Extensibility of Association Schemes and GRH-Based Deterministic Polynomial Factoring

Dissertation

zur

Erlangung des Doktorgrades (Dr. rer. nat.)

der

Mathematisch-Naturwissenschaftlichen Fakultät

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

vorgelegt von

Manuel Arora

aus

Lohne (Oldenburg)

Bonn, Januar 2013

Angefertigt mit Genehmigung der Mathematisch-Naturwissenschaftlichen

Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn

1. Gutachter: Prof. Dr. Nitin Saxena

2. Gutachter: Prof. Dr. Marek Karpinski

Tag der Promotion: 12. März 2013

Erscheinungsjahr: 2013

Contents

Contents **iii**

Synopsis **1**

1 Introduction **5**

1.1 Polynomial Factoring over Finite Fields 5

1.2 Extensibility of Association Schemes 10

1.3 Efficient Matrix Multiplication 12

2 Association Schemes **15**

2.1 Basic Notions 16

2.2 The Adjacency Algebra 19

2.3 Character Theory of Association Schemes 21

2.4 Characters of the Complex Adjacency Algebra 25

2.5 Association Schemes of Prime Order 30

2.6 Association Schemes with Bounded Valencies and Indistinguishing Numbers 35

3 m-Schemes **41**

3.1 Basic Notions 42

3.2 3-Schemes from Association Schemes 45

3.3 Orbit m-Schemes 47
3.4 Matchings 48
3.5 The Schemes Conjecture 50
3.6 An Improved Matching Bound 52

4 GRH-Based Deterministic Polynomial Factoring 57
4.1 Algebraic Prerequisites 59
4.2 Description of the IKS-algorithm 61
4.3 From m-Schemes to Factoring 65
4.4 Factoring Prime Degree Polynomials 67
4.5 Connection to Linnik's Constant 69

5 Extensibility of Association Schemes 73
5.1 Height t Presuperschemes 74
5.2 Adjacency Tensors 78
5.3 The Association Scheme Extension Algorithm 80
5.4 Computational Results 85

6 Efficient Matrix Multiplication using Association Schemes 87
6.1 The Exponent of Matrix Multiplication 88
6.2 The Cohn-Umans Approach 90
6.3 Connection to Association Schemes 92

7 Conclusion 95

Acknowledgments 99

Bibliography 101

Index 113

Synopsis

The subject of the present work, titled "Extensibility of Association Schemes and GRH-Based Polynomial Factoring", is the application of the theory of combinatorial schemes to problems in computational algebra. The principal notions of combinatorial schemes which are studied in this work are *association schemes* (Bannai & Ito (1984), Zieschang (1996, 2005)), *m-schemes* (Ivanyos, Karpinski & Saxena (2009), Arora *et al.* (2012)), and *presuper-schemes* (Smith (1994, 2007), Wojdyło (1998, 2001)). The main computational problems considered in this work are polynomial factoring over finite fields, the *Schurity problem* of association schemes (and its relaxation in the notion of *extensibility*), and matrix multiplication. We show that each of the latter problems admits a deep connection to the theory of combinatorial schemes, and describe natural algebraic-combinatorial frameworks which capture the essence of their algebraic complexity. As a logical application, we delineate how structural results for combinatorial schemes can translate to fundamental improvements in the realm of computational algebra.

Consider the classical problem of finding a nontrivial factor of a given polynomial $f(x)$ over a finite field $\mathbb{F}_q$. This problem 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). A large part of this work is devoted to the recent results by

Arora *et al.* (2012), which improve the state of the art of polynomial factoring by putting the focus on prime degree polynomials. Suppose $f(x)$ is a polynomial of prime degree n. We show that if $(n-1)$ has a 'large' r-smooth divisor s, then it is possible to find a nontrivial factor of $f(x)$ in deterministic $\mathrm{poly}(n^r, \log q)$ time; assuming GRH and that $s = \Omega(\sqrt{n/2^r})$. In particular, for $r = O(1)$ we have a polynomial time algorithm. Further, for $r = \Omega(\log\log n)$ there are infinitely many prime degrees n for which the algorithm is applicable and better than the best known; assuming GRH. The framework underlying the above results builds on the algebraic-combinatorial notions of association schemes and m-schemes. We show that the m-schemes on n points which implicitly appear in the factoring algorithm have an exceptional structure; leading to the improved time complexity. The structure theorem at the heart of this argument proves the existence of small intersection numbers in any association scheme that has many relations, and roughly equal valencies and indistinguishing numbers. We note that this structure theorem could also be of independent (combinatorial) interest.

