Deterministic Polynomial Factoring over Finite Fields with Restricted Galois Groups

Zeyu Guo*

Department of Computer Science, University of Haifa
zguotcs@gmail.com

Abstract

Let $\tilde{f}(X) \in \mathbb{Z}[X]$ be a degree-n polynomial such that $f(X) := \tilde{f}(X) \bmod p$ factorizes into n distinct linear factors over $\mathbb{F}_p$. We study the problem of *deterministically* factoring f over $\mathbb{F}_p$ given $\tilde{f}$. Under the generalized Riemann hypothesis (GRH), we give a deterministic algorithm that completely factorizes f in time polynomial in $k^{\log k}$ and the size of the input, where k is the smallest integer such that the nonabelian composition factors of the Galois group G of $\tilde{f}$ are all subquotients of $\mathrm{Sym}(k)$. In particular, if $k = 2^{O(\sqrt{\log n})}$, the algorithm runs in polynomial time.

This result greatly extends Evdokimov's polynomial-time algorithm for solvable polynomials $\tilde{f}$, which corresponds to the case $k \leq 4$. It also subsumes or generalizes several previously known results on deterministic polynomial factoring over finite fields, including Evdokimov's quasipolynomial-time factoring algorithm, which corresponds to the general case $k \leq n$.

Our result is derived from a more general theorem that bounds the time complexity of the factoring algorithm in terms of the alternating groups and the classical groups among the composition factors of G. The proof of this theorem uses techniques from permutation group theory as well as the machinery of $\mathcal{P}$-schemes recently developed by the author.

1 Introduction

The problem of univariate polynomial factoring over finite fields states as follows: Given a univariate monic polynomial $f(X) \in \mathbb{F}_q[X]$ over a finite field $\mathbb{F}_q$, we want to completely factorize f over $\mathbb{F}_q$, i.e., we want to compute the factorization

$$f(X) = \prod_{i=1}^{k} f_i(X)$$

where each $f_i(X)$ is a monic irreducible factor of $f(X)$ over $\mathbb{F}_q$.

This problem plays a fundamental role in computer algebra and has numerous applications to various areas in or related to computer science, such as coding theory, cryptography, algebraic complexity theory, and computation number theory. For example, it is used as a subproblem in the algorithms for polynomial factorization over the rationals or over number fields [LLL82, Len83, Lan85], for multivariate polynomial factorization [Kal85, KT90], for constructing error-correcting codes [Ber68, MS77], for designing public-key cryptosystems [CR88, Odl85], etc.

Univariate polynomial factoring over finite fields has been extensively studied over the years. See, e.g., [vzGP01, Kal03, vzGG13] for general surveys on this problem. In particular, it has been long known that this problem can be solved in *randomized* polynomial time [Ber70, CZ81, vzGS92, KS98, Uma08, KU11].

*Part of this work was done while the author was at the CMS department, Caltech.

On the other hand, finding a *deterministic* polynomial-time algorithm for this problem remains open, despite a lot of attacks [AMM77, Ber67, Ber70, Sch85, vzG87, Rón88, Rón89, Pil90, Sho90, Sho91, Hua91a, Hua91b, Evd92, Rón92, Evd94, CH00, Gao01, IKS09, Gua09, IKRS12, Aro13, BKS15, Guo20]. Finding such an algorithm has great theoretical interest because of the fundamental role of univariate polynomial factoring over finite fields as mentioned above. In this paper, we make progress towards this goal: We give a deterministic algorithm that, assuming the generalized Riemann hypothesis, factorizes $f(X) \in \mathbb{F}_p[X]$ in polynomial time provided that we are also given a polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ lifting $f(X)$ whose Galois group satisfies some moderate restrictions.

1.1 Previous work

Given a degree-n polynomial $f(X) \in \mathbb{F}_q[X]$, a truly polynomial-time factoring algorithm must factorize f in time $\mathrm{poly}(n, \log q)$. Berlekamp [Ber67] gave a deterministic factoring algorithm whose running time is $\mathrm{poly}(n, q)$ instead of $\mathrm{poly}(n, \log q)$. He later improved the time complexity to $\mathrm{poly}(n, \log q, p)$ in [Ber70], where p is the characteristic of $\mathbb{F}_q$. This is still exponential-time when p is exponential in n and $\log q$. In fact, all known (unconditional) deterministic algorithms [Ber67, Ber70, Sho90, BKS15] require exponential time in this setting. The papers [Sho90, BKS15] achieve the running time $\mathrm{poly}(n, \log q) \cdot p^{1/2}$. The $p^{1/2}$-dependence on the characteristic p remains the best known [BKS15]. Faster algorithms are known in some special cases [vzG87, Rón89, Sho91, Sch85, Pil90, IKRS12].

A lot more is known if one accepts the generalized Riemann hypothesis (GRH). Assuming GRH, the paper [AMM77] gave a deterministic polynomial-time algorithm factorizing polynomials of the form $X^n - a \in \mathbb{F}_p[X]$, where a has an n-th root in $\mathbb{F}_p$. Several GRH-based deterministic algorithms were proposed since then. In particular, Rónyai [Rón88] showed that a polynomial $f(X) \in \mathbb{F}_q[X]$ of degree n can be factorized deterministically in time $\mathrm{poly}(n^n, \log q)$ under GRH. Building on Rónyai's work, Evdokimov [Evd94] gave a deterministic $\mathrm{poly}(n^{\log n}, \log q)$-time factoring algorithm under GRH. Evdokimov's algorithm remains the best-known result on GRH-based deterministic polynomial factoring, although the $O(\log n)$ exponent of the running time was later improved by a certain constant factor [CH00, IKS09, Gua09, Aro13].

Efforts were made to understand the combinatorics behind Rónyai's and Evdokimov's algorithms [CH00, Gao01], culminating in the work [IKS09] that proposed the notion of *m-schemes* together with an algorithm that subsumes those in [Rón88, Evd94]. See also the follow-up work [Aro13, AIKS14]. An m-scheme, parametrized by $m \in \mathbb{N}^+$, is a collection of partitions of sets that satisfies a list of axioms. It was shown in [IKS09] that whenever the algorithm fails to produce a proper factorization of $f(X)$, there always exists an m-scheme satisfying strict combinatorial properties. Evdokimov's result can then be interpreted as the fact that such an m-scheme does not exist for sufficiently large $m = O(\log n)$.

In a different approach [Hua91a, Hua91b, Evd92, Rón92], the finite field over which f is defined is assumed to be a prime field $\mathbb{F}_p$, and a *lifted polynomial* of f is assumed to be given, i.e., a monic polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ satisfying $\tilde{f}(X) \bmod p = f(X)$. In particular, Huang [Hua91a, Hua91b] proved that f can be deterministically factorized in polynomial time under GRH if the Galois group G of $\tilde{f}$ (i.e., the automorphism group of the splitting field of $\tilde{f}$) is abelian. This was generalized in [Evd92] to the case that G is solvable. For a general Galois group G, Rónyai [Rón92] gave a deterministic algorithm under GRH that runs in time polynomial in $|G|$ and the size of the input. In general, however, the cardinality of G may be as large as $n!$, attained by the symmetric group of degree n. Thus the algorithm in [Rón92] may take exponential time.

Recently, the author [Guo17, Guo20] proposed a unifying approach for deterministic polynomial factoring over finite fields, which combines the ideas in [Rón88, Evd94, IKS09] and those in the Galois-theoretic approach [Hua91a, Hua91b, Evd92, Rón92]. This approach is based on new combinatorial objects called *$\mathcal{P}$-schemes*, where $\mathcal{P}$ is a collection of subgroups of a finite group G, and G is chosen to be the Galois group of $\tilde{f}$ in applications.

It was shown in [Guo20] that the old results can be derived in a uniform way from this new approach based on $\mathcal{P}$-schemes. More importantly, the techniques developed in this approach may potentially lead to faster factoring algorithms for new families of Galois group G that have special structures. As an example, a deterministic polynomial-time factoring algorithm was given in [Guo20] (under GRH) for the case that G, as a permutation group on the set of roots of $\tilde{f}$, is an almost simple primitive permutation

group whose socle is a subgroup of $\mathrm{Sym}(k)$, where $k = 2^{O(\sqrt{\log n})}$.

1.2 Our results

For simplicity, we make the following assumption about the input polynomial f throughout the paper:

Assumption 1. *f is a monic polynomial defined over a prime field $\mathbb{F}_p$ that factorizes completely into distinct linear factors over $\mathbb{F}_p$, i.e., the roots of f are distinct and all live in $\mathbb{F}_p$.*

Remark. Assumption 1 is not essential and can be safely removed if we replace the $\mathcal{P}$-scheme algorithm [Guo20] used in our proof by the generalized $\mathcal{P}$-scheme algorithm in [Guo17] which works for arbitrary f. For details, see [Guo17, Chapter 5]. In addition, we note that there exists a standard reduction in literature to the case that f factorizes into distinct linear factors [Ber70, Yun76].

Recall that a *subquotient* (or *section*) of a group G is a quotient group of a subgroup of G. For $k \in \mathbb{N}^+$, define a family $\mathcal{C}_k$ of finite groups as follows.

$$\mathcal{C}_k := \{G : \text{every nonabelian composition factor}^1 \text{ of } G \text{ is a subquotient of } \mathrm{Sym}(k)\}.$$

In particular, as $\mathrm{Sym}(4)$ is solvable, $\mathcal{C}_k$ is just the family of finite solvable groups when $k \leq 4$.

We call a monic polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ a *lifted polynomial* of f if $\tilde{f}(X) \bmod p = f(X)$. The following theorem is the easiest to state among our results.

Theorem 1.1. *Under GRH, there exists a deterministic algorithm that, given a degree-n polynomial $f(X) \in \mathbb{F}_p[X]$ satisfying Assumption 1 and a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of f with Galois group G, completely factorizes f over $\mathbb{F}_p$ in time polynomial in $k^{\log k}$ and the size of the input, where k is the smallest positive integer satisfying $G \in \mathcal{C}_k$. In particular, the algorithm runs in polynomial time if $k = 2^{O(\sqrt{\log n})}$.*

Theorem 1.1 greatly extends the main result of [Evd92]: In [Evd92], Evdokimov proved that under GRH, f can be factorized in polynomial time using $\tilde{f}$ when G is solvable, i.e., when $G \in \mathcal{C}_k$ for $k = 4$. This holds more generally for any bounded k, which can be proved by combining the proof in [Evd92] with the result in [BCP82] on primitive permutation groups. However, it is not clear if the techniques in [Evd92] can be easily adapted to give a polynomial-time algorithm for unbounded k. The algorithm in Theorem 1.1, on the other hand, runs in polynomial time for k up to $2^{O(\sqrt{\log n})}$.

Achieving $k = n$ in the last statement of Theorem 1.1 would solve the general problem of deterministic univariate polynomial factoring over finite fields under GRH, as can be seen as follows: By [Ber70, Yun76], this general problem reduces to the problem of factoring f satisfying Assumption 1. We may lift f to some $\tilde{f}(X) \in \mathbb{Z}[X]$ in polynomial time. Note the Galois group G of $\tilde{f}$ can be embedded in $\mathrm{Sym}(n)$, which implies $G \in \mathcal{C}_n$. So it suffices to achieve $k = n$ in the last statement of Theorem 1.1. We move closer to this goal by achieving $k = 2^{O(\sqrt{\log n})}$. See Table 1 for a summary.

Table 1: Known deterministic polynomial-time factoring algorithms for $G \in \mathcal{C}_k$

k	Reference
4	[Evd92]
$O(1)$	[Evd92] + [BCP82]
$2^{O(\sqrt{\log n})}$	**This paper**
n	Goal

Similarly, by choosing $k = n$, the first part of Theorem 1.1 implies a deterministic algorithm that factorizes a degree-n polynomial $f(X) \in \mathbb{F}_q[X]$ in time $\mathrm{poly}(n^{\log n}, \log q)$ under GRH. This matches the

[1]Recall that a *composition series* of G is a finite sequence $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$ such that G_i/G_{i-1} is a simple group for $i \in [k]$. The groups G_i/G_{i-1} are called the *composition factors* of G. By the *Jorden–Hölder Theorem*, the set of composition factors of G does not depend on the choice of composition series.

running time of Evdokimov's algorithm [Evd94]. Thus, Theorem 1.1 may be viewed as a generalization and a "scaled" version of the main result of [Evd94]. Its proof is much more involved, however.

Finally, Theorem 1.1 also generalizes the result in [Guo20] that f can be factorized in deterministic polynomial time using $\tilde{f}$ under GRH if G belongs to the family of almost simple primitive permutation groups whose socle is a subgroup of $\mathrm{Sym}(k)$ with $k = 2^{O(\sqrt{\log n})}$. This is a very special subfamily of $\mathcal{C}_k$,[2] where we make the assumption that G is both primitive and almost simple. This assumption is no longer required in Theorem 1.1.

Example. Suppose $k = 2^{\Theta(\sqrt{\log n})}$ and $m = n/k \in \mathbb{N}$. It is known that there exists a degree-n monic irreducible polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ whose Galois group G is imprimitive (on the set of roots of $\tilde{f}$) and isomorphic to the wreath product $C_m \wr \mathrm{Sym}(k)$ [KM00, §2.2.3]. By Chebotarev's density theorem [Neu99], there exist infinitely many primes $p \in \mathbb{N}$ such that $\tilde{f}(X) \bmod p$ factorizes into n distinct linear factors over $\mathbb{F}_p$. Fix such p. As $G \in \mathcal{C}_k$, our algorithm in Theorem 1.1 factorizes $f(X) := \tilde{f}(X) \bmod p$ using $\tilde{f}$ in time polynomial in the size of $\tilde{f}$ under GRH. On the other hand, Evdokimov's algorithm [Evd94] runs in quasipolynomial time, and Rónyai's algorithm [Rón92] runs in time polynomial in $|G|$ and the size of $\tilde{f}$, where $|G| = m^k k!$ is doubly exponential in $\sqrt{\log n}$.

A more general theorem in terms of alternating groups and classical groups. We derive Theorem 1.1 from a more general theorem (Theorem 1.2). It establishes a finer relationship between the complexity of factoring f using $\tilde{f}$ and the complexity of the group G. Here, the complexity of G is measured in terms of its composition factors, which we explain now.

Recall that the composition factors of a finite group are all *finite simple groups*. By the *classification of finite simple groups (CFSG)*, a finite simple group has one of the following types: a cyclic group of prime order, an alternating group $\mathrm{Alt}(m)$ ($m \geq 5$), a classical group, an exceptional group of Lie type, or one of the 26 sporadic simple groups.

It turns out that only alternating groups and classical groups matter here: we will describe an algorithm that factorizes f using $\tilde{f}$, and its time complexity is controlled by the alternating groups and the classical groups among the composition factors of G.

First, we introduce some notations. It is known that a finite simple classical group has one of the following forms [KL90]:

$$\mathrm{PSL}_m(q),\ \ \mathrm{PSU}_m(q^{1/2}),\ \ \mathrm{PSp}_m(q),\ \ \mathrm{P}\Omega^{\pm}_m(q)\ (m \text{ even}),\ \ \Omega_m(q)\ (m \text{ odd}).$$

We use $\mathrm{Cl}_m(q)$ to denote a group G that has one of the above forms (m is the $\mathbb{F}_q$-dimension of the natural module $\mathbb{F}_q^m$ of G). And we say G has *rank m over the field $\mathbb{F}_q$*. We also write $\mathrm{Cl}_m(q) \in S$ if S is a set that contains a group of one of the above forms. For more details about finite classical groups, see Appendix A.

For a finite group G, define $\mathcal{A}(G)$ (resp. $\mathcal{C}(G)$) to be the set of the alternating groups (resp. classical groups) among the nonabelian composition factors of G. In addition, we need two functions $d_{\mathrm{Sym}}(m)$ and $d_{\mathrm{Lin}}(m, q)$, which will be defined in Section 3 (see Definition 3.16). Theorem 1.2 then states as follows.

Theorem 1.2. *Under GRH, there exists a deterministic algorithm that, given a degree-n polynomial $f(X) \in \mathbb{F}_p[X]$ satisfying Assumption 1 and a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of f with Galois group G, completely factorizes f over $\mathbb{F}_p$ in time polynomial in $N(G)$ and the size of the input, where*

$$\begin{aligned}
&N(G) := \max\{N_{\mathcal{A}}, N_{\mathcal{C}}\},\\
&N_{\mathcal{A}}(G) := \max\{m^{d_{\mathrm{Sym}}(m^c)} : m \in \mathbb{N}^+, \mathrm{Alt}(m) \in \mathcal{A}(G)\},\\
&N_{\mathcal{C}}(G) := \max\{q^{m d_{\mathrm{Lin}}(cm,q)} : m \in \mathbb{N}^+, q \textit{ prime power}, \mathrm{Cl}_m(q) \in \mathcal{C}(G)\},
\end{aligned}$$

and $c \in \mathbb{N}^+$ is a large enough absolute constant. Here $N_{\mathcal{A}}(G)$ (resp. $N_{\mathcal{C}}(G)$) is defined to be zero if $\mathcal{A}(G)$ (resp. $\mathcal{C}(G)$) is empty.

[2]For an almost simple primitive permutation group G with socle T, we have that $T \leq G \leq \mathrm{Aut}(T)$ and T is a finite simple group. By the (now verified) *Schreier Conjecture* [DM96, Section 4.7], the *outer automorphism group* $\mathrm{Aut}(T)/T$ is solvable. It follows that the socle T is the only nonabelian composition factor of G. So $G \in \mathcal{C}_k$ if T is a subgroup of $\mathrm{Sym}(k)$.

If $G \in \mathcal{C}_k$, then every group in $\mathcal{A}(G)$ or $\mathcal{C}(G)$ is a subquotient of $\mathrm{Sym}(k)$. In this case, we will establish the bound $N(G) \leq \mathrm{poly}(k^{\log k})$. Theorem 1.1 then follows immediately from Theorem 1.2.

Theorem 1.2 reduces the factoring problem to proving upper bounds for the functions d_{Sym} and d_{Lin}. It is conjectured that these functions are bounded by an absolute constant [IKS09, Guo20], which together with Theorem 1.2 would imply a deterministic polynomial-time factoring algorithm under GRH. Currently, we have upper bounds $d_{\mathrm{Sym}}(m) = O(\log m)$ and $d_{\mathrm{Lin}}(m, q) \leq m$. Using these bounds, we will derive the following theorem from Theorem 1.2.

Theorem 1.3. *Under GRH, there exists a deterministic algorithm that, given a degree-n polynomial $f(X) \in \mathbb{F}_p[X]$ satisfying Assumption 1 and a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of f with Galois group G, completely factorizes f over $\mathbb{F}_p$ in time polynomial in*

$$N'_{\mathcal{A}}(G) := \max\{m^{\log m} : m \in \mathbb{N}^+, \mathrm{Alt}(m) \in \mathcal{A}(G)\},$$
$$N'_{\mathcal{C}}(G) := \max\{q^{m^2} : m \in \mathbb{N}^+, q \textit{ prime power}, \mathrm{Cl}_m(q) \in \mathcal{C}(G)\},$$

and the size of the input. Here $N'_{\mathcal{A}}(G)$ (resp. $N'_{\mathcal{C}}(G)$) is defined to be zero if $\mathcal{A}(G)$ (resp. $\mathcal{C}(G)$) is empty.

Moreover, the algorithm runs in polynomial time if every alternating group $\mathrm{Alt}(m)$ in $\mathcal{A}(G)$ has degree $m = 2^{O(\sqrt{\log n})}$ and every classical group $\mathrm{Cl}_m(q)$ in $\mathcal{C}(G)$ has rank $m = O(1)$.

Note $|\mathrm{Alt}(m)| = m!/2 \gg m^{\log m}$ and $|\mathrm{Cl}_m(q)| = q^{\Theta(m^2)}$. So Theorem 1.3 strengthens Rónyai's result [Rón92] that under GRH, f can be factorized deterministically using $\tilde{f}$ in time polynomial in $|G|$ and the size of the input.

Remark. The algorithm in Theorem 1.2 and Theorem 1.3 has its time complexity bounded in terms of the sets $\mathcal{A}(G)$ and $\mathcal{C}(G)$. This bears some similarities to a well-known result of Babai, Cameron and Pálfy [BCP82], which states that the order of a primitive permutation group G on a finite set S is polynomial in $|S|$ if all the members of $\mathcal{A}(G)$ have bounded degree and all the members of $\mathcal{C}(G)$ have bounded rank. In fact, our proof relies on works on primitive permutation groups [GSS98, LS99, LS02, LS14] that followed and strengthened the result of Babai et al.

Functions d_{Sym} and d_{Lin}. We briefly discuss the functions d_{Sym} and d_{Lin} to be defined in Section 3. For every finite group G acting on a finite set, an integer $d(G) \in \mathbb{N}^+$ was defined in [Guo20], which is related to the time complexity of a factoring algorithm given in [Guo20]. The functions d_{Sym} and d_{Lin} are defined in terms of $d(G)$: we let $d_{\mathrm{Sym}}(m) = d(G)$ where G is chosen to be the symmetric group $\mathrm{Sym}(m)$ acting naturally on $[m]$. The definition of $d_{\mathrm{Lin}}(m, q)$ is similar except that we use natural actions of (subgroups of) general linear groups. The insight of Theorem 1.2 is that, instead of bounding $d(G)$ for G associated with an arbitrary group action, we just need to bound d_{Sym} and d_{Lin} which are associated with very special group actions (namely, natural actions of symmetric groups or linear groups).

Future work. As mentioned above, Theorem 1.3 is derived from Theorem 1.2 using known upper bounds $d_{\mathrm{Sym}}(m) = O(\log m)$ and $d_{\mathrm{Lin}}(m, q) \leq m$. Improvements over these bounds would further improve the time complexity in Theorem 1.3. In fact, one such improvement over d_{Lin} was recently achieved in [Guo19]: Let $m \in \mathbb{N}^+$, q be a prime power and $n = q^m$. We know $d_{\mathrm{Lin}}(m, q) \leq m = O(\log n)$ since $q \geq 2$. Using tools from additive combinatorics, the paper [Guo19] proved $d_{\mathrm{Lin}}(m, q) = o(\log n)$ regardless of q. A corollary of this result is that in Theorem 1.2, the contribution $N_{\mathcal{C}}(G)$ from classical groups is $n^{o(\log n)}$. So the contribution $N_{\mathcal{A}}(G)$ from alternating groups is the only bottleneck for finding an $n^{o(\log n)}$-time deterministic factoring algorithm under GRH. In particular, the algorithm in Theorem 1.2 runs in time polynomial in $n^{o(\log n)}$ and the size of the input if every alternating group $\mathrm{Alt}(m)$ in $\mathcal{A}(G)$ has degree $m = n^{o(1)}$.

1.3 Overview of the proof

We present an overview of the proof of Theorem 1.2. It consists of the following steps:

1) Applying the machinery of $\mathcal{P}$-schemes. The first step of the proof is using the machinery of $\mathcal{P}$-schemes developed in [Guo17, Guo20] to reduce the problem to a combinatorial problem regarding the Galois group G of $\tilde{f}$.

Specifically, let L be the splitting field of $\tilde{f}$. By Galois theory, the subfields of L correspond one-to-one to the subgroups of G. It was proved in [Guo20] that, roughly speaking, if one can construct a collection $\mathcal{F}$ of subfields L, such that for the corresponding set $\mathcal{P}$ of Galois subgroups of G, a certain combinatorial condition about $\mathcal{P}$-schemes is satisfied, then f can be factorized in time $\mathrm{poly}(T)$ under GRH, where T is the time needed to construct $\mathcal{F}$. We restate this result formally as Theorem 3.6 and apply it as a black box. This theorem reduces the problem of factoring f using $\tilde{f}$ to the problem of constructing a set $\mathcal{F}$ of number fields and verifying that the corresponding set $\mathcal{P}$ of subgroups satisfies the required combinatorial condition.

Our algorithm of constructing $\mathcal{F}$ is relatively straightforward. The rest of the proof then focuses on the new problem of verifying the combinatorial condition as required by Theorem 3.6.

2) Reducing to the case of primitive permutation groups. The new problem is defined with respect to the Galois group G, which may be regarded as a permutation group on the set of roots of $\tilde{f}$. Thus, we may apply ideas and techniques from (finite) permutation group theory to analyze the problem. First, we reduce to the case that G is a *primitive permutation group*. These groups are considered to be building blocks in permutation group theory, which are better understood than general or transitive permutation groups. The reduction we use was originally developed in [LM85, Evd92]. It has the effect of replacing the group G with certain subquotients G_i of G. These subquotients, which are primitive permutation groups, are called "primitive components" of G in [Wie64].

One problem we need to solve in order to establish the reduction is showing that replacing G with each G_i does not increase the complexity of the group by much, where the complexity of a finite group is measured in terms of its nonabelian composition factors as in Theorem 1.2. A similar problem exists in [LM85, Evd92] which addresses only solvable groups. But it has an easy solution in these papers because the groups G_i are subquotients of G, and solvability is preserved by taking a subquotient. We prove a lemma (Lemma 4.5) which states that even for general finite groups, taking a subquotient does not blow up the complexity by much. Its proof uses a result of Kovács and Praeger [KP00] on the degree of minimal faithful permutation representation of finite groups. This lemma itself may be of independent interest.

3) Applying the O'Nan-Scott theorem for primitive permutation groups. Finally, we verify the combinatorial condition in Theorem 3.6 for primitive permutation groups. This is formally stated as Lemma 5.3, and its proof is the most technical part of this paper.

To prove Lemma 5.3, we apply the O'Nan-Scott theorem for finite primitive permutation groups [LPS88], which classifies finite primitive permutation groups into the following five types: almost simple type, affine type, diagonal type, product type, and twisted wreath type. Then we prove Lemma 5.3 for each of these five cases.

The almost simple type and the affine type are the most difficult cases. To prove Lemma 5.3 for G of almost simple type, we invoke a theorem of Liebeck and Shalev [LS99] that classifies primitive permutation groups G of almost simple type with unbounded minimal base size. The socle of such G is either an alternating group or a simple classical group. The former case was already addressed in [Guo20]. In the latter case, G is equipped with a "subspace action" [LS99]. We then prove Lemma 5.3 for these subspace actions.

To address G of affine type, we first reduce to the case of irreducible linear groups, and then to the case of primitive linear groups. Next, we apply a structure theorem of Liebeck and Shalev [LS02, LS14] which states that roughly speaking, a primitive linear group G admits a "tensor product decomposition" and is built up from smaller groups that are symmetric groups and classical groups. This allows us to reduce the problem to smaller subproblems, which leads to a proof of Lemma 5.3 for G of affine type.

The remaining three cases (diagonal type, product type, and twisted wreath type) can either be analyzed directly or reduced to other cases: Specifically, when G is of the diagonal type, we show that the algorithm always runs in polynomial time. The product type is tackled by reducing to the almost

simple type and the diagonal type. The twisted wreath type is tackled by reducing to the product type, where we use an observation in [Pra90] that a group of twisted wreath type can be embedded in another group of product type.

Figure 1 illustrates the logical dependencies among the various families of groups in our proof.

Remark. We remark that the above steps (reducing to the primitive case, applying the O'Nan-Scott Theorem, and then analyzing each case individually) follow a common framework for the study of problems related to finite permutation groups. See [Asc08, Page 2] for an explanation of this framework. The specific analysis under this framework varies with each problem.

Regarding our problem, we show that it has some interesting connection to the well-studied problem of bounding the *minimum base size* of primitive permutation groups [GSS98, LS99, LS02, Ben05, LS14, HLM19]. In particular, our algorithm runs in polynomial time if the Galois group G has a constant minimum base size. This is very useful since there are various results in the literature of the form "a permutation group G from some family $\mathcal{C}$ either has a constant minimum base size or is in one of few special cases". See, e.g., [LS99, LS02, LS14]. Therefore, given $G \in \mathcal{C}$, we may assume G is in one of the few special cases.

Another technique repeatedly used in our analysis is a lemma introduced in [Guo17, Guo20] called the *self-reduction lemma*. Roughly speaking, it has the effect of replacing the group G with its stabilizer subgroups, which often dramatically simplifies the problem. We use this lemma to reduce the problems for various group actions appearing in our analysis to the problems for the natural action of symmetric groups or linear groups. See Section 6 for more details.

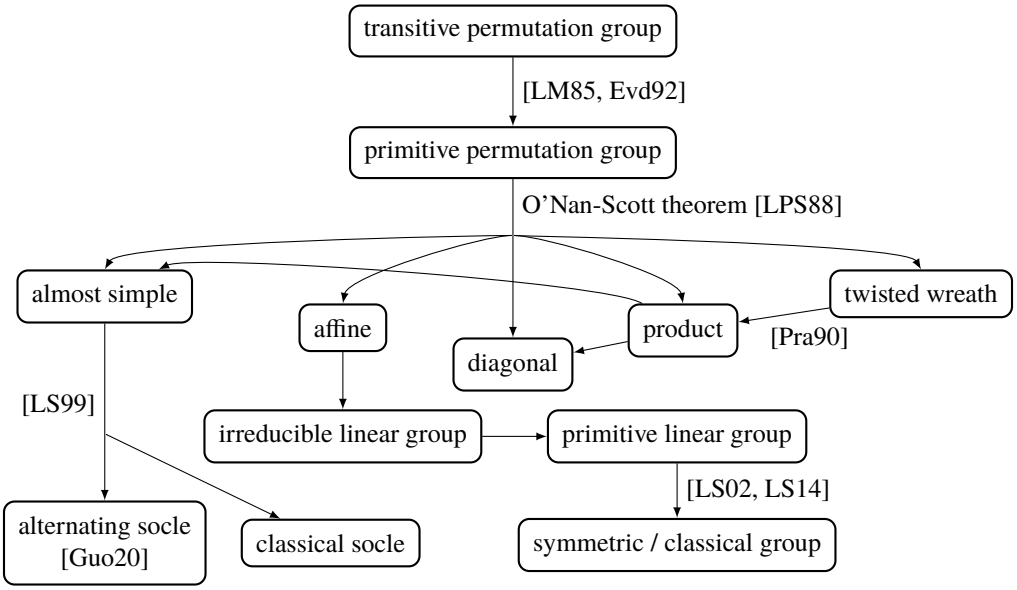

Figure 1: Logical dependencies among the various families of groups

Outline of the paper. Preliminaries and notations are given in Section 2. In Section 3, we define $\mathcal{P}$-schemes and list some useful results about these objects, mostly proven in [Guo20]. We also define and discuss the functions d_{Sym} and d_{Lin}. In Section 4, we establish a reduction to the case of primitive permutation groups. The proofs of Theorem 1.1–1.3 are given in Section 5, assuming Lemma 5.3 which states that a certain combinatorial condition is satisfied by primitive permutation groups.

Section 6 is devoted to the proof of Lemma 5.3: We first state the self-reduction lemma in Subsection 6.1 and the O'Nan-Scott theorem in Subsection 6.2. Next, in Subsections 6.3–6.6, we prove that Lemma 5.3 holds for each of the five types of primitive permutation groups in the O'Nan-Scott theorem, which completes the whole proof.

Finally, some open problems are given in Section 7.

2 Preliminaries and notations

Let $\mathbb{N} := \{0, 1, 2, \dots\}$ and $\mathbb{N}^+ := \{1, 2, \dots\}$. Let $[k] := \{1, 2, \dots, k\}$. For sets A, B, write $A - B$ for the set difference $\{x : x \in A \text{ and } x \notin B\}$. The cardinality of a set S is $|S|$. Denotes by $\mathbb{F}_q$ the finite field of cardinality q, where q is a prime power. The identity element of a group is denoted by e.

The dual space of a vector space V is denoted by V^*. For vectors $x_1, \dots, x_k \in V$, write $\langle x_1, \dots, x_k \rangle$ for their linear span. For subspaces $U_1, U_2 \subseteq V$, write $U_1 + U_2$ for their sum, i.e., the linear span of $U_1 \cup U_2$. The sum is a *direct sum* if $U_1 \cap U_2 = \{0\}$, in which case we also write $U_1 \oplus U_2$. A *complement* of a subspace $U \subseteq V$ in V is a subspace $W \subseteq V$ such that $V = U \oplus W$.

A *partition* of a set S is a set P of nonempty subsets of S satisfying $S = \coprod_{B \in P} B$, where $\coprod$ denotes the disjoint union. Each $B \in P$ is called a *block* of P. Denote by 0_S the coarsest partition of S and by ∞_S the finest partition of S, i.e., $0_S = \{S\}$ and $\infty_S = \{\{x\} : x \in S\}$. For $T \subseteq S$ and a partition P of S, we have the partition $P|_T := \{B \cap T : B \in S\} - \{\emptyset\}$ of T, called the *restriction* of P to T.

Let G be a group and S be a set. A *(left) action* of G on S is a function $\varphi : G \times S \to S$ satisfying (1) $\varphi(e, x) = x$ for all $x \in S$ and (2) $\varphi(g, \varphi(h, x)) = \varphi(gh, x)$ for all $x \in S$ and $g, h \in G$. We also say G *acts on* S and S is a *G-set*. Write ${}^g x$ for $\varphi(g, x)$ when φ is clear from the context. Sometimes we write G^S in place of G to indicate that S is the underlying set on which G acts.

Let S be a G-set. The *orbit* or *G-orbit* of $x \in S$ is $Gx := \{{}^g x : g \in G\}$. A subset of a G-set is a *G-subset* if it is a disjoint union of G-orbits. For $T \subseteq S$, denote by G_T the (pointwise) stabilizer subgroup $\{g \in G : {}^g x = x \text{ for } x \in T\}$. We also write $G_{x_1,\dots,x_k}$ for G_T when $T = \{x_1, \dots, x_k\}$.

An action of G on a set S is *transitive* if it has only one orbit. It is *semiregular* if G_x is trivial for all $x \in S$. An action is *regular* if it is both transitive and semiregular. For $k \in \mathbb{N}^+$, an action of G on S induces an action on S^k via ${}^g(x_1, \dots, x_k) = ({}^g x_1, \dots, {}^g x_k)$, called the *diagonal action* of G on S^k.

Definition 2.1 (left and inverse right translation)**.** *Let H and K be subgroups of G. We say K acts on G/H by* left translation *if ${}^g hH = ghH$ for $hH \in G/H$ and $g \in K$. Similarly, K acts on $H\backslash G$ by* inverse right translation *if ${}^g Hh = Hhg^{-1}$ for $Hh \in H\backslash G$ and $g \in K$.*

Denote by $\mathrm{Gal}(L/K)$ the Galois group of a Galois extension L/K. For a subgroup $H \leq \mathrm{Gal}(L/K)$, denote by L^H the *fixed subfield* of H, i.e., $L^H := \{a \in L : {}^g a = a \text{ for } g \in H\}$.

The Galois group of a polynomial $f(X) \in K[X]$ over K is defined to be $\mathrm{Gal}(L_f/K)$, where L_f is the splitting field of f over K. Also denote this group by $\mathrm{Gal}(f/K)$. We assume $K = \mathbb{Q}$ if it is not explicitly mentioned.

Permutation groups. An action of G on a set S gives a group homomorphism $\rho : G \to \mathrm{Sym}(S)$, called a *permutation representation* of G on S. Call $|S|$ the *degree* of ρ. We say ρ is *faithful* if it is injective. The image $\rho(G)$ is called a *permutation group* on S. When ρ is faithful and clear from the context, we simply say G is a permutation group on S.

A *base* of a permutation group G on a set S is a subset $T \subseteq S$ such that the pointwise stabilizer G_T is trivial. Denote by $b(G)$ the *minimal base size* of G.

Equivalent actions and permutation isomorphic actions. Let G be a group and let S, T be G-sets. We say the action of G on S and that on T are *equivalent* if there exists a bijective map $\lambda : S \to T$ satisfying $\lambda({}^g x) = {}^g(\lambda(x))$ for $x \in S$ and $g \in G$.

More generally, suppose $\phi : G \to H$ is a group isomorphism, S is a G-set, and T is an H-set. We say the action of G on S is *permutation isomorphic* to the action of H on T under the map ϕ if there exists a bijective map $\lambda : S \to T$ satisfying $\lambda({}^g x) = {}^{\phi(g)}(\lambda(x))$ for $x \in S$ and $g \in G$. When the actions are clear, we often simply say G is permutation isomorphic to H under ϕ (with respect to λ).

It is well known that any transitive group action is equivalent to the action on a left (resp. right) coset space by left (resp. inverse right) translation. We state it formally for right coset spaces as follows.

Lemma 2.2. *Let G be a group acting transitively on a set S. For any $x \in S$, the map $\lambda_x : S \to G_x\backslash G$ sending ${}^g x$ to $G_x g^{-1}$ for $g \in G$ is well-defined and is an equivalence between the action of G on S and that on $G_x\backslash G$ by inverse right translation.*

Finally, we need the following definition that further generalizes the notion of permutation isomorphism.

