LMS J. Comput. Math. 17 (1) (2014) 123–140 © 2014 Authors
doi:10.1112/S1461157013000296

Deterministic polynomial factoring and association schemes

Manuel Arora, Gábor Ivanyos, Marek Karpinski and Nitin Saxena

Abstract

The problem of finding a nontrivial factor of a polynomial $f(x)$ over a finite field $\mathbb{F}_q$ has many known efficient, but randomized, algorithms. The deterministic complexity of this problem is a famous open question even assuming the generalized Riemann hypothesis (GRH). In this work we improve the state of the art by focusing on prime degree polynomials; let n be the degree. If $(n-1)$ has a 'large' r-smooth divisor s, then we find a nontrivial factor of $f(x)$ in deterministic $\mathrm{poly}(n^r, \log q)$ time, assuming GRH and that $s = \Omega(\sqrt{n/2^r})$. Thus, for $r = O(1)$ our algorithm is polynomial time. Further, for $r = \Omega(\log\log n)$ there are infinitely many prime degrees n for which our algorithm is applicable and better than the best known, assuming GRH. Our methods build on the algebraic-combinatorial framework of m-schemes initiated by Ivanyos, Karpinski and Saxena (ISSAC 2009). We show that the m-scheme on n points, implicitly appearing in our factoring algorithm, has an exceptional structure, leading us to the improved time complexity. Our structure theorem proves the existence of small intersection numbers in any association scheme that has many relations, and roughly equal valencies and indistinguishing numbers.

1. *Introduction*

We consider the classical problem of finding a nontrivial factor of a given polynomial over a finite field. There exist various randomized polynomial time algorithms for this problem, such as Berlekamp [6], Rabin [41], Cantor and Zassenhaus [12], von zur Gathen and Shoup [51], Kaltofen and Shoup [32], and Kedlaya and Umans [35], but its deterministic time complexity is a longstanding open problem. It pertains to the general derandomization question in computational complexity theory, that is whether any problem solvable in probabilistic polynomial time can also be solved in deterministic polynomial time.

In this paper, we consider the deterministic time complexity of the problem of polynomial factoring over finite fields assuming the generalized Riemann hypothesis (GRH) (Section 3.1). GRH enables us to find primitive rth 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 polynomials of the type $x^r - a$ over $\mathbb{F}_q$ [1]. Assuming GRH, there are many deterministic factoring algorithms known but all of them are super-polynomial time except on special input instances: Rónyai [45] showed that under GRH, any polynomial $f(x) \in \mathbb{Z}[x]$ can be factored modulo p deterministically in polynomial time in the order of the Galois group of $f(x)$, except for finitely many primes p. Rónyai's result generalizes previous work by Huang [29], Evdokimov [17], and Adleman, Manders and Miller [1]. Bach, von zur Gathen and Lenstra [4] 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 $\phi_k(p)$ is the kth cyclotomic polynomial. This result generalizes previous work by Rónyai [44], Mignotte and Schnorr [38], von zur Gathen [50], Camion [11], and Moenck [39].

The line of research which interests us was started by Rónyai [43]. He used GRH to find a nontrivial factor of a polynomial $f(x) \in \mathbb{F}_q[x]$, where $n = \deg f$ has a small prime factor, in deterministic polynomial time. Rónyai's framework relies on the discovery that finding a nontrivial automorphism in certain algebras (such as $\mathcal{A} := \mathbb{F}_q[x]/f(x)$ and its tensor powers) yields an efficient decomposition of these algebras under GRH. Building on Rónyai's ideas,

Received 1 February 2013; revised 3 September 2013.

2010 Mathematics Subject Classification 12Y05, 05E30 (primary), 05E10, 03D15, 68W30 (secondary).

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

Evdokimov [18] showed that an arbitrary degree n polynomial $f(x) \in \mathbb{F}_q[x]$ can be factored deterministically in time $\mathrm{poly}(\log q, n^{\log n})$ under GRH. This line of approach has since been investigated, in an attempt to either remove GRH [30] or improve the time complexity, leading to several analytic number theory, algebraic-combinatorial conjectures and special case solutions [13, 23, 31, 46].

Our method in this paper, building on [31], encompasses the known algebraic-combinatorial (if not analytic number theory) methods and ends up relating the complexity of polynomial factoring to 'purely' combinatorial objects (called *schemes* and *intersection numbers*) that are central to the research area of algebraic combinatorics. The methods of [13, 18, 23, 43, 46] arrange the underlying roots of the polynomial in a combinatorial object that satisfies *some* of the defining properties of schemes. This paper contributes to the understanding of schemes by making progress on a related purely combinatorial conjecture, which is naturally connected with polynomial factoring.

1.1. *Our main result*

We study the problem of finding a nontrivial factor of a polynomial of *prime* degree. Intuitively, this case should not be any easier. However, it turns out that our combinatorial framework is quite well behaved over a prime number of roots and gives an improved time complexity. We call a number $s \in \mathbb{N}$ *r-smooth* if each prime factor of s is at most r.

THEOREM 1.1 (Factoring). *Let $f(x)$ be a polynomial of prime degree n over $\mathbb{F}_q$. Assume $(n-1)$ has an r-smooth divisor s, with $s \geqslant \sqrt{n/\ell} + 1$ and $\ell \in \mathbb{N}_{>0}$. Then we can find a nontrivial factor of $f(x)$ deterministically in time $\mathrm{poly}(\log q, n^{r+\log \ell})$ under GRH.*

Naturally, one asks if there exist infinitely many primes n for which Theorem 1.1 is a significant improvement. A well-known number theory conjecture concerning primes in arithmetic progressions is connected to this question (Section 5.1). Under the conjecture that $L = 2$ is admissible for Linnik's constant [37], we prove that there exist infinitely many primes n for which the time complexity in Theorem 1.1 is polynomial. Even simply under GRH the factoring algorithm has an improved time complexity over the best known ones, for infinitely many n.

COROLLARY 1.2 (Infinite family). *Assuming GRH, there exist infinitely many primes n such that every polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n can be factored deterministically in time $\mathrm{poly}(\log q, n^{\log\log n})$.*

Further, if $L = 2$ is admissible for Linnik's constant, then there exist infinitely many primes n such that every polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n can be factored deterministically in time $\mathrm{poly}(\log q, n)$.

The techniques known before our work do not give a result as strong as ours on this particular infinite family of degrees. The best one could have done before is $\mathrm{poly}(\log q, n^{\log n})$ time, by the general purpose algorithm of Evdokimov [18]. At the core of our algorithmic result lies a new combinatorial theorem; we prove the existence of 'small' intersection numbers in a fairly large class of schemes. The formal statement is Theorem 1.3, together with an evidence of its optimality in Section 5.2. We now motivate the concept of schemes briefly.

1.2. *Idea of m-schemes*

The GRH based algorithm for factoring polynomials over finite fields by Ivanyos *et al.* [31] (called IKS-*algorithm* in the following) relies on the use of combinatorial schemes, more specifically m-schemes (for a given positive integer m). If we denote $[n] := \{1, \ldots, n\}$, then an m-scheme can be described as a partition of the set $[n]^s$, for each $1 \leqslant s \leqslant m$, which satisfies certain natural properties called compatibility, regularity and invariance (Section 2.1). The notion of m-scheme is closely related to the concepts of presuperscheme [54–56],

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

superscheme [48], association scheme [5, 58], coherent configuration [27], cellular algebra [53] and Krasner algebra [36]. Curiously, techniques initiated by [53] are used in another outstanding problem: deciding graph isomorphism. Moreover, coherent configurations provide a natural framework for fast matrix multiplication [15].

The IKS-algorithm (Section 3.2) associates to a polynomial $f(x) \in \mathbb{F}_q[x]$ the natural quotient algebra $\mathcal{A} := \mathbb{F}_q[x]/f(x)$ and explicitly calculates special subalgebras of its tensor powers $\mathcal{A}^{\otimes s}$ $(1 \leqslant s \leqslant m)$. Through a series of operations on systems of ideals of these algebras (which can be performed efficiently under GRH), the IKS-algorithm either finds a zero divisor in $\mathcal{A}$, which is equivalent to factoring $f(x)$, or obtains an m-scheme from the combinatorial structure of $\mathcal{A}^{\otimes s}$ $(1 \leqslant s \leqslant m)$. In the latter case, the m-scheme obtained may be interpreted as the 'reason' why the IKS-algorithm could not find a zero divisor in $\mathcal{A}$. It is not difficult to prove that the IKS-algorithm always finds a zero divisor in $\mathcal{A}$ if we choose m large enough (namely, in the range $\log n$), yielding that the IKS-algorithm deterministically factors $f(x)$ in time $\mathrm{poly}(n^{\log n}, \log q)$. Moreover, it is conjectured that even choosing m as constant, say $m = c$ where $c \geqslant 4$, is enough to find a zero divisor in $\mathcal{A}$ (and hence factor f), which would give the IKS-algorithm a polynomial running time under GRH. This is the subject of the so-called *schemes conjecture* (Section 2.4) on the existence of *matchings* (Sections 2.3 and 3.3).

