Schemes for Deterministic Polynomial Factoring

Gábor Ivanyos
Computer and Automation Research Institute
Lágymányosi u. 11
1111 Budapest, Hungary
Gabor.Ivanyos@sztaki.hu

Marek Karpinski
Department of Computer Science
University of Bonn
53117 Bonn, Germany
marek@cs.uni-bonn.de

Nitin Saxena
Hausdorff Center for Mathematics
Endenicher Allee 62
53115 Bonn, Germany
ns@hcm.uni-bonn.de

ABSTRACT

In this work we relate the deterministic complexity of factoring polynomials (over finite fields) to certain combinatorial objects, we call m-schemes, that are generalizations of permutation groups. We design a new generalization of the known conditional deterministic subexponential time polynomial factoring algorithm to get an underlying m-scheme. We then demonstrate how progress in understanding m-schemes relate to improvements in the deterministic complexity of factoring polynomials, assuming the Generalized Riemann Hypothesis (GRH).

In particular, we give the first deterministic polynomial time algorithm (assuming GRH) to find a nontrivial factor of a polynomial of prime degree n where $(n-1)$ is a constant-smooth number. We use a structural theorem about association schemes on a prime number of points, which Hanaki and Uno (2006) proved by representation theory methods.

Categories and Subject Descriptors

F.1.3 [**Complexity Measures and Classes**]: Derandomization; G.2.1 [**Discrete Mathematics**]: Combinatorics; I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms

General Terms

Algorithms, Theory

Keywords

GRH, Polynomial Factoring, Representation Theory

1. INTRODUCTION

We consider the classical problem of finding a nontrivial factor of a given polynomial over a finite field. This problem has various randomized polynomial time algorithms – Berlekamp [3], Rabin [19], Cantor and Zassenhaus [8], von zur Gathen and Shoup [27], Kaltofen and Shoup [15] – but its deterministic complexity is a longstanding open problem. It bears upon the general derandomization question in Computational Complexity theory, i.e. whether BPP=P?

In this paper we study the deterministic complexity of factoring assuming the Generalized Riemann Hypothesis (GRH). The assumption of GRH in this paper is needed only to find primitive r-th nonresidues in a finite field $\mathbb{F}_q$ which are in turn used to find a root x (if it exists in $\mathbb{F}_q$) of "special" polynomials: $x^r - a$ over $\mathbb{F}_q$ (see [1]).

Assuming GRH, there are many deterministic factoring algorithms known but all of them are super-polynomial time except on special instances: Rónyai [22] showed under GRH that any polynomial $f(x) \in \mathbb{Z}[x]$ can be factored modulo p deterministically in time polynomial in the Galois group of f, except for finitely many primes p. Rónyai's result generalizes previous results by Huang [14], Evdokimov [10] and Adleman, Manders and Miller [1]. Bach, von zur Gathen and Lenstra [2] showed that polynomials over finite fields of characteristic p can be factored in deterministic polynomial time if $\phi_k(p)$ is smooth for some integer k, where $\phi_k(x)$ is the k-th cyclotomic polynomial. This result generalizes the previous works of Rónyai [21], Mignotte and Schnorr [16], von zur Gathen [26], Camion [7] and Moenck [18].

The line of research, in which this paper makes progress, was started by Rónyai [20]. There it was shown how to use GRH to find a nontrivial factor of a polynomial $f(x)$, where the degree n of $f(x)$ has a small prime factor, in deterministic polynomial time. The basic idea of [20], in the case when n is even, was to go to a ring extension $\mathcal{A}^{(2)} := \mathbb{F}_q[x_1, x_2]/(f(x_1), f_2(x_1, x_2))$ of $\mathcal{A}^{(1)} := \mathbb{F}_q[x_1]/(f(x_1))$, where $f_2(x_1, x_2) := \frac{f(x_2)}{x_2 - x_1}$, and then use the symmetry of $\mathcal{A}^{(2)}$ to decompose $\mathcal{A}^{(2)}$ under GRH. A decomposition of $\mathcal{A}^{(2)}$ gives us a nontrivial factor of $f(x)$ since n is even. [20] showed that this basic idea can be extended to the case when a prime $r|n$ but then the deterministic algorithm finds a nontrivial factor of $f(x)$ in time $poly(\log q, n^r)$. The n^r dependence appears in the complexity estimate because this is roughly the dimension of the algebras, like:

$$\mathbb{F}_q[x_1, \ldots, x_r]/(f(x_1), \ldots, f_r(x_1, \ldots, x_r)) \qquad (1)$$

in which the algorithm does computation. Naively, it would seem that this algorithm will take time $poly(\log q, n^n)$ in the worst case (for example when n is a prime). But Evdokimov [11] showed that the special properties of the intermediate algebras that appear in Rónyai's algorithm can be exploited so that it is enough to work with algebras like (1) with a significantly smaller $r \leq \log n$, thus, polynomial factoring can be done deterministically in time $poly(\log q, n^{\log n})$ under GRH.

ISSAC'09, July 28–31, 2009, Seoul, Republic of Korea.

This line of approach has since been investigated, in an attempt to remove GRH or improve the time complexity, leading to several algebraic-combinatorial conjectures and quite special case solutions (see [9, 12, 23]). Our method in this paper encompasses these known methods and ends up relating the complexity of polynomial factoring to "purely" combinatorial objects (called *schemes*) that are central to the research area of algebraic combinatorics. It is easy to verify that the methods of [20, 11, 9, 12, 23] arrange the underlying roots of the polynomial in a combinatorial object that satisfies *some* of the defining properties of schemes. Then [20, 11, 9] use the combinatorial properties of this object while [12, 23] also use the conjectured *field-theoretic* properties to factor the polynomial. This paper generalizes the former line of attack by formalizing a combinatorial object and a purely combinatorial conjecture, both of which seem naturally connected with polynomial factoring. We see this as an exciting bridge between the well studied areas of polynomial factoring and algebraic combinatorics.

We extend Evdokimov's algorithm by working in a more general framework of *tensor powers* (in Section 3) and this leads to the analysis of a more general underlying combinatorial structure (in Section 4) that we call an *m-scheme*. An *m-scheme on n points* is, roughly speaking, a partition $\mathcal{P}$ of the set $[n]^m$, where $[n]$ denotes the set $\{1, \ldots, n\}$:

$$[n]^m = \cup_{P \in \mathcal{P}} P$$

that satisfies certain "natural" properties (defined in Section 2). The fundamental nature of m-schemes can be gauged from the fact that there is an abundance of their examples in algebraic combinatorics, for example, strongly regular graphs, coherent configurations, association schemes, cellular algebras, orbits of groups, and superschemes. Below we elaborate a bit on some of these and in Section 2.4 we compare our m-schemes with known similar abstractions.

• a regular graph on n vertices is an example of a 2-scheme on n points,

• a strongly regular graph (see [6]) on n vertices is an example of a 3-scheme on n points,

• an association scheme (see [6, 30]) gives rise to a 3-scheme and vice-versa. See Section 2.2 for these kind of examples.

• n-schemes on n points *always* arise from permutation groups. See Section 2.3 for constructing them from groups and [25] for the converse. This important example suggests that m-schemes can be considered as a generalization of finite permutation groups. See [17] for some practical implementations of group schemes.

• curiously enough, m-schemes on n points also appear when the $(m-1)$-dimensional Weisfeiler-Lehman method for the graph isomorphism problem is applied to a graph on n vertices, see [5].

