Forum of Mathematics, Sigma (2026), **Vol. 14**:e111 1–47
doi:10.1017/fms.2026.10258

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Separating subsets from their images

Marco Barbieri[1], Maruša Lekše[2], Primož Potočnik[3] and Kamilla Rekvényi[4]

[1]Faculty of Mathematics and Physics, University of Ljubljana, Slovenia; Email: marco.barbieri@fmf.uni-lj.si.
[2]Institute of Mathematics, Physics and Mechanics, Ljubljana, and Faculty of Mathematics and Physics, University of Ljubljana, Slovenia; E-mail: marusa.lekse@imfm.si.
[3]Faculty of Mathematics and Physics, University of Ljubljana, and Institute of Mathematics, Physics and Mechanics, Ljubljana, Slovenia; E-mail: primoz.potocnik@fmf.uni-lj.si.
[4]Department of Mathematics, University of Manchester, and Heilbronn Institute for Mathematical Research, Bristol, UK; E-mail: kamilla.rekvenyi@manchester.ac.uk (Corresponding author).

Received: 23 December 2025 UTC; **Revised:** 26 May 2026 UTC; **Accepted:** 18 June 2026 UTC

2020 Mathematical Subject Classification: *Primary* – 20B05; *Secondary* – 05B30, 20-08, 20B15, 20B25

Abstract

Let G be a transitive permutation group acting on Ω. In this paper, we introduce and study the parameter $\mathrm{sep}(G)$, which denotes the size of the smallest set of points A such that, for every permutation $g \in G$, $A \cap A^g$ is nonempty. In particular, we focus on deriving general bounds for arbitrary transitive groups, and on the asymptotic behaviour of certain families of primitive groups. We also provide a classification of transitive groups with $\mathrm{sep}(G)$ largest possible, namely with $\mathrm{sep}(G) = \lceil (|\Omega| + 1)/2 \rceil$.

Contents

1 Introduction **2**
1.1 Historical appearances . . . 4
2 Results **5**
2.1 General bounds . . . 5
2.2 Permutation groups with bounded stabilisers . . . 6
2.3 Reduction to primitive permutation groups . . . 7
2.4 Primitive permutation groups . . . 8
3 Properties of $\mathrm{sep}(G)$ **11**
3.1 Monotonicity with respect to subgroups and subfamilies . . . 11
3.2 Monotonicity with respect to quotients and extensions . . . 12
3.3 Monotonicity with respect to change of action . . . 13
4 Proof of Theorem C **15**
5 Proof of Theorem F **16**
6 Proof of Theorem J **18**
7 Proof of Theorem D **21**
7.1 Primitive groups meeting the upper bound . . . 21
7.2 Imprimitive groups meeting the upper bound . . . 24
7.2.1 Permutation groups admitting blocks of size 2 . . . 25
7.2.2 Permutation groups admitting two blocks of size m . . . 31
8 Primitive groups **34**

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

8.1 Almost simple type 34
8.2 Simple diagonal type 41
References 45

1. Introduction

Let us begin by presenting a graph-theoretical problem which spurred our interest in the topic of the paper and led us to define and investigate the notions presented here.

Suppose we are given a simple finite graph Γ on n vertices and we want to know whether its complement contains an isomorphic copy of Γ as a subgraph, or equivalently, whether two copies of Γ can be packed into the complete graph $\mathbf{K}_n$. Clearly, if Γ contains more than $2^{-1}\binom{n}{2}$ edges, then such a packing is impossible. On the other hand, if Γ is very sparse (e.g., if it has maximum valence 1 and at least 3 vertices), then the packing will very likely exist. It is thus natural to ask what is the largest integer m such that every graph on n vertices and at most m edges can be packed twice into $\mathbf{K}_n$. Since such a packing is clearly impossible for the complete bipartite graph $\mathbf{K}_{1,n-1}$, we see that $m \leq n-2$. Surprisingly, as was elegantly proved independently in [14, Theorem 1] and in [25, Section 2], this bound is sharp, in the sense that every graph on n vertices and at most $n-2$ edges lies in its complement as a subgraph.

The above problem for graphs can actually be translated into the language of permutation groups. Suppose Γ is a graph with vertex set $[n] := \{1, 2, \ldots, n\}$ and edge set $E \subseteq \binom{[n]}{2}$. An isomorphism from Γ to a graph contained in the complement of Γ is a permutation of $[n]$ which, when viewed as a permutation on the unordered pairs $\binom{[n]}{2}$, maps E to a set disjoint from E. In short, two copies of Γ can be packed into $\mathbf{K}_n$ if and only if the group $\mathrm{Sym}(n)$ in its action on $\binom{[n]}{2}$ contains an element g such that $E \cap E^g = \emptyset$. We say that such a set E is self-separable, and if there is no such element g then we say it is non-self-separable (see Definition 1.1). The graph-theoretical theorem mentioned above is equivalent to the assertion that the size of the smallest non-self-separable set for the action of $\mathrm{Sym}(n)$ on $\binom{[n]}{2}$ is $n-1$. In fact, this interpretation was already noted in [25], where not only the size of the smallest non-self-separable set (which was called a sprawling set there) but also all non-self-separable sets of minimal cardinality were determined (see [25, Theorem 2]).

In this paper we show that viewing the original packing problem in this general group-theoretical context reveals connections to several classical problems and theorems in combinatorics, finite geometry, and group theory, and opens a plethora of new and interesting questions. We will address some of these and suggest further directions to explore.

Definition 1.1. Let G be a transitive permutation group on a finite set Ω with $|\Omega| \geq 2$. A subset $A \subseteq \Omega$ is said to be *self-separable* for G provided that there exists $g \in G$ such that $A \cap A^g = \emptyset$, and is *non-self-separable* otherwise. Further, let

$$\mathrm{sep}(G) := \min\{|A| \in \mathbb{N} \mid A \subseteq \Omega \text{ is not self-separable for } G\}$$

be the size of a smallest non-self-separable set for G.

Observe that the parameter $\mathrm{sep}(G)$ is also equal to the largest integer such that all sets of size less than that integer are self-separable, that is,

$$\mathrm{sep}(G) = \max\{t \in \mathbb{N} \mid \forall A \subseteq \Omega : |A| < t \Rightarrow A \text{ is self-separable}\}.$$

The main theme of this paper is to address the following:

Problem A. Given a transitive permutation group G, determine the parameter $\mathrm{sep}(G)$.

The above question can be approached from several angles, ranging from algorithmic considerations to exact theoretical results. We mainly focus on theoretical ways, but briefly consider the computational approach too.

The computational task of determining $\mathrm{sep}(G)$ for a given permutation group G appears to be highly challenging. The only algorithm we devised during the preparation of this paper involves an exhaustive search (see [7] and Section 7) using a theoretical lower bound we establish in Theorem C. Our algorithm

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

systematically tests all subsets A of the domain whose sizes exceed the theoretical lower bound in Theorem C, and stops when we find the minimal example A that is non-self-separable for G. When G is known to be k-homogeneous, we may limit the search space to subsets containing a fixed k-subset. No further improvements of this naïve approach are known to us. Therefore we ask the following:

Question 1.2. *Does there exist a significantly more efficient algorithm for computing the parameter* $\mathrm{sep}(G)$ *given a permutation group* G *(perhaps, subexponential in the degree)?*

In this paper, however, we will be especially interested in asymptotic (lower and upper) bounds on $\mathrm{sep}(G)$ in terms of the degree of G. Theorem C tells us that, for every group G of degree n, the parameter $\mathrm{sep}(G)$ always satisfies $\sqrt{n} \leq \mathrm{sep}(G) \leq \lceil (n+1)/2 \rceil$. Moreover, infinite families of transitive groups exist for which $\mathrm{sep}(G)$ is asymptotically the square root of the degree (e.g., the family of symmetric groups acting on unordered pairs, which is our motivating example) as well as infinite families where $\mathrm{sep}(G)$ is asymptotically linear in the degree of the group (e.g., the symmetric groups in their natural action).

To understand asymptotic behaviours better, we need the following definitions. For an infinite family $\mathcal{C}$ of finite permutation groups and for an integer n, let $\mathcal{C}_n$ be the subfamily of permutation groups in $\mathcal{C}$ that have degree n, and let

$$X_{\mathcal{C}} := \{n \in \mathbb{N} \mid \mathcal{C}_n \neq \emptyset\}.$$

The asymptotic behaviour of the parameter $\mathrm{sep}(G)$ for $G \in \mathcal{C}$ will be analysed in terms of the functions:

$$\mathbf{f}_{\mathcal{C}} : X_{\mathcal{C}} \to \mathbb{N}, \quad n \mapsto \min\{\mathrm{sep}(G) \mid G \in \mathcal{C}_n\},$$

and

$$\mathbf{F}_{\mathcal{C}} : X_{\mathcal{C}} \to \mathbb{N}, \quad n \mapsto \max\{\mathrm{sep}(G) \mid G \in \mathcal{C}_n\}.$$

Remark 1.3. We can immediately observe that, for every two families $\mathcal{D} \subseteq \mathcal{C}$ and for every positive integer $n \in X_{\mathcal{C}}$,

$$\mathbf{f}_{\mathcal{C}}(n) \leq \mathbf{f}_{\mathcal{D}}(n) \leq \mathbf{F}_{\mathcal{D}}(n) \leq \mathbf{F}_{\mathcal{C}}(n).$$

To understand the behaviour of these functions on large classes of transitive permutation groups, we will consider the following problem.

Question 1.4. Given an infinite class $\mathcal{C}$ of transitive permutation groups, what is the asymptotic behaviour of $\mathbf{f}_{\mathcal{C}}(n)$ and of $\mathbf{F}_{\mathcal{C}}(n)$? In particular, do there exist two positive constants $r \in \left(\frac{1}{2}, 1\right)$ and c, and an infinite family $\mathcal{C}$ such that

$$\liminf_n \frac{\mathbf{f}_{\mathcal{C}}(n)}{n^r} = \limsup_n \frac{\mathbf{F}_{\mathcal{C}}(n)}{n^r} = c?$$

That is, does there exist a family $\mathcal{C}$ such that the expected asymptotic behaviour of $\mathrm{sep}(G)$, for a generic $G \in \mathcal{C}$, is neither square root nor linear?

To give a taste of the statements that we will be proving, let us list some of them. In the case of the class $\mathcal{C}_{\mathrm{tr}}$ of all transitive permutation groups, we prove that $\liminf \mathbf{f}_{\mathcal{C}_{\mathrm{tr}}}(n)$ grows asymptotically as $\sqrt{n}$ (see Theorem E), while $\limsup \mathbf{F}_{\mathcal{C}_{\mathrm{tr}}}(n)$ is asymptotically $\frac{n}{2}$ (see Theorem C), or to be precise:

$$\liminf_n \frac{\mathbf{f}_{\mathcal{C}_{\mathrm{tr}}}(n)}{\sqrt{n}} = 1 \quad \text{and} \quad \limsup_n \frac{\mathbf{F}_{\mathcal{C}_{\mathrm{tr}}}(n)}{n} = \frac{1}{2}.$$

Further, as is stated in Theorem F, for the class $\mathcal{C}_{\mathrm{reg}}$ of regular permutation groups, the asymptotic bound for $\mathbf{F}_{\mathcal{C}_{\mathrm{reg}}}$ can be significantly improved to

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}_{\mathrm{reg}}}(n)}{\sqrt{n}} \leq \frac{4}{\sqrt{3}}.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Particular attention is also given to the class $\mathcal{C}_{\mathrm{pr}}$ of primitive permutation groups, specifically to the following problem.

Problem B. Determine what is the largest subclass $\mathcal{C} \subseteq \mathcal{C}_{\mathrm{pr}}$ where a bound of the form

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}}(n)}{\sqrt{n}} \leq C$$

holds for some constant C.

To facilitate smooth reading, Section 2 provides an extended abstract of the results proved in this paper. The proofs can be found in later sections.

1.1. Historical appearances

The concept of self-separability is so natural that it is not surprising that it appears in many different contexts and guises.

For example, an elementary fact – now referred to as Neumann Separation Lemma (see Lemma 4.1) – first appeared in the context of infinite permutation groups in [47]. There, Neumann related the problem of covering an infinite group with finitely many cosets to the existence of a set of points that can be separated from itself by a group element. (The latter group-theoretical formulation was posed earlier in [44].) This lemma had been used to prove the Separation Theorem (see [48, Theorem 1.1] or [50]), which states that if G is an infinite group of finitary permutations whose orbits are all infinite, then $\mathrm{sep}(G)$ is infinite. The contrapositive of this theorem states that if $\mathrm{sep}(G)$ is finite, then at least one orbit of G is finite. This gives a satisfactory solution to Problem A for infinite groups of finitary permutations.

Apart from the graph-theoretical connection to the packing problem mentioned earlier (see [14, 25]), problems concerning separation also appeared in the context of block designs and the theory of hypergraphs. In the former setting, the existence of a self-separable set can be used as an ingredient in the construction of combinatorial designs (see [31] and [61, Section 4.5]). On the hypergraph side, [24] attributes to Erdős and Bollobás the conjecture that the union of the edges of a k-uniform hypergraph contains at most $k^2 - k + 1$ vertices. This conjecture was first proved by Lovász in 1975. In 1981, Füredi reproved the result using the theory of fractional matchings and fractional transversals in hypergraphs (see [24, Corollary 4]). Füredi's proof also shows that any example attaining this bound arises from a projective plane of order $k - 1$. (This characterisation can also be related to the classical work of Singer on difference sets [59], see Section 5). A third proof, using only elementary counting arguments and the language of tactical configurations, was found by Praeger and Neumann in [45]. As shown in [45, Corollary 1], they obtained a lower bound on the parameter $\mathrm{sep}(G)$ that is slightly weaker than the bound in our Theorem C, but without explicitly defining the notion of self-separability or the parameter $\mathrm{sep}(G)$. Surprisingly, the combinatorial bound from [45, Theorem 1] had previously been proved independently in [23] via intersecting hypergraphs, and in [15] using the theory of Bose–Mesner algebras of association schemes.

In a later paper, Praeger [50] introduced the concept of movement for permutation groups, that is, the maximum cardinality of the difference between a subset and one of its images. Using this notion, a subset is self-separable if and only if its movement and its cardinality coincide. In particular, the parameter $\mathrm{sep}(G)$ can be equivalently defined as the largest integer t such that, for every set Γ of points of size at most t, the movement of Γ is equal to its cardinality. The philosophy underlying earlier work on movement, however, is diametrically opposed to most of our investigation: requiring that all subsets have small movement forces the permutation group to have small degree (see, for instance, [1, 2, 18, 27, 30, 46]). For instance, in the seminal work [51], Praeger proves that if a permutation group G fixes no points and k is a positive integer such that no element of G moves any subset by more than k, then the degree of G is at most $5k - 2$. On the other hand, in this paper, we mostly look for the size of the smallest non-self-separable subset, that is, for the cardinality of the smallest set whose movement is distinct from its cardinality.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Nevertheless, despite these numerous historical appearances of the notion of self-separability, relatively little seems to be known about the parameter $\mathrm{sep}(G)$ in general.

2. Results

2.1. General bounds

We start our investigation by determining some general bounds on $\mathrm{sep}(G)$.

Theorem C. *Let G be a transitive permutation group on Ω with $|\Omega| = n$, and let $\alpha \in \Omega$ be a point. Then*

$$\mathrm{sep}(G) \geq \frac{1}{2|G_\alpha|} + \sqrt{n - \frac{1}{|G_\alpha|} + \frac{1}{4|G_\alpha|^2}}, \tag{2.1}$$

with equality if and only if G is a regular group of collineations of a projective plane. In particular, if $\mathcal{C}_{\mathrm{tr}}$ is the class of all transitive permutation groups, then

$$\liminf_n \frac{\mathbf{f}_{\mathcal{C}_{\mathrm{tr}}}(n)}{\sqrt{n}} = 1.$$

The proof of Theorem C (given in Section 4) relies on the Neumann Separation Lemma (see [10, 47]), and the characterisation of the equality depends on considerations from incidence geometry. We remark that Theorem C is a slightly improved version of [45, Corollary 1], where the bound

$$\mathrm{sep}(G) \geq \frac{1}{2} + \sqrt{n - \frac{3}{4}}$$

is proved using elementary counting techniques from design theory, and the two bounds coincide for regular actions.

We now focus on an upper bound for $\mathrm{sep}(G)$. Clearly, for every transitive permutation group G of degree n, two subsets containing strictly more than $\lfloor n/2 \rfloor$ points cannot have trivial intersection. Hence,

$$\mathrm{sep}(G) \leq \left\lceil \frac{n+1}{2} \right\rceil. \tag{2.2}$$

Classifying the groups that attain the upper bound in Inequality (2.2) is a nontrivial problem and is interesting in its own right. For example, a very natural subproblem that needs to be addressed is: *Determine all primitive permutation groups G of even degree such that every subset of the domain of size half of the degree can be mapped to its complement by an element of G.* Clearly, the alternating and symmetric groups have this property, but it is somewhat surprising that so do some other permutation groups.

Theorem D. *Let G be a transitive permutation group of degree n. If G attains the upper bound in Inequality (2.2), then G satisfies one of the following conditions.*

(a) *G is primitive, and either $n \leq 24$ or $\mathrm{Alt}(\Omega) \leq G \leq \mathrm{Sym}(\Omega)$. (The precise list of such groups can be found in Lemma 7.1).*
(b) *G is imprimitive with a system of imprimitivity consisting of $n/2$ blocks of size 2, and either $n \leq 24$ or the action on the block system is isomorphic to either $\mathrm{Alt}(n/2)$ or $\mathrm{Sym}(n/2)$. (The precise list of such groups can be found in Lemma 7.12).*
(c) *G is imprimitive with a system of imprimitivity consisting of two blocks of size $n/2$, and either $n \leq 24$ or the action induced on a block is isomorphic to either $\mathrm{Alt}(n/2)$ or $\mathrm{Sym}(n/2)$. (The precise list of such groups can be found in Lemma 7.18).*

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

We stress that not all groups with the conditions above reach the putative upper bound. A complete characterisation is provided in Section 7 (once again, see Lemmas 7.1, 7.12, and 7.18).

Since Theorem D yields infinite families of permutation groups attaining the bound in Inequality (2.2), we have the following consequence:

Theorem E. *Let $\mathcal{C}_{\mathrm{tr}}$ be the class of all transitive permutation groups. Then*

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_{\mathrm{tr}}}(n)}{n} = \frac{1}{2}.$$

2.2. Permutation groups with bounded stabilisers

In the previous section, we determined the asymptotic behaviour of $\mathbf{f}_{\mathcal{C}_{\mathrm{tr}}}$ and $\mathbf{F}_{\mathcal{C}_{\mathrm{tr}}}$ for the class of all transitive permutation groups. Note, however, that the gap between the square root asymptotics of $\liminf \mathbf{f}_{\mathcal{C}_{\mathrm{tr}}}(n)$ and the linear growth of $\mathbf{F}_{\mathcal{C}_{\mathrm{tr}}}(n)$ leaves many questions about the parameter $\mathrm{sep}(G)$ for a generic transitive permutation group G open. In what follows, we will try to identify subclasses $\mathcal{C} \subseteq \mathcal{C}_{\mathrm{tr}}$ for which we are able to exert a more effective control. That is, families for which the gap between $f_{\mathcal{C}_{\mathrm{tr}}}$ and $F_{\mathcal{C}_{\mathrm{tr}}}$ is smaller. In fact, we will observe that for many important families of permutation groups $\mathcal{C} \subseteq \mathcal{C}_{\mathrm{tr}}$, $\mathbf{F}_{\mathcal{C}}(n)$ is asymptotically proportional to $\sqrt{n}$ (as well as $\mathbf{f}_{\mathcal{C}}(n)$, by consequence). The class of regular permutation groups provides such a family.

Theorem F. *Let G be a regular permutation group of degree n. Then*

$$\mathrm{sep}(G) \leq \frac{4}{\sqrt{3}}\sqrt{n}.$$

In particular, if $\mathcal{C}_{\mathrm{reg}}$ is the family of all regular permutation groups, then

$$1 = \liminf_n \frac{\mathbf{f}_{\mathcal{C}_{\mathrm{reg}}}(n)}{\sqrt{n}} \leq \limsup_n \frac{\mathbf{F}_{\mathcal{C}_{\mathrm{reg}}}(n)}{\sqrt{n}} \leq \frac{4}{\sqrt{3}}.$$

We will prove this result in Section 5. This result follows from Remark 5.1, which asserts that for a subset A not being self-separable for a regular group G is equivalent to A being a difference basis for G:

Definition 2.1. A subset A of a group G such that $AA^{-1} = G$ is a *difference basis for G*

Let us remark that asymptotic results for the minimal size of a difference basis for a generic group G are still an open problem in additive combinatorics.

If every nontrivial element of G can be written uniquely as ab^{-1} for some $a, b \in A$, then the difference basis A is called a *difference set*, which is a widely used tool in finite geometries. For instance, if q is the order of a classical projective plane, a paper [59] by Singer proves the existence of a difference set of size $q+1$ for the cyclic group of order q^2+q+1. Observe that these permutation groups are precisely those that meet the lower bound in Theorem C.

Let G be an abstract group and suppose that G induces multiple faithful actions on some finite sets Ω_i. To distinguish them, we will use the symbol $G \curvearrowright \Omega_i$ to denote the permutation groups induced by the action of G on the domain Ω_i. For instance, if $G = \mathrm{PSL}_d(q)$ and V^k denotes the set of k-dimensional subspaces of the natural module, then the permutation group induced by the natural action of G on V^k can be denoted by $\mathrm{PSL}_d(q) \curvearrowright V^k$. Similarly, if H is a core-free subgroup of G, we denote the permutation group that G induces on the right coset space G/H by $G \curvearrowright G/H$.

Let $H \leq K$ be two core-free subgroups of G. In Lemma 3.3, we establish that $\mathrm{sep}(G \curvearrowright G/K) \leq \mathrm{sep}(G \curvearrowright G/H)$. By combining this fact with Theorem F, we obtain the following corollaries of theorems of Cameron, Praeger, Saxl, and Seitz [17] and of Gardiner, Trofimov, and Weiss [26, 62, 63, 65, 66].

Corollary G. *For every positive integer d, there exists a constant $\mathbf{c}(d)$ such that, for every primitive permutation group G of degree n and minimal nontrivial subdegree at most d, the following inequality*

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

holds

$$\mathrm{sep}(G) \leq \mathbf{c}(d)\sqrt{n}.$$

In particular, if $\mathcal{C}_d$ is the family of primitive permutation groups of minimal nontrivial subdegree at most d, then

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}_d}(n)}{\sqrt{n}} \leq \mathbf{c}(d).$$

Corollary H. *For every positive integer d, there exists a constant $\mathbf{c}(d)$ such that, for every 2-arc-transitive group of automorphisms G of a connected graph with n vertices and of valency at most d, the following inequality holds*

$$\mathrm{sep}(G) \leq \mathbf{c}(d)\sqrt{n}.$$

In particular, if $\mathcal{C}_d$ is the family of 2-arc-transitive groups of automorphisms of connected graphs of valency at most d, then

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}_d}(n)}{\sqrt{n}} \leq \mathbf{c}(d).$$

The proofs of these results are in Section 5.

2.3. Reduction to primitive permutation groups

A standard approach in permutation group theory is to investigate whether and to what extent the problem can be reduced to the setting of primitive groups.

