GLOBAL OORT GROUPS

TED CHINBURG, ROBERT GURALNICK, AND DAVID HARBATER

ABSTRACT. We study the Oort groups for a prime p, i.e. finite groups G such that every G-Galois branched cover of smooth curves over an algebraically closed field of characteristic p lifts to a G-cover of curves in characteristic 0. We prove that all Oort groups lie in a particular class of finite groups that we characterize, with equality of classes under a conjecture about local liftings. We prove this equality unconditionally if the order of G is not divisible by $2p^2$. We also treat the local lifting problem and relate it to the global problem.

1. INTRODUCTION

This paper, which is a sequel to [8] and [9], concerns the question of when covers of curves in characteristic $p > 0$ lift to covers in characteristic zero. We begin with a G-Galois finite branched cover $X \to Y$ of smooth projective curves over an algebraically closed field k of characteristic p. By a *lifting* we mean a G-Galois branched cover $\mathcal{X} \to \mathcal{Y}$ of normal projective curves over a complete discrete valuation ring R such that the following is true. The fraction field of R has characteristic zero, the residue field of R is isomorphic to k, and the closed fiber of $\mathcal{X} \to \mathcal{Y}$ is G-isomorphic to the given cover $X \to Y$. Lifting a G-Galois cover $X \to Y$ is equivalent to lifting the action of G on X to an action of G on $\mathcal{X}$.

In [16], Grothendieck showed that all tamely ramified covers lift, and in particular a cover lifts if the Galois group has order prime to p. Later, in [21, Sect. I.7], F. Oort posed the following conjecture:

Conjecture 1.1. *(Oort Conjecture) Every cyclic Galois cover of k-curves lifts to characteristic zero.*

Motivated by this conjecture, in [8] we defined a finite group G to be a (global) *Oort group* for k if every G-Galois cover of smooth projective k-curves lifts to characteristic zero. We asked which finite groups are Oort groups. Recently, Conjecture 1.1 was proven by the combined work of Obus and Wewers [20] and Pop [24], so we now know that every cyclic group is an Oort group. A brief history is as follows: In [22] and later in [15], it was shown that a cyclic group G is an Oort group provided that its order is exactly divisible by p, respectively by p^2. More recently, in [20], it was shown that a cyclic group G is an Oort group provided that its order is divisible at most by p^3, or more generally if its higher ramification groups satisfy a certain condition. Finally, by deforming a general cover to one in the special case treated in [20], the full conjecture was proven in [24].

While the above conjecture considered only cyclic groups, some results have been obtained about more general groups. Apart from Grothendieck's result on prime-to-p groups being Oort groups, it is known that the dihedral group D_{2p} of order $2p$ is an Oort group for algebraically closed fields of characteristic p (see [23] for $p = 2$, [5] for p odd), and A_4 is an Oort group for algebraically closed fields of characteristic 2 (see [5] and [19]). Note that these groups are cyclic-by-p, i.e. they are extensions of a cyclic group of order prime to p by a normal Sylow p-subgroup. The significance of understanding Oort groups of this form is that a group G is an Oort group if and only if each cyclic-by-p subgroup of G is an Oort group [8, Corollary 2.8].

In [8, Corollary 3.4, Theorem 4.5], we proved that if a cyclic-by-p group G is an Oort group for an algebraically closed field of characteristic p, then G is either a cyclic group C_m of order m, a dihedral group D_{2p^n} for some n, or A_4 if $p = 2$. We also conjectured the converse in [8]:

Conjecture 1.2. *(Strong Oort Conjecture) If k is an algebraically closed field of characteristic p, then a cyclic-by-p group G is an Oort group for k if and only if G is of the form C_m, D_{2p^n}, or A_4 (the last case only if $p = 2$).*

This conjecture would imply that for a given prime p, all the algebraically closed fields of characteristic p have the same set of Oort groups. In fact, it is even expected that an assertion of this sort would hold for non-algebraically closed fields with enough roots of unity. Some partial results in this direction have been obtained by Astrand [3].

Motivated by the above conjecture, we define a group G to be an O-*group* for the prime p if every cyclic-by-p subgroup of G is of the form C_m, D_{2p^n}, or A_4 (if $p = 2$, in this last case). By [8, Corollaries 3.5 and 4.6], every Oort group for an algebraically closed field k of characteristic p is an O-group for p.

In this paper we consider the converse to this last assertion, i.e. whether every O-group is an Oort group. We show that this implication would follow from Conjecture 1.2, and that it holds unconditionally for groups whose orders are not divisible by $2p^2$ (see Theorem 2.2 and Corollary 2.3). We also give a classification of O-groups, in Theorems 2.4, 2.6, and 2.7, using finite

group theory, including the classification theorem of finite simple groups. If Conjecture 1.2 is later proven to hold in general, this would fully classify Oort groups for k and show that the set of Oort groups depends only on p (as has been conjectured). Unconditionally, our classification of O-groups restricts the set of finite groups that can be Oort groups in characteristic p.

We also consider the companion notation of "local Oort groups", i.e. groups for which every local cover lifts. More precisely, G is a *local Oort group* for k if every connected normal G-Galois branched cover of $\mathrm{Spec}(k[[t]])$ lifts to such a cover of $\mathrm{Spec}(R[[t]])$, for some complete discrete valuation ring R whose fraction field has characteristic zero and whose residue field is k. Since Galois groups over $k((t))$ are all cyclic-by-p, so are all local Oort groups for k. In [8, Theorem 2.4], it was shown that G is a global Oort group for k if and only if every cyclic-by-p subgroup of G is a local Oort group for k; and every cyclic-by-p Oort group for k is a local Oort group for k [8, Corollary 2.6]. In Theorem 2.1 of the present paper we prove the converse of this last assertion; thus local Oort groups are the same as cyclic-by-p global Oort groups. Hence local Oort groups are preserved under taking subquotients; the corresponding property of *global* Oort groups was shown in [8, Corollary 2.7]. In this way, Conjecture 1.2 can be regarded as a conjecture about local liftings.

The paper is organized as follows. In Section 2, we state the main results about O-groups, global Oort groups, and local Oort groups. The proof of the classification of O-groups in odd characteristic p is given in Section 3, and the proof in characteristic 2 is given in Section 4. We remark that the proof for odd p requires the classification of finite simple groups. The proof for $p = 2$ requires only an older result about the classification of finite simple groups with a dihedral Sylow 2-subgroup and the Feit-Thompson theorem.

We thank the referees for their helpful comments.

Notation and Terminology

In this paper, k is an algebraically closed field of characteristic $p \neq 0$. *Curves* over k are smooth, connected projective k-schemes of dimension one. For a discrete valuation ring R, an *R-curve* is a separated flat projective R-scheme whose fibers are curves. A *G-Galois cover* is a finite generically separable morphism of connected normal schemes $X \to Y$ together with a faithful action of G on X such that $Y = X/G$.

Given a group G with subgroups N, H, we write $G = NH$ if H normalizes N and G is the set of products nh with $n \in N$ and $h \in H$. This is a semi-direct product if and only if $N \cap H = 1$. We write C_m for the cyclic group of order m, and D_{2n} for the dihedral group of order $2n$.

We have from [2] some basic notions and results about finite groups. See also [13, 2.5] as a general reference about automorphism groups of simple groups, e.g. in connection with Theorem 3.8.

We write $H \leq G$ to indicate that H is a subgroup of G, and write $H < G$ to indicate that it is a proper subgroup. A *section* (or *subquotient*) of a group

G is a group H/K where K is normal in H and $H \leq G$. A *chief factor* of a group G is a non-trivial section H/K where H, K are both normal in G and there are no normal subgroups of G properly between H and K. If moreover H is contained in some subgroup $E \leq G$, we also say that H/K is a *G-chief factor* of E.

A subgroup H of G is *subnormal* in G if there is a finite chain of subgroups $H = H_0 < H_1 \cdots < H_n = G$ such that H_i is normal in H_{i+1} for all i. The *automizer* of a subgroup $H \leq G$ is $N_G(H)/C_G(H)$, where $N_G(H)$, $C_G(H)$ denote the normalizer and centralizer of H in G. Let $Z(G)$ be the center of G.

Given a set of primes π, write π' for the complement of π. If G is a finite group, let $\pi(G)$ denote the set of prime divisors of the order $|G|$ of G. We say G is a *π-group* if $\pi(G) \subseteq \pi$. Let $O_\pi(G)$ be the largest normal π-subgroup of G. We write $O_p(G)$ for $O_{\{p\}}(G)$ and write $O(G)$ for $O_{2'}(G)$. If P is a p-group, then $\Omega_1(P)$ is the subgroup of P generated by all elements of order p.

A group G is *perfect* if it is equal to its commutator subgroup $[G, G]$; and it is *quasisimple* if it is perfect and $G/Z(G)$ is simple. A *component* of a finite group is a subnormal quasisimple subgroup. It is known that any two distinct components commute. We write $E(G)$ for the subgroup of G generated by all components.