A related topic, which represents another focal point of this work, is the notion of extensibility of association schemes, which was introduced by Arora & Zieschang (2012). An association scheme $\mathfrak{X} = (Q, \Gamma)$ is said to be extensible to height t if $\mathfrak{X}$ is associated to a height t presuperscheme. Smith (1994, 2007) showed that an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ is Schurian (i.e. induced by a group) iff $\mathfrak{X}$ is extensible to height $(d-2)$. In this work, we formalize the maximal height $t_{\max}(\mathfrak{X})$ of an association scheme $\mathfrak{X}$ as the largest number $t \in \mathbb{N}$ such that $\mathfrak{X}$ is extensible to height t (we also include the possibility $t_{\max}(\mathfrak{X}) = \infty$, which is equivalent to $t_{\max}(\mathfrak{X}) \geq (d-2)$). Intuitively, the maximal height provides a natural measure of how close an association scheme is to being

Schurian. Moreover, the maximal height lies at the core of the question under which conditions certain types of m-schemes can be 'embedded' into a larger $(m+k)$-scheme (where $k > 0$); the latter observation links the notion of the maximal height to the subject of polynomial factoring. For computing the maximal height, we introduce the association scheme extension algorithm, which on input an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$, decides in time $d^{O(t)}$ if the scheme $\mathfrak{X}$ is extensible to height t. In particular, if t is a fixed constant, then the running time of the association scheme extension algorithm is polynomial in the order of $\mathfrak{X}$. The association scheme extension algorithm is used to show that all non-Schurian association schemes up to order 26 are completely inextensible, i.e. they are not extensible to any positive height $t \in \mathbb{N}_{>0}$. The above results may be viewed as a first step towards understanding the algebraic and combinatorial properties possessed by association schemes which are extensible to a certain height; the latter topic is of particular interest for the polynomial factoring connection delineated in this work.

As an additional application of the theory of association schemes to problems in algebraic complexity, we describe the recent approach by Cohn & Umans (2012) to efficient matrix multiplication. The term 'efficient matrix multiplication' refers to the problem of minimizing the number of arithmetic operations necessary to multiply two matrices with entries in some field k. We outline here why the problem is considered to be central in computational algebra and theoretical computer science as a whole, describe some of the past breakthroughs in obtaining upper bounds on the matrix multiplication exponent ω, and delineate in detail the Cohn-Umans 'algebra-embedding' approach and the progress it has made towards the famous open conjecture $\omega = 2$. In addition, we describe how association schemes and their adjacency

algebras pertain to the Cohn-Umans fast matrix multiplication framework, and explain their important role in further research plans.

The material in this work is organized as follows. Chapter 1 provides a detailed overview of the concepts and problems which represent our main topics of study. Chapter 2 introduces the notion of association schemes, which is central throughout the whole of this work – and discusses important and recent structural results in association scheme theory. In Chapter 3, we define the concept of m-schemes and describe properties of this object which are intimately connected to the subject of polynomial factoring over finite fields. In Chapter 4, we delineate the GRH-based IKS-framework for polynomial factoring over finite fields (Ivanyos, Karpinski & Saxena (2009), Arora *et al.* (2012)), which builds on the theory of m-schemes. Moreover, we describe how structural results for association schemes and m-schemes may be used to obtain improvements in the domain of polynomial factoring via the IKS-framework. Chapter 5 introduces the notion of extensibility of association schemes, a concept closely related to both the Schurity problem of association schemes and the IKS-polynomial factoring framework. Chapter 6 delineates the recent framework of Cohn & Umans (2012) for efficient matrix multiplication, which connects the complexity of matrix multiplication to purely combinatorial properties of association schemes and their *adjacency algebras*. Chapter 7 provides a conclusion of the methods and results depicted in this work, and considers some of the questions which were left open.

Chapter 1

Introduction

In the following, we provide a detailed overview of the concepts and problems which are central throughout the whole of this work. §1.1 introduces the problem of polynomial factoring over finite fields, and outlines the idea of the IKS polynomial factoring framework [IKS09, AIKS12] which is based on the theory of combinatorial schemes. §1.2 provides an overview of the notion of extensibility of association schemes, which is connected to both the Schurity problem of association schemes and the IKS-polynomial factoring framework. §1.3 introduces the subject of efficient matrix multiplication, and discusses a new approach to this topic, suggested by Cohn and Umans [CU12], which centers around a scheme-theoretic framework.

