$\mathcal{P}$-schemes: a unifying framework for deterministic polynomial factoring over finite fields

(research summary)

Zeyu Guo

Abstract

We introduce a family of mathematical objects called *$\mathcal{P}$-schemes*, generalizing the notions of association schemes and m-schemes [IKS09]. Based on these objects, we develop a unifying framework for deterministic polynomial factoring over finite fields under the generalized Riemann hypothesis (GRH). It allows us to not only recover most of the known results but also discover new ones. In particular, we prove that a polynomial $f(X) \in \mathbb{F}_p[X]$ can be factorized in polynomial time given an irreducible polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ lifting $f(X)$ whose Galois group is in Γ_k for $k = 2^{O(\sqrt{\log n})}$, where Γ_k denotes the family of finite groups whose noncyclic composition factors are isomorphic to subgroups of $\mathrm{Sym}(k)$. Previously this was known only for bounded k.

We also initiate an approach towards the schemes conjecture in [IKS09] by introducing analogous conjectures about $\mathcal{P}$-schemes with respect to various families of permutation groups. The conjectures form a hierarchy of relaxations of the schemes conjecture and have consequences on deterministic polynomial factoring over finite fields.

1 Introduction

We study the problem of *polynomial factoring* over finite fields: Given a monic polynomial $f(X) \in \mathbb{F}_q[X]$ of degree n, where $\mathbb{F}_q$ is the finite field of cardinality q, we want to factorize $f(X)$ into irreducible polynomials over $\mathbb{F}_q$ in polynomial time:

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

As it takes $O(n \log q)$ bits to describe $f(X)$, a truly polynomial-time factoring algorithm should run in time $(n \log q)^{O(1)}$. If randomness is allowed, such efficient algorithms are well known [Ber67; CZ81; GS92; KS98; KU11]. For *deterministic* factoring, a lot of algorithms were proposed with various running time and assumptions [Ber67; Ber70; AMM77; Sch85; Gat87;

MS88; Rón88; Rón89; Pil90; Sho90; Sho91; Hua91a; Hua91b; Rón92; Evd92; Evd94; CH00; BGL01; Gao01; Sah08; IKS09; IKRS12; Aro13; AIKS14; BKS15; GHL16]. However, despite much effort, it remains a long-standing open problem to find a deterministic polynomial-time factoring algorithm, even assuming standard number-theoretic assumptions like the generalized Riemann hypothesis (GRH). Currently, the best known deterministic algorithm (assuming GRH) runs in time $(n^{\log n} \log q)^{O(1)}$, given by Evdokimov [Evd94].

In this project, we make progress towards solving this problem by introducing a family of mathematical objects called $\mathcal{P}$*-schemes*, and using them to develop a unifying framework for deterministic polynomial factoring. This framework allows us to not only recover most of the known results but also discover new ones. Along the way, we develop a theory of $\mathcal{P}$-schemes that not only has applications to deterministic polynomial factoring but also has natural connections to other objects in algebra and combinatorics like permutation groups, association schemes and m-schemes.

GRH is commonly assumed in the literature for deterministic polynomial factoring, and we assume it as well.[1] For simplicity, assume $\mathbb{F}_q$ is a prime field $\mathbb{F}_p$. Like the algorithms in [Hua91a; Hua91b; Evd92; Rón92], our factoring algorithm employs a polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of degree $n = \deg(f(X))$ satisfying $\tilde{f}(X) \bmod p = f(X)$, called a *lifted polynomial* of $f(X)$. Such a lifted polynomial can always be obtained by simply lifting $f(X)$ to $\mathbb{Z}[X]$. Moreover, we may assume it is irreducible.[2] One of our results relates the complexity of deterministically factoring $f(X)$ to the complexity of the Galois group G of $\tilde{f}(X)$ in terms of its noncyclic composition factors. In particular, we obtain a deterministic polynomial-time factoring algorithm for the case $G \in \Gamma_k$, $k = 2^{O(\sqrt{\log n})}$, where Γ_k denotes the family of finite groups whose noncyclic composition factors are isomorphic to subgroups of $\mathrm{Sym}(k)$.

We also investigate the *schemes conjecture* proposed in [IKS09], whose positive resolution would solve the problem of deterministic polynomial factoring over finite fields in polynomial time under GRH. Using the notion of $\mathcal{P}$-schemes, we formulate analogous conjectures for various families of finite permutation groups, which have applications on deterministic polynomial factoring as well. Moreover, we show that these conjectures in fact form a hierarchy of relaxations of the schemes conjecture in [IKS09]. Thus a natural approach towards the schemes conjecture is to first study these relaxations, and we believe that progress on the later may indeed shed some light on the original schemes conjecture.