The *Fitting subgroup*, $F(G)$, is the largest normal nilpotent subgroup of G. Equivalently, $F(G)$ is the direct product of $O_p(G)$, as p ranges over $\pi(G)$. The *generalized Fitting subgroup* of G is the group $F^*(G) := E(G)F(G)$. This group satisfies the important property that $C_G(F^*(G)) = Z(F(G))$. A group G is called *almost simple* if $F^*(G)$ is a non-abelian simple group (or equivalently, $S \leq G \leq \mathrm{Aut}(S)$ where S is a non-abelian simple group).

2. Main Results

We fix an algebraically closed field k of characteristic p, and consider Oort groups for k. Cyclic-by-p Oort groups are local Oort groups by [8], and Oort groups are O-groups by [8, Corollaries 3.5 and 4.6]. Using the (now-proven) Oort Conjecture together with additional results (especially from [8]), we prove the converse of the first fact and a partial converse of the second. We also give an explicit description of O-groups; this restricts the forms that Oort groups can have, and would classify those groups if it is shown that Oort groups and O-groups are the same in general.

Theorem 2.1. *A cyclic-by-p group is an Oort group for k if and only if it is a local Oort group for k.*

Proof. The forward direction was shown at [8, Corollary 2.6]. For the reverse direction, let G be a local Oort group for k.

If $p \neq 2$, then G is either cyclic or is dihedral of order $2p^n$ for some n by [8, Theorem 3.3]. In the former case, G is an Oort group for k by [24]. In the latter case, every quotient of G is a local Oort group, by [8, Proposition 2.11].

Hence for all $m \leq n$, the group D_{2p^m} is a local Oort group. But also every cyclic group is an Oort group by [24], and hence is a local Oort group by the forward direction of the theorem. Thus every subgroup of G is a local Oort group. It then follows from [8, Theorem 2.4] that G is an Oort group.

Next suppose that $p = 2$. By [8, Theorem 4.4], G is either cyclic, or is a dihedral 2-group, or is the alternating group A_4, or is a semi-dihedral or generalized quaternion group of order at least 16. In the first two cases, the conclusion follows as for the case of p odd. If $G = A_4$, then every proper subgroup of G is either cyclic or a Klein four group. But these subgroups are Oort groups by [24] and [23] respectively, and hence are local Oort groups as above. So G is an Oort group by [8, Theorem 2.4]. As for the remaining two cases, in fact they do not occur. Namely, semi-dihedral groups of order at least 16 are not local Oort groups, because [9, Theorem 4.1] says that every local Oort group is a KGB-group (see [9, Definition 1.1] for the definition of that notion), and because such semi-dihedral groups are not KGB groups by [9, Theorem 1.2]. Moreover generalized quaternion groups are also not local Oort groups, by [6, Proposition 4.7, Theorem 4.8]. $\qquad\square$

Hence the set of local Oort groups for k is closed under taking subquotients, since this holds for the set of Oort groups for k [8, Corollary 2.7]. (In [8, Proposition 2.11] it was shown the local Oort groups are closed under taking quotients; but it had been left open whether closure also held for subgroups.)

The next two results give a partial converse to the fact (see [8, Corollaries 3.5 and 4.6]) that every Oort group is an O-group.

Theorem 2.2. *Let k be an algebraically closed field of characteristic p.*

(1) *Let n be a positive integer, and suppose that the dihedral group D_{2p^n} is an Oort group for k. Then for every finite group G of order not divisible by $2p^{n+1}$, G is an Oort group for k if and only if G is an O-group for p.*

(2) *In particular, if $2p^2$ does not divide the order of a finite group G, then G is an Oort group for k if and only if G is an O-group for p.*

Proof. Every Oort group is an O-group by [8, Corollaries 3.5 and 4.6], so it suffices to show the reverse implication, under the hypothesis of the theorem. By [8, Theorem 2.4], it is enough to show that every cyclic-by-p subgroup H of G is a local Oort group, or equivalently (by Theorem 2.1 above) that H is an Oort group.

Let G be O-group for p whose order is not divisible by $2p^{n+1}$. Then every cyclic-by-p subgroup of G is either cyclic, or of the form D_{2p^m} for some $m \leq n$, or (if $p = 2$) isomorphic to A_4. Cyclic groups are Oort groups by [20] and [24], and A_4 is an Oort group for algebraically closed fields of characteristic 2 (see [5] and [19]). By hypothesis, D_{2p^n} is an Oort group, and hence so is its quotient group D_{2p^m} for $m \leq n$, by [8, Corollary 2.7]. So

indeed every cyclic-by-p subgroup H of G is a (local) Oort group, proving part (1).

Part (2) then follows immediately, using that D_{2p} is a local Oort group by [5]. □

Thus unconditionally, if G is an O-group whose order is odd or divisible by p at most once (or at most twice if $p = 2$), then G is an Oort group. As another application of Theorem 2.2, every O-group for 3 whose order is not divisible by 54 is an Oort group for any algebraically closed field k of characteristic 3. This follows from the fact that the dihedral group of order 18 is a local Oort group for k by [18], and hence is an Oort group for k by Theorem 2.1.

Corollary 2.3. *Let k be an algebraically closed field of characteristic p. Then the following assertions are equivalent:*

(1) *For every n, the dihedral group D_{2p^n} is an Oort group for k.*
(2) *The Strong Oort Conjecture 1.2 holds.*
(3) *The class of Oort groups for k is the same as the class of O-groups for p.*

Proof. The implication (1) $\Rightarrow$ (3) is immediate from Theorem 2.2, and the implications (3) $\Rightarrow$ (2) $\Rightarrow$ (1) are trivial. □

We next turn to our classification results for O-groups. For p odd, the almost simple O-groups are given explicitly in Theorem 3.8 below. Using that result, we will obtain the following classification theorem for more general O-groups with p odd (see the proof at the end of Section 3):

Theorem 2.4. *Let p be an odd prime. Let G be a finite group. Set $R = O_{p'}(G)$. Let P be a Sylow p-subgroup of G. Then G is an O-group if and only if: P is cyclic and one of the following two (disjoint) conditions holds:*

(1) *$G = RP$, or equivalently $N_G(P) = C_G(P)$; or*
(2) *$|N_G(P)/C_G(P)| = 2$, the order p subgroup $Q \leq P$ has the property that $C_G(Q)$ is abelian and every element of $N_G(Q) \smallsetminus C_G(Q)$ is an involution that inverts $C_G(Q)$.*

Moreover, if (2) holds, then R is solvable and either G/R is a dihedral group of order $2p^a$ or G/R is an almost simple group given in (1)-(4) of Theorem 3.8.

If G has odd order, the previous two results immediately give:

Corollary 2.5. *Let p be an odd prime and G a group of odd order. Then the following are equivalent:*

(1) *G is an Oort group;*
(2) *G is an O-group;*
(3) *a Sylow p-subgroup P of G is cyclic and $N_G(P) = C_G(P)$; and*
(4) *a Sylow p-subgroup P of G is cyclic and $G = RP$ where $R = O_{p'}(G)$.*

For $p = 2$, there is an even more explicit description of O-groups:

Theorem 2.6. *Let G be a finite group with a Sylow 2-subgroup P. Then G is an O-group for $p = 2$ if and only if either*

(1) *P is cyclic, which implies $G = RP$ where we write R for the solvable group $O(G)$; or*

(2) *P is dihedral, and $C_G(K) = K$ for all elementary abelian subgroups $K \leq P$ of order 4.*

The above theorem is proven at the beginning of Section 4. For the dihedral case of Theorem 2.6, the next assertion provides a more precise structure result. Its proof appears at the end of Section 4.

Theorem 2.7. *Let G be an O-group when $p = 2$. Set $R = O(G)$. Let P be a Sylow 2-subgroup of G and suppose P is dihedral. Set $N = N_G(P)$. Then $[R, R]$ is nilpotent and every elementary abelian subgroup of order 4 in G acts fixed point freely on the non-identity elements of R. Moreover, one of the following holds:*

(1) *A_4 is not a subgroup of G, and $G = RP$; or*

(2) *A_4 is a subgroup of G, and*

    (a) *$G = RA_4$ is semi-direct and every A_4-invariant section of R is an irreducible 3-dimensional A_4-module; or*

    (b) *$G = RS_4$ is semi-direct and every A_4-invariant section of R is an irreducible 3-dimensional A_4-module in which an element of order 4 has trace 1; or*

    (c) *G is not solvable, R is nilpotent, $G/R \cong \mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ with $q > 4$ a power of an odd prime r, and all G invariant sections of R are 3-dimensional absolutely irreducible modules (over the G-endomorphism ring). Moreover, R is an r-group unless possibly $q = 5$ or 7 with $G/R = \mathrm{PSL}(2, q)$.*

3. O-GROUPS FOR ODD PRIMES

In this section we prove Theorem 2.4, classifying the finite groups that are O-groups for an odd prime p. We begin with two lemmas that apply for all primes p.

