ON THE RELATIONAL COMPLEXITY OF A FINITE PERMUTATION GROUP

GREGORY CHERLIN

ABSTRACT. The relational complexity $\rho(X,G)$ of a finite permutation group is the least k for which the group can be viewed as an automorphism group acting naturally on a homogeneous relational system whose relations are k-ary (an explicit permutation group theoretic version of this definition is also given). In the context of primitive permutation groups, the natural questions are (a) rough estimates, or (preferably) precise values for ρ in natural cases; (b) a rough determination of the primitive permutation groups with ρ either very small (bounded), or very large (much larger than the logarithm of the degree). The rough version of (a) is relevant to (b). Our main result is an explicit characterization of the binary ($\rho = 2$) primitive affine permutation groups. We also compute the precise relational complexity of Alt_n acting on k-sets, correcting [5, Example 5].

INTRODUCTION

The Notion of Relational Complexity. The relational complexity of a finite permutation group was introduced in [6] and reviewed in [5], under a different name ("arity"), where the following conjecture regarding the classification of primitive binary permutation groups ($\rho = 2$) was given.

Conjecture 1. *A finite primitive binary permutation group (X,G) must be one of the following.*

- *The symmetric group Sym_n acting naturally on n elements.*
- *A cyclic group of prime order acting regularly on itself.*
- *An affine orthogonal group $V{\cdot}O(V)$ with V a vector space over a finite field equipped with an anisotropic quadratic form, acting on itself by translation, with complement the full orthogonal group $O(V)$.*

We will prove this conjecture for the case of affine groups. Combining this result with more recent work of Joshua Wiscons [19], the conjecture reduces to the almost simple case; that is, if there are finite primitive binary permutation groups not listed above, then there must be at least one such with a nonabelian simple socle.

We will also compute the relational complexity of the alternating group acting on k-sets precisely, revisiting and correcting [5, Example 5]. This is a particularly interesting example at the opposite end of the spectrum, that is, with very high relational complexity.

Date: June, 2015.

Key words and phrases. Permutation group, primitive, affine, binary, relational complexity, simple group, orthogonal group, homogeneity, finite model theory.

It is included here to provide a simple illustration of the precise meaning of the concept of relational complexity in a nontrivial context.

In structure theoretic terms, the relational complexity $\rho(X, G)$ of the permutation group (X, G) may be defined as the least k for which (X, G) can be viewed as $(\hat{X}, \mathrm{Aut}(\hat{X}))$ with $\hat{X}$ a homogeneous structure whose relations are k-ary. In more direct permutation group theoretic terms, the relational complexity may be defined in terms of the orbits of G on n-tuples from X (n varies) as the least k such that for all $\mathbf{a}, \mathbf{b} \in X^n$ we have

$$\mathbf{a} \sim_k \mathbf{b} \iff \mathbf{a} \sim \mathbf{b}$$

where on the left, $\sim_k$ means that any corresponding k-tuples from $\mathbf{a}$ and $\mathbf{b}$ lie in the same G-orbit, and on the right, $\sim$ means that $\mathbf{a}$ and $\mathbf{b}$ lie in the same G-orbit.

If a permutation group has at least one nontrivial orbit $\mathcal{O}$, then its relational complexity must be at least 2, since a pair of the form (a, a) with $a \in \mathcal{O}$ is not conjugate under the action to a pair of distinct elements of $\mathcal{O}$; in other words, equality is a binary relation. So with our conventions, in all nontrivial cases the minimal value of the relational complexity is 2; and then we may restrict our attention to n-tuples with distinct entries. In particular, the relational complexity is at most the degree d; or actually (if $d \geq 3$), at most $d-1$, since the action of a group element is uniquely determined once we know the action on $d-1$ elements. This extreme is represented by the alternating group Alt_d acting naturally.

An instructive and well known example to bear in mind is the Petersen graph on 10 points: the language of graphs is binary, but the relational complexity of the graph (i.e., of the automorphism group, with its action on the graph) is 3: there are triples of independent sets which are not conjugate under the isomorphism group. If one adds in an appropriate ternary relation, the structure becomes homogeneous; and if one wants to recognize the Petersen graph as encoding pairs of points from a 5 element set, then one will normally exploit such a ternary relation.

Another, possibly more typical, example is given by the group $\mathrm{GL}(V)$ acting on a vector space V over a finite field. Here the relational complexity is $d+1$, where d is the dimension, unless the base field has order 2, in which case it drops to d. The relevant relations are simply the relations of linear dependence.

There are three problems which finite permutation group theorists should be well equipped to take on, in the primitive case.

- *Natural Actions:* Calculate precisely the relational complexity of natural primitive actions of almost simple groups.
- *Low End:* For each k, determine the structure of a typical primitive permutation group of relational complexity at most k.
- *High End:* For primitive groups of degree n, for $k >> \log n$ and n large, determine the primitive permutation groups of relational complexity k.

We note that rough estimates of the relational complexity of natural actions of almost simple groups should be easy to come by (and adequate for any purposes relevant to the other two questions), but precise values are likely to exhibit some interestingly erratic behavior. The precise analysis of the relational complexity of wreath products is bound to

be difficult: the precise relational complexity of the full wreath product $\mathrm{Sym}_n \wr \mathrm{Sym}_k$ in its natural product action was computed precisely by Saracino in a series of three remarkable papers [16], with a very subtle result.

Behind these questions lurks a more fundamental but intrinsically vague question, namely the actual *meaning* of relational complexity as an invariant, from the point of view of finite permutation groups. In the case of the general linear group acting naturally it is close to the dimension, but it seems more natural to view it as a measure of computational complexity—one that does not ask about the complexity of the representation of group elements, but rather the complexity of certain natural questions about the action. We will not attempt to formalize this more precisely.

Statement of Results. Our main result is the classification of the primitive affine binary permutation groups, where by "primitive affine" we mean "primitive with abelian socle," and by "binary" we mean "having relational complexity at most 2" (hence in all cases of interest, equal to 2). This classification may be stated as follows.

Theorem 1. *Let (A, AG) be a primitive affine binary permutation group. Then either $|G| \leq 2$ and $|A| \cong C_p$ is cyclic of prime order, or else A can be given the structure of a two-dimensional vector space over a finite field $\mathbb{F}_q$ with $G = O_2^-(q)$, where A acts by translation and G acts naturally.*

As we mentioned at the outset, Conjecture 1 can be reduced to the almost simple case by combining Theorem 1 with the recent reduction theorem of [19]. There is a highly developed theory of such groups (beginning with the study of maximal subgroups of simple groups), which is likely to give a great deal of relevant information, though whether that case can be treated in full remains to be seen.

We also revisit the computation of the relational complexity of Alt_n acting on k-sets, where (without loss of generality) $2k \leq n$. This corrects the account sketched in [5, Example 5], where an exceptional case was overlooked. The relational complexity of this action is remarkably large: typically, the complexity is $n - 3$.

Theorem 2. *For $2k \leq n$, the relational complexity $\rho_A(n, k)$ of Alt_n acting on k-sets is $n - 3$, apart from the following cases, where the values are as shown.*

Case	*Value*
$k = 1$	$\rho_A(n, k) = n - 1$
$k = 2$	$\rho_A(n, k) = \max(n - 2, 3)$
$k \geq 3$, $n = 2k + 2$	$\rho_A(n, k) = n - 2$

For $2k < n$ the action is primitive, but we include the imprimitive case $2k = n$ as the analysis is the same. The "bump" at $n = 2k + 2$ was missed in [5]. Our proof explains this bump in graph theoretic terms, but one could wish for a more intrinsic interpretation.

For the proof of Theorem 1 we rely on the explicit classification of the finite simple groups, as well as their covering groups and automorphism groups. We find some very strong properties of primitive affine binary groups, which have no obvious analogs for larger relational complexity—but we would imagine that there should be qualitatively similar results for any fixed relational complexity.

The socle of a primitive affine permutation group is an elementary abelian p-group for some prime p, which we will call the *characteristic.* We treat the cases of characteristic 2 and odd characteristic separately.

We first show that in characteristic p the group G has no element of order

$$\begin{cases} 4 & \text{if } p = 2 \\ p & \text{if } p > 2 \end{cases}$$

So in characteristic 2 the Sylow 2-subgroups are elementary abelian, and one knows a great deal about G from the beginning. As a result, the characteristic 2 analysis goes quickly. The odd characteristic analysis wanders about.

In odd characteristic, we look mainly at the structure of the generalized Fitting subgroup $F^*(G) = F(G)E(G)$, and we also consider the $2'$-core OG of G, which is the largest normal subgroup of G of odd order. Our plan is to show

- $EG = 1$;
- OG is cyclic;
- F_2G is cyclic or dihedral.

Then we can easily recognize our standard examples (where if $|G| > 2$, then G is dihedral).

The analysis is essentially inductive: one takes a counterexample (A, AG) with A minimal. One should be a little careful about the nature of the induction: in general *any* structure with transitive automorphism group is a quotient of a binary structure (namely, the structure given by the regular action of the group on itself). But in several cases (A, AG) has proper sections of the form $(V, VN_G(V))$ which are again primitive and binary.

Our proof of Theorem 2 in §5 depends on the computation of the relational complexity for the symmetric group on k-sets, given in [6]. Apart from this, the analysis proceeds from first principles.

Notation. We denote primitive affine permutation groups by (A, AG), with A an abelian group and G the stabilizer of the point 0. (For more detail, see §1.)

A *section* of (A, AG) will mean the action on a subgroup $V \leq A$ induced by $V \cdot N_G(V)$, in other words $(V, VN_G(V)/C_G(V))$. We will write $(V, VN_G(V))$, with the understanding that the kernel of the action should be factored out. Observe also our use of N_G and C_G for the setwise and pointwise stabilizers.

If (X, G) is any permutation group we may consider the corresponding action of G on X^n (which one may interpret either as the full cartesian power, or as the set of n-tuples with distinct entries, according to one's taste). If $\mathbf{a}, \mathbf{b} \in X^n$ are in the same G-orbit, we say they are *conjugate* (or G-conjugate, if necessary) and we write

$$\mathbf{a} \sim \mathbf{b}$$

We repeat the definition of relational complexity in a more explicit form.

Definition. Let (X, G) be a permutation group and (X^n, G) the corresponding action on n-tuples.

1. If $\mathbf{a} \in X^n$ for some n and $I \subseteq \{1, \ldots, n\}$, then $\mathbf{a} \restriction I$ denotes the subsequence of $\mathbf{a}$ obtained by restriction to the indices in I. This is an element of X^I.

2. For $k \leq n$, and $\mathbf{a}, \mathbf{b} \in X^n$, we say that $\mathbf{a}$ and $\mathbf{b}$ are *k-equivalent,* and we write

$$\mathbf{a} \sim_k \mathbf{b}$$

if we have

$$\mathbf{a} \restriction I \sim_k \mathbf{b} \restriction I$$

for all k-subsets I of $\{1, \ldots, n\}$.

3. The *relational complexity* of the action of the group G on the set X is the least k for which the following holds.

> If $\mathbf{a}, \mathbf{b}$ are arbitrary n-tuples of distinct elements of X, with $k \leq n \leq |X|$,
> then $\mathbf{a} \sim_k \mathbf{b} \iff \mathbf{a} \sim \mathbf{b}$.

We write $m_2(G)$ for the maximal rank of an elementary abelian 2-subgroup and $n_2(G)$ for the maximal rank of a normal elementary abelian 2-subgroup. We use the notation $G^\#$ for $G \setminus (1)$.

We rely largely on [7, 18, 12] for necessary information (and a good deal of relevant notation) relating to finite groups. Not cited often, but generally helpful, is [4], and the GAP programming language, which has the Atlas available as a library. Our first explorations of the subject, many years ago, used Cayley and Charlie Sims' library of primitive permutation groups of degree at most 50. Already in that context the action of Alt_n on k-sets stood out at the "high end."

Two useful general references are [8], for the general theory of permutation groups and the O'Nan-Scott-Aschbacher classification of primitive permutation groups (the latter becomes more relevant in [19]), and [3], for the relationship between the group theoretic and model theoretic point of view, and, in particular, Fraïssé's theory, which is closely connected with the notion of relational complexity.