While we limit our discussion to the case $\mathbb{F}_q = \mathbb{F}_p$ for simplicity, our results hold for any finite field $\mathbb{F}_q$, where the coefficients of $\tilde{f}(X)$ take values in a number ring instead of $\mathbb{Z}$ in general.

[1] Unconditionally, even finding a deterministic factoring algorithm for quadratic polynomials over $\mathbb{F}_p$ that runs in time $p^{o(1)}$ is a open problem.

[2] If $\tilde{f}(X)$ is reducible, we compute the factorization $\tilde{f}(X) = \prod_i \tilde{g}_i(X)$ over $\mathbb{Q}$ using the classical LLL algorithm [LLL82] and reduce to the subproblem for each $g_i(X) := \tilde{g}_i(X) \bmod p$ and the irreducible lifted polynomial $\tilde{g}_i(X)$.

2 Galois groups, m-schemes, and $\mathcal{P}$-schemes

Our framework is inspired by two approaches to deterministic polynomial factoring. One of them is Galois-theoretic and group-theoretic, whereas the other is more combinatorial.

The Galois-theoretic approach [Hua91a; Hua91b; Evd92; Rón92] uses a lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of $f(X)$ as we do. Let G be the Galois group of $\tilde{f}(X)$, i.e., $G = \mathrm{Gal}(L/\mathbb{Q})$ where L is the splitting field of $\tilde{f}(X)$. Huang [Hua91a; Hua91b] gave a deterministic algorithm that factorizes $f(X)$ in polynomial time provided that G is abelian, and it was later extended to the case that G is solvable [Evd92]. For general G, Rónyai [Rón92] described a deterministic algorithm running in time polynomial in n, $\log p$ and $|G|$.

On the other hand, Evdokimov [Evd94] as well as its precursor [Rón88] took a different approach that uses tensor powers of the ring $\mathbb{F}_p[X]/(f(X))$ instead of lifted polynomials or Galois groups, leading to Evdokimov's quasipolynomial-time algorithm [Evd94]. Efforts were made to understand the combinatorics behind these algorithms [CH00; Gao01; IKS09]. In particular, the work [IKS09] introduced a family of combinatorial objects called *m-schemes*, parameterized by $m \in \mathbb{N}^+$, that generalize the central and well-studied notion of *association schemes* in algebraic combinatorics [BI84]. As noted in [IKS09], the correctness of Evdokimov's algorithm is explained by the fact that for sufficiently large $m = O(\log n)$, there exists no m-scheme on $[n]$ satisfying some special properties called *antisymmetry* and the *nonexistence of a matching*.

$\mathcal{P}$-schemes. Our notion of $\mathcal{P}$-schemes can be seen as a further generalization of m-schemes, which exhibits both group-theoretic and combinatorial flavors. Given a finite group G and a poset $\mathcal{P}$ of subgroups of G, we define a $\mathcal{P}$-scheme to be a collection of partitions

$$\mathcal{C} = \{C_H : H \in \mathcal{P}\}$$

satisfying certain constraints, where each C_H is a partition of the right coset space $H\backslash G = \{Hg : g \in G\}$. The formal definition of a $\mathcal{P}$-scheme is omitted in this summary and can be found in Chapter 2 of the author's PhD thesis [Guo17].

When G is chosen to be a symmetric group and $\mathcal{P}$ is a poset of *stabilizer subgroups* (with respect to the natural action of G), we recover the definition of m-schemes:

Theorem 1 (informal)**.** *A $\mathcal{P}$-scheme is equivalent to an m-scheme on $[n]$ if $G = \mathrm{Sym}(n)$ acts naturally on $[n]$ and $\mathcal{P}$ consists of the (pointwise) stabilizers G_T for $T \subseteq [n]$ and $1 \le |T| \le m$.*

See [Guo17, Theorem 2.1] for the formal statement.

In this way, we regard the theory of m-schemes as part of the richer theory of $\mathcal{P}$-schemes. The advantage of adopting the notion of $\mathcal{P}$-schemes is that these objects capture not only the combinatorial structure of m-schemes but also the information provided by the group G and the

poset $\mathcal{P}$, which allows us to carry out both the Galois-theoretic/group-theoretic approach and the combinatorial approach in a uniform way.