Such a large variety of examples makes a classification attempt for m-schemes quite infeasible. But the m-schemes that appear in our polynomial factoring algorithm possess a special structure and we believe that their properties can be exploited to get a deterministic and efficient polynomial factoring algorithm (under GRH). We demonstrate that this belief in fact works in several cases (in Sections 4.1, 5 and 6). In particular, we challenge the algebraic combinatorialists with the following conjecture (see Section 4):

Schemes Conjecture: *There exists a constant $m \geq 4$ such that every homogeneous, antisymmetric m-scheme contains a matching.*

It is a standard result that to solve polynomial factoring it is enough to factor polynomials that split completely over prime fields (see Berlekamp [3, 4] and Zassenhaus [29]). Thus, we will assume in this paper that the input polynomial $f(x)$ of degree n has n distinct roots in $\mathbb{F}_p$ for some prime p. Our algorithm for factoring $f(x)$ constructs an r-scheme on the n roots while working in the algebra of Equation (1), over a suitable $\mathbb{F}_q \supseteq \mathbb{F}_p$. We give several results in this work showing how to utilise the properties of these underlying r-schemes to efficiently find a nontrivial factor of $f(x)$. The most striking of our results makes use of a recent structural theorem of association schemes on a *prime* number of points, which in turn was proven using representation theory of association schemes (see [13]):

Main Theorem: *If $n > 2$ is prime, r is the largest prime factor of $(n-1)$ and $f(x)$ is a degree n polynomial over $\mathbb{F}_p$ then we can find a nontrivial factor of $f(x)$ deterministically in time poly$(\log p, n^r)$ under GRH.*

The paper is organized as follows. We formally define m-schemes in Section 2 and exhibit two important examples. In Section 3 we introduce our framework of the tensor powers $\mathcal{A}^{\otimes m}$ of the algebra $\mathcal{A} := \mathbb{F}_p[x]/(f(x))$ and present our algorithm that constructs an underlying m-scheme, on the n roots of $f(x)$, while working in $\mathcal{A}^{\otimes m}$. In Section 4 we identify properties of this m-scheme that help in polynomial factoring and show that the schemes conjecture if true would make our algorithm deterministic polynomial time under GRH. We also prove the conjecture in the important example of m-schemes arising from permutation groups. In Section 5 we complete the proof of our Main Theorem. In Section 6 we show that the *levels* r (as in Equation (1)) in Evdokimov's algorithm can be reduced to $\frac{\log n}{1.5}$ using properties of m-schemes. In Section 7 we introduce a concept of *primitivity* in m-schemes, inspired from the connectivity of graphs, and give some hints how it could improve the factoring algorithm.

2. INTRODUCING M-SCHEMES

In this section we define special partitions of the set $[n]^m$ that we call m-schemes on n points. These combinatorial objects are closely related to superschemes which were first defined in [25].

2.1 Basic Definitions

We will denote $\{1, \ldots, n\}$ by $[n]$.

Let $V = \{v_1, \ldots, v_n\}$ be a set of n distinct elements. For $1 \leq s \leq n$, define the set of s-tuples:
$V^{(s)} := \{(v_{i_1}, \ldots, v_{i_s}) \in V^s \mid v_{i_1}, \ldots, v_{i_s}$ are s distinct elements of $V\}$.

Projections: If $s > 1$ then we define s *projections*, $\pi_1^s, \ldots, \pi_s^s : V^{(s)} \to V^{(s-1)}$ as:
$\pi_i^s : (v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_s) \mapsto (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_s)$.

Permutations: The symmetric group on s elements Symm_s acts on $V^{(s)}$ in a natural way by permuting the coordinates of the s-tuples. To be more accurate, the action is the following: for $\sigma \in \text{Symm}_s$,
$(v_1, \ldots, v_i, \ldots, v_s)^\sigma := (v_{1^\sigma}, \ldots, v_{i^\sigma}, \ldots, v_{s^\sigma})$.

m-collection: For $1 \leq m \leq n$, an *m-collection* on V is a set Π of partitions $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m$ of $V^{(1)}, V^{(2)}, \ldots, V^{(m)}$ respectively.

Colors: For $1 \leq s \leq m$, we denote by $\equiv_{\mathcal{P}_s}$ the equivalence relation on $V^{(s)}$ corresponding to the partition $\mathcal{P}_s$. We call the equivalence classes of the relation $\equiv_{\mathcal{P}_s}$ *colors at level s*.

We define below some natural properties of collections that are relevant to us. Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be an m-collection on V.

P1 (Compatibility): We say that Π is *compatible* at level $1 < s \leq m$, if $\bar{u}, \bar{v} \in P \in \mathcal{P}_s$ implies that for every $1 \leq i \leq s$ there exists $Q \in \mathcal{P}_{s-1}$ such that $\pi_i^s(\bar{u}), \pi_i^s(\bar{v}) \in Q$.

In other words, if two tuples (at level s) have the same color then for every projection the projected tuples (at level $s-1$) have the same color as well. It follows that for a class $P \in \mathcal{P}_s$, the sets $\pi_i^s(P) := \{\pi_i^s(\bar{v}) | \bar{v} \in P\}$, for all $i \in [s]$, are colors in $\mathcal{P}_{s-1}$.

P2 (Regularity): We say that Π is *regular* at level $1 < s \leq m$, if $\bar{u}, \bar{v} \in Q \in \mathcal{P}_{s-1}$ implies that for every $1 \leq i \leq s$ and for every $P \in \mathcal{P}_s$,
$\#\{\bar{u}' \in P \mid \pi_i^s(\bar{u}') = \bar{u}\} = \#\{\bar{v}' \in P \mid \pi_i^s(\bar{v}') = \bar{v}\}$

Fibers: We call the tuples in $P \cap (\pi_i^s)^{-1}(\bar{u})$ as π_i^s-*fibers* of $\bar{u}$ in P. So regularity, in other words, means that the cardinalities of the fibers above a tuple depend only on the color of the tuple.

Subdegree: The above two properties motivate the definition of the *subdegree of a color P over a color Q* as $\frac{\#P}{\#Q}$ assuming that $\pi_i^s(P) = Q$ for some i and that Π is regular at level s.

P3 (Invariance): We say that Π is *invariant* at level $1 < s \leq m$, if for every $P \in \mathcal{P}_s$ and $\sigma \in \mathrm{Symm}_s$ we have: $P^\sigma := \{\bar{v}^\sigma | \bar{v} \in P\} \in \mathcal{P}_s$.

In other words, the partitions $\mathcal{P}_1, \ldots, \mathcal{P}_m$ are invariant under the action of the corresponding symmetric group.

P4 (Homogeneity): We say that Π is *homogeneous* if $|\mathcal{P}_1| = 1$.

P5 (Antisymmetry): We say that Π is *antisymmetric* at level s if for every $P \in \mathcal{P}_s$ and $1 \neq \sigma \in \mathrm{Symm}_s$, we have $P^\sigma \neq P$.

P6 (Symmetry): We say that Π is *symmetric* at level s if for every $P \in \mathcal{P}_s$ and $\sigma \in \mathrm{Symm}_s$, we have $P^\sigma = P$.

An m-collection is called compatible, regular, invariant, symmetric, or antisymmetric if it is at every level $1 < s \leq m$, compatible, regular, invariant, symmetric, or antisymmetric respectively.