Definition 2.3. *Let G be a group acting on a set S and H be a group acting on a set T. So we have permutation representations $\rho : G \to \mathrm{Sym}(S)$ and $\rho' : H \to \mathrm{Sym}(T)$. We say G acting on S and H acting on T* have permutation isomorphic images *if the action of $\rho(G)$ on S is permutation isomorphic to the action of $\rho'(H)$ on T.*

Obviously, the relation of having permutation isomorphic images is an equivalence relation. The following lemma gives a sufficient condition for this relation. Its proof is routine and can be found in Appendix B.

Lemma 2.4. *Let G (resp. H) be a group acting transitively on a set S (resp. T). Let $\bar{H} \leq \mathrm{Sym}(T)$ be the image of H under the permutation representation $H \to \mathrm{Sym}(T)$. Let $x \in S$ and $y \in T$. Suppose $\phi : G \to H$ is a group homomorphism such that (1) $G_x = \phi^{-1}(H_y)$ and (2) the image of $\phi(G) \leq H$ in $\bar{H}$ equals $\bar{H}$. Then G acting on S and H acting on T have permutation isomorphic images.*

3 $\mathcal{P}$-schemes

In this section, we review the theory of $\mathcal{P}$-schemes developed in [Guo20]. We also introduce related notions including the functions d_{Sym} and d_{Lin}.

3.1 Definition of $\mathcal{P}$-schemes

Let G be a finite group. A set $\mathcal{P}$ of subgroups of G is called a *subgroup system over G* if $\mathcal{P}$ is closed under conjugation, i.e., $gHg^{-1} \in \mathcal{P}$ for $H \in \mathcal{P}$ and $g \in G$. Define the following two kinds of maps between right coset spaces $H\backslash G$ for various subgroups $H \leq G$:

- For $H \leq H' \leq G$, define the *projection* $\pi_{H,H'} : H\backslash G \to H'\backslash G$ to be the map sending $Hg \in H\backslash G$ to $H'g \in H'\backslash G$.
- For $H \leq G$ and $g \in G$, define the *conjugation* $c_{H,g} : H\backslash G \to gHg^{-1}\backslash G$ to be the map sending $Hh \in H\backslash G$ to $(gHg^{-1})gh \in gHg^{-1}\backslash G$.

Definition 3.1 ($\mathcal{P}$-scheme)**.** *Let $\mathcal{P}$ be a subgroup system over G. A* $\mathcal{P}$-collection *is a set $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ indexed by $\mathcal{P}$, where C_H is a partition of $H\backslash G$ for $H \in \mathcal{P}$. Moreover, we say $\mathcal{C}$ is a* $\mathcal{P}$-scheme *if it has the following properties:*

(Compatibility): *For $H, H' \in \mathcal{P}$ with $H \leq H'$ and $x, x' \in H\backslash G$ in the same block of C_H, $\pi_{H,H'}(x)$ and $\pi_{H,H'}(x')$ are in the same block of $C_{H'}$.*

(Invariance): *For $H \in \mathcal{P}$ and $g \in G$, the map $c_{H,g} : H\backslash G \to gHg^{-1}\backslash G$ maps any block of C_H bijectively to a block of $C_{gHg^{-1}}$.*

(Regularity): *For $H, H' \in \mathcal{P}$ with $H \leq H'$, any block $B \in C_H$, $B' \in C_{H'}$, the number of $x \in B$ satisfying $\pi_{H,H'}(x) = y$ is a constant when y ranges over the set B'.*

In addition, we say a $\mathcal{P}$-scheme $\mathcal{C}$ is discrete *on $H \in \mathcal{P}$ if C_H is the finest partition $\infty_{H\backslash G}$ of $H\backslash G$.*

Lemma 3.2 ([Guo20])**.** *Let $\mathcal{P}$ be a subgroup system over G and $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ be a $\mathcal{P}$-scheme. For $H, H' \in \mathcal{P}$ with $H \leq H'$, we have $C_{H'} = \{\pi_{H,H'}(B) : B \in C_H\}$. In particular, if $C_H = \infty_{H\backslash G}$, then $C_{H'} = \infty_{H'\backslash G}$.*

Proof. Consider $B \in C_H$ and $B' \in C_{H'}$ such that $\pi_{H,H'}(B) \cap B' \neq \emptyset$. By compatibility of $\mathcal{C}$, we have $\pi_{H,H'}(B) \subseteq B'$. Assume to the contrary that $\pi_{H,H'}(B) \neq B'$. Choose $y \in \pi_{H,H'}(B)$ and $y' \in B' - \pi_{H,H'}(B)$. Then we have $|\{x \in B : \pi_{H,H'}(x) = y\}| > 0$ but $|\{x \in B : \pi_{H,H'}(x) = y'\}| = 0$, which contradicts regularity of $\mathcal{C}$. So $\pi_{H,H'}(B) = B'$. □

Next, we define *strong antisymmetry* of $\mathcal{P}$-schemes, which is crucial for the factoring algorithm in [Guo20].

Definition 3.3 (strong antisymmetry)**.** *A $\mathcal{P}$-scheme $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ is* strongly antisymmetric *if for any sequence of subgroups $H_0, \ldots, H_k \in \mathcal{P}$, $B_0 \in C_{H_0}, \ldots, B_k \in C_{H_k}$, and maps $\sigma_1, \ldots, \sigma_k$ satisfying*

1. *σ_i is a bijective map from B_{i-1} to B_i,*
2. *σ_i is of the form $c_{H_{i-1},g}|_{B_{i-1}}$, $\pi_{H_{i-1},H_i}|_{B_{i-1}}$, or $(\pi_{H_i,H_{i-1}}|_{B_i})^{-1}$,*
3. *$H_0 = H_k$ and $B_0 = B_k$,*

the composition $\sigma_k \circ \cdots \circ \sigma_1$ is the identity map on $B_0 = B_k$. In other words, $\mathcal{C}$ is strongly antisymmetric if no nontrivial permutation of any block in any partition C_H can be obtained by composing maps of the form $c_{H_{i-1},g}|_{B_{i-1}}$, $\pi_{H_{i-1},H_i}|_{B_{i-1}}$, or $(\pi_{H_i,H_{i-1}}|_{B_i})^{-1}$.

Relating $\mathcal{P}$-schemes to polynomial factoring. For a Galois extension L/F of number fields and a collection $\mathcal{F}$ of intermediate fields between L and F, we associate a subgroup system $\mathcal{P}$ as follows.

Definition 3.4. *Let L/F be a Galois extension of number fields, and let $\mathcal{F}$ be a collection of number fields that contain F and are isomorphic to subfields of L over F. Define*

$$\mathcal{P} = \left\{H \leq \mathrm{Gal}(L/F) : \textit{there exist } K \in \mathcal{F} \textit{ and an isomorphism between } L^H \textit{ and } K \textit{ over } F\right\}.$$

Then $\mathcal{P}$ is a subgroup system over $G := \mathrm{Gal}(L/F)$, called the subgroup system associated with $(\mathcal{F}, L/F)$.

We are mostly interested in the case $F = \mathbb{Q}$ in Definition 3.4, but part of the proof in this paper requires us to work over a general base field F.

For convenience, we also make the following definition.

Definition 3.5. *Let $\mathcal{P}$ be a subgroup system over G and let $H \in \mathcal{P}$. We call $(\mathcal{P}, G, H)$ a* factoring system *if all strongly antisymmetric $\mathcal{P}$-schemes $\mathcal{C} = \{C_K : K \in \mathcal{P}\}$ are discrete on H, i.e., $C_H = \infty_{H\backslash G}$.*

The following result is the main theorem of [Guo20], which relates $\mathcal{P}$-schemes to polynomial factoring over finite fields.

Theorem 3.6 ([Guo20, Theorem 1.2])**.** *Let $\mathcal{I}$ be a family of instances of the input $(f, \tilde{f})$ where $f(X) \in \mathbb{F}_p[X]$ satisfies Assumption 1 and $\tilde{f}(X) \in \mathbb{Z}[X]$ is a lifted polynomial of f. Suppose there exists a deterministic algorithm that given an instance $s = (f, \tilde{f}) \in \mathcal{I}$, constructs in time $T(s)$ a collection $\mathcal{F}$ of number fields that are isomorphic to subfields of the splitting field L of $\tilde{f}$ over $\mathbb{Q}$, such that*

(1) $\mathbb{Q}[X]/(\tilde{f}_i(X)) \in \mathcal{F}$ for all monic irreducible factors $\tilde{f}_i$ of $\tilde{f}$ over $\mathbb{Q}$, and

(2) $(\mathcal{P}, G, G_\alpha)$ is a factoring system for all $\alpha \in S$, where S is the set of roots of $\tilde{f}$ in L, $G := \mathrm{Gal}(L/\mathbb{Q})$ is regarded a permutation group on S, and $\mathcal{P}$ is the subgroup system over G associated with $(\mathcal{F}, L/\mathbb{Q})$.

Then under GRH, there exists a deterministic algorithm that given $s = (f, \tilde{f}) \in \mathcal{I}$, outputs the complete factorization of f over $\mathbb{F}_p$ in time polynomial in $T(s)$ and the size of s.

We use Theorem 3.6 as a black box throughout this paper. Its proof and the corresponding algorithm can be found in [Guo20].

3.2 Basic facts about $\mathcal{P}$-schemes

We list some facts about $\mathcal{P}$-schemes that will be used later. First, we note that G acts on the set of $\mathcal{P}$-schemes by inverse right translation:

Lemma 3.7. *G acts on the set of $\mathcal{P}$-schemes via ${}^g\mathcal{C} = \{{}^gC_H : H \in \mathcal{P}\}$ for $g \in G$, where ${}^gC_H := \{{}^gB : B \in C_H\}$ and ${}^gB := \{Hhg^{-1} : Hh \in B\} \subseteq H\backslash G$ for $B \in C_H$ and $H \in \mathcal{P}$.*

Proof. We just need to verify that ${}^g\mathcal{C}$ is a $\mathcal{P}$-scheme if $\mathcal{C}$ is. Observe that the maps $\pi_{H,H'}$ and $c_{H,h}$ defined in Subsection 3.1 are G-invariant with respect to the action of G by inverse right translation (see [Guo20, Lemma 3.1]). It is then straightforward to check that if $\mathcal{C}$ satisfies the three properties in Definition 3.1 (compatibility, invariance, and regularity), so does ${}^g\mathcal{C}$. □

The following result was essentially proved in [Guo20].

Lemma 3.8. *Suppose G is a finite group, G' is a subgroup of G, and $\mathcal{P}$ is a subgroup system over G. Let $\mathcal{P}' = \{G' \cap H : H \in \mathcal{P}\}$, which is a subgroup system over G'. For $H \in \mathcal{P}$, if $(\mathcal{P}, G, H)$ is a factoring system, then $(\mathcal{P}', G', G' \cap gHg^{-1})$ is a factoring system for all $g \in G$.*

Proof. By [Guo20, Definition B.2 and Theorem B.3], if there exists a strongly antisymmetric $\mathcal{P}'$-scheme that is not discrete on $G' \cap gHg^{-1}$ for some $g \in G$, then there exists a strongly antisymmetric $\mathcal{P}$-scheme that is not discrete on H. Its contrapositive is just the lemma. □

Restriction to a subgroup. We need a construction called the *restriction of $\mathcal{P}$-schemes* [Guo20]. For a subgroup system $\mathcal{P}$ over a finite group G and a subgroup $G' \leq G$, let $\mathcal{P}|_{G'} := \{H \in \mathcal{P} : H \leq G'\}$, which is a subgroup system over G'.

Definition 3.9 ([Guo20, Definition 5.1])**.** *Suppose $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ is a $\mathcal{P}$-scheme. For $H \in \mathcal{P}|_{G'}$, regard $H\backslash G'$ as a subset of $H\backslash G$ in the obvious way. Then for $H \in \mathcal{P}|_{G'}$, the partition C_H of $H\backslash G$ restricts to a partition of $H\backslash G'$, which we denote by $C_H|_{G'}$. Define $\mathcal{C}|_{G'} := \{C_H|_{G'} : H \in \mathcal{P}|_{G'}\}$, called the* restriction *of $\mathcal{C}$ to G'.*

Lemma 3.10 ([Guo20, Lemma 5.2])**.** *$\mathcal{C}|_{G'}$ in Definition 3.9 is a $\mathcal{P}|_{G'}$-scheme. Moreover, if $\mathcal{C}$ is strongly antisymmetric, so is $\mathcal{C}|_{G'}$.*

Passing to a quotient group. If N is a normal subgroup of G such that $N \leq H$ for all $H \in \mathcal{P}$, we can quotient N out and replace G with G/N. This gives:

Lemma 3.11. *Suppose G is a finite group and N is a normal subgroup of G. Let $\mathcal{P}$ be a subgroup system over G such that $N \leq H$ for all $H \in \mathcal{P}$. Let $\bar{\mathcal{P}} = \{H/N : H \in \mathcal{P}\}$, which is a subgroup system over G/N. For $H \in \mathcal{P}$, there exists a strongly antisymmetric $\mathcal{P}$-scheme that is not discrete on H iff there exists a strongly antisymmetric $\bar{\mathcal{P}}$-scheme that is not discrete on H/N.*

Proof. Fix $H \in \mathcal{P}$. Observe that the map $H \mapsto H/N$ is a bijection between $\mathcal{P}$ and $\bar{\mathcal{P}}$. Moreover, for each $H \in \mathcal{P}$, the map $Hg \mapsto (H/N)\bar{g}$ is a bijection between $H\backslash G$ and $(H/N)\backslash(G/N)$, where $\bar{g} := gN \in G/N$. By identifying $H\backslash G$ with $(H/N)\backslash(G/N)$ for $H \in \mathcal{P}$, we see that a $\mathcal{P}$-scheme may be viewed as a $\bar{\mathcal{P}}$-scheme and vice versa, where all the properties in Definition 3.1 and Definition 3.3 are preserved. The lemma follows immediately. □

Corollary 3.12. *Let $\mathcal{P}$, $\bar{\mathcal{P}}$, G, N, and H be as in Lemma 3.11. Then $(\mathcal{P}, G, H)$ is a factoring system iff $(\bar{\mathcal{P}}, G/N, H/N)$ is a factoring system.*

3.3 Functions d_{Sym} and d_{Lin}

We define the functions d_{Sym} and d_{Lin} in this subsection. First, we need a special kind of subgroup systems called *systems of stabilizers*.

Definition 3.13 (system of stabilizers)**.** *Let G be a finite group acting on a finite set S. For $m \in \mathbb{N}^+$, define the set of stabilizers*

$$\mathcal{P}_{G,m} := \{G_{x_1,\ldots,x_k} : x_1, \ldots, x_k \in S, 1 \leq k \leq m\}.$$

Then $\mathcal{P}_{G,m}$ is a subgroup system over G, called the system of stabilizers of depth m *(with respect to the action of G on S).*

The following function $d(G)$ was introduced in [Guo20].

Definition 3.14 ([Guo20, Definition 3.12])**.** *For a finite group G acting on a finite set S, define $d(G)$ to be the smallest $m \in \mathbb{N}^+$ such that $(\mathcal{P}_{G,m}, G, G_\alpha)$ is a factoring system for every $\alpha \in S$.*[3]

[3]Such m always exists. See Lemma 3.17.

In Definition 3.14, we do not assume the permutation representation $\rho : G \to \mathrm{Sym}(S)$ is faithful. However, we may always reduce to the faithful case by the following lemma.

Lemma 3.15. *For G and S as in Definition 3.13, we have $d(G) = d(\rho(G))$, where ρ is the permutation representation $\rho : G \to \mathrm{Sym}(S)$.*

Proof. Let $N = \ker(\rho)$. So $\rho(G) \cong G/N$. Then note $d(G) = d(G/N)$ by Corollary 3.12. □

The function $d(G)$ indicates how large we need to choose m to be in order to get a factoring system. Now we define d_{Sym} and d_{Lin} in terms of $d(G)$:

Definition 3.16 (d_{Sym} and d_{Lin})**.** *For $m \in \mathbb{N}^+$, define $d_{\mathrm{Sym}}(m) = d(\mathrm{Sym}(m))$, where $\mathrm{Sym}(m)$ acts naturally on $[m]$.*

For $m \in \mathbb{N}^+$ and a prime power q, define $d_{\mathrm{Lin}}(m, q)$ to be the maximum of $d(G^S)$, where G ranges over the set of subgroups of a general linear group $\mathrm{GL}_{m'}(q')$ acting naturally on $\mathbb{F}_{q'}^{m'}$, S ranges over the set of G-subsets of $\mathbb{F}_{q'}^{m'}$, and (m', q') ranges over the set of pairs satisfying $m' \le m$, $q'^{m'} \le q^m$ and $\gcd(q, q') \neq 1$.

The definition of $d_{\mathrm{Lin}}(m, q)$ is a bit artificial as it involves subgroups of $\mathrm{GL}_{m'}(q')$ for pairs (m', q') other than (m, q). This is useful when we prove that replacing a finite group by its subquotient does not blow up the complexity by much, where the complexity of a group is defined in terms of d_{Sym} and d_{Lin}.

Properties and bounds. We list some basic properties and bounds about $d(G)$, d_{Sym} and d_{Lin}.

Lemma 3.17 ([Guo20])**.** *The function $d(G)$ has the following properties:*

(1) $d(G) \le \max\{b(G), 1\}$.

(2) Suppose G is a permutation group on a finite set S. Let $m \in \mathbb{N}^+$ and $\mathcal{P} = \mathcal{P}_{G,m}$. If $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ is a strongly antisymmetric $\mathcal{P}$-scheme such that C_{G_x} has a block of cardinality $k > 1$ for some $x \in S$, then $m \le \log k$. In particular, $d(G) = O(\log |S|)$.

(3) Suppose G is a permutation group on a finite set S and G' is a permutation subgroup of G on S. Then $d(G') \le d(G)$.

(4) Suppose G acting on S and H acting on T have permutation isomorphic images (see Definition 2.3). Then $d(G) = d(H)$.

Proof. For (1) and (3), see [Guo20, Lemma 3.13] and [Guo20, Lemma 3.18] respectively. The claim $d(G) = O(\log |S|)$ in (2) was proved as [Guo20, Theorem 3.20 (1)]. The same proof actually proves the stronger claim that $m \le \log k$ (see also [AIKS14, Theorem 2.5]). To prove (4), note that $d(G) = d(H)$ if G and H are permutation isomorphic themselves. By Corollary 3.12, this can be extended to the case that G and H have permutation isomorphic images. □

Lemma 3.18. *The functions d_{Sym} and d_{Lin} have the following properties:*

(1) $d_{\mathrm{Sym}}(m)$ *is non-decreasing in* m.

(2) $d_{\mathrm{Lin}}(m, q)$ *is non-decreasing in* m *for fixed* q.

(3) $d_{\mathrm{Sym}}(m)$ *is the maximum of* $d(G^S)$*, where* G *ranges over the set of subgroups of* $\mathrm{Sym}(m)$ *acting naturally on* $[m]$ *and* S *ranges over the set of* G*-subsets of* $[m]$.

(4) $d_{\mathrm{Sym}}(m) = O(\log m)$ *and* $d_{\mathrm{Lin}}(m, q) \le m$.

(5) $d_{\mathrm{Sym}}(m) \le d_{\mathrm{Lin}}(m, q) \le d_{\mathrm{Sym}}(q^m)$.

Proof. (1): See [Guo20, Lemma B.4].

(2): Let $m' \le m$. Identifying $\mathbb{F}_q^{m'}$ with a subspace of $\mathbb{F}_q^m$, the group $\mathrm{GL}_{m'}(q)$ on $\mathbb{F}_q^{m'}$ may be identified with a permutation subgroup of $\mathrm{GL}_m(q)$ on $\mathbb{F}_q^m$, which acts trivially on a complement of $\mathbb{F}_q^{m'}$. Then claim then follows from the definition of d_{Lin}.

(3): Let G be a subgroup of $\mathrm{Sym}(m)$ acting naturally on $S \subseteq [m]$. It suffices to show $d(G) \le d_{\mathrm{Sym}}(m)$. Let $m' = |S|$. By relabeling, we may assume $S = [m'] \subseteq [m]$. By Lemma 3.15, we

may assume G is a permutation group on S, i.e., $G \leq \mathrm{Sym}(m')$. By Lemma 3.17 (3), we have $d(G) \leq d(\mathrm{Sym}(m')) = d_{\mathrm{Sym}}(m') \leq d_{\mathrm{Sym}}(m)$, where the last inequality holds by (1).

(4): The fact $d_{\mathrm{Sym}}(m) = O(\log m)$ follows from the definition and Lemma 3.17 (2). To see $d_{\mathrm{Lin}}(m, q) \leq m$, consider $G \leq \mathrm{GL}_{m'}(q')$ acting naturally on $S \subseteq \mathbb{F}_{q'}^{m'}$, where $m' \leq m$. The action of G on S defines a permutation representation $\rho : G \to \mathrm{Sym}(S)$. We have $d(G) = d(\rho(G)) \leq b(\rho(G))$ by Lemma 3.15 and Lemma 3.17 (1). Finally, note $b(\rho(G)) \leq m'$.

(5): The latter inequality follows from (3) and the permutation representation $\mathrm{GL}_m(q) \hookrightarrow \mathrm{Sym}(\mathbb{F}_q^m) \cong \mathrm{Sym}(q^m)$. The former follows by considering the embedding $\mathrm{Sym}(m) \hookrightarrow \mathrm{GL}_m(q)$ sending $g \in \mathrm{Sym}(m)$ to the corresponding permutation matrix (also known as the *(linear) permutation representation* of $\mathrm{Sym}(m)$). □

4 Reduction to primitive group actions

Suppose $\tilde{f}(X) \in \mathbb{Q}[X]$ is an *irreducible* polynomial over $\mathbb{Q}$. Let $F = \mathbb{Q}[X]/(\tilde{f}(X))$, and let L be the Galois closure of $F/\mathbb{Q}$, i.e., L is the splitting field of $\tilde{f}$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/F)$. Let S be the set of roots of $\tilde{f}$ in L. Then G is a transitive permutation group on S since $\tilde{f}$ is irreducible. As $F \cong \mathbb{Q}(\alpha)$ for any $\alpha \in S$, the action of G on S is equivalent to its action on $H\backslash G$ by inverse right translation.

In this section, we establish a reduction that allows us to assume G is a *primitive* permutation group on S (or on $H\backslash G$). First, we recall the definition of (finite) primitive permutation groups.

Definition 4.1 (primitive permutation group)**.** *Suppose G is a transitive permutation group on a finite set S. A partition P of S is G-*invariant *if ${}^gP = P$ for all $g \in G$, where ${}^gP := \{{}^gB : B \in P\}$. We say G is* primitive *if there is no G-invariant partition of S other than the coarsest partition 0_S and the finest partition ∞_S. Otherwise we say G is* imprimitive*.*

It is well known that primitivity is equivalent to maximality of stabilizers:

Lemma 4.2 ([Wie64, Theorem 7.4])**.** *Let S be a finite set with $|S| > 1$, and let $x \in S$. A transitive permutation group G on S is primitive iff G_x is maximal in G. In particular, for a proper subgroup H of G, the action of G on $H\backslash G$ by inverse right translation is primitive iff H is maximal in G.*

Thus, we want to reduce to the case that $H = \mathrm{Gal}(L/F)$ is maximal in $G = \mathrm{Gal}(L/\mathbb{Q})$. By Galois theory, this is equivalent to the maximality of $\mathbb{Q}$ in F.

While $\mathbb{Q}$ is not maximal in F in general, the following lemma states that one can efficiently refine the field extension $F/\mathbb{Q}$ into a sequence of extensions F_i/F_{i-1} such that each F_{i-1} is maximal in F_i.

Lemma 4.3 ([LM85])**.** *There exists a polynomial-time algorithm that given a number field F, computes a tower of number fields*

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{k-1} \subseteq F_k = F$$

together with the natural inclusions $F_{i-1} \hookrightarrow F_i$ for $i \in [k]$, such that F_{i-1} is maximal in F_i for $i \in [k]$.

To reduce to the primitive case, we also need the following lemma.

Lemma 4.4. *Suppose $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k \subseteq L$ is a tower of number fields, where L/F_0 is Galois. For $i \in [k]$, suppose*

- *$L_i \subseteq L$ is the Galois closure of F_i/F_{i-1},*
- *$G_i := \mathrm{Gal}(L_i/F_{i-1})$ and $H_i := \mathrm{Gal}(L_i/F_i) \subseteq G_i$,*
- *$\mathcal{F}_i$ is a set of number fields that contain F_{i-1} and are isomorphic to subfields of L_i over F_{i-1}, such that $F_i \in \mathcal{F}_i$, and*
- *$\mathcal{P}_i$ is the subgroup system over G_i associated with $(\mathcal{F}_i, L_i/F_{i-1})$ for $i \in [k]$.*

Let $\mathcal{F} = \bigcup_{i=1}^k \mathcal{F}_i$, $G = \mathrm{Gal}(L/F_0)$ and $H = \mathrm{Gal}(L/F_k) \leq G$. Let $\mathcal{P}$ be the subgroup system over G associated with $(\mathcal{F}, L/F_0)$. If $(\mathcal{P}_i, G_i, H_i)$ is a factoring system for all $i \in [k]$, then $(\mathcal{P}, G, H)$ is a factoring system.

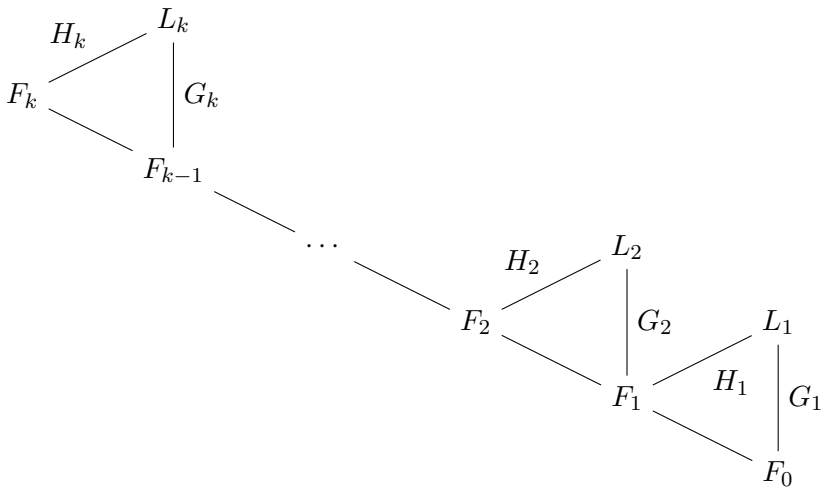

Figure 2: Fields and Galois groups in Lemma 4.4.

See Figure 2 for an illustration of the fields F_i, L_i and the Galois groups G_i, H_i.

Proof of Lemma 4.4. Assume $(\mathcal{P}, G, H)$ is not a factoring system, i.e., there exists a strongly antisymmetric $\mathcal{P}$-scheme $\mathcal{C} = \{C_{H'} : H' \in \mathcal{P}\}$ that is not discrete on H. Then we can choose two different elements $Hg, Hg' \in H\backslash G$ contained in the same block of C_H. We will prove that $(\mathcal{P}_i, G_i, H_i)$ is not a factoring system for some $i \in [k]$.

For $0 \le i \le k$, let $\widetilde{H}_i := \mathrm{Gal}(L/F_i) \le G$. So $H = \widetilde{H}_k \le \widetilde{H}_{k-1} \le \cdots \le \widetilde{H}_1 \le \widetilde{H}_0 = G$. Note $\widetilde{H}_i \in \mathcal{P}$ for $i \in [k]$ since $F_i \in \mathcal{F}_i \subseteq \mathcal{F}$. Pick the greatest integer $i \in [k]$ satisfying $\widetilde{H}_{i-1}g = \widetilde{H}_{i-1}g'$. Such i exists since $\widetilde{H}_0 g = \widetilde{H}_0 g' = Ge$. By the maximality of i and the fact $Hg \neq Hg'$, we have $\widetilde{H}_i g \neq \widetilde{H}_i g'$. As Hg, Hg' are in the same block of C_H and $\mathcal{C}$ is compatible, we know $\widetilde{H}_i g = \pi_{H,\widetilde{H}_i}(Hg)$ and $\widetilde{H}_i g' = \pi_{H,\widetilde{H}_i}(Hg')$ are in the same block of $C_{\widetilde{H}_i}$.

By replacing $\mathcal{C}$ with ${}^g\mathcal{C}$ (see Lemma 3.7), we may assume $g = e$. Then $g' \in \widetilde{H}_{i-1}$ since $\widetilde{H}_{i-1}g = \widetilde{H}_{i-1}g'$. By Lemma 3.10, the restriction $\mathcal{C}|_{\widetilde{H}_{i-1}} = \{C_{H'}|_{\widetilde{H}_{i-1}} : H' \in \mathcal{P}|_{\widetilde{H}_{i-1}}\}$ is a strongly antisymmetric $\mathcal{P}|_{\widetilde{H}_{i-1}}$-scheme. As $\widetilde{H}_i g, \widetilde{H}_i g'$ are in the same block of $C_{\widetilde{H}_i}$, they are also in the same block of $C_{\widetilde{H}_i}|_{\widetilde{H}_{i-1}}$ (see Definition 3.9). As $\widetilde{H}_i g \neq \widetilde{H}_i g'$, we know $\mathcal{C}|_{\widetilde{H}_{i-1}}$ is not discrete on $\widetilde{H}_i$.

Let $N := \mathrm{Gal}(L/L_i)$. By Galois theory, N is a normal subgroup of $\widetilde{H}_{i-1} = \mathrm{Gal}(L/F_{i-1})$ and we may identify $G_i = \mathrm{Gal}(L_i/F_{i-1})$ with $\widetilde{H}_{i-1}/N$. Let $\pi : \widetilde{H}_{i-1} \to G_i$ be the quotient map. Let $\widetilde{\mathcal{P}}_i := \{\pi^{-1}(H') : H' \in \mathcal{P}_i\}$, which is a subgroup system over $\widetilde{H}_{i-1}$. As $\widetilde{H}_i/N \cong \mathrm{Gal}(L_i/F_i) = H_i \in \mathcal{P}_i$, we known $\widetilde{H}_i \in \widetilde{\mathcal{P}}_i$.

We claim $\widetilde{\mathcal{P}}_i \subseteq \mathcal{P}$. To see this, consider arbitrary $H' \in \mathcal{P}_i$. By definition, there exists a field $K \in \mathcal{F}_i$ isomorphic to $L_i^{H'}$ over F_{i-1}. Note $\pi^{-1}(H') = \mathrm{Gal}(L/L^{H'})$. As $K \in \mathcal{F}_i \subseteq \mathcal{F}$, we have $\pi^{-1}(H') \in \mathcal{P}$ by definition. This proves the claim $\widetilde{\mathcal{P}}_i \subseteq \mathcal{P}$. As the members of $\widetilde{\mathcal{P}}_i$ are all subgroups of $\widetilde{H}_{i-1}$, we actually have $\widetilde{\mathcal{P}}_i \subseteq \mathcal{P}|_{\widetilde{H}_{i-1}}$.

As $\widetilde{\mathcal{P}}_i \subseteq \mathcal{P}|_{\widetilde{H}_{i-1}}$, we may construct a strongly antisymmetric $\widetilde{\mathcal{P}}_i$-scheme that is not discrete on $\widetilde{H}_i$ from the $\mathcal{P}|_{\widetilde{H}_{i-1}}$-scheme $\mathcal{C}|_{\widetilde{H}_{i-1}}$ (this is done by simply ignoring the partition of $H'\backslash\widetilde{H}_{i-1}$ for every H' not in $\widetilde{\mathcal{P}}_i$). So $(\widetilde{\mathcal{P}}_i, \widetilde{H}_{i-1}, \widetilde{H}_i)$ is not a factoring system. By Corollary 3.12, $(\mathcal{P}_i, G_i, H_i)$ is not a factoring system, as desired. □

We will apply Lemma 4.4 to the tower of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k$ that comes from Lemma 4.3. By Lemma 4.4, to construct $\mathcal{F}$ such that $(\mathcal{P}, G, H)$ is a factoring system, it suffices to construct $\mathcal{F}_i$ such that $(\mathcal{P}_i, G_i, H_i)$ is a factoring system for $i \in [k]$. Moreover, as H_i is maximal in G_i, we know G_i acts primitively on $H_i\backslash G_i$ by inverse right translation.

Note that the groups G_i are subquotients of G. We still need to show that the complexity of these groups is not too much greater than that of G. This will be addressed in the next subsection.

4.1 Bounding the complexity of subquotients of G

The main result of this subsection is the following lemma.

Lemma 4.5. *For a finite group G and a constant $c \in \mathbb{N}^+$, define*

$$N_c(G) := \max\{N_{\mathcal{A},c}(G), N_{\mathcal{C},c}(G)\},$$
$$N_{\mathcal{A},c}(G) := \max\{m^{d_{\mathrm{Sym}}(m^c)} : m \in \mathbb{N}^+, \mathrm{Alt}(m) \in \mathcal{A}(G)\},$$
$$N_{\mathcal{C},c}(G) := \max\{q^{md_{\mathrm{Lin}}(cm,q)} : m \in \mathbb{N}^+, q \text{ prime power}, \mathrm{Cl}_m(q) \in \mathcal{C}(G)\},$$

and $N_{\mathcal{A},c}(G)$ (resp. $N_{\mathcal{C},c}(G)$) is defined to be zero if $\mathcal{A}(G)$ (resp. $\mathcal{C}(G)$) is empty. Now, let G be a finite permutation group of degree n, and let H be a subquotient of G. For any constant $c \in \mathbb{N}^+$, there exist $c', c'' \in \mathbb{N}^+$ depending only on c such that $N_c(H) \le (nN_{c'}(G))^{c''}$.

The proof of Lemma 4.5 uses the following facts.

Lemma 4.6 ([LS03, Proposition 16.4.10], [DM96, Theorem 5.7A])**.** *Suppose $\mathrm{Alt}(k)$ is a subquotient of a general linear group $\mathrm{GL}_m(q)$ over a finite field $\mathbb{F}_q$. Then $m \ge ck$ for some absolute constant $c > 0$.*

Lemma 4.7 ([LS03, Proposition 16.4.4])**.** *Suppose G is a finite simple classical group of rank m. Then $\mathrm{Alt}(k)$ is a subquotient of G for some $k \ge cm$, where $c > 0$ is an absolute constant.*

Lemma 4.8 ([LS03, Proposition 16.4.29])**.** *Suppose p is a prime and ℓ is a prime power not divisible by p. Then a Sylow p-subgroup of $\mathrm{GL}_m(\mathbb{F}_\ell)$ has order less than $(2\ell)^m$.*

For a finite group G, denote by $\mu(G)$ the minimal degree of a faithful permutation representation of G. We also need the following result proved by Kovács and Praeger [KP00].

Lemma 4.9 ([KP00, Theorem 1])**.** *Let G be a finite group. If G/N is a quotient of G that has no nontrivial abelian normal subgroup, then $\mu(G/N) \le \mu(G)$. In particular, this holds when G/N is nonabelian and simple.*

Corollary 4.10. *Suppose $G \le \mathrm{Sym}(n)$, H is a subquotient of G, and H is also a nonabelian finite simple classical group of rank m over a finite field $\mathbb{F}_q$. Then $q^m \le n^c$ for some absolute constant $c > 0$.*

Proof. We have $\mu(H) \le \mu(G) \le n$ by Lemma 4.9. It is also known that $\mu(H) = q^{\Omega(m)}$ (see Lemma A.14 in the appendix). So $q^m = n^{O(1)}$. □

Now we are ready to prove Lemma 4.5.

Proof of Lemma 4.5. Let $c' = c_0 c$ where $c_0 \in \mathbb{N}^+$ is a large enough absolute constant. It is an easy exercise to show that every nonabelian composition factor H_0 of H is (isomorphic to) a subquotient of a nonabelian composition factor G_0 of G. Moreover, $\mu(G_0) \le \mu(G) \le n$ by Lemma 4.9. By replacing G and H with G_0 and H_0 respectively, we may assume G and H are nonabelian and simple. We may also assume H is isomorphic to either an alternating group or a classical group (otherwise $N_c(H) = 0$ by definition).

Case 1: H is isomorphic to an alternating group $\mathrm{Alt}(k)$. We have $N_c(H) = N_{\mathcal{A},c}(H)$. This case is further divided into the following sub-cases:

(1) First assume G is isomorphic to an alternating group $\mathrm{Alt}(m)$. Then $k \le m$. By Lemma 3.18 (1), we have $N_c(H) = k^{d_{\mathrm{Sym}}(k^c)} \le m^{d_{\mathrm{Sym}}(m^{c'})} = N_{c'}(G)$.

