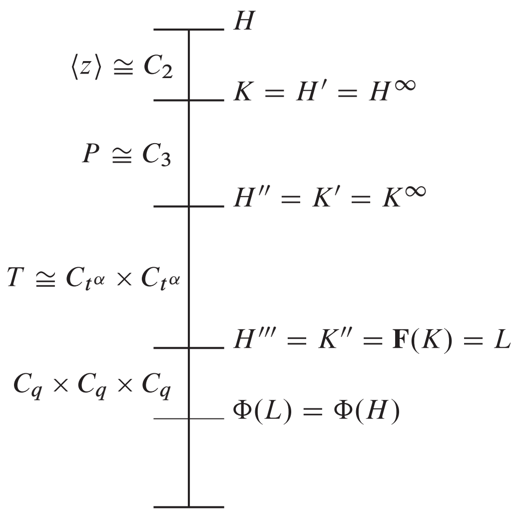

Figure 2. Structure of group H in part (b)

$K' = H''$, since H/H' is abelian and $\mathbf{O}^{2'}(H/H') = H/H'$, that is, $H/H' \cong \langle z \rangle$. Then

$$K'/L = (H/L)'' \text{ char } H/L.$$

Since K'/L is also abelian, then $K'/L \leq \mathbf{F}(H/L)$. But $\mathbf{F}(H/L)$ is a t-group by Proposition 3.6. So K'/L is a t-group and $t \neq q$, since $L < K'$ and $L \in \mathrm{Syl}_q(H)$, and $t \neq p$, since $K' = K^\infty$ is the residual nilpotent of K. In conclusion, we have $K'/L \trianglelefteq H/L$ and $K'/L \in \mathrm{Syl}_t(H/L)$. So, by Proposition 3.6, we must have $\mathbf{F}(H/L) = K'/L$.

We have that H/L satisfies the hypotheses of Proposition 3.7. So we get that H/L is 2-Frobenius with lower kernel a homocyclic abelian t-group of rank 2, upper complement of order 2 and lower complement a cyclic p-group, with $p \neq t$. Then, in particular, we have that K/L is a Frobenius group. Let P be a Sylow p-subgroup of H. We can assume that $z \in N_H(P)$ and so z acts fixed-point free on P, that is, z inverts every element of P. Also, let T be a Sylow t-subgroup of H such that $TP \leq H$, which exists since H has Hall $\{t, p\}$-subgroups.

Now we want to prove that $\mathbf{Z}(K') = 1$ so that $C_L(T) = 1$, as in the proof of Proposition 3.7. Let $\tilde{T}$ be a conjugate in H of T that contains a non-trivial real element inverted by z, which exists by [3, Corollary B]. Note that, obviously, $K' = L \rtimes \tilde{T}$. Working by contradiction, assume that $\mathbf{Z}(K') > 1$. The action of z on $\mathbf{Z}(K')$ is not trivial; otherwise, since $\mathbf{O}^{2'}(H) = H$, we would get $1 < \mathbf{Z}(K') \leq \mathbf{Z}(H)$, contradicting Theorem 3.5. So, by Lemma 2.1 (4), there is a real $1 \neq x = ly \in \mathbf{Z}(K')$, with $l \in L$, $y \in \tilde{T}$, inverted by z. If $l \neq 1$, then a suitable power of x is a non-trivial real q-element inverted by z that commutes with $\tilde{T}$, contradicting **P**. Then $l = 1$, $x \in \tilde{T}$ and x commutes with L, again contradicting **P**.

We can now prove that $|P| = 3$. Recall $TP \cong K/L$ is a Frobenius group, with kernel T and complement P. Consider the section $\overline{L} = L/\Phi(L)$. Since TP acts coprimely on $\overline{L}$, by the previous paragraph, we have $C_{\overline{L}}(T) = \overline{C_L(T)} = 1$ (see, for instance, [9, 8.2.2]). Also, $\overline{L}$ is a $\mathbb{Z}_q$-vector space. So $\overline{L}$ is a $\mathbb{Z}_q[TP]$-module with $C_{\overline{L}}(T) = 1$. Then, by [7, Theorem 15.16], we get that $|P|$ divides $\dim_{\mathbb{Z}_q}(\overline{L}) = \mathrm{rank}(L)$, which is at most 3 by Theorem 3.5. Therefore, we have $|P| = \mathrm{rank}(L) = 3$.