***m*-scheme:** An m-collection is called an *m-scheme* if it is compatible, regular and invariant.

We should remark that the m-schemes that appear in our factoring algorithm are homogeneous and antisymmetric as well. As a warmup to these definitions we prove below an easy nonexistence result for schemes.

Lemma 1. *Let $r > 1$ be a divisor of n. Then for $m \geq r$ there does not exist a homogeneous and antisymmetric m-scheme on n points.*

PROOF. For any $m \geq r$ clearly every m-scheme contains an r-scheme. Thus, we will prove the statement for $m = r$. Suppose $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r\}$ is an r-scheme on points $[n]$. By definition $\mathcal{P}_r$ partitions $n(n-1)\cdots(n-r+1)$ tuples of $V^{(r)}$ into, say, t_r colors. By antisymmetricity every such color P has $r!$ associated colors, namely $\{P^\sigma | \sigma \in \mathrm{Symm}_r\}$. Further, by homogeneity the size of every color at level r is divisible by n. Thus by a simple counting of r-tuples we deduce $r!n | n(n-1)\cdots(n-r+1)$, implying $r! | (n-1)\cdots(n-r+1)$. This contradicts $r | n$, thus Π cannot exist. □

Let us now see some easily describable examples of m-schemes that do exist.

2.2 Example: 3-schemes from Coherent Configurations

Coherent configurations are standard combinatorial objects that have strongly regular graphs as examples (see [6]). Recall that a coherent configuration is essentially a 2-scheme $\{\mathcal{P}_1, \mathcal{P}_2\}$ that also has a composition property:

Composition: For any $P_i, P_j, P_k \in \mathcal{P}_2$ and any $(\alpha, \beta) \in P_k$ the number: $\#\{\gamma \in V \mid (\alpha, \gamma) \in P_i \text{ and } (\gamma, \beta) \in P_j\}$ is independent of which tuple (α, β) in P_k we chose.

In other words, the relations P_i and P_j can be "composed" to get a bigger relation that is just a "linear combination" of the relations in $\mathcal{P}_2$.

Association Scheme: In the literature a homogeneous coherent configuration is usually called an *association scheme*.

These standard coherent configurations turn out to be similar to our notion of 3-schemes: From a coherent configuration $\{\mathcal{P}_1, \mathcal{P}_2\}$ we can define a partition $\mathcal{P}_3$ on the triples such that for any two triples (u_1, u_2, u_3) and (v_1, v_2, v_3) we have:
$(u_1, u_2, u_3) \equiv_{\mathcal{P}_3} (v_1, v_2, v_3)$ if and only if $(u_1, u_2) \equiv_{\mathcal{P}_2} (v_1, v_2)$, $(u_1, u_3) \equiv_{\mathcal{P}_2} (v_1, v_3)$, $(u_2, u_3) \equiv_{\mathcal{P}_2} (v_2, v_3)$.

It is easy to show that $\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ satisfies compatibility, regularity and invariance: it is a 3-scheme. Similarly:

Lemma 2. *If $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ is a homogeneous 3-scheme then $\{\mathcal{P}_1, \mathcal{P}_2\}$ is an association scheme.*

PROOF. By the hypothesis we already have that $\{\mathcal{P}_1, \mathcal{P}_2\}$ is a homogeneous 2-scheme. Thus, we only need to show the composition property. Let $P_i, P_j, P_k \in \mathcal{P}_2$ and let $(\alpha, \beta) \in P_k$. Then there exists a subset $\mathcal{S} \subseteq \mathcal{P}_3$ such that the set: $\{\gamma \in V \mid (\alpha, \gamma) \in P_i, (\gamma, \beta) \in P_j\}$ can be partitioned as:

$$\sqcup_{P \in \mathcal{S}} \{\gamma \in V \mid (\alpha, \gamma) \in P_i, (\gamma, \beta) \in P_j, (\alpha, \gamma, \beta) \in P\}$$

which by the compatibility of Π at level 3 is:

$$\sqcup_{P \in \mathcal{S}} \{\gamma \in V \mid (\alpha, \gamma, \beta) \in P\}$$

again by the regularity of Π at level 3 the size of the above sets is simply $\frac{\#P}{\#P_k}$, which is independent of the choice of (α, β). Thus, $\{\mathcal{P}_1, \mathcal{P}_2\}$ has the composition property. □

2.3 Example: Orbit Schemes

Permutation groups provide a host of examples (see [25]). Let $G \leq \mathrm{Symm}_V$ be a permutation group. The *orbits* of G on the s-tuples ($1 \leq s \leq m \leq n$) give an m-scheme. More formally, define the partition $\mathcal{P}_s$ as: for any two s-tuples $(u_1, \ldots, u_s)$ and $(v_1, \ldots, v_s)$ in $V^{(s)}$, $(u_1, \ldots, u_s) \equiv_{\mathcal{P}_s} (v_1, \ldots, v_s)$ iff $\exists \sigma \in G$, $(\sigma(u_1), \ldots, \sigma(u_s)) = (v_1, \ldots, v_s)$. It is easy to see that these partitions naturally satisfy compatibility, regularity and invariance properties and hence form an m-scheme. We call m-schemes arising in this way *orbit m-schemes*.

It is easy to see that the orbit scheme is homogeneous if and only if G is transitive. Furthermore, assume that G is transitive and for some integer $1 \leq m < n$, $\gcd(m!, |G|) = 1$. Then the corresponding orbit m-scheme is both homogeneous and antisymmetric. Our attention to this class of examples has been drawn by D. Pasechnik.

At the moment, we are not aware of any other examples of homogeneous antisymmetric m-schemes with $m \to \infty$. The homogeneous antisymmetric m-schemes are the ones that arise in our factoring algorithm and we do believe that their parameters satisfy more stringent conditions than the general m-schemes. For a conjecture along these lines see Section 4.1.

2.4 Difference between Various Notions of Schemes

The term *schemes* arises in the mathematical literature in many contexts. Our m-schemes should not be confused with the notion of *schemes* in algebraic geometry. However, our m-schemes are closely related to *association schemes*, *superschemes* (Smith [25]) and *height t presuperschemes* (Wojdyło [28]). Smith's superschemes are m-schemes that also satisfy a suitable higher dimensional generalization of the composition property. It is not difficult to see that a superscheme on n points is just a n-scheme on n points. Wojdyło's height t presuperscheme consists of the bottom t levels of a superscheme. In particular, a level 0 presuperscheme is just an association scheme. It can be shown that a height t presuperscheme on n-points consists just of the first $(t+2)$ levels of a $(t+3)$-scheme on n points.

3. DECOMPOSITION OF TENSOR POWERS OF ALGEBRAS

In this section we describe our polynomial factoring algorithm and simultaneously show how m-schemes appear in the algorithm. Recall that in the input we are given a polynomial $f(x) \in \mathbb{F}_p$ of degree n having distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}_p$. For any extension field k of $\mathbb{F}_p$ we have the natural associated algebra $\mathcal{A} := k[X]/(f(X))$. Note that $\mathcal{A}$ is a completely split semisimple n-dimensional algebra over the field k, i.e. $\mathcal{A}$ is isomorphic to k^n the direct sum of n copies of the one-dimensional k-algebra k. We interpret $\mathcal{A}$ as the set of all functions,

$$V := \{\alpha_1, \ldots, \alpha_n\} \to k.$$

Algorithmically, we have $\mathcal{A}$ by structure constants with respect to some basis $b_1, \ldots, b_n$ (for example, $1, X, \ldots, X^{n-1}$) and the problem of factoring $f(X)$ completely can be viewed as finding an explicit isomorphism from $\mathcal{A}$ to k^n.