We note that the schemes conjecture is a purely algebraic-combinatorial conjecture concerning the structure of certain kinds of m-schemes. We also note that the schemes conjecture is already proven for an important class of m-schemes, namely the so-called orbit m-schemes (Theorem 2.7). In this current work, we prove the schemes conjecture for an interesting class of m-schemes on a prime number of points, culminating in a somewhat surprising result about the factorization of prime-degree polynomials. Our proof builds on the strong relationship of m-schemes and association schemes (Section 2.2), and involves fundamental structure results about association schemes of prime order by Hanaki and Uno [25] and Muzychuk and Ponomarenko [40].

1.3. *Idea of association schemes*

Underlying Theorem 1.1 is a structural result about association schemes with bounded valencies and indistinguishing numbers. Recall [40, 58] that an *association scheme* is a pair (X, G) which consists of a finite set X and a partition G of $X \times X$ such that:

(1) G contains the *identity* relation $1 := \{(x, x) \mid x \in X\}$;
(2) if $g \in G$, then $g^* := \{(y, x) \mid (x, y) \in g\} \in G$; and
(3) for all $f, g, h \in G$, there exists an *intersection number* $c^h_{fg} \in \mathbb{N}$ such that for all $(\alpha, \beta) \in h$, $c^h_{fg} = \#\{\gamma \in X \mid (\alpha, \gamma) \in f, (\gamma, \beta) \in g\}$.

An element $g \in G$ is called a *relation* (or *color*) of (X, G). We call $|X|$ the *order* of (X, G). For each $g \in G$, we define its *valency* $n_g := c^1_{gg^*}$, and its *indistinguishing number* $c(g) := \sum_{v \in G} c^g_{vv^*}$.

Whenever it helps, an association scheme can also be thought of as a colored directed graph with X as vertices and G as edges. But it is richer in algebraic structure than a graph and often evokes the feeling 'group theory without groups' [5]. Below we formulate our main scheme theory result; it essentially proves that a large number of relations means the existence of small intersection numbers (assuming bounded valency and indistinguishing number). It is vaguely related to the structural results in the literature that concern the so-called *Schurity* of schemes [19–21, 40]. We are concerned 'merely' with two small intersection numbers and hence we are able to work with better parameters.

THEOREM 1.3 (Small intersection numbers). *Let (X, G) be an association scheme. Assume there exist $c, k, \ell \in \mathbb{N}$ and $0 < \delta_1, \delta_1', \delta_2' \leqslant 1$ with $1 < \ell < (\delta_1^2/\delta_1') \cdot k$ such that for all $1 \neq g \in G$,*

$$\delta_1 \cdot k \leqslant n_g \leqslant \delta_1' \cdot k \quad \text{and} \quad c(g) \leqslant \delta_2' \cdot c.$$

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

If $|G| \geqslant 2(\delta_1'/\delta_1)^3\delta_2' \cdot c/(\ell-1)+2$ *then there exist nontrivial relations* $u \neq v, w \neq w' \in G$ *such that* $0 < c^w_{u^*v} \leqslant c^{w'}_{u^*v} < \ell$.

The above theorem establishes the existence of small intersection numbers in association schemes where both the valencies and indistinguishing numbers of nontrivial relations are confined to a certain range. Interestingly, we give evidence that the result is optimal (Section 5.2). An important example of association schemes of this type are schemes of prime order (Sections 4.1 and 5.2). There the nontrivial relations have equal valency, say k [**25**] and equal indistinguishing numbers $(k-1)$ [**40**].

COROLLARY 1.4 (Prime scheme). *Let* (X, G) *be an association scheme of prime order* $n = |X|$ *and valency* k. *Let* $\ell \in \mathbb{N}_{>1}$. *If* $|G| \geqslant 2(k-1)/(\ell-1)+2$ *then there exist nontrivial relations* $u \neq v, w \neq w' \in G$ *such that* $0 < c^w_{u^*v} \leqslant c^{w'}_{u^*v} < \ell$.

Drawing on the connection of association schemes and m-schemes, we deduce from Corollary 1.4 the existence of *matchings* in certain m-schemes on a prime number of points that helps in algebra decomposition (Section 4.2). This is the prime source of our results in the domain of polynomial factoring.

1.4. *Organization*

Section 2 provides an introduction to the notion of m-schemes and surveys important results and concepts associated therewith. We put a special emphasis on explaining the connection between association schemes and m-schemes (§ 2.2). In § 3 we describe the IKS-algorithm for factoring polynomials over finite fields, which builds on the theory of m-schemes. Theorem 3.4 delineates how to factor polynomials by exploiting m-scheme structure. In § 4 we prove our main results: Theorem 1.1 on the factorization of polynomials of prime degree and Theorem 1.3 on the existence of small intersection numbers in association schemes with bounded valencies and indistinguishing numbers. In addition, § 5 explains how Theorem 1.1 ties in with the density of primes in arithmetic progressions (§ 5.1) and discusses in which sense the bounds given in Theorem 1.3 are optimal (§ 5.2).

2. *Preliminaries: 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 were first defined in [**31**]. They occur naturally as part of the IKS-algorithm for factoring polynomials over finite fields. In the following, we give an overview of the basic theory of m-schemes.

2.1. *Basic definitions*

In this section, we introduce the necessary definitions for the study of m-schemes. For reference purposes, the terminology used here is the same as in the paper [**31**].

s-tuples. Throughout this section, V is an arbitrary set of n distinct elements. For $1 \leqslant s \leqslant n$, we define the set of *essential* s-tuples by

$$V^{(s)} := \{(v_1, v_2, \ldots, v_s) \mid v_1, v_2, \ldots, v_s \text{ are } s \text{ distinct elements of } V\}.$$

Projections. For $s > 1$, we define s projections $\pi^s_1, \pi^s_2, \ldots, \pi^s_s : V^{(s)} \longrightarrow V^{(s-1)}$ by

$$\pi^s_i : (v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_s) \longrightarrow (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_s).$$

Moreover, for $1 \leqslant i_1 < \ldots < i_k \leqslant s$ we define

$$\pi^s_{i_1,\ldots,i_k} : V^{(s)} \longrightarrow V^{(s-k)}, \quad \pi^s_{i_1,\ldots,i_k} = \pi^{s-k+1}_{i_1} \circ \ldots \circ \pi^s_{i_k}.$$

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

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. More accurately, the action of $\tau \in \mathrm{Symm}_s$ on $(v_1, \ldots, v_i, \ldots, v_s) \in V^{(s)}$ is defined as

$$(v_1, \ldots, v_i, \ldots, v_s)^\tau := (v_{\tau(1)}, \ldots, v_{\tau(i)}, \ldots, v_{\tau(s)}).$$

m-Collection. For $1 \leqslant m \leqslant n$, 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 $1 \leqslant s \leqslant m$, the equivalence relation on $V^{(s)}$ corresponding to the partition $\mathcal{P}_s$ will be denoted by $\equiv_{\mathcal{P}_s}$. Moreover, we refer to the elements $P \in \mathcal{P}_s$ as *s-colors*.

Below, we discuss some natural properties of m-collections that are relevant to us. In the following, let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be an m-collection on V.

*P*1 (*Compatibility*). We say that Π is *compatible* at level $1 < s \leqslant m$, if $\bar{u}, \bar{v} \in P \in \mathcal{P}_s$ implies that for every $1 \leqslant i \leqslant s$ 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 $\pi_i^s(P) := \{\pi_i^s(\bar{v}) \mid \bar{v} \in P\}$, for all $1 \leqslant i \leqslant s$, are colors in $\mathcal{P}_{s-1}$.

*P*2 (*Regularity*). We call Π *regular* at level $1 < s \leqslant m$, if $\bar{u}, \bar{v} \in Q \in \mathcal{P}_{s-1}$ implies that for every $1 \leqslant i \leqslant s$ and for every $P \in \mathcal{P}_s$,

$$\#\{\bar{u}' \in P \mid \pi_i^s(\bar{u}') = \bar{u}\} = \#\{\bar{v}' \in P \mid \pi_i^s(\bar{v}') = \bar{v}\}.$$

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

Subdegree. The above two properties motivate the definition of the *subdegree of an s-color P over an $(s-k)$-color Q* as $s(P,Q) := |P|/|Q|$, assuming $\pi^s_{i_1,\ldots,i_k}(P) = Q$ for some $1 \leqslant i_1 < \ldots < i_k \leqslant s$ and that Π is regular at all levels $2, \ldots, s$.

*P*3 (*Invariance*). We say that Π is *invariant* at level $1 < s \leqslant m$, if for every $P \in \mathcal{P}_s$ and $\tau \in \mathrm{Symm}_s$, we have:

$$P^\tau := \{\bar{v}^\tau \mid \bar{v} \in P\} \in \mathcal{P}_s.$$

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

*P*4 (*Homogeneity*). We say that Π is *homogeneous* if $|\mathcal{P}_1| = 1$.

*P*5 (*Antisymmetry*). We say that Π is *antisymmetric* at level $1 < s \leqslant m$, if for every $P \in \mathcal{P}_s$ and $id \neq \tau \in \mathrm{Symm}_s$, we have $P^\tau \neq P$.

*P*6 (*Symmetry*). We say that Π is *symmetric* at level $1 < s \leqslant m$, if for every $P \in \mathcal{P}_s$ and $\tau \in \mathrm{Symm}_s$, we have $P^\tau = P$.

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

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

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

We start with an easy non-existence lemma for m-schemes [31, Lemma 1]. Note that the lemma below puts the main content of [43] in a more general framework.