Recall that every imprimitive permutation group G can be reduced to an iterated wreath product of primitive permutation groups as follows. Let Σ be a system of imprimitivity for G and let B be a block in Σ. As usual, we denote the permutation group that the setwise stabiliser G_B induces on B by G_B^B, and the permutation group that G induces on Σ by G^Σ. Then G embeds into the imprimitive wreath product $G_B^B \operatorname{wr} G^\Sigma$. Moreover, if Σ is a coarsest system of imprimitivity, then G^Σ is primitive, meanwhile if Σ is a finest system of imprimitivity, then G_B^B is primitive.

The following theorem is proved in Section 3.2.

Theorem I. *Let G be a group, and suppose that G embeds into the imprimitive wreath product $H \operatorname{wr} K$. Then*

$$\mathrm{sep}(K) + \mathrm{sep}(H) - 1 \leq \mathrm{sep}(G) \leq \mathrm{sep}(K)\mathrm{sep}(H)\,.$$

The following example shows that the upper bound is asymptotically sharp. Let K and H be isomorphic to the cyclic group of degree q^2+q+1 with regular action, and let $G = K \operatorname{wr} H$. Note that the degree of G is $(q^2+q+1)^2$. For large q, using Theorem C to find the lower bound for $\mathrm{sep}(G)$ and the upper bounds for $\mathrm{sep}(K)$ and $\mathrm{sep}(H)$,

$$q^2 + o(q^2) \leq \mathrm{sep}(G) \leq \mathrm{sep}(K)\mathrm{sep}(H) \leq (q + o(q))^2 = q^2 + o(q^2).$$

This proves the asymptotic sharpness of the upper bound of Theorem I.

Furthermore, if K and H are regular groups, using the above argument and Theorem F, we can show that $\mathrm{sep}(G) \leq \frac{8}{3}\sqrt{n}$ – matching the optimal lower bound up to a multiplicative constant.

On the other hand, we are unable to prove the sharpness of the lower bound. We show, however, that there exists a family of permutation groups for which the lower bound is asymptotically tight up to a constant. The following result, of independent interest, will be essential in finding such a family.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Theorem J. *If G is the wreath product $\mathrm{Sym}(a)$ wr $\mathrm{Sym}(b)$ endowed with the imprimitive action on ab points, then*

$$\mathrm{sep}(G) = \begin{cases} a+b-2 & \text{if } a=3 \text{ and } b \text{ is odd, or } b=3 \text{ and } a \text{ is odd} \\ a+b-1 & \text{otherwise}. \end{cases}$$

In particular, if G is an imprimitive permutation group with a block system of cardinality b whose blocks contain a points, then

$$\mathrm{sep}(G) \leq a+b-1\,.$$

The proof of this result is given in Section 6. Let a and b be two even positive integers, and let $K = \mathrm{Sym}(a)$ and $H = \mathrm{Sym}(b)$. By choosing $G = K$ wr H, Theorem J implies that

$$\mathrm{sep}(G) = a+b-1 = 2\mathrm{sep}(K) + 2\mathrm{sep}(H) - 5.$$

On the other hand, Theorem I yields

$$\mathrm{sep}(G) \geq \mathrm{sep}(K) + \mathrm{sep}(H) - 1.$$

If we allow a and b to grow as two arbitrary unbounded functions, we find that, asymptotically, $\mathrm{sep}(G)$ is twice the lower bound of Theorem I – proving the asymptotic sharpness up to the multiplicative constant 2. This leads to the following questions.

Question 2.2. Is the lower bound stated in Theorem I asymptotically sharp? If it is not, is $2(\mathrm{sep}(K) + \mathrm{sep}(H))$ an asymptotically sharp lower bound? Furthermore, by excluding an appropriate infinite family of transitive groups, is it possible to obtain a larger lower bound?

2.4. Primitive permutation groups

Recall that, for $\mathrm{Alt}(n)$ and $\mathrm{Sym}(n)$ in their action on n points, $\mathrm{sep}(\mathrm{Alt}(n)) = \mathrm{sep}(\mathrm{Sym}(n)) = \lceil (n+1)/2 \rceil$. At the moment, they constitute the single infinite family of primitive permutation groups where we can prove that a linear asymptotic behaviour is exhibited. We suspect that, possibly apart from a few well-understood infinite families, the size of the smallest non-self-separable subset is asymptotically proportional to the square root of the degree of the group. This intuition is captured by the following question.

Question 2.3. Does there exist a constant C such that, for the infinite class $\mathcal{C}^*_{\mathrm{pr}}$ of all primitive permutation groups apart from alternating and symmetric groups in their natural action,

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}^*_{\mathrm{pr}}}(n)}{\sqrt{n}} = C?$$

Natural candidates that might exhibit a different behaviour are primitive permutation groups of product action type whose socle is a direct product of alternating groups in their natural action (see Corollary N and Lemma 7.1). If the answer to Question 2.3 has a negative answer, then we still propose Problem B, already stated in Section 1, as a possible direction of investigation.

In view of this and the already established square-root lower bound (see Theorem C), we focus on obtaining upper bounds for $\mathrm{sep}(G)$, and thus avoiding the computation of $\mathbf{f}_{\mathcal{C}^*_{\mathrm{pr}}}(n)$. Let us consider the following example.

Example 2.4. Let $\mathrm{PSL}_d(q) \trianglelefteq G \leq \mathrm{P\Gamma L}_d(q)$ act on the projective space $\mathrm{PG}(d-1, q)$. To find an upper bound on $\mathrm{sep}(G)$, one needs to find a subset A of the projective space such that every image of A under a collineation always intersects A. An obvious candidate is a projective subspace of dimension at least

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

half of that of the ambient $\mathrm{PG}(d-1,q)$. In this case, we can check that if $d-1$ is even, we can take a subspace of dimension $(d-1)/2$, and we find that, for large n,

$$\mathrm{sep}(G) \leq \sqrt{n} + o(\sqrt{n}).$$

Otherwise, if $d-1$ is odd, we take a subspace of dimension $d/2$, and hence we find

$$\mathrm{sep}(G) \leq n^{\frac{d}{2(d-1)}} + o\left(n^{\frac{d}{2(d-1)}}\right).$$

This construction is not meaningful for $d = 2$, since in that case we cannot take any projective subspace apart from the line itself. In fact, we know very little of the behaviour of $\mathrm{sep}(G)$ where $G \leq \mathrm{Aut}(PG(1,q))$ and q is large. Furthermore, even for $d \geq 4$, the exponent $d/(2(d-1))$ is always larger than $1/2$ (though it converges to $1/2$ as d goes to infinity), suggesting that these groups might also provide a negative answer to Question 2.3. However, we believe that subsets distinct from subspaces might provide an example of a smaller non-self-separable set. It would be fascinating if some subgeometry A of $\mathrm{PG}(d-1,q)$ were not self-separable, but all the obvious candidates (such as ovoids or Galois subgeometries) seem to be self-separable or too large.

Similar reasoning can produce a large array of upper bounds for primitive groups of almost simple type in their standard action. As in [37], the term *standard actions* refers to permutation groups that are either alternating, symmetric, or classical, and, in the former two cases, the domain consists of k-subsets, while in the latter the groups are endowed with a *subspace action*. (For the list of subspace actions, we refer to [13, Chapter 4].)

Theorem K. *Let G be a primitive group of almost simple type in its standard action on the domain Ω. Then, an asymptotic upper bound for* $\mathrm{sep}(G)$ *can be found in the third column of Table 1.*

This theorem is proved in Section 8.1.

Remark 2.5. If $f, g : \mathbb{N} \to \mathbb{R}^+$ are two functions such that the limit of the quotient $\limsup f(n)/g(n)$ lies in the interval $[0,1]$, then we write $f \lesssim g$. Hence the expressions in the last column of Table 1 consist of the leading term of the asymptotic expansion of the cardinality of the non-self-separable subsets we construct in the proofs.

Observe that in the last column of Table 1 the symbols (♠) and (♣) appear. The first symbol (♠) appears every time the socle of the classical group into consideration is orthogonal and the action is on nondegenerate parabolic $(2k+1)$-subspaces. In this case, we have a precise value for the asymptotic upper bound computed, which can be read from Table 3. The symbol (♣) appears whenever we encounter the action of a classical group on totally isotropic or totally singular subspaces. Although we have an explicit upper bound for $\mathrm{sep}(G)$, which can be derived from Table 2, the expressions are so complicated that we cannot provide a precise asymptotic, even if aided by a calculator. Still, some experimentation with these functions shows that, if one fixes k and allows d to grow to infinity, the expected outcome is the asymptotic behaviour $\lesssim \sqrt{n}$.

Remark 2.6. For most standard actions, for a fixed even value of the parameter k in Table 1, we see that $\mathrm{sep}(G) \lesssim \sqrt{n}$. Hence, if the degree is large enough, we can expect $\mathrm{sep}(G)$ to be arbitrarily close to the lower bound given in Theorem C. For these actions, if k is odd, we note that, as k gets larger, the upper bound computed in Theorem K gets arbitrarily close to $\sqrt{n}$. Explicitly, if $s(k,n)$ is the first term of the asymptotic expansion of the upper bounds we have computed, then

$$\lim_k \frac{s(k,n)}{\sqrt{n}} = 1.$$

Let us now move on to the other types of primitive groups as described in the O'Nan–Scott Theorem [36]. In what follows, we adopt the partition into eight classes proposed in [49]. We will recall the properties of the classes we address in Section 8.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Table 1. *Upper bound for the standard actions of the primitive groups of almost simple type. The asymptotic notation and the symbols (♠) and (♣) are explained in Remark 2.5.*

	soc(G)	Domain Ω	sep$(G \curvearrowright \Omega)$
(a)	$\mathrm{Alt}(m)$	k-subsets	$\lesssim \frac{k!^{\frac{1}{k}\lceil\frac{k}{2}\rceil}}{\lceil\frac{k}{2}\rceil!} n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(b)	$\mathrm{PSL}_d(q)$	k-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(c)	$\mathrm{PSL}_d(q)$	pairs (X,Y) of subspaces in direct sum, with $\dim(X)=k$	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(d)	$\mathrm{PSL}_d(q)$	pairs (X,Y) of subspaces with $X \leq Y$, $\dim(X)=k$, $\dim(Y)=d-k$	$\lesssim n^{\frac{k\lceil\frac{d-3k}{2}\rceil+(d-k)\lceil\frac{k}{2}\rceil}{k(2d-3k)}}$
(e)	$\mathrm{PSU}_d(q)$	totally isotropic k-subspaces	$(\clubsuit)$
(f)	$\mathrm{PSU}_d(q)$	nondegenerate k-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(g)	$\mathrm{PSp}_{2d}(q)$	totally isotropic k-subspaces	$(\clubsuit)$
(h)	$\mathrm{PSp}_{2d}(q)$	nondegenerate $2k$-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(i)	$\mathrm{P}\Omega^+_{2d}(q)$	totally singular k-subspaces	$(\clubsuit)$
(j)	$\mathrm{P}\Omega^-_{2d}(q)$	totally singular k-subspaces	$(\clubsuit)$
(k)	$\Omega_{2d+1}(q)$	totally singular k-subspaces, q odd	$(\clubsuit)$
(l)	$\Omega^\epsilon_{2d}(q)$	nonsingular 1-subspaces, q even	$\leq \lfloor \frac{n}{2} \rfloor$
(m)	$\mathrm{P}\Omega^+_{2d}(q)$	nondegenerate hyperbolic $2k$-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(n)	$\mathrm{P}\Omega^+_{2d}(q)$	nondegenerate parabolic $(2k+1)$-subspaces, q odd	$(\spadesuit)$
(o)	$\mathrm{P}\Omega^+_{2d}(q)$	nondegenerate elliptic $2k$-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$
(p)	$\mathrm{P}\Omega^-_{2d}(q)$	nondegenerate parabolic $(2k+1)$-subspaces, q odd	$(\spadesuit)$
(q)	$\mathrm{P}\Omega^-_{2d}(q)$	nondegenerate elliptic $2k$-subspaces	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$
(r)	$\Omega_{2d+1}(q)$	nondegenerate hyperbolic $2k$-subspaces, q odd	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(s)	$\Omega_{2d+1}(q)$	nondegenerate elliptic $2k$-subspaces, q odd	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$

We start with primitive permutation groups of simple diagonal type.

Theorem L. *Let G be a quasiprimitive permutation group of simple diagonal type, let $k \geq 3$ be the number of direct simple factors of its socle, and let ε be* 1 *if the socle type is a group of Lie type, and* 0 *otherwise. Then,*

$$\mathrm{sep}(G) \leq 4\left(\frac{16}{3}\right)^{\frac{k-1}{2}} n^{\frac{1}{2}+\frac{1}{k-1}} \left(\frac{1}{4k}\log_2 n\right)^{\epsilon}.$$

In particular, if $\mathcal{C}$ is the family of all quasiprimitive groups of simple diagonal type, then

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}}(n)}{n^{\frac{1}{2}+\frac{1}{k-1}}\log_2(n)} \leq \frac{1}{k}\left(\frac{16}{3}\right)^{\frac{k-1}{2}}.$$

The proof of Theorem L, provided in Section 8.2, also holds for primitive permutation groups of type holomorph of simple and holomorph of compound, but in these cases the resulting upper bound for $\mathrm{sep}(G)$ is meaningless as it exceeds n. We leave all the holomorph types out of our analysis.

We now concentrate on primitive groups of product action type and of compound diagonal type. They can be described as being the output of the construction of a primitive wreath product applied to almost simple and simple diagonal types, respectively. This fact inspired us to obtain the following general theorem (proved in Section 3.2).

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Theorem M. *Let $G \leq H$ wr K be a permutation group in product action on the domain $\Omega = \mathrm{Fun}(\Gamma, \Delta)$. Then,*

$$\mathrm{sep}(G) \leq \mathrm{sep}(H)^{|\Gamma|}.$$

Therefore, we obtain these corollaries immediately, assuming Question 2.3 holds for primitive permutation groups of almost simple type and primitive permutation groups of simple diagonal type, respectively.

Corollary N. *Suppose that there exists a constant C such that, for the class $\mathcal{C}^*_{\mathrm{as}}$ of all the primitive permutation groups of almost simple type of nonalternating socle we have*

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}^*_{\mathrm{pr}}}(n)}{\sqrt{n}} = C.$$

Then, for the infinite class $\mathcal{C}^*_{\mathrm{pa}}$ of all primitive permutation groups of type product action whose socle is not isomorphic to a direct product of alternating groups,

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}^*_{\mathrm{pa}}}(n)}{\sqrt{n}} \leq C.$$

Corollary O. *Suppose that there exists a constant C such that, for the class $\mathcal{C}_{\mathrm{sd}}$ of all the primitive permutation groups of type simple diagonal type we have*

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}^*_{\mathrm{pr}}}(n)}{\sqrt{n}} = C.$$

Then, for the infinite class $\mathcal{C}_{\mathrm{cd}}$ of all primitive permutation groups of type compound diagonal,

$$\limsup_n \frac{\mathbf{F}_{\mathcal{C}_{\mathrm{cd}}}(n)}{\sqrt{n}} \leq C.$$

This concludes the extended summary of our work, while the rest of the paper is devoted to the proofs.

3. Properties of $\mathrm{sep}(G)$

In this section, we investigate the monotonicity of $\mathrm{sep}(G)$, $\mathbf{f}_{\mathcal{C}}(n)$, and $\mathbf{F}_{\mathcal{C}}(n)$ under certain natural operations applied either to the group G or to the family $\mathcal{C}$.

3.1. Monotonicity with respect to subgroups and subfamilies

Recall that $\mathcal{C}$ is an infinite family of transitive permutation groups, and that $\mathcal{C}_n$ is the subfamily of permutation groups of degree n.

Observe that, for every $G \in \mathcal{C}_n$, every subset A of the domain of G satisfying $|A| < \mathbf{f}_{\mathcal{C}}(n) \leq \mathrm{sep}(G)$ is self-separable for G by definition. Therefore, to find a lower bound $a(n)+1$ for $\mathbf{f}_{\mathcal{C}}(n)$, we need to prove that, for all $G \in \mathcal{C}_n$ and for every subset A in the domain of G such that $|A| \leq a(n)$, A is self-separable for G. Similarly, every subset A of the domain of G with the property that $|A| \geq \mathbf{F}_{\mathcal{C}}(n) \geq \mathrm{sep}(G)$ is not self-separable. Hence, to find an upper bound $b(n)+1$ for $\mathbf{F}_{\mathcal{C}}(n)$, we need to prove that, for all $G \in \mathcal{C}_n$, there exists a subset A in the domain of G such that $|A| \geq b(n)$ and A is not self-separable for G, that is, for every $g \in G$, we can prove that $|A \cap A^g| \geq 1$.

Lemma 3.1. *Let $H \leq G$ be two transitive permutation groups. Then*

$$\mathrm{sep}(H) \leq \mathrm{sep}(G).$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Proof. Let A be a set such that $|A| \leq \mathrm{sep}(H)$. By definition of $\mathrm{sep}(H)$, there exists a permutation $h \in H$ such that $A \cap A^h$ is empty. Since $h \in G$, the bound follows. □

Finally, recall from Remark 1.3 that for families $\mathcal{D} \subseteq \mathcal{C}$ and for every positive integer $n \in X_{\mathcal{C}}$,

$$\mathbf{f}_{\mathcal{C}}(n) \leq \mathbf{f}_{\mathcal{D}}(n) \leq \mathbf{F}_{\mathcal{D}}(n) \leq \mathbf{F}_{\mathcal{C}}(n).$$

3.2. *Monotonicity with respect to quotients and extensions*

Let G be a transitive permutation group on Ω, let N be a normal subgroup of G, and let $G \curvearrowright \Omega/N$ be the permutation induced by the natural action of G on the orbit-space

$$\Omega/N = \left\{\omega^N \mid \omega \in \Omega\right\}.$$

Lemma 3.2. *Let G be a transitive permutation group on Ω, and let N be a normal subgroup of G. Then*

$$\mathrm{sep}(G) \geq \mathrm{sep}(G \curvearrowright \Omega/N).$$

Proof. Let A be a subset of Ω such that $|A| \leq \mathrm{sep}(G \curvearrowright \Omega/N) - 1$. Then A^N is a subset of Ω/N such that $|A^N| \leq \mathrm{sep}(G \curvearrowright \Omega/N) - 1$. Hence, there exists $g \in G$ such that $A^N \cap (A^N)^g$ is empty. Therefore, A is self-separable for G, which proves the lemma. □

In the case of permutation groups, we focus on examining how the parameter of interest relates between a wreath product $H \operatorname{wr} K$ and its constituents H and K. We start with the imprimitive action for $H \operatorname{wr} K$. Explicitly, if Δ is the domain of H and Γ of K, $H \operatorname{wr} K$ acts on the Cartesian product $\Delta \times \Gamma$ by

$$(\delta, \gamma)^{(h_1, h_2, \ldots, h_{|\Gamma|})k} = (\delta^{h_\gamma}, \gamma^k),$$

where $\delta \in \Delta$, $\gamma \in \Gamma$, $(h_1, h_2, \ldots, h_{|\Gamma|}) \in \mathrm{Fun}(\Gamma, H)$, and $k \in K$. (Recall that $\mathrm{Fun}(\Gamma, H)$ is the group of functions from Γ to H, and it can be identified with the $|\Gamma|$-fold direct product $H^{|\Gamma|}$.)

Proof of Theorem I. Let G be a transitive permutation group that embeds in $H \operatorname{wr} K$ with imprimitive action, acting on $\Delta \times \Gamma$ as described above. For each element of $\gamma \in \Gamma$, we will use the notation $\Delta^\gamma = \{(\delta, \gamma) | \delta \in \Delta\}$. Note that the set of disjoint copies of Δ forms a block system for G, and we will refer to these copies as blocks in the proof.

We start by proving the lower bound. Let A be any set of points of size $\mathrm{sep}(H) + \mathrm{sep}(K) - 2$. Either there exists $\gamma \in \Gamma$ such that $A^\gamma \cap A \geq \mathrm{sep}(H)$ points or not. If the latter holds, then there is an element g of the base group $\mathrm{Fun}(\Gamma, H)$, such that A and A^g intersect trivially. On the other hand, if there is such γ, then A has a nontrivial intersection with at most $\mathrm{sep}(K) - 1 < \frac{|\Gamma|}{2}$ copies of Δ, hence there exists an element $g \in K$ from the top group that maps the blocks intersecting A to blocks that do not. In any case, we are able to find a permutation g such that $A \cap A^g$ is empty, and hence every set of size $\mathrm{sep}(H) + \mathrm{sep}(K) - 2$ is self-separable for G. The lower bound immediately follows.

For the upper bound, consider a subset of points

$$A = \{(x, y) \mid x \in X \subseteq \Delta, y \in Y \subseteq \Gamma, 1 \leq |X| \leq \mathrm{sep}(H),\ 1 \leq |Y| \leq \mathrm{sep}(K)\},$$

where we identified the domain of G with the Cartesian product $\Delta \times \Gamma$. By the definition of $\mathrm{sep}(H)$ and $\mathrm{sep}(K)$, it follows that, for every $g \in G$, $|A \cap A^g| \geq 1$. This is enough to prove the upper bound. □

Now, we focus on wreath products in product action. The wreath product $H \operatorname{wr} K$ can be endowed with an action on $\mathrm{Fun}(\Gamma, \Delta)$, which we understand as the $|\Gamma|$-fold Cartesian power of Δ. Indeed, for every $g = (h_1, h_2, \ldots, h_{|\Gamma|})k \in H \operatorname{wr} K$, for every $f \in \mathrm{Fun}(\Gamma, \Delta)$ and for every $\gamma \in \Gamma$, we let

$$f^g(\gamma) = f\left(k^{-1}\gamma\right)^{h_{k^{-1}\gamma}}.$$

(For ease of reading, we are denoting the action of K on Γ as left multiplication.)

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Proof of Theorem M. Let $R \subseteq \Delta$ be a subset with $|R| = \mathrm{sep}(H)$. Hence, for every $h \in H$, $R \cap R^h$ is not empty, and consider

$$A = \mathrm{Fun}(\Gamma, R) = \{f \in \mathrm{Fun}(\Gamma, \Delta) \mid f(\gamma) \in R\} \forall \gamma \in \Gamma.$$

For every $g = (h_1, h_2, \ldots, h_{|\Gamma|})k \in H \operatorname{wr} K$, every $f \in A$ and every $\gamma \in \Gamma$, we see that

$$f^g(\gamma) = f\left(k^{-1}\gamma\right)^{h_{k^{-1}\gamma}} \in R^{h_{\gamma k^{-1}}}.$$

We now observe that

$$A \cap A^g = \mathrm{Fun}(\Gamma, R) \cap \left(R^{h_{1k^{-1}}} \times R^{h_{2k^{-1}}} \times \ldots \times R^{h_{|\Gamma|k^{-1}}}\right)$$

is not empty due to the choice of R. In particular, by applying Lemma 3.1, we obtain that

$$\mathrm{sep}(G) \leq \mathrm{sep}(H)^{|\Gamma|}.$$

□

3.3. Monotonicity with respect to change of action

We complete the section by establishing a connection between the self-separability parameter for two different actions of the same abstract group.

