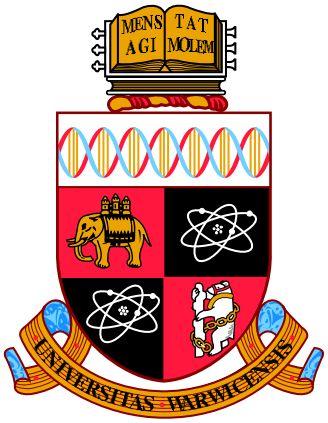

TOPICS IN COMPUTATIONAL GROUP THEORY RELATING TO CLASSIFICATIONS OF PERMUTATION GROUPS

by

Benjamin Mark Stratford

Thesis

Submitted to the University of Warwick
for the degree of

Doctor of Philosophy
in
Mathematics

Department of Mathematics

January 2022

Contents

List of Figures

List of Tables

Acknowledgements. First and foremost I would like to thank my supervisors Professor Derek Holt and Doctor Inna Capdeboscq, without whom my thesis would not exist. I will always be grateful for the time that they generously invested in me during this journey, especially during the uncertainty of the last few years, and for their continued support and expert guidance during this period.

Secondly I would like to thank my wife Beth who has been a constant source of encouragement, even during the long evenings of work.

I would like to thank my parents Tim and Jen and my brothers Sam and Josh, with whom I could always find a listening ear.

Finally I would like to thank my friends who have made this entire process easier and more enjoyable.

DECLARATIONS. This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. It has been composed by myself and has not been submitted in any previous application for any degree or professional qualification.

Except where it is stated otherwise, the work presented (including data generated and data analysis) was carried out by the author.

Abstract. In this thesis we extend the classification of primitive permutation groups of degree d to include $4096 \leq d < 8192$. We make heavy use of the O'Nan-Scott Theorem, Aschbacher's Theorem for general linear groups, and the Classification of the Finite Simple Groups. We follow the method given in [13] making the necessary changes and computations.

This work required the construction of a deterministic test which outputs whether a subgroup of $\mathrm{GL}(d, q)$ is semilinear.

We have also produced a general function which, for a given $1 \leq d \leq 1000000$, outputs all non-affine primitive groups of degree d.

Finally we have classified the quasiprimitive groups up to degree 3600, making use of Praeger's "O'Nan-Scott Theorem" for quasiprimitive groups given in [33].

1. Introduction and Basic Results from the Literature

This thesis focuses on several problems in Computational Group Theory. We use the computational algebra system MAGMA [5] extensively and our results will likely be added to its databases.

A *primitive* permutation group G of degree n is a transitive subgroup of S_n such that every point stabilizer in G is a maximal subgroup of G.

The classification of primitive groups of low degree has been achieved for many different ranges of degree over the course of the last two centuries. The electronic publication of the resulting databases forms an important part of Computational Group Theory. For a more detailed history of the classification of primitive groups we refer the reader to [24, Chapter 11] or [13, Section 1]. Prior to this thesis the classification was complete up to degree 4095.

By classification of groups we mean that all of the groups with the stated property have been determined, up to an equivalence. The equivalence that we use throughout this thesis is permutation isomorphism.

In Section 3 we extend the classification of primitive permutation groups of degree d up to degree $d < 8192$, following a similar method to [13]. Our approach is highly computational as this minimises the possibility of human error and many of the calculations are impossible to do by hand. We discovered that some of the known methods used to produce primitive groups are too computationally intensive at higher degrees and so we implemented several new methods to produce these groups. An example of this is that we developed new techniques to deal with groups of affine type, see Section 3.1. This problem is equivalent to finding all irreducible subgroups of $\mathrm{GL}(k, p)$, for some k and prime p. In particular the groups of degree 3^8 were the most challenging; the method in this case included producing a method to determine whether a group is *semilinear*. This motivated the material that we discuss in Section 2.

In Section 2 we create and describe a test which determines whether a subgroup G of $\mathrm{GL}(d, q)$ is semilinear. We then also give a refined and shorter version of the test. Here a subgroup $G \leq \mathrm{GL}(d, q)$ is semilinear if G is isomorphic to a subgroup of $\Gamma\mathrm{L}(d/e, q^e)$ for some non-trivial divisor e of d (see Definition 2.50).

The possible degrees for which we can classify primitive groups is held back by the groups of affine type. These groups arise at any prime power degree and classifying them for larger degrees becomes increasingly computationally intensive. In Section 4 we produce a general function in MAGMA which, for any integer input d with

$1 \leq d \leq 1000000$, outputs all non-affine primitive groups of degree d.

A *quasiprimitive* permutation group G of degree n is a transitive subgroup of S_n such that every normal subgroup of G is also transitive. We note that every primitive group is also quasiprimitive (as shown in Lemma 1.4).

In Section 5 we produce a classification of the quasiprimitive permutation groups of degree $1 \leq d \leq 3600$. This degree range was chosen because this is the smallest range such that there are examples of every different type of quasiprimitive group (see Theorem 5.1). It has come to our attention that D. Bernhardt has independently classified the quasiprimitive permutation groups up to degree 4096, although this work is currently unpublished and we are unaware of their methods or results.

Finally in Section 6 we tabulate the classifications produced in Sections 3 and 5. We also provide tables that are of use in Section 4.

We will be making heavy and continuous use of the following well known results: the O'Nan-Scott Theorem (1.11), the Classification of the Finite Simple Groups (1.23), Aschbacher's Theorem for general linear groups (1.25), and Praeger's "O'Nan-Scott Theorem" for quasiprimitive groups (5.1), (see [39], [17], [2], and [33] respectively).

We will take p to always be a prime, and q to always be a prime power (of p). We always consider d and n to be positive integers. Every group will be assumed to be finite.

We will be displaying the ideas of our code in the following way throughout:

Procedure name

Input: Our input.
Output: Our desired output.

Step 1: $\cdots$

Step 2: $\cdots$

We note that these procedures are the ideas of the code; some of the details are missing. This was done to aid the clarity of reading. These details do appear in the discussions preceding the code.

1.1. **Group actions and permutation groups.** In this section we give a brief description of group actions, including the definitions of primitive and quasiprimitive groups.

Definition 1.1. Let G be a finite group and Ω a finite set. An *action* of G on Ω is a map $\Omega \times G \to \Omega$ where $(\alpha, g) \mapsto \alpha^g$, satisfying

(i) $\alpha^1 = \alpha$ for all $\alpha \in \Omega$,

(ii) $(\alpha^g)^h = \alpha^{gh}$ for all $\alpha \in \Omega$ and all $g, h \in G$.

The *degree* of this action is $|\Omega|$.

Equivalently an action of G on Ω, where $|\Omega| = n$ can be defined as a group homomorphism $\phi : G \to \mathrm{Sym}(\Omega) \cong S_n$. We write α^g for $\phi(g)$ where $g \in G$ and $\alpha \in \Omega$. Here $\mathrm{Im}(\phi)$, which we denote by G^Ω, is a permutation group on Ω.

We call an action of G on Ω *faithful* if $\ker(\phi) = 1$. So the action is faithful if and only if $G^\Omega \cong G$.

Let $\alpha \in \Omega$, the *orbit* of α under G is the set $\alpha^G := \{\alpha^g \mid g \in G\}$, and the *stabilizer* of α in G is $G_\alpha := \{g \in G \mid \alpha^g = \alpha\}$.

We now state the Orbit-Stabilizer Theorem.

Lemma 1.2. *Let G be a group acting on a finite set Ω and $\alpha \in \Omega$. Then $|\alpha^G| = |G : G_\alpha|$.*

We say that G acts *transitively* on Ω if $\alpha^G = \Omega$ for some, and hence all, $\alpha \in \Omega$. Otherwise we call G *intransitive*. We call a transitive action of G on Ω *regular* if $G_\alpha = 1$ for all $\alpha \in \Omega$.

Definition 1.3. Let G be a group acting transitively on a set Ω. A *block* for the action of G on Ω is a non-empty subset $\emptyset \neq \Delta \subseteq \Omega$ such that for all $g \in G$

$$\Delta^g \cap \Delta = \Delta \text{ or } \Delta^g \cap \Delta = \emptyset.$$

We call Δ *trivial* if $|\Delta| = 1$ or $\Delta = \Omega$.

We call a transitive action of G on Ω *primitive* if the action has no non-trivial blocks. Otherwise we call the action *imprimitive*.

The following is [16, Theorem 1.6A(v)].

Lemma 1.4. *Let G be a group acting primitively on a finite set Ω. Let $H \trianglelefteq G$ be a non-trivial normal subgroup of G, then H acts transitively on Ω.*

This motivates the following definition.

Definition 1.5. Let G be a finite group acting transitively on a finite set Ω, with $|\Omega| > 1$. We say that G is acting *quasiprimitively* if every non-trivial normal subgroup of G acts transitively on Ω.

If $G \leq S_n$ then G has a natural action on $\Omega = \{1, \ldots, n\}$, where each element of G permutes the elements of Ω in the natural way. In this case we call the group G

transitive, *primitive*, or *quasiprimitive* when this action is transitive, primitive, or quasiprimitive respectively.

The following is [16, Corollary 1.5A].

Lemma 1.6. *Let $G \leq S_n$ be transitive, with $n > 1$. Then G is primitive if and only if every point stabilizer G_α of G is a maximal subgroup of G.*

In particular, the study of finite primitive permutation groups is equivalent to the study of (core free) maximal subgroups of finite groups.

Definition 1.7. Let G_1 and G_2 be two groups acting on the sets Ω_1 and Ω_2 respectively. We say that G_1 and G_2 are *permutation isomorphic* if there is a bijection $\lambda : \Omega_1 \to \Omega_2$ and a group isomorphism $\phi : G_1 \to G_2$ such that

$$\lambda(\alpha^g) = \lambda(\alpha)^{\phi(g)}$$

for all $g \in G_1$ and $\alpha \in \Omega_1$. Equivalently two subgroups of S_n are permutation isomorphic if and only if they are conjugate in S_n, see Lemma 1.17.

In Section 3 we classify all primitive permutation groups of degree $4096 \leq d < 8192$ up to permutation isomorphism. In Section 5 we classify all quasiprimitive permutation groups of degree at most 3600 up to permutation isomorphism.

We now define a wreath product as in [16, p.46]. This is in essence a way of combining two groups so that one acts as a permutation group on a direct product of copies of the other.

Lemma 1.8. *Let G be a finite group and let Γ be a finite set of size m. We let G^m denote the direct product of m copies of G and we define $\mathrm{Fun}(\Gamma, G)$ to be the set of all functions $\phi : \Gamma \to G$. Then $\mathrm{Fun}(\Gamma, G)$ is a group under pointwise multiplication, that is*

$$\phi\psi(\gamma) := \phi(\gamma)\psi(\gamma)$$

for all $\phi, \psi \in \mathrm{Fun}(\Gamma, G)$, and all $\gamma \in \Gamma$, with identity $\mathbb{1}$ where $\mathbb{1}(\gamma) = 1_G$ for all $\gamma \in \Gamma$. Furthermore $\mathrm{Fun}(\Gamma, G) \cong G^m$.

Proof. Without loss of generality we write $\Gamma = \{1, \ldots, m\}$.
Closure: We have for any $\phi, \psi \in \mathrm{Fun}(\Gamma, G)$ and for all $\gamma \in \Gamma$ that $\phi\psi(\gamma) = \phi(\gamma)\psi(\gamma) \in G$ and so $\mathrm{Fun}(\Gamma, G)$ is closed under pointwise multiplication.
Associativity: This follows from the associativity of G.
Identity: For any $\phi \in \mathrm{Fun}(\Gamma, G)$ and $\gamma \in \Gamma$, we have that $\phi\mathbb{1}(\gamma) = \phi(\gamma) = \mathbb{1}\phi(\gamma)$.
Inverses: Define the element $\phi^{-1} \in \mathrm{Fun}(\Gamma, G)$ via $\phi^{-1}(\gamma) := (\phi(\gamma))^{-1}$. Then $\phi\phi^{-1}(\gamma) = \mathbb{1}(\gamma) = \phi^{-1}\phi(\gamma)$.
Thus $\mathrm{Fun}(\Gamma, G)$ forms a group under pointwise multiplication.

Consider the map $f : \mathrm{Fun}(\Gamma, G) \to G^m$ defined for all $\phi \in \mathrm{Fun}(\Gamma, G)$, by $f(\phi) := (\phi(1), \ldots, \phi(m))$. Then for all $\phi, \psi \in \mathrm{Fun}(\Gamma, G)$ we have $f(\phi\psi) = (\phi\psi(1), \ldots, \phi\psi(m))$

$= (\phi(1)\psi(1), \ldots, \phi(m)\psi(m)) = (\phi(1), \ldots, \phi(m))(\psi(1), \ldots, \psi(m)) = f(\phi)f(\psi)$ and so f is a homomorphism.

For any element $g = (g_1, \ldots, g_m) \in G^m$ we consider the map $\psi_g \in \mathrm{Fun}(\Gamma, G)$ defined by $\psi_g(i) = g_i$ for $1 \leq i \leq m$. Then $f(\psi_g) = g$ and so f is onto. Let $k \in \ker(f)$, then $f(k) = (1_G, \ldots, 1_G)$, *i.e.* for all $\gamma \in \Gamma$ we have that $k(\gamma) = 1_G$ and so $k = \mathbb{1}$ and the kernel is trivial. Therefore $\mathrm{Fun}(\Gamma, G)$ is isomorphic to G^m. □

Lemma 1.9. *Let G and H be non-trivial finite groups and suppose that H acts on a finite nonempty set $\Gamma = \{1, \ldots, m\}$. For every $\phi \in \mathrm{Fun}(\Gamma, G)$, we define*

$$\phi^h(\gamma) := \phi(\gamma^{h^{-1}})$$

for all $\gamma \in \Gamma$, and $h \in H$ where γ^h is the image of γ under the action of $h \in H$. Then this defines an action of H on $\mathrm{Fun}(\Gamma, G)$.

Proof. We have that $\phi^{1_H}(\gamma) = \phi(\gamma)$ and $\phi^{h_1h_2}(\gamma) = \phi(\gamma^{(h_1h_2)^{-1}}) = \phi(\gamma^{h_2^{-1}h_1^{-1}}) = \phi^{h_1}(\gamma^{h_2^{-1}}) = (\phi^{h_1})^{h_2}(\gamma)$ and so this does define an action. □

Definition 1.10. Let G and H be non-trivial finite groups and suppose that H acts on a finite nonempty set $\Gamma = \{1, \ldots, m\}$. The *wreath product* $G \wr_\Gamma H$ is defined to be the semidirect product

$$G \wr_\Gamma H := \mathrm{Fun}(\Gamma, G) \rtimes H = \{(\phi, h) \mid \phi \in \mathrm{Fun}(\Gamma, G), h \in H\},$$

with multiplication between the pairs (ϕ, h) and (ψ, s) defined as follows:

$$(\phi, h)(\psi, s) = (\phi\psi^{h^{-1}}, hs).$$

We call the subgroup

$$B := \{(\phi, 1_H) \mid \phi \in \mathrm{Fun}(\Gamma, G)\} \cong \mathrm{Fun}(\Gamma, G) \cong G^m$$

the *base group* of the wreath product.

We can identify the base group B with the direct product G^m, via $(\phi, 1_H) \mapsto (\phi(1), \ldots, \phi(m))$ and if we denote $(\phi(1), \ldots, \phi(m))$ by $(b_1, \ldots, b_m)$ then we can see that the action of H on B corresponds to permuting the components of this direct product, *i.e.*

$$(b_1, \ldots, b_m)^{h^{-1}} = (b_{1'}, \ldots, b_{m'})$$

for all $(b_1, \ldots, b_m) \in B$ and $h \in H$ where i' is the image of i under the permutation h.

We may also identify the group $\{(\mathbb{1}, h) \mid h \in H\}$ with the group H. Then the elements (ϕ, h) of $G \wr_\Gamma H$ may be written as products ϕh.

When the elements $(\phi, h) \in G \wr_\Gamma H$ are written as products we now have that

$$h^{-1}\phi h = (\mathbb{1}, h^{-1})(\phi, 1_H)(\mathbb{1}, h) = (\phi^h, h^{-1})(\mathbb{1}, h) = (\phi^h, 1_H) = \phi^h.$$

When the set Γ is clear, for example if H is a permutation group, then we write $G \wr H$ in place of $G \wr_\Gamma H$.

We recall that a group G is *simple* if G contains no non-trivial, proper normal subgroups. A *minimal normal subgroup* of a group G is a non-trivial normal subgroup of G which does not properly contain any other non-trivial normal subgroup of G. The *socle* of a group G, denoted $\mathrm{Soc}(G)$, is the subgroup of G generated by all of the minimal normal subgroups of G.

We now state the O'Nan-Scott Theorem [39] as in [16, Chapter 4]. This is an extremely important result which partitions primitive permutation groups into five disjoint classes. In Sections 3 and 4, we go through each of these classes in turn and find the primitive permutation groups with degrees in our range. The intersection of all pairs of classes is empty, so we do not find any group in more than one class. We give more detailed explanations of the classes in Section 3.

Theorem 1.11. [O'Nan, Scott, and Aschbacher] Let G be a finite primitive group of degree d, and let H be the socle of G. Then $H \cong T^m$ the direct product of m copies of some simple group T. We have two situations, one in which the socle is regular and one in which it is not.

If H is regular then one of the following holds:

(i) *Affine Type:* H is an elementary abelian p-group, $d = p^m$ and we may identify G with a subgroup of the affine group $\mathrm{AGL}(m, p)$ containing the translations. The stabilizer G_α of G is an irreducible subgroup of $\mathrm{GL}(m, p)$. See Section 3.1 for a full description of this type.

(ii) *Regular Non-abelian Type:* H and T are non-abelian, $d = |T|^m$, $m \geq 6$ and the group G can be constructed as a *twisted wreath product*. The stabilizer G_α of G is isomorphic to some transitive subgroup of S_m whose point stabilizers have some composition factor which is isomorphic to T. We refer the reader to [16, Theorem 4.7B] for more information on this type.

If H is not regular, then H and T are non-abelian and one of the following holds:

(iii) *Almost Simple Type:* H is a simple group (*i.e.* $H = T$) and $G \leq \mathrm{Aut}(H)$.

(iv) *Diagonal Type:* $H = T^m$ with $m \geq 2$, $d = |T|^{m-1}$, and G is permutation isomorphic to a subgroup of a wreath product with the diagonal action, which will be described in Section 3.3. This action is of degree $|T|^{m-1}$. The stabilizer satisfies $\mathrm{Inn}(T) \leq G_\alpha \leq \mathrm{Aut}(T) \times S_m$.

(v) *Product Type:* $H = T^m$ with $m = rs$ and $s > 1$. There is a primitive non-regular group U which has the socle T^r and is of type (iii) or (iv) such that G is permutation isomorphic to a subgroup of the wreath product $U \wr S_s$ with the product action, which will be defined in Section 3.4. The degree d of G in this case is $(d_U)^s$ where d_U is the degree of U.

We now give some additional background results which we will refer to in later sections.

Definition 1.12. Let G be a group and let H be a subgroup of G. For any $g \in G$ we denote $g^{-1}Hg$ by H^g. The *normalizer* of H in G is defined to be

$$N_G(H) := \{g \in G \mid H^g = H\}.$$

The following are well known.

Lemma 1.13. *Let G be a group and let H be a subgroup of G. Then for any $g \in G$ we have $N_G(H^g) = N_G(H)^g$.*

Proof. Take any $x \in N_G(H^g)$. Then $(H^g)^x = H^g$ if and only if $H^{gxg^{-1}} = H$. In this case $x^{g^{-1}} \in N_G(H)$ and so $x \in N_G(H)^g$. Following the same argument backwards we see that if $x \in N_G(H)^g$ then $x \in N_G(H^g)$. □

Lemma 1.14. *Let $G \leq \mathrm{Sym}(\Omega)$ and let $\alpha \in \Omega$. Let $N \trianglelefteq G$ be a regular normal subgroup of G, then $G = N \rtimes G_\alpha$.*

Proof. We take any $g \in G$. By the transitivity of N there exists some $n \in N$ such that $\alpha^g = \alpha^n$. Therefore $y := gn^{-1} \in G_\alpha$. Furthermore $g = yn$ which implies that $g \in G_\alpha N$. Hence $G = G_\alpha N$. Since N is a normal subgroup of G we have that $G_\alpha N = NG_\alpha$ and so $G = NG_\alpha$. The intersection $G_\alpha \cap N = N_\alpha$ and since N is regular we have that $N_\alpha = \mathrm{Id}_G$. Hence $G = N \rtimes G_\alpha$. □

Lemma 1.15. *Let G be a finite group acting transitively on a finite set Ω. Then $|\Omega|$ divides $|G|$.*

Proof. Let $\alpha \in \Omega$. Then the orbit of α in G is Ω. The set Ω is finite and so by the Orbit-Stabilizer Theorem $|\Omega| = |G : G_\alpha|$ and so $|\Omega|$ divides $|G|$. □

The following is [26, Kapitel II, Satz 1.3].

Lemma 1.16. *Let G be a finite group acting transitively on a set Ω. If $|\Omega|$ is prime, then G is acts primitively on Ω.*

The following are well known.

Lemma 1.17. *Let G and H be groups with $G, H \leq \mathrm{Sym}(\Omega)$. Then G and H are permutation isomorphic if and only if they are conjugate in $\mathrm{Sym}(\Omega)$.*

Proof. ($\Rightarrow$): Let G and H be permutation isomorphic. Then there exists some $\lambda \in \mathrm{Sym}(\Omega)$ (a bijection $\Omega \to \Omega$) and an isomorphism $\phi : G \to H$ such that, for any $\alpha \in \Omega$ and $g \in G$ we have

$$(\alpha^g)^\lambda = (\alpha^\lambda)^{g\phi}.$$

We take any $\alpha \in \Omega$ and set $\beta := \alpha^{\lambda^{-1}}$. Then

$$(\beta^g)^\lambda = (\beta^\lambda)^{g\phi}$$
$$((\alpha^{\lambda^{-1}})^g)^\lambda = (\alpha^{\lambda^{-1}\lambda})^{g\phi}$$
$$\alpha^{\lambda^{-1}g\lambda} = \alpha^{g\phi}$$

thus $g\phi = \lambda^{-1}g\lambda$. Hence $G\phi = \lambda^{-1}G\lambda = H$ and so G and H are conjugate in $\mathrm{Sym}(\Omega)$.

($\Leftarrow$): Let G and H be conjugate in $\mathrm{Sym}(\Omega)$. Let $\lambda \in \mathrm{Sym}(\Omega)$ be such that $H = \lambda^{-1}G\lambda$ and define the isomorphism $\phi : G \to H$ via $\phi : g \mapsto \lambda^{-1}g\lambda$. Then for any $\alpha \in \Omega$ and $g \in G$ we have

$$(\alpha^g)^\lambda = ((\alpha^{\lambda\lambda^{-1}})^g)^\lambda = (\alpha^\lambda)^{\lambda^{-1}g\lambda} = (\alpha^\lambda)^{g\phi}.$$

Therefore G and H are permutation isomorphic. □

Lemma 1.18. *Let G act transitively on a set Ω. Then this action is permutation isomorphic to the action of G on the right cosets of the subgroup $H = G_\alpha$ of G, for some $\alpha \in \Omega$.*

Proof. Fix $\alpha \in \Omega$ and take $H = G_\alpha$. Define a map $\lambda : \{Hg : g \in G\} \to \Omega$ via $\lambda(Hg) = \alpha^g$. Then λ is well defined as $Hg_1 = Hg_2$ implies that $g_1 = hg_2$ for some $h \in H$, so $\alpha^{g_1} = \alpha^{hg_2} = \alpha^{g_2}$. Furthermore λ is surjective as G is acting transitively on Ω and λ is injective as $\lambda(Hg_1) = \lambda(Hg_2)$ implies that $\alpha^{g_1} = \alpha^{g_2}$, in this case $g_1g_2^{-1} \in H$ and so $Hg_1 = Hg_2$. Thus λ is a bijective function.

For any g_1, g_2 in G we have that $\lambda((Hg_1)^{g_2}) = \lambda(Hg_2g_2) = \alpha^{g_1g_2} = (\alpha^{g_1})^{g_2} = \lambda(Hg_1)^{g_2}$ and so the two actions are permutation isomorphic. □

Definition 1.19. Let $G \leq \mathrm{Sym}(\Omega)$ and $n \geq 1$. We say that G is *n-transitive* if $|\Omega| \geq n$ and for any distinct $\alpha_1, \ldots, \alpha_n \in \Omega$ and any distinct $\beta_1, \ldots, \beta_n \in \Omega$ there exists $g \in G$ such that

$$\alpha_i^g = \beta_i \text{ for } 1 \leq i \leq n.$$

Lemma 1.20. *Let $G \leq \mathrm{Sym}(\Omega)$ be a 2-transitive group. Then G is a primitive group.*

Proof. Suppose that $\Delta \subset \Omega$ is a non-trivial block for G. Then $|\Delta| > 1$ and so we may take $\alpha, \beta \in \Delta$ with $\alpha \neq \beta$. Let $\gamma \in \Omega \setminus \{\alpha\}$. As G is 2-transitive, there exists an element $g \in G$ with $\alpha^g = \alpha$ and $\beta^g = \gamma$. Then $\alpha^g = \alpha$ implies that $\alpha \in \Delta \cap \Delta^g$ and so $\Delta = \Delta^g$ as Δ is a block. However $\gamma = \beta^g \in \Delta^g$ implies that $\gamma \in \Delta$ and so $\Omega = \Delta$. This is a contradiction and so G is primitive. □

The following lemma is stated in [16, p.48].

Lemma 1.21. *Let G and H be non-trivial finite groups acting on finite sets Δ and $\Gamma = \{1, \ldots, m\}$, respectively. Then the wreath product $G \wr_\Gamma H$ acts on the set $\Delta \times \Gamma$ in the following way:*

$$(\delta, \gamma)^{\phi h} = (\delta^{\phi(\gamma)}, \gamma^h)$$

for all $(\delta, \gamma) \in \Delta \times \Gamma$ and all $\phi \in \mathrm{Fun}(\Gamma, G)$ and $h \in H$.

This action has a system of blocks of the form $\Delta \times \{\gamma\}$, for each $\gamma \in \Gamma$. Furthermore $G \wr_\Gamma H$ acts transitively on $\Delta \times \Gamma$ if and only if G and H act transitively on Δ and Γ, respectively. In this case the action of $G \wr_\Gamma H$ on $\Delta \times \Gamma$ is imprimitive.

Proof. We consider the identity element $\mathbb{1}1_H$ of $G \wr_\Gamma H$ and take any element $(\delta, \gamma) \in \Delta \times \Gamma$. We have that $(\delta, \gamma)^{\mathbb{1}1_H} = (\delta^{\mathbb{1}(\gamma)}, \gamma^{1_H}) = (\delta, \gamma)$.

We now take any elements $\phi_1 h_1, \phi_2 h_2 \in G \wr_\Gamma H$, so $\phi_1, \phi_2 \in \mathrm{Fun}(\Gamma, G)$ and $h_1, h_2 \in H$. We then have for any $(\delta, \gamma) \in \Delta \times \Gamma$ that

$$\begin{aligned}(\delta, \gamma)^{(\phi_1 h_1)(\phi_2 h_2)} &= (\delta, \gamma)^{\phi_1 \phi_2^{h_1^{-1}} h_1 h_2} = (\delta^{(\phi_1 \phi_2^{h_1^{-1}}(\gamma))}, \gamma^{h_1 h_2}) = (\delta^{\phi_1(\gamma)\phi_2(\gamma^{h_1})}, \gamma^{h_1 h_2}) \\ &= (\delta^{\phi_1(\gamma)}, \gamma^{h_1})^{\phi_2 h_2} = ((\delta, \gamma)^{\phi_1 h_1})^{\phi_2 h_2}.\end{aligned}$$

Hence $G \wr_\Gamma H$ acts on $\Delta \times \Gamma$ as described.

We now take any $\gamma \in \Gamma$ and we consider the set $\mathcal{B}_\gamma := \{(\delta, \gamma) : \delta \in \Delta\}$. Then for any element $(\delta, \gamma) \in \mathcal{B}_\gamma$ and every $\phi h \in G \wr_\Gamma H$ we have $(\delta, \gamma)^{\phi h} = (\delta^{\phi(\gamma)}, \gamma^h)$. Therefore $\mathcal{B}_\gamma^{\phi h} = \{(\delta^{\phi(\gamma)}, \gamma^h) : \delta \in \Delta\}$ and so $\mathcal{B}_\gamma^{\phi h} = \mathcal{B}_\gamma$ if $\gamma^h = \gamma$ and $\mathcal{B}_\gamma^{\phi h} \cap \mathcal{B}_\gamma = \emptyset$ in all other cases. Thus $\mathcal{B}_\gamma$ is a block for the action of $G \wr_\Gamma H$ on $\Delta \times \Gamma$. We can observe that the collection of all $\mathcal{B}_\gamma$, for each $\gamma \in \Gamma$, partitions the set $\Delta \times \Gamma$.

We consider any two elements $(\delta_1, \gamma_1), (\delta_2, \gamma_2) \in \Delta \times \Gamma$. Then $G \wr_\Gamma H$ is transitive on $\Delta \times \Gamma$ if there exists some $\phi h \in G \wr_\Gamma H$ with $(\delta_1, \gamma_1)^{\phi h} = (\delta_2, \gamma_2)$. In particular we require $\delta_1^{\phi(\gamma_1)} = \delta_2$ and $\gamma_1^h = \gamma_2$. This is satisfied if and only if G and H are acting transitively on Δ and Γ respectively. □

The following result is given in [31, 22.11, p.45].

Lemma 1.22. *Let G, P and H be non-trivial groups with H acting on a finite set $\Gamma = \{1, \ldots, m\}$ and let $\rho : G \to P$ be an epimorphism of G onto P. We let $G \wr_\Gamma H$ and $P \wr_\Gamma H$ be wreath products defined via the same action of H on Γ. We define $^* : \mathrm{Fun}(\Gamma, G) \to \mathrm{Fun}(\Gamma, P)$ by $\phi^*(\gamma) := \phi(\gamma)\rho$, for all $\gamma \in \Gamma$, $\phi \in \mathrm{Fun}(\Gamma, G)$. Then the map $\psi : G \wr_\Gamma H \to P \wr_\Gamma H$ defined by $(\phi h)\psi = \phi^* h$, for all $\phi h \in G \wr_\Gamma H$, is an epimorphism.*

Proof. We observe that $\psi : G \wr_\Gamma H \to P \wr_\Gamma H$ is a surjection as every element of $P \wr_\Gamma H$ is of the form $\phi_P h$ where $\phi_P \in \mathrm{Fun}(\Gamma, P)$, $h \in H$, and any element of $\mathrm{Fun}(\Gamma, P)$ can be produced via the map * as ρ is surjective.

We note that for all $\phi_1, \phi_2 \in \mathrm{Fun}(\Gamma, G)$ and for all $\gamma \in \Gamma$, we have $(\phi_1\phi_2)^*(\gamma) = (\phi_1\phi_2(\gamma))\rho = (\phi_1(\gamma)\phi_2(\gamma))\rho = (\phi_1(\gamma))\rho(\phi_2(\gamma))\rho = \phi_1^*(\gamma)\phi_2^*(\gamma) = \phi_1^*\phi_2^*(\gamma)$. Also, for all $h \in H, \gamma \in \Gamma$ and $\phi \in \mathrm{Fun}(\Gamma, G)$ we have that $(\phi^h)^*(\gamma) = (\phi^h(\gamma))\rho = (\phi(\gamma^{h^{-1}}))\rho = \phi^*(\gamma^{h^{-1}}) = (\phi^*)^h(\gamma)$.

We now take $\phi_1 h_1, \phi_2 h_2 \in G \wr_\Gamma H$, then $(\phi_1 h_1 \phi_2 h_2)\psi = (\phi_1 \phi_2^{h_1^{-1}} h_1 h_2)\psi = (\phi_1 \phi_2^{h_1^{-1}})^* h_1 h_2 = \phi_1^* (\phi_2^*)^{h_1^{-1}} h_1 h_2 = (\phi_1^* h_1)(\phi_2^* h_2) = (\phi_1 h_1)\psi(\phi_2 h_2)\psi$.

Hence $\psi : G \wr_\Gamma H \to P \wr_\Gamma H$ is a homomorphism and so an epimorphism. □

1.2. **Simple groups.** The following theorem is one of the most important and influential theorems in finite group theory. For more information see for example [17]. We will make significant use of this theorem in Sections 3.2, 4.1, and 5.1.

Theorem 1.23 (The Classification of the Finite Simple Groups)**.** *Let G be a finite simple group. Then G is isomorphic to a group which lies in at least one of the following classes.*

- *The cyclic groups C_p of prime order p.*
- *The alternating groups A_n for $n \geq 5$.*
- *The simple groups of Lie type (classical and exceptional groups).*
- *The 26 sporadic groups.*

We denote the simple classical groups as in the $\mathbb{ATLAS}$ [12]. We refer the reader to [44, Chapter 3] for a complete description of these groups. Let q be a prime power and n, m positive integers. The linear groups are denoted by $\mathrm{L}_n(q)$, the symplectic groups are denoted by $\mathrm{S}_{2m}(q)$, the unitary groups are denoted by $\mathrm{U}_n(q)$, the orthogonal groups in odd dimension are denoted by $\mathrm{P}\Omega_{2m+1}(q)$, and the orthogonal groups in even dimension are denoted by $\mathrm{P}\Omega^\epsilon_{2m}(q)$ where $\epsilon \in \{+, -\}$.

Using the notation from the $\mathbb{ATLAS}$ (see [12]), the exceptional groups are:

$$E_6(q), E_7(q), E_8(q), F_4(q), G_2(q), {}^2B_2(2^{2m+1}) = \mathrm{Sz}(2^{2m+1}),$$
$${}^3D_4(q), {}^2E_6(q), {}^2F_4(2^{2m+1}), {}^2G_2(3^{2m+1})$$

where q is a power of a prime and m is a non-negative integer. We refer the reader to [44, Chapter 4] for a complete description of these groups.

Furthermore the 26 sporadic simple groups are:

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, \mathrm{HS}, J_2, \mathrm{Co}_1, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{McL}, \mathrm{Suz}, \mathrm{He},$$
$$\mathrm{HN}, \mathrm{Th}, \mathrm{Fi}_{22}, \mathrm{Fi}_{23}, \mathrm{Fi}_{24}', \mathrm{B}, \mathrm{M}, J_1, \mathrm{O'N}, J_3, \mathrm{Ru}, J_4, \mathrm{Ly}.$$

We refer the reader to [44, Chapter 5] for a complete description of these groups.

The following is well known, see for example [28, Theorem 2.1.3], [28, Proposition 2.9.1], and [17, Vol. 3 Theorem 2.2.10].

Theorem 1.24. *The list below includes all isomorphisms between pairs of alternating, classical, and exceptional groups.*

$\mathrm{U}_2(q) \cong \mathrm{S}_2(q) \cong \mathrm{L}_2(q)$, $\mathrm{L}_3(2) \cong \mathrm{L}_2(7)$, $\mathrm{L}_2(4) \cong \mathrm{L}_2(5) \cong A_5$,
$\mathrm{L}_2(9) \cong \mathrm{S}_4(2)' \cong A_6$, $\mathrm{L}_4(2) \cong A_8$, $\mathrm{U}_4(2) \cong \mathrm{S}_4(3)$,
$\mathrm{P}\Omega_{2m+1}(2^i) \cong \mathrm{S}_{2m}(2^i), i > 1$, $\mathrm{P}\Omega_3(q) \cong \mathrm{L}_2(q), q$ *odd*, $\mathrm{P}\Omega_5(q) \cong \mathrm{S}_4(q), q$ *odd*,
$\mathrm{P}\Omega_4^-(q) \cong \mathrm{L}_2(q^2)$, $\mathrm{P}\Omega_6^+(q) \cong \mathrm{L}_4(q)$, $\mathrm{P}\Omega_6^-(q) \cong \mathrm{U}_4(q)$,
$G_2(2)' \cong \mathrm{U}_3(3)$, ${}^2G_2(3)' \cong \mathrm{L}_2(8)$.

Let G be a classical group. Then G is simple with the following exceptions: $G \cong \mathrm{L}_2(q)$ for $q \leq 3$, $G \cong \mathrm{P}\Omega_2^{\pm}(q)$, $G \cong \mathrm{S}_4(2)$, $G \cong \mathrm{P}\Omega_4^+(q)$, or $G \cong \mathrm{U}_3(2)$.
Let G be an exceptional group. Then G is simple with the following exceptions: $G \cong G_2(2)$, $G \cong \mathrm{Sz}(2)$, $G \cong {}^2F_4(2)$, or $G \cong {}^2G_2(3)$.
Furthermore the group ${}^2F_4(2)'$ is simple, (this group will be considered as an exceptional group from now on).

We shall always treat groups as the right hand side of the above isomorphisms.

1.3. **Some representation theory.** Throughout this thesis we will be making heavy use of Aschbacher's Theorem [2]. We reproduce a version of this theorem here, using [22] and [30].

Theorem 1.25 (Aschbacher)**.** *Let G be a subgroup of $\mathrm{GL}(d,q)$ and $V = \mathbb{F}_q^d$ be the underlying vector space upon which G acts. Let $Z \leq G$ denote the subgroup of scalar matrices, that is $Z = Z(\mathrm{GL}(d,q)) \cap G$. Then at least one of the following is true:*

(i) **Reducible groups:** *G acts reducibly on V. That is, G preserves a proper non-zero subspace of V.*

(ii) **Imprimitive groups:** *G acts imprimitively on V. That is G preserves a decomposition of V as a direct sum $V_1 \oplus \cdots \oplus V_r$ of $r > 1$ subspaces of dimension s, which are permuted transitively by G and so $G \subseteq \mathrm{GL}(s,q) \wr S_r$.*

(iii) **Semilinear groups:** *G acts on V as a group of semilinear automorphisms of a d/e-dimensional space over the extension field $\mathbb{F}_{q^e}$, for some $e > 1$, so G embeds in $\Gamma\mathrm{L}(d/e, q^e)$. (See Section 2 for more details).*

(iv) **Simple tensor products:** *G preserves a decomposition of V as a tensor product $U \otimes W$ of spaces of dimensions $r, s > 1$ over $\mathbb{F}_q$. Then G is a subgroup of the central product of $\mathrm{GL}(r,q)$ and $\mathrm{GL}(s,q)$. More precisely $G/Z \subseteq \mathrm{PGL}(r,q) \times \mathrm{PGL}(s,q)$.*

(v) **Groups defined over a proper subfield modulo scalars:** *Modulo Z, G is conjugate to a subgroup of $\mathrm{GL}(d,q')$, for some proper subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$, that is $G^g \subseteq \mathrm{GL}(d,q').Z$ for some $g \in \mathrm{GL}(d,q)$.*

(vi) **Groups of extraspecial or symplectic type:** *For some prime r, $d = r^m$ and G is contained in the normalizer of an r-group R, of order either r^{2m+1} or 2^{2m+2}. Either R is extraspecial (in the first case) or R is a 2-group of*

symplectic type, that is, a central product of an extraspecial 2-group with a cyclic group of order 4.

(vii) **Wreathed tensor products or tensor induced groups:** *G preserves a decomposition of V as a symmetric tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_m$ of spaces all of dimension $r > 1$ over $\mathbb{F}_q$, where $d = r^m$. The components of the product are permuted by G, and so G is an amalgamated wreath product of a subgroup of $\mathrm{GL}(r, q)$ by a subgroup of S_m. More precisely, $G/Z \subseteq \mathrm{PGL}(r, q) \wr S_m$.*

(viii) **Groups of classical type:** *G is contained in the normalizer of a quasisimple classical group in its natural representation. (G/Z contains the derived subgroup of $\mathrm{PGO}(d, q)$, $\mathrm{PGSp}(d, q)$, $\mathrm{PGU}(d, q)$ or $\mathrm{PGL}(d, q)$ and G itself is a subgroup of $\mathrm{GO}(d, q)Z$, $\mathrm{GSp}(d, q)Z$, $\mathrm{GU}(d, q)Z$ or $\mathrm{GL}(d, q)Z$ respectively.)*

(ix) **Other almost simple groups modulo scalars:** *$T \subset G/Z \subseteq \mathrm{Aut}(T)$, for some non-abelian simple $T = G_0/Z$ for some subgroup G_0 of G.*

Aschbacher's theorem will be used in the most computationally intensive part of the classification; finding the primitive groups of affine type. (See Section 3.1).

Definition 1.26. We say that a group $G \leq \mathrm{GL}(d, q)$ is *irreducible* if it is not reducible, *i.e.* if V is the underlying d-dimensional vector space over $\mathbb{F}_q$ then G does not preserve a proper non-zero subspace of V.

Definition 1.27. We say that a group $G \leq \mathrm{GL}(d, q)$ is *absolutely irreducible* if the image of G under the natural embedding $G \to \mathrm{GL}(d, q^e)$ is irreducible for all e.

We will be considering irreducible groups which are not necessarily absolutely irreducible in more detail in Section 2.

The following definition is found in [1, p.452].

Definition 1.28. Let G be a finite group, $\mathbb{F}$ a field and V a finite dimensional $\mathbb{F}G$-module. If W is an $\mathbb{F}G$-submodule of V then we define the *quotient module* V/W as

$$V/W := \{W + v \mid v \in V\}.$$

This has the structure of an $\mathbb{F}G$-module with the action defined, for $W + v \in V/W$ and $g \in G$ by

$$(W + v)^g = W + v^g.$$

The following is described in [18, p.75]

Definition 1.29. Let G be a group and let V and W be G-modules over the field $\mathbb{F}$ ($\mathbb{F}G$-modules). Then a map $\phi : V \to W$ is a G-homomorphism if for all $v_1, v_2 \in V$, $a_1, a_2 \in \mathbb{F}$, and $g \in G$ we have

$$(a_1 v_1 + a_2 v_2)\phi = a_1(v_1)\phi + a_2(v_2)\phi,$$
$$(v_1^g)\phi = (v_1\phi)^g.$$

We denote the set of all G-homomorphisms of V into W by $\mathrm{Hom}_G(V, W)$.

Lemma 1.30. *Let $V = \mathbb{F}_q^d$ and $G \leq \mathrm{GL}(d,q)$. Then $\mathrm{Hom}_G(V,V)$ can be identified with $C_{\mathrm{M}(d,q)}(G)$.*

Proof. This follows directly from the definition. □

We now collect together some well known results on G-modules, as seen in [1, p.452].

Proposition 1.31. *Let G be a finite group, $\mathbb{F}$ a field, V a finite dimensional $\mathbb{F}G$-module, and W a submodule of V.*

(i) **The First Isomorphism Theorem for Modules**. *Let $\phi : V \to V'$ be an $\mathbb{F}G$-module homomorphism. Then $V/\ker(\phi) \cong \mathrm{Im}(\phi)$.*

(ii) **The Correspondence Theorem for Modules**. *There is a bijective correspondence between the submodules of V/W and the submodules of V which contain W.*

(iii) W is a maximal submodule of V if and only if V/W is irreducible.

The following result is well known, see for example [1, Corollary 4.15].

Lemma 1.32. *Let V and W be finite dimensional vector spaces over the same field. Then V is isomorphic to W if and only if $\dim(V) = \dim(W)$.*

The following result is well known.

Lemma 1.33. *Let V be a finite dimensional vector space over a finite field of prime order, $\mathbb{F}_p$. Let $(V,+)$ denote the additive group of V. Then*

$$\mathrm{Aut}((V,+)) = \mathrm{GL}(V).$$

Proof. We observe that any element of $\mathrm{GL}(V)$ is an automorphism of $(V,+)$ so $\mathrm{GL}(V) \subseteq \mathrm{Aut}((V,+))$. Let $f \in \mathrm{Aut}((V,+))$ then $f : V \to V$ and for all $v, u \in V$, $f(v+u) = f(v)+f(u)$. We let $\lambda \in \mathbb{F}_p$, then as $\mathbb{F}_p$ is of prime order we may think of the elements of $\mathbb{F}_p$ as the integers $\{0, 1, \ldots, p-1\}$. We then have that $\lambda v = v + v \cdots + v$ (v added to itself λ times) and so $f(\lambda v) = f(v + \cdots + v) = f(v) + \cdots + f(v) = \lambda f(v)$ and so $f \in \mathrm{GL}(V)$. Hence $\mathrm{Aut}((V,+)) = \mathrm{GL}(V)$. □

Let $\mathbb{F}$ be a finite field. Recall that an element α of an extension of $\mathbb{F}$ is *algebraic* over $\mathbb{F}$ if there exists a non-zero polynomial m, with coefficients in $\mathbb{F}$, such that $m(\alpha) = 0$. The following result is [1, Proposition 2.6, p.495].

Proposition 1.34. *Suppose that α is algebraic over a field $\mathbb{F}$, and let $m(x)$ be its minimal polynomial over $\mathbb{F}$. The map $\mathbb{F}[x]/(m) \to \mathbb{F}[\alpha]$ is an isomorphism, and $\mathbb{F}[\alpha]$ is a field. Thus $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$ (here $\mathbb{F}[\alpha]$ denotes the polynomial ring in α over $\mathbb{F}$ and $\mathbb{F}(\alpha)$ denotes the smallest field containing $\mathbb{F}$ and α).*

The following lemma is given in [28, Lemma 2.10.1]. This is often used as an alternate definition of absolute irreducibility.

Lemma 1.35. *Let V be a vector space over the field $\mathbb{F}$. Let $G \leq \mathrm{GL}(V, \mathbb{F})$ act irreducibly on V. Then G acts* absolutely irreducibly *on V if and only if $C_{\mathrm{GL}(V,\mathbb{F})}(G) = \mathbb{F}^*$; the scalar subgroup of $\mathrm{GL}(V, \mathbb{F})$.*

The following result is [18, Chapter 3, Theorems 5.1, 5.2].

Theorem 1.36. *Let V be a G-module over the field $\mathbb{F}$, then $\mathrm{Hom}_G(V, V)$ is a finite dimensional algebra over $\mathbb{F}$. If V is an irreducible G-module then $\mathrm{Hom}_G(V, V)$ is a division algebra with $\mathbb{F}$ in its centre. In particular, every non-zero element of $\mathrm{Hom}_G(V, V)$ is a G-isomorphism.*

In other words the endomorphism ring, $\mathrm{Hom}_G(V, V)$, of an irreducible representation is a division ring.

The following theorem is [18, Chapter 3, Theorem 5.4].

Theorem 1.37. *Let G be a group acting on the vector space V over the field $\mathbb{F}$, such that V decomposes as the direct sum of (pairwise) isomorphic G-modules, $V = V_1 \oplus \cdots \oplus V_t$. Then we have*

(i) $\mathrm{Hom}_G(V_1, V_1)$ *and* $\mathrm{Hom}_G(V_i, V_j)$ *are G-isomorphic for all $1 \leq i, j \leq t$.*

(ii) $\mathrm{Hom}_G(V_i, V)$ *and* $\mathrm{Hom}_G(V_i, V_1) \oplus \cdots \oplus \mathrm{Hom}_G(V_i, V_t)$ *are G-isomorphic for all $1 \leq i \leq t$.*

(iii) If $\mathrm{Hom}_G(V_1, V_1) = \mathbb{F}$ *then* $\mathrm{Hom}_G(V, V)$ *is isomorphic to the algebra of all $t \times t$ matrices over $\mathbb{F}$.*

We follow similar arguments to the proof of Theorem 1.37 (iii) to find the following result.

Lemma 1.38. *Let G be a group acting on the vector space V over the field $\mathbb{F}_q$, so that V decomposes as the direct sum of (pairwise) isomorphic G-modules, $V = V_1 \oplus \cdots \oplus V_t$. Let $\mathbb{F}_{q^k}$ be an extension field of $\mathbb{F}_q$. If $\mathrm{Hom}_G(V_1, V_1) = \mathbb{F}_{q^k}$ then $\mathrm{Hom}_G(V, V)$ is isomorphic to the ring of all $t \times t$ matrices over $\mathbb{F}_{q^k}$.*

Proof. We note by Theorem 1.37 (i), that $\mathrm{Hom}_G(V_1, V_1) = \mathbb{F}_{q^k}$ implies that $\mathrm{Hom}_G(V_i, V_j) = \mathbb{F}_{q^k}$ for all $1 \leq i, j \leq t$.

For $1 \leq i \leq t$, we define $\rho_i \in \mathrm{Hom}_G(V_i, V)$ to be the natural embedding of V_i into V and we let $\pi_i \in \mathrm{Hom}_G(V, V_i)$ be the projection map of V onto V_i. Then the following relations hold (composing left to right):

$$\rho_i \pi_i = 1_i, \text{ and } \rho_i \pi_j = 0_{i,j} \text{ for } i \neq j, \qquad (*)$$

where 1_i is the identity element of $\mathrm{Hom}_G(V_i, V_i)$ and $0_{i,j}$ is the zero element of $\mathrm{Hom}_G(V_i, V_j)$. Furthermore

$$\sum_{i=1}^{t} \pi_i \rho_i = 1 \qquad (**)$$

where 1 is the identity element of $\mathrm{Hom}_G(V,V)$.

For $\phi \in \mathrm{Hom}_G(V,V)$ we define the element $\phi_{i,j} := \rho_i \phi \pi_j \in \mathrm{Hom}_G(V_i, V_j)$, so $\phi_{i,j}$ lies in $\mathbb{F}_{q^k}$. Therefore $(\phi_{i,j})$ (for all choices of $1 \leq i,j \leq t$) is a $t \times t$ matrix over $\mathbb{F}_{q^k}$.

We let $\mathrm{M}(t, q^k)$ denote the ring of all $t \times t$ matrices over $\mathbb{F}_{q^k}$. We may now define a mapping $\beta : \mathrm{Hom}_G(V,V) \to \mathrm{M}(t,q^k)$ by $\phi\beta = (\phi_{i,j})$.