LEMMA 2.1. *Let $r > 1$ be a divisor of n. Then for $m \geqslant r$ there does not exist a homogeneous and antisymmetric m-scheme on n points.*

Proof. For $m \geqslant r$, clearly every m-scheme contains an r-scheme (hint: project the tuples to the first r places). Hence it suffices to prove the above statement for $m = r$. Suppose for the sake of contradiction that there exists a homogeneous and antisymmetric r-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r\}$ on $V = \{v_1, v_2, \ldots, v_n\}$. Then by definition $\mathcal{P}_r$ partitions $n(n-1)\ldots(n-r+1)$ tuples of $V^{(r)}$ into, say, t_r colors. By antisymmetry, every such color P has $r!$ associated colors, namely $\{P^\tau \mid \tau \in \mathrm{Symm}_r\}$. Moreover, by homogeneity, the size of every color at level r is divisible by n. Hence, $r!n \mid n(n-1)\ldots(n-r+1)$. But this implies $r!mid(n-1)\ldots(n-r+1)$, which contradicts $r \mid n$. Therefore, Π cannot exist. □

In the following section, we describe the relationship between m-schemes and association schemes.

2.2. 3-*schemes from association schemes*

The notion of m-schemes is closely related to the concept of association schemes. Association schemes are standard combinatorial objects for which there exists extensive literature [5, 9, 10, 16, 58]. We recall some important identities which involve the valencies of association schemes. Note that the identities given below can all be found in [58].

LEMMA 2.2. *Let (X, G) be an association scheme and let $d, e, f \in G$. The following hold:*

(i) $c_{de}^{f} = c_{e^* d^*}^{f^*}$;

(ii) $c_{df}^{e} \cdot n_e = c_{ef^*}^{d} \cdot n_d$;

(iii) $\sum_{g \in G} c_{ge}^{f} = n_{e^*}$;

(iv) $\sum_{g \in G} c_{ef}^{g} \cdot n_g = n_e \cdot n_f$.

We now show that the concepts of 3-scheme and association scheme are essentially equivalent (strictly speaking, the former is a refinement of the latter). The following lemma states that the first two levels of any 3-scheme constitute an association scheme (up to containment of the identity relation).

LEMMA 2.3. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ be a homogeneous 3-scheme on the set $V = \{v_1, v_2, \ldots, v_n\}$. Then $(V, \mathcal{P}_2 \cup \{1\})$ constitutes an association scheme, where $1 = \{(v, v) \mid v \in V\}$ denotes the identity relation.*

Proof. We prove that for all $P_i, P_j, P_k \in \mathcal{P}_2$, there exists an integer c_{ij}^{k} such that for all $(\alpha, \beta) \in P_k$,

$$c_{ij}^{k} = \#\{\gamma \in V \mid (\alpha, \gamma) \in P_i, (\gamma, \beta) \in P_j\}.$$

The trivial case where at least one of P_i, P_j, P_k is the identity relation is omitted. By the compatibility and regularity of Π at level 3, there exists a subset $\mathcal{S} \subseteq \mathcal{P}_3$ such that for all $(\alpha, \beta) \in P_k$, the set $\{\gamma \in V \mid (\alpha, \gamma) \in P_i, (\gamma, \beta) \in P_j\}$ can be partitioned as

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

By the compatibility of Π at level 3, this partition can simply be written as

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

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

By the regularity of Π at level 3, the size of each set in the above partition is $|P|/|P_k|$, which means that

$$\#\{\gamma \in V \mid (\alpha,\gamma) \in P_i, (\gamma,\beta) \in P_j\} = \sum_{P \in \mathcal{S}} \frac{|P|}{|P_k|}.$$

Since the above equation is independent of the choice of $(\alpha,\beta) \in P_k$, it follows that $(V, \mathcal{P}_2 \cup \{1\})$ is an association scheme. □

The next lemma states that, in turn, every association scheme also naturally gives rise to a 3-scheme.

LEMMA 2.4. *Let $(V,\mathcal{P}_2)$ be an association scheme on $V = \{v_1, v_2, \ldots, v_n\}$. Let $\equiv_{\mathcal{P}_2}$ denote the equivalence relation on $V \times V$ corresponding to the partition $\mathcal{P}_2$. Let $\mathcal{P}_3$ be the partition of $V^{(3)}$ such that for 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*

$$(u_1,u_2) \equiv_{\mathcal{P}_2} (v_1,v_2), \quad (u_1,u_3) \equiv_{\mathcal{P}_2} (v_1,v_3), \quad (u_2,u_3) \equiv_{\mathcal{P}_2} (v_2,v_3).$$

Then $\{\{V\}, \mathcal{P}_2 - \{1\}, \mathcal{P}_3\}$ is a homogeneous 3-scheme.

Proof. It is an easy exercise to show that $\{\{V\}, \mathcal{P}_2 - \{1\}, \mathcal{P}_3\}$ satisfies compatibility, regularity and invariance. □

2.3. *Matchings*

We now define the notion of *matchings*, certain special colors of m-schemes that play an important role in the IKS-factoring algorithm described later. This combinatorial object, matching, provides an algebraic object: ideal automorphism. As before, let $V = \{v_1, v_2, \ldots, v_n\}$ be a set of n distinct elements and let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be an m-scheme on V.

Matching. A color $P \in \mathcal{P}_s$ at any level $1 < s \leqslant m$ is called a *matching* if for some positive integer k there exists $1 \leqslant i_1 < \ldots < i_k \leqslant s$ and $1 \leqslant j_1 < \ldots < j_k \leqslant s$ with $(i_1,\ldots,i_k) \neq (j_1,\ldots,j_k)$ such that $\pi^s_{i_1,\ldots,i_k}(P) = \pi^s_{j_1,\ldots,j_k}(P)$ and $|\pi^s_{i_1,\ldots,i_k}(P)| = |P|$.

Note that the paper [31] which originally defined the concept of matchings had the restriction that $k = 1$. The above definition is broader and constitutes a natural generalization of the previous (limited) notion of matchings. The next theorem gives an important sufficient condition for the existence of matchings in m-schemes [31, Lemma 8].

THEOREM 2.5. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be an m-scheme on the set $V = \{v_1, v_2, \ldots, v_n\}$. Assume Π is antisymmetric at level 2. Moreover, assume there exist colors $P_t \in \mathcal{P}_t$ and $P_{t-1} := \pi^t_i(P_t) \in \mathcal{P}_{t-1}$ for some $1 < t < m$ and $1 \leqslant i \leqslant t$ such that $1 < s(P_t, P_{t-1}) = |P_t|/|P_{t-1}| \leqslant \ell$ and $m \geqslant t - 1 + \log_2 \ell$, where $\ell \in \mathbb{N}$. Then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$.*

Proof. Without loss of generality, let us assume that $P_{t-1} = \pi^t_t(P_t) \in \mathcal{P}_{t-1}$. We outline an iterative way of finding a matching in Π. Note that the set

$$U_{t+1} := \{\bar{v} \in V^{(t+1)} \mid \pi^{t+1}_t(\bar{v}), \pi^{t+1}_{t+1}(\bar{v}) \in P_t\}$$

is a nonempty union of colors in $\mathcal{P}_{t+1}$. Let P_{t+1} be a color of $\mathcal{P}_{t+1}$ such that $P_{t+1} \subseteq U_{t+1}$. Then by the antisymmetry of Π we have

$$s(P_{t+1}, P_t) = \frac{|P_{t+1}|}{|P_t|} < \frac{s(P_t, P_{t-1})}{2} \leqslant \frac{\ell}{2}.$$

Evidently, if $s(P_{t+1}, P_t) = 1$ then P_{t+1} is a matching. Otherwise, if $s(P_{t+1}, P_t) > 1$ we proceed to level $t+2$ and again strictly halve the subdegree (by the same argument as above). This procedure finds a matching in at most $\log_2 \ell$ rounds. □

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

As an easy consequence of the above theorem, we obtain the following corollary.

COROLLARY 2.6. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be a homogeneous m-scheme on the set $V = \{v_1, v_2, \ldots, v_n\}$. Let Π be antisymmetric at level 2. If $m \geqslant \log_2 n$ then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$.*

2.4. *The schemes conjecture*

In Corollary 2.6 it was shown that every antisymmetric m-scheme on n points (for large enough m) contains a matching between levels 1 and $\log_2 n$. Below, we formulate a conjecture which asserts the existence of a constant $c \geqslant 4$ that could replace the above $\log_2 n$-bound.

SCHEMES CONJECTURE. *There exists a constant $c \geqslant 4$ such that every homogeneous, antisymmetric m-scheme with $m \geqslant c$ contains a matching.*

In Section 3 we recall [**31**] that, under GRH, the correctness of the schemes conjecture implies a deterministic polynomial time algorithm for the factorization of polynomials over finite fields (Theorem 3.4). The schemes conjecture is especially motivated by the fact that it is known to be true for an important class of m-schemes, called *orbit schemes*. An exact definition of orbit schemes follows. Let $V = \{v_1, v_2, \ldots, v_n\}$ be a set of n distinct elements and $G \leqslant \mathrm{Symm}_V$ a permutation group. Fix $1 \leqslant m \leqslant n$. For $1 \leqslant s \leqslant m$, let $\mathcal{P}_s$ be the partition on $V^{(s)}$ such that for any two s-tuples $(u_1, u_2, \ldots, u_s)$ and $(v_1, v_2, \ldots, v_s)$, we have $(u_1, u_2, \ldots, u_s) \equiv_{\mathcal{P}_s} (v_1, v_2, \ldots, v_s)$ if and only if

$$\exists \sigma \in G : \quad (\sigma(u_1), \sigma(u_2), \ldots, \sigma(u_s)) = (v_1, v_2, \ldots, v_s).$$

Then $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ is an m-scheme on V. We call m-schemes which arise in the above-described manner *orbit m-schemes*. Note that $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ is homogeneous if and only if G acts transitively on V. Moreover, note that $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ is antisymmetric if and only if $\gcd(m!, |G|) = 1$. Orbit m-schemes suggest that the notion of m-schemes generalizes that of finite permutation groups.