3 Deterministic polynomial factoring via $\mathcal{P}$-schemes

The theory of $\mathcal{P}$-schemes is applied to deterministic polynomial factoring as follows. Suppose an irreducible polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ lifting $f(X) \in \mathbb{F}_p[X]$ is given. Let L be the splitting field of $\tilde{f}(X)$ over $\mathbb{Q}$ and let $G = \mathrm{Gal}(L/\mathbb{Q})$. By Galois theory, we have an one-to-one correspondence between the subgroups of G and the subfields of L

$$H = \mathrm{Gal}(L/K) \longleftrightarrow K = L^H$$

where L^H denotes the fixed field of H. Thus any poset $\mathcal{P}$ of subgroups of G corresponds to a poset $\mathcal{P}^\sharp := \{L^H : H \in \mathcal{P}\}$ of subfields of L.

Roughly speaking, our algorithm proceeds by (1) constructing a poset $\mathcal{P}^\sharp$ of subfields of L, (2) computing a certain "ring decomposition" for each subfield $K \in \mathcal{P}^\sharp$, and (3) extracting a factorization of $f(X)$ from these ring decompositions.

We show that the algorithm always produces the desired factorization of $f(X)$, unless the ring decompositions induce a very special $\mathcal{P}$-scheme, characterized by certain properties called *strong antisymmetry* and *(non-)discreteness*. Thus the correctness of the algorithm would hold if we rule out the existence of such a $\mathcal{P}$-scheme. This is formulated by the following theorem as one of our main results.

Theorem 2 (informal)**.** *Let $f(X) \in \mathbb{F}_p[X]$ be a polynomial of degree n and let $\tilde{f}(X)$, L, G be as above. Let $G_0 = \mathrm{Gal}(L/\mathbb{Q}(\alpha))$ where α is a root of $\tilde{f}(X)$ in L. Suppose $\mathcal{P} \ni G_0$ is a poset of subgroups of G such that*

- *the poset $\mathcal{P}^\sharp$ of subfields can be constructed in time T, and*
- *all strongly antisymmetric $\mathcal{P}$-schemes are discrete on G_0.*

Then given $\tilde{f}(X)$, the polynomial $f(X)$ can be fully factorized in time polynomial in n, $\log p$, and T, assuming GRH.

For the formal statement, see [Guo17, Theorem 3.9] for the case that $f(X)$ factorizes into n distinct linear factors, and [Guo17, Theorem 5.9] for the general case.

Theorem 2 is a generic result: We may choose various posets $\mathcal{P}$ of subgroups to obtain different specific algorithms, as long as the subfields in $\mathcal{P}^\sharp$ can be effectively constructed. By choosing various $\mathcal{P}$ and verifying the conditions in Theorem 2, we easily recover the aforementioned results obtained by the Galois-theoretic approach [Hua91a; Hua91b; Evd92; Rón92]. More specifically,

the factoring algorithm for abelian groups [Hua91a; Hua91b] and that for general groups [Rón92] both correspond to the case that $\mathcal{P}$ consists of the trivial subgroup and the conjugates of G_0 in G. For a solvable Galois group G, we construct the poset $\mathcal{P}^\sharp$ of subfields using a technique in [LM85; Evd92] that has the effect of replacing G with its primitive components. It was introduced in [LM85] for the problem of solvability testing of Galois groups and later used in [Evd92] for deterministic polynomial factoring. Constructing $\mathcal{P}^\sharp$ in this way yields a polynomial-time factoring algorithm for solvable groups, reproving the main result of [Evd92].

The connection with m-schemes. Now we explain the connection between $\mathcal{P}$-schemes and m-schemes, and use it to reprove Evdokimov's result that deterministic polynomial factoring can be solved in quasipolynomial time. Let $\tilde{f}(X)$, L, G be as above. Denote by $S = \{\alpha_1, \ldots, \alpha_n\}$ the set of roots of $\tilde{f}(X)$ in L, so that G is a permutation group on S. One possible choice of $\mathcal{P}$ is a poset of stabilizers

$$\mathcal{P}_m := \{G_T : T \subseteq S, 1 \leq |T| \leq m\}$$

for some $m \in \mathbb{N}^+$, with respect to the action of G on S. The corresponding poset $\mathcal{P}^\sharp$ of subfields consists of the fields $\mathbb{Q}(\alpha_{i_1}, \ldots, \alpha_{i_k})$ obtained by adjoining k roots of $\tilde{f}(X)$ where $1 \leq k \leq m$.