We now demonstrate that this is a ring homomorphism. The maps ρ_i and π_j are linear transformations, so it follows that, for all $\phi, \psi \in \mathrm{Hom}_G(V,V)$ we have

$$(\phi+\psi)\beta = ((\phi+\psi)_{i,j}) = (\rho_i(\phi+\psi)\pi_j) = (\rho_i\phi\pi_j + \rho_i\psi\pi_j) = (\phi_{i,j} + \psi_{i,j}) = \phi\beta + \psi\beta$$

and by $(**)$ we have that

$$\begin{aligned}(\phi\psi)\beta = ((\phi\psi)_{i,j}) = (\rho_i(\phi\psi)\pi_j) &\overset{(**)}{=} \left(\rho_i\phi\left(\sum_{n=1}^{t}\pi_n\rho_n\right)\psi\pi_j\right) \\ &= \left(\sum_{n=1}^{t}(\rho_i\phi\pi_n)(\rho_n\psi\pi_j)\right) = \left(\sum_{n=1}^{t}\phi_{i,n}\psi_{n,j}\right).\end{aligned}$$

By the definition of matrix multiplication, for any $1 \leq l,m \leq t$ we have that

$$\left(\sum_{n=1}^{t}\phi_{i,n}\psi_{n,j}\right)_{l,m} = \left(\left(\phi_{i,j}\right)\left(\psi_{i,j}\right)\right)_{l,m}$$

and so

$$((\phi\psi)\beta) = (\phi\beta)(\psi\beta).$$

By $(*)$, we have that

$$1\beta = (\rho_i 1 \pi_j) \overset{(*)}{=} \mathrm{Id}_t.$$

Therefore $\beta : \mathrm{Hom}_G(V,V) \to \mathrm{M}(t,q^k)$ is a ring homomorphism. We now show that β is an isomorphism.

Let $(a_{i,j})$ be an element of $\mathrm{M}(t,q^k)$, so $a_{i,j} \in \mathbb{F}_{q^k} = \mathrm{Hom}(V_i, V_j)$. We set $\phi \in \mathrm{Hom}_G(V,V)$ to be

$$\phi := \sum_{n,m=1}^{t}\pi_n a_{n,m}\rho_m.$$

Then by $(*)$, we have, for any choice of $1 \leq i,j \leq t$ that

$$\phi_{i,j} = \rho_i\phi\pi_j = \rho_i\left(\sum_{n,m=1}^{t}\pi_n a_{n,m}\rho_m\right)\pi_j \overset{(*)}{=} a_{i,j}.$$

Therefore $\phi\beta = (a_{i,j})$ and so β is surjective.

It remains to show that β is injective. We suppose that $\phi\beta = (0)$ for some $\phi \in \mathrm{Hom}_G(V,V)$. By $(**)$, and as 1 is the identity of $\mathrm{Hom}_G(V,V)$, we have that

$$\phi = 1\phi 1 \overset{(**)}{=} \left(\sum_{i=1}^{t} \pi_i\rho_i\right) \phi \left(\sum_{j=1}^{t} \pi_j\rho_j\right) = \sum_{i,j=1}^{t} \pi_i(\rho_i\phi\pi_j)\rho_j.$$

By our assumption ($\phi\beta = 0$), we have that $\phi_{i,j} = \rho_i\phi\pi_j = 0$ for all i, j. Hence $\phi = 0$. Thus β is an injection and $\mathrm{Hom}_G(V,V)$ is isomorphic to $\mathrm{M}(t, q^k)$. □

The following theorem is a well known result of Wedderburn [32].

Theorem 1.39. *Every finite division ring is a field.*

The following is Schur's Lemma.

Lemma 1.40 (Schur's Lemma)**.** *Let G be a group and let $\rho_1 : G \to \mathrm{GL}(V_1)$ and $\rho_2 : G \to \mathrm{GL}(V_2)$ be two irreducible representations of G over the same field $\mathbb{F}$. Let $T : V_1 \to V_2$ be a linear map such that $\rho_2(g)T = T\rho_1(g)$ for all $g \in G$. Then:*

(i) if ρ_1 and ρ_2 are not isomorphic, then $T = 0$.

(ii) if $V_1 = V_2$ and $\rho_1 = \rho_2$ is absolutely irreducible, then T is a scalar multiple of the identity.

The following result is [14, Theorem 29.7, p.200].

Theorem 1.41. *Let G be a finite group, $\mathbb{F}$ a finite field, and V_1, V_2 be $\mathbb{F}G$-modules. Extend $\mathbb{F}$ to an algebraically closed field $\bar{\mathbb{F}}$. If V_1 and V_2 are non-isomorphic $\mathbb{F}G$-modules then V_1 and V_2 are non-isomorphic $\bar{\mathbb{F}}G$-modules.*

The following result is taken from [24, p.50] and follows from Theorem 1.36 and Theorem 1.39.

Lemma 1.42. *Let G be a finite group, $\mathbb{F}_q$ a finite field and V an irreducible $\mathbb{F}_qG$-module. Then $\mathrm{End}_{\mathbb{F}_qG}(V) = \mathrm{Hom}_G(V,V)$ is a field, and is isomorphic to $\mathbb{F}_{q^k}$ for some $k \geq 1$.*

The following is [18, p.64].

Definition 1.43. Let G be a finite group. We call a field $\mathbb{F}$ a *splitting field* for G if every irreducible representation of G on a vector space V over $\mathbb{F}$ is absolutely irreducible.

The following result is [18, Corollary 5.8, Chapter 3] and follows from Schur's Lemma.

Lemma 1.44. *Let G be a group, $\mathbb{F}$ a field, and V an irreducible $\mathbb{F}G$-module. If $\mathbb{F}$ is a splitting field for G then $\mathrm{Hom}_G(V,V) = \mathbb{F}$.*

The following is [28, Lemma 2.10.2].

Lemma 1.45. *Let V be a d-dimensional vector space over the field $\mathbb{F}_q$. Let G be an irreducible but not absolutely irreducible subgroup of $\mathrm{GL}(V)$. Then $\mathrm{Hom}_G(V,V) = \mathbb{F}_{q^e}$ is an extension field of $\mathbb{F}_q$ of degree e, where $e \neq 1$ divides d.*

Definition 1.46. Let G be a group and V a vector space over a field $\mathbb{F}$. A *projective representation* of G on V is a group homomorphism $\rho : G \to \mathrm{PGL}(V) = \mathrm{GL}(V)/Z(\mathrm{GL}(V))$.

The following definition is essentially [3, p.2].

Definition 1.47. Let G be a finite group, let $\mathbb{F}$ be a field, and let V be an $\mathbb{F}G$-module. A *composition series* for V is a chain of $\mathbb{F}G$-submodules of V

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_{t-1} \subset V_t = V$$

such that V_{i+1}/V_i is an irreducible module for each $0 \leq i \leq t$. We call t the *length* of the series and we call the modules V_{i+1}/V_i the *composition factors* of the series.

The following is [27, Theorem 11.3 p.146].

Proposition 1.48. *Let G be a finite group, let $\mathbb{F}$ be a field, and let V be a finite dimensional $\mathbb{F}G$-module. Then V has a composition series. Furthermore let W be a submodule of V. Then W and V/W both have composition series.*

The following is the Jordan-Hölder Theorem for modules, see for example [3, Theorem 1.2].

Theorem 1.49. *Let G be a finite group, let $\mathbb{F}$ be a field, and let V be a finite dimensional $\mathbb{F}G$-module. Then every composition series for V has the same length and the same composition factors, up to isomorphism.*

The following is well known.

Lemma 1.50. *Let G be a finite group, $\mathbb{F}$ be a field, and V an irreducible G-module. Then there exists a (right) ideal, I of $\mathbb{F}[G]$ such that $V \cong \mathbb{F}[G]/I$ as G-modules.*

Proof. Fix a non-zero element v of V. We define $\phi_v : \mathbb{F}[G] \to V$ by $\phi_v\left(\sum_{g\in G} a_g g\right) = v\sum_{g\in G} a_g g$ for all $\sum_{g\in G} a_g g \in \mathbb{F}[G]$. Then ϕ_v is a G-module homomorphism and so the image of ϕ_v is a submodule of V containing v. As V is irreducible we must have that $\mathrm{Im}(\phi_v) = V$. Hence by the First Isomorphism Theorem for Modules, $V = \mathrm{Im}(\phi_v) \cong \mathbb{F}[G]/\ker(\phi_v)$. Furthermore

$$\ker(\phi_v) = \left\{ \sum_{g\in G} a_g g \in \mathbb{F}[G] \;\middle|\; v\sum_{g\in G} a_g g = 0 \right\}$$

is closed under multiplication by the elements of G and so $\ker(\phi_v)$ is an ideal of $\mathbb{F}[G]$. □

2. A Semilinear Test

In this section we give the method that we used to create a deterministic semilinear test in MAGMA for irreducible matrix groups.

We begin by describing the general semilinear group. The following definition is from [42, p.7].

Definition 2.1. Let V and W be vector spaces over the same field $\mathbb{F}$. A *semilinear map* is a pair (f, α) with $f : V \to W$ and $\alpha \in \mathrm{Aut}(\mathbb{F})$ such that:

- for all $v_1, v_2 \in V$ we have $(v_1 + v_2)f = (v_1)f + (v_2)f$ and
- for all scalars $\lambda \in \mathbb{F}$ and for all $v \in V$ we have $(\lambda v)f = \lambda^\alpha (v)f$ where λ^α is the image of $\lambda \in \mathbb{F}$ under $\alpha \in \mathrm{Aut}(\mathbb{F})$.

We may use the term "f is an α-semilinear map" to describe the pair (f, α).

We will be interested in the case that $V = W$.

Lemma 2.2. *Let V be a vector space over a field $\mathbb{F}$. The set*

$$\Gamma\mathrm{L}(V) := \{(f, \alpha) \mid f \text{ is an } \alpha\text{-semilinear map and } f : V \to V \text{ is invertible}\}$$

forms a group with operation, for $(f, \alpha), (g, \beta) \in \Gamma\mathrm{L}(V)$, $(f, \alpha)(g, \beta) = (fg, \alpha\beta)$.

Proof. Take $(f, \alpha), (g, \beta) \in \Gamma\mathrm{L}(V)$. Then for any $v_1, v_2 \in V$ and $\lambda \in \mathbb{F}$ we have

$$(v_1 + v_2)fg = ((v_1 + v_2)f)g = (v_1 f + v_2 f)g = (v_1 f)g + (v_2 f)g = (v_1)fg + (v_2)fg,$$

$$(\lambda v)fg = ((\lambda v)f)g = (\lambda^\alpha (v)f)g = (\lambda^\alpha)^\beta (v)fg = \lambda^{\alpha\beta}(v)fg.$$

Thus fg is an $(\alpha\beta)$-semilinear map and fg is invertible as both f and g are invertible, thus $(fg, \alpha\beta) \in \Gamma\mathrm{L}(V)$.

We let $1 \in \mathrm{Aut}(\mathbb{F})$ be the identity automorphism and we let $\mathrm{Id} : V \to V$ be the identity map. Then $(\mathrm{Id}, 1) \in \Gamma\mathrm{L}(V) \neq \emptyset$ satisfies

$$(v)f \ \mathrm{Id} = (v)f = (v) \ \mathrm{Id}f, \text{ and}$$

$$(\lambda v)f \ \mathrm{Id} = (\lambda^\alpha (v)f) \ \mathrm{Id} = \lambda^\alpha (v)f = (\lambda v)f = (\lambda v) \ \mathrm{Id}f.$$

Hence for any $(f, \alpha) \in \Gamma\mathrm{L}(V)$ we have $(\mathrm{Id}, 1)(f, \alpha) = (f, \alpha) = (f, \alpha)(\mathrm{Id}, 1)$.

For any $(f, \alpha) \in \Gamma\mathrm{L}(V)$ we consider $(f^{-1}, \alpha^{-1}) \in \Gamma\mathrm{L}(V)$. Then

$$(v)ff^{-1} = v \text{ and } (\lambda v)ff^{-1} = \lambda^\alpha (v)f^{-1} = \lambda v,$$

so $(f, \alpha)^{-1} = (f^{-1}, \alpha^{-1})$.

Finally one may check that the operation is associative and so $\Gamma\mathrm{L}(V)$ forms a group with the above operation. □

The group $\Gamma\mathrm{L}(V)$, defined in Lemma 2.2, is called the *general semilinear group*.

Remark 2.3. Let $D := \{(g,1) \mid (g,1) \in \Gamma\mathrm{L}(V)\}$. Then $(g,1) \in D$ if $g : V \to V$ is an invertible map such that, for all $v_1, v_2 \in V$ and $\lambda \in \mathbb{F}$, we have

- $(v_1 + v_2)g = v_1 g + v_2 g$, and
- $(\lambda v_1)g = \lambda^1 (v_1)g = \lambda (v_1)g$.

Hence $g \in \mathrm{GL}(V)$ and it follows that $\mathrm{GL}(V) \cong D \leq \Gamma\mathrm{L}(V)$.

In fact, for any $(f,\alpha) \in \Gamma\mathrm{L}(V)$ and $(g,1) \in D$ we have that $(f,\alpha)^{-1}(g,1)(f,\alpha) = (f^{-1},\alpha^{-1})(gf,\alpha) = (f^{-1}gf,1) \in D$. Hence $D \trianglelefteq \Gamma\mathrm{L}(V)$.

Lemma 2.4. *Let V be a vector space over a field $\mathbb{F}$, then for any basis B of V, we may write any vector $v \in V$ as $v = \sum_{b\in B} \lambda_b b$ for $\lambda_b \in \mathbb{F}$ and*

(i) for any $\alpha \in \mathrm{Aut}(\mathbb{F})$ the map $f_\alpha : V \to V$ defined by $\left(\sum_{b\in B} \lambda_b b\right) f_\alpha := \sum_{b\in B} \lambda_b^\alpha b$ is an invertible α-semilinear map,
(ii) the set $A := \{(f_\alpha,\alpha) \mid \alpha \in \mathrm{Aut}(\mathbb{F})\}$ is a subgroup of $\Gamma\mathrm{L}(V)$ and $A \cong \mathrm{Aut}(\mathbb{F})$,
(iii) for any $(f,\alpha) \in \Gamma\mathrm{L}(V)$ the map $y_f : V \to V$ defined by $\left(\sum_{b\in B} \lambda_b b\right) y_f := \sum_{b\in B} \lambda_b (b) f$ is an invertible linear map,
(iv) $\Gamma\mathrm{L}(V) \cong \mathrm{GL}(V) \rtimes \mathrm{Aut}(\mathbb{F})$.

Proof. (i) For any $v_1 = \sum_{b\in B} \lambda_b b$ and $v_2 = \sum_{b\in B} \mu_b b \in V$ we have: $(v_1 + v_2)f_\alpha = \left(\sum_{b\in B} (\lambda_b + \mu_n) b\right) f_\alpha = \sum_{b\in B} (\lambda_b + \mu_b)^\alpha b = \sum_{b\in B} \lambda_b^\alpha b + \sum_{b\in B} \mu_b^\alpha b = v_1 f_\alpha + v_2 f_\alpha$.

We also have for any $\lambda \in \mathbb{F}$ and any $v = \sum_{b\in B} \lambda_b b \in V$ that
$(\lambda v)f_\alpha = \left(\sum_{b\in B} \lambda\lambda_b b\right) f_\alpha = \sum_{b\in B} (\lambda\lambda_b)^\alpha b = \lambda^\alpha \sum_{b\in B} \lambda_b^\alpha b = \lambda^\alpha (v) f_\alpha$.

Finally for any $v_1 = \sum_{b\in B} \lambda_b b, v_2 = \sum_{b\in B} \mu_b b \in V$, and $\lambda \in \mathbb{F}$ we have

$$\begin{aligned}(v_1 + \lambda v_2) f_\alpha f_{\alpha^{-1}} &= \left(\sum_{b\in B} \lambda_b b + \sum_{b\in B} \lambda\mu_b b\right) f_\alpha f_{\alpha^{-1}} \\ &= \left(\sum_{b\in B} (\lambda_b + \lambda\mu_b) b\right) f_\alpha f_{\alpha^{-1}} \left(\sum_{b\in B} (\lambda_b + \lambda\mu_b)^\alpha b\right) f_{\alpha^{-1}} \\ &= \sum_{b\in B} (\lambda_b + \lambda\mu_b) b = v_1 + \lambda v_2.\end{aligned}$$

Thus $f_{\alpha^{-1}} = (f_\alpha)^{-1}$ and so f_α is an invertible α-semilinear map, that is $(f_\alpha,\alpha) \in \Gamma\mathrm{L}(V)$.

(ii) For any $(f_\alpha,\alpha), (f_\beta,\beta) \in A$ and $v = \sum_{b\in B} \lambda_b b \in V$ we have $(v) f_\alpha f_\beta = \left(\sum_{b\in B} \lambda_b b\right) f_\alpha f_\beta = \left(\sum_{b\in B} \lambda_b^\alpha b\right) f_\beta = \sum_{b\in B} \lambda_b^{\alpha\beta} b = (v) f_{\alpha\beta}$.

Thus $f_\alpha f_\beta = f_{\alpha\beta}$ and so $(f_\alpha,\alpha)(f_\beta,\beta) = (f_\alpha f_\beta, \alpha\beta) = (f_{\alpha\beta},\alpha\beta) \in A$. We have that $(\mathrm{Id},1) = (f_1,1) \in A$ and $(f_\alpha,\alpha)^{-1} = (f_{\alpha^{-1}},\alpha^{-1}) \in A$. Thus $A \leq \Gamma\mathrm{L}(V)$.

We define $\phi : \mathrm{Aut}(\mathbb{F}) \to A$ via $(\alpha)\phi = (f_\alpha,\alpha)$ for all $\alpha \in \mathrm{Aut}(\mathbb{F})$.

Take any $\alpha, \beta \in \mathrm{Aut}(\mathbb{F})$. Then $(\alpha\beta)\phi = (f_{\alpha\beta}, \alpha\beta) = (f_\alpha, \alpha)(f_\beta, \beta) = (\alpha)\phi(\beta)\phi$. Therefore ϕ is a group homomorphism.

For any $\alpha \in \mathrm{Aut}(\mathbb{F})$ we have that $\alpha \in \ker(\phi)$ if and only if $(\alpha)\phi = (f_1, 1)$ if and only if $\alpha = 1$. Thus ϕ is an injection. Hence as ϕ is a surjection, ϕ is a group isomorphism. Therefore $\mathrm{Aut}(\mathbb{F}) \cong A \leq \Gamma\mathrm{L}(V)$.

(iii) By Remark 2.3, we have that $\mathrm{GL}(V) \cong D := \{(g, 1) \mid (g, 1) \in \Gamma\mathrm{L}(V)\} \trianglelefteq \Gamma\mathrm{L}(V)$. We note that $A \cap D = \{(\mathrm{Id}, 1)\}$.

For any $v_1 = \sum_{b\in B} \lambda_b b, v_2 = \sum_{b\in B} \mu_b b \in V$ and $\lambda \in \mathbb{F}$ we have $(v_1 + v_2)y_f = \left(\sum_{b\in B}(\lambda_b + \mu_b)b\right) y_f = \sum_{b\in B}(\lambda_b + \mu_b)(b)f = \left(\sum_{b\in B} \lambda_b b\right) y_f + \left(\sum_{b\in B} \mu_b b\right) y_f = (v_1)y_f + (v_2)y_f$, and $(\lambda v_1)y_f = \left(\sum_{b\in B} \lambda\lambda_b b\right) y_f = \sum_{b\in B} \lambda\lambda_b(b)f = \lambda \sum_{b\in B} \lambda_b(b)f = \lambda(v_1)y_f$. Therefore y_f is a linear map.

We let $x_f : V \to V$ be defined by: $vx_f = \left(\sum_{b\in B} \lambda_b b\right) x_f = \sum_{b\in B} \lambda_b(b)f^{-1}$. Then $(v)y_f x_f = \left(\sum_{b\in B} \lambda_b b\right) y_f x_f = \left(\sum_{b\in B} \lambda_b(b)f\right) x_f = \sum_{b\in B} \lambda_b b = v$ and $(v)x_f y_f = \left(\sum_{b\in B} \lambda_b b\right) x_f y_f = \left(\sum_{b\in B} \lambda_b(b)f^{-1}\right) y_f = \sum_{b\in B} \lambda_b b = v$. Therefore $x_f = y_f^{-1}$. Thus $(y_f, 1) \in D \cong \mathrm{GL}(V)$.

(iv) Take any $(f, \alpha) \in \Gamma\mathrm{L}(V)$. Then for $(x_f, 1) \in D$ we have that $(f, \alpha)(x_f, 1) = (fx_f, \alpha)$. For every $v = \sum_{b\in B}(\lambda_b b) \in V$ we have $(v)fx_f = \left(\sum_{b\in B} \lambda_b^\alpha(b)f\right) x_f = \sum_{b\in B} \lambda_b^\alpha b$. Hence $fx_f = f_\alpha$ and so $(fx_f, \alpha) = (f_\alpha, \alpha) \in A$. It follows that $(f, \alpha) = (f_\alpha, \alpha)(y_f, 1)$.

Therefore $\Gamma\mathrm{L}(V) = \mathrm{GL}(V) \rtimes \mathrm{Aut}(\mathbb{F})$. □

Lemma 2.5. *Let $V = \mathbb{F}_q^d$ be a d-dimensional vector space over the field of order q. Let $e > 1$ be a divisor of d, then there is an $\mathbb{F}_q$-vector space isomorphism between $\mathbb{F}_q^d$ and $\mathbb{F}_{q^e}^{d/e}$.*

Proof. By, for example [1, Section 13.3, p.496], the field $\mathbb{F}_{q^e}$ is an e-dimensional vector space over $\mathbb{F}_q$. Hence $\mathbb{F}_{q^e}^{d/e}$ is a d-dimensional vector space over $\mathbb{F}_q$. By Lemma 1.32, vector spaces of the same dimension over the same scalar field are isomorphic and so $\mathbb{F}_q^d \cong \mathbb{F}_{q^e}^{d/e}$. □

2.1. **Constructing an embedding of general linear groups.** For computational purposes, we require a specific isomorphism between $\mathbb{F}_q^d$ and $\mathbb{F}_{q^e}^{d/e}$, where e divides d.

Let $\alpha \in \mathbb{F}_{q^e}$ be a primitive element (an element of order $q^e - 1$), and let $m(x) := a_0 + a_1 x + a_2 x^2 + \cdots + a_{e-1}x^{e-1} + x^e$ be the minimal polynomial of α over $\mathbb{F}_q$ (in particular $m(\alpha) = 0$). Then $B := (1, \alpha, \ldots, \alpha^{e-1})$ is an ordered basis for $\mathbb{F}_{q^e}$ over $\mathbb{F}_q$ (as it spans and if B were not linearly independent then there would exist a smaller

degree polynomial). Hence any element $\lambda \in \mathbb{F}_{q^e}$ may be written uniquely as a linear combination $c_0 + c_1\alpha + \cdots + c_{e-1}\alpha^{e-1}$, where $c_i \in \mathbb{F}_q$ for $0 \leq i \leq e-1$.

Construction 2.6. We define $\phi_e : \mathbb{F}_q^e \to \mathbb{F}_{q^e}$ via

$$(b_0, b_1, \ldots, b_{e-1})\phi_e := \left(\sum_{i=0}^{e-1} b_i\alpha^i\right)$$

for $(b_0, \ldots, b_{e-1}) \in \mathbb{F}_q^e$.

Take any $(a_0, a_1, \ldots, a_{e-1}), (b_0, b_1, \ldots, b_{e-1}) \in \mathbb{F}_q^e$.
If $(a_0, \ldots, a_{e-1})\phi_e = (b_0, \ldots, b_{e-1})\phi_e$ then $\sum_{i=0}^{e-1} a_i\alpha^i = \sum_{i=0}^{e-1} b_i\alpha^i$. Since $(1, \alpha, \ldots, \alpha^{e-1})$ is a basis, we must have that $a_i = b_i$ for all $0 \leq i \leq e-1$, and so ϕ_e is injective. The map ϕ_e is surjective as the order of $\mathbb{F}_q[\alpha]$ is equal to the order of $\mathbb{F}_q^e$. Thus ϕ_e is a bijection.

Furthermore $(a_0, \ldots, a_{e-1})\phi_e + (b_0, \ldots, b_{e-1})\phi_e = \sum_{i=0}^{e-1} a_i\alpha^i + \sum_{i=0}^{e-1} b_i\alpha^i = \sum_{i=0}^{e-1}(a_i + b_i)\alpha^i = (a_0 + b_0, a_1 + b_1, \ldots, a_{e-1} + b_{e-1})\phi_e = ((a_0, \ldots, a_{e-1}) + (b_0, \ldots, b_{e-1}))\,\phi_e$. Thus ϕ_e is a homomorphism of additive groups.

Let $\lambda \in \mathbb{F}_q$. Then $((a_0, \ldots a_{e-1})\lambda)\phi_e = (a_0\lambda, \ldots, a_{e-1}\lambda)\phi_e = \sum_{i=0}^{e-1} a_i\lambda\alpha^i = \lambda\left(\sum_{i=0}^{e-1} a_i\alpha^i\right) = \lambda(a_0, \ldots, a_{e-1})\phi_e$. Therefore ϕ_e is a linear map between the vector spaces $\mathbb{F}_q^e$ and $\mathbb{F}_{q^e}$.

Therefore ϕ_e is an $\mathbb{F}_q$-vector space isomorphism. □

Remark 2.7. For any $v = (b_0, \ldots, b_{e-1}) \in \mathbb{F}_q^e$ we have: $(v\phi_e)\alpha = \left(\sum_{i=0}^{e-1} b_i\alpha^i\right)\alpha = \sum_{i=0}^{e-1} b_i\alpha^{i+1} = \sum_{i=0}^{e-2} b_i\alpha^{i+1} + b_{e-1}\alpha^e = \sum_{i=0}^{e-2} b_i\alpha^{i+1} - b_{e-1}\left(\sum_{i=0}^{e-1} a_i\alpha^i\right) = \sum_{i=1}^{e-1} b_{i-1}\alpha^i - \sum_{i=0}^{e-1} a_ib_{e-1}\alpha^i = -b_{e-1}a_0 - \sum_{i=1}^{e-1}(b_{i-1} - b_{e-1}a_i)\,\alpha^i = -b_{e-1}a_0 + (b_0 - b_{e-1}a_1)\alpha + \cdots + (b_{e-2} - b_{e-1}a_{e-1})\alpha^{e-1} = (-b_{e-1}a_0, \ldots, b_{e-2} - b_{e-1}a_{e-1})\phi_e = ((b_0, \ldots, b_{e-1})C_\alpha)\,\phi_e = (vC_\alpha)\phi_e$, where

$$C_\alpha := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{e-1} \end{pmatrix}$$

is the $e \times e$ *companion matrix* of m over $\mathbb{F}_q$.

Example 2.8. We consider the field $\mathbb{F}_{7^2}$ in the following way:

$$\mathbb{F}_{7^2} \cong \mathbb{F}_7[X]/(X^2 + 5X + 3).$$

We let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element, with minimal polynomial $m(x) = x^2 + 5x + 3$. Then the companion matrix of m over $\mathbb{F}_7$ is

$$C_\alpha = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}.$$

Let $(b_0, b_1) \in \mathbb{F}_7^2$ then $(b_0, b_1)\phi_2 = (b_0 + b_1\alpha)$. We now consider multiplication in $\mathbb{F}_{7^2}$ by the element $\alpha \notin \mathbb{F}_7$ and find the equivalent operation in $\mathbb{F}_7^2$.

$$\begin{aligned}(b_0, b_1)\phi_2\alpha &= (b_0 + b_1\alpha)\alpha = (b_0\alpha + b_1\alpha^2) = (b_0\alpha + b_1(-5\alpha - 3)) \\ &= (-3b_1 + (b_0 - 5b_1)\alpha) = (-3b_1, b_0 - 5b_1)\phi_2 \\ &= (4b_1, b_0 + 2b_1)\phi_2 = \left((b_0, b_1)\begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}\right)\phi_2 \\ &= ((b_0, b_1)C_\alpha)\,\phi_2.\end{aligned}$$

Remark 2.9. We observe that for any $v \in \mathbb{F}_q^e$ we have $(v\phi)\alpha = (vC_\alpha)\,\phi_e$. Hence for any $1 \leq i \leq q^e - 1$ we have that $(v\phi)\alpha^i = (v(C_\alpha)^i)\,\phi_e$. For each $1 \leq i \neq j \leq q^e - 2$ we have that $(v\phi)\alpha^i \neq (v\phi)\alpha^j$. Since $\left(v(C_\alpha)^{q^e-1}\right)\phi_e = (v\phi)\alpha^{q^e-1} = v\phi$, the multiplicative order of C_α is equal to the multiplicative order of α.

We now give two results relating to companion matrices. These are [25, Theorem 3.3.14] and [25, Theorem 3.3.15], respectively.

Lemma 2.10. *Every monic polynomial is both the minimal and characteristic polynomial of its companion matrix.*

Lemma 2.11. *A matrix A is similar to the companion matrix of its minimal polynomial if and only if the minimal and characteristic polynomials of A coincide.*

Construction 2.12. Let d be a number which is divisible by e. We may extend the isomorphism $\phi_e : \mathbb{F}_q^e \to \mathbb{F}_{q^e}$ coordinatewise to construct the isomorphism $\phi : \mathbb{F}_q^d \to \mathbb{F}_{q^e}^{d/e}$. We define ϕ via, for any $(b_0, b_1, \ldots, b_{d-1}) \in \mathbb{F}_q^d$,

$$\begin{aligned}(b_0, \ldots, b_{d-1})\phi &= ((b_0, \ldots, b_{e-1})\phi_e, \ldots, (b_{d-e}, \ldots, b_{d-1})\phi_e) \\ &= \left(\sum_{i=0}^{e-1} b_i\alpha^i, \sum_{i=0}^{e-1} b_{e+i}\alpha^i, \ldots, \sum_{i=0}^{e-1} b_{d-e+i}\alpha^i\right).\end{aligned}$$ □

Remark 2.13. Consider an element $v = (b_0, \ldots, b_{d-1}) \in \mathbb{F}_q^d$. Then

$$\begin{aligned}(v\phi)\alpha &= ((b_0, \ldots, b_{d-1})\phi)\alpha = ((b_0, \ldots, b_{e-1})\phi_e, \ldots, (b_{d-e}, \ldots, b_{d-1})\phi_e)\alpha \\ &= \left(\sum_{i=0}^{e-1} b_i\alpha^i, \sum_{i=0}^{e-1} b_{e+i}\alpha^i, \ldots, \sum_{i=0}^{e-1} b_{d-e+i}\alpha^i\right)\alpha \\ &= \left(\sum_{i=0}^{e-1} b_i\alpha^{i+1}, \sum_{i=0}^{e-1} b_{e+i}\alpha^{i+1}, \ldots, \sum_{i=0}^{e-1} b_{d-e+i}\alpha^{i+1}\right) \\ &= (((b_0, \ldots, b_{e-1})C_\alpha)\phi_e, \ldots, ((b_{d-e}, \ldots, b_{d-1})C_\alpha)\phi_e) \\ &= ((b_0, \ldots, b_{e-1})C_\alpha, \ldots, (b_{d-e}, \ldots, b_{d-1})C_\alpha)\,\phi \\ &= \left((b_0, \ldots, b_{d-1})\mathrm{Diag}_{d/e}(C_\alpha)\right)\phi = \left(v\mathrm{Diag}_{d/e}(C_\alpha)\right)\phi,\end{aligned}$$

where $\mathrm{Diag}_{d/e}(C_\alpha)$ is the block diagonal matrix containing d/e copies of C_α. Thus $(v\phi)\alpha = \left(v\mathrm{Diag}_{d/e}(C_\alpha)\right)\phi$.

Example 2.14. As in Example 2.8 we consider the field $\mathbb{F}_{7^2} \cong \mathbb{F}_7[X]/(X^2+5X+3)$ and we let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element with minimal polynomial

$m(x) = x^2+5x+3$. Then for $(b_0, b_1, b_2, b_3, b_4, b_5) \in \mathbb{F}_7^6$ we have $(b_0, b_1, b_2, b_3, b_4, b_5)\phi = (b_0 + b_1\alpha, b_2 + b_3\alpha, b_4 + b_5\alpha)$. We now consider multiplication in $\mathbb{F}_{7^2}^3$ by the element $\alpha \notin \mathbb{F}_7$ and find the equivalent operation in $\mathbb{F}_7^6$.

$$\begin{aligned}
(b_0, b_1, b_2, b_3, b_4, b_5)\phi\alpha &= (b_0 + b_1\alpha, b_2 + b_3\alpha, b_4 + b_5\alpha)\alpha \\
&= (b_0\alpha + b_1\alpha^2, b_2\alpha + b_3\alpha^2, b_4\alpha + b_5\alpha^2) \\
&= (b_0\alpha + b_1(2\alpha + 4), b_2\alpha + b_3(2\alpha + 4), b_4\alpha + b_5(2\alpha + 4)) \\
&= (4b_1, b_0 + 2b_1, 4b_3, b_2 + 2b_3, 4b_5, b_4 + 2b_5)\phi \\
&= \left((b_0, b_1, b_2, b_3, b_4, b_5) \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 4 & 2 \end{pmatrix} \right) \phi \\
&= \left((b_0, b_1, b_2, b_3, b_4, b_5)\mathrm{Diag}_3(C_\alpha)\right)\phi.
\end{aligned}$$

Lemma 2.15. *Consider $\mathbb{F}_q$ as a subfield of $\mathbb{F}_{q^e}$. Let $\alpha \in \mathbb{F}_{q^e}$ be a primitive element with minimal polynomial $m(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{e-1}x^{e-1} + x^e$. As in Construction 2.6 we will write*

$$C_\alpha := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{e-1} \end{pmatrix}$$

for the companion matrix of m. Then the ring

$$\mathbb{F}_q[C_\alpha] := \{0_{e\times e}, C_\alpha, \ldots, (C_\alpha)^{q^e-2}, (C_\alpha)^{q^e-1} = \mathrm{Id}_{e\times e}\}$$

is isomorphic to the field $\mathbb{F}_{q^e}$, with isomorphism $f : \mathbb{F}_{q^e} \to \mathbb{F}_q[C_\alpha]$ where $(\alpha^i)f = (C_\alpha)^i$ for all $1 \le i \le q^e - 1$ and $(0)f = 0_{e\times e}$.

Proof. By Lemma 2.10, the minimal polynomial of C_α is m. Therefore by Proposition 1.34, addition and multiplication in $\mathbb{F}_q[C_\alpha]$ are defined via m and the multiplicative order of C_α. Moreover in the field $\mathbb{F}_q$ addition and multiplication are defined via m and the multiplicative order of α.

We define the map

$$f : \mathbb{F}_{q^e} \to \mathbb{F}_q[C_\alpha] \text{ by } (x)f = \begin{cases} (C_\alpha)^i & \text{if } x = \alpha^i \in \mathbb{F}_{q^e} \\ 0_{e\times e} & \text{if } x = 0 \in \mathbb{F}_{q^e} \end{cases}.$$

We now show that this map is an isomorphism. Firstly we note that f is surjective and if $(\alpha^i)f = (\alpha^j)f$ then this implies that $(C_\alpha)^i = (C_\alpha)^j$. By Remark 2.9, the multiplicative orders of C_α and α are equal, thus $i = j$ and f is injective. Hence f

is a bijection.

Take any non zero $x, y \in \mathbb{F}_{q^e}$ then $(xy)f = (\alpha^i\alpha^j)f$ for some $1 \leq i, j \leq q^e - 1$ and $(\alpha^i\alpha^j)f = (\alpha^{i+j})f = (\alpha^k)f$ for some $1 \leq k \leq q^e - 1$. By Remark 2.9, the multiplicative orders of α and C_α are equal and so $(\alpha^k)f = (C_\alpha)^k = (C_\alpha)^i(C_\alpha)^j$. For any $x \in \mathbb{F}_{q^e}$ we have $(0x)f = (x0)f = (0)f = 0_{e\times e} = (x)f(0)f = (0)f(x)f$. Thus $(xy)f = (x)f(y)f$ for all $x, y \in \mathbb{F}_q$.

Furthermore $(x+y)f = (\alpha^i+\alpha^j)f = (\alpha^r)f$ where we determine r via the minimal polynomial, m, of α over $\mathbb{F}_q$ and by the multiplicative order of α. We have that $(C_\alpha)^i + (C_\alpha)^j = (C_\alpha)^t$ where t is determined by the minimal polynomial of C_α and the multiplicative order of C_α.

By the definition of the companion matrix, the minimal polynomial for C_α is m and the multiplicative order of C_α is the multiplicative order of α. Hence $r = t$, as they must be determined in the same way.

Thus $(x + y)f = (\alpha^i + \alpha^j)f = (\alpha^r)f = (C_\alpha)^r = (C_\alpha)^i + (C_\alpha)^j = (\alpha^i)f + (\alpha^j)f = (x)f + (y)f$. If either x or y were equal to 0 the result would still hold. Hence $(x + y)f = (x)f + (y)f$ for all $x, y \in \mathbb{F}_{q^e}$.

Therefore f is an isomorphism of rings. □

Example 2.16. We consider the field $\mathbb{F}_{3^2} \cong \mathbb{F}_3[X]/(X^2 + X + 2)$, and we let $\alpha \in \mathbb{F}_{3^2}$ be a primitive element with minimal polynomial $m(x) = x^2 + x + 2$. Then $C_\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$ and $f : \mathbb{F}_{3^2} \to \mathbb{F}_3[C_\alpha]$ such that

$$(x)f = \begin{cases} (C_\alpha)^i & \text{if } x = \alpha^i \in \mathbb{F}_{3^2} \\ 0_{2\times 2} & \text{if } x = 0 \in \mathbb{F}_{3^2} \end{cases}$$

is an isomorphism of fields.

We have that $\alpha^2 + \alpha + 2 = 0$ thus

$$\alpha^2 = 2\alpha + 1, \alpha^3 = 2\alpha^2 + \alpha = 2\alpha + 2, \alpha^4 = 2\alpha^2 + 2\alpha = 2,$$
$$\alpha^5 = 2\alpha, \alpha^6 = 2\alpha^2 = \alpha + 2, \alpha^7 = \alpha^2 + 2\alpha = \alpha + 1, \alpha^8 = \alpha^2 + \alpha = 1.$$

Then $(\alpha + \alpha)f = (2\alpha)f = (\alpha^5)f = (C_\alpha)^5 = \begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix} = 2C_\alpha = C_\alpha + C_\alpha = (\alpha)f + (\alpha)f$.

Example 2.17. As in Example 2.8 we consider the field $\mathbb{F}_{7^2} \cong \mathbb{F}_7[X]/(X^2+5X+3)$ and we let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element with minimal polynomial $m(x) = x^2 +$

$5x+3$. The isomorphism $f : \mathbb{F}_{7^2} \to \mathbb{F}_7[C_\alpha]$ is defined by:

$$(x)f = \begin{cases} (C_\alpha)^i & \text{if } x = \alpha^i \in \mathbb{F}_{7^2} \\ 0_{2\times 2} & \text{if } x = 0 \in \mathbb{F}_{7^2} \end{cases},$$

where $C_\alpha = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}$.

Then $(\alpha+\alpha)f = (\alpha^{17})f = (C_\alpha)^{17} = \begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} = 2C_\alpha = C_\alpha + C_\alpha = (\alpha)f + (\alpha)f$.

Also $(\alpha^2+\alpha^7)f = (\alpha^{44})f = (C_\alpha)^{44} = \begin{pmatrix} 6 & 1 \\ 4 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 2 & 6 \\ 3 & 0 \end{pmatrix} = (C_\alpha)^2 + (C_\alpha)^7 = (\alpha^2)f + (\alpha^7)f$.

This gives rise to a general construction.

Construction 2.18. We let $G = \mathrm{GL}(d,q)$ and $H = \mathrm{GL}(d/e, q^e)$ where e is a divisor of d and q is a power of a prime p. We construct an embedding of H into G as follows.

Let $\alpha \in \mathbb{F}_{q^e}$ be a primitive element of $\mathbb{F}_{q^e}$ and let C_α be the $e \times e$ companion matrix of the minimal polynomial, m, of α over $\mathbb{F}_q$ as in Construction 2.6. Then if $m(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{e-1}x^{e-1} + x^e$,

$$C_\alpha = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{e-1} \end{pmatrix}.$$

For each matrix $A \in \mathrm{GL}(d/e, q^e)$, each entry $A_{i,j} \in \mathbb{F}_{q^e}$ of A is either equal to α^k for some $1 \le k \le q^e - 1$, or it is equal to zero.

If $A_{i,j} = \alpha^k$ then replace it with the $e \times e$ matrix $(C_\alpha)^k$. If $A_{i,j} = 0$ then replace it by the $e \times e$ zero matrix.

We now show that this defines an embedding of $\mathrm{GL}(d/e, q^e)$ into $\mathrm{GL}(d,q)$.

Consider the isomorphism $f : \mathbb{F}_{q^e} \to \mathbb{F}_q[C_\alpha]$ defined in Lemma 2.15. For all $x, y \in \mathbb{F}_{q^e}$ we have that $f(xy) = f(x)f(y)$ and $f(x+y) = f(x) + f(y)$.

For each $A \in \mathrm{GL}(d/e, q^e)$ we define a map $\psi : \mathrm{GL}(d/e, q^e) \to \mathrm{GL}(d,q)$ via

$$\psi(A) := \begin{pmatrix} f(A_{1,1}) & \cdots & f(A_{1,d/e}) \\ \vdots & & \vdots \\ f(A_{d/e,1}) & \cdots & f(A_{d/e,d/e}) \end{pmatrix}.$$

Then for all $A, B \in \mathrm{GL}(d/e, q^e)$ we have

$$\psi(A)\psi(B) = \begin{pmatrix} f(A_{1,1}) & \cdots & f(A_{1,d/e}) \\ \vdots & & \vdots \\ f(A_{d/e,1}) & \cdots & f(A_{d/e,d/e}) \end{pmatrix} \begin{pmatrix} f(B_{1,1}) & \cdots & f(B_{1,d/e}) \\ \vdots & & \vdots \\ f(B_{d/e,1}) & \cdots & f(B_{d/e,d/e}) \end{pmatrix}.$$

Hence for each $e \times e$ block entry $C_{i,j}$ of $\psi(A)\psi(B)$ we have

$$C_{i,j} = \sum_{k=1}^{d/e} f(A_{i,k})f(B_{k,j}) = \sum_{k=1}^{d/e} f(A_{i,k}B_{k,j}) = f\left(\sum_{k=1}^{d/e} A_{i,k}B_{k,j}\right).$$

This is the same as each block of $\psi(AB)$. Thus $\psi(A)\psi(B) = \psi(AB)$.

Also

$$\psi(\mathrm{Id}_{d/e \times d/e}) = \begin{pmatrix} f(1) & \cdots & f(0) \\ \vdots & \ddots & \vdots \\ f(0) & \cdots & f(1) \end{pmatrix} = \mathrm{Id}_{d \times d}.$$

For each $A \in \mathrm{GL}(d/e, q^e)$ there exists an inverse $A^{-1} \in \mathrm{GL}(d/e, q^e)$ and $\mathrm{Id}_{d\times d} = \psi(\mathrm{Id}_{d/e,d/e}) = \psi(AA^{-1}) = \psi(A)\psi(A^{-1})$, hence $\psi(A)^{-1} = \psi(A^{-1})$ and so $\psi(A) \in \mathrm{GL}(d, q)$.

If $\psi(A) = \psi(B)$ then each entry must be equal, hence $f(A_{i,j}) = f(B_{i,j})$ for all $1 \leq i, j \leq d/e$. The map f is injective, so the homomorphism ψ must be injective also. □

This construction enables us to write a group in a way that is easier to work with.

Example 2.19. As in Example 2.8 we consider the field

$$\mathbb{F}_{7^2} \cong \mathbb{F}_7[X]/(X^2 + 5X + 3),$$

we let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element with minimal polynomial m such that $m(x) = x^2 + 5x + 3$. So the companion matrix of m over $\mathbb{F}_7$ is

$$C_\alpha := \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}.$$

In MAGMA ver. 2.24, the group $\mathrm{GL}(2, 7^2)$ is generated by

$$\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 6 & 1 \\ 6 & 0 \end{pmatrix}.$$

We have that $\alpha = \alpha^1$, $1 = \alpha^{48}$, and $6 = \alpha^{24}$. Therefore using Construction 2.18 we replace these entries by the matrices

$$(C_\alpha)^1 = C_\alpha,\ (C_\alpha)^{48} = \mathrm{Id}_{e\times e},\ \text{and } (C_\alpha)^{24} = \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} \text{ respectively.}$$

Thus, there is an embedding $\psi : \mathrm{GL}(2, 7^2) \to \mathrm{GL}(4, 7)$ where the generators of the image are

$$\left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\right)\psi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \left(\begin{pmatrix} 6 & 1 \\ 6 & 0 \end{pmatrix}\right)\psi = \begin{pmatrix} 6 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \\ 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \end{pmatrix}.$$

Lemma 2.20. *Let $\psi_1, \psi_2 : \mathrm{GL}(d/e, q^e) \to \mathrm{GL}(d, q)$ be two embeddings, defined as in Construction 2.18 corresponding to different choices of primitive elements of $\mathbb{F}_{q^e}$. Then $\mathrm{GL}(d/e, q^e)\psi_1$ is conjugate in $\mathrm{GL}(d, q)$ to $\mathrm{GL}(d/e, q^e)\psi_2$.*

Proof. Let $\alpha, \beta \in \mathbb{F}_{q^e}$ be two different primitive elements with minimal polynomials m_1 and m_2 corresponding to the embeddings ψ_1 and ψ_2 respectively.

Since α is a primitive element of $\mathbb{F}_{q^e}$, we have that $\beta = \alpha^k$ for some $1 \leq k \leq q^e - 1$. Thus the minimal polynomial of α^k is m_2.

By Lemma 2.15, the map

$$f : \mathbb{F}_{q^e} \to \mathbb{F}_q[C_\alpha] \text{ defined by } (x)f = \begin{cases} (C_\alpha)^i & \text{if } x = \alpha^i \in \mathbb{F}_{q^e} \\ 0_{e\times e} & \text{if } x = 0 \in \mathbb{F}_{q^e} \end{cases}$$

is an isomorphism of rings. As m_2 is the minimal polynomial of α^k we have that

$$\begin{aligned}(0)f = ((\alpha^k)m_2)f &= \left(a_0 + a_1\alpha^k + a_2(\alpha^k)^2 + \cdots + a_{e-1}(\alpha^k)^{e-1} + (\alpha^k)^e\right) f \\ &= a_0\mathrm{Id}_{e\times e} + a_1((C_\alpha)^k) + a_2((C_\alpha)^k)^2 + \cdots + a_{e-1}((C_\alpha)^k)^{e-1} + ((C_\alpha)^k)^e \\ &= 0_{e\times e}.\end{aligned}$$

Hence $((C_\alpha)^k)m_2 = 0$ and as m_2 is minimal for α^k we must have that m_2 is minimal for $(C_\alpha)^k$.

The characteristic polynomial for an $e \times e$ matrix is monic and of degree e and the minimal polynomial of a matrix must divide the characteristic polynomial. The minimal polynomial m_2 of $(C_\alpha)^k$ is of degree e. Therefore the minimal and characteristic polynomials of $(C_\alpha)^k$ must coincide. Thus by Lemma 2.11, the matrix $(C_\alpha)^k$ is conjugate in $\mathrm{GL}(e, q)$ to C_β, the companion matrix of m_2.

Take $B \in \mathrm{GL}(e, q)$, such that $B^{-1}C_\beta B = (C_\alpha)^k$. Then for any $1 \leq i \leq q^e - 1$ there exists some $1 \leq j \leq q^e - 1$ such that $(C_\alpha)^i = B^{-1}(C_\beta)^j B$.

For any $A \in \mathrm{GL}(d/e, q^e)$ we have that

$$A\psi_2 = \begin{pmatrix} a_{1,1} & \dots & a_{1,d/e} \\ \vdots & \ddots & \vdots \\ a_{d/e,1} & \dots & a_{d/e,d/e} \end{pmatrix}\psi_2 = \begin{pmatrix} A_{1,1} & \dots & A_{1,d/e} \\ \vdots & \ddots & \vdots \\ A_{d/e,1} & \dots & A_{d/e,d/e} \end{pmatrix}$$

where $A_{i,j} \in \langle C_\beta \rangle$ if $a_{i,j} \neq 0$ and $A_{i,j} = 0_{e\times e}$ if $a_{i,j} = 0$.

We then have that

$$\begin{aligned}\mathrm{Diag}_{d/e}(B)^{-1}(A\psi_2)\mathrm{Diag}_{d/e}(B) &= \begin{pmatrix} B^{-1}A_{1,1}B & \dots & B^{-1}A_{1,d/e}B \\ \vdots & \ddots & \vdots \\ B^{-1}A_{d/e,1}B & \dots & B^{-1}A_{d/e,d/e}B \end{pmatrix} \\ &= \begin{pmatrix} A'_{1,1} & \dots & A'_{1,d/e} \\ \vdots & \ddots & \vdots \\ A'_{d/e,1} & \dots & A'_{d/e,d/e} \end{pmatrix}\end{aligned}$$

where $A'_{i,j} \in \langle C_\alpha \rangle$ if $a_{i,j} \neq 0$ and $A'_{i,j} = 0_{e\times e}$ if $a_{i,j} = 0$.

Thus $\mathrm{Diag}_{d/e}(B)^{-1}(\mathrm{GL}(d/e, q^e)\psi_2)\mathrm{Diag}_{d/e}(B) \subseteq \mathrm{GL}(d/e, q^e)\psi_1$.

The groups $\mathrm{GL}(d/e, q^e)\psi_1$ and $\mathrm{Diag}_{d/e}(B)^{-1}(\mathrm{GL}(d/e, q^e)\psi_2)\mathrm{Diag}_{d/e}(B)$ have the same cardinality.