THEOREM 2.7 (Schemes conjecture for orbit m-schemes). *For $m \geqslant 4$, every homogeneous, antisymmetric orbit m-scheme contains a matching.*

Proof. This is shown in [**31**, § 4.1]. □

3. *Preliminaries: the IKS-algorithm*

In this section, we discuss the GRH based IKS-algorithm for factoring polynomials over finite fields [**31**]. It fundamentally relies on the theory of m-schemes. It was shown in [**31**] that the IKS-algorithm has a deterministic polynomial running time for factoring polynomials of prime degree n, where $(n-1)$ is a *constant-smooth* number. In Section 4, we significantly improve this result to polynomials of prime degree n, where $(n-1)$ has a *large* constant-smooth factor. This relaxation implies that under a well-known number theory conjecture involving Linnik's constant, there are infinitely many primes n such that any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n can be factored by the IKS-algorithm in time $\mathrm{poly}(n, \log q)$.

3.1. *Algebraic prerequisites*

We now discuss algebraic prerequisites for the description of the IKS-algorithm. Below, we recapitulate some of the basic concepts of polynomial factoring over finite fields.

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

Associated quotient algebra $\mathcal{A}$. In order to solve polynomial factoring over finite fields, it is enough to factor polynomials $f(x)$ of degree n over $\mathbb{F}_q$ that have n distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}_q$ [6, 7]. Given a polynomial $f(x) \in \mathbb{F}_q[x]$, for any field extension $k \supseteq \mathbb{F}_q$, we have the *associated quotient algebra*

$$\mathcal{A} := k[x]/(f(x)).$$

It is isomorphic to the direct product of n fields. In the following, we interpret $\mathcal{A}$ as the algebra of all functions

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

The factors of $f(x)$ appear as zero divisors in $\mathcal{A}$. Assume $y(x)z(x) = 0$ for some nonzero polynomials $y(x), z(x) \in \mathcal{A}$. Then $f(x) \mid y(x) \cdot z(x)$, which implies $\gcd(f(x), z(x))$ factors $f(x)$ nontrivially. Since the gcd of polynomials can be computed by the Euclidean algorithm in deterministic polynomial time, factoring $f(x)$ is, up to polynomial time reductions, equivalent to finding a zero divisor in $\mathcal{A}$.

Ideals of $\mathcal{A}$ and roots of $f(x)$. For an ideal I of $\mathcal{A}$, we define the *support* of I as

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

Via the support, ideal decompositions of $\mathcal{A}$ induce partitions on the set V. This is the subject of the following lemma.

LEMMA 3.1. *If $I_1, \ldots, I_t$ are pairwise orthogonal ideals of $\mathcal{A}$ (that is $I_i I_j = 0$ for all $i \neq j$) such that $\mathcal{A} = I_1 + \ldots + I_t$, then V can be partitioned as*

$$V = \mathrm{Supp}(I_1) \sqcup \ldots \sqcup \mathrm{Supp}(I_t).$$

Tensor powers of $\mathcal{A}$. For $1 \leqslant m \leqslant n$, we denote by $\mathcal{A}^{\otimes m}$ the mth tensor power of $\mathcal{A}$ (as k-modules). We may regard $\mathcal{A}^{\otimes m}$ as the algebra of all functions from V^m to k. In this interpretation, the rank one tensor element $h_1 \otimes \ldots \otimes h_m$ corresponds to a function that maps $(v_1, \ldots, v_m) \mapsto h_1(v_1) \ldots h_m(v_m)$.

Essential part of tensor powers. We define the *essential part* $\mathcal{A}^{(m)}$ of $\mathcal{A}^{\otimes m}$ to be the (unique) ideal of $\mathcal{A}^{\otimes m}$ 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 $i \neq j$. One may interpret $\mathcal{A}^{(m)}$ as the algebra of all functions $V^{(m)} \longrightarrow k$.

Ideals of $\mathcal{A}^{(m)}$ and roots of $f(x)$. As in the case $m = 1$, we define the *support* of an ideal I of $\mathcal{A}^{(m)}$ as

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

Using this convention, Lemma 3.1 can be generalized as follows.

LEMMA 3.2. *For $s \leqslant n$, if $I_{s,1}, \ldots, I_{s,t_s}$ are pairwise orthogonal ideals of $\mathcal{A}^{(s)}$ such that $\mathcal{A}^{(s)} = I_{s,1} + \ldots + I_{s,t_s}$, then $V^{(s)}$ can be partitioned as*

$$V^{(s)} = \mathrm{Supp}(I_{s,1}) \sqcup \ldots \sqcup \mathrm{Supp}(I_{s,t_s}).$$

Connection with GRH. As we already mentioned, the IKS-algorithm relies on the assumption of the generalized Riemann hypothesis (GRH) [8, 14, 42]. We formally state the hypothesis below. Recall that a *Dirichlet character*, of *order* $k \in \mathbb{N}_{>1}$, is defined as a completely multiplicative arithmetic function $\chi : (\mathbb{Z}, +) \longrightarrow (\mathbb{C}, \cdot)$ such that $\chi(n + k) = \chi(n)$ for all n, and $\chi(n) = 0$ whenever $\gcd(n, k) > 1$. Given a Dirichlet character χ, we define the

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

corresponding *Dirichlet L-function* by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for all complex numbers s with real part greater than 1. By analytic continuation, this function can be extended to a meromorphic function defined on all of $\mathbb{C}$. The generalized Riemann hypothesis asserts that, for every Dirichlet character χ, the zeros of $L(\chi, s)$ in the *critical strip* $0 < \mathrm{Re}\ s < 1$ all lie on the *critical line* $\mathrm{Re}\ s = 1/2$.

Under the assumption of GRH, Rónyai [45] showed that the knowledge of any explicit nontrivial automorphism $\sigma \in \mathrm{Aut}(\mathcal{A})$ of $\mathcal{A}$ immediately gives us a nontrivial factor of $f(x)$. The latter result is used in the routine of the IKS-algorithm. In [45], the ability of computing *radicals* (rth roots for prime r) in finite fields is used. This can be done assuming GRH by a result of Huang [28]. Thus, GRH 'acts' in fact through Huang's result. The motivating case of a prime field and $r = 2$ can be easily explained by Ankeny's theorem [2] on the smallest primitive root.

3.2. *Description of the IKS-algorithm*

We will now describe the routine of the IKS-algorithm. In the following, let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree n having n distinct roots $V = \{\alpha_1, \ldots, \alpha_n\}$ in $\mathbb{F}_q$. For some field extension $k \supseteq \mathbb{F}_q$, let $\mathcal{A} := k[x]/(f(x))$ be the associated quotient algebra. With regards to the algorithm, we assume $\mathcal{A}$ is given by structure constants with respect to some basis $b_1, \ldots, b_n$. It was shown in [31, Lemma 4] that we can efficiently compute the essential parts $\mathcal{A}^{(s)}$ $(1 \leqslant s \leqslant n)$.

LEMMA 3.3. *A basis for* $\mathcal{A}^{(m)} = (k[X]/(f(X)))^{(m)}$ *over* $k \supseteq \mathbb{F}_q$ *can be computed by a deterministic algorithm in time* $\mathrm{poly}(\log |k|, n^m)$.

We now proceed to give an overview of the routine of the IKS-algorithm. Namely, we describe how an m-scheme can be obtained from the ideal decompositions of the essential parts $\mathcal{A}^{(s)}$ $(1 \leqslant s \leqslant n)$. For referential purposes, let us quickly recapitulate the algorithmic data.

Input. A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n having n distinct roots $V = \{\alpha_1, \ldots, \alpha_n\}$ in $\mathbb{F}_q$.

Also $1 < m \leqslant n$ is given, and we can assume that we have the smallest field extension $k \supseteq \mathbb{F}_q$ having sth nonresidues for all $1 \leqslant s \leqslant m$ (computing k will take $\mathrm{poly}(\log q, m^m)$ time under GRH).

Output. A nontrivial factor of $f(x)$ or a homogeneous, antisymmetric m-scheme on $V = \{\alpha_1, \ldots, \alpha_n\}$. (In the latter case we get the m-scheme only implicitly via a system of ideals of $\mathcal{A}^{(m)}$.)

Description of the algorithm. We define $\mathcal{A}^{(1)} = \mathcal{A} = k[x]/(f(x))$ and compute the essential parts $\mathcal{A}^{(s)}$ $(1 < s \leqslant m)$ of the tensor powers of $\mathcal{A}$ (this takes $\mathrm{poly}(\log q, n^m)$ time by Lemma 3.3).