We want to apply Theorem 2 with $\mathcal{P} = \mathcal{P}_m$ for a suitably chosen integer m to obtain a factoring algorithm. In order to bound the time complexity, we want m to be small (ideally a constant), while at the same time the condition on $\mathcal{P}$-schemes in Theorem 2 needs to be satisfied. We introduce the notation $d(G)$ for the smallest $m \in \mathbb{N}^+$ satisfying this condition:

Definition 1. *For a permutation group G on a finite set S, define $d(G)$ to be the smallest integer $m \in \mathbb{N}^+$ such that for $\mathcal{P} = \mathcal{P}_m$ and all $\alpha \in S$, all strongly antisymmetric $\mathcal{P}$-schemes are discrete on the stabilizer $G_\alpha \in \mathcal{P}$.*

Then we are led to the following problem.

Problem 1. *Let G be a permutation group on a finite set S of cardinality $n \in \mathbb{N}^+$. Prove an upper bound for $d(G)$ in terms of n.*

When G is the full symmetric group $\mathrm{Sym}(S) \cong \mathrm{Sym}(n)$, a $\mathcal{P}$-scheme with $\mathcal{P} = \mathcal{P}_m$ is equivalent to an m-scheme by Theorem 1. Thus Problem 1 reduces to a problem about m-schemes. The latter problem is addressed in [Evd94; IKS09; Aro13], leading to a bound $d(G) = O(\log n)$. In general, G is only a subgroup of $\mathrm{Sym}(S)$. One of our key results is that $G = \mathrm{Sym}(S)$ is actually the worst case, as implied by the following lemma.

Lemma 1. *Let G be a permutation group on S and let G' be a subgroup of G. Let*

$$\mathcal{P} = \{G_T : T \subseteq S, 1 \leq |T| \leq m\} \quad \textit{and} \quad \mathcal{P}' = \{G'_T : T \subseteq S, 1 \leq |T| \leq m\}$$

for some $m \in \mathbb{N}^+$. If there exists a strongly antisymmetric $\mathcal{P}'$-scheme that is not discrete on G'_α for some $\alpha \in S$, there also exists a strongly antisymmetric $\mathcal{P}$-scheme that is not discrete on G_α.

See [Guo17, Corollary 6.2]. By Lemma 1, we have $d(G) = O(\log n)$ for any permutation group G on a finite set S of cardinality n. Thus Theorem 2 allows us to factorize $f(X)$ in time polynomial in $n^{\log n}$ and $\log p$, which recovers Evdokimov's result [Evd94; IKS09].

While this result is old, the new insight we obtain is that Evdokimov's algorithm [Evd94] and its interpretation in terms of m-schemes [IKS09] become more natural when viewed from a Galois-theoretic perspective, where they address the (worst) case of symmetric groups.

4 Towards the schemes conjecture

The work [IKS09] proposed a combinatorial conjecture on m-schemes, called the *schemes conjecture*, whose positive resolution would imply a deterministic polynomial-time factoring algorithm under GRH. Proving this conjecture appears to be difficult. However, as noted in Section 3, an m-scheme is essentially a $\mathcal{P}$-scheme in the (worst) case of symmetric groups, with respect to a poset $\mathcal{P}$ of pointwise stabilizers. This observation suggests that one should first formulate and attack the analogous conjectures for "less complex" Galois groups.

In the following, we formulate the analogous conjectures for families of permutation groups and observe that they form a hierarchy of relaxations of the original schemes conjecture in [IKS09]. We hope that the study of these relaxations may shed some light on the original schemes conjecture and provide a way towards the resolution of deterministic polynomial factoring.

Let $\mathcal{G}$ be a family of finite permutation groups. We formulate the *schemes conjecture for* $\mathcal{G}$ as follows.

Conjecture 1 (schemes conjecture for $\mathcal{G}$)**.** *There exists a constant $c > 0$ such that $d(G) \leq c$ for all $G \in \mathcal{G}$.*

See [Guo17, Conjecture 6.3]. Denote by $\mathcal{G}_{\mathrm{Sym}}$ the family of symmetric groups $\mathrm{Sym}(n)$ acting naturally on $[n]$ where n ranges over $\mathbb{N}^+$. It can be shown that the schemes conjecture for $\mathcal{G}_{\mathrm{Sym}}$ is a relaxation of the original schemes conjecture.

There exist reductions among the schemes conjectures for various families of finite permutation groups: For two families $\mathcal{G}$ and $\mathcal{G}'$, write $\mathcal{G} \preceq \mathcal{G}'$ if every member G of $\mathcal{G}$ is permutation isomorphic[3] to a subgroup of some $G' \in \mathcal{G}'$. Then $\preceq$ is a partial order on the set of families of finite permutation groups. The following lemma holds by Lemma 1.