Therefore $\mathrm{GL}(d/e, q^e)\psi_1 = \mathrm{Diag}_{d/e}(B)^{-1}(\mathrm{GL}(d/e, q^e)\psi_2)\mathrm{Diag}_{d/e}(B)$, and so $\mathrm{GL}(d/e, q^e)\psi_1$ is conjugate in $\mathrm{GL}(d, q)$ to $\mathrm{GL}(d/e, q^e)\psi_2$. □

Example 2.21. We consider the field $\mathbb{F}_{7^2}$ in two ways:

$$\begin{aligned}\mathbb{F}_{7^2} &\cong \mathbb{F}_7[X]/(X^2 + 5X + 3) \\ &\cong \mathbb{F}_7[X]/(X^2 + 6X + 3).\end{aligned}$$

This creates two different embeddings of $\mathrm{GL}(2, 7^2)$ into $\mathrm{GL}(4, 7)$. We let α, β be primitive elements of $\mathbb{F}_{7^2}$ with minimal polynomials $m_1(x) = x^2+5x+3$ and $m_2(x) = x^2 + 6x + 3$, respectively. Then

$$C_\alpha = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} \text{ and } C_\beta = \begin{pmatrix} 0 & 1 \\ 4 & 1 \end{pmatrix}.$$

Here $(C_\alpha)^{19} = \begin{pmatrix} 2 & 2 \\ 1 & 6 \end{pmatrix}$ has the same minimal polynomial as C_β and

$$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}^{-1} C_\beta \begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix} = (C_\alpha)^{19}.$$

Using the same method as Example 2.19 we may now construct the embeddings $\psi_1 : \mathrm{GL}(2, 7^2) \to \mathrm{GL}(4, 7)$ and $\psi_2 : \mathrm{GL}(2, 7^2) \to \mathrm{GL}(4, 7)$ where the generators of the images are:

$$\left(\begin{pmatrix} \alpha_1 & 0 \\ 0 & 1 \end{pmatrix}\right)\psi_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \left(\begin{pmatrix} 6 & 1 \\ 6 & 0 \end{pmatrix}\right)\psi_1 = \begin{pmatrix} 6 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \\ 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \end{pmatrix},$$

and

$$\left(\begin{pmatrix}\alpha_2 & 0\\ 0 & 1\end{pmatrix}\right)\psi_2 = \begin{pmatrix}0 & 1 & 0 & 0\\ 4 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix} \text{ and } \left(\begin{pmatrix}6 & 1\\ 6 & 0\end{pmatrix}\right)\psi_2 = \begin{pmatrix}6 & 0 & 1 & 0\\ 0 & 6 & 0 & 1\\ 6 & 0 & 0 & 0\\ 0 & 6 & 0 & 0\end{pmatrix}.$$

Then $\mathrm{GL}(2,7^2)\psi_2$ is conjugate in $\mathrm{GL}(4,7)$ to $\mathrm{GL}(2,7^2)\psi_1$ with conjugating element

$$\begin{pmatrix}1 & 0 & 0 & 0\\ 2 & 2 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 2 & 2\end{pmatrix}.$$

Definition 2.22. We define the group $G_{\psi,e}(d,q)$ to be the image of $\mathrm{GL}(d/e,q^e)$ under the embedding ψ given in Construction 2.18. In particular $\mathrm{GL}(d/e,q^e) \cong G_{\psi,e}(d,q) \leq \mathrm{GL}(d,q)$.

The following is Zsigmondy's Theorem [45]. Case (iii) is due to [4].

Theorem 2.23. *Let $a > b > 0$ be coprime integers. Then for any natural number d there exists a prime p such that p divides $a^d - b^d$ but p does not divide $a^k - b^k$ for any natural number $k < d$, with the following exceptions:*

(i) $d = 1, a - b = 1$, then $a^d - b^d = 1$ which clearly has no prime divisors,

(ii) $d = 2, a + b$ is a power of 2. Then any odd prime factors of $a^2 - b^2 = (a+b)(a^1 - b^1)$ must be contained in $a^1 - b^1$,

(iii) $d = 6, a = 2, b = 1$, then $a^6 - b^6 = 63 = (a^2 - b^2)^2(a^3 - b^3)$.

We call the prime p a primitive prime divisor *of $a^d - b^d$.*

The following is [21, p. 493].

Lemma 2.24. *Let $V = \mathbb{F}_q^d$ and $G = \mathrm{GL}(d,q)$. Then G contains a cyclic subgroup S of order $q^d - 1$. We call S a* Singer subgroup *of G, and we call a generator of S a* Singer cycle.

Lemma 2.25. *Let $V = \mathbb{F}_q^d$ and $G \leq \mathrm{GL}(d,q)$. If $G \cong \mathrm{GL}(d/e,q^e)$ then G acts irreducibly on V. In particular $G_{\psi,e}(d,q)$ is an irreducible subgroup of* $\mathrm{GL}(d,q)$

Proof. As G is isomorphic to $\mathrm{GL}(d/e,q^e)$, by Lemma 2.24, there exists a Singer subgroup $S \leq G$ of order $(q^e)^{(d/e)} - 1 = q^d - 1$. By Zsigmondy's Theorem, in the non exceptional cases, there exists a primitive prime divisor r, of $q^d - 1$, so r divides $q^d - 1$ but r does not divide $q^k - 1$ for any $k < d$. Then there is an element g of G of order r and g cannot preserve any subspaces of V. Hence $\langle g \rangle \leq G$ is irreducible. Thus G acts irreducibly on V.

We now consider the exceptional cases. We cannot have $d = 1$. If $d = 2$ and $q + 1$ is a power of 2, then $G \cong \mathrm{GL}(1,q^2)$ is a subgroup of $\mathrm{GL}(2,q)$. We consider

any proper non-trivial subspace $U \subset V$. Then U must be 1-dimensional and so any subgroup of $\mathrm{GL}(2,q)$ which stabilizes U must be of the form

$$R := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a,b,d \in \mathbb{F}_q, ad \neq 0 \right\},$$

with respect to some choice of basis. The order of R is $q(q-1)^2$. Since $G \cong \mathrm{GL}(1,q^2) \cong C_{q^2-1} = C_{(q-1)(q+1)}$, there exists an element $g \in G$ of order $q+1$. We observe that $q+1$ divides $q(q-1)^2$ if and only if $q+1=4$. Hence if $q+1 \neq 4$ then g is acting irreducibly. If $q+1=4$, then $G = \mathrm{GL}(1,9) \cong C_8$ is a subgroup of $\mathrm{GL}(2,3)$ and so G contains an element g of order 4. However in this case $R \cong \mathrm{D}_{12}$ which does not contain an element of order 4. Hence $\langle g \rangle \leq G$ must be irreducible, and so G is irreducible.

If $d=6$ and $q=2$ then $G \cong \mathrm{GL}(1,64), \mathrm{GL}(2,8)$, or $\mathrm{GL}(3,4)$ as a subgroup of $\mathrm{GL}(6,2)$. By Lemma 2.24, each of these possible subgroups contains a Singer subgroup of order 63, and so each of these groups contains an element g of order 9. We have that 9 divides 2^6-1, but does not divide 2^k-1 for any $k<6$. Hence as above, $\langle g \rangle \leq G$ must act irreducibly on V and so G must be irreducible. □

Definition 2.26. Let $\mathbb{F}_q$ be the finite field with q elements and let $\mathbb{F}_{q^e}$ be an extension of $\mathbb{F}_q$ by an irreducible polynomial of degree e. Then $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ is the group of automorphisms of $\mathbb{F}_{q^e}$ that fix $\mathbb{F}_q$ pointwise, *i.e.*

$$\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q) = \{\alpha \in \mathrm{Aut}(\mathbb{F}_{q^e}) \mid a^\alpha = a \text{ for all } a \in \mathbb{F}_q\}.$$

The following is well known.

Lemma 2.27. *Let $\mathbb{F}_q$ be the finite field with q elements, where $q=p^n$, a prime power and let $\mathbb{F}_{q^e}$ be an extension of $\mathbb{F}_q$ by an irreducible polynomial of degree e. Then* $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ *is cyclic of order e. Furthermore* $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ *is generated by the* Frobenius automorphism*, $F : a \mapsto a^q$.*

Proof. We consider the extension of $\mathbb{F}_{q^e}$ over $\mathbb{F}_p$. We have that $\mathbb{F}_{q^e}$ is the splitting field of $x^{q^e}-x$ over $\mathbb{F}_p$, and so $\mathbb{F}_{q^e}$ is Galois over $\mathbb{F}_p$. Therefore $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_p)$ has order $|\mathbb{F}_{q^e} : \mathbb{F}_p| = en$. We consider the Frobenius automorphism $F : a \mapsto a^p$. We observe that $F \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_p)$, and the order of F is en. Thus $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_p)$ must be the cyclic group generated by F.

As $\mathbb{F}_{q^e}$ is an extension of $\mathbb{F}_q$ we have that $\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{q^e}$. Then $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ is a subgroup of $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_p)$, which is cyclic. Furthermore $\alpha \mapsto \alpha^q$ has order e. □

Definition 2.28. Let $V_e = \mathbb{F}_{q^e}^{d/e}$ be a d/e-dimensional vector space over $\mathbb{F}_{q^e}$ where e is a non-trivial divisor of d. Define the set

$$\Gamma\mathrm{L}(d/e, q^e) := \{(f,\alpha) \mid (f,\alpha) \in \Gamma\mathrm{L}(V_e) \text{ and for all } a \in \mathbb{F}_q \,;\, a^\alpha = a\},$$

in other words $\alpha \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$. We observe that $\Gamma\mathrm{L}(d/e, q^e)$ is a subgroup of $\Gamma\mathrm{L}(V_e)$.

Remark 2.29. Observe that for example, $\Gamma\mathrm{L}(4, 2^4) \neq \Gamma\mathrm{L}(4, 4^2)$. Each element of the former is a semilinear transformation with an associated field automorphism that fixes $\mathbb{F}_2$. Alternatively in the latter the associated field automorphism for each element fixes $\mathbb{F}_4$.

The following is essentially a repetition of Lemma 2.4.

Lemma 2.30. *Let V_e be a d/e-dimensional vector space over $\mathbb{F}_{q^e}$, where e is a non-trivial divisor of d. Then*

$$\Gamma\mathrm{L}(d/e, q^e) \cong \mathrm{GL}(d/e, q^e) \rtimes \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$$

where $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ *acts on* $\mathrm{GL}(d/e, q^e)$ *by inducing the automophism onto each matrix entry.*

Proof. Fix a basis $B = [b_1, \ldots, b_{d/e}]$ of V_e. Then any vector $v \in V_e$ may be written as $v = \sum_{b\in B} \lambda_b b$ for $\lambda_b \in \mathbb{F}_{q^e}$, $b \in B$.

For each $\alpha \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$, define $f_\alpha : V_e \to V_e$ to be a map such that

$$\left(\sum_{b\in B} \lambda_b b\right) f_\alpha = \sum_{b\in B} \lambda_b^\alpha b.$$

Then as in Lemma 2.4 (i), f_α is an invertible α-semilinear map, and furthermore, we observe that $(f_\alpha, \alpha) \in \Gamma\mathrm{L}(d/e, q^e)$.

Define the set A:= $\{(f_\alpha, \alpha) \mid \alpha \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)\} \subseteq \Gamma\mathrm{L}(d/e, q^e)$. We observe that similarly to Lemma 2.4 (ii), A forms a subgroup of $\Gamma\mathrm{L}(d/e, q^e)$.

Let $\phi : \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q) \to A$ be defined via $(\alpha)\phi = (f_\alpha, \alpha)$ for all $\alpha \in \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$. Then as in Lemma 2.4 (ii), the map ϕ is a group isomorphism. Therefore $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q) \cong A \leq \Gamma\mathrm{L}(d/e, q^e)$.

We have that $\mathrm{GL}(d/e, q^e) \cong D := \{(g, 1) \mid (g, 1) \in \Gamma\mathrm{L}(d/e, q^e)\}$ and as in Remark 2.3, $D \trianglelefteq \Gamma\mathrm{L}(d/e, q^e)$. We note that $A \cap D = \{(\mathrm{Id}, 1)\}$.

For any $(f, \alpha) \in \Gamma\mathrm{L}(d/e, q^e)$ we define $y_f : V_e \to V_e$ by:

$$\left(\sum_{b\in B} \lambda_b b\right) y_f := \sum_{b\in B} \lambda_b(b) f.$$

Then as in Lemma 2.4 (iii), y_f is an invertible linear map, with inverse $x_f : V_e \to V_e$, defined by: $\left(\sum_{b\in B} \lambda_b b\right) x_f = \sum_{b\in B} \lambda_b(b) f^{-1}$. Thus $(y_f, 1) \in D$.

We now consider $(f,\alpha)(x_f,1) = (fx_f,\alpha)$. Then for any $v = \sum_{b\in B}(\lambda_b b) \in V$ we have $(v)fx_f = \left(\sum_{b\in B}\lambda_b^\alpha (b)f\right)x_f = \sum_{b\in B}\lambda_b^\alpha b$. Hence $(fx_f,\alpha) = (f_\alpha,\alpha) \in A$.

It follows that $(f,\alpha) = (f_\alpha,\alpha)(y_f,1)$ and so $\Gamma\mathrm{L}(d/e,q^e) = \mathrm{GL}(d/e,q^e)\rtimes\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$.

We consider the action of $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ on $\mathrm{GL}(d/e,q^e)$ in this semidirect product.

Let $A = (a_{i,j})$ be the matrix representation of the linear map $y_f : V_e \to V_e$ with respect to the basis B. Then for any basis vector $b_i \in B$, we have that

$$(b_i)y_f = (b_i)f = (a_{i,1},\ldots,a_{i,d/e}) = \sum_{j=1}^{d/e} a_{i,j}b_j.$$

For any $(f,\alpha) \in \Gamma\mathrm{L}(d/e,q^e)$, we have

$$(f_\alpha,\alpha)^{-1}(y_f,1)(f_\alpha,\alpha) = (f_{\alpha^{-1}}y_f f_\alpha,1).$$

Then for any $v = \sum_{i=1}^{d/e}\lambda_{b_i}b_i \in V$ we have

$$(v)f_{\alpha^{-1}}y_f f_\alpha = \left(\sum_{i=1}^{d/e}\lambda_{b_i}b_i\right)f_{\alpha^{-1}}y_f f_\alpha = \left(\sum_{i=1}^{d/e}\lambda_{b_i}^{\alpha^{-1}}(b_i)f\right)f_\alpha$$

$$= \left(\sum_{i=1}^{d/e}\sum_{j=1}^{d/e}\lambda_{b_i}^{\alpha^{-1}}a_{i,j}b_j\right)f_\alpha = \sum_{i=1}^{d/e}\sum_{j=1}^{d/e}\lambda_{b_i}(a_{i,j})^\alpha b_j = \left(\sum_{i=1}^{d/e}\lambda_{b_i}b_i\right)y'_f.$$

Where $y'_f : V_e \to V_e$ is the map defined by

$$\left(\sum_{b\in B}\lambda_b b\right)y'_f := \sum_{b\in B}\lambda_b(b)A',$$

and A' is the matrix obtained by applying α to each of the entries of A. So we have that $(v)f_{\alpha^{-1}}y_f f_\alpha = (v)y'_f$. □

Construction 2.31. We construct an embedding of the group $\Gamma\mathrm{L}(d/e,q^e)$ into $\mathrm{GL}(d,q)$ using the proof of Lemma 2.20 as our framework.

By Lemma 2.30, $\Gamma\mathrm{L}(d/e,q^e) \cong \mathrm{GL}(d/e,q^e)\rtimes\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$, where $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ acts on $\mathrm{GL}(d/e,q^e)$ by inducing the automorphism onto each matrix entry. By Lemma 2.27, we have that $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ is isomorphic to the cyclic group of order e.

Take a primitive element $\alpha \in \mathbb{F}_{q^e}$, with minimal polynomial m over $\mathbb{F}_q$. Let C_α be the companion matrix of m and let $\psi : \mathrm{GL}(d/e,q^e) \to \mathrm{GL}(d,q)$ be the corresponding embedding (see Construction 2.18), giving rise to the group $G_{\psi,e}(d,q)$.

If C_α is conjugate in $\mathrm{GL}(e,q)$ to $(C_\alpha)^k$ for some k, then C_α and $(C_\alpha)^k$ have the same minimal polynomial. So by Lemma 2.15, α and α^k must have the same minimal polynomial over $\mathbb{F}_q$. This minimal polynomial is therefore m and m is of degree

e. Hence there can be at most e distinct roots of m and so there can be at most e elements of $\mathbb{F}_{q^e}$ with m as their minimal polynomial.

As $\alpha^q, \alpha^{q^2} \ldots, \alpha^{q^{e-1}}$ all have m as their minimal polynomial, these must be the only e elements. Hence C_α is only conjugate to $(C_\alpha)^k$ if $k = 1, q, \ldots, q^{e-1}$.

Since C_α is conjugate to $(C_\alpha)^q$, there exists a matrix $B \in \mathrm{GL}(e, q)$ such that $B^{-1}C_\alpha B = (C_\alpha)^q$.

We claim that we may select such a $B \in \mathrm{GL}(e, q)$, so that the order of B is e.

The subgroup $\langle C_\alpha \rangle \leq \mathrm{GL}(e, q)$ is of order $q^e - 1$ and is self centralizing in $\mathrm{GL}(e, q)$. We set $t := (q^e - 1)/(q - 1)$, then $(C_\alpha)^t$ is a scalar matrix of order $q - 1$.

Let $S := B^e$, then S commutes with C_α and so S must lie in $\langle C_\alpha \rangle$. Therefore S must be a power of C_α, say $S = (C_\alpha)^k$. Furthermore S commutes with B and $B^{-1}(C_\alpha)^k B = (C_\alpha)^k$ if and only if $(C_\alpha)^k$ is scalar. Hence S must be a scalar matrix.

Every scalar matrix must be a power of $(C_\alpha)^t$ and so $S^{-1} = (C_\alpha)^{tu}$ for some $u \geq 1$.

We have that

$$\begin{aligned}
(B(C_\alpha)^u)^e &= (B(C_\alpha)^u)(B(C_\alpha)^u)(B(C_\alpha)^u)\ldots(B(C_\alpha)^u) \\
&= B(BB^{-1})(C_\alpha)^u(B(C_\alpha)^u)(B(C_\alpha)^u)\ldots(B(C_\alpha)^u) \\
&= B^2(B^{-1}(C_\alpha)^u B(C_\alpha)^u)(B(C_\alpha)^u)\ldots(B(C_\alpha)^u) \\
&= B^3(B^{-2}(C_\alpha)^u B^2)(B^{-1}(C_\alpha)^u)(B(C_\alpha)^u)\ldots(B(C_\alpha)^u) \\
&= \ldots \\
&= B^e(B^{-(e-1)}(C_\alpha)^u B^{e-1})(B^{-(e-2)}(C_\alpha)^u B^{e-2})\ldots(B^{-1}(C_\alpha)^u B)(C_\alpha)^u \\
&= B^e(C_\alpha)^{u(q^{e-1}+q^{e-2}+\cdots+q+1)} \\
&= B^e(C_\alpha)^{ut} \\
&= SS^{-1} \\
&= \mathrm{Id}_{e\times e}.
\end{aligned}$$

So by replacing B by $B(C_\alpha)^u$ we have a matrix B such that $B^{-1}C_\alpha B = (C_\alpha)^q$ and the order of B is e. In particular we may identify $\langle B \rangle$ with $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$.

For any $A \in \mathrm{GL}(d/e, q^e)$ we consider the image of A in $G_{\psi,e}(d, q)$:

$$A\psi = \begin{pmatrix} a_{1,1} & \ldots & a_{1,d/e} \\ \vdots & \ddots & \vdots \\ a_{d/e,1} & \ldots & a_{d/e,d/e} \end{pmatrix} \psi = \begin{pmatrix} A_{1,1} & \ldots & A_{1,d/e} \\ \vdots & \ddots & \vdots \\ A_{d/e,1} & \ldots & A_{d/e,d/e} \end{pmatrix},$$

where $A_{i,j} \in \langle C_\alpha \rangle$ if $a_{i,j} \neq 0$ and $A_{i,j} = 0_{e\times e}$ if $a_{i,j} = 0$.

We then have that

$$\begin{aligned}\mathrm{Diag}_{d/e}(B)^{-1}(A\psi)\mathrm{Diag}_{d/e}(B) &= \begin{pmatrix} B^{-1}A_{1,1}B & \dots & B^{-1}A_{1,d/e}B \\ \vdots & \ddots & \vdots \\ B^{-1}A_{d/e,1}B & \dots & B^{-1}A_{d/e,d/e}B \end{pmatrix} \\ &= \begin{pmatrix} A'_{1,1} & \dots & A'_{1,d/e} \\ \vdots & \ddots & \vdots \\ A'_{d/e,1} & \dots & A'_{d/e,d/e} \end{pmatrix}.\end{aligned}$$

Where $A'_{i,j} \in \langle (C_\alpha)^q \rangle = \langle C_\alpha \rangle$ if $a_{i,j} \neq 0$ and $A'_{i,j} = 0_{e\times e}$ if $a_{i,j} = 0$.

Thus $\mathrm{Diag}_{d/e}(B)^{-1}(G_{\psi,e}(d,q))\mathrm{Diag}_{d/e}(B) \subseteq G_{\psi,e}(d,q)$ and so $\mathrm{Diag}_{d/e}(B)^{-1}(G_{\psi,e}(d,q))\mathrm{Diag}_{d/e}(B) = G_{\psi,e}(d,q)$. In particular $\mathrm{Diag}_{d/e}(B)$ normalises $G_{\psi,e}(d,q)$.

We consider the subgroup $\hat{G} := \langle G_{\psi,e}(d,q), \mathrm{Diag}_{d/e}(B) \rangle \leq \mathrm{GL}(d,q)$. Then $\hat{G} \cong \mathrm{GL}(d/e, q^e) \rtimes \mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ and $\mathrm{Gal}(\mathbb{F}_{q^e}/\mathbb{F}_q)$ is acting on $\mathrm{GL}(d/e, q^e)$ by inducing the automorphism onto the each matrix entry.

Thus, by Lemma 2.30, $\hat{G} \cong \Gamma\mathrm{L}(d/e, q^e)$ and we have an embedding of $\Gamma\mathrm{L}(d/e, q^e)$ inside of $\mathrm{GL}(d,q)$. □

Example 2.32. We consider the embedding of $\mathrm{GL}(2,7^2)$ into $\mathrm{GL}(4,7)$ as in Examples 2.19 and 2.21. We let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element with minimal polynomial $m(x) = x^2+5x+3$. Then we may construct the embedding $\psi : \mathrm{GL}(2,7^2) \to \mathrm{GL}(4,7)$ where the generators of the image are

$$\left(\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\right)\psi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ and } \left(\begin{pmatrix} 6 & 1 \\ 6 & 0 \end{pmatrix}\right)\psi = \begin{pmatrix} 6 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \\ 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \end{pmatrix},$$

giving the group $G_{\psi,2}(4,7) \leq \mathrm{GL}(4,7)$.

The matrices

$$C_\alpha = \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix} \text{ and } (C_\alpha)^7 = \begin{pmatrix} 2 & 6 \\ 3 & 0 \end{pmatrix}$$

have the same minimal polynomial, which is of degree 2. So by Lemma 2.11, they are conjugate in $\mathrm{GL}(2,7)$. In this case a conjugating matrix is

$$B = \begin{pmatrix} 1 & 0 \\ 2 & 6 \end{pmatrix}.$$

As shown in Construction 2.31, $\mathrm{Diag}_2(B)$ normalizes $G_{\psi,2}(4,7)$ and furthermore the order of B is $e=2$. So we may construct the semidirect product

$$\begin{aligned}\hat{G} &:= G_{\psi,2}(4,7) \rtimes \langle \mathrm{Diag}_2(B) \rangle \\ &= \left\langle \begin{pmatrix} 0 & 1 & 0 & 0 \\ 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 & 1 & 0 \\ 0 & 6 & 0 & 1 \\ 6 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 6 \end{pmatrix} \right\rangle \leq \mathrm{GL}(4,7),\end{aligned}$$

and $\hat{G} \cong \mathrm{GL}(2,7^2) \rtimes C_2 \cong \Gamma\mathrm{L}(2,7^2)$.

Definition 2.33. We define $\Gamma_{\psi,e}(d,q)$ to be the image of $\Gamma\mathrm{L}(d/e,q^e)$ under the embedding demonstrated in Construction 2.31. In particular $\Gamma\mathrm{L}(d/e,q^e) \cong \Gamma_{\psi,e}(d,q) \leq \mathrm{GL}(d,q)$.

Remark 2.34. We consider a field extension $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^e}/\mathbb{F}_q$, where $\alpha \in \mathbb{F}_{q^e}$ is a primitive element. By [1, Chapter 13, Prop. 2.7], the field $\mathbb{F}_{q^e}$ is an $\mathbb{F}_q$-vector space with basis $(1,\alpha,\ldots,\alpha^{e-1})$. Thus $\mathbb{F}_q$ is isomorphic to a subfield $\hat{\mathbb{F}}_q \leq \mathbb{F}_{q^e}$, written as the degree 0 polynomials. *i.e.* The element $a_0 + a_1\alpha + \cdots + a_{e-1}\alpha^{e-1}$ lies in $\hat{\mathbb{F}}_q$ if $a_i = 0$ for all $1 \leq i \leq e-1$.
Therefore we may construct an embedding $i : \mathrm{GL}(d,q) \to \mathrm{GL}(d,q^e)$ where

$$(\mathrm{GL}(d,q))i = \{A = (a_{i,j}) \in \mathrm{GL}(d,q^e) \mid a_{i,j} \in \hat{\mathbb{F}}_q \text{ for all } 1 \leq i,j \leq d\} \leq \mathrm{GL}(d,q^e).$$

Lemma 2.35. *The group $G_{\psi,e}(d,q) \cong \mathrm{GL}(d/e,q^e)$ is not absolutely irreducible as a subgroup of $\mathrm{GL}(d,q)$. In particular, when $G_{\psi,e}(d,q) \leq \mathrm{GL}(d,q)$ is embedded naturally in $\mathrm{GL}(d,q^e)$, it acts reducibly on $\mathbb{F}_{q^e}^d$.*

Proof. Let C_α be a matrix in $\mathrm{GL}(e,q)$ which corresponds to the minimal polynomial m of a generator α of $\mathbb{F}_{q^e}^*$. Then the elements of $G_{\psi,e}(d,q)$ which have been embedded in $\mathrm{GL}(d,q)$ are block matrices consisting of $(d/e)^2$ blocks each of which are elements of $\langle C_\alpha \rangle \cup \{0_{e\times e}\}$. We label the blocks for an element $A \in G_{\psi,e}(d,q)$ as follows:

$$A = \begin{pmatrix} A_{1,1} & \ldots & A_{1,d/e} \\ \vdots & \ddots & \vdots \\ A_{d/e,1} & \ldots & A_{d/e,d/e} \end{pmatrix}.$$

The polynomial m is a defining polynomial of the field extension $\mathbb{F}_{q^e}/\mathbb{F}_q$. When written over $\mathbb{F}_{q^e}$ the polynomial m splits into e linear factors $\{l_1,\ldots,l_e\}$. Further, by Lemma 2.10, these l_i's are eigenvalues for C_α, when we consider C_α as an element of $\mathrm{GL}(e,q^e)$.

Let $v = (v_1,\ldots,v_e) \in \mathbb{F}_{q^e}^e$ be an eigenvector for $C_\alpha \in \mathrm{GL}(e,q^e)$, with eigenvalue l. Then $vA_{i,j} = l_{i,j}v$, where $l_{i,j} = l^k$ if $A_{i,j} = (C_\alpha)^k$ and $l_{i,j} = 0$ if $A_{i,j} = 0_{e\times e}$.

Define $a_i := (0, \ldots, 0, v_1, \ldots, v_e, 0, \ldots, 0) \in \mathbb{F}_{q^e}^d$, for $1 \leq i \leq d/e$, where there are $(i-1)(d/e)$ zeros appearing before v_1. Then for any $A \in G_{\psi,e}(d,q)$ we have that

$$\begin{aligned} a_i A &= (0, \ldots, 0, v_1, \ldots, v_e, 0, \ldots, 0) \begin{pmatrix} A_{1,1} & \ldots & A_{1,d/e} \\ \vdots & \ddots & \vdots \\ A_{d/e,1} & \ldots & A_{d/e,d/e} \end{pmatrix} \\ &= (vA_{i,1}, vA_{i,2}, \ldots, vA_{i,d/e}) \\ &= l_{i,1}a_1 + \cdots + l_{i,d/e}a_{d/e} \\ &\in \langle a_1, \ldots, a_{d/e} \rangle \subset \mathbb{F}_{q^e}^d. \end{aligned}$$

It follows that each element in $G_{\psi,e}(d,q)$ must map the subspace $U := \langle a_1, a_2, \ldots, a_{d/e} \rangle$ to itself.

Furthermore if we take $w \in \mathbb{F}_{q^e}^e$ such that w is not an eigenvector for C_α (w exists as C_α is non-scalar), then the vector $(w, 0, \ldots, 0) \in \mathbb{F}_{q^e}^d \setminus U$. Thus U is a proper subspace of $\mathbb{F}_{q^e}^d$.

Therefore $G_{\psi,e}(d,q)$ acts reducibly on $\mathbb{F}_{q^e}^d$ and so $G_{\psi,e}(d,q)$ is not absolutely irreducible. □

Example 2.36. As in Example 2.8 we consider the field

$$\mathbb{F}_{7^2} \cong \mathbb{F}_7[X]/(X^2 + 5X + 3).$$

Let $\alpha \in \mathbb{F}_{7^2}$ be a primitive element with minimal polynomial m where $m(x) = x^2 + 5x + 3$. So the companion matrix of m over $\mathbb{F}_7$ is

$$C_\alpha := \begin{pmatrix} 0 & 1 \\ 4 & 2 \end{pmatrix}.$$

We then embed $\mathrm{GL}(2, 7^2)$ into $\mathrm{GL}(4, 7)$ in the same way as in Example 2.19. We let $G = G_{\psi,2}(4,7) \cong \mathrm{GL}(2, 7^2)$.

We consider C_α as an element of $\mathrm{GL}(2, 7^2)$. Then $v := (1, \alpha^{17}) \in \mathbb{F}_{7^2}^2$ is an eigenvector for C_α, with corresponding eigenvalue α.

Define $a_1 := (1, \alpha^{17}, 0, 0)$, $a_2 := (0, 0, 1, \alpha^{17}) \in \mathbb{F}_{7^2}^4$ and

$$A := \begin{pmatrix} 3 & 6 & 2 & 2 \\ 6 & 6 & 1 & 6 \\ 2 & 5 & 0 & 2 \\ 6 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} (C_\alpha)^{26} & (C_\alpha)^{19} \\ (C_\alpha)^{36} & (C_\alpha)^{17} \end{pmatrix} \in G_{\psi,2}(4,7).$$

Then

$$a_1 A = (\alpha^{26}, \alpha^{43}, \alpha^{19}, \alpha^{36}) = (v(C_\alpha)^{26}, v(C_\alpha)^{19}) = \alpha^{26}a_1 + \alpha^{19}a_2$$

and

$$a_2A = (\alpha^{36}, \alpha^5, \alpha^{17}, \alpha^{34}) = (v(C_\alpha)^{36}, v(C_\alpha)^{17}) = \alpha^{36}a_1 + \alpha^{17}a_2.$$

Hence A stabilizes $\langle a_1, a_2\rangle$. (This is true for any $A \in G_{\psi,2}(4,7)$.)

2.2. **The theory behind the test.** To create our semilinear test we will require the use of Clifford's Theorem [11] as used in [22, p.5-6] and [23, p.5]. We give the relevant parts of Clifford's Theorem here.

Theorem 2.37 (Clifford's Theorem)**.** *Let G be a matrix group, over any field $\mathbb{F}$, which acts absolutely irreducibly on a d-dimensional $\mathbb{F}$-vector space V. Let N be a normal non-scalar subgroup of G (i.e. N is not a subgroup of $Z(G)$). Then for some $t \geq 1$ the vector space V splits as a direct sum $V = W_1 \oplus W_2 \oplus \cdots \oplus W_t$ of irreducible $\mathbb{F}N$-modules which are all of the same dimension.*

For some $r, s \geq 1$, with $rs = t$, these W_i's partition into r sets containing s pairwise isomorphic $\mathbb{F}N$-modules. Define $V_1, V_2, \ldots, V_r$ to each be the sum of s pairwise isomorphic W_i's so that, if $W_i \in V_k$ and $W_j \in V_{k'}$ where $1 \leq k \neq k' \leq r$ then W_i is not isomorphic to W_j. Hence $V = V_1 \oplus V_2 \oplus \cdots \oplus V_r$.

Then G permutes the V_i's transitively and furthermore:

(i) If $r > 1$ then the group G is imprimitive with the subspaces V_i forming the blocks of a non-trivial system of imprimitivity and N preserves each of these V_i.

(ii) If $r = 1$ then V decomposes as a direct sum of t irreducible, pairwise isomorphic, $\mathbb{F}N$-modules $W_1, \ldots, W_t$ each of dimension d/t over $\mathbb{F}$. Either all of the W_i are absolutely irreducible (as $\mathbb{F}N$-modules), or all are not.

Definition 2.38. Let $G \leq \mathrm{GL}(d,q)$ be an absolutely irreducible subgroup (acting on $V = \mathbb{F}_q^d$). We say that a normal subgroup $N \trianglelefteq G$ acts *homogeneously* on V if V decomposes as a direct sum of irreducible, pairwise isomorphic $\mathbb{F}_qN$-modules each of the same dimension over $\mathbb{F}_q$ (*cf.* Clifford's Theorem (2.37 (ii))). In this case we also call N a *homogeneous* subgroup of G.

Lemma 2.39. *Let $C := C_{\mathrm{GL}(d,q)}(G_{\psi,e}(d,q))$ be the centralizer of $G_{\psi,e}(d,q)$ in $\mathrm{GL}(d,q)$. Then C is a subgroup of $G_{\psi,e}(d,q)$ isomorphic to the cyclic group $\mathbb{F}_{q^e}^*$ of the field $\mathbb{F}_{q^e}$ and $G_{\psi,e}(d,q) = C_{\mathrm{GL}(d,q)}(C)$. Furthermore C acts homogeneously on $V = \mathbb{F}_q^d$.*

Proof. We consider the centre $\hat{Z} := Z(\mathrm{GL}(d/e, q^e))$. Then $\hat{Z}$ consists of the $q^e - 1$ scalar matrices of $\mathrm{GL}(d/e, q^e)$. We embed $\mathrm{GL}(d/e, q^e)$ into $\mathrm{GL}(d,q)$ via ψ, this gives the subgroup $G_{\psi,e}(d,q) \leq \mathrm{GL}(d,q)$.

Define $Z := (\hat{Z})\psi$. The embedding ψ is an isomorphism, hence $Z = Z(G_{\psi,e}(d,q))$ and Z consists of the images of the scalar matrices of $\mathrm{GL}(d/q, q^e)$ under ψ. In particular $Z \cong \mathbb{F}_{q^e}^*$.

By the construction of ψ we have,

$$Z = \left\{ \begin{pmatrix} (C_\alpha)^k & & 0 \\ & \ddots & \\ 0 & & (C_\alpha)^k \end{pmatrix} \middle| \, 1 \leq k \leq q^e - 1 \right\} \leq G_{\psi,e}(d,q).$$

Define the following subspaces of V:

$$\begin{aligned} W_1 :=& \{(a_1, \ldots, a_e, 0, \ldots, 0) \mid a_k \in \mathbb{F}_q\}, \\ W_2 :=& \{(0, \ldots, 0, a_{e+1}, \ldots, a_{2e}, 0, \ldots, 0) \mid a_k \in \mathbb{F}_q\}, \\ & \vdots \\ W_{d/e} :=& \{(0, \ldots, 0, a_{d-e+1}, \ldots, a_d) \mid a_k \in \mathbb{F}_q\}. \end{aligned}$$

In particular,

$$W_i := \{(0, \ldots, 0, a_{(i-1)e+1}, \ldots, a_{ie}, 0, \ldots, 0) \in V \mid a_k \in \mathbb{F}_q\}$$

for $1 \leq i \leq d/e$ and $V = W_1 \oplus \cdots \oplus W_{d/e}$.

For any $A \in Z$ and any $v = (0, \ldots, 0, a_{(i-1)e+1}, \ldots, a_{ie}, 0, \ldots, 0) \in W_i$ we have that

$$vA = (0, \ldots, 0, a_{(i-1)e+1}, \ldots, a_{ie}, 0, \ldots, 0) \begin{pmatrix} (C_\alpha)^k & & 0 \\ & \ddots & \\ 0 & & (C_\alpha)^k \end{pmatrix}$$

for some $1 \leq k \leq q^e - 1$. The jth coordinate of vA is

$$(vA)_j = \sum_{k=1}^{d} v_k A_{k,j}.$$

Hence $(vA)_j = 0$ if $j \notin \{(i-1)e + 1, \ldots, ie\}$. Thus $vA \in W_i$ and so each W_i is Z-invariant.

We observe that for each $1 \leq i \leq d/e$, the action of Z on W_i is equivalent to the action of $\langle C_\alpha \rangle$ on $\mathbb{F}_q^e$.

We have that $|\langle C_\alpha \rangle| = q^e - 1$ and there are $q^e - 1$ non-zero vectors in $\mathbb{F}_q^e$. For any non-zero vector $v \in \mathbb{F}_q^e$, we have that $v(C_\alpha)^k \neq v(C_\alpha)^n$ for $1 \leq n \neq k \leq q^e - 1$.

Hence the action of $\langle C_\alpha \rangle$ on $\mathbb{F}_q^e$ is transitive on the non-zero vectors. Therefore for each $1 \leq i \leq d/e$, the (equivalent) action of Z on W_i is transitive on the non-zero vectors of W_i. Thus each W_i is an irreducible Z-module.

The action of Z on V is therefore homogeneous.

For all $v_1, v_2 \in V$, $a, b \in \mathbb{F}_q$, $z \in Z$, and $M \in C_{\mathrm{GL}(d,q)}(Z)$ we have that

$$(av_1 + bv_2)M = a(v_1M) + b(v_2M) \text{ and } (v_1z)M = (v_1M)z.$$

Hence $C_{\mathrm{GL}(d,q)}(Z) \subseteq \mathrm{Hom}_Z(V, V)$.

Let $f \in \mathrm{Hom}_Z(V, V)$ be invertible. Then for all $v_1, v_2 \in V$ and $a, b \in \mathbb{F}_q$ we have that

$$(av_1 + bv_2)f = a(v_1f) + b(v_2f).$$

Hence $f \in \mathrm{GL}(d, q)$.

Furthermore for all $v \in V$ and $z \in Z$ we have

$$(vz)f = (vf)z$$

and so $f \in C_{\mathrm{GL}(d,q)}(Z)$.

For any non-invertible $g \in \mathrm{Hom}_Z(V, V)$ we have that $g \notin C_{\mathrm{GL}(d,q)}(Z)$. Thus the centralizer $C_{\mathrm{GL}(d,q)}(Z)$ is exactly the invertible elements of $\mathrm{Hom}_Z(V, V)$.

We now consider the subspace $W := W_1$. By Lemmas 1.42 and 1.44, $\mathrm{Hom}_Z(W, W)$ is isomorphic to $\mathbb{F}_{q^e}$. Then by Lemma 1.38, we have that $\mathrm{Hom}_Z(V, V)$ is isomorphic to the ring $\mathrm{M}(d/e, q^e)$, of all $d/e \times d/e$ matrices over $\mathbb{F}_{q^e}$.

The centralizer $C_{\mathrm{GL}(d,q)}(Z)$ is the invertible elements of $\mathrm{Hom}_Z(V, V)$, so we have that $C_{\mathrm{GL}(d,q)}(Z)$ must be isomorphic to $\mathrm{GL}(d/e, q^e)$ ($\subseteq \mathrm{M}(d/e, q^e)$). The group $G_{\psi,e}(d, q)$ must lie in $C_{\mathrm{GL}(d,q)}(Z)$ and $G_{\psi,e}(d, q)$ has the same cardinality as $\mathrm{GL}(d/e, q^e)$. Hence the centralizer of Z in $\mathrm{GL}(d, q)$ must be $G_{\psi,e}(d, q)$.

Since Z is a subgroup of $G_{\psi,e}(d, q)$, every element of C must centralize Z. Hence $C \leq C_{\mathrm{GL}(d,q)}(Z) = G_{\psi,e}(d, q)$. Thus $C = Z$. □

Remark 2.40. The centralizer $C_{\mathrm{GL}(d,q)}(G_{\psi,e}(d, q))$ is isomorphic to $\mathbb{F}_{q^e}^*$ and so is not isomorphic to $\mathbb{F}_q^*$. Therefore by Lemma 1.35, the group $G_{\psi,e}(d, q)$ is *not* absolutely irreducible (as we already proved in Lemma 2.35).

Definition 2.41. Let G be a group and H a subgroup of G. A *right transversal* S, of H in G is a set containing exactly one element from each right coset Hg of H in G.

We now describe a general construction taken from [19], as described in [8].

Construction 2.42. Let H be any subgroup of a group G, and let S be a right transversal of H in G which contains the identity element of G. For each $g \in G$ we denote the unique element in $Hg \cap S$ by $\bar{g}$. We let $\alpha : G \to P$ be the permutation representation of G acting by right multiplication on the right cosets of H in G. Therefore $P = \mathrm{Sym}(G/H)$ and we can think of P as acting on the set S;

interchanging representatives rather than cosets.

We recall Definition 1.10 of a wreath product. We define $X := H \wr_S P$ to be the wreath product using the action of P on S. The base group Y of the wreath product X is the set $\mathrm{Fun}(S, H)$ of functions from S to H. This is a group under pointwise multiplication; for all $y_1, y_2 \in Y$, $s \in S$ define $(y_1 y_2)(s) := y_1(s) y_2(s)$.

The action $y \to y^p$ of P on Y is given by

$$y^p(s) = y(s^{p^{-1}})$$

for $y \in Y$, $p \in P$, and $s \in S$. With this we have that $X = Y \rtimes P$.

For all $s \in S$ and $g \in G$ we observe that $\overline{sg^{-1}} \in Hsg^{-1}$ and so $\overline{sg^{-1}} g s^{-1} \in H$. We may therefore define the function $y_g \in \mathrm{Fun}(S, H)$ via $y_g(s) := \overline{sg^{-1}} g s^{-1}$ for all $s \in S$.

We note that for all $s \in S$ and $g \in G$ we have that $s^{\alpha(g)} \in S$ and $s^{\alpha(g)} \in Hsg$, hence $s^{\alpha(g)} = \overline{sg}$.

Define $\pi : G \to X$ by $\pi(g) = y_g^{\alpha(g)^{-1}} \alpha(g)$ for $g \in G$.

We have that

$$y_g^{\alpha(g)^{-1}}(s) = y_g(s^{\alpha(g)}) = y_g(\overline{sg}) = \overline{\overline{sg} g^{-1}} g (\overline{sg})^{-1} = sg(\overline{sg})^{-1}.$$

Take any $g_1, g_2 \in G$ then

$$\begin{aligned}
\pi(g_1)\pi(g_2) &= y_{g_1}^{\alpha(g_1)^{-1}} \alpha(g_1) y_{g_2}^{\alpha(g_2)^{-1}} \alpha(g_2) \\
&= y_{g_1}^{\alpha(g_1)^{-1}} y_{g_2}^{\alpha(g_2)^{-1}\alpha(g_1)^{-1}} \alpha(g_1)\alpha(g_2) \\
&= y_{g_1}^{\alpha(g_1)^{-1}} y_{g_2}^{\alpha(g_1 g_2)^{-1}} \alpha(g_1 g_2)
\end{aligned}$$

and for any $s \in S$ we have

$$\begin{aligned}
y_{g_1}^{\alpha(g_1)^{-1}} y_{g_2}^{\alpha(g_1 g_2)^{-1}}(s) &= y_{g_1}^{\alpha(g_1)^{-1}}(s) y_{g_2}^{\alpha(g_1 g_2)^{-1}}(s) \\
&= y_{g_1}(s^{\alpha(g_1)}) y_{g_2}(s^{\alpha(g_1 g_2)}) \\
&= y_{g_1}(\overline{sg_1}) y_{g_2}(\overline{sg_1 g_2}) \\
&= (\overline{\overline{sg_1} g_1^{-1}} g_1 (\overline{sg_1})^{-1})(\overline{\overline{sg_1 g_2} g_2^{-1}} g_2 (\overline{sg_1 g_2})^{-1}) \\
&= (sg_1(\overline{sg_1})^{-1})(\overline{sg_1} g_2 (\overline{sg_1 g_2})^{-1}) \\
&= sg_1 g_2 (\overline{sg_1 g_2})^{-1} \\
&= y_{g_1 g_2}^{\alpha(g_1 g_2)^{-1}}(s).
\end{aligned}$$

Therefore

$$\pi(g_1)\pi(g_2) = y_{g_1}^{\alpha(g_1)^{-1}} y_{g_2}^{\alpha(g_1 g_2)^{-1}} \alpha(g_1)\alpha(g_2) = y_{g_1 g_2}^{\alpha(g_1 g_2)^{-1}} \alpha(g_1 g_2) = \pi(g_1 g_2)$$

and so $\pi : G \to X$ is a group homomorphism.

If $t \in \ker(\alpha)$ then $Hst = Hs$ for all $s \in S$. In particular $\overline{st^{-1}} = s$. Hence $\pi(t) = y_t \in Y$, where $y_t(s) = sts^{-1}$ for all $s \in S$.

Take any $k \in \ker(\pi)$, then $\pi(k) = y_k^{\alpha(k)^{-1}}\alpha(k) = \mathbb{1}1_P$ and so $k \in \ker(\alpha)$. Therefore $\pi(k) = y_k$ where $y_k(s) = sks^{-1}$ for all $s \in S$. Hence $y_k = \mathbb{1}$ if and only if $sks^{-1} = 1$ for all $s \in S$. Thus $k = 1$ and the kernel of π is trivial.

We call $\pi : G \to X = H \wr_S P$ the *wreathed monomorphism* induced by H and S. □

We need this construction to work in a more specific case, embedding $G \leq \mathrm{GL}(d, q)$ into a wreath product of $H|_W \wr P$ where H is the stabilizer of a subspace $W \subseteq V = \mathbb{F}_q^d$ and P is defined as above.

Construction 2.43. Let G be an irreducible imprimitive matrix group acting on the vector space $V = \mathbb{F}_q^d$. As in Aschbacher's Theorem (1.25 (ii)), G is irreducible and preserves a direct sum decomposition $V = V_1 \oplus \cdots \oplus V_e$, where each of these V_i are of the same dimension and G transitively permutes the subspaces $V_1, \ldots, V_e$.

Let H be the stabilizer of V_1 in G and we let S be a right transversal of H in G which contains the identity element, as above. For each $g \in G$ we denote the unique element in $Hg \cap S$ by $\bar{g}$. We let $\alpha : G \to P$ be the permutation representation of G acting by right multiplication on the set of right cosets of H in G.

We define $\lambda : G/H \to \{V_1, \ldots, V_e\}$ by $\lambda(Hg) = V_1^g$ for $Hg \in G/H$.

The group G acts transitively on $\{V_1, \ldots, V_e\}$ and so for any $V_i \in \{V_1, \ldots, V_e\}$ there exists a $g_i \in G$ with $V_1^{g_i} = V_i$. If $g_i \neq \bar{g}_i$ then there exists some $h \in H$ with $hg_i = \bar{g}_i$. In this case we have that $\lambda(H\bar{g}_i) = V_1^{hg_i} = V_1^{g_i} = V_i$ and so λ is surjective. Furthermore if $\lambda(Hg) = \lambda(Hg')$ then $V_1^g = V_1^{g'}$ and so $V_1^{gg'^{-1}} = V_1$. Therefore $gg'^{-1} \in H$ and so $Hg = Hg'$. Hence λ is injective and hence a bijection.

We let $f : G \to G$ be the group isomorphism $f(g) = g$. Then for $Hs \in G/H$ we have

$$\lambda((Hs)^g) = \lambda(Hsg) = V_1^{sg}$$

and

$$(\lambda(Hs))^{f(g)} = (V_1^s)^g = V_1^{sg}.$$

Hence the action of G on the subspaces $V_1, \ldots, V_e$ is permutation isomorphic to the action of G on the right cosets of H in G.

In particular, for any $V_i \in \{V_1, \ldots, V_e\}$ the stabilizer in G of V_i is a conjugate of H in G, which we will denote by H_i. Here we have that $H_1 = H$.

We let $X := H \wr_S P$ be the wreath product as described in Construction 2.42. Hence G embeds in X via the wreathed monomorphism $\pi : G \to X$ induced by H and S.

For each $1 \leq i \leq e$, we let $\rho_i : H_i \to \mathrm{GL}(V_i)$ be the representation of H_i in $\mathrm{GL}(V_i)$ (as H_i is the stabilizer of V_i) and we denote $\rho_i(H_i)$ by $H_i|_{V_i}$ (H_i restricted to V_i).

We denote V_1 by W, ρ_1 by ρ and we consider $H|_W \wr_S P$.

By Lemma 1.22, there exists a surjective homomorphism $\bar{\rho} : H \wr_S P \to H|_W \wr_S P$, defined by $\bar{\rho}(y\alpha(g)) = y^*\alpha(g)$, where $y\alpha(g) \in X$, with $g \in G$ and $y \in Y$, and $y^*(s) = \rho(y(s))$ for all $s \in S$.

We consider the kernel of the composition $\bar{\rho} \circ \pi : G \to H|_W \wr_S P$. Let $k \in \ker(\bar{\rho} \circ \pi)$. Then $\pi(k) = y_k^{\alpha(k)^{-1}} \alpha(k)$, where $y_k \in \mathrm{Fun}(S, H)$ is defined by $y_k(s) = \overline{sk^{-1}}ks$ for all $s \in S$. Now $\bar{\rho}(\pi(k)) = \bar{\rho}(y_k^{\alpha(k)^{-1}} \alpha(k)) = (y_k^{\alpha(k)^{-1}})^* \alpha(k)$.

As $k \in \ker(\bar{\rho} \circ \pi)$, we have that $(y_k^{\alpha(k)^{-1}})^* \alpha(k) = \mathbb{1}1_P$. Hence $k \in \ker(\alpha)$ and so by Construction 2.42, $\pi(k) = y_k$ where $y_k(s) = sks^{-1}$ for all $s \in S$.

Thus for all $s \in S$ we have that $(y_k^{\alpha(k)^{-1}})^*(s) = (y_k)^*(s) = \rho(sks^{-1})$ and so $(y_k^{\alpha(k)^{-1}})^* = \mathbb{1}$ if and only if $sks^{-1} \in \ker(\rho)$ for all $s \in S$. Therefore

$$k \in \bigcap_{s \in S} s^{-1} \ker(\rho) s.$$

We take any $v \in V$, as $V = V_1 \oplus \cdots \oplus V_e$, we have that $v = v_1 + \cdots + v_e$ for some $v_i \in V_i$ with $1 \leq i \leq e$.

Since k lies in the intersection $\bigcap_{s \in S} s^{-1} \ker(\rho) s$, for each $1 \leq i \leq e$ we have that $k = {s_i}^{-1} t_i s_i$ for some $t_i \in \ker(\rho)$ and $s_i \in S$ where $W^{s_i} = V_i$.

We consider the image of v under k,

$$v^k = (v_1 + \cdots + v_e)^k = v_1^k + \cdots + v_e^k = v_1^{s_1^{-1} t_1 s_1} + \cdots + v_e^{s_e^{-1} t_e s_e}$$

and

$$v_i^{s_i^{-1} t_i s_i} = (v_i^{s_i^{-1}})^{t_i s_i} = (v_i^{s_i^{-1}})^{s_i} = v_i$$

for each $1 \leq i \leq e$ (as $v_i^{s_i^{-1}} \in W$ and $t_i \in \ker(\rho)$).