(2) Now assume G is isomorphic to a finite simple classical group of rank m over a finite field $\mathbb{F}_q$. Then $N_c(H) = k^{d_{\mathrm{Sym}}(k^c)} = 2^{O(\log^2 k)}$ by Lemma 3.18 (4). Note $k = O(m)$ by Lemma 4.6 and $q^m = n^{O(1)}$ by Corollary 4.10. So $N_c(H) = 2^{O(\log^2 m)} = n^{O(1)}$.

(3) Now assume G is non-isomorphic to alternating groups and finite simple classical groups. We claim k is bounded by an absolute constant. This is obvious if G is a sporadic finite simple group.

So by CFSG, we may assume G is an exceptional group of Lie type. In this case, it is known that G can be embedded in a general linear group $\mathrm{GL}_m(q)$ where $m = O(1)$ [LS03, Corollary 16.4.5 and Proposition 16.4.6]. As H is a subquotient of G, it is also a subquotient of $\mathrm{GL}_m(q)$. So $k = O(m) = O(1)$ by Lemma 4.7. This proves the claim. It follows that $N_c(H) = k^{d_{\mathrm{Sym}}(k^c)} = O(1)$.

Case 2: H is isomorphic to a finite simple classical group of rank k over a finite field $\mathbb{F}_q$. We have $N_c(H) = N_{\mathcal{C},c}(H)$. This case is further divided into the following sub-cases:

(1) Suppose G is isomorphic to an alternating group $\mathrm{Alt}(m)$. As H is a subquotient of G, we have $\mu(H) \le \mu(G) \le m$ by Lemma 4.9. On the other hand, we have $\mu(H) = q^{\Omega(k)}$ by Lemma A.14. So $q^k \le m^{c_0}$ as $c_0 > 0$ is assumed to be large enough. By Lemma 3.18 (1) and (5), we have

$$d_{\mathrm{Lin}}(ck, q) \le d_{\mathrm{Sym}}(q^{ck}) \le d_{\mathrm{Sym}}(m^{c'})$$

and hence

$$N_c(H) = q^{kd_{\mathrm{Lin}}(ck,q)} \le m^{c_0 d_{\mathrm{Sym}}(m^{c'})} = (N_{c'}(G))^{c_0}.$$

(2) Now suppose G is isomorphic to a finite simple classical group of rank m over a finite field $\mathbb{F}_\ell$. By Lemma 4.9, we have $\mu(H) \le \mu(G) = \ell^{O(m)}$. On the other hand, we have $\mu(H) = q^{\Omega(k)}$ by Lemma A.14. So $q^k = \ell^{O(m)}$. Also, note $k = O(m)$ by Lemma 4.6 and Lemma 4.7. As $c_0 > 0$ is assumed to be large enough, we have $q^k \le \ell^{c_0 m}$ and $k \le c_0 m$.

Assume $\gcd(q, \ell) \ne 1$. As $ck \le c'm$ and $q^{ck} \le \ell^{c'm}$, we have $d_{\mathrm{Lin}}(ck, q) \le d_{\mathrm{Lin}}(c'm, \ell)$ by the definition of d_{Lin}. Therefore

$$N_c(H) = q^{kd_{\mathrm{Lin}}(ck,q)} \le \ell^{c_0 m d_{\mathrm{Lin}}(c'm,\ell)} = (N_{c'}(G))^{c_0}.$$

Now assume $\gcd(q, \ell) = 1$. Let $p = \mathrm{char}(\mathbb{F}_q)$. Let P be a p-Sylow group of H. As H is a subquotient of G, we have $|P| = \ell^{O(m)}$ by Lemma 4.8. On the other hand, it is known that $|P| = q^{\Theta(k^2)}$ (see Table 2 in Appendix A). So $q^{k^2} = \ell^{O(m)}$. By Lemma 3.18 (4) and Corollary 4.10,

$$N_c(H) = q^{kd_{\mathrm{Lin}}(ck,q)} \le q^{ck^2} = \ell^{O(m)} = n^{O(1)}.$$

(3) Finally, assume G is non-isomorphic to alternating groups and finite simple classical groups. By Lemma 4.7, there exists $m = \Omega(k)$ such that $\mathrm{Alt}(m)$ is a subquotient of H. So $\mathrm{Alt}(m)$ is also a subquotient of G. But we know $m = O(1)$ as shown in Case 1 (3). So $k = O(m) = O(1)$. It follows that $N_c(H) = q^{kd_{\mathrm{Lin}}(ck,q)} = q^{O(k)} = n^{O(1)}$ by Lemma 3.18 (4) and Corollary 4.10.

In all the cases above, we have $N_c(H) \le \mathrm{poly}(N_{c'}(G), n)$. This concludes the proof of the lemma. □

5 Proof of the main theorems

We prove Theorem 1.1–1.3 in this section modulo the proof of Lemma 5.3 stated below. This is achieved by constructing a set $\mathcal{F}$ of number fields that satisfies the requirement in Theorem 3.6.

Constructing a set of number fields. Recall that for a finite group G acting on a finite set S, we denote by $\mathcal{P}_{G,m}$ the subgroup system $\{G_{x_1,\ldots,x_k} : x_1, \ldots, x_k \in S, 1 \le k \le m\}$. Now we define a more delicate kind of subgroup systems $\mathcal{P}_{G,m,N}$ as follows.

Definition 5.1. *Let G be a finite group acting on a finite set S. For $m, N \in \mathbb{N}^+$, define $\mathcal{P}_{G,m,N} := \mathcal{P}_{G,m} \cup \mathcal{P}'$, where*

$$\mathcal{P}' = \{H_{x_1,\ldots,x_k} : H, K \in \mathcal{P}_{G,m},\ K \le H,\ x_1, \ldots, x_k \in K\backslash H,\ 1 \le k \le [H : K],\ [H : K]^k \le N\}.$$

Here $H_{x_1,\ldots,x_k}$ denotes the stabilizer of $x_1, \ldots, x_k$ with respect to the action of H on $K\backslash H$ by inverse right translation.

It is easy to see that $\mathcal{P}_{G,m,N}$ is closed under conjugation and hence a subgroup system. The corresponding set of number fields can be constructed by the following lemma. Its proof can be found in Appendix B.

Lemma 5.2. *There exists an algorithm that given the following data*

- *a number field F,*
- *a polynomial $g(X) \in F[X]$ of degree n, whose Galois group over F is denoted by G and splitting field over F is denoted by L, and*
- *$m, N \in \mathbb{N}^+$,*

runs in time polynomial in n^m, N, and the size of the input, and computes a set $\mathcal{F}$ of number fields that contain F and are isomorphic to subfields of L over F, such that the subgroup system associated with $(\mathcal{F}, L/F)$ is $\mathcal{P}_{G,m,N}$, where G is regarded as a permutation group acting naturally on the set of roots of g in L.

The following lemma will be proved in Section 6.

Lemma 5.3. *Let G be a primitive permutation group on a finite set S of cardinality n. Let $\mathcal{P} = \mathcal{P}_{G,c_0,N}$, where $N = (nN_{c_1}(G))^{c_2}$, $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants and $N_{c_1}(G)$ is as defined in Lemma 4.5. Then $(\mathcal{P}, G, G_x)$ is a factoring system for all $x \in S$.*

Proofs of Theorem 1.1–1.3. We are now ready to prove Theorem 1.1–1.3.

Proof of Theorem 1.2. Let $c_0, c_1, c_2 \in \mathbb{N}^+$ be as in Lemma 5.3. We assume the constant c in Theorem 1.2 is large enough so that by Lemma 4.5, it holds that $N_{c_1}(H) \le (nN_c(G))^{c''} = (nN(G))^{c''}$ for any subquotient H of G, where $c'' > 0$ is some constant.

The algorithm runs as follows. Given f and $\tilde{f}$, first factorize $\tilde{f}$ into monic irreducible factors $\tilde{f}_1(X), \ldots, \tilde{f}_s(X)$ over $\mathbb{Q}$ using the LLL algorithm [LLL82]. As $\tilde{f}(X) \in \mathbb{Z}[X]$ is monic, we have $\tilde{f}_i(X) \in \mathbb{Z}[X]$ for $i \in [s]$ by Gauss's lemma [Lan02]. For $i \in [s]$, the Galois group $\mathrm{Gal}(\tilde{f}_i/\mathbb{Q})$ is a homomorphic image of G, which implies $N(\mathrm{Gal}(\tilde{f}_i/\mathbb{Q})) \le N(G)$. Thus, by replacing $(f, \tilde{f})$ with $(\tilde{f}_i \bmod p, \tilde{f}_i)$ for each $i \in [s]$, we may assume $\tilde{f}$ is irreducible over $\mathbb{Q}$. Let L be the splitting field of $\tilde{f}$. Then G is a transitive permutation group on the set of roots of $\tilde{f}$ in L.

Let $F := \mathbb{Q}[X]/(\tilde{f}(X))$ and $H := \mathrm{Gal}(L/F)$. Run the algorithm in Theorem 4.3 to compute in polynomial time a tower of number fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{k-1} \subseteq F_k = F$ together with the natural inclusions $F_{i-1} \hookrightarrow F_i$ for $i \in [k]$, such that F_{i-1} is maximal in F_i for $i \in [k]$.

For each $i \in [k]$, pick $\alpha_i \in F_i - F_{i-1}$ and compute the minimal polynomial $g_i(X) \in F_{i-1}[X]$ of α over F_{i-1} in polynomial time, so that F_i is isomorphic to $F_{i-1}[X]/(g_i(X))$ over F_{i-1}. Let $G_i = \mathrm{Gal}(g_i/F_{i-1})$, which is a subquotient of G. Let $n_i := \deg(g_i) \le n$. Let L_i be the Galois closure of F_i/F_{i-1}, which is also the splitting field of g_i over F_{i-1}. Let $H_i := \mathrm{Gal}(L_i/F_i) \le G$. The maximality of F_{i-1} in F_i implies that H_i is maximal in G_i, which in turn implies that G_i is a primitive permutation group on the set of roots of g_i in L_i.

Let $N := \max_{i\in[k]}\{(n_i N_{c_1}(G_i))^{c_2}\} \le (nN(G))^{c_2 c''}$. For each $i \in [k]$, run the algorithm in Lemma 5.2 on F_{i-1}, g_i, c_0, and N to compute a set $\mathcal{F}_i$ of number fields in time polynomial in $n_i^{c_0}$, N and the size of the input, such that the subgroup system $\mathcal{P}_i$ associated with $(\mathcal{F}_i, L_i/F_{i-1})$ equals $\mathcal{P}_{G_i,c_0,N}$. By adding F_i to $\mathcal{F}_i$ if necessary, we may assume $F_i \in \mathcal{F}_i$. By Lemma 5.3, $(\mathcal{P}_i, G_i, (G_i)_x)$ is a factoring system for all roots x of g_i in L_i. As F_i is isomorphic to $F_{i-1}[X]/(g_i(X))$ over F_{i-1}, we know $(\mathcal{P}_i, G_i, H_i)$ is a factoring system.

Let $\mathcal{F} := \bigcup_{i=1}^k \mathcal{F}_i$ and let $\mathcal{P}$ be the subgroup system associated with $(\mathcal{F}, L/\mathbb{Q})$. Then $(\mathcal{P}, G, H)$ is a factoring system by Lemma 4.4. Note $H = G_x$ for some root x of $\tilde{f}$ in L. As G acts transitively on the set of roots of $\tilde{f}$ in L, invariance of $\mathcal{P}$-schemes implies that $(\mathcal{P}, G, G_x)$ is a factoring system for every root x of $\tilde{f}$ in L .

Finally, feed $\mathcal{F}$ to the algorithm in Theorem 3.6 to output the complete factorization of $f(X)$. Note $\mathcal{F}$ is constructed in time polynomial in $N \le \mathrm{poly}(nN(G))$ and the size of the input. So the algorithm has the desired running time by Theorem 3.6.

The above analysis assumes the value of N is known. Now suppose N is not known. We may replace N by some integer N' between N and $2N$, and find such N' by trying $N' = 1, 2, 4, 8, \ldots$ until f is completely factorized. This increases the time complexity by a factor of $O(\log N) = O(\log n + \log N(G))$. □

Proof of Theorem 1.1. Let $G \in \mathcal{C}_k$. By Theorem 1.2, it suffices to prove that $N(G)$ as defined in Theorem 1.2 is polynomial in $k^{\log k}$. Suppose H is a nonabelian composition factor of G. As H is a subquotient of $\mathrm{Sym}(k)$, Lemma 4.5 implies that $N(H) = N_c(H) \leq \mathrm{poly}(N_{c'}(\mathrm{Sym}(k)), k)$ for some absolute constant $c' \in \mathbb{N}^+$. By Lemma 3.18 (4), we have $N_{c'}(\mathrm{Sym}(k)) \leq k^{d_{\mathrm{Sym}}(k^{c'})} = k^{O(\log k)}$. So $N(H)$ is polynomial in $k^{\log k}$. As this holds for any nonabelian composition factor H of G, we know $N(G)$ is also polynomial in $k^{\log k}$, as desired. □

Proof of Theorem 1.3. The first part of the theorem follows immediately from Theorem 1.2 and the bounds $d_{\mathrm{Sym}}(m) = O(\log m)$ and $d_{\mathrm{Lin}}(m, q) \leq m$ (see Lemma 3.18 (4)). To prove the last part, it suffices to show that q^m is polynomial in n for any classical group $\mathrm{Cl}_m(q) \in \mathcal{C}(G)$. This follows from Corollary 4.10. □

6 Proof for the case of primitive permutation groups

We prove Lemma 5.3 in this section. The proof is based on the O'Nan-Scott theorem for finite primitive permutation groups and careful case-by-case analysis.

6.1 The self-reduction lemma

We first state a useful lemma called the *self-reduction lemma*, which reduces the problem of proving discreteness of $\mathcal{P}$-schemes with respect to a group G to a collection of subproblems with respect to subgroups of G. A less general form of this lemma already appeared in [Guo20].

We need the following technical lemma.

Lemma 6.1 ([Guo20, Lemma 5.3])**.** *Suppose G is a finite group, $\mathcal{P}$ is a subgroup system over G, and $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ is a $\mathcal{P}$-scheme. Suppose H_0, H_1, H_2 are subgroups in $\mathcal{P}$ such that $H_0 \leq H_1 \cap H_2$ and $\mathcal{C}|_{H_1}, \mathcal{C}|_{H_2}$ are discrete on H_0. For $i = 0, 1, 2$, let B_i be the block in C_{H_i} containing $H_i e \in H_i \backslash G$, so that we have maps $\pi_{H_0,H_1}|_{B_0} : B_0 \to B_1$ and $\pi_{H_0,H_2}|_{B_0} : B_0 \to B_2$. Then $\pi_{H_0,H_2}|_{B_0} \circ (\pi_{H_0,H_1}|_{B_0})^{-1}$ is a well-defined bijection from B_1 to B_2 sending $H_1 e \in H_1 \backslash G$ to $H_2 e \in H_2 \backslash G$.*

For a $\mathcal{P}$-scheme $\mathcal{C}$, we define an equivalence relation $\sim_{\mathcal{C}}$ on $\mathcal{P}$ as follows.

Definition 6.2. *Let G be a finite group. Suppose $\mathcal{P}$ is a subgroup system over G and $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ is a $\mathcal{P}$-scheme. Define the (symmetric) binary relation $\leftrightarrow_{\mathcal{C}}$ on $\mathcal{P}$ such that for $H_1, H_2 \in \mathcal{P}$, $H_1 \leftrightarrow_{\mathcal{C}} H_2$ iff there exists $H_0 \in \mathcal{P}$ satisfying (1) $H_0 \leq H_1 \cap H_2$ and (2) $\mathcal{C}|_{H_1}$ and $\mathcal{C}|_{H_2}$ are both discrete on H_0. Let $\sim_{\mathcal{C}}$ be the equivalence relation on $\mathcal{P}$ generated by $\leftrightarrow_{\mathcal{C}}$, i.e., $H \sim_{\mathcal{C}} H'$ iff there exists a finite sequence $H_0, H_1, \ldots, H_k \in \mathcal{P}$ such that $H_0 = H$, $H_k = H'$ and $H_{i-1} \leftrightarrow_{\mathcal{C}} H_i$ for $i \in [k]$.*

Lemma 6.3 (self-reduction lemma, general form)**.** *Let $\mathcal{C} = \{C_H : H \in \mathcal{P}\}$ be a strongly antisymmetric $\mathcal{P}$-scheme. Fix $H \in \mathcal{P}$ and let $O = \{gHg^{-1} : g \in G\} \subseteq \mathcal{P}$. Suppose $H \sim_{\mathcal{C}} H'$ for all $H' \in O$, i.e., O is a subset of the equivalence class of H under $\sim_{\mathcal{C}}$. Then $\mathcal{C}$ is discrete on H.*

Proof. Consider arbitrary $g, h \in G$. Let $H' = g^{-1}Hg, H'' = h^{-1}Hh \in O$. As $H' \sim_{\mathcal{C}} H''$, there exists a finite sequence $H_0, H_1, \ldots, H_k \in \mathcal{P}$ such that $H_0 = H'$, $H_k = H''$ and $H_{i-1} \leftrightarrow_{\mathcal{C}} H_i$ for $i \in [k]$. For $0 \leq i \leq k$, let B_i be the block of C_{H_i} containing $H_i e \in H_i \backslash G$. Applying Lemma 6.1 for each $i \in [k]$ gives a bijection $B_{i-1} \to B_i$ sending $H_{i-1}e$ to $H_i e$. Let $\tau : B_0 \to B_k$ be the composition of these maps. Then $c_{H'',h} \circ \tau \circ c_{H,g^{-1}}$ sends Hg to Hh. By strong antisymmetry of $\mathcal{C}$, we know Hg and Hh are in different blocks of C_H if $Hg \neq Hh$. As g, h are arbitrary, we conclude $C_H = \infty_{H\backslash G}$, i.e., $\mathcal{C}$ is discrete on H. □

Corollary 6.4 ([Guo20])**.** *Let G be a finite group acting on a finite set S. Suppose $\mathcal{P}$ is a subgroup system over G and $\mathcal{C}$ is a strongly antisymmetric $\mathcal{P}$-scheme. Let $x \in S$ such that $G_x \in \mathcal{P}$. Suppose for every $y \in Gx$, there exists a finite sequence $x = x_0, x_1, \ldots, x_k = y$ in S such that for $i \in [k]$, (1) $G_{x_i}, G_{x_{i-1},x_i} \in \mathcal{P}$ and (2) $\mathcal{C}|_{G_{x_{i-1}}}$ and $\mathcal{C}|_{G_{x_i}}$ are discrete on G_{x_{i-1},x_i}. Then $\mathcal{C}$ is discrete on G_x.*

Proof. This follows from Lemma 6.3 since $O = \{gG_xg^{-1} : g \in G\}$ is just $\{G_y : y \in Gx\}$. □

Corollary 6.5. *Let A be a finite group acting transitively on a finite set S. Let $G, H \leq A$ where H is transitive on S. Let $\mathcal{P}$ be a subgroup system over G that is closed under conjugation by elements in H. Let Z be a generating set of H such that $g^{-1}, hgh^{-1} \in Z$ for $g \in Z$ and $h \in H$. Let $x \in S$ such that $G_x \in \mathcal{P}$. Suppose for every $g \in Z$, we have $G_{x,{}^g x} \in \mathcal{P}$ and $(\mathcal{P}|_{G_x}, G_x, G_{x,{}^g x})$ is a factoring system. Then $(\mathcal{P}, G, G_y)$ is a factoring system for all $y \in S$.*

Proof. As $G_x \in \mathcal{P}$ and H is transitive on S, we have $G_y \in \mathcal{P}$ for every $y \in S$. As H is transitive on S and Z is a generating set of H which is closed under taking inverses, for every $y, z \in S$, there exists a finite sequence $y = x_0, x_1, \ldots, x_k = z$ and $g_1, \ldots, g_k \in Z$ such that $x_i = {}^{g_i} x_{i-1}$ for $i \in [k]$. By Corollary 6.4, it suffices to prove that for every $y \in S$ and $g \in Z$, it holds that $G_{y,{}^g y} \in \mathcal{P}$ and $(\mathcal{P}|_{G_y}, G_y, G_{y,{}^g y})$ is a factoring system. Choose $h \in H$ such that $y = {}^h x$. Then $G_y = hG_x h^{-1}$ and $G_{y,{}^g y} = hG_{x,{}^{g'} x}h^{-1}$, where $g' = h^{-1}gh \in Z$. The map $a \mapsto hah^{-1}$ defines a permutation isomorphism between the action of G_x on ${G_x}^{g'} x$ and the action of G_y on ${G_y}^{g} y$ (with respect to $z \mapsto {}^h z$). As $\mathcal{P}$ is closed under conjugation by elements in H, we just need to prove $G_{x,{}^{g'} x} \in \mathcal{P}$ and $(\mathcal{P}|_{G_x}, G_x, G_{x,{}^{g'} x})$ is a factoring system, which hold by assumption. □

Remark. The condition $G_{x_i}, G_{x_{i-1},x_i} \in \mathcal{P}$ in Corollary 6.4 and the condition $G_{x,{}^g x} \in \mathcal{P}$ in Corollary 6.5 are typically straightforward to verify. For example, these conditions are satisfied as long as $\mathcal{P}_{G,2} \subseteq \mathcal{P}$. We often omit the proofs of these conditions and leave them to the reader.

6.2 The O'Nan-Scott theorem

The O'Nan-Scott theorem for finite primitive permutation groups [LPS88] is one of the most influential theorems in permutation group theory. In this subsection, we describe this theorem and the related definitions.

First, we need the notion of the *socle* of a finite group.

Definition 6.6 (socle)**.** *The* socle *of a finite group G, denoted by $\mathrm{soc}(G)$, is the subgroup generated by the minimal normal subgroups of G.*

Next, we define the five categories of groups in the O'Nan-Scott theorem.

Almost simple type. A finite group is *almost simple* if it is isomorphic to a group G satisfying $T \leq G \leq \mathrm{Aut}(T)$ for some nonabelian finite simple group T. Here we regard T as a normal subgroup of $\mathrm{Aut}(T)$ by identifying it with the inner automorphism group $\mathrm{Inn}(T) \trianglelefteq \mathrm{Aut}(T)$.

Definition 6.7 (almost simple type)**.** *A finite permutation group is of* almost simple type *if it is primitive and almost simple.*

If G is of almost simple type satisfying $T \leq G \leq \mathrm{Aut}(T)$ for a nonabelian finite simple group T, then the socle of G is just T [DM96].

Affine type. For a vector space V, the *affine general linear group* $\mathrm{AGL}(V)$ is the group of all affine linear transformations on V. Finite permutation groups of *affine type* arise as subgroups of affine general linear groups.

Definition 6.8 (affine type)**.** *A finite permutation group is said to be of* affine type *if it is permutation isomorphic to a subgroup G of an affine general linear group $\mathrm{AGL}(V)$ acting naturally on a finite-dimensional vector space V over a prime field $\mathbb{F}_p$, and G contains the subgroup of translations $V^\sharp := \{x \mapsto x + u : u \in V\}$.*

Diagonal type. Let T be a nonabelian finite simple group and let $k \geq 2$ be an integer. Consider the subgroup $A \leq \mathrm{Aut}(T)^k$ defined by

$$A := \{(a_1, \ldots, a_k) \in \mathrm{Aut}(T)^k : a_i \mathrm{Inn}(T) = a_j \mathrm{Inn}(T) \text{ for all } i, j \in [k]\}.$$

The symmetric group $\mathrm{Sym}(k)$ acts on A by permuting the k coordinates, sending $(a_1, \ldots, a_k) \in A$ to $(a_{\pi^{-1}(1)}, \ldots, a_{\pi^{-1}(k)})$. So we can form the semidirect product

$$W := A \rtimes \mathrm{Sym}(k).$$

Define the subgroups $M, D \leq W$ by

$$M := \mathrm{Inn}(T)^k \leq A \leq W$$

and

$$D := \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in \mathrm{Sym}(k)\} \leq W.$$

Definition 6.9 (diagonal type)**.** *A finite permutation group is said to be of* diagonal type *if it is permutation isomorphic to a group G satisfying $M \leq G \leq W$ acting on $D\backslash W$ by inverse right translation, where D, M, W are as above.*

Product type. Let K be a permutation group on a finite set Γ of almost simple type or diagonal type. Let $k \geq 2$ be an integer. Define the wreath product

$$W := K \wr \mathrm{Sym}(k) = K^k \rtimes \mathrm{Sym}(k),$$

where $\mathrm{Sym}(k)$ permutes the k factors of K^k. The group W has a natural action on Γ^k called the *primitive wreath product action*, where K^k acts coordinatewise and $\mathrm{Sym}(k)$ permutes the coordinates. Define

$$M := \mathrm{soc}(K)^k \leq W.$$

Definition 6.10 (product type)**.** *A finite permutation group is said to be of* product type *if it is permutation isomorphic to a group G satisfying $M \leq G \leq W$ acting on Γ^k via the primitive wreath product action, where M, W, Γ, k are as above.*

Twisted wreath type. Let T be a nonabelian finite simple group. Let P be a transitive permutation group on $[k]$ where $k \geq 2$. Denote by $\mathrm{Map}(P, T)$ the set of the maps from P to T. Suppose $\varphi : P_1 \to \mathrm{Aut}(T)$ is a group homomorphism from the stabilizer P_1 of $1 \in [k]$ to $\mathrm{Aut}(T)$. Define

$$B := \{f \in \mathrm{Map}(P, T) : f(pq^{-1}) = {}^{\varphi(q)}(f(p)) \text{ for all } p \in P, q \in P_1\},$$

which is a group under coordinatewise multiplication. The group P acts on B via $({}^p f)(px) = f(x)$, or equivalently,

$$({}^p f)(x) = f(p^{-1}x) \qquad \text{for all } p, x \in P, f \in B.$$

It is easy to check that this is a well-defined action. So we can form the semidirect product $G := B \rtimes P$ with respect to this action. The group G is also called the *twisted wreath product* with respect to the data (T, P, φ), denoted by $T \,\mathrm{twr}_\varphi\, P$ [Neu63, DM96].

Definition 6.11 (twisted wreath type)**.** *A finite permutation group is said to be of* twisted wreath type *if it is permutation isomorphic to a group $G = T \,\mathrm{twr}_\varphi\, P$ acting on the left coset space G/P by left translation, where T, P, and φ are as above.*

The O'Nan-Scott theorem. Now we are ready to state the O'Nan-Scott theorem for finite primitive permutation groups [LPS88].

Theorem 6.12 (O'Nan-Scott theorem)**.** *A finite primitive permutation group is of one of the following types: almost simple type, affine type, diagonal type, product type, and twisted wreath type.*

6.3 Almost simple type

In this subsection, we prove Lemma 5.3 for primitive permutation groups of almost simple type. We start by proving it for a special case, namely classical groups G in subspace actions [LS99]. Then we extend it to general G of almost simple type.

6.3.1 Subspace actions of finite classical groups

Our analysis in this part assumes some preliminaries and notations about finite classical groups, which can be found in Appendix A.

Permutation of subspaces by almost simple classical groups. Let V be a vector space of dimension n over $\mathbb{F}_q$, and let $\mathcal{S}$ be the set of all subspaces of V. The general semilinear group $\Gamma\mathrm{L}(V)$ has an action on $\mathcal{S}$ induced from its natural action on V. Let $B = \{e_1, e_2, \ldots, e_n\}$ be a basis of V, and let $\iota : \mathrm{GL}(V) \to \mathrm{GL}(V)$ be the transpose-inverse automorphism in the basis B. Then we can form the semidirect product $A := \Gamma\mathrm{L}(V) \rtimes \langle \iota \rangle$ as explained in Appendix A. The action of $\Gamma\mathrm{L}(V)$ on $\mathcal{S}$ naturally extends to an action of A on $\mathcal{S}$: For $W = {}^g\langle e_1, e_2, \ldots, e_k\rangle \in \mathcal{S}$ where $g \in \mathrm{GL}(V)$, let ${}^\iota W = {}^{g'}\langle e_{k+1}, \ldots, e_n\rangle$ where $g' = \iota g \iota^{-1} = {}^\iota g \in \mathrm{GL}(V)$. So ι exchanges k-dimensional subspaces with $(n-k)$-dimensional subspaces.

As the group of scalars $\mathbb{F}_q^\times$ acts trivially on $\mathcal{S}$, we have an induced action of $\bar{A} := A/\mathbb{F}_q^\times$ on $\mathcal{S}$. Now let G be a finite almost simple classical group G whose natural module is V. By Theorem A.13, G is a subgroup of $\bar{A}$ (provided that $n = \dim V > 8$). So we have an action of G on $\mathcal{S}$, i.e., G permutes the subspaces of V.

Subspace actions. Liebeck and Shalev introduced the notion of *subspace actions* as follows.

Definition 6.13 ([LS99])**.** *Let G be a finite almost simple classical group with socle G_0 and natural module V over a finite field $\mathbb{F}_q$ of characteristic p. A maximal subgroup M of G is called a* subspace subgroup *of G if one of the following holds:*

(1) $M = G_U := \{g \in G : {}^gU = U\}$ for some proper nonzero subspace U of V, where U is totally singular, non-degenerate, or, if G is orthogonal and $p = 2$, a non-singular 1-space.

(2) $G_0 = \mathrm{PSL}(V)$, G contains a transpose-inverse automorphism, and M is the stabilizer $G_{\{U,W\}}$ of an unordered pair $\{U, V\}$ where U, W are proper nonzero subspaces of V, $\dim V = \dim U + \dim W$, and either $U \subseteq W$ or $V = U \oplus W$.

(3) $G_0 = \mathrm{Sp}_{2m}(q)$, $p = 2$ and $M \cap G_0 = \mathrm{O}^{\pm}_{2m}(q)$.

If M is a subspace subgroup of G, we call the action of G on the coset space $M\backslash G$ by inverse right translation a subspace action *of the classical group G.*

Remark. Aschbacher [Asc84] classified maximal subgroups of finite classical groups into various classes. Readers familiar with this work may notice that (1) and (2) in Definition 6.13 correspond to *Aschbacher's class $\mathcal{C}_1$* (and $\mathcal{C}_1'$) while (3) is a special case of *Aschbacher's class $\mathcal{C}_8$*. See [KL90] for a detailed exposition about these classes.

We will prove the following lemma for subspace actions.

Lemma 6.14. *Let G be a primitive permutation group of almost simple type with a subspace action on a finite set S of cardinality n. Let H be a subgroup of G on S. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = N_{c_1}(G)^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$.*

The case of bounded minimal base size. As $d(H) \le b(H) \le b(G)$, Lemma 6.14 follows immediately if the minimal base size $b(G)$ is bounded by an absolute constant. By the following lemma, this includes the case that $\dim V$ is bounded by an absolute constant.

Lemma 6.15 ([GSS98])**.** *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that if G is a primitive permutation group of almost simple type and a finite classical group of rank d, then $b(G) \le f(d)$.*

It also includes the case that G is in Case (1) or Case (2) of Definition 6.13, and $\epsilon \dim V \le \dim U \le (1-\epsilon)\dim V$ for some absolute constant $\epsilon \in (0, 1)$. This follows from the following lemma.

Lemma 6.16 ([Ben05, HLM19])**.** *Let G, V and U be as in Case (1) or (2) of Definition 6.13. Then $b(G) \le c \cdot \dim V / \min\{\dim U, \dim V - \dim U\}$ where $c > 0$ is an absolute constant.*

In the following, assume G is a finite classical group and a primitive permutation group of almost simple type with a subspace action on $M\backslash G$ as in Definition 6.13, and $b(G) > C$ for some large enough absolute constant $C > 0$. This implies that $\dim V > C'$ for some large enough constant $C' > 0$ by Lemma 6.15. We prove Lemma 6.14 by analyzing each of the three cases of Definition 6.13.

Proof of Case (1). Suppose G is in Case (1) of Definition 6.13. By Lemma 2.2, the action of G on $M\backslash G$ is equivalent to its action on the G-orbit of U. We will prove Lemma 6.14 with respect to the later action. So S in Lemma 6.14 is assumed to be the G-orbit of U.

We assume G contains no transpose-inverse automorphism (i.e., $G \leq \mathrm{P\Gamma L}(V)$). This can be justified as follows: As G primitive, the normal subgroup G_0 is transitive on S [Wie64, Proposition 7.1]. So the subspaces in S have the same dimension. If G contains a transpose-inverse automorphism ι, then as ι sends U to a subspace of dimension $\dim V - \dim U$, we have $\dim U = \frac{1}{2}\dim V$. But then $b(G)$ is bounded by an absolute constant by Lemma 6.16.

We also assume $\dim U \leq \frac{1}{2}\dim V$, which can be justified as follows: If V is in Cases **S**, **U** or **O** and $\dim U > \frac{1}{2}\dim V$, then U must be a non-degenerate subspace by Lemma A.2 (4). In this case, we may replace U by $U^\perp$ (since $G_U = G_{U^\perp}$), and $\dim U \leq \frac{1}{2}\dim V$ holds after the replacement. If V is in Case **L**, let ι be a transpose-inverse automorphism. Note the action of G on $M\backslash G$ and the action of $\iota G\iota^{-1}$ on $(\iota M\iota^{-1})\backslash(\iota G\iota^{-1})$ are permutation isomorphic. By replacing the former with the latter if necessary, we have $\dim U \leq \frac{1}{2}\dim V$, since ι sends subspaces of dimension k to subspaces of dimension $\dim V - k$.

We also observe the following fact, whose proof is given in Appendix B.

Lemma 6.17. *S is the set of all subspaces of V isometric to U.*

To prove Lemma 6.14 for Case (1), we will actually prove a more general statement as follows.

Lemma 6.18. *Let G, V and U be as in Case (1) of Definition 6.13, and let S be as above. Let W_0 be a complement of U in V. Suppose S' is a subset of S such that the following holds:*

- *If the space V is in Case* **L**, *then either $S' = S$ or S' is the set of all subspaces that are complements of W_0 in V.*
- *Otherwise, $S' = S$.*

Let H be a subgroup of G acting on S such that S' is an H-subset. Let $\mathcal{P}' = \mathcal{P}_{H,c_0,N}$, defined with respect to the action of H on S' (instead of S), where c_0 and N are as in Lemma 6.14. Then $(\mathcal{P}', H, H_x)$ is a factoring system for all $x \in S'$.

In other words, if V is in Case **L**, Lemma 6.14 still holds if S is replaced by the set of complements of W_0 in V. While this generalization is not necessary for the analysis in Case (1), it is useful when we address Case (2) later.

In the following, let G, H, V, U, W_0, S, S' and $\mathcal{P}'$ be as in Lemma 6.18.

Bounded $\dim U$. We first address the case that $\dim U$ is bounded by an absolute constant. We need the following lemma, whose proof is given in Appendix B.

Lemma 6.19. *Suppose $U_0 \in S'$ and $\dim U_0$ is bounded by some absolute constant $c > 0$. Then there exist a subspace W of V and $U_1, \ldots, U_k \in S'$ such that*

(1) $U_0, U_1, \ldots, U_k \subseteq W$ and $W = \sum_{i=0}^{k} U_i$,

(2) the restriction of any $g \in G_{U_0,U_1,\ldots,U_k} \leq G_W$ to W, denoted by $g|_W \in \mathrm{P\Gamma L}(W)$, is the identity, and

(3) $\dim W$ and k are bounded by an absolute constant $c' > 0$.

Using Lemma 6.19, we prove

Lemma 6.20. *Lemma 6.18 holds if $\dim U$ is bounded by some absolute constant $c > 0$.*

Proof. Fix $U_0 \in S'$. So $\dim U_0 = \dim U \le c$. We want to prove that $(\mathcal{P}', H, H_{U_0})$ is a factoring system. Let $W \subseteq V$ and $U_1, \dots, U_k \in S'$ be as in Lemma 6.19 (with respect to U_0). Let $B = \{U_0, \dots, U_k\}$. As $H_B \le H_{U_0}$, by Lemma 3.2, it suffices to prove that $(\mathcal{P}', H, H_B)$ is a factoring system. By Corollary 6.5, it suffices to prove for all $g \in H$ that $(\mathcal{P}'|_{H_B}, H_B, H_{B \cup {}^g B})$ is a factoring system. Fix $g \in H$.

Let $\{x_1, \dots, x_k\}$ be a basis of ${}^g W$. Define H^* to be the subgroup of $\mathrm{GL}(V)$ consisting of the elements h such that ${}^h x_1 = x_1$ and the image of h in $\mathrm{PGL}(V)$ is in $H_B \le \mathrm{P\Gamma L}(V)$. Then we have a group homomorphism $\phi : H^* \to H_B$ sending $g \in H^*$ to its image in $\mathrm{P\Gamma L}(V)$.