Lemma 3.1. *Let G be an O-group in characteristic p. Then every section of G is an O-group.*

Proof. First note that it suffices to consider sections that are quotient groups, since subgroups of O-groups are O-groups. We now reduce to the case in which G is cyclic by p. To make this reduction, it will suffice to show that if $\pi : G \to \Gamma$ is a surjection of groups and T is a cyclic-by-p subgroup of Γ, there is a cyclic by p-subgroup T' of G such that $\pi(T') = T$. Let P_T be the (normal) Sylow p-subgroup of T. Every Sylow p-subgroup $P_{T''}$ of $T'' = \pi^{-1}(P_T)$ surjects onto P_T under π, and all such $P_{T''}$ are contained in the kernel J of $\pi^{-1}(T) \to T/P_T$. So if t' is a element of $\pi^{-1}(T)$ whose image

in T/P_T generates T/P_T, we know that $t'P_{T''}t'^{-1} = t_0 P_{T''} t_0^{-1} \leq J$ for some $t_0 \in J$. Now $t = t_0^{-1} t'$ normalizes $P_{T''}$ so we can take T' to be the group generated by t and $P_{T''}$.

If p is odd, this implies that either G is cyclic (and so every section is also cyclic) or G is dihedral of order $2p^a$ (and so every section is either cyclic or dihedral of order $2p^b$).

If $p = 2$, G is either cyclic, A_4 or a dihedral 2-group and the result is clear.   □

We will use the above result often and usually without comment.

See [28] for the next result. All proofs of this lemma seem to require the classification of finite simple groups. Here $C_G(\sigma)$ denotes the subgroup of G consisting of elements fixed by an automorphism σ.

Lemma 3.2. *Let G be a finite group with σ an automorphism of order coprime to $|G|$. If $C_G(\sigma)$ is abelian, then G is solvable.*

For the remainder of the section, we fix an odd prime p. Let G be a finite group with a Sylow p-subgroup P, and let $\mathcal{C}_p(G)$ be the set of cyclic-by-p subgroups of G. Our goal is to characterize all O-groups for p; i.e. all finite groups G such that every $H \in \mathcal{C}_p(G)$ either is cyclic or is dihedral of order twice a power of p.

In [8, §3], the conclusion of the following result was proven under the (a priori stronger) hypothesis that G is an Oort group:

Lemma 3.3. *Let G be an O-group. Then:*
  (1) *A Sylow p-subgroup P of G is cyclic.*
  (2) *If $1 \neq Q \leq P$, then either*
     (a) *$N_G(Q) = C_G(Q)$, or*
     (b) *$N_G(Q)/C_G(Q)$ has order 2 and every element in $N_G(Q)$ either centralizes Q or is an involution that acts as inversion on $C_G(Q)$, and $C_G(Q)$ is abelian.*

Proof. Part (1) is a trivial consequence of the hypothesis. For part (2), note that Q is a cyclic p-group by part (1). If $x \in N_G(Q) \setminus C_G(Q)$, the group $\langle x, Q \rangle$ is a cyclic-by-p group which is not abelian. Hence since G is an O-group, $\langle x, Q \rangle$ is a dihedral group of order $2p^n$ for some n. Since x does not centralize Q this means x must be an involution. Choose one such involution x. If $g \in C_G(Q)$, then xg is also in $N_G(Q) \setminus C_G(Q)$, so it is also an involution. This implies x acts as inversion on $C_G(Q)$. Since conjugation by x is a homomorphism, $C_G(Q)$ is abelian.   □

It is easy to handle one case.

Lemma 3.4. *Let G be a finite group with a cyclic Sylow p-subgroup P. Let $R = O_{p'}(G)$. The following are equivalent:*
  (1) *$G = RP$.*
  (2) *$N_G(P) = C_G(P)$.*

(3) $N_G(Q) = C_G(Q)$ *for every non-trivial subgroup Q of P.*

If any of these conditions hold then G is an O-*group.*

Proof. Suppose first that $N_G(P) = C_G(P)$. By Burnside's normal p-complement theorem [17, p. 419], $G = R'P$ with R' a normal p'-subgroup which is a complement to P. Because P is a p-group, R' must be $R = O_{p'}(G)$ so $G = RP$.

Suppose now that $G = RP$. Let us prove that $N_G(P) = C_G(P)$. We have $N_G(P) = R'P$ where $R' = N_G(P) \cap R$. Now both P and R' are normal in $N_G(P)$ and they have trivial intersection, so $N_G(P)$ is isomorphic to the product of P and R'. This implies $N_G(P) = C_G(P)$.

We have now shown that conditions (1) and (2) are equivalent, and clearly (3) implies (2). So it will suffice to show that if (1) and (2) hold then (3) holds. Let Q be a subgroup of P and let $G' = RQ$. Then $N_{G'}(Q) = C_{G'}(Q)$ by applying the equivalence of conditions (1) and (2) for the group G'. So since P is cyclic, we get $N_G(Q) = \langle P, N_{G'}(Q) \rangle = \langle P, C_{G'}(Q) \rangle = C_G(Q)$.

For the final assertion in the Lemma, we suppose condition (3) holds. If Q is any subgroup of P, then $N_G(Q) = C_G(Q)$. Since P is cyclic, this implies that every cyclic-by-p subgroup of G is in fact cyclic, so G is an O-group. $\square$

We now turn to the other case of Lemma 3.3, i.e. of O-groups G such that $N_G(P) \neq C_G(P)$.

Lemma 3.5. *Let G be an* O-*group with Sylow p-subgroup P, such that $N_G(P) \neq C_G(P)$. Let τ be an element of $N_G(P) \smallsetminus C_G(P)$. Then τ is an involution that acts as inversion on the abelian subgroup $C_G(P)$. Since P is cyclic, τ normalizes each subgroup of P. Let $1 \neq Q \leq P$.*

(1) *Every element of $\tau C_G(Q)$ is an involution and acts as inversion on $C_G(Q)$.*
(2) *$C_G(Q) = C_G(P)$ is abelian.*
(3) *$N_G(Q) = N_G(P)$.*
(4) *Every member of the set $\mathcal{C}_p(G)$ of cyclic by p subgroups of G either has order prime to p or is conjugate to a subgroup of $N_G(P)$.*

Proof. The first statement concerning τ was shown in Lemma 3.3. If $g \in C_G(Q)$, then $\langle Q, \tau g \rangle$ is in $\mathcal{C}_p(G)$ and is not cyclic, whence it must be dihedral of order $2p^a$ for some a. In particular, every element either is a p-element or has order 2. Thus, τg is an involution and so τ inverts g. This proves the first statement.

Since inversion is an automorphism of $C_G(Q)$, it follows that $C_G(Q)$ is abelian. Since $C_G(Q)$ contains P we conclude that $C_G(Q) = C_G(P)$. By Lemma 3.3, $N_G(Q) = \langle C_G(Q), \tau \rangle = \langle C_G(P), \tau \rangle = N_G(P)$.

If $X \in \mathcal{C}_p(G)$ and does not have order prime to p, then, by conjugating, we may assume that $Q := O_p(X) \leq P$, whence $X \leq N_G(Q) = N_G(P)$. $\square$

This gives the following nice criterion for checking for O-groups.

Corollary 3.6. *Let p be an odd prime, G a finite group with cyclic Sylow p-subgroup P. The following conditions are equivalent:*

(1) *G is an O-group.*
(2) *$N_G(\Omega_1(P))$ is an O-group.*
(3) *Either $N_G(P) = C_G(P)$, or there is an involution τ inverting the abelian group $C_G(\Omega_1(P))$ and $N_G(\Omega_1(P)) = \langle C_G(\Omega_1(P)), \tau \rangle$.*

Proof. That (1) implies (2) is immediate. Since the Sylow p-subgroups of G are cyclic, any cyclic-by-p subgroup of G can be conjugated into $N_G(\Omega_1(P))$, so (2) implies (1). To show (2) implies (3), note first that the normalizer in G of any non-trivial subgroup of P is contained in $N_G(\Omega_1(P))$. Hence (2) implies (3) on replacing G by $N_G(\Omega_1(P))$ and on letting $Q = \Omega_1(P)$ in Lemmas 3.3 and 3.5. Suppose finally that condition (3) holds. If $N_G(P) = C_G(P)$ then (1) holds by Lemma 3.4. So we now suppose that there is an involution τ as in part (3). Suppose that X is a cyclic by p subgroup of G. By conjugating X inside G, we can suppose that X is contained in $N_G(\Omega_1(P))$, which by hypothesis is $\langle C_G(\Omega_1(P)), \tau \rangle$. From the fact that τ is an involution inverting the abelian group $C_G(\Omega_1(P))$, we now see that X is either cyclic or dihedral of order $2p^n$ for some integer n. Hence (1) holds. $\square$

Note that the above results prove that G is an O-group if and only if its Sylow p-subgroup is cyclic and either (1) or (2) of Theorem 2.4 holds; see the proof of Theorem 2.4 at the end of this section for details. The following results will enable us to complete the proof of that theorem.

Lemma 3.7. *Let G be an O-group with Sylow p-subgroup P, such that $N_G(P) \neq C_G(P)$. Then $R := O_{p'}(G)$ is solvable.*

Proof. The hypotheses imply that the Sylow p-subgroup P is cyclic. Let Q be the subgroup of P of order p. We know furthermore by Lemma 3.3 that there is an involution $\tau \in G$ which normalizes Q. The group D generated by Q and τ is dihedral of order $2p$. If τ were in the normal p'-subgroup R, then we would have $g\tau g^{-1} \in R$ when g generates Q. Then $\tau^{-1} g\tau g^{-1} = g^{-2} \in R$, but this is a non-trivial element of Q because p is odd, contradicting the fact that R has order prime to p. Thus τ does not lie in R, so the semi-direct product RD has order $|R| \cdot 2p$. We now observe that $R' = O_{p'}(RD)$ equals R, since R' contains R and R'/R is a normal p'-subgroup of the dihedral group $D = RD/R$ of order $2p$. Hence we can reduce to the case in which $G = RD$, so now $P = Q$.