I would also like to note my indebtedness to the much regretted Chat Ho (1946-2005) for stimulating discussions of finite group theory.

1. Binary Affine Groups: General Principles

A primitive affine permutation group is a pair (A, AG) where AG is a primitive group with elementary abelian socle A. Then the set acted on may be identified with the socle A, and $AG = A \rtimes G$ is a semidirect product with G the stabilizer of the point $0 \in A$. Here A acts on itself by translation, and G acts on A by automorphisms, and its action is irreducible.

We generally suppose, tacitly, that the group A is finite, but we make an exception in Lemma 1.1 below. That lemma makes sense in the infinite case as well, and at that level of generality involves a significantly wider variety of examples than the finite case, with no limitation on the dimension.

Taking A to be finite, it will be an elementary abelian p-group for some p, called the *characteristic.*

In the affine case, we may interpret the relation $\mathbf{a} \sim_2 \mathbf{b}$ more explicitly as follows.

$$\mathbf{a} \sim_2 \mathbf{b} \text{ under the affine group } AG \text{ iff}$$
$$a_i - a_j \sim b_i - b_j \text{ under } G, \text{ for all pairs } i, j.$$

This fact will be used throughout.

In this section, we take up five points of general use in analyzing primitive affine binary groups. After that, the analysis will split apart into two cases, according as the characteristic is even or odd.

The points to be established are the following.

- Anisotropic orthogonal groups give rise to binary affine groups.
- Binary affine groups contain many involutions (Corollaries 1.4 and 1.5, Lemmas 1.6 and 1.7).
- Binary 1-dimensional semilinear groups are as conjectured.
- There is no p-torsion in odd characteristic p, and no element of order 4 if $p = 2$.
- Irreducible submodules for normal subgroups of G give rise to binary sections of (A, G) (and we have some further variations on this theme).

1.1. **The anisotropic orthogonal case.** Recall that a quadratic form Q is *anisotropic* if there are no nonzero vectors v for which $Q(v) = 0$.

Lemma 1.1. *Let F be a field, V a vector space equipped with an anisotropic quadratic form, and $O(V)$ the corresponding orthogonal group. Then the action of the affine group $VO(V)$ on V is binary.*

Here we may suspend the hypothesis that everything is finite.

Proof. This is in essence Witt's Lemma, with the remark that in the anisotropic case one can work out linear dependence relations from inner products.

In detail, suppose $\mathbf{u} = (u_0, \ldots, u_n)$ and $\mathbf{u}' = (u'_0, ..., u'_n)$ are $2-$equivalent under the action of $VO(V)$. We may suppose that $u_0 = u'_0 = 0$. We claim that the sequences are $O(V)$-conjugate.

By 2-equivalence, the function f from $\mathbf{u}$ to $\mathbf{u}'$ taking u_i to u'_i is an isometry. Let W, W' be the span of $\mathbf{u}$ and $\mathbf{u}'$ respectively in V. We claim that f extends to an isometry $\hat{f}$ from W to W'; then Witt's Lemma applies.

We may suppose that some initial segment $(u_1, \ldots, u_m)$ of $\mathbf{u}$ is a basis of W. Then the restriction of f to $u_1, \ldots, u_m$ extends to a linear isometry $\tilde{f}$ from W to W' ($\tilde{f}$ is 1-1 because the form is anisotropic). So it will suffice to check that $\tilde{f}$ extends f.

Suppose $m < i \leq n$ and $u_i = \sum_{j=1}^m a_j u_j$. As $\mathbf{u} \sim_2 \mathbf{u}'$,the quadratic form Q satisfies

$$Q\left(u'_i - \sum_{j=1}^m a_j u'_j\right) = Q\left(u_i - \sum_{j=1}^m a_j u_j\right) = 0$$

and hence $u'_i = \sum_{j=1}^m a_j u'_j = \tilde{f}(u_i)$. □

At the finite level, this gives us examples in 1 and 2 dimensions.

The 1-dimensional case gives a group $A\langle\pm 1\rangle$ which is primitive only if A is 1-dimensional over $\mathbb{F}_p$ (AG is a dihedral group).

The 2-dimensional case gives a family of examples $VO_2^-(q)$ where V is 2-dimensional over a finite field $\mathbb{F}_q$. This can be described more explicitly as follows. Identify V with the quadratic extension $\mathbb{F}_{q^2}$ of the base field. Then $O_2^-(q)$ can be thought of as $K\langle\sigma\rangle$ where $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ and K is the kernel of the norm map from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. Since in this case $G = K\langle\sigma\rangle$ is dihedral, this sets up the target for our subsequent analysis.

We also have the binary affine group which consists of a cyclic group A of prime order acting on itself by translation (i.e., $G = 1$). We will group the various cases as follows.

- 1-dimensional (over $\mathbb{F}_p$): C_p cyclic and D_{2p} dihedral, acting naturally on C_p, with p odd;
- 2-dimensional (over some $\mathbb{F}_q$): $VO_2^-(q)$ acting naturally on V.

Definition 1.2. Affine anistropic permutation groups in dimension 2 ($VO_2^-(q)$ acting naturally on V, with $\dim V = 2$) will be called groups of *type* AO_2^-.

Permutation groups of either type above (type AO_2^-, or the 1-dimensional groups C_p, D_{2p} acting on C_p) will be referred to as *standard type*.

The dividing line between dimensions 1 and 2 here, in group theoretic terms, is simply: $|G| \leq 2$, or $|G| > 2$. Thus we will easily distinguish the two targets of our analysis.

We will give a weak converse to Lemma 1.1 in a moment, providing a useful target for the analysis leading to Theorem 1. Namely, the permutation groups of standard type are 1-dimensional semilinear groups, and we will check at the outset that any primitive binary 1-dimensional semilinear group must be standard. But first we must pay some attention to the role of involutions in binary affine groups.

1.2. **Involutions in binary affine groups.**

Lemma 1.3. *Let (A, AG) be a binary affine permutation group and let $g \in G^{\#}$, $a \in A$. Set $A_0 = C_A(g^2)$. Then there is an involution $t \in G$ such that*

$$x^g = x^t \text{ for } x \in A_0 \cup \{a\}$$

Proof. We proceed by induction on $|A \setminus A_0|$. We may suppose

$$A_0 \neq A \text{ and } a \notin A_0$$

Let $X = A_0 \cup \{a, a^g\}$. Take an ordering $<$ on X for which $a < a^g$. Define $f_1, f_2 : X \to A$ as follows.

$$f_1(x) = \begin{cases} x & \text{if } x \geq x^g \\ -x & \text{if } x < x^g \end{cases} \qquad f_2(x) = \begin{cases} x^{g^{-1}} & \text{if } x \geq x^g \\ -x^g & \text{if } x < x^g \end{cases}$$

We claim that there is $h \in G$ such that

$$f_1(x)^h = f_2(x) \text{ for } x \in X$$

So consider a pair $x_1, x_2 \in X$ and set $u_i = f_1(x_i)$, $u_i' = f_2(x_i)$ for $i = 1, 2$. We claim that (u_1, u_2) and (u_1', u_2') are AG-conjugate.

If either u_1 or u_2 is fixed by g^2, then the pairs (u_1, u_2) and (u_1', u_2') are conjugate by g or g^{-1}. So we need only consider the case in which (x_1, x_2) is the pair (a, a^g), and so

$$(u_1, u_2) = (-a, a^g),\ (u_1', u_2') = (-a^g, a)$$

But these two pairs are conjugate by a translation.

By binarity, we have the desired element $h \in AG$, and as $0 \in X$, we have $h \in G$.

For $x \in X$, x^h must be x^g or $x^{g^{-1}}$, and thus h agrees with g on A_0. Also $a^h = a^g$, and $(a^g)^h = a \neq a^g$. Therefore $A_0 \cup \{a, a^g\} \subseteq C_A(h^2)$ and so by induction there is some involution $t \in G$ whose action agrees with the action of h on $C_A(h^2)$ and, in particular, with the action of g on $C_A(g^2) \cup \{a\}$. □

Corollary 1.4. *Let (A, AG) be a binary affine permutation group. If two distinct elements of A are G-conjugate then they are conjugate by an involution of G.*

Corollary 1.5. *Let (A, AG) be a binary affine permutation group. Then for any $X \subseteq A$, the stabilizer $C_G(X)$ is generated by involutions. In particular, G is generated by involutions.*

Proof. If $g \in G$ and $Y = C_A(g)$, it suffices to show that g is a product of involutions fixing Y. Proceed by induction on $|A \setminus Y|$, applying Lemma 1.3. □

The following variation on the foregoing will be useful in the case of odd characteristic.

Lemma 1.6. *Let (A, AG) be a primitive affine binary permutation group with G nontrivial. Then some element of G inverts A.*

Proof. By Corollary 1.5 the group G contains at least one involution t. Take $b \in A \setminus C_A(t)$ and let $a = [t, b]$. Then $a \in A^\#$ is inverted by t. Let $\mathcal{O}$ be the orbit a^G. We claim that some $g \in G$ satisfies

$$x^g = -x \text{ for } x \in \mathcal{O} \cup \{0\}$$

By binarity, we need to check that for $a_1, a_2 \in \mathcal{O}$, the pairs $(0, a_1)$ and $(0, -a_1)$ are conjugate, and the pairs (a_1, a_2) and $(-a_1, -a_2)$ are conjugate, with respect to the action of AG. In the first case, we just use the fact that a_1 is conjugate to a under G.

In the second case, as a_1 and a_2 are conjugate we have an involution s swapping a_1 and a_2, by Corollary 1.4. Hence $a_2 - a_1$ is conjugate to $a_1 - a_2$ under G, and (a_1, a_2) is conjugate to $(-a_1, -a_2)$ under AG. This gives the desired element $g \in AG$ fixing 0, that is $g \in G$.

By G-irreducibility $\mathcal{O}$ spans A, so our claim follows. □

We have the following further variation on the same theme.

Lemma 1.7. *Let (A, AG) be primitive, affine, and binary. Let $X \subseteq G$ be abelian and nontrivial. Let $\mathcal{O} \subseteq A$ be an X-orbit. Then there is an involution $t \in N_G(\mathcal{O})$ so that*

- *t fixes a point of $\mathcal{O}$*
- *For any $g \in X$, g^t acts on $\mathcal{O}$ like g^{-1}.*

Proof. Fix $u \in \mathcal{O}$. We claim that $(u^g : g \in X)$ is conjugate under G to $(u^{g^{-1}} : g \in X)$. We add the term 0 to both sequences and apply binarity to the action of AG.

So we have to check that all the differences $u^g - 0$ and $u^g - u^h$ with $g, h \in X$ are conjugate to the corresponding differences $u^{g^{-1}} - 0$ and $u^{g^{-1}} - u^{h^{-1}}$. The first case is trivial. On the other hand

$$(u^g - u^h)^{g^{-1}h^{-1}} = (u^{h^{-1}} - u^{g^{-1}})$$

so Lemma 1.6 completes the proof. □

Corollary 1.8. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Then $|ZG| = 2$.*

Proof. By Lemma 1.6 there is an element $z \in ZG$ acting by inversion on A.

Now suppose $g \in ZG$ is arbitrary and apply Lemma 1.7 to each g-orbit. Thus g and g^{-1} have the same action, and $g^2 = 1$. As A is G-irreducible, $ZG = \langle z \rangle$. □

1.3. **1-Dimensional semilinear groups.**

Lemma 1.9. *Let V be a 1-dimensional vector space over a finite field $\mathbb{F}$ of characteristic p, and let G be a subgroup of the product $[\mathbb{F}^\# \cdot \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)]$. If (V, VG) is binary then either G is an elementary abelian 2-group of rank at most 2, or G is of the form $K\langle\sigma\rangle$ where $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ has order 2 and K is the kernel of the norm map from $\mathbb{F}$ to the fixed field of σ.*

Proof. By Corollary 1.5, G is generated by involutions. If G is contained in $\mathbb{F}^\#$ then this forces $G \subseteq \langle \pm 1 \rangle$ and everything is clear.