Hence $v^k = v$ for all $v \in V$ and so $k = 1$ and the kernel of $\bar{\rho} \circ \pi$ is trivial. Therefore the composition $\bar{\rho} \circ \pi$ is injective.

Thus we have an embedding of G into $H|_W \wr_S P$. □

The following result is well known.

Lemma 2.44. *Let G be the cyclic group of order n. Let $\mathbb{F}_q$ be the field of order $q = p^k$, where p does not divide n. Then all of the non-trivial faithful, irreducible representations of G over $\mathbb{F}_q$ are of the same dimension e and e is the smallest positive integer such that n divides $q^e - 1$.*

Proof. The group algebra $\mathbb{F}_q[G]$ is isomorphic to the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Let $f(x) := x^n - 1$ then $f'(x) = nx^{n-1}$ and so, as p does not divide n we have that $\gcd(f(x), f'(x)) = 1$. So $f(x)$ has no repeated zeros in any extension of $\mathbb{F}_q$.

Therefore $f(x)$ factorizes in $\mathbb{F}_q[x]$ as

$$f(x) = f_1(x)f_2(x)\dots f_t(x)$$

where $t \leq n$ and each of the irreducible factors $f_i(x)$ are distinct for $1 \leq i \leq t$. The roots of the factors f_i are the roots of unity of order d where $d \mid n$.

We consider the splitting field K of $x^n - 1$ over $\mathbb{F}_q$. This field is by definition an extension field of $\mathbb{F}_q$, so $K = \mathbb{F}_{q^e}$ for some $e \geq 1$. As $\gcd(n, p) = 1$, there are exactly n (distinct) roots lying in K, (as there are no repeated zeros). We denote this set of n roots by Ω. Let $\alpha, \beta \in \Omega$ be two such roots. Then

$$f(\alpha\beta^{-1}) = (\alpha\beta^{-1})^n - 1 = \alpha^n(\beta^{-1})^n - 1 = 0.$$

Thus Ω forms a subgroup of order n, of $K^* \cong C_{q^e-1}$. In particular this implies that $n \mid q^e - 1$.

As the splitting field is a minimal extension, e must be minimal as it arises as the degree of this extension.

Thus over $\mathbb{F}_q$ all non-trivial, faithful, irreducible representations of G must be of dimension e. □

Example 2.45. We show that all of the faithful irreducible representations of the group $G = C_{14}$ acting over the field $\mathbb{F}_3$ are of dimension 6. Let α be a primitive 14^{th} root of unity in some extension field of $\mathbb{F}_3$ (*i.e.* $\alpha^{14} = 1$ and $\alpha^i \neq 1$ for all $i < 14$). Let $F : x \mapsto x^3$ be the Frobenius automorphism of this extension field.

We have that $F(\alpha) = \alpha^3$, $F(\alpha^3) = \alpha^9$, $F(\alpha^9) = \alpha^{27} = \alpha^{13}$, $F(\alpha^{13}) = \alpha^{39} = \alpha^{11}$, $F(\alpha^{11}) = \alpha^{33} = \alpha^5$, and $F(\alpha^5) = \alpha^{15} = \alpha$. Hence the minimal polynomial of α over

this extension is

$$m(x) := (x-\alpha)(x-\alpha^3)(x-\alpha^9)(x-\alpha^{13})(x-\alpha^{11})(x-\alpha^5).$$

We may similarly find that the minimal polynomial for α^2 is

$$m_2(x) := (x-\alpha^2)(x-\alpha^6)(x-\alpha^4)(x-\alpha^{12})(x-\alpha^8)(x-\alpha^{10}).$$

Both $\alpha^0 = 1$ and $\alpha^7 = -1 = 2$ lie in the ground field $\mathbb{F}_3$ and so their minimal polynomials are linear (degree 1).

Therefore the polynomial $x^{14}-1$ splits into a product of two linear and two degree 6 factors in $\mathbb{F}_3[x]$. Thus the irreducible representations of C_{14} over $\mathbb{F}_3$ have dimensions $1, 1, 6$, and 6 respectively.

For a representation of C_{14} to be faithful over $\mathbb{F}_3$ we need a field extension $\mathbb{F}_{3^e}$ of $\mathbb{F}_3$ which has C_{14} as a subgroup of its multiplicative group. In particular we require that 14 divides $3^e - 1$. This is true for $e = 6$, but not for $e = 1$.

Therefore all faithful, irreducible representations of C_{14} over $\mathbb{F}_3$ are of dimension 6.

Lemma 2.46. *Let $V = \mathbb{F}_q^d$ be a d-dimensional vector space over $\mathbb{F}_q$ and let G be a subgroup of $\mathrm{GL}(d,q)$ with $G \cong \mathrm{GL}(d/e, q^e)$ for some divisor $e \mid d$. Then G is conjugate in $\mathrm{GL}(d,q)$ to $G_{\psi,e}(d,q)$; the image of $\mathrm{GL}(d/e,q^e)$ under the embedding ψ, (See Construction 2.18).*

Proof. By Lemma 2.25, G is irreducible. Hence by Lemma 1.42, the ring $\mathrm{Hom}_G(V,V)$ is isomorphic to some extension field $\mathbb{F}$, of $\mathbb{F}_q$. By Lemma 1.30, we may identify $\mathrm{Hom}_G(V,V)$ with $E := C_{\mathrm{M}(d,q)}(G) \subseteq \mathrm{M}(d,q)$. Then $C := C_{\mathrm{GL}(d,q)}(G)$ is exactly the invertible elements of E and so $C \cong \mathbb{F}^*$ and $E = C \cup \{0\}$.

The centre $Z := Z(G)$ is isomorphic to $\mathbb{F}_{q^e}^*$. Since $Z \leq C$ we have that $q^e - 1$ must divide $|C|$. Thus $\mathbb{F}$ must contain $\mathbb{F}_{q^e}$ as a subfield and so $\mathbb{F} = \mathbb{F}_{q^{ek}}$ for some $k \geq 1$.

By Lemma 1.30, we may identify $E_C := C_{\mathrm{M}(d,q)}(C) \cong \mathrm{Hom}_C(V,V)$. So $C_{\mathrm{GL}(d,q)}(C)$ is exactly the invertible elements of E_C. Furthermore $E_C = C_{\mathrm{GL}(d,q)}(C) \cup \{0\}$.

The group G commutes with C and so G is a subgroup of $C_{\mathrm{GL}(d,q)}(C)$. Furthermore $C_{\mathrm{GL}(d,q)}(C)$ consists of the invertible elements of E_C and so $C_{\mathrm{GL}(d,q)}(C)$ is the set of C-isomorphisms of V. Therefore $C_{\mathrm{GL}(d,q)}(C)$ must fix each of the homogeneous components of the action of C on V. The group G is irreducible and $G \leq C_{\mathrm{GL}(d,q)}(C)$ and so there can be only one homogeneous component in the action of C on V. Hence C acts homogeneously on V.

Therefore V splits as a direct sum $V = V_1 \oplus \cdots \oplus V_r$ of isomorphic irreducible C-modules and the action of C on each V_i has the same kernel. In particular either all are faithful or all are not.

As C is a subgroup of $\mathrm{GL}(d, q)$, C acts faithfully on V. Therefore the action of C on each V_i must be faithful.

Since $C \cong \mathbb{F}^*$, we have that C is isomorphic to the cyclic group $C_{q^{ek}-1}$. Therefore by Lemma 2.44, all of the faithful irreducible representations of C over $\mathbb{F}_q$ are of dimension ek.

We may therefore apply Lemma 1.38 which demonstrates that there is a ring isomorphism $\beta : E_C \to \mathrm{M}(d/(ek), q^{ek})$.

For any invertible element $\phi \in E_C$ we have that $1 = (\phi\phi^{-1})\beta = (\phi\beta)(\phi^{-1}\beta)$ and so $(\phi\beta)^{-1} = (\phi^{-1}\beta)$. In particular $\phi\beta \in \mathrm{GL}(d/(ek), q^{ek})$.

Define the map $\bar{\beta} : C_{\mathrm{GL}(d,q)}(C) \to \mathrm{GL}(d/(ek), q^{ek})$ by restricting β to the invertible elements of E_C. As β is a ring isomorphism, this map is a group isomorphism.

We consider the case that $k > 1$. By Construction 2.18, we may embed the group $\mathrm{GL}(d/(ek), q^{ek})$ into $\mathrm{GL}(d/e, q^e)$. However any invertible matrix of the form

$$M := \begin{pmatrix} A & B_{1,2} & \dots & B_{1,d/e} \\ B_{2,1} & B_{2,2} & \dots & B_{2,d/e} \\ \vdots & \vdots & \ddots & \vdots \\ B_{d/e,1} & B_{d/e,2} & \dots & B_{d/e,d/e} \end{pmatrix} \in \mathrm{GL}(d/e, q^e)$$

where

$$A := \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{M}(k, q^e)$$

and $B_{i,j} \in \mathrm{M}(k, q^e)$ lies in $\mathrm{GL}(d/e, q^e)$ but not in the image of $\mathrm{GL}(d/(ek), q^{ek})$ under any embedding formed in Construction 2.18, as $A \neq 0$ is not invertible and so is not conjugate to the power of any companion matrix in $\mathrm{GL}(k, q^e)$. Thus $|\mathrm{GL}(d/(ek), q^{ek})| < |\mathrm{GL}(d/e, q^e)| = |G|$.

On the other hand $G \leq C_{\mathrm{GL}(d,q)}(C)$, and so $|G| \leq |C_{\mathrm{GL}(d,q)}(C)| = |\mathrm{GL}(d/(ek), q^{ek})| < |\mathrm{GL}(d/e, q^e)| = |G|$; a contradiction.

Therefore $k = 1$ and $C_{\mathrm{GL}(d,q)}(C) \cong \mathrm{GL}(d/e, q^e)$ so $C_{\mathrm{GL}(d,q)}(C) = G$. Furthermore $E \cong \mathbb{F} \cong \mathbb{F}_{q^e}$ and $\bar{\beta} : C_{\mathrm{GL}(d,q)}(C) = G \to \mathrm{GL}(d/e, q^e)$ is a group isomorphism.

The centre Z of G is isomorphic to $\mathbb{F}_{q^e}^*$ and so is equal to C.

We have that $Z = C$ acts homogeneously on V with each faithful irreducible $\mathbb{F}_q$-module of dimension e. Therefore, up to conjugacy in $\mathrm{GL}(d, q)$, we may write Z as a group of block diagonal matrices:

$$Z = \left\{ \begin{pmatrix} A_i & & 0 \\ & \ddots & \\ 0 & & A_i \end{pmatrix} \;\middle|\; A_i \in \mathrm{GL}(e, q), 1 \leq i \leq q^e - 1 \right\}.$$

Let $A_{\mathrm{gen}} = \begin{pmatrix} A & & 0 \\ & \ddots & \\ 0 & & A \end{pmatrix} \in Z$ be a generator of Z. Then A_{gen} has order $q^e - 1$ and $A \in \mathrm{GL}(e, q)$.

We identify A_{gen} with A and with a primitive element α, of the field $\mathbb{F}_{q^e}$. This element α has a minimal polynomial m of degree e over the field $\mathbb{F}_q$. Hence the minimal polynomial of $A \in \mathrm{GL}(e, q)$ is of degree e. The characteristic polynomial of an $e \times e$ matrix is a monic polynomial of degree e, and the minimal polynomial divides the characteristic polynomial. Thus the minimal and characteristic polynomials of A coincide.

Therefore by Lemma 2.11, A is conjugate in $\mathrm{GL}(e, q)$ to the companion matrix C_α of m. Hence by the method used in the proof of Lemma 2.20, Z is conjugate in $\mathrm{GL}(d, q)$ to $Z(G_{\psi,e}(d, q))$. By Lemma 2.39, $G_{\psi,e}(d, q)$ is the centralizer of $Z(G_{\psi,e}(d, q))$ in $\mathrm{GL}(d, q)$. Therefore G is conjugate in $\mathrm{GL}(d, q)$ to $G_{\psi,e}(d, q)$. □

Corollary 2.47. *Let $V = \mathbb{F}_q^d$ and let $G \leq \mathrm{GL}(d, q)$ be irreducible with $C := C_{\mathrm{GL}(d,q)}(G) \cong \mathbb{F}_{q^e}^*$ where $e \mid d$. Then $C_{\mathrm{GL}(d,q)}(C)$ is conjugate in $\mathrm{GL}(d, q)$ to $G_{\psi,e}(d, q)$, the image of $\mathrm{GL}(d/e, q^e)$ under the embedding ψ, as defined in Construction 2.18.*

Proof. This proof is mostly a repetition of the proof of 2.46 above, but we include it for completeness.

By Lemma 1.30, we may identify $\mathrm{Hom}_C(V, V)$ with $E_C := C_{\mathrm{M}(d,q)}(C) \subseteq \mathrm{M}(d, q)$ and so $C_{\mathrm{GL}(d,q)}(C) = E_C \setminus \{0\}$.

The group G commutes with C and so G is a subgroup of $C_{\mathrm{GL}(d,q)}(C)$. Furthermore $C_{\mathrm{GL}(d,q)}(C)$ is the set of C-isomorphisms of V and so $C_{\mathrm{GL}(d,q)}(C)$ must fix each of the homogeneous components of the action of C on V. However G is irreducible

and a subgroup of $C_{\mathrm{GL}(d,q)}(C)$, therefore $C_{\mathrm{GL}(d,q)}(C)$ is also irreducible over V. In particular there can be only one homogeneous component of the action of C on V. Hence C acts homogeneously on V.

The group C is a subgroup of $\mathrm{GL}(d,q)$ and so C acts faithfully on V. Hence the action of C on each of its irreducible components V_i must be faithful (as the action of C on each V_i must have the same kernel).

By Lemma 2.44, all of the faithful irreducible representations of C over $\mathbb{F}_q$ are of dimension e. Therefore by Lemma 1.38, there is a ring isomorphism $\beta : E_C \to \mathrm{M}(d/e, q^e)$ that restricts to a group isomorphism $\bar{\beta} : C_{\mathrm{GL}(d,q)}(C) \to \mathrm{GL}(d/e, q^e)$.

We therefore have that $C_{\mathrm{GL}(d,q)}(C)$ is irreducible and isomorphic to $\mathrm{GL}(d/e, q^e)$. Thus by Lemma 2.46, $C_{\mathrm{GL}(d,q)}(C)$ is conjugate in $\mathrm{GL}(d,q)$ to $G_{\psi,e}(d,q)$. □

Lemma 2.48. *Let $N_G := N_{\mathrm{GL}(d,q)}(G_{\psi,e}(d,q))$ then $N_G = \Gamma_{\psi,e}(d,q)$, the image of $\Gamma\mathrm{L}(d/e, q^e)$ in $\mathrm{GL}(d,q)$ under the embedding described in Construction 2.31.*

Proof. Let $C := Z(G_{\psi,e}(d,q))$. By Lemma 2.39, $G_{\psi,e}(d,q) = C_{\mathrm{GL}(d,q)}(C)$. Therefore $N_{\mathrm{GL}(d,q)}(G_{\psi,e}(d,q)) = N_{\mathrm{GL}(d,q)}(C)$.

Let $\alpha \in \mathbb{F}_{q^e}$ be the primitive element used in the definition of ψ and let C_α be the companion matrix of the minimal polynomial of α. We note that C is generated by $c := \mathrm{Diag}_{d/e}(C_\alpha)$.

If c is conjugate in $\mathrm{GL}(d,q)$ to c^k for some k, then c and c^k must have the same minimal polynomial by Lemma 2.11. Hence α and α^k must have the same minimal polynomial over $\mathbb{F}_q$. This minimal polynomial must be of degree e. There can therefore be at most e elements of $\mathbb{F}_{q^e}$ with this minimal polynomial and so, as in Construction 2.31, these elements must be $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{e-1}}$.

Therefore c has at most e distinct conjugates in $N_{\mathrm{GL}(d,q)}(C)$, and by Construction 2.31, c has e distinct conjugates in $\Gamma_{\psi,e}(d,q)$. Furthermore $\Gamma_{\psi,e}(d,q)$ contains $C_{\mathrm{GL}(d,q)}(C)$ and so $N_G = N_{\mathrm{GL}(d,q)}(G_{\psi,e}(d,q)) = N_{\mathrm{GL}(d,q)}(C) = \Gamma_{\psi,e}(d,q)$. □

Corollary 2.49. *Let G be an irreducible subgroup of $\mathrm{GL}(d,q)$ with $G \cong \Gamma\mathrm{L}(d/e, q^e)$ for some divisor $e \mid d$. Then G is conjugate in $\mathrm{GL}(d,q)$ to $\Gamma_{\psi,e}(d,q)$, the image of $\Gamma\mathrm{L}(d/e, q^e)$ under the embedding described in Construction 2.31.*

Proof. As $G \cong \Gamma\mathrm{L}(d/e, q^e)$ we have that $G \cong \mathrm{GL}(d/e, q^e) \rtimes C_e$. Hence there exists $H \leq G$ such that $H \cong \mathrm{GL}(d/e, q^e)$. Thus by Lemma 2.25, H is irreducible and so by Lemma 2.46, H is conjugate in $\mathrm{GL}(d,q)$ to $G_{\psi,e}(d,q)$. Therefore by Lemma 2.48, G is conjugate in $\mathrm{GL}(d,q)$ to $G_{\psi,e}(d,q) \rtimes C_e = \Gamma_{\psi,e}(d,q)$. □

Definition 2.50. Let G be an irreducible subgroup of $\mathrm{GL}(d,q)$. We call G *semilinear* if G is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $\Gamma_{\psi,e}(d,q)$.

Corollary 2.51. *Let $G \leq \mathrm{GL}(d,q)$ be irreducible but not absolutely irreducible. Then G is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$ for some divisor e of d. In particular, G is semilinear.*

Proof. Let $V := \mathbb{F}_q^e$. The group $G \leq \mathrm{GL}(d,q)$ is irreducible but not absolutely irreducible. Therefore by Lemma 1.45, we have that $\mathrm{Hom}_G(V,V) \cong \mathbb{F}_{q^e}$ for some $e \mid d$. By Lemma 1.30 we may identify $\mathrm{Hom}_G(V,V)$ with $E := C_{\mathrm{M}(d,q)}(G) \subseteq \mathrm{M}(d,q)$. Hence $C := C_{\mathrm{GL}(d,q)}(G)$ is equal to $E \setminus \{0\} \cong \mathbb{F}_{q^e}^*$.

By Corollary 2.47, we have that $C_{\mathrm{GL}(d,q)}(C)$ is conjugate in $\mathrm{GL}(d,q)$ to $G_{\psi,e}(d,q)$.

We observe that every element of G must commute with every element of C and so $G \leq C_{\mathrm{GL}(d,q)}(C)$. Thus G is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$.

As $G_{\psi,e}(d,q) \leq \Gamma_{\psi,e}(d,q)$ we have that G is semilinear. □

Lemma 2.52. *Let G be an absolutely irreducible subgroup of $\mathrm{GL}(d,q)$ where $d > 1$. Suppose that G contains a normal subgroup N of prime index e. Then N is non-scalar.*

Proof. As the index of N in G is a prime e, we have that $G = N\langle g \rangle$ where $g^e \in N$ but $g \notin N$. If every element of N was a scalar then this would imply that G is abelian. Therefore the absolutely irreducible representations of G would have dimension 1. This is a contradiction and so N is non-scalar. □

Lemma 2.53. *Let G be an absolutely irreducible subgroup of $\mathrm{GL}(d,q)$. Suppose that G has a homogeneous normal subgroup N and that there exists a divisor $e \mid d$ such that for any irreducible component, W of N, $\mathrm{Hom}_N(W,W) \cong \mathbb{F}_{q^e}$. Then N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$ and G is semilinear.*

Proof. We suppose that N has t irreducible components in its action on $V = \mathbb{F}_q^d$. Then as $\mathrm{Hom}_N(W,W) \cong \mathbb{F}_{q^e}$, by Lemma 1.38, we have that $C_N := C_{\mathrm{GL}(d,q)}(N)$ is isomorphic to $\mathrm{GL}(t,q^e)$. We observe that C_N acts transitively on the set of irreducible N-submodules of V. Therefore the subgroup $N_C := \langle N, C_N \rangle$ acts irreducibly on V.

The centre of N_C contains the centre of $C_N \cong \mathrm{GL}(t,q^e)$. In particular the centre of N_C contains a cyclic subgroup C, of order $q^e - 1$, and there exists an isomorphism which maps C onto the centre of $\mathrm{GL}(t,q^e)$. We may therefore identify C with the centre of $\mathrm{GL}(t,q^e)$.

As C is the centre of an irreducible group, C must act homogeneously on V. Therefore as in the proof of Corollary 2.47, C is conjugate in $\mathrm{GL}(d,q)$ to the centre

of $G_{\psi,e}(d,q)$. Therefore by Lemma 2.48, $N_{\mathrm{GL}(d,q)}(C) = \Gamma_{\psi,e}(d,q)$.

The normalizer of N must also normalize $Z(C_{\mathrm{GL}(d,q)}(N))$ and so the claim follows. □

Lemma 2.54. *Let G be an absolutely irreducible subgroup of $\mathrm{GL}(d,q)$. If G is semilinear, then for some prime divisor e of d, G has a non-scalar normal subgroup N of index e such that N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$.*

Proof. If G is semilinear then G is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $\Gamma_{\psi,e}(d,q)$ for some $e \mid d$ and embedding $\psi : \mathrm{GL}(d/e, q^e) \to \mathrm{GL}(d,q)$. We may choose e to be prime, as for any non-prime $e = ab$ we have the following embedding,

$$\Gamma\mathrm{L}(d/(ab), q^{(ab)}) \to \Gamma\mathrm{L}(d/a, q^a).$$

Thus, setting $e := a$ we may repeat this embedding until e is prime.

By Construction 2.31, we have that $\Gamma_{\psi,e}(d,q) \cong \Gamma\mathrm{L}(d/e, q^e) = \mathrm{GL}(d/e, q^e) \rtimes C_e$. Hence $\Gamma_{\psi,e}(d,q)$ has a normal subgroup $\hat{N}$ which is conjugate in $\mathrm{GL}(d,q)$ to $\mathrm{GL}(d/e, q^e)$ and $\hat{N}$ is of index e, a prime in $\Gamma_{\psi,e}(d,q)$. In particular $\hat{N}$ is *not* absolutely irreducible.

The intersection $N := \hat{N} \cap G$ is a normal subgroup of G, conjugate to a subgroup of $G_{\psi,e}(d,q)$, with index either 1 or e in G, as e is prime. If the index is 1, then $G = N$ is conjugate to a subgroup of $G_{\psi,e}(d,q)$ and hence is not absolutely irreducible; a contradiction. Therefore the index must be e. The group G is absolutely irreducible and N has prime index $e \mid d$. Hence by Lemma 2.52, N is non-scalar. □

Lemma 2.55. *Let $G \leq \mathrm{GL}(d,q)$ be absolutely irreducible (acting on $V = \mathbb{F}_q^d$) and $N \trianglelefteq G$ a non-scalar normal subgroup. By Clifford's Theorem (2.37), V decomposes as a direct sum, $V = W_1 \oplus W_2 \oplus \cdots \oplus W_t$, of irreducible $\mathbb{F}_q N$-modules each of the same dimension. The modules W_i for $1 \leq i \leq t$ are isomorphic to the composition factors for V as an $\mathbb{F}_q N$-module.*

Proof. We consider the series

$$\{0\} \subset W_1 \subset W_1 \oplus W_2 \subset \cdots \subset W_1 \oplus \cdots \oplus W_t = V.$$

This is a composition series for V with composition factors $W_1, \ldots, W_t$. Hence by the Jordan-Hölder Theorem (1.49), the W_i's are the unique (up to isomorphism) composition factors for V as an $\mathbb{F}_q N$-module. □

Definition 2.56. We denote a linear representation of a group G over a field $\mathbb{F}$ by U_G. Thus for some $d \in \mathbb{N}$, we have a homomorphism $U_G : G \to \mathrm{GL}(d, \mathbb{F})$. For a subgroup $N \leq G$ the representation U_G gives rise to a representation U_N where $U_N : N \to \mathrm{GL}(d, \mathbb{F})$ with $U_N(n) := U_G(n)$, called the restriction of U_G to N. We define $U_N^{(1)}, \ldots, U_N^{(m)}$ to be a complete list of the inequivalent irreducible representations of N which occur in the decomposition of U_N.

The following result is [11, Theorem 3].

Theorem 2.57. *Let G be a group and $N \trianglelefteq G$. We let U_G be a linear representation of G over an algebraically closed field $\mathbb{F}$ and we let U_N be the restriction of U_G to N. We assume that all of the irreducible components of U_N are isomorphic, i.e. $U_N = l \cdot U_N^{(1)}$ for some $l \in \mathbb{N}$. Then there exist irreducible projective representations, C and Γ, of G such that*

$$U_G(g) = C(g) \otimes \Gamma(g),$$

where Γ is of degree l and C has the same degree as $U_N^{(1)}$. Moreover $g \mapsto \Gamma(g)$ is an irreducible projective representation of the factor group G/N.

Remark 2.58. Theorem 2.57 assumes that all of the irreducible components of U_N are isomorphic. This is equivalent to assuming that N is a homogeneous subgroup of G.

2.3. **Constructing the test.** In this section we will construct our semilinear test.

Proposition 2.59. *Let G be an absolutely irreducible subgroup of $\mathrm{GL}(d,q)$ and let $V = \mathbb{F}_q^d$ be its natural module. The group G is semilinear if and only if there exists a homogeneous normal subgroup $N \trianglelefteq G$, such that N is of prime index $e \mid d$ in G, N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$, N acts on V with irreducible constituents $W_1, \ldots, W_t$, and N does not act absolutely irreducibly on its irreducible constituents. In this case for each W_i, the restriction $N|_{W_i} \leq \mathrm{GL}(W_i)$ is conjugate in $\mathrm{GL}(W_i) \cong \mathrm{GL}(d/t,q)$ to a subgroup of $G_{\psi_t,e}(d/t,q) \cong \mathrm{GL}(d/(te),q^e)$; where the embedding $\psi_t : \mathrm{GL}(d/(te),q^e) \to \mathrm{GL}(d/t,q)$ is defined in the same way as in Construction 2.18.*

Proof. ($\Leftarrow$) Suppose that G has such an N. Then N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$, the index of N in G is a prime dividing d, and N is homogeneous. Furthermore N acts irreducibly but not absolutely irreducibly on each irreducible constituent W and so by Lemma 1.45, $\mathrm{Hom}_N(W,W) = \mathbb{F}_{q^e}$. Therefore G is semilinear as demonstrated in Lemma 2.53.

($\Rightarrow$) Let G be semilinear. Then by Lemma 2.54, there exists a non-scalar normal subgroup N of G such that N is of prime index $|G : N| = e$, where $e \mid d$ and N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$. In particular $G = N\langle g \rangle$ for some $g \in G \setminus N$ with $g^e \in N$.

The group G acts absolutely irreducibly on V and as N is a non-scalar normal subgroup of G, we may apply Clifford's Theorem (2.37). This demonstrates that V decomposes as a direct sum $V = W_1 \oplus \cdots \oplus W_t$ of irreducible $\mathbb{F}_q N$-modules each of dimension d/t.

If $t = 1$, then N acts irreducibly on V and our conclusion holds. Therefore we suppose that $t > 1$.

By Clifford's Theorem (2.37), for some $r, s \geq 1$ with $rs = t$, the set $\{W_1, \ldots, W_t\}$ partitions into r subsets, each containing s pairwise isomorphic $\mathbb{F}_q N$-modules. Furthermore if $V_1, \ldots, V_r$ are each defined to be the sum of s pairwise isomorphic W_i then $V = V_1 \oplus \cdots \oplus V_r$, and G permutes the V_i's transitively.

Case 1: $r > 1$**.** In this case N is inhomogeneous. The group G/N has order e, a prime, and permutes the r homogeneous components transitively. Therefore, by Lemma 1.15, $r = e$ and there are exactly e homogeneous components.

By Clifford's Theorem (2.37 (i)), the stabilizer in G of the first component, V_1, is N. So, by Construction 2.43, G embeds in $N|_{V_1} \wr C_e$ (as e is prime).

If $N|_{V_1}$ is not absolutely irreducible, then $N|_{V_1}$ becomes reducible over an extension field, say $\mathbb{F}$ of $\mathbb{F}_q$. We assume that the image of $N|_{V_1}$ under this extension fixes a subspace X of the image of V_1 over $\mathbb{F}$. Then the image of $N|_{V_1} \wr C_e$ under this extension fixes the subspace $X_1 \oplus \cdots \oplus X_e$ of the image of V over $\mathbb{F}$, where $X_1 = X$ and X_i is the image of X under the permutation mapping $1 \mapsto i$. Hence $N|_{V_1} \wr C_e$ is not absolutely irreducible. This is contrary to the assumption that G acts absolutely irreducibly. Thus we assume that $N|_{V_1}$ is absolutely irreducible.

Then by Lemma 1.35, we have that $C_{\mathrm{GL}(V_i)}(N|_{V_i}) \cong \mathbb{F}_q^*$ for $1 \leq i \leq e$. Under the action of N on V the homogeneous components, $V_1, \ldots, V_e$, are mutually non-isomorphic $\mathbb{F}_q N$-modules.

By Lemma 1.30, we may identify $\mathrm{Hom}_N(V, V)$ with $E_N := C_{\mathrm{M}(d,q)}(N)$. Then the centralizer $C_{\mathrm{GL}(d,q)}(N) = E_N \setminus \{0\}$ is exactly the invertible elements of E_N. Thus every element of $C_{\mathrm{GL}(d,q)}(N)$ is an $\mathbb{F}_q N$-module isomorphism $V \to V$ and so each element of $C_{\mathrm{GL}(d,q)}(N)$ maps each (non-isomorphic) homogeneous component to itself.

It follows that $C_{\mathrm{GL}(d,q)}(N) \leq C_{\mathrm{GL}(V_1)}(N|_{V_1}) \times \cdots \times C_{\mathrm{GL}(V_e)}(N|_{V_e})$, where $N|_{V_i} \leq \mathrm{GL}(V_i)$ and $1 \leq i \leq e$. Therefore $C_{\mathrm{GL}(d,q)}(N) \leq (C_{q-1})^e$.

By Lemma 2.39, $C := C_{\mathrm{GL}(d,q)}(G_{\psi,e}(d,q)) \cong \mathbb{F}_{q^e}^*$ and $C \leq G_{\psi,e}(d,q)$. Furthermore N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$. Therefore there exists a group $C_N \cong C$ such that $C_N \leq C_{\mathrm{GL}(d,q)}(N) \leq (C_{q-1})^e$. This is a contradiction as $(C_{q-1})^e$ does not contain an element of order $q^e - 1$.

Case 2: $r = 1$**.** In this case N is homogeneous and V decomposes as a direct sum $V = W_1 \oplus \cdots \oplus W_t$ of pairwise isomorphic, irreducible $\mathbb{F}_q N$-modules. We let

$W := W_1$ and we let a denote the dimension of W, then $d = at$ (where $t > 1$).

By Lemma 1.42, $\mathrm{Hom}_N(W, W)$ is isomorphic to a field of order q^k for some $k \geq 1$. By Lemma 1.30, we may identify $\mathrm{Hom}_N(W, W)$ with $E := C_{\mathrm{M}(a,q)}(N)$. Hence $E \setminus \{0\} = C_{\mathrm{GL}(a,q)}(N) \cong \mathbb{F}^*_{q^k}$.

As V splits as a direct sum of t pairwise isomorphic N-modules and $\mathrm{Hom}_N(W, W) \cong \mathbb{F}_{q^k}$, by Lemma 1.38, we have that $\mathrm{Hom}_N(V, V)$ is isomorphic to $\mathrm{M}(t, q^k)$ and so

$$C_{\mathrm{GL}(d,q)}(N) \cong \mathrm{GL}(t, q^k). \qquad (\star)$$

We define an embedding $\rho : \mathrm{GL}(a/k, q^k) \to \mathrm{GL}(a, q)$ in the same way as in Construction 2.18. We denote the image of $\mathrm{GL}(a/k, q^k)$ under this embedding by $G_{\rho,k}(a, q)$.

Since $C_{\mathrm{GL}(a,q)}(N) \cong \mathbb{F}^*_{q^k}$, Corollary 2.47 demonstrates that, $C_{\mathrm{GL}(a,q)}(C_{\mathrm{GL}(a,q)}(N))$ is conjugate in $\mathrm{GL}(a, q)$ to $G_{\rho,k}(a, q)$.

The group $N|_W$ commutes with $C_{\mathrm{GL}(a,q)}(N)$ and so $N|_W$ is a subgroup of $C_{\mathrm{GL}(a,q)}(C_{\mathrm{GL}(a,q)}(N))$. Hence $N|_W$ is conjugate in $\mathrm{GL}(a, q)$ to a subgroup of $G_{\rho,k}(a, q)$.

Case 2(a): e does not divide k. By $(\star)$, we have that the centralizer of N in $\mathrm{GL}(d, q)$ is isomorphic to $\mathrm{GL}(t, q^k)$.

By Lemma 2.39, the centralizer of $G_{\psi,e}(d, q)$ in $\mathrm{GL}(d, q)$ is homogeneous and isomorphic to $\mathbb{F}^*_{q^e}$. The group N is conjugate in $\mathrm{GL}(d, q)$ to a subgroup of $G_{\psi,e}(d, q)$ and so the centralizer of N in $\mathrm{GL}(d, q)$ contains a homogeneous cyclic subgroup of order $q^e - 1$. In particular $q^e - 1$ divides $|\mathrm{GL}(t, q^k)|$.

We claim that $t \geq e$.

Consider the order

$$|\mathrm{GL}(t, q^k)| = (q^{kt} - 1)(q^{k(t-1)} - 1)(q^{k(t-2)} - 1) \dots (q^k - 1)q^{km} \qquad (\star\star)$$

where $m = \sum_{i=1}^{t-1} i$.

We now apply Zsigmondy's Theorem (Theorem 2.23) with $a = q$, $b = 1$, and $d = e$.

If $q, 1$, and d are not exceptions to Zsigmondy's Theorem then we have the following.

There exists a primitive prime divisor l, of $q^e - 1$. In this case q is of order e modulo l. We have that $(q^e - 1)$ divides $|\mathrm{GL}(t, q^k)|$, which implies that l must also

divide the order $|\mathrm{GL}(t, q^k)|$. Hence l divides $(q^{kc} - 1)$ for some $1 \leq c \leq t$. Since l is a primitive prime divisor of $q^e - 1$, we must have that e divides kc. In which case e divides c, as e does not divide k. Therefore $t \geq e$.

We now go through the exceptions to Zsigmondy's Theorem in turn to check whether they arise, and if so whether they satisfy the outcome of our claim.

- In the first case we have that $e = 1$ which contradicts the primality of e. So this case does not arise.
- In the second case we have that $e = 2$. Since $t > 1$ we still have that $t \geq e$ here.
- In the last case we have that $e = 6$ which contradicts the primality of e. So this case does not arise.

Therefore we always have $t \geq e$ (when e does not divide k).

The normal subgroup N has e cosets in G, which may be represented by g^i for $1 \leq i \leq e$. There can be at most e different images, W^{g^i} of W under g^i, for $1 \leq i \leq e$. Define $W' := \langle W^{g^i} \mid 1 \leq i \leq e \rangle$. As $\dim(W) = a$ we have that $\dim(W^{g^i}) = a$ for all $1 \leq i \leq e$. Therefore $\dim(W') \leq ae$. Since the group G is irreducible and W' is non-trivial and stabilized by G, we have that $W' = V$. So $at = \dim(V) = \dim(W') \leq ae$. Hence $t \leq e$.

Therefore $t = e$ and so the order of $\langle g \rangle$ is equal to the number of isomorphic irreducible $\mathbb{F}_q N$-modules. We make the following notation change. Let $W_1 = W$ and for each $2 \leq i \leq t$ we define $W_i := W g^{i-1}$.

Therefore g permutes the W_i's transitively and N is the stabilizer of W. Thus G embeds in $N|_W \wr C_e$ as in **Case 1** - the inhomogeneous case.

We observe that, as in **Case 1**, $N|_W$ is absolutely irreducible as otherwise $N|_W \wr C_e$ is not absolutely irreducible, which is a contradiction.

We extend $\mathbb{F}_q$ to an algebraically closed field $\mathbb{F}$. Let $\iota : \mathrm{GL}(d, q) \to \mathrm{GL}(d, \mathbb{F})$ be the natural embedding and let $\tilde{G}$ be the image of G under ι, so $G \cong \tilde{G} \leq \mathrm{GL}(d, \mathbb{F})$. As G is absolutely irreducible, $\tilde{G}$ is also absolutely irreducible.

Define $\tilde{N}$ to be the image of N under ι. So $N \cong \tilde{N} \trianglelefteq \tilde{G}$. As $N|_W$ is absolutely irreducible, when we extend to $\mathbb{F}$ the W_i's remain irreducible. The group $\tilde{G}$ acts absolutely irreducibly on $\tilde{V} := \mathbb{F}^d$ and $\tilde{N}$ is a non-scalar normal subgroup of $\tilde{G}$, so we may apply Clifford's Theorem (2.37). Therefore the vector space $\tilde{V}$ decomposes as a direct sum $\tilde{V} = \tilde{W}_1 \oplus \cdots \oplus \tilde{W}_t$ of irreducible $\mathbb{F}\tilde{N}$-modules each of the same dimension d/t.

As N acts homogeneously on V and acts absolutely irreducibly on its components, $\tilde{N}$ acts homogeneously on $\tilde{V}$. Therefore $\tilde{V}$ decomposes as a direct sum of pairwise isomorphic, irreducible $\mathbb{F}\tilde{N}$-modules. In particular, in the notation of Theorem 2.57, $U_{\tilde{N}} = t \cdot U_{\tilde{N}}^{(1)}$.

Hence by Theorem 2.57, there exists an irreducible projective representation Γ, of $\tilde{G}/\tilde{N}$ of degree t. However $\tilde{G}/\tilde{N}$ is cyclic and so all projective irreducible representations of $\tilde{G}/\tilde{N}$ are of degree 1. Hence $t = 1$ and so as $t = e$ a prime, this is a contradiction.

Case 2(b): e divides k. Here we have that $k = ef$ for some $f \in \mathbb{N}$. The restriction $N|_W$ is conjugate in $\mathrm{GL}(a, q)$ to a subgroup of $G_{\rho,k}(a, q)$, and

$$G_{\rho,k}(a, q) \cong \mathrm{GL}(a/k, q^k) = \mathrm{GL}(a/(ef), q^{(ef)}).$$

By the same method as in Construction 2.18, we may define an embedding, $\psi_t : \mathrm{GL}(d/(te), q^e) \to \mathrm{GL}(d/t, q)$ so that the group $G_{\rho,k}(a, q)$ is conjugate in $\mathrm{GL}(a, q)$ to a subgroup of the image, $G_{\psi_t,e}(a, q)$, of $\mathrm{GL}(d/(te), q^e)$ under the embedding ψ_t. So

$$G_{\psi_t,e}(a, q) \cong \mathrm{GL}(a/e, q^e) = \mathrm{GL}(d/(te), q^e).$$

Thus, writing $A \overset{\text{conj}}{\underset{\mathrm{GL}(a,q)}{\leq}} B$, to denote that A is conjugate to a subgroup of B in $\mathrm{GL}(a, q)$, we have

$$N|_W \overset{\text{conj}}{\underset{\mathrm{GL}(a,q)}{\leq}} G_{\rho,k}(a, q) \overset{\text{conj}}{\underset{\mathrm{GL}(a,q)}{\leq}} G_{\psi_t,e}(a, q) = G_{\psi_t,e}(d/t, q).$$

Hence, $N|_W$ is conjugate in $\mathrm{GL}(a, q) = \mathrm{GL}(d/t, q)$ to a subgroup of $G_{\psi_t,e}(d/t, q)$. Therefore we have proved our proposition in this case. □

2.4. **The test.** We now give the semilinear test.

The Semilinear Test

Input: An irreducible group $G \leq \mathrm{GL}(d, q)$.
Output: **true** if G is semilinear, **false** if G is not semilinear.

Step 1: Check for absolute irreducibility.
If G is not absolutely irreducible then:
Return: true, *G is semilinear by Corollary 2.51.*

Step 2: Define the list **Norm** of all normal subgroups of G whose index is a prime dividing d.
If **Norm** is empty then:
Return: false, *G is not semilinear by Proposition 2.59.*

Step 3: For each normal subgroup $N \in$ **Norm** do the following:

Step 3(a): Define M to be the natural d-dimensional $\mathbb{F}_q N$-module of N.

Step 3(b): Test whether the composition factors of M are isomorphic.
If they are not isomorphic then:
Continue: N.
If they are not isomorphic then N is not acting homogeneously in the way described in Proposition 2.59. So we move on to test the next N in **Norm**.

Step 3(c): *The composition factors of M must be isomorphic.*
Test whether the composition factors of M are absolutely irreducible.
If they are not then:
Return: true, *G is semilinear.*

Step 4: *No choice of N proves that G is not semilinear.*
Return: false.

2.5. **A cleaner test.** We are now going to refine the semilinear test. We give the theory behind this new test, and the test, below.

We use Theorem 2.57 together with Proposition 2.59 to prove Theorem 2.60, which is the theoretical base for our new semilinear test.

Theorem 2.60. *Let $G \leq \mathrm{GL}(d,q)$ be an absolutely irreducible subgroup.*

(i) If G is semilinear then there exists a normal subgroup, $N \trianglelefteq G$ of index e, where e is a prime divisor of d, such that N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$, and N is irreducible.

(ii) If there exists an irreducible normal subgroup, $N \trianglelefteq G$ of index e, where e is a prime divisor of d, such that N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$, then G is semilinear.

Proof. (i) Let $G \leq \mathrm{GL}(d,q)$ be an absolutely irreducible semilinear group. By Proposition 2.59 there exists a homogeneous normal subgroup $N \trianglelefteq G$ such that N is of prime index $e = |G : N|$, where $e \mid d$, and N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$.

It remains to show that N is irreducible. We follow the same reasoning as the proof of **Case 2(a)** in Proposition 2.59.

We extend $\mathbb{F}_q$ to an algebraically closed field $\mathbb{F}$, and we consider the natural embedding, $\iota : \mathrm{GL}(d,q) \to \mathrm{GL}(d,\mathbb{F})$. Let $\tilde{G}$ be the image of G under ι, so $G \cong \tilde{G} \leq \mathrm{GL}(d,\mathbb{F})$. As G is absolutely irreducible, $\tilde{G}$ is also absolutely irreducible.

Define $\tilde{N}$ to be the image of N under ι. So $N \cong \tilde{N} \trianglelefteq \tilde{G}$. The group $\tilde{G}$ acts absolutely irreducibly on $\tilde{V} := \mathbb{F}^d$ and $\tilde{N}$ is a non-scalar normal subgroup of $\tilde{G}$, so we may apply Clifford's Theorem (2.37). This demonstrates that the vector space $\tilde{V}$ decomposes as a direct sum $\tilde{V} = \tilde{W}_1 \oplus \cdots \oplus \tilde{W}_t$ of irreducible $\mathbb{F}\tilde{N}$-modules each of the same dimension d/t.

If $\tilde{N}$ acts homogeneously on $\tilde{V}$ then $\tilde{V}$ decomposes as a direct sum of pairwise isomorphic, irreducible $\mathbb{F}\tilde{N}$-modules. In particular, in the notation of Theorem 2.57, $U_{\tilde{N}} = t \cdot U_{\tilde{N}}^{(1)}$.

Therefore by Theorem 2.57, there exists an irreducible projective representation, Γ, of $\tilde{G}/\tilde{N}$ of degree t. However $\tilde{G}/\tilde{N}$ is cyclic and so all projective irreducible representations of $\tilde{G}/\tilde{N}$ are of degree 1. Hence $t = 1$ and so $\tilde{N}$ is irreducible.

This implies that N is absolutely irreducible, a contradiction as N is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of $G_{\psi,e}(d,q)$, a non-absolutely irreducible group.

Hence $\tilde{N}$ must act inhomogeneously on $\tilde{V}$. So $\tilde{V}$ decomposes as a direct sum $\tilde{V} = \tilde{W}_1 \oplus \cdots \oplus \tilde{W}_t$ of irreducible d/t-dimensional $\mathbb{F}\tilde{N}$-modules which are not all pairwise isomorphic.

The quotient $\tilde{G}/\tilde{N}$ has prime order e and permutes the components transitively. Therefore by Lemma 1.15, there are exactly e homogeneous components, so $\tilde{V} = \tilde{V}_1 \oplus \cdots \oplus \tilde{V}_e$. We note that $t \geq e$.

Let $\tilde{g}$ be a generator of $\tilde{G}/\tilde{N}$. There can be at most e different images $\tilde{W}_1^{\tilde{g}^i}$, of $\tilde{W}_1$ under $\tilde{g}^i$ for $1 \leq i \leq e$. We consider $\tilde{W}' := \langle \tilde{W}_1^{\tilde{g}^i} \mid 1 \leq i \leq e \rangle$. We have that $\dim(\tilde{W}_1^{\tilde{g}^i}) = \dim(\tilde{W}_1)$ for all $1 \leq i \leq e$. Therefore $\dim(\tilde{W}') \leq \dim(\tilde{W}_1)e$. Since $\tilde{G}$ is irreducible and $\tilde{W}'$ is non-trivial, $\tilde{W}' = \tilde{V}$. We have that $\dim(\tilde{W}_1)t = \dim(\tilde{V}) = \dim(\tilde{W}') \leq \dim(\tilde{W}_1)e$. Hence $t \leq e$.

Therefore as $t \geq e$, we have that $t = e$ and so each $\tilde{V}_i$ must be irreducible. Hence by Lemma 2.55, $\tilde{V}$ has e composition factors which are mutually non-isomorphic.

We now reconsider $N \trianglelefteq G \leq \mathrm{GL}(d,q)$. We know that N is homogeneous and we assume that V decomposes as the sum of $s > 1$ isomorphic irreducible $\mathbb{F}_q N$-modules, so $V = W_1 \oplus \cdots \oplus W_s$. Therefore by Lemma 2.55, there are s isomorphic composition

factors for V.

From Theorem 1.41, we see that by extending $\mathbb{F}_q$ to $\mathbb{F}$, each of these s composition factors are mapped to isomorphic composition factors of $\tilde{V}$. Therefore each composition factor of $\tilde{V}$ must occur at least s times.

Hence $s = 1$ and so N is irreducible.

(ii) This is a special case of the converse direction of Proposition 2.59 ($t = 1$). □

We now give the new test. This test is far shorter to code than the original, although it currently takes around the same time to run.

The New Semilinear Test

Input: An irreducible group $G \leq \mathrm{GL}(d, q)$.
Output: **true** if G is semilinear, **false** if G is not semilinear.

Step 1: Check for absolute irreducibility.
If G is not absolutely irreducible then:
Return: true, *G is semilinear by Corollary 2.51.*

Step 2: Define the list **Norm** of all irreducible but not absolutely irreducible subgroups of G of prime index dividing d.
If **Norm** is empty then:
Return: false, *G is not semilinear by Theorem 2.60 (i)*
If **Norm** is non-empty then:
Return: true, *G is semilinear by Theorem 2.60 (ii).*

3. Classification of Primitive Groups of Degree $4096 \leq d < 8192$

In this section we classify the primitive permutation groups of degree $4096 \leq d < 8192$ up to permutation isomorphism (see Definition 1.7), following similar methods to [13]. We use the O'Nan-Scott Theorem (Theorem 1.11) to break this classification into five disjoint cases.

As in [15, p.213], we shall divide the set of all primitive groups into *cohorts*, where two primitive groups G_1 and G_2 lie in the same cohort if and only if $\deg(G_1) = \deg(G_2)$ and the socle of G_1 is permutation isomorphic to the socle of G_2.

We see immediately that there are no twisted wreath product (regular non-abelian) type groups with degree less than 8192, since the smallest degree of such a group is $|A_5|^6 = 60^6 = 46656000000$.

We begin with some additional results from the literature.

The following lemma is well known.

Lemma 3.1. *Let $G, H \leq \mathrm{Sym}(\Omega)$ be permutation isomorphic groups. Then $N_{\mathrm{Sym}(\Omega)}(G)$ is permutation isomorphic to $N_{\mathrm{Sym}(\Omega)}(H)$*

Proof. By Lemma 1.17, G and H are conjugate in $\mathrm{Sym}(\Omega)$, so there exists some $\sigma \in \mathrm{Sym}(\Omega)$ such that $G^\sigma = H$. Then by Lemma 1.13, $N_{\mathrm{Sym}(\Omega)}(H) = N_{\mathrm{Sym}(\Omega)}(G^\sigma) = N_{\mathrm{Sym}(\Omega)}(G)^\sigma$ and so $N_{\mathrm{Sym}(\Omega)}(H)$ is permutation isomorphic to $N_{\mathrm{Sym}(\Omega)}(G)$. □

Hence identifying two permutation isomorphic groups also identifies their normalizers in the symmetric group of their degree.

From now on we identify permutation isomorphic groups.

We observe that if $G \leq \mathrm{Sym}(\Omega)$ is primitive with $H := \mathrm{Soc}(G)$ then G lies in $N := N_{\mathrm{Sym}(\Omega)}(H)$. Hence the cohort to which G belongs must consist precisely of all primitive subgroups of N which have H as their socle.

The following is [15, Lemma 3].

Lemma 3.2. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive group with $H := \mathrm{Soc}(G)$ and let $N := N_{\mathrm{Sym}(\Omega)}(H)$. Furthermore suppose that H is either abelian or non-regular. Then every primitive group K with $H \leq K \leq N$ has $\mathrm{Soc}(K) = H$. In particular, K lies in the same cohort as G.*

Remark 3.3. By the O'Nan-Scott Theorem (1.11), as noted above, all primitive groups with degree in the range $4096 \leq d < 8192$ have either abelian or non-regular socles. Hence for our degree range, every primitive group between H and N lies in the same cohort and N is the *unique* largest element in that cohort.

Lemma 3.4. *Let $G_1, G_2 \leq \mathrm{Sym}(\Omega)$ with $\mathrm{Soc}(G_1) = \mathrm{Soc}(G_2) = H$. Then G_1 is permutation isomorphic to G_2 if and only if G_1 is conjugate to G_2 in $N_{\mathrm{Sym}(\Omega)}(H)$.*

Proof. If G_1 is permutation isomorphic to G_2 then by Lemma 1.17, there exists $\sigma \in \mathrm{Sym}(\Omega)$ such that $G_1^\sigma = G_2$. Therefore as $\mathrm{Soc}(G_1) = \mathrm{Soc}(G_2) = H$ we have that $H^\sigma = H$ and so $\sigma \in N_{\mathrm{Sym}(\Omega)}(H)$. On the other hand, if G_1 is conjugate to G_2 in $N_{\mathrm{Sym}(\Omega)}(H)$ then by Lemma 1.17, G_1 is permutation isomorphic to G_2. □

The following result is [16, Corollary 4.3A].