We claim that ϕ is surjective. To see this, consider $h \in H_B$ and lift it to $h' \in \Gamma\mathrm{L}(V)$. Then h' restricts to a scaling transformation on W by Lemma 6.19. We may assume h' is the identity on W by multiplying it with some $\lambda \in \mathbb{F}_q^\times$. Then ${}^{h'} x_1 = x_1$. Moreover, as $h'|_W$ is the identity, we have $\sigma(h') = \sigma(h'|_W) = e$. So $h' \in \mathrm{GL}(V)$. By definition, $h' \in H^*$. This proves the claim that $\phi : H^* \to H_B$ is surjective.

Let $x = (x_1, \dots, x_k) \in V^k$. The group H^* acts diagonally on V^k. We claim $H^*_x = \phi^{-1}(H_{B \cup {}^g B})$. To see this, note any $h \in H^*_x$ is the identity on ${}^g W$ and hence fixes all subspaces in ${}^g B$. So $H^*_x \le \phi^{-1}(H_{B \cup {}^g B})$. Conversely, consider $h \in H^*$ such that $\phi(h) \in H_{B \cup {}^g B}$. Then $g^{-1}\phi(h)g$ is in H_B and, by Lemma 6.19, its restriction on W is the identity. So the restriction of h on ${}^g W$ is a scaling transformation. As ${}^h x_1 = x_1$ (by the definition of H^*) and $x_1 \in {}^g W$, we know h restricts to the identity on ${}^g W$. So $h \in H^*_x$. This proves the claim $H^*_x = \phi^{-1}(H_{B \cup {}^g B})$.

Let $O \subseteq V^k$ be the H^*-orbit of x and let $O' = H_{B \cup {}^g B} \backslash H_B$. By Lemma 2.4, H^* acting on O and H_B acting on O' by inverse right translation have permutation isomorphic images. On the other hand, as H^* acts diagonally on V^k, we have a linear representation $H^* \to \mathrm{GL}(V^k)$. Let $\bar{H}$ be the image of H^* under this map. Then the action of H^* on O factor through the action of $\bar{H}$. So

$$d(H_B^{O'}) = d((H^*)^O) = d(\bar{H}^O) \le d_{\mathrm{Lin}}(\dim(V^k), q) \le d_{\mathrm{Lin}}(c'd, q),$$

where $d := \dim V$ and the constant c' is as in Lemma 6.19. Also note $|O'| = |O| \le |V|^k \le q^{dc'}$. Let $m = d(H_B^{O'})$. Then as $N_{c_1}(G) = q^{d \cdot d_{\mathrm{Lin}}(c_1 d, q)}$, $N = N_{c_1}(G)^{c_2}$, and c_1, c_2 are large enough constants, we have

$$[H_B : H_{B \cup {}^g B}]^m = |O'|^m \le q^{dc' \cdot d_{\mathrm{Lin}}(c'd, q)} \le N_{c_1}(G)^{c_2} = N.$$

Let $\mathcal{P}''$ be the system of stabilizers of depth m over H_B with respect to the action of H_B on $H_{B \cup {}^g B} \backslash H_B$ by inverse right translation. Then $\mathcal{P}'' \subseteq \mathcal{P}'|_{H_B} = \mathcal{P}_{H, c_0, N}|_{H_B}$ by definition. As $(\mathcal{P}'', H_B, H_{B \cup {}^g B})$ is a factoring system by the choice of m, $(\mathcal{P}'|_{H_B}, H_B, H_{B \cup {}^g B})$ is a factoring system, as desired. □

Unbounded $\dim U$. From now on, assume $\dim U > c$, where $c > 0$ is a large enough constant. In particular, either the subspaces in S are all totally singular, or they are all non-degenerate.

We need the following lemma, whose proof is given in Appendix B.

Lemma 6.21. *Let $U_0, U_1, U_2 \in S'$ such that $U \cap U_i$ has dimension $\dim U - 1$ for $i = 1, 2, 3$. Further assume there exist $g \in \Gamma(V)_U$ and $h \in \Gamma(V)_{U, U_0}$ such that $U_1 = {}^g U_0$ and $U_2 = {}^h U_1$. Then there exists a finite sequence of subspaces $Z_0, \dots, Z_k \in S'$ such that $\dim U \cap Z_i = \dim U - 1$ for $0 \le i \le k$, $Z_0 = U_1$, $Z_k = U_2$, and at least one of the following holds for each $i \in [k]$:*

(1) $U \cap Z_{i-1} = U \cap Z_i$.

(2) $U + Z_{i-1} = U + Z_i$.

The next two lemmas address the two cases in Lemma 6.21 respectively.

Lemma 6.22. *Let $U_1, U_2 \in S'$ such that $\dim U \cap U_1 = \dim U \cap U_2 = \dim U - 1$ and $U \cap U_1 = U \cap U_2$. Then $(\mathcal{P}'|_{H_{U, U_1}}, H_{U, U_1}, H_{U, U_1, U_2})$ is a factoring system.*

Proof. We assume $U_1 \ne U_2$ as otherwise the statement is trivial. Pick $u_0 \in U_2 - U$ and $w \in U_1 - U$. Choose a set B of subspaces of V as follows:

- If $S' = S$, let W_0' be a complement of $U_1 + U_2$ in V. Otherwise, let W_0' be a complement of $U + U_1 + U_2$ in V contained in W_0.
- Choose independent and singular $v_1, v_2 \in (U_1 + U_2)^\perp \cap W_0'$.[4]

[4]This is possible if $\dim((U_1 + U_2)^\perp \cap W_0') \ge \dim V - 2 \dim U - 3 \ge 3$, which is implied by the assumption $b(G) \ge C$ for a large enough constant $C > 0$ by Lemma 6.16.

- Let $u_1 = u_0 + v_1$, $u_2 = u_0 + v_2$, $u_3 = u_0 + v_1 + v_2$, $u_4 = u_0 + \alpha v_1$ and $u_5 = w + v_1$, where α is an element in $\mathbb{F}_q$ that is not in any proper subfield.
- For $0 \le i \le 5$, let $W_i = (U \cap U_1) + \langle u_i \rangle = (U \cap U_2) + \langle u_i \rangle$. Note $W_0 = U_2$.
- Let $B = \{U, U_1\} \cup \{W_0, W_1, \dots, W_5\}$.

As v_1, v_2 are singular and orthogonal to U_1 and U_2, the subspaces $W_1, \dots, W_5$ are isometric to U_1 or U_2, as one can construct an isometry that fixes $U \cap U_1 = U \cap U_2$ pointwisely and sends u_i to u_0 or w. Moreover, as $u_0, w \notin U$, it is easy to see that $W_1, \dots, W_5$ are complements of W_0 in V. It follows that $W_1, \dots, W_5 \in S'$. So $B \subseteq S'$.

As $H_B \le H_{U,U_1,U_2}$, it suffices to prove that $(\mathcal{P}'|_{H_{U,U_1}}, H_{U,U_1}, H_B)$ is a factoring system by Lemma 3.2. By Corollary 6.5, it suffices to prove that $(\mathcal{P}'|_{H_B}, H_B, H_{B\cup {}^g B})$ is a factoring system for all $g \in H_{U,U_1}$. Fix $g \in H_{U,U_1}$. Lift g to $\tilde{g} \in \Gamma\mathrm{L}(V)$. Let $u_i' = {}^{\tilde{g}}u_i$ for $0 \le i \le 5$. Let $v_1' = {}^{\tilde{g}}v_1$ and $v_2' = {}^{\tilde{g}}v_2$.

Let $\bar{V} := V/(U \cap U_1)$. As $H_B \le H_{U,U_1}$ fixes $U \cap U_1$, we have a group homomorphism $\phi : H_B \to \mathrm{P\Gamma L}(\bar{V})$. Let $\bar{H} = \phi(H_B)$. For $v \in V$, write $\bar{v}$ for $v + (U \cap U_1) \in \bar{V}$. If $v \notin U \cap U_1$, then $\langle \bar{v} \rangle$ may be viewed as a point in the projective space $\mathbb{P}\bar{V}$. Let

$$x = (\langle \bar{u}_0' \rangle, \dots, \langle \bar{u}_5' \rangle) \in (\mathbb{P}\bar{V})^6.$$

and let O be the $\bar{H}$-orbit of x under the diagonal action. As H_B fixes $U \cap U_1$, for $0 \le i \le 5$, an element $h \in H_B$ fixes ${}^g W_i = (U \cap U_1) + \langle u_i' \rangle$ iff $\phi(h)$ fixes $\langle \bar{u}_i' \rangle$. So $H_{B\cup {}^g B} = (H_B)_{{}^g W_0, {}^g W_1, \dots, {}^g W_5} = \phi^{-1}(\bar{H}_x)$. By Lemma 2.4, H_B acting on $H_{B\cup {}^g B}\backslash H_B$ by inverse right translation and $\bar{H}$ acting on O have permutation isomorphic images.

We also need the following claim, whose proof is straightforward and given in Appendix B.

Claim 6.23. *Let V_0 be a vector space over $\mathbb{F}_q$. Suppose $u_0, w, v_1, v_2 \in V_0$ are linearly independent. Let $u_1 = u_0 + v_1$, $u_2 = u_0 + v_2$, $u_3 = u_0 + v_1 + v_2$, $u_4 = u_0 + \alpha v_1$ and $u_5 = w + v_1$, where α is an element in $\mathbb{F}_q$ that is not in any proper subfield. Then $\Gamma\mathrm{L}(V_0)_{\langle u_0 \rangle, \langle u_1 \rangle, \dots, \langle u_5 \rangle, \langle w \rangle} = \mathbb{F}_q^\times(\mathrm{GL}(V_0)_{u_0, u_1, \dots, u_5, w})$.*

Define H^* to be the subgroup of $\mathrm{GL}(\bar{V})$ consisting of the elements h such that ${}^h\bar{w} = \bar{w}$ and the image of h in $\mathrm{PGL}(\bar{V})$ is in $\bar{H}$. So we have a group homomorphism $\psi : H^* \to \bar{H}$. We claim that ψ is surjective and $H^*_{\bar{u}_0', \dots, \bar{u}_5'} = \psi^{-1}(\bar{H}_x)$.

To prove the claims, consider arbitrary $h \in \bar{H} \le \mathrm{P\Gamma L}(\bar{V})$ and lift it to $\tilde{h} \in \Gamma\mathrm{L}(\bar{V})$. Then $\tilde{h}$ fixes $\langle \bar{u}_0 \rangle, \dots, \langle \bar{u}_5 \rangle$. It also fixes $\langle \bar{w} \rangle$ since $\bar{H}$ fixes $U_1 = (U \cap U_1) + \langle w \rangle$. Applying Claim 6.23 to $\bar{u}_0, \bar{w}, \bar{v}_1, \bar{v}_2 \in \bar{V}$, which are independent vectors by the choice of u_0, w, v_1, v_2 and the assumption $U_1 \ne U_2$, we see $\tilde{h} \in \mathbb{F}_q^\times(\mathrm{GL}(\bar{V})_{\bar{u}_0, \bar{u}_1, \dots, \bar{u}_5, \bar{w}})$. By scaling, we may assume $\tilde{h} \in \mathrm{GL}(\bar{V})_{\bar{u}_0, \bar{u}_1, \dots, \bar{u}_5, \bar{w}}$. So $\tilde{h} \in H^*$. This proves the first claim that ψ is surjective.

Now suppose $h \in \bar{H}_x$. Let $\tilde{h} \in H^*$ be a preimage of h under ψ. So $\tilde{h}$ fixes $\langle \bar{u}_0' \rangle, \dots, \langle \bar{u}_5' \rangle$ and $\langle \bar{w} \rangle$. Applying Claim 6.23 with $\bar{u}_i$ replaced by $\bar{u}_i'$ for $0 \le i \le 5$ and $\bar{v}_j$ replaced by $\bar{v}_j'$ for $j = 1, 2$, we see that $\tilde{h} \in \mathbb{F}_q^\times(\mathrm{GL}(\bar{V})_{\bar{u}_0', \bar{u}_1', \dots, \bar{u}_5', \bar{w}})$. As $\tilde{h} \in H^*$, it fixes $\bar{w}$. So $\tilde{h} \in H^*_{\bar{u}_0', \dots, \bar{u}_5'}$. This proves the second claim that $H^*_{\bar{u}_0', \dots, \bar{u}_5'} = \psi^{-1}(\bar{H}_x)$.

Let $y = (\bar{u}_0', \dots, \bar{u}_5')$. So $H^*_{\bar{u}_0', \dots, \bar{u}_5'} = H^*_y$, where H^* acts on $\bar{V}^6 \ni y$ diagonally. Let O' be the H^*-orbit of y. By Lemma 2.4, $\bar{H}$ acting on O and H^* acting on O' have permutation isomorphic images. So H_B acting on $O'' := H_{B\cup {}^g B}\backslash H_B$ by inverse right translation and H^* acting on O' have permutation isomorphic images. So

$$d(H_B^{O''}) = d((H^*)^{O'}) \le d_{\mathrm{Lin}}(\dim(\bar{V}^6), q) \le d_{\mathrm{Lin}}(6d, q),$$

where $d := \dim V$. Also note $|O''| = |O'| \le |\bar{V}|^6 \le q^{6d}$. Let $k = d(H_B^{O''})$. Then as $N_{c_1}(G) = q^{d \cdot d_{\mathrm{Lin}}(c_1 d, q)}$, $N = N_{c_1}(G)^{c_2}$, and c_1, c_2 are large enough constants, we have

$$[H_B : H_{B\cup {}^g B}]^k = |O''|^k \le q^{6d \cdot d_{\mathrm{Lin}}(6d, q)} \le N_{c_1}(G)^{c_2} = N.$$

Let $\mathcal{P}''$ be the system of stabilizers of depth k over H_B with respect to the action of H_B on $H_{B\cup {}^g B}\backslash H_B$ by inverse right translation. Then $\mathcal{P}'' \subseteq \mathcal{P}'|_{H_B} = \mathcal{P}_{H, c_0, N}|_{H_B}$ by definition. As $(\mathcal{P}'', H_B, H_{B\cup {}^g B})$ is a factoring system by the choice of k, $(\mathcal{P}'|_{H_B}, H_B, H_{B\cup {}^g B})$ is a factoring system, as desired. $\square$

Lemma 6.24. *Let $U_1, U_2 \in S'$ such that $\dim U \cap U_1 = \dim U \cap U_2 = \dim U - 1$ and $U + U_1 = U + U_2$. Then $(\mathcal{P}'|_{H_{U,U_1}}, H_{U,U_1}, H_{U,U_1,U_2})$ is a factoring system.*

Proof. The proof is very similar to that of Lemma 6.22, the main difference being that the quotient space $V/(U \cap U_1)$ is replaced by (the dual of) the subspace $U + U_1$.

We may assume $U \cap U_1 \neq U \cap U_2$ since otherwise the statement holds by Lemma 6.22. Let $W := U + U_1$. Then U, U_1, U_2 are hyperplanes of W. Choose $u_0, w \in W^*$ such that $\ker(u_0) = U_2$ and $\ker(w) = U_1$. Then $u_0, w \in U^*$ are linearly independent since $U_1 \neq U_2$. Choose a set B of subspaces of V as follows:

- If U is totally singular and $S' = S$, let $W_0' = W^*$. If U is totally singular and S' is the set of complements of W_0 in V, let W_0' be the hyperplane of W^* vanishing on $W_0 \cap W$. Finally, if U is non-degenerate, let W_0' be the hyperplane of W^* vanishing on $U^\perp \cap W$.
- If U is totally singular, choose $v_1, v_2 \in W_0'$ such that $u_0, w, v_1, v_2 \in W^*$ are linearly independent. On the other hand, if U is non-degenerate, choose $u_0^*, w^* \in U$ such that $\langle u_0^* \rangle = \ker(u_0|_U)^\perp \cap U$ and $\langle w^* \rangle = \ker(w|_U)^\perp \cap U$. Then choose $v_1, v_2 \in W_0' \cong U^*$ such that u_0, w, v_1, v_2 are linearly independent, $v_i(u_0^*) = v_i(w^*) = 0$ for $i = 1, 2$, and the one-dimensional subspaces $\ker(v_1|_U)^\perp \cap U$, $\ker(v_2|_U)^\perp \cap U$ are spanned by singular vectors.[5]
- Let $u_1 = u_0 + v_1$, $u_2 = u_0 + v_2$, $u_3 = u_0 + v_1 + v_2$, $u_4 = u_0 + \alpha v_1$ and $u_5 = w + v_1$, where α is an element in $\mathbb{F}_q$ that is not in any proper subfield.
- For $0 \leq i \leq 5$, let $W_i = \ker(u_i) \subseteq W$. Note $W_0 = U_2$.
- Let $B = \{U, U_1\} \cup \{W_0, W_1, \ldots, W_5\}$.

The following claim is proved in Appendix B.

Claim 6.25. $W_1, \ldots, W_5 \in S'$.

As $H_B \leq H_{U,U_1,U_2}$, it suffices to prove that $(\mathcal{P}'|_{H_{U,U_1}}, H_{U,U_1}, H_B)$ is a factoring system by Lemma 3.2. By Corollary 6.5, it suffices to prove that $(\mathcal{P}'|_{H_B}, H_B, H_{B \cup {}^g B})$ is a factoring system for all $g \in H_{U,U_1}$. Fix $g \in H_{U,U_1}$. Lift $g|_W$ to $\tilde{g} \in \Gamma\mathrm{L}(W)$. The group $\Gamma\mathrm{L}(W)$ acts semilinearly on W^* via ${}^h L)(x) = {}^{\sigma(h)}(L({}^{h^{-1}}x))$ for $h \in \Gamma\mathrm{L}(W)$, $L \in W^*$ and $x \in W$ (see Appendix B). Let $u_i' = {}^{\tilde{g}}u_i \in W^*$ for $0 \leq i \leq 5$. Let $v_1' = {}^{\tilde{g}}v_1$ and $v_2' = {}^{\tilde{g}}v_2$.

As $H_B \leq H_{U,U_1}$ fixes $U + U_1 = W$, we have a group homomorphism $\phi : H_B \to \mathrm{P\Gamma L}(W^*)$. The image $\phi(h)$ of $h \in H_B$ is defined as follows: lift h to $\tilde{h} \in \Gamma\mathrm{L}(V)$ and restrict it to the subspace W, which gives $\tilde{h}|_W \in \Gamma\mathrm{L}(W)$. As $\Gamma\mathrm{L}(W)$ acts semilinearly on W^*, the image of $\tilde{h}|_W$ under the permutation representation $\Gamma\mathrm{L}(W) \to \mathrm{Sym}(W^*)$ is an element of $\Gamma\mathrm{L}(W^*)$. Define $\phi(h)$ to be its reduction modulo scalars.

Let $\bar{H} = \phi(H_B) \leq \mathrm{P\Gamma L}(W^*)$. Let

$$x = (\langle u_0' \rangle, \ldots, \langle u_5' \rangle) \in (\mathbb{P}W^*)^6.$$

and let O be the $\bar{H}$-orbit of x under the diagonal action. Note that for $h \in H_B$ and $0 \leq i \leq 5$, h fixes ${}^g W_i = \ker(u_i')$ iff $\phi(h)$ fixes $\langle u_i' \rangle$. So $H_{B \cup {}^g B} = (H_B)_{{}^g W_0, {}^g W_1, \ldots, {}^g W_5} = \phi^{-1}(\bar{H}_x)$. By Lemma 2.4, H_B acting on $H_{B \cup {}^g B} \backslash H_B$ by inverse right translation and $\bar{H}$ acting on O have permutation isomorphic images.

Define H^* to be the subgroup of $\mathrm{GL}(W^*)$ consisting of the elements h such that ${}^h w = w$ and the image of h in $\mathrm{PGL}(W^*)$ is in $\bar{H}$. So we have a group homomorphism $\psi : H^* \to \bar{H}$. We claim that ψ is surjective and $H^*_{u_0', \ldots, u_5'} = \psi^{-1}(\bar{H}_x)$.

To prove the claims, consider arbitrary $h \in \bar{H} \leq \mathrm{P\Gamma L}(W^*)$ and lift it to $\tilde{h} \in \Gamma\mathrm{L}(W^*)$. Then $\tilde{h}$ fixes $\langle u_0 \rangle, \ldots, \langle u_5 \rangle$. It also fixes $\langle w \rangle$ since H_B fixes $U_1 = \ker(w)$. Applying Claim 6.23 to $u_0, w, v_1, v_2 \in W^*$, we see $h \in \mathbb{F}_q^\times(\mathrm{GL}(W^*)_{u_0, u_1, \ldots, u_5, w})$. By scaling, we may assume $h \in \mathrm{GL}(W^*)_{u_0, u_1, \ldots, u_5, w}$. So $h \in H^*$. This proves the first claim that ψ is surjective.

Now suppose $h \in \bar{H}_x$. Let $\tilde{h} \in H^*$ be a preimage of h under ψ. So $\tilde{h}$ fixes $\langle u_0' \rangle, \ldots, \langle u_5' \rangle$ and $\langle w \rangle$. Applying Claim 6.23 with u_i replaced by u_i' for $0 \leq i \leq 5$ and v_j replaced by v_j' for $j = 1, 2$, we see that

[5] Such v_1 and v_2 exist as U is non-degenerate and we assume $\dim U > c$ for a large enough constant $c > 0$.

$\tilde{h} \in \mathbb{F}_q^\times(\mathrm{GL}(W^*)_{u_0',u_1',\ldots,u_5',w})$. As $\tilde{h} \in H^*$, it fixes w. So $\tilde{h} \in H^*_{u_0',\ldots,u_5'}$. This proves the second claim that $H^*_{u_0',\ldots,u_5'} = \psi^{-1}(\bar{H}_x)$.

Let $y = (u_0', \ldots, u_5')$. So $H^*_{u_0',\ldots,u_5'} = H^*_y$, where H^* acts on $(W^*)^6 \ni y$ diagonally. Let O' be the H^*-orbit of y. By Lemma 2.4, $\bar{H}$ acting on O and H^* acting on O' have permutation isomorphic images. So H_B acting on $O'' := H_{B\cup {}^g B}\backslash H_B$ by inverse right translation and H^* acting on O' have permutation isomorphic images. So

$$d(H_B^{O''}) = d((H^*)^{O'}) \le d_{\mathrm{Lin}}(\dim((W^*)^6), q) \le d_{\mathrm{Lin}}(6d, q),$$

where $d := \dim V$. Also note $|O''| = |O'| \le |W^*|^6 \le q^{6d}$. Let $k = d(H_B^{O''})$. Then as $N_{c_1}(G) = q^{d\cdot d_{\mathrm{Lin}}(c_1 d, q)}$, $N = N_{c_1}(G)^{c_2}$, and c_1, c_2 are large enough constants, we have

$$[H_B : H_{B\cup {}^g B}]^k = |O''|^k \le q^{6d\cdot d_{\mathrm{Lin}}(6d,q)} \le N_{c_1}(G)^{c_2} = N.$$

Let $\mathcal{P}''$ be the system of stabilizers of depth k over H_B with respect to the action of H_B on $H_{B\cup {}^g B}\backslash H_B$ by inverse right translation. Then $\mathcal{P}'' \subseteq \mathcal{P}'|_{H_B} = \mathcal{P}_{H,c_0,N}|_{H_B}$ by definition. As $(\mathcal{P}'', H_B, H_{B\cup {}^g B})$ is a factoring system by the choice of k, $(\mathcal{P}'|_{H_B}, H_B, H_{B\cup {}^g B})$ is a factoring system, as desired. □

Now we are ready to prove Lemma 6.18.

Proof of Lemma 6.18. Let $x \in S'$. We want to prove that $(\mathcal{P}', H, H_x)$ is a factoring system. By relabeling, we may assume $x = U$.

We claim that for every $U' \in S'$, there exists a finite sequence $Y_0, \ldots, Y_k \in S'$ such that $Y_0 = U$, $Y_k = U'$, and $\dim Y_{i-1} \cap Y_i \ge \dim U - 1$ for $i \in [k]$. First consider the case that V is in Case **L**.The claim is obvious when $S' = S$. So assume S' is the set of complements of W_0 in V. Pick a basis B of U, a basis B' of U', and a basis B'' of W_0. We construct each Y_i together with a basis B_i of Y_i. Let $Y_0 = U$ and $B_0 = B$. Suppose Y_{i-1} and B_{i-1} are already constructed. If $Y_{i-1} = U'$ then we are done. Otherwise, choose $u \in B' - B_{i-1}$. Then the set $B_{i-1} \cup \{u\} \cup B''$ is linearly dependent since Y_{i-1} is a complement of W_0 in V. Moreover, the linear dependence must involve some element $v \in B_{i-1} - B'$ since $U' \cap W_0 = \{0\}$. Let $B_i = (B_{i-1} \cup \{u\}) - \{v\}$ and let Y_i be the span of B_i. The basis exchange property of matroids guarantees that $B_i \cup B''$ is linearly independent and hence Y_i is a complement of W_0 in V. Note $\dim Y_{i-1} \cap Y_i \ge \dim U - 1$ and $|B_i \cap B'| > |B_{i-1} \cap B'|$. Continue this process until $Y_i = U'$.

Now consider the case that V is in Case **S**, **U** or **O**. So $S' = S$. Let K be the subgroup of $I(V)$ generated by the transvections and the reflections. By Lemma A.16, the image of K in $\mathrm{P\Gamma L}(V)$ contains G_0 as a subgroup. So K is transitive on S. Thus we may construct a sequence $U = Y_0, Y_1, \ldots, Y_k = U'$ of subspaces in S such that for each $i \in [k]$, $Y_i = {}^{g_i}Y_{i-1}$ where g_i is a transvection or a reflection. As each transvection (resp. reflection) fixes a hyperplane of V pointwisely, we see $\dim Y_{i-1} \cap Y_i \ge \dim U - 1$. So the claim holds.

By Lemma 6.3, it suffices to prove for every $U', U_0 \in S'$ satisfying $\dim U' \cap U_0 = \dim U - 1$ that $(\mathcal{P}'|_{H_{U'}}, H_{U'}, H_{U',U_0})$ is a factoring system. For such U' and U_0, we may choose $g \in G$ that sends U' to U and, if V is in Case **L** and S' is the set of complements of W_0 in V, then g fixes W_0. By replacing each group K by its conjugate gKg^{-1}, we may assume $U' = U$, i.e., it suffices to prove $(\mathcal{P}'|_{H_U}, H_U, H_{U,U_0})$ is a factoring system for all $U_0 \in S'$ satisfying $\dim U \cap U_0 = \dim U - 1$. Fix such U_0.

By Corollary 6.5, we just need to prove for all $g \in H_U$ that $(\mathcal{P}'|_{H_{U,U_0}}, H_{U,U_0}, H_{U,U_0,U_1})$ is a factoring system, where $U_1 = {}^g U_0$. Fix $g \in H_U$. Applying Corollary 6.5 again, we see it suffices to prove for all $h \in H_{U,U_0}$ that $(\mathcal{P}'|_{H_{U,U_0,U_1}}, H_{U,U_0,U_1}, H_{U,U_0,U_1,U_2})$ is a factoring system, where $U_2 = {}^h U_1$. Fix $h \in H_{U,U_0}$.

By Lemma 6.21, there exists a finite sequence of subspaces $Z_0, \ldots, Z_\ell \in S'$ such that $\dim U \cap Z_i = \dim U - 1$ for $0 \le i \le \ell$, $Z_0 = U_1$, $Z_\ell = U_2$, and at least one of the following holds for each $i \in [\ell]$:

(1) $U \cap Z_{i-1} = U \cap Z_i$.

(2) $U + Z_{i-1} = U + Z_i$.

By Lemma 6.3, it suffices to prove for every $i \in [\ell]$ that $(\mathcal{P}'|_{H_{U,U_0,Z_{i-1}}}, H_{U,U_0,Z_{i-1}}, H_{U,U_0,Z_{i-1},Z_i})$ and $(\mathcal{P}'|_{H_{U,U_0,Z_i}}, H_{U,U_0,Z_i}, H_{U,U_0,Z_{i-1},Z_i})$ are factoring systems. Fix $i \in [\ell]$.

Let $H^* := H_{U_0}$. Then $\mathcal{P}_{H^*,c_0-1,N} \subseteq \mathcal{P}_{H,c_0,N} = \mathcal{P}'$, where $\mathcal{P}_{H^*,c_0-1,N}$ and $\mathcal{P}_{H,c_0,N}$ are defined with respect to the actions of H^* and H on S'. Applying Lemma 6.22 and Lemma 6.24 with H replaced by H^*, we see $(\mathcal{P}'|_{H_{U,U_0,Z_{i-1}}}, H_{U,U_0,Z_{i-1}}, H_{U,U_0,Z_{i-1},Z_i})$ and $(\mathcal{P}'|_{H_{U,U_0,Z_i}}, H_{U,U_0,Z_i}, H_{U,U_0,Z_{i-1},Z_i})$ are factoring systems, as desired. □

Corollary 6.26. *Lemma 6.14 holds when G is in Case (1) of Definition 6.13.*

Proof of Case (2). Now suppose G is in Case (2) of Definition 6.13. So V is in Case **L**. Let S be the G-orbit of the unordered pair $\{U, W\}$. Then the action of G on $M\backslash G$ is equivalent to its action on S. Let $\iota \in G$ such that ι is the transpose-inverse automorphism with respect to a basis B of V.

Lemma 6.27. *Lemma 6.14 holds when G is in Case (2) of Definition 6.13.*

Proof. We have $\dim U \neq \dim W$ for $\{U, W\} \in S$ since otherwise $\dim U = \frac{1}{2}\dim V$ holds, which implies $b(G) = O(1)$ by Lemma 6.16, contradicting our assumption.

For $\{U_1, W_1\}, \{U_2, W_2\} \in S$, where $\dim U_1 < \dim W_1$ and $\dim U_2 < \dim W_2$, write $\{U, W\} \sim \{U', W'\}$ if either of the following holds:

- $U_1 = U_2$ and $\dim W_1 \cap W_2 = \dim W_1 - 1 = \dim W_2 - 1$;
- $\dim U_1 \cap U_2 = \dim U_1 - 1 = \dim U_2 - 1$ and $W_1 = W_2$.

As $G_0 = \mathrm{PSL}(V)$, it is easy to see that for any $\{U_1, W_1\}, \{U_2, W_2\} \in S$, there exist a sequence $Z_0, \ldots, Z_k \in S$ such that $Z_0 = \{U_1, W_1\}$, $Z_k = \{U_2, W_2\}$, and $Z_{i-1} \sim Z_i$ for $i \in [k]$.

By Lemma 6.4, it suffices to prove for every $\{U_1, W_1\}, \{U_2, W_2\} \in S$ satisfying $\{U_1, W_1\} \sim \{U_2, W_2\}$ that $(\mathcal{P}|_{H_{\{U_1,W_1\}}}, H_{\{U_1,W_1\}}, H_{\{U_1,W_1\},\{U_2,W_2\}})$ is a factoring system. Fix such $\{U_1, W_1\}$ and $\{U_2, W_2\}$, where $\dim U_1 < \dim W_1$ and $\dim U_2 < \dim W_2$.

Let $H^* := H_{\{U_1,W_1\},\{U_2,W_2\}}$. Suppose there exists $g \in H^*$ that is not in $\mathrm{P\Gamma L}(V)$. Then g exchanges U_1 with W_1 and U_2 with W_2. But this is not possible since $\{U_1, W_1\} \sim \{U_2, W_2\}$ (which implies either $U_1 = U_2$ or $W_1 = W_2$, but $\{U_1, W_1\} \neq \{U_2, W_2\}$). So $H^* \leq \mathrm{P\Gamma L}(V)$ and $H^* = H_{U_1,W_1,U_2,W_2}$.

By Lemma 6.5, it suffices to prove, for every $g \in H_{\{U_1,W_1\}}$, that $(\mathcal{P}|_{H^*}, H^*, H^*_{g\{U_2,W_2\}})$ is a factoring system. Fix $g \in H_{\{U_1,W_1\}}$ and let $\{U_3, W_3\} := {}^g\{U_2, W_2\}$ where $\dim U_3 < \dim W_3$. Then either of the following holds:

- $U_1 = U_3$ and $\dim W_1 \cap W_3 = \dim W_1 - 1 = \dim W_3 - 1$;
- $\dim U_1 \cap U_3 = \dim U_1 - 1 = \dim U_3 - 1$ and $W_1 = W_3$.

Note H and $\iota H \iota^{-1}$ are permutation isomorphic on S with respect to the map $\{U_0, W_0\} \mapsto \{{}^\iota W_0, {}^\iota U_0\}$. By replacing H with $\iota H \iota^{-1}$ and every subspace U_0 with ${}^\iota U_0$ if necessary, we may assume the second case above holds, i.e., $\dim U_1 \cap U_3 = \dim U_1 - 1 = \dim U_3 - 1$ and $W_1 = W_3$. Then $H^*_{g\{U_2,W_2\}} = H^*_{\{U_3,W_3\}} = H^*_{U_3}$ and we want to prove that $(\mathcal{P}|_{H^*}, H^*, H^*_{U_3})$ is a factoring system.

As $W_1 = W_3$, we know either $U_1, U_3 \subseteq W_1$ or $V = U_1 \oplus W_1 = U_3 \oplus W_1$. First assume $U_1, U_3 \subseteq W_1$. Let T be the set of all subspaces of W_1 of dimension $\dim U_1$. As H^* fixes W_1, it permutes the members of T. Note for every $U_0 \in T$, we have $\{U_0, W_1\} \in S$ and $H^*_{\{U_0,W_1\}} = H^*_{U_0}$. So $\mathcal{P}|_{H^*}$ contains $\mathcal{P}' := \mathcal{P}_{H^*,c_0-2,N}$ with respect to the action of H^* on T. By Corollary 6.26 (applied to $H^*|_{W_1} \leq \mathrm{P\Gamma L}(W_1)$), $(\mathcal{P}', H^*, H^*_{U_3})$ is a factoring system. As $\mathcal{P}' \subseteq \mathcal{P}|_{H^*}$, $(\mathcal{P}|_{H^*}, H^*, H^*_{U_3})$ is a factoring system, as desired.

Now assume $V = U_1 \oplus W_1 = U_3 \oplus W_1$. Let S' be the set of all complements of W_1 in V. As H^* fixes W_1, it permutes the members of S'. Note for every $U_0 \in S'$, we have $\{U_0, W_1\} \in S$ and $H^*_{\{U_0,W_1\}} = H^*_{U_0}$. So $\mathcal{P}|_{H^*}$ contains $\mathcal{P}' := \mathcal{P}_{H^*,c_0-2,N}$ with respect to the action of H^* on S'. By Lemma 6.18, $(\mathcal{P}', H^*, H^*_{U_3})$ is a factoring system. As $\mathcal{P}' \subseteq \mathcal{P}|_{H^*}$, $(\mathcal{P}|_{H^*}, H^*, H^*_{U_3})$ is a factoring system, as desired. □

Proof of Case (3). We identify G_0 with $I(V, F) \cong \mathrm{Sp}_{2m}(q)$ and $M \cap G_0$ with $I(V, Q) \cong \mathrm{O}^{\pm}_{2m}(q)$, where Q is a non-degenerate quadratic form on $V \cong \mathbb{F}_q^{2m}$ and F is the associated bilinear form $F(x, y) = Q(x + y) - Q(x) - Q(y)$.[6] The group $\Gamma\mathrm{L}(V) \geq G$ acts on the set of quadratic forms

[6]Here $I(V, F)$ is isomorphic to $\overline{\Omega(V, F)}$ [KL90, Table 2.1.C and Table 2.1.D].

$Q : V \to \mathbb{F}_q$ via $({}^gQ)(x) = {}^{\sigma(g)}(Q({}^{g^{-1}}x))$, where $\sigma(g) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is as defined in Definition A.10 in the appendix. For two quadratic forms Q_1 and Q_2, write $Q_1 \sim Q_2$ if $Q_1 = \lambda Q_2$ for some $\lambda \in \mathbb{F}_q^\times$, and write $[Q_1]$ for the equivalence class of a quadratic form Q_1 under $\sim$. Then $\Gamma\mathrm{L}(V)$ also acts on the set of equivalence classes of quadratic forms under $\sim$. Let S be the G-orbit of $[Q]$.