Suppose

$$G \not\leq \mathbb{F}^\#$$

Then the image of G in $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ must be cyclic of order 2. Let σ generate this image and let K be the kernel of the norm map from $\mathbb{F}$ to the fixed field $\mathbb{F}_0$ of σ. Thus K is the subgroup of $\mathbb{F}^\#$ inverted by σ.

Thus $G = X \cdot \langle t \rangle$ where $X = G \cap \mathbb{F}^\#$, and $t = a\sigma$ is an involution, so $a \in K$. As G is generated by involutions, $X \leq K$.

If $X \leq \langle \pm 1 \rangle$ our claim holds, so suppose $X \not\leq \langle \pm 1 \rangle$. We claim $X = K$. Fix $k \in X \setminus \langle \pm 1 \rangle$. Note that $-1 \in G$ by Lemma 1.6.

Let $c \in K$ be arbitrary and take $u \in \mathbb{F}^\times$ with $u^\sigma = acu$ (Hilbert's Theorem 90). We may check the conjugacy

$$(0, u, (1+k)u) \sim (0, u, (1+k^{-1})u)$$

under VG, by checking the G-conjugacy of corresponding differences of pairs.

So $(u, (1+k)u) \sim (u, (1+k^{-1})u)$ under G. Let $g \in G$ fix u and take ku to $k^{-1}u$. Since $ku \neq k^{-1}u$, $g \neq 1$. Therefore g has the form $c'\sigma$ with $c'\sigma$ fixing u. By the choice of u we find $c' = ac$ and thus $g = ct$. Since $t \in G$ we have $c \in G$.

Thus $X = K$ and $G = K\langle\sigma\rangle$ as claimed. □

This lemma will provide the template for the final recognition of G (with its action).

1.4. **On p-torsion in characteristic p.** If (A, AG) is a primitive affine permutation group (A, AG) and the group A is an elementary abelian p-group, we refer to p as the *characteristic*. The first step in the analysis of the binary case is the following.

Lemma 1.10. *Let (A, AG) be primitive, affine, and binary, of characteristic p.*

(1) *If p is odd then G is a p'-group.*
(2) *If $p = 2$ then G contains no element of order 4.*

Proof.

Ad 1. We suppose $p > 2$ and $g \in G$ has order p. Find $a \in A^{\#}$ so that

$$a^g = a + u,\ u^g = u \neq 0$$

For any fixed $i \in \mathbb{F}_p^{\#}$ the set

$$\mathcal{O}_i = ia + \mathbb{F}_p u$$

is a single orbit under the action of g. So by binarity we arrive at the following contradiction

$$(0, a, 2a) \sim (0, a, 2a + u)$$

Ad 2. We suppose $p = 2$ and $g \in G$ has order 4. Find $u \in A^{\#}$ so that

$$u \notin C_A(g^2), u^g - u \in C_A(g^2)$$

Let $v = u^g - u$ and $w = v^g - v$. Then

$$v^g = v + w \text{ with } w^g = w \neq 0,\ u^{g^2} = u + w, \text{ and } (u+v)^{g^2} = u + v + w$$

By binarity we deduce the contradiction

$$(0, u, v, u + v) \sim (0, u, v, u + v + w)$$

□

In odd characteristic, we will also need to exclude some subgroups containing elements of order 4, but we will return to this later.

1.5. **Irreducible Sections.** Recall that a *section* of the affine permutation group (A, AG) means an action $(V, V[N_G(V)/C_G(V)])$, written by abuse of notation $(V, VN_G(V))$. We will generally work in an inductive setting where all (relevant) proper primitive binary sections are of standard type.

Lemma 1.11. *Let (A, AG) be affine and binary, $H \lhd G$, and $V \leq A$ an irreducible H-submodule. Then the corresponding section $(V, VN_G(V))$ is binary and primitive.*

Proof. As V is H-irreducible, the action is primitive. We must check that it is also binary.

It suffices to check that if $(v_1, \ldots, v_n)$ and $(v_1', \ldots, v_n')$ are sequences from V which are AG-conjugate then they are $VN_G(V)$-conjugate. Translating by V, we may suppose

$$v_1 = v_1' = 0$$

and the sequences are G-conjugate. For $g \in G$, either $V^g = V$ or $V^g \cap V = (0)$, and our claim follows. □

Notation 1.12. If E is an elementary abelian 2-subgroup of G, and the characteristic is odd, then we will denote the eigenspace decomposition of A with respect to E by

$$A = \bigoplus_{\Lambda} A_\lambda$$

Here A_λ is the subgroup of A in which E acts according to the homomorphism $\lambda : E \to \{\pm\}$, that is

$$A_\lambda = \{a \in A \,:\, a^e = a^{\lambda(e)} \text{ (all } e \in E)\}$$

The index set Λ consists of those homomorphisms $\lambda : E \to \{\pm 1\}$ such that the corresponding space A_λ is nontrivial.

Lemma 1.13. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Suppose that $E \lhd G$ is an elementary abelian 2-subgroup, and let*

$$A = \bigoplus_{\Lambda} A_\lambda$$

be the corresponding eigenspace decomposition. Then each section $(A_\lambda, A_\lambda N_G(A_\lambda))$ is binary and primitive.

Proof. For $\lambda \in \Lambda$ and $g \in G$, either $A_\lambda^g = A_\lambda$, or $A_\lambda \cap A_\lambda^g = (0)$. It follows that $(A_\lambda, AN_G(A_\lambda))$ is binary.

Let $V_\lambda \leq A_\lambda$ be $N_G(A_\lambda)$-irreducible. Then

$$A = \sum_{g \in G} V_\lambda^g$$

and hence $A_\lambda = \sum_{g \in N_G(A_\lambda)} V_\lambda^g = V_\lambda$. □

Arguing as in Lemma 1.9 gives two further variations on this theme.

Lemma 1.14. *Let (A, AG) be primitive, affine, and binary, and let $C \leq G$ be cyclic, with $|C| > 2$. Let $V \leq A$ be C-irreducible, and let $\mathbb{F} = C_{\mathrm{End}(V)}(C)$.*

Then $(V, VN_G(V)/C_G(V))$ is of type AO_2^-. That is, $\mathbb{F}$ is a quadratic extension of a field $\mathbb{F}_0$, and G may be identified with $K \operatorname{Gal}(\mathbb{F}/\mathbb{F}_0)$ where K is the kernel of the corresponding norm map, all acting naturally on $\mathbb{F}$.

Proof. Let $\mathcal{O} \subseteq V^\#$ be a C-orbit. By Lemma 1.7 there is some $\sigma \in N_G(\mathcal{O})$ fixing a point of $\mathcal{O}$ and inverting the action of C on $\mathcal{O}$.

Now σ normalizes the image of C in $\mathrm{End}(V)$ and hence acts on the field $\mathbb{F}$ as an involution (since $|C| > 2$). Let $\mathbb{F}_0$ be the fixed field. Note that C is contained in the kernel of the norm.

Let c be inverted by σ and let $v \in V^\#$ be taken so that

$$v^\sigma = cv$$

Let $\mathcal{O}_1$ be the orbit of v under C. By Lemma 1.7 there is $\tau \in N_G(\mathcal{O}_1)$ so that

$$v^{g\tau} = v^{g^{-1}} \text{ for } g \in C$$

Also

$$(v^g)^{c\sigma} = (cv^g)^\sigma = c^{-1}v^{\sigma g^\sigma} = c^{-1}(cv)^{g^{-1}} = v^{g^{-1}}$$

and thus τ acts as $c\sigma$ on $\mathcal{O}_1$ and hence also on V. Thus $\tau\sigma$ acts as c on V. □

We insert an observation on scalars.

Lemma 1.15. *If (A, AG) is affine and binary, $g \in G$, $u \in A$, and $u^g \in \langle u \rangle$, then $u^g = \pm u$.*

Proof. By Corollary 1.4 there is an involution $t \in G$ such that $u^g = u^t$. □

Lemma 1.16. *If (A, AG) is primitive, affine, and binary, in odd characteristic, and $V \leq A$ is 2-dimensional over the prime field $\mathbb{F}_p$, then*

1. *$(V, VN_G(V))$ is binary;*
2. *Either $N_G(V)$ induces an elementary abelian 2-group on V, or $N_G(V)$ induces $O_2^-(p)$ on V.*

Proof. We claim first that for $u, v \in V$ we have

$$u \sim v \text{ under } G \implies u \sim v \text{ under } N_G(V) \tag{1}$$

So fix u, v G-conjugate. We may suppose $u \neq v$. Then by Corollary 1.4 there is an involution $t \in G$ with $u^t = v$. If $\langle u, v \rangle = V$ then $V^t = V$ and we are done. Otherwise, Lemmas 1.15 and 1.6 suffice.

From Claim (1), Conclusion (1) follows easily.

Now let H be $N_G(V)/C_G(V)$, viewed as a subgroup of $\mathrm{GL}(V)$ and let $H_0 = H \cap \mathrm{SL}(V)$. By Corollary 1.5 H is generated by involutions, so $H = H_0\langle t \rangle$ for some involution t. By Lemma 1.10 H_0 contains no element of order p. We claim that H_0 is abelian.

If H_0 is nonabelian then $H_0/\langle \pm I \rangle$ is dihedral and H_0 contains an element of order 4. By Lemma 1.15 the element of order 4 has no eigenvalue in $\mathbb{F}_p$ so $p \equiv -1 \mod 4$. Then H_0 is a subgroup of a group of order $4(p-1)$ conjugate to $N_G(T)$, the normalizer of the diagonal subgroup T. But $H_0 \cap T \leq \langle \pm I \rangle$, again by Lemma 1.15.

Thus H_0 is abelian. If V is H_0-irreducible we arrive immediately at the hypotheses of Lemma 1.9. If V is H_0-reducible then H_0 is an elementary abelian 2-group by Lemma 1.15, hence $H_0 \leq \langle \pm I \rangle$ and H is elementary abelian. □

We also have a useful criterion for an involution to belong to $N_G(V)$, which we will apply repeatedly, to the point that it may be considered our main technical device.

Lemma 1.17 (Main Lemma)**.** *Let (A, AG) be affine and binary. Let $H \lhd G$ and let $V \leq A$ be an irreducible H-submodule.*

Suppose that $t \in G$ is an involution, and that there are elements $h \in H$, $v \in V$ satisfying

$$v^h \neq \pm v$$
$$v^t - v \sim v^{ht} - v^h \text{ under } G$$

Then $V^t = V$.

Proof. Set $(u_1, u_2, u_3, u_4) = (0, v + v^h, v + v^t, v^h + v^t)$. Let $u_4' = v + v^{ht}$. We check that

$$(u_1, u_2, u_3, u_4) \sim (u_1, u_2, u_3, u_4')$$

We have

$$(u_1, u_3, u_4)^t = (u_1, u_3, u_4')$$

Furthermore our hypothesis states that $(u_2, u_4) \sim (u_2, u_4')$. So by binarity we have some $g \in G$ taking one 4-tuple to the other, that is g fixes u_2, u_3 while taking u_4 to u_4'.

Notice that $u_2 \in V^\#$ and hence $V^g = V$. Furthermore

$$u_4 - u_3 = u^h - u \in V^\#$$

and hence $u_4' - u_3 \in V^\#$. But $u_4' - u_3 = u^{ht} - u^t \in V^t$, so $V^t = V$ as claimed. □

We insert a word about the motivation for this lemma. This goes back to a point arising in the classification of the finite homogeneous graphs [10, 17].

Example 1.18. Let Γ_n be the graph with vertex set n^2 and edge relation $E((a_1, a_2), (b_1, b_2))$ defined by

$$a_1 = b_1 \text{ or } a_2 = b_2, \text{ and } (a_1, a_2) \neq (b_1, b_2)$$

(sometimes denoted $K_n \otimes K_n$, or $E(K_{n,n})$). Then the relational complexity of Γ is 4 for $n \geq 4$, and is 2 for $n = 2, 3$.

The relation to our lemma arises from the circumstance that the automorphism groups of these graphs act primitively and are affine for $n \leq 4$. Thinking about what happens when $n = 4$ gives the previous lemma.