At this point, we are able to conclude part (b). By Theorem 2.4, $N = \mathbf{F}(G)$, as, by hypothesis, $N > 1$. Recall also we are assuming N to be elementary abelian. Therefore, we have $C_G(N) = N$ and so N is a faithful $G/N \cong H$-module. Let us consider the action of TP on N. We know that $|P| = 3$, P acts faithfully (actually fixed-point free) on the t-group T and TP acts faithfully on N. In particular, N is a faithful $\mathbb{Z}_2[TP]$-module. Then, by [1, 36.2], we have $C_N(P) > 1$. With the same argument as in the last paragraph of (a), we get a contradiction. Therefore, even if $K/\mathbf{F}(H)$ is metabelian, K is a p-group.

So, in any case, K is a $\langle z\rangle$-invariant p-section and then we have that $[K, z]$ is cyclic, since H satisfies (H2). By Lemma 2.5, $[K, z] = K$ and so K is cyclic. Then, by Lemma 2.6, we have $C_K(z) = 1$. Therefore, z inverts every element of K, proving that $H = K \rtimes \langle z\rangle$ is a dihedral group. □

Since we just did the hard work in Theorem 3.8, we can now prove Theorem A.

Proof of Theorem A. It is obvious that (3) implies (1).

Let us prove that (1) implies (2). Assume that every real element of G has prime power order, that is, G satisfies **P**. By Theorem 3.1, there exists $H \leq G$ with $G = N \rtimes H$. So $H \cong G/N$. Let $Q \in \mathrm{Syl}_2(H)$. Then, by Theorem 2.4, we have $H = K \rtimes Q$, where K is the normal 2-complement of H, and also, since $N = \mathbf{O}_2(G) > 1$, Q is cyclic. Let z be its unique involution.

Suppose $|Q| > 2$. Then, still by Theorem 2.4, we have that K is cyclic. Therefore, since also $C_K(z) = C_K(Q)$, by Lemmas 2.7 and 2.6, K is a p-group and $C_K(z) = 1$, so that every element of K is real inverted by z. Moreover, $H = K \rtimes Q$ is a Frobenius group. Indeed, if $1 \neq q \in Q$ were such that $C_K(q) > 1$, then, since $z \in \langle q\rangle$, we would have $C_K(z) > 1$, which is not true.

If $|Q| = 2$, then by Theorem 3.8, we have that K is a cyclic p-group and H is a dihedral group. In particular, every element of K is real inverted by z.

In any case, we note that G is a $\{2, p\}$-group and $H = K \rtimes Q$ is a Frobenius group.

Now we verify that even $N \rtimes K$ is a Frobenius group. Working by contradiction, assume that there exists $1 \neq k \in K$ with $C_N(k) > 1$. We see that z acts on $C_N(k)$, since $C_N(k)^z = C_{N^z}(k^z) = C_N(k^{-1}) = C_N(k)$. Then, considering the action of z on $C_N(k) - \{1\}$, we see that there is a fixed point, that is, an element $1 \neq x \in C_N(k)$ with $x^z = x$. If we take a suitable power of x, then we have an involution $y \in C_N(k)$ with $y^z = y = y^{-1}$. Therefore, by Lemma 2.2, ky is a real element of G inverted by z with non-prime power order, contradicting **P**. So $G = NKQ$ is a 2-Frobenius group.

Finally, let us prove that (2) implies (3). Let $x \in G$ be an involution. Since K acts fixed-point free on N and Q acts fixed-point free on K, we have that $C_G(x)$ is a 2-group. So G is a CIT-group (see [12] for the definition and more). Since G is a $\{2, p\}$-group and a CIT-group, we have that every element of G has prime power order. □

Let $\pi_{\mathbb{R}}(G)$ denote the set of primes occurring as the order of real elements of G.

Corollary 3.9. *Let G be a finite solvable group in which every real element has prime power order. Suppose also that $\mathbf{O}_2(G) > 1$. Then either $\pi_{\mathbb{R}}(G) = \{2\}$ or $\pi_{\mathbb{R}}(G) = \{2, p\}$ for some odd prime p.*