Lemma 6.28. *G_0 is transitive on S and the action of G on S is equivalent to its action on $M\backslash G$ by inverse right translation.*

Proof. Consider $Q' = {}^gQ$ where g is an arbitrary element in G. Let F' be the associated bilinear form of Q', i.e.,

$$F'(x,y) = Q'(x+y) - Q'(x) - Q'(y) = {}^{\sigma(g)}(F({}^{g^{-1}}x, {}^{g^{-1}}y)).$$

As $g \in G \leq \Gamma(V,F)$, we have $F({}^{g^{-1}}x, {}^{g^{-1}}y) = \lambda \cdot {}^{\sigma(g^{-1})}(F(x,y))$ where $\lambda \in \mathbb{F}_q^\times$ and $\sigma(g^{-1}) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ are independent of x and y. As σ is a group homomorphism, we have $\sigma(g^{-1}) = \sigma(g)^{-1}$ and $F' = \lambda' F$, where $\lambda' = {}^{\sigma(g)}\lambda$.

Let $Q'' = \lambda'^{-1}Q'$. Note Q, Q' and Q'' are non-degenerate quadratic forms of the same Witt index. So (V,Q) is isometric to (V,Q'') by Lemma A.7. In other worlds, there exists $h \in \mathrm{GL}(V)$ such that $Q''(x) = Q({}^hx)$. Then

$$F_{Q''}(x,y) = Q''(x+y) - Q''(x) - Q''(y) = Q({}^hx + {}^hy) - Q({}^hx) - Q({}^hy) = F({}^hx, {}^hy)$$

is the associated bilinear form of Q''. On the other hand, the associated bilinear form of Q'' is $\lambda'^{-1}F' = F$. So $F({}^hx, {}^hy) = F(x,y)$ for $x, y \in V$, i.e., $h \in I(V,F) = G_0$. Then $h^{-1} \in G_0$. By definition, we have

$$({}^{h^{-1}}Q)(x) = {}^{\sigma(h^{-1})}(Q({}^hx)) = Q({}^hx) = Q''(x)$$

for $x \in V$. So $Q'' = {}^{h^{-1}}Q$. Then $[Q'] = [Q''] = {}^{h^{-1}}[Q]$. As $[Q'] \in S$ is arbitrary, G_0 is transitive on S.

It was shown in [Dye80, Theorem 3] that $M \cap G_0 = I(V,Q)$ is maximal in $G_0 = I(V,F)$ (provided $m > 1$), or equivalently, G_0 acts primitively on $M\backslash G$ by inverse right translation. As $G_0 = I(V,F)$ where F is the associated bilinear form of Q, any $g \in G_0$ fixing $[Q]$ also fixes Q. So $(G_0)_{[Q]} = (G_0)_Q = M \cap G_0$. Therefore, the action of G_0 on S is equivalent to its action on $M\backslash G$. The former action extends to an action of G on S, whereas the latter action extends to an action of G on $M\backslash G$ by inverse right translation. Both actions of G are primitive since G_0 is primitive on S and $M\backslash G$.

To show these two actions of G are equivalent, it suffices to show that a primitive action of G extending the action of G_0 on $M\backslash G$ by inverse right translation is unique. Consider such an action of G. The stabilizer G_x of $x := Me \in M\backslash G$ is contained in $N_G((G_0)_x)$, since $g(G_0)_x g^{-1} = (G_0)_{gx} = (G_0)_x$ for $g \in G_x$. If $N_G((G_0)_x) = G$ then G and G_0 both act regularly on $M\backslash G$ and we are done. So assume $N_G((G_0)_x) \lneq G$. Maximality of G_x in G then implies $G_x = N_G((G_0)_x)$. So the stabilizer G_x is uniquely determined. It follows that the action of G is uniquely determined, as desired. □

For $v \in V - \{0\}$ and $\lambda \in \mathbb{F}_q^\times$, denote by $t_{v,\lambda} : V \to V$ the transvection $x \mapsto x + \lambda F(x,v)v$, which is a member of $G_0 = I(V,F)$ by Lemma A.15. Also denote by $L_{v,\lambda}$ the linear form

$$L_{v,\lambda} : x \mapsto (\lambda^2 Q(v) + \lambda)^{1/2} F(x,v)$$

on V, which is a member of the dual space V^*. Note the square root is well-defined and unique since $p = 2$. As usual, let $\Gamma\mathrm{L}(V)$ act on V^* via $({}^gL)(x) = {}^{\sigma(g)}(L({}^{g^{-1}}x))$. Then we have the following lemma.

Lemma 6.29. *Let $v \in V - \{0\}$, $\lambda \in \mathbb{F}_q^\times$, and $Q' = {}^{t_{v,\lambda}^{-1}}Q$. Then $\Gamma\mathrm{L}(V)_{[Q],[Q']} = \mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_{v,\lambda}})$.*

Proof. As $Q' = {}^{t_{v,\lambda}^{-1}}Q$ and $t_{v,\lambda} \in G_0 = I(V,F)$, F is the associated bilinear form of both Q and Q'. Consider $g \in \Gamma\mathrm{L}(V)_{[Q],[Q']}$. We know g sends Q to cQ and Q' to $c'Q'$ for some $c, c' \in \mathbb{F}_q^\times$. Then g sends F to both cF and $c'F$, which implies $c = c'$. Let $g' = c^{1/2}g \in \Gamma\mathrm{L}(V)$. Then $({}^{g'}Q)(x) = ({}^gQ)(c^{-1/2}x) = c^{-1}({}^gQ)(x) = Q(x)$. Similarly, $({}^{g'}Q')(x) = Q'(x)$. So g' fixes both Q and Q'.

By definition, we have

$$\begin{aligned} Q'(x) &= ({}^{t_{v,\lambda}^{-1}}Q)(x) = Q({}^{t_{v,\lambda}}x) = Q(x + \lambda F(x,v)v) \\ &= Q(x) + Q(\lambda F(x,v)v) + F(x, \lambda F(x,v)v) \\ &= Q(x) + (\lambda^2 Q(v) + \lambda)F(x,v)^2 \\ &= Q(x) + L_{v,\lambda}(x)^2. \end{aligned}$$

Similarly, we have

$$({}^{g'}Q')(x) = ({}^{g'}Q)(x) + ({}^{g'}L_{v,\lambda})(x)^2. \tag{1}$$

As g' fixes Q and Q', it also fixes $L_{v,\lambda}$ (note $p = 2$). Therefore $g = c^{-1/2}g' \in \mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_{v,\lambda}})$.

Conversely, suppose $g \in \mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_{v,\lambda}})$. Then $g = \lambda g'$ for some $g' \in \Gamma\mathrm{L}(V)_{Q,L_{v,\lambda}}$ and $\lambda \in \mathbb{F}_q^\times$. As g' fixes Q and $L_{v,\lambda}$, it also fixes Q' by Equation (1). So $g = \lambda g'$ fixes $[Q]$ and $[Q']$, which implies $g \in \Gamma\mathrm{L}(V)_{[Q],[Q']}$. □

Lemma 6.30. *Lemma 6.14 holds when G is in Case (3) of Definition 6.13.*

Proof. By Lemma 6.28, the action of G on $M\backslash G$ by inverse right translation is equivalent to its action on the set S of equivalence classes of quadratic forms. We prove Lemma 6.14 with respect to the latter action.

By Lemma 6.28, G_0 is transitive on S. By Lemma A.16, G_0 is generated by the set of transvections it contains. Such a transvection has the form $t_{v,\lambda}$ for some $v \in V - \{0\}$ and $\lambda \in \mathbb{F}_q^\times$. Fix v and λ. Let $Q' = {}^{t_{v,\lambda}^{-1}}Q$. By Corollary 6.5, it suffices to prove that $(\mathcal{P}|_{H_{[Q]}}, H_{[Q]}, H_{[Q],[Q']})$ is a factoring system.

First assume $q = 2$. Then $H_{[Q]} = H_Q \leq \mathrm{GL}(V)$. And $H_{[Q],[Q']} = H \cap \mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_{v,\lambda}}) = H_{[Q],L_{v,\lambda}}$ by Lemma 6.29. So the action of $H_{[Q]}$ on $O := H_{[Q]}[Q']$ is equivalent to its action on the $H_{[Q]}$-orbit of $L_{v,\lambda} \in V^*$. Denote the $H_{[Q]}$-orbit of $L_{v,\lambda}$ by O'. Then $d(H_{[Q]}^O) = d(H_{[Q]}^{O'}) \leq d_{\mathrm{Lin}}(2m, q)$ by the definition of d_{Lin}. Also note $|O| = |O'| \leq |V^*| = q^{2m}$. Let $\mathcal{P}'$ be the system of stabilizer of depth $k := d(H_{[Q]}^O)$ over $H_{[Q]}$ with respect to the action of $H_{[Q]}$ on O. As $N = (N_{c_1}(G))^{c_2}$, $N_{c_1}(G) = q^{2md_{\mathrm{Lin}}(2c_1m,q)}$, and $c_1, c_2 \in \mathbb{N}^+$, we have

$$[H_{[Q]} : H_{[Q],[Q']}]^k = |O|^k \leq q^{2md_{\mathrm{Lin}}(2m,q)} \leq N_{c_1}(G) \leq N.$$

Then $\mathcal{P}' \subseteq \mathcal{P}|_{H_{[Q]}}$ by the definition of $\mathcal{P}$. So $(\mathcal{P}|_{H_{[Q]}}, H_{[Q]}, H_{[Q],[Q']})$ is a factoring system, as desired.

Now assume $q > 2$. As F is a non-degenerate bilinear form and $q > 2$, for every $u \in V^* - \{0\}$, we may choose $v(u) \in V - \{0\}$ and $\lambda(u) \in \mathbb{F}_q^\times$ such that u is the linear map $x \mapsto F(x, v(u))$ and $\lambda(u)^2Q(v(u)) + \lambda(u) \neq 0$. Then $\langle L_{v(u),\lambda(u)}\rangle = \langle u\rangle$. We write $L(u)$ for $L_{v(u),\lambda(u)}$.

Let $L_0 = L_{v,\lambda}$. Choose $u_1 \in V^* - \langle L_0\rangle$ and let $L_1 = L(u_1)$. Let $u_2 = L_0 + \alpha L_1$ and $L_2 = L(u_2)$, where $\alpha \in \mathbb{F}_q$ is not in any proper subfield. For $i = 1, 2$, let $Q_i = {}^{t_{v(u_i),\lambda(u_i)}^{-1}}Q$. Let $B = \{[Q], [Q'], [Q_1], [Q_2]\} \subseteq S$.

As $H_{[Q],[Q']} \leq H_B$, it suffices to prove that $(\mathcal{P}|_{H_{[Q]}}, H_{[Q]}, H_B)$ is a factoring system by Lemma 3.2. By Corollary 6.5, it suffices to prove for all $g \in H_{[Q]}$ that $(\mathcal{P}|_{H_B}, H_B, H_{B\cup {}^gB})$ is a factoring system. Fix $g \in H_{[Q]}$. Let $x := ({}^g[Q'], {}^g[Q_1], {}^g[Q_2]) \in S^3$ and let $O \subseteq S^3$ be the H_B-orbit of x under the diagonal action. Note $H_{B\cup {}^gB} = (H_B)_x$. Let $\overline{H_B} := H_B/(H_B \cap \mathbb{F}_q^\times) \leq \mathrm{P\Gamma L}(V)$. As the group of scalars $\mathbb{F}_q^\times$ acts trivially on O, the action of H_B on O factors through the action of $\overline{H_B}$. So H_B and $\overline{H_B}$ have permutation isomorphic images on O.

Let H^* be the subgroup of $\mathrm{GL}(V)$ consisting of all $g \in \mathrm{GL}(V)$ such that ${}^gQ = Q$ and the image of g in $\mathrm{PGL}(V)$ is in $\overline{H_B}$. We have the natural map $\phi : H^* \to \overline{H_B}$. We claim ϕ is surjective. To see this, consider $\bar{h} \in \overline{H_B}$ and lift it to $h \in \mathrm{P\Gamma L}(V)$. Then h fixes $[Q]$. By multiplying h by a scalar, we may assume h fixes Q. It remains to show $h \in \mathrm{GL}(V)$, which implies $h \in H^*$ and $\phi(h) = \bar{h}$. We know h fixes Q and $[Q'], [Q_1], [Q_2]$. By Lemma 6.29, we have

$$h \in (\mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_0})) \cap (\mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_1})) \cap (\mathbb{F}_q^\times(\Gamma\mathrm{L}(V)_{Q,L_2})).$$

As h fixes Q, it must also fix L_0, L_1, L_2. As $\langle L_2\rangle = \langle u_2\rangle$, there exists $c \in \mathbb{F}_q^\times$ such that $L_2 = cu_2 = c(L_0 + \alpha L_1)$. Then h sends L_2 to ${}^{\sigma(h)}c \cdot (L_0 + {}^{\sigma(h)}\alpha \cdot L_1) = L_2$. As L_0 and L_1 are linearly independent, this implies ${}^{\sigma(h)}\alpha = \alpha$. So $\sigma(h) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is the identity, i.e., $h \in \mathrm{GL}(V)$. This proves the claim that ϕ is surjective.

Next, we claim $h \in H^*$ fixes ${}^gQ', {}^gQ_1, {}^gQ_2$ iff $\phi(h)$ fixes $x = ({}^g[Q'], {}^g[Q_1], {}^g[Q_2])$. The "only if" part is obvious. Conversely, suppose $\phi(h)$ fixes x. Then h multiplies ${}^gQ', {}^gQ_1, {}^gQ_2$ by scalars. Note $Q = {}^gQ$ and ${}^gQ', {}^gQ_1, {}^gQ_2$ have the same associated bilinear form (since $t_{v,\lambda}, t_{v(u_1),\lambda(u_1)}, t_{v(u_2),\lambda(u_2)} \in I(V, F)$). As h fixes Q, it must also fix ${}^gQ', {}^gQ_1, {}^gQ_2$, as claimed.

On the other hand, any $h \in H^*$ fixes ${}^gQ', {}^gQ_1, {}^gQ_2$ iff it fixes ${}^gL_0, {}^gL_1, {}^gL_2$ (see Equation (1) in the proof of Lemma 6.29). Let $O' \subseteq (V^*)^3$ be the H^*-orbit of $({}^gL_0, {}^gL_1, {}^gL_2)$ under the diagonal action. By Lemma 2.4, H^* acting on O' and $\overline{H_B}$ acting on O have permutation isomorphic images. So H^* acting on O' and H_B acting on O have permutation isomorphic images. Therefore,

$$d(H_B^O) = d((H^*)^{O'}) \le d_{\mathrm{Lin}}(3 \dim V^*, q) = d_{\mathrm{Lin}}(6m, q).$$

Also note $|O| = |O'| \le |(V^*)^3| = q^{6m}$. Let $\mathcal{P}'$ be the system of stabilizer of depth $k := d(H_B^O)$ over H_B with respect to the action of H_B on $H_{B\cup {}^gB}\backslash H_B$ by inverse right translation. As $N = N_{c_1}(G)^{c_2}$, $N_{c_1}(G) = q^{2md_{\mathrm{Lin}}(2c_1m,q)}$, and c_1, c_2 are large enough constants, we have

$$[H_B : H_{B\cup {}^gB}]^k = |O|^k \le q^{6md_{\mathrm{Lin}}(6m,q)} \le N_{c_1}(G)^{c_2} = N.$$

which implies $\mathcal{P}' \subseteq \mathcal{P}|_{H_B}$. So $(\mathcal{P}|_{H_B}, H_B, H_{B\cup {}^gB})$ is a factoring system, as desired. □

Lemma 6.14 now follows from Corollary 6.26, Lemma 6.27 and Lemma 6.30.

6.3.2 Primitive permutation groups of almost simple type

We need the following result of Liebeck and Shalev.

Theorem 6.31 ([LS99, Theorem 1.3])**.** *Let G be a primitive permutation group of almost simple type. Then one of the following holds:*

(1) G is $\mathrm{Alt}(m)$ or $\mathrm{Sym}(m)$ acting on k-subsets of $[m]$ or on partitions of $[m]$ into k parts of size m/k;

(2) G is a classical group in a subspace action;

(3) $b(G) \le c$, where $c \in \mathbb{N}^+$ is an absolute constant.

Case (1) of Theorem 6.31 was analyzed in [Guo20], where the following statement was proved.

Lemma 6.32 ([Guo20, Lemma 5.9 and Lemma 5.12])**.** *Let G be as in Case (1) of Theorem 6.31, acting on a finite set S. Let H be a subgroup of G on S. Suppose $\mathcal{P}$ is a subgroup system over H such that*

(1) $H_{x,y} \in \mathcal{P}$ for all $x, y \in S$, and

(2) $(H_{x,y})_U \in \mathcal{P}$ for all $x, y, z \in S$ and $U \subseteq H_{x,y}z$ satisfying $|H_{x,y}z| \le 4m$ and $|U| \le d_{\mathrm{Sym}}(4m)$.

Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$.

Now we are ready to show that Lemma 5.3 holds for finite primitive permutation groups of almost simple type, or more generally for subgroups of such groups.

Lemma 6.33. *Let G be a primitive permutation group of almost simple type on a finite set S of cardinality n. Let H be a subgroup of G on S. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = N_{c_1}(G)^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$. In particular, Lemma 5.3 holds for finite primitive permutation groups of almost simple type.*

Proof. Suppose G is as in Case (1) of Theorem 6.31. As c_0, c_1, c_2 are large enough constants, we have $N = N_{c_1}(G)^{c_2} \ge N_{c_1}(\mathrm{Alt}(m))^{c_2} \ge (4m)^{d_{\mathrm{Sym}}(4m)}$ and the conditions in Lemma 6.32 about $\mathcal{P}$ are satisfied. So $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$ by Lemma 6.32.

Next, in Case (2) of Theorem 6.31, the lemma holds by Lemma 6.14. Finally, in Case (3) of Theorem 6.31, the lemma holds since $d(H) \le b(H) \le b(G) \le c$. □

6.4 Affine type

In this subsection, we verify Lemma 5.3 for finite primitive permutation groups of affine type. First, we define irreducible linear groups and primitive linear groups.

Definition 6.34. *A group $H \leq \mathrm{GL}(V)$ is said to be an* irreducible linear group *on V if H does* not *fixes any subspace $W \subseteq V$ other than $\{0\}$ and V. And H is said to be a* primitive linear group *on V if it is an irreducible linear group on V, and V* cannot *be written as a direct sum $V = \bigoplus_{i=1}^{k} V_i$ with $k > 1$ such that H permutes the direct summands V_i.*

The following fact is well known (see, e.g., [Sup76, Section I.4]).

Lemma 6.35. *Let G be a finite primitive permutation group G of affine type on a vector space V over a prime field $\mathbb{F}_p$. Then the stabilizer $G_0 \subseteq \mathrm{GL}(V)$ of the origin $0 \in V$ is an irreducible linear group on V.*

We prove Lemma 5.3 for affine type by analyzing the stabilizer G_0. In the following, we first discuss the case that G_0 is a primitive linear group over $\mathbb{F}_p$), and then discuss the more general case of irreducible linear groups.

Primitive linear groups. Our analysis is based on the work [LS02, LS14] on primitive linear groups. We start with the following definitions.

Definition 6.36 (fully deleted permutation module [KL90])**.** *Let $k \in \mathbb{N}^+$ and let q be a prime power. Define*

$$\begin{aligned} E(k,q) &:= \{(a,\ldots,a) : a \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^k, \\ M(k,q) &:= \{(a_1,\ldots,a_k) \in \mathbb{F}_q^k : a_1 + \cdots + a_k = 0\}, \\ U(k,q) &:= M(k,q)/(M(k,q) \cap E(k,q)). \end{aligned}$$

Note $\mathrm{Sym}(k)$ acts on $\mathbb{F}_q^k$ by permuting the k coordinates, which induces an action on $U(k,q)$. We call $U(k,q)$ the fully deleted permutation module *for $\mathrm{Sym}(k)$ over $\mathbb{F}_q$.*

Definition 6.37 ([LS02, LS14])**.** *Let $V_1,\ldots,V_k$ be vector spaces over a finite field $\mathbb{F}_q$. Let $G_1,\ldots,G_k$ be finite groups where $G_i \leq \mathrm{GL}(V_i)$ for $i \in [k]$. Define an action of $G_1 \times \cdots \times G_k$ on the tensor product $U := V_1 \otimes \cdots \otimes V_k$ (over $\mathbb{F}_q$) by letting*

$$^{(g_1,\ldots,g_k)}a_1 \otimes \cdots \otimes a_k = {}^{g_1}a_1 \otimes \cdots \otimes {}^{g_k}a_k$$

and extending it to all tensors multilinearly. This gives a linear representation $\rho : G_1 \times \cdots \times G_k \to \mathrm{GL}(U)$. Write $g_1 \otimes \cdots \otimes g_k$ for $\rho(g_1,\ldots,g_k) \in \mathrm{GL}(U)$. And write $G_1 \otimes \cdots \otimes G_k$ for $\rho(G_1 \times \cdots \times G_k) \leq \mathrm{GL}(U)$, called the tensor product *of $G_1,\ldots,G_k$ (over $\mathbb{F}_q$).*

We need the following structure theorem in [LS14] on primitive linear groups.

Theorem 6.38 ([LS14, Theorem 1])**.** *Let V be a finite-dimensional vector space over a prime field $\mathbb{F}_p$, and G be a primitive linear group on V. Choose the largest power q of p such that V can be identified with a vector space $V(q)$ over $\mathbb{F}_q$ and $G \leq \Gamma\mathrm{L}(V(q))$. Let $G^* := G \cap \mathrm{GL}(V(q))$ act naturally on $V(q)$. Then there exists an absolute constant $C \in \mathbb{N}^+$ such that either $b(G^*) \leq C$, or $V(q)$ can be identified with a tensor product over $\mathbb{F}_q$*

$$V(q) = \bigotimes_{i=1}^{s} U(k_i,q) \otimes W_0 \otimes \bigotimes_{j=1}^{t} W_j,$$

where $U(k_i,q)$ is the fully deleted permutation module for $\mathrm{Sym}(k_i)$ over $\mathbb{F}_q$ for $i \in [s]$ and W_j is a vector space of dimension d_j over $\mathbb{F}_q$ for $0 \leq j \leq t$. Here $k_i \geq C$ for $i \in [s]$ and $d_j \geq C$ for $j \in [t]$.[7] *Moreover, if $b(G^*) > C$, then G^* is a subgroup of*

$$\bigotimes_{i=1}^{s} \mathrm{Sym}(k_i) \otimes D_0 \otimes \bigotimes_{j=1}^{t} D_j$$

[7] If $k_i < C$ (resp. $d_j < C$), we may let W_0 absorb the factor $U(k_i,q)$ (resp. W_j). See [LS02, Lemma 3.3].

acting on $V(q)$ that satisfies the following conditions:

(1) For $i \in [s]$, the group $\mathrm{Sym}(k_i)$ acts faithfully on $U(k_i, q)$ by permuting the coordinates.[8]

(2) $D_0 \leq \mathrm{GL}(W_0)$ acts naturally on W_0 and $b(D_0) \leq C$.

(3) For $j \in [t]$, the group D_j is the normalizer in $\mathrm{GL}(W_j) \cong \mathrm{GL}_{d_j}(q)$ of one of the classical groups $\mathrm{SL}_{d_j}(q_j)$, $\mathrm{SU}_{d_j}(q_j^{1/2})$, $\mathrm{Sp}_{d_j}(q_j)$, $\Omega^{\pm}_{d_j}(q_j)$ (d_j even), $\Omega_{d_j}(q_j)$ (d_j odd). Here $\mathbb{F}_{q_j}$ is a subfield of $\mathbb{F}_q$, and $\mathrm{GL}(W_j)$ is identified with $\mathrm{GL}_{d_j}(q)$ by fixing an $\mathbb{F}_q$-basis B_j of W_j.

(4) G^* contains the group $\bigotimes_{i=1}^{s} \mathrm{Alt}(k_i) \otimes \{e\} \otimes \bigotimes_{j=1}^{t} D_j^{(\infty)}$, where $D_j^{(\infty)}$ denotes the last term in the derived series of D_j.

Each group D_j in Definition 6.38 is a subgroup of $\mathbb{F}_q^{\times}\mathrm{GL}_{d_j}(q_j)$ by the following lemma.

Lemma 6.39. *Suppose $\mathbb{F}_{q_0} \subseteq \mathbb{F}_q$, and G is one of the classical groups $\mathrm{SL}_d(q_0)$, $\mathrm{SU}_d(q_0^{1/2})$, $\mathrm{Sp}_d(q_0)$, $\Omega^{\pm}_d(q_0)$ (d even), $\Omega_d(q_0)$ (d odd), where $d > 2$. Then $N_{\mathrm{GL}_d(q)}(G) \leq \mathbb{F}_q^{\times}\mathrm{GL}_d(q_0)$.*

Proof. By [KL90, Proposition 2.10.6], G is absolutely irreducible on $\mathbb{F}_{q_0}^d$, i.e., it remains irreducible on $\mathbb{F}_{q_0}^d \otimes \mathbb{F}$ for all extension fields $\mathbb{F}$ of $\mathbb{F}_{q_0}$, where the tensor product is taken over $\mathbb{F}_{q_0}$. By [KL90, Proposition 2.10.6 (iv)], this implies that the irreducible $\mathbb{F}_{q_0}G$-submodules of $\mathbb{F}_q^d$ are precisely the subspaces $\mathbb{F}_{q_0}^d \otimes \lambda$, with $\lambda \in \mathbb{F}_q^{\times}$. Suppose $g \in N_{\mathrm{GL}_d(q)}(G)$, then it sends the irreducible $\mathbb{F}_{q_0}G$-submodule $\mathbb{F}_{q_0}^d \otimes 1$ to another irreducible $\mathbb{F}_{q_0}G$-submodule, which is of the form $\mathbb{F}_{q_0}^d \otimes \lambda$. Then $g' := \lambda^{-1}g$ preserves the subspace $\mathbb{F}_{q_0}^d$. So the matrix form of g' in the standard basis has all its entries in $\mathbb{F}_{q_0}$, i.e., $g' \in \mathrm{GL}_d(q_0)$. It follows that $g' = \lambda g \in \mathbb{F}_q^{\times}\mathrm{GL}_d(q_0)$. □

For convenience, we also make the following definition.

Definition 6.40. *Use the notations in Theorem 6.38 and assume $b(G) > C$. So V is identified with the tensor product*

$$\bigotimes_{i=1}^{s} U(k_i, q) \otimes W_0 \otimes \bigotimes_{j=1}^{t} W_j$$

over $\mathbb{F}_q$ by Theorem 6.38. We say a vector $x \in V - \{0\}$ is a primary *if it has can be written as $x = u_1 \otimes \cdots \otimes u_s \otimes w_0 \otimes w_1 \otimes \cdots \otimes w_t$ such that the following conditions are satisfied:*

(1) $u_i \in U(k_i, q)$ for $i \in [s]$, $w_0 \in W_0$, and $w_j \in W_j'$ for $j \in [t]$, where $W_j' \subseteq W_j$ is the $\mathbb{F}_{q_j}$-subspace spanned by the $\mathbb{F}_q$-basis B_j (see Definition 6.38 (3)).

(2) For $i \in [s]$, $u_i \in U(k_i, q)$ lifts to an element in $M(k_i, q) \leq \mathbb{F}_{q_i}^{k_i}$ that has exactly two nonzero coordinates.

We say $u_1, \ldots, u_s$ and $w_0, w_1, \ldots, w_t$ are the factors *of the above tensor product. For two primary vectors $x, y \in V - \{0\}$, write $x \sim y$ if x and y can be written as tensor products of vectors satisfying (1) and (2) above, and their factors differ at no more than one position.*

Remark. In (1) of Definition 6.40, it is equivalent to assume for $j \in [t]$ that w_j is in the set $\mathbb{F}_q^{\times}W_j' := \{\lambda w : \lambda \in \mathbb{F}_q^{\times}, w \in W_j'\}$ instead of W_j', since we may replace w_j with $\lambda^{-1}w_j \in W_j'$ and w_0 with λw_0 by multilinearity.

Lemma 6.41. *Assume $b(G) > C$. Then G^* sends primary vectors to primary vectors.*

Proof. Consider $g = \bigotimes_{i=1}^{s} g_i \otimes h_0 \otimes \bigotimes_{j=1}^{t} h_j \in G^*$. For $i \in [s]$, $g_i \in \mathrm{Sym}(k_i)$ clearly preserves the conditions in Definition 6.40 about u_i. For $j \in [t]$, we know $h_j \in \mathbb{F}_q^{\times}\mathrm{GL}_{d_j}(q_j)$ by Lemma 6.39. Then h_j preserves the set $\mathbb{F}_q^{\times}W_j'$. The lemma follows. □

[8] Here $\mathrm{Sym}(k_i)$ is regarded as a subgroup of $\mathrm{GL}(U(k_i, q))$ via the natural linear representation $\mathrm{Sym}(k_i) \hookrightarrow \mathrm{GL}(U(k_i, q))$.

Note that in Definition 6.40, $M(k_i, q)$ is spanned by vectors with exactly two nonzero coordinates over $\mathbb{F}_p$, and W_j is spanned by vectors in W_j' over $\mathbb{F}_q$ and hence spanned by vectors in $\mathbb{F}_q^\times W_j'$ over $\mathbb{F}_p$. So any vector in V can be written as a finite sum of primary vectors. Also note that for any two primary vectors $x, y \in V - \{0\}$, there exists a finite sequence of primary vectors $x_0, \ldots, x_k \in V - \{0\}$ such that $x_0 = x$, $x_k = y$, and $x_{i-1} \sim x_i$ for all $i \in [k]$. This sequence can be constructed by substituting the factors in a tensor product expression for x with those for y one by one.

We now prove the following lemma, which states that Lemma 5.3 holds for any subgroup of a primitive linear group on a vector space over $\mathbb{F}_p$.

Lemma 6.42. *Let G be a primitive linear group on a finite-dimensional vector space V over $\mathbb{F}_p$, and let H be a subgroup of G on V. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = (|V|N_{c_1}(G))^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in V$.*

Proof. Use the notations in Theorem 6.38. Choose $\alpha \in \mathbb{F}_q$ that is not in any proper subfield of $\mathbb{F}_q$. First assume $b(G^*) \le C$. Let $B \subseteq V$ be a base of G^* of cardinality at most C. Pick a nonzero element $z \in B$. Then $B \cup \{\alpha z\}$ is a base of G since $G_{z,\alpha z} \le G \cap \mathrm{GL}(V(q)) = G^*$. So $d(H) \le b(H) \le b(G) \le C + 1$. As c_0 is large enough, we may assume $C + 1 \le c_0$, so that $\mathcal{P}_{H,d(H)} \subseteq \mathcal{P}$. Then the lemma holds by the definition of $d(H)$.

So assume $b(G^*) > C$. Then $V(q) = \bigotimes_{i=1}^s U(k_i, q) \otimes W_0 \otimes \bigotimes_{j=1}^t W_j$ and $G^* \le \bigotimes_{i=1}^s \mathrm{Sym}(k_i) \otimes D_0 \otimes \bigotimes_{j=1}^t D_j$ as in Theorem 6.38. Let $\mathcal{C}$ be a strongly antisymmetric $\mathcal{P}$-scheme, and let $x \in V$. We want to prove that $\mathcal{C}$ is discrete on H_x. By Lemma 3.2, it suffices to prove that $\mathcal{C}$ is discrete on $H_{x,\alpha x}$.

Consider the diagonal action of H on $V \times V$, and let O be the H-orbit of $(x, \alpha x)$. The elements in O are of the form $(y, \beta y)$, where $y \in V$ and $\beta \in \mathbb{F}_q^\times$ is a conjugate of α, i.e., $\beta = {}^g\alpha$ for some $g \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. As we have noted, for all distinct $y, z \in V$, the difference $z - y$ can be written as a finite sum of primary vectors. By Corollary 6.4, it suffices to prove, for all distinct $y, z \in V$ whose difference $z - y$ is primary, and all conjugates $\beta, \gamma \in \mathbb{F}_q^\times$ of α, that $\mathcal{C}|_{H_{y,\beta y}}$ is discrete on $H_{y,\beta y,z,\gamma z}$. Fix such y, z, β, γ.

Let $H^* = H \cap \mathrm{GL}(V(q))$. Then $H_{y,\beta y} = H_y^*$ and $H_{y,\beta y,z,\gamma z} = H_{y,z}^* = H_{y,z-y}^*$. So we want to prove that $\mathcal{C}|_{H_y^*}$ is discrete on $H_{y,z-y}^*$. By Lemma 6.41, every element in the H_y^*-orbit of $z - y$ is primary. As we have noted, for any primary $u, v \in V - \{0\}$, there exists a finite sequence of primary vectors $x_1, \ldots, x_k \in V - \{0\}$ such that $x_1 = u$, $x_k = v$, and $x_{i-1} \sim x_i$ for all $i \in [k]$. Again by Corollary 6.4, it suffices to prove, for all primary $u, v \in V - \{0\}$ satisfying $u \sim v$, that $\mathcal{C}|_{H_{y,u}^*}$ is discrete on $H_{y,u,v}^*$ (note $H_{y,u}^* = H_{y,\beta y,u}$ and $H_{y,u,v}^* = H_{y,\beta y,u,v}$ are in $\mathcal{P}$). Fix such u, v. It suffices to prove that $(\mathcal{P}|_{H_{y,u}^*}, H_{y,u}^*, H_{y,u,v}^*)$ is a factoring system.

Suppose $u = u_1 \otimes \cdots \otimes u_s \otimes w_0 \otimes \cdots \otimes w_t$ where $u_i \in U(k_i, q)$ for $i \in [s]$ and $w_j \in W_j$ for $0 \le j \le t$ satisfy the conditions in Definition 6.40. First consider the case that v has the form

$$v = u_1 \otimes \cdots \otimes u_{r-1} \otimes u_r' \otimes u_{r+1} \otimes \cdots \otimes u_s \otimes w_0 \otimes \cdots \otimes w_t,$$

where $r \in [s]$ and $u_r' \in U(k_r, q)$ lifts to a vector in $M(k_r, q)$ with exactly two nonzero coordinates a and $-a$. Let $n = |H_{y,u}^* v|$. As u and v differ only at the r-th factor, it is easy to see that any element $v' \in H_{y,u}^* v$ can be obtained from v by replacing the factor u_r' by another factor in $U(k_r, q)$ which lifts to a vector in $M(k_r, q)$ with exactly two nonzero coordinates a and $-a$. It follows that $n \le k_r^2$. Also note $|V| \ge |U(k_r, q)| \ge q^{k_r - 2}$. Then $n = O(\log^2 |V|)$ and

$$n^{d_{\mathrm{Sym}}(n)} = n^{O(\log n)} = |V|^{O(1)} \le N = (|V|N_{c_1}(G))^{c_2}$$

as c_2 is a large enough constant. Therefore by definition, $\mathcal{P}|_{H_{y,u}^*}$ contains the system of stabilizers of depth $d_{\mathrm{Sym}}(n)$ with respect to the action of $H_{y,u}^*$ on $H_{y,u}^* v$. So $\mathcal{C}|_{H_{y,u}^*}$ is discrete on $H_{y,u,v}^*$, as desired.

Next, consider the case that v has the form

$$v = u_1 \otimes \cdots \otimes u_s \otimes w_0 \otimes \cdots \otimes w_{r-1} \otimes w_r' \otimes w_{r+1} \otimes \cdots \otimes w_t$$

where $0 \le r \le t$ and the factors of the tensor product satisfy the conditions in Definition 6.40. Let $u' = u_1 \otimes \cdots \otimes u_s \otimes w_0 \otimes \cdots \otimes w_{r-1} \otimes w_{r+1} \otimes \cdots \otimes w_t$, i.e., u' is obtained from u by omitting the factor u_r. Let $\widetilde{H}$ be the group of $g \in \prod_{i=1}^s \mathrm{Sym}(k_i) \times \mathrm{GL}(W_0) \times \prod_{j=1}^t \mathrm{GL}(W_j)$ such that

(1) g fixes u' (with respect to the natural action where the direct factor D_r acts trivially), and (2) the image of g in $\bigotimes_{i=1}^{s} \mathrm{Sym}(k_i) \otimes \mathrm{GL}(W_0) \otimes \bigotimes_{j=1}^{t} \mathrm{GL}(W_j)$ is in $H^*_{y,u}$. Then we have a natural map $\widetilde{H} \to H^*_{y,u}$. We claim this map is surjective. To see this, consider any $\bar{g} \in H^*_{y,u}$. Lift $\bar{g}$ to $g \in \prod_{i=1}^{s} \mathrm{Sym}(k_i) \times \mathrm{GL}(W_0) \times \prod_{j=1}^{t} \mathrm{GL}(W_j)$. Then g sends u' to $\lambda u'$ for some $\lambda \in \mathbb{F}_q^\times$. By multiplying the coordinate of g in $\mathrm{GL}(W_r)$ by λ and some other coordinate by λ^{-1}, we may assume g fixes u'. Then $g \in \widetilde{H}$. This proves the claim that the map $\widetilde{H} \to H^*_{y,u}$ is surjective.