Automorphisms and ideal decompositions of $\mathcal{A}^{(s)}$ $(1 < s \leqslant m)$. Observe that for each $\tau \in \mathrm{Symm}_s$, the map defined by

$$\tau : \mathcal{A}^{(s)} \longrightarrow \mathcal{A}^{(s)}, \quad (b_{i_1} \otimes \ldots \otimes b_{i_s})^{\tau} \mapsto b_{i_{1^\tau}} \otimes \ldots \otimes b_{i_{s^\tau}}$$

is an algebra automorphism of $\mathcal{A}^{(s)}$. By [45], this knowledge of explicit automorphisms of $\mathcal{A}^{(s)}$ can be used to efficiently decompose $\mathcal{A}^{(s)}$ under GRH: namely, one can compute mutually orthogonal ideals $I_{s,1}, \ldots, I_{s,t_s}$ $(t_s \geqslant 2)$ of $\mathcal{A}^{(s)}$ such that

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

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

By Lemma 3.2, the above decomposition of $\mathcal{A}^{(s)}$ induces a partition $\mathcal{P}_s$ on $V^{(s)}$:

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

Together with $\mathcal{P}_1 := \{V\}$ this yields an m-collection $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ on V.

We will now show how to refine the m-collection Π 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 $\mathcal{A}^{(s-1)} \longrightarrow \mathcal{A}^{(s)}$. For each $1 < s \leqslant m$ we define s natural algebra embeddings $\iota_1^s, \ldots, \iota_s^s : \mathcal{A}^{\otimes(s-1)} \longrightarrow \mathcal{A}^{\otimes s}$ which map $b_{i_1} \otimes \ldots \otimes b_{i_{s-1}}$ to $b_{i_1} \otimes \ldots \otimes b_{i_{j-1}} \otimes 1 \otimes b_{i_j} \otimes \ldots \otimes b_{i_{s-1}}$ respectively (for the s positions of 1). By restricting ι_j^s to $\mathcal{A}^{(s-1)}$ and multiplying its image by the identity element of $\mathcal{A}^{(s)}$, we obtain s algebra embeddings $\mathcal{A}^{(s-1)} \longrightarrow \mathcal{A}^{(s)}$ denoted also by $\iota_1^s, \ldots, \iota_s^s$. In the following, we interpret $\iota_j^s(\mathcal{A}^{(s-1)})$ as the set of functions $V^{(s)} \longrightarrow k$ which do not depend on the jth coordinate.

The algorithm is now best described by explaining the five kinds of refinement procedures which *implicitly* refine Π. (Remember we cannot see V but only have access to it via the ideal $\langle f \rangle$.)

R1 (*Compatibility*). If for any $1 < s \leqslant m$, 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 $I_{s,i'}$ and thus, refine $I_{s,i'}$ and the m-collection Π.

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

R2 (*Regularity*). If for any $1 < s \leqslant m$, 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 $I_{s-1,i}$ and thus, refine $I_{s-1,i}$ and the m-collection Π.

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

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

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

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

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

R5 (*Antisymmetry*). If for some $1 < s \leqslant m$, for some ideal $I_{s,i}$ and for some $\tau \in \mathrm{Symm}_s \setminus \{id\}$, we have $I_{s,i}^{\tau} = I_{s,i}$, then τ is an algebra automorphism of $I_{s,i}$. By [45], this means we can find a subideal of $I_{s,i}$ efficiently under GRH and hence, refine $I_{s,i}$ and the m-collection Π.

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

Summary. The algorithm executes the ideal operations R1–R5 described above on $\mathcal{A}^{(s)}$ $(1 \leqslant s \leqslant m)$ until either we get a nontrivial factor of $f(x)$ or the underlying m-collection Π becomes a homogeneous, antisymmetric m-scheme on V. It is routine to verify that the time complexity of the IKS-algorithm is $\mathrm{poly}(\log q, n^m)$.

3.3. *From m-schemes to factoring*

We saw in the last subsection how to either find a nontrivial factor of a given $f(x)$ or construct an m-scheme on the n roots of $f(x)$. In the following, we explain how to deal with the 'bad

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

case', when we get a homogeneous, antisymmetric m-scheme instead of a nontrivial factor. We will see how the properties of homogeneous and antisymmetric m-schemes can be used to obtain a nontrivial factorization of $f(x)$ even in this case. The next theorem is of crucial importance (it is [**31**, Theorem 7] extended to our general notion of matchings).

THEOREM 3.4 (Matchings refine). *Let $f(x)$ be a polynomial of degree n over $\mathbb{F}_q$ having n distinct roots $V = \{\alpha_1, \ldots, \alpha_n\}$ in $\mathbb{F}_q$. Assuming GRH, we either find a nontrivial factor of $f(x)$ or we construct a homogeneous, antisymmetric m-scheme on V having no matchings, deterministically in time* $\mathrm{poly}(\log q, n^m)$.

Proof. We apply the algorithm from Section 3.2. Suppose it yields a homogeneous, antisymmetric m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ on V. For the sake of contradiction, assume that some color $P \in \mathcal{P}_s$ is a matching. Let $1 \leqslant i_1 < \ldots < i_k \leqslant s$ and $1 \leqslant j_1 < \ldots < j_k \leqslant s$ with $(i_1, \ldots, i_k) \neq (j_1, \ldots, j_k)$ be such that $\pi^s_{i_1,\ldots,i_k}(P) = \pi^s_{j_1,\ldots,j_k}(P)$ and $|\pi^s_{i_1,\ldots,i_k}(P)| = |P|$. Then $\pi^s_{i_1,\ldots,i_k}(\pi^s_{j_1,\ldots,j_k})^{-1}$ is a nontrivial permutation of $\pi^s_{i_1,\ldots,i_k}(P)$. For the corresponding orthogonal ideal decompositions of $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(m)}$, this means that the embeddings

$$\iota^s_{i_1,\ldots,i_k} := \iota^s_{i_1} \circ \ldots \circ \iota^{s-k+1}_{i_k}, \quad \iota^s_{j_1,\ldots,j_k} := \iota^s_{j_1} \circ \ldots \circ \iota^{s-k+1}_{j_k}$$

both give isomorphisms $I_{s-k,l'} \longrightarrow I_{s,l}$, where the ideals $I_{s-k,l'}$ and $I_{s,l}$ correspond to $\pi^s_{i_1,\ldots,i_k}(P)$ and P, respectively. Hence, the map $(\iota^s_{i_1,\ldots,i_k})^{-1}\iota^s_{j_1,\ldots,j_k}$ is a nontrivial automorphism of $I_{s-k,l'}$. By [**45**], this means we can find a subideal of $I_{s-k,l'}$ efficiently under GRH and thus, refine the m-scheme Π. □

Combining the above result with Corollary 2.6, we conclude that one can completely factor $f(x)$ in time $\mathrm{poly}(\log q, n^{\log n})$ under GRH. This reproves Evdokimov's result [**18**], which is based on a framework less general than that of m-schemes described above. Note that any progress towards the schemes conjecture (Section 2.4) will directly result in an improvement of the time complexity of the IKS-algorithm. A proof of the schemes conjecture, for parameter c, would imply that the total time taken for the factorization of $f(x)$ would improve to $\mathrm{poly}(\log q, n^c)$.

In the special case that $f(x)$ is a polynomial of prime degree n, where $(n-1)$ satisfies certain divisibility conditions, we study the structure of association schemes of prime order to show that for a 'small' m the 'bad' case in Theorem 3.4 never happens. This is discussed in the following section.

4. *Factoring prime-degree polynomials*

In this section we show that the IKS-algorithm has polynomial running time for the factorization of polynomials $f(x) \in \mathbb{F}_q[x]$ of prime degree n, where $(n-1)$ has a large constant-smooth factor. By this we mean a number $s \in \mathbb{N}$ of magnitude $\sqrt{n/\ell}$ such that $s \mid (n-1)$ and all prime factors of s are smaller than r. The exact relationship between ℓ, r and the time will appear later. Previously, the IKS-algorithm was only known to have polynomial running time for the factorization of polynomials of prime degree n, where $(n-1)$ is constant-smooth [**31**]. Our new results imply that under a well-known number theory conjecture involving Linnik's constant, there are infinitely many primes n such that any polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n can be factored by the IKS-algorithm in time $\mathrm{poly}(\log q, n)$. As a main tool, we employ structural results about association schemes of prime order, most notably [**25**, **40**].

4.1. *Schemes with bounded valencies and indistinguishing numbers*

We now prove Theorem 1.3, which concerns the existence of small intersection numbers in association schemes (with bounded valencies and indistinguishing numbers) assuming a large

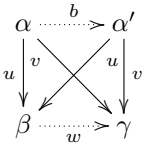
https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

number of relations. Note that Theorem 1.3 is the principal scheme theory result underlying our main theorem about the factorization of prime degree polynomials (Theorem 1.1). It is a counting argument on the graph of the scheme. It is elementary assuming the fundamental theorems about schemes, but it yields a new interesting property for this class of schemes.

Proof of Theorem 1.3. Fix a relation $1 \neq u \in G$ and a pair $(\alpha, \beta) \in u$. For all $v \in G \setminus \{1, u\}$, define

$$S_v := \{(\alpha', \gamma) \in X^2 \mid (\alpha', \beta) \in u; (\alpha, \gamma) \neq (\alpha', \gamma) \in v\}.$$

The set S_v consists of those pairs $(\alpha', \gamma) \in X^2$ which together with (α, β) form a non-degenerate quadrilateral of the type seen below.