Proof. If G is a 2-group, then $\pi_{\mathbb{R}}(G) = \{2\}$. Assume that G is not a 2-group and consider $H = \mathbf{O}^{2'}(G)$. We have that H is a solvable group in which every real element has prime power order and $\mathbf{O}^{2'}(H) = H$. Also, recall that $\mathbf{O}_2(G) \leq \mathbf{O}_2(H)$, and so we have $\mathbf{O}_2(H) > 1$. Moreover, the real elements of G are the real elements of H and so we have $\pi_{\mathbb{R}}(G) = \pi_{\mathbb{R}}(H)$. If H is a 2-group, then it is a Sylow 2-subgroup of G. In this case, $\pi_{\mathbb{R}}(G) = \{2\}$. Lastly, suppose that H is not a 2-group. Then H satisfies the hypotheses of Theorem A and so H is a $\{2, p\}$-group for some odd prime p. Then, in this case, $\pi_{\mathbb{R}}(G) = \{2, p\}$. □

So, given a $\{2, p\}$-group G as in Theorem A, we are able to say a lot about the structure of G/N. But, in general, there is not much we can say about the structure of N. While, for a fixed p, we know by [6] that there is an upper bound for $\mathrm{dl}(N)$, the derived length of N, depending only on p, we can show that, as p varies, there are groups with $\mathrm{dl}(N)$ arbitrarily large.

Example 3.10. This example is based on a construction of I. M. Isaacs contained in [8]. Although our results are very similar to those in [8], since our working hypotheses are different, where necessary, we will give explicit proofs.

Let $k = 2^a$, with $a \geq 1$ positive integer and let $\mathbb{F} = \mathrm{GF}(2^k)$. Consider then $\mathcal{G} = \mathrm{Gal}(\mathbb{F}|\mathbb{F}_2)$, which is cyclic of order k, generated by σ, the Frobenius automorphism. Thus we can define $\mathbb{F}\{X\}$, the "twisted polynomial ring" in the indeterminate X, that is, the ring of "polynomials" $\alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$ for which

$X\alpha = \alpha^\sigma X$ for every $\alpha \in \mathbb{F}$. It is known that this does define a ring. We note that X^k is central in $\mathbb{F}\{X\}$. Then we consider the quotient $R = \mathbb{F}\{X\}/(X^k)$ and we write x to denote the image of X in R under the natural homomorphism. So every element of R is of the form $\alpha_0 + \alpha_1 x + \cdots + \alpha_{k-1}x^{k-1}$ and then $|R| = (2^k)^k$. Also, $x^k = 0$ and $x\alpha = \alpha^\sigma x$ for every $\alpha \in \mathbb{F}$. Moreover, we have that $xR = Rx$ is a nilpotent ideal and $R/xR \cong \mathbb{F}$. Therefore, $xR = J(R)$, the Jacobson radical of R, that we denote as J. We have $J^i = x^i R = Rx^i$ and so $J^{k-1} \neq 0$ e $J^k = 0$. Let $S = 1 + J = \{1 + \alpha_1 x + \cdots + \alpha_{k-1}x^{k-1} \mid \alpha_i \in \mathbb{F}\}$, where 1 is the identity element of R. It is a known fact in ring theory that S is a subgroup of the group of units of R; in this case, it is a 2-group. For $u \geq 1$ integer, we write $S_u = 1 + J^u$. Then $S_u \leq S$ and $S = S_1 > S_2 > \cdots > S_{k-1} > S_k = 1$. Every element $s \in S_u$ is uniquely of the form $s = 1 + \alpha x^u + y$, with $y \in J^{u+1}$ and $\alpha \in \mathbb{F}$. We can then define $\psi_u \colon S_u \to \mathbb{F}$ with $\psi_u(s) = \alpha$. It is easy to prove that ψ_u is a homomorphism from S_u to the additive group of $\mathbb{F}$ and that $\ker(\psi_u) = S_{u+1}$, so $S_{u+1} \trianglelefteq S_u$. By [8, Corollary 4.2], we have $[S_u, S_v] \leq S_{u+v}$ if $u, v \geq 1$. Furthermore, if $u + v \leq k - 1$, $s \in S_u$, $t \in S_v$ and $\psi_u(s) = \alpha$ and $\psi_v(t) = \beta$, then $\psi_{u+v}([s,t]) = \alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v}$.

We now have to study the map $\langle \cdot, \cdot \rangle \colon \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ given by

$$\langle \alpha, \beta \rangle = \alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v},$$

in the case u odd. Let us consider $\mathbb{F}$ as a vector space over $\mathbb{F}_2$. Note that $\langle \cdot, \cdot \rangle$ is $\mathbb{F}_2$-bilinear.