Theorem 3.5. *Let G be a non-trivial finite group and H a minimal normal subgroup of G. Then H is either an elementary abelian p-group for some prime p, or $Z(H)$ is trivial.*

The following is [16, Theorem 4.2A].

Theorem 3.6. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive and let $C := C_{\mathrm{Sym}(\Omega)}(G)$. Then C is transitive if and only if G is regular. Furthermore if C is transitive (so G is regular) then C is conjugate in $\mathrm{Sym}(\Omega)$ to G, and so C is regular.*

The following is [16, Theorem 4.2B].

Theorem 3.7. *Let $G \leq \mathrm{Sym}(\Omega)$ and $N := N_{\mathrm{Sym}(\Omega)}(G)$. Then N acts on G by conjugation, giving a homomorphism $\Psi : N \to \mathrm{Aut}(G)$ where $\Psi(x) : u \mapsto x^{-1}ux$. Let $\alpha \in \Omega$, $\sigma \in \mathrm{Aut}(G)$, and suppose that G is transitive. Then $\sigma \in \mathrm{Im}(\Psi)$ if and only if $(G_\alpha)^\sigma$ is a point stabilizer for G.*

The following is [16, Corollary 4.2B].

Lemma 3.8. *Let $G \leq \mathrm{Sym}(\Omega)$, and let N and Ψ be defined as in Theorem 3.7. If G is regular then $\mathrm{Im}(\Psi) = \mathrm{Aut}(G)$. In this case, for any $\alpha \in \Omega$ we have $N_\alpha \cong \mathrm{Aut}(G)$, and $N = G \rtimes N_\alpha \cong G \rtimes \mathrm{Aut}(G)$.*

Proof. As G is regular, every point stabilizer of G is trivial, and so by Theorem 3.7, $\mathrm{Im}(\Psi) = \mathrm{Aut}(G)$. By Theorem 3.6, $C := C_{\mathrm{Sym}(\Omega)}(G)$ is regular and isomorphic to G. Thus by Lemma 1.14, as $C \trianglelefteq N$ we have, $N = C \rtimes N_\alpha$. Therefore $\mathrm{Aut}(G) = \mathrm{Im}(\Psi) \cong N/\ker(\Psi) = N/C \cong N_\alpha$. Hence $N \cong G \rtimes \mathrm{Aut}(G)$. □

The following is well known.

Lemma 3.9. *Let $G \leq \mathrm{Sym}(\Omega)$ be transitive. If G is abelian, then G is regular.*

Proof. Take any $\alpha \in \Omega$ and consider G_α, the stabilizer of α in G. Let $g \in G_\alpha$ and let $h \in G$, then $\alpha^{hg} = \alpha^{gh} = \alpha^h$. As G is transitive, α^h can be any element of Ω. Thus g fixes every element in Ω and so $g = 1$. Therefore G is regular. □

The following is well known, see for example [15, p.213].

Lemma 3.10. *Let $G, H \leq \mathrm{Sym}(\Omega)$ be transitive. Then G is permutation isomorphic to H if and only if, for any $\alpha, \beta \in \Omega$, there is a group isomorphism $\phi : G \to H$ such that, $\phi(G_\alpha) = H_\beta$.*

Corollary 3.11. *Let $G, H \leq \mathrm{Sym}(\Omega)$ be regular groups. If $G \cong H$ then G and H are permutation isomorphic.*

Proof. As G and H are regular, $G_\alpha = 1$ and $H_\beta = 1$ for any $\alpha, \beta \in \Omega$. Let $\phi : G \to H$ be an isomorphism. Then $\phi(G_\alpha) = H_\beta$ and so by Lemma 3.10, G and H are permutation isomorphic. □

3.1. **Groups of affine type.** We will now classify the primitive groups of affine type of degree d for $4096 \leq d < 8192$.

The following definition is essentially [16, p.54].

Definition 3.12. Let $V = \mathbb{F}_p^k$, where p is prime. The *affine general linear group* $\mathrm{AGL}(k, p)$ is the group consisting of all maps $f_{a,u} : V \to V$ where $a \in \mathrm{GL}(k, p)$ and $u \in V$, such that $f_{a,u}(v) = va + u$.

We have that

$$\begin{aligned}\mathrm{AGL}(k,p)_{0_V} &= \{f_{a,u} : V \to V \mid f_{a,u}(0_V) = 0_V, a \in \mathrm{GL}(k,p), u \in V\} \\ &= \{f_{a,0} : V \to V \mid a \in \mathrm{GL}(k,p)\} \cong \mathrm{GL}(k,p).\end{aligned}$$

The following lemma is essentially [16, p.54].

Lemma 3.13. *Let $V = \mathbb{F}_p^k$, where p is prime and let $T := \{f_{1,u} : V \to V \mid u \in V\}$. Then T is a regular normal subgroup of $\mathrm{AGL}(k, p)$ and $T = \mathrm{Soc}(\mathrm{AGL}(k, p))$.*

We call T the subgroup of *translations* of $\mathrm{AGL}(k, p)$ and we may identify T with the (additive) group $(V, +)$, of the vector space $V = \mathbb{F}_p^k$.

Observe that Lemma 1.14 implies that the group $\mathrm{AGL}(k, p)$ is the semidirect product of T by $\mathrm{AGL}(k, p)_{0_V}$. Hence, as $T \cong V$ and $\mathrm{AGL}(k, p)_{0_V} \cong \mathrm{GL}(k, p)$ we have

$$\mathrm{AGL}(k, p) \cong V \rtimes \mathrm{GL}(k, p)$$

where $\mathrm{GL}(k, p)$ is acting on V via matrix multiplication.

Remark 3.14. By Lemma 1.33, $\mathrm{GL}(k, p) = \mathrm{Aut}(\mathbb{F}_p^k, +)$, so we have that

$$\mathrm{AGL}(k, p) \cong \mathbb{F}_p^k \rtimes \mathrm{Aut}(\mathbb{F}_p^k, +).$$

Lemma 3.15. *The group $\mathrm{AGL}(k, p)$ acts primitively on the vector space $V := \mathbb{F}_p^k$. Thus we may consider $\mathrm{AGL}(k, p)$ as a primitive subgroup of $\mathrm{Sym}(\Omega)$ where $|\Omega| = p^k$. Furthermore $\mathrm{AGL}(k, p) = N_{\mathrm{Sym}(\Omega)}(T)$.*

Proof. We show that $\mathrm{AGL}(k, p)$ acts 2-transitively on V.

Consider any $v_1 \neq v_2 \in V$ and $w_1 \neq w_2 \in V$, so $v_2 - v_1 \neq 0$ and $w_2 - w_1 \neq 0$. Then $f_{\mathrm{Id},-v_1}(v_1) = 0$, $f_{\mathrm{Id},-v_1}(v_2) = v_2 - v_1$, $f_{\mathrm{Id},w_1}(0) = w_1$, and $f_{\mathrm{Id},w_1}(w_2 - w_1) = w_2$.

The group $\mathrm{GL}(k,p)$ acts transitively on the non-zero vectors of V and so there exists $a \in \mathrm{GL}(k,p)$ such that $(v_2 - v_1)a = w_2 - w_1$. Hence the element $f_{a,0} \in \mathrm{AGL}(k,p)$ is such that $f_{a,0}(0) = 0$ and $f_{a,0}(v_2 - v_1) = w_2 - w_1$.

Thus $f_{\mathrm{Id},w_1}(f_{a,0}(f_{\mathrm{Id},-v_1}(v_1))) = w_1$ and $f_{\mathrm{Id},w_1}(f_{a,0}(f_{\mathrm{Id},-v_1}(v_2))) = w_2$. Therefore $\mathrm{AGL}(k,p)$ acts 2-transitively on V. So by Lemma 1.20, $\mathrm{AGL}(k,p)$ acts primitively on V.

We may therefore consider $\mathrm{AGL}(k,p)$ as a primitive subgroup of $\mathrm{Sym}(\Omega)$ where $|\Omega| = p^k$.

As $T \trianglelefteq \mathrm{AGL}(k,p)$ is a regular normal subgroup we may see that by Lemma 3.8, $N_{\mathrm{Sym}(\Omega)}(T) \cong T \rtimes \mathrm{Aut}(T)$. By Remark 3.14, $T \rtimes \mathrm{Aut}(T) \cong \mathrm{AGL}(k,p)$. Thus as $|N_{\mathrm{Sym}(\Omega)}(T)| = |\mathrm{AGL}(k,p)|$ and $T \trianglelefteq \mathrm{AGL}(k,p)$ we have that $\mathrm{AGL}(k,p) = N_{\mathrm{Sym}(\Omega)}(T)$. □

The following is essentially [16, Theorem 4.7A].

Proposition 3.16. *Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive permutation group with $|\Omega| > 1$. Let $H := \mathrm{Soc}(G)$ be abelian. Then there exists a prime p and an integer $k \geq 1$ such that $|\Omega| = p^k$. Furthermore if $V := \mathbb{F}_p^k$, then there is an irreducible subgroup $K \leq \mathrm{GL}(k,p)$ and an isomorphism $\phi : G \to V \rtimes K \leq \mathrm{AGL}(k,p)$ such that $\phi(G_\alpha) = K$, for all $\alpha \in \Omega$.*

Proof. By Lemma 1.4, as G is primitive, H is transitive. Therefore by Lemma 3.9, as H is abelian, H acts regularly on Ω. We show that H is permutation isomorphic to the subgroup of translations $T \trianglelefteq \mathrm{AGL}(k,p)$ for some prime p and some $k \geq 1$. As H is abelian, $Z(H) = H$. Therefore by Theorem 3.5, H is an elementary abelian p-group and so $|H| = p^k$ for some prime p and $k \geq 1$. Since H is regular, $|\Omega| = p^k$ and by Corollary 3.11, H is permutation isomorphic to $T = (V, +)$. So we may identify H with $(V, +)$.

Fix $\alpha \in \Omega$ and consider an arbitrary $\beta \in \Omega$. The subgroup H is regular and so there exists a unique $h \in H$ such that $\alpha^h = \beta$. Define a map $\lambda : \Omega \to H$ via $\lambda(\beta) = \lambda(\alpha^h) = h$. As h is unique, the map λ is well defined and invertible. Hence λ is a bijection. Then G acts on H via $\lambda(\beta)^g = \lambda(\beta^g)$ for all $g \in G$ as

$$\lambda(\beta)^1 = \lambda(\beta^1) = \lambda(\beta) \text{ and } \lambda(\beta)^{xy} = \lambda(\beta^{xy}) = \lambda((\beta^x)^y) = \lambda(\beta^x)^y = (\lambda(\beta)^x)^y$$

for all $x, y \in G$.

We consider the action of G_α on H. Let $g \in G_\alpha$ and $h \in H$ then

$$h^g = \lambda(\alpha^h)^g = \lambda(\alpha^{hg}) = \lambda(\alpha^{gg^{-1}hg}) = \lambda(\alpha^{g^{-1}hg}) = g^{-1}hg.$$

As H is abelian, $H \leq C := C_{\mathrm{Sym}(\Omega)}(H)$. Furthermore H is regular, so by Theorem 3.6, C is regular and conjugate to H in $\mathrm{Sym}(\Omega)$, so $H = C$. By Lemma 1.14, we then have that $G = C \rtimes G_\alpha$. In particular $C \cap G_\alpha = 1$. Hence as G_α acts on $H = C$ by conjugation, G_α must act faithfully on H and so G_α is isomorphic to a subgroup of $\mathrm{Aut}(H)$. We have identified H with $(V, +)$ so we may see that $\mathrm{Aut}(H) \cong \mathrm{GL}(k, p)$. Therefore G_α is isomorphic to a subgroup of $\mathrm{GL}(k, p)$ and $G = H \rtimes G_\alpha \cong V \rtimes K$ where $K \leq \mathrm{GL}(k, p)$. So G is isomorphic to a subgroup of $\mathrm{AGL}(k, p)$.

Finally we show that G_α acts irreducibly on V. Suppose that there exists some proper non-zero subspace W of V. Then by our identification of H with the additive group of V, the subspace W corresponds to a proper non-trivial subgroup $\tilde{H} < H$. We assume that G_α stabilizes W. Then for all $g \in G_\alpha$ we have that $g^{-1}\tilde{H}g = \tilde{H}$. Hence $\tilde{H}$ is normalized by G_α and so $G_\alpha < \tilde{H} \rtimes G_\alpha < G = H \rtimes G_\alpha$. However G is primitive and so by Lemma 1.6, G_α is a maximal subgroup of G; a contradiction. □

The following is stated in [36, p.158].

Proposition 3.17. *Let $T \leq G \leq \mathrm{AGL}(k, p)$, where p is prime and $k \geq 1$. Then G is primitive if and only if G_{0_V} is an irreducible subgroup of $\mathrm{GL}(k, p)$.*

Proof. Assume that G is imprimitive. Then we may fix a non-trivial block system for G and we let $\Delta \subset V$ be the block containing the zero vector. If a vector $v \in V$ lies in Δ then $v \in \Delta \cap (\Delta + v)$ and so $\Delta + v = \Delta$. As v is an arbitrary vector and $\mathbb{F}_p$ is a finite field, this shows that all scalar multiples of v must also lie in Δ. But then Δ is a proper non-zero subspace of V and so G_{0_V} is acting reducibly on V.

Now suppose that G_{0_V} is reducible and let $\Delta \subset V$ be a proper non-zero G_{0_V}-invariant subspace of V. Let $g = f_{a,v} \in G$, where $v \in V$ and $a \in G_{0_V}$. Then we have that $\Delta^g = \Delta a + v = \Delta + v$ and so Δ^g is a right coset of Δ in V. Therefore either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$. Hence Δ is a non-trivial block for the action of G on V and so G is imprimitive. □

The following definition is found in [13, p.4].

Definition 3.18. Let $G \leq \mathrm{Sym}(\Omega)$ be a primitive permutation group. We say that G is of *affine type* if $|\Omega| = p^k$ for a prime p and $k \geq 1$ and G is permutation isomorphic to a subgroup of $\mathrm{AGL}(k, p)$, in such a way that $\mathrm{Soc}(G)$ is permutation isomorphic to the subgroup of translations $T \trianglelefteq \mathrm{AGL}(k, p)$.

We may therefore identify primitive groups of affine type of degree p^k with the corresponding subgroup of $\mathrm{AGL}(k, p)$.

By Proposition 3.17, any primitive group of affine type is permutation isomorphic to a semidirect product $V \rtimes K$ acting on V, where V is the additive group of a vector space $\mathbb{F}_p^k$, for p prime, $k \geq 1$, and K an irreducible subgroup of $\mathrm{GL}(k, p)$.

Lemma 3.19. *Let $P_1, P_2 \leq \mathrm{AGL}(k,p)$ be two primitive groups of affine type of degree p^k. Let $T = \mathrm{Soc}(P_1) = \mathrm{Soc}(P_2)$, where T is the subgroup of translations of $\mathrm{AGL}(k,p)$. Then P_1 is permutation isomorphic to P_2 if and only if P_1 is conjugate to P_2 in $\mathrm{AGL}(k,p)$.*

Proof. By Lemma 1.17, P_1 is permutation isomorphic to P_2 if and only if P_1 is conjugate in S_{p^k} to P_2. Furthermore, as $T = \mathrm{Soc}(P_1) = \mathrm{Soc}(P_2)$ any element conjugating P_1 to P_2 must send $T \leq P_1$ to $T \leq P_2$.

Let $\sigma \in S_{p^k}$ be such that $P_1^\sigma = P_2$. Hence $T^\sigma = T$ and so $\sigma \in N_{S_{p^k}}(T)$. However by Lemma 3.15, $N_{S_{p^k}}(T) = \mathrm{AGL}(k,p)$. Thus if P_1 and P_2 are permutation isomorphic then they are conjugate in $\mathrm{AGL}(k,p)$.

On the other hand, if P_1 and P_2 are conjugate in $\mathrm{AGL}(k,p)$ then they are conjugate in S_{p^k} and so by Lemma 1.17, they are permutation isomorphic. □

The following is stated in [13, p.4].

Lemma 3.20. *Let $P_1, P_2 \leq \mathrm{AGL}(k,p)$ be two primitive groups of affine type of degree p^k. Suppose that $P_1 = T \rtimes G_1$, where $T = \mathrm{Soc}(P_1) = \mathrm{Soc}(P_2)$ and $G_1 \leq \mathrm{GL}(k,p)$ is irreducible. Then P_1 is permutation isomorphic to P_2 if and only if $P_2 = T \rtimes G_2$, where $G_2 \leq \mathrm{GL}(k,p)$ is irreducible and G_2 is conjugate to G_1 in $\mathrm{GL}(k,p)$.*

Proof. We assume that P_1 and P_2 are permutation isomorphic. By Lemma 3.19, P_1 is permutation isomorphic to P_2 if and only if P_1 is conjugate to P_2 in $\mathrm{AGL}(k,p)$.

Take an element $ua \in \mathrm{AGL}(k,p)$, where $u \in T$ and $a \in \mathrm{GL}(k,p)$ such that $P_1^{ua} = P_2$. Then for any $vg \in P_1$, where $v \in T$ and $g \in G_1$ we have

$$\begin{aligned}(vg)^{ua} &= a^{-1}u^{-1}(vg)ua \\ &= a^{-1}(u^{-1}v)aa^{-1}gua \\ &= (u^{-1}v)^a(a^{-1}g)u(a^{-1}g)^{-1}(a^{-1}g)a \\ &= (u^{-1}v)^a u^{(a^{-1}g)^{-1}} g^a.\end{aligned}$$

Here $u^{(a^{-1}g)^{-1}} \in T$ as $u \in T$. Moreover $(u^{-1}v)^a \in T$ as $v, u \in T$. Hence $t_{ua} := (u^{-1}v)^a u^{(a^{-1}g)^{-1}} \in T$ and so $(vg)^{ua} = t_{ua}g^a \in T \rtimes (G_1)^a$. As $|P_2| = |T \rtimes (G_1)^a|$ we have that $P_2 = T \rtimes (G_1)^a$ and $G_2 := (G_1)^a$ is irreducible because G_1 is.

We now assume that $P_2 = T \rtimes G_2 = T \rtimes (G_1)^a$ for some $a \in \mathrm{GL}(k,p)$. Then the action of G_1 on T is permutation isomorphic to the action of G_2 on T. Hence $P_1 \cong P_2$ and both P_1 and P_2 are permutation isomorphic in their action on T. □

Therefore the classification of the affine primitive permutation groups of degree $4096 \leq d < 8192$ corresponds to classifying the irreducible subgroups of $\mathrm{GL}(k,p)$

with $4096 \leq p^k = d < 8192$, up to conjugacy in $\mathrm{GL}(k,p)$.

Case 1: If $k = 1$ all subgroups of $\mathrm{GL}(1,p)$ are irreducible. There is one conjugacy class of affine type groups for each divisor of $p-1$.

Case 2: If $k > 1$ then we find all pairs (k,p) with $k > 1$ and p prime, such that $4096 \leq p^k < 8192$. Hence

$$(k,p) \in \{(2,67),(2,71),(2,73),(2,79),(2,83),(2,89),(3,17),(3,19),(8,3),(12,2)\}.$$

The corresponding subgroups of $\mathrm{AGL}(k,p)$ are constructed by taking semidirect products of the irreducible subgroups of $\mathrm{GL}(k,p)$ with their natural modules.

3.1.1. *The method.* We now give an algorithm which works for all pairs (k,p) above, other than $(k,p) = (8,3)$.

The Affine Type Groups: Procedure 1

Input: A group $G = \mathrm{GL}(k,p)$, for $p^k \in \{67^2, 71^2, 73^2, 79^2, 83^2, 89^2, 17^3, 19^3, 2^{12}\}$.

Output: A list **Primitive**, consisting of all primitive groups of affine type of degree p^k.

Step 1: Define a list **Affine** consisting of the group G. Define empty lists **Primitive** and **Tested**.

Step 2: For each item A in **Affine** such that A is not in **Tested**:
Create a list **Max** consisting of conjugacy class representatives of all irreducible maximal subgroups of A, via "MaximalSubgroups".
For each M in **Max**, if M is not conjugate in G to any member of **Affine** then append M to **Affine**.
Append A to **Tested**.
Repeat Step 2 until all elements in **Affine** have been considered.

Step 3 For each item A in **Affine**:
Define **Mod** to be the natural k-dimensional $\mathbb{F}_pG$-module of G. Construct the semidirect product S of **Mod** and A, where A acts on **Mod** as on the module.
Append S to **Primitive**.

Step 4: Return: Primitive.

The MAGMA function "MaximalSubgroups" used above does not work for $\mathrm{GL}(8,3)$ in MAGMA ver.2.24-5. We therefore use a different method.

We separate the maximal subgroups of $G := \mathrm{GL}(8,3)$ into their Aschbacher classes, see Theorem 1.25. As we want only the irreducible maximal subgroups of G, we do not consider the first class, which consists of all of the maximal reducible subgroups of $\mathrm{GL}(8,3)$.

Lemma 3.21. *Let $G = \mathrm{GL}(8,3)$, then there are no maximal subgroups of G in the Aschbacher classes (v),(vi),(vii), and (ix).*

Proof. We prove this computationally in MAGMA by checking all of the classes. □

The following is essentially [35, Lemma 4.3, Proposition 4.5, Theorem 4.11, and Lemma 4.13].

Lemma 3.22. *Let $H \leq \mathrm{GL}(d,q)$. Then the following hold:*

(i) If H is imprimitive then H is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of a maximal imprimitive subgroup of $\mathrm{GL}(d,q)$.

(ii) If H is semilinear then H is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of a maximal semilinear group.

(iii) If H is a simple tensor product then H is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of a maximal simple tensor product group.

(iv) If H is a group of classical type then H is conjugate in $\mathrm{GL}(d,q)$ to a subgroup of a maximal classical type group.

The Affine Type Groups: Procedure 2

Input: The group $G = \mathrm{GL}(8,3)$.

Output: A list **Primitive**, consisting of the primitive groups of affine type of degree 3^8.

Step 1: Use "ClassicalMaximals" to find conjugacy class representatives of the maximal subgroups of G, split into their Aschbacher classes. Call these **Affine1**, ... **Affine9**. Discard **Affine1** - reducible groups. Discard **Affine5**, **Affine6**, **Affine7**, **Affine9** as they are empty. Define empty lists **Primitive** and **Tested**.

Step 2: For each **Affine** in {**Affine2**, **Affine3**, **Affine4**, **Affine8**} do the following:
For each A in **Affine** such that A is not in **Tested**:
Create a list **Max** consisting of conjugacy class representatives all irreducible maximal subgroups of A, via "MaximalSubgroups".
For each M in **Max**, if M is not conjugate in G to any member of **Affine** then append M to **Affine**.
Append A to **Tested**.
Repeat Step 2 until all elements in **Affine** have been considered.

Step 3: Consider the classes **Affine2**, **Affine3**, **Affine4**, and **Affine8**.

(a): **Affine2** (imprimitive groups): for each item A in **Affine2**:
Define **Mod** to be the natural 8-dimensional $\mathbb{F}_3G$-module of G. Construct the semidirect product S of **Mod** and A, where A acts on **Mod** as on the module.
Append S to **Primitive**.

(b): **Affine3** (semilinear groups): first remove any imprimitive groups from **Affine3** using the function "LMGIsPrimitive". Then
for each item A in **Affine3**:
Define **Mod** to be the natural 8-dimensional $\mathbb{F}_3G$-module of G. Construct the semidirect product S of **Mod** and A, where A acts on **Mod** as on the module.
Append S to **Primitive**.

(c): **Affine4** (simple tensor products): first remove any imprimitive groups from **Affine4** using the function "LMGIsPrimitive", also remove any semilinear groups via the semilinear test described in Section 2.4. Then
for each item A in **Affine4**:
Define **Mod** to be the natural 8-dimensional $\mathbb{F}_3G$-module of G. Construct the semidirect product S of **Mod** and A, where A acts on **Mod** as on the module.
Append S to **Primitive**.

(d) **Affine8** (groups of classical type): first remove any imprimitive groups from **Affine4** using the function "LMGIsPrimitive", also remove any semilinear groups via the semilinear test described in Section 2.4, finally remove any simple tensor products using the function "IsTensor". Then
for each item A in **Affine8**:
Define **Mod** to be the natural 8-dimensional $\mathbb{F}_3G$-module of G. Construct the semidirect product S of **Mod** and A, where A acts on **Mod** as on the module.
Append S to **Primitive**.

Step 4: **Return: Primitive**.

Example 3.23. Let $G = \mathrm{GL}(8, 3)$, we now follow Procedure 2.

Step 1: We produce the lists **Affine2**, **Affine3**, **Affine4**, and **Affine8** of sizes $2, 1, 2$, and 5 respectively. We also produce the empty lists **Primitive** and **Tested**.

Step 2: We extend the lists **Affine2**, **Affine3**, **Affine4**, and **Affine8** by iteratively appending non-conjugate irreducible maximal subgroups.

Step 3(a): **Affine2** is a list of size 8088. We create the primitive groups of affine type arising from **Affine2** and Append them to **Primitive**.

Step 3(b): We remove imprimitive groups from **Affine3**, producing a list of size 801. We then create the primitive groups of affine type arising from **Affine3** and Append them to **Primitive**.

Step 3(c): We remove imprimitive groups from **Affine4** and then we remove any semilinear groups, producing a list of size 72. We then create the primitive groups of affine type arising from **Affine4** and Append them to **Primitive**.

Step 3(d): We remove imprimitive groups from **Affine8**, then we remove any semilinear groups, and then we remove any simple tensor product groups, producing a list of size 67. We then create the primitive groups of affine type arising from **Affine8** and Append them to **Primitive**.

This produces the list **Primitive** which consists of the 9028 primitive groups of affine type of degree 3^8.

Theorem 3.24. *Let G be a primitive permutation group of affine type of degree $4096 \leq d < 8192$.*

(i) If d is prime then $G \cong C_d \rtimes C_r$ where $r \mid (d-1)$.

(ii) If d is a non trivial power of a prime, then $d = p^k$ for $p^k \in \{67^2, 71^2, 73^2, 79^2, 83^2, 89^2, 17^3, 19^3, 3^8, 2^{12}\}$. In this case $G \cong \mathbb{F}_p^k \rtimes K$ where K is an irreducible subgroup of $\mathrm{GL}(k,p)$. For each non trivial, prime power $4096 \leq d < 8192$ we give the number of primitive groups of affine type of degree d in Table 9.

Proof. (i) If d is a prime then we are considering all irreducible subgroups of $\mathrm{GL}(1,d)$. All non-trivial subgroups of $\mathrm{GL}(1,d) \cong C_{d-1}$ are irreducible, and there exists exactly one irreducible subgroup K for every r dividing $d-1$. Thus the affine type groups are exactly the groups $T \rtimes K \cong C_d \rtimes C_r$.

(ii) We use Procedure 1 above together with Example 3.23, to find all primitive groups of affine type with non-prime degree $4096 \leq d < 8191$. □

3.2. **Almost simple groups.** In this section we classify the primitive almost simple groups of degree $4096 \leq d < 8192$. This will require the use of the Classification of the Finite Simple Groups, see Theorem 1.23.

Definition 3.25. Let G be a group. We call a subgroup $H \leq G$ *core-free* if the normal core, $\bigcap_{g \in G} g^{-1} H g$, is trivial.

By Lemma 1.18, any transitive action of a group G is permutation isomorphic to the action of G on the right cosets of a point stabilizer of the action. By Lemma 1.6, the point stabilizers of a primitive group action are all maximal subgroups of G. Hence any primitive action of a group G is permutation isomorphic to the action of G on the right cosets of some maximal subgroup of G.

For a coset action to be faithful, we require that the kernel of this action, the normal core, is trivial. Thus the faithful primitive actions of a group G correspond to the conjugacy classes of its core-free maximal subgroups.

Hence to classify the almost simple primitive permutation groups of degree $4096 \leq d < 8192$ we must find all of the core-free maximal subgroups of almost simple groups, up to conjugacy in the automorphism group of the simple group, such that the index of any maximal subgroup lies in that range.

Let G be an almost simple group with socle T. We call a maximal subgroup M of G:

- *ordinary* if $M \cap T$ is maximal in T,
- a *novelty* if $M \cap T$ is non-maximal in T and $M \cap T$ is a proper subgroup of T,
- a *triviality* if $T \leq M$.

If M is a triviality then it corresponds to a non-faithful action. As stated in [13, p.3], the index of any novelty maximal subgroup of G is always greater than the index in $\mathrm{Soc}(G)$ of its largest ordinary maximal.

To find all almost simple primitive groups with socle isomorphic to T, we find the possible cohorts of primitive groups first and then construct the primitive groups in each of these cohorts.

For a non-abelian simple group T and $A := \mathrm{Aut}(T)$ we find the maximal subgroups of T up to conjugacy in A. We also find the intersections of any novelty maximals with T, again up to conjugacy in A. The corresponding permutation representations of T acting on the set Ω of cosets of these subgroups produces a list of primitive groups $G \leq \mathrm{Sym}(\Omega)$ with $\mathrm{Soc}(G) \cong T$. Exactly one of these groups G lies in each possible cohort of primitive almost simple groups with socle isomorphic to T. We call these groups G *cohort representatives*.

For each cohort representative G, we calculate $N := N_{\mathrm{Sym}(\Omega)}(\mathrm{Soc}(G))$ and we find all of the conjugacy classes of subgroups of N which contain $\mathrm{Soc}(G)$. The primitive groups found here are the primitive groups in the cohort.

The following definition is given in [13, p.5].

Definition 3.26. Let G be an almost simple group. We denote by $P(G)$ the minimal integer d such that G has a faithful primitive permutation representation of degree d.

The following lemma is [36, Lemma 4.1].

Lemma 3.27. *Let G be an almost simple group with socle T and suppose that $T \leq G \leq \mathrm{Aut}(T)$. Then $P(G) \geq P(T)$.*

Proof. Let G_α be the point stabilizer in a primitive faithful action for G of degree $P(G)$. Since the action is faithful, G_α must be core free. Thus $T \nleq G_\alpha$. By Lemma 1.4, T is acting transitively and so by the Orbit-Stabilizer Theorem (1.2), the degree of the action is

$$|G : G_\alpha| = |T : (T \cap G_\alpha)|.$$

So if $T \cap G_\alpha$ is maximal in T we have that

$$P(G) = |G : G_\alpha| = |T : (T \cap G_\alpha)| = P(T).$$

However if $T \cap G_\alpha$ is not maximal in T then we have

$$P(G) = |G : G_\alpha| = |T : (T \cap G_\alpha)| > |T : \tilde{T}| = P(T)$$

for some core free maximal subgroup $\tilde{T}$ of T. □

3.2.1. *Alternating groups.* In this section we classify the almost simple primitive groups of degree $4096 \leq d < 8192$ with alternating socles. For this we will require a different version of the O'Nan-Scott Theorem (1.11), see for example [29, p.2].

Theorem 3.28. *Let H be a proper subgroup of S_n or A_n such that $H \neq A_n$. Then H is a subgroup of at least one of the following groups.*

(i) An intransitive group $S_k \times S_m$, where $n = k + m$.
(ii) An imprimitive group $S_k \wr S_m$, where $n = km$.
(iii) A primitive group, see Theorem 1.11.

Definition 3.29. For $n > 4$ the groups A_n and S_n in their natural action form a single cohort. We call the groups in this cohort *improper* primitive groups.

In what follows we do not consider improper primitive groups further, as they arise for every degree.

The following is Bochert's Theorem, [26, Kapitel 2, Satz 4.6].

Theorem 3.30. *Let $G \leq S_n$ be a primitive group and suppose that $A_n \nleq G$. Then*

$$|S_n : G| \geq \lfloor (n+1)/2 \rfloor !$$

Proposition 3.31. *If $G = A_n$ or S_n has a faithful primitive action, other than the natural action, of degree $4096 \leq d < 8192$, then $n \leq 128$. If the stabilizer G_α in this action acts transitively on $\{1, \ldots, n\}$ then $n \leq 16$ and G_α is not primitive on $\{1, \ldots, n\}$.*

Proof. As $|S_n| = n!$ and $6! < 4096$ we may assume that $n \geq 7$. If $G = A_n$ then let H_0 be a point stabilizer of a faithful primitive action of G (a proper maximal subgroup of G) such that H_0 is not conjugate to A_{n-1} (we are not considering the improper action). If $G = S_n$ then let $H_0 = G_0 \cap A_n$ where G_0 is a maximal subgroup of S_n.

Case 1: Suppose that H_0 is primitive in its action on $\{1, \ldots, n\}$. Then by Bochert's Theorem (3.30), we have

$$|S_n : H_0| \geq \lfloor (n+1)/2 \rfloor !$$

and so, since $|A_n : H_0| < 8192$, we have that $|S_n : H_0| < 16384$. This implies that $n \leq 14$.

We now use MAGMA to find all of the maximal subgroups of A_n and S_n for $7 \leq n \leq 14$ that are acting primitively on $\{1, \ldots, n\}$. Only A_{12} and S_{12} have maximal subgroups with indices in the range $4096 \leq d < 8192$. For both A_{12} and S_{12} there is one such conjugacy class of maximal subgroups. These subgroups are of index 5775 but neither of these subgroups are primitive on $\{1 \ldots n\}$. So in this case we find no primitive groups in our range.

Case 2: Suppose that H_0 is transitive but imprimitive in its action on $\{1, \ldots, n\}$. Let k be the size of a non-trivial block, and $m := n/k$. Then by Theorem 3.28, $H_0 \leq (S_k \wr S_m)$. Hence if $G = A_n$ then $H_0 = (S_k \wr S_m) \cap A_n$. Furthermore if $G = S_n$ then $H_0 = G_0 \cap A_n$ where G_0 is transitive on $\{1, \ldots, n\}$, as H_0 is transitive on $\{1, \ldots, n\}$. We have shown in Case 1 that there is no maximal subgroup $G_0 \leq S_n$ such that G_0 is of index $4096 \leq d < 8192$ and G_0 is acting primitively on $\{1, \ldots, n\}$, thus G_0 must be acting transitively and so $H_0 = (S_k \wr S_m) \cap A_n$ for this choice of G also. Thus $|H_0| = (k!)^m (m!)/2$. It follows that

$$|A_n : H_0| = |S_n : G_0| = (mk)!/(k!)^m m! =: f(m,k).$$

The function $f(m,k)$ increases monotonically in both variables. For $(m,k) \in \{(2,7),(3,3),(4,2),(5,2)\}$ the value of $f(m,k)$ is less than 4096. For $(m,k) \in \{(2,9),(3,5)(4,3),(5,3),(6,2)\}$ the value of $f(m,k)$ is greater than 8192. This leaves only $(m,k) \in \{(2,8),(3,4)\}$. Here $f(2,8) = 6435$ and $f(3,4) = 5775$. Thus we consider the groups A_n and S_n where $n = mk$. Here A_{12}, A_{16}, S_{12}, and S_{16} each have a single conjugacy class of imprimitive maximal subgroup of index $4096 \leq d < 8192$.

Case 3: Suppose that H_0 is intransitive in its action on $\{1, \ldots, n\}$. We first show that H_0 can have no orbits of length 1.

If H_0 has an orbit of length 1 then H_0 is conjugate to some subgroup of A_{n-1}. If G is A_n, then $H_0 \leq_{\max} G$ and so we must have that $H_0 = A_{n-1}$. However the action is then the natural action which is a contradiction. Hence $G = S_n$ and so $H_0 = G_0 \cap A_n$. Then $|G_0 : H_0| = 2$ and so the orbit of any

fixed point of H_0 under the action of G_0 has length at most 2.

If $a, b \in \{1, \ldots, n\}$ both have orbits of length one under the action of G_0, then $G_0 < \langle G_0, (a, b)\rangle < S_n$, contradicting the maximality of G_0. So G_0 has at most one orbit of length 1.

If G_0 has one orbit of length 1 then since $G_0 \leq_{\max} S_n$ we must have that $G_0 = S_{n-1}$ which is a contradiction as the action is then the natural action.

Therefore G_0 has no orbits of length 1 and so G_0 must have an orbit of length 2. Hence by Theorem 3.28, $G_0 \cong S_2 \times S_{n-2}$. But in this case $H_0 = G_0 \cap A_n$ has no fixed points, which is a contradiction as we assumed that H_0 had an orbit of length 1.

Hence H_0 has no orbits of length 1.

Let α^{H_0} be the smallest orbit of H_0, and set $k := |\alpha^{H_0}|$, here $1 < k \leq n/2$. Then $H_0 \leq (S_k \times S_{n-k}) \cap A_n$. It follows directly that

$$|H_0| \leq k!(n-k)!/2.$$

Thus

$$|A_n : H_0| \geq n!/k!(n-k)! = \binom{n}{k} \geq \binom{n}{2}.$$

Therefore, as $|A_n : H_0| < 8192$, we have that $n \leq 128$.

□

Primitive Almost Simple Groups with Alternating Socles

Input: The Symmetric group $S := S_n$, for $7 \leq n \leq 128$.

Output: A list **Primitive**, consisting of all almost simple primitive groups with socle A_n.

Step 1: Define $T := \mathrm{Soc}(S)$, so $T = A_n$. Define an empty list **Primitive**.

Step 2(a): If $7 \leq n \leq 16$ then:

Step 2(a)(i): Create the list $\mathbf{Max}_S$ of representatives of the conjugacy classes of the transitive but imprimitive maximal subgroups of S with index between 4096 and 8191.

Step 2(a)(ii): Create the list $\mathbf{Max}_T$ of representatives of the conjugacy classes of the transitive but imprimitive subgroups of S which are maximal subgroups of T with index between 4096 and 8191.

Step 2(b): If $17 \leq n \leq 128$ then: if $4096 \leq \binom{n}{k} \leq 8191$ for some $1 < k \leq n/2$ then:

Step 2(b)(i): Create the list $\mathbf{Max}_S$ of representatives of the conjugacy classes of the intransitive maximal subgroups of S with index between 4096 and 8191.

Step 2(b)(ii): Create the list $\mathbf{Max}_T$ of representatives of the conjugacy classes of the intransitive subgroups of S which are maximal subgroups of T with index between 4096 and 8191.

Step 3(a): For each M_S in $\mathbf{Max}_S$ do $C := \text{CosetImage}(M_S, S)$.
The image of the permutation representation of S acting on the cosets of M_S.
Append C to **Primitive**.

Step 3(b): For each M_T in $\mathbf{Max}_T$ do $C := \text{CosetImage}(M_T, T)$.
The image of the permutation representation of T acting on the cosets of M_T.
Append C to **Primitive**.

Step 4: Return: Primitive.

Theorem 3.32. *Let G be a primitive almost simple group of degree $4096 \leq d < 8192$ with socle A_n. Then G appears on Table 10.*

Proof. We use the proof of Proposition 3.31 to determine which possibilities there are for primitive almost simple groups with alternating socles. We then use MAGMA to construct these groups via the procedure described above. □

3.2.2. *Classical groups.* We recall Section 1.2 and we take q to always be a prime power. We denote a simple classical group by $\text{Cl}_n(q)$. In this section we classify all of the almost simple primitive groups of degree $4096 \leq d < 8192$ with classical socles.

In the following proposition we find the maximum values of n and q such that $P(\text{Cl}_n(q)) < 8192$.

Proposition 3.33. *Let G be an almost simple group with a classical socle H. Suppose that G has a faithful primitive permutation action of degree less than 8192. Then if H is not alternating, H appears on Table 1.*

Proof. By Lemma 3.27 we only need to consider the *simple* classical groups. The formulae for $P(H)$ are given in [28, p.175, Table 5.2A] and corrected and extended in [20, Table 4]. These formulae are all monotonically increasing in each variable. We shall also rely upon Theorem 1.24, which lists al isomorphisms between finite

alternating, classical, and exceptional simple groups.

Linear: For $(n,q) \notin \{(2,5),(2,7),(2,9),(2,11),(4,2)\}$ we have that

$$P(\mathrm{L}_n(q)) = (q^n-1)/(q-1).$$

For (n,q) in the set, the order of $\mathrm{L}_n(q)$ is less than 4096, other than $\mathrm{L}_4(2) \cong A_8$ which has already been considered.

Symplectic: Since $\mathrm{S}_2(q) = \mathrm{L}_2(q)$ we assume that $m > 1$, and as $\mathrm{S}_4(2) \cong S_6$ we take $(m,q) \neq (2,2)$. We then have that for $m \geq 3$

$$P(\mathrm{S}_{2m}(2)) = 2^{m-1}(2^m-1).$$

If $m \geq 2$ and $q \geq 3$ then

$$P(\mathrm{S}_{2m}(q)) = (q^{2m}-1)/(q-1),$$

with the exception of $(m,q) = (2,3)$ in which case $P(\mathrm{S}_4(3)) = 27$.

Unitary: We assume that $n > 2$ as $\mathrm{U}_2(q) \cong \mathrm{S}_2(q) \cong \mathrm{L}_2(q)$. We also assume that $(n,q) \notin \{(3,2),(4,2)\}$ as $\mathrm{U}_3(2)$ is not simple and $\mathrm{U}_4(2) \cong \mathrm{S}_4(3)$.

(i) If $q \neq 2,5$ then

$$P(\mathrm{U}_3(q)) = q^3+1.$$

Here we are not considering $\mathrm{U}_3(2)$ and $P(\mathrm{U}_3(5)) = 50$.

(ii) If $q \neq 2$ then

$$P(\mathrm{U}_4(q)) = q^4+q^3+q+1.$$

We now consider $n \geq 5$.

(iii) When n is even we have that

$$P(\mathrm{U}_n(2)) = 2^{n-1}(2^n-1)/3.$$

(iv) Otherwise we have that

$$P(\mathrm{U}_n(q)) = (q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})/(q^2-1).$$

Orthogonal Odd Dimension: We assume that q is odd, since $\mathrm{P}\Omega_{2m+1}(2^i) \cong \mathrm{S}_{2m}(2^i)$ for all $i \geq 1$. We also assume that $m \geq 3$ as $\mathrm{P}\Omega_3(q) \cong \mathrm{L}_2(q)$ and $\mathrm{P}\Omega_5(q) \cong \mathrm{S}_4(q)$ for q odd. Then

(i) for $q = 3$ we have

$$P(\mathrm{P}\Omega_{2m+1}(3)) = 3^m(3^m-1)/2,$$

(ii) for $q \geq 5$ we have

$$P(\mathrm{P}\Omega_{2m+1}(q)) = (q^{2m}-1)/(q-1).$$

Orthogonal Plus and Minus Types: We assume that $m \geq 4$ as $\mathrm{P}\Omega_4^+(q)$ is not simple, $\mathrm{P}\Omega_4^-(q) \cong \mathrm{L}_2(q^2)$, $\mathrm{P}\Omega_6^+(q) \cong \mathrm{L}_4(q)$, and $\mathrm{P}\Omega_6^-(q) \cong \mathrm{U}_4(q)$. Then

(i) for $q = 2$ we have

$$P(\mathrm{P}\Omega^+_{2m}(2)) = 2^{m-1}(2^m - 1),$$

(ii) for $q = 3$ we have

$$P(\mathrm{P}\Omega^+_{2m}(3)) = 3^{m-1}(3^m - 1)/2,$$

(iii) for $q \geq 4$ and $\epsilon = +$, or for all q and $\epsilon = -$ we have

$$P(\mathrm{P}\Omega^\epsilon_{2m}(q)) = (q^m - \epsilon)(q^{m-1} + \epsilon)/(q - 1).$$

□

Group	n	q
$\mathrm{L}_n(q)$	$n = 2$	$q \leq 8179$
	$n = 3$	$q \leq 89$
	$n = 4$	$q \leq 19$
	$n = 5$	$q \leq 9$
	$n = 6$	$q \leq 5$
	$n = 7$	$q \leq 4$
	$n = 8$	$q \leq 3$
	$9 \leq n \leq 13$	$q = 2$
$\mathrm{S}_{2m}(q)$	$m = 2$	$q \leq 19$
	$m = 3$	$q \leq 5$
	$m = 4$	$q \leq 3$
	$5 \leq m \leq 7$	$q = 2$
$\mathrm{U}_n(q)$	$n = 3$	$q \leq 19$
	$n = 4$	$q \leq 9$
	$n = 5$	$q \leq 3$
	$n = 6$	$q = 2$
	$n = 7$	$q = 2$
$\mathrm{P}\Omega_{2m+1}(q)$	$m = 3$	$q \leq 5$
	$m = 4$	$q = 3$
$\mathrm{P}\Omega^+_{2m}(q)$	$m = 4$	$q \leq 4$
	$5 \leq m \leq 7$	$q = 2$
$\mathrm{P}\Omega^-_{2m}(q)$	$m = 4$	$q \leq 4$
	$5 \leq m \leq 7$	$q = 2$

TABLE 1. Classical socles of primitive almost simple groups with minimal degree at most 8191.

Primitive Almost Simple Groups with Classical Socles

Input: The Automorphism group A of a simple classical group T, described in Table 1.

Output: A list **Primitive**, consisting of all almost simple primitive groups with socle T.

Step 1: Define $T := \mathrm{Soc}(A)$. Construct empty lists **CohortReps** and **Primitive**.

Step 2 Define the empty list **Max**.

Step 2(a): Append to **Max** the representatives of the conjugacy classes of any subgroups of A which are maximal subgroups of T with index in T between 4096 and 8191.

Step 2(b): Append to **Max** the representatives of the conjugacy classes of any subgroups of A that are not maximal in T but are maximal in some non-trivial extension of T with index between 4096 and 8191 in that extension.

Step 3: For each $m \in$ **Max**, let C be the image of the action of T on the cosets of m via "CosetImage". Append C to **CohortReps**.

Step 4: For each $P \in$ **CohortReps**, Calculate $N := N_{\mathrm{Sym}(\mathrm{Deg}(P))}(\mathrm{Soc}(P))$ and the quotient $Q := N/\mathrm{Soc}(P)$, together with the epimorphism $\phi : N \to Q$. For each conjugacy class representative S of the subgroups of Q, if the preimage s of S under ϕ is primitive then Append s to **Primitive**.

Step 5: Return: Primitive.

Some groups in Table 1, and their automorphism groups, do not currently (MAGMA ver.2.24) have computable maximal subgroups using the function "MaximalSubgroups", these groups are: $\mathrm{L}_8(3), \mathrm{S}_{14}(2), \mathrm{P}\Omega^-_{14}(2)$, and $\mathrm{P}\Omega^+_{14}(2)$. For these four groups we used the function "ClassicalMaximals".

Theorem 3.34. *The primitive almost simple classical groups of degree* $4096 \leq d < 8192$ *are displayed in Tables 11, 12, 13, and 14.*

Proof. Input the automorphism groups of each of the simple classical groups displayed on Table 1 into the procedure above. □

3.2.3. *Worked examples.* In this section we give worked examples of some of the cases that arise when classifying the primitive almost simple groups with classical socles.

Throughout, a primitive group will be denoted by G and we will denote the socle of G by $H \leq G$. We will denote any (not necessarily maximal) subgroup of H by $H_0 < H$. If H_0 is not maximal we will call the cohort obtained in that instance a

novelty cohort. Finally we denote by $[n]$ a soluble group of order n.

In general if H_0 is a maximal subgroup of H, we use the procedure above (adding to **Max** in **Step 2(a)**) to find all primitive groups with simple classical socles.

We give examples of what happens when we are considering a (novelty) subgroup H_0 of H which is not maximal in H but whose normalizer is maximal in some other almost simple group with classical socle H.

By [6, 1.7.2, p.36], a presentation for the outer automorphism group of $H = \mathrm{L}_n(q)$, where $n \geq 3$ and $q = p^e$ for some prime p, is given by

$$\mathrm{Out}(H) = \langle \delta, \gamma, \phi \mid \delta^{(q-1,n)} = \gamma^2 = \phi^e = [\gamma, \phi] = 1, \delta^\gamma = \delta^{-1}, \delta^\phi = \delta^p \rangle.$$

We refer to the generators δ, γ, and ϕ as the diagonal, graph and field automorphisms respectively. These names come from the theory of algebraic groups and will not be discussed here.

We first give a non-novelty example.

Example 3.35. We begin by considering the cohort of primitive almost simple groups corresponding to $H = \mathrm{L}_3(67)$ of degree $d = 4557$. We let G be any group in this cohort. The simple group $\mathrm{L}_3(67)$ contains a maximal subgroup H_0 of index 4557. This group is $67^2.[22].\mathrm{L}_2(67).2$. We note that 3 divides $(67 - 1)$ and so there is a non-trivial diagonal automorphism. The outer automorphism group is

$$\mathrm{Out}(H) = \langle \delta, \gamma, \phi \mid \delta^3 = \gamma^2 = \phi = 1, \delta^\gamma = \delta^{-1} \rangle \cong S_3.$$

According to [6, p.378] the stabilizer of the conjugacy class of H_0 under the action of $\mathrm{Out}(H)$ is $\langle \delta, \phi \rangle \cong C_3$. Hence the normalizer of G in S_d is $H.3$. We consider Figure 1, the conjugacy class subgroup diagram of $\mathrm{Out}(H)$.

In this case there are two conjugacy classes of subgroups contained in $\langle \delta, \phi \rangle$. Thus the number of groups in the cohort is 2.

Example 3.36. We next consider the primitive almost simple groups corresponding to $H = \mathrm{L}_3(17)$ of degree $d = 5526$. We let G be any group in this cohort. The simple group $\mathrm{L}_3(17)$ contains no maximals in the index range $4096 \leq d < 8192$. However there exists a subgroup $H_0 < H$ of index 5526 such that $H_0.2$ is maximal in $\mathrm{L}_3(17).2$. This group is $17^{1+2} : [16^2]$. We have that

$$\mathrm{Out}(H) = \langle \delta, \gamma, \phi \mid \delta = \gamma^2 = \phi = 1 \rangle \cong C_2.$$

According to [6, p.378] the stabilizer of the conjugacy class of H_0 under the action of $\mathrm{Out}(H)$ is $\langle \delta, \gamma, \phi \rangle$ which is the whole outer automorphism group. Hence the normalizer of G in S_d is $H.2$. Our maximal subgroup is described as an $N1$ subgroup in [6, p.378]. Therefore it is maximal under subgroups not contained in $\langle \delta, \phi \rangle = \langle \delta \rangle$, by

[6, p.378]. We consider Figure 2, the conjugacy class subgroup diagram of $\mathrm{Out}(H)$.

In this case, only one conjugacy class of subgroups not contained in $\langle\delta,\phi\rangle = \langle\delta\rangle$. Hence the number of groups in the cohort is 1.