For $w \in W_r$, define

$$a_w := u_1 \otimes \cdots \otimes u_s \otimes w_0 \otimes \cdots \otimes w_{r-1} \otimes w \otimes w_{r+1} \otimes \cdots \otimes w_t \in V.$$

In particular, $u = a_{w_r}$ and $v = a_{w'_r}$. Let $T = \{a_w : w \in W_r\}$. Then both $\widetilde{H}$ and $H^*_{y,u}$ act on T, and the action of $\widetilde{H}$ on T factors through that of $H^*_{y,u}$.

On the other hand, we have the natural projection $\pi : \widetilde{H} \to \mathrm{GL}(W_r)$. Let $\bar{H} := \pi(\widetilde{H}) \leq \mathrm{GL}(W_r)$ and $P := \ker(\pi)$. As $\widetilde{H}$ fixes u', it is easy to see that $P \leq \widetilde{H}$ acts trivially on T. So the action of $\widetilde{H}$ on T induces an action of $\widetilde{H}/P$ on T, and this action is permutation isomorphic to the action of $\bar{H}$ on W_r under $gP \mapsto \pi(g)$ (with respect to the bijection $a_w \mapsto w$ between T and W_r).

Assume $r = 0$. By the above discussion and Corollary 3.12, we have $d((H^*_{y,u})^T) = d(\bar{H}^{W_0})$, where the superscripts denote the underlying sets on which the groups act. Note $\bar{H} \leq \mathbb{F}_q^\times D_0$. So

$$d(\bar{H}^{W_0}) \leq b(\bar{H}^{W_0}) \leq b((\mathbb{F}_q^\times D_0)^{W_0}) \leq b(D_0^{W_0}) + 1 \leq C + 1$$

where the third inequality holds by [LS02, Lemma 3.1]. Let $\mathcal{P}'$ be the system of stabilizers of depth $d((H^*_{y,u})^T) \leq C + 1$ over $H^*_{y,u}$ with respect to the action of $H^*_{y,u}$ on T. Then $\mathcal{P}' \subseteq \mathcal{P}$ since c_0 is a large enough constant. So $(\mathcal{P}|_{H^*_{y,u}}, H^*_{y,u}, H^*_{y,u,v})$ is a factoring system, as desired.

Now assume $r > 0$. Let $T_1 \subseteq T$ be the $H^*_{y,u}$-orbit of v, and let $T_2 \subseteq W_r$ be the $\bar{H}$-orbit of w'_r. By the above discussion and Corollary 3.12, we have $d((H^*_{y,u})^{T_1}) = d(\bar{H}^{T_2})$.

We know $\bar{H} = \pi(\widetilde{H}) \leq \mathrm{GL}(W_r)$. We claim that actually $\bar{H} \leq \mathrm{GL}(W'_r)$. To see this, note $w_r \in W'_j$ by Condition (1) in Definition 6.40. As $\widetilde{H}$ fixes both u' and u, it also fixes w_r. So $\bar{H} = \pi(\widetilde{H})$ fixes w_r. By Lemma 6.39, we have $D_r \leq \mathbb{F}_q^\times \mathrm{GL}(W'_r)$ and hence

$$\bar{H} \leq (\mathbb{F}_q^\times \mathrm{GL}(W'_r))_{w_r} \leq \mathrm{GL}(W'_r)_{w_r} \leq \mathrm{GL}(W'_r)$$

as claimed. So $d(\bar{H}^{T_2}) \leq d_{\mathrm{Lin}}(d_r, q_r)$.

Let $k := d((H^*_{y,u})^{T_1})$. Then $k = d(\bar{H}^{T_2}) \leq d_{\mathrm{Lin}}(d_r, q_r)$. As $w'_r \in W'_j$, we have $T_2 = \bar{H} w'_r \subseteq W'_j$ and hence

$$|H^*_{y,u} v| = |T_1| = |T_2| \leq |W'_j| = q_r^{d_r}.$$

By Theorem 6.38 (4), the set $\mathcal{C}(G)$ contains a finite simple classical group $\mathrm{Cl}_{d_r}(q_r)$. So $N_{c_1}(G) \geq q_r^{d_r d_{\mathrm{Lin}}(c_1 d_r, q_r)}$. As $N = (|V| N_{c_1}(G))^{c_2}$, where $c_1, c_2 \in \mathbb{N}^+$, we have

$$|H^*_{y,u,v} v|^k \leq q_r^{d_r d_{\mathrm{Lin}}(d_r, q_r)} \leq q_r^{d_r d_{\mathrm{Lin}}(c_1 d_r, q_r)} \leq N_{c_1}(G) \leq N,$$

Let $\mathcal{P}'$ be the system of stabilizers of depth k over $H^*_{y,u}$ with respect to the action of $H^*_{y,u}$ on $H^*_{y,u} v$. As $|H^*_{y,u,v} v|^k \leq N$, we have $\mathcal{P}' \leq \mathcal{P}_{H,c_0,N} = \mathcal{P}$. So $(\mathcal{P}|_{H^*_{y,u}}, H^*_{y,u}, H^*_{y,u,v})$ is a factoring system, as desired. □

Irreducible linear groups. For a group $G \leq \mathrm{GL}(V)$ and a subspace $W \subseteq V$, the stabilizer $G_W = \{g \in G : {}^g W = W\}$ acts on W, which gives a linear representation $\pi_W : G_W \to \mathrm{GL}(W)$. Write $G_W|_W$ for the image $\pi_W(G_W) \leq \mathrm{GL}(W)$.

We need the following lemma, whose proof can be found in, e.g., [Sup76, IV.15].

Lemma 6.43. *Let G be an irreducible linear group on a finite-dimensional vector space $V \neq \{0\}$ over $\mathbb{F}_p$. Then there exists a nonzero subspace $W \subseteq V$ such that $G_W|_W$ is a primitive linear group on W over $\mathbb{F}_p$, V equals the direct sum $\bigoplus_{W' \in S_W} W'$ where $S_W := \{{}^g W : g \in G\}$, and G permutes the subspaces in S_W.*

Now we extend Lemma 6.42 to irreducible linear groups over $\mathbb{F}_p$.

Lemma 6.44. *Let G be an irreducible linear group on a finite-dimensional vector space V over $\mathbb{F}_p$, and let H be a subgroup of G on V. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = (|V|N_{c_1}(G))^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in V$.*

Proof. Assume $V \neq \{0\}$ as otherwise the claim is trivial. Choose a nonzero subspace $W \subseteq V$ as in Lemma 6.43. Then $G_W|_W$ is a primitive linear group on W, and G permutes the subspaces in S_W. Note $|S_W| = \log|V|/\log|W|$.

Suppose $\mathcal{C} = \{C_K : K \in \mathcal{P}\}$ is a strongly antisymmetric $\mathcal{P}$-scheme. We want to show that all strongly antisymmetric $\mathcal{P}$-schemes are discrete on H_x for all $x \in V$. As $V = \bigoplus_{W' \in S_W} W'$, for any $x, y \in V$, we may choose a sequence of elements $z_0, \ldots, z_t \in S$ such that $z_0 = x$, $z_t = y$, and for all $i \in [t]$, the vector $z_i - z_{i-1}$ is in ${}^gW$ for some $g \in G$. By Corollary 6.4, it suffices to prove, for all $x, y \in V$ and $g \in G$ satisfying $x - y \in {}^gW$, that $\mathcal{C}|_{H_x}$ is discrete on $H_{x,y}$. Fix such $x, y \in V$ and $g \in G$.

Let $z = y - x$. Then $H_{x,y} = H_{x,z}$. Every element in $H_x z$ is in a subspace ${}^{g'}W$ for some $g' \in G$. Consider arbitrary $h, h' \in H_x$ such that $u := {}^h z$ and $v = {}^{h'} z$ are two different elements in the same subspace $W' := {}^{g'}W$ for some $g' \in G$. Note that the condition u and v are different is equivalent to $H_{x,z}h^{-1} \neq H_{x,z}h'^{-1}$. We claim that $H_{x,z}h^{-1}$ and $H_{x,z}h'^{-1}$ are in different blocks of the partition $C_{H_{x,z}}|_{H_x} \in \mathcal{C}|_{H_x}$.

To prove this claim, we first show that $\mathcal{C}|_{H_{x,u}}$ and $\mathcal{C}|_{H_{x,v}}$ are discrete on $H_{x,u,v}$. As $u \in W'$ and $H_{x,u}$ fixes u, we have $H_{x,u} \leq G_{W'}$. Note $G_{W'}|_{W'}$ is a primitive linear group on W' since $G_W|_W$ is a primitive linear group on W. Let $\mathcal{P}' := \mathcal{P}_{H_{x,u},c_0-2,N'}$ with respect to the action of $H_{x,u}$ on W', where $N' = (|W'|N_{c_1'}(G_{W'}|_{W'}))^{c_2'}$ and $c_1', c_2' \in \mathbb{N}^+$ are large enough constants. By Lemma 6.42, Corollary 3.12 and the fact that $G_{W'}|_{W'}$ is a primitive linear group on W', we know $(\mathcal{P}', H_{x,u}, H_{x,u,v})$ is a factoring system. Note $\mathcal{P}_{H_{x,u},c_0-2} \subseteq \mathcal{P}_{H,c_0}$. As $G_{W'}|_{W'}$ is a subquotient of G and c_1, c_2 are large enough constants, we have $N' \leq N$ by Lemma 4.5. It follows that $\mathcal{P}' \subseteq \mathcal{P}|_{H_{x,u}}$. Therefore $\mathcal{C}|_{H_{x,u}}$ is discrete on $H_{x,u,v}$. Similarly, $\mathcal{C}|_{H_{x,v}}$ is also discrete on $H_{x,u,v}$.

By Lemma 6.1, we have a bijection of the form $\pi_{H_{x,u,v},H_{x,v}}|_{B_0} \circ (\pi_{H_{x,u,v},H_{x,u}}|_{B_0})^{-1}$ (where B_0 is a block of $C_{H_{x,u,v}}$) that sends $H_{x,u}e$ to $H_{x,v}e$. By composing this map with $c_{H_{x,z},h}$ and $c_{H_{x,v},h'^{-1}}$, we obtain a bijection between blocks that sends $H_{x,z}h^{-1}$ to $H_{x,z}h'^{-1}$. By strong antisymmetry of $\mathcal{C}$, we know $H_{x,z}h^{-1}$ and $H_{x,z}h'^{-1}$ are in different blocks of $C_{H_{x,z}}$. So they are also in different blocks of $C_{H_{x,z}}|_{H_x}$. This proves the claim.

Recall that we want to prove $\mathcal{C}|_{H_x}$ is discrete on $H_{x,y} = H_{x,z}$. Assume to the contrary that there exists a block $B = \{H_{x,z}g_1^{-1}, \ldots, H_{x,z}g_k^{-1}\} \in C_{H_{x,z}}|_{H_x}$ of cardinality $k > 1$. By the claim just proved, the elements ${}^{g_1}z, \ldots, {}^{g_k}z$ are in distinct subspaces in the set S_W. So $k \leq |S_W| = \log|V|/\log|W|$. Let $n = |H_x z|$. Note $n \leq |S_W| \cdot |W|$. So

$$n^{\log k+1} \leq (|S_W| \cdot |W|)^{\log(\log|V|/\log|W|)+1} = |V|^{O(1)} \leq N.$$

Therefore $\mathcal{P}|_{H_x}$ contains the system of stabilizers of depth $\lfloor \log k \rfloor + 1 > \log k$ with respect to the action of H_x on $H_x z$. But this contradicts Lemma 3.17 (2). So $\mathcal{C}|_{H_x}$ is discrete on $H_{x,y}$, as desired. □

Now we are ready to prove Lemma 5.3 for finite primitive permutation groups of affine type.

Lemma 6.45. *Lemma 5.3 holds for finite primitive permutation groups of affine type.*

Proof. Let G be a finite primitive permutation groups of affine type. By definition, G is a subgroup of $\mathrm{AGL}(V)$ acting transitively on a vector space V over a prime field $\mathbb{F}_p$, and the group of translations $V^\sharp$ is a subgroup of G. The stabilizer G_0 of $0 \in V$ is an irreducible linear group on V by Lemma 6.35. Note $G \cong V^\sharp \rtimes G_0$. So the G and G_0 have the same set of nonabelian composition factors.

Let $\mathcal{P} = \mathcal{P}_{G,c_0,N}$, where $N = (|V|N_{c_1}(G))^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Let $x \in V$. By Corollary 6.5, to prove the lemma, it suffices to prove that $(\mathcal{P}|_{G_0}, G_0, (G_0)_y)$ is a factoring system for all $y \in V$. Let $\mathcal{P}' := \mathcal{P}_{G_0,c_0-1,N}$ with respect to the action of G_0 on V. As $\mathcal{P}_{G_0,c_0-1} \subseteq \mathcal{P}_{G,c_0}$, we have $\mathcal{P}' \subseteq \mathcal{P}|_{G_0}$. By Lemma 6.44, $(\mathcal{P}', G_0, (G_0)_y)$ is a factoring system for all $y \in V$. So $(\mathcal{P}|_{G_0}, G_0, (G_0)_y)$ is a factoring system for all $y \in V$, as desired. □

6.5 Diagonal type

In this subsection, we verify Lemma 5.3 for finite permutation groups G of diagonal type. By Definition 6.9, we may assume G is a permutation group satisfying $M \leq G \leq W$ and acting on $S := D\backslash W$ by inverse right translation, where

$$\begin{aligned} A &= \{(a_1, \ldots, a_k) \in \mathrm{Aut}(T)^k : a_i\mathrm{Inn}(T) = a_j\mathrm{Inn}(T) \text{ for all } i, j \in [k]\}, \\ W &= A \rtimes \mathrm{Sym}(k), \\ M &= \mathrm{Inn}(T)^k \leq A \leq W, \\ D &= \{(a, \ldots, a)\pi : a \in \mathrm{Aut}(T), \pi \in \mathrm{Sym}(k)\} \leq W \end{aligned}$$

for a nonabelian finite simple group T and an integer $k \geq 2$. The cardinality of S is $|W|/|D| = |T|^{k-1}$. Note $W \subseteq DM$. So M and G on transitive on S. We do not need to assume G to be primitive.

Let x_0 denote the element $De \in S$ so that $G_{x_0} = D \cap G$. It is a consequence of CFSG that every finite simple group can be generated by two elements ([AG84, Theorem B]). So we can choose $r, s \in \mathrm{Inn}(T) - \{e\}$ that generate $\mathrm{Inn}(T) \cong T$. For $g \in \mathrm{Inn}(T)$, define $a_g := (g, e, \ldots, e) \in M$. We have the following lemma.

Lemma 6.46. *For $U = \{x_0, {}^{a_r}x_0, {}^{a_s}x_0, {}^{a_{rs}}x_0\}$, it holds that $W_U = \mathrm{Sym}(k)_1$.*

Proof. Note that

$$W_U = D \cap a_r D a_r^{-1} \cap a_s D a_s^{-1} \cap a_{rs} D a_{rs}^{-1}$$

from which it is straightforward to see $\mathrm{Sym}(k)_1 \leq W_U$.

To prove $W_U \leq \mathrm{Sym}(k)_1$, consider $g = (a, \ldots, a)\pi \in W_U$, where $a \in \mathrm{Aut}(T)$ and $\pi \in \mathrm{Sym}(k)$. We have

$$a_r^{-1} g a_r = a_r^{-1}(a, \ldots, a)\pi a_r = a_r^{-1}(a, \ldots, a)\,{}^{\pi}a_r\pi \in D \tag{2}$$

since $a_r^{-1} W_U a_r \leq D$.

First assume $k > 2$. Suppose π sends 1 to $i \in [k]$. Note that all coordinates of a_r (resp. ${}^{\pi}a_r$) are equal to the identity except that the first (resp. i-th) coordinate is $r \neq e$. As $k > 2$ and $a_r^{-1}(a, \ldots, a)\,{}^{\pi}a_r\pi \in D$, we must have $i = 1$ and $r^{-1}ar = a$. So $\pi \in \mathrm{Sym}(k)_1$. The same argument using the fact $a_s^{-1} W_U a_s \leq D$ implies $s^{-1}as = a$. Then a commutes with $\langle r, s\rangle = \mathrm{Inn}(T)$. Note that the isomorphism $T \cong \mathrm{Inn}(T)$ sending $h \in T$ to the inner automorphism $x \mapsto hxh^{-1}$ is an equivalence between the action of $\mathrm{Aut}(T)$ on T and that on $\mathrm{Inn}(T)$ by conjugation. So a fixes T pointwisely, which implies $a = e$. Then we have $g = \pi \in \mathrm{Sym}(k)_1$, as desired.

Next assume $k = 2$. If $\pi = e$, we have $a_r^{-1} g a_r = (r^{-1}ar, a) \in D$ by (2). So $r^{-1}ar = a$, and the same argument using the fact $a_s^{-1} W_U a_s \leq D$ implies $s^{-1}as = a$. Again we conclude that a commutes with $\langle r, s\rangle = \mathrm{Inn}(T)$, which implies $a = e \in \mathrm{Sym}(k)_1$. Now consider the case $\pi \neq e$, i.e., $\pi = (1\ 2) \in \mathrm{Sym}(2)$. Note that the proof for the previous case $\pi = e$ shows $W_U \cap A = \{e\}$. Therefore

$$|W_U| = [W_U : W_U \cap A] \leq [W : A] = |\mathrm{Sym}(k)| = 2.$$

The claim $W_U \leq \mathrm{Sym}(k)_1$ is trivial if $|W_U| = 1$. So assume $|W_U| = 2$. Then $W_U = \{e, g\}$, where $g = (a, a)\pi$ is as above. By (2), we have $(r^{-1}a, ar)\pi \in D$. So $ara^{-1} = r^{-1}$. The same argument using the facts $a_s^{-1} W_U a_s \leq D$ and $a_{rs}^{-1} W_U a_{rs} \leq D$ implies $asa^{-1} = s^{-1}$ and $arsa^{-1} = (rs)^{-1} = s^{-1}r^{-1}$. On the other hand, we have $arsa^{-1} = (ara^{-1})(asa^{-1}) = r^{-1}s^{-1}$. So r commutes with s. Then $T = \langle r, s\rangle$ is abelian, contradicting the assumption that T is a nonabelian finite simple group. □

Now we prove Lemma 5.3 for G of diagonal type. In fact, we prove the statement in the following form that also applies to any subgroup $H \leq G$.

Lemma 6.47. *Let G be a finite permutation group of diagonal type on $S = D\backslash W$ as above, and let H be a subgroup of G on S. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = |S|^{c_1}$ and $c_0, c_1 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$. In particular, Lemma 5.3 holds for finite primitive permutation groups of diagonal type.*

Proof. Define Z to be the set of elements $g \in M = \mathrm{Inn}(T)^k$ such that g has exactly one coordinate different from the identity. Then Z is a generating set of M such that $g^{-1}, hgh^{-1} \in Z$ for $g \in Z$ and $h \in M$. Let g be an arbitrary element in Z. As M is transitive on S, by Corollary 6.5, it suffices to prove that $(\mathcal{P}|_{H_{x_0}}, H_{x_0}, H_{x_0,{}^g x_0})$ is a factoring system. Let $\mathcal{C} = \{C_K : K \in \mathcal{P}\}$ be a strongly antisymmetric $\mathcal{P}$-scheme. We want to prove that $\mathcal{C}|_{H_{x_0}}$ is discrete on $H_{x_0,{}^g x_0}$.

Suppose the i-th coordinate of g is different from the identity. Choose $U = \{x_0, {}^{a_r}x_0, {}^{a_s}x_0, {}^{a_r s}x_0\}$ as in Lemma 6.46, and let $U' := {}^{(1\ i)}U$, where $(1\ i) \in \mathrm{Sym}(k) \leq D$ is the transposition exchanging 1 and k. As $x_0 \in U$ and $(1\ i) \in D$ fixes $x_0 = De$, we have $x_0 \in U'$. By Lemma 6.46, we have

$$H_{U'} = \mathrm{Sym}(k)_i \cap H = \mathrm{Sym}(k)_i \cap H_{x_0}. \tag{3}$$

Note $g \in N_G(\mathrm{Sym}(k)_i)$. Therefore

$$\mathrm{Sym}(k)_i = g\mathrm{Sym}(k)_i g^{-1} \leq gDg^{-1} = gW_{x_0}g^{-1} = W_{{}^g x_0}.$$

So $H_{U'} \leq H_{x_0,{}^g x_0}$. By Lemma 3.2, it suffices to prove that $\mathcal{C}|_{H_{x_0}}$ is discrete on $H_{U'}$. By Corollary 6.4, it suffices to prove that $\mathcal{C}|_{H_{{}^h U'}}$ is discrete on $H_{{}^h U' \cup {}^{h'} U'}$ for all $h, h' \in H_{x_0}$.

Fix $h, h' \in H_{x_0}$. Write $h = b\pi$ and $h' = b'\pi'$ where $b, b' \in A$ and $\pi, \pi' \in \mathrm{Sym}(k)$. As $h \in H_{x_0} \leq D$, the k coordinates of b are equal. So b commutes with $\mathrm{Sym}(k)$. By (3), we have

$$H_{{}^h U'} = h(\mathrm{Sym}(k)_i \cap H_{x_0})h^{-1} = \mathrm{Sym}(k)_{\pi i} \cap H_{x_0}.$$

Similarly, we have $H_{{}^{h'} U'} = \mathrm{Sym}(k)_{\pi' i} \cap H_{x_0}$ and $H_{{}^h U' \cup {}^{h'} U'} = \mathrm{Sym}(k)_{\pi i, \pi' i} \cap H_{x_0}$.

Let $n := [H_{{}^h U'} : H_{{}^h U' \cup {}^{h'} U'}]$. Then

$$n = [H_{{}^h U'} : H_{{}^h U' \cup {}^{h'} U'}] \leq [\mathrm{Sym}(k)_{\pi i} : \mathrm{Sym}(k)_{\pi i, \pi' i}] \leq k.$$

Also note $k = (\log |S| / \log |T|) + 1 = O(\log |S|)$. So $n^{d_{\mathrm{Sym}}(n)} = k^{O(\log k)} = |S|^{O(1)} \leq N$. By definition, $\mathcal{P}|_{H_{{}^h U'}}$ contains as a subset the system of stabilizers of depth $d_{\mathrm{Sym}}(n)$ with respect to the action of $H_{{}^h U'}$ on $H_{{}^h U' \cup {}^{h'} U'} \backslash H_{{}^h U'}$ by inverse right translation. This implies that $\mathcal{C}|_{H_{{}^h U'}}$ is discrete on $H_{{}^h U' \cup {}^{h'} U'}$, as desired. □

6.6 Product type and twisted wreath type

In this subsection, we verify Lemma 5.3 for finite primitive permutation groups of product type and those of twisted wreath type.

Product type. Suppose G is a finite permutation group of product type. By Definition 6.10, there exist an integer $k \geq 2$ and a permutation group K of almost simple type or diagonal type on a finite set Γ such that G is a subgroup of $W := K \wr \mathrm{Sym}(k) = K^k \rtimes \mathrm{Sym}(k)$ acting on $S := \Gamma^k$, and $M := \mathrm{soc}(K)^k \leq W$ is a subgroup of G.

Lemma 6.48. *Let G be a finite permutation group of product type on S of cardinality $n = |\Gamma|^k$ as above, and let H be a subgroup of G on S. Let $\mathcal{P} = \mathcal{P}_{H,c_0,N}$, where $N = (nN_{c_1}(G))^{c_2}$ and $c_0, c_1, c_2 \in \mathbb{N}^+$ are large enough absolute constants. Then $(\mathcal{P}, H, H_x)$ is a factoring system for all $x \in S$. In particular, Lemma 5.3 holds for finite primitive permutation groups of product type.*

Proof. Suppose $\mathcal{C} = \{C_{H'} : H' \in \mathcal{P}\}$ is a strongly antisymmetric $\mathcal{P}$-scheme. Let $x \in S$. We want to prove that $\mathcal{C}$ is discrete on H_x. Note that for any $y, z \in S$, we may choose a sequence of elements $y_0, \ldots, y_t \in S$ such that $y_0 = y$, $y_t = z$, and for all $i \in [t]$, the elements $y_{i-1}, y_i \in S = \Gamma^k$ differ at exactly one coordinate. By Corollary 6.4, it suffices to prove, for all $y, z \in S$ differing at exactly one coordinate, $\mathcal{C}|_{H_y}$ is discrete on $H_{y,z}$. Fix such $y, z \in S$. Then every element in $H_y z$ differs from y at exactly one coordinate. In particular, we have $|H_y z| \leq k|\Gamma|$.

Consider arbitrary $g, g' \in H_y$ such that $u := {}^{g}z$ and $v := {}^{g'}z$ are different, and they differ from y at the same coordinate (say the i-th coordinate). Note that the condition u and v are different is equivalent to $H_{y,z}g^{-1} \neq H_{y,z}g'^{-1}$.

We claim that $H_{y,z}g^{-1}$ and $H_{y,z}g'^{-1}$ are in different blocks of $C_{H_{y,z}}|_{H_y} \in \mathcal{P}|_{H_y}$. To prove the claim, we first show that $\mathcal{C}|_{H_{y,u}}$ and $\mathcal{C}|_{H_{y,v}}$ are discrete on $H_{y,u,v}$. As $H_{y,u}$ fixes y and u which differ only at the i-th coordinate, the image of $H_{y,u}$ under the quotient map $K^k \rtimes \mathrm{Sym}(k) \to \mathrm{Sym}(k)$ fixes $i \in [k]$. Let $\phi : H_{y,u} \to K$ be the map sending $(g_1, \ldots, g_k)\pi$ to g_i. Then ϕ is a group homomorphism with the kernel

$$P := \{(g_1, \ldots, g_k)\pi \in H_{y,u} : g_i = e\}.$$

Let $\bar{H} := \phi(H_{y,u}) \leq K$. Suppose $u = (u_1, \ldots, u_k) \in S = \Gamma^k$. For $t \in \Gamma$, define

$$v_t := (u_1, \ldots, u_{i-1}, t, u_{i+1}, \ldots, u_k) \in S.$$

Let $T = \{v_t : t \in \Gamma\} \subseteq S$. Then $H_{y,u}$ acts on T and its normal subgroup P acts trivially on T. So $H_{y,u}/P$ acts on T. It is straightforward to see that $H_{y,u}/P$ acting on T is permutation isomorphic to $\bar{H}$ acting on Γ under the map $((g_1, \ldots, g_k)\pi)P \mapsto g_i$, with respect to the bijection $v_t \mapsto t$ between T and Γ.

Let $\mathcal{P}_1 = \mathcal{P}_{\bar{H},c_0',N'}$ with respect to the action of $\bar{H}$ on Γ, where c_0', c_1', c_2' are large enough constants, $N' := (|\Gamma| N_{c_1'}(\mathrm{soc}(K)))^{c_2'}$ if K is of almost simple type, and $N' := |\Gamma|^{c_2'}$ if K is of diagonal type. In the case that K is of almost simple type, we know K and $\mathrm{soc}(K)$ have the same set of nonabelian composition factors by the (now verified) *Schreier Conjecture* [DM96, Section 4.7], and hence $N' = (|\Gamma| N_{c_1'}(K))^{c_2'}$. By Lemma 6.33 and Lemma 6.47, $(\mathcal{P}_1, \bar{H}, \bar{H}_t)$ is a factoring system for all $t \in \Gamma$. Let $\mathcal{P}_2 = \mathcal{P}_{H_{y,u},c_0',N'}$ with respect to the action $H_{y,u}$ on T. By Lemma 3.12 and the fact that $H_{y,u}/P$ and $\bar{H}$ are permutation isomorphic, $(\mathcal{P}_2, H_{y,u}, H_{y,u,t})$ is a factoring system for all $t \in T$. In particular, $(\mathcal{P}_2, H_{y,u}, H_{y,u,v})$ is a factoring system. Also note $N' \leq (nN_{c_1}(G))^{c_2} = N$ and hence $\mathcal{P}_2 \subseteq \mathcal{P}|_{H_{y,u}}$ by Lemma 4.5 and the assumption that c_0, c_1, c_2 are large enough constants. So $(\mathcal{P}|_{H_{y,u}}, H_{y,u}, H_{y,u,v})$ is a factoring system. In particular, $\mathcal{C}|_{H_{y,u}}$ is discrete on $H_{y,u,v}$. Similarly, $\mathcal{C}|_{H_{y,v}}$ is also discrete on $H_{y,u,v}$.

By Lemma 6.1, we have a bijection of the form $\pi_{H_{y,u,v},H_{y,v}}|_{B_0} \circ (\pi_{H_{y,u,v},H_{y,u}}|_{B_0})^{-1}$ (where B_0 is a block of $C_{H_{y,u,v}}$) that sends $H_{y,u}e$ to $H_{y,v}e$. By composing this map with $c_{H_{y,z},g}$ and $c_{H_{y,v},g'^{-1}}$, we obtain a bijection between blocks that sends $H_{y,z}g^{-1}$ to $H_{y,z}g'^{-1}$. By strong antisymmetry of $\mathcal{C}$, we know $H_{y,z}g^{-1}$ and $H_{y,z}g'^{-1}$ are in different blocks of $C_{H_{y,z}}$. So they are also in different blocks of $C_{H_{y,z}}|_{H_y}$. This proves the claim.

Recall that we want to prove $\mathcal{C}|_{H_y}$ is discrete on $H_{y,z}$. Assume to the contrary that there exists a block $B = \{H_{y,z}g_1^{-1}, \ldots, H_{y,z}g_r^{-1}\} \in C_{H_{y,z}}|_{H_y}$ of cardinality $r > 1$. By the claim just proved, the elements ${}^{g_1}z, \ldots, {}^{g_r}z$ differ from y at distinct coordinates. So $r \leq k = \log n / \log |\Gamma|$. Let $n' = |H_y z|$. Note $n' \leq k|\Gamma|$. So

$$n'^{\log r + 1} \leq (k|\Gamma|)^{\log(\log n / \log |\Gamma|) + 1} = n^{O(1)} \leq N.$$

Therefore $\mathcal{P}|_{H_y}$ contains the system of stabilizers of depth $\lfloor \log r \rfloor + 1 > \log r$ with respect to the action of H_y on $H_y z$. But this contradicts Lemma 3.17 (2). So $\mathcal{C}|_{H_y}$ is discrete on $H_{y,z}$, as desired. □

Twisted wreath type. Suppose G is a finite primitive permutation group of twisted wreath type. By Definition 6.11, we may assume $G = B \rtimes P$ acting on $S := G/P$ by left translation, where

- T is a noncyclic finite simple group,
- $P \leq \mathrm{Sym}(k)$ is a transitive permutation group on $[k]$ for some integer $k \geq 2$,
- φ is a group homomorphism from P_1 to $\mathrm{Aut}(T)$,
- B is the group $\{f \in \mathrm{Map}(P, T) : f(pq^{-1}) = {}^{\varphi(q)}(f(p)) \text{ for all } p \in P, q \in P_1\}$ under coordinate-wise multiplication, and
- P acts on B via $({}^{p}f)(x) = f(p^{-1}x)$ for $p, x \in P$, $f \in B$.

As $\mathrm{Aut}(T)$ acts naturally on T, we may form the semidirect product $\mathrm{Hol}(T) := T \rtimes \mathrm{Aut}(T)$, called the *holomorph* of T. It is a permutation group on the set T with the action ${}^{hg}h' = h\,{}^{g}h'$ for $h, h' \in T$ and $g \in \mathrm{Aut}(T)$. It turns out that G can be embedded in the permutation group $\mathrm{Hol}(T) \wr P$ of product type. This was observed in [Pra90, Section 3.6].

Lemma 6.49. *Let G be a finite primitive permutation group of twisted wreath type on $S = G/P$ as above. Then G is permutation isomorphic to a subgroup of the permutation group $\mathrm{Hol}(T) \wr P$ of product type on T^k.*

For the proof of Lemma 6.49, see Appendix B. The groups $G = T \operatorname{twr}_\varphi P$ and $\mathrm{Hol}(T) \wr P$ in Lemma 6.49 have the same set of nonabelian composition factors by the (now verified) *Schreier Conjecture* [DM96, Section 4.7]. Then by Lemma 6.48 and Lemma 6.49, we have

Lemma 6.50. *Lemma 5.3 holds for finite primitive permutation groups of twisted wreath type.*

Finishing the proof of Lemma 5.3. Lemma 5.3 now follows from the O'Nan-Scott theorem together with Lemmas 6.33, 6.45, 6.47, 6.48, and 6.50.

7 Open Problems

We believe improving the $O(\log m)$ upper bound for the function $d_{\mathrm{Sym}}(m)$ is the most important open problem here, as it would give a faster GRH-based deterministic factoring algorithm for the general case. The *Schemes Conjecture*, introduced in [IKS09], is equivalent to $d_{\mathrm{Sym}}(m) = O(1)$.

One may also try to prove better bounds for the function $d_{\mathrm{Lin}}(m, q)$, which may help us understand how the set of finite simple classical groups $\mathcal{C}(G)$ contributes to the time complexity of our factoring algorithm. However, while improving upper bounds for $d_{\mathrm{Lin}}(m, q)$ seems more achievable, it can be shown that if such an improvement is significant enough, it would also lead to an improvement over the $O(\log m)$ bound for $d_{\mathrm{Sym}}(m)$. In particular, Lemma 3.18 (5) shows that $d_{\mathrm{Lin}}(m, q) = O(1)$ is equivalent to $d_{\mathrm{Sym}}(m) = O(1)$, and hence is equivalent to the Schemes Conjecture.

On the other hand, perhaps it is possible to improve the dependence of the running time of our algorithm on $\mathcal{C}(G)$ without proving better bounds for $d_{\mathrm{Lin}}(m, q)$. One first step in this direction is answering the following question.

Question. *Does there exist a function $f(m) = o(m)$ such that $d(\mathrm{GL}_m(q)) \leq f(m)$ holds for all $m \in \mathbb{N}^+$ and prime powers q, where $d(\cdot)$ is as in Definition 3.14 and $\mathrm{GL}_m(q)$ acts naturally on $S = \mathbb{F}_q^m$?*

The trivial upper bound is $d(\mathrm{GL}_m(q)) \leq m$ (Lemma 3.18 (4)). A sublinear bound $d(\mathrm{GL}_m(q)) = o(m)$ was recently proved in [Guo19], but only for small q.[9]

Acknowledgments. The author would like to thank Chris Umans, Nitin Saxena, Manuel Arora, and Anand Kumar Narayanan for helpful discussions. The author is also grateful to Noga Ron-Zewi for carefully reading the introduction of this paper and giving useful comments.

Appendix A Finite classical groups

This section contains preliminaries and notations on *finite classical groups*. Standard references include [Asc00, KL90].

Spaces with forms. Throughout this section, let V be finite dimensional vector space over a finite field $\mathbb{F}_q$ of characteristic $p > 0$. Let $F : V \times V \to \mathbb{F}_q$ be a function such that $F(x+y, z) = F(x, z)+F(y, z)$, $F(x, y + z) = F(x, y) + F(x, z)$, and $F(cx, y) = cF(x, y)$ for $x, y, z \in V$ and $c \in \mathbb{F}_q$.

Definition A.1. *We say F is*

- *a* symmetric form *if $F(x, y) = F(y, x)$ for $x, y \in V$,*
- *a* skew-symmetric form *if $F(x, y) = -F(y, x)$ for $x, y \in V$, and*
- *a* Hermitian form *if $\mathbb{F}_q$ is a quadratic extension of a finite field $\mathbb{F}_{q'}$ and $F(x, y) = {}^{\alpha}(F(y, x))$ for $x, y \in V$, where $\alpha : x \mapsto x^{q^{1/2}}$ is the nontrivial involution in $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_{q'})$.*

[9] In fact, it was shown in [Guo19] that $d_{\mathrm{Lin}}(m, q) = o(m)$ when q is small enough.

Note that if F is symmetric or skew-symmetric, we have $F(x, cy) = cF(x, y)$ and hence F is bilinear. On the other hand, if F is Hermitian, we have $F(x, cy) = {}^{\alpha}c \cdot F(x, y)$.

In the rest of this section, assume F is a symmetric, skew-symmetric or Hermitian form on V.

For $x, y \in V$, if $F(x, y) = 0$, we say x and y are *orthogonal* and write $x \perp y$. For a subspace U of V, define $U^{\perp} := \{y \in V : y \perp x \text{ for all } x \in U\}$, called the *orthogonal complement* of U. If V is a direct sum $U \oplus W$ and $u \perp w$ holds for all $u \in U$ and $w \in W$, we say V is the *orthogonal direct sum* of U and W and write $V = U \perp W$. In particular, if $V = U \oplus U^{\perp}$, then $V = U \perp U^{\perp}$.