Passing to a quotient, we may also assume that R contains no non-trivial normal solvable subgroup of G. We will suppose R is non-trivial and obtain a contradiction. Since R is normal in G, there is a non-trivial minimal normal subgroup N of G which is contained in R. This N must be the product of some number of copies of isomorphic simple groups, which by assumption must be non-abelian. Thus, P acts on R and on N, and $C_R(P)$ is abelian because $C_G(P)$ is abelian by Lemma 3.5.

Suppose there is a simple factor of N which is not fixed by $P = Q$. Then P would permute some number of factors. Because $|P| = p$, P would then centralize a subgroup of N which is a diagonally embedded copy of one simple factor. This contradicts the fact that $C_R(P)$ abelian since the simple factors of N are not abelian. Thus P fixes each factor of N.

Let N_0 be one of the simple factors of N, so that P normalizes N_0. A generator σ of P then acts on N_0. The centralizer $C_{N_0}(\sigma)$ is contained in the abelian group $C_R(P)$ so it is abelian. Therefore by Lemma 3.2, N_0 must be solvable, contradicting the fact that it is a non-abelian simple group. This contradiction completes the proof. □

We next classify the almost simple O-groups. This seems to require the classification of finite simple groups.

Theorem 3.8. *Let G be a finite group and let p be an odd prime. Suppose that G is almost simple, i.e. that $S := F^*(G)$ is a non-abelian simple group. Then G is an O-group if and only if one of the following holds:*

(1) $G = \mathrm{PSL}(2, q)$ *or* $\mathrm{PGL}(2, q)$ *with $q > 3$ and p dividing $q^2 - 1$.*
(2) $G = S = \mathrm{Sz}(q)$ *with $q = 2^{2k+1} > 2$ and $p|(q-1)$.*
(3) $G = S = \mathrm{Re}(q)$ *with $q = 3^{2k+1} > 3$ and p dividing $q - 1$.*
(4) $S = \mathrm{PSL}(3, 4)$ *and $[G : S] = 1, 2$ or 4 with $p = 5$.*
(5) $N_G(P) = C_G(P)$ *for P a Sylow p-subgroup of G.*

Proof. We begin by supposing that G is an O-group. We can also suppose that (5) does not hold. Therefore p divides the order of G, and by Lemma 3.3, a Sylow p-subgroup P of G is cyclic and $N_G(P)/C_G(P)$ has order 2, where there is an involution $\tau \in G$ which inverts P. Then S is also an O-group.

Let us show that S contains P. Let $H = SP$. Then H is an O-group since $H \leq G$. If $C_H(P) = N_H(P)$ then by Burnside's normal p-complement theorem, $H = O_{p'}(H)P$. Since P is cyclic, and S a non-abelian simple group, the image of S in $H/O_{p'}(H)$ is trivial, so $S \leq O_{p'}(H)$. But $S = F^*(G)$ is normal in G, so $H = SP = O_{p'}(H)P$ implies $S = O_{p'}(H)$. By Lemma 3.7, $O_{p'}(G)$ is solvable. But S is normal in G and $S = O_{p'}(H)$ has order prime to p, so $S \leq O_{p'}(G)$. This is a contradiction because S is not solvable. Therefore, $C_H(P) \neq N_H(P)$ so $N_H(P)$ is generated by $C_H(P)$ and an involution $\tau \in N_H(P)$ which inverts P by Corollary 3.6. Since p is odd, this means $P \leq [H, H]$, and $[H, H] = S$ since $H = SP$. Thus $P \leq S = H$ and $N_S(P) \neq C_S(P)$. In particular, case (5) does not hold when G is replaced by S; we will need this fact later.

We now first consider the case that $S = G$. In particular, Lemmas 3.3 and 3.5 shows that if $1 \neq x \in P$, then $|x^S \cap P| = 2$, where x^S is the set of S-conjugates of x. If S is a sporadic group, this can never happen (see [13, 5.3]). If S is the alternating group A_n, then an element of order p has at least $(p-1)/2$ conjugates, whence $p \leq 5$. Since P is cyclic, this forces $n = 5$ for $p = 3$. Then $S = A_5 \cong \mathrm{PSL}(2, 4)$. If $p = 5$ and $n \geq 7$, then a p-cycle is

rational (i.e. is conjugate to all its non-trivial powers). So $n = 5$ or 6. Thus, $S = G = \mathrm{PSL}(2, q)$ with $q = 4$ or 9. So if $S = A_n$ we are in case (1).

So we may assume that S is a simple finite group of Lie type in characteristic r. If $p = r$, then $S = \mathrm{PSL}(2, p)$ (since the Sylow p-subgroup is cyclic). An element of order p is conjugate to $(p-1)/2$ of its powers, whence $p \le 5$. Since S is simple, $p \ge 5$ and so $p = 5$ is the only possibility. Then $S = G = \mathrm{PSL}(2, 5) \cong \mathrm{PSL}(2, 4)$ and we are in case (1).

So assume that $p \ne r$. We require some facts about maximal tori in the finite groups of Lie type. See [26, §14] and [25, II.1] for details. Since P is cyclic and its centralizer is abelian, it follows that $C_S(P)$ is a maximal torus T and P is generated by a semi-simple regular element. In particular, T is a non-degenerate maximal torus. These are parametrized by (twisted) conjugacy classes of elements in the Weyl group W of S. Moreover, $N_G(T)/T$ is isomorphic to the centralizer of this element in the Weyl group and has order 2. Inspection of the Weyl groups shows that this forces S to be either a rank one Chevalley group (i.e. $S \cong \mathrm{PSL}(2, q)$, $\mathrm{PSU}(3, q)$, $\mathrm{Sz}(q)$ or $\mathrm{Re}(q)$) or else $S = \mathrm{PSL}(3, q)$.

In the case that $S = \mathrm{PSL}(3, q)$, T is the maximal torus that is cyclic of order $(q^2 - 1)/(3, q-1)$. The normalizer of T acts on T by sending a generator x to x^q. On the other hand, the normalizer also acts by inversion on T by Lemma 3.5. Hence $(q - 1)/(3, q - 1) \le 2$, whence $q = 2, 4$ or 7. Moreover, $p|(q+1)$. So $q \ne 7$, since p is odd. If $q = 2$, then $S = \mathrm{PSL}(3, 2) = \mathrm{PSL}(2, 7)$, as in case (1). Finally, if $q = 4$ then $p = 5$ as in case (4).

Now consider the rank 1 Chevalley groups. The only maximal torus in the Suzuki or Ree groups with automizer of order 2 is the quasi-split torus (i.e. the torus contained in a Borel subgroup and so the torus has order $q - 1$; note that this rules out the group $\mathrm{Re}(3)'$). Note that since $P \le T$ this means $p|(q - 1)$. The other conditions on p and q for the Suzuki and Ree groups follow from the fact that S is simple, so these cases fall into Cases (2) and (3). For the group $\mathrm{PSL}(2, q)$, we must have $q > 3$ and $p|(q^2 - 1)$ as in case (1). If $S = \mathrm{PSU}(3, q)$, we argue as above in the case of $\mathrm{PSL}(3, q)$. Now $p|(q - 1)$ and the involution normalizing the maximal torus must be inversion but also raises a generator to the $-q$th power. This implies that $(q + 1)/(3, q + 1) \le 2$, whence $q = 2$ and the group is solvable.

We now continue to suppose G is an O-group, but we drop the assumption that $G = S$. The above arguments show that S must be as in (1) - (4), since S is an O-group and we proved earlier that (5) cannot hold for S. Since $P < S$ is a Sylow p-subgroup of S, Sylow's Theorems and the Frattini argument imply that $G = SN_G(P)$.

Since S is not in case (5), $|N_S(P)/C_S(P)| = 2$ by Lemma 3.3 and there is an involution τ of $N_S(P)$ which acts by inversion on P. If β is in $N_G(P)$ then either $\beta \in C_G(P)$ or $\tau\beta \in C_G(P)$. So since $\tau \in S$ and $G = SN_G(P)$ we conclude that $G = SC_G(P)$. Since $\tau \in S$ and S is normal in G, we have $[\tau, C_G(P)] \le S$. Because τ inverts $C_G(P)$, we have $\tau c \tau^{-1} c^{-1} = c^{-2}$

for $c \in C_G(P)$ so all squares in $C_G(P)$ are contained in S. Thus, G/S is an elementary abelian 2-group.

Let us prove that $G = S$ in cases (2) and (3). Since $S = F^*(G)$ is a non-abelian simple group, we know $S \leq G \leq \mathrm{Aut}(S)$. However, for the S in (2) and (3), $\mathrm{Aut}(S)/S = \mathrm{Out}(S)$ has odd order, so the 2-group G/S is trivial and $G = S$ and we have already treated this case.