Lemma 2. *The schemes conjecture for $\mathcal{G}$ is implied by that for $\mathcal{G}'$ if $\mathcal{G} \preceq \mathcal{G}'$.*

See [Guo17, Theorem 6.4]. Note that $\mathcal{G} \preceq \mathcal{G}_{\mathrm{Sym}}$ holds for any family $\mathcal{G}$ of finite permutation groups. So the schemes conjectures defined above form a hierarchy of relaxations of the original schemes conjecture in [IKS09], among which $\mathcal{G}_{\mathrm{Sym}}$ is the most difficult one.

[3]Two permutation groups G and G' on sets S and S' respectively are *permutation isomorphic* if there exist a group isomorphism $\rho : G \to G'$ and a bijection $\phi : S \to S'$ satisfying $\phi(gx) = \rho(g)\phi(x)$ for $g \in G$ and $x \in S$.

Thus one approach towards the original conjecture is to first investigate its relaxations in this hierarchy, which are formally easier to prove. Indeed, it can be shown that the schemes conjecture for $\mathcal{G}$ is true whenever the *minimal base sizes* of all $G \in \mathcal{G}$ are bounded by a constant. This includes the case that $\mathcal{G}$ is a family of primitive solvable permutation groups, for example [Ser96].

So we are led to investigate the schemes conjectures for families of permutation groups with unbounded minimal base sizes. A particularly interesting case is the family of finite general linear groups $\mathrm{GL}(V)$ acting naturally on $V - \{0\}$ of cardinality $n = |V| - 1$ for which the corresponding schemes conjecture is open. In fact, it is not known if the upper bound $d(G) = O(\log n)$ (which holds by the analysis for symmetric groups) can be improved. We believe that obtaining such an improvement is within reach, and it would be a first step towards proving the schemes conjecture for the family of general linear groups:

> *Prove that there exists a function $m(n) = o(\log n)$ such that for any finite general linear group $G = \mathrm{GL}(V)$ acting naturally on $S := V - \{0\}$ of cardinality $n = |V| - 1$, it holds that $d(G) \leq m(n)$.*

Finally, we note that by Theorem 2, our schemes conjectures imply deterministic polynomial factoring algorithms for various families of Galois groups:

Theorem 3 (informal)**.** *Let $\mathcal{G}$ be a family of finite permutation groups, and assume the schemes conjecture for $\mathcal{G}$ is true. Let $f(X) \in \mathbb{F}_p[X]$ and let $\tilde{f}(X), L, G$ be as in Theorem 2. Then given $\tilde{f}(X)$, the polynomial $f(X)$ can be deterministically factorized in polynomial time provided that G acting on the set of roots of $\tilde{f}(X)$ in L is permutation isomorphic to some member of $\mathcal{G}$.*

For the formal statement, see [Guo17, Theorem 6.3].

5 Galois groups with restricted composition factors

Using our framework of $\mathcal{P}$-schemes, we also obtain new results on deterministic polynomial factoring, in particular a factoring algorithm for Galois groups with restricted *composition factors*, which we explain now.

Recall that a composition factor of a finite group is a *finite simple group*, and by the *classification of finite simple groups* (CFSG), it is isomorphic to one of the following groups: a cyclic group of prime order, an alternating group, a classical group, an exceptional group of Lie type, or one of the 26 sporadic simple groups. Denote by $\mathcal{S}(G)$ the set of composition factors of G. We give an algorithm whose running time is controlled by the alternating groups and the classical groups in $\mathcal{S}(G)$. The dependence on the classical groups is still under investigation, but for now we are able to prove a result in the following form.

Theorem 4. *Assuming GRH, there exists an algorithm that given $f(X) \in \mathbb{F}_p[X]$ and an irreducible lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of $f(X)$ with the Galois group G, fully factorizes*

$f(X)$ in time polynomial in n, $\log p$, $k(G)^{\log k(G)}$ and $r(G)$, where $k(G)$ denotes the maximum degree of the alternating groups in $\mathcal{S}(G)$ and $r(G)$ denotes the maximum order of the classical groups in $\mathcal{S}(G)$.

See [Guo17, Theorem 8.2]. The proof relies on Theorem 2 and employs various techniques and results in permutation group theory, including the O'Nan-Scott theorem for primitive permutation groups [LPS88] and results on the base size of primitive permutation groups [LS99; LS02; LS14].