Lemma 3.3. *Let G be an abstract group, and let H and K be two core-free subgroups of G with $H \leq K$. Then*

$$\frac{\mathrm{sep}(G \curvearrowright G/H)}{|K : H|} \leq \mathrm{sep}(G \curvearrowright G/K) \leq \mathrm{sep}(G \curvearrowright G/H).$$

Proof. Let m be a positive integer such that $m \leq \mathrm{sep}(G \curvearrowright G/K) - 1$, and let A be an m-subset of G/H, say

$$A = \{Ha_1, Ha_2, \ldots, Ha_m\}.$$

Without loss of generality, we can define

$$A' = \{Ka_1, Ka_2, \ldots, Ka_k\},$$

such that for all $i' \in \{1, 2, \ldots, m\}$, there exists $i \in \{1, 2, \ldots, k\}$ such that $Ha_{i'} \subset Ka_i$. Now A' is a k-subset of G/K, for some $k \leq m$. By our choice of m, there exists a group element $g \in G$ such that $A' \cap A'g$ is empty, or, more explicitly, such that

$$\left(\bigcup_{i=1}^{k} Ka_i g\right) \cap \left(\bigcup_{j=1}^{k} Ka_j\right) \quad \text{is empty}.$$

Since, for every $i' \in \{1, 2, \ldots, m\}$, there exists $i \in \{1, 2, \ldots, k\}$ such that $Ha_{i'} \subset Ka_i$, and since the right multiplication by g is a bijection on G/H, it follows that

$$\left(\bigcup_{i=1}^{m} Ha_i g\right) \cap \left(\bigcup_{j=1}^{m} Ha_j\right) \quad \text{is empty}.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

In particular,

$$m \leq \mathrm{sep}(G \curvearrowright G/H) - 1,$$

and, by taking the maximum on both sides, we establish the upper bound for $\mathrm{sep}(G \curvearrowright G/K)$.

Let now h be a positive integer such that $h \geq \mathrm{sep}(G \curvearrowright G/K)$, and let B be a h-subset of G/K, say

$$B = \{Kb_1, Kb_2, \ldots, Kb_h\}.$$

Let $\{k_1, k_2, \ldots, k_{|K:H|}\}$ be a set of representatives for the right cosets of H in K, and consider

$$B' = \{Hk_1b_1, Hk_1b_2, \ldots, Hk_1b_m, Hk_2b_1, \ldots, Hk_{|K:H|}b_h\}.$$

Observe that $|B'| = h|K : H|$, and that

$$\bigcup_{i=1}^{h} Kb_i = \bigcup_{i=1}^{h} \left(\bigcup_{j=1}^{|K:H|} Hk_jb_i \right).$$

Since B is not self-separable for G, the previous equality implies that B' is not self-separable for G. Therefore,

$$h|K : H| \geq \mathrm{sep}(G \curvearrowright G/H).$$

By taking the minimum on both sides, we obtain the desired lower bound.

Hence, the proof of Lemma 3.3 is complete. □

We would like to point out that Lemma 3.3 is quite weak in a general setting. For instance, consider the symmetric group $\mathrm{Sym}(n)$ in its natural action (that is, with stabiliser $\mathrm{Sym}(n-1)$) and in its regular action (that is, with a trivial stabiliser). Then, applying the upper bounds from Lemma 3.3 and Theorem F, we deduce that

$$\mathrm{sep}(\mathrm{Sym}(n) \curvearrowright [n]) \leq \mathrm{sep}(\mathrm{Sym}(n) \curvearrowright \mathrm{Sym}(n)) \leq \frac{4}{\sqrt{3}}\sqrt{n!}\,.$$

The upper bound is comically ineffective, as the domain of $\mathrm{Sym}(n) \curvearrowright [n]$ contains only n points. This is caused by the fact that the order of the stabiliser $\mathrm{Sym}(n-1)$ is enormous.

On the other hand, if the index $|K : H|$ can be bounded by a constant, Lemma 3.3 can produce significant estimates. (For two functions $f, g : \mathbb{N} \to \mathbb{R}^+$, we write $f \asymp g$ if there exists a positive integer M and a positive constant C such that, for every $n \geq M$, their quotient $f(n)/g(n)$ is positive and bounded from above by C.)

Lemma 3.4. *Let $\mathcal{C}$ and $\mathcal{D}$ be two families of permutation groups such that, for every abstract group G, if G appears in $\mathcal{C}$ with stabiliser K, then G appears in $\mathcal{D}$ with stabiliser H. Suppose that there is a constant d such that, for every G, $|K : H| \leq d$. Then*

$$\mathbf{f}_{\mathcal{C}} \asymp \mathbf{f}_{\mathcal{D}} \quad \textit{and} \quad \mathbf{F}_{\mathcal{C}} \asymp \mathbf{F}_{\mathcal{D}}.$$

Proof. The claimed results are obtained by taking the minimum and the maximum of the inequalities from Lemma 3.3 and observing that a linear dilatation of the argument of the function does not change the asymptotic behaviour. □

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

4. Proof of Theorem C

We give a proof of Neumann's separation lemma (see [10, 47] for the seminal version of this result, and [3, Theorem 5.3] for our version), and we derive the lower bound in Theorem C as a corollary.

Lemma 4.1. *Let G be a transitive permutation group on Ω, and let A and B be two subsets of Ω. Then*

$$\frac{1}{|G|}\sum_{g\in G}|A\cap B^g| = \frac{|A||B|}{|\Omega|}.$$

Proof. We define the set

$$X = \{(\alpha,\beta,g)\in\Omega\times\Omega\times G \mid \alpha\in A,\beta\in B,\alpha=\beta^g\}.$$

For every $\alpha,\beta\in\Omega$, the set of elements $g\in G$ satisfying $\alpha=\beta^g$ is a right coset of the stabiliser G_α. Therefore,

$$|X| = |A||B||G_\alpha| = \frac{|A||B||G|}{|\Omega|}. \tag{4.1}$$

On the other hand, for every g, we can count the number of pairs (α,β) such that $\alpha=\beta^g$, which is equal to $|A\cap B^g|$. Hence,

$$|X| = \sum_{g\in G}|A\cap B^g|. \tag{4.2}$$

The result is obtained by equating Eqs. (4.1) and (4.2). □

Proof of Theorem C. Let G be a transitive permutation group on Ω of degree n, and let A be a subset of Ω. By Lemma 4.1, we have

$$\frac{1}{|G|}\sum_{g\in G}|A\cap A^g| = \frac{|A|^2}{n}. \tag{4.3}$$

If there does not exist $g\in G$ such that $A\cap A^g$ is empty, then

$$\frac{1}{|G|}\sum_{g\in G}|A\cap A^g| \geq \frac{1}{|G|}\sum_{g\in G\setminus\{1\}}1+\frac{|A|}{|G|} = 1+\frac{|A|-1}{|G|},$$

where equality is attained if and only if $|A\cap A^g|=1$ for every nontrivial $g\in G$.

By (4.3), we also see that

$$\frac{|A|^2}{n}\geq 1+\frac{|A|-1}{|G|},$$

and thus solving the quadratic inequality gives

$$|A|\geq\frac{1+\sqrt{1-4|G|(1-|G|)/n}}{2|G|/n} = \frac{1}{2|G_\alpha|}+\sqrt{n-\frac{1}{|G_\alpha|}+\frac{1}{4|G_\alpha|^2}}.$$

Let us denote the expression on the right-hand side by $\alpha(G)$. We have shown that, if a subset A is not self-separable for G, its size needs to be at least $\alpha(G)$. Therefore, $\mathrm{sep}(G)\geq\alpha(G)$, as required.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Now, we shall prove that the lower bound is met if and only if Ω is the point-set of a projective plane and G is a regular group on Ω. Let

$$A^G = \{A^g \mid g \in G\},$$

and consider the incidence structure (or design) (A^G, Ω), where A^g is incident with ω if $\omega \in A^g$. Observe that G preserves this incidence relation.

Recall that, if $|A| = \alpha(G)$, then $|A \cap A^g| = 1$ for every nontrivial permutation $g \in G$. Thus, the set-wise stabiliser G_A of A is trivial, and hence the action of G is regular on A^G. The transitivity of G on Ω and A^G gives us that (A^G, Ω) is uniform and regular. Clearly, the design is incomplete, and the hypothesis that, for $g \in G \setminus \{1\}$ $|A \cap A^g| = 1$ implies that it is balanced. Therefore, (A^G, Ω) is a balanced incomplete block design, and we can apply Fisher's inequality. Doing so, we obtain

$$|G| = |A^G| \leq |\Omega| = n.$$

Therefore, G is regular on Ω, and hence the design is symmetric. Using our hypothesis on the intersections of sets in A^G, (A^G, Ω) is a projective plane, and so is its dual (Ω, A^G). □

We would like to note here that, if G acts regularly on a nondegenerate projective plane of order q, then the right-hand side of Inequality (2.1) in Theorem C is an integer. In fact,

$$\alpha(G) = \frac{1}{2} + \sqrt{q^2 + q + 1 - 1 + \frac{1}{4}} = \frac{1}{2} + \sqrt{\left(q + \frac{1}{2}\right)^2} = q + 1.$$

Furthermore, we observe that the equality can hold if and only if such right-hand side is an integer, which in turn happens if and only if n is of the form $n = (m|\alpha|)^2 + (2|G_\alpha| - 1)m + 1$ for some positive integer m. When the right-hand side is not an integer, then the lower bound for $\mathrm{sep}(G)$ can be improved by taking the ceiling of that value. This makes us pose the following:

Question 4.2. Does there exist a transitive permutation group G of degree n not of the form $(m|G_\alpha|)^2 + (2|G_\alpha| - 1)m + 1$ for any $m \in \mathbb{N}$ such that

$$\mathrm{sep}(G) = \left\lceil \left(\frac{1}{2|G_\alpha|} + \sqrt{n - \frac{1}{|G_\alpha|} + \frac{1}{4|G_\alpha|^2}} \right) \right\rceil ?$$

If not, how can the bound in Theorem C be improved in this case?

5. Proof of Theorem F

We start this section by focusing our attention on groups acting regularly. Then, we will generalise our result on regular groups to families of permutation groups with stabilisers of bounded order.

Remark 5.1. Let G be a regular permutation group of degree n on Ω. As usual, we identify G with Ω, so that the action we are dealing with is the action of G on itself by right multiplication. Let A be a subset of G. Suppose that there is a $g \in G$ such that $A \cap Ag$ is empty. Then g is not an element of $A^{-1}A$, and thus $A^{-1}A$ is a proper subset of G. On the other hand, if $A \cap Ag$ is nonempty for every $g \in G$, then $A^{-1}A = G$. Therefore, A is not self-separable if and only if A^{-1} is a difference basis (see Definition 2.1). Hence, $\mathrm{sep}(G)$ is the size of the smallest difference basis for G.

A notion closely related to that of difference basis appears in additive combinatorics, introduced in [52] by Rédei and Rényi, where they consider subsets $A \subseteq \mathbb{Z}$ such that the difference set $A - A$ covers the finite subset $\{0, 1, 2, \ldots, n\}$. The problem of constructing such sets A of minimal possible size remains a relevant question in additive number theory (see, for instance, [8, 57]).

These ideas also intersect naturally with classical topics in combinatorics and finite geometry. For instance, *planar difference sets* are difference bases $A \subseteq G$ with the additional property that, for every

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

$g \in G$, there exists a unique pair $(a, b) \in A^2$ such that $g = ab^{-1}$. Such sets play a fundamental role in the construction of finite projective planes. In particular, in his seminal work [59], Singer showed that every finite projective plane admits a cyclic collineation group of order equal to the number of its points. Observe that this fact is directly connected to the sharpness of the lower bound in Theorem C.

Another related concept is that of a *basis for a group* G: a subset $A \subseteq G$ such that $A^2 = G$. If A is inverse-closed, then the notions of basis and difference basis coincide. This concept originates with Rohrbach [54], and has since been developed further in [9, 33, 43]. We would like to note that, as observed in [38], the existence of small bases is related to the *degree-diameter problem* for Cayley graphs of diameter 2.

The cardinality of a minimal difference basis is bounded below by the size of a minimal difference set, and an upper bound of $3\sqrt{|G|}$ is given in [34]. Determining the exact minimal size of a difference basis remains an active area of research, even for specific families of groups (see [4, 5, 6]). Any improvement to these bounds would lead to immediate improvements in the asymptotic estimates computed in Theorem F. For example, for any finite Abelian p-group G in its regular right action, where p is a prime with $p \geq 11$, the result of [6] implies that

$$\operatorname{sep}(G) < \frac{\sqrt{2}(\sqrt{p}-1)}{\sqrt{p}-3}\sqrt{|G|}.$$

Proof of Theorem F. Let G be a finite group, and suppose that G acts regularly on itself by right multiplication. By Remark 5.1, we need to build a difference basis A for G of as small size as possible. By [33, Theorem 1], there exist two positive constants c_1 and c_2 and two subsets B and C such that

$$|B| = c_1\sqrt{|G|}, \quad |C| = c_2\sqrt{|G|}, \quad c_1 + c_2 \leq 4/\sqrt{3}, \quad BC = G.$$

Hence, the subset $A = B \cup C^{-1}$ is a difference basis containing at most $4\sqrt{|G|}/\sqrt{3}$ elements. Indeed,

$$AA^{-1} \subseteq G = BC \subseteq (B \cup C^{-1})(B^{-1} \cup C) = AA^{-1}.$$

Therefore,

$$\operatorname{sep}(G) \leq \frac{4}{\sqrt{3}}\sqrt{|G|}.$$

Now we can compute the limit for $\mathbf{f}_C(n)$ using Theorem C and the bound for the limit for $\mathbf{F}_C(n)$ follows immediately. □

Surprisingly, [33, Theorem 1] relies on the fact that every group which is not cyclic of prime order contains a proper subgroup H whose order exceeds $|G|^{1/2}$ (see [35] for a proof of this fact), which in turn relies on the classification of finite simple groups. In a classification free context, if G has even order, the best result known is that there exists a subgroup H with $|H| \geq |G|^{1/3}$, as the famous result of Brauer and Fowler in [12] states. On the other hand, if G is of odd order, then, by the Feit–Thompson Theorem [22], G is solvable, and solvability is enough to prove the existence of a subgroup of order exceeding the square root of the order of the group.

We can reproduce the proof of [33, Theorem 1] under the additional assumption that all groups involved are solvable. In this setting the argument no longer relies on the classification of finite simple groups, and it still yields the same constant $4/\sqrt{3}$, which is sharp for the cyclic group C_3. Hence, Theorem F remains valid for solvable groups in the classification-free context. This prompts us to ask the following question.

Question 5.2. Without using the classification of finite simple groups, can we find a function $\mathbf{g} : \mathbb{N} \to \mathbb{R}$ such that, for every nonsolvable regular permutation group G of order n,

$$\operatorname{sep}(G) \leq \mathbf{g}(n)?$$

We now turn our attention to families of transitive permutation groups whose stabilisers are bounded.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Remark 5.3. Observe that, by applying Lemma 3.4 with $\mathcal{D}$ equal to the family of regular permutation groups, we obtain that, for every $\mathcal{C}$ family of transitive permutation groups with stabilisers of bounded order,

$$\mathbf{f}_{\mathcal{C}} \asymp \mathbf{F}_{\mathcal{C}} \asymp \sqrt{n}.$$

Actually, since we have an explicit upper bound for $\mathbf{f}_D$ and $\mathbf{F}_{\mathcal{D}}$, an immediate computation shows that, if $\mathbf{c}$ is the maximum order of a stabiliser in $\mathcal{C}$, then

$$\sqrt{n} \leq \mathbf{f}_{\mathcal{C}}(n) \leq \mathbf{F}_{\mathcal{C}}(n) \leq 4\sqrt{\frac{\mathbf{c}n}{3}}.$$

We do not focus on this precise upper bound because, for the following application, the precise value of $\mathbf{c}$ is not known.

Proof of Corollary G. We want to apply Lemma 3.4 to the families

$$\mathcal{C}_d = \{G \mid G \text{ is a primitive permutation group with minimal subdegree } d\},$$
$$\mathcal{D} = \{G \mid G \text{ is regular and it appears as an abstract group in } \mathcal{C}\}.$$

By the positive solution to Sims's Conjecture in [17], there exists a function $\mathbf{g}$ such that the order of any stabiliser of a permutation group in $\mathcal{C}_d$ is at most $\mathbf{g}(d)$. Therefore, combining Theorems C and F with Remark 5.3, we find that there exists a constant $\mathbf{c}(d) > 0$ such that

$$\sqrt{n} \leq \mathbf{f}_{\mathcal{C}_d}(n) \leq \mathbf{F}_{\mathcal{C}_d}(n) \leq \mathbf{c}(d)\sqrt{n}.$$

The claims of Corollary G immediately follow. □

The proof of Corollary H follows *verbatim* that of Corollary G, where $\mathcal{C}$ is the family of G which are 2-arc-transitive groups of automorphisms of some graphs Γ, whose valency does not exceed d, and the positive solution to Sims's Conjecture is substituted with the positive solution to Weiss's Conjecture for 2-arc-transitive graphs obtained in [26, 62, 63, 65, 66].

This result can actually be generalised to a larger class of automorphism groups of graphs. Given a graph Γ and a vertex-transitive group of automorphisms G, the *local group L of the pair* (Γ, G) is the permutation group that a vertex-stabiliser induces on the neighbourhood of its fixed point. A permutation group L is *graph-restrictive* if there exists a constant such that, for every pair (Γ, G) that witnesses L as a local group, then the order of a vertex-stabiliser is bounded by this constant. For instance, the property we have used above is that 2-transitive permutation groups are graph-restrictive. Therefore, our proof actually extends beyond the scope of Corollary H. For instance, in [19], it is conjectured that any *semiprimitive* permutation group is graph-restrictive. For the curious reader, examples of graph-restrictive permutation groups can be found in [28, 29, 40, 41, 60, 64].

6. Proof of Theorem J

As stated in the introduction, to discuss the sharpness of the bounds in Theorem I we need to understand $\mathrm{sep}(\mathrm{Sym}(a) \operatorname{wr} \mathrm{Sym}(b))$, where the wreath product of symmetric groups is endowed with its imprimitive action.

Proof of Theorem J. Let $G = \mathrm{Sym}(a) \operatorname{wr} \mathrm{Sym}(b)$, and let Σ be its block system. We denote by $B_1, \dots, B_b$ the blocks of Σ. First, we show that $\mathrm{sep}(G) \leq a + b - 1$. Consider any subset of the domain of the form

$$A = B_1 \cup \{\omega_2\} \cup \cdots \cup \{\omega_b\},$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

where $\omega_i \in B_b$ for $2 \le i \le a$. Note that $|A| = a + b - 1$. Observe that, for every permutation $g \in G$, the set A^g contains the block B_1^g, and, as A intersects every block in at least one point, A and A^g have nonempty intersection. Hence, A is not self-separable for G, and the claim follows.

From here on, the proof is divided into multiple cases. First, we prove by induction on b that, if b is even or if $b \ge 5$ is odd and $a \ne 3$, then $\mathrm{sep}(G) = a + b - 1$. The cases with a or b equal to 3 are delicate, hence we need to treat them separately.

Assume that b is even. Let A be a subset of $[a] \times [b]$ of size not exceeding $a + b - 2$. Our base case is $b = 2$. Let $\ell = |A \cap B_1|$, and note that $|A \cap B_2| \le a - \ell$. Now by a-transitivity of $\mathrm{Sym}(a)$, there exists $g \in \mathrm{Sym}(a) \,\mathrm{wr}\, C_2$ that switches the blocks B_1 and B_2 such that $A \cap B_1 \cap (A \cap B_2)^g$ and $A \cap B_2 \cap (A \cap B_1)^g$ are both empty. Thus, A and A^g have trivial intersection, and A is self-separable for G.

Now, assume that the property holds for b, and we claim that it also holds for $b + 2$. We again have two cases to consider.

If there does not exist a block $B \in \Sigma$, such that $|B \cap A| \ge \lceil (a+1)/2 \rceil$, then, there exists an element g of the base group $\mathrm{Sym}(a)^b$ such that, for every $B \in \Sigma$, $|A \cap B \cap (A \cap B)^g| = 0$. Therefore, A is self-separable for G.

Otherwise, without loss of generality, we suppose that $|B_1 \cap A| = \ell \ge \lceil (a+1)/2 \rceil$. We aim to prove the existence of a block $B \in \Sigma$ such that $|B \cap A| \le a - \ell$. Aiming for a contradiction, we assume that, for every $2 \le i \le a$, $|B_i \cap A| \ge a - \ell + 1$. We compute

$$\begin{aligned} |A| &= \sum_{B_i \in \Sigma} |B_i \cap A| \\ &\ge \ell + (b-1)(a - \ell + 1) \\ &= (b-1)(a+1) - \ell(b-2) \\ &\ge (b-1)(a+1) - a(b-2) \\ &= a + b - 1. \end{aligned}$$

This goes against the assumption that $|A| \le a + b - 2$. Therefore, without loss of generality, we can assume that $|B_2 \cap A| \le a - \ell$. We define

$$A_0 = A \cap (B_1 \cap B_2) \quad \text{and} \quad A_1 = A \cap \left(\bigcup_{i=3}^{b} B_i \right),$$

and we observe that $|A_0| \le a$ and that $|A_1| \le a + b - \ell - 2 \le a + b - 4$. We can apply the inductive hypothesis on the pairs $(A_0, \mathrm{Sym}(a) \,\mathrm{wr}\, C_2)$ and $(A_1, \mathrm{Sym}(a) \,\mathrm{wr}\, \mathrm{Sym}(b-2))$, thus obtaining that there exists a permutation $g \in (\mathrm{Sym}(a) \,\mathrm{wr}\, C_2) \times (\mathrm{Sym}(a) \,\mathrm{wr}\, \mathrm{Sym}(b-2)) \le \mathrm{Sym}(a) \,\mathrm{wr}\, \mathrm{Sym}(b)$ such that $A \cap A^g$ is empty. Hence, A is self-separable for G, and the proof of this case is complete.

Assume that $b \ge 5$ is odd and that $a \ne 3$. Let A be a subset of $[a] \times [b]$ of size not exceeding $a + b - 2$. By the restraint on b, our base case is $b = 5$. We claim that $|A \cap B_i| > a/2$ cannot happen for three blocks at once. Without loss of generality, assume we have $|A \cap B_i| > a/2$ for $i = 1, 2$, and 3. Then

$$|A \cap (B_1 \cup B_2 \cup B_3)| \ge 3 \left\lceil \frac{a+1}{2} \right\rceil \ge a + \frac{7}{2}.$$

(Observe that the last inequality does not hold if $a = 3$.) This contradicts the assumption that $|A| \le a + b - 2 = a + 3$. Hence, the number of blocks containing more than $a/2$ points is at most 2.

There are three cases to consider, corresponding to the number of blocks with $|A \cap B_i| > a/2$.

If there are no such blocks, we can find a permutation g of the base group such that $A \cap A^g$ is empty, as we did for the case $b = 2$. Suppose now that there exists exactly one block for which its intersection with A contains more than $a/2$ points, and, without loss of generality, we assume that this block is B_1, and we let $\ell = |B_1 \cap A|$. We aim to show that then there exists a block B_i for which $|B_i \cap A| \le b - \ell$.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Suppose for a contradiction that, for every $2 \leq i \leq 5$, $|B_i \cap A| \geq a - \ell + 1$. Then

$$\begin{aligned} |A| &= \sum_{B_i \in \Sigma} |B_i \cap A| \\ &\geq \ell + 4(a - \ell + 1) \\ &= 4a - 3\ell + 4 \\ &\geq a + 4. \end{aligned}$$

contradicting the cardinality assumption on A. So, without loss of generality, $|B_2 \cap A| \leq a - \ell$. Hence, reasoning as in the previous base case, we see that there exists an element g such that g stabilises the blocks B_3, B_4, and B_5, it swaps the blocks B_1 and B_2 and $A \cap A^g$ is empty. A similar argument can be carried out to deal with the remaining case. Henceforth, we have proved that every subset A containing less than $a + 4$ points is self-separable for $\mathrm{Sym}(a)$ wr $\mathrm{Sym}(5)$ (and $a \neq 3$).