Example 3.37. We now consider the primitive almost simple groups corresponding to $H = \mathrm{L}_3(19)$ of degree $d = 7620$. We let G be any group in this cohort. This is a very similar case to Example 3.36 above, there exists a subgroup $H_0 < H$ of index 7620 such that $H_0.2$ is maximal in $\mathrm{L}_3(19).2$. This group is $19^{1+2} : [108]$. The difference here is that 3 divides $(19-1)$, which means that there is a non-trivial diagonal automorphism. In this case our outer automorphism group is of the form

$$\mathrm{Out}(H) = \langle\delta,\gamma,\phi \mid \delta^3 = \gamma^2 = \phi = 1, \delta^\gamma = \delta^{-1}\rangle \cong S_3.$$

Similarly to Example 3.36 above we use [6, p.378] to find that the stabilizer of the conjugacy class of H_0 under the action of $\mathrm{Out}(H)$ is $\langle\delta,\gamma,\phi\rangle$, which is the whole outer automorphism group. Hence the normalizer of G in S_d is $H.S_3$. Our subgroup is described as an $N1$ group in [6, p.378], and so it is maximal under subgroups not contained in $\langle\delta,\phi\rangle$, by [6, p.378]. We consider Figure 3, the conjugacy class subgroup diagram of $\mathrm{Out}(H)$.

In this case there are 2 conjugacy classes of subgroups which are not contained in $\langle\delta,\phi\rangle$ and so the size of the cohort is 2.

Example 3.38. We next consider the primitive almost simple groups corresponding to $H = \mathrm{L}_3(3^2)$ of degree $d = 7371$. We let G be any group in this cohort. This is also similar to Example 3.36 with a subgroup $H_0 \cong \mathrm{GL}_2(9) < H$, of index 7371 such that $H_0.2$ is maximal in $\mathrm{L}_3(3^2).2$ (in fact there are two such groups). In this case since $q = 3^2$ is a power of a prime with non-trivial index we have a non-trivial field automorphism. Here

$$\mathrm{Out}(H) = \langle\delta,\gamma,\phi \mid \delta = \gamma^2 = \phi^2 = [\gamma,\phi] = 1\rangle \cong C_2 \times C_2.$$

Similar to the examples above we use [6, p.378] to find that the stabilizer of the conjugacy class of H_0 under the action of $\mathrm{Out}(H)$ is $\langle\delta,\gamma,\phi\rangle$ which is the whole outer automorphism group. Hence the normalizer of G in S_d is $H.2^2$. Our subgroup is described as an $N1$ novelty in [6, p.378], so it is maximal under subgroups not contained in $\langle\delta,\phi\rangle = \langle\phi\rangle$, by [6, p.378]. We consider Figure 4, the conjugacy class subgroup diagram of $\mathrm{Out}(H)$.

There are 3 conjugacy classes of subgroups in this case which are not contained in $\langle\delta,\phi\rangle = \langle\phi\rangle$ and so the cohort has size 3. This cohort contains two groups of minimal order, the groups $H_0.\langle\gamma\rangle$ and $H_0.\langle\gamma\phi\rangle$.

Example 3.39. We consider the primitive almost simple groups corresponding to $H = \mathrm{L}_3(2^4)$ of degree $d = 4641$. We let G be any group in this cohort. In this case

3 divides $(2^4 - 1)$ and 2^4 is a prime power with non-trivial index. Hence there is a non-trivial diagonal automorphism and a non-trivial field automorphism. Here

$$\mathrm{Out}(H) = \langle \delta, \gamma, \phi \mid \delta^3 = \gamma^2 = \phi^4 = [\gamma, \phi] = 1, \delta^\gamma = \delta^{-1}, \delta^\phi = \delta^{-1} \rangle \cong 4 \times S_3.$$

In this case $H_0 = 2^{4+8}.[75] < H$ is a subgroup of index 4641 such that $H_0.2$ is maximal in $\mathrm{L}_3(2^4).2$ (in fact there are again two such groups). According to [6, p.378] the stabilizer of the conjugacy class of H_0 under the action of the outer automorphism group is $\langle \delta, \gamma, \phi \rangle$, the full outer automorphism group. Therefore the normalizer of G in S_d is $H.(4 \times S_3)$. Our subgroup is described as an $N1$ group in [6, p.378], hence according to [6, p.378] it is maximal under subgroups not contained in $\langle \delta, \phi \rangle$. We consider the conjugacy class subgroup diagram in Figure 5.

In this case there are 10 conjugacy classes of subgroups not contained in $\langle \delta, \phi \rangle$ and so the cohort is of size 10. This cohort contains two groups of minimal order, the groups $H_0.\langle \gamma \rangle$ and $H_0.\langle \gamma\phi^2 \rangle$.

3.2.4. *Subgroup diagrams.* Here we give the conjugacy class subgroup diagrams of the outer automorphism groups described above. The subgroups coloured red correspond to maximal subgroups of the almost simple group and so correspond to almost simple primitive groups. The edges are labeled by the index of the adjacent subgroup. Some of the edges of the graphs are coloured green when they overlap other edges, this is just for clarity of reading.

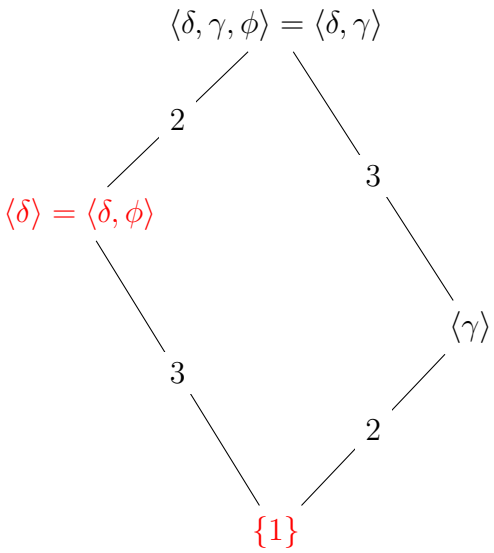

FIGURE 1. The conjugacy class subgroup diagram of $\mathrm{Out}(\mathrm{L}_3(67))$

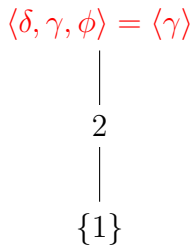

FIGURE 2. The conjugacy class subgroup diagram of $\mathrm{Out}(\mathrm{L}_3(17))$

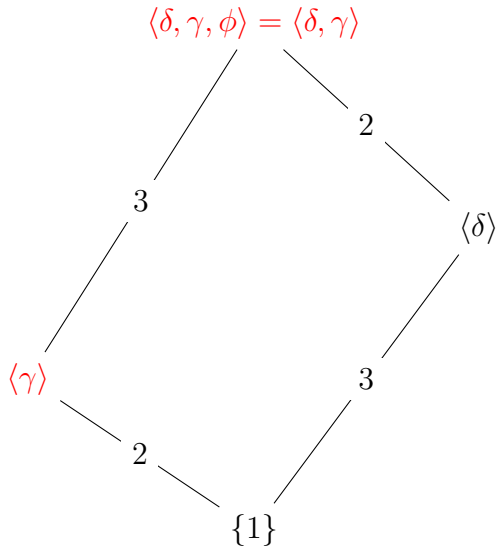

FIGURE 3. The conjugacy class subgroup diagram of $\mathrm{Out}(\mathrm{L}_3(19))$

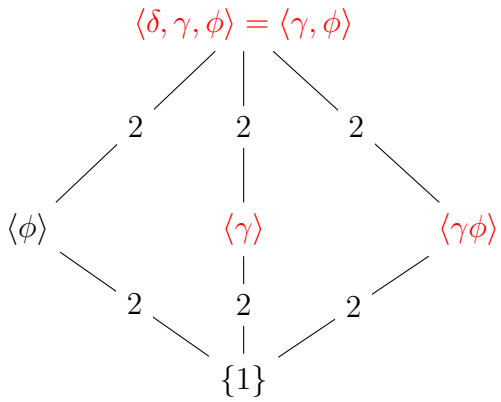

FIGURE 4. The conjugacy class subgroup diagram of $\mathrm{Out}(\mathrm{L}_3(3^2))$

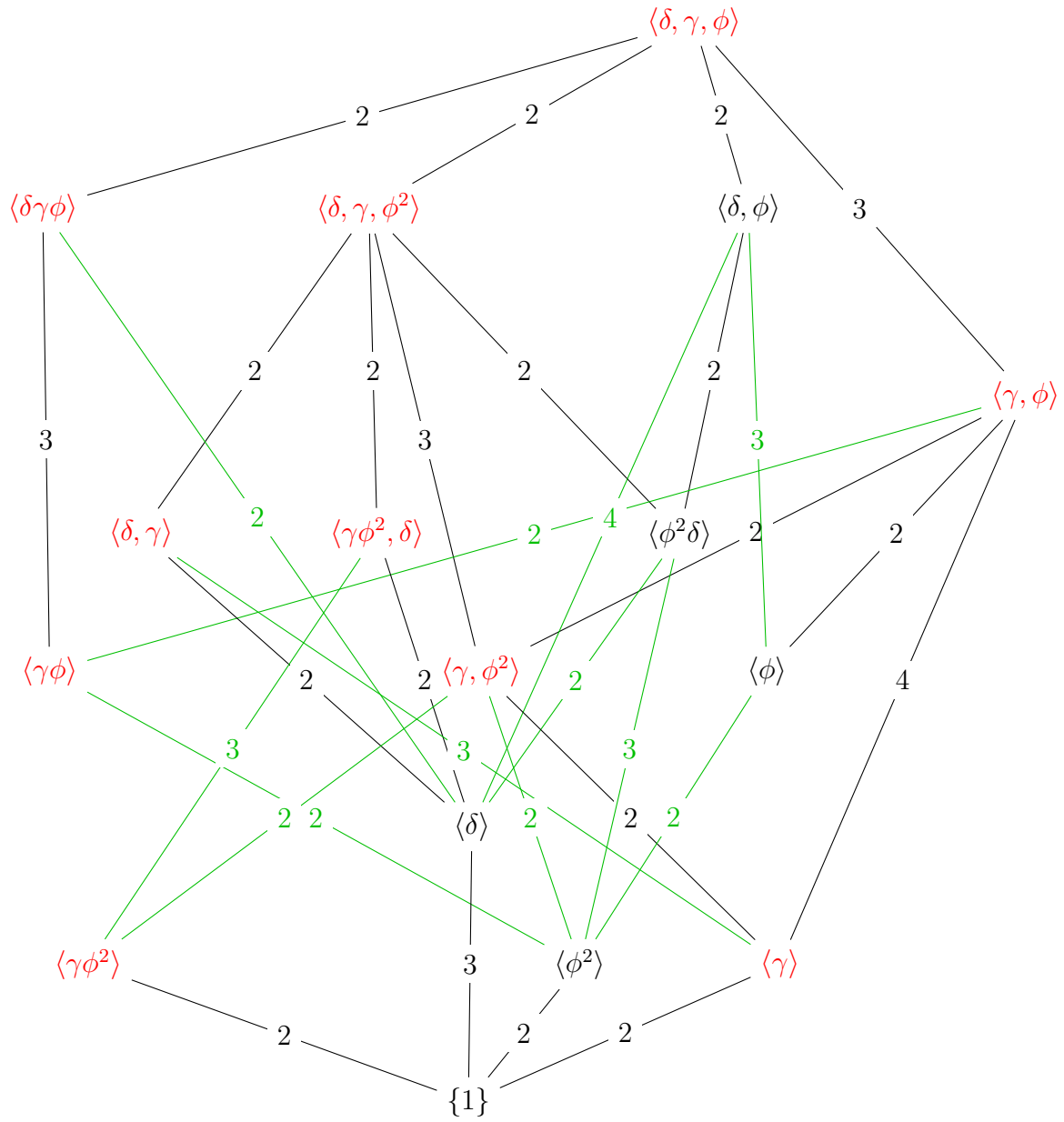

FIGURE 5. The conjugacy class subgroup diagram of $\mathrm{Out}(\mathrm{L}_3(2^4))$

3.2.5. *Exceptional groups of Lie type.* In this section we classify all of the almost simple primitive groups of degree $4096 \leq d < 8192$ with exceptional socles.

Proposition 3.40. *Let G be an almost simple group with an exceptional socle such that G has a faithful primitive permutation action of degree d where $4096 \leq d < 8192$. Suppose that $G \not\cong G_2(2)' \cong \mathrm{U}_3(3)$ and $G \not\cong {}^2G_2(3) \cong \mathrm{L}_2(8) : 3$, then $H := \mathrm{Soc}(G)$ is one of $G_2(3)$ or $G_2(5)$.*

Proof. As in Proposition 3.33, we only need to consider the *simple* exceptional groups.

The formulae for $P(H)$ are given in [20, Table 4]. They are all monotonically increasing in q. In the case of $H = E_7(q)$ there is a mistake in [20, Table 4] and so we use [43, Theorem 2], this is also monotonically increasing in q.

We begin by looking at the untwisted groups: $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, and $G_2(q)$.

$E_6(q)$: Here
$$P(E_6(q)) = \frac{(q^9-1)(q^8+q^4+1)}{q-1}.$$
Thus $P(E_6(2)) = 139503 > 8192$, and so $P(E_6(q)) > 8192$ for all q. Hence there are no almost simple groups with socle $E_6(q)$ in our range.

$E_7(q)$: Here
$$P(E_7(q)) = \frac{(q^{14}-1)(q^9+1)(q^5+1)}{q-1}$$
which is larger than 8192 for all q. Hence there are no almost simple groups with socle $E_7(q)$ in our range.

$E_8(q)$: Here
$$P(E_8(q)) = \frac{(q^{30}-1)(q^{12}+1)(q^{10}+1)(q^6+1)}{q-1}$$
which is larger than 8192 for all q. Hence there are no almost simple groups with socle $E_8(q)$ in our range.

$F_4(q)$: Here
$$P(F_4(q)) = \frac{(q^{12}-1)(q^4+1)}{q-1}.$$
This gives $P(F_4(2)) = 69615 > 8192$ and this does not lie in the range we are considering. Hence there are no almost simple groups with socle $F_4(q)$ in our range.

$G_2(q)$: For all $q > 4$ we have that the minimal degree of $G_2(q)$ is
$$P(G_2(q)) = q^5 + q^4 + q^3 + q^2 + q + 1.$$
Therefore $P(G_2(q)) > 8192$ for all $q > 5$. Furthermore $G_2(2)$ is not simple and we are not considering $G_2(2)' \cong \mathrm{U}_3(3)$. The groups $G_2(3)$ and $G_2(3).2$ both have one conjugacy class of maximal subgroups of index $4096 \leq d < 8192$. Their indices are both 7371 by the $\mathbb{ATLAS}$ [12]. Neither of the groups

$G_2(4)$ and $\mathrm{Aut}(G_2(4)) \cong G_2(4).2$ have maximal subgroups with index in the correct range. The group $G_2(5) \cong \mathrm{Aut}(G_2(5))$ contains two conjugacy classes of maximal subgroups of index between $4096 \leq d < 8192$. One with index 7750 and the other with index 7875.

We now look at the twisted groups: ${}^2B_2(2^{2m+1}) = \mathrm{Sz}(2^{2m+1})$, ${}^3D_4(q)$, ${}^2E_6(q)$, ${}^2F_4(2^{2m+1})$, and ${}^2G_2(3^{2m+1})$.

$\mathrm{Sz}(2^{2m+1})$: Here

$$P(\mathrm{Sz}(2^{2m+1})) = (2^{2m+1})^2 + 1.$$

Hence for all $m \geq 3$ we see that this minimal degree is greater than 8191. Thus we only need to consider $\mathrm{Sz}(32)$ and $\mathrm{Sz}(8)$. By the $\mathbb{ATLAS}$ [12], no maximal subgroups of $\mathrm{Sz}(32), \mathrm{Aut}(\mathrm{Sz}(32)) \cong \mathrm{Sz}(32).5$, $\mathrm{Sz}(8)$, or $\mathrm{Aut}(\mathrm{Sz}(8)) \cong \mathrm{Sz}(8).3$ have indices in the range $4096 \leq d < 8192$. Hence there are no almost simple groups with socle $\mathrm{Sz}(2^{2m+1})$ in our range.

${}^3D_4(q)$: Here

$$P({}^3D_4(q)) = (q^8 + q^4 + 1)(q + 1).$$

Thus if $q \geq 3$ then the degree is larger than 8191. So we consider $H = {}^3D_4(2)$. By the $\mathbb{ATLAS}$ [12], neither ${}^3D_4(2)$, nor $\mathrm{Aut}({}^3D_4(2)) \cong {}^3D_4(2).3$ have maximal subgroups with indices in our range. Hence there are no almost simple groups with socle ${}^3D_4(q)$ in our range.

${}^2E_6(q)$: Here

$$P({}^2E_6(q)) = \frac{(q^{12} - 1)(q^6 - q^3 + 1)(q^4 + 1)}{q - 1}.$$

This is greater than 8191 for any q. Hence there are no almost simple groups with socle ${}^2E_6(q)$ in our range.

${}^2F_4(2^{2m+1})$: Here

$$P({}^2F_4(q)) = (q^6 + 1)(q^3 + 1)(q + 1)$$

for $q = 2^{2m+1}$ an odd power of 2. Therefore $P({}^2F_4(q)) > 8192$ for all $q > 2$. By the $\mathbb{ATLAS}$ [12], neither of the groups ${}^2F_4(2)'$ nor $\mathrm{Aut}({}^2F_4(2)') \cong {}^2F_4(2)'.2$ have maximal subgroups in our required range. Hence there are no almost simple groups with socle ${}^2F_4(2^{2m+1})$ in our range.

${}^2G_2(3^{2m+1})$: Here

$$P({}^2G_2(3^{2m+1})) = (3^{2m+1})^3 + 1.$$

Hence $P({}^2G_2(3^{2m+1})) > 8191$ for all $m \geq 1$. Thus all that remains is $H = {}^2G_2(3)$, but in this case ${}^2G_2(3) \cong \mathrm{L}_2(8) : 3$. Hence there are no almost simple groups with socle ${}^2G_2(3^{2m+1})$ in our range.

□

Theorem 3.41. *The primitive almost simple groups G with exceptional socles such that G is of degree $4096 \leq d < 8192$ are displayed in Table 15.*

Proof. We input the automorphism groups of the simple groups described in Proposition 3.40 ($G_2(3)$ and $G_2(5)$) into the procedure below (in Section 3.2.6). □

3.2.6. *Sporadic simple groups.* In this section we classify the almost simple primitive groups of degree $4096 \leq d < 8192$ with sporadic socles.

The list of maximal subgroups of the sporadic groups is complete with the exception of the monster group M. However M has no transitive permutation representation of degree < 8192. By the $\mathbb{ATLAS}$ [12], the sporadic simple groups which have a primitive permutation permutation representation of degree $d < 8192$ are displayed on Table 2. Most of these groups are not the socle of an almost simple group with degree $4096 \leq d < 8192$. We have highlighted (with $\star$) those which are the socle of an almost simple group of degree $4096 \leq d < 8192$.

Simple Group	Simple Group
M_{11}	Co_3
M_{12}	McL $\star$
M_{22}	Suz
M_{23}	He
M_{24}	Fi_{22}
HS $\star$	J_1 $\star$
J_2	J_3 $\star$
Co_2	Ru

TABLE 2. Sporadic socles of almost simple groups with minimal degree at most 8191.

Theorem 3.42. *The primitive almost simple groups G with a sporadic socle such that G is of degree $4096 \leq d < 8192$ are displayed in Table 15.*

Proof. We input the automorphism groups of the sporadic groups described above (J_1, J_2, HS, and McL) into the procedure below. □

For both the exceptional groups of Lie type and the sporadic simple groups we use the MAGMA function "MaximalSubgroups" to produce the conjugacy class representatives of their maximal subgroups.

Primitive Almost Simple Groups with Exceptional or Sporadic Socles

Input: The Automorphism group A of an exceptional or sporadic group T, described in Proposition 3.40 or Section 3.2.6.

Output: A list **Primitive**, consisting of all almost simple primitive groups with socle T.

Step 1: Define $T := \mathrm{Soc}(A)$, Construct empty lists **CohortReps** and **Primitive**.

Step 2 Define the empty list **Max**.

Step 2(a): Append to **Max** the representatives of the conjugacy classes of any subgroups of A which are maximal subgroups of T with index in T between 4096 and 8191.

Step 2(b): Append to **Max** the representatives of the conjugacy classes of any subgroups of A that are maximal in some non-trivial extension of T with index between 4096 and 8191 in that extension.

Step 3: For each $m \in$ **Max**, let C be the image of the action of T on the cosets of m via "CosetImage". Append C to **CohortReps**.

Step 4: For each $P \in$ **CohortReps**, calculate $N := N_{\mathrm{Sym}(\mathrm{Deg}(P))}(\mathrm{Soc}(P))$ and the quotient $Q := N/\mathrm{Soc}(P)$, together with the epimorphism $\phi : N \to Q$. For each conjugacy class representative S of the subgroups of Q, if the preimage s of S under ϕ is primitive then Append s to **Primitive**.

Step 5: **Return: Primitive**.

3.3. **Groups of diagonal type.** In this section we classify the primitive groups of diagonal type of degree $4096 \leq d < 8192$.

The following is [16, Theorem 4.3A].

Theorem 3.43. *Let G be a non-trivial finite group.*

(i) If H is a minimal normal subgroup of G and L is any normal subgroup of G, then either $H \leq L$ or $\langle H, L\rangle = H \times L$.

(ii) There exist minimal normal subgroups $H_1, \ldots, H_k$ of G such that $\mathrm{Soc}(G) = H_1 \times \cdots \times H_k$.

(iii) Every minimal normal subgroup H of G is a direct product $H = T_1 \times \cdots \times T_m$ where the T_i are simple normal subgroups of H which are conjugate under the action of G.

(iv) If the subgroups H_i are all non-abelian, then $H_1, \ldots, H_k$ are the only minimal normal subgroups of G. Similarly if the T_i are non-abelian, then these are the only minimal normal subgroups of H.

Let T be a non-abelian simple group and $m > 1$ be an integer.

We recall Definition 1.10 and define $W := \mathrm{Aut}(T) \wr S_m$. So

$$W = \{(a_1, \ldots, a_m)\pi \mid a_i \in \mathrm{Aut}(T), 1 \leq i \leq m, \pi \in S_m\}.$$

Observe that for any $(a_1, \ldots, a_m)\pi, (b_1, \ldots, b_m)\rho \in W$, we have

$$(a_1, \ldots, a_m)\pi(b_1, \ldots, b_m)\rho = (a_1 b_{1^\pi}, \ldots, a_m b_{m^\pi})\pi\rho.$$

We introduce the following notation

$$(a_1, \ldots, a_m)^\pi := (1, \ldots, 1)\pi^{-1}(a_1, \ldots, a_m)1(1, \ldots, 1)\pi = (a_{1\pi^{-1}}, \ldots, a_{m\pi^{-1}}).$$

We define $K \subseteq W$ by

$$K := \{(a_1, \ldots, a_m)\pi \mid a_i \in \mathrm{Aut}(T), \pi \in S_m, a_i \equiv a_j \bmod(\mathrm{Inn}(T)) \text{ for all } i, j\}.$$

One can observe that K is a subgroup of W.

By [16, Theorem 4.5A], the socle of K is

$$H := \{(a_1, \ldots, a_m)1 \mid a_i \in \mathrm{Inn}(T), 1 \leq i \leq m\} \cong T^m$$

and K is an extension of H by $\mathrm{Out}(T) \times S_m$, *i.e.* we have $K = H.(\mathrm{Out}(T) \times S_m) \cong T^m.(\mathrm{Out}(T) \times S_m)$. We observe that H is also the socle of W.

We define the inclusion maps $\phi : \mathrm{Aut}(T) \to W$ and $\psi : S_m \to W$ by $(a)\phi := (a, 1 \ldots, 1)1$ and $(\pi)\psi := (1, \ldots, 1)\pi$. We note that $\mathrm{Im}(\phi) = \{(a, 1, \ldots, 1)1 \mid a \in \mathrm{Aut}(T)\} \cong \mathrm{Aut}(T)$ and $\mathrm{Im}(\psi) = \{(1, \ldots, 1)\pi \mid \pi \in S_m\} \cong S_m$.

As T is a non-abelian simple group, we have that

$$\mathrm{Soc}(\mathrm{Im}(\phi)) = \{(t, 1, \ldots, 1)1 \mid t \in \mathrm{Inn}(T)\} \cong \mathrm{Inn}(T) \cong T.$$

The following may be found in [24, Definition 2.7].

Definition 3.44. Let G be a group and A a subset of G. The *normal closure* N of A in G is the intersection of all normal subgroups of G containing A,

$$N = \bigcap_{A \subseteq X \trianglelefteq G} X.$$

Let N be the normal closure of $\mathrm{Soc}(\mathrm{Im}(\phi))$ in W. As $\mathrm{Soc}(\mathrm{Im}(\phi)) \leq H \trianglelefteq W$ we have that $N \leq H \cong T^m$.

For $1 \leq i \leq m$ we define T_i to be the subgroup of H consisting of the m-tuples with 1 in all but the i^{th} component, so that $T_i \cong T$ and $H \cong T_1 \times \cdots \times T_m$.

By Theorem 3.43 (iv), $T_1, \ldots, T_m$ are the only minimal normal subgroups of H. We observe that $\mathrm{Soc}(\mathrm{Im}(\phi)) = T_1$.

Take the element $w := (1, \ldots, 1)\rho \in W$ where ρ is the transposition $(1, i)$, for some $1 \leq i \leq m$. Then for any element $(t, 1, \ldots, 1)1 \in T_1$ we have that

$$w^{-1}(t, 1, \ldots, 1)1w = (t, 1, \ldots, 1)^\rho = (1, \ldots, 1, t, 1, \ldots, 1)1$$

where t is in the i^{th} position. In particular $w^{-1}(t, 1, \ldots, 1)1w \in T_i$.

As $T_1 = \mathrm{Soc}(\mathrm{Im}(\phi)) \leq N$ and $N \trianglelefteq W$ we must have that N contains all conjugates of T_1 in W. So N contains $T_1, \ldots, T_m$ and so $H \leq N$. Thus $N = H$.

We define the subgroup W_D of W via

$$W_D := \{(a, \ldots, a)1 \mid a \in \mathrm{Aut}(T)\} \cong \mathrm{Aut}(T).$$

Lemma 3.45. *The subgroup of W generated by N, W_D, and $\mathrm{Im}(\psi)$ is K.*

Proof. We observe that $N, W_D, \mathrm{Im}(\psi) \leq K$ and so $\langle N, W_D, \mathrm{Im}(\psi)\rangle \leq K$.

Fix an element $(a_1, \ldots, a_m)\pi \in K$. As $a_i \equiv a_j \bmod (\mathrm{Inn}(T))$ for all $1 \leq i, j \leq m$, we have that $a_i = ta_j$ for some $t \in \mathrm{Inn}(T)$. In particular a_i and a_j lie in the same coset of $\mathrm{Inn}(T)$. Thus there exists some coset representative $a \in \mathrm{Aut}(T)$ and $t_i \in \mathrm{Inn}(T)$ such that $a_i = t_i a$.

Let $(t_1, \ldots, t_m)1 \in N$, $(a, \ldots, a)1 \in W_D$, and $(1, \ldots, 1)\pi \in \mathrm{Im}(\psi)$, where t_i and a are defined as above. Then

$$\begin{aligned}(t_1, \ldots, t_m)1(a, \ldots, a)1(1, \ldots, 1)\pi &= (t_1, \ldots, t_m)1(a, \ldots, a)\pi \\ &= (t_1 a, \ldots, t_m a)\pi \\ &= (a_1, \ldots, a_m)\pi.\end{aligned}$$

Thus $K \leq \langle N, W_D, \mathrm{Im}(\psi)\rangle$ and so $K = \langle N, W_D, \mathrm{Im}(\psi)\rangle$. □

We observe that W_D commutes with $\mathrm{Im}(\psi)$ and their intersection is trivial, so $D := \langle W_D, \mathrm{Im}(\psi)\rangle \cong \mathrm{Aut}(T) \times S_m \cong T.(\mathrm{Out}(T) \times S_m)$. In fact we have that

$$D = \{(a, \ldots, a)\pi \mid a \in \mathrm{Aut}(T), \pi \in S_m\}.$$

We call D the *diagonal subgroup* of K. The action of K by right multiplication on the set Ω of cosets of D in K is called the *diagonal action* of K.

The degree of this action is $|\Omega| = |K : D| = |T|^{m-1}$. We will write the image of the permutation representation of K with the diagonal action as K^Ω. As $H \leq K$, H also acts on Ω and we write H^Ω for the image of this corresponding permutation representation.

We say that a group $\hat{G}$ is of *diagonal type* if it is permutation isomorphic to a group G such that $H^\Omega \leq G \leq K^\Omega$ with the diagonal action.

By [16, Lemma 4.5B], $\mathrm{Soc}(G) = H^\Omega \cong T^m$, the degree d of G is equal to $|T|^{m-1}$, and the full normalizer of $\mathrm{Soc}(G)$ in S_d is equal to K^Ω.

Define $\Gamma := \{T_1, \ldots, T_m\}$. For any diagonal type group G we have $H \trianglelefteq G$ and $T_1, \ldots, T_m$ are the only minimal normal subgroups of H. Hence G acts on Γ by

conjugation.

The following is [16, Theorem 4.5A].

Theorem 3.46. *A diagonal type group $H^\Omega \leq G \leq K^\Omega$ is primitive if and only if either*

(i) $m = 2$; or

(ii) $m \geq 3$ and the action of G on Γ is primitive.

We are finding the primitive diagonal type groups of degree $4096 \leq d = |T|^{m-1} < 8192$. Thus the possible finite non-abelian simple groups T are M_{11}, $\mathrm{L}_2(23)$, $\mathrm{L}_2(25)$, $\mathrm{L}_3(3)$, and $\mathrm{U}_3(3)$ with $m = 2$ and there are no groups with $m \geq 3$ in our range.

We give the following procedure for general m as it will be useful in Section 4.2.

The Diagonal Type Groups

Input: A non-abelian simple group T such that $4096 \leq |T|^{m-1} \leq 8191$ for some $m \geq 2$.

Output: The full cohort of diagonal type primitive groups with socle T^m.

Step 1: Construct an empty list **Primitive**.

Step 2: For each $m \geq 2$ such that $4096 \leq |T|^{m-1} \leq 8191$ do the following.

Step 2(a): Define $A := \mathrm{Aut}(T)$ and construct the wreath product $W := A \wr S_m$. Let $\phi : A \to W$ be the inclusion of A into W given by $a \mapsto (a, 1, \ldots, 1)1$ and let $\psi : S_m \to W$ be the inclusion of S_m into W given by $\pi \mapsto (1, \ldots, 1)\pi$.

Step 2(b): Construct the following groups.

Step 2(b)(i): Define N as the normal closure in W of the socle of $\mathrm{Im}(\phi)$. $N = \{(a_1, \ldots, a_m)1 \mid a_i \in \mathrm{Inn}(T), 1 \leq i \leq m\} \leq W$.

Step 2(b)(ii) Define W_D as $W_D = \{(a, \ldots, a)1 \mid a \in \mathrm{Aut}(T)\}$.

Step 2(b)(iii) Define K as the subgroup of W generated by N, W_D and $\mathrm{Im}(\psi)$.

Step 2(b)(iv) Define D as the subgroup of W generated by W_D and $\mathrm{Im}(\psi)$.

Step 2(c): Define P to be the image of the action of K on cosets of D via "CosetImage". Define Q to be the quotient $P/\mathrm{Soc}(P)$, and define ρ to be the natural epimorphism $P \to Q$.

Step 2(d): Define **Sub** to be a list of conjugacy class representatives of the subgroups of Q.

Step 2(e): For each $s \in$ **Sub**, if the preimage in P of s under ρ is primitive then Append the preimage of s under ρ to **Primitive**.

Step 3: Return: Primitive.

Theorem 3.47. *The primitive permutation groups of diagonal type with degree in the range* $4096 \leq d < 8192$ *are given in Table 16.*

Proof. Input the non-abelian simple groups T with $4096 \leq |T|^{m-1} < 8192$, for some $m \geq 2$, into the procedure above. So $m = 2$ and $T = M_{11}$, $\mathrm{L}_2(23)$, $\mathrm{L}_2(25)$, $\mathrm{L}_3(3)$, or $\mathrm{U}_3(3)$. □

3.4. **Groups of product type.** In this section we classify the primitive groups of product type of degree $4096 \leq d < 8192$.

The following definition is [44, p.21].

Definition 3.48. Let A be a group acting on a set Δ and let $W := A \wr S_k$. The *product action* of $(a_1, \ldots, a_k)\sigma \in W$ on $(\delta_1, \ldots, \delta_k) \in \Delta^k$ is defined as follows:

$$(\delta_1, \ldots, \delta_k)^{(a_1,\ldots,a_k)\sigma} = (\delta_1^{a_1}, \ldots, \delta_k^{a_k})^{\sigma} = (\delta_{1\sigma^{-1}}^{a_{1\sigma^{-1}}}, \ldots, \delta_{k\sigma^{-1}}^{a_{k\sigma^{-1}}}).$$

We call the permutation representation of W with the product action in $\mathrm{Sym}(\Delta^k)$ the *product action wreath product*.

Definition 3.49. Let G be a primitive permutation group with $\mathrm{Soc}(G) \cong T^m$ for some $m > 1$. We say that G is of *product type* if there exists a non-trivial divisor $l \mid m$ and a primitive group P of almost simple or diagonal type, with $\mathrm{Soc}(P) \cong T^l$, such that G is permutation isomorphic to a subgroup of a product action wreath product $W := P \wr S_{m/l}$.

If G is of product type then we identify G with the corresponding subgroup of W.

If P is of degree n then $W \leq S_{n^{m/l}}$. Hence the degree of any group of product type is $n^{m/l}$.

By [16, Lemma 4.5A], W is the normalizer of $\mathrm{Soc}(G)$ in S_d and we have that $\mathrm{Soc}(G) = \mathrm{Soc}(W) \cong \mathrm{Soc}(P)^{m/l}$.

We therefore find the groups G such that $\mathrm{Soc}(W) \leq G \leq W$, for which G is a primitive permutation group (of degree $n^{m/l}$).

Since P is of almost simple or diagonal type, the degree n of P is at least 5. Our condition that $4096 \leq d = n^{m/l} < 8192$ implies that $m/l \leq 5$ and the following values of n can occur:

- $m/l = 2$ and $64 \leq n < 91$,
- $m/l = 3$ and $16 \leq n < 21$,
- $m/l = 4$ and $8 \leq n < 10$, or

- $m/l = 5$ and $n = 6$.

The primitive groups of degree less than 91 all appear in the primitive groups library of MAGMA.

Using this library we find all primitive almost simple and diagonal type groups of degree at most 91. We define P to be the largest primitive group in its cohort; by Remark 3.3, this is a unique group. We create a new list consisting of these groups which we call maximal cohort representatives.

The only diagonal type group in this list is $A_5^2.2^2$ which has socle isomorphic to $A_5 \times A_5$ and is of degree 60. No power of 60 lies in our range so for $l > 1$ we will not find any primitive groups of product type with degree in our range.

Every other primitive group P must be of almost simple type. Hence $l = 1$ and $m = 2, 3, 4$, or 5.

For each P we construct the product action wreath product $W = P \wr S_{m/l}$. We then take the quotient $Q := W/\mathrm{Soc}(W)$ and corresponding epimorphism $\rho : W \to Q$. For any subgroup S of Q, we consider the preimage of S under ρ, *i.e.* the subgroups of W containing its socle. The primitive preimages are the primitive product type groups of degree $n^{m/l}$.

We give the following procedure for a general primitive group P of almost simple or diagonal type, as it will be useful in Section 4.3.

The Product Type Groups

Input: A primitive almost simple or diagonal type group P of degree n, with $4096 \leq n^{m/l} \leq 8191$ such that $\mathrm{Soc}(P) \cong T^l$ for some non-abelian simple group T, $l \geq 1$, $m \geq 2$, and $m > l$.

Output: The full cohort of primitive product type groups of degree $n^{m/l}$ with socle T^m.

Step 1: Construct an empty list **Primitive**.

Step 2: Construct the product action wreath product $W = P \wr S_{m/l}$ via "PrimitiveWreathProduct". Construct the quotient $Q = W/\mathrm{Soc}(W)$, and define ρ to be the epimorphism $W \to Q$.

Step 3: Define a list **Sub** of conjugacy class representatives of the subgroups of Q.

Step 4: For each $S \in$ **Sub** if the preimage G, of S under ρ is primitive then Append G to **Primitive**.

Step 5: **Return: Primitive**.

Theorem 3.50. *The product action type primitive permutation groups of degree* $4096 \leq d < 8192$ *are given in Table 17.*

Proof. Input every almost simple primitive group of degree at most 91 into the procedure above. □

4. A Non-Affine Primitive Group Function up to Degree 1000000

In this section we discuss the methods that we used to produce a general function in MAGMA which, for a given $1 \leq d \leq 1000000$, outputs all non-affine primitive groups of degree d.

We chose to omit the affine type groups as this is a major bottleneck in producing primitive groups of larger degrees. For example, producing the affine type groups of degree 3^8 required around one week of computation time.

4.1. **Almost simple groups.** As in Section 3.2, we split the almost simple groups into different cases depending upon their socle. We begin with an empty list **Primitive** to which we will add sublists of cohorts of primitive groups.

4.1.1. *Alternating groups.* Recall Definition 3.29, for any degree $d > 4$ the groups A_d and S_d in their natural action form a single cohort. Thus we may add these groups as a cohort to **Primitive**.

We now find the indices n such that A_n or S_n have a primitive action of degree d other than the natural action. We use the methods from the proof of Proposition 3.31. This produces three (possibly empty) lists of indices corresponding to the three cases in the proof.

For each of these indices we produce the almost simple groups with socle A_n and then find any maximal subgroups of degree d using the function "MaximalSubgroups" in MAGMA. If any are found we add the corresponding primitive groups to **Primitive**.

Primitive Almost Simple Groups with Alternating Socles

Input: An integer $1 \leq d \leq 1000000$.
Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with an alternating socle.

Step 1: Add $[A_d, S_d]$ under their natural actions to a list **Primitive**.

Step 2: Define three empty lists $A1, A2$, and $A3$.
Step 2(a): For each integer $5 \leq i \leq 18$ if $2d \leq \lfloor (i+1)/2 \rfloor !$ then add i to $A1$.
Step 2(b): For each $2 \leq i \leq 7$ and $2 \leq j \leq 11$, if $(ij)!/((j!)^i i!) = d$ then add ij to $A2$.
Step 2(c): For each integer $i \geq 5$ such that $\binom{i}{2} \leq d$ consider every integer $k \geq 2$ such that $k \leq \lceil (i-1)/2 \rceil$. If $d = i!/(k!(i-k)!)$ then add i to $A3$.

Step 3: For n in $A1$, define $S := S_n$ and $A := \mathrm{Soc}(S)$. Then:

Step 3(a): Create the list $\mathbf{Max}_S$ of representatives of the conjugacy classes of the primitive maximal subgroups of S with index d. For each M_S in $\mathbf{Max}_S$ do $C := \mathrm{CosetImage}(M_S, S)$ and Append C to **Primitive**.

Step 3(b): Create the list $\mathbf{Max}_A$ of representatives of the conjugacy classes of the primitive subgroups of S which are maximal subgroups of A with index d in A. For each M_A in $\mathbf{Max}_A$ do $C := \mathrm{CosetImage}(M_A, A)$ and Append C to **Primitive**.

Step 4: For n in $A2$, define $S := S_n$ and $A := \mathrm{Soc}(S)$. Then proceed as in **Step 3(a)** and **Step 3(b)** but for transitive, imprimitive maximal subgroups of S.

Step 5: For n in $A3$, define $S := S_n$ and $A := \mathrm{Soc}(S)$. Then proceed as in **Step 3(a)** and **Step 3(b)** but for intransitive maximal subgroups of S.

Step 6: Return: Primitive.

We note that, for clarity of reading, we have omitted the almost simple groups with socle A_6, as $\mathrm{Aut}(A_6) \ncong S_6$. These primitive groups are of index at most 45 and are described in detail in [36].

4.1.2. *Classical groups.* In this section we give the methods we used to produce our general function in MAGMA which, for a given $d \leq 1000000$, outputs all of the almost simple type groups with classical socles. Recall that q is always a prime power.

We first consider the groups $T = \mathrm{L}_2(q)$. For any $q \geq 7$ with $q \neq 9$, there is an almost simple primitive group of degree $q+1$ with socle $\mathrm{L}_2(q)$. For each input $d \leq 1000000$, calculating the maximal subgroups of all $\mathrm{L}_2(q)$'s with $q+1 \leq d$ would be computationally intensive. For example, the input $d = 1000000$ would give 78729 such q's. Finding the maximal subgroups for each corresponding $\mathrm{L}_2(q)$ would not be feasible.

However the maximal subgroups of $\mathrm{L}_2(q)$ are well known, see for example [6, Table 8.1 and Table 8.2]. We can therefore directly check, via the possible orders of maximal subgroups, whether there exists some q such that $\mathrm{L}_2(q)$ has a maximal subgroup of index d.

If $T \neq \mathrm{L}_2(q)$ then we use the same method as Proposition 3.33, to find all possible classical simple groups that are the socle of a primitive group of degree $d \leq 1000000$.

Proposition 4.1. *Let G be an almost simple group with a faithful primitive permutation action of degree less than* 1000000 *such that the socle H of G is classical. Then H appears in Table 3.*

Proof. The proof is a repeat of the proof of Proposition 3.33, but for degree 1000000. □

For each input $d \leq 1000000$, it is again impractical to search through each classical group T with $P(T) \leq 1000000$ to determine whether T has a maximal subgroup of index d. Therefore for each group T in Table 3, we used the MAGMA functions "MaximalSubgroups" and "ClassicalMaximals" to find and store the indices of every maximal subgroup $M \leq T$ such that $|T : M| \leq 1000000$. These functions were created via the tables in [6] and [28]. We also stored the indices of any novelties.

We stored these indices in lookup tables, Tables 25, 26, 27, 28, 29, and 30. If d appears in a lookup table, then we know the associated simple group T. Therefore for a given input $1 \leq d \leq 1000000$, we calculate only the corresponding almost simple groups with classical socle T. For the method to use these tables we refer the reader to Section 6.3.

Primitive Almost Simple Groups with Classical Socles

Input: An integer $1 \leq d \leq 1000000$.

Output: A list, **Primitive**, consisting of all almost simple primitive groups of degree d with a classical socle.

Step 1: Define an empty list **SimpleGroups**.

Step 2(a): Use known results on the possible indices of maximal subgroups of $\mathrm{L}_2(q)$ to determine for which q there is a maximal subgroup of index d in $\mathrm{L}_2(q)$. For each such q, Append $\mathrm{L}_2(q)$ to **SimpleGroups**.

Step 2(b): Use the lookup tables (25, 26, 27, 28, 29, and 30) to find the possibilities for the classical socles of the almost simple group of degree d (other than non-novelty $\mathrm{L}_2(q)$). Append each of these groups to **SimpleGroups**.

Step 2(c): If **SimpleGroups** is empty then **Return: SimpleGroups**.

Step 3: For each $T \in$ **SimpleGroups**, input $A := \mathrm{Aut}(T)$ into the classical almost simple groups procedure (See Section 3.2.2), with bounds of d for the index of any maximal subgroups. This outputs a new list **Primitive**.

Step 4: **Return: Primitive**.

Group	n	q
$\mathrm{L}_n(q)$	$n = 2$	$7 \leq q \leq 999983$, $q \neq 9$
	$n = 3$	$3 \leq q \leq 997$
	$n = 4$	$3 \leq q \leq 97$
	$n = 5$	$2 \leq q \leq 31$
	$n = 6$	$2 \leq q \leq 13$
	$n = 7$	$2 \leq q \leq 9$
	$n = 8$	$2 \leq q \leq 7$
	$n = 9$	$2 \leq q \leq 5$
	$n = 10$	$2 \leq q \leq 4$
	$11 \leq n \leq 13$	$2 \leq q \leq 3$
	$14 \leq n \leq 19$	$q = 2$
$\mathrm{S}_{2m}(q)$	$m = 2$	$3 \leq q \leq 97$
	$m = 3$	$2 \leq q \leq 13$
	$m = 4$	$2 \leq q \leq 7$
	$m = 5$	$2 \leq q \leq 4$
	$m = 6$	$2 \leq q \leq 3$
	$7 \leq m \leq 10$	$q = 2$
$\mathrm{U}_n(q)$	$n = 3$	$3 \leq q \leq 97$
	$n = 4$	$2 \leq q \leq 31$
	$n = 5$	$2 \leq q \leq 7$
	$n = 6$	$2 \leq q \leq 4$
	$n = 7$	$2 \leq q \leq 3$
	$8 \leq n \leq 11$	$q = 2$
$\mathrm{P}\Omega_{2m+1}(q)$	$m = 3$	$3 \leq q \leq 13$
	$m = 4$	$3 \leq q \leq 7$
	$5 \leq m \leq 6$	$q = 3$
$\mathrm{P}\Omega^+_{2m}(q)$	$m = 4$	$2 \leq q \leq 9$
	$m = 5$	$2 \leq q \leq 5$
	$6 \leq m \leq 7$	$2 \leq q \leq 3$
	$8 \leq m \leq 10$	$q = 2$
$\mathrm{P}\Omega^-_{2m}(q)$	$m = 4$	$2 \leq q \leq 9$
	$m = 5$	$2 \leq q \leq 5$
	$6 \leq m \leq 7$	$2 \leq q \leq 3$
	$8 \leq m \leq 10$	$q = 2$

TABLE 3. Classical socles of almost simple groups with minimal degree at most 1000000.

4.1.3. *Exceptional groups of Lie type and Sporadic Simple Groups.* In this section we give the methods we used to produce our general function in MAGMA which, for a given $d \leq 1000000$, outputs all of the almost simple type groups with exceptional or sporadic socles. Recall that q is always a prime power.

The following is essentially Proposition 3.40.

Proposition 4.2. *Let G be an almost simple group with a faithful primitive permutation action of degree d where $d \leq 1000000$ such that $\mathrm{Soc}(G)$ is an exceptional group. Suppose that $\mathrm{Soc}(G)$ is not an alternating or classical group. Then $\mathrm{Soc}(G)$ appears on Table 4.*

Proof. This proof is exactly the proof of Proposition 3.40, but with $d \leq 1000000$. □

Group	Conditions
$E_6(2)$	
$F_4(2)$	
$G_2(q)$	$3 \leq q \leq 13$
$\mathrm{Sz}(2^{2m+1})$	$1 \leq m \leq 4$
${}^3D_4(q)$	$2 \leq q \leq 4$
${}^2F_4(2)'$	
${}^2G_2(3^3)$	

TABLE 4. Exceptional socles of almost simple groups with minimal degree at most 1000000.

.

The list of maximal subgroups of the sporadic groups is complete with the exception of the monster group M. The minimal degree of a faithful permutation representation of M is $\approx 10^{20} >> 1000000$.

Proposition 4.3. *Let G be an almost simple group with a sporadic socle. If G has a faithful primitive permutation action of degree d where $d \leq 1000000$ then $\mathrm{Soc}(G)$ appears in Table 5.*

Proof. We use the $\mathbb{ATLAS}$ [12] to find the maximal subgroups of the sporadic groups T with indices at most 1000000. These maximal subgroups correspond to faithful primitive group actions with socle T. □

Each of the groups in Tables 4 and 5 have computable maximal subgroups in MAGMA using the "MaximalSubgroups" function with the following exceptions: ${}^3D_4(3)$, ${}^3D_4(4)$, $\mathrm{Sz}(128)$, $\mathrm{Sz}(512)$, $E_6(2)$, Co_1, $\mathrm{Fi}_{24}{}'$, O'N, and $G_2(q)$ for $7 \leq q \leq 13$.

We have stored all of the indices and novelty indices in lookup tables, Tables 31 and 32. For the method to use these tables we refer the reader to Section 6.3.

The procedure described below works for all $d \leq 1000000$ with the following exceptions, $d = 16385, 19608$, 26572, 37449, 58653, 58996, 66430, 98280, 122760, 130816, 131328, 139503, 177156, 186004, 262145, 265356, 266085, 306936, 328965, 402234, 664300, 885115, and 886446. These exceptions correspond to the indices of maximal subgroups of the simple groups which do not have computable maximal subgroups in MAGMA, described above.

Simple Group	Simple Group
M_{11}	McL
M_{12}	Suz
M_{22}	He
M_{23}	Fi_{22}
M_{24}	Fi_{23}
HS	Fi_{24}'
J_2	J_1
Co_1	O'N
Co_2	J_3
Co_3	Ru

TABLE 5. Sporadic socles of almost simple groups with minimal degree at most 1000000.

.

Primitive Almost Simple Groups with Exceptional or Sporadic Socles

Input: An integer $d \leq 1000000$, with d not one of the exceptions listed above.

Output: A list **PrimitiveGroups**, consisting of all almost simple primitive groups of degree $d \leq 1000000$ with an exceptional or sporadic socle.

Step 1: Define empty lists **SimpleGroups** and **PrimitiveGroups**. Use the lookup tables (31, 32) to determine whether there is an almost simple group of degree d with an exceptional or sporadic socle, T. Append each such T to **SimpleGroups**.

Step 2: If **SimpleGroups** is empty then **Return: SimpleGroups**.

Step 3: For each $T \in$ **SimpleGroups**:

Step 3(a): Define $A := \mathrm{Aut}(T)$ and input A into a procedure identical to the exceptional or sporadic group procedure described in Section 3.2.6, but with degree at most 1000000. This returns a list **Primitive**.

Step 3(b): For each $P \in$ **Primitive** append P to **PrimitiveGroups**.

Step 4: **Return: PrimitiveGroups**.

4.1.4. *The exceptions.* We now explicitly construct the almost simple primitive groups of degree d with exceptional or sporadic socles, where d is one of the exceptions. In each case we demonstrate how to compute the maximal subgroup, of index d, of the corresponding almost simple group. We then find the full cohort of primitive groups corresponding to this maximal subgroup via the same methods as the procedure given in Section 3.2.6. In several of the cases we find the maximal subgroup of the

almost simple group as the stabilizer of a subspace of a vector space upon which the image of a faithful representation of the group is acting.

The group ${}^3D_4(3)$.

Input: An integer $d = 26572$ or $d = 186004$.

Output: A list **Primitive** containing the full cohort of almost simple primitive groups with socle ${}^3D_4(3)$ of degree d.