Suppose $S = \mathrm{PSL}(2, q)$ as in case (1). We have shown $G = SC_G(P)$ and that $S \leq G \leq \mathrm{Aut}(S)$, with G/S an elementary abelian 2-group. Further $P < S$ is cyclic of order p^n for some odd prime p, and p is prime to q. Therefore a generator g of P lifts to an element $\tilde{g} \in \mathrm{SL}(2, q)$ of order p^n, and $\tilde{g}$ is semi-simple with distinct eigenvalues. Thus, the centralizer T of P in $\mathrm{SL}(2, q)$ is a maximal torus T that is cyclic of order $q + 1$. Moreover, $C_G(P) = C_G(T)$. Only an outer automorphism of $S = \mathrm{PSL}(2, q)$ coming from conjugation by an element of $\mathrm{PGL}(2, q)$ centralizes T. Since $G = SC_G(P) = SC_G(T)$, $G = \mathrm{PGL}(2, q)$ or $G = \mathrm{PSL}(2, q)$ are the only possibilities.

Suppose now that $S = \mathrm{PSL}(3, 4)$ is as in case (4). We know $\mathrm{Aut}(S)/S$ is the dihedral group of order 12, and $S \leq G \leq \mathrm{Aut}(S)$. Since $G = SC_G(P)$, we find that $|G/S| = 1, 2$ or 4. This completes the proof of the 'only if' part of Theorem 3.8.

As for the 'if' part of the proof, it is straightforward to see that if G is any of the groups listed in (1) - (3) of the theorem, then the normalizer of any non-trivial p-subgroup is dihedral. Therefore G is an O-group. With the above notation we showed groups for which (5) is true are O-groups by Lemma 3.4.

Suppose now that G is as in case (4), so $S = \mathrm{PSL}(3, 4)$ and $[G : S] = 1, 2$ or 4 with $p = 5$. Then $S \leq G \leq \mathrm{Aut}(S)$ and $\mathrm{Aut}(S)/S$ is the dihedral group of order 12. Thus, up to conjugation, we may assume that $G \leq H := \langle S, x, y \rangle$ where x induces transpose inverse on S and y induces the Frobenius automorphism of order 2 on S. Let P be a Sylow 5-subgroup of G. It is straightforward to compute that $N_H(P) = D \times L$ where D is dihedral of order 2 and L is elementary abelian of order 4. Thus, every element in $N_H(P) \setminus C_H(P)$ is an involution and acts as inversion on $C_H(P)$. This completes the proof of the 'if' direction of Theorem 3.8. $\qquad \square$

Theorem 3.9. *Let G be an* O-*group with Sylow p-subgroup P, such that $N_G(P) \neq C_G(P)$. Let $R = O_{p'}(G)$. Then either $G = RD$ with D dihedral of order $2p^a$ for some $a > 0$ or else $G/R \cong S$, where S is an almost simple group given in (1) - (4) of Theorem 3.8.*

Proof. First suppose that G/R has a non-trivial normal p-subgroup. Let Q be the subgroup of order p in P. Then RQ/R is a subgroup of order p in a (cyclic, normal, non-trivial) p-subgroup of G/R so RQ/R is normal in G/R. Now RQ is normal in G, so the Frattini argument shows $G = RN_G(Q)$. Since $N_G(Q)$ contains $C_G(Q) = C_G(P)$ with index 2, this means $RC_G(P)$ is normal of index 1 or 2 in G. We have shown $C_G(Q) = C_G(P) = A \times P$

where A is an abelian subgroup of order prime to p and the involution τ of $N_G(Q)$ acts by inversion on $C_G(Q)$. This implies that RA is stable under conjugation by P and by τ, so RA is in fact normal in G. Thus $A \leq R = O_{p'}(G)$. Let D be the dihedral group of order $2|P|$ generated by τ and P. We conclude that $G = RD$ is the semi-direct product of R and D, since $D \cap R$ must be a normal p'-subgroup of D, which forces $D \cap R$ to be trivial.

So we may assume that G/R has no non-trivial normal p-subgroup. By Lemma 3.1, we may pass to G/R and assume that $R = 1$. Thus every normal subgroup of G has order divisible by p but is not a p-group.

In other words, $O_p(G) = O_{p'}(G) = 1$. In particular, $F(G) = 1$ and so $F^*(G) = E(G)$ is a direct product of (non-abelian) simple subgroups of order divisible by p. Since a Sylow p-subgroup of G is cyclic, this implies that $S := F^*(G)$ is simple. Thus $S \leq G \leq \mathrm{Aut}(S)$. The result now follows by Theorem 3.8 and the hypothesis that $N_G(P) \neq C_G(P)$. $\square$

Using the above results, we can now prove Theorem 2.4:

Proof of Theorem 2.4. Suppose first that G is an O-group. By Lemma 3.3, a Sylow p-subgroup P of G is cyclic. Then $N_G(P) = C_G(P)$ if and only if $G = RP$ by Lemma 3.4. Suppose now that $N_G(P) \neq C_G(P)$. Then condition (2b) of Lemma 3.3 holds for the group $Q = P$. This means that there is an involution τ which acts by inversion on the abelian group $C_G(P)$. Here $P \leq C_G(P)$ and P is cyclic of odd order, so τ acts non-trivially by inversion on every non-trivial subgroup Q of P. This means that condition (2b) of Lemma 3.3 holds for all such Q. We have now shown that if G is an O-group then condition (1) or (2) of Theorem 2.4 must hold. Conversely, if a Sylow p-subgroup P of G is cyclic and one of conditions (1) or (2) of Theorem 2.4 holds, then G is an O-group by Corollary 3.6. The last statement of Theorem 2.4 follows immediately from Lemma 3.7 and Theorem 3.9. $\square$

In general, it seems difficult to give a more detailed classification of O-groups for p odd, i.e. to say much more than that D acts on the solvable group R with $C_R(P)$ abelian and inverted by D (with notation as in Theorem 3.9).

Problem 1. Classify the groups R admitting such an action by a dihedral group of order $2p^a$.

4. O-GROUPS FOR THE PRIME 2

In this section, we characterize O-groups in characteristic 2 — i.e. those finite groups G such that every cyclic-by-2 subgroup H of G is either cyclic, a dihedral 2-group or isomorphic to A_4. We begin by proving Theorem 2.6 and conclude by proving Theorem 2.7.

Proof of Theorem 2.6. If G is an O-group, then P must be either cyclic or dihedral. The group $R = O(G) = O_{2'}(G)$ is solvable by the Feit-Thompson Theorem. First suppose that P is cyclic. Burnside's normal p-complement theorem says that R is a normal complement to P in G if P is central in its normalizer $N_G(P)$. If $\sigma \in N_G(P)$ has odd order, then conjugation by σ must induce the trivial automorphism of P since $\mathrm{Aut}(P)$ is a 2-group. Thus σ centralizes P, and $G = RP$ follows.

Now suppose P is dihedral. Then P contains a Klein four subgroup K. For each such K, there can be no subgroup of G of the form $K \times X$ with X non-trivial, since G is an O-group. Since $C_P(K) = K$, it follows that $C_G(K) = K$.

So now assume conversely that either P is cyclic, or else P is dihedral and that each elementary abelian subgroup $K \leq P$ of order 4 satisfies $C_G(K) = K$.

Let $H \leq G$ be a cyclic-by-2 subgroup; i.e. $H/O_2(H)$ is cyclic of odd order. We may assume that $O_2(H) \leq P$. Then $O_2(H)$ is either cyclic or dihedral. In order to show that G is an O-group, we want to show that H is either cyclic, or a dihedral 2-group, or is isomorphic to A_4.

Suppose first that $O_2(H)$ is not an elementary abelian subgroup of order 4. Then the automorphism group of $O_2(H)$ is a 2-group, whence $H = O_2(H) \times O(H)$ with $O(H)$ cyclic. If $O_2(H)$ is cyclic, then H is cyclic. If $O_2(H) \leq P$ is not cyclic, then $O_2(H)$ contains a Klein four subgroup K. But then $O(H)$ centralizes K, whence $O(H) = 1$ because we have assumed $C_G(K) = K$. Therefore $H = O_2(H)$ is a cyclic or dihedral 2-group.

Finally, suppose $K := O_2(H)$ is elementary abelian of order 4. Then H is contained in the normalizer $N_G(K)$, and $N_G(K)/K = N_G(K)/C_G(K)$ embeds in $\mathrm{Aut}(K) \cong S_3$. This implies $H = K$ or A_4 since $K = O_2(H)$ is the Sylow 2-subgroup of H. So again H is of the permissible form, concluding the proof. □

Remark. (1) In Theorem 2.6(1), there is also a more elementary proof that $G = RP$ if P is cyclic when $p = 2$. Namely, embed G in S_n via the regular representation, and observe that G does not embed in A_n. So G contains a normal subgroup of index 2. The assertion follows by induction.

(2) In Theorem 2.6(2), one must have the condition for *all* elementary abelian Klein 4-subgroups, not just a single one. This can be seen by considering the semi-direct product $G = AD_8$, where A is abelian of odd order and D_8 acts by inversion on A with the kernel of the action being an elementary abelian subgroup K of order 4. Here the other Klein four subgroup of D_8 is self-centralizing in G, but K is not, and G is not an O-group.