In graph theoretic terms, there are two classes of "parallelism" classes of edges in Γ_n. To see that the relational complexity is at least 4 when $n \geq 4$ one exploits this by comparing 4-tuples with two disjoint edges, parallel in one case and not in the other. Lemma 1.17 is saying that the involution t which interchanges the two classes (by swapping coordinates) should not exist, if a suitable element h is also present.

Lemma 1.19. *Let (A, AG) be primitive, affine, and binary. Let $H \lhd G$ and let $V \leq A$ be an irreducible H-submodule. Then the kernel K of the action of H on V is an elementary abelian 2-group.*

Proof. If K is not elementary abelian then on some conjugate V^g of V, some element of K induces an automorphism α of order greater than 2. Fix $v \in V$ so that

$$(v^g)^\alpha \neq \pm v^g$$

By Corollary 1.4 there is an involution $t \in G$ with $v^t = v^g$. Then $V^t = V^g$. Let $\bar{K}$ be the image of K in $\mathrm{Aut}(V \oplus V^t)$. Then $\bar{K}$ acts trivially on V and faithfully on V^t. Thus $\langle K, K^t \rangle$ acts as $\bar{K}^t \times \bar{K}$ on $V \oplus V^t$. Take $h \in H$ inducing the automorphism (α^t, α) of $V \oplus V^t$. Then

$$(v^t - v)^h = (v^t)^\alpha - v^h = v^{\alpha^t t} - v^h = v^{ht} - v^h$$

Thus by Lemma 1.17 we have $V^t = V$ and $\bar{K} = 1$, a contradiction. □

Lemma 1.20. *Let (A, AG) be primitive, affine, and binary. Suppose $H \lhd G$ is abelian of odd order. Then H is cyclic.*

Proof. Let $V \leq A$ be an irreducible H-submodule. By Lemma 1.19 the action of H on V is faithful. So H is cyclic. □

This brings us to the consideration of groups of *symplectic type:* a p-group is said to be of symplectic type if every characteristic abelian subgroup is cyclic.

Corollary 1.21. *Let (A, AG) be primitive, affine, and binary. Then for p odd, $F_p(G)$ is of symplectic type.*

These groups were classified by Philip Hall (cf. [11]).

Fact 1.22. *The symplectic p-groups have the following structure.*

- *For p odd: central products*
$$E * C$$
with E extraspecial of exponent p and C cyclic.
- *For $p = 2$: central products*
$$E * Q$$
with E extraspecial and Q cyclic, dihedral, generalized quaternion, or semidihedral.

Lemma 1.23. *Let (A, AG) be primitive, affine, and binary. Then the $2'$-core OG is cyclic.*

Proof. First we will show

$$O(FG) \text{ is cyclic} \tag{2}$$

If not, then for some odd prime p we have F_pG a central product of the form

$$E * C$$

with E extraspecial of exponent p and nontrivial, and with C cyclic.

Let $X \leq F_pG$ be maximal abelian. By hypothesis $X < F_pG$. Fix $g \in F_pG \setminus X$. Let $V \leq A$ be an irreducible X-submodule.

By maximality the cyclic factor C is contained in X. As A is generated by the conjugates of V, C acts faithfully on V. Let Y be the kernel of the action of X on V. Then

$$X = Y \times C$$

Now $X^g = X$. But

$$[g, Y] = [g, X] \neq 1$$

so $[g, Y] = \Omega_1 C \not\leq Y$, and $Y^g \neq Y$. Therefore $V^g \neq V$ and the action of X on $V \oplus V^g$ contains an elementary abelian p-group of rank 2.

Fix $v \in V^\#$. Let $\hat{Y} = C_{F_pG}(v)$. Then $Y \subseteq \hat{Y}$. But $\hat{Y} \cap C = 1$ so $\hat{Y}$ is abelian. As $X \subseteq \hat{Y}C$ we find $X = \hat{Y}C$ and $\hat{Y} = Y$.

By Corollary 1.4 there is an involution $t \in G$ with $v^t = v^g$. As $Y = C_{F_pG}(v)$ it follows that $Y^t = Y^g \neq Y$ and $X^t = Y^t C = Y^g C = X$. Hence $V^t = V^g$.

Fix $h \in (\Omega_1 C)^\#$. Let $\alpha \in \mathrm{Aut}(V \oplus V^t)$ act as h on V and as h^t on V^t. Then X induces α on $V \oplus V^t$ and hence $v^t - v$ is G-conjugate to $v^{ht} - v^h$. By Lemma 1.17 we find $V^t = V$, a contradiction. This proves (2).

Now let $H = O(FG)$. As H is cyclic, $G/C(H)$ is abelian. By Corollary 1.5, $G/C(H)$ is an elementary abelian 2-group. Therefore $OG \leq C(H)$. As OG is solvable, $C_{OG}(H) \leq H$ and hence $OG = H$ is cyclic. □

The rest of the analysis splits into two cases, according as the characteristic p is even or odd.

2. Primitive Affine Binary Groups in Characteristic 2

Lemma 2.1. *Let (A, AG) be primitive, affine, and binary, in characteristic 2. If the Fitting subgroup FG is nontrivial, then (A, AG) is of standard type.*

Proof. As the characteristic is 2 and the action of G on A is irreducible, $F_2G = 1$. So by Lemma 1.23, FG is cyclic. Fix an odd prime p for which F_pG is nontrivial.

By Lemma 1.10 a Sylow 2-subgroup of G is elementary abelian. We show that the Sylow 2-subgroups are cyclic of order 2.

Suppose that G contains a 4-subgroup E. Then some involution $t \in E$ centralizes F_pG. Let V be an irreducible F_pG-submodule of A. Take $h \in F_pG^\#$ and $v \in V$ with $v^h \neq v$. As h and t commute Lemma 1.17 applies and shows that $V^t = V$. As t centralizes F_pG and the characteristic is 2, we find that t acts trivially on V. As A is generated by conjugates of V we find $t = 1$, a contradiction.

So the Sylow 2-subgroups of G have order 2. Fix an involution $\sigma \in G$. Then $G = OG \cdot \langle \sigma \rangle$.

Now we easily recognize the context of Lemma 1.9, and we may conclude.

□

It remains to eliminate the case $FG = 1$. We apply Bender's theorem on the structure of groups with elementary abelian subgroups, together with the subsequent clarification of the structure of groups of type JR (*Janko-Ree*).

Fact 2.2 ([1], cf. [9, Theorem A, p. 40])**.** *Let G be a finite group with abelian Sylow 2-subgroups. Then G has a normal subgroup H of odd index such that H/OH is a product of an abelian 2-group with simple groups of type L_2 or JR, the latter being either of type J_1 or ${}^2G_2(q)$ with $q = 3^{2n+1}$ $(n \geq 1)$.*

Lemma 2.3. *Let (A, AG) be primitive, affine, and binary, in characteristic 2, with $FG = 1$. Then G is simple of type $L_2(q)$, J_1, or ${}^2G_2(q)$ where $q = 3^{2n+1}$.*

Proof. By Lemma 1.10 the Sylow 2-subgroups of G are elementary abelian. As G is generated by involutions, and $FG = 1$, Bender's theorem says that G is a product of simple groups of the stated forms.

Fix $L \lhd G$ simple. Let $V \leq A$ be an irreducible L-submodule. Then Lemma 1.17 shows that any other simple factor $L_1 \lhd G$ belongs to $N_G(V)$, a contradiction as V is irreducible. Thus $G = L$. □

We consider the remaining possibilities individually.

Lemma 2.4. *There is no primitive affine binary permutation group (A, AG) in characteristic 2 for which $G = \mathrm{SL}_2(q)$ with q a power of 2 and $q > 2$.*

Proof. Supposing the contrary, let $B = N_G(U) = UT$ with U a Sylow 2-subgroup and $T \cong \mathbb{F}_q^\#$ the corresponding torus (conjugate to the subgroup of diagonal matrices).

Set $A_0 = C_A(U)$. Then T acts on A_0. Let $\mathcal{O} \subseteq A_0^\#$ be a T-orbit. By Lemma 1.7 there is an involution $t \in N_G(\mathcal{O})$ fixing a point $u \in \mathcal{O}$ and inverting the action of T on $\mathcal{O}$.

As $\langle t, U\rangle$ fixes the point u we have $t \in U$. So for $g \in T$, the elements g and g^{-1} have the same action on $\mathcal{O}$, and g^2 acts trivially on $\mathcal{O}$. Hence T acts trivially on $\mathcal{O}$, and $\mathcal{O}$ consists of just one point u, with stabilizer UT.

Therefore the action of G on the orbit of u may be identified with the natural action of G on the projective line $\mathbb{P}^1(\mathbb{F}_q)$. This action is both binary and 2-transitive. It must therefore give the action of the full symmetric group on the points of the projective line. As $q > 2$, this is a contradiction. □

Lemma 2.5. *Let (A, AG) be primitive, affine, and binary, in characteristic 2. Then G is not of the form $\mathrm{PSL}_2(q)$ with $q > 3$.*

Proof. By Lemma 2.4 $q = p^n$ must be odd. Let U be a Sylow p-subgroup of G and $V \leq A$ an irreducible U-submodule.

If $n > 1$ then $U_0 = C_U(V)$ is nontrivial. In this case let $H = C_G(V)$. Then $H \leq N_G(U_0) \leq N_G(U) = UT$ with T a torus. By Corollary 1.5 we may suppose that H contains the involution t of T. But t inverts U and does not commute with the action of U on V. So we cannot have $t \in H$, a contradiction.

Thus $q = p$ is an odd prime. By Lemma 1.14 the induced action of $N_G(V)$ on V has the standard form $K\,\mathrm{Gal}(\mathbb{F}/\mathbb{F}_0)$. So $U = K$ has order $p = 2^d + 1$ where $|\mathbb{F}_0| = 2^d$. Now if $d \geq 3$ then T contains an element of order 4, contradicting Lemma 1.10. But if $d = 2$ then $L_2(p) \cong L_2(4)$, a case already disposed of. □

Lemma 2.6. *There is no primitive affine binary group (A, AG) with $G \cong J_1$ or ${}^2G_2(3^{2n+1})$.*

Proof. Suppose first that $G \cong J_1$. Let $S \leq G$ be cyclic of order 19. Then $N_G(S) = \mathbb{F}_{19} \cdot T$ with $T \leq \mathbb{F}_{19}^\#$ acting naturally on S, and any proper subgroup of G containing S is contained in $N_G(S)$.

Let V be a nontrivial irreducible S-submodule of A. By Lemma 1.14 there is a subgroup K of G containing S and acting on V like the kernel of the norm for some quadratic extension $[\mathbb{F} : \mathbb{F}_0]$.

Then $K < G$ and K contains S, so $K \leq N_G(S)$. Furthermore the action of K commutes with the action of S, which acts faithfully on V, so $K \leq C(S) = S$. It follows that $|K| = 19$ should be of the form $2^d + 1$ with $|\mathbb{F}_0| = 2^d$, and we have a contradiction.

Now consider the possibility

$$G \cong {}^2G_2(q) \text{ with } q = 3^{2n+1}$$

We refer to [18, Chapter 13] for the structure of the group.

Let S be a Sylow 3-subgroup of G and $U = ZS$. Then $N_G(U) = ST$ with $UT \cong \mathbb{F}_q \rtimes \mathbb{F}_q^{\#}$.

Let $V \leq A$ be an irreducible S-submodule with U acting nontrivially. If $q = 3$ then G is not generated by involutions, so we suppose $q > 3$. Then we set $U_0 = C_U(V) > 1$, and $V < A$. Thus $N_G(V) \leq N_G(U)$.

Now $C_G(V) \leq ST$ and $C_G(V)$ is generated by involutions in view of Corollary 1.5. Thus $C_G(V)$ contains an involution $t \in ST$, which operates on U by inversion. But then the action of t on V cannot commute with the action of U, a contradiction. □

Proposition 2.7. *If (A, AG) is primitive, affine, and binary, in characteristic 2, then the action is of standard type (1-dimensional or AO_2^-).*

Proof. If $G = 1$ then $|A| = 2$.