We determine the cardinality of S_v. Note that for any relation $b \in G$, there are exactly c^u_{bu} choices for $\alpha' \in X$ such that $(\alpha, \alpha') \in b$ and $(\alpha', \beta) \in u$. Moreover, after choosing α', there are exactly $c^b_{vv^*}$ choices for $\gamma \in X$ such that $(\alpha, \gamma), (\alpha', \gamma) \in v$. Thus, $|S_v| = \sum_{b \in G} c^u_{bu} \cdot c^b_{vv^*}$. In particular,

$$\sum_{v \in G \setminus \{1,u\}} |S_v| = \sum_{1 \neq b \in G} c^u_{bu} \cdot \sum_{v \in G \setminus \{1,u\}} c^b_{vv^*} \leqslant \sum_{1 \neq b \in G} c^u_{bu} \cdot \delta_2' \cdot c \leqslant \delta_1' \cdot \delta_2' \cdot c \cdot k,$$

where the last inequality follows from Lemma 2.2(iii).

For the sake of contradiction, assume that for all $v \in G \setminus \{1, u\}$ we have either $c^w_{u^*v} = 0$ or $c^w_{u^*v} \geqslant \ell$ for all except at most one relation $w \in G$. We derive a lower bound on $|S_v|$ in order to obtain the contradiction. For $v \in G \setminus \{1, u\}$ define

$$W_v := \{w \in G \mid c^w_{u^*v} \neq 0\}.$$

Note that for each relation $w \in W_v$ there are exactly $c^u_{vw^*}$ choices for γ such that $(\beta, \gamma) \in w$ and $(\alpha, \gamma) \in v$. Moreover, after choosing γ, there are exactly $c^w_{u^*v} - 1$ choices for α' such that $(\alpha', \beta) \in u$ and $(\alpha', \gamma) \in v$. Thus, $|S_v| = \sum_{w \in W_v} c^u_{vw^*} \cdot (c^w_{u^*v} - 1)$. Now observe that $c^u_{vw^*} \geqslant c^w_{u^*v} \cdot (\delta_1/\delta_1')$ for all $w \in W_v$ by Lemma 2.2(i), (ii). Since we assume that $c^w_{u^*v} \geqslant \ell$ for all except at most one relation $w \in W_v$ we conclude

$$|S_v| \geqslant \frac{\delta_1}{\delta_1'} \cdot \sum_{w \in W_v} c^w_{u^*v}(c^w_{u^*v} - 1) \geqslant \frac{\delta_1}{\delta_1'} \cdot \left((\ell - 1) \cdot \sum_{w \in W_v} c^w_{u^*v} - \frac{\ell^2}{4} \right).$$

Note that the last inequality is based on the summand-wise inequality: $(\ell-1)c^w_{u^*v} - c^w_{u^*v}(c^w_{u^*v} - 1) \leqslant (\ell^2/4)$. From the equation $\sum_{w \in W_v} c^w_{u^*v} \cdot n_w = n_{u^*} \cdot n_v$ (see Lemma 2.2(iv)) it follows that $\sum_{w \in W_v} c^w_{u^*v} \geqslant (\delta_1^2/\delta_1') \cdot k$. Moreover, using the assumption $1 < \ell < (\delta_1^2/\delta_1') \cdot k$, we deduce

$$|S_v| \geqslant \frac{\delta_1}{\delta_1'} \cdot (\ell - 1) \cdot \left(\frac{\delta_1^2}{\delta_1'} \cdot k - \frac{\ell^2}{4(\ell - 1)} \right) > \frac{\delta_1^3}{2(\delta_1')^2} \cdot (\ell - 1)k.$$

In particular, we have

$$\sum_{v \in G \setminus \{1,u\}} |S_v| > (|G| - 2) \cdot \frac{\delta_1^3}{2(\delta_1')^2} \cdot (\ell - 1)k.$$

This yields $\delta_1'\delta_2' \cdot ck > (|G|-2) \cdot (\delta_1^3/2(\delta_1')^2) \cdot (\ell-1)k$ and hence $2(\delta_1'/\delta_1)^3\delta_2' \cdot (c/(\ell-1)) + 2 > |G|$, a contradiction. □

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

Let us now consider the special case where (X, G) is an association scheme of prime order $n := |X|$. Hanaki–Uno's theorem [25] tells us that in this case, there exists $k \in \mathbb{N}$ such that $k = n_g$ for all $1 \neq g \in G$ (that is all nontrivial valencies coincide). We will refer to k simply as the *valency* of (X, G). It was shown in [40, Theorem 3.2] that for prime order association schemes (X, G) of valency k, every nontrivial relation $g \in G$ has indistinguishing number $c(g) = (k-1)$. Combining the above considerations with Theorem 1.3, we immediately obtain Corollary 1.4 about prime order association schemes.

4.2. *Factoring algorithm for prime-degree polynomials*

Drawing on the scheme theory results from the preceding subsection, we obtain the following lemma about the existence of matchings in homogeneous antisymmetric m-schemes on a prime number of points.

LEMMA 4.1. *Let $\Pi = \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ be a homogeneous, antisymmetric m-scheme on V, where $n := |V|$ is a prime number. Let k denote the valency of the association scheme $(V, \mathcal{P}_2 \cup \{1\})$. Assume that $m \geqslant 2\log_2 \ell + 3$ and $|\mathcal{P}_2| \geqslant 2(k-1)/(\ell-1) + 1$ for some $\ell \in \mathbb{N}_{>1}$. Then there exists a matching in Π.*

Proof. By Corollary 1.4, there exist nontrivial relations $u \neq v, w \neq w' \in \mathcal{P}_2$ such that $0 < c^w_{u^*v} \leqslant c^{w'}_{u^*v} < \ell$. Hence there exist $\alpha, \beta, \gamma, \gamma' \in V$ such that $(\alpha, \beta) \in u$, $(\alpha, \gamma), (\alpha, \gamma') \in v$, $(\beta, \gamma) \in w$ and $(\beta, \gamma') \in w'$. Clearly, the relation $P \in \mathcal{P}_4$ containing the tuple $(\beta, \alpha, \gamma, \gamma')$ satisfies $\pi^4_{1,3}(P) = \pi^4_{1,4}(P) = v$. Also, $|P|/|v| = |P|/|u| \leqslant c^w_{u^*v} \cdot c^{w'}_{u^*v} \leqslant \ell^2$, thus P has subdegree at most ℓ^2 over v. Now if $s(P, v) = 1$ then P is a matching. On the other hand, if $s(P, v) > 1$ then we define $Q := \pi^4_4(P) \in \mathcal{P}_3$ and consider the equation $s(P, v) = s(P, Q) \cdot s(Q, v)$. It implies that at least one of the subdegrees $s(P, Q), s(Q, v)$ is both at least 2 and at most ℓ^2, thus we get a matching in Π by suitably invoking Theorem 2.5. □

Using the above lemma about the existence of matchings in m-schemes on a prime number of points, we can now prove our main result, Theorem 1.1.

Proof of Theorem 1.1. Let $\ell' := (2\ell + 1)$. It suffices to consider the case that $f(x)$ has n distinct roots $V = \{\alpha_1, \ldots, \alpha_n\}$ in $\mathbb{F}_q$. Let $m := \max\{r + 1, 2\log_2 \ell' + 3\}$. We apply the IKS-algorithm (Section 3) and by Theorem 3.4 either find a nontrivial factor of $f(x)$ or construct a homogeneous, antisymmetric m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ on V having no matchings, deterministically in time $\mathrm{poly}(\log q, n^m)$. Suppose for the sake of contradiction that the latter case occurs.

Clearly, $(V, \mathcal{P}_2 \cup \{1\})$ is an association scheme of prime order n, where 1 denotes the trivial relation. Thus, by Hanaki–Uno's theorem [25] there exists $k \mid (n-1)$ such that $|P| = kn$ for all $P \in \mathcal{P}_2$. Hence, $|\mathcal{P}_2| = (n-1)/k$. We distinguish between the following two cases.

Case I: $\gcd(s, k) = 1$. Then $|\mathcal{P}_2| = (n-1)/k \geqslant s \geqslant \sqrt{2n/(\ell'-1)} + 1$. Thus,

$$k < \sqrt{n(\ell'-1)/2} = \sqrt{2n/(\ell'-1)} \cdot (\ell'-1)/2 \leqslant (s-1)(\ell'-1)/2,$$

implying $|\mathcal{P}_2| \geqslant s > 1 + 2k/(\ell'-1)$. In particular, Π contains a matching by Theorem 4.1, contrary to our assumption.