We firstly prove that if u is odd and $u + v \leq k - 1$, then, for $0 \neq \alpha \in \mathbb{F}$, $\langle \alpha, \mathbb{F} \rangle$ contains a hyperplane of $\mathbb{F}$. Since $\langle \alpha, \cdot \rangle$ is $\mathbb{F}_2$-linear, it is enough to prove that its kernel is of dimension at most 1. So let $\langle \alpha, \beta \rangle = 0 = \langle \alpha, \gamma \rangle$, with $\beta \neq 0$. We then have

$$\alpha\beta^{\sigma^u} - \beta\alpha^{\sigma^v} = 0 = \alpha\gamma^{\sigma^u} - \gamma\alpha^{\sigma^v},$$

which implies that if $\gamma \neq 0$, then

$$\beta^{-1}\beta^{\sigma^u} = \alpha^{-1}\alpha^{\sigma^v} = \gamma^{-1}\gamma^{\sigma^u},$$

so $\gamma\beta^{-1} = (\gamma\beta^{-1})^{\sigma^u}$. Since u is odd, we have $\langle \sigma^u \rangle = \langle \sigma \rangle$ and hence $\gamma\beta^{-1} \in \mathbb{F}_2$.

Now we prove, still under the assumption that $u + v \leq k - 1$, that there exist $0 \neq \alpha, \beta \in \mathbb{F}$ for which $\langle \alpha, \mathbb{F} \rangle \neq \langle \beta, \mathbb{F} \rangle$ (even if u is not odd). To do so, we will use the trace of the Galois extension $\mathbb{F}|\mathbb{F}_2$, that is,

$$T \colon \mathbb{F} \to \mathbb{F}_2 \quad \text{with } T(\alpha) = \sum_{i=0}^{k-1} \sigma^i(\alpha).$$

Recall that T is invariant with respect to $\mathcal{G} = \mathrm{Gal}(\mathbb{F}|\mathbb{F}_2)$. Then, if $\alpha = 1$, we have

$$T(\langle 1, \gamma \rangle) = T(\gamma^{\sigma^u} - \gamma) = T(\gamma^{\sigma^u}) - T(\gamma) = T(\gamma) - T(\gamma) = 0.$$

Therefore, it suffices to find $\beta, \gamma \in \mathbb{F}$ with $T(\langle \beta, \gamma \rangle) \neq 0$. We have

$$T(\langle \beta, \gamma \rangle) = T(\beta \gamma^{\sigma^u}) - T(\gamma \beta^{\sigma^v}) = T(\beta^{\sigma^v} \gamma^{\sigma^{u+v}}) - T(\gamma \beta^{\sigma^v})$$
$$= T(\beta^{\sigma^v} (\gamma^{\sigma^{u+v}} - \gamma)).$$

As $u + v \leq k - 1$, we have $k \nmid u + v$, so we can choose γ with $\gamma^{\sigma^{u+v}} - \gamma \neq 0$. Moreover, simply because σ^v is an automorphism of $\mathbb{F}$, we can choose $0 \neq \beta$ so that $\beta^{\sigma^v}(\gamma^{\sigma^{u+v}} - \gamma)$ is an arbitrary element of $\mathbb{F}$ and, in particular, one with non-zero trace. Thus $\langle 1, \mathbb{F} \rangle \neq \langle \beta, \mathbb{F} \rangle$ if β is as stated.

To estimate the derived length of S, it is enough to verify that $[S_u, S_u] = S_{2u}$ when u is odd. Indeed, assuming this is true, and denoting by $S^{(n)}$ the $n + 1$-th term of the derived series, by induction over n, we prove that $S^{(n)} \geq S_{t_n}$, where $\{t_n\}_{n=1}^{\infty}$ is the succession defined by $t_1 = 2$ and $t_{n+1} = 2t_n + 2 = 2(t_n + 1)$ (note that every term of t_n is even and so $t_n + 1$ is odd).

If $n = 1$, we have $S^{(1)} = [S, S] = [S_1, S_1] = S_2$. If $n > 1$, then

$$S^{(n+1)} = [S^{(n)}, S^{(n)}] \geq [S_{t_n}, S_{t_n}] \geq [S_{t_n+1}, S_{t_n+1}] = S_{2t_n+2} = S_{t_{n+1}}.$$

Therefore, if we take k with $k - 1 \geq t_n$, then $S^{(n)} \geq S_{t_n} > 1$ and so $\mathrm{dl}(S) > n$.