If $FG > 1$ then $G = O_2^-(q)$ acting naturally (Lemma 2.1).

If $FG = 1$ and $G > 1$ then G is simple by Lemma 2.3, of type $L_2(q)$, J_1, or ${}^2G_2(q)$, and each possibility has been eliminated. □

3. Primitive Affine Binary groups in Odd characteristic: the Base Case

We will show that in odd characteristic as well, the only primitive affine binary permutation groups (A, AG) are the standard ones.

Our analysis proceeds by showing (in the next section) that $EG = 1$ and that $F_2(G)$ is cyclic or dihedral, after which we may apply Lemma 3.4 below. First we show that G contains no quaternion subgroup, which conveniently eliminates some cases with $n_2(F_2G) = 1$, and reduces the number of cases to be considered in showing $EG = 1$. The proof of Lemma 3.4 is given in §3.2.

The elimination of quaternion subgroups and Lemma 3.3 (relating to the structure of $C(OG)$) will both continue to play a role in the following section.

3.1. Forbidding Q_8.

Lemma 3.1. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Then G contains no quaternion subgroup $Q \cong Q_8$ of order 8. Furthermore, there is no $V \leq A$ such that the image of $N_G(V)$ in $\mathrm{Aut}(V)$ contains a central extension of a quaternion subgroup.*

Proof. Suppose first that $V \leq A$ and the group H induced on V by $N_G(V)$ contains a subgroup $Q \cong Q_8$. The Q-module V is completely reducible, so we may suppose that it is irreducible (and the action of Q remains faithful).

Let the characteristic be p. There is a unique faithful irreducible $\tilde{\mathbb{F}}_p$ module for Q given over $\mathbb{F}_p$ by

$$Q = \left\langle \begin{bmatrix} a & b \\ b & -a \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\rangle$$

where $a^2 + b^2 = -1$. Thus V is 2-dimensional, over $\mathbb{F}_p$, contradicting Lemma 1.16.

Now suppose instead that the group H induced on V contains a central extension $\hat{Q}$ of Q with kernel K. Then we may take K to be a 2-group. Again, we may take V to be $\hat{Q}$-irreducible, allowing $\hat{Q}$ to be replaced by a quotient which still covers Q. Now $Z\hat{Q}$ is cyclic.

Let $i, j \in \hat{Q}$ represent generators of Q modulo K, and let $z = [i, j]$. As $i^2, j^2 \in zK$, it follows that z commutes with i and j, and hence with $\hat{Q}$. So $j^2 \in Z\hat{Q}$ and thus $z = [i, j]$ is a central involution of $\hat{Q}$. As $Z\hat{Q}$ is cyclic and $z \notin K$, it follows that $K = 1$, and thus we have reduced to the previous case. □

Corollary 3.2. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, and $H \leq G$ a 2-subgroup with $m_2(H) = 1$. Then H is cyclic.*

Proof. The group H is either cyclic or generalized quaternion and as quaternion subgroups are excluded, generalized quaternion subgroups are excluded. □

3.2. **Recognition in odd characteristic.** We begin with a generally useful lemma.

Lemma 3.3. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, with OG nontrivial. Suppose that A is OG-reducible and every proper primitive affine binary section of the form $(V, N_G(V))$ with $OG \leq N_G(V)$ is of type AO_2^-. Then*

1. *The set of involutions in G which commute with some nontrivial element of OG forms an elementary abelian subgroup of $C(OG)$.*
2. *$[G : C_G(OG)] = 2$, and $G/C(OG)$ acts on OG by inversion.*

Proof. By Lemma 1.23, OG is cyclic.

Let V be OG-irreducible. Then A is generated by conjugates of V, so the action of OG on V is faithful. If the involution t commutes with a nontrivial element of OG then this applies also to the action of t on V, and then our hypothesis on sections implies that t acts as ± 1 on V. Evidently the set of such involutions forms an elementary abelian subgroup of $C(OG)$. This proves the first point.

For the second, note that $G/C(OG)$ is generated by involutions (Corollary 1.5), so it suffices to consider the action of an involution $t \in G \setminus C(OG)$ on OG. By point (1), the action is by inversion.

□

Lemma 3.4. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, with $EG = 1$, $G \neq 1$, and F_2G either cyclic or dihedral. Then (A, AG) is of the form $(A, AO(A))$ for some anisotropic form on A.*

Proof. We may suppose inductively that any section of (A, AG) of the form $(V, VN_G(V))$ with the same properties has the form $(V, VO_2^-(V))$.

Suppose first that

$$F_2G \text{ is cyclic} \tag{3}$$

Then by Lemma 1.23, $FG = F_2G \cdot OG$ is cyclic. So $G/FG = G/C(FG)$ is abelian. In particular G is solvable and any proper affine binary section will satisfy the same hypotheses as (A, G).

By Corollary 1.5, G is generated by involutions, so $G/FG = G/C(FG)$ is an elementary abelian 2-group. In particular $C(OG)/OG$ is a 2-group, so $C(OG)$ splits and $C(OG) = FG$.

We may suppose

$$C(OG) < G, \text{ and in particular } OG > 1$$

Otherwise $G = FG$ is cyclic. As G is generated by involutions we then have $|G| = 2$ and our claim follows easily.

If A is FG-irreducible we set $\mathbb{F} = C_{\mathrm{End}\,A}(FG)$ and we arrive at the situation of Lemma 1.9. So suppose

$$A \text{ is } FG\text{-reducible}$$

By Lemma 3.3, $[G : C(OG)] = 2$ and $G = C(OG)\langle t\rangle = FG\langle t\rangle$ where t is an involution inverting OG.

Let V be an FG-irreducible submodule of A. As $V < A$, applying our hypothesis to $(V, VN_G(V))$, as OG acts nontrivially on V, we find that $N_G(V) > FG$. Then $N_G(V) = G$, contradicting the irreducibility of A.

Our second alternative is

$$F_2G \text{ is dihedral of order at least } 8 \tag{4}$$

We claim in this case

$$OG = 1$$

Otherwise, as $F_2(G)$ commutes with OG, A is OG-reducible. and then Lemma 3.3 provides a contradiction.

Then $C(F_2G) = ZF_2(G)$ and it follows that G is a 2-group, that is $G = F_2(G)$ is dihedral of order at least 8. Let C be the cyclic normal subgroup of G of index 2. It follows as above that A is C-irreducible and that we arrive at the configuration of Lemma 1.9. □

4. Primitive Affine Binary Groups in Odd Characteristic: EG and FG

Before entering into the analysis proper, we show in §4.1 that our group G does not contain the alternating group Alt_4, and in §4.2 we study the decomposition of A with respect to the action of an elementary abelian subgroup.

4.1. **Forbidding** Alt_4**.**

Lemma 4.1. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Then there is no $V \leq A$ such that the induced automorphism group $N_G(V)/C_G(V)$ contains the alternating group* Alt_4*.*

Proof. We suppose on the contrary that $\bar{H} = N_G(V)/C_G(V)$ contains $\bar{X} \cong \mathrm{Alt}_4$. We may take V to be X-irreducible. Write

$$\bar{X} = \bar{E}\langle\bar{\sigma}\rangle$$

where $\bar{E}$ is the normal 4-subgroup and $\bar{\sigma}$ is identified with the 3-cycle (123) in Alt_4.

Consider the corresponding eigenspace decomposition

$$V = \bigoplus_{\Lambda} V_\lambda$$

with respect to the action of $\bar{E}$, where the indices λ are homomorphisms from $\bar{E}$ to $\{\pm 1\}$ (Notation 1.12).

Fix $\lambda \in \Lambda$ and $u_1 \in V_\lambda^\#$, and set $u_2 = u_1^\sigma$, $u_3 = u_2^\sigma$. By irreducibility of V we find

$$\dim V = |\Lambda| = 3$$

and $V = \langle u_1, u_2, u_3\rangle$.

By Lemma 1.7 there is an involution t in G fixing u_3 and switching u_1, u_2. Thus $t \in N_G(V)$ and

$$\bar{X}\langle t\rangle \cong \mathrm{Sym}_4$$

with t acting as (12) in Sym_4.

Let $V_i = \langle u_i\rangle$ and $V_{ij} = V_i \oplus V_j$. Let $\bar{e} = (12)(34)$ in $\bar{E}$. As $\bar{e}$ commutes with (12), it acts trivially on V_3 and as -1 on V_1, V_2.

Let $\bar{q} = (1234)z = \bar{t}\bar{e}\bar{\sigma}z$ where $z \in ZG$ acts by inversion. Then q acts on V as follows.

$$u_1^q = u_3$$
$$u_2^q = u_2$$
$$u_3^q = -u_1$$

Thus $N_G(V)/C_G(V)$ contains an element $\bar{q}$ of order 4 fixing u_2.

If $p \equiv 1 \mod 4$ then $\bar{q}$ has an eigenvalue other than ± 1, contradicting Lemma 1.15. Thus

$$p \equiv -1 \mod 4$$

Thus the action of q on V_{13} is irreducible. Let $\mathbb{F} = C_{\mathrm{End}(V_{13})}(\bar{q})$. Then $\mathbb{F}$ is a field of order p^2.

Identify $\mathbb{F}$ with V_{13} via $f \leftrightarrow u_1^f$. The element $\bar{\tau} = (12)(34)z$ inverts $\bar{q}$ and acts on V_1 as $+1$, on V_3 as -1. As $\bar{\tau}$ fixes u_1, the actions of τ on $\mathbb{F}$ and V_{13} are compatible. Thus τ is a field automorphism with fixed field V_1.

The norm from V_{13} to V_1 is given by

$$N(au_1 + cu_3) = (a^2 + c^2)u_1$$

Define Q on V by $Q(au_1+bu_2+cu_3) = a^2+b^2+c^2$. By Lemma 1.16 the action of $N_G(V_{13})$ on V_{13} is $O_2^-(V_{13})$. We claim that the stabilizer of u_2 in $N_G(V_{13})$ induces the same action.

Let $c \in \mathbb{F}^\#$ have order $p+1$ and choose $u \in V_{13}$ so that $u^\tau = cu$. We claim that

$$(u, u_2, u^q) \sim (u, u_2, u^{q^{-1}})$$

under the action of G.

Now

$$\begin{aligned} u^q &\sim u^{q^{-1}} && \text{via } q^{-2} \\ u^q - u &\sim u^{q^{-1}} - u && \text{via } q^{-1}z \\ u^q - u_2 &\sim u^{q^{-1}} - u_2 && \text{via } q^{-2} \end{aligned}$$

so by binarity $(u, u_2, u^q) \sim (u, u_2, u^{q^{-1}})$ under G. A conjugating element of G will fix u_2, normalize V_{13}, and act as $c\bar{\tau}$ on V_{13}. thus the stabilizer of u_2 in $N_G(V_{13})$ induces both $\bar{\tau}$ and $c\bar{\tau}$, and hence the full group $O_2^-(V_{13})$.

Now we claim that the index of $[N_G(V)/C_G(V)] \cap O(V)$ in the full group $O(V)$ is at most 2. This will then imply that p divides $|G|$, which contradicts Lemma 1.10.

We will work with the subgroup K of $O(V)$ generated by the groups $O(V_{12})$, $O(V_{13})$, and $O(V_{23})$, and we make the same claim for K. We already have the stabilizer of u_1 in $O(V)$ inside K, so it suffices to consider the orbit of u_1 under K.

Let $u = au_1 + bu_2 + cu_3$ satisfy $Q(u) = 1$.

If $c = 0$ then u is conjugate to u_1 under K. So suppose $c \neq 0$.

If there is some vector $u' = a'u_1 + b'u_2 + c'u_3$ in the orbit of u_1 under K with $c' = c$, then as

$$Q(u - cu_3) = Q(u' - c'u_3)$$

we may conjugate u to u' under K.

In particular, if $1-c^2$ is a square, we take $a'^2 = 1-c^2$, $b' = 0$, $c' = c$ and conclude that u is conjugate to u_1.

So if we can also find u' conjugate to u_1 with c' a nonsquare, then all u with $Q(u) = 1$ are conjugate under K.