The inductive step for b odd (and $a \neq 3$) is similar to the one we used for b even.

Assume that $b = 3$ and a is odd. We first show that $\mathrm{sep}(G) \leq a + b - 2 = a + 1$. Indeed, we choose A so that

$$|B_1 \cap A| = |B_2 \cap A| = \frac{a+1}{2}.$$

Then, for every $g \in G$, A^g and A will intersect B_1 or B_2 in at least one point. Hence A is not self-separable. Our objective is to show that every set A whose cardinality is at most a is self-separable for $\mathrm{Sym}(a)$ wr $\mathrm{Sym}(3)$.

Let A be a set of cardinality a. Then either $|B_i \cap A| < (a+1)/2$ for all $i \in \{1, 2, 3\}$, or, up to permuting the indices of the blocks, $|B_1 \cap A| \geq (a+1)/2$. In the latter case, since $|B_1 \cap A| + |B_2 \cap A| + |B_3 \cap A| = a$, we can assume that $|B_2 \cap A| \leq a - \ell$, and that $|B_3 \cap A| \leq (a + 1)/2$.

Using our usual arguments, our claim implies that there exists a permutation $g \in \mathrm{Sym}(a)$ wr $\mathrm{Sym}(3)$ such that g swaps the blocks B_1 and B_2, fixes B_3, and $A \cap A^g$ is empty. Therefore, we established the theorem in this setting.

Assume that $b = 3$ and a is even. Let A be a subset of cardinality at most $a + 1$. We can deal with the case with every block containing less than $a/2$ points as usual. Hence, without loss of generality, we suppose that $|B_1 \cap A| = \ell \geq a/2 + 1$. It cannot be that both $|B_2 \cap A| \geq a - \ell + 1$ and $|B_2 \cap A| \geq a - \ell + 1$, as that would imply that

$$|A| \geq \sum_{B_i \in \Sigma} |A \cap B_i| = \ell + 2(a - \ell + 1) \geq a + 2,$$

contradicting the cardinality assumption on A. Without loss of generality, we have that $|A \cap B_2| \leq a - \ell$. Therefore, there exists a permutation g fixing B_3 and swapping B_1 and B_2 such that $A \cap A^g$ is trivial. Thus, A is self-separable for $\mathrm{Sym}(a)$ wr $\mathrm{Sym}(3)$, and the desired equality follows.

Assume that b is odd and $a = 3$. Observe that, in this setting, there exists a set of size $b + 1$ which is not self-separable. Indeed, let A be a subset of $[a] \times [b]$ such that, for every $i \leq \lceil (b + 1)/2 \rceil$, $|A \cap B_i| = 2$, and $A \cap B_i$ is empty otherwise. Now, for every permutation $g \in \mathrm{Sym}(3)$ wr $\mathrm{Sym}(b)$, there exists an index i such that

$$|(A \cap B_i) \cap (A \cap B_i)^g| \geq 1.$$

Hence $\mathrm{sep}(G) \leq b + 1$.

Finally, we argue by induction on b. The base case $b = 3$ was already taken care of before, while the induction argument is the same as above.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

This last case exhausts the possibilities for the pairs (a, b), and hence it completes the proof of the first part of the statement of Theorem J.

If G is an imprimitive permutation group, and Σ is a system of blocks such that $|\Sigma| = b$ and each block contains a points, then G embeds in $\mathrm{Sym}(a) \operatorname{wr} \mathrm{Sym}(b)$. The second part of the statement then follows combining the first one with Lemma 3.1. □

7. Proof of Theorem D

In this section, we prove Theorem D, that is, we characterise transitive permutation groups of degree n with $\mathrm{sep}(G) = \lceil (n+1)/2 \rceil$, which is the upper bound from Theorem E.

We divide the discussion into two fundamentally distinct cases: primitive groups (see Section 7.1) and imprimitive groups (see Section 7.2).

7.1. Primitive groups meeting the upper bound

The characterisation of primitive permutation groups G meeting the upper bound on the parameter $\mathrm{sep}(G)$ from Theorem E is summarised in the following lemma.

Lemma 7.1. *Let G be a primitive permutation group of degree n. Then $\mathrm{sep}(G) = \lceil (n+1)/2 \rceil$ if and only if one of the following holds:*

- *$n \geq 2$ and $G \cong \mathrm{Sym}(n)$ in its natural action;*
- *$n \geq 3$ and $G \cong \mathrm{Alt}(n)$ in its natural action;*
- *$n = 5$ and $G \cong \mathrm{C}_5$, $\mathrm{Dih}(5)$, and $\mathrm{AGL}_1(5)$;*
- *$n = 6$ and $G \cong \mathrm{Sym}(5)$ in its action on 6 points;*
- *$n = 7$ and $G \cong \mathrm{Dih}(7)$, $\mathrm{AGL}_1(7)$;*
- *$n = 8$ and $G \cong \mathrm{AGL}_1(8)$, $\mathrm{A\Gamma L}_1(8)$, $\mathrm{ASL}_3(2)$, $\mathrm{PSL}_2(7)$, and $\mathrm{PGL}_2(7)$;*
- *$n = 9$ and $G \cong \mathrm{AGL}_1(9)$, $\mathrm{PSU}_3(2)$, $\mathrm{A\Gamma L}_1(9)$, $\mathrm{ASL}_2(3)$, $\mathrm{AGL}_2(3)$, $\mathrm{PSL}_2(8)$, and $\mathrm{P\Gamma L}_2(8)$;*
- *$n = 10$ and $G \cong \mathrm{PGL}_2(9)$, $\mathrm{P\Gamma L}_2(9)$;*
- *$n = 12$ and $G \cong \mathrm{PGL}_2(11)$, $\mathrm{P\Gamma L}_2(11)$, M_{11}, and M_{12};*
- *$n = 14$ and $G \cong \mathrm{PGL}_2(13)$;*
- *$n = 16$ and $G \cong \mathrm{AGL}_4(2)$;*
- *$n = 24$ and $G \cong M_{24}$.*

The rest of the section is devoted to the proof of the above characterisation. We start our analysis with two general observations that will greatly reduce the possibilities for primitive permutation group meeting the bound from Theorem E.

Lemma 7.2. *Let G be a permutation group acting on a set Ω of size n, let $c(g)$ be the number of cycles in the cycle decomposition of $g \in G$, let $\ell(g)$ be the length of the shortest odd cycle in that decomposition (with $\ell(g) = 0$ if g contains no odd cycles), and for a non-negative integer i, let $\mathcal{O}_i$ be the set of elements g in G whose cycle decomposition contains at most i odd cycles. Further, let $r(G)$ be the number of orbits of G in its induced action on $\binom{\Omega}{\lfloor n/2 \rfloor}$. Suppose that $\mathrm{sep}(G) = \lceil (n+1)/2 \rceil$. Then, if n is even,*

$$r(G)|G| = \sum_{A \in \binom{\Omega}{n/2}} |G_A| = \sum_{g \in \mathcal{O}_0} 2^{c(g)},$$

and, if n is odd,

$$r(G)|G| = \sum_{A \in \binom{\Omega}{\lfloor n/2 \rfloor}} |G_A| \leq \sum_{g \in \mathcal{O}_1} 2^{c(g)-1} \ell(g) \leq \left\lceil \frac{n}{2} \right\rceil \sum_{A \in \binom{\Omega}{\lfloor n/2 \rfloor}} |G_A| = \left\lceil \frac{n}{2} \right\rceil r(G)|G|.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Proof. Let us start by observing that the equality

$$r(G)|G| = \sum_{A \in \binom{\Omega}{\lfloor n/2 \rfloor}} |G_A|$$

appearing in both formulas, for n odd and for n even, is just a restatement of the Cauchy-Frobenius Lemma (see [21, Theorem 1.7A]).

In what follows, we shall assume without loss of generality that $\Omega = [n]$. By double counting the set

$$\left\{(A, g) \in \binom{[n]}{\lfloor n/2 \rfloor} \times G \;\middle|\; A \cap A^g = \emptyset\right\},$$

we see that

$$\sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |\{g \in G \mid A \cap A^g = \emptyset\}| = \sum_{g \in G} \left|\left\{A \in \binom{[n]}{\lfloor n/2 \rfloor} \;\middle|\; A \cap A^g = \emptyset\right\}\right|. \tag{7.1}$$

First, we focus on the case when n is even. By assumption, every $(n/2)$-subset A is self-separable, and there is a unique image of A that is disjoint from it. Hence, it follows that $\{g \in G \mid A \cap A^g = \emptyset\} = G_A h$, where $h \in G$ is any element such that $A \cap A^h = \emptyset$. Hence,

$$\sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |\{g \in G \mid A \cap A^g = \emptyset\}| = \sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |G_A|.$$

Let us now count how many $(n/2)$-subsets can be separated from themselves by a fixed $g \in G$. Suppose g is written as a product of $c(g)$ disjoint cycles, and let A be such a set. Observe that A must meet every cycle of the decomposition in precisely half of the points of that cycle. In particular, every cycle has even length. Furthermore, if $\pi = (\pi_1, \pi_2, \ldots, \pi_{2\ell})$ is one of the cycles of g, A must contain either all the π_i whose indices are odd or all those whose indices are even. In particular, we can choose in two ways which points of each of the $c(g)$ cycles to include in A. Hence, there exist $2^{c(g)}$ sets A such that $|A| = n/2$ and $A \cap A^g$ is empty. This gives us

$$\sum_{g \in G} \left|\left\{A \in \binom{[n]}{n/2} \;\middle|\; A \cap A^g = \emptyset\right\}\right| = \sum_{g \in \mathcal{O}_0} 2^{c(g)},$$

proving the lemma in the case when n is even.

Suppose now that n is odd. We start by considering the left-hand side of (7.1). Fix a set $A \in \binom{[n]}{\lfloor n/2 \rfloor}$. Let $\mathcal{B}_A = \{A^g \mid g \in G, A \cap A^g = \emptyset\}$, and for each $B \in \mathcal{B}_A$ choose an element $h_B \in G$ mapping A to B. Let $T = \{h_B : B \in \mathcal{B}_A\}$. Clearly, $|T| = |\mathcal{B}_A| \leq \lceil n/2 \rceil$. Similarly as in the even case, we see that for each $B \in \mathcal{B}_A$, the set of elements $g \in G$ mapping A to B equals $G_A h_B$. Now observe that

$$|\{g \in G \mid A \cap A^g = \emptyset\}| = |\{g \in G \mid A^g \in \mathcal{B}_A\}| = \sum_{B \in \mathcal{B}_A} |\{g \in G \mid A^g = B\}| = |\mathcal{B}_A|\,|G_A|.$$

Therefore the left-hand side of (7.1) is equal to

$$\sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |\mathcal{B}_A||G_A|,$$

and since $1 \leq |\mathcal{B}_A| \leq \lceil n/2 \rceil$, it is bounded below and above by the quantities

$$\sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |G_A| \quad \text{and} \quad \left\lceil \frac{n}{2} \right\rceil \sum_{A \in \binom{[n]}{\lfloor n/2 \rfloor}} |G_A|,$$

respectively.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

It remains to show that the right-hand side of (7.1) is equal to $\sum_{g\in\mathcal{O}_1} 2^{c(g)-1}\ell(g)$. Again, for a given permutation $g \in G$, we count all the possible $\lfloor n/2\rfloor$-subsets A such that A and A^g are disjoint. The situation is slightly more complex in this case. In the same way as before, we observe that, if g contains more than one odd cycle, such an A does not exist. Hence, we assume that g contains precisely one odd cycle of length $\ell(g)$, and $c(g)-1$ even cycles. Note that A intersects the odd cycle in precisely $\lfloor \ell(g)/2\rfloor$ points. Moreover, no two consecutive points of the odd cycle are contained in A, implying that precisely two consecutive points are excluded from A. Once these two consecutive points are determined, the remaining points of the cycle contained in A are uniquely determined (by the requirement that they need to alternate between being contained and not in A). Since there are $\ell(g)$ choices for the two consecutive points excluded from A, and repeating the same reasoning as before for the points belonging to an even cycle, we obtain

$$\sum_{g\in\mathcal{O}_1}\left|\left\{A\in\binom{[n]}{\lfloor n/2\rfloor}\;\middle|\; A\cap A^g=\emptyset\right\}\right| = \sum_{g\in\mathcal{O}_1} 2^{c(g)-1}\ell(g).$$

This concludes the proof. □

Given two functions $f, g : \mathbb{N}\to\mathbb{R}^+$, we write $f\sim g$ if the limit of the quotient $f(n)/g(n)$, as n goes to infinity, is 1.

Lemma 7.3. *Suppose that G is a permutation group of degree n such that* $\mathrm{sep}(G)=\lceil (n+1)/2\rceil$. *Then, if n is even,*

$$|G| \geq \frac{1}{2^{n/2}}\binom{n}{n/2} \sim \frac{1}{\sqrt{2\pi}}\cdot 2^{\frac{1}{2}(n-\log_2 n)},$$

while, if n is odd,

$$|G| \geq \frac{1}{2^{\frac{n-1}{2}}n}\binom{n}{\frac{n-1}{2}} \sim \sqrt{\frac{2}{\pi}}\cdot 2^{\frac{1}{2}(n-3\log_2 n)}.$$

Proof. These bounds are obtained by disregarding the exclusion of the elements from $\mathcal{O}_i$, by substituting in the formulae from Lemma 7.2 the lower bound 1 for $|G_A|$ and the upper bound $2^{n/2}$ for $2^{c(g)}$ and n for $\ell(g)$, and by applying Stirling's formula to derive the asymptotic expansion. □

We are ready to characterise which primitive permutation groups meet the putative upper bound.

Proof of Lemma 7.1. By [39, Theorem 1.1], a primitive group whose degree exceeds 24 is either a subgroup of $\mathrm{Sym}(a)\,\mathrm{wr}\,\mathrm{Sym}(b)$ with socle isomorphic to $\mathrm{Alt}(a)^b$, where the action of $\mathrm{Sym}(a)$ is on k-subsets (for some $1\leq k\leq a/2$), the action of $\mathrm{Sym}(b)$ is on b points, and the wreath product is endowed with the product action, or

$$|G| \leq n^{1+\log_2 n}. \tag{7.2}$$

By elementary computations and by using the improved error term for Stirling's formula proved in [53], we show that, for even integers $n\leq 300$,

$$\frac{1}{2^{n/2}}\binom{n}{n/2} \geq n^{1+\log_2 n},$$

and that, for odd integers $n\leq 300$,

$$\frac{1}{2^{\frac{n-1}{2}}n}\binom{n}{\frac{n-1}{2}} \geq n^{1+\log_2 n}.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Moreover, by checking a finite number of cases with a calculator, we can decrease these bounds even further. Indeed, the function appearing in Lemma 7.3 is greater than the bound from (7.2) whenever n is an even integer greater than or equal to 116, or n is an odd integer greater than or equal to 147.

We have two cases to consider. If the degree of the permutation group G exceeds 116 or 147, depending on the parity of its degree, by Theorem M, for every $a \geq 4$ and $b \geq 2$,

$$\operatorname{sep}(\operatorname{Sym}(a) \operatorname{wr} \operatorname{Sym}(b)) \leq \left\lceil \frac{a+1}{2} \right\rceil^b < \left\lceil \frac{a^b+1}{2} \right\rceil.$$

In particular, if the degree exceeds 16, we can assume that G is of almost simple type. Moreover, Lemma 8.1 implies that G is permutation isomorphic to either $\operatorname{Alt}(n)$ or $\operatorname{Sym}(n)$ endowed with their actions on n points.

Let us now deal with the groups of small degree, where we can use a computational approach. We started with a list of all primitive permutation groups of degree at most 146 in the database of primitive groups in Magma, where we excluded the symmetric groups and the alternating groups in their natural actions from consideration. (This database is based on [20, 55, 56, 58].) Each of these primitive groups of even degree was tested against the inequality

$$\binom{n}{\frac{n}{2}} \leq \sum_{g \in \mathcal{O}_0} 2^{c(g)},$$

while those of odd degree against

$$\binom{n}{\frac{n-1}{2}} \leq \sum_{g \in \mathcal{O}_1} 2^{c(g)-1} \ell(g).$$

Both inequalities are obtained from Lemma 7.2, by substituting to each $|G_A|$ a 1 in the sum on the right hand side of the expressions.

Our search list gets significantly shortened: the possible groups have degree at most 32, with the only candidate of degree 32 being $\operatorname{AGL}(5,2)$. We use a different approach for it. By randomly sampling subsets of size at most 16 of the domain $\mathbb{F}_2^5$ and then testing them for existence of a group element that maps them to their complement, we found a number of sets of size 15 that are not self-separable, thus showing that $\operatorname{sep}(\operatorname{AGL}(5,2)) \leq 15$ (and we believe that 15 is the exact value). The remaining groups all have degree 24 or less, with the only group of order 24 being the Mathieu group M_{24}. These groups were dealt with an exhaustive search of $\lfloor (n+1)/2 \rfloor$-subsets which are not self-separable. The groups where such a set was found were excluded from the list, and those that survived are precisely the ones listed in Lemma 7.1. Our code for these computations can be found in [7]. This concludes the proof. □

7.2. Imprimitive groups meeting the upper bound

Let us now move to imprimitive permutation groups G meeting the upper bound on the parameter $\operatorname{sep}(G)$ from Theorem E. A complete characterisation of these groups is given in Lemmas 7.12 and 7.18, which together with its primitive counterpart (Lemma 7.1) finishes the proof of Theorem E.

By Theorem J, the degree n of an imprimitive permutation group G with $\operatorname{sep}(G) = \lceil (n+1)/2 \rceil$ is even, and G admits either a system of $n/2$ blocks of size 2 or two blocks of size $n/2$. We shall consider these two cases separately. We start our analysis with the following lemma of independent interest, which gives a necessary condition for a permutation group to be k-homogeneous. (Recall that, for a positive integer k, a permutation group is *k-homogeneous* if it acts transitively on the set of k-subsets of its domain.)

Lemma 7.4. *Let G be a transitive permutation group acting on a set Ω of size n, and let $k \leq \lceil n/2 \rceil - 1$. Suppose that, for every two disjoint subsets $A, B \subseteq \Omega$ of size k, there exists $g \in G$ mapping A to B. Then G is k-homogeneous.*

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Proof. Aiming for a contradiction, suppose that the statement is false. Then the set

$$\mathcal{E} = \{(A, B) \mid A, B \subseteq \Omega, |A| = |B| = k, A^g \neq B \text{ for every } g \in G\}$$

is nonempty. Among all $(A, B) \in \mathcal{E}$, we choose one which minimises $|A \cap B|$. Observe that, by our assumptions, the size t of the intersection $A \cap B$ satisfies $1 \leq t \leq k-1$. Thus,

$$|\Omega \setminus (A \cup B)| = n - 2k + t \geq t + 1.$$

This allows us to choose a subset $C \subseteq \Omega \setminus (A \cup B)$ with $|C| = t$. Now, let

$$A' = (B \setminus A) \cup C,$$

and observe that $A \cap A'$ is empty. Hence, by the assumptions, there exists $g \in G$ such that $A^g = A'$.

Observe that the sets $A \setminus B$ and $\Omega \setminus (A \cup B \cup C)$ are disjoint and of cardinalities $k - t$ and $n - 2k$, respectively. Their union is, therefore, of size $n - k - t$. If $n - k - t \geq k$, then let A'' be an arbitrary k-subset of this union. Note that such a set A'' is disjoint from A', implying that there exists $g' \in G$ such that $A'^{g'} = A''$. Observe also that $B \cap A'' = \emptyset$, implying that there exists $h \in G$ such that $A''^h = B$. But then $A^{gg'h} = B$, contradicting the fact that $(A, B) \in \mathcal{E}$. This contradiction implies that $n - k - t < k$, or equivalently, $2k + t - n = k - (n - k - t) > 0$. Since $2k \leq n - 1$, it follows that $2k + t - n \leq t - 1$, allowing us to choose a $(2k - n + t)$-subset D of $A \cap B$. Now let

$$A'' = (A \setminus B) \cup (\Omega \setminus (A \cup B \cup C)) \cup D,$$

and observe that $|A''| = k$ and $A'' \cap A' = \emptyset$. Similarly as above, there exists $g' \in G$ such that $A'^{g'} = A''$. Observe also that $|B \cap A''| = |D| < t$, implying that there exists $h \in G$ such that $A''^h = B$, which contradicts the fact that $(A, B) \in \mathcal{E}$.

Hence $\mathcal{E}$ is empty, and the statement is proved. □

Remark 7.5. Note that the upper bound on k in the assumptions of the above lemma cannot be improved to $\lceil n/2 \rceil$ since that would imply that every transitive permutation group G of even degree n and with $\mathrm{sep}(G) = n/2$ is k-homogeneous. However, as we show later in this section, this is far from true.

7.2.1. Permutation groups admitting blocks of size 2

We shall now turn our attention to transitive permutation groups G that admit a system of imprimitivity Σ consisting of blocks of size 2. A natural approach to analyse such groups is by considering the permutation module over the field of order 2 of the permutation group G^Σ, induced by the action of G on Σ. While a complete classification of permutation groups with blocks of size 2 is beyond the scope of this paper, we shall pursue this strategy to the point that is needed to prove Lemma 7.12 and leave a more thorough analysis for the future.

Suppose that G is a transitive permutation group on a set Ω, $|\Omega| = 2m$, admitting a system of imprimitivity Σ with m blocks of size 2. Let $H = G^\Sigma$ denote the permutation group induced by the action of G on Σ. Then G is permutation isomorphic to a subgroup of $C_2 \operatorname{wr} H$ in its imprimitive action on $\{0, 1\} \times \Sigma$. Let us make this more explicit.

Let $\mathbb{F}_2^\Sigma$ be the vector space of all functions from Σ to $\mathbb{F}_2$, endowed with the point-wise addition. Further, for $\chi \in \mathbb{F}_2^\Sigma$ and $g \in H$, let $\chi^g \in \mathbb{F}_2^\Sigma$ be defined by $\chi^g(B) = \chi(B^{g^{-1}})$ for every $B \in \Sigma$. This defines a linear representation $H \to \mathrm{GL}(\mathbb{F}_2^\Sigma)$ and thus turns $\mathbb{F}_2^\Sigma$ into an $\mathbb{F}_2 H$-module, called the *permutation module of* H.

Further, for $B \in \Sigma$, define τ_B to be the permutation on Ω swapping the two elements in B and fixing everything else. It is convenient to identify τ_B with the characteristic function $\chi_B : \Sigma \to \mathbb{F}_2$ of the element $B \in \Sigma$. Such an identification clearly yields an isomorphism between the group $N := \langle \tau_B \mid B \in \Sigma \rangle$ and the additive group $\mathbb{F}_2^\Sigma$. Moreover, under this identification, the conjugate $(\tau_B)^g = \tau_{B^g}$ of τ_B by $g \in G$ corresponds to the function $(\chi_B)^{\bar{g}}$, where χ_B is the characteristic function of B representing

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

τ_B and $\bar{g}$ is the permutation induced by g on Σ. This shows that we may think of N not only as the vector space $\mathbb{F}_2^\Sigma$ but also as the $\mathbb{F}_2H$-permutation module (with the multiplication by $h \in H \leq \mathbb{F}_2H$ given via conjugation by an element $g \in G$, whose induced action on Σ is h).