In order to prove Theorem 2.7, we now further study the structure of O-groups in characteristic 2.

If the Sylow 2-subgroup P of an Oort group G is not cyclic, then P is dihedral, as in Theorem 2.6. In this situation, we next investigate the center of G.

Lemma 4.1. *Let G be an* O-*group in characteristic* 2 *with a non-cyclic Sylow* 2-*subgroup P, and set $R = O(G)$. Assume that $Z(G) \neq 1$. Then $|Z(G)| = 2$ or 4, and G is solvable. Moreover one of the following holds:*

(1) *G is elementary abelian of order* 4.
(2) *$|Z(G)| = 2$, R is abelian and $G = RP$. Moreover $C_P(R)$ is a cyclic subgroup of index 2 in P, and all elements of P not in $C_P(R)$ induce inversion on R.*

Proof. Let K be an elementary abelian subgroup of order 4 contained in P. Since $C_G(K) = K$ by Theorem 2.6, we see that $Z(G) \leq K$. This proves the first statement, on the order of $Z(G)$. Note that $|Z(P)| = 2$ unless $P = K$. So if $|Z(G)| = 4$, then $G = C_G(K) = K$ and so (1) holds.

The remaining case is that $Z(G)$ has order 2. This condition implies that $Z(G)$ is contained in every elementary abelian subgroup of order 4 of G.

We claim that this implies that $N_G(X)/C_G(X)$ is a 2-group for any non-trivial 2-subgroup X of G. If X is cyclic or dihedral of order greater than 4, this is clear since the automorphism group of X is a 2-group. If X is elementary abelian of order 4, then $X \cap Z(G) \neq 1$. The unique non-trivial element σ of $X \cap Z(G)$ must be fixed by conjugation by every element of $N_G(X)$. We conclude that $N_G(X)/C_G(X)$ embeds into the group of automorphisms of the Klein four group X which fix σ. This implies $N_G(X)/C_G(X)$ is a 2-group.

Thus by Thompson's normal p-complement theorem [27, Theorem 2.27] $G = RP$. Since $C_G(K) = K$, K acts without non-trivial fixed points on R. Therefore if x is a non-central involution in K, the map which sends $r \in R$ to $rxr^{-1} \in Rx$ is injective. Since $|R| = |Rx|$, every element of Rx is of the form rxr^{-1} for some $r \in R$. But $(rxr^{-1})^2 = e$, so every element of Rx is an involution. This implies conjugation by x is inversion on R, so R is abelian.

If $P = K$, then $C_P(R) = Z(G)$, a cyclic subgroup of index 2 in P. Condition (2) then holds.

On the other hand, if K is a proper subgroup of P, then there are other elementary abelian subgroups of order 4, and the same analysis applies to each of them. It follows that every involution in $P \smallsetminus Z(P)$ induces inversion on R, whence the product of any two such involutions centralizes R. Hence condition (2) again holds. This completes the proof. $\square$

The remaining case to treat is that $Z(G) = 1$. We first point out some restrictions on R.

Lemma 4.2. *Let G be an* O-*group for $p = 2$ with trivial center and with a non-cyclic Sylow* 2-*subgroup P. Set $R = O(G)$.*

(1) *$[R, R]$ is nilpotent.*
(2) *If A_4 is not a subgroup of G, then $G = RP$ with $C_R(K) = 1$, where $K \leq P$ is elementary abelian of order* 4.

Proof. For part (1) of the lemma, note that K acts on R without fixed points other than the identity, by case (2) of Theorem 2.6. Now apply [4, Theorem 2].

For part (2) of the lemma, we apply Thompson's normal p-complement result as in the proof of Lemma 4.1. $\square$

We next consider more specifically the special case that $R = 1$.

Lemma 4.3. *Under the hypotheses of Lemma 4.2, assume that $R = 1$ and $A_4 \leq G$. Then one of the following holds:*

(1) $G = A_4$ *or* S_4*; or*
(2) $G = \mathrm{PSL}(2, q)$ *or* $\mathrm{PGL}(2, q)$ *with q an odd prime power and $q > 4$.*

Proof. Let A be a minimal normal subgroup of G. Then A has even order since $R = 1$. If A is a 2-group, then it is elementary abelian. Since $Z(G) = 1$, $|A| > 2$. By case (2) of Theorem 2.6, one has $C_G(K) = K$ for every Klein four subgroup K of G. So A must be elementary abelian of order 4 and $A = C_G(A)$. Therefore $N_G(A)/A$ embeds in $\mathrm{Aut}(A) \cong \mathrm{GL}(2, 2) \cong S_3$ and is not a 2-group since $Z(G) = 1$ and $G = N_G(A)$. Thus, $G/A \cong \mathbb{Z}/3$ or S_3. It is trivial to see this is a split extension and $G \cong A_4$ or S_4.

Now suppose, on the other hand, that no minimal normal subgroup of G is a 2-group. Then $O_2(G) = 1$, and so $F(G) = 1$ (since $R = 1$). Thus $S := F^*(G) = E(G)$ is a direct product of non-abelian simple groups. Each factor of E has even order. Since S is an Oort group at 2, S has a dihedral Sylow 2-subgroup, whence S cannot be a non-trivial direct product. Thus, S is simple with a dihedral Sylow 2-subgroup. By the classification of simple groups with dihedral Sylow 2-subgroups [14, Theorem 1], we see that $S = \mathrm{PSL}(2, q)$ with q odd and $q > 4$. Note that since $F^*(G) = S$ we have $S \leq G \leq \mathrm{Aut}(S)$.

Let P be a Sylow 2-subgroup of G and set $Q = P \cap S$. Then Q and P are dihedral. Since elementary abelian subgroups of order 4 are self-centralizing by Theorem 2.6, we see that $C_G(Q) \leq Q$. By Thompson's normal p-complement theorem, or by inspection, S contains a group isomorphic to A_4.

By Sylow's theorems, $G = \langle S, N_G(Q) \rangle$. It follows that either $|Q| = 4$ and $N_G(Q) \cong A_4$, whence $N_G(P) \leq S$ and so $G = S$, or else P is non-abelian and dihedral, whence $N_G(Q) = P$ (since the automorphism group of Q is a 2-group). Since P is dihedral, it is generated by involutions, as is S, and so G is generated by involutions in $\mathrm{Aut}(S)$.

Recall that $\mathrm{Aut}(S)$ is generated by $\mathrm{PGL}(2, q)$ and the Frobenius automorphism. It follows by [12, 7.6] that any involution x in $\mathrm{Aut}(S)$ is either contained in $\mathrm{PGL}_2(q)$ or $q = q_0^2$ and x is conjugate to the q_0-Frobenius automorphism. In the latter case, $C_S(x)$ contains a copy of $\mathrm{PSL}_2(q_0)$, whence x centralizes an elementary abelian subgroup of order 4. Such an x cannot be in G by Theorem 2.6. Thus, $\mathrm{PSL}(2, q) \leq G \leq \mathrm{PGL}(2, q)$ with $4 < q$ odd. $\square$

Lemma 4.4. *Let $H = \mathrm{PSL}(2, q)$ or $\mathrm{PGL}(2, q)$ with q odd and $q > 4$. Let F be a field of characteristic $r \neq 2$, and let V be an absolutely irreducible FH-module. Suppose that there is a subgroup J of H isomorphic to A_4 such that there are no fixed points for the action of the Klein four subgroup $K := O_2(J) \leq J$ on V. Then the following hold:*

 (1) *$\dim V = 3$;*
 (2) *every involution x in J has trace -1 on V;*
 (3) *either $r | q$ or $H = \mathrm{PSL}(2, q), q \leq 7$.*

Proof. Without loss of generality, we can base change to the algebraic closure of F to be able to assume that F is algebraically closed. Let χ denote the Brauer character of H on V. For all $r \neq 2$, the three-dimensional irreducible representation M of A_4 over F is projective and injective as a module for FH. If V is not the direct sum of copies of M (as an A_4-module), then the socle of V contains a one-dimensional J-submodule, and this character is trivial on K. Since K acts fixed point freely on V, this is contradiction. So V is a direct sum of copies of M, and $\chi(x) = -\dim V/3$ for each $x \in J$ of order 2, because the restriction of M to K is the sum of the three non-trivial one-dimensional submodules of M.

By considering the structure of V as an A_4-module, we see that V is tensor indecomposable.

First assume that $r | q$. We view V as a module for $\mathrm{SL}(2, q)$. By Steinberg's tensor product theorem and the fact that V is tensor indecomposable, we see that V is a Frobenius twist of a module $L(d)$, where $L(d)$ can be identified with the space of homogenous polynomials in two variables of degree d for $0 \leq d < r$. So $\dim V = d + 1$. Since the central involution in $\mathrm{SL}(2, q)$ acts trivially, d is even. It is easy to compute that the character value of an involution in $\mathrm{PSL}(2, q)$ on $L(d)$ lies in $\{-1, 0, 1\}$. However, we know that $\chi(x) = -\dim V/3$ for at least one involution x, namely one lying in K. Therefore $\chi(x) \in \{-1, 0, 1\}$ implies that $d = 2$, V is 3-dimensional and $\chi(x) = -1$.