In the contrary case, the orbit of u_1 under K consists precisely of the vectors with $Q(u) = 1$ for which $1-c^2$ is a square (and in this case, a similar condition applies to the other coordinates). We may then calculate that the length of the orbit of u_1 under K is exactly half the length of the full orbit under $O(V)$.

Thus the index $[OG : K] \leq 2$. This yields our claim, and the contradiction $p||G|$. □

4.2. **Eigenspace Decompositions.**

Lemma 4.2. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Let $E \leq G$ be a maximal elementary abelian 2-subgroup of G, and let*

$$A = \bigoplus_{\Lambda} A_\lambda$$

be the corresponding eigenspace decomposition. Then Λ is a basis for $E^* = \mathrm{Hom}(E, \{\pm 1\})$.

Proof. The elements of Λ span E^*, as otherwise there would be some nontrivial $e \in E$ acting trivially on each factor. So we must check their linear independence.

Recall that ZG contains an element z acting as -1 on A (Lemma 1.6). Then $z \in E$.

Let $f : \Lambda \to \{\pm 1\}$ be arbitrary and let $\hat{f} : A \to A$ be the automorphism which acts on A_λ as $f(\lambda)$. We claim that there is $g \in G$ with

$$u^g = \hat{f}(u) \text{ for } u \in A$$

For this, it will suffice to have the same condition restricted to $u \in \bigcup_\Lambda A_\lambda$. By binarity, this reduces to checking the conjugacy of (u, v) with $(f(\lambda)u, f(\lambda')v)$ for $u \in A_\lambda$ and $v \in A_{\lambda'}$.

If $f(\lambda) = f(\lambda') = \pm 1$ this is evident, so we suppose $f(\lambda) \neq f(\lambda')$. In particular $\lambda \neq \lambda'$. We take $e \in E$ with $\lambda(e) \neq \lambda'(e)$. Replacing e by ez if necessary, we may suppose that $\lambda(e) = f(\lambda)$ and $\lambda'(e) = f(\lambda')$, and our claim follows.

Thus we have $g \in G$ acting via $u^g = \hat{f}(u)$. In particular g acts as ± 1 on each factor A_λ and hence commutes with E. Thus $g \in E$ and our claim becomes

$$\lambda(g) = f(\lambda)$$

for all λ. Thus the elements of Λ are linearly independent. □

The following slightly sharper statement was essentially proved along the way, but it can also be recovered from the statement of Lemma 4.2.

Corollary 4.3. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Let $E \leq G$ be an elementary abelian 2-subgroup of G, and let*

$$A = \bigoplus_\Lambda A_\lambda$$

be the corresponding eigenspace decomposition. Then for every function $f : \Lambda \to \{\pm 1\}$ there is an element $g \in C_G(E)$ such that

$$u^g = f(\lambda)u \text{ for } \lambda \in \Lambda$$

Proof. Extend E to a maximal elementary abelian subgroup of G and apply Lemma 4.2. □

The following reformulation of Lemma 4.2 introduces some additional notation which is convenient in practice.

Corollary 4.4. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Let $E \leq G$ be a maximal elementary abelian 2-subgroup of G, and let*

$$A = \bigoplus_\Lambda A_\lambda$$

be the corresponding eigenspace decomposition. Then for each λ in Λ there is a unique element e_λ in E such that e_λ acts as -1 on A_λ and as $+1$ on all other factors. The elements e_λ form a basis for E.

Lemma 4.5. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Suppose that $E \leq G$ is an elementary abelian subgroup. Let*

$$A = \bigoplus_{\Lambda} A_\lambda$$

be the eigenspace decomposition of A with respect to the action of E. Then every $N_G(E)$-orbit on Λ has length at most two.

Proof. Suppose that λ_1 and λ_2 are distinct elements of Λ which are conjugate under the action of $N_G(E)$. Choose representatives $u_i \in A^{\#}_{\lambda_i}$ which are conjugate under $N_G(E)$. We claim that there is an element $g \in G$ which interchanges u_1 and u_2, while fixing all elements of A_λ for $\lambda \neq \lambda_1, \lambda_2$.

Consider the set $X = \{u_1 \pm u_2\} \cup \bigcup_{\lambda \neq \lambda_1, \lambda_2} A_\lambda$ and the function $f : X \to X$ with

$$f(u_1 - u_2) = u_2 - u_1$$
$$f(x) = x \text{ otherwise}$$

We show that the function f is induced by some element $g \in G$. By binarity this reduces to the following two claims.

$$(u_1 - u_2) - (u_1 + u_2) \sim (u_2 - u_1) - (u_1 + u_2)$$
$$(u_1 - u_2) - u \sim (u_2 - u_1) - u \text{ for } u \in A_\lambda,\ \lambda \neq \lambda_1, \lambda_2$$

where $\sim$ denotes conjugacy under the action of G.

The first holds since u_1, u_2 are conjugate. For the second, apply Corollary 4.3.

Now let $g \in G$ induce the function f on X. Then g fixes A_λ for all $\lambda \neq \lambda_1, \lambda_2$. Since g fixes $u_1 + u_2$ and inverts $u_1 - u_2$, g interchanges u_1, u_2.

So at this point we have, in all cases, an element $g \in G$ interchanging u_1 and u_2 and fixing the remaining spaces A_λ.

Now suppose we have an orbit for $N_G(E)$ of length at least 3 and choose $\lambda_1, \lambda_2, \lambda_3$ distinct in this orbit. We may also choose representatives $u_i \in A^{\#}_{\lambda_i}$ which are $N_G(E)$-conjugate. So all transpositions on the set $\{u_1, u_2, u_3\}$ are induced by G, and thus there is also a 3-cycle σ of type $(1, 2, 3)$ on these elements. Then $\langle e_{\lambda_1} e_{\lambda_2}, e_{\lambda_1} e_{\lambda_3} \rangle \cdot \langle \sigma \rangle$ gives an action of Alt_4 on $\langle u_1, u_2, u_3 \rangle$. This contradicts Lemma 4.1. □

4.3. $EG = 1$.

Lemma 4.6. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, and $L \lhd EG$ quasisimple. Then L is one of the following.*

- $A_1(q) = \mathrm{PSL}_2(q)$ *with $q = 2^{2n+1}$ an odd power of 2.*
- ${}^2B_2(2^{2n+1}) = \mathrm{Sz}(q)$ *with $q > 2$ an odd power of 2, or a covering group of* $\mathrm{Sz}(8)$.

Proof. The simple quotient $\bar{L} = L/ZL$ contains no quaternion subgroup by Lemma 3.1, so must be one of the following.

- Janko's first sporadic group J_1
- $A_1(q)$ or $A_2(2^n)$ with n odd.

- $B_2(2^n)$
- ${}^2B_2(2^{2n+1})$
- ${}^2G_2(3^{2n+1})$
- Alt_7

To see this, first check the sporadic groups using the Atlas, starting with the minimal sporadic groups Mc, M_{11}, M_{22}, Ru, J_1, J_3. Only J_1 survives; the remaining sporadic groups contain one of the excluded groups (in the case of O'Nan's group, M_{11}).

Among the alternating groups one should retain Alt_5 through Alt_7, but $\mathrm{Alt}_5, \mathrm{Alt}_6$ are listed in the guise of $A_1(q)$ for $q = 5$ or 9.

So one comes down to Chevalley groups, possibly twisted. By [12, Lemma 3.2.8] we have an embedding of $\mathrm{SL}_2(q)$ apart from the cases of $A_1(q)$, ${}^2B_2(q)$, and ${}^2G_2(q)$, so for q odd this takes us down to the list shown. For q a power of 2 one may consult the Atlas again for the minimal cases, over fields of order 2 or 4.

With the list of possibilities for $\bar{L}$ in hand, we must check their quasisimple central extensions using Lemma 4.1; there must be no subgroup isomorphic to Alt_4.

For the simple quotients, we note that J_1 contains Alt_5, $A_1(q)$ contains Alt_4 for q odd, $A_1(4) \cong \mathrm{Alt}_5$, $A_2(2)$ contains Sym_4, and $B_2(2)' \cong \mathrm{Alt}_6$. Finally, ${}^2G_2(3)$ has $A_2(8)$ as its commutator subgroup.

We must also consider proper central extensions of these groups. The possibilities are laid out systematically in [18]. The cases with nontrivial Schur multiplier are as follows.

1. Typically the universal cover of $A_1(q)$ is $\mathrm{SL}_2(q)$. For q odd this contains the quaternion group Q_8.

There are exceptional covers in two cases:

- $A_1(4) \cong A_1(5)$ and the universal cover of $A_1(4)$ is $\mathrm{SL}_2(5)$, which gives nothing new; and
- $A_1(9) \cong \mathrm{Alt}_6$ has a Schur multiplier which is cyclic of order 6. In the triple cover, the extension of Alt_5 splits. In the double cover, Q_8 embeds.

2. $A_2(2^n)$ with n odd has trivial Schur multiplier unless $n = 1$, in which case we have only the usual cover of the isomorphic group $A_1(7)$.

3. $B_2(2^n)$ has trivial Schur multiplier, apart from the case $B_2(2)' \cong \mathrm{Alt}_6$ already discussed.

4. The Schur multiplier of $\mathrm{Sz}(8)$ is a 4-group. □

Proposition 4.7. *If (A, AG) is a primitive, affine, binary permutation group in odd characteristic, then $EG = 1$.*

Proof. If $EG > 1$, then EG is a product of quasisimple components of type $A_1(2^{2n+1})$, ${}^2B_2(2^{2n+1})$, or a central extension of the latter with $n = 1$.

Fix a quasisimple component L of EG.

Suppose first

$$L \text{ is of type } A_1(2^q) \text{ with } q > 2 \text{ an odd power of } 2$$

Let E_L be a Sylow 2-subgroup of L. Let

$$A = \bigoplus_{\Lambda} A_\lambda$$

be the corresponding eigenspace decomposition of A. By Lemma 4.5, the orbits of $N_G(E_L)$ on Λ have length at most 2. On the other hand there is a torus $T \cong \mathbb{F}_q^\#$ in $N_G(E_L)$ acting on Λ, and of odd order. Hence T must fix all points of Λ, and as T is transitive on $E_L^\#$, Λ can contain only the constant function 1, which means E_L acts trivially on A, a contradiction.

If L is of type ${}^2B_2(2^{2n+1})$, argue similarly with E_L the center of a Sylow 2-subgroup, which may be identified with the additive group of the field, with the action of the multiplicative group in the normalizer. This picture lifts to central extensions when $n = 1$.

□

4.4. F_2G.

Lemma 4.8. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, and $H \lhd G$ an abelian 2-subgroup. Then H is cyclic or elementary abelian.*

Proof. Let $E = \Omega_1 H$, and suppose $|E| > 2$. Let

$$A = \bigoplus_{\Lambda} A_\lambda$$

be the corresponding eigenspace decomposition. Fix $\lambda \in \Lambda$ not identically 1, and $V \leq A_\lambda$ H-irreducible. The kernel E_V of the action of H on V is contained in E by Lemma 1.19, and

$$H = E_V \oplus C$$

with C cyclic.

Suppose H is not elementary abelian and fix $h \in C$ of order 4. Take $t \in G$ an involution such that $\lambda^t \neq \lambda$. Then $h^t \in h^{\pm 1} E_V$, so

$$(v^t - v)^h = v^{h^t t} - v^h = \pm v^{ht} - v^h$$

As $v^h \in A_\lambda$ and $v^{ht} \in A_{\lambda^t}$, there is $e \in E \cdot ZG$ acting as -1 on A_{λ^t} and as $+1$ on A_λ. Thus $(v^t - v)^h$ is conjugate under G to $v^{ht} - v^h$. This contradicts Lemma 1.17. □

Lemma 4.9. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, with $OG > 1$. Suppose that $H \lhd G$ is a 2-subgroup such that A is $H \cdot OG$-reducible, and that every section $(V, VN_G(V))$ with V $H \cdot OG$-invariant is of type AO_2^-. Then H is abelian.*

Proof. Let $V \leq A$ be $H \cdot OG$-irreducible. As A is a sum of conjugates of V, the action of OG on V is nontrivial. By our hypothesis, the image of H acting on V is commutative. Varying V, H is commutative. □

Lemma 4.10. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, with $OG > 1$. Suppose that every proper primitive affine binary section $(V, N_G(V))$ with V OG-invariant is of standard type. Then F_2G is abelian.*

Proof. By Lemma 1.23, $FG = F_2G \cdot OG$. By Lemma 4.9, with $H = F_2G$, if A is FG-reducible the claim follows. So we suppose

$$A \text{ is } FG\text{-irreducible}$$

In particular

$$m_2(ZF_2G) = 1$$

If A is OG-irreducible the claim holds by Schur's Lemma. So we suppose

$$A \text{ is } OG\text{-reducible}$$

If $m_2(F_2G) = 1$, then F_2G is cyclic, by Lemma 3.2. So suppose

$$m_2(F_2G) > 1$$

By Lemma 3.3 we have

$$n_2(F_2G) = m_2(F_2G)$$

Thus $n_2(F_2G) > 1$, and therefore $n_2(Z_2F_2G) > 1$.