Case II: $\gcd(s, k) > 1$. The colors in $\{\mathcal{P}_2, \ldots, \mathcal{P}_{r+1}\}$ can be used to define a homogeneous, antisymmetric r-scheme on k points as follows: pick $P_0 \in \mathcal{P}_2$ and define $V' := \{\alpha \in V \mid (\alpha_1, \alpha) \in P_0\}$. Furthermore, define an r-collection $\Pi' = \{\mathcal{P}'_1, \ldots, \mathcal{P}'_r\}$ on V' such that for all $1 \leqslant i \leqslant r$ and for each color $P \in \mathcal{P}_{i+1}$, we put a color $P' \in \mathcal{P}'_i$ such that

$$P' := \{\bar{v} \in V'^{(i)} \mid (\alpha_1, \bar{v}) \in P\}.$$

Then $|V'| = k$, and $\Pi' = \{\mathcal{P}'_1, \ldots, \mathcal{P}'_r\}$ is a homogeneous, antisymmetric r-scheme on k points. On the other hand, by $\gcd(s, k) > 1$ we know that k has a prime divisor which is at most r; therefore, Π' cannot exist by Lemma 2.1. □

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

5. *Number theory considerations*

In the present section, we point out that, under a well-known number theory conjecture involving Linnik's constant, there are infinitely many primes n for which the time complexity in Theorem 1.1 is polynomial.

5.1. *Primes n of Theorem 1.1*

Linnik's theorem in number theory answers a natural question about primes in arithmetic progressions. For coprime integers a, s such that $1 \leqslant a \leqslant s-1$, let $p(a,s)$ denote the smallest prime in the arithmetic progression $\{a+is\}_i$. Linnik's theorem states that there exist (effective) constants $c, L > 0$ such that

$$p(a,s) < cs^L.$$

There has been much effort directed towards determining the smallest admissible value for the *Linnik constant* L. The smallest admissible value currently known is $L = 5$, as proven by Xylouris [**57**]. It has been conjectured numerous times that $L \leqslant 2$ [**26**, **33**, **34**, **47**] as noted below.

Conjecture 1. There exists $c > 0$ such that for all coprime integers a, s with $1 \leqslant a \leqslant s-1$, the smallest prime $p(a,s)$ in the arithmetic progression $\{a + is \mid i \in \mathbb{N}\}$ satisfies $p(a,s) < cs^2$.

Note that the above conjecture is not known to be true under GRH. The result that comes closest to it, is [**3**, Theorem 5.3]: $p(a,s) < 2(s \log s)^2$.

Let us consider how the primes of the type we described in Theorem 1.1 relate to $p(1,s)$. This is the subject of Corollary 1.2, which we prove below.

Proof of Corollary 1.2. For the first part, we just assume GRH. Let $r \in \mathbb{N}_{>1}$ be a constant and $s \in \mathbb{N}$ a (large enough) r-smooth number. By [**3**, Theorem 5.3] there is a prime $n = p(1,s) < 2(s \log s)^2$. Hence, $s > \sqrt{n/2}/\log\, s \geqslant (\sqrt{n/2}/\log\, n) + 1 = \sqrt{n/(2\log^2 n)} + 1$. Thus, we can generate infinitely many primes n such that Theorem 1.1 applies for $\ell := \ell(n) = 2\log^2 n$, and proves a time complexity of $\mathrm{poly}(\log q, n^{\log\log n})$.

For the second part, we additionally assume Conjecture 1. Let $r \in \mathbb{N}_{>1}$ be a constant and $s \in \mathbb{N}$ a (large enough) r-smooth number. By the conjecture there is a prime $n = p(1,s) < cs^2$. Thus, $s > \sqrt{n/c} \geqslant \sqrt{n/(c+1)} + 1$. Thus, we can generate infinitely many primes n such that Theorem 1.1 applies for $\ell := (c+1)$, and proves a time complexity of $\mathrm{poly}(\log q, n)$. □

5.2. *Optimality of Theorem 1.3*

Naturally, one asks if it is possible to further relax the conditions which Theorem 1.1 places on the prime number n (that is the degree of the polynomial we want to factor). In our current framework, this translates to asking to what extent we can relax the conditions for the existence of small intersection numbers in schemes of bounded valency and indistinguishing number (Theorem 1.3). However, the example of the *cyclotomic scheme* below shows that the conditions of Theorem 1.3 cannot be relaxed (up to constant factors).

Recall the definition of a cyclotomic scheme [**16**, **24**]. Let p be a prime and let $e \mid (p-1)$. Let α be a generator of the multiplicative group $\mathbb{F}_p^*$ of the field $\mathbb{F}_p$. We denote by $\langle \alpha^e \rangle$ the subgroup generated by α^e. Let $\mathcal{P} := \{P_i \mid 0 \leqslant i \leqslant e\}$ be the partition on $\mathbb{F}_p \times \mathbb{F}_p$ such that $P_0 := \{(x,x) \mid x \in \mathbb{F}_p\}$ and

$$P_i := \{(x,y) \in \mathbb{F}_p \times \mathbb{F}_p \mid x - y \in \alpha^i \langle \alpha^e \rangle\}$$

for $i = 1, \ldots, e$. Then it can be checked that $(X,G) = (\mathbb{F}_p, \mathcal{P})$ is an association scheme. Moreover, the definition of $(\mathbb{F}_p, \mathcal{P})$ does not depend on the choice of the generator α. We call $(\mathbb{F}_p, \mathcal{P})$ the *cyclotomic scheme in* (p,e).

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

In the following, let $(\mathbb{F}_p, \mathcal{P})$ be the cyclotomic scheme in (p, e) as above and let $k := (p-1)/e$. For nontrivial relations $P_r, P_s, P_t \in \mathcal{P}$ and $(x, y) \in P_t$, we have

$$\begin{aligned} c_{rs}^t &= \#\{z \in \mathbb{F}_p \mid (x-z) \in \alpha^r\langle\alpha^e\rangle, (z-y) \in \alpha^s\langle\alpha^e\rangle\} \\ &= \#\{(y_1, y_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^* \mid \alpha^r y_1^e + \alpha^s y_2^e = (x-y)\}/e^2. \end{aligned}$$

We divide by e^2 because that is exactly the number of *repetitions* of a value (y_1^e, y_2^e) as we vary $y_1, y_2 \in \mathbb{F}_p^*$.

By the Hasse–Weil bound [49, 52], we have

$$|\#\{(y_1, y_2) \in \mathbb{F}_p \times \mathbb{F}_p \mid \alpha^r y_1^e + \alpha^s y_2^e = (x-y)\} - (p+1)| \leqslant e^2\sqrt{p} + O(1),$$

from which it follows that

$$\left| c_{rs}^t - \frac{(p+1)}{e^2} \right| \leqslant \sqrt{p} + O(1).$$

To make the 'error' term small, we fix p and e such that $e = k^{1/3}/c \succeq p^{1/4}$ for a large enough constant $c \in \mathbb{N}$ (note that there are infinitely many primes p for which there exists such e by [22, Theorem 7]). Now $(p+1)/e^2 \geqslant 2\sqrt{p}$ and we can estimate that

$$c_{rs}^t > \frac{k}{2e} > (c/2) \cdot k^{2/3} \succeq p^{1/2}.$$

Also, $|G| > e \geqslant k/(ck^{2/3})$. Thus, we have an association scheme where both the number of relations and the intersection numbers are large, that is in the range $k^{\frac{1}{3}}$ and $k^{\frac{2}{3}}$, respectively. This matches the parameters of Corollary 1.4 exactly.

This proves that our scheme theory result, especially Corollary 1.4, is optimal. But when $|G|$ is larger than $k^{1/3}$ the Hasse–Weil bound has too large an error. We do not know whether new 'small' nonzero intersection numbers start showing up.

6. *Conclusion*

We studied polynomial factoring over finite fields, under GRH, mainly through algebraic-combinatorial techniques. These are very effective when the polynomial has a prime degree. We are able to give an infinite family of prime degrees for which our analysis is much better than the known techniques.

The main open question here is to extend this study to factor all prime degree polynomials. The key here is to study the underlying m-scheme that the factoring algorithm gets 'stuck' with. Its 3-subscheme is a nice association scheme (it is equi-valenced). Since its intersection numbers, and other deeper representation theory invariants, manifest in the higher levels of the m-scheme, the schemes conjecture (Section 2.4) might be approachable.

Another question is to slightly improve Corollary 1.4. We do show that it cannot be improved in generality, but that does not rule out the following improvement: there exist at least two constant-small intersection numbers when $|G| \approx k/\log k$. This would be enough to give an infinite family of primes n so that Theorem 1.1 has a polynomial time complexity (only assuming GRH).

Finally, we leave the question of extending Theorem 1.3, so that it becomes applicable to composite order association schemes, open. Improvements there would likely translate to factoring polynomials of new composite degrees.

Acknowledgements. This work was done while M.A. and N.S. were employed in the Hausdorff Center for Mathematics, Bonn (HCM). We would like to thank HCM and the Department of Computer Science, University of Bonn for its support. Especially, for hosting G.I. for a crucial part of the research, and for helping organize a related workshop on algebraic-combinatorial techniques. We thank Sergei Evdokimov, Akihide Hanaki, Mikhail

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

Muzychuk, Ilya Ponomarenko, Igor Shparlinski and Paul-Hermann Zieschang for the many fruitful conversations. Especially, M.A. is grateful to Ilya for the numerous, still ongoing, discussions, explanations and pointers.