Step 1: Define an empty list **Primitive**. Define G to be the matrix representation of ${}^3D_4(3)$ in $\mathrm{GL}(8, 27)$ via $G :=$ "ChevalleyGroup("3D", 4, 3)". Define $V := \mathbb{F}_{27}^8$ to be the vector space upon which G is acting.

Step 2: If $d = 26572$ then define M to be the stabilizer in G of a 2-dimensional subspace of V, generated by the first two basis vectors of V.
If $d = 186004$ then define M to be the stabilizer in G of a 1-dimensional subspace of V, generated by the first basis vector of V.

Step 3: Define P to be the image of the permutation representation of G acting on the cosets of M in G via "CosetImage".

Step 4: Calculate $N := N_{S_d}(\mathrm{Soc}(P))$ and the quotient $Q := N/\mathrm{Soc}(N)$ with corresponding epimorphism $\rho : N \to Q$.
For each conjugacy class representative S of the subgroups of Q, if the preimage s of S under ρ is primitive then Append s to **Primitive**.

Step 5: **Return: Primitive**.

The group ${}^3D_4(4)$.

Input: The integer $d = 328965$.

Output: A list **Primitive** containing the full cohort of almost simple primitive groups with socle ${}^3D_4(4)$ of degree d.

Step 1: Define an empty list **Primitive**.

Step 2: Construct A as the image of a permutation representation of $\mathrm{Aut}({}^3D_4(4))$ via "AutomorphismGroupSimpleGroup("3D4", 4)".
This representation is primitive of degree d.

Step 3: Construct the quotient $Q = A/\mathrm{Soc}(A)$ with corresponding epimorphism $\rho : A \to Q$.

For each conjugacy class representative S of the subgroups of Q, if the preimage s of S under ρ is primitive then Append s to **Primitive**.

Step 4: Return: Primitive.

The groups $G_2(q)$ for $7 \leq q \leq 13$.

Input: An integer $d = 19608, 37449, 66430, 177156$, or 402234.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle $G_2(q)$ for some $7 \leq q \leq 13$.

Step 1: Define empty lists **Primitive** and **CohortReps**.

Step 2(a): If $d = 19608$ then define $q := 7$.
Step 2(b): If $d = 37449$ then define $q := 8$.
Step 2(c): If $d = 66430$ then define $q := 9$.
Step 2(d): If $d = 177156$ then define $q := 11$.
Step 2(b): If $d = 402234$ then define $q := 13$.

Step 3(a): Define G to be the matrix representation of $G_2(q)$ in $\mathrm{GL}(7, q)$ via $G :=$ "ChevalleyGroup("G", 2, q)". Define V to be the vector space on which G is acting.

Step 3(b)(i): Define V_1, V_2 to be $1, 2$-dimensional subspaces of V, generated by the first, and first and second basis vectors of V respectively.
Step 3(b)(ii): Define P_i to be image of the permutation representation of the action of G on the cosets of the stabilizer in G of V_i via "CosetImage".
Append P_1 and P_2 to **CohortReps**.

Step 4: For each $P \in$ **CohortReps** construct $N_{S_d}(\mathrm{Soc}(P))$ and $Q := N/\mathrm{Soc}(P)$ with corresponding epimorphism $\rho : N \to Q$.
Define the list **Sub** of conjugacy class representatives of subgroups of Q.
For each $S \in$ **Sub** if the preimage G of S under ρ is primitive then Append G to **Primitive**.

Step 5: Return: Primitive.

The groups $G_2(q)$ for $q = 7, 11$.

Input: An integer $d = 58653, 58996, 886446$, or 885115.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle $G_2(q)$ for $q = 7$ or 11.

Step 1: Define empty lists **Primitive** and **CohortReps**.

Step 2(a): If $d = 58996$ or 58653 then define G to be the matrix representation of $G_2(7)$ in GL(7, 7) via "ChevalleyGroup("G", 2, 7)", and $V = \mathbb{F}_7^7$ to be the vector space upon which G is acting. Finally define $v := (1, 4, 0, 0, 1, 1, 2) \in V$ if $d = 58996$, or $v := (1, 5, 5, 3, 0, 4, 5) \in V$ if $d = 58653$.

Step 2(b): If $d = 886446$ or 885115 then define G to be the matrix representation of $G_2(11)$ in GL(7, 11) via "ChevalleyGroup("G", 2, 11)", and $V = \mathbb{F}_{11}^7$ to be the vector space upon which G is acting. Finally define $v := (1, 4, 9, 0, 3, 3, 4) \in V$ if $d = 886446$, or $v := (1, 1, 9, 5, 10, 6, 10) \in V$ if $d = 885115$.

Step 3: Define W to be the 1-dimensional subspace of V generated by v.
Define P to be the image of the permutation representation of G acting on the cosets of the stabilizer in G of W via "CosetImage".
Append P to **CohortReps**

Step 4: For each $P \in$ **CohortReps** construct $N_{S_d}(\mathrm{Soc}(P))$ and $Q := N/\mathrm{Soc}(P)$ with corresponding epimorphism $\rho : N \to Q$.
Define the list **Sub** of conjugacy class representatives of subgroups of Q.
For each $S \in$ **Sub** if the preimage G of S under ρ is primitive then Append G to **Primitive**.

Step 5: **Return: Primitive**.

The group $G_2(8)$.

Input: An integer $d = 130816, 131328$.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle $G_2(8)$.

Step 1: Define empty lists **Primitive** and **CohortReps**.

Step 2: Define G to be the matrix representation of $G_2(8)$ in $\mathrm{GL}(7,8)$ via "ChevalleyGroup("G", 2, 8)". Define $V = \mathbb{F}_8^7$ to be the vector space upon which G is acting. Let α be a primitive element of $\mathbb{F}_8$.

Step 3(a): If $d = 130816$ then define $v_1, \ldots, v_6 \in V$ via
$v_1 := (1,0,0,0,0,0,0)$, $v_2 := (0,1,0,0,0,0,1)$, $v_3 := (0,0,1,0,0,0,0)$, $v_4 := (0,0,0,1,0,0,\alpha^6)$, $v_5 := (0,0,0,0,1,0,\alpha^6)$, $v_6 := (0,0,0,0,0,1,\alpha^4)$.
Define W to be the 6-dimensional subspace of V generated by v_i with $1 \leq i \leq 6$.
Construct P as the image of the permutation representation arising from the action of G on the cosets of the stabilizer in G of W via "CosetImage".

Step 3(b): If $d = 131328$ then define $v_1, \ldots, v_3 \in V$ via
$v_1 := (1,0,0,\alpha^4,\alpha^3,\alpha^5,\alpha)$, $v_2 := (0,1,0,\alpha^2,\alpha^5,\alpha^4,\alpha^5)$, $v_3 := (0,0,1,\alpha^6,\alpha^5,\alpha^5,\alpha^3)$.
Define W to be the 3-dimensional subspace of V generated by v_i with $1 \leq i \leq 3$.
Construct I as the image of the permutation representation arising from the action of G on the cosets of the stabilizer in G of W via "CosetImage".
I is imprimitive of degree $262656 = 2d$.
Construct P as the image of the permutation representation arising from the action of I on one of its blocks $B =$ "MinimalPartition(I)" via "BlocksAction".

Step 3(c): Append P to **CohortReps**

Step 4: For each $P \in$ **CohortReps** construct $N_{S_d}(\mathrm{Soc}(P))$ and $Q := N/\mathrm{Soc}(P)$ with corresponding epimorphism $\rho : N \to Q$.
Define the list **Sub** of conjugacy class representatives of subgroups of Q.
For each $S \in$ **Sub** if the preimage G of S under ρ is primitive then Append G to **Primitive**.

Step 5: **Return: Primitive**.

The group $G_2(9)$.

Input: An integer $d = 266085, 265356, 664300$.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle $G_2(9)$.

Step 1: Define empty lists **CohortReps** and **Primitive**.

Step 2(a): If $d = 266085$ then define G to be a matrix representation of $G_2(9)$ in GL$(7, 9)$ via "ChevalleyGroup("G", 2, 9)" and define $V = \mathbb{F}_9^7$ to be the vector space upon which G is acting. Let α be a primitive element of $\mathbb{F}_9$.

Step 2(b): Define $v_1, \ldots, v_3 \in V$ via $v_1 := (1, 0, \alpha^2, \alpha, 0, \alpha^5, \alpha^2)$, $v_2 := (0, 0, 0, 0, 1, \alpha^5, \alpha^6)$, $v_3 := (0, 1, \alpha^5, \alpha^2, 0, 1, 2)$.
Define W to be the 3-dimensional subspace of V generated by v_i with $1 \leq i \leq 3$.
Construct I as the image of the permutation representation arising from the action of G on the cosets of the stabilizer in G of W via "CosetImage".
I is imprimitive of degree $532170 = 2d$.
Construct P as the image of the permutation representation arising from the action of I on one of its blocks $B =$ "MinimalPartition(I)" via "BlocksAction".
Then P is primitive of degree d.

Step 2(c): Append P to **CohortReps**.

Step 3(a): If $d = 265356$ then define G to be a matrix representation of $G_2(9)$ in GL$(7, 9)$ via "ChevalleyGroup("G", 2, 9)" and define $V = \mathbb{F}_9^7$ to be the vector space upon which G is acting. Let α be a primitive element of $\mathbb{F}_9$.

Step 3(b): Define $v_1, \ldots, v_6 \in V$ via $v_1 := (0, 0, 1, 0, 0, 0, \alpha)$, $v_2 := (0, 0, 0, 0, 1, 0, 2)$, $v_3 := (1, 0, 0, 0, 0, 0, \alpha)$, $v_4 := (0, 1, 0, 0, 0, 0, \alpha^6)$, $v_5 := (0, 0, 0, 1, 0, 0, \alpha^7)$, $v_6 := (0, 0, 0, 0, 0, 1, 2)$.
Define W to be the 6-dimensional subspace of V generated by v_i with $1 \leq i \leq 6$.
Construct P as the image of the permutation representation arising from the action of G on the cosets of the stabilizer in G of W via "CosetImage".
Then P is primitive of degree d.

Step 3(c): Append P to **CohortReps**.

Step 4(a): If $d = 664300$ then define A to be the image of a permutation representation of $\mathrm{Aut}(G_2(9))$ of degree 132860 via $A :=$ "AutomorphismGroupSimpleGroup("G2", 9)". Define $G := \mathrm{Soc}(A)$.

Step 4(b): Define S to be a Sylow 3-subgroup of G.
Define M to be the normalizer in A of S and P to be the image of the permutation representation of A acting on the cosets of M in A via "CosetImage".
M is a maximal subgroup of A of index d and P is the only group in its cohort.

Step 4(c): Append P to **Primitive**.

Step 5: For each $P \in$ **CohortReps**, calculate $N := N_{S_d}(\mathrm{Soc}(P))$ and the quotient $Q := N/\mathrm{Soc}(P)$, together with the epimorphism $\rho : N \to Q$. For each conjugacy class representative S of the subgroups of Q, if the preimage s of S in ρ is primitive then Append s to **Primitive**.

Step 6: **Return: Primitive**.

The groups Sz(128) and Sz(512).

Input: An integer $d = 16385$ or 262145.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle Sz(128) or Sz(512).

Step 1: Define an empty list **Primitive**.

Step 2(a): If $d = 16385$ then construct A as the image of a permutation representation of $\mathrm{Aut}(\mathrm{Sz}(128))$ via "AutomorphismGroupSimpleGroup("2B2", 128)".
This representation is of degree d and is primitive.

Step 2(b): Define $G := \mathrm{Soc}(A)$.
Here $G \cong \mathrm{Sz}(128)$ and G is primitive of degree d. Furthermore $A \cong G.7$, so these are the only groups in the cohort.

Step 2(c): Append A and G to **Primitive**.

Step 3(a): If $d = 262145$ then construct A as the image of a permutation representation of $\mathrm{Aut}(\mathrm{Sz}(512))$ via "AutomorphismGroupSimpleGroup("2B2", 512)".
This representation is of degree d and is primitive.

Step 3(b): Define $G := \mathrm{Soc}(A)$.
Then $G \cong \mathrm{Sz}(512)$ and G is primitive of degree d.

Step 3(c): Define $N := N_{S_d}(G)$ and define $Q := N/\mathrm{Soc}(N)$ with corresponding epimorphism $\rho : N \to Q$. For each conjugacy class representative S of the subgroups of Q, if the preimage P of S in ρ is primitive then Append P to **Primitive**.

Step 4: **Return: Primitive**.

The group $E_6(2)$.

Input: An integer $d = 139503$.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle $E_6(2)$.

Step 1: Define an empty list **Primitive**.

Step 3: Construct a matrix representation G, of $E_6(2)$ in $\mathrm{GL}(27, 2)$ via $G :=$"ChevalleyGroup("E", 6, 2)". Define $V := \mathbb{F}_2^{27}$ to be the vector space upon which G is acting.

Step 4: Construct the image P of the permutation representation of the action of G on the one dimensional subspace of V generated by the first basis vector via "OrbitImage".
Then P is primitive of degree d and P equals the normalizer in S_d of its socle, so P is the only group in this cohort.
Append P to **Primitive**.

Step 5: **Return: Primitive**.

The groups Co_1, Fi_{24}', and O'N.

Input: An integer $d = 98280, 122760$, or 306936.

Output: A list **Primitive**, consisting of all almost simple primitive groups of degree d with socle Co_1, Fi_{24}', or O'N.

Step 1: Define an empty list **Primitive**.

Step 2: If $d = 98280$ then construct A as the image of a permutation representation of $\mathrm{Aut}(\mathrm{Co}_1)$ via "AutomorphismGroupSimpleGroup("Co1")".

This representation is of degree d and is primitive. Furthermore $\mathrm{Aut}(\mathrm{Co}_1) = \mathrm{Co}_1$*, so this is the only group in the cohort.*
Append A to **Primitive**.

Step 3(a): If $d = 122760$ then construct A as the image of a permutation representation of Aut(O'N) via "AutomorphismGroupSimpleGroup("ON")".
Then A is of degree $2d$.

Step 3(b): Define $G := \mathrm{Soc}(A)$.
Then $G \cong$ O'N and G is intransitive of degree $2d$, with 2 orbits.

Step 3(c): Define P to be the image of the permutation representation of G acting on one of its orbits via "OrbitImage".
Then P is primitive of degree d and P equals the normalizer in S_d of its socle, so P is the only group in this cohort.

Step 3(d): Append P to **Primitive**.

Step 4(a): If $d = 306939$ then construct A as the image of a permutation representation of $\mathrm{Aut}(\mathrm{Fi}_{24}')$ via "AutomorphismGroupSimpleGroup("Fi24")".
This representation is of degree d and is primitive.

Step 4(b): Define $G := \mathrm{Soc}(A)$.
Then $G \cong \mathrm{Fi}_{24}'$ and G is primitive of degree d. Furthermore $A \cong G.2$ and so the only possibilities for primitive groups in this cohort are A and G.

Step 4(c): Append A and G to **Primitive**.

Step 5: Return: Primitive.

4.2. **Diagonal type groups.** The procedure given in Section 3.3 is directly generalisable for $d \leq 1000000$. We are only required to determine for which d we use the procedure, and the corresponding simple group to input.

The degree of a primitive group of diagonal type is $|T|^{m-1}$ for some non-abelian simple group T. The smallest non-abelian simple group is A_5 and $|A_5|^3 = 216000 < 1000000 < |A_5|^4 = 12960000$. Thus $m \leq 4$. We therefore need to consider simple groups such that $|T| \leq 1000000$ for $m = 2$, $|T| \leq 1000$ for $m = 3$, and $|T| \leq 100$ for $m = 4$.

We therefore check whether there exists a possible T and m such that $|T|^{m-1} = d$. If there is then we input T into the diagonal groups procedure.

We display the simple groups T and the integers m, corresponding to primitive groups of degree $|T|^{m-1} \leq 1000000$ in Table 6.

Simple Group T	Conditions	Possible m
A_5		2,3,4
A_6		$2, 3$
A_n	$7 \leq n \leq 9$	2
$\mathrm{L}_2(q)$	$7 \leq q \leq 11$	$2, 3$
$\mathrm{L}_2(q)$	$13 \leq q \leq 125$	2
$\mathrm{L}_3(q)$	$3 \leq q \leq 5$	2
$\mathrm{U}_3(q)$	$3 \leq q \leq 5$	2
$\mathrm{S}_4(q)$	$3 \leq q \leq 4$	2
$\mathrm{Sz}(8)$		2
M_n	$n = 11, 12, 22$	2
J_n	$n = 1, 2$	2

TABLE 6. Simple groups T corresponding to diagonal type groups with socle T^m and minimal degree at most 1000000.

.

The Diagonal Type Groups

Input: An integer $d \leq 1000000$.

Output: A list **PrimitiveGroups**, consisting of all diagonal type primitive groups of degree $d \leq 1000000$.

Step 1: Define an empty list **PrimitiveGroups**. Check whether $d = |T|^{m-1}$ for any simple group T and $2 \leq m \leq 4$.
Use Table 6 to determine the possibilities for T and m.

Step 2: If there exists some simple group T and $2 \leq m \leq 4$ such that $d = |T|^{m-1}$. Then

Step 2(a): for each such T, input T into the diagonal type groups procedure (given in Section 3.3), with bounds of d.
This returns a list **Primitive**.
For each group P in **Primitive**, Append P to **PrimitiveGroups**.

Step 2(b): **Repeat Step 2** until all groups T have been considered.

Step 3: **Return: PrimitiveGroups**.

4.3. **Product type groups.** The procedure given in Section 3.4 is directly generalisable for $d \leq 1000000$. We are required only to determine for which d we use the procedure, and which groups to input for those d.

The degree of any primitive group of product type is $n^{m/l}$, where n is the degree of an almost simple, or diagonal type group, and $m/l \geq 2$. Therefore $n \leq 1000$. Since $n \geq 5$ we also have that $m/l \leq 8$.

For an input $d \leq 1000000$ we produce lists of integers $d_1, \ldots, d_7$ such that ${d_i}^{i+1} = d$. Then as all primitive groups of degree up to 1000 have been classified, we can find any corresponding almost simple, or diagonal type groups.

The Product Type Groups

Input: An integer $d \leq 1000000$.

Output: A list **PrimitiveGroups**, consisting of all product type primitive groups of degree $d \leq 1000000$.

Step 1: For $1 \leq i \leq 7$ define $d_i := \lfloor d^{1/(i+1)} \rfloor$ and define the corresponding lists P_i consisting of the largest cohort representatives from each cohort of primitive almost simple or diagonal type groups of degree d_i. Define an empty list **PrimitiveGroups**.

Step 2: For each $1 \leq i \leq 7$,

Step 2(a): for each group P in P_i,

Step 2(a)(i): if $\deg(P)^i = d$ then input P into the product type groups procedure.
This returns a list **Primitive**.
For each group G in **Primitive**, Append G to **PrimitiveGroups**.

Step 2(a)(ii): If $\deg(P)^i \neq d$ then **Continue** P.

Step 3: Return: PrimitiveGroups.

5. Classification of Quasiprimitive Groups of Degree $d \leq 3600$

In this section we classify the quasiprimitive permutation groups of degree $d \leq 3600$ up to permutation isomorphism. This will rely heavily upon an "O'Nan-Scott" type theorem given by C. Praeger in 1993 [33, Theorem 1].

Recall Definition 1.5, a transitive permutation group is *quasiprimitive* if all of its non-trivial normal subgroups are transitive.

Theorem 5.1 (Praeger,'93)**.** *Let $G \leq \mathrm{Sym}(\Omega)$ be a finite quasiprimitive permutation group with $|\Omega| = d$. Let $H \leq G$ be the socle of G. Then $H \cong T^m$ for some finite simple group T, $m \geq 1$ and G is permutation isomorphic to a group of exactly one of the following types.*

- **I** *(Affine Type) Here $T \cong C_p$ for some prime p, and H is the unique minimal normal subgroup of G and is regular on Ω of degree $d = p^m$. The set Ω can be identified with $H \cong C_p^m$ so that G is a subgroup of the affine group $\mathrm{AGL}(m,p)$ with H the translation group and for $\alpha \in \Omega$ the stabilizer $G_\alpha = G \cap \mathrm{GL}(m,p)$ is irreducible on H. Moreover G is primitive on Ω.*
- **II** *(Almost Simple Type) Here $m = 1$ and T is a non-abelian simple group. $T \leq G \leq \mathrm{Aut}(T)$ and for $\alpha \in \Omega$, $G = TG_\alpha$.*
- **III** *In this case $H \cong T^m$ with $m \geq 2$ and T is a non-abelian simple group. We split this case into three types.*

III(a) *(Simple Diagonal Type) Define*

$$W := \{(a_1, \ldots, a_m) \cdot \pi \mid a_i \in \mathrm{Aut}(T), \pi \in S_m, a_i \equiv a_j \ \mathrm{Mod}(\mathrm{Inn}(T)) \text{ for all } i,j\}$$

where $\pi \in S_m$ permutes the components a_i in the natural way.

Then W is a group with socle $H \cong T^m$ and W is a not necessarily split extension of H by $\mathrm{Out}(T) \times S_m$, i.e. we have $W = H.(\mathrm{Out}(T) \times S_m)$.

Define an action of W on Ω by setting, for any $\alpha \in \Omega$,

$$W_\alpha = \{(a, \ldots, a) \cdot \pi \mid a \in \mathrm{Aut}(T), \pi \in S_m\}.$$

Thus $W_\alpha \cong \mathrm{Aut}(T) \times S_m$, $H_\alpha \cong T$, and $d = |T|^{m-1}$.

For $1 \leq i \leq m$ define T_i to be the subgroup of H consisting of the m-tuples with 1 in all but the i^{th} component, so that $T_i \cong T$ and $H \cong T_1 \times \cdots \times T_m$.

Put $\Gamma := \{T_1, \ldots, T_m\}$, so that W acts on Γ.

We say that a subgroup G of W is of type **III(a)** *if $H \leq G$ and one of the following holds:*

(i) $m = 2$ and and G acts trivially on Γ.

(ii) G acts transitively on Γ,

Let P be the permutation group G^Γ. We then have that $G_\alpha \leq \mathrm{Aut}(T) \times P$, and $G \leq H \cdot (\mathrm{Out}(T) \times P)$.

Moreover in case (i) G has two minimal normal subgroups T_1 and T_2, both regular on Ω, and G is primitive *on Ω. In case (ii) H is the unique minimal normal subgroup of G and G is* primitive *on Ω if and only if P is* primitive *on Γ.*

III(b) *(Product Type) Let U be a quasiprimitive permutation group on a set Γ, of type* **II** *or* **III(a)**. *For $k > 1$, let $W = U \wr S_k$, and take W to act on $\Delta = \Gamma^k$ in its natural product action. Then for $\gamma \in \Gamma$ and $\delta = (\gamma, \ldots, \gamma) \in \Delta$ we have $W_\delta = U_\gamma \wr S_k$ and $|\Delta| = |\Gamma|^k$. If K is the socle of U then the socle H of W is K^k.*

W acts naturally on the k factors in K^k, and we say that a subgroup G of W is of type **III(b)** *if $H \leq G$, G acts transitively on these k factors and one of the following holds:*

- *(i) U is of type* **II**, *$K \cong T$, $m = k$ and H is the unique minimal normal subgroup of G; further Δ is a G-invariant partition of Ω and, for α in the part $\delta \in \Delta$, $H_\delta = T_\gamma^m < H$ and for some nontrivial normal subgroup N of T_γ, H_α is a subdirect product of N^m, that is H_α projects surjectively onto each of the direct factors N.*
- *(ii) H is of type* **III(a)**, *$\Omega = \Delta$, $K \cong T^{m/k}$ and G and U both have l minimal normal subgroups where $l \leq 2$; if $l = 2$ then each of the two minimal normal subgroups of G is regular on Ω.*

III(c) *(Twisted Wreath Type) Here G is a twisted wreath product $T twr_\phi P$, defined as follows.*

Let P have a transitive action on $\{1, \ldots, m\}$ and let Q be the stabilizer P_1 of the point 1 in this action. We suppose that there is a homomorphism $\phi : Q \to \mathrm{Aut}(T)$ such that $\bigcap_{x \in P} \phi^{-1}(\mathrm{Inn}(T))^x = \{1\}$.

Define

$$H = \{f : P \to T \mid f(pq) = f(p)^{\phi(q)} \text{ for all } p \in P, q \in Q\}.$$

Then H is a group under pointwise multiplication, and $H \cong T^m$. Let P act on H by

$$f^p(x) = f(px) \text{ for } p, x \in P.$$

Define $T twr_\phi P$ to be the semidirect product of H by P with this action. Define an action of G on Ω by setting $G_\alpha = P$ for some $\alpha \in \Omega$. We say that G is of type **III(c)**. *Here $d = |T^m|$ and H is the unique minimal normal subgroup of G and H acts regularly on Ω.*

Remark 5.2. A quasiprimitive group is of type **I** (affine type) if and only if it is a primitive group of affine type. These groups are already classified to degree $8191 > 3600$ so we do not discuss these further.

5.1. **Type II: Almost simple groups.** In this section we will classify the quasiprimitive groups of type **II** of degree $d \leq 3600$. This will require the use of the Classification of Finite Simple Groups, see Theorem 1.23.

Let G be an almost simple group. As in Section 3.2, we denote by $P(G)$ the minimal integer d such that G has a faithful primitive permutation action of degree d. We denote by $Q(G)$ the minimal integer d such that G has a faithful, imprimitive, quasiprimitive permutation action of degree d. We note that $Q(G) > P(G)$ for all G. Therefore we may restate Lemma 3.27 as follows:

Lemma 5.3. *Let G be an almost simple group with socle T. Then $Q(G) > P(G) \geq P(T)$.*

A Quasiprimitive Test

Input: A permutation group G.
Output: **true** if G is quasiprimitive or **false** if G is not quasiprimitive.

Step 1: Construct the list **Normal** of conjugacy class representative of the normal subgroups of G.

Step 2: For each $N \in$ **Normal**, if N is intransitive then **Return: false**.

Step 4: Return: true.

5.1.1. *Alternating groups.* In this section we classify the quasiprimitive groups of type **II** of degree $d \leq 3600$, with alternating socles.

We recall Definition 3.29, for $d > 4$ the groups A_d and S_d in their natural action form a single cohort of size 2, of *improper* primitive groups. We do not consider these further.

Proposition 5.4. *If $G = A_n$ or S_n has a faithful quasiprimitive action, other than the natural action, of degree $d \leq 3600$, then $n \leq 85$. If the stabilizer G_α in this action acts transitively on $\{1, \ldots, n\}$ then $n \leq 14$.*

Proof. Let T be the socle of G. By Lemma 5.3, we have that $Q(G) > P(G) \geq P(T)$. Therefore, as in Proposition 3.31, we can consider simple groups and primitive groups to find this upper bound for n.

The proof may now be obtained by following the same argument as in the proof of Proposition 3.31 but with $d \leq 3600$. □

Type **II** Groups

Input: The automorphism group A of a non-abelian simple group T such that $P(T) \leq 3600$.

Output: A list **Quasiprimitive** consisting of all type **II** quasiprimitive groups with socle T.

Step 1: Construct an empty list **Quasiprimitive**.

Step 2: Define a list **Groups** consisting of conjugacy class representatives of all subgroups of A containing $\mathrm{Soc}(A) \cong T$.

Step 3: For each $G \in$ **Groups** create a list **Sub** consisting of conjugacy class representatives in A of the subgroups of G with index at most 3600. Create an empty list **Candidates**.

Step 3(a): For each $S \in$ **Sub** define C to be the image of the permutation representation of G acting on the cosets of S in G via "CosetImage". Append C to **Candidates**.

Step 3(b): For each C in **Candidates**, if C is quasiprimitive *(check via above quasiprimitive test)* then Append C to **Quasiprimitive**.

Step 3: Return: Quasiprimitive.

Theorem 5.5. *Let G be a quasiprimitive almost simple group of degree $d \leq 3600$ with socle A_n. Then G appears in Table 18.*

Proof. We use Proposition 5.4 to determine the possibilities for quasiprimitive almost simple groups with alternating socles.
For each alternating group A_n described in Proposition 5.4, we input $\mathrm{Aut}(A_n)$ into the above procedure. □

5.1.2. *Classical groups.* In this section we classify the quasiprimitive groups of type **II** of degree $d \leq 3600$, with classical socles.

Recall Section 1.2, and as in Section 3.2.2, we denote a simple classical group by $\mathrm{Cl}_n(q)$.

In the following proposition we find the maximum values of n and q (where q is a prime power) such that $P(\mathrm{Cl}_n(q)) \leq 3600$

Proposition 5.6. *Let G be an almost simple group with a classical socle, such that there exists a faithful quasiprimitive permutation action of G of degree less than or equal to* 3600*. Then the socle of G appears in Table 7.*

Proof. By Lemma 5.3 we only need to consider the *simple* classical groups.

The formulae for $P(H)$ are given in [28, p.175, Table 5.2A] and corrected and extended in [20, Table 4]. They are all monotonically increasing in each variable.

We may now complete the proof by using the same method as in the proof of Proposition 3.33 but for degree 3600, which we do not repeat here. □

Group	n	q
$\mathrm{L}_n(q)$	$n = 2$	$7 \leq q \leq 3593$, $q \neq 9$
	$n = 3$	$3 \leq q \leq 59$
	$n = 4$	$3 \leq q \leq 13$
	$n = 5$	$2 \leq q \leq 7$
	$n = 6$	$2 \leq q \leq 4$
	$7 \leq n \leq 8$	$2 \leq q \leq 3$
	$9 \leq n \leq 11$	$q = 2$
$\mathrm{S}_{2m}(q)$	$m = 2$	$3 \leq q \leq 13$
	$m = 3$	$2 \leq q \leq 4$
	$m = 4$	$2 \leq q \leq 3$
	$5 \leq m \leq 6$	$q = 2$
$\mathrm{U}_n(q)$	$n = 3$	$3 \leq q \leq 13$
	$n = 4$	$3 \leq q \leq 7$
	$n = 5$	$2 \leq q \leq 3$
	$6 \leq n \leq 7$	$q = 2$
$\mathrm{P}\Omega_{2m+1}(q)$	$m = 3$	$q = 3$
$\mathrm{P}\Omega^+_{2m}(q)$	$m = 4$	$2 \leq q \leq 3$
	$5 \leq m \leq 6$	$q = 2$
$\mathrm{P}\Omega^-_{2m}(q)$	$m = 4$	$2 \leq q \leq 3$
	$5 \leq m \leq 6$	$q = 2$

TABLE 7. Classical socles of almost simple groups with minimal degree at most 3600.

Theorem 5.7. *The quasiprimitive almost simple groups of degree $d \leq$ 3600 with classical socles are displayed in Table 18.*

Proof. We input the automorphism group of each of the simple classical groups which appear in Table 7 into the procedure for type **II** groups. □

5.1.3. *Exceptional groups of Lie type.* In this section we classify the quasiprimitive groups of type **II** of degree $d \leq 3600$ with exceptional socles.

Proposition 5.8. *Let G be an almost simple group with a faithful quasiprimitive permutation action of degree d where $d \leq 3600$ such that $\mathrm{Soc}(G)$ is an exceptional group. Suppose that $\mathrm{Soc}(G)$ is not an alternating or classical group. Then $\mathrm{Soc}(G)$ is one of $G_2(3)$, $G_2(4)$, $\mathrm{Sz}(8)$, $\mathrm{Sz}(32)$, ${}^3D_4(2)$, or ${}^2F_4(2)'$.*

Proof. By Lemma 5.3, we only need to consider the *simple* exceptional groups.

We then follow the same arguments as Proposition 3.40 but for $d \leq 3600$, which we do not repeat here. □

Theorem 5.9. *The quasiprimitive almost simple groups of degree $d \leq 3600$ with exceptional socles are displayed in Table 19.*

Proof. We input the automorphism group of each of the simple exceptional groups which appear in Proposition 5.8 into the procedure for type **II** groups. □

5.1.4. *Sporadic simple groups.* In this section we classify the quasiprimitive groups of type **II** of degree $d \leq 3600$ with sporadic socles.

The list of maximal subgroups of the sporadic groups is complete with the exception of the monster group M. However M has no transitive permutation representation of degree ≤ 3600. The sporadic groups which have primitive, and so quasiprimitive, permutation representations of degree $d \leq 3600$ are

$$M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, \mathrm{HS}, J_2, \mathrm{Co}_2, \mathrm{Co}_3, \mathrm{McL}, \mathrm{Suz}, \mathrm{He}, \mathrm{Fi}_{22}, \text{and } J_1.$$

Theorem 5.10. *The quasiprimitive almost simple groups of degree $d \leq 3600$ with sporadic socles are displayed in Table 19.*

Proof. We input the automorphism group of each of the sporadic simple groups described above into the procedure for type **II** groups. □

5.2. **Type III.** In this section we classify the quasiprimitive groups of degree $d \leq 3600$ which arise as type **III** groups in Theorem 5.1.

We note that any quasiprimitive group G of type **III** is permutation isomorphic to a subgroup of $W := \mathrm{Aut}(T) \wr S_m$ for some non-abelian simple group T and $m > 1$. We identify the group G with the corresponding subgroup of W. In this case $H := \mathrm{Soc}(W) \cong T^m$ is a subgroup of G.

The image of G in S_m under the projection map $p : W \to S_m$, defined by $(a_1, \ldots, a_m)\pi \mapsto \pi$, is either transitive in cases **III(b)(i)** and **III(c)**, or has two orbits of equal length in cases **III(a)** and **III(b)(ii)**.

As in Section 3.3, for $1 \leq i \leq m$ we define T_i to be the subgroup of H consisting of the m-tuples with 1 in all but the i^{th} component, so that $T_i \cong T$ and $H \cong T_1 \times \cdots \times T_m$.

By Theorem 3.43 (iv), $T_1, \ldots, T_m$ are the only minimal normal subgroups of H.

The following appears in [33, Proof of Theorem 1].

Lemma 5.11. *Let $G \leq \mathrm{Sym}(\Omega)$ be a quasiprimitive group of type* **III**. *Then G is permutation isomorphic to a subgroup of $\mathrm{Aut}(T) \wr S_m$, the socle of G is $H = \{(a_1, \ldots, a_m)1 \mid a_i \in \mathrm{Inn}(T), 1 \leq i \leq m\} \cong T^m$, and the set of direct factors of H is $\{T_1, \ldots, T_m\}$ (as described above). For $1 \leq i \leq m$ define π_i to be the projection map of H onto T_i via $((a_1, \ldots, a_m)1)\pi_i = (1, \ldots, 1, a_i, 1, \ldots, 1)1$. Fix $\alpha \in \Omega$.*

(i) If $(H_\alpha)\pi_i = T_i$ for some $1 \leq i \leq m$ then G is of type **III(a)** *or* **III(b)(ii)**.

(ii) If $(H_\alpha)\pi_i$ is a proper subgroup of T_i for every $1 \leq i \leq m$ then H is a minimal normal subgroup of G and $G = HG_\alpha$.

(a) If $(H_\alpha)\pi_1 = 1$ then $H_\alpha = 1$ and G is of type **III(c)**.

(b) If $(H_\alpha)\pi_1 < T_1$ and $\pi_1(H_\alpha) \neq 1$ then G is of type **III(b)(i)**.

We consider each of the type **III** groups in turn.

5.2.1. *Type* **III(a)**: *Diagonal type groups.* This is almost exactly the description of the primitive groups of diagonal type given in Section 3.3. There is the following difference. If G is a primitive group of diagonal type with $m > 2$ then G must act *primitively* on the set of minimal normal subgroups of $\mathrm{Soc}(G)$ by conjugation. However if G is a quasiprimitive group of type **III(a)** with $m > 2$, then G must act *transitively*, but not necessarily primitively, on the set of minimal normal subgroups of $\mathrm{Soc}(G)$ by conjugation.

Therefore the method we used to produce the primitive groups of diagonal type may be used to construct the quasiprimitive groups of type **III(a)** with only the following minor change. We use the procedure described in Section 3.3, however in **Step 2(e)**, instead of constructing the preimages of all primitive groups, we construct the preimages of all transitive groups.

The degree of any quasiprimitive group of type **III(a)**, is $|T|^{m-1}$ where T is a non-abelian simple group and $m \geq 2$. Thus the options for T are:

$$A_5, A_6, A_7, \mathrm{L}_2(7), \mathrm{L}_2(8), \mathrm{L}_2(11), \mathrm{L}_2(13), \mathrm{L}_2(17), \text{and } \mathrm{L}_2(19)$$

with $m = 2$ and

$$A_5$$

with $m = 3$.

Theorem 5.12. *Let G be a quasiprimitive group of type* **III**(a) *such that the degree of G is at most 3600. Then G is described on Table 20.*

Proof. In general we input the groups T, described above, into the procedure described below. Let G be a quasiprimitive group of degree d of type **III(a)**.

If $m = 2$ then by Theorem 5.1, G is primitive. Therefore we only need to consider the case $T = A_5$ and $m = 3$.
By Theorem 5.1, if $m > 2$ then G acts transitively on the set of minimal normal subgroups of $\mathrm{Soc}(G) = T$ by conjugation. Furthermore G is primitive if and only if G acts primitively on the set of minimal normal subgroups of T by conjugation. By Lemma 1.16, every transitive group of prime degree is primitive. Thus every quasiprimitive group of degree $d \leq 3600$, of type **III(a)** is primitive. □

We give the general method for finding type **III(a)** groups of degree d below.

Type **III(a)** Groups

Input: A non-abelian simple group T such that $|T|^{m-1} = d$ for some $m \geq 2$.

Output: A list **Quasiprimitive** consisting of all diagonal type quasiprimitive groups with socle T^m.

Step 1: Construct an empty list **Quasiprimitive**.

Step 2(a): For each $m \geq 2$ such that $|T|^{m-1} = d$ follow Steps **2(a)**, ..., **2(d)** in the procedure in Section 3.3 with the bound of $|T|^{m-1} = d$ in **Step 2**.

Step 2(b): Follow **Step 2(e)** in the procedure in Section 3.3 with the following change: if the preimage of s under ρ acts *transitively* then Append the preimage of s under ρ to **Quasiprimitive**.

Step 3: Return: Quasiprimitive.

Example 5.13. The lowest possible degree for an imprimitive, quasiprimitive group of type **III(a)** is $|T|^{m-1} = 60^3 = 216000$. This is because we require $m \geq 4$ (so that G can have a transitive but imprimitive action on the set of minimal normal subgroups of $\mathrm{Soc}(G)$) and T must be a non-abelian simple group.

Let $T = A_5$ and input T into the above procedure with $m = 4$ and degree range $|T|^{4-1} = 216000$. This produces 5 primitive groups and 11 imprimitive but quasiprimitive groups of type **III(a)**. All of these groups have socle isomorphic to ${A_5}^4$.

5.2.2. *Type* **III(b)**: *Product type groups.* The description of groups of this type differs significantly from the corresponding class in the O'Nan-Scott Theorem (Product

type), see Section 3.4.

By Theorem 5.1, any group G of type **III(b)** is permutation isomorphic to a subgroup of the product action wreath product $W := U \wr S_k$ acting on a set Ω, where U is a quasiprimitive permutation group of type **II** or **III(a)**. We identify G with this subgroup. We then also have that $\mathrm{Soc}(G) = \mathrm{Soc}(W) \leq G$ and G acts transitively on the k factors of $\mathrm{Soc}(W)$.

In case **III(b)(i)**, U is a quasiprimitive group of type **II** and so $m = k$ and there exists a non-abelian simple group T such that $T \leq U \leq \mathrm{Aut}(T)$. We observe that unlike in Section 3.4, the degree d of G is not necessarily equal to n^m where n is the degree of U. However d is bounded below by n^m.

Hence by Lemma 5.3 and as $\deg(U) \geq 5$, we must have one of the following:

- $m = 2$ and T has a primitive action of degree at most 60,
- $m = 3$ and T has a primitive action of degree at most 15,
- $m = 4$ and T has a primitive action of degree at most 7,
- $m = 5$ and T has a primitive action of degree at most 5.

We display the possible non-abelian simple groups and their corresponding m's on Table 8.

Simple Group T	Conditions	Possible m
A_5		2, 3, 4, 5
A_n	$6 \leq n \leq 7$	$2, 3, 4$
A_n	$8 \leq n \leq 15$	$2, 3$
A_n	$16 \leq n \leq 60$	2
$\mathrm{L}_2(7)$		2, 3, 4
$\mathrm{L}_2(q)$	$q = 8, 11, 13$	2, 3
$\mathrm{L}_2(q)$	$16 \leq q \leq 59$	2
$\mathrm{L}_3(3)$		2, 3
$\mathrm{L}_3(q)$	$4 \leq q \leq 7$	2
$\mathrm{L}_4(3)$		2
$\mathrm{L}_5(2)$		2
$\mathrm{U}_3(3)$		2
$\mathrm{U}_4(2)$		2
$\mathrm{S}_6(2)$		2
M_n	$n = 11, 12$	2, 3
M_n	$n = 22, 23, 24$	2

TABLE 8. Simple groups T corresponding to groups of type **III(b)(i)** with socle T^m, and minimal degree at most 3600.

All quasiprimitive groups G of type **III(b)(i)** and of degree $d \leq 3600$ are therefore subgroups of $W := \mathrm{Aut}(T) \wr S_m$ for some T, m described in Table 8.

As noted above, any quasiprimitive group $G \leq W$ of type **III(b)(i)** has the following properties:

$$\mathrm{Soc}(W) \leq G \text{ and } G \text{ acts transitively on the } m \text{ factors of } \mathrm{Soc}(W). \qquad (\star)$$

We may therefore search directly for conjugacy classes of subgroups of W with these properties, $(\star)$, and test every transitive action of degree $d \leq 3600$ of conjugacy class representatives for quasiprimitivity.

Unfortunately it would be impractical to consider all of these transitive actions. We recall that by Lemma 1.18, any transitive action of a group corresponds to the action of right multiplication on the set of cosets of a subgroup S of that group and a point stabilizer in G of this action is S.

Let G be a subgroup of W with the properties $(\star)$ and let H be the socle of G, so $H = \mathrm{Soc}(W)$. Let S be a subgroup of G such that the action of G on the set of cosets of S in G corresponds to a quasiprimitive action of type **III(b)(i)** on a set Ω, of degree $d \leq 3600$. Then there exists $\alpha \in \Omega$ such that $S = G_\alpha$ and $|G : S| \leq 3600$. By Lemma 5.11 (ii), $H_\alpha = S \cap H$ is non-trivial and $G = HS$. Furthermore by Lemma 5.11 (ii)(b), H_α does not project onto T_1 under π_1.

We may therefore refine the list of subgroups S of G to a more manageable number by removing any without these properties described above. In particular we require S such that, $G = \mathrm{Soc}(W)S$, $S \cap \mathrm{Soc}(W) \neq \{1\}$, and $(S \cap \mathrm{Soc}(W))\pi_1 \neq T_1$.

We may then produce all transitive groups corresponding to the action of G by right multiplication on the set of cosets of S and test them for quasiprimitivity, via the quasiprimitive test. By applying this method to all subgroups G of W with the properties $(\star)$, we find all possible quasiprimitive groups of type **III(b)(i)** with socle T^m.

We are not currently attempting to determine exactly which type **II** quasiprimitive group U is. It is unclear from the statement of Theorem 5.1 whether U is uniquely determined by the group G. We do however know the socle T of U.

Type **III(b)(i)** Groups

Input: An integer $m > 1$ and a non-abelian simple group T such that T has a faithful primitive action of degree d where $d^m \leq 3600$.
Described in Table 8.

Output: A list **Quasiprimitive** consisting of all type **III(b)(i)** quasiprimitive groups with socle isomophic to T^m.

Step 1: Construct empty lists **Quasiprimitive** and **Candidates**.

Step 2: Define $W := \mathrm{Aut}(T) \wr S_m$ and the projection map $p : W \to S_m$ given by $(a_1, \ldots, a_m)\pi \mapsto \pi$.

Step 3: Define $Q := W/\mathrm{Soc}(W)$ with corresponding epimorphism $\rho : W \to Q$. For each conjugacy class representative S of the subgroups of Q, if the image under p, of the preimage G of S under ρ acts transitively then Append G to **Candidates**.
These are representatives of the subgroups of W which contain $\mathrm{Soc}(W)$ *and act transitively on the factors of* $\mathrm{Soc}(W)$.

Step 4: For each $G \in$ **Candidates:**

Step 4(a): Define **Sub** to be a list of conjugacy class representatives of the subgroups of G of index at most 3600.

Step 4(b): For each $S \in$ **Sub**: if $S \cap \mathrm{Soc}(W)$ is trivial or if $\langle S, \mathrm{Soc}(W)\rangle \neq G$ or if S projects onto the factors of $\mathrm{Soc}(W)$ then **Remove:** S.

Step 4(c): Define $N := N_W(G)$. Define **ConjReps** to be a list of conjugacy class representatives of the groups in **Sub** under N.

Step 4(d): For each $C \in$ **ConjReps**, Append the image of the permutation representation of G acting on the cosets of C in G, to **Quasiprimitive**.

Step 5: Return: Quasiprimitive.

In case **III(b)(ii)**, U is a quasiprimitive group of type **III(a)** and so the degree of U is $n := |T|^{m-1}$ for some $m \geq 2$.

By Theorem 5.1, the degree of a quasiprimitive group of type **III(b)(ii)** is $n^k = |T|^{(m-1)k}$. As $k \geq 2$ and T is a non-abelian simple group, the only possibilities are $k = 2$ and U is a type **III(a)** group with socle ${A_5}^2$, of degree 60.

The largest group in this cohort is $P := {A_5}^2.2^2$. We let $W := P \wr S_2$ with the product action.

In this case the properties $(\star)$ must still hold and so we consider all subgroups G of W of index 3600 such that $\mathrm{Soc}(W) \leq G$ and G acts transitively on the direct factors

of Soc(W). We then directly check each of these subgroups for quasiprimitivity. Any quasiprimitive subgroup found is of type **III(b)(ii)**.

Type **III(b)(ii)** Groups

Input: The diagonal type primitive group $P = {A_5}^2.2^2$ of degree 60.
The largest diagonal type primitive group of degree 60.

Output: A list **Quasiprimitive** consisting of all type **III(b)(ii)** quasiprimitive groups with socle isomophic to $({A_5}^2)^2$.

Step 1: Construct an empty list **Quasiprimitive**.

Step 2: Construct the product action wreath product $W = P \wr S_2$ via "PrimitiveWreathProduct".
Construct the quotient $Q = W/\mathrm{Soc}(W)$, and define ρ to be the corresponding epimorphism $W \to Q$.

Step 3: Define a list **Sub** of conjugacy class representatives of the subgroups of Q.

Step 4: For each $S \in$ **Sub** if the preimage G, of S under ρ is quasiprimitive then Append G to **Quasiprimitive**.

Step 5: **Return: Quasiprimitive**.

Theorem 5.14. *Let G be a quasiprimitive group of type* **III(b)** *such that the degree of G is at most* 3600. *Then G is described in Tables 21, 22, or 23.*

Proof. We input all possible non-abelian simple groups T and integers $k \geq 2$ such that T has a faithful primitive action of degree d, where $d^k \leq 3600$, into the above procedures for type **III(b)(i)** and **III(b)(ii)** groups. This returns all quasiprimitive groups of type **III(b)(i)** and **III(b)(ii)**. □

5.2.3. *Type* **III(c)**: *Twisted wreath type groups.* This case has the most significant changes from the corresponding class in the O'Nan-Scott Theorem 1.11. These changes are large enough that the minimal degree of a primitive group of twisted wreath (regular non-abelian) type is 60^6 whereas the minimal degree of a quasiprimitive group of type **III(c)** is 3600.

By Theorem 5.1, degree of a quasiprimitive group of type **III(c)** is $d = |T|^m$ where T is a non-abelian simple group and $m \geq 2$. Hence the only options for $d \leq 3600$ are $T = A_5$, $m = 2$, and $d = 3600$.

We consider $W := \mathrm{Aut}(A_5) \wr S_2$. Then any quasiprimitive group G of type **III(c)** of degree $d \leq 3600$ may be identified with a subgroup of W acting on a set Ω of size d. Furthermore $H := \mathrm{Soc}(W) = \mathrm{Soc}(G)$.

By Lemma 5.11, for any $\alpha \in \Omega$ we have that $H_\alpha = 1$. We therefore find all subgroups of W containing H, of which there are 8 up to conjugacy. For each of these groups we find conjugacy class representatives of all of the subgroups of index 3600. These are the point stabilizers of transitive actions of degree 3600. As $H_\alpha = 1$ we require that each of these representatives has trivial intersection with H.

Type **III(c)** Groups

Input: An integer $m > 1$ and a non-abelian simple group T such that $|T|^m \leq 3600$.
So $m = 2$ *and* $T = A_5$.

Output: A list **Quasiprimitive** consisting of all type **III(c)** quasiprimitive groups with socle isomophic to T^m.

Step 1: Construct empty lists **Quasiprimitive** and **Candidates**.

Step 2: Define $W := \mathrm{Aut}(T) \wr S_m$.

Step 3: Define $X := W/\mathrm{Soc}(W)$ with corresponding epimorphism $\rho : W \to X$. For each conjugacy class representative S of the subgroups of X, Append the preimage G of S under ρ to **Candidates**.
These are representatives of the subgroups of W *which contain* $\mathrm{Soc}(W)$.

Step 4: For each $G \in$ **Candidates:**

Step 4(a): Define **Sub** to be a list of conjugacy class representatives of all subgroups of G of index at most 3600. Define an empty list **TrivialSubs**.

Step 4(b): For each $S \in$ **Sub** if $S \cap \mathrm{Soc}(W)$ is trivial then Append S to **TrivialSubs**.

Step 4(c): For each $S \in$ **TrivialSubs**, if the image C of the permutation representation of G acting on the cosets of S in G is quasiprimitive then Append C to **Quasiprimitive**.

Step 5: Return: Quasiprimitive.

Theorem 5.15. *The quasiprimitive groups of type* **III(c)** *of degree* $d \leq 3600$ *appear on Table 24.*

Proof. We follow the above procedure with $T = A_5$ and $m = 2$. This returns 5 quasiprimitive groups of type **III(c)** with socle ${A_5}^2$. □

6. Tables

In this section we give the tables of the primitive permutation groups of degree $4096 \leq d < 8192$, the quasiprimitive permutation groups of degree $d \leq 3600$, and some lookup tables used in Section 4.1. Recall that we take p to always be prime, q to always be a prime power, and we always consider n to be a positive integer. The dihedral group of order $2n$ will be denoted by D_{2n} and we denote by $[n]$ a soluble group of order n. We also recall the notation for simple groups given in Section 1.2.