Let us now turn our attention to the kernel K of the action of G on Σ. Note that $K \leq N$, and hence $K = G \cap N$. Since K is normal in G, the above identification of N with $\mathbb{F}_2^\Sigma$ turns K into the $\mathbb{F}_2H$-submodule of the permutation module $N \cong \mathbb{F}_2^\Sigma$. Understanding imprimitive groups with blocks of size 2 is thus reduced to the study of submodules of the permutation modules these groups induce on the block system, together with the question of determining different (not permutation isomorphic) extensions of these modules by the induced permutation groups on the block system.

Note that the $\mathbb{F}_2H$-permutation module always contains the trivial submodule, the one dimensional *trace module* T spanned by $\Pi_{B\in\Sigma}\tau_B$, and the *augmentation module* A of codimension 1 consisting of all products of an even number of τ_B's. While other submodules might exist in general, this will not be the case for most of the groups H appearing in our analysis.

We shall now present a series of lemmas and constructions that determine some transitive permutation groups (up to isomorphism) admitting blocks of size 2 that appear in our analysis. We begin with the case in which K is trivial.

Lemma 7.6. *Let G be a transitive permutation group on Ω admitting a system of imprimitivity Σ consisting of m blocks of size 2. Let $B \in \Sigma$ and let G_B be the setwise stabiliser of B in G. Suppose that the kernel of the action of G on Σ is trivial. Then, there exists an index 2 subgroup S of G_B, with trivial core in G, and G is permutation isomorphic to the action of G on the coset space G/S by right multiplication.*

Proof. Let $\omega \in \Omega$ and let $B \in \Sigma$ be such that $\omega \in B$. Take S to be the vertex-stabiliser G_ω and observe that S has index 2 in G_B and is core-free in G. Furthermore, since $S = G_\omega$, G is permutation isomorphic to the action of G on the coset space G/S by right multiplication. □

Construction 7.7. In the case when $G = \mathrm{Sym}(m)$ acting on the cosets of the subgroup $S = \mathrm{Alt}(m-1)$, the permutation action of G on the coset space G/S has a more combinatorial description. Consider the set $\Omega := \{1,\dots,m\} \times \{0,1\}$. For $g \in G$, let $\bar{g}$ be the permutation of Ω defined by $(\sigma,i)^{\bar{g}} = (\sigma^g, i)$ for each $(\sigma,i) \in \Omega$, and let τ be the permutation acting as $(\sigma,i)^\tau = (\sigma, 1-i)$. Now consider the permutation group

$$\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1}) := \{\bar{g} : g \in \mathrm{Alt}(m)\} \cup \{\tau\bar{g} : g \in \mathrm{Sym}(m) \setminus \mathrm{Alt}(m)\}.$$

Observe first that the function $\iota\colon \mathrm{Sym}(m) \to \mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$ mapping g to $\bar{g}$ if $g \in \mathrm{Alt}(m)$ and to $\tau\bar{g}$ if $g \in \mathrm{Sym}(m) \setminus \mathrm{Alt}(m)$ is an isomorphism of (abstract) groups, mapping the subgroup $\mathrm{Alt}(m-1) \leq \mathrm{Sym}(m)$ to the stabiliser of the point $(m,0) \in \Omega$ in $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$. This implies that $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$ is permutation isomorphic to the group $\mathrm{Sym}(m)$ acting on the cosets of $\mathrm{Alt}(m-1)$.

Lemma 7.6 can also be used in the case where the kernel K of the action of G on Σ is nontrivial and possesses a complement $\overline{H} \cong G^\Sigma$ which is transitive on Ω (the situation where the complement is intransitive is considered in Lemma 7.9). Namely, one can then let $\overline{H}$ take the place of G in the lemma, and conclude that the block-stabiliser $\overline{H}_B$ has a core-free index 2 subgroup S with $\overline{H}$ acting on Ω permutation isomorphic to the coset action on $\overline{H}/S$. This will be evident in Construction 7.10.

We now consider the case in which K is nontrivial and it admits an intransitive complement in G.

Construction 7.8. Let H be a transitive permutation group with domain Σ, let K be a nontrivial submodule of the permutation $\mathbb{F}_2H$-module $\mathbb{F}_2^\Sigma$, and let $\Omega = \Sigma \times \{0,1\}$. For each $h \in H$ let $\overline{h}$ be the permutation on Ω defined by $(\sigma,i) \mapsto (\sigma^h, i)$ and let $\overline{H} = \{\overline{h} \mid h \in H\}$. Further, for each $\chi \in K$, let $\overline{\chi}$ be the permutation of Ω which swaps the two elements in $\{\sigma\} \times \{0,1\}$ when $\chi(\sigma) = 1$, and fixes them when $\chi(\sigma) = 0$. Finally, let $\overline{K} = \{\overline{\chi} \mid \chi \in K\}$. Observe that $K \cong \overline{K}$, $H \cong \overline{H}$, $\overline{K} \cap \overline{H} = 1$, and that $\overline{K}$ normalises $\overline{H}$. This allows us to define the permutation group $\overline{K} \rtimes \overline{H}$ on Ω, which we shall denote simply

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

as $K \rtimes H$, and when $K = \mathsf{T} \cong C_2$ is the trace submodule, we shall also write $C_2 \times H$ instead. Note that, since K is nontrivial, $K \rtimes H$ is transitive, with a system of imprimitivity $\overline{\Sigma} = \{\{\sigma\} \times \{0,1\} \mid \sigma \in \Sigma\}$. Moreover, the kernel of the action of G on $\overline{\Sigma}$ is $\overline{K} \cong K$ and the induced permutation group on $\overline{\Sigma}$ is permutation isomorphic to H.

Lemma 7.9. *Let G be a transitive permutation group on Ω admitting a system of imprimitivity Σ consisting of m blocks of size 2, let H be the permutation group induced by G on Σ, and let K be the kernel of the action of G on Σ (viewed as a submodule of the permutation module $\mathbb{F}_2^\Sigma$). Suppose that K is nontrivial and it has a complement in G which is intransitive on Ω. Then G is isomorphic to $H \rtimes K$, as defined in Construction 7.8.*

Proof. Let $\overline{H}$ be an intransitive complement of K in G. Since K acts trivially on Σ, $\overline{H}$ acts transitively, and since it is intransitive on Ω, it intersects each block in Σ in exactly one point. Without loss of generality we can label the points in a block $\sigma \in \Sigma$ by $(\sigma, 0)$ and $(\sigma, 1)$ in such a way that the two orbits of $\overline{H}$ are $\Sigma \times \{0\}$ and $\Sigma \times \{1\}$. It is straightforward to verify that under this labelling, $\overline{H}$ is precisely the corresponding permutation group $\overline{H}$ from Construction 7.8, and that K acts on Σ in the same way as $\overline{K}$. In particular, this labelling yields a permutation isomorphism between G and $H \rtimes K$. □

The following construction and lemma deal with the situation where the kernel K is the augmentation ideal.

Construction 7.10. Let H be a transitive permutation group on the domain Σ, let S be an index 2 normal subgroup of H, and let A be the augmentation submodule of $\mathbb{F}_2^\Sigma$. Consider the group $\overline{\mathsf{A}} \rtimes \overline{H}$, acting on $\Omega = \Sigma \times \{0,1\}$, as explained in Construction 7.8, and observe that it contains $\overline{\mathsf{A}} \rtimes \overline{S}$ as an index 2 subgroup. Choose τ in $\mathbb{F}_2^\Sigma \setminus \mathsf{A}$ and $h \in H \setminus S$, and let $G = \langle \overline{\mathsf{A}} \rtimes \overline{S}, \tau\overline{h} \rangle$. Observe that $\overline{\mathsf{A}} \rtimes \overline{S}$ has index 2 in G, that G does not depend on the choice of τ and h, and that it is a transitive permutation group on Ω with a system of imprimitivity $\overline{\Sigma} = \{\{\sigma\} \times \{0,1\} \mid \sigma \in \Sigma\}$. Moreover, the kernel of the action of G on $\overline{\Sigma}$ is $\overline{A}$ and $G^{\overline{\Sigma}}$ is permutation isomorphic to H. We shall denote the group G as $\mathrm{mix}(H, S, \mathsf{A})$.

Lemma 7.11. *Let G be a transitive permutation group on Ω admitting a system of imprimitivity Σ consisting of m blocks of size 2. Suppose that the kernel of the action of G on Σ is the augmentation ideal A. Let $H = G^\Sigma$ be the permutation group induced by the action of G on Σ. Then, either G is isomorphic to $\mathsf{A} \rtimes H$, or H has an index 2 subgroup S and G is isomorphic to $\mathrm{mix}(H, S, \mathsf{A})$, as defined in Construction 7.10.*

Proof. For each $B \in \Sigma$, choose one point from B and label it by $(B, 0)$, and label the other point with $(B, 1)$. This labelling establishes a bijection between Ω and $\Sigma \times \{0,1\}$, allowing us to assume that $\Omega = \Sigma \times \{0,1\}$, with the block system consisting of *fibres* $\{\sigma\} \times \{0,1\}$, for $\sigma \in \Sigma$. Let $\overline{H}$ and $\overline{\mathsf{A}}$ be as in Construction 7.10. Observe first that G is an index 2 subgroup of $\mathbb{F}_2^\Sigma \rtimes \overline{H}$. Observe that $\overline{\mathsf{A}} \rtimes \overline{H}$ has the prescribed properties, and hence $G = \overline{\mathsf{A}} \rtimes \overline{H}$ gives the first possibility of the statement.

We can thus assume that $X := G \cap (\overline{\mathsf{A}} \rtimes \overline{H})$ is a normal subgroup of $\mathbb{F}_2^\Sigma \rtimes \overline{H}$ of index 4. Since G contains A, we also see that $X = \overline{\mathsf{A}} \rtimes (G \cap \overline{H})$. This implies that $\overline{S} := G \cap \overline{H}$ has index 2 in G. Let $S = \overline{S}^\Sigma$, that is, the subgroup of H containing all those $h \in H$ for which $\overline{h} \in \overline{S}$. Then clearly S has index 2 in H, and we may apply Construction 7.10 to obtain the group $\mathrm{mix}(H, S, \mathsf{A})$.

Since X is a normal subgroup of index 4 in $\mathbb{F}_2^\Sigma \rtimes \overline{H}$, the open interval of subgroups between X and $\mathbb{F}_2^\Sigma \rtimes \overline{H}$ consists of either one or three groups (depending on whether the quotient by X is cyclic or the Klein group). However, we see that this interval contains three distinct groups, namely $\overline{\mathsf{A}} \rtimes \overline{H}$, $\mathbb{F}_2^\Sigma \rtimes S$, and $\mathrm{mix}(H, S, \mathsf{A})$. It is straightforward to check that precisely $\mathsf{A} \rtimes H$ and $\mathrm{mix}(H, S, \mathsf{A})$ are such that the group G^Σ is H and that $K = \mathsf{A}$. Hence, G is permutation isomorphic to one of these two groups. □

Lemma 7.12. *Let $m \geq 2$ be a positive integer, and let G be an imprimitive group with block system Σ that consists of m blocks of size 2. Then $\mathrm{sep}(G) = m + 1$ if and only if G is permutation isomorphic to one of the following:*

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

(i) $C_2 \times C_2$, C_4, *or* $\mathrm{Dih}(4)$ *acting transitively on* 4 *points;*
(ii) $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$, *where* $m \geq 3$ *(see Remark 7.7);*
(iii) $\mathsf{T} \rtimes H \cong C_2 \times H$ *(see Construction 7.8), where m and H satisfy one of:*
- $m \geq 3$ *and* $H = \mathrm{Sym}(m)$*;*
- $m \geq 4$ *and* $H = \mathrm{Alt}(m)$*;*
- $m = 4$ *and* $H = C_2 \times C_2$ *or* $\mathrm{Dih}(4)$*;*
- $m = 6$ *and* $H = \mathrm{PGL}_2(5)$.

(iv) $\mathsf{A} \rtimes H \cong C_2^{m-1} \rtimes H$ *(see Construction 7.8), where m and H satisfy one of:*
- $m \geq 4$ *is even and* $H = \mathrm{Alt}(m)$ *or* $\mathrm{Sym}(m)$*;*
- $m = 4$ *and* $H = C_2 \times C_2$ *or* $\mathrm{Dih}(4)$*;*
- $m = 6$ *and* $H = \mathrm{PGL}_2(5)$*;*
- $m = 8$ *and* $H = \mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, *or* $\mathrm{ASL}_3(2)$*;*
- $m = 12$ *and* $H = M_{12}$.

(v) $\mathrm{mix}(H, S, \mathsf{A})$ *(see Construction 7.10), where m, H, and S are one of:*
- $m \geq 3$, $H = \mathrm{Sym}(m)$ *and* $S = \mathrm{Alt}(m)$*;*
- $m = 4$ *and* $(H, S) = (C_2 \times C_2, C_2)$, $(\mathrm{Dih}(4), C_2 \times C_2)$, *or* $(\mathrm{Dih}(4), C_4)$*;*
- $m = 5$, $H = \mathrm{AGL}_1(5)$ *and* $S = \mathrm{Dih}(5)$*;*
- $m = p + 1$, $H = \mathrm{PGL}_2(p)$ *and* $S = \mathrm{PSL}_2(p)$, *for* $p \in \{5, 7\}$.

(vi) $C_2 \operatorname{wr} H \cong C_2^m \rtimes H$ *where m and H satisfy one of:*
- $m \geq 3$ *and* $H = \mathrm{Sym}(m)$*;*
- $m \geq 4$ *and* $H = \mathrm{Alt}(m)$*;*
- $m = 4$ *and* $H = C_2 \times C_2$ *or* $\mathrm{Dih}(4)$*;*
- $m = 5$ *and* $H = \mathrm{AGL}_1(5)$*;*
- $m = 6$ *and* $H = \mathrm{PGL}_2(5)$*;*
- $m = 8$ *and* $H = \mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, *or* $\mathrm{ASL}_3(2)$*;*
- $m = 9$ *and* $H = \mathrm{PSL}_2(8)$ *or* $\mathrm{P\Gamma L}_2(8)$*;*
- $m = 12$ *and* $H = M_{12}$.

(vii) *one of six transitive groups of degree* 8 *or* 16 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` (n, i) *for* $n = 8$ *and* $i \in \{17, 18, 19\}$ *and for* $n = 16$ *and* $i \in \{1506, 1804, 1805\}$.

Remark 7.13. Let us provide some additional information on the six exceptional groups appearing in the last item of the lemma. For each of these groups G, let $H := G^\Sigma$ and let K be the kernel of the action of G on Σ, viewed as a submodule of the permutation $\mathbb{F}_2 H$-module $\mathbb{F}_2^\Sigma$.

The three exceptional transitive groups of degree 8 all arise from the group $H = \mathrm{Dih}(4)$ (in its action on 4 points) and the 2-dimensional submodule $K \leq \mathbb{F}_2^\Sigma$ generated by the characteristic function of a block of imprimitivity of $\mathrm{Dih}(4)$. The group `TransitiveGroup` $(8, 18)$ is then just the semidirect product $K \rtimes H \cong \mathbb{F}_2^2 \rtimes \mathrm{Dih}(4)$ (see Construction 7.8). The other two groups of degree 8 are both nonsplit extensions of K by $\mathrm{Dih}(4)$ (that is, in both cases, K has no complement in G). Interestingly, both of them contain two nonconjugate copies of $\mathrm{Dih}(4)$, one acting regularly on the 8 points and one intransitively, but both intersecting K nontrivially. Moreover, all three groups `TransitiveGroup` $(8, i)$, $i \in \{17, 18, 19\}$, also admit a system of imprimitivity with two blocks of size 4, meaning that they will appear again later, when this situation is analysed.

Further, two of the three exceptional groups of degree 16 induce the group $H = \mathrm{ASL}_3(2)$ (in its natural affine action) with the kernel K corresponding to the unique 4-dimensional submodule of the permutation $\mathbb{F}_2 H$-module $\mathbb{F}_2^\Sigma \cong \mathbb{F}_2^8$. One of these two groups (`TransitiveGroup` $(16, 1804)$, to be precise) is a semidirect product $K \rtimes H \cong \mathbb{F}_2^4 \rtimes \mathrm{ASL}_3(2)$, while `TransitiveGroup` $(16, 1805)$ is a nonsplit extension of K by $\mathrm{ASL}_3(2)$ (and contains no subgroups isomorphic to $\mathrm{ASL}_3(2)$).

Finally, the remaining exceptional group, namely `TransitiveGroup` $(16, 1506)$ is simply a semidirect product $K \rtimes H$ where $H = \mathrm{PSL}_2(7)$ in its natural action on 8 points, and where $K \cong \mathbb{F}_2^4$ is a cyclic $\mathbb{F}_2 \mathrm{PSL}_2(7)$-module generated by the characteristic function of the set $\{x^2 \mid x \in \mathbb{F}_7 \setminus \{0\}\} \cup \{\infty\}$, viewed as the subset of the projective line $\mathbb{F}_7 \cup \{\infty\}$.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Proof of Lemma 7.12. For $m \leq 9$, the validity of the lemma has been checked computationally by checking all transitive groups of degree at most 18 from the Library of Transitive Groups in Magma [11] (the results and the code are available at [7]). We shall assume henceforth that $m \geq 10$, that is, that the degree of G is at least 20.

Let us show that all the permutation groups G of degree $2m \geq 20$ listed in Lemma 7.12 satisfy $\mathrm{sep}(G) = m + 1$. The permutation groups G that we need to consider are:

- $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$;
- $C_2 \times \mathrm{Alt}(m)$; and
- $\mathsf{A} \rtimes M_{12}$.

Namely, all other groups listed in the lemma are overgroups of the above.

Suppose first that G is either $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$ or $C_2 \times \mathrm{Alt}(m)$. Then G acts on the set $\Omega = \{1, \ldots, m\} \times \{0, 1\}$, as explained in Remark 7.7 or Construction 7.8. In both cases, for every $g \in \mathrm{Alt}(m)$, the group G contains the permutation $\bar{g}$ acting on Ω according to the rule $(x, i)^{\bar{g}} = (x^g, i)$. Moreover, if $G = C_2 \times \mathrm{Alt}(m)$, then G contains also the central permutation τ, defined by $(x, i)^\tau = (x, 1 - i)$, and if $G = \mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$, then G contains an element $\tau\bar{g}$ for every $g \in \mathrm{Sym}(m) \setminus \mathrm{Alt}(m)$.

For $i \in \{1, \ldots, m\}$ let $\sigma_i = \{(i, 0), (i, 1)\} \subseteq \Omega$. Further, let A be a subset of Ω of size m, and let X, Y, Z be subsets of $\{1, \ldots, m\}$ defined by

$$X = \{i \mid \sigma_i \subseteq A\}, \quad Y = \{i \mid \sigma_i \cap A = \emptyset\}, \quad \text{and} \quad Z = \{i \mid |\sigma_i \cap A| = 1\}.$$

Note that the sets X, Y, and Z form a partition of $\{1, \ldots, m\}$ and that $2|X| + \mathcal{Z} = |A|$. Since $|A| = m = |X| + |Y| + |Z|$, it follows that $|X| = |Y|$. Furthermore, for $j \in \{0, 1\}$, let $Z_j = \{i \in Z \mid (i, j) \in A\}$ and observe that Z_0 and Z_1 form a partition of Z.

If $|X| \geq 1$, then there exists an odd permutation $g \in \mathrm{Sym}(m) \setminus \mathrm{Alt}(m)$ that fixes every element in Z pointwise and maps X to Y (note that such a permutation always exists). In this case, the permutation $\tau\bar{g} \in \mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$, maps A to its complement, as required.

Moreover, if $|X| \geq 2$, then there is also an even permutation $h \in \mathrm{Alt}(m)$ that fixes Z pointwise and swaps X with Y. This yields an element $\tau\bar{h} \in C_2 \times \mathrm{Alt}(m)$ mapping A to its complement, as required. Similarly, if $|X| = 1$, then $|Z| = m - 2 \geq 8$ allowing us to pick two distinct elements $s, t \in Z_j$ for some $j \in \{0, 1\}$. Now, let g be the transposition $(s\,t) \in \mathrm{Sym}(m)$ and let $h \in \mathrm{Sym}(m)$ be the transposition swapping X and Y. Then $\tau\bar{g}\bar{h}$ is an element of $C_2 \times \mathrm{Alt}(m)$ that maps A to its complement.

Finally, if $X = Y = \emptyset$, then $|Z| = m \geq 3$ (we are in fact assuming $m \geq 10$), implying that there exists $j \in \{0, 1\}$ and $s, t \in Z_j$, $s \neq t$. Let $g = (i\,j) \in \mathrm{Sym}(m)$. If $G = C_2 \times \mathrm{Alt}(m)$, then τ is an element of G that maps A to its complement. On the other hand, if $G = \mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$, then $\tau\bar{g} \in G$ will do the same.

We are now left with the case where $G = \mathsf{A} \rtimes M_{12}$, acting on the set $\Omega = \{1, \ldots, 12\} \times \{0, 1\}$. The proof that every set of size 12 is self-separable in this case was done computationally, but with the following short-cut that significantly sped up the computations. Observe first that the group $M_{12} \leq \mathrm{Sym}(12)$ is 5-transitive. Moreover, for every integer $k \leq 6$ and every two disjoint subsets $X, Y \subseteq \{1, \ldots, 12\}$ there exists $g \in M_{12}$ simultaneously mapping X to Y and Y to X. Note that for $k = 6$ this fact is equivalent to saying that M_{12} (in its action on 12 points) meets the upper bound $\mathrm{sep}(M_{12}) = 6$, which was already established in Lemma 7.1, while for $k \leq 5$, due to 5-transitivity of M_{12}, we may assume that $X = \{1, \ldots, k\}$ and that Y contains elements $k + 1, \ldots, k + 5$.

Once this is established (computationally or theoretically), we may take a subset $A \subseteq \Omega$ of size 12 and define the sets σ_i, X, Y, and Z, as well as the permutations τ and $\bar{g}$ for $g \in M_{12}$, in the same way as we did in the case of the groups $C_2 \times \mathrm{Alt}(m)$. Let $g \in M_{12}$ be the permutation, existence of which we have established computationally, that swaps the sets X and Y. Since $|Z| = 12 - |X| - |Y| = 12 - 2|X|$ is even in this case, there exists an element $\tau_Z \in \mathsf{A}$ that swaps the two elements in σ_i for each $i \in Z$ and fixes all other elements of Ω. Then $\tau_Z\bar{g}$ is an element of G that maps A to its complement. This completes the proof that all the groups G of degree $2m$ listed in Lemma 7.12 satisfy $\mathrm{sep}(G) = m + 1$.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Let us now prove that, if $\mathrm{sep}(G) = m+1$ and $2m \geq 20$, then G appears in the list in Lemma 7.12. Let K denote the kernel of the action of G on Σ and let $H = G^\Sigma \cong G/K$ denote the permutation group induced by this action. As explained earlier in this section, we may view K as a submodule of the permutation module $\mathbb{F}_2^\Sigma \cong \mathbb{F}_2^m$.