Let us prove that $[S_u, S_u] = S_{2u}$ when u is odd. Actually, we prove a stronger condition: if u and v are positive integers with u odd, then $[S_u, S_v] = S_{u+v}$. For that, we fix u odd. We know that $[S_u, S_v] \leq S_{u+v}$ if u, v are positive integers. If $u + v > k - 1$, we have $S_{u+v} = 1$ and we are done. Assume then that $u + v \leq k - 1$. We work by induction over $(k - 1 - u) - v$. We know that $\psi_{u+v}([S_u, S_v])$ is a $\mathbb{F}_2$-subspace of $\mathbb{F}$ which contains all the elements of the form $\langle \alpha, \beta \rangle$, with $\alpha, \beta \in \mathbb{F}$. Since $u + v \leq k - 1$, we have also seen that $\psi_{u+v}([S_u, S_v])$ contains two different hyperplanes of $\mathbb{F}$ and so it has to be all of $\mathbb{F}$. Then

$$\psi_{u+v}([S_u, S_v]) = \psi_{u+v}(S_{u+v}).$$

If $(k - 1 - u) - v = 0$, that is, $u + v = k - 1$, then $\ker(\psi_{u+v}) = S_k = 1$. So ψ_{u+v} is injective and then, since $\psi_{u+v}([S_u, S_v]) = \psi_{u+v}(S_{u+v})$, we deduce that $[S_u, S_v] = S_{u+v}$, as desired.

If $(k - 1 - u) - v > 0$, we have, by inductive hypothesis, that

$$\ker(\psi_{u+v}) = S_{u+v+1} = S_{u+(v+1)} = [S_u, S_{v+1}] \leq [S_u, S_v].$$

Therefore, since

$$\ker(\psi_{u+v}) = S_{u+v+1} \leq [S_u, S_v] \quad \text{and} \quad \psi_{u+v}([S_u, S_v]) = \psi_{u+v}(S_{u+v}),$$

we conclude that $[S_u, S_v] = S_{u+v}$.

In conclusion, we have proved that, for a fixed positive integer n, if we take k sufficiently large, we have $\mathrm{dl}(S) > n$.

Consider now the semidirect product $\mathbb{F}^\times \rtimes \mathscr{G}$. We have $|\mathbb{F}^\times| = 2^k - 1$. Recall that $k = 2^a$, with $a \geq 1$ a positive integer. Then we take a primitive divisor p of $2^k - 1$, that is, $p \mid 2^k - 1$ and $p \nmid 2^i - 1$ for every positive $i < k$, which exists by Zsigmondy's theorem [11, Theorem 6.2]. Since $p \nmid 2^{k/2} - 1$, it follows that $p \mid 2^{k/2} + 1$. Let P be a Sylow p-subgroup of $\mathbb{F}^\times$. Then we have $P \leq [\mathbb{F}^\times, z]$, where z is the unique involution of $\mathscr{G}$, since $\mathbb{F}^\times = [\mathbb{F}^\times, z] \times C_{\mathbb{F}^\times}(z)$ by the coprime action (see, for instance, [9, 8.4.2]) and $|C_{\mathbb{F}^\times}(z)| = 2^{k/2} - 1$ by Galois theory, and so $\mathscr{G}$ acts fixed-point free on P. Moreover, P is the unique Sylow p-subgroup of $\mathbb{F}^\times \rtimes \mathscr{G}$ and so $P \trianglelefteq (\mathbb{F}^\times \rtimes \mathscr{G})$. We identify P with the subgroup $1 \cdot P$ of the unit group $R^\times$ of R.

Now we prove that the action of P on S is fixed-point free. Let $s \in S$, $\gamma \in P$ and assume that $s \neq 1$. So $s \in S_u$ for some positive integer $u \leq k - 1$, and we write $s = 1 + \alpha x^u + y$, with $0 \neq \alpha \in \mathbb{F}$ and $y \in J^{u+1}$. We have

$$\gamma^{-1} s \gamma = 1 + \alpha \gamma^{-1} x^u \gamma + \gamma^{-1} y \gamma = 1 + \alpha \gamma^{-1} \gamma^{\sigma^u} x^u + \gamma^{-1} y \gamma.$$

It follows that the action of $\gamma \in P$ on $s \in S$ consists in multiplying the u-th coefficient of s by $\gamma^{-1}\gamma^{\sigma^u}$ for $u = 1, \ldots, k-1$. Recall that σ is the Frobenius automorphism of the field $\mathbb{F}$, which is of characteristic 2; thus $\sigma(\alpha) = \alpha^2$ for every $\alpha \in \mathbb{F}$, and so $\gamma^{-1}\gamma^{\sigma^u} = \gamma^{2^u - 1}$. If $1 \neq s$ were fixed by $1 \neq \gamma \in P$, there would be some integer u, $1 \leq u \leq k-1$, such that the u-th coefficient of s would be non-zero and that would imply $\gamma^{2^u - 1} = 1$, so that $p \mid 2^u - 1$, contradicting the choice of p.