How do the factors of $f(X)$ appear in $\mathcal{A}$? They appear as *zero divisors* in $\mathcal{A}$. Recall that a zero divisor is a nonzero element $z(X) \in \mathcal{A}$ such that $y(X)z(X) = 0$ for some nonzero element $y(X) \in \mathcal{A}$. This means that $f(X)|y(X) \cdot z(X)$ which implies (by the nonzeroness of y and z) $gcd(f(X), z(X))$ factors $f(X)$ nontrivially. As gcd of polynomials can be computed by the deterministic polynomial time Euclidean algorithm, we infer that finding a zero divisor in the factor algebra $k[X]/(f(X))$ is – up to polynomial time deterministic reductions – equivalent to finding a nontrivial divisor of $f(X)$. Furthermore, computing an explicit isomorphism with k^n is equivalent to factoring $f(X)$ completely.

How are the ideals of $\mathcal{A}$ related to the roots of $f(x)$? Let I be an ideal of $\mathcal{A}$. The *support of* I, $\mathrm{Supp}(I)$, is defined as:

$$\mathrm{Supp}(I) := V \setminus \{v \in V \mid a(v) = 0 \text{ for every } a \in I\}$$

Conversely, for $U \subseteq V$, the ideal $\mathrm{I}(U)$ is defined as:

$$\mathrm{I}(U) := \{b \in \mathcal{A} \mid b(u) = 0 \text{ for every } u \in U\}$$

and $\mathrm{I}^{\perp}(U)$ is the *annihilator* of $\mathrm{I}(U)$:

$$\mathrm{I}^{\perp}(U) := \{a \in \mathcal{A} \mid ab = 0 \text{ for every } b \in \mathrm{I}(U)\}.$$

It can be easily seen that Supp is an inclusion preserving bijection from the ideals of $\mathcal{A}$ to the subsets of V with inverse map $\mathrm{I}^{\perp}$. In view of this correspondence, partial decompositions of $\mathcal{A}$ into sums of pairwise orthogonal ideals correspond to partitions of the set V. Let us formulate the above discussion in a lemma.

Lemma 3. *If $I_1, \ldots, I_t$ are pairwise orthogonal ideals of $\mathcal{A}$ (i.e. $I_i I_j = 0$ for all $i \neq j$) such that $\mathcal{A} = I_1 + \cdots + I_t$ then $V = \mathrm{Supp}(I_1) \sqcup \cdots \sqcup \mathrm{Supp}(I_t)$.*

We now move up to the tensor powers of $\mathcal{A}$ and there we show a way of getting the partitions of $V^{(m)}$.

Functional interpretation of tensor powers: For $m \in [n]$, let $\mathcal{A}^{\otimes m}$ denote the mth tensor power of $\mathcal{A}$. $\mathcal{A}^{\otimes m}$ is also a completely split semisimple algebra; it is isomorphic to k^{n^m}. We again interpret it as the algebra of functions from V^m to k.

Note that in this interpretation the rank one tensor element $h_1 \otimes \cdots \otimes h_m$ corresponds to a function $V^m \to k$ that maps $(v_1, \ldots, v_m) \mapsto h_1(v_1) \cdots h_m(v_m)$.

Essential part of tensor powers: We define the *essential part* $\mathcal{A}^{(m)}$ of $\mathcal{A}^{\otimes m}$ to be its (unique) ideal consisting of the functions which vanish on all the m-tuples $(v_1, \ldots, v_m) \in V^m$ with $v_i = v_j$ for some $i \neq j$.

Then $\mathcal{A}^{(m)}$ can be interpreted as the algebra of functions $V^{(m)} \to k$. We note below that a basis for $\mathcal{A}^{(m)}$ can be computed easily and then this is the algebra where our factoring algorithm does computations.

Lemma 4. *Given $f(X)$, a polynomial of degree n having n distinct roots in $\mathbb{F}_p$, a basis for $\mathcal{A}^{(m)} = (k[X]/(f(X)))^{(m)}$ over $k \supseteq \mathbb{F}_p$ can be computed by a deterministic algorithm in time poly$(\log |k|, n^m)$.*

Proof. To see this consider embeddings μ_i, for all $i \in [m]$, of $\mathcal{A}$ into $\mathcal{A}^{\otimes m}$ given as $\mu_i : a \mapsto 1 \otimes \ldots \otimes 1 \otimes a \otimes 1 \otimes \ldots \otimes 1$ where a is in the i-th place. In the interpretation as functions, $\mu_i(\mathcal{A})$ correspond to the functions on V^m which depend only on the ith element in the tuples. Observe that the set, for $1 \leq i < j \leq m$:

$$\Delta^m_{i,j} = \{b \in \mathcal{A}^{\otimes m} \mid (\mu_i(a) - \mu_j(a))b = 0 \text{ for every } a \in \mathcal{A}\}$$

is the ideal of $\mathcal{A}^{\otimes m}$ consisting of the functions which are zero on every tuple $(v_1, \ldots, v_m) \in V^m$ with $v_i \neq v_j$. Given a basis for $\mathcal{A}$, a basis for $\Delta^m_{i,j}$ can be computed by solving a system of linear equations in time polynomial in the dimension of $\mathcal{A}^{\otimes m}$ (over k) which is n^m. Finally, notice that $\mathcal{A}^{(m)}$ is just the annihilator of $\sum_{1 \leq i < j \leq m} \Delta^m_{i,j}$ and hence can be computed in $poly(n^m)$ field operations. □

Ideals of $\mathcal{A}^{(m)}$ and roots of $f(x)$: Like the case of $m = 1$, ideals and partial decompositions of $\mathcal{A}^{(m)}$ into pairwise orthogonal ideals correspond to subsets and partitions of the set $V^{(m)}$ respectively.

If I is an ideal of $\mathcal{A}^{(m)}$ then we again define the *support of* I, $\mathrm{Supp}(I)$, as:
$\mathrm{Supp}(I) := V^{(m)} \setminus \{\bar{v} \in V^{(m)} \mid a(\bar{v}) = 0 \text{ for every } a \in I\}$
and Lemma 3 generalizes to:

Lemma 5. *For any $s \leq n$, if $I_{s,1}, \ldots, I_{s,t_s}$ are pairwise orthogonal ideals of $\mathcal{A}^{(s)}$ such that $\mathcal{A}^{(s)} = I_{s,1} + \cdots + I_{s,t_s}$ then $V^{(s)} = \mathrm{Supp}(I_{s,1}) \sqcup \cdots \sqcup \mathrm{Supp}(I_{s,t_s})$.*

Now we will describe our polynomial factoring algorithm that produces m-schemes.

Algorithm Description

Input: a degree n polynomial $f(x)$ having n distinct roots in $\mathbb{F}_p$.

Given $1 < m \leq n$ we can wlog assume that we also have the smallest field extension $k \supseteq \mathbb{F}_p$ having s-th nonresidues for all $s \in [m]$ (computing k will take $poly(\log p, m^m)$ time under GRH).

Output: a nontrivial factor of $f(x)$ or a homogeneous, antisymmetric m-scheme on the n points, $V := \{\alpha \in \mathbb{F}_p | \ f(\alpha) = 0\}$.