Now suppose that r does not divide q. The irreducible modular representations of H are well known [7], and indeed they are all reductions of characteristic zero representations. It follows that $\chi(x) = -\dim V/3$ if and only if $\dim V = 3$. Since the smallest non-trivial irreducible representation of $\mathrm{PSL}(2, q)$ has dimension $(q - 1)/2$, it follows that $q = 5$ or 7. The smallest non-trivial irreducible representation of $\mathrm{PGL}(2, q)$ is $q - 1$, whence $H = \mathrm{PSL}(2, q)$. $\square$

Remark. If $H = \mathrm{PSL}(2, q)$ and V is an irreducible module of dimension 3, then V satisfies the hypotheses of the previous lemma. If $G = \mathrm{PGL}(2, q)$ and $r | q$, then each irreducible 3-dimensional module for $\mathrm{PSL}(2, q)$ in characteristic r has two extensions to $\mathrm{PGL}(2, q)$, and exactly one of those extensions will satisfy the hypotheses of the previous lemma (because an involution outside H must have trace -1).

Corollary 4.5. *Let $H = \mathrm{PSL}(2, q)$ with q odd and $q > 4$. Let R be a finite abelian group on which H acts. Suppose there is a subgroup J of H isomorphic to A_4 whose Klein four subgroup K acts fixed point freely on the non-identity elements of R. If $a \in R$ is non-trivial, then K has a regular orbit on Ha.*

Proof. Since K acts fixed point freely on the non-identity elements of R, R has odd order. There is no harm in assuming that R is generated as a $\mathbb{Z}H$-module by a. We can also pass to a quotient and assume that R is an irreducible H-module. Let $E = \mathrm{End}_H(R)$. Thus, E is a field of characteristic $r > 2$, and we may view R as an absolutely irreducible EH-module.

By Lemma 4.4, R is 3-dimensional. Let L be the stabilizer of a in K. Since K acts fixed point freely, $L \neq K$. If $L = 1$, the result follows. So we may assume that $|L| = 2$. Let $1 \neq x \in L$. By part (2) of Lemma 4.4, x has a 1-dimensional fixed space on R. This space must be the span of a since L stabilizes a. So the stabilizer of the line W generated by a contains $C_H(x)$. The subalgebra $A(x)$ of $\mathrm{Mat}_2(\mathbb{F}_q)$ which is generated over $\mathbb{F}_q$ by an inverse image of x in $\mathrm{SL}(2, q)$ is commutative and semi-simple of dimension 2 over $\mathbb{F}_q$. Each inverse image in $\mathrm{SL}(2, q)$ of an element of $C_H(x)$ must conjugate $A(x)$ back to itself. By considering the possible actions of such elements on $A(x)$, one sees that $C_H(x)$ is the normalizer $N_H(T)$ of the maximal torus T in H which contains x, and $|N_H(T)| = q \pm 1$.

If r divides q, then (up to a Frobenius twist which does not affect the result) R is the representation of H which results from the action of $\mathrm{SL}(2, q)$ on quadratic polynomials, and $x \in H$ lifts to an element $\tilde{x} \in \mathrm{SL}(2, q)$ having eigenvalues $\pm\sqrt{-1}$.

The representation R of H over E is self-dual, so there is a non-degenerate H-invariant quadratic form on R. We can decompose R into the direct sum of the eigenspaces of x, and eigenspaces with different eigenvalues are orthogonal and stabilized by the action of H. In particular, W and its orthogonal complement are non-degenerate for the quadratic form. The stabilizer in H of the line W through a leaves invariant the orthogonal complement of W. Since x acts as -1 on this complement, we see that the stabilizer of the line containing a is precisely $C_H(x) = N_H(T)$. By considering the cases in which T is split or not split, and using the above description of the three dimensional representation R, one sees that T is the stabilizer of a, where T has index 2 in $C_H(x) = N_H(T)$. Note that $Ha \cap W = \{\pm a\}$ (since they are the only two vectors in W with the same norm with respect to the H-invariant quadratic form). Since every non-trivial element of K is a conjugate of x by an element of J, it follows that any non-trivial element of K fixes exactly 2 points in Ha. Therefore, as long as $|Ha| = [H : T] \geq q(q - 1) > 6$, there will be $b \in Ha$ not fixed by any non-trivial element of K, as required.

We now suppose that r does not divide q. So $q = 5$ or 7 by Lemma 4.4. If $q = 5$, then $\mathrm{PSL}(2, 5) \cong A_5$. All irreducible representations of A_5 are self

dual (in any characteristic) and so precisely the same argument as above applies.

Finally, assume that $q = 7$. Note that $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$ and that $S := N_H(T)$ is a Sylow 2-subgroup of H (of order 8). We claim that S is precisely the stabilizer of W. Since S is a Borel subgroup of H (considered as $\mathrm{PSL}(3,2)$), the only proper overgroups of S are the two parabolic subgroups containing S each isomorphic to S_4. If S_4 preserves W, then its derived subgroup A_4 acts trivially on W, a contradiction to K having no fixed points. So S is the stabilizer of W and contains the stabilizer of a. Let S^h be the opposite Borel subgroup to S, so that S^h is a conjugate of S. We have $K \leq C_H(x) = S$. Thus, $K \cap S^h \leq S \cap S^h = 1$ and so K is disjoint from some stabilizer on the set Ha, whence K has a regular orbit on Ha.   □

Corollary 4.6. *Let G be a non-solvable* O*-group. Let $R = O(G)$. Then:*
  (1) *R is nilpotent.*
  (2) *G/R is either $\mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$, with q odd and $q > 4$.*
  (3) *Every chief factor $X = H/N$ of G for which H is contained in R has the following properties. The action of R on X is trivial, and X is an irreducible 3-dimensional G/R-module (over the endomorphism ring of X as G/R-module) satisfying the conditions on V in Lemma 4.4. There are no fixed points for the action of K on X.*
  (4) *If $q > 7$ or $G/R = \mathrm{PGL}(2,q)$, then R is an r-group where $r|q$.*

Proof. By Theorem 2.6, a Sylow 2-subgroup of G/R is not cyclic because G/R is not solvable. Now we apply Lemma 4.1 to conclude that $Z(G/R)$ is trivial because G/R is not solvable. Hence G/R satisfies the hypotheses of Lemma 4.2. We may therefore apply Lemma 4.3 to G/R. It is impossible that G/R is isomorphic to A_4 or S_4 since G is not solvable. Hence Lemma 4.3 shows $G/R \cong \mathrm{PSL}(2,q)$ or $\mathrm{PGL}(2,q)$ with q odd and $q > 4$. The proves part (2) of Corollary 4.6.

We now focus on proving part (1) of the corollary. By Lemma 4.2 applied to G/R, there is an A_4 subgroup J of G/R. Since R is normal of odd order, there is an elementary abelian subgroup K of G of order 4 such that KR/R is contained in J. By case (2) of Theorem 2.6, K acts fixed point freely on R. Since G/R has trivial center, the center of G is contained in R; but no non-trivial element of R is fixed by K. Hence G has trivial center, so by applying part (1) of Lemma 4.2 to G we conclude that $M := [R,R]$ is nilpotent. If M is trivial then R is abelian and hence (1) of the corollary holds. Therefore we now assume M is non-trivial, so that $Z(M)$ is non-trivial because M is nilpotent.

Since $Z(M)$ is a non-trivial normal subgroup of G, there exists a minimal non-trivial normal subgroup A of G contained in $Z(M)$. Then G/A is an O-group by Lemma 3.1. To prove part (1) of the corollary, we may assume by induction that R/A is nilpotent. Since M centralizes A, the action of R on A factors through $R/[R,R]$, so R acts on A as an abelian group. If R centralizes A, then we see that R is nilpotent by considering the ascending central series

of R together with the fact that R/A is nilpotent. Thus to prove that (1) holds, it will suffice to derive a contradiction from the assumption that R acts non-trivially on A.

View A as G-module over the field E, the G-endomorphism ring of A. So A is an absolutely irreducible $E[G]$-module with K acting fixed point freely on A. We know that R acts as abelian group on A, and we are supposing this action is non-trivial. Let ℓ be the characteristic of E. The Sylow ℓ-subgroup of $R/[R,R]$ fixes a non-trivial $E[G]$-submodule of A. So since A is absolutely irreducible as an $E[G]$-module, it follows that the action of $R/[R,R]$ on A factors through the maximal prime-to-ℓ quotient of $R/[R,R]$. In particular, this action is semi-simple.

Let $V = A \otimes_E k$ where k is an algebraic closure of E. Then V is an irreducible kG-module. Since K acts fixed point freely on R, the $E[K]$-module A contains no non-trivial K-invariants, so the same is true for the $k[K]$-module V. Hence K acts fixed point freely on V, and we have shown that R acts semi-simply as a non-trivial abelian group. So V is the direct sum of R-eigenspaces on V and G permutes these eigenspaces transitively. Since the action of R is non-trivial, there must be an eigenspace associated to a non-trivial character λ of the abelian group $R^{\#} := \mathrm{Hom}(R, k^{\times})$. (Note that in fact, R has no fixed points on V, since that would be an invariant subspace). Consider the action of G on $R^{\#}$. Of course, $R \leq G$ acts trivially on this group and so we may view $\mathrm{PSL}(2,q) \leq G/R$ acting on $R^{\#}$. We have assumed that K acts fixed point freely on the non-trivial element of R. Since R is solvable of order prime to $|K|$, the action of K on the non-trivial elements of $R^{\#}$ is also fixed point free. By Corollary 4.5, K has a regular orbit on $\mathrm{PSL}(2,q)\lambda$ and so on the R-eigenspaces on V. Thus V contains a free $k[K]$-submodule, and so K has fixed points on V which is a contradiction. This shows that R centralizes A and so R is nilpotent and we have proved part (1) of the corollary.