Families Γ_k of finite groups. We apply Theorem 4 to the case $G \in \Gamma_k$, where Γ_k for $k \in \mathbb{N}^+$ denotes the family of finite groups whose noncyclic composition factors are isomorphic to subgroups of $\mathrm{Sym}(k)$. These families play a significant role in graph isomorphism testing [Luk82; Mil83], asymptotic group theory [BCP82; Pyb93; PS97] and computational group theory [Luk93; Ser03]. It is known that a classical group of order r lies in Γ_k only if $r = k^{O(\log k)}$ [Coo78]. So by Theorem 4, we have

Theorem 5. *Assuming GRH, there exists an algorithm that given $f(X) \in \mathbb{F}_p[X]$ of degree n and an irreducible lifted polynomial $\tilde{f}(X) \in \mathbb{Z}[X]$ of $f(X)$ with the Galois group G, fully factorizes $f(X)$ in time polynomial in n, $\log p$ and $k^{\log k}$, where k is the smallest positive integer satisfying $G \in \Gamma_k$. In particular, the algorithm runs in polynomial time if $k = 2^{O(\sqrt{\log n})}$.*

By Theorem 5, we have a deterministic polynomial-time algorithm that factorizes $f(X)$ given $\tilde{f}(X)$ whose Galois group is in Γ_k for $k = 2^{O(\sqrt{\log n})}$ (note that achieving $k = n$ would fully resolve the problem of deterministic polynomial factoring under GRH). Previously, such an algorithm was known only for bounded k: For $k \leq 4$ this follows directly from the deterministic polynomial-time factoring algorithm for solvable Galois groups [Evd92]. For $k = O(1)$, it follows from the proof in [Evd92] together with the bound in [BCP82] for the orders of primitive permutation groups. See Table 1 for a summary.

Table 1: Known deterministic polynomial-time factoring algorithms for Γ_k

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

6 A theory of $\mathcal{P}$-schemes

A significant part of our research is devoted to developing a theory of $\mathcal{P}$-schemes, which serves as the mathematical foundation of our framework of deterministic polynomial factoring. In the following, we discuss some aspects of the theory.

Constructing new $\mathcal{P}$-schemes from old. In [Guo17, Chapter 6], we develop various general techniques of constructing new $\mathcal{P}$-schemes from old ones, including

1. Restriction of $\mathcal{P}$-schemes.
2. Induction of $\mathcal{P}$-schemes.
3. Passing to a quotient subgroup.
4. Extension of $\mathcal{P}$-schemes.

The techniques above have a common form: They use a $\mathcal{P}$-schemes $\mathcal{C}$ to construct a $\mathcal{P}'$-scheme $\mathcal{C}'$, where $\mathcal{P}$ (resp. $\mathcal{P}'$) is a poset of subgroups of a group G (resp. G'). For example, in the first case (restriction of $\mathcal{P}$-schemes), the group G' is a subgroup of G, $\mathcal{P}'$ is the poset $\{H \in \mathcal{P} : H \subseteq G'\}$ of subgroups of G', and $\mathcal{C}'$ is called the *restriction* of $\mathcal{C}$ to G'. In the second case, we have $G' \supseteq G$ and $\mathcal{C}'$ is called the *induction* of $\mathcal{C}$ to $\mathcal{P}'$. In the third case, G' is a quotient group of G. And in the last one, we have $G = G'$ and $\mathcal{P}' \supseteq \mathcal{P}$.

These techniques are very useful for studying the existence of special $\mathcal{P}$-schemes for various groups G and posets $\mathcal{P}$ of subgroups of G, allowing us to reduce one case to another. For example, Lemma 1 is in fact a special form of the induction of $\mathcal{P}$-schemes.

In addition, we define two binary operations called the *direct product* and the *wreath product* of $\mathcal{P}$-schemes, generalizing the corresponding operations of permutation groups and association schemes [SS98; Bai04]. We also define the direct product and the wreath product of m-schemes, and use them to show that either the schemes conjecture in [IKS09] is true, or it has infinitely many counterexamples.

Orbit schemes. An important family of m-schemes called *orbit schemes* was introduced in [IKS09]. The same paper also showed that the schemes conjecture is true when restricted to orbit schemes, by proving that all homogeneous antisymmetric orbit m-schemes have a matching for $m \geq 4$.[4] We prove that the later statement in fact holds for $m \geq 3$ [Guo17, Theorem 6.5].

We also show that the notion of orbit schemes can be naturally generalized to $\mathcal{P}$-schemes, leading to the notion of *orbit $\mathcal{P}$-schemes*: An orbit $\mathcal{P}$-scheme $\mathcal{C}$ is a $\mathcal{P}$-scheme associated with a group $K \subseteq G$, such that the partitions of the coset spaces in $\mathcal{C}$ are just partitions into the K-orbits (under the action of K by inverse right translation).