Let $E = \Omega_1(Z_2F_2G)$ and set $H = C_{F_2G}(E)$. By Lemma 3.3, E is elementary abelian and H contains $\Omega_1(F_2G)$. Thus $E \leq Z(H \cdot OG)$. Therefore A is $H \cdot OG$-reducible. So by Lemma 4.9, H is abelian. By Lemma 4.8, H is elementary abelian. Thus

$$H = \Omega_1(F_2G)$$

For $e \in E \setminus ZF_2G$, the index of $C_{F_2G}(e)$ in F_2G is 2, so F_2G/H is an elementary abelian 2-group. As $\Omega_1(F_2G) = H$, the elements of $F_2G \setminus H$ all have order 4.

Consider the eigenspace decomposition with respect to H

$$A = \bigoplus_{\Lambda} A_\lambda$$

As A is FG-irreducible, FG acts transitively on Λ. As $H \cdot OG$ fixes Λ, F_2G/H acts transitively on Λ.

Suppose $x \in F_2G$ fixes Λ. Then x centralizes H and hence $x \in H$. Thus the elementary abelian group F_2G/H acts transitively and faithfully, hence regularly, on Λ.

Now apply Corollary 4.3. For $\lambda \in \Lambda$ there is $h_\lambda \in C_G(H)$ such that h_λ acts as -1 on A_λ and as $+1$ on the remaining factors. As OG commutes with F_2G, OG acts on each factor A_λ and hence commutes with h_λ. Thus $h_\lambda \in C(OG)$, and by definition h_λ is an involution. Therefore by Lemma 3.3 we have $h_\lambda \in \Omega_1(F_2G) = H$. Thus the h_λ form a basis for H.

We suppose $F_2G \neq H$. Choose $x \in F_2G \setminus H$ so that when the square $h = x^2 \in H^\#$ is expressed as a product

$$h = \prod_{\lambda \in \Lambda_0} h_\lambda$$

the cardinality of Λ_0 is minimized. As x commutes with h, x must stabilize Λ_0. The orbits of x on Λ have length 2. Therefore for $\lambda_0 \in \Lambda_0$, the element $(xh_{\lambda_0})^2 = \prod_{\Lambda_0'} h_\lambda$ with

$$\Lambda_0' = \Lambda \setminus \{\lambda_0, \lambda_0^x\}$$

This is a contradiction. Thus $F_2G = H$ is elementary abelian. □

Lemma 4.11. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Suppose that $E \lhd G$ is an elementary abelian 2-group which is not cyclic. Then we have the following.*

(1) *E is a 4-group containing ZG.*
(2) *$[G : C_G(E)] = 2$*
(3) *For $V \leq A$ $C_G(E)$-irreducible,*
   - *the kernel of the action of $C_G(E)$ on V is contained in E;*
   - *$A = V \oplus V^t$, with t an involution and $G = C_G(E)\langle t\rangle$.*

Proof. We consider the eigenspace decomposition

$$A = \bigoplus_{\Lambda} A_\lambda$$

with respect to the action of E. Then G acts transitively on Λ. By Lemma 4.5 we have $|\Lambda| \leq 2$. As $|E| > 2$ we find

$$|E| = 4,\ |\Lambda| = 2$$

By Corollary 1.8, $ZG = \langle z\rangle$ where z inverts A. As the reasoning above applies to $E \cdot ZG$ we find

$$ZG \leq E$$

This implies

$$[G : C_G(E)] = 2$$

Now consider a $C_G(E)$-irreducible submodule $V \leq A$. Then $V < A$ and there is an element $t \in G$ such that $A = V \oplus V^t$. By Corollary 1.4, t may be taken to be an involution. We have

$$G = C_G(E)\langle t\rangle$$

Let K be the kernel of the action of $C_G(E)$ on V. By Lemma 1.19, the kernel K is an elementary abelian 2-group. Thus $K \oplus K^t$ is a normal elementary abelian subgroup of G. Therefore $|K \oplus K^t| \leq 4$. But K contains an involution of E, so $K \oplus K^t = E$ and $K \leq E$ has order 2.

□

Lemma 4.12. *Let (A, AG) be primitive, affine, and binary, in odd characteristic,with $OG > 1$. Suppose that every proper primitive affine binary section $(V, N_G(V))$ with V OG-invariant is of standard type. Then F_2G is cyclic.*

Proof. By Lemmas 4.10, 4.8, and 4.11, F_2G is either cyclic or a 4-group. So suppose F_2G is a 4-group. The centralizer in $C(OG)$ of F_2G is FG, and $C(OG)/FG$ acts on F_2G fixing ZG, so $[C(OG) : FG] \leq 2$. Thus $C(OG)/OG$ is a 2-group and hence $C(OG)$ splits as $C(OG) = F_2G \cdot OG = FG$. So by Lemma 3.3 we have $G = FG\langle t\rangle$ with t an involution.

Let V be an irreducible FG-submodule of A. As F_2G is a 4-group, $V < A$. As the induced action of $N_G(V)$ on V cannot be abelian, $N_G(V) = G$. This contradicts the G-irreducibility of A. □

Lemma 4.13. *Let (A, AG) be primitive, affine, and binary, in odd characteristic. Suppose that $E \lhd G$ is an elementary abelian 2-group which is not cyclic. Suppose further that $OG = 1$ and that every proper primitive affine binary section $(V, VN_G(V))$ with V $C_G(E)$-invariant is of standard type. Then G is a 2-group, and either*

- *G is a dihedral group of order 8, or*
- *for $s \in E \setminus ZG$, $C_G(E)/\langle s \rangle$ is a dihedral group of order 8.*

Proof. Fix $V \leq A$ a $C_G(E)$-irreducible submodule. Lemma 4.11 applies.

Let $ZG = \langle z \rangle$. We show first

$$\text{There is no } h \in C_G(E) \text{ with } h^2 = z.$$

Suppose toward a contradiction that $h \in C_G(E)$ and $h^2 = z$ acts on A by inversion. Then $h^t \in C_G(E)$ has the same square and hence acts on V as $\pm h$.

We apply Lemma 1.17. Take $v \in V^\#$ so that $v^h \neq \pm v$. Then

$$(v^t - v)^h = v^{h^t t} - v^h = \pm v^h t - v^h$$

Since $-v^{ht} - v^h \sim v^{ht} - v^h$, Lemma 1.17 gives a contradiction.

By Lemma 4.11 and our hypothesis on sections, $C_G(E)$ is a subdirect product of two isomorphic dihedral groups

$$C_G(E) \hookrightarrow D_1 \times D_2$$

As $OG = 1$, it follows that D_1, D_2, and G are 2-groups.

For $s \in E \setminus ZG$, $\langle s \rangle$ is the kernel of the action of $C_G(E)$ on V or V^t; say V. Then $C_G(E)/\langle s \rangle = N_G(V)/C_G(V)$ is a dihedral group. Denote its order by 2^{n+1}. Then $C_G(E)/\langle s \rangle = \bar{C} \cdot \langle \bar{u} \rangle$ where $\bar{C}$ is cyclic and $\bar{u}$ is an involution inverting C. Let C be the preimage of $\bar{C}$ in $C_G(E)$.

If $n > 2$ then the elements of maximal order in $C_G(E)$ belong to C. Let $x \in C_G(E)$ have maximal order, say 2^k. If $k > n$ then $x^{2^k} = s$ and $C_G(E)/\langle sz \rangle$ is not a dihedral group. So $k = n$ and $x^{2^{n-1}} = z$ or sz. We have already eliminated z as a possibility so

$$x^{2^{n-1}} = sz$$

Then $C_G(E)/\langle sz \rangle$ is not a dihedral group.

If $n = 1$ then $C_G(E)$ is a subdirect product of abelian groups, hence abelian. By Lemma 4.8 since $C_G(E)$ contains E it is elementary abelian, that is $C_G(E) = E$. Then G is dihedral of order 8.

In the remaining case $n = 2$ and $C_G(E)/\langle s \rangle$ is dihedral of order 8. □

Lemma 4.14. *Let (A, AG) be primitive, affine, and binary, in odd characteristic, with $F^*G = F_2G$. Suppose that for any normal elementary abelian subgroup E of G, any proper primitive affine binary section which is $C_G(E)$-invariant is of standard type. Then F_2G is of symplectic type. That is, F_2G has no noncyclic characteristic abelian subgroup.*

Proof. Suppose toward a contradiction that E *char* F_2G is noncyclic and elementary abelian. As $E \lhd G$, Lemma 4.11 applies. So

$$A = V \oplus V^t$$

where V is $C_G(E)$-irreducible and the kernel of the action of $N_G(V)$ on V is a cyclic subgroup $\langle s\rangle$ of E, where

$$E = \langle s, z\rangle, ZG = \langle z\rangle$$

Furthermore $G = F_2G$ and $G/\langle s\rangle$ is a dihedral group. We may suppose G is not itself a dihedral group, so $C_G(E)/\langle s\rangle$ is dihedral of order 8 and V may be identified with $\mathbb{F}_9$.

Take $h \in C_G(E)$ acting as an element of order 4 on V. Then $h^2 = sz$ by Lemma 4.11. Thus h^t acts as an involution on V. As $h^t \notin E$, this is a noncentral involution in the action on V, that is an element of the form $c\sigma$ where σ is the involutory automorphism of $\mathbb{F}_9$ and c is an element of norm 1.

Take $v \in V$ so that $v^\sigma = icv$ where the scalar i represents the action of h: $v^h = iv$, $i^2 = -1$. Then

$$v^{h^t} = v^{c\sigma} = c^{-1}v^\sigma = iv = v^h$$
$$(v^t - v)^h = v^{h^t t} - v = v^{ht} - v$$

and Lemma 1.17 applies to give a contradiction. □

Lemma 4.15. *Suppose that (A, AG) is primitive, affine, and binary, in odd characteristic, and F_2G is of symplectic type. Then F_2G is cyclic or dihedral.*

Proof. By Fact 1.22 F_2G must have the structure

$$E * Q$$

where E is extraspecial and Q is one of the following: cyclic, dihedral, generalized quaternion, or semidihedral. The generalized quaternion and semidihedral cases are eliminated by Lemma 3.1, and by the same token E is either dihedral of order 8 or trivial.

If E is dihedral then as $E * Q$ contains no quaternion subgroup, $Q = 1$. Thus the possibilities are as stated: F_2G is either dihedral or cyclic. □

Proposition 4.16. *If (A, AG) is primitive, affine, and binary, in odd characteristic, then the action is of standard type (1-dimensional or AO_2^-).*

Proof. We may suppose that every proper primitive affine binary section $(V, VN_G(V))$ is of standard type. By Lemma 4.7, $EG = 1$.

If $OG > 1$ then by Lemma 4.12, F_2G is cyclic. If $OG = 1$ then by Lemmas 4.14 and 4.15, F_2G is either cyclic or dihedral.

By Lemma 3.4, the action is of standard type. □

Proof of Theorem 1. Propositions 2.7 and 4.16. □

5. The Alternating Group on k-Sets

We calculate the relational complexity of Alt_n acting on k-sets.