Algorithm overview:

We define $\mathcal{A}^{(1)} = \mathcal{A} = k[x]/(f(x))$ and compute $\mathcal{A}^{(s)}$, for all $s \in [m]$, in time $poly(\log p, n^m)$ (by Lemma 4).

Now observe that $Aut_k(\mathcal{A}^{(s)})$ contains Symm_s. To see this, just note that there is an action of Symm_s on $\mathcal{A}^{\otimes s}$ as a group of algebra automorphism, for $\sigma \in \mathrm{Symm}_s$ this action is the linear extension of: $(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_{1\sigma}} \otimes \cdots \otimes b_{i_{s\sigma}}$.

This knowledge of explicit automorphisms of $\mathcal{A}^{(s)}$ can be exploited to efficiently decompose these algebras under GRH (see Theorem 2.3 in [22]). Thus, for all $1 < s \leq m$ we can compute mutually orthogonal $t_s \geq 2$ ideals $I_{s,i}$ of $\mathcal{A}^{(s)}$, such that:

$$\mathcal{A}^{(s)} = I_{s,1} + \ldots + I_{s,t_s}$$

By Lemma 5, the above decomposition induces partitions $\mathcal{P}_s$ for all $1 < s \leq m$ such that:

$$\mathcal{P}_s : \quad V^{(s)} = \mathrm{Supp}(I_{s,1}) \sqcup \cdots \sqcup \mathrm{Supp}(I_{s,t_s})$$

Thus, together with $\mathcal{P}_1 := \{V\}$ we have an m-collection $\Pi := \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ on the set V.

Now we will show how to *refine* this m-collection to an m-scheme using algebraic operations on the ideals $I_{s,i}$ of $\mathcal{A}^{(s)}$. To do that, we first need a tool to relate lower level ideals $I_{s-1,i}$ to higher level ideals $I_{s,i'}$.

Algebra Embeddings $\mathcal{A}^{(s-1)} \to \mathcal{A}^{(s)}$: For every $1 < s \leq m$, we have s embeddings $\iota_j^s : \mathcal{A}^{\otimes(s-1)} \to \mathcal{A}^{\otimes s}$ sending $b_{i_1} \otimes \cdots \otimes b_{i_{s-1}}$ to $b_{i_1} \otimes \cdots \otimes b_{i_{j-1}} \otimes 1 \otimes b_{i_j} \otimes \cdots b_{i_{s-1}}$. Restricting to $\mathcal{A}^{(s-1)}$ and multiplying the images of ι_j^s by the identity element of $\mathcal{A}^{(s)}$, we obtain algebra embeddings $\mathcal{A}^{(s-1)} \to \mathcal{A}^{(s)}$ denoted also by $\iota_1^s, \ldots, \iota_s^s$.

In the function interpretation, $\iota_j^s(\mathcal{A}^{(s-1)})$ is just the set of functions in $\mathcal{A}^{(s)}$ which do not depend on the jth coordinate of tuples.

The algorithm is best explained by describing the five kinds of *refinement* procedures that implicitly refine Π.

R1 (Compatibility): If for any $1 < s \leq m$, for any pair of ideals $I_{s-1,i}$ and $I_{s,i'}$ in the decomposition of $\mathcal{A}^{(s-1)}$ and $\mathcal{A}^{(s)}$ respectively, and for any $j \in \{1, \ldots, s\}$, the ideal $\iota_j^s(I_{s-1,i})I_{s,i'}$ is neither zero nor $I_{s,i'}$ then we can efficiently compute a subideal of $I_{s,i'}$, hence, refine $I_{s,i'}$ and the m-collection Π.

Note that R1 fails to refine Π only when it is a compatible collection.

R2 (Regularity): If for any $1 < s \leq m$, for any pair of ideals $I_{s-1,i}$ and $I_{s,i'}$ in the decomposition of $\mathcal{A}^{(s-1)}$ and $\mathcal{A}^{(s)}$ respectively, and for any $j \in \{1, \ldots, s\}$, $\iota_j^s(I_{s-1,i})I_{s,i'}$ is not a free module over $\iota_j^s(I_{s-1,i})$ then by trying to find a free basis, we can efficiently compute a zero divisor in $I_{s-1,i}$, hence, refine $I_{s-1,i}$ and the m-collection Π.

Note that R2 fails to refine Π only when it is a regular collection.

Compatibility and regularity of Π create a natural connection between the ideals of levels $(s-1)$ and s, for all $1 < s \leq m$. In the case when a pair of ideals $I_{s-1,i}$ and $I_{s,i'}$ in the decomposition of $\mathcal{A}^{(s-1)}$ and $\mathcal{A}^{(s)}$ respectively, satisfies $\iota_j^s(I_{s-1,i})I_{s,i'} = I_{s,i'}$: $I_{s,i'}$ is a free module over $\iota_j^s(I_{s-1,i})$ which in other words means that the elements in $I_{s,i'}$ can be viewed as univariate polynomials with coefficients in $I_{s-1,i}$. The rank of the free module $I_{s,i'}$ over $\iota_j^s(I_{s-1,i})$ can easily be seen to be equal to the subdegree of $\mathrm{Supp}(I_{s,i'})$ over $\mathrm{Supp}(I_{s-1,i})$.

R3 (Invariance): If for some $1 < s \leq m$ and some $\sigma \in \mathrm{Symm}_s$ the decomposition of $\mathcal{A}^{(s)}$ is not σ-invariant, then we can find two ideals $I_{s,i}$ and $I_{s,i'}$ such that $I_{s,i}^\sigma \cap I_{s,i'}$ is neither zero nor $I_{s,i'}$, thus, we can efficiently refine $I_{s,i'}$ and the m-collection Π.

Note that R3 fails to refine Π only when it is an invariant collection.

R4 (Homogeneity): If the algebra $\mathcal{A}^{(1)} = \mathcal{A}$ is in a (known) decomposed form then trivially we can find a nontrivial factor of $f(x)$ from that decomposition.

Note that R4 fails to refine Π only when it is a homogeneous collection.

R5 (Antisymmetricity): If for some $1 < s \leq m$, for some ideal $I_{s,i}$ and for some $\sigma \in \mathrm{Symm}_s \setminus \{id\}$, $I_{s,i}^\sigma = I_{s,i}$ then σ is an algebra automorphism of $I_{s,i}$ and hence we can find its subideal efficiently under GRH by [22], thus, refine $I_{s,i}$ and the m-collection Π.

Note that R5 fails to refine Π only when it is an antisymmetric collection.

It can be easily seen that invariance and antisymmetricity at level s together entail $s! \mid t_s$.

To sum up the algorithm: we keep doing ideal operations in the algebras $\mathcal{A}^{(s)}$, $s \in [m]$ (dictated by the procedures R1 to R5) till either we get a nontrivial factor of $f(x)$ or the underlying m-collection Π becomes a homogeneous, antisymmetric m-scheme on n points. It is routine to show that the time taken by our algorithm is $poly(\log p, n^m)$.