For a subspace $W \subseteq V$, define

$$\mathrm{Rad}(W) := W \cap W^{\perp} = \{y \in W : y \perp x \text{ for all } x \in W\}.$$

called the *radical* of W. We say W is *non-degenerate* if $\mathrm{Rad}(W) = \{0\}$. We say F itself is non-degenerate if V is non-degenerate, i.e., $\mathrm{Rad}(V) = \{0\}$. We say $x \in V$ is *isotropic* if $x \perp x$. A subspace U of V is *totally isotropic* if $U \subseteq U^{\perp}$.

Lemma A.2 ([Asc00, (19.2) and (19.3)])**.** *Let F be non-degenerate and let U be a subspace of V. We have*

(1) $\dim U^{\perp} = \operatorname{codim} U$.

(2) U is non-degenerate iff $V = U \oplus U^{\perp}$.

(3) $(U^{\perp})^{\perp} = U$.

(4) If U is totally isotropic, then $\dim U \leq \frac{1}{2} \dim V$ and every complement of U in $U^{\perp}$ is non-degenerate.

Symplectic, orthogonal, and unitary spaces. Given a function $Q : V \to \mathbb{F}_q$, define $F_Q : V \times V \to \mathbb{F}_q$ by

$$F_Q(x, y) := Q(x + y) - Q(x) - Q(y).$$

We say Q is a *quadratic form* if F_Q is bilinear and $Q(cx) = c^2 Q(x)$ for all $x \in V$ and $c \in \mathbb{F}_q$, and in this case we call F_Q the *associated bilinear form*. Note that the associated bilinear form F_Q is also a symmetric form, and if $p = 2$, then $F_Q(x, x) = 0$ for all $x \in V$. We say a quadratic form Q is *non-degenerate* if F_Q is non-degenerate.

Note that when $p \neq 2$, a quadratic form Q is uniquely determined by the associated bilinear form F_Q via $Q(x) = \frac{1}{2} F_Q(x, x)$. However, when $p = 2$, there may be many quadratic forms associated with the same bilinear form.

Definition A.3. *A* symplectic space *is a pair (V, F) where F is a non-degenerate skew-symmetric form on V, and when $p = 2$, $F(x, x) = 0$ for all $x \in V$.*[10] *A* unitary space *is a pair (V, F) where F is a non-degenerate unitary form on V. An* orthogonal space *is a pair (V, Q) where Q is a non-degenerate quadratic form on V. When F or Q is clear from the context, we simply say V is a symplectic, orthogonal, or unitary space.*

For a symplectic or unitary space (V, F), the relation $\perp$ above is defined using the form F. For an orthogonal space (V, Q), it is defined using the associated bilinear form F_Q.

Let (V, Q) be an orthogonal space. We say $x \in V$ is *singular* if $Q(x) = 0$. Note that if x is singular, then it is also isotropic (under the associated bilinear form F_Q). The converse holds when $p \neq 2$ since $Q(x) = \frac{1}{2} F_Q(x, x)$. However, when $p = 2$, there may exist $x \in V$ that is isotropic but not singular. A subspace U of V is *totally singular* if $Q|_U = 0$, i.e., $Q(x) = 0$ for all $x \in U$.

Let (V, F) be a symplectic space or a unitary space. We say $x \in V$ is *singular* if it is isotropic, and we say a subspace $U \subseteq V$ is *totally singular* if $F|_U = 0$, where $F|_U$ denotes the restriction of F to $U \times U$.

Finally, we are also interested in spaces (V, F) with a trivial form $F = 0$. In this case, every $x \in V$ is singular and every subspace $U \subseteq V$ is totally singular.

The *Witt index* of V is defined to be the maximum dimension of a totally singular subspace of V. By Lemma A.2 (4), when V is a symplectic, orthogonal, or unitary space, the Witt index of V is at most $\frac{1}{2} \dim V$.

[10] As F is skew-symmetric, the condition $F(x, x) = 0$ for $x \in V$ automatically holds if $p \neq 2$.

Isometries and similarities. We define isometries and similarities, which are invertible linear maps that preserve a form or scale it by a factor.

Definition A.4 (isometry and similarity)**.** *An* isometry *between spaces (V, F) and (V', F') is an invertible linear map $\alpha : V \to V'$ such that $F'(\alpha(x), \alpha(y)) = F(x, y)$ for $x, y \in V$. If (V, Q) and (V', Q') are orthogonal spaces then we require $Q'(\alpha(x)) = Q(x)$ for $x \in V$ instead.*

More generally, a similarity *between spaces (V, F) and (V', F') is an invertible linear map $\alpha : V \to V'$ such that $F'(\alpha(x), \alpha(y)) = \lambda(\alpha)F(x, y)$ for all $x, y \in V$, where $\lambda(\alpha) \in \mathbb{F}_q^\times$ depends on α but not on x or y. If (V, Q) and (V', Q') are orthogonal spaces then we require $Q'(\alpha(x)) = \lambda(\alpha)Q(x)$ for $x \in V$ instead.*

We are mostly interested in forms on subspaces that are restrictions of the same form on V: Fix (V, F) (resp. (V, Q)). Then an isometry between subspaces $U, W \subseteq V$ is just an isometry between $(U, F|_U)$ and $(W, F|_W)$ (resp. $(U, Q|_U)$ and $(W, Q|_W)$). It is also called an isometry of U if $U = W$. Similarities between U and W are defined analogously.

We say $U, W \subseteq V$ are isometric (or similar) if there exists an isometry (or similarity) between them. We say $x, y \in V$ are isometric if $F(x, x) = F(y, y)$ (or $Q(x) = Q(y)$ if V is an orthogonal space).

The following lemma is very important in the study of finite classical groups. Its proof can be found in [Asc00, Section 20].

Lemma A.5 (Witt's Lemma)**.** *Let V be a symplectic, orthogonal, or unitary space. Let U, W be subspaces of V and let $\alpha : U \to W$ be an isometry between U and W. Then α extends to an isometry of V.*

Definition A.6 (isometry group)**.** *For a space (V, F) (or (V, Q)), denote by $I(V, F)$ (or $I(V, Q)$) its isometry group, i.e., the group of all isometries of V. We also write $I(V)$ for the isometry group when the form F or Q is clear from the context.*[11]

Note that if $\alpha : V \to V'$ is a similarity between two spaces V and V', then $\tau : V \to V$ is an isometry of V iff $\alpha\tau\alpha^{-1}$ is an isometry of V'. Thus, to classify the isometry groups of symplectic, orthogonal, and unitary spaces up to isomorphism, we just need to classify the equivalence classes of these spaces under the relation of similarity. To classify these equivalence classes, we need the following definitions.

Let V be a symplectic, orthogonal, or unitary space equipped with a form $F : V \times V \to \mathbb{F}_q$, where F is chosen to be the associated bilinear form F_Q if (V, Q) is orthogonal. A two-dimensional subspace $U \subseteq V$ is called a *hyperbolic plane* if there exists a basis $\{x, y\}$ of U such that x, y are singular and $F(x, y) = 1$. The pair (x, y) is called a *hyperbolic pair*. We say a subspace $U \subseteq V$ is *hyperbolic* if it is an orthogonal direct sum of hyperbolic planes. Obviously, the dimension of every hyperbolic space is even. We say U is *definite* if it possesses no nontrivial singular vectors. It is known that if the Witt index of V is m iff V is the orthogonal direct sum of a hyperbolic subspace of dimension $2m$ and a (possibly zero) definite subspace [Asc00, (19.15)].

A basis $\{x_1, \ldots, x_n\}$ of V is called an *orthonormal basis* if $F(x_i, x_i) = 1$ for $i \in [n]$ and $F(x_i, x_j) = 0$ for distinct $i, j \in [n]$.

Lemma A.7 ([Asc00, (21.6)])**.** *Suppose V has dimension n over $\mathbb{F}_q$. We have*

- *V admits a symplectic form F iff n is even, in which case (V, F) is unique up to isometry and is hyperbolic.*
- *V admits a unitary form F iff q is a square, in which case (V, F) is unique up to isometry and has an orthonormal basis. The Witt index of (V, F) is $n/2$ if n is even and $(n-1)/2$ if n is odd.*
- *Suppose n is even. Then there are two equivalence classes of orthogonal spaces (V, Q) under isometry, whose Witt indices are $n/2$ and $n/2 - 1$ respectively. They are also the two equivalence classes under similarity.*
- *Suppose n is odd. If q is odd, there are two equivalence classes of orthogonal spaces (V, Q) under isometry, which are similar and have Witt index $(n-1)/2$. If q is even, then V does not admit a non-degenerate quadratic form.*

[11] The isometry group is denoted by $O(V, F)$ or $O(V, Q)$ in [Asc00]. We use the notations from [KL90] instead.

Corollary A.8. *Let V be a symplectic, orthogonal, or unitary space of dimension at least three. Then V contains a hyperbolic plane.*

Lemma A.9. *Let V be a symplectic, orthogonal, or unitary space equipped with a form F or Q. Then we have:*

(1) If $\dim V \geq 3$, every vector $u \in V$ is contained in a hyperbolic plane.

(2) More generally, if $\dim V \geq 2k+1$, every subspace $U \subseteq V$ of dimension k is a subspace of some hyperbolic space $W \subseteq V$ of dimension at most $2k$.

Proof. (1): Let (x, y) be a hyperbolic pair, whose existence is guaranteed by Corollary A.8. If V is symplectic, let $u' = x$. Then u and u' are both singular. If V is unitary, let $u' = tx + y$ where we choose $t \in \mathbb{F}_q$ such that the trace $t + t^{q^{1/2}}$ of t equals $F(u, u)$. Such t exists since $F(u, u) = F(u, u)^{q^{1/2}} \in \mathbb{F}_{q^{1/2}}$ and the trace map $t \mapsto t + t^{q^{1/2}}$ from $\mathbb{F}_q$ to $\mathbb{F}_{q^{1/2}}$ is surjective. Then $F(u', u') = F(u, u)$. If V is orthogonal, let $u' = tx + y$ where $t = Q(u)$. Then $Q(u') = F_Q(tx, y) = tF_Q(x, y) = t = Q(u)$. In each case, u' is isometric to u. So by Witt's Lemma, there is an isometry of V sending u' to u and $\langle x, y\rangle \ni u'$ to a hyperbolic plane $P \ni u$.

(2): We maintain a hyperbolic subspace $W \subseteq V$ such that $\dim W \leq 2\dim(U \cap W)$. Initially, $W = \{0\}$. If $U \subseteq W$ then we are done. Otherwise, let $u \in U - W$. Write $u = u_1 + u_2$ such that $u_1 \in W$ and $u_2 \in W^\perp$. Note $\dim W^\perp = \dim V - \dim W \geq \dim V - 2\dim(U \cap W) \geq (2k+1) - 2(k-1) \geq 3$. By (1), u_2 is contained in a hyperplane $P \subseteq W^\perp$. Then $W + P$ contains u_2 and hence also contains $u = u_1 + u_2$. Replace W by $W + P$, which increases $\dim W$ by two and increases $\dim(U \cap W)$ by at least one. Repeat this process until $U \subseteq W$. □

Finite classical groups. Suppose V is an n-dimensional vector space over $\mathbb{F}_q$ equipped with a form $F : V \times V \to \mathbb{F}_q$ or $Q : V \to \mathbb{F}_q$. We consider four cases:

(1) $F = 0$ is trivial,

(2) (V, F) is a symplectic space,

(3) (V, F) is a unitary space, and

(4) (V, Q) is an orthogonal space.

We call these four cases **L**, **S**, **U**, and **O** respectively.

By definition, the isometry group $I(V)$ is a subgroup of the general linear group $\mathrm{GL}(V)$. In Case **L**, we have $F = 0$ and $I(V)$ is just $\mathrm{GL}(V)$.

In Case **S**, there is a unique symplectic form on V up to isometry by Lemma A.7. The corresponding isometry group $I(V)$ is the *symplectic group* $\mathrm{Sp}(V)$.

In Case **U**, there is a unique unitary form on V up to isometry. The corresponding isometry group $I(V)$ the *unitary group* $\mathrm{U}(V)$.

Finally, in Case **O**, we need to distinguish two cases according to the parity of n. If n is even, there are two different orthogonal spaces (V, Q) up to similarity. One has Witt index $n/2$ and the other has Witt index $n/2 - 1$. The corresponding isometry groups are the *orthogonal groups* $\mathrm{O}^+(V)$ and $\mathrm{O}^-(V)$ respectively. If n is odd, then there is a unique orthogonal space up to similarity. The corresponding isometry group is the *orthogonal group* $\mathrm{O}(V)$.

Define the *special isometry group* $S(V) := I(V) \cap \mathrm{SL}(V)$, i.e., $S(V)$ consists of the isometries of determinant one. For the cases **L**, **O**, and **U**, this yields the *special linear group* $\mathrm{SL}(V)$, the *special unitary group* $\mathrm{SU}(V)$, and the *special orthogonal groups* $\mathrm{SO}^+(V)$, $\mathrm{SO}^-(V)$, $\mathrm{SO}(V)$ respectively. For Case **S**, it is known that $\mathrm{Sp}(V) \leq \mathrm{SL}(V)$ [Asc00, (22.4)]. So $S(V)$ is simply $\mathrm{Sp}(V)$ in this case.

When V is in Case **O**, $n = \dim V \geq 2$ and $I(V) \neq \mathrm{O}_4^+(2)$, the group $S(V)$ has a unique subgroup Ω of index two [KL90, Proposition 2.5.7], and we define $\Omega(V) = \Omega$. In the other cases, let $\Omega(V) = S(V)$. When $I(V)$ equals $\mathrm{O}^+(V)$ or $\mathrm{O}^-(V)$, we also write $\Omega^+(V)$ or $\Omega^-(V)$ for $\Omega(V)$.

We also define the *semisimilarity group* $\Gamma(V)$. But first, we need to define semilinear transformations.

Definition A.10. *A* semilinear transformation *of V is a map $\alpha : V \to V$ such that for all $x, y \in V$ and $c \in \mathbb{F}_q$, we have $\alpha(x + y) = \alpha(x) + \alpha(y)$ and $\alpha(cx) = {}^{\sigma(\alpha)}c \cdot \alpha(x)$, where $\sigma(\alpha) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$*

is determined by α. The general semilinear group $\Gamma\mathrm{L}(V)$ *is the group of all invertible semilinear transformations of V.*

The function $\sigma(\cdot)$ in Definition A.10 is a group homomorphism from $\Gamma\mathrm{L}(V)$ to $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, and its kernel is precisely $\mathrm{GL}(V)$.

For (V, F) in the cases **L**, **S** and **U**, the group $\Gamma(V, F)$ is the group of $\alpha \in \Gamma\mathrm{L}(V)$ such that $F(\alpha(x), \alpha(y)) = \lambda(\alpha) \cdot {}^{\sigma(\alpha)}F(x, y)$ for $x, y \in V$, where $\lambda(\alpha) \in \mathbb{F}_q^\times$ and $\sigma(\alpha) \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ depend on α but not on x or y. When (V, Q) is in Case **O**, we require $Q(\alpha(x)) = \lambda(\alpha) \cdot {}^{\sigma(\alpha)}Q(x)$ for $x \in V$ instead. (Such a map α is called a *semisimilarity*.) It is easy to see $\sigma(\alpha)$ here coincides with $\sigma(\alpha)$ in Definition A.10. Write $\Gamma(V)$ for $\Gamma(V, F)$ or $\Gamma(V, Q)$ when F or Q is clear from the context. Note $\Gamma(V) = \Gamma\mathrm{L}(V)$ when V is in Case **L**. The isometry group $I(V)$ is a normal subgroup of $\Gamma(V)$.

Fix a basis B of V so that elements in $\mathrm{GL}(V)$ are represented by $n \times n$ matrices over $\mathbb{F}_q$. Note $\mathrm{GL}(V)$ has an involution (i.e., an automorphism of order two) ι that sends every g to $(g^{-1})^T$, the transpose of g^{-1} in the basis B. We call ι the *transpose-inverse automorphism* (in the basis B).

Now we define the group $A(V)$ as follows: Identifying $\Gamma\mathrm{L}(V)$ with the semidirect product $\mathrm{GL}(V) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$, the action of $\langle\iota\rangle$ on $\mathrm{GL}(V)$ extends to an action on $\Gamma\mathrm{L}(V)$ that is trivial on the subgroup $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$. So we may form the semidirect product $\Gamma\mathrm{L}(V) \rtimes \langle\iota\rangle$. Let $A(V) = \Gamma\mathrm{L}(V) \rtimes \langle\iota\rangle$ if V is in Case **L**. Otherwise let $A(V) = \Gamma(V)$.

As $V \cong \mathbb{F}_q^n$, we also use the notations $\mathrm{Sp}_n(q), \mathrm{SO}_n(q), \Omega_n^+(q)$, etc. to denote the groups defined above, except that we use $\mathrm{U}_n(q^{1/2})$ and $\mathrm{SU}_n(q^{1/2})$ instead of $\mathrm{U}_n(q)$ and $\mathrm{SU}_n(q)$ when V is in Case **U**.

So far, we have a chain of groups $\Omega(V) \le S(V) \le I(V) \le \Gamma(V) \le A(V)$. Note the group of scalars $\mathbb{F}_q^\times$ is normal in $A(V)$. So we may consider the quotients of this chain of groups modulo scalars, which we denote by $\overline{\Omega(V)} \le \overline{S(V)} \le \overline{I(V)} \le \overline{\Gamma(V)} \le \overline{A(V)}$. For a group $X \le \Gamma\mathrm{L}(V)$ defined above, we also denote its quotient modulo scalars $X/(X \cap \mathbb{F}_q^\times)$ by $\mathrm{P}X$ (e.g., $\mathrm{P}\Gamma\mathrm{L}(V)$, $\mathrm{PSp}_n(q)$, etc.).

The quotient map $S(V) \to \overline{S(V)}$ is an isomorphism if V is in Case **S** and q is even, or if V is in Case **O** and n is odd [KL90, Table 2.1.C and Table 2.1.D]. So we write $\mathrm{Sp}(V)$ for $\mathrm{PSp}(V)$ and $\Omega(V)$ for $\mathrm{P}\Omega(V)$ in these cases.

Now we are ready to define finite classical groups.

Definition A.11 (finite classical group)**.** *Suppose V is in one of the four cases* **L**, **S**, **U**, *and* **O**. *A group G satisfying $\Omega(V) \le G \le A(V)$ or $\overline{\Omega(V)} \le G \le \overline{A(V)}$ is called a* finite classical group*, and V is called the* natural module *of G.*

It is easy to show that $\overline{\Omega(V)}$ is a normal subgroup of $\overline{A(V)}$. So a finite simple classical subgroup has the form $\overline{\Omega(V)}$. The following theorem states that $\overline{\Omega(V)}$ is indeed nonabelian simple when $n = \dim V$ is large enough.

Theorem A.12 ([KL90, Theorem 2.1.3])**.** *Assume that $n = \dim V$ is at least 2, 3, 4, 7 in cases* **L**, **U**, **S** *and* **O**, *respectively. Then $\overline{\Omega(V)}$ is nonabelian simple, except for $\mathrm{PSL}_2(2)$, $\mathrm{PSL}_2(3)$, $\mathrm{PSU}_3(2)$ and $\mathrm{Sp}_4(2)$.*

So we have the following families of finite simple classical groups:

$$\mathrm{PSL}_n(q),\ \ \mathrm{PSU}_n(q^{1/2}),\ \ \mathrm{PSp}_n(q),\ \ \mathrm{P}\Omega_n^{\pm}(q)\ (n \text{ even}),\ \ \Omega_n(q)\ (m \text{ odd}).$$

The group $\overline{A(V)}$ acts on $\overline{\Omega(V)}$ by conjugation, which gives a map $\overline{A(V)} \to \mathrm{Aut}(\overline{\Omega(V)})$. The following theorem states that this map is an isomorphism when $n = \dim V$ is large enough.

Theorem A.13 ([KL90, Theorem 2.1.4])**.** *Assume that $\overline{\Omega(V)}$ is nonabelian simple and that n is as in Theorem A.12. Then $\overline{A(V)} = \mathrm{Aut}(\overline{\Omega(V)})$, except when $\Omega(V) = \mathrm{Sp}_4(q)$ with q even and when $\Omega(V) = \mathrm{P}\Omega_8^+(q) \cong \Omega_8^+(q)$.*

Orders of finite simple classical groups. Table 2 lists the orders of all finite simple classical groups. It can be deduced from [CCNP85, Table 6] or [KL90, Table 2.1.C and Table 2.1.D].

G	$\lvert G\rvert$
$\mathrm{PSL}_n(q)$	$\frac{q^{n(n-1)/2}}{\gcd(q-1,n)} \prod_{i=2}^{n}(q^i-1)$
$\mathrm{PSU}_n(q)$	$\frac{q^{n(n-1)/2}}{\gcd(q+1,n)} \prod_{i=2}^{n}(q^i-(-1)^i)$
$\mathrm{PSp}_n(q)$	$\frac{q^{n^2/4}}{\gcd(q-1,2)} \prod_{i=1}^{n/2}(q^{2i}-1)$
$\mathrm{P}\Omega_n^{\pm}(q)$, n even	$\frac{q^{n(n-2)/4}(q^{n/2}\mp 1)}{\gcd(q^{n/2}\mp 1,4)} \prod_{i=1}^{n/2-1}(q^{2i}-1)$
$\Omega_n(q)$, nq odd	$q^{(n-1)^2/4} \prod_{i=1}^{(n-1)/2}(q^{2i}-1)$

Table 2: $|G|$ for G a finite simple classical group

Minimal degrees of permutation representations. For a finite simple group G, a permutation representation $\rho : G \to \mathrm{Sym}(S)$ is nontrivial iff it is faithful since $\ker(\rho) \lneq G \Rightarrow \ker(\rho) = \{e\}$. The minimal degrees $\mu(G)$ of (nontrivial) permutation representations of finite simple classical groups G have been completely determined by Cooperstein [Coo78] and Patton [Pat72]. We include a table from [KL90] that summarizes their results (see Table 3).

G	minimal degree $\mu(G)$
$\mathrm{PSL}_n(q)$ $(n,q) \neq (2,5),(2,7),(2,9),(2,11),(4,2)$	$(q^n-1)/(q-1)$
$\mathrm{PSL}_n(q)$ $(n,q) = (2,5),(2,7),(2,9),(2,11),(4,2)$	$5, 7, 6, 11, 8$
$\mathrm{PSp}_{2m}(q), m \geq 2, q > 2, (m,q) \neq (2,3)$	$(q^{2m}-1)/(q-1)$
$\mathrm{Sp}_{2m}(2), m \geq 3$	$2^{m-1}(2^m-1)$
$\mathrm{PSp}_4(3)$	27
$\Omega_{2m+1}(q), m \geq 3, q$ odd, $q \geq 5$	$(q^{2m}-1)(q-1)$
$\Omega_{2m+1}(3), m \geq 3$	$3^m(3^m-1)/2$
$\mathrm{P}\Omega_{2m}^{+}(q), m \geq 4, q \geq 3$	$(q^m-1)(q^{m-1}+1)/(q-1)$
$\mathrm{P}\Omega_{2m}^{+}(2), m \geq 2$	$2^{m-1}(2^m-1)$
$\mathrm{P}\Omega_{2m}^{-}(q), m \geq 2$	$(q^m+1)(q^{m-1}-1)/(q-1)$
$\mathrm{PSU}_3(q), q \neq 5$	q^3+1
$\mathrm{PSU}_3(5)$	50
$\mathrm{PSU}_4(q)$	$(q+1)(q^3+1)$
$\mathrm{PSU}_n(q), n \geq 5, (n,q) \neq (6m,2)$	$(q^n-(-1)^n)(q^{n-1}-(-1)^{n-1})/(q^2-1)$
$\mathrm{PSU}_n(2), 6 \mid n$	$2^{n-1}(2^n-1)/3$

Table 3: $\mu(G)$ for G a finite simple classical group [KL90, Table 5.2.A]

The following lemma follows directly from Table 3.

Lemma A.14. *There exists an absolute constant $c > 0$ such that $\mu(G) \geq q^{cm}$ for any finite simple classical group G of rank m over a finite field $\mathbb{F}_q$.*

Semilinear action of $\Gamma\mathrm{L}(V)$ on V^*. The natural action of $\Gamma\mathrm{L}(V)$ on V induces an action of $\Gamma\mathrm{L}(V)$ on the dual space V^*, given by

$$({}^gL)(x) = {}^{\sigma(g)}(L({}^{g^{-1}}x)) \quad \text{for } L \in V^* \text{ and } x \in V$$

where $\sigma(g)$ is as in Definition A.10. It is easy to see that this action is also semilinear, i.e., ${}^g(L+L') = {}^gL + {}^gL'$ and ${}^g(cL) = {}^{\sigma(g)}c \cdot {}^gL$ for $g \in \Gamma\mathrm{L}(V)$, $L, L' \in V^*$ and $c \in \mathbb{F}_q$.

Note $({}^gL)({}^gx) = {}^{\sigma(g)}(L(x)) = 0$ iff $L(x) = 0$. So ${}^g\ker(L) = \ker({}^gL)$ for $g \in \Gamma\mathrm{L}(V)$ and $L \in V^*$.

Transvections and reflections. For a linear map $t : V \to V$, define $[V,t] := \{t(v) - v : v \in V\}$ and $C_V(t) = \{v \in V : t(v) = v\}$, which are subspaces of V. We say t is a *transvection* if $[V,t]$ is one-dimensional, $C_V(t)$ is a hyperplane of V, and $[V,t] \subseteq C_V(t)$.

Suppose (V,Q) is an orthogonal space and $\mathrm{char}(\mathbb{F}_q) \neq 2$. We say a linear map $t : V \to V$ is a *reflection* if $[V,t]$ is spanned by a nonsingular vector, $C_V(t)$ is a hyperplane of V, and $C_V(t) = [V,t]^\perp$. It can be shown that every reflection t is an involution, i.e., $t = t^{-1}$ [Asc00].

Lemma A.15 ([Asc00, (22.3)])**.** *Let (V,F) be a symplectic space. Then a linear map $t : V \to V$ is a transvection in $I(V,F)$ iff t has the form $x \mapsto x + \lambda F(x,v)v$ where $v \in V - \{0\}$ and $\lambda \in \mathbb{F}_q^\times$.*

Lemma A.16 ([Asc00, (22.7)])**.** *Let V be a vector space of dimension n over a finite field $\mathbb{F}_q$. We have:*

- *If V is a symplectic space, then $I(V) = \mathrm{Sp}(V)$ is generated by the set of transvections in $I(V)$.*
- *If V is a unitary space, then $S(V) = \mathrm{SU}(V)$ is generated by the set of transvections in $I(V)$ unless $(n,q) = (3,4)$.*
- *If V is an orthogonal space, then $I(V)$ is generated by the set of reflections (or the set of transvections if $\mathrm{char}(\mathbb{F}_q) = 2$) in $I(V)$ unless $(n,q) = (4,2)$ and $I(V) = \mathrm{O}^+(V)$.*

Appendix B Omitted proofs

Proof of Lemma 2.4. Let $\bar{G} \leq \mathrm{Sym}(S)$ be the image of G under the permutation representation $G \to \mathrm{Sym}(S)$. We claim the map $\lambda : S \to T$ sending ${}^gx$ to ${}^{\phi(g)}y$ for $g \in G$ is a bijection, and $\bar{G}$ is permutation isomorphic to $\bar{H}$ with respect to λ. This claim implies the lemma.

As $G_x \leq \phi^{-1}(H_y)$, the map λ is well-defined. As G is transitive on S and $\phi^{-1}(H_y) \leq G_x$, λ is injective. It is also surjective since the image of $\phi(G)$ in $\bar{H}$ equals $\bar{H}$ which is transitive on T. So λ is a well-defined bijection.

For $g \in G$ (resp. $g \in H$), denote by $\bar{g}$ its image in $\bar{G}$ (resp. $\bar{H}$). Define a map $\bar{\phi} : \bar{G} \to \bar{H}$ by $\bar{\phi}(\bar{g}) = \overline{\phi(g)}$, which is well-defined since $\phi(\bigcap_{z \in S} G_z) \leq \bigcap_{z \in T} H_z$. It is surjective by Condition (2). Also note $\lambda({}^{\bar{g}}z) = {}^{\bar{\phi}(\bar{g})}(\lambda(z))$ by the definition of λ and that of $\bar{\phi}$. On the other hand, the bijection λ between S and T induces a permutation isomorphism ψ between $\bar{G}$ and a subgroup of $\mathrm{Sym}(T)$. It remains to check that $\psi = \bar{\phi}$, which implies that $\bar{\phi}$ is injective. Consider $g \in G$ and $z \in T$. As $\phi(G)$ is transitive on T, we may choose $h \in G$ such that $z = {}^{\phi(h)}y$. Then ${}^{\psi(\bar{g})}z = {}^{\psi(\bar{g})}({}^{\phi(h)}y) = {}^{\psi(\bar{g})}\lambda({}^hx) = \lambda({}^{gh}x)$ and ${}^{\bar{\phi}(\bar{g})}z = {}^{\overline{\phi(g)}}({}^{\phi(h)}y) = {}^{\phi(gh)}y = \lambda({}^{gh}x)$. So $\psi = \bar{\phi}$, as desired. □

Now we prove Lemma 5.2. We first show that the same result holds for $\mathcal{P}_{G,m}$ in place of $\mathcal{P}_{G,m,N}$:

Lemma B.1. *There exists an algorithm that given the following data*

- *a number field F,*
- *a polynomial $g(X) \in F[X]$ of degree n, whose Galois group over F is denoted by G and splitting field over F is denoted by L, and*
- *$m \in \mathbb{N}^+$,*

runs in time polynomial in n^m and the size of the input, and computes a set $\mathcal{F}$ of number fields that contain F and are isomorphic to subfields of L over F, such that the subgroup system associated with $(\mathcal{F}, L/F)$ is $\mathcal{P}_{G,m}$, where G is regarded as a permutation group acting naturally on the set of roots of g in L.

Proof. The set $\mathcal{F}$ simply consists of the fields that are obtained by adjoining at most m roots of g to F. Formally, we construct $\mathcal{F}$ as follows: Let S be the set of roots of g in L. For $i = 1, 2, \ldots, m$, we inductively compute $\mathcal{F}_i$ such that subgroup system associated with $(\mathcal{F}_i, L/F)$ is $\mathcal{P}_{G,i}$. Let $\mathcal{F}_0 = \{F\}$.

Suppose $\mathcal{F}_{i-1}$ is constructed. Compute the set $\mathcal{K}_i$ of fields $K' = K[X]/(h(X))$, where K ranges over $\mathcal{F}_{i-1}$ and $h(X)$ ranges over the set of nonlinear irreducible factors of $g(X)$ over K (these factors are computed using known factoring algorithms for polynomials over number fields [Len83, Lan85]). We need to encode such a field K' by an irreducible polynomial h_0 over F (i.e., $K' = F[X]/(h_0(X))$). This is done by efficiently finding a primitive element over F. See [Rón92] for details. Let $\mathcal{F}_1 = \mathcal{K}_1$ and $\mathcal{F}_i = \mathcal{F}_{i-1} \cup \mathcal{K}_i$ for $i > 1$.

Note that the subgroup system associated with $(\mathcal{F}_1, L/F)$ is $\mathcal{P}_{G,1}$. A simple induction shows that for $i = 2, 3, \ldots, m$, the subgroup system associated with $(\mathcal{K}_i, L/F)$ is

$$\mathcal{P}'_i := \{H_x : H \in \mathcal{P}_{G,i-1}, x \in S, H_x \lneq H\}$$

and the subgroup system associated with $(\mathcal{F}_i, L/F)$ is $\mathcal{P}_{G,i-1} \cup \mathcal{P}'_i = \mathcal{P}_{G,i}$, as desired. Again by induction, the number of fields in $\mathcal{F}_i$ and the maximum degree of these fields over F are both bounded by n^m. So the running time is polynomial in n^m and the size of the input. □

Proof of Lemma 5.2. The algorithm runs as follows. First, use Lemma B.1 to construct a set $\mathcal{F}_0$ of number fields in time polynomial in n^m and the size of the input, such that the subgroup system associated with $(\mathcal{F}_0, L/F)$ is $\mathcal{P}_{G,m}$. Next, enumerate $F_1, F_2 \in \mathcal{F}_0$ and F-linear field embedding $\phi : F_1 \hookrightarrow F_2$. Here ϕ is found as follows: Suppose F_1 is represented by an irreducible polynomial $g(X) \in F[X]$ over F, i.e., $F_1 = F[X]/(g(X))$. Let $\alpha = X + (g(X)) \in F_1$, which is a root of g. Then $\phi : F_1 \hookrightarrow F_2$ is determined by the image $\phi(\alpha)$ which is a root of g in F_2. So we can enumerate ϕ by finding all the roots of g in F_2 using a factoring algorithm for polynomials over number fields [Len83, Lan85].

Let $\mathcal{K} = \emptyset$. For each (F_1, F_2, ϕ) above, regard F_1 as a subfield of F_2 using ϕ. Find an irreducible polynomial $h(X)$ over F_1 such that F_2 is isomorphic to $F_1[X]/(h(X))$ over F_1. Such h can be found by computing the minimal polynomial of a primitive element of F_2 over F_1. Choose the largest integer m' such that $m' \le [F_2 : F_1]$ and $[F_2 : F_1]^{m'} \le N$. If $m' > 0$, run the algorithm in Lemma B.1 on F_1, h and m' to compute a set of fields in time polynomial in $\deg(h)^m = [F_2 : F_1]^{m'} \le N$ and the size of (F_1, h, m') (which is polynomial in n^m and the size of the input), and then add these fields to $\mathcal{K}$. Finally, after enumerating all (F_1, F_2, ϕ), output $\mathcal{F} := \mathcal{F}_0 \cup \mathcal{K}$. The total running time is polynomial in N, n^m, and the size of the input.

The enumeration of (F_1, F_2, ϕ) corresponds to the enumeration of $H, K \in \mathcal{P}_{G,m}$ with $K \le H$ under the Galois correspondence. Moreover, if we identify $F_2 \cong F_1[X]/(h(X))$ with L^K, and F_1 with L^H, then the natural action of $H = \mathrm{Gal}(L/F_1)$ on the set of roots of h in L is equivalent to its action on $K\backslash H$ by inverse right translation. So by Galois theory and Lemma B.1, the subgroup system associated with $(\mathcal{F}, L/F)$ is precisely $\mathcal{P}_{G,m,N}$. □

Proof of Lemma 6.17. Let S' be the set of all subspaces isometric to U. We want to prove $S = S'$. As G is primitive, G_0 is transitive on S [Wie64, Proposition 7.1]. As $G_0 \le \overline{I(V)}$, we have $S \subseteq S'$. So we just need to prove that G_0 is transitive on S'.

Assume to the contrary that G_0 is intransitive on S'. It is known that either (a) $\overline{I(V)}_U = N_{\overline{I(V)}}((G_0)_U)$ or (b) $\overline{I(V)}_U G_0 = \overline{I(V)}$ [KL90, Theorem 3.1.2]. As $\overline{I(V)}$ is transitive on S' by Witt's Lemma whereas G_0 is not, (b) does not hold. So (a) holds. This means the action of $\overline{I(V)}$ on S' is equivalent to its action on $C := \{g(G_0)_U g^{-1} : g \in \overline{I(V)}\}$ by conjugation. As G_0 is intransitive on S', it is also intransitive on C.

The group $\overline{\Gamma(V)} \ge \overline{I(V)}$ acts on $C' := \{g(G_0)_U g^{-1} : g \in \overline{\Gamma(V)}\} \supseteq C$ by conjugation. Denote by T the set of G_0-orbits in C'. Then $\overline{\Gamma(V)}$ permutes the members of T. So we have a permutation representation $\pi : \overline{\Gamma(V)} \to \mathrm{Sym}(T)$. By the previous paragraph, we have $\overline{I(V)} \not\le \ker(\pi)$.

The map π has been completely determined in Table 3.5.G of [KL90]. See also Tables 3.5.A–3.5.F, Column V and the rows corresponding to the class $\mathcal{C}_1$. From these tables, it can be seen that $\overline{I(V)} \not\le \ker(\pi)$ holds only when G is in Case **O** and U is a totally singular subspace of dimension $\frac{1}{2}\dim V$. Indeed, in this case, the set S' of subspaces W has two G_0-orbits distinguished by the parity

of $\dim W \cap U$ [KL90, Lemma 2.5.8]. However, the case $\dim U = \frac{1}{2}\dim V$ is excluded by Lemma 6.16 as we assume $b(G) > C$ for a large enough constant C. □

Proof of Lemma 6.19. Let $d = \dim U_0$. Let $\{e_1, \ldots, e_d\}$ be a basis of U_0. We divide the proof into the following cases.