1.1 Polynomial Factoring over Finite Fields

We consider the classical problem of finding a nontrivial factor of a given polynomial over a finite field. This problem is known to admit randomized polynomial time algorithms, such as Berlekamp [Ber67], Rabin [Rab80], Cantor & Zassenhaus [CZ81], von zur Gathen & Shoup [vzGS92], Kaltofen

& Shoup [KS98], and Kedlaya & Umans [KU11], but its deterministic time complexity is a longstanding open problem. The computational problem of polynomial factoring over finite fields is embedded into the larger derandomization question in computational complexity theory, i.e. whether any problem solvable in probabilistic polynomial time can also be solved in deterministic polynomial time.

In this work, we consider the deterministic time complexity of polynomial factoring over finite fields assuming the generalized Riemann hypothesis (GRH) (see Section 4.1). GRH ensures that we efficiently 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 polynomials of the type $x^r - a$ over $\mathbb{F}_q$ [AMM77]. There are many known GRH-based deterministic factoring algorithms but all of them are super-polynomial time except on special input instances: Rónyai [Rón92] showed that under GRH, any polynomial $f(x) \in \mathbb{Z}[x]$ can be factored modulo p deterministically in time polynomial in the order of the Galois group of $f(x)$, except for finitely many primes p. Rónyai's result generalizes previous work by Huang [Hua91], Evdokimov [Evd89], and Adleman, Manders & Miller [AMM77]. Bach, von zur Gathen & Lenstra [BvzGL01] 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 k-th cyclotomic polynomial. This result generalizes previous work by Rónyai [Rón89], Mignotte & Schnorr [MS88], von zur Gathen [vzG87], Camion [Cam83], and Moenck [Moe77].

The line of research which the present work connects to was started by Rónyai [Rón88]. There GRH was used 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. The framework of Rónyai [Rón88] 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 the work of Rónyai, Evdokimov [Evd94] showed that an arbitrary degree n polynomial $f(x) \in \mathbb{F}_q[x]$ can be factored deterministically in time $\text{poly}(\log q, n^{\log n})$ under GRH. Since Evdokimov's work, there have been several attempts to either remove GRH [IKRS12] or improve the time complexity, leading to several analytic number theory, algebraic-combinatorial conjectures and special case solutions [CH00, Gao01, Sah08, IKS09, AIKS12].

In this work, we delineate the methods of [IKS09, AIKS12], which subsume the known algebraic-combinatorial approaches to polynomial factoring over finite fields [Rón88, Evd94, CH00, Gao01, Sah08]. The framework which we describe here relates the complexity of polynomial factoring to 'purely' combinatorial objects (called *schemes*) that are central to the research area of algebraic combinatorics. Note that the methods of [Rón88, Evd94, CH00, Gao01, Sah08] arrange the underlying roots of the polynomial in a combinatorial object that satisfies *some* of the defining properties of schemes. In this work, we further the understanding of schemes by making progress on a related combinatorial conjecture, which is naturally connected to the subject of polynomial factoring.

A special case which is of particular interest to the present work is the factorization of prime-degree polynomials over finite fields. It is perhaps surprising that this case should be easier than the problem of polynomial factoring in general, but it turns out that the combinatorial framework introduced in [IKS09, AIKS12] behaves quite well for prime-degree polynomials and gives an improved time complexity (see Section 4.4). The reason for this behavior is found in the theory of combinatorial schemes; in particu-

lar in certain structural results about association schemes of prime order (see Sections 2.5 & 2.6) and m-schemes on a prime number of points (see Section 3.5). We delineate the core ideas of these notions below.

Association Schemes and m-Schemes

The GRH-based algorithm for factoring polynomials over finite fields by Ivanyos, Karpinski and Saxena [IKS09, Aro10, AIKS12] (called *IKS-algorithm* in the following) relies on the use of combinatorial schemes, more specifically association schemes and m-schemes (for a given positive integer m). If we denote $[n] := \{1, ..., n\}$, then an m-scheme can be described as a partition of the set $[n]^s$, for each $1 \leq s \leq m$, which satisfies certain natural properties called compatibility, regularity and invariance (Section 3.1). The notion of m-scheme is closely related to the concepts of presuperscheme [Woj01a, Woj98, Woj01b], superscheme [Smi94], association scheme [BI84, Zie05], coherent configuration [Hig70], cellular algebra [WL68] and Krasner algebra [Kra38]. The reader may note that the techniques initiated by [WL68] are closely related to another open problem in computational complexity - deciding graph isomorphism. Moreover, coherent configurations provide a natural framework for fast matrix multiplication [CU12].