Remark 6. *At this point we are able to reprove Rónyai's result [20]: under GRH, we can deterministically find a nontrivial factor of a degree n polynomial over $\mathbb{F}_p$ in time $poly(\log p, n^r)$, where r is the smallest prime divisor of n. The proof is to try constructing an r-scheme by our algorithm above but by Lemma 1 there exist no homogeneous, antisymmetric r-scheme on n points. This guarantees that our algorithm will indeed find a nontrivial factor of $f(x)$ in this case.*

4. FROM m-SCHEMES TO FACTORING

We saw in the last section how to either find a nontrivial factor of a given $f(x)$ or construct an m-scheme on the n roots of $f(x)$. Our aim is to analyse the "bad case" of the algorithm when we get no nontrivial factor but instead we get an antisymmetric, homogeneous m-scheme. Can the properties of these m-schemes be used to factor $f(x)$? In the rest of the paper we will try to answer that question. But we first need to identify certain special colors in our schemes called *matchings* that help in factoring $f(x)$. Along the way

we also reprove Evdokimov's result [11] in our framework of m-schemes.

Matchings: A color $P \in \mathcal{P}_s$, for $1 < s \leq m$, in an m-scheme $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ is called a *matching* if there exist $1 \leq i < j \leq s$ such that $\pi_i^s(P) = \pi_j^s(P)$ and $|\pi_i^s(P)| = |P|$.

We now show that if our m-scheme has a matching then we can further refine the m-scheme efficiently.

Theorem 7. *Given a degree n polynomial $f(x)$ having n distinct roots in $\mathbb{F}_p$. Assuming GRH, we either nontrivially factor $f(x)$ or we construct a homogeneous, antisymmetric m-scheme having no matchings, deterministically in time poly$(\log p, n^m)$.*

PROOF. We first apply the algorithm given in the last section, say it yields a homogeneous and antisymmetric m-scheme $\Pi = \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ on the n roots $V := \{\alpha \in \mathbb{F}_p | f(\alpha) = 0\}$. For the sake of contradiction assume that a color $P \in \mathcal{P}_s$ is a matching.

Following the notation of the above definition of matchings, it is obvious that both π_i^s and π_j^s are bijections, therefore the map $\pi_i^s(\pi_j^s)^{-1}$ is a permutation of $\pi_j^s(P)$. Furthermore, this permutation is nontrivial as $P \subseteq V^{(s)}$.

So in the corresponding orthogonal ideals decomposition of $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(m)}$, both the maps ι_i^s and ι_j^s give isomorphisms $I_{s-1,\ell'} \to I_{s,\ell}$, where the ideals $I_{s-1,\ell'}$ and $I_{s,\ell}$ correspond to $\pi_j^s(P)$ and P respectively. This means that the map $(\iota_i^s)^{-1}\iota_j^s$ is a nontrivial automorphism of $I_{s-1,\ell'}$. It follows from [22] that, assuming GRH, we can obtain a proper decomposition of $I_{s-1,\ell'}$ and hence refine the m-scheme Π. □

Now we apply the idea of Evdokimov [11] to prove that *antisymmetric* m-schemes always have a matching if we pick $m = \lceil \log_2 n \rceil$.

Lemma 8. *If the m-scheme $\Pi := \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ on n points is antisymmetric at the second level, $|\mathcal{P}_1| < n$ and $m \geq \log_2 n$ then there is a matching in $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$.*

PROOF. We will give an effective way of finding a matching given such a Π. Choose $P_1 \in \mathcal{P}_1$ with $d_1 := |P_1| > 1$. It is clear that $Q_2 := P_1^{(2)}$ is a disjoint union of some colors in $\mathcal{P}_2$. Choose a smallest color $P_2 \in \mathcal{P}_2$ with $P_2 \subseteq Q_2$. By compatibility: $\pi_1^2(P_2) = \pi_2^2(P_2) = P_1$. Also, by antisymmetry we can infer that $d_2 := \frac{|P_2|}{|P_1|} < d_1/2$. If $d_2 = 1$ then observe that P_2 is a matching.

If $d_2 > 1$ then we proceed in the following iterative way. Suppose that, for some $2 < s < m$, we have already chosen colors $P_1 \in \mathcal{P}_1, \ldots, P_{s-1} \in \mathcal{P}_{s-1}$ with $\pi_{i-1}^i(P_i) = \pi_i^i(P_i) = P_{i-1}$ and $1 < d_i := \frac{|P_i|}{|P_{i-1}|} < d_{i-1}/2$ for every $2 \leq i \leq s-1$. Since $d_{s-1} > 1$, the set $Q_s := \{\bar{v} \in V^{(s)} | \pi_{s-1}^s(\bar{v}), \pi_s^s(\bar{v}) \in P_{s-1}\}$ is nonempty. Let P_s be a smallest class from $\mathcal{P}_s$ with $P_s \subseteq Q_s$. Again antisymmetry implies that $d_s := \frac{|P_s|}{|P_{s-1}|} < d_{s-1}/2$. If $d_s = 1$ then P_s is clearly a matching. Otherwise we proceed to the level $(s+1)$ and further halve the subdegree. This procedure finds a matching in at most $\log_2 d_1 \leq \log_2 n$ rounds. □

The above property of matchings together with Theorem 7 gives us that, under GRH, we can completely factor $f(x)$ deterministically in *poly*$(\log p,\ n^{\log n})$ time. This was first proved by Evdokimov [11] by using a framework less general than ours.

For instance, note that the proof of the above lemma requires antisymmetry merely at level 2 of the m-scheme. Indeed, if a compatible and regular m-collection $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ is antisymmetric at level 2 then for every $1 < s \leq m$ and every s-element subset $\{v_1, \ldots, v_s\} \subseteq V$ we have $(v_1, \ldots, v_{s-1}, v_s) \not\equiv_{\mathcal{P}_s} (v_1, \ldots, v_s, v_{s-1})$ (this can be seen by projecting to the last two coordinates), and this is the only use of antisymmetry in the proof of Lemma 8.

4.1 A Conjecture about Matchings

We saw in Lemma 8 that using an m-scheme as large as $m = \lceil \log_2 n \rceil$ is enough. But we conjecture that our m-schemes are special enough to contain a matching even for a (large enough) *constant* m. We support our conjecture by showing that $m = 4$ works in the case of orbit schemes.

Conjecture 9. *There exists a constant $m \geq 4$ such that every homogeneous, antisymmetric m-scheme contains a matching.*

It is clear by Theorem 7 that a proof of this conjecture would result in a deterministic polynomial time algorithm for factoring polynomials over finite fields (under GRH). Interestingly, we prove below the conjecture (with $m = 4$) in the case of orbit schemes. Also, orbit schemes are the only (infinite) family of 4-schemes we currently know that are homogeneous and antisymmetric.

Proof of Conjecture 9 for orbit schemes: We will infact show that every homogeneous, antisymmetric, orbit 4-scheme contains a matching. It is easy to see that the 2-scheme associated to a permutation group G is antisymmetric if and only if $|G|$ is odd. Assume that G is a nontrivial permutation group of odd order on $V = \{1, \ldots, n\}$. Let H be a subgroup minimally containing the stabilizer G_1 of G. Let $B = \mathrm{Orb}(H, 1)$ be the orbit of 1 under the action of H. Then H acts as a primitive permutation group on B. Also, by [24], there is a base of size $s \leq 3$ of H. This is a subset $\{b_1, \ldots, b_s\} \subseteq B$ such that $H_{b_1} \cap \cdots \cap H_{b_s} = N$, where N is the kernel of the permutation representation of H on B. We assume that this base is irredundant, in particular $K = H_{b_1} \cap \cdots \cap H_{b_{s-1}} > N$. Since $K_{b_s} = N < K$ there exists $b_{s+1} \in \mathrm{Orb}(K, b_s) \setminus \{b_s\}$.