Case 1: V is in Case **L** and $d = 1$.

In this case, $U_0 = \langle e_1 \rangle$. If $S' = S$, pick $e_0, e_0' \in V - U_0$ such that e_0, e_0', e_1 are linearly independent. Otherwise, S' is the set of complements of the hyperplane W_0 in V, and we pick linearly independent $e_0, e_0' \in W_0 - \{0\}$. Let $W = \langle e_0, e_0', e_1 \rangle$. Let $k = 4$ and

$$U_1 = \langle e_0 + e_1 \rangle, U_2 = \langle e_0' + e_1 \rangle, U_3 = \langle e_0 + e_0' + e_1 \rangle, U_4 = \langle e_0 + \alpha e_1 \rangle$$

where α is an element of $\mathbb{F}_q$ not contained in any proper subfield. Then Condition (1) and Condition (3) hold. Note $W \cap W_0 = \langle e_0, e_0' \rangle$. If S' is the set of complements of W_0 in V, then $U_i \cap W_0 = U_i \cap W \cap W_0 = \{0\}$ for $i \in [4]$. So $U_i \in S'$ for $i \in [4]$.

It remains to verify Condition (2). Consider any $g \in G_{U_0, U_1, \ldots, U_k}$. Lift $g|_W \in \mathrm{P\Gamma L}(W)$ to $g' \in \Gamma\mathrm{L}(W)$. We want to prove $g' \in \mathbb{F}_q^\times$. As $e_0 + e_0' + e_1 = -e_1 + (e_0 + e_1) + (e_0' + e_1)$ and g' fixes U_0, U_1, U_2, U_3, we know g' multiplies e_1, $e_0 + e_1$ and $e_0' + e_1$ by the same factor. Then g' also multiplies e_0, e_0' and e_1 by the same factor. As g' also fixes $\langle e_0 + \alpha e_1 \rangle$, we have ${}^{\sigma(g')}\alpha = \alpha$ and hence $g' \in \mathrm{GL}(W)$. So $g' \in \mathbb{F}_q^\times$, as desired.

Case 2: V is in Case **L** and $d \geq 2$.

If $S' = S$, pick $e_0 \in V - U_0$. Otherwise, S' is the set of complements of W_0 in V, and we pick $e_0 \in W_0 - \{0\}$. Let $W = \langle e_0, \ldots, e_d \rangle$. For $0 \leq i \leq d$, let $e_i^* \in W^*$ be the linear form sending e_i to one and e_j to zero for $j \neq i$. Let

$$B = \{e_0^* + e_i^* : i \in [d]\} \cup \{e_0^* + e_i^* + e_{i+1}^* : i \in [d-1]\} \cup \{e_0^* + \alpha e_1^*\}.$$

where α is an element of $\mathbb{F}_q$ not contained in any subfield. Let $k = |B| = 2d$, and choose hyperplanes $U_1, \ldots, U_k$ of W such that $\{U_1, \ldots, U_k\} = \{\ker(L) : L \in B\}$. Then $U_1, \ldots, U_k \in S$. If S' is the set of complements of W_0 in V, then as $W \cap W_0 = \langle e_0 \rangle$ and $L(e_0) \neq 0$ for all $L \in B$, we have $U_i \cap W_0 = U_i \cap W \cap W_0 = \{0\}$ for $i \in [k]$. So $U_i \in S'$ for $i \in [k]$.

Condition (3) of the lemma follows from the construction. Note $\ker(e_0^*) = U_0$ and $\ker(e_0^*) + \ker(e_0^* + e_1^*) = W$. So Condition (1) also holds. It remains to verify Condition (2). We have a semilinear action of $\Gamma\mathrm{L}(W)$ on W^* via $({}^g L)(x) = {}^{\sigma(g)}(L({}^{g^{-1}}x))$ (see Appendix A). Consider any $g \in G_{U_0, U_1, \ldots, U_k}$. Lift $g|_W \in \mathrm{P\Gamma L}(W)$ to $g' \in \Gamma\mathrm{L}(W)$. We want to prove $g' \in \mathbb{F}_q^\times$. For every $L \in B$, as g' fixes $\ker(L)$, we have $\ker(L) = {}^{g'}\ker(L) = \ker({}^{g'}L)$. So g' fixes $\langle L \rangle$ for $L \in B$. For $i \in [d-1]$, the linear form $e_0^* + e_i^* + e_{i+1}^*$ can be written as the linear combination $-e_0^* + (e_0^* + e_i^*) + (e_0^* + e_{i+1}^*)$. So g' multiplies e_0^*, $e_0^* + e_i^*$ and $e_0^* + e_{i+1}^*$ by the same factor. As this holds for all $i \in [d-1]$, we see that g' multiplies e_i^* by the same factor for $0 \leq i \leq d$. As g' also fixes $\langle e_0^* + \alpha e_1^* \rangle$, we have ${}^{\sigma(g')}\alpha = \alpha$ and hence $g' \in \mathrm{GL}(W)$. So $g' \in \mathbb{F}_q^\times$, as desired.

Case 3: V is in Case **S**, **U** or **O**.

We have $S = S'$. Let W be a non-degenerate subspace of V such that $U_0 \subseteq W$ and $c'/2 \leq \dim W \leq c'$, where $c' > 0$ is a large enough constant. The existence of W follows from, e.g., Lemma A.9 (2). Let $S|_W := \{U \in S : U \subseteq W\} \ni U_0$. So $S|_W$ is the set of subspaces isometric to U_0 in the space $(W, F|_W)$ (or $(W, Q|_W)$). Let $G_W|_W$ be the image of $G_W = \{g \in W : {}^g W = W\}$ in $\mathrm{P\Gamma L}(W)$.

We claim that the permutation representation of $G_W|_W$ on $S|_W$ is faithful, i.e., any $g \in G_W|_W$ fixing all subspaces in $S|_W$ is the identity. Consider $g \in G_W|_W$ fixing every subspace in S. We first show that g fixes $\langle u \rangle$ for every singular $u \in W$.

Assume U_0 contains a singular vector u_0. Extend it to a basis $\{u_0, \ldots, u_d\}$ of U_0, where $d = \dim U_0 - 1$. Let W' be a complement of $\mathrm{Rad}(U_0) \cap W$ in $U_0^\perp \cap W$. Find a totally singular subspace $\langle v_1, \ldots, v_d \rangle$ of dimension d in W'. Then U_0 is isometric to $U_0' := \langle u_0, u_1 + v_1, \ldots, u_d + v_d \rangle$ under the

linear map defined by $u_0 \mapsto u_0$ and $u_i \mapsto u_i + v_i$ for $i \in [d]$. So $U_0' \in S|_W$. Moreover, $U_0 \cap U_0' = \langle u_0 \rangle$. So g fixes $\langle u_0 \rangle$. By Witt's Lemma and the $I(W)$-symmetry, g fixes $\langle u \rangle$ for every singular vector $u \in W$.

Now suppose U_0 contains no singular vector. Pick $u_0 \in U_0$. The same proof in the previous paragraph still shows that g fixes $\langle u_0 \rangle$. So by Witt's Lemma and the $I(W)$-symmetry, g fixes $\langle u \rangle$ for every $u \in W$ isometric to u_0. Pick a singular vector $v \in \langle u_0 \rangle^\perp \cap W$. Then $u_0 + v$ is isometric to u_0. So g fixes both $\langle u_0 \rangle$ and $\langle u_0 + v \rangle$. Then it also fixes the plane $P := \langle u_0, u_0 + v \rangle$. By Witt's Lemma and the $I(W)$-symmetry, g fixes the set T of all subspaces in W isometric to P. Note P contains the singular vector v. Applying the proof in the previous paragraph with $(U_0, S|_W)$ replaced by (P, T), we see that g fixes every singular vector in W. It also follows that g fixes every hyperbolic plane in W.

Next, we show that g fixes $\langle u \rangle$ for every $u \in W$. Fix $u \in W$. By Lemma A.9 (1), we can find a hyperbolic pair (x, y) such that $\langle u, y \rangle = \langle x, y \rangle \subseteq W$. Pick a singular vector $v \in \langle u, y \rangle^\perp \cap W$. Then $\langle u, y \rangle$ is isometric to $\langle u, y + v \rangle$, so they are both hyperbolic planes and are fixed by g. Then g fixes $\langle u, y \rangle \cap \langle u, y + v \rangle = \langle u \rangle$, as desired. As $u \in W$ is arbitrary, this proof also shows $W = \sum_{U \in S|_W} U$.

Finally, we prove that g is the identity. Lift g to $g' \in \Gamma\mathrm{L}(W)$. We want to prove $g' \in \mathbb{F}_q^\times$. Let $\{x_1, \dots, x_s\}$ be a basis of W. As g' fixes $\langle x_1 \rangle, \dots, \langle x_s \rangle$ and $\langle x_1 + x_2 + \cdots + x_s \rangle$, it multiplies x_i by the same factor for $i \in [s]$. As g' also fixes $x_1 + \alpha x_2$ where α is an element of $\mathbb{F}_q$ not in any proper subfield, we have ${}^{\sigma(g')}\alpha = \alpha$ and hence $g' \in \mathrm{GL}(W)$. So $g' \in \mathbb{F}_q^\times$, as desired. This proves the claim that any $g \in G_W|_W$ fixing $S|_W$ pointwisely is the identity.

By [GSS98, LS91], there exists a base $B \subseteq S|_W$ of $G_W|_W$ acting on $S|_W$ such that $|B|$ is bounded by a constant depending only on $\dim W$. Then any $g \in G_W|_W$ fixing B pointwisely acts trivially on $S|_W$. Find a minimal set $B' \subseteq S|_W$ such that $W = \sum_{U \in B'} U$, which is possible since $W = \sum_{U \in S|_W} U$. Then $G_{B'}$ fixes W. So $G_{B \cup B'} \leq (G_W)_B \leq (G_W)_{S|_W}$. By claim proved above, the restriction of any $g \in G_{B \cup B'}$ to W is the identity. Suppose $B \cup B' = \{U_1, \dots, U_k\}$. Then W and $U_1, \dots, U_k$ satisfy the conditions in the lemma. □

The next lemma is used in the proof of Lemma 6.21.

Lemma B.2. *Let V be a symplectic, unitary or orthogonal space over $\mathbb{F}_q$. Let $H \subseteq U \subseteq W$ be a chain of subspaces of V such that U is non-degenerate and $\dim U = \dim H + 1 = \dim W - 1$. Then we have:*

(1) Let $T = \{{}^g H : g \in \Gamma(U)\}$. Then there are at most two equivalence classes under isometry in T, where the equivalence class of each $H_0 \in T$ is $[H_0] := \{{}^g H_0 : g \in I(U)\}$. The group $\Gamma(U)$ permutes these equivalence classes.

(2) Suppose $H' \in [H]$. If there exists $Z \subseteq W$ isometric to U such that $U \cap Z = H$, then there exists $Z' \subseteq W$ isometric to U such that $U \cap Z' = H'$.

Proof. Choose $w \in W - U$. As U is non-degenerate, we may write $w = w_1 + w_2$ where $w_1 \in U$ and $w_2 \in U^\perp$. By replacing w with w_2, we may assume $w \perp U$. Note (2) follows from Witt's Lemma: Let $\sigma : H \to H'$ be an isometry from H to H'. By Witt's Lemma, we may extend σ to an isometry of U. Further extend it to an isometry σ' of W by letting $\sigma'(w) = w$. Let $Z' = \sigma'(Z)$. Then $Z' \cap U = \sigma'(Z) \cap \sigma'(U) = \sigma'(H) = H'$, as desired.

Now we prove (1). First, we note that if $\sigma : H_1 \to H_2$ is an isometry between $H_1, H_2 \in T$, then for $g \in \Gamma(U)$, the map $g\sigma g^{-1}$ is an isometry between ${}^g H_1$ to ${}^g H_2$. So $\Gamma(U)$ permutes the equivalence classes in T.

If H is non-degenerate, then every $H_0 \in T$ is non-degenerate. In this case, there are at most two equivalence classes of H_0 under isometry by Lemma A.7. So (1) holds.

So assume H is not non-degenerate, i.e., $\mathrm{Rad}(H) \neq 0$. As U is non-degenerate, we have $\dim \mathrm{Rad}(H) \leq \dim U - \dim H \leq 1$. So $\dim \mathrm{Rad}(H) = 1$. Then $\dim \mathrm{Rad}(H_0) = 1$ for $H_0 \in T$.

Consider $H_0 \in T$, and let M be a complement of $\mathrm{Rad}(H_0)$ in H_0. Then M is non-degenerate and $H_0 = M \perp \mathrm{Rad}(H_0)$. If $\mathrm{Rad}(H)$ is totally singular, then so is $\mathrm{Rad}(H_0)$. The case that $\mathrm{Rad}(H)$ is not totally singular can happen only when V is an orthogonal space with $\mathrm{char}(\mathbb{F}_q) = 2$. In this case, we can always find $u \in \mathrm{Rad}(H_0)$ such that $Q(u) = 1$ by scaling, using the fact every element in $\mathbb{F}_q^\times$ is a square when $\mathrm{char}(\mathbb{F}_q) = 2$. In either case, $\mathrm{Rad}(H_0)$ is unique up to isometry when H is given. There are at most two equivalence classes of M under isometry by Lemma A.7. So there at most two equivalence classes of H_0 under isometry. □

Proof of Lemma 6.21. Recall that $\dim U \leq \dim V/2$. We further have $2\dim U + 3 \leq \dim V$ since otherwise $b(G)$ is bounded by an absolute constant by Lemma 6.16.

First assume the subspaces in S' are totally singular. We will find $v \in V - U$ such that $(U \cap U_1) + \langle v\rangle, (U \cap U_2) + \langle v\rangle \in S'$. The sequence $U_1, (U \cap U_1) + \langle v\rangle, (U \cap U_2) + \langle v\rangle, U_2$ then satisfies the requirements in the lemma.

If $S' = S$, just choose any singular $v \in U^\perp - U$, which exists by Lemma A.2 (4), Lemma A.9 (1) and the fact $\dim U^\perp - \dim U = \dim V - 2\dim U \geq 3$. Then $(U \cap U_1) + \langle v\rangle$ and $(U \cap U_2) + \langle v\rangle$ are totally singular and hence in S.

If V is in Case **L** and S' is the set of complements of W_0 in V, choose $u \in U - (U_1 \cup U_2)$, $w \in W_0 - \{0\}$ and let $v = u + w$. We have $v \notin U$ since $w \notin U$. And the intersection of $(U \cap U_1) + \langle v\rangle$ (resp. $(U \cap U_2) + \langle v\rangle$) with W_0 is zero since $u \notin U_1 \cup U_2$. So $(U \cap U_1) + \langle v\rangle, (U \cap U_2) + \langle v\rangle \in S'$.

Now assume the subspaces in S' are non-degenerate. Then V is in Case **S**, **U** or **O**, and $S' = S$. By assumption, there exist $g \in \Gamma(V)_U$ and $h \in \Gamma(V)_{U,U_0}$ such that $U_1 = {}^gU_0$ and $U_2 = {}^hU_1 = {}^{hg}U_0$. Let $W = U + U_1$, $H = U \cap U_0 \subseteq W$ and $T = \{{}^gH : g \in \Gamma(U)\}$. Then $H, U \cap U_1, U \cap U_2 \in T$. As h fixes H, it fixes the equivalence classes of the members of T under isometry by Lemma B.2 (1). So $U \cap U_2 = {}^h(U \cap U_1)$ is isometric to $U \cap U_1$. By Lemma B.2 (2), there exists $Z \subseteq W$ isometric to U such that $U \cap Z = U \cap U_2$ if there exists $Z' \subseteq W$ isometric to U such that $U \cap Z' = U \cap U_1$. Such Z' exists, as we can choose $Z' = U_1$. So there exists $Z \subseteq W$ such that $Z \in S$ and $U \cap Z = U \cap U_2$. Note $U + Z = W = U + U_1$. The sequence U_1, Z, U_2 then satisfies the requirements in the lemma. □

Proof of Claim 6.23. Let $g \in \Gamma\mathrm{L}(V_0)_{\langle u_0\rangle,\langle u_1\rangle,\ldots,\langle u_5\rangle,\langle w\rangle}$. We want to prove $g \in \mathbb{F}_q^\times \mathrm{GL}(V_0)_{u_0,u_1,\ldots,u_5,w}$. Suppose g sends u_i to c_iu_i for $0 \leq i \leq 5$ and sends w to cw, where $c_0, c_1, \ldots, c_5, c \in \mathbb{F}_q^\times$.

Note $u_3 = -u_0 + u_1 + u_2$. As u_0, u_1, u_2 are linearly independent, this is the unique way of writing u_3 as a linear combination of u_0, u_1, u_2. Also note $c_3u_3 = {}^gu_3 = {}^g(-u_0 + u_1 + u_2) = -c_0u_0 + c_1u_1 + c_2u_2$. It follows that $c_0 = c_1 = c_2 = c_3$. As $u_1 = u_0 + v_1$ and $u_2 = u_0 + v_2$, g also multiplies v_1 and v_2 by c_0.

As w, v_1 are linearly independent and ${}^g\langle u_5\rangle = \langle u_5\rangle$, a similar argument using the linear combination $u_5 = w + v_1$ shows $c_0 = c_5 = c$. Finally, as $u_4 = u_0 + \alpha v_1$, the LHS of the equation ${}^g\langle u_4\rangle = \langle u_4\rangle$ equals $\langle cu_0 + {}^{\sigma(g)}\alpha cv_1\rangle = \langle u_0 + {}^{\sigma(g)}\alpha v_1\rangle$ and the RHS equals $\langle u_0 + \alpha v_1\rangle$. As u_0 and v_1 are linearly independent, we have ${}^{\sigma(g)}\alpha = \alpha$ and hence $g \in \mathrm{GL}(V_0)$. Using the fact $u_4 = u_0 + \alpha v_1$, we see $c_4 = c$. Then $c^{-1}g \in \mathrm{GL}(V_0)$ fixes $u_0, u_1, \ldots, u_5, w$. So $g \in \mathbb{F}_q^\times(\mathrm{GL}(V_0)_{u_0,u_1,\ldots,u_5,w})$. □

Proof of Claim 6.25. First assume the subspaces in S are totally singular. As $U \cap U_1 \neq U \cap U_2$, we have $U = (U \cap U_1) + (U \cap U_2)$ and $U_1 = (U \cap U_1) + (U_1 \cap U_2)$. Combining this with the fact that U, U_1, U_2 are totally singular, we see U is orthogonal to U_1. So $W = U + U_1$ is totally singular. It follows that $W_1, \ldots, W_5 \subseteq W$ are totally singular and hence in S. So if $S' = S$ then we are done. Now suppose S' is the set of complements of W_0 in V. So V is in Case **L**. Choose $z \in W$ such that $\langle z\rangle = W_0 \cap W$. As $U_2 \in S'$, we know $U_2 = \ker(u_0)$ is a complement of W_0 in V, or equivalently, $u_0(z) \neq 0$. On the other hand, we have $v_1(z) = 0$ since $v_1 \in W_0'$. So $u_1 = u_0 + v_1$ satisfies $u_1(z) \neq 0$, i.e., $W_1 = \ker(u_1)$ is a complement of W_0 in V. So $W_1 \in S'$. The same argument shows $W_2, \ldots, W_5 \in S'$.

Now assume the subspaces in S are non-degenerate. So V is in Case **S**, **U** or **O**, and $S' = S$. Then the form $F|_U : U \times U \to \mathbb{F}_q$ is non-degenerate. (Here F is the associated bilinear form of Q if V is in Case **O**.) So the map $\phi : y \mapsto (x \mapsto F(x, y))$ is an $\mathbb{F}_p$-linear invertible map from U to U^*. It is also $\mathbb{F}_q$-linear if V is in Cases **S** and **O** since F is bilinear in these cases. When V is in Case **U**, the condition $\phi(\lambda y) = \lambda\phi(y)$ needs to be replaced by $\phi(\lambda y) = \lambda^{q^{1/2}}\phi(y)$ since F is a Hermitian form. We say ϕ is *twisted-linear* in this case.

For $L = \phi(y) \in U^*$, we have $\ker(L)^\perp \cap U = \langle y\rangle = \langle \phi^{-1}(L)\rangle$ since $x \in U$ is in $\ker(L)^\perp$ iff $F(z, x) = 0$ for all $z \in U$ satisfying $F(z, y) = 0$.

We verify that $W_4 = \ker(u_0 + \alpha v_1)$ is in S. The proofs for the other W_i are similar. Choose $t \in W - U$ orthogonal to U, which is possible since U is non-degenerate. Then W is the orthogonal direct sum of U and $\langle t\rangle$. So we may regard U^*, $\langle t\rangle^*$ as subgroups of W^*, where every $L \in U^*$ vanishes on $\langle t\rangle$ and every $L \in \langle t\rangle^*$ vanishes on U. Each $L \in W^*$ then uniquely decomposes into $L = L|_U + L|_{\langle t\rangle}$. Note $\langle t\rangle = U^\perp \cap W$. So the hyperplane W_0' of W^* is just U^*. Thus we may regard $v_1, v_2 \in W_0'$ as members of U^*, which vanish on $\langle t\rangle$.

Note $\phi^{-1}(u_0|_U + \alpha v_1) = \phi^{-1}(u_0|_U) + \alpha'\phi^{-1}(v_1)$ by (twisted-)linearity of ϕ, where $\alpha' = \alpha$ if V is in Cases **S** and **O** and $\alpha' = \alpha^{q^{1/2}}$ if V is in Case **U**. Recall that $\langle u_0^* \rangle = \ker(u_0|_U)^\perp \cap U$. On the other hand, we know $\ker(u_0|_U)^\perp \cap U = \langle \phi^{-1}(u_0|_U) \rangle$. So $\langle \phi^{-1}(u_0|_U) \rangle = \langle u_0^* \rangle$. By definition, there exists a singular vector v_1^* such that $\langle v_1^* \rangle = \ker(v_1|_U)^\perp \cap U = \ker(v_1)^\perp \cap U$. Then similarly, $\langle \phi^{-1}(v_1) \rangle = \langle v_1^* \rangle$ and hence $\phi^{-1}(v_1)$ is singular. As $v_1(u_0^*) = 0$, we have $u_0^* \in \ker(v_1)$. As $\langle v_1^* \rangle = \ker(v_1)^\perp \cap U$, we have $u_0^* \perp v_1^*$. So $\phi^{-1}(u_0|_U) \perp \phi^{-1}(v_1)$. Combine this with the fact $\phi^{-1}(v_1)$ is singular, we see $\phi^{-1}(u_0|_U + \alpha v_1) = \phi^{-1}(u_0|_U) + \alpha'\phi^{-1}(v_1)$ is isometric to $\phi^{-1}(u_0|_U)$. By Witt's Lemma, there exists an isometry $\tau : U \to U$ that sends $\phi^{-1}(u_0|_U)$ to $\phi^{-1}(u_0|_U + \alpha v_1)$. As t is orthogonal to U, we may extend τ to an isometry $\sigma' : W \to W$ that fixes t. Then σ' fixes the two orthogonal summands U and $\langle t \rangle$ of W.

We claim $\tau'(\ker(u_0)) \subseteq \ker(u_0 + \alpha v_1)$. To see this, consider $x \in \ker(u_0)$. Write $x = x_1 + x_2$ such that $x_1 \in U$ and $x_2 \in \langle t \rangle$. Then

$$0 = u_0(x) = u_0|_U(x_1) + u_0|_{\langle t \rangle}(x_2) = F(x_1, \phi^{-1}(u_0|_U)) + u_0|_{\langle t \rangle}(x_2)$$

and we have

$$\begin{aligned}
(u_0 + \alpha v_1)(\tau'(x)) &= (u_0|_U + \alpha v_1)(\tau(x_1)) + u_0|_{\langle t \rangle}(\tau'(x_2)) \\
&= F(\tau(x_1), \phi^{-1}(u_0|_U + \alpha v_1)) + u_0|_{\langle t \rangle}(x_2) \\
&= F(\tau(x_1), \tau(\phi^{-1}(u_0|_U))) + u_0|_{\langle t \rangle}(x_2) \\
&= F(x_1, \phi^{-1}(u_0|_U)) + u_0|_{\langle t \rangle}(x_2) \\
&= 0.
\end{aligned}$$

So $\tau'(\ker(u_0)) \subseteq \ker(u_0 + \alpha v_1)$, as claimed. Therefore τ' restricts to an isometry from $\ker(u_0) = U_2$ to $\ker(u_0 + \alpha v_1) = W_4$, which implies $W_4 \in S$. □

Proof of Lemma 6.49. It is easy to see that $\mathrm{Hol}(T)$ is of diagonal type on T. This follows by considering the inclusion $\mathrm{Hol}(T) \hookrightarrow \mathrm{Aut}(T)^2$ given by $gh \mapsto (\tau_g h, h)$ for $g \in T$ and $h \in \mathrm{Aut}(T)$, where τ_g denotes the inner automorphism $x \mapsto gxg^{-1}$. So $\mathrm{Hol}(T) \wr \mathrm{Sym}(k) = \mathrm{Hol}(T)^k \rtimes \mathrm{Sym}(k)$ is of product type on T^k.

Note that $G = B \rtimes P$ is a permutation group on the set B via ${}^{f\pi}g = f\,{}^{\pi}g$ for $f, g \in B$ and $\pi \in P$. As the stabilizer of $e \in B$ is P, this action is equivalent to the action of G on $S = G/P$. We will prove the lemma for G as a permutation group on B instead of on S.

Pick $g_1, \ldots, g_k \in P$ such that ${}^{g_i}1 = i \in [k]$. Then $g_1, \ldots, g_k$ form a complete set of representatives of P/P_1. Identify B with T^k via the group isomorphism $\phi : B \to T^k$ sending $f \in B$ to $(f(g_1), \ldots, f(g_k))$. Similarly, we identify $G = B \rtimes P$ with $T^k \rtimes P$. Then G becomes a permutation group on T^k. Note $T^k \leq G$ and $T^k \leq \mathrm{Hol}(T)^k \leq \mathrm{Hol}(T) \wr P$ both act on T^k itself by left translation. Next, we determine how $P \leq G$ acts on T^k. Let $\pi \in P$ and $i \in [k]$. By definition, $({}^{\pi}f)(g_i) = f(\pi^{-1}g_i)$ for $f \in B$. As $\pi^{-1}g_i$ and $g_{\pi^{-1}i}$ both send 1 to ${}^{\pi^{-1}}i \in [k]$, we have $\pi^{-1}g_i P_1 = g_{\pi^{-1}i} P_1$. So $\pi^{-1}g_i = g_{\pi^{-1}i} h_i^{-1}$ for some $h_i \in P_1$. Then $({}^{\pi}f)(g_i) = f(g_{\pi^{-1}i} h_i^{-1}) = {}^{\varphi(h_i)}f(g_{\pi^{-1}i})$ by definition. So $\pi \in P \leq G$, as a permutation on T^k, coincides with $(\varphi(h_1), \ldots, \varphi(h_k))\pi \in \mathrm{Hol}(T) \wr P$. It follows that the permutation group G can be embedded in $\mathrm{Hol}(T) \wr P$. □

References

[AG84] M. Aschbacher and R. Guralnick. Some applications of the first cohomology group. *Journal of Algebra*, 90(2):446–460, 1984.

[AIKS14] M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena. Deterministic polynomial factoring and association schemes. *LMS Journal of Computation and Mathematics*, 17(01):123–140, 2014.

[AMM77] L. Adleman, K. Manders, and G. Miller. On taking roots in finite fields. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 175–178, 1977.

[Aro13] M. Arora. *Extensibility of association schemes and GRH-based deterministic polynomial factoring*. PhD thesis, Universitäts-und Landesbibliothek Bonn, 2013.

[Asc84] M. Aschbacher. On the maximal subgroups of the finite classical groups. *Inventiones Mathematicae*, 76(3):469–514, 1984.

[Asc00] M. Aschbacher. *Finite Group Theory*. Cambridge University Press, 2000.

[Asc08] M. Aschbacher. The subgroup structure of finite alternating and symmetric groups. *Lecture Notes for the Summer School on Finite Groups and Related Geometrical Structures*, 2008.

[BCP82] L. Babai, P. J. Cameron, and P. P. Pálfy. On the orders of primitive groups with restricted nonabelian composition factors. *Journal of Algebra*, 79(1):161–168, 1982.

[Ben05] C. Benbenisty. *On actions of primitive groups*. PhD thesis, Hebrew University of Jerusalem, 2005.

[Ber67] E. R. Berlekamp. Factoring polynomials over finite fields. *Bell System Technical Journal*, 46(8):1853–1859, 1967.

[Ber68] E. R. Berlekamp. *Algebraic Coding Theory*. World Scientific, 1968.

[Ber70] E. R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24(111):713–735, 1970.

[BKS15] J. Bourgain, S. Konyagin, and I. Shparlinski. Character sums and deterministic polynomial root finding in finite fields. *Mathematics of Computation*, 84(296):2969–2977, 2015.

[CCNP85] J. H. Conway, R. T. Curtis, S. P. Norton, and R. A. Parker. *ATLAS of Finite Groups*. Oxford University Press, 1985.

[CH00] Q. Cheng and M. A. Huang. Factoring polynomials over finite fields and stable colorings of tournaments. In *Proceedings of the 4th Algorithmic Number Theory Symposium*, pages 233–245, 2000.

[Coo78] B. N. Cooperstein. Minimal degree for a permutation representation of a classical group. *Israel Journal of Mathematics*, 30(3):213–235, 1978.

[CR88] B. Chor and R. L. Rivest. A knapsack-type public key cryptosystem based on arithmetic in finite fields. *IEEE Transactions on Information Theory*, 34(5):901–909, 1988.

[CZ81] D. G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36(154):587–592, 1981.

[DM96] J. D. Dixon and B. Mortimer. *Permutation Groups*. Springer, 1996.

[Dye80] R. H. Dye. On the maximality of the orthogonal groups in the symplectic groups in characteristic two. *Mathematische Zeitschrift*, 172(3):203–212, 1980.

[Evd92] S. A. Evdokimov. Factorization of solvable polynomials over finite fields and the generalized Riemann hypothesis. *Journal of Soviet Mathematics*, 59(3):842–849, 1992.

[Evd94] S. A. Evdokimov. Factorization of polynomials over finite fields in subexponential time under GRH. In *Proceedings of the 1st Algorithmic Number Theory Symposium*, pages 209–219, 1994.

[Gao01] S. Gao. On the deterministic complexity of factoring polynomials. *Journal of Symbolic Computation*, 31(1):19–36, 2001.

[GSS98] D. Gluck, Á. Seress, and A. Shalev. Bases for primitive permutation groups and a conjecture of Babai. *Journal of Algebra*, 199(2):367–378, 1998.

[Gua09] Y. Guan. *Factoring polynomials and Grobner bases*. PhD thesis, Clemson University, 2009.

[Guo17] Z. Guo. *$\mathcal{P}$-schemes and deterministic polynomial factoring over finite fields*. PhD thesis, Caltech, 2017.

[Guo19] Z. Guo. Factoring polynomials over finite fields with linear Galois groups: an additive combinatorics approach, 2019. Manuscript. `https://zeyuguo.bitbucket.io/papers/linear.pdf`.

[Guo20] Z. Guo. Deterministic polynomial factoring over finite fields: a uniform approach via $\mathcal{P}$-schemes. *Journal of Symbolic Computation*, 96:22–61, 2020. To appear. `https://doi.org/10.1016/j.jsc.2019.02.011`.

[HLM19] Z. Halasi, M. W. Liebeck, and A. Maróti. Base sizes of primitive groups: bounds with explicit constants. *Journal of Algebra*, 521:16–43, 2019.

[Hua91a] M. A. Huang. Factorization of polynomials over finite fields and decomposition of primes in algebraic number fields. *Journal of Algorithms*, 12(3):482 – 489, 1991.

[Hua91b] M. A. Huang. Generalized Riemann hypothesis and factoring polynomials over finite fields. *Journal of Algorithms*, 12(3):464 – 481, 1991.

[IKRS12] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. *Mathematics of Computation*, 81(277):493–531, 2012.

[IKS09] G. Ivanyos, M. Karpinski, and N. Saxena. Schemes for deterministic polynomial factoring. In *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*, pages 191–198, 2009.

[Kal85] E. Kaltofen. Polynomial-time reductions from multivariate to bi-and univariate integral polynomial factorization. *SIAM Journal on Computing*, 14(2):469–489, 1985.

[Kal03] E. Kaltofen. Polynomial factorization: a success story. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 3–4, 2003.

[KL90] P. B. Kleidman and M. W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. Cambridge University Press, 1990.

[KM00] J. Klüners and G. Malle. Explicit Galois realization of transitive groups of degree up to 15. *Journal of Symbolic Computation*, 30(6):675–716, 2000.

[KP00] L. G. Kovács and C. E. Praeger. On minimal faithful permutation representations of finite groups. *Bulletin of the Australian Mathematical Society*, 62(02):311–317, 2000.

[KS98] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Mathematics of Computation*, 67(223):1179–1197, 1998.

[KT90] E. Kaltofen and B. M. Trager. Computing with polynomials given by black boxes for their evaluations: Greatest common divisors, factorization, separation of numerators and denominators. *Journal of Symbolic Computation*, 9(3):301–320, 1990.

[KU11] K. S. Kedlaya and C. Umans. Fast polynomial factorization and modular composition. *SIAM Journal on Computing*, 40(6):1767–1802, 2011.

[Lan85] S. Landau. Factoring polynomials over algebraic number fields. *SIAM Journal on Computing*, 14(1):184–195, 1985.

[Lan02] S. Lang. *Algebra*. Springer, 2002.

[Len83] A. K. Lenstra. Factoring polynomials over algebraic number fields. *Computer Algebra*, pages 245–254, 1983.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4):515–534, 1982.

[LM85] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *Journal of Computer and System Sciences*, 30(2):179–208, 1985.

[LPS88] M. W. Liebeck, C. E. Praeger, and J. Saxl. On the O'Nan-Scott theorem for finite primitive permutation groups. *Journal of the Australian Mathematical Society (Series A)*, 44(03):389–396, 1988.

[LS91] M. W. Liebeck and J. Saxl. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proceedings of the London Mathematical Society*, 3(2):266–314, 1991.

[LS99] M. W. Liebeck and A. Shalev. Simple groups, permutation groups, and probability. *Journal of the American Mathematical Society*, 12(2):497–520, 1999.

[LS02] M. W. Liebeck and A. Shalev. Bases of primitive linear groups. *Journal of Algebra*, 252(1):95–113, 2002.

[LS03] A. Lubotzky and D. Segal. *Subgroup Growth*. Birkhäuser, 2003.

[LS14] M. W. Liebeck and A. Shalev. Bases of primitive linear groups II. *Journal of Algebra*, 403:223–228, 2014.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Elsevier, 1977.

[Neu63] B. H. Neumann. Twisted wreath products of groups. *Archiv der Mathematik*, 14(1):1–6, 1963.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.

[Odl85] A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In *Advances in Cryptology: Proceedings of EUROCRYPT 84*, pages 224–314, 1985.

[Pat72] W. H. Patton. *The minimum index for subgroups in some classical groups: a generalization of a theorem of Galois*. PhD thesis, University of Illinois at Chicago, 1972.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

[Pra90] C. E. Praeger. The inclusion problem for finite primitive permutation groups. *Proceedings of the London Mathematical Society*, 3(1):68–88, 1990.

[Rón88] L. Rónyai. Factoring polynomials over finite fields. *Journal of Algorithms*, 9(3):391–400, 1988.

[Rón89] L. Rónyai. Factoring polynomials modulo special primes. *Combinatorica*, 9(2):199–206, 1989.

[Rón92] L. Rónyai. Galois groups and factoring polynomials over finite fields. *SIAM Journal on Discrete Mathematics*, 5(3):345–365, 1992.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985.

[Sho90] V. Shoup. On the deterministic complexity of factoring polynomials over finite fields. *Information Processing Letters*, 33(5):261–267, 1990.

[Sho91] V. Shoup. Smoothness and factoring polynomials over finite fields. *Information Processing Letters*, 38(1):39–42, 1991.

[Sup76] D. A. Suprunenko. *Matrix Groups*. American Mathematical Society, 1976.

[Uma08] C. Umans. Fast polynomial factorization and modular composition in small characteristic. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing*, pages 481–490, 2008.

[vzG87] J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52(1):77–89, 1987.

[vzGG13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, 2013.

[vzGP01] J. von zur Gathen and D. Panario. Factoring polynomials over finite fields: A survey. *Journal of Symbolic Computation*, 31(1-2):3–17, 2001.

[vzGS92] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Computational Complexity*, 2(3):187–224, 1992.

[Wie64] H. Wielandt. *Finite Permutation Groups*. Academic Press, 1964.