Theorem (2). *For $2k \leq n$, the relational complexity $\rho = \rho_A(n, k)$ of Alt_n acting on k-sets is at least $n - 3$, and is exactly $n - 3$, apart from the following exceptional cases:*

$k = 1$	$\rho = n - 1$
$k = 2$	$\rho = \max(n - 2, 3)$
$k \geq 3$, $n = 2k + 2$	$\rho = n - 2$

Proof. We may suppose throughout that

$$k \geq 2$$

We first deal with the lower bound

$$\rho \geq n - 3$$

We partition $\{1, \ldots, n\}$ into three sets A_1, A_2, A_3 with the first two of size $k - 1$. We fix elements $a_i \in A_i$ for $i = 1, 2, 3$. We define the k-sets $X_i = \{i\} \cup A_1$ for $i \notin A_1 \cup \{a_2, a_3\}$ and $Y_j = \{j\} \cup A_2$ for $j \in A_1 \setminus \{a_1\}$. This gives us a total of $n - 3$ sets X_i, Y_j which we arrange in a sequence ξ. Let ξ^* be the image of ξ under some odd permutation σ.

The sets X_i and Y_j separate the points of $\{1, \ldots, n\}$. Hence the only element of Sym_n carrying ξ to ξ^* is σ, and thus the sequences ξ and ξ^* are not conjugate under the action of Alt_n. On the other hand, if we delete one of the sets from ξ and delete its image under σ from ξ^*, we claim that the truncated sequences ξ', $\xi^{*\prime}$ are conjugate under the action of Alt_n. For this it suffices to check that the sets in the truncated sequence ξ' do not separate the points of $\{1, \ldots, n\}$, as then we can compose σ with a transposition that fixes ξ'.

If X_i is omitted where $i \in A_\ell$, then i and a_ℓ are not separated. If Y_j is omitted then j and a_1 are not separated.

This shows that the relational complexity of the action is at least $n - 3$.

(Notice that our analysis above leads to particular consideration of the pairs (a_ℓ, x) with $x \in A_\ell$, $x \neq a_\ell$, and that if we take these to be the edges of a graph then the graph has three components, which are stars of orders $k - 1$, $k - 1$, and $n - 2(k - 1)$. These graphs will reappear in our proof of the upper bounds.)

Now if $k = 2$ we let $X_i = \{i, n - 1\}$ for $i \leq n - 2$. Let ξ be the sequence $(X_i)_{i \leq n-2}$ and let ξ^* be the image of ξ under an odd permutation. Again, the sets X_i separate points, since $N \geq 4$. Evidently if we delete X_i from the sequence ξ then i and n are not separated. So the argument used above now shows that $\rho \geq n - 2$ in this case. It is easy to see that $\rho \geq 3$ for $k = 2$, $n \geq 4$. So we have the desired lower bound for $k = 2$.

(In this argument, the pairs (i, n) for $i \leq n - 2$ play a distinguished role, and if we view these as the edges of a graph, it now has a single component, a star of order $n - 1$.)

Our last lower bound applies when $n = 2k + 2$. We partition $\{1, \ldots, n\}$ into two sets A_1, A_2 of order $k + 1$ and fix $a_i \in A_i$ for $i = 1, 2$. For $i \in A_\ell \setminus \{a_\ell\}$ we set $X^i_\ell = A_\ell \setminus \{i\}$, getting $2k = n - 2$ k-sets, which we form into a sequence ξ, and again let ξ^* be the image of ξ under an odd permutation σ. Again the sets X_i separate points in $\{1, \ldots, n\}$, while this is no longer true if we delete one of the sets X^i_ℓ.

(In this case the relevant pairs are (i, a_ℓ) with $i \in A_\ell \setminus \{a_\ell\}$, and if we view these as forming a graph we have two components, each a star of order $k + 1$, covering n vertices.)

It remains to check the upper bounds on ρ by verifying that graphs of the above types must come into play in the analysis, except in marginal cases where ρ happens to coincide with the relational complexity of the full symmetric group on k-sets.

We first recall from [6] that the relational complexity $\rho_S(n,k)$ of the action of Sym_n on k-sets is

$$\lfloor \log_2(k) \rfloor + 2$$

for $k \geq 2$.

This leads to the following observation.

If $\rho \leq \rho_S(n,k)$ then our stated formula for ρ is correct

We may check in this case that our lower bound forces both $\rho = \rho_S(n,k)$ and that this formula is in agreement with the one given by the theorem. For $k = 2$, the inequality $\rho \leq \rho_S(n,k)$ implies

$$n - 2 \leq \rho \leq \rho_S(n,k) = 3$$

and so $n \leq 5$. In case $n = 5$ we would conclude $\rho = \rho_S(n,k) = 3 = n-2$ as stated. In case $n = 4$ we already have the lower bound $\rho \geq 3$ so again $\rho = 3$.

For $k > 2$, the inequality $\rho \leq \rho_S(n,k)$ implies

$$2k - 3 \leq n - 3 \leq \rho \leq \rho_S(n,k) = \lfloor \log_2(k) \rfloor + 2$$

So $2k \leq \lfloor \log_2(k) \rfloor + 5$ and thus $k = 3$, $n = 6$. We wind up with $\rho = \rho_S(n,k) = 3$ in this case, the predicted value.

With these marginal cases out of the way, we deal systematically with the upper bound on ρ, under the assumption that

$$\rho > \rho_S(n,k)$$

We fix two sequences ξ and ξ^* of length ρ, consisting of k-subsets of $\{1,\ldots,n\}$, where (1) ξ is not conjugate to ξ^* under Alt_n, but (2) for any subsequences $\hat{\xi}$, $\hat{\xi}^*$ corresponding to the deletion of the i-th set, the sequences $\hat{\xi}$ and $\hat{\xi}'$ are conjugate under the action of Alt_n, and hence under Sym_n. Now since $\rho > \rho_S(n,k)$ it follows that there is a permutation $\sigma \in \mathrm{Sym}_n$ carrying ξ to ξ^*; but there is no such even permutation. In particular

The sets in the sequence ξ separate points in $\{1,\ldots,n\}$

But if the sets in the truncated sequence $\hat{\xi}$ also separated points in $\{1,\ldots,n\}$, then σ would again be the only permutation taking one truncated sequence to the other; and then our condition on conjugacy under Alt_n would fail. Thus we have the following.

For $1 \leq i \leq \rho$ there is a pair (a_i, b_i) of elements of $\{1,\ldots,n\}$ such that

the sequence $\hat{\xi}$ obtained by deleting the i-th entry of ξ does not separate a_i, b_i

Consider the graph $\Gamma = \Gamma_\xi$ with vertices $\{1,\ldots,n\}$ and with edges (a_i, b_i) as above for $1 \leq i \leq \rho$. Observe that for each i we select only one suitable edge, and thus Γ has exactly ρ edges.

Now we show

Γ is an acyclic graph

Suppose that $(u_0, \ldots, u_{m-1})$ form a cycle in Γ. Let X be the unique entry of ξ which separates (u_0, u_1). Then X does not separate any other pair forming an edge of Γ. But then we could trace around the cycle from u_1 back to u_0 and conclude that X does not separate u_0 and u_1. So Γ is acyclic.

If the graph Γ has at least 3 components then $\rho \leq n - 3$, and by our lower bound $\rho = n - 3$; in particular we are not in any of the exceptional cases. In this case we are done. At the corresponding point in our lower bound analysis, we saw such a graph with three components.

Now suppose that Γ contains either one or two components.

First, consider the case in which some component C of Γ contains at least $k+2$ vertices; this includes the case of a unique component. Consider a leaf v of C and a set X in the sequence ξ which separates the leaf v from its neighbor. Then arguing as in the case of a cycle, X separates v from $C \setminus \{v\}$. But $C \setminus \{v\}$ contains at least $k+1$ points, and $|X| = k$, so this tells us that the leaf v is in X and the rest of C is disjoint from X. As $k > 1$ there must be a second component C' which X meets, and hence contains. Thus $X = \{v\} \cup C'$ and $|C'| = k - 1$. Since $|C'| < k$, any set Y in ξ which separates points on an edge of C' must meet, and hence contain, the component C. As this would be a contradiction, C' has no edges and therefore consists of a unique vertex. But $|C'| = k - 1$, so $k = 2$. As $|C| \geq k + 2$ we have $n \geq 5$. Now Γ has $n - 2$ edges so in this case we have $\rho = n - 2$, the predicted value.

Second, we suppose that Γ contains exactly two components, and that each component of Γ has at most $k + 1$ vertices. In particular $n \leq 2k + 2$. Also both components are nontrivial, as otherwise $n = k + 2 \geq 2k + 2$ and $k = 2$, $n = 4$, which by inspection falls under the case $\rho = \rho_S(n, k)$.

If one of the components C has at most k vertices, then any set X which separates two vertices forming an edge of C must contain the other component, and then the other component has at most $k - 1$ vertices. It then follows that both components have at most $k - 1$ vertices and $n < 2k$, a contradiction. So we now arrive at our final case: $n = 2k + 2$ and $\rho = n - 2$, as stated. □

References

[1] H. Bender, *On groups with abelian 2-subgroups,* Math. Zeitshr. **117** (1970), 164–176.

[2] N. Blackburn, *Generalizations of certain elementary theorems on p-groups,* Proc. London Math. Soc. **11** (1961), 1–22.

[3] P. J. Cameron, *Oligomorphic Permutation Groujps,* London Mathematical Society Lecture Note Series **152** (1990), 172 pp., Cambridge University Press.

[4] R. Carter, *Simple Groups of Lie Type,* Pure and Applied Mathematics 28, John Wiley and Sons, 1972 (reprinted 1989).

[5] G. Cherlin, *Sporadic homogeneous structures,* The Gelfand Mathematical Seminars, 1996-1999, pp. 15-48, Birkhäuser, 2000.

[6] G. Cherlin, G. Martin, and D. Saracino, *Arities of permutation groups: Wreath products and k-sets*, J. Combinatorial Theory, Ser. A **74**, 249-286 (1996)

[7] J. Conway, S. Norton, R. Parker, and R. Wilson, *Atlas of Finite Groups: Maximal Subgroups and Characters for Simple Groups,* Oxford University Press, 1985.

[8] J. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics **163** (1996), 348 pp., Springer.
[9] T. Gagen, *Topics in Finite Groups*, LMS Lecture Note Series 16, Cambridge University Press, 1976.
[10] A. Gardiner, *Homogeneous graphs,* J. Comb. Th. **20** (1976), 94-102.
[11] D. Gorenstein, *On a theorem of Philip Hall*, Pacific J. Math. **19** 1966, 77–80.
[12] D. Gorenstein, R. Lyons, R. Solomon, *The Classification of the Finite Simple Groups, Number 3. Part I, Chapter A: Almost simple K-groups.* Mathematical Surveys and Monographs, 40.3. American Mathematical Society, Providence, RI, 1998. xvi+419 pp
[13] R. Griess, *Finite groups whose involutions lie in the center,* Quart. J. Mathematics **29** (1978), 241–247.
[14] W. Kantor, M. Liebeck, and H. D. Macpherson, $\aleph_0$*-categorical structures smoothly approximated by finite substructures,* Proc. London Math. Soc. (3) **59** (1989), 439–463.
[15] A. Patterson, *On Sylow 2-subgroups with no normal subgroups of rank 3, in finite fusion-simple groups,* Transactions Amer. Math. Soc. **187** (1974), 1–67.
[16] D. Saracino, *On a combinatorial problem from the model theory of wreath products I-III,* I, II: J. Combin. Theory Ser. A **86** (1999), 281–305, 306–322. III: J. Combin. Theory Ser. A **89** (2000), 231–269.
[17] J. Sheehan, *Smoothly embeddable subgraphs,* J. London Math. Soc. **9** (1974), 212-218.
[18] R. Wilson, *The finite simple groups,* Graduate Texts in Mathematics, 251. Springer-Verlag London, Ltd., London, 2009. xvi+298 pp. ISBN: 978-1-84800-987-5
[19] J. Wiscons, *A reduction theorem for primitive binary permutation groups.* Preprint (submitted, 2015), 9 pp.

Department of Mathematics, Rutgers University