In order to simplify notation, we assume $b_1 = 1, b_2 = 2, \ldots, b_{s+1} = s+1$. The first equality $b_1 = 1$ can be ensured using the transitivity of H on B, while the others can be achieved by renumbering V. From $G_1 < H$ we infer that $N = H_1 \cap \cdots \cap H_t = G_1 \cap \cdots \cap G_t$ holds for every $t \in \{1, \ldots, s+1\}$. Let P be the G-orbit of $(1, \ldots, s+1)$. Since $(1, \ldots, s-1, s)$ and $(1, \ldots, s-1, s+1)$ are in the same orbit, we have $\pi_s^{s+1}(P) = \pi_{s+1}^{s+1}(P)$. Also, since the $(1, \ldots, s)$ and $(1, \ldots, s, s+1)$ both have stabilizer N, the size of the orbits of both tuples coincide with $|G : N|$. These properties imply that P is a matching.

5. FACTORING POLYNOMIALS OF SMOOTH PRIME DEGREE

We saw in Section 3 how to obtain a homogeneous m-scheme on n points from a given polynomial of degree n and we also saw in Lemma 2 that a homogeneous 3-scheme is an association scheme. Recently Hanaki and Uno [13] classified the structure of association schemes, on a *prime* number of points, using representation theory. Their result when applied to our m-schemes gives a way to factor polynomials when n is a constant-smooth prime number.

Proof of Main Theorem: Wlog we can assume that $f(x)$ has n distinct roots $V := \{\alpha_1, \ldots, \alpha_n\}$ in $\mathbb{F}_p$. From Section 3 we can again assume that we have constructed a homogeneous antisymmetric $(r+1)$-scheme on n points: $(\mathcal{P}_1, \ldots, \mathcal{P}_{r+1})$. Now from Lemma 2 we know that $(\mathcal{P}_1, \mathcal{P}_2)$ is an antisymmetric association scheme. From [13]: $\exists d|(n-1)$, $\forall P \in \mathcal{P}_2$, $\#P = dn$. If $d = 1$ then we have matchings in $\mathcal{P}_2$ and hence by the proof of Theorem 7 we can find a nontrivial factor of $f(x)$.

On the other hand, if $d > 1$ then the colors in $(\mathcal{P}_2, \ldots, \mathcal{P}_{r+1})$ can be used to define a homogeneous antisymmetric r-scheme on d points as follows: pick some relation $P_0 \in \mathcal{P}_2$ and define $V' := \{\alpha \in V | (\alpha_1, \alpha) \in P_0\}$. Note that $|V'| = d$. Next define an r-collection $\Pi' := (\mathcal{P}'_1, \ldots, \mathcal{P}'_r)$ on V' where for all $i \in [r]$ and for each color $P \in \mathcal{P}_{i+1}$ we put a color $P' \in \mathcal{P}'_i$ such that $P' := \{\bar{v} \in V'^{(i)} | (\alpha_1, \bar{v}) \in P\}$. It is routine to verify that Π' is a homogeneous and antisymmetric r-scheme on d points. As d has a prime divisor which is at most r such a Π' cannot exist by Lemma 1.

The time complexity follows routinely from our algorithm overview. □

6. A (SMALL) STEP TOWARDS SCHEMES CONJECTURE

We saw in Lemma 8 that a homogeneous m-scheme on n points that is antisymmetric at level 2 has a matching below the $\lceil \log_2 n \rceil$-th level. Recall from Section 3 that from a polynomial we can construct an m-scheme that is antisymmetric at *every* level > 1 and not just at level 2. Are we then guaranteed to get a matching at a level less than $\log_2 n$? We conjecture that there should be a matching at a much smaller level (4?) as intuitively antisymmetricity reduces the subdegrees of the colors, but we could currently prove only a constant fraction of $\log_2 n$ upper bound on the number of levels. First we prove the lemma:

Lemma 10. *Let $\Pi = (\mathcal{P}_1, \ldots, \mathcal{P}_4)$ be a homogeneous, antisymmetric 4-scheme on $n > 8$ points. Then there is a color $P \in \mathcal{P}_2$ and its π_3^3-fiber $Q \in \mathcal{P}_3$ such that $\pi_2^3(Q) = \pi_3^3(Q) = P$ and the subdegree of Q over P is less than $\frac{n}{8}$.*

Proof. Clearly, $\mathcal{P}_1$ just has one color, i.e. $[n]$. If $\mathcal{P}_2$ has more than two colors then by antisymmetry it has at least 4 colors and hence one of the colors $P \in \mathcal{P}_2$ will have subdegree over $[n]$ less than $\frac{n}{4}$. Again by antisymmetry there has to be a π_3^3-fiber $Q \in \mathcal{P}_3$ of P having subdegree $< \frac{n}{8}$ and $\pi_2^3(Q) = \pi_3^3(Q) = P$, thus we are done.

In the case when $\mathcal{P}_2$ has just two colors - P and its "flipped" color P^T - let us define:

$$Q_1 := \{x \in [n] \mid (1, x) \in P\}$$
$$Q_2 := \{x \in [n] \mid (1, x) \in P^T\}$$

Then obviously Q_1, Q_2 are disjoint sets of size $n_1 := \frac{n-1}{2}$ partitioning $\{2, \ldots, n\}$. Clearly, the image of the colors in $\mathcal{P}_3$ restricting the first coordinate to 1 gives us an antisymmetric partition Γ of the sets $Q_1^{(2)}$, $Q_1 \times Q_2$, $Q_2 \times Q_1$ and $Q_2^{(2)}$; which is an association scheme on $Q_1^{(2)}$ and $Q_2^{(2)}$. By the antisymmetricity of Π, the colors corresponding to $Q_2 \times Q_1$ are just the transpose (i.e. swap the two coordinates) of those corresponding to $Q_1 \times Q_2$. Each color in Γ can be naturally viewed as a $n_1 \times n_1$ zero/one matrix. For example, a color R corresponding to $Q_1 \times Q_2$ can be represented as a matrix whose rows are indexed by Q_1 and whose columns are indexed by Q_2 such that: for all $(i, j) \in Q_1 \times Q_2$, $R_{i,j} = 1$ if $(i, j) \in R$ and $R_{i,j} = 0$ if $(i, j) \notin R$. Interestingly, in the matrix representation the composition property of Lemma 2 simply means that the linear combinations of the identity matrix I and the colors in the partition of $Q_1 \times Q_1$ (or $Q_2 \times Q_2$) by Γ is a matrix algebra, say $\mathcal{A}_1$ (or $\mathcal{A}_2$).

If $Q_1^{(2)}$ (or $Q_2^{(2)}$) is partitioned by Γ into more than two parts then by antisymmetry there will be ≥ 4 parts which means that one of the parts will have subdegree $< \frac{n}{8}$. This gives us a required π_3^3-fiber $Q \in \mathcal{P}_3$ of a $P \in \mathcal{P}_2$.

So we can assume that $Q_1^{(2)}$ and $Q_2^{(2)}$ are both partitioned into exactly two parts. Say,

- R and R^T are the two matrices representing the partition of $Q_1^{(2)}$ by Γ.
- S and S^T are the two matrices representing the partition of $Q_2^{(2)}$ by Γ.

Note that: $R + R^T = S + S^T = J - I$ where I is the identity matrix and J is the all one matrix of dimensions $n_1 \times n_1$.