6.1. **The primitive groups of degree** $4096 \leq d < 8192$**.** The table for the groups of affine type (Table 9) lists the number of soluble and insoluble primitive groups of degree p^k for $k > 1$. We omit the number of primitive subgroups of $\mathrm{AGL}(1, p) \cong p : (p-1)$ as this is equal to the number of divisors of $p - 1$.

The tables for the almost simple primitive groups (Tables 10 – 15) give the smallest group G in the cohort. In the cases where there are multiple smallest groups in the cohort, one group is given and we indicate the number l of smallest groups by (l). These tables also list the degree of G (and the other groups in the cohort), the number of groups in the cohort, the structure of the normalizer N of G in S_d in terms of the socle H of G, and the structure of a point stabilizer of G.

The table for the primitive groups of diagonal type (Table 16) lists the smallest group in the cohort, the degree of the groups in the cohort, and the number of groups in the cohort. The table for the primitive groups of product type (Table 17) lists the structure of the socle of the groups in the cohort, the degree of the groups in the cohort, and the number of groups in the cohort.

p^k	Soluble	Insoluble	Total
67^2	118	8	126
71^2	192	12	204
73^2	261	12	273
79^2	166	12	178
83^2	82	4	86
89^2	226	14	240
17^3	66	19	85
19^3	185	31	216
3^8	7778	1250	9028
2^{12}	934	457	1391

Table 9. Primitive groups of affine type.

Smallest Cohort Rep. G	Conditions	Degree	Stabilizer in G	N	Cohort size
A_n	$92 \leq n \leq 128$	$\binom{n}{2}$	S_{n-2}	$H.2$	2
	$31 \leq n \leq 37$	$\binom{n}{3}$	$(A_{n-3} \times 3) : 2$	$H.2$	2
	$20 \leq n \leq 22$	$\binom{n}{4}$	$(A_{n-4} \times A_4) : 2$	$H.2$	2
	$16 \leq n \leq 17$	$\binom{n}{5}$	$(A_{n-5} \times A_5) : 2$	$H.2$	2
	$15 \leq n \leq 16$	$\binom{n}{6}$	$(A_{n-6} \times A_6) : 2$	$H.2$	2
	15	$\binom{15}{7}$	$(A_8 \times A_7) : 2$	$H.2$	2
A_{12}		5775	$(A_4 \wr 3).2^2.2$	$H.2$	2
A_{16}		6435	$(A_8 \wr 2) : 2$	$H.2$	2

TABLE 10. Primitive almost simple groups with alternating socle.

Smallest Cohort Representative G	Conditions	Degree	Stabilizer in G	N	Cohort Size
$\mathrm{L}_2(p)$	$4099 \leq p \leq 8191$	$p+1$	$p : ((p-1)/2)$	$H.2$	2
	$97 \leq p \leq 127$	$\binom{p}{2}$	D_{p+1}	$H.2$	2
	$97 \leq p \leq 127$	$\binom{p+1}{2}$	D_{p-1}	$H.2$	2
$\mathrm{L}_2(53)$		6201	A_4	$H.2$	2
$\mathrm{L}_2(71)$		7455	S_4	H	1
$\mathrm{L}_2(73)$		8103	S_4	H	1
$\mathrm{L}_2(79)$		4108	A_5	H	1
$\mathrm{L}_2(89)$		5874	A_5	H	1
$\mathrm{L}_2(p^2)$	$67 \leq p \leq 89$	p^2+1	$p^2 : ((p^2-1)/2)$	$H.2^2$	5
$\mathrm{L}_2(2^6)$		4368	A_5	$H.6$	4
$\mathrm{L}_2(11^2)$		7260	D_{122}	$H.2^2$	5
		7381	D_{120}	$H.2^2$	5
$\mathrm{L}_2(5^3)$		7875	D_{124}	$H.6$	4
		7750	D_{126}	$H.6$	4
$\mathrm{L}_2(2^7)$		8128	D_{258}	$H.7$	2
$\mathrm{L}_2(2^8)$		4112	$\mathrm{L}_2(2^4)$	$H.8$	4
$\mathrm{L}_2(23^2)$		6095	$\mathrm{L}_2(23).2 \cong \mathrm{PGL}(2,23)$	H	1
$\mathrm{L}_2(5^4)$		7825	$\mathrm{L}_2(5^2).2 \cong \mathrm{PGL}(2,5^2)$	$H.4$	3
$\mathrm{L}_2(2^{12})$		4097	$2^{12}.(2^{12}-1)$	$H.12$	6
$\mathrm{L}_2(3^8)$		6562	$3^8.((3^8-1)/2)$	$H.2.8$	11
$\mathrm{L}_2(p^3)$	$17 \leq p \leq 19$	p^3+1	$p^3 : ((p^3-1)/2)$	$H.6$	4

TABLE 11. Primitive almost simple groups with socle $\mathrm{L}_2(q)$.

Smallest Cohort Representative G	Degree	Stabilizer in G	N	Cohort Size
$\mathrm{L}_3(7)$	5586	$\mathrm{SO}_3(7)$	$H.2$	2
$\mathrm{L}_3(17).2$	5526	$17^{1+2} : [16^2].2$	$H.2$	1
$\mathrm{L}_3(19).2$	7620	$19^{1+2} : [108].2$	$H.S_3$	2
$\mathrm{L}_3(67)$	4557	$67^2.[22].\mathrm{L}_2(67).2$	$H.3$	2
$\mathrm{L}_3(71)$	5113	$71^2.[70].\mathrm{L}_2(71).2$	H	1
$\mathrm{L}_3(73)$	5403	$73^2.[24].\mathrm{L}_2(73).2$	$H.3$	2
$\mathrm{L}_3(79)$	6321	$79^2.[26].\mathrm{L}_2(79).2$	$H.3$	2
$\mathrm{L}_3(83)$	6973	$83^2.[82].\mathrm{L}_2(83).2$	H	1
$\mathrm{L}_3(89)$	8011	$89^2.[88].\mathrm{L}_2(89).2$	H	1
$\mathrm{L}_3(2^3).2$	4672	$D_{14} \times \mathrm{L}_2(2^3)$	$H.6$	2
$\mathrm{L}_3(3^2)$	7560	$\mathrm{L}_3(3)$	$H.2^2$	5
	7020	$\mathrm{U}_3(3)$	$H.2^2$	5
$\mathrm{L}_3(3^2).2$ (2)	7371	$\mathrm{GL}_2(3^2).2$	$H.2^2$	3
$\mathrm{L}_3(2^4).2$ (2)	4641	$2^{4+8}.[150]$	$H.(4 \times S_3)$	10
$\mathrm{L}_3(2^6)$	4161	$[2^{12}].[21].\mathrm{L}_2(2^6)$	$H.(3 \times S_3)$	9
$\mathrm{L}_3(3^4)$	6643	$[3^8].[80].\mathrm{L}_2(3^4).2$	$H.4$	3
$\mathrm{L}_4(3).2$ (2)	5265	$\mathrm{SL}_2(3) : A_4.D_8$	$H.2^2$	3
$\mathrm{L}_4(5).2$ (2)	4836	$5^{1+4}.8.S_5$	$H.D_8$	5
$\mathrm{L}_4(17)$	5220	$[17^3].[4].\mathrm{L}_3(17)$	$H.4$	3
$\mathrm{L}_4(19)$	7240	$[19^3].[9].\mathrm{L}_3(19).3$	$H.2$	2
$\mathrm{L}_4(2^2).2$ (2)	5440	$3.\mathrm{L}_3(4).6$	$H.2^2$	3
$\mathrm{L}_4(2^3)$	4745	$[2^{12}].7.\mathrm{L}_2(2^3)^2$	$H.6$	4
$\mathrm{L}_4(3^2)$	7462	$[3^8].[4].\mathrm{L}_2(3^2)$	$H.(2 \times D_8)$	27
$\mathrm{L}_4(2^4)$	4369	$[2^{12}].[15].\mathrm{L}_3(2^4).3$	$H.4$	3
$\mathrm{L}_5(3).2$	4840	$3^{1+6}.2^2.\mathrm{L}_3(3).2$	$H.2$	1
$\mathrm{L}_5(2^2)$	5797	$[2^{12}].3.\mathrm{L}_3(2^2).\mathrm{L}_2(2^2).3$	$H.2$	2
$\mathrm{L}_5(2^3)$	4681	$[2^{12}].7.\mathrm{L}_4(2^3)$	$H.3$	2
$\mathrm{L}_5(3^2)$	7381	$[3^8].[8].\mathrm{L}_4(3^2).4$	$H.2$	2
$\mathrm{L}_7(2).2$	8128	$\mathrm{L}_6(2).2$	$H.2$	1
	8001	$2^{1+10}.\mathrm{L}_5(2).2$	$H.2$	1
$\mathrm{L}_7(2^2)$	5461	$[2^{12}].3.\mathrm{L}_6(2^2).3$	$H.2$	2
$\mathrm{L}_{13}(2)$	8191	$[2^{12}].\mathrm{L}_{12}(2)$	H	1

TABLE 12. Primitive almost simple groups with linear socles other than $\mathrm{L}_2(q)$.

Smallest Cohort Representative G	Degree	Stabilizer in G	N	Cohort Size
$\mathrm{S}_4(5)$	6500	$S_3 \times S_5$	$H.2$	2
	4875	$[2^4].A_5$	$H.2$	2
$\mathrm{S}_4(11)$	7260	$\mathrm{S}_2(11^2).2$	$H.2$	2
	7381	$2.\mathrm{S}_2(11)^2.2$	$H.2$	2
$\mathrm{S}_4(17)$	5220	$17^{1+2}.[2^4].\mathrm{L}_2(17)$	$H.2$	2
	5220	$17^3.[2^3].\mathrm{L}_2(17).2$	$H.2$	2
$\mathrm{S}_4(19)$	7240	$19^{1+2}.[18].\mathrm{L}_2(19)$	$H.2$	2
	7240	$19^3.[3^2].\mathrm{L}_2(19).2$	$H.2$	2
$\mathrm{S}_4(2^2).4$	4896	$\mathrm{Aut}(D_{10}) \wr 2$	$H.4$	1
$\mathrm{S}_4(2^3).2$	5265	$[2^{12}].7.14$	$H.6$	2
$\mathrm{S}_4(2^4)$	4369	$2^{12}.[15].\mathrm{L}_2(2^4)$	$H.4$	3
$\mathrm{S}_6(3)$	7371	$\mathrm{SL}_2(3).\mathrm{S}_4(3)$	$H.2$	2
$\mathrm{S}_6(2^2)$	5525	$[2^{12}].3.\mathrm{L}_3(2^2).3$	$H.2$	2
$\mathrm{S}_8(2)$	5440	$\mathrm{S}_6(2) \times S_3$	H	1
	5355	$2^3.2^8.S_3.A_6.2$	H	1
$\mathrm{S}_{14}(2)$	8128	$2.\Omega^-_{14}(2)$	H	1

TABLE 13. Primitive almost simple groups with symplectic socles.

Smallest Cohort Representative G	Degree	Stabilizer in G	N	Cohort Size
$\mathrm{U}_3(5).3$	6000	$(3 \times 7) : 3$	$H.S_3$	2
$\mathrm{U}_3(17)$	4914	$17^{1+2}.[96]$	$H.S_3$	4
$\mathrm{U}_3(19)$	6860	$19^{1+2}.[360]$	$H.2$	2
$\mathrm{U}_3(3^2)$	5913	$\mathrm{GU}_2(9)$	$H.4$	3
$\mathrm{U}_3(2^4)$	4097	$2^4.2^8.[255]$	$H.8$	4
$\mathrm{U}_4(3)$	4536	$A_6.2$	$H.(2 \times 2)$	5
$\mathrm{U}_4(3).2$	4536	$S_6.2$	$H.D_8$	4
$\mathrm{U}_4(2^3)$	4617	$[2^{12}].7.\mathrm{L}_2(8)^2$	$H.6$	4
$\mathrm{U}_4(3^2)$	7300	$[3^8].[2^3].\mathrm{L}_2(81)$	$H.(2 \times 4)$	8
$\mathrm{U}_5(3)$	6832	$3^{4+4}.[8].A_6.2$	$H.2$	2
	4941	$[4].\mathrm{U}_4(3).[4]$	$H.2$	2
$\mathrm{U}_6(2)$	6336	$\mathrm{S}_6(2)$	$H.2$	2
	6237	$2^{4+8}.S_3.A_5$	$H.S_3$	4
$\mathrm{P}\Omega_7(5)$	7875	$2.\mathrm{L}_4(5).2$	$H.2$	2
	7750	$\mathrm{U}_4(5).2$	$H.2$	2
$\mathrm{P}\Omega_8^+(2^2)$	5525	$[2^{12}].3.\mathrm{S}_4(4)$	$H.(2 \times 2)$	5
$\mathrm{P}\Omega_{14}^+(2)$	8128	$\mathrm{S}_{12}(2)$	$H.2$	2
$\mathrm{P}\Omega_8^-(2^2)$	5397	$[2^{12}].3.\mathrm{U}_4(4)$	$H.4$	3
$\mathrm{P}\Omega_{14}^-(2)$	8127	$[2^{12}].\mathrm{P}\Omega_{12}^-(2)$	$H.2$	2

TABLE 14. Primitive almost simple groups with other classical socles.

Smallest Cohort Representative G	Degree	Stabilizer in G	N	Cohort Size
$G_2(3)$	7371	$2_+^{1+4} : 3^2 \cdot 2$	$H : 2$	2
$G_2(5)$	7750	$3 \cdot \mathrm{U}_3(5) : 2$	H	1
	7875	$\mathrm{L}_3(5) : 2$	H	1
J_1	4180	$7 : 6$	H	1
J_3	6156	$\mathrm{L}_2(16) : 2$	$H : 2$	2
HS	4125	$4^3 : \mathrm{L}_3(2)$	$H : 2$	2
	5600	M_{11}	H	1
	5775	$4 \cdot 2^4 : S_5$	$H : 2$	2
McL	7128	$\mathrm{U}_3(5)$	$H : 2$	2

TABLE 15. Primitive almost simple groups with exceptional or sporadic socles.

Smallest Cohort Representative G	Degree	Cohort Size
$\mathrm{L}_2(23)^2$	6072	5
$\mathrm{L}_2(25)^2$	7800	16
$\mathrm{L}_3(3)^2$	5616	5
$\mathrm{U}_3(3)^2$	6048	5
${M_{11}}^2$	7920	2

TABLE 16. Primitive groups of diagonal type.

Socle	Conditions	Degree	Cohort Size
${A_n}^2$	$64 \leq n \leq 90$	n^2	4
$\mathrm{L}_2(p)^2$	$67 \leq p \leq 89$	$(p+1)^2$	4
$\mathrm{L}_2(25)^2$		4225	4
$\mathrm{Sz}(8)^2$		4225	4
$\mathrm{U}_3(4)^2$		4225	11
$\mathrm{L}_2(64)^2$		4225	16
$\mathrm{L}_2(11)^2$		4356	3
${M_{11}}^2$		4356	1
${M_{12}}^2$		4356	1
${A_{12}}^2$		4356	4
$\mathrm{L}_2(16)^2$		4624	11
$\mathrm{L}_3(8)^2$		5329	4
${M_{22}}^2$		5929	4
$\mathrm{L}_2(13)^2$		6084	4
${A_{13}}^2$		6084	4
$\mathrm{L}_2(81)^2$		6724	76
${A_9}^2$		7056	4
$\mathrm{S}_4(4)^2$		7225	4
$\mathrm{L}_4(4)^2$		7225	4
${A_n}^3$	$16 \leq n \leq 20$	n^3	10
$\mathrm{L}_2(16)^3$		4913	24
$\mathrm{L}_2(17)^3$		5832	10
$\mathrm{L}_2(19)^3$		8000	10
${A_n}^4$	$8 \leq n \leq 9$	n^4	45
$\mathrm{L}_2(7)^4$		4096	45
$\mathrm{L}_2(8)^4$		6561	34
${A_5}^5$		7776	26
${A_6}^5$		7776	26

TABLE 17. Primitive groups of product type.

6.2. **The quasiprimitive groups of degree $d \leq 3600$.** In this section we give tables for each of the O'Nan-Scott type classes of quasiprimitive groups of degree $d \leq 3600$. The first column contains the socle of the quasiprimitive group. We give the number of quasiprimitive groups for each given socle and the number of these which are primitive. The tables for the type **III** groups (Tables 20, 21, 22, 23, and 24) also contain the degrees of the quasiprimitive groups. In Tables 21 and 22, we indicate the degrees at which primitive groups occur via **bold text**.

Socle	Conditions	#Quasiprimitive groups	#Primitive groups
A_n	$5 \leq n \leq 85$	1194	277
$\mathrm{L}_2(q)$	$7 \leq q \leq 3593$, $q \neq 9$	2665	1361
$\mathrm{L}_3(q)$	$3 \leq q \leq 59$	612	107
$\mathrm{L}_4(q)$	$3 \leq q \leq 13$	252	73
$\mathrm{L}_5(q)$	$2 \leq q \leq 7$	40	11
$\mathrm{L}_6(q)$	$2 \leq q \leq 4$	16	12
$\mathrm{L}_7(q)$	$2 \leq q \leq 3$	4	3
$\mathrm{L}_8(q)$	$2 \leq q \leq 3$	3	3
$\mathrm{L}_9(q)$	$q = 2$	1	1
$\mathrm{L}_{10}(q)$	$q = 2$	1	1
$\mathrm{L}_{11}(q)$	$q = 2$	1	1
$\mathrm{S}_4(q)$	$3 \leq q \leq 13$	483	70
$\mathrm{S}_6(q)$	$2 \leq q \leq 4$	105	18
$\mathrm{S}_8(q)$	$2 \leq q \leq 3$	8	6
$\mathrm{S}_{10}(q)$	$q = 2$	5	3
$\mathrm{S}_{12}(q)$	$q = 2$	2	2
$\mathrm{U}_3(q)$	$3 \leq q \leq 13$	289	59
$\mathrm{U}_4(q)$	$3 \leq q \leq 7$	309	81
$\mathrm{U}_5(q)$	$2 \leq q \leq 3$	40	12
$\mathrm{U}_6(q)$	$q = 2$	17	14
$\mathrm{U}_7(q)$	$q = 2$	4	4
$\mathrm{P}\Omega_7(q)$	$q = 3$	19	10
$\mathrm{P}\Omega_8^+(q)$	$2 \leq q \leq 3$	46	26
$\mathrm{P}\Omega_{10}^+(q)$	$q = 2$	5	5
$\mathrm{P}\Omega_{12}^+(q)$	$q = 2$	4	4
$\mathrm{P}\Omega_8^-(q)$	$2 \leq q \leq 3$	33	17
$\mathrm{P}\Omega_{10}^-(q)$	$q = 2$	4	4
$\mathrm{P}\Omega_{12}^-(q)$	$q = 2$	4	4

TABLE 18. Quasiprimitive groups of type **II** with alternating or classical socles.

Socle	#Quasiprimitive groups	#Primitive groups
$G_2(3)$	21	8
$G_2(4)$	10	10
${}^2B_2(8)$	22	8
${}^2B_2(32)$	2	2
${}^3D_4(2)$	4	4
${}^2F_4(2)'$	11	7
M_{11}	36	5
M_{12}	78	16
M_{22}	68	13
M_{23}	9	6
M_{24}	9	6
HS	14	7
J_2	48	16
Co_2	1	1
Co_3	2	1
McL	3	3
Suz	2	2
He	2	2
Fi_{22}	2	2
J_1	11	6

TABLE 19. Quasiprimitive groups of type **II** with exceptional or sporadic socles.

Socle	Degree	Number
${A_5}^2$	60	5
${A_6}^2$	360	16
${A_7}^2$	2520	5
$\mathrm{L}_2(7)^2$	168	5
$\mathrm{L}_2(8)^2$	504	4
$\mathrm{L}_2(11)^2$	660	5
$\mathrm{L}_2(13)^2$	1092	5
$\mathrm{L}_2(17)^2$	2448	5
$\mathrm{L}_2(19)^2$	3420	5
${A_5}^3$	3600	5

TABLE 20. Quasiprimitive groups of type **III(a)**. All of these groups are also primitive.

Socle	Conditions	Degree	#Quasiprimitive groups	#Primitive groups
${A_5}^2$		**25**, **36**, 72, 75, **100**, 144, 200, 225, 300, 360, 400, 450, 600, 720, 900, 1200, 1800	108	12
${A_6}^2$		**36**, **100**, 200, **225**, 400, 450, 800, 900, **1296**, 1350, 1600, **2025**, 2160, 2400, 2592, 2700, 3600	252	72
${A_7}^2$		**49**, **225**, **441**, 882, **1225**, 1764, 2450	48	13
${A_8}^2$		**64**, **225**, **784**, **1225**, 1568, 2450, **3136**	50	17
${A_9}^2$		**81**, **1296**, 2592	19	8
${A_n}^2$	$10 \leq n \leq 11$	$\mathbf{n^2}$, $\binom{\mathbf{n}}{\mathbf{2}}^{\mathbf{2}}$	8	8
${A_n}^2$	$12 \leq n \leq 60$	$\mathbf{n^2}$	4	4
$\mathrm{L}_2(7)^2$		**49**, **64**, 98, 192, 196, 294, **441**, 576, 588, **784**, 882, 1176, 1344, 1568, 1764, 2352, 3136, 3528	111	11
$\mathrm{L}_2(11)^2$		**121**, **144**, 720, **3025**, 3600	25	12
$\mathrm{L}_2(13)^2$		**196**, 392, 588, 784, 1176, 1764, 2352, 3528	43	4
$\mathrm{L}_2(17)^2$		**324**, 648, 1296, 2592	35	4
$\mathrm{L}_2(19)^2$		**400**, 1200, **3249**, 3600	25	5
$\mathrm{L}_2(27)^2$		**900**, 1800, 3600	11	4
$\mathrm{L}_2(31)^2$		**1024**, 3072	12	4
$\mathrm{L}_2(37)^2$		**1444**, 2888	10	4
$\mathrm{L}_2(41)^2$		**1764**, 3528	10	4
$\mathrm{L}_2(p)^2$	$p \in \{23, 43, 47, 53, 59\}$	$(\mathbf{p+1})^{\mathbf{2}}$	4	4
$\mathrm{L}_2(2^3)^2$		**81**, 567, **784**, **1296**, 1568, 2592, 3136	36	12
$\mathrm{L}_2(2^4)^2$		**289**, 867, 1445, 2601	40	11
$\mathrm{L}_2(5^2)^2$		**676**, 1352, 2028, 2704	130	24
$\mathrm{L}_2(3^3)^2$		**784**	16	16
$\mathrm{L}_2(2^5)^2$		**1089**	4	4
$\mathrm{L}_2(7^2)^2$		**2500**	24	24

TABLE 21. Quasiprimitive groups of type **III(b)(i)** (1/2).

Socle	Conditions	Degree	#Quasiprimitive groups	#Primitive groups
$\mathrm{L}_3(3)^2$		**169**, 338, 676, 1014, 1521, 2028, **2704**, 3042	18	4
$\mathrm{L}_3(5)^2$		**961**, 1922	3	1
$\mathrm{L}_3(7)^2$		**3249**	4	4
$\mathrm{L}_3(2^2)^2$		**441**, **3136**	35	35
$\mathrm{L}_4(3)^2$		**1600**	4	4
$\mathrm{L}_5(2)^2$		**961**	1	1
$\mathrm{U}_3(3)^2$		**784**, **1296**, 1568, 3136	36	8
$\mathrm{U}_4(2)^2$		**729**, **1296**, **1600**, **2025**, 2592, 3200	42	20
$\mathrm{S}_6(2)^2$		**784**, **1296**, 1568, 2592, 3136	7	2
${M_{11}}^2$		**121**, **144**, 242, 484, **3025**	6	3
${M_{12}}^2$		**144**	1	1
${M_{22}}^2$		**484**	4	4
${M_{23}}^2$		**529**	1	1
${M_{24}}^2$		**576**	1	1
${A_5}^3$		**125**, **216**, 375, 432, 864, **1000**, 1125, 1728, 2000, 3375	90	30
${A_6}^3$		**216**, **1000**, 2000, **3375**	149	105
${A_7}^3$		**343**, **3375**	12	12
${A_8}^3$		**512**, **3375**	12	12
${A_n}^3$	$9 \leq n \leq 15$	$\mathbf{n^3}$	10	10
$\mathrm{L}_2(7)^3$		**343**, **512**, 686, 1372, 1536, 2744	34	12
$\mathrm{L}_2(8)^3$		**729**	10	10
$\mathrm{L}_2(11)^3$		**1331**, **1728**	12	12
$\mathrm{L}_2(13)^3$		**2744**	10	10
$\mathrm{L}_3(3)^3$		**2197**	2	2
${M_{11}}^3$		**1331**, **1728**, 2662	7	4
${M_{12}}^3$		**1728**	2	2
${A_5}^4$		**625**, **1296**, 1875, 2592	208	90
${A_n}^4$	$6 \leq n \leq 7$	$\mathbf{n^4}$	45	45
$\mathrm{L}_2(7)^4$		**2401**	5	5
${A_5}^5$		**3125**	26	26

TABLE 22. Quasiprimitive groups of type **III(b)(i)** (2/2).

Socle	Degree	Number
$({A_5}^2)^2$	3600	24

TABLE 23. Quasiprimitive groups of type **III(b)(ii)**.

Socle	Degree	Number
${A_5}^2$	3600	5

TABLE 24. Quasiprimitive groups of type **III(c)**.

6.3. **Lookup tables.** In this section we give the lookup tables used in Section 4.1. Each row lists the indices of maximal subgroups of almost simple groups with the given socle, of index at most 1000000. We list the novelty maximals separately. We highlight any indices of maximal subgroups which are not computable in MAGMA via "MaximalSubgroups" or "ClassicalMaximals" in **bold text**. Here q is a prime power such that for a classical group $\mathrm{Cl}(q)$ we have $P(\mathrm{Cl}(q)) \leq 1000000$ (see Table 3).

We give some examples of using these tables and then a general procedure below.

Example 6.1. Let $d = 16105$. We want to find all proper, primitive, almost simple groups of degree d. We search through the lookup tables for any appearances of d and one may find that d occurs once and it is on Table 25 on the row corresponding to $n = 5$. So $T = \mathrm{L}_5(q)$ for some prime power q.

Therefore we will be using the procedure from Section 4.1.2 to find the corresponding primitive groups. We note that Table 25 shows that d does not correspond to a novelty. We now look at Table 3 which demonstrates that with $n = 5$ we have that $2 \leq q \leq 31$.

As d does not correspond to a novelty we check for each $2 \leq q \leq 31$, whether $d \mid \mathrm{L}_5(q)$. If d does divide this order, then it is possible that $\mathrm{L}_5(q)$ has a maximal subgroup of index d. We find that $d \mid \mathrm{L}_5(q)$ only when $q = 11$.

We now Append $\mathrm{L}_5(11)$ to **SimpleGroups** in **Step 2(b)** in the procedure in Section 4.1.2.

Example 6.2. Let $d = 74273$. We want to find all proper, primitive, almost simple groups of degree d. We now search through the lookup tables for any appearances of d and find that d occurs once and it is on Table 26 on the row corresponding to $2m = 4$ and d corresponds to a novelty. So $T = \mathrm{S}_4(q)$ for some prime power q.

Therefore we will be using the procedure from Section 4.1.2 to find the corresponding primitive groups. We now look at Table 3 which demonstrates that for $2m = 4$ we have that $2 \leq q \leq 97$.

As d corresponds to a novelty we check, for each $2 \leq q \leq 97$, whether $d \mid \mathrm{Aut}(\mathrm{S}_4(q))$. If d does divide this order, then it is possible that $\mathrm{Aut}(\mathrm{S}_4(q))$ has a maximal subgroup of index d. We find that $d \mid \mathrm{S}_4(q)$ only when $q = 16$.

We now Append $\mathrm{S}_4(16)$ to **SimpleGroups** in **Step 2(b)** in the procedure in Section 4.1.2.

Recall Section 1.2

Using the Lookup Tables

Input: An integer $1 \leq d \leq 1000000$.

Output: A list, **SimpleGroups**, consisting of possible socles of any almost simple groups with a primitive action of degree d.

Step 1: Construct empty lists **Dim-and-Type**, **Dim-and-Type-Nov**, and **SimpleGroups**.

Step 2: If d appears on Tables 25 – 30 then

Step 2(a): If d does not correspond to a novelty then Append the pair (n,"Cl") to **Dim-and-Type**, where n is given by the table row and "Cl" corresponds to the type of classical group described by the table.

Step 2(a)(i): for each pair (n, "Cl") in **Dim-and-Type** do

Step 2(a)(ii) for each q in the corresponding row of Table 3 do

Step 2(a)(iii) if $d \mid |\mathrm{Cl}_n(q)|$ then Append $\mathrm{Cl}_n(q)$ to **SimpleGroups**.

Step 2(b): If d corresponds to a novelty then Append the pair (n,"Cl") to **Dim-and-Type-Nov**, where n is given by the table row and "Cl" corresponds to the type of classical group described by the table.

Step 2(b)(i): for each pair (n, "Cl") in **Dim-and-Type-Nov** do

Step 2(b)(ii) for each q in the corresponding row of Table 3 do

Step 2(b)(iii) if $d \mid |\mathrm{Aut}(\mathrm{Cl}_n(q))|$ then Append $\mathrm{Cl}_n(q)$ to **SimpleGroups**.

Step 3: if d appears on Table 31 or Table 32 then Append the group corresponding to its row on the table to **SimpleGroups**.

$n = 3$: 7, 8, 13, 21, 31, 56, 57, 73, 91, 120, 133, 144, 183, 234, 273, 280, 307, 381, 553, 651, 757, 871, 993, 1057, 1407, 1723, 1893, 2257, 2451, 2863, 3100, 3541, 3783, 3875, 4000, 4161, 4557, 5113, 5403, 5586, 6321, 6643, 6973, 7020, 7560, 8011, 9507, 10303, 10713, 11557, 11991, 12883, 14763, 15751, 16257, 16513, 17293, 18907, 19461, 22351, 22848, 22953, 24807, 26068, 26733, 28057, 28731, 30103, 32221, 32928, 32943, 36673, 37443, 39007, 39801, 44733, 49953, 51757, 52671, 54523, 56064, 57361, 58323, 58968, 59293, 63253, 65793, 66307, 69433, 70720, 72631, 73713, 75264, 77007, 79243, 80373, 83811, 86143, 94557, 97033, 98112, 98283, 100807, 109893, 110565, 113907, 117993, 120757, 122151, 123708, 124963, 129241, 130683, 135057, 136500, 139503, 144021, 147073, 151711, 155520, 158007, 160930, 161203, 167691, 175981, 177663, 186193, 187923, 193161, 196693, 202051, 209307, 212983, 214833, 218557, 229921, 237657, 241573, 249501, 253513, 259591, 262657, 271963, 274053, 280371, 293223, 299757, 310807, 317533, 324331, 326613, 333507, 345157, 352243, 354046, 359401, 361803, 369057, 376383, 381307, 383781, 391251, 398793, 403000, 411523, 414093, 419257, 427063, 434941, 437583, 453603, 459007, 467173, 478173, 492103, 503391, 517681, 529257, 532171, 532400, 538023, 546861, 552793, 564753, 573807, 579883, 592131, 598303, 620157, 636007, 655291, 658533, 674863, 678153, 684757, 688071, 704761, 708123, 728463, 735307, 738741, 745633, 770007, 777043, 780573, 787657, 823557, 825246, 830833, 845481, 863971, 878907, 886423, 897757, 909163, 924483, 936057, 938119, 943813, 955507, 967273, 983073, 995007
$n = 4$: 8, 15, 28, 35, 40, 56, 85, 117, 130, 156, 357, 400, 585, 806, 820, 1008, 1464, 1550, 2106, 2380, 2850, 4369, 4745, 5220, 7240, 7462, 8379, 8424, 10530, 12720, 16226, 16276, 20440, 24192, 25260, 29484, 30784, 31110, 32704, 33825, 38080, 45696, 48960, 52060, 70161, 70644, 80465, 81400, 89030, 106080, 120100, 137922, 151740, 155000, 185562, 208920, 230764, 251875, 266305, 293090, 305320, 363024, 394420, 407526, 465000, 499360, 503750, 538084, 552610, 578760, 709784, 712980, 733382, 922180, 955266
$n = 5$: 31, 121, 155, 341, 781, 1210, 2801, 4681, 5797, 7381, 16105, 20306, 30941, 64512, 69905, 88741, 137561, 140050, 292561, 304265, 406901, 551881, 605242, 732541, 954305
$n = 6$: 63, 364, 651, 1365, 1395, 3906, 11011, 13888, 19608, 33880, 37449, 55552, 66430, 93093, 177156, 357120, 376805, 402234, 508431
$n = 7$: 127, 1093, 2667, 5461, 11811, 19531, 99463, 137257, 299593, 597871, 925771
$n = 8$: 255, 3280, 10795, 21845, 97155, 97656, 200787, 896260, 960800
$n = 9$: 511, 9841, 43435, 87381, 488281, 788035
$n = 10$: 1023, 29524, 174251, 349525
$n = 11$: 2047, 88573, 698027
$n = 12$: 4095, 265720
$n = 13$: 8191, 797161
$n = 14$: 16383
$n = 15$: 32767
$n = 16$: 65535
$n = 17$: 131071
$n = 18$: 262143
$n = 19$: 524287
Novelties
$n = 2$: 21, 28, 36, 45, 55, 66, 285, 1015, 8555, 9455, 42925, 53955, 93665, 111895, 137825, 238965, 247065, 391405, 500365, 658875, 811035
$n = 3$: 21, 28, 52, 105, 117, 186, 336, 456, 657, 775, 910, 960, 1596, 2562, 2793, 4641, 4672, 5526, 7371, 7620, 13272, 16093, 16926, 21196, 26130, 30927, 31776, 34881, 53466, 69888, 72366, 83292, 88723, 108336, 122550, 137541, 154602, 212460, 234546, 270465, 292537, 309876, 368136, 399822, 406875, 505680, 544726, 551853, 585732, 720990, 732511, 931686, 954273
$n = 4$: 105, 120, 520, 1080, 1785, 4836, 5265, 5440, 19500, 22800, 42705, 74620, 137200, 194712, 299520, 435540, 597780
$n = 5$: 465, 496, 1085, 4840, 9801, 9920, 15730, 28985, 87296, 121737, 121836, 488125, 629486, 882090
$n = 6$: 1953, 2016, 22785, 44044, 88452, 166656, 465465
$n = 7$: 8001, 8128, 177165, 397852, 413385, 796797
$n = 8$: 32385, 32640
$n = 9$: 130305, 130816
$n = 10$: 522753, 523776

TABLE 25. Lookup table for almost simple groups with socle $\mathrm{L}_n(q)$.

$m = 2$: 27, 36, 40, 45, 85, 120, 136, 156, 300, 325, 400, 585, 820, 1176, 1225, 1360, 1464, 2016, 2080, 2380, 3240, 3321, 4369, 4875, 5220, 6500, 7240, 7260, 7381, 9750, 12720, 13000, 14196, 14365, 16276, 20440, 25260, 30784, 32640, 32896, 33210, 33825, 36288, 41616, 41905, 51450, 52060, 54880, 64980, 65341, 68600, 70644, 72030, 81400, 106080, 120100, 139656, 140185, 151740, 195000, 195625, 208920, 230764, 239112, 265356, 266085, 266305, 298890, 305320, 353220, 354061, 363024, 394420, 461280, 462241, 499360, 523776, 524800, 538084, 578760, 712980, 811910, 922180, 936396, 937765, 974292
$m = 3$: 28, 36, 63, 120, 135, 315, 336, 364, 960, 1120, 1365, 2016, 2080, 3640, 3906, 5525, 7371, 16320, 19608, 19656, 23205, 37449, 66430, 69888, 101556, 110565, 130816, 131328, 137600, 155520, 177156, 189540, 300105, 402234, 406875, 408240, 598600, 980400
$m = 4$: 120, 136, 255, 2295, 3280, 5355, 5440, 11475, 13056, 21845, 24192, 32640, 32896, 45696, 91840, 97656, 298480, 597780, 918400, 960800
$m = 5$: 496, 528, 1023, 29524, 75735, 86955, 87296, 349525, 523776, 524800, 782595
$m = 6$: 2016, 2080, 4095, 265720
$m = 7$: 8128, 8256, 16383
$m = 8$: 32640, 32896, 65535
$m = 9$: 130816, 131328, 262143
$m = 10$: 523776, 524800
Novelties
$m = 2$: 425, 4896, 5265, 14400, 74273, 823200
$m = 3$: 110565, 408240
$m = 4$: 45696

TABLE 26. Lookup table for almost simple groups with socle $\mathrm{S}_{2m}(q)$.

$n = 3$: 28, 36, 50, 63, 65, 126, 175, 208, 344, 416, 513, 525, 730, 1332, 1600, 2107, 2198, 3648, 4097, 4914, 5913, 6860, 12168, 13431, 14749, 15626, 16856, 19684, 24390, 25536, 26533, 29792, 32769, 34048, 43904, 50654, 53724, 59130, 61696, 68922, 70956, 78897, 79508, 96768, 103824, 117650, 123823, 148878, 194400, 196988, 205380, 226982, 246235, 262145, 268203, 300764, 357912, 371462, 375625, 389018, 473382, 493040, 512487, 531442, 571788, 638880, 683733, 689858, 704970, 894691, 912674, 984940
$n = 4$: 112, 126, 162, 280, 325, 540, 567, 756, 1040, 1105, 1296, 1575, 2752, 2835, 3264, 3276, 4536, 4617, 7300, 8428, 13000, 15984, 17200, 28288, 29565, 30772, 32832, 33345, 41600, 59860, 69649, 80586, 88452, 102900, 137200, 162504, 170625, 185731, 232960, 236250, 292032, 339456, 373660, 406276, 478224, 551152, 568750, 710073, 731700, 945000, 953344
$n = 5$: 165, 176, 297, 1408, 2440, 3520, 4941, 6832, 17425, 20736, 52480, 66625, 81276, 325625, 393876, 444690, 840400
$n = 6$: 672, 693, 891, 1408, 6237, 6336, 20736, 22204, 27328, 44226, 59136, 98560, 228096, 279825, 333125, 621712, 838656
$n = 7$: 2709, 2752, 38313, 89397, 199108, 398763, 924672
$n = 8$: 10880, 10965, 114939
$n = 9$: 43605, 43776
$n = 10$: 174592, 174933
$n = 11$: 698709, 699392
Novelties
$n = 3$: 750, 1750, 6000
$n = 4$: 4536, 8505
$n = 6$: 157696

TABLE 27. Lookup table for almost simple groups with socle $\mathrm{U}_n(q)$.

$m = 3$: 351, 364, 378, 1080, 1120, 3159, 3640, 3906, 7750, 7875, 12636, 19608, 19656, 22113, 28431, 39000, 58653, 58996, 66430, 101556, 137600, 177156, 265356, 266085, 331695, 402234, 411600, 598600, 885115, 886446, 980400
$m = 4$: 3240, 3280, 3321, 91840, 97656, 195000, 195625, 298480, 918400, 960800
$m = 5$: 58806, 59048, 59292
$m = 6$: 65356, 265720, 266085

TABLE 28. Lookup table for almost simple groups with socle $\mathrm{P}\Omega_{2m+1}(q)$.

$m = 4$: 120, 135, 960, 1080, 1120, 1575, 5525, 11200, 12096, 16320, 19656, 28431, 36400, 39000, 137600, 189540, 300105, 394485, 411600, 598600
$m = 5$: 496, 527, 2295, 9801, 9922, 19840, 23715, 87637, 91840, 118575, 261888, 488906, 976250
$m = 6$: 2016, 2079, 75735, 88452, 88816, 333312, 365211
$m = 7$: 8128, 8255, 796797, 797890
$m = 8$: 32640, 32895
$m = 9$: 130816, 131327
$m = 10$: 523776, 524799
Novelties
$m = 4$: 2025, 14175, 14400, 44800, 408240, 435456, 469625, 518400, 582400
$m = 5$: 71145

TABLE 29. Lookup table for almost simple groups with socle $\mathrm{P}\Omega^+_{2m}(q)$.

$m = 4$: 119, 136, 765, 1066, 1071, 1107, 1632, 5397, 16448, 19406, 22960, 24192, 29848, 39125, 45696, 136914, 209223, 283985, 350805, 411943
$m = 5$: 495, 528, 9760, 9882, 19635, 23936, 25245, 75735, 87125, 104448, 262400, 487656, 609280, 976875
$m = 6$: 2015, 2080, 88330, 88695, 332475, 366080
$m = 7$: 8127, 8256, 796432, 797526
$m = 8$: 32639, 32896
$m = 9$: 130815, 131328
$m = 10$: 523775, 524800
Novelties
$m = 4$: 388557

TABLE 30. Lookup table for almost simple groups with socle $\mathrm{P}\Omega^-_{2m}(q)$.

${}^3D_4(2)$: 819, 2457, 17472, 69888, 89856, 163072, 179712, 978432
${}^3D_4(3)$: **26572**, **186004**
${}^3D_4(4)$: **328965**
Sz(8): 65,560,1456,2080
Sz(32): 1025, 198400, 325376, 524800
Sz(128): **16385**
Sz(512): **262145**
$\mathrm{F}_4(2)$: 69615, 69888
$G_2(3)$: 351, 364, 378, 2808, 3159, 3888, 7371,
$G_2(4)$: 416, 1365, 2016, 2080, 20800, 69888, 230400
$G_2(5)$: 3906, 7750, 7875, 406875, 484375
$G_2(7)$: **19608**, **58653**, **58996**
$G_2(8)$: **37449**, **130816**, **131328**
$G_2(9)$: **66430**, **265356**, **266085**
$G_2(11)$: **177156**, **885115**, **886446**
$G_2(13)$: **402234**
$E_6(2)$: **139503**
${}^2G_2(27)$: 19684, 512487
${}^2F_4(2)'$: 1600, 1755, 2304, 2925, 12480, 14976
Novelties
$G_2(3)$: 1456 $G_2(9)$: **664300**
${}^2F_4(2)'$: 83200, 230400

TABLE 31. Lookup table for almost simple groups with exceptional socles.

M_{11}: 11, 12, 55, 66, 165
M_{12}: 12, 66, 144, 220, 396, 495, 880, 1320
M_{22}: 22, 77, 176, 231, 330, 616, 672
M_{23}: 23, 253, 506, 1288, 1771, 40320
M_{24}: 24, 276, 759, 1288, 1771, 2024, 3795, 40320
HS: 100, 176, 1100, 3850, 4125, 5600, 5775, 15400, 36960
J_2: 100, 280, 315, 525, 840, 1008, 1800, 2016, 10080
Co_1: **98280**
Co_2: 2300, 46575, 47104, 56925, 476928
Co_3: 276, 11178, 37950, 48600, 128800, 170775, 655776, 708400
McL: 275, 2025, 7128, 15400, 22275, 113400, 299376
Suz: 1782, 22880, 32760, 135135, 232960, 370656, 405405, 926640
He: 2058, 8330, 29155, 187425, 244800, 266560, 652800, 999600
Fi_{22}: 3510, 14080, 61776, 142155, 694980
Fi_{23}: 31671, 137632
Fi_{24}': **306936**
J_1: 266, 1045, 1463, 1540, 1596, 2926, 4180
O'N: **122760**
J_3: 6156, 14688, 17442, 20520, 23256, 26163, 43605
Ru: 4060, 188500, 417600, 424125, 593775
Novelties
M_{12}: 1584
HS: 22176
McL: 779625
He: 279888, 437325
J_3: 293760

TABLE 32. Lookup table for almost simple groups with sporadic socles.

References

[1] Artin M. *Algebra*. Prentice Hall; 1991

[2] Aschbacher M. *On the Maximal Subgroups of the Finite Classical Groups*. Inventiones Mathematicae, Vol.76(3), pages 469-514; 1984

[3] Auslander M. and Reiten I. and Smalø S. O. *Representation Theory of Artin Algebras*. Cambridge University Press; 1995

[4] Bang A.S. *Taltheoretiske Undersøgelser*. Tidsskrifft for Mathematik 5, Vol.4, pages 70-80 and 130-137; 1886

[5] Bosma W. and Cannon J. and Playoust C. *The Magma algebra system. I. The user language*, Journal of Symbolic Computation, Vol.24, pages 235-265; 1997

[6] Bray J. N. and Holt D.F. and Roney-Dougal C.M. *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*. Cambridge University Press New York; 2013

[7] Cameron P. J. *Permutation Groups*. Cambridge University Press; 1999

[8] Cannon J. and Holt D.F. *Computing Maximal Subgroups of Finite Groups*. Journal of Symbolic Computation, Vol.37, pages 589-609; 2004

[9] Carter R. W. *Simple Groups of Lie Type*. John Wiley and Sons; 1972

[10] Cayley A. *On the Theory of Groups as Depending on the Symbolic Equation '$\theta^n = 1$'*. Philosophical Magazine, Vol.7(42), pages 40-47; 1854

[11] Clifford A.H. *Representations Induced in an Invariant Subgroup*. Annals of Mathematics, Second Series, Vol. 38, No.3, pages 533-550; 1937

[12] Conway J.H. and Curtis R.T. and Norton S.P. and Parker R.A. and Wilson R.A. *Atlas of Finite Groups*. Oxford University Press, Oxford; 1985

[13] Coutts H. J. and Quick M. and Roney-Dougal C. M. *The Primitive Permutation Groups of Degree Less Than* 4096. Communications in Algebra, Vol.39, pages 3526-3546; 2008

[14] Curtis C.W. and Reiner I. *Representation Theory of Finite Groups and Associative Algebras*. Wiley-Interscience, New York; 1962

[15] Dixon J. D. and Mortimer B. *The Primitive Permutation Groups of Degree Less Than 1000*. Mathematical Proceedings of the Cambridge Philosophical Society, Vol.102(2), pages 213-238; 1988

[16] Dixon J. D. and Mortimer B. *Permutation Groups*. Springer-Verlag New York inc; 1996

[17] Gorenstein D. and Lyons R. and Solomon R. *The Classification of the Finite Simple Groups*. Mathematical Surveys and Monographs, Vol.40.1, American Mathematical Society, Providence, RI; 1994

[18] Gorenstein D. *Finite Groups*. American Mathematical Society; 1980

[19] Gross F. and Kovacs L.G. *On Normal Subgroups which are Direct Products*. Journal of Algebra, Vol.90, pages 133-168; 1984

[20] Guest S. and Morris J. and Praeger C.E. and Spiga P. *On The Maximum Orders of Elements of Finite Almost Simple Groups and Primitive Permutation Groups*. Transactions of the American Mathematical Society, Vol. 367, pages 7665-7694; 2015

[21] Hestenes M.D. *Singer Groups*. Canadian Journal of Mathematics, Vol.22, Issue 3, pages 492-513; 1970

[22] Holt D. F. and O'Brien E. A. and Leedham-Green C. R. and Rees S. *Computing Matrix Group Decompositions with Respect to a Normal Subgroup*. Journal of Algebra, Vol.184, Issue 3, pages 818-838; 1996

[23] Holt D. F. and O'Brien E. A. and Leedham-Green C. R. and Rees S. *Testing Matrix Groups for Primitivity*. Journal of Algebra, Vol.184, Issue 3, pages 795-817; 1996

[24] Holt D. F. and O'Brien E. A. *Handbook of Computational Group Theory*. Chapman and Hall/CRC Press; 2005

[25] Horn R. A. and Johnson C. R. *Matrix Analysis*. Cambridge University Press; 1985

[26] Huppert B. *Endliche Gruppen. I (Die Grundlehren der Mathematischen Wissenscaften)* (Finite Groups I). Springer-Verlag, Berlin; 1967

[27] Isaacs I. M. *Algebra: A Graduate Course*. Brooks/Cole; 1994

[28] Kleidman P. B. and Liebeck M . W. *The Subgroup Structure of the Finite Classical Groups*. Cambridge University Press; 1990

[29] Liebeck M. W. and Praeger C. E. and Saxl J. *A Classification of the Maximal Subgroups of the Finite Alternating and Symmetric Groups*. Journal of Algebra, Vol.111, pages 365-383; 1987

[30] Neumann P.M. and Praeger C.E. *A Recognition Algorithm for Special Linear Groups*. Proceedings of the London Mathematical Society, (3), Vol.65, pages 555-603; 1992

[31] Neumann H. *Varieties of Groups*. Springer-Verlag Berlin Heidelberg; 1967

[32] Maclagan-Wedderburn J.H. *A Theorem on Finite Algebras*. Transactions of the American Mathematical Society, Vol.6, No.3, pages 349-352; 1905

[33] Praeger C. E. *An O'Nan-Scott Theorem for Finite Quasiprimitive Permutation Groups and an Application to 2-Arc Transitive Graphs*. Journal of the London Mathematical Society, Vol.47(2), pages 227-239; 1992

[34] Roney-Dougal C. M. and Unger W. R. *The Affine Primitive Permutation Groups of Degree Less Than 1000*. Journal of Symbolic Computation, Vol.35, pages 421-439; 2003

[35] Roney-Dougal C. M. *Conjugacy of Subgroups of the General Linear Group*. Experimental Mathematics, Vol.13(2), pages 151-163; 2004

[36] Roney-Dougal C. M. *The Primitive Permutation Groups of Degree Less Than 2500*. Journal of Algebra, Vol.292, pages 154-183; 2005

[37] Rotman J. J. *An Introduction to the Theory of Groups*. Springer-Verlag New York inc. 5th Edition; 1995

[38] Rotman J. J. *Advanced Modern Algebra*. Prentice-Hall, Pearson Education; 2002

[39] Scott L. L. *Representations in characteristic p*. Santa Cruz conference on finite groups, Proc. Sympos. Pure Math., vol 37, Amer. Math. Soc., Providence, R.I. pages 318-331; 1980.

[40] Schur I. *Neue Begründung der Theorie der Gruppencharaktere* (New foundation for the theory of group characters). Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin, pages 406-432; 1905

[41] Suprunenko D.A. *Matrix Groups*. Translations of Mathematical Monographs, Vol.45, American Mathematical Society, Providence; 1976

[42] Taylor D. E. *The Geometry of the Classical Groups*. Sigma Series in Pure Mathematics, Vol.9, Heldermann Verlag Berlin; 1992

[43] Vasilyev A. V. *Minimal Permutation Representations of Finite Simple Exceptional Groups of Types E_6, E_7, and E_8*. Algebra and Logic, Vol.36, No.5; 1997

[44] Wilson R. A. *The Finite Simple Groups*. Springer-Verlag London ltd; 2009

[45] Zsigmondy K. *Zur Theorie der Potenzreste*. Journal Monatshefte für Mathematik, Vol.3, pages 265-284; 1892