[4] See [IKS09] for the meaning of this statement.

7 Conclusions and future research

In summary, we introduce the notion of $\mathcal{P}$-schemes and use it to develop a unifying framework for deterministic polynomial factoring over finite fields. In particular, we obtain a generic factoring algorithm (Theorem 2) that allows us to derive most of the known results in a uniform way. It also leads to new results, most notably a factoring algorithm for Galois groups with restricted composition factors (Theorem 4 and Theorem 5).

For future research, we formulate the schemes conjectures for various families $\mathcal{G}$ of permutation groups (Conjecture 1). As we have observed, proving these conjectures are intermediate steps towards proving the original schemes conjecture in [IKS09]. We are particularly interested in the schemes conjecture for the family of finite general linear groups $\mathrm{GL}(V)$ acting naturally on the set $V - \{0\}$ of cardinality $n = |V| - 1$. A first step towards proving this conjecture, which we believe is a reachable goal, would be proving a upper bound $d(\mathrm{GL}(V)) = o(\log n)$.

References

[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*. 1977, pp. 175–178.

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

[AIKS14] M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena. "Deterministic polynomial factoring and association schemes". In: *LMS Journal of Computation and Mathematics* 17.01 (2014), pp. 123–140.

[BCP82] L. Babai, P. J. Cameron, and P. P. Pálfy. "On the orders of primitive groups with restricted nonabelian composition factors". In: *Journal of Algebra* 79.1 (1982), pp. 161–168.

[BGL01] E. Bach, J. von zur Gathen, and H. W. Lenstra Jr. "Factoring polynomials over special finite fields". In: *Finite Fields and Their Applications* 7.1 (2001), pp. 5–28.

[Bai04] R. A. Bailey. *Association Schemes: Designed Experiments, Algebra and Combinatorics*. Vol. 84. Cambridge University Press, 2004.

[BI84] E. Bannai and T. Ito. *Algebraic Combinatorics*. Benjamin/Cummings, 1984.

[Ber67] E. R. Berlekamp. "Factoring polynomials over finite fields". In: *Bell System Technical Journal* 46.8 (1967), pp. 1853–1859.

[Ber70] E. R. Berlekamp. "Factoring polynomials over large finite fields". In: *Mathematics of Computation* 24.111 (1970), pp. 713–735.

[BKS15] J. Bourgain, S. Konyagin, and I. Shparlinski. “Character sums and deterministic polynomial root finding in finite fields”. In: *Mathematics of Computation* 84.296 (2015), pp. 2969–2977.

[CZ81] D. G. Cantor and H. Zassenhaus. “A new algorithm for factoring polynomials over finite fields”. In: *Mathematics of Computation* 36.154 (1981), pp. 587–592.

[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*. 2000, pp. 233–245.

[Coo78] B. N. Cooperstein. “Minimal degree for a permutation representation of a classical group”. In: *Israel Journal of Mathematics* 30.3 (1978), pp. 213–235.

[Evd92] S. A. Evdokimov. “Factorization of solvable polynomials over finite fields and the generalized Riemann hypothesis”. In: *Journal of Soviet Mathematics* 59.3 (1992), pp. 842–849.

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

[Gao01] S. Gao. “On the deterministic complexity of factoring polynomials”. In: *Journal of Symbolic Computation* 31.1 (2001), pp. 19–36.

[Gat87] J. von zur Gathen. “Factoring polynomials and primitive elements for special primes”. In: *Theoretical Computer Science* 52.1 (1987), pp. 77–89.

[GS92] J. von zur Gathen and V. Shoup. “Computing Frobenius maps and factoring polynomials”. In: *Computational Complexity* 2.3 (1992), pp. 187–224.

[GHL16] B. Grenet, J. van der Hoeven, and G. Lecerf. “Deterministic root finding over finite fields using Graeffe transforms”. In: *Applicable Algebra in Engineering, Communication and Computing* 27.3 (2016), pp. 237–257.

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

[Hua91a] M. A. Huang. “Factorization of polynomials over finite fields and decomposition of primes in algebraic number fields”. In: *Journal of Algorithms* 12.3 (1991), pp. 482–489.

[Hua91b] M. A. Huang. “Generalized Riemann hypothesis and factoring polynomials over finite fields”. In: *Journal of Algorithms* 12.3 (1991), pp. 464–481.