We shall first prove that the permutation group H (of degree m) is k-homogeneous, where $k = (\lceil m/2 \rceil - 1) \geq 4$. By Lemma 7.4, it suffices to show that for any pair X, Y of disjoint subsets of the block system Σ of size k there exists $g \in G$ such that $X^g = Y$. Let $X, Y \subseteq \Sigma$ be two such sets, and let A be a set that contains both points from each block in Y, no points from any block in X, and precisely one point from each block in $\Sigma \setminus (X \cup Y)$. Note that $|A| = m < \mathrm{sep}(G)$, implying that A is self-separable. Hence there exists $g \in G$ which maps A to its complement and thus (viewed as a permutation of Σ) maps X to Y. Therefore, H is indeed k-homogeneous, as claimed. The list of k-homogeneous groups of degree m with $k = (\lceil m/2 \rceil - 1)$ is quite short: by combining [21, Theorem 9.4B] and [16, Section 7] (and using the assumption that the degree of G^Σ is at least 10), we see that

(a) $\mathrm{Alt}(m) \leq H \leq \mathrm{Sym}(m)$, or
(b) $m = 12$ and $H \cong M_{12}$.

As was proved in [42], the only submodules of the permutation module $\mathbb{F}_2^\Sigma$ of H are then either the trivial module $\mathbf{1}$, the trace module T, the augmentation module A, or, of course, $\mathbb{F}_2^\Sigma$ itself.

Suppose first that the kernel K is trivial. By Lemma 7.6, the stabiliser of a point in H contains a subgroup S of index 2, excluding the cases $H \cong \mathrm{Alt}(m)$ and $H \cong M_{12}$. Hence $H = \mathrm{Sym}(m)$ and thus $S = \mathrm{Alt}(m-1)$. Lemma 7.6 then implies that G is permutation isomorphic to the action of $\mathrm{Sym}(m)$ on the cosets of $\mathrm{Alt}(m-1)$, and thus permutation isomorphic to $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$, as explained in Remark 7.7.

Suppose now that $K = \mathsf{T}$. Then G is a central 2-extension of H. Note also that $K = \langle \tau \rangle$ where τ swaps the two points in every block in Σ.

If the extension is split with the complement $\overline{H} \cong H$, then $G = C_2 \times \overline{H}$. Further, if $\overline{H}$ is intransitive, then by Lemma 7.9, $G = \mathsf{T} \rtimes H$, as in Construction 7.8. A direct computation in the case of $H = M_{12}$ exhibits a non-self-separable subset of points whose size is 12 (see [7] for such a set), showing that $\mathrm{sep}(\mathsf{T} \rtimes M_{12}) \leq 12$, contradicting our assumptions.

On the other hand, if $\overline{H}$ is transitive, then we may apply the previous paragraph with $\overline{H}$ in place of G to conclude that $\overline{H} \cong \mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathbf{1})$ in its action on $\Omega' := \{1, \ldots, m\} \times \{0, 1\}$. In this setting, the block system Σ corresponds to the partition of Ω' into pairs $\{\sigma\} \times \{0, 1\}$, and the generator τ of the kernel K to the permutation τ' of Ω' that swaps both elements in each of these pairs. The permutation group G is thus permutation isomorphic to the action of $\langle \overline{H}, \tau' \rangle$ on Ω', which is clearly isomorphic to the permutation group $\mathsf{T} \rtimes H$, as in Construction 7.8. This completes the proof in the case where the extension of K by H is split.

Now suppose that G is a nonsplit extension of $K = \langle \tau \rangle$ by H. Let $\pi \colon G \to G^\Sigma = H$ be the corresponding epimorphism with kernel K. Since the stabiliser G_ω of a point $\omega \in \Omega$ intersects K trivially, π maps G_ω isomorphically to the stabiliser H_B of a point $B \in \Sigma$. Furthermore, $\pi^{-1}(H_B) = G_B = \langle \tau \rangle \times G_\omega$.

Suppose first that $H = \mathrm{Sym}(m)$. Then (as is well known) there exist two nonisomorphic nonsplit central 2-extensions, usually denoted by $2.\mathrm{Sym}(m)^+$ and $2.\mathrm{Sym}(m)^-$. In both cases the central element is contained in the derived subgroup $[P, P]$ of the preimage P of the group $\mathrm{Sym}(m-1)$. In our context that implies that $\tau \in [G_B, G_B]$, which clearly contradicts the fact that τ is a direct (central) factor in G_B. Similarly, if $H = \mathrm{Alt}(m)$, then G is isomorphic to the unique nonsplit central 2-extension of $\mathrm{Alt}(m)$, usually denoted by $2.\mathrm{Alt}(m)$. Here it can also be seen that τ resides within the derived subgroup $[G_B, G_B]$, again yielding a contradiction.

We are thus left with the case where $H = M_{12}$. Since M_{12} is a perfect simple group and has the Schur multiplier of order 2, there exists a unique nonsplit 2-extension, namely the group usually denoted by $2.M_{12}$. It can be checked computationally that this group has a unique permutation representation of degree 24 (admitting blocks of size 2 and acting on them as M_{12}), which can be found in the Database

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

of Transitive Permutation Groups in Magma [11] under the name `TransitiveGroup` (24, 18440). One can check computationally that this group admits a non-self-separable set of size 12, implying that $\mathrm{sep}(G) \leq 12$, contradicting our assumption on $\mathrm{sep}(G)$ (see [7] for the computational details). This finishes the proof in the case where $K = \mathsf{T}$.

Let us now assume that $K = \mathsf{A}$. If $H \cong \mathrm{Alt}(m)$ or M_{12}, then Lemma 7.11 implies that $G = \mathsf{A} \rtimes H$. However, if m is odd, then the subset $A := \{1, \dots, m\} \times \{0\}$ of the domain of $\mathsf{A} \rtimes H$ (see Construction 7.8) cannot be separated from itself since G does not contain the trace submodule T. On the other hand, if $H \cong \mathrm{Sym}(m)$, then G is isomorphic either to $\mathsf{A} \rtimes \mathrm{Sym}(m)$ (and as above, m needs to be even) or to $\mathrm{mix}(\mathrm{Sym}(m), \mathrm{Alt}(m), \mathsf{A})$.

Finally, if $K = \mathbb{F}_2^\Sigma$, then the single option is $G = \mathbb{F}_2^\Sigma \rtimes H = C_2 \operatorname{wr} H$. This concludes the proof of the lemma. □

This concludes our analysis of permutation groups admitting blocks of size 2.

7.2.2. Permutation groups admitting two blocks of size *m*

We start by describing some quirky permutation subgroups of $H \operatorname{wr} C_2$.

Construction 7.14. Let H be a transitive permutation group of degree n, and let $f \in \mathrm{Sym}(n)$ be a permutation such that $f^2 \in H$ (and thus $f \in \mathbf{N}_{\mathrm{Sym}(n)}(H)$). We denote the permutation group

$$\{(h, h) \mid h \in H\} \cong H,$$

whose action is diagonal on $\Omega^{\{0,1\}}$, by $\mathbf{q}_0(H)$. Note that $\mathbf{q}_0(H)$ is intransitive with two orbits, and that its transitive constituents are permutation isomorphic to H. We define

$$\mathbf{q}(H, f) = \langle \mathbf{q}_0(H), \bar{f} \rangle,$$

where

$$(\omega, 0)^{\bar{f}} = (\omega^f, 1), \quad \text{and} \quad (\omega, 1)^{\bar{f}} = (\omega^f, 0).$$

Note that $\mathbf{q}(H, f)$ is transitive on $\Omega^{\{0,1\}}$, and that $\mathbf{q}_0(H)$ is an index 2 subgroup of $\mathbf{q}(H, f)$. Further, observe that $\mathbf{q}(H, 1) = H \times C_2$.

Construction 7.14 captures, up to permutational isomorphism, every permutation group which is an imprimitive extension of H of degree 2, as stated in the following lemma.

Lemma 7.15. *Let H be a permutation group on Ω, let $s \in \mathrm{Sym}(\Omega^{\{0,1\}})$ be a permutation with the properties that it swaps the two sets $\Omega^{\{0\}}$ and $\Omega^{\{1\}}$, and that $s^2 \in \mathbf{q}_0(H)$ endowed with its diagonal action on $\Omega^{\{0,1\}}$. Denote by G the permutation group on $\Omega^{\{0,1\}}$ generated by $\mathbf{q}_0(H)$ and s. Then G is permutation isomorphic to $\mathbf{q}(H, f)$, for some $f \in \mathrm{Sym}(\Omega)$.*

Proof. Aiming for a contradiction, suppose that, for every $f \in \mathrm{Sym}(\Omega)$,

$$s \notin \bar{f}^{\mathbf{N}_{\mathrm{Sym}(\Omega^{\{0,1\}})}(\mathbf{q}_0(H))}.$$

In particular, there exist two distinct permutations $a, b \in \mathrm{Sym}(\Omega)$ such that

$$(\omega, 0)^s = (\omega^a, 1), \quad \text{and} \quad (\omega, 1)^s = (\omega^b, 0).$$

From the fact that $s^2 \in \mathbf{q}_0(H)$, it follows that

$$s \in \mathbf{N}_{\mathrm{Sym}(\Omega^{\{0,1\}})}(\mathbf{q}_0(H)) = \langle \mathbf{q}_0\big(\mathbf{N}_{\mathrm{Sym}(\Omega)}(H)\big), \bar{1} \rangle.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

But no element in the normaliser has the desired form, which is a contradiction. Hence, s and $\bar{f}$ are conjugate in $\mathbf{N}_{\mathrm{Sym}(\Omega^{\{0,1\}})}(\mathbf{q}_0(H))$, which proves the permutational isomorphism (see [21, Exercise 1.6.1]). □

Example 7.16. We specialise Construction 7.14 for the alternating and symmetric groups. Let $m \geq 5$ be an integer. Observe that, if $f \in \mathrm{Alt}(m)$ is an even permutation, then $(f, f)\bar{f} = \bar{1}$, and hence

$$\mathbf{q}(\mathrm{Alt}(m), f) = \mathbf{q}(\mathrm{Alt}(m), 1) = \mathrm{Alt}(m) \times C_2.$$

Analogously, if $f \in \mathrm{Sym}(m)$ is odd, then, by choosing $g \in \mathrm{Alt}(m)$ such that $gf = (1, 2)$, we have $(g, g)\bar{f} = \overline{(1, 2)}$. Therefore,

$$\mathbf{q}(\mathrm{Alt}(m), f) = \mathbf{q}(\mathrm{Alt}(m), (1, 2)).$$

On the other hand, the same reasoning shows that, for every permutation $f \in \mathrm{Sym}(m)$,

$$\mathbf{q}(\mathrm{Sym}(m), f) = \mathbf{q}(\mathrm{Sym}(m), 1).$$

The appearance of such subgroups in our setting is justified by the following observation.

Lemma 7.17. *Let H be an almost simple primitive permutation group with socle T, and let G be an imprimitive permutation group with two blocks of imprimitivity, B and C, such that $G_B^B = H$. Then, either $T \operatorname{wr} C_2 \leq G \leq H \operatorname{wr} C_2$, or G is permutation isomorphic to $\mathbf{q}(H, f)$, for some $f \in \mathrm{Sym}(\Omega)$ as defined in Construction 7.14.*

Proof. We start by computing the socle of G. We note that $G_{(\Sigma)} = G_B = G_C$ and that G is an extension of C_2 by $G_{(\Sigma)}$. Let N be a minimal normal subgroup of $G_{(\Sigma)}$. Consider the projections $\pi_B : G_{(\Sigma)} \to G_B^B$ and $\pi_C : G_{(\Sigma)} \to G_C^C$. Since N is minimal normal, so are N^{π_B} and N^{π_C}. Observe that, as G is faithful, the two images cannot be concurrently trivial. In particular, T is a subgroup of N, and hence the socle of G is of the form T^ℓ, for some positive integer ℓ. As $G \leq \mathrm{Sym}(|B|) \operatorname{wr} C_2$, we see that $\ell \leq 2$, and hence either $\ell = 1$ or $\ell = 2$. On one hand, if $\ell = 2$, it follows at once that

$$T \operatorname{wr} C_2 \leq G \leq H \operatorname{wr} C_2.$$

On the other hand, suppose that $\ell = 1$. Since G acts transitively on Σ, there exists a permutation $s \in G$ such that $B^s = C$ and $s^2 \in G_{(\Sigma)}$. Observe that G_B^B and G_C^C are permutation isomorphic: the requested bijections are s for the domains and the conjugation by s for the groups. By Lemma 7.15, G is permutation isomorphic to $\mathbf{q}(H, f)$, where f is a permutation with the property that $\bar{f} = s$. □

We can now state the main result of the section.

Lemma 7.18. *Let $m \geq 2$ be a positive integer, and let G be an imprimitive group with block system Σ that consists of two blocks of size m. Then $\mathrm{sep}(G) = m + 1$ if and only if G is permutation isomorphic to one of the following:*

(i) *$C_2 \times C_2$, C_4, or $\mathrm{Dih}(4)$ acting transitively on 4 points;*
(ii) *$\mathbf{q}(H, 1) \cong H \times C_2$ (see Construction 7.14), where m and H satisfy one of:*
   - *$m \geq 3$ and $H = \mathrm{Sym}(m)$;*
   - *$m \geq 4$ and $H = \mathrm{Alt}(m)$;*
   - *$m = 4$ and $H = C_2 \times C_2$ or $\mathrm{Dih}(4)$;*
   - *$m = 6$ and $H = \mathrm{PGL}_2(5)$;*

(iii) *$\mathbf{q}(\mathrm{Alt}(m), (1, 2))$ for $m \geq 5$ (see Construction 7.14);*
(iv) *$H \operatorname{wr} C_2 \cong H^2 \rtimes C_2$ where m and H satisfy one of:*
   - *$m \geq 3$ and $H = \mathrm{Sym}(m)$;*
   - *$m \geq 4$ and $H = \mathrm{Alt}(m)$;*

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

- $m = 4$ *and* $H = C_4$, $C_2 \times C_2$, *or* $\mathrm{Dih}(4)$;
- $m = 5$ *and* $H = \mathrm{AGL}_1(5)$;
- $m = 6$ *and* $H = \mathrm{PGL}_2(5)$;
- $m = 8$ *and* $H = \mathrm{PSL}_2(7)$, $\mathrm{PGL}_2(7)$, $\mathrm{AGL}_1(8)$, $\mathrm{A\Gamma L}(1,8)$, *or* $\mathrm{ASL}_3(2)$;
- $m = 9$ *and* $H = \mathrm{PSL}_2(8)$ *or* $\mathrm{P\Gamma L}_2(8)$;
- $m = 12$ *and* $H = M_{12}$;

(v) *one of transitive groups of degree* 6 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(6,i)$ *for* $i \in \{9, 10\}$.

(vi) *one of transitive groups of degree* 8 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(8,i)$ *for* $i \in \{19, 21, 22, 26, 28, 29, 30, 31, 33, 34, 41, 45, 46\}$.

(vii) *one of transitive groups of degree* 10 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(10,i)$ *for* $i \in \{17, 19, 20, 27, 41, 42\}$.

(viii) *one of transitive groups of degree* 12 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(12,i)$ *for* $i \in \{181, 182, 229, 278, 279, 297, 298\}$.

(ix) *one of transitive groups of degree* 14 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(14,i)$ *for* $i \in \{59, 60\}$.

(x) *one of transitive groups of degree* 16 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(16,i)$ *for* $i \in \{1078, 1502, 1798, 1799, 1801, 1802, 1882, 1883, 1950, 1951\}$.

(xi) *one of transitive groups of degree* 18 *that can be found in the Library of Transitive Groups in [11] under the names* `TransitiveGroup` $(18,i)$ *for* $i \in \{937, 938, 979, 980\}$.

Remark 7.19. Observe that $\mathbf{q}(\mathrm{Alt}(m),(1,2)) \cong \mathrm{mix}(\mathrm{Sym}(m),\mathrm{Alt}(m),\mathbf{1})$ and that $\mathbf{q}(H,1) \cong H \times C_2$ for all $m \geq 3$. Besides these groups, the following groups appear both in Lemma 7.12 and Lemma 7.18.

- For degree 4, $C_2 \times C_2$, C_4, or $\mathrm{Dih}(4)$, all acting transitively on 4 points;
- For degree 8,
  - the groups `TransitiveGroup` $(8,i)$ for $i \in \{21, 22, 26, 28, 29, 30, 31\}$, which appear in Lemma 7.18 and are identified in Lemma 7.12,
  - the groups `TransitiveGroup` $(8,17)$ and `TransitiveGroup` $(8,18)$, which appear in Lemma 7.12 and are identified in Lemma 7.18,
  - and the group `TransitiveGroup` $(8,19)$, which is not identified in either Lemma 7.12 or Lemma 7.18.

Proof. As for Lemma 7.12, the statement has been verified computationally for $m \leq 9$ (see [7]). Therefore, we can assume that $m \geq 10$.

Let us show that all the permutation groups G of degree $2m \geq 20$ listed in Lemma 7.18 satisfy $\mathrm{sep}(G) = m + 1$. As every other group appearing is an overgroup of both $\mathrm{Alt}(m) \times C_2$ and $\mathbf{q}(\mathrm{Alt}(m),(1,2))$, we just need to consider these two cases. Observe that $\mathrm{Alt}(n) \times C_2$ has blocks of size two, and hence the conclusion follows from Lemma 7.12.

Hence, we need to consider $\mathbf{q}(\mathrm{Alt}(m),(1,2))$. Let A be a k-subset of points, for some $4 \leq k \leq n$. We can suppose that A and A^s are not disjoint. We label the points of B by $\{1_B, 2_B, \ldots, n_B\}$, and those of C by $\{1_C, 2_C, \ldots, n_C\}$. We can also assume that $1_B^s = 2_C$, $2_B^s = 1_C$, $1_C^s = 2_B$, $2_C^s = 1_B$, while, for every integer $3 \leq x \leq n$, $x_B^s = x_C$ and $x_C^s = x_B$. We define the integers

$$z = |A \cap \{1_B, 2_B, 1_C, 2_C\}|, \quad z_B = |A \cap \{1_B, 2_B\}|, \quad z_C = |A \cap \{1_C, 2_C\}|.$$

Observe that there exist two integers $a, b \leq n$ such that

$$4 - z = |A \cap \{a_B, b_B, a_C, b_C\}|, \quad 2 - z_B = |A \cap \{a_B, b_B\}|, \quad 2 - z_C = |A \cap \{a_C, b_C\}|.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

It is immediate to check that there exists a double transposition t such that $t \in \mathrm{Alt}(4)$ and

$$\{1_B, 2_B, 1_C, 2_C, a_B, b_B, a_C, b_C\} \cap \{1_B, 2_B, 1_C, 2_C, a_B, b_B, a_C, b_C\}^{st} = \emptyset.$$

Finally, the pointwise stabiliser of the set $\Omega - \{1_B, 2_B, 1_C, 2_C, a_B, b_B, a_C, b_C\}$ contains $\mathrm{Alt}(n-4)$. The choice of a suitable h so that A and A^{sth} are disjoint is the same as in the corresponding case in Lemma 7.12.

Let us now prove that, if $\mathrm{sep}(G) = m+1$ and $2m \geq 20$, then G appears in the list in Lemma 7.18. Suppose that G admits a system of imprimitivity Σ consisting of two blocks of size m. Let us denote these blocks by B and C, and let X, Y be two subsets of B of equal size $k < m/2$. We will show that there exists a permutation in G mapping X to Y. Let g be an arbitrary permutation that swaps the two blocks B and C. Consider the subset

$$A = X \cup \left(C \setminus Y^{g^{-1}}\right).$$

Since $|A| = m < \mathrm{sep}(G)$, there exists a permutation h such that $A \cap A^h$ is empty. Observe that $X^h = Y^{g^{-1}}$, and hence $X^{hg} = Y$. By the arbitrariness of X and Y, we conclude that the permutation group G_B^B, induced by the action of G_B on B, is k-homogeneous, for every $k < m/2$. Using again [16, Section 7] and [21, Theorem 9.4B] and that $m \geq 10$, we see that either $\mathrm{Alt}(n) \leq G_B^B \leq \mathrm{Sym}(n)$ or $M_{12} = G_B^B$. In the latter scenario, in view of Lemma 7.17, we have two candidate groups: namely, $M_{12} \operatorname{wr} C_2$ and $\mathbf{q}(M_{12}, 1) \cong M_{12} \times C_2$. (Note that Construction 7.14 produces no other subgroup as $\mathbf{N}_{\mathrm{Sym}(12)}(M_{12}) = M_{12}$.) We have verified by a computer-aided calculation that $M_{12} \operatorname{wr} C_2$ reaches the upper bound, while $M_{12} \times C_2$ does not. Therefore, we are left with $\mathrm{Alt}(n) \leq G_B^B \leq \mathrm{Sym}(n)$, and the conclusion follows by Example 7.16 and Lemma 7.17. □

8. Primitive groups

This section is devoted to the proofs of our results concerning primitive permutation groups. The subsections are organised according to the type of primitive group under consideration, as classified by the O'Nan–Scott Theorem. As previously mentioned, we follow the partition of primitive groups into eight classes proposed in [49].

8.1. Almost simple type

The proof of Theorem K is divided into several lemmas depending on the socle of the group considered.

We start by considering the action of the alternating group $\mathrm{Alt}(m)$ or the symmetric group $\mathrm{Sym}(m)$ on the set $\binom{[m]}{k}$ of k-subsets of the set $[m] = \{1, 2, \ldots, m\}$. Observe that the degree of this permutation representation is $\binom{m}{k}$. The next simple observation has already been established in [25, Lemma 2]. (Lemma 8.1 takes care of the case (a) in Table 1).

Lemma 8.1. *Let $2 \leq k < m$ be two integers. Then*

$$\mathrm{sep}\left(\mathrm{Alt}(m) \curvearrowright \binom{[m]}{k}\right) \leq \mathrm{sep}\left(\mathrm{Sym}(m) \curvearrowright \binom{[m]}{k}\right) \leq \binom{m - \lfloor \frac{k}{2} \rfloor}{\lceil \frac{k}{2} \rceil}.$$

Consequently, if $\mathcal{C}_k$ is the family of symmetric (or alternating) groups acting on k-subsets, then

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{\sqrt{n}} \leq \frac{\sqrt{k!}}{(k/2)!} \quad \textit{for } k \textit{ even},$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

and

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{n^{\frac{k+1}{2k}}} \leq \frac{k!^{\frac{k+1}{2k}}}{\lceil k/2 \rceil !} \quad \textit{for } k \textit{ odd.}$$

Proof. For the sake of simplicity, let $r = \lfloor k/2 \rfloor$. Consider the subset

$$A = \left\{ X \in \binom{[m]}{k} \,\middle|\, \{1, 2, \ldots, r\} \subseteq X \right\}.$$

For every $g \in \mathrm{Sym}(m)$, we compute

$$A \cap A^g = \left\{ X \in \binom{[m]}{k} \,\middle|\, \{1, 2, \ldots, r\} \cup \{1^g, 2^g, \ldots, r^g\} \subseteq X \right\}.$$

This intersection is never empty, and, if g does not stabilise $\{1, 2, \ldots, r\}$, A^g and A are not equal. Hence, A is not self-separable for $\mathrm{Sym}(m)$. This proves the upper bound of $\mathrm{sep}(\mathrm{Sym}(m))$.