How do the partitions of $Q_1 \times Q_2$ look like? Let U be a matrix in the partition of $Q_1 \times Q_2$ by Γ. If $U = J$ (i.e. Γ partitions $Q_1 \times Q_2$ in a trivial way) then by antisymmetricity $\mathcal{P}_3$ has exactly $3! = 6$ colors each of cardinality $n \cdot \#U = n \cdot n_1^2$. But this is a contradiction as $6 \cdot n \cdot n_1^2$ is not $n(n-1)(n-2)$. Thus, Γ partitions $Q_1 \times Q_2$ into at least 2 colors. Now since by antisymmetricity the number of colors in $\mathcal{P}_3$ has to be a multiple of 6, we deduce that Γ partitions $Q_1 \times Q_2$ into at least 4 colors, say, $\{U_1, \ldots, U_4\}$. By the composition property of Γ, $U_1 U_1^T$ is in $\mathcal{A}_1$. In other words, there are positive integers α, β such that:

$$\begin{aligned} U_1 U_1^T &= \alpha I + \beta(R + R^T) \\ &= \beta J + (\alpha - \beta) I \end{aligned}$$

Thus, if U_1 is a singular matrix then $U_1 U_1^T = \beta J$ implying that U_1 has equal rows. We can repeat the same argument with $U_1^T U_1$ (which is in $\mathcal{A}_2$) and deduce that U_1 has equal columns. Now a zero/one matrix U_1 can have equal rows and equal columns iff $U_1 = J$. This contradiction implies that U_1 is an invertible matrix. But then:

$$\{U_1 U_1^T, U_1 U_2^T, U_1 U_3^T, U_1 U_4^T\}$$

is a set of 4 linearly independent matrices in $\mathcal{A}_1$ which contradicts the fact that $\mathcal{A}_1$ is a matrix algebra of dimension 3. This contradiction implies that one of $Q_1^{(2)}$ or $Q_2^{(2)}$ is partitioned into at least four parts.

Thus, in all the cases the lemma is true. □

From the above lemma we see that at 2 levels higher we get a suitable color with subdegree reduced to a fraction of 2^{-3}. This immediately gives us the following constant-factor improvement to Lemma 8.

Proposition 11. *If the m-scheme $\Pi := \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ on n points is antisymmetric at the first three levels, $|\mathcal{P}_1| < n$ and $m \geq \frac{2}{3} \log_2 n$ then there is a matching in $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$.*

7. PRIMITIVITY OF M-SCHEMES AND FURTHER RESEARCH

A 2-scheme $\Pi = (\mathcal{P}_1, \mathcal{P}_2)$ on n points can be viewed as a complete directed colored graph on n vertices, where vertices of one color correspond to a $P \in \mathcal{P}_1$ and the edges of one color correspond to a $Q \in \mathcal{P}_2$. If an m-scheme is coming from a polynomial $f(x)$, over k, then we can try to relate graph properties of the m-scheme to the algebraic properties of the ideals defining the m-scheme. It turns out that such m-schemes can be efficiently tested for one such property: connectivity. One can introduce a related notion - primitivity - which is actually an extension of the primitivity of association schemes. The details had to be left out for the lack of space. We feel that primitivity imposes strong conditions on the parameters of an m-scheme but we do not know how to exactly use primitivity or imprimitivity and leave that for future research.

Acknowledgements. The authors thank Hausdorff Research Institute of Mathematics, Bonn for its hospitality. Research of the first author was also supported by Hungarian Research Fund (OTKA), grants T72845 and T77476. The last author would also like to thank Centrum voor Wiskunde en Informatica, Amsterdam for the postdoc grants BRICKS AFM1 and NWO VICI.

8. REFERENCES

[1] L. Adleman, K. Manders, and G. Miller. On taking roots in finite fields. In *Proc. 18th FOCS*, pages 175–178, 1977.

[2] E. Bach, J. von zur Gathen, and H. W. Lenstra, Jr. Factoring polynomials over special finite fields. *Finite Fields and Their Applications*, 7:5–28, 2001.

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

[4] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24:713–735, 1970.

[5] J. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12:389–410, 1992.

[6] P. J. Cameron. *Permutation Groups*. LMS Student Text 45. Cambridge University Press, Cambridge, 1999.

[7] P. Camion. A deterministic algorithm for factorizing polynomials of $\mathbb{F}_q[x]$. *Ann. Discr. Math.*, 17:149–157, 1983.

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

[9] Q. Cheng and M. A. Huang. Factoring polynominals over finite fields and stable colorings of tournaments. In *ANTS*, pages 233–246, 2000.

[10] S. A. Evdokimov. Factorization of a solvable polynomial over finite fields and the Generalized Riemann Hypothesis. *Zapiski Nauchnyck Seminarov LOMI*, 176:104–117, 1989.

[11] S. A. Evdokimov. Factorization of polynomials over finite fields in subexponential time under GRH. In *Proc. 1st ANTS*, pages 209–219. Lecture Notes In Computer Science 877, Springer-Verlag, 1994.

[12] S. Gao. On the deterministic complexity of factoring polynomials. *J. of Symbolic Computation*, 31(1-2):19–36, 2001.

[13] A. Hanaki and K. Uno. Algebraic structure of association schemes of prime order. *J. Algebraic. Combin.*, 23:189–195, 2006.

[14] M. A. Huang. Generalized Riemann Hypothesis and factoring polynomials over finite fields. *J. Algorithms*, 12:464–481, 1991.

[15] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. *Math. Comp.*, 67:1179–1197, 1998.

[16] M. Mignotte and C.-P. Schnorr. Calcul déterministe des racines d'un polynôme dans un corps fini. *Comptes Rendus Académie des Sciences (Paris)*, 306:467–472, 1988.

[17] I. Miyamoto. A computation of some multiply homogeneous superschemes from transitive permutation groups. In *ISSAC '07: Proceedings of the International Symposium on Symbolic and Algebraic Computation*, pages 293–298, 2007.

[18] R. T. Moenck. On the efficiency of algorithms for polynomial factoring. *Math. Comp.*, 31:235–250, 1977.

[19] M. O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput*, 9:273–280, 1980.

[20] L. Rónyai. Factoring polynomials over finite fields. *Journal of Algorithms*, 9:391–400, 1988.

[21] L. Rónyai. Factoring polynomials modulo special primes. *Combinatorica*, 9:199–206, 1989.

[22] L. Rónyai. Galois groups and factoring polynomials over finite fields. *SIAM J. on Discrete Mathematics*, 5:345–365, 1992.

[23] C. Saha. Factoring polynomials over finite fields using balance test. In *STACS*, pages 609–620, 2008.

[24] A. Seress. The minimal base size of primitive solvable permutation groups. *J. London Math. Soc.*, 53:243–255, 1996.

[25] J. D. H. Smith. Association schemes, superschemes, and relations invariant under permutation groups. *European J. Combin.*, 15(3):285–291, 1994.

[26] J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52:77–89, 1987.

[27] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2:187–224, 1992.

[28] J. Wojdyło. An inextensible association scheme associated with a 4-regular graph. *Graphs and Combinatorics*, 17(1):185–192, 2001.

[29] H. Zassenhaus. On Hensel factorization, I. *J. Number Theory*, 1:291–311, 1969.

[30] P.-H. Zieschang. *Theory of Association Schemes*. Springer, Berlin, 2005.