So we have proved that SP is a Frobenius group with Frobenius kernel S and complement P. Moreover, the automorphism σ of $\mathbb{F}$ can be extended to an automorphism of the ring R by setting $x^\sigma = x$. We note that such an extension, which we still denote by σ, fixes S setwise and so $\mathscr{G} = \langle \sigma \rangle$ acts on S. Then we have the group $G = S \rtimes (P \rtimes \mathscr{G})$, that is, a $\{2, p\}$-group and a 2-Frobenius group. It easily follows then that every element of G has prime power order. It is also not difficult to verify that $S = \mathbf{O}_2(G)$ and $\mathbf{O}^{2'}(G) = G$.

In conclusion, we have built a family of groups as in Theorem A, parameterized by $k = 2^a$, such that, denoting $N = S = \mathbf{O}_2(G)$, if $k - 1 \geq t_n$, we have $\mathrm{dl}(N) > n$. So, as k increases, we get $\mathrm{dl}(N)$ arbitrarily large.

4 Case $\mathbf{O}_2(G) = 1$ and consequences on $\Gamma_{\mathbb{R}}(G)$

Let us now consider a non-trivial finite solvable group G, with $\mathbf{O}^{2'}(G) = G$ and $\mathbf{O}_2(G) = 1$. Suppose that G satisfies **P**. Let $Q \in \mathrm{Syl}_2(G)$. By Theorem 2.4 (1), we have that Q is cyclic or generalized quaternion, G has a normal 2-complement K and also $C_K(Q) = C_K(z)$, where z is the unique involution of Q.

Regarding the structure of $\mathbf{F}(G)$, we can easily deduce the following result.

Lemma 4.1. *Let G be a non-trivial finite solvable group, with $\mathbf{O}^{2'}(G) = G$ and $\mathbf{O}_2(G) = 1$. Suppose that G satisfies $\mathbf{P}$. Then there is one and only one (odd) prime p for which $\mathbf{O}_p(G) \nleq \mathbf{Z}(G)$.*

Proof. Let us first prove that there exists at least one prime p with $\mathbf{O}_p(G) \nleq \mathbf{Z}(G)$. Working by contradiction, assume this is not true. Then we have $\mathbf{F}(G) \leq \mathbf{Z}(G)$ and so $C_G(\mathbf{F}(G)) = G$. Since G is solvable, $\mathbf{F}(G)$ is self-centralizing and so we must have $\mathbf{F}(G) = G$, which implies that G is nilpotent. Since $\mathbf{O}^{2'}(G) = G$, we have that G is a 2-group, contradicting our assumptions.

Assume now by contradiction that there are two different (odd) primes p, q with $\mathbf{O}_p(G) \nleq \mathbf{Z}(G)$ and $\mathbf{O}_q(G) \nleq \mathbf{Z}(G)$. Recall that $Q \in \mathrm{Syl}_2(G)$ and z is its unique involution. We have that z does not centralize either $\mathbf{O}_p(G)$ or $\mathbf{O}_q(G)$; otherwise, as already seen many times, we would get $\mathbf{O}_p(G) \leq \mathbf{Z}(G)$ and $\mathbf{O}_q(G) \leq \mathbf{Z}(G)$. Therefore, there exist, by Lemma 2.1 (4), a non-trivial real element $x \in \mathbf{O}_p(G)$ and a non-trivial real element $y \in \mathbf{O}_q(G)$, which are both inverted by z. Since they commute, xy is a non-trivial real element of non-prime power order, contradicting property $\mathbf{P}$. □

It is not difficult to see that $\mathbf{Z}(G) \leq K$. Also, since $\mathbf{O}^{2'}(G/G') = G/G'$ and G/G' is abelian, we have that G' has 2-power index, that is, $K \leq G'$; actually,

$$G' = (K \rtimes Q)' = K'[K, Q]Q' = KQ',$$

since $[K, Q] = K$ by Lemma 2.5. So $\mathbf{Z}(G) \leq G'$ and therefore $\mathbf{Z}(G) \leq \Phi(G)$, but this by itself obviously does not force $\mathbf{Z}(G) = 1$. If $\mathbf{Z}(G) = 1$ were true, then we could infer that $\mathbf{F}(G)$ is a p-group.