Let $X = H/N$ be a chief factor of G for which H is contained in R. Then R acts trivially on X, since otherwise $[H,R]N$ would be a normal subgroup of G properly between N and H. Thus X is a G/R-module which must be irreducible. We know that $H \leq R$, K acts fixed point freely on R, R is nilpotent and that H is normal in G. It follows that X can have no fixed points under the action of K, since these would lift to fixed points for K acting on H. Now the hypotheses of Lemma 4.4 are satisfied for the G/R-module $V = X$ when we let F be the G/R-endomorphism ring of X. The remaining assertions (3) and (4) now follow by Lemma 4.4. $\qquad\square$

Using the above results, we can now prove Theorem 2.7, completing the classification of O-groups for the prime 2.

Proof of Theorem 2.7. Let G be as in the theorem. Then $[R,R]$ is nilpotent by Lemmas 4.1 and 4.2, and these lemmas also show that $G = RP$ if G has no subgroup isomorphic to A_4. Every elementary abelian subgroup of

order 4 acts fixed point freely on the non-trivial elements of R by case (2) of Theorem 2.6.

For the remainder of the proof, we assume that G has a subgroup isomorphic to A_4, and we will show that either (2a), (2b), or (2c) of the theorem holds. Since G is an O-group, so is G/R, by Lemma 3.1. Lemma 4.3 shows G/R is one of $A_4, S_4, \mathrm{PSL}(2,q)$, or $\mathrm{PGL}(2,q)$ with $q > 4$ and q odd. For the last two of those groups, case (2c) of the theorem holds by Corollary 4.6. So we now assume that $G/R \cong A_4$ or S_4, and show that (2a) or (2b) respectively holds.

We now show that G has a complement to R of the form $N_G(K)$ for some Klein four subgroup K. First, since G/R contains a normal elementary abelian subgroup of order 4, and since the order of R is odd, Schur-Zassenhaus implies that G contains an elementary abelian subgroup K of order 4 that is normal modulo R. It acts fixed point freely on the non-identity elements of R. If $g \in G$, then $RK^{g^{-1}} = RK$ by normality modulo R, and so K and $K^{g^{-1}}$ are Sylow 2-subgroups of the group RK. By Sylow's theorem, $K^{g^{-1}x} = K$ for some $x \in R$. Hence $K = K^{x^{-1}g}$ and so $x^{-1}g \in N_G(K)$. Thus $g = x(x^{-1}g) \in RN_G(K)$, proving $G = RN_G(K)$. So to prove that $N_G(K)$ is a complement to R in G, it suffices to show that if $y \in N_R(K) = N_G(K) \cap R$ then y is trivial. Suppose y is not trivial. Then y and K must generate a cyclic-by-2 O-group $K\langle r \rangle$ which is not a 2-group. This forces $K\langle r \rangle$ to be isomorphic to A_4, so $y \in R$ has order 3 and acts as a cyclic permutation of the non-trivial elements of K. By $G = RN_G(K)$ and the fact that G/R contains a subgroup isomorphic to A_4, we can find an element $s \in N_G(K)$ whose image in G/R has order 3 and whose action on K is the same as that of y. Then sy^{-1} is an element of $C_G(K)$ with image of order 3 in G/R, and this is impossible since $C_G(K) = K$ by case (2) of Theorem 2.6. This contradiction shows that in fact $N_R(K) = N_G(K) \cap R$ is trivial, so that $N_G(K)$ is a complement to R, proving the claim. Here this complement is isomorphic to A_4 or S_4 respectively, by the assumption on G/R.

Consider any $N_G(K)$-invariant section $X = H/N$ of R that is irreducible as an $N_G(K)$-module. Then X has the properties listed in part (3) of Corollary 4.6 as a module for G/R, where $G/R \cong A_4$ or S_4. It is an elementary exercise to show that A_4 and S_4 have precisely one irreducible module over $\mathbb{Z}/r$ in which every elementary abelian subgroup of order 4 acts without fixed points. It has order r^3 and has the properties stated in parts (2a) and (2b) of Theorem 2.7. This completes the proof. $\qquad\square$

References

[1] J. Alperin, R. Brauer and D. Gorenstein, Finite simple groups of 2-rank two. Scripta Math. **29** (1973), 191–214.

[2] M. Aschbacher, Finite Group Theory. Cambridge University Press, Cambridge, 1986.

[3] M. Astrand. Lifting problems and their independence of the coefficient field. Ph.D. thesis, University of Pennsylvania, 2015.

[4] S. F. Bauman, The Klein group as an automorphism group without fixed point. Pacific J. Math. **18** (1966), 9–13.

[5] I. Bouw, S. Wewers. The local lifting problem for dihedral groups. Duke Math. J. **134** (2006), 421–452.

[6] L. Brewis and S. Wewers, Artin characters, Hurwitz trees and the lifting problem. Math. Ann. **345** (2009), 711–730.

[7] R. Burkhardt, Die Zerlegungsmatrizen der Gruppen $PSL(2, p^f)$. J. Algebra **40** (1976), 75–96.

[8] T. Chinburg, R. Guralnick and D. Harbater, Oort groups and lifting problems. Compositio Math., **114** (2008), 849–866.

[9] T. Chinburg, R. Guralnick and D. Harbater, The local lifting problem for actions of finite groups on curves. Annales scientifiques de l'ENS, **44** (2011), 537–605.

[10] L. Dornhoff, Group representation theory. Part B: Modular representation theory. Pure and Applied Mathematics, vol. 7. Marcel Dekker, Inc., New York, 1972.

[11] D. Gorenstein, Finite Groups, 2nd Edition. Chelsea Publishing, New York, 1998.

[12] D. Gorenstein and R. Lyons, The local structure of finite groups of characteristic 2 type, Mem. Amer. Math. Soc. 42 (1983), no. 276,

[13] D. Gorenstein, R. Lyons and R. Solomon, The Classification of Finite Simple Groups. Mathematics Surveys and Monographs Volume 40, Number 3, Amer. Math. Soc., Providence, RI, 1998.

[14] D. Gorenstein and J. Walter, The characterization of finite groups with dihedral Sylow 2-subgroups. I, II, III Journal of Algebra **2** (1965), 85–151, 218–270, 354–393.

[15] B. Green and M. Matignon, Liftings of Galois covers of smooth curves. Compositio Math., **113** (1998), 237–272.

[16] A. Grothendieck. "Revêtements étales et groupe fondamental" (SGA 1). Lecture Notes in Mathematics, vol. 224, Springer-Verlag, 1971.

[17] B. Huppert, Endliche Gruppen I. Springer-Verlag, Berlin, 1967.

[18] A. Obus. A generalization of the Oort Conjecture. 2015 manuscript. Available at arXiv:1502.07623.

[19] A. Obus. The local lifting problem for A_4. 2016 manuscript, to appear in Algebra and Number Theory. Available at arXiv:1602.01596.

[20] A. Obus and S. Wewers. Cyclic extensions and the local lifting problem. Ann. of Math., (2) **180** (2014), no. 1, 233–284.

[21] F. Oort, Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero. Proc. Symp. Pure Math., vol. 46, 1987.

[22] F. Oort, T. Sekiguchi, N. Suwa. On the deformation of Artin-Schreier to Kummer. Ann. Sci. École Norm. Sup. **22** (1989), 345–375.

[23] G. Pagot. Relèvement en caractéristique zéro d'actions de groupes abéliens de type $(p, \ldots, p)$. Ph.D. thesis, Université Bordeaux 1, 2002.

[24] F. Pop, The Oort conjecture on lifting covers of curves. Ann. of Math. (2) **180** (2014), 285–322.

[25] T.A. Springer and R. Steinberg, Conjugacy classes. In: Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics, vol. 131, Springer, Berlin, 1970, pp. 167–266.

[26] R. Steinberg, Endomorphisms of linear algebraic groups. Memoirs of the American Mathematical Society, No. 80, American Mathematical Society, Providence, R.I., 1968.

[27] M. Suzuki, Group theory. II., Grundlehren der Mathematischen Wissenschaften 248, Springer–Verlag, New York, 1986.

[28] Y. Wang and Z. Chen, Solubility of finite groups admitting a coprime order operator group. Boll. Un. Mat. Ital. A (7) **7** (1993), 325–331.

Department of Mathematics, University of Pennsylvania, Philadelphia, PA 19104-6395, USA
  E-mail address: `ted@math.upenn.edu`

Department of Mathematics, University of Southern California, Los Angeles, CA 90089-2532, USA
  E-mail address: `guralnic@usc.edu`

Department of Mathematics, University of Pennsylvania, Philadelphia PA 19104-6395, USA
  E-mail address: `harbater@math.upenn.edu`