Note that

$$|A| = \binom{m-r}{k-r} = \frac{1}{(k-r)!} m^{k-r} + o\left(m^{k-r}\right), \quad \text{and} \quad n = \binom{m}{k} = \frac{1}{k!} m^k + o\left(m^k\right).$$

A direct computation is now sufficient to determine the claimed asymptotic behaviours of $\mathbf{f}_{\mathcal{C}}(n)$ and $\mathbf{F}_{\mathcal{C}}(n)$. □

We now turn our attention to the standard actions of the classical groups. We are going to follow the notation established in [13, Chapters 2 and 4].

We start by considering the possible subspace actions of a classical group whose socle is isomorphic to $\mathrm{PSL}_d(q)$. There are three actions to consider: that on k-subspaces, that on pairs of complementing subspaces, and that on pairs of subspaces, one containing the other. From here on, the symbol $V^{(k)}$ denotes the set of k-dimensional subspaces of the natural module of a classical group. (Lemma 8.2 takes care of the cases (b), (c) and (d) in Table 1).

Lemma 8.2. *Let G be a classical group with linear socle and associated natural module $\mathbb{F}_q^d$ endowed with a subspace action.*

(i) *If the domain of the action is the set of k-subsets, with $k \leq d/2$, then*

$$\mathrm{sep}(G) \leq \begin{bmatrix} d - \lfloor k/2 \rfloor \\ k - \lfloor k/2 \rfloor \end{bmatrix}_q.$$

Consequently, if $\mathcal{C}_k$ is the family of such permutation groups, then

$$\lim_n \frac{\mathbf{f}_{\mathcal{C}_k}(n)}{\sqrt{n}} = \lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{\sqrt{n}} = 1 \quad \textit{for } k \textit{ even,}$$

and

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{n^{\frac{k+1}{2k}}} \leq 1 \quad \textit{for } k \textit{ odd.}$$

(ii) *If the domain of the action is the set of pairs of subspaces complementing each other, one of which has dimension $k \leq d/2$, then*

$$\mathrm{sep}(G) \leq q^{k(d-k)} \begin{bmatrix} d - \lfloor k/2 \rfloor \\ k - \lfloor k/2 \rfloor \end{bmatrix}_q.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Consequently, if $\mathcal{C}_k$ is the family of such permutation groups, then

$$\lim_n \frac{\mathbf{f}_{\mathcal{C}_k}(n)}{\sqrt{n}} = \lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{\sqrt{n}} = 1 \quad \textit{for } k \textit{ even},$$

and

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{n^{\frac{k+1}{2k}}} \leq 1 \quad \textit{for } k \textit{ odd}.$$

(iii) *If the domain of the action is the set of pairs of subspaces, one of dimension $k < d/2$ and the other of dimension $d - k$, the smaller contained in the larger, then*

$$\operatorname{sep}(G) \leq \begin{bmatrix} \lceil (d-k)/2 \rceil \\ \lceil (d-3k)/2 \rceil \end{bmatrix}_q \begin{bmatrix} \lceil (2d-3k)/2 \rceil \\ \lceil k/2 \rceil \end{bmatrix}_q.$$

Consequently, if $\mathcal{C}_k$ is the family of such permutation groups, then

$$\lim_n \frac{\mathbf{F}_{\mathcal{C}_k}(n)}{n^{\frac{k\left\lceil \frac{d-3k}{2} \right\rceil + (d-k)\left\lceil \frac{k}{2} \right\rceil}{k(2d-3k)}}} \leq 1.$$

Proof. We start by considering the action of G on k-subspaces. Let

$$U = \langle e_1, e_2, \ldots, e_{\lfloor k/2 \rfloor} \rangle,$$

and consider the subset

$$A = \left\{ X \in V^{(k)} \,\middle|\, U \leq X \right\}.$$

For every $g \in G$, we can choose a subspace $X_g \in V^{(k)}$ such that

$$U + U^{g^{-1}} \leq X_g.$$

(Note that such a subspace exists because $\dim(U + U^{g^{-1}}) \leq k$.) By construction,

$$U^g + U \leq X_g^g \in A \cap A^g.$$

Hence $A \cap A^g$ is nonempty, and A is self-separable. Observe that

$$|A| = \begin{bmatrix} d - \lfloor k/2 \rfloor \\ k - \lfloor k/2 \rfloor \end{bmatrix}_q = q^{\left(k - \lceil \frac{k}{2} \rceil\right)(d-k)} + O\left(q^{\left(k - \lceil \frac{k}{2} \rceil\right)(d-k)-1}\right),$$

and

$$|V^{(k)}| = \begin{bmatrix} d \\ k \end{bmatrix}_q = q^{k(d-k)} + O\left(q^{k(d-k)-1}\right).$$

Therefore, we can compute that

$$|A| \sim n^{\frac{1}{k}\lceil \frac{k}{2} \rceil}.$$

This concludes the proof of (i).

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Let us now consider the action on pairs of complementary subspaces. Suppose that the smallest one has dimension k. Define

$$U = \langle e_1, e_2, \dots, e_{\lfloor k/2 \rfloor} \rangle,$$

and consider

$$A = \left\{ (X, Y) \in V^{(k)} \times V^{(d-k)} \,\middle|\, V = X \oplus Y \text{ and } U \leq Y \right\}.$$

For every $g \in G$, we choose $(X_g, Y_g) \in V^{(k)} \times V^{(d-k)}$ so that

$$U + U^{g^{-1}} \leq X_g \quad \text{and} \quad V = X_g \oplus Y_g.$$

A similar argument as in the first case shows that A is not self-separable, because $(X_g, Y_g)^g \in A \cap A^g$. Moreover,

$$|A| = q^{k(d-k)} \begin{bmatrix} d - \lfloor k/2 \rfloor \\ k - \lfloor k/2 \rfloor \end{bmatrix}_q = q^{k(d-k)\left(k - \lceil \frac{k}{2} \rceil\right)(d-k)} + O\left(q^{k(d-k)\left(k - \lceil \frac{k}{2} \rceil\right)(d-k)-1}\right),$$

and

$$|\Omega| = q^{k(d-k)} \begin{bmatrix} d \\ k \end{bmatrix}_q = q^{2k(d-k)} + O\left(q^{2k(d-k)-1}\right).$$

Therefore,

$$|A| \sim n^{\frac{1}{k}\lceil \frac{k}{2} \rceil},$$

which is enough to conclude (ii).

Finally, we need to consider the domain of pairs of subspaces, say X and Y, so that $X \in V^{(k)}$, $Y \in V^{(d-k)}$ and $X \leq Y$. In this case, we have to set

$$U = \langle e_1, \dots, e_{\lfloor k/2 \rfloor} \rangle$$

and

$$W = \langle e_1, \dots, e_{\lfloor (d-k)/2 \rfloor} \rangle.$$

Considering the set

$$A = \{ (X, Y) \in V^{(k)} \times V^{(d-k)} \mid X \leq Y,\ U \leq X,\ W \leq Y \},$$

and using similar strategies as before, we conclude that A is not self-separable. In particular, we have

$$\begin{aligned} |A| &= \begin{bmatrix} d - \lfloor (d-k)/2 \rfloor \\ d - k - \lfloor (d-k)/2 \rfloor \end{bmatrix}_q \begin{bmatrix} d - k - \lfloor k/2 \rfloor \\ k - \lfloor k/2 \rfloor \end{bmatrix}_q \\ &= \begin{bmatrix} \lceil (d-k)/2 \rceil \\ \lceil (d-3k)/2 \rceil \end{bmatrix}_q \begin{bmatrix} \lceil (2d-3k)/2 \rceil \\ \lceil k/2 \rceil \end{bmatrix}_q \\ &= q^{k\lceil \frac{d-3k}{2} \rceil + (d-k)\lceil \frac{k}{2} \rceil} + O\left(q^{k\lceil \frac{d-3k}{2} \rceil + (d-k)\lceil \frac{k}{2} \rceil - 1}\right) \end{aligned}$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

and

$$|\Omega| = \begin{bmatrix} d-k \\ k \end{bmatrix}_q \begin{bmatrix} d \\ d-k \end{bmatrix}_q = q^{k(2d-3k)} + O\left(q^{k(2d-3k)-1}\right).$$

Therefore,

$$|A| \sim n^{\frac{k\left\lceil \frac{d-3k}{2} \right\rceil + (d-k)\left\lceil \frac{k}{2} \right\rceil}{k(2d-3k)}}.$$

This completes the proof of the missing case (iii). □

Now let G be a classical group whose socle is not isomorphic to $\mathrm{PSL}_d(q)$. We start by considering the action of G on the totally isotropic or totally singular k-subspaces of its natural module. From here on, with the symbol $V_\bullet^{(k)}$ we refer to the set of k-dimensional subspaces of the formed space $(V, \mathbf{b})$ where $\bullet$ signals a given property, which is clear from context. For instance, in the next proof $V_\bullet^{(k)}$ denotes in a unified way the totally isotropic and totally singular k-subspaces. (Lemma 8.3 takes care of the cases (e), (g), (i), (j) and (k) in Table 1. Moreover, we adopt the notation that if in a product $\prod_{i=a}^{b} x_i$, a is greater than b, then the product is equal to 1).

Lemma 8.3. *Let G be a classical group whose socle is not linear, and consider its subspace action on totally isotropic or totally singular k-subspaces of its natural module V. Then there exists a non-self-separable subset A of the domain whose exact cardinality, as well as the cardinality of the domain, are collected in Table 2.*

Observe that in the first row of Table 2 the symbol δ appears. We have that $\delta = |(2, d) - 2|$, that is, $\delta = 0$ if d is even, and $\delta = 1$ if d is odd.

Moreover, the expressions for $|\Omega|$ and $|A|$ appearing in Table 2 are too complicated to yield a clean explicit asymptotic description. Instead, we content ourselves with the observation that our upper bound can be (trivially) rewritten as

$$|\Omega|^{\log_{|\Omega|} |A|}.$$

By numerical experimentation, for fixed k, the exponent $\log_{|\Omega|} |A|$ appears to approach $1/2$ as $d \to \infty$.

Proof of Lemma 8.3. For the sake of uniformity, let us introduce the parameter

$$m = \dim(V) - 2\dim(M),$$

where M is any totally isotropic or totally singular subspace of maximal dimension. We fix a totally isotropic or a totally singular subspace U with

$$\dim(U) = \frac{\dim(V) - m}{2} - k.$$

Consider the set

$$A = \left\{ X \in V_\bullet^{(k)} \mid X \perp U \right\},$$

and let M be a totally isotropic or totally singular subspace of maximal dimension containing U. For every $g \in G$, we define

$$X_g = (U + U^{g^{-1}})^\perp \cap M.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Note that

$$\dim(X_g) = \dim(M) - \dim\left(\frac{U^{g^{-1}}}{U^{g^{-1}} \cap M}\right) \geq \frac{\dim(V) - m}{2} - \dim(U) = k.$$

We can now choose Y_g, a k-subspace of X_g. Observe that

$$Y_g \leq X_g \leq M = M^{\perp} \leq X_g^{\perp} \leq Y_g^{\perp}$$

and that, by construction,

$$Y_g^g \perp U^g + U,$$

and thus $Y_g^g \in A \cap A^g$. Therefore, A is not self-separable.

We now need to focus on computing $|A|$ and the degree of the actions. Note that the latter is the number of totally isotropic or totally singular k-subspaces in a given formed space: this value can be found in [13, Table 4.1.2]. On the other hand, to count the elements of A we just need to count the number of totally isotropic or totally singular subspaces of $U^{\perp}$. Observe that, as $\mathbf{b}\downarrow_U$ is trivial, $U^{\perp}$ can be written as the orthogonal direct sum $U^{\perp} = U \oplus U^{\perp}/U$, where U is totally isotropic or totally singular, and $(U^{\perp}/U, \mathbf{b}\downarrow_{U^{\perp}/U})$ is a formed space of the same type as $(V, \mathbf{b})$. Furthermore,

$$\dim(U^{\perp}) = \dim(V) - \dim(M) + k = \frac{\dim(V) + m}{2} + k,$$

and

$$\dim(U^{\perp}/U) = \dim(V) - 2\dim(M) + 2k = 2k + m.$$

To every $X \in A$, we can uniquely assign a direct sum decomposition

$$X = (X \cap U) \oplus \left(X \cap U^{\perp}/U\right).$$

Hence, X can be identified with a pair (X_0, X_1), where X_1 is a totally isotropic or totally singular h-subspace in $U^{\perp}/U$, and X_0 with a $(k-h)$-subspace of U. Therefore, if $N_h(U^{\perp}/U)$ denotes the number of totally isotropic or totally singular h-subspaces of $U^{\perp}/U$, we proved that

$$|A| = \sum_{h=\max\{0,2k-\dim(M)\}}^{k} \begin{bmatrix} \dim(M) - k \\ k - h \end{bmatrix}_q N_h(U^{\perp}/U).$$

(Note that the Gaussian coefficient loses meaning if $\dim(M) - k < k - h$. This explains why h varies in the prescribed range.) Finally, by using the formulae of [13, Table 4.1.2], we can compute $|A|$. We have explained a way to compute all the data appearing in Table 2, which completes the proof of Lemma 8.3. □

Once again, let G be a classical group whose socle is not isomorphic to $\mathrm{PSL}_d(q)$. We study the action of G on the nondegenerate k-subspaces of its natural module. (Lemma 8.4 takes care of the cases (f), (h), (m), (n), (o), (p), (q), (r) and (s) in Table 1).

Lemma 8.4. *Let G be a classical group whose socle is not linear, and consider its subspace action on nondegenerate k-subspaces of its natural module V. Then there exists a non-self-separable subset A of the domain whose exact cardinality and asymptotic size in relation to the degree are collected in Table 3.*

In Table 3, the letters B and C refer to the functions

$$B(k,d) = -2 + 3d - 2k \quad \text{and} \quad C(k,d) = -2 + 4d - 4k.$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

In particular, it is interesting to note that, for k fixed,

$$\lim_d \frac{B(k,d)}{C(k,d)} = \frac{3}{4} \quad \text{and} \quad \lim_d \frac{1}{C(k,d)} = 0.$$

Proof. As in the proof of Lemma 8.3, we start by fixing a subspace U. Unlike before, we need to make different choices of U depending on the socle of G and, if the bilinear form is symmetric, depending on whether the subspaces we are acting on are hyperbolic, parabolic, or elliptic. Our choices for U are as follows.

(i) If $\mathrm{soc}(G)$ is unitary, and we are acting on nondegenerate k-subspaces, U is any nondegenerate $\lfloor k/2 \rfloor$-subspace.
(ii) If $\mathrm{soc}(G)$ is symplectic, and we are acting on nondegenerate $2k$-subspaces, U is any nondegenerate $2\lfloor k/2 \rfloor$-subspace.
(iii) If $\mathrm{soc}(G)$ is orthogonal, and we are acting on nondegenerate hyperbolic $2k$-subspaces, U is any nondegenerate hyperbolic $2\lfloor k/2 \rfloor$-subspace.
(iv) If $\mathrm{soc}(G)$ is orthogonal, and we are acting on nondegenerate parabolic $(2k+1)$-subspaces, U is any nondegenerate hyperbolic $2\lfloor k/2 \rfloor$-subspace.
(v) If $\mathrm{soc}(G)$ is orthogonal, and we are acting on nondegenerate elliptic $2k$-subspaces, U is any nondegenerate hyperbolic $2\lfloor (k-1)/2 \rfloor$-subspace.

Consider

$$A = \left\{ X \in V_\bullet^{(h)} \mid U \leq X \right\},$$

where $h \in \{k, 2k, 2k+1\}$ depending on the case we are considering. For every $g \in G$, define

$$X_g = U + U^{g^{-1}}.$$

Note that the restricted form $\mathbf{b}\downarrow_{X_g}$ is sesquilinear, alternating, or symmetric (hyperbolic or parabolic depending on the dimension of X) according to the socle being unitary, symplectic, or orthogonal, respectively. Furthermore,

$$\dim(X_g) \leq 2\dim(U) \leq 2^\epsilon k - \delta,$$

where $\epsilon = 0$ if the socle is unitary, and $\epsilon = 1$ otherwise, and $\delta = 1$ if the socle is orthogonal and the formed subspace is parabolic, $\delta = 2$ if the socle is orthogonal and the formed subspace is elliptic, and $\delta = 0$ otherwise. It is now immediate to build a subspace $Y_g \in V_\bullet^{(k)}$ such that $X_g \leq Y_g$. Moreover, by construction, $Y_g \in A \cap A^g$. Therefore, A is not self-separable.

We need to deal with computing the size of A. Observe that, in any case, $(U, \mathbf{b}\downarrow_U)$ is a nondegenerate formed space whose bilinear form is either sesquilinear, alternating, or hyperbolic bilinear, depending on the socle of G. Therefore, by quotienting by U, A can be thought of as the set of nondegenerate $(h - \dim(U))$-subspaces of V/U. Therefore, the formulae for computing $|A|$ and the degree are readily available in [13, Table 4.1.2]. This information completes the proof of Lemma 8.4. □

We end Section 8.1 on a sour note. An attentive reader might have noticed that we have not discussed case (l) in Table 1, which is the last step to complete the proof of Theorem K. In this case, the socle of G is isomorphic to $\Omega^\epsilon_{2d}(2^f)$, and the domain consists of nonsingular 1-subspaces of the natural module of G. As stated in Remark 2.6, our current method does not give us any control on 1-dimensional subspaces, and we have not developed an *ad hoc* approach for this scenario. Hence, the bound that appears in Theorem K is actually the general bound from Theorem E.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Table 2. *Computation of degree, $|A|$, and asymptotics for $|A|$ for classical groups acting on totally singular or totally isotropic k-subspaces.*

$\mathrm{soc}(G)$	$\lvert\Omega\rvert$	$\lvert A\rvert$
(i) $\mathrm{PSU}_d(q)$	$\dfrac{\prod_{i=d-2k+1}^{d}(q^i-(-1)^i)}{\prod_{i=1}^{k}(q^{2i}-1)}$	$\sum_{h=\max\{0,2k-\lfloor\frac{d}{2}\rfloor\}}^{k}\begin{bmatrix}\lfloor\frac{d}{2}\rfloor-k\\ k-h\end{bmatrix}_q\dfrac{\prod_{i=2k-2h+1+\delta}^{2k+\delta}(q^i-(-1)^i)}{\prod_{i=1}^{h}(q^{2i}-1)}$
(ii) $\mathrm{PSp}_{2d}(q)$	$\dfrac{\prod_{i=d-k+1}^{d}(q^{2i}-1)}{\prod_{i=1}^{k}(q^i-1)}$	$\sum_{h=\max\{0,2k-d\}}^{k}\begin{bmatrix}d-k\\ k-h\end{bmatrix}_q\dfrac{\prod_{i=k-h+1}^{k}(q^{2i}-1)}{\prod_{i=1}^{h}(q^i-1)}$
$(iii)\mathrm{P}\Omega^{+}_{2d}(q)$	$\dfrac{(q^d-1)(q^{d-k}+1)\prod_{i=d-k+1}^{d-1}(q^{2i}-1)}{2^{\delta(d,k)}\prod_{i=1}^{k}(q^i-1)}$	$\sum_{h=\max\{0,2k-d\}}^{k}\begin{bmatrix}d-k\\ k-h\end{bmatrix}_q\dfrac{(q^k-1)(q^{k-h}+1)\prod_{i=k-h+1}^{k-1}(q^{2i}-1)}{2^{\delta(k,h)}\prod_{i=1}^{h}(q^i-1)}$
$(iv)\mathrm{P}\Omega^{-}_{2d}(q)$	$\dfrac{(q^d+1)(q^{d-k}-1)\prod_{i=d-k+1}^{d-1}(q^{2i}-1)}{\prod_{i=1}^{k}(q^i-1)}$	$\sum_{h=\max\{0,2k-d-1\}}^{k}\begin{bmatrix}d-1-k\\ k-h\end{bmatrix}_q\dfrac{(q^{k+1}+1)(q^{k-h+1}-1)\prod_{i=k-h+2}^{k}(q^{2i}-1)}{\prod_{i=1}^{h}(q^i-1)}$
(v) $\Omega_{2d+1}(q)$	$\dfrac{\prod_{i=d-k+1}^{d}(q^{2i}-1)}{\prod_{i=1}^{k}(q^i-1)}$	$\sum_{h=\max\{0,2k-d\rfloor\}}^{k}\begin{bmatrix}d-k\\ k-h\end{bmatrix}_q\dfrac{\prod_{i=k-h+1}^{k}(q^{2i}-1)}{\prod_{i=1}^{h}(q^i-1)}$

8.2. Simple diagonal type

Let us first recall the definition of primitive groups of *simple diagonal type*. Let T be a nonabelian simple group, and let $k \geq 3$ be an integer. Note that we can naturally define three actions on T^k – the right-regular permutation representation of T^k, the component-wise action of $\mathrm{Aut}(T)$, and the action of $\mathrm{Sym}(k)$ permuting indices. We can consider the action induced by these actions on the domain $\Omega = T^k/\mathrm{diag}(T^k)$, where

$$\mathrm{diag}(T^k) = \{(t,\dots,t) \mid t \in T\},$$

Observe that the latter two actions preserve the diagonal of T^k, hence they fall in the stabiliser of a point. For simplicity, we can identify Ω with T^{k-1} via the set of representatives

$$\{(t_1,\dots,t_{k-1},1) \mid t_1,\dots,t_{k-1} \in T\}.$$

Observe that, via this identification, the first $k-1$ components of T^k act on Ω regularly by right multiplication, while the last component acts semiregularly by left multiplication. In particular, every inner automorphism can be realised by choosing two suitable elements in T^{k-1} and T. Therefore, every subgroup of $\mathrm{Sym}(\Omega)$ that preserves the algebraic structure of the domain as $T^k/\mathrm{diag}(T^k)$ can be written as

$$T^k \rtimes (\mathrm{Out}(T) \times \mathrm{Sym}(k))$$

endowed with the action we just described. Therefore, a primitive permutation group G is of simple diagonal type if

$$T^k \trianglelefteq G \leq T^k \rtimes (\mathrm{Out}(T) \times \mathrm{Sym}(k)).$$

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Table 3. *Computation of degree, $|A|$, and asymptotics for $|A|$ for classical groups acting on nondegenerate h-subspaces.*