As already announced in the introduction, in this paper we were not able to precisely describe the structure of these groups, but we concentrated our efforts on finding the following examples, that prove that, in this case, G is not necessarily a $\{2, p\}$-group.

Example 4.2. Consider S_3 and its unique, up to isomorphism, irreducible $\mathbb{Z}_5[S_3]$-module V of dimension 2. We can consider the semidirect product $G = V \rtimes S_3$. In [13], G is `SmallGroup(150,5)`. Obviously, G is solvable and its structure is $(C_5 \times C_5) \rtimes S_3$. We can verify that

- the normal subgroups of G are 1,

$$G'' = \mathbf{F}(G) \cong (C_5 \times C_5), \quad G' \cong (C_5 \times C_5) \rtimes C_3,$$

  and G, so we have $\mathbf{O}_2(G) = 1$ and $\mathbf{O}^{2'}(G) = G$;
- the orders of the real elements of G are $\{1, 2, 3, 5\}$, that is, $|\pi_{\mathbb{R}}(G)| = 3$ and every real element has prime (power) order;
- $\mathbf{Z}(G) = 1$ (consistent with the fact that $\mathbf{F}(G)$ is a 5-group).

Note that the structure of G resembles that in Figure 1.

We can also extend G by considering the semidirect product with a suitable irreducible $\mathbb{Z}_{11}[G]$-module W of dimension 3. Unfortunately, since the resulting group $H = W \rtimes G$ has order 199650, it is not listed in GAP libraries. So we will identify W, and so also H, by saying that G acts on W as a group of matrices, with generators

$$\begin{bmatrix} \bar{0} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \\ \bar{1} & \bar{0} & \bar{0} \end{bmatrix} \begin{bmatrix} \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{0} \end{bmatrix} \begin{bmatrix} \bar{9} & \bar{0} & \bar{0} \\ \bar{0} & \bar{3} & \bar{0} \\ \bar{0} & \bar{0} & \bar{9} \end{bmatrix} \begin{bmatrix} \bar{5} & \bar{0} & \bar{0} \\ \bar{0} & \bar{9} & \bar{0} \\ \bar{0} & \bar{0} & \bar{1} \end{bmatrix},$$

respectively of order $2, 3, 5, 5$. Obviously, H is solvable and its structure is

$$(C_{11} \times C_{11} \times C_{11}) \rtimes ((C_5 \times C_5) \rtimes S_3).$$

We can verify that

- the normal subgroups of H are 1,

$$\begin{aligned} H''' &= \mathbf{F}(H) \cong C_{11} \times C_{11} \times C_{11}, \\ H'' &= (C_{11} \times C_{11} \times C_{11}) \rtimes (C_5 \times C_5), \\ H' &= (C_{11} \times C_{11} \times C_{11}) \rtimes ((C_5 \times C_5) \rtimes C_3) \end{aligned}$$

  and H, so we have $\mathbf{O}_2(H) = 1$ and $\mathbf{O}^{2'}(H) = H$;
- the orders of the real elements of H are $\{1, 2, 3, 5, 11\}$, that is, $|\pi_{\mathbb{R}}(H)| = 4$ and every real element has prime (power) order;
- $\mathbf{Z}(H) = 1$ (consistent with the fact that $\mathbf{F}(G)$ is an 11-group).

Note that the structure of H resembles that in Figure 2.

It could be an interesting topic for future research to see if there are further extensions and how much it is possible to increase $|\pi_{\mathbb{R}}(G)|$, preserving the hypothesis that every real element has prime power order.

We will now, for our final considerations, switch to the framework of the real prime graph $\Gamma_{\mathbb{R}}(G)$. Let us also consider other known graphs associated to G and then compare their properties with the ones of $\Gamma_{\mathbb{R}}(G)$.

Regarding the Gruenberg–Kegel graph $\Gamma(G)$, we have to recall the following simple, but still extremely important, result by M. S. Lucido, also known as Lucido's Lemma (see [10, Proposition 1]).