[IKRS12] G. Ivanyos, M. Karpinski, L. Rónyai, and N. Saxena. “Trading GRH for algebra: algorithms for factoring polynomials and related structures”. In: *Mathematics of Computation* 81.277 (2012), pp. 493–531.

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

[KS98] E. Kaltofen and V. Shoup. “Subquadratic-time factoring of polynomials over finite fields”. In: *Mathematics of Computation* 67.223 (1998), pp. 1179–1197.

[KU11] K. S. Kedlaya and C. Umans. “Fast polynomial factorization and modular composition”. In: *SIAM Journal on Computing* 40.6 (2011), pp. 1767–1802.

[LM85] S. Landau and G. L. Miller. “Solvability by radicals is in polynomial time”. In: *Journal of Computer and System Sciences* 30.2 (1985), pp. 179–208.

[LLL82] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. “Factoring polynomials with rational coefficients”. In: *Mathematische Annalen* 261.4 (1982), pp. 515–534.

[LPS88] M. W. Liebeck, C. E. Praeger, and J. Saxl. “On the O’Nan-Scott theorem for finite primitive permutation groups”. In: *Journal of the Australian Mathematical Society (Series A)* 44.03 (1988), pp. 389–396.

[LS99] M. W. Liebeck and A. Shalev. “Simple groups, permutation groups, and probability”. In: *Journal of the American Mathematical Society* 12.2 (1999), pp. 497–520.

[LS02] M. W. Liebeck and A. Shalev. “Bases of primitive linear groups”. In: *Journal of Algebra* 252.1 (2002), pp. 95–113.

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

[Luk82] E. M. Luks. “Isomorphism of graphs of bounded valence can be tested in polynomial time”. In: *Journal of Computer and System Sciences* 25.1 (1982), pp. 42–65.

[Luk93] E. M. Luks. “Permutation groups and polynomial-time computation”. In: *Groups and Computation*. Vol. 11. DIMACS series in Discrete Mathematics and Theoretical Computer Science. 1993, p. 139.

[MS88] M. Mignotte and C. P. Schnorr. “Calcul déterministe des racines d’un polynôme dans un corps fini”. In: *Comptes Rendus de l Académie des Sciences* 306 (1988), pp. 467–472.

[Mil83] G. L. Miller. “Isomorphism of k-contractible graphs. A generalization of bounded valence and bounded genus”. In: *Information and Control* 56.1 (1983), pp. 1–20.

[Pil90] J. Pila. “Frobenius maps of abelian varieties and finding roots of unity in finite fields”. In: *Mathematics of Computation* 55.192 (1990), pp. 745–763.

[Pyb93] L. Pyber. “Asymptotic results for permutation groups”. In: *Groups and Computation*. Vol. 11. DIMACS series in Discrete Mathematics and Theoretical Computer Science. 1993, pp. 197–219.

[PS97] L. Pyber and A. Shalev. “Asymptotic results for primitive permutation groups”. In: *Journal of Algebra* 188.1 (1997), pp. 103–124.

[Rón88] L. Rónyai. “Factoring polynomials over finite fields”. In: *Journal of Algorithms* 9.3 (1988), pp. 391–400.

[Rón89] L. Rónyai. “Factoring polynomials modulo special primes”. In: *Combinatorica* 9.2 (1989), pp. 199–206.

[Rón92] L. Rónyai. “Galois groups and factoring polynomials over finite fields”. In: *SIAM Journal on Discrete Mathematics* 5.3 (1992), pp. 345–365.

[Sah08] C. Saha. “Factoring polynomials over finite fields using balance test”. In: *Proceedings of the 25th International Symposium on the Theoretical Aspects of Computer Science*. 2008, pp. 609–620.

[Sch85] R. Schoof. “Elliptic curves over finite fields and the computation of square roots mod p”. In: *Mathematics of Computation* 44.170 (1985), pp. 483–494.

[SS98] K. See and S. Y. Song. “Association schemes of small order”. In: *Journal of Statistical Planning and Inference* 73.1 (1998), pp. 225–271.

[Ser96] Á. Seress. “The minimal base size of primitive solvable permutation groups”. In: *Journal of the London Mathematical Society* 53.2 (1996), pp. 243–255.

[Ser03] Á. Seress. *Permutation Group Algorithms*. Vol. 152. Cambridge University Press, 2003.

[Sho90] V. Shoup. “On the deterministic complexity of factoring polynomials over finite fields”. In: *Information Processing Letters* 33.5 (1990), pp. 261–267.

[Sho91] V. Shoup. “Smoothness and factoring polynomials over finite fields”. In: *Information Processing Letters* 38.1 (1991), pp. 39–42.