	$\mathrm{soc}(G)$	Domain	$\lvert\Omega\rvert$	$\lvert A\rvert$	Asymptotics
(i)	$\mathrm{PSU}_d(q)$	k-nondegenerate	$\dfrac{q^{k(d-k)}\prod_{i=d-k+1}^{d}(q^i-(-1)^i)}{\prod_{i=1}^{k}(q^i-(-1)^i)}$	$\dfrac{q^{\lceil\frac{k}{2}\rceil(d-k)}\prod_{i=d-k+1}^{d-\lfloor\frac{k}{2}\rfloor}(q^i-(-1)^i)}{\prod_{i=1}^{\lceil\frac{k}{2}\rceil}(q^i-(-1)^i)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(ii)	$\mathrm{PSp}_{2d}(q)$	$2k$-nondegenerate	$\dfrac{q^{2k(d-k)}\prod_{i=d-k+1}^{d}(q^{2i}-1)}{\prod_{i=1}^{k}(q^{2i}-1)}$	$\dfrac{q^{2\lceil\frac{k}{2}\rceil(d-k)}\prod_{i=d-k+1}^{d-\lfloor\frac{k}{2}\rfloor}(q^{2i}-1)}{\prod_{i=1}^{\lceil\frac{k}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(iii)	$\mathrm{P}\Omega^{+}_{2d}(q)$	$2k$-hyperbolic	$\dfrac{q^{2k(d-k)}(q^d-1)\prod_{i=d-k}^{d-1}(q^{2i}-1)}{2(q^k-1)(q^{d-k}-1)\prod_{i=1}^{k-1}(q^{2i}-1)}$	$\dfrac{q^{2\lceil\frac{k}{2}\rceil(d-k)}(q^{d-\lfloor\frac{k}{2}\rfloor}-1)\prod_{i=d-k}^{d-\lfloor\frac{k}{2}\rfloor-1}(q^{2i}-1)}{2(q^{\lceil\frac{k}{2}\rceil}-1)(q^{d-k}-1)\prod_{i=1}^{\lceil\frac{k}{2}\rceil-1}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(iv)	$\mathrm{P}\Omega^{+}_{2d}(q)$	$(2k+1)$-parabolic	$\dfrac{q^{(2k+1)(2d-2k-1)-1}(q^d-1)\prod_{i=d-k}^{d-1}(q^{2i}-1)}{2\prod_{i=1}^{k}(q^{2i}-1)}$	$\dfrac{q^{(2\lceil\frac{k}{2}\rceil+1)(2d-2k-1)-1}(q^{d-\lfloor\frac{k}{2}\rfloor}-1)\prod_{i=d-k}^{d-\lfloor\frac{k}{2}\rfloor-1}(q^{2i}-1)}{2\prod_{i=1}^{\lceil\frac{k}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{\lceil\frac{k}{2}\rceil+\frac{B}{C}-\frac{1}{C}\lfloor\frac{k}{2}\rfloor}{k+\frac{B}{C}}}$
(v)	$\mathrm{P}\Omega^{+}_{2d}(q)$	$2k$-elliptic	$\dfrac{q^{2k(d-k)}(q^d-1)\prod_{i=d-k}^{d-1}(q^{2i}-1)}{2(q^k+1)(q^{d-k}+1)\prod_{i=1}^{k-1}(q^{2i}-1)}$	$\dfrac{q^{2\lceil\frac{k+1}{2}\rceil(d-k)}(q^{d-\lfloor\frac{k-1}{2}\rfloor}-1)\prod_{i=d-k}^{d-\lfloor\frac{k-1}{2}\rfloor-1}(q^{2i}-1)}{2(q^{\lceil\frac{k+1}{2}\rceil}+1)(q^{d-k}+1)\prod_{i=1}^{\lceil\frac{k-1}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$

(Continued)

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

Table 3. *Continued*

	soc(G)	Domain	$\lvert\Omega\rvert$	$\lvert A\rvert$	Asymptotics
(vi)	$\mathrm{P}\Omega^-_{2d}(q)$	$(2k+1)$-parabolic	$\dfrac{q^{(2k+1)(2d-2k-1)-1}(q^d+1)\prod_{i=d-k}^{d-1}(q^{2i}-1)}{2\prod_{i=1}^{k}(q^{2i}-1)}$	$\dfrac{q^{(2\lceil\frac{k}{2}\rceil+1)(2d-2k-1)-1}(q^{d-\lfloor\frac{k}{2}\rfloor}+1)\prod_{i=d-k}^{d-\lfloor\frac{k}{2}\rfloor-1}(q^{2i}-1)}{2\prod_{i=1}^{\lceil\frac{k}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{\lceil\frac{k}{2}\rceil+\frac{B}{C}-\frac{1}{C}\lfloor\frac{k}{2}\rfloor}{k+\frac{B}{C}}}$
(vii)	$\mathrm{P}\Omega^-_{2d}(q)$	$2k$-elliptic	$\dfrac{q^{2k(d-k)}(q^d+1)\prod_{i=d-k}^{d-1}(q^{2i}-1)}{2(q^k+1)(q^{d-k}-1)\prod_{i=1}^{k-1}(q^{2i}-1)}$	$\dfrac{q^{2\lceil\frac{k+1}{2}\rceil(d-k)}(q^{d-\lfloor\frac{k-1}{2}\rfloor}+1)\prod_{i=d-k}^{d-\lfloor\frac{k-1}{2}\rfloor-1}(q^{2i}-1)}{2(q^{\lceil\frac{k+1}{2}\rceil}+1)(q^{d-k}-1)\prod_{i=1}^{\lceil\frac{k-1}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$
$(viii)$	$\Omega_{2d+1}(q)$	$2k$-hyperbolic	$\dfrac{q^{k(2d-2k+1)}\prod_{i=d-k+1}^{d}(q^{2i}-1)}{2(q^k-1)\prod_{i=1}^{k-1}(q^{2i}-1)}$	$\dfrac{q^{\lceil\frac{k}{2}\rceil(2d-2k+1)}\prod_{i=d-k+1}^{d-\lfloor\frac{k}{2}\rfloor}(q^{2i}-1)}{2(q^{\lceil\frac{k}{2}\rceil}-1)\prod_{i=1}^{\lceil\frac{k}{2}\rceil-1}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k}{2}\rceil}$
(ix)	$\Omega_{2d+1}(q)$	$2k$-elliptic	$\dfrac{q^{k(2d+1-2k)}\prod_{i=d-k+1}^{d}(q^{2i}-1)}{2(q^k+1)\prod_{i=1}^{k-1}(q^{2i}-1)}$	$\dfrac{q^{\lceil\frac{k+1}{2}\rceil(2d-2k+1)}\prod_{i=d-k+1}^{d-\lfloor\frac{k-1}{2}\rfloor}(q^{2i}-1)}{2(q^{\lceil\frac{k+1}{2}\rceil}+1)\prod_{i=1}^{\lceil\frac{k-1}{2}\rceil}(q^{2i}-1)}$	$\lesssim n^{\frac{1}{k}\lceil\frac{k+1}{2}\rceil}$

Note that, to ensure that G is primitive, we need to impose that the action it induces on the k direct factors of T^k is primitive. Meanwhile, G is quasiprimitive if this action is transitive.

Proof of Theorem L. In view of Lemma 3.1, we can concentrate on $G = T^k \rtimes (\mathrm{Out}(T) \times S_k)$, the largest primitive group of diagonal type with socle T^k acting on T^{k-1}. We will build a set $A \subseteq T^{k-1}$ that is not self-separable.

First, let B be any set of elements of T such that

$$|B| \leq \frac{4}{\sqrt{3}}|T|^{\frac{1}{2}},$$

$1 \in B$, and for every $t \in T$, $B \cap Bt$ is nonempty. (Recall that its existence is guaranteed by Theorem F). Define

$$A_0 = B \times \ldots \times B$$

as the direct product of $k-1$ copies of B. Note that

$$|A_0| = |B|^{k-1} \leq \left(\frac{16}{3}|T|\right)^{\frac{k-1}{2}}.$$

Next, let

$$A_1 = TA_0,$$

where the left multiplication by T corresponds to the semiregular action of the last component of the socle. Observe that

$$|A_1| \leq |A_0||T| \leq \left(\frac{16}{3}\right)^{\frac{k-1}{2}} |T|^{\frac{k+1}{2}}.$$

Finally, we let

$$A = A_1^{\mathrm{Out}(T)}.$$

If T is not of Lie type, then $|\mathrm{Out}(T)| \leq 4$. Meanwhile, if T is of Lie type, a direct computation shows that $|\mathrm{Out}(T)| \leq \log_2 |T|$ (see, e.g., [32]). Therefore, by setting $\epsilon = 1$ if T is of Lie type, and $\epsilon = 0$ otherwise,

$$\begin{aligned} |A| &\leq |\mathrm{Out}(T)||A_1| \\ &\leq 4\left(\frac{16}{3}\right)^{\frac{k-1}{2}} |T|^{\frac{k+1}{2}} \left(\frac{1}{4}\log_2 |T|\right)^{\epsilon} \\ &= 4\left(\frac{16}{3}\right)^{\frac{k-1}{2}} n^{\frac{1}{2}+\frac{1}{k-1}} \left(\frac{1}{4k}\log_2 n\right)^{\epsilon}. \end{aligned}$$

It remains to prove that the set A satisfies our conditions, that is, for an arbitrary $g \in G$ we have that $A \cap A^g$ is nonempty. For every $g \in G$, there exist $a \in \mathrm{Sym}(k)$, $b \in \mathrm{Out}(t)$, $c \in T$, and $d \in T^{k-1}$ such that $g = abcd$. We claim that, by construction, A is stabilised by $\mathrm{Sym}(k)$, by $\mathrm{Out}(T)$ and by the left semiregular action of T. The claim is clear for the latter two actions, while we shall prove it for $\mathrm{Sym}(k)$. Recall that $\mathrm{Sym}(k)$ acts on T^k by permuting components, and hence, for every point

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

$(t_1, \dots, t_{k-1}, 1)\mathrm{diag}(T^k)$ and for every $a \in \mathrm{Sym}(k)$,

$$\begin{aligned}\mathrm{diag}(T^k)(t_1, t_2, \dots, t_{k-1}, 1)^a &= \mathrm{diag}(T^k)(t_{1a^{-1}}, t_{2a^{-1}}, \dots, t_{(k-1)x^{-1}}, t_{ka^{-1}}) \\ &= \mathrm{diag}(T^k)(t_{ka^{-1}}^{-1}t_{1a^{-1}}, t_{ka^{-1}}^{-1}t_{2a^{-1}}, \dots, t_{ka^{-1}}^{-1}t_{(k-1)a^{-1}}, 1).\end{aligned}$$

(For simplicity, we denote the action of $\mathrm{Sym}(k)$ on the indices as right multiplication. Moreover, to avoid a cumbersome notation, we identify $1 = t_k$.) Observe that every direct factor of A is equal, and hence the previous formula proves the claim, because

$$A^{\mathrm{Sym}(k)} \subseteq TA = A.$$

Hence, $A^{abc} = A$. Finally, we act with d by component-wise right multiplication. By our choice of B, it follows that

$$|A \cap A^d| \geq |A_0 \cap A_0^d| \geq 1.$$

Therefore, A is not self-separable for G, which completes the proof of the upper bound for $\mathrm{sep}(G)$.

The asymptotic estimates for $\mathbf{F}_{\mathcal{C}}(n)$ are obtained by restricting the attention to the groups of simple diagonal type whose socle is isomorphic to a k-fold Cartesian product of groups of Lie type. (Actually, groups of Lie type of characteristic 2 are those for which the bound on $|\mathrm{Out}(T)|$ cannot be improved, see [32], and thus meet the maximum in $\mathbf{F}_{\mathcal{C}}(n)$.) □

We observe that it would be tempting to retrace the same proof we used for simple diagonal for every family of primitive permutation groups whose socle is regular and nonabelian. Unfortunately, this approach fails because these groups have automorphism groups which contain an isomorphic image of the socle, and hence the resulting upper bound would exceed the degree.

Moreover, in the proof of Theorem L, our starting choice of A_0 implies that the size of A depends on k as an exponential function. Meanwhile, if we had chosen A_0 to be any difference basis of the socle of appropriate size, by imposing the stability of A under the action of $\mathrm{Sym}(k)$, the constant would have been factorial in k. Perhaps, a similar trick could extend our approach beyond the permutation groups of simple diagonal type – but there is no reason not to suspect that the trick would be specific to some limited family of socles, rather than an arbitrary semisimple group.

Acknowledgements. We thank Urban Jezernik for drawing our attention to the graph-theoretic problem that motivated this work. We are grateful to Pablo Spiga for several helpful conversations, particularly regarding the Neumann Separation Lemma, and for identifying an error in an earlier version of the proof of Lemma 7.1. We also thank the anonymous referee for pointing out to us some of the historical context mentioned in Section 1.1.

Competing interests. The authors have no competing interests to declare.

Financial support. The research presented in this paper was initiated during a research visit by Marco Barbieri and Kamilla Rekvényi to IMFM, funded by the Slovenian Research and Innovation Agency, research programme number P1-0294. They gratefully acknowledge the support and hospitality provided. Marco Barbieri is supported by the Slovenian Research Agency programme P1-0222 and grant J1-50001, and he is a member of the Italian GNSAGA INdAM research group. Maruša Lekše and Primož Potočnik are supported by the Slovenian Research and Innovation Agency, programme number P1-0294.

References

[1] M. Alaeiyan, 'On permutation groups with constant movement', *J. Aust. Math. Soc.* **74**(2) (2003), 287–294.
[2] M. Alaeiyan and H. A. Tavallaee, 'Improvement on the bound of intransitive permutation groups with bounded movement', *Bull. Belg. Math. Soc. Simon Stevin* **13**(3) (2006), 471–477.
[3] J. Araújo, P. J. Cameron and B. Steinberg, 'Between primitive and 2-transitive: Synchronization and its friends', *EMS Surv. Math. Sci.* **4** (2017), 101–184.
[4] T. O. Banakh and V. M. Gavrylkiv, 'Difference bases in cyclic groups', *J. Algebra Appl.* **18**(5) (2019), 1950081, 18.
[5] T. O. Banakh and V. M. Gavrylkiv, 'Difference bases in dihedral groups', *Int. J. Group Theory* **8**(1) (2019), 43–50.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

[6] T. O. Banakh and V. M. Gavrylkiv, 'Difference bases in finite Abelian groups', *Acta Sci. Math. (Szeged)* **85**(1-2) (2019), 119–137.
[7] M. Barbieri, M. Lekše, P. Potočnik and K. Rékvenyi, Code supporting the paper 'Separating subsets from their images', URL: https://github.com/barb-maTHrco/Separating-subsets-from-their-images, 2025. Commit f3a672b.
[8] A. Bernshteyn and M. Tait, 'Improved lower bound for difference bases', *J. Number Theory* **205** (2019), 50–58.
[9] E. A. Bertram and M. Herzog, 'On medium-size subgroups and bases of finite groups', *J. Combin. Theory Ser. A* **57**(1) (1991), 1–14.
[10] B. J. Birch, R. G. Burns, S. O. Macdonald and P. M. Neumann, 'On the orbit-sizes of permutation groups containing elements separating finite subsets', *Bull. Aust. Math. Soc.* **14**(1) (1976), 7–10.
[11] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.
[12] R. Brauer and K. A. Fowler, 'On groups of even order', *Ann. of Math.* **62**(3) (1955), 565–583, https://doi.org/10.2307/1970080.
[13] T. C. Burness and M. Giudici, *Classical Groups, Derangements and Primes*, Australian Mathematical Society Lecture Series (Cambridge University Press, 2016).
[14] D. Burns and S. Schuster, 'Every p,p-2 graph is contained in its complement', *J. Graph Theory* **1**(3) (1977), 277–279.
[15] A. R. Calderbank, 'Symmetric designs as the solution of an extremal problem in combinatorial set theory', *European J. Combin.* **9**(2) (1988), 171–173.
[16] P. J. Cameron, 'Finite permutation groups and finite simple groups', *Bull. Lond. Math. Soc.* **13**(1) (1981), 1–22.
[17] P. J. Cameron, C. E. Praeger, J. Saxl and G. M. Seitz, 'On the Sims conjecture and distance transitive graphs', *Bull. Lond. Math. Soc.* **15**(5) (1983), 499–506.
[18] J. R. Cho, P. S. Kim and C. E. Praeger, 'The maximal number of orbits of a permutation group with bounded movement', *J. Algebra* **214**(2) (1999), 625–630.
[19] P. Potočnik, P. Spiga and G. Verret, 'On graph-restrictive permutation groups', *J. Combin. Theory Ser. B* **102**(3) (2012), 820–831.
[20] H. J. Coutts, M. Quick and C. M. Roney-Dougal, 'The primitive permutation groups of degree less than 4096', *Comm. Algebra* **39**(10) (2011), 3526–3546.
[21] J. D. Dixon and B. Mortimer, *Permutation Groups*, Graduate Texts in Mathematics vol. 163 (Springer-Verlag, New York, 1996).
[22] W. Feit and J. G. Thompson, 'Solvability of groups of odd order', *Pacific J. Math.* **13** (1963), 775–1029.
[23] P. Frankl and Z. Füredi, 'Finite projective spaces and intersecting hypergraphs', *Combinatorica* **6** (1986), 335–354.
[24] Z. Füredi, 'Maximum degree and fractional matchings in uniform hypergraphs', *Combinatorica* **1**(2) (1981), 155–162.
[25] B. Ganter, J. Pelikan and L. Teirlinck, 'Small sprawling systems of equicardinal sets', *Ars Combin.* **4** (1977), 133–142.
[26] A. Gardiner, 'Arc transitivity in graphs. III', *Q. J. Math.* **27**(107) (1976), 313–323.
[27] A. Gardiner and C. E. Praeger, 'Transitive permutation groups with bounded movement', *J. Algebra* **168**(3) (1994), 798–803.
[28] M. Giudici and L. Morgan, 'A class of semiprimitive groups that are graph-restrictive', *Bull. Lond. Math. Soc.* **46**(6) (2014), 1226–1236.
[29] M. Giudici and L. Morgan, 'On locally semiprimitive graphs and a theorem of Weiss', *J. Algebra* **427** (2015), 104–117.
[30] A. Hassani, M. Khayaty, E. I. Khukhro and C. E. Praeger, 'Transitive permutation groups with bounded movement having maximal degree', *J. Algebra* **214**(1) (1999), 317–337.
[31] A. S. Hedayat, G. B. Khosrovshahi and D. Majumdar, 'A prospect for a general method of constructing t-designs', *Discrete Appl. Math.* **42**(1) (1993), 31–50.
[32] S. Kohl, 'A bound on the order of the outer automorphism group of a finite simple group of given order', online note, 2003, https://stefan-kohl.github.io/preprints/outbound.pdf.
[33] G. Kozma and A. Lev, 'Bases and decomposition numbers of finite groups', *Arch. Math. (Basel)* **58**(5) (1992), 417–424.
[34] D. Kleitman, L. Finkelstein and T. Leighton, 'Applying the classification theorem for finite simple groups to minimize pin count in uniform permutation architectures (extended abstract)', in *VLSI Algorithms and Architectures (Corfu, 1988)*, Lecture Notes in Comput. Sci. vol. 319 (Springer, New York, 1988), 247–256.
[35] A. Lev, 'On large subgroups of finite groups', *J. Algebra* **152**(2) (1992), 434–438.
[36] M. W. Liebeck, C. E. Praeger and J. Saxl, 'On the O'Nan-Scott theorem for finite primitive permutation groups', *J. Aust. Math. Soc.* **44**(3) (1988), 389–396.
[37] M. W. Liebeck and A. Shalev, 'Bases of primitive permutation groups', in *Groups, Combinatorics and Geometry* (World Scientific, Durham, UK, 2003), 147–154.
[38] H. Macbeth, J. Šiagiová and J. Širáň, 'Cayley graphs of given degree and diameter for cyclic, abelian, and metacyclic groups', *Discrete Math.* **312**(1) (2012), 94–99. Algebraic Graph Theory — A Volume Dedicated to Gert Sabidussi on the Occasion of His 80th Birthday.
[39] A. Maróti, 'On the orders of primitive groups', *J. Algebra* **258**(2) (2002), 631–640.
[40] L. Morgan, 'Vertex-transitive graphs with local action the symmetric group on ordered pairs', *J. Group Theory* **26**(3) (2023), 519–531.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press

[41] L. Morgan, P. Spiga and G. Verret, 'On the order of Borel subgroups of group amalgams and an application to locally-transitive graphs', *J. Algebra* **434** (2015), 138–152.
[42] B. Mortimer, 'The modular permutation representations of the known doubly transitive groups', *Proc. Lond. Math. Soc.* (3) **41**(1) (1980), 1–20.
[43] B. Nathanson, 'On a problem of Rohrbach for finite groups', *J. Number Theory* **41** (1992), 69–76.
[44] B. H. Neumann, 'Groups covered by permutable subsets', *J. Lond. Math. Soc.* **29** (1954), 236–248.
[45] P. M. Neumann and C. E. Praeger, 'An inequality for tactical configurations', *Bull. Lond. Math. Soc.* **28**(5) (1996), 471–475.
[46] P. M. Neumann and C. E. Praeger, 'On the movement of a permutation group', *J. Algebra* **214**(2) (1999), 631–635.
[47] P. M. Neumann, 'The structure of finitary permutation groups', *Arch. Math. (Basel)* **27**(1) (1976), 3–17.
[48] C. E. Praeger, 'The separation theorem for group actions', in *Ordered Groups and Infinite Permutation Groups*, Math. Appl. vol. 354 (Kluwer Acad. Publ., Dordrecht, 1996), 195–219.
[49] C. E. Praeger, 'Finite quasiprimitive graphs', in *Surveys in Combinatorics, 1997 (London)*, London Mathematical Society Lecture Note Series vol. 241 (Cambridge University Press, Cambridge, 1997), 65–85.
[50] C. E. Praeger, 'Movement and separation of subsets of points under group actions', *J. Lond. Math. Soc. (2)* **56**(3) (1997), 519–528.
[51] C. E. Praeger, 'On permutation groups with bounded movement', *J. Algebra* **144**(2) (1991), 436–442.
[52] L. Rédei and A. A. Rényi, 'On the representation of the numbers 1,2, . . . ,N by means of differences', *Mat. Sb. (N.S.)* **24 /66** (1949), 385–389.
[53] H. Robbins, 'A remark on Stirling's formula', *Amer. Math. Monthly* **62**(1) (1955), 26–29.
[54] H. Rohrbach, 'Anwendung eines satzes der additiven zahlentheorie auf eine gruppentheoretische frage', *Math. Z.* **42** (1937), 538–542.
[55] C. M. Roney-Dougal, 'The primitive permutation groups of degree less than 2500', *J. Algebra* **292**(1) (2005), 154–183.
[56] C. M. Roney-Dougal and W. R. Unger, 'The affine primitive permutation groups of degree less than 1000', *J. Symbolic Comput.* **35**(4) (2003), 421–439.
[57] T. Schoen, 'Difference covers', *Combin. Probab. Comput.* **16**(5) (2007), 775–787.
[58] C. C. Sims, 'Computational methods in the study of permutation groups', in *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)* (Pergamon, Oxford-New York-Toronto, Ont., 1970), 169–183.
[59] J. Singer, 'A theorem in finite projective geometry and some applications to number theory', *Trans. Amer. Math. Soc.* **43**(3) (1938), 377–385.
[60] P. Spiga, 'An application of the local $\mathcal{C}(G,T)$ theorem to a conjecture of Weiss', *Bull. Lond. Math. Soc.* **48**(1) (2016), 12–18.
[61] A. P. Street and D. J. Street, *Combinatorics of Experimental Design* (Oxford University Press, Oxford, 1987).
[62] V. I. Trofimov, 'Vertex stabilizers of graphs with projective suborbits', *Dokl. Akad. Nauk SSSR* **315**(3) (1990), 544–546.
[63] V. I. Trofimov, 'Graphs with projective suborbits', *Izv. Akad. Nauk SSSR Ser. Mat.* **55**(4) (1991), 890–916.
[64] V. I. Trofimov, 'On the Weiss conjecture. I', *Trudy Inst. Mat. Mekh.* **28**(1) (2022), 247–256.
[65] R. Weiss, 'Groups with a B, N-pair and locally transitive graphs', *Nagoya Math. J.* **74** (1979), 1–21.
[66] R. Weiss, 'Graphs which are locally Grassmann', *Math. Ann.* **297**(2) (1993), 325–334.

https://doi.org/10.1017/fms.2026.10258 Published online by Cambridge University Press