Lemma 4.3. *Let G be a finite solvable group. If p, q, r are three distinct primes that divide $|G|$, then G contains an element whose order is the product of two of these primes.*

It is immediate that Lemma 4.3 is equivalent to the fact that $\Gamma(G)$ does not contain a set of three pairwise non-adjacent vertices, so, in particular, $n(\Gamma(G)) \leq 2$. Since the group H (also G) from Example 4.2 is such that $\Gamma_{\mathbb{R}}(H)$ contains sets of three pairwise non-adjacent vertices, we deduce that an analogous version of Lemma 4.3 for real elements does not hold.

Beyond the comparison with $\Gamma(G)$ already mentioned, we can compare this feature of $\Gamma_{\mathbb{R}}(G)$ with two other notorious graphs associated to G, that historically have maintained certain similarities with respect to $\Gamma_{\mathbb{R}}(G)$. These are $\Gamma_{\text{cd},\mathbb{R}}(G)$, the prime graph on real character degrees, and $\Gamma_{\text{cs},\mathbb{R}}(G)$, the prime graph on real class sizes.

Regarding the least upper bound for the number of connected components of these graphs, we have the following results, respectively [4, Theorem 5.1 (ii)] and [4, Theorem 6.2].

Theorem 4.4. *Let G be a finite solvable group. Then $n(\Gamma_{\text{cd},\mathbb{R}}(G)) \leq 2$.*

Theorem 4.5. *Let G be a finite group. Then $n(\Gamma_{\text{cs},\mathbb{R}}(G)) \leq 2$.*

So we deduce that, at least in this case, there is a breaking of the symmetry between $\Gamma_{\text{cs},\mathbb{R}}(G)$, $\Gamma_{\text{cd},\mathbb{R}}(G)$ and $\Gamma_{\mathbb{R}}(G)$. Furthermore, we note that the least upper bound for $n(\Gamma_{\mathbb{R}}(G))$, if it exists, has to be at least 4. So determining such a bound, even though there is now a little more information about it, remains an open question of interest.

Acknowledgments. The author would like to thank Professor S. Dolfi for bringing this problem to his attention and for the invaluable advice received while working under his supervision on this research. The author would also like to thank the referee for their careful reading of the manuscript and for the insightful suggestions and constructive comments that significantly improved the clarity and presentation of the paper. The author is also grateful to the editor for helpful remarks and suggestions.

Bibliography

[1] M. Aschbacher, *Finite Group Theory*, 2nd ed., Cambridge Stud. Adv. Math. 10, Cambridge University, Cambridge, 2000.

[2] S. Dolfi, D. Gluck and G. Navarro, On the orders of real elements of solvable groups, *Israel J. Math.* **210** (2015), no. 1, 1–21.

[3] S. Dolfi, G. Malle and G. Navarro, The finite groups with no real p-elements, *Israel J. Math.* **192** (2012), no. 2, 831–840.

[4] S. Dolfi, G. Navarro and P. H. Tiep, Primes dividing the degrees of the real characters, *Math. Z.* **259** (2008), no. 4, 755–774.

[5] M. E. Harris, On p'-automorphisms of abelian p-groups, *Rocky Mountain J. Math.* **7** (1977), no. 4, 751–752.

[6] G. Higman, Finite groups in which every element has prime power order, *J. Lond. Math. Soc.* **32** (1957), 335–342.

[7] I. M. Isaacs, *Character Theory of Finite Groups*, Pure Appl. Math. 69, Academic Press, New York, 1976.

[8] I. M. Isaacs, Coprime group actions fixing all nonlinear irreducible characters, *Canad. J. Math.* **41** (1989), no. 1, 68–82.

[9] H. Kurzweil and B. Stellmacher, *The Theory of Finite Groups*, Universitext, Springer, New York, 2004.

[10] M. S. Lucido, The diameter of the prime graph of a finite group, *J. Group Theory* **2** (1999), no. 2, 157–172.

[11] O. Manz and T. R. Wolf, *Representations of Solvable Groups*, London Math. Soc. Lecture Note Ser. 185, Cambridge University, Cambridge, 1993.

[12] M. Suzuki, Finite groups with nilpotent centralizers, *Trans. Amer. Math. Soc.* **99** (1961), 425–470.

[13] Groups, algorithms, and programming, Version 4.12.1, The GAP Group, 2022, https://www.gap-system.org/.

Received March 25, 2025; revised October 27, 2025

Author information

Alessandro Giorgi, Dipartimento di Matematica e Informatica “Ulisse Dini”,
Università degli Studi di Firenze, Firenze, Italy.
E-mail: alessandro.giorgi@unifi.it