References

1. L. Adleman, K. Manders and G. Miller, 'On taking roots in finite fields', *Proceedings of the 18th FOCS* (1977) 175–178.
2. N. C. Ankeny, 'The least quadratic non residue', *Ann. of Math.* (2) 55 (1952) 65–72.
3. E. Bach and J. Sorenson, 'Explicit bounds for primes in residue classes', *Math. Comput.* 65 (1996) 1717–1735.
4. E. Bach, J. von zur Gathen and H. W. Lenstra Jr, 'Factoring polynomials over special finite fields', *Finite Fields Appl.* 7 (2001) 5–28.
5. E. Bannai and T. Ito, *Algebraic combinatorics I: association schemes* (Benjamin-Cummings, 1984).
6. E. R. Berlekamp, 'Factoring polynomials over finite fields', *Bell Syst. Tech. J.* 46 (1967) 1853–1859.
7. E. R. Berlekamp, 'Factoring polynomials over large finite fields', *Math. Comp.* 24 (1970) 713–735.
8. P. Borwein, S. Choi, B. Rooney and A. Weirathmueller (eds), *The Riemann hypothesis: a resource for the afficionado and virtuoso alike*, CMS Books in Mathematics (Springer, 2008).
9. R. C. Bose and D. M. Mesner, 'On linear associative algebras corresponding to association schemes of partially balanced designs', *Ann. Math. Statist.* 30 (1959) 21–38.
10. R. C. Bose and K. R. Nair, 'Partially balanced incomplete block designs', *Sankhyā* 4 (1939) 337–372.
11. P. Camion, 'A deterministic algorithm for factorizing polynomials of $\mathbb{F}_q[x]$', *Ann. Discrete Math.* 17 (1983) 149–157.
12. D. G. Cantor and H. Zassenhaus, 'A new algorithm for factoring polynomials over finite fields', *Math. Comput.* 36 (1981) 587–592.
13. Q. Cheng and M. A. Huang, 'Factoring polynomials over finite fields and stable colorings of tournaments', *Proceedings of the 4th ANTS* (2000) 233–246.
14. S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem* (Gordon and Breach, 1965).
15. H. Cohn and C. Umans, 'Fast matrix multiplication using coherent configurations', Preprint, 2012, arXiv:1207.6528.
16. P. Delsarte, 'An algebraic approach to the association schemes of coding theory', Technical Report, Philips Research Reports, Supplement No. 10, 1973.
17. S. A. Evdokimov, 'Factorization of a solvable polynomial over finite fields and the generalized Riemann hypothesis', *Zap. Nauchn. Sem. LOMI* 176 (1989) 104–117.
18. S. A. Evdokimov, 'Factorization of polynomials over finite fields in subexponential time under GRH', *Proc. 1st ANTS*, Lecture Notes in Computer Science 877 (Springer, 1994) 209–219.
19. S. A. Evdokimov and I. N. Ponomarenko, 'Separability number and Schurity number of coherent configurations', *Electron. J. Combin.* 7 (2000).
20. S. A. Evdokimov and I. N. Ponomarenko, 'Characterization of cyclotomic schemes and normal Schur rings over a cyclic group', *St. Petersburg Math. J.* 14 (2003) 189–221.
21. S. A. Evdokimov and I. N. Ponomarenko, 'Permutation group approach to association schemes', *European J. Combin.* 30 (2009) 1456–1476.
22. K. Ford, 'The distribution of integers with a divisor in a given interval', *Ann. of Math.* (2) 168 (2008) 367–433.
23. S. Gao, 'On the deterministic complexity of factoring polynomials', *J. Symbolic Comput.* 31 (2001) 19–36.
24. R. W. Goldbach and H. L. Claasen, 'Cyclotomic schemes over finite rings', *Indag. Math.* 3 (1992) 301–312.
25. A. Hanaki and K. Uno, 'Algebraic structure of association schemes of prime order', *J. Algebraic Combin.* 23 (2006) 189–195.
26. D. R. Heath-Brown, 'Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression', *Proc. Lond. Math. Soc.* 64 (1992) 265–338.
27. D. G. Higman, 'Coherent configurations I', *Rend. Semin. Mat. Univ. Padova* 44 (1970) 1–25.
28. M. A. Huang, 'Factorization of polynomials over finite fields and factorization of primes in algebraic number fields', *Proceedings of the 16th Annual ACM Symposium on Theory of Computing (STOC)* (1984) 175–182.
29. M. A. Huang, 'Generalized Riemann hypothesis and factoring polynomials over finite fields', *J. Algorithms* 12 (1991) 464–481.
30. G. Ivanyos, M. Karpinski, L. Rónyai and N. Saxena, 'Trading GRH for algebra: algorithms for factoring polynomials and related structures', *Math. Comput.* 81 (2012) 493–531.
31. G. Ivanyos, M. Karpinski and N. Saxena, 'Schemes for deterministic polynomial factoring', *34th International Symposium on Symbolic and Algebraic Computation*, 2009, 191–198.
32. E. Kaltofen and V. Shoup, 'Subquadratic-time factoring of polynomials over finite fields', *Math. Comput.* 67 (1998) 1179–1197.
33. H. J. Kanold, 'Elementare Betrachtungen zur Primzahltheorie', *Arch. Math.* 14 (1963) 147–151.

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press

34. H. J. Kanold, 'Über Primzahlen in Arithmetischen Folgen', *Math. Ann.* 156 (1964) 393–395.
35. K. S. Kedlaya and C. Umans, 'Fast polynomial factorization and modular composition', *SIAM J. Comput.* 40 (2011) 1767–1802.
36. M. Krasner, 'Une généralisation de la notion de corps', *J. Math. Pures Appl.* 17 (1938) 367–385.
37. Y. V. Linnik, 'On the least prime in an arithmetic progression I. The basic theorem', *Rec. Math.* (*Mat. Sbornik*) *N.S.* 15 (1944) 139–178.
38. M. Mignotte and C. P. Schnorr, 'Calcul déterministe des racines d'un polynôme dans un corps fini', *C. R. Math. Acad. Sci.* 306 (1988) 467–472.
39. R. T. Moenck, 'On the efficiency of algorithms for polynomial factoring', *Math. Comp.* 31 (1977) 235–250.
40. M. Muzychuk and I. Ponomarenko, 'On pseudocyclic association schemes', *ARS Math. Contemp.* 5 (2012) 1–25.
41. M. O. Rabin, 'Probabilistic algorithms in finite fields', *SIAM J. Comput.* 9 (1980) 273–280.
42. B. Riemann, 'Über die Anzahl der Primzahlen unter einer gegebenen Grösse', *Monatsberichte Berliner Akad.*, 1859.
43. L. Rónyai, 'Factoring polynomials over finite fields', *J. Algorithms* 9 (1988) 391–400.
44. L. Rónyai, 'Factoring polynomials modulo special primes', *Combinatorica* 9 (1989) 199–206.
45. L. Rónyai, 'Galois groups and factoring polynomials over finite fields', *SIAM J. Discrete Math.* 5 (1992) 345–365.
46. C. Saha, 'Factoring polynomials over finite fields using balance test', *25th STACS* (2008) 609–620.
47. A. Schinzel and W. Sierpinski, 'Sur certaines hypothèses concernant les nombres premiers', *Acta Arith.* 4 (1958) 345–365.
48. J. D. H. Smith, 'Association schemes, superschemes, and relations invariant under permutation groups', *European J. Combin.* 15 (1994) 285–291.
49. J. Voight, 'Curves over finite fields with many points: an introduction', *Computational aspects of algebraic curves*, Lecture Notes Series on Computing 13 (ed. Shaska Tanush; World Scientific, Hackensack, NJ, 2005) 124–144.
50. J. von zur Gathen, 'Factoring polynomials and primitive elements for special primes', *Theoret. Comput. Sci.* 52 (1987) 77–89.
51. J. von zur Gathen and V. Shoup, 'Computing Frobenius maps and factoring polynomials', *Comput. Complexity* 2 (1992) 187–224.
52. A. Weil, *Courbes Algébriques et Variétés Abelienne* (Hermann, 1971).
53. Y. B. Weisfeiler and A. A. Lehman, 'Reduction of a graph to a canonical form and an algebra which appears in this process (Russian)', *Sci.-Technol. Investig.* 9 (1968) 12–16.
54. J. Wojdyło, 'Relation algebras and t-vertex condition graphs', *European J. Combin.* 19 (1998) 981–986.
55. J. Wojdyło, 'An inextensible association scheme associated with a 4-regular graph', *Graphs Combin.* 1 (2001) 185–192.
56. J. Wojdyło, 'Presuperschemes and colored directed graphs', *JCMCC* 38 (2001) 45–54.
57. T. Xylouris, 'Über die Nullstellen der Dirichletschen L-Funktionen und die Kleinste Primzahl in einer Arithmetischen Progression', PhD Thesis, Mathematisch-Naturwissenschaftliche Fakultät der Universität Bonn, 2011.
58. P.-H. Zieschang, *Theory of association schemes* (Springer, 2005).

Manuel Arora
Department of Computing and Mathematical Sciences
California Institute of Technology
Pasadena, CA 91125
USA
arora@caltech.edu

Gábor Ivanyos
Institute for Computer Science and Control
Hungarian Academy of Sciences (MTA SZTAKI)
Kende u. 13-17, H-1111 Budapest
Hungary
Gabor.Ivanyos@sztaki.mta.hu

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

Nitin Saxena
Department of Computer Science and Engineering
IIT Kanpur
Kanpur 208016
India
nitin@cse.iitk.ac.in

https://doi.org/10.1112/S1461157013000296 Published online by Cambridge University Press