The IKS-algorithm (Section 4.2) 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 $\mathcal{A}^{\otimes s}$ $(1 \leq s \leq m)$. It then performs a series of operations on systems of ideals of these algebras (which are efficient under GRH), and 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 $\mathcal{A}^{\otimes s}$ $(1 \leq s \leq m)$. In the latter case (which we think of as the 'bad' case), the m-scheme obtained may be interpreted as the 'reason' why the

IKS-algorithm could not find a zero divisor in $\mathcal{A}$. However, it is not difficult to prove that the IKS-algorithm always finds a zero divisor in $\mathcal{A}$ if we choose m large enough (viz. in the range $\log n$), yielding that the IKS-algorithm deterministically factors $f(x)$ in time $\text{poly}(n^{\log n}, \log q)$. Moreover, it is conjectured that even choosing m as constant, say $m = c$ where $c \geq 4$, is enough to find a zero divisor in $\mathcal{A}$ (and thus 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 3.5) on the existence of *matchings* (Sections 3.4 & 4.3).

We remark that the schemes conjecture is a purely combinatorial conjecture which concerns structure of certain types of m-schemes. The schemes conjecture is especially motivated by the fact that it is already proven for an important class of m-schemes, namely the so-called *orbit* m-schemes (Theorem 3.5.2). In this current work, we outline the argument of [AIKS12], which gives a proof of the schemes conjecture for an interesting class of m-schemes on a prime number of points. Via the IKS polynomial factoring framework, the latter result translates to a (perhaps surprising) theorem about the factorization of prime degree polynomials over finite fields (see Theorem 4.4.1). The proof builds on the intimate connection of m-schemes and association schemes (see Section 3.2), and involves some strong structural results about association schemes of prime order by Hanaki & Uno [HU06] and Muzychuk & Ponomarenko [MP12]. We provide some intuition for the above-mentioned results in the following.

Recall [Zie05, MP12] 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 *trivial* 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* $c_{fg}^h \in \mathbb{N}$ such that for all $(\alpha, \beta) \in h$, $c_{fg}^h = \#\{\gamma \in X \mid (\alpha, \gamma) \in f, (\gamma, \beta) \in g\}$.

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* $n_g := c_{gg^*}^1$, and its *indistinguishing number* $c(g) := \sum_{v \in G} c_{vv^*}^g$.

One may think of an association scheme (X, G) as a colored directed graph with vertices X and edges G. However, association schemes are significantly richer in algebraic structure than a graph – in fact, they can be regarded as a natural generalization of the notion of groups (which is why the field of association schemes has frequently been referred to as "group theory without groups" [BI84]). The central scheme-theoretic result of this work proves the existence of *small* intersection numbers in association schemes where both the nontrivial valencies and indistinguishing numbers are confined to a certain range (see Theorem 2.6.1). The latter theorem especially applies to association schemes of prime order - yielding a strong structural result for this class of schemes (see Theorem 2.5.5 and Corollary 2.6.2). Drawing on the connection of association schemes and m-schemes, we deduce from Corollary 2.6.2 the existence of matchings in certain m-schemes on a prime number of points (see Theorem 3.5.3). Via the IKS polynomial factoring framework, the latter result translates to significant improvements in the domain of polynomial factoring (see Theorem 4.4.1 and Corollary 4.5.2).

1.2 Extensibility of Association Schemes

A substantial part of this work is devoted to the notion of extensibility of association schemes, a concept which was first defined in [AZ12]. We motivate the notion of extensibility below. Let X be a finite set and G a partition of $X \times X$. We call the partition G *group-induced* if there exists a transitive

permutation group $\mathcal{G}$ acting on X such that the partition G is the set of diagonal orbits of $X \times X$ under the action of $\mathcal{G}$. It is a natural problem to ask for an efficient algorithmic method to determine whether a given partition G of $X \times X$ is group-induced. Note that this amounts to the same problem as asking for an efficient algorithm to detect whether a colored complete digraph is exactly determined by its automorphism group.

A necessary condition for the partition G of $X \times X$ to be group-induced is that the pair (X, G) forms an association scheme (see Section 2.1) – a condition which can be checked in time polynomial in $|X|$. A necessary and sufficient condition for G to be group-induced is that the pair (X, G) forms a *Schurian* association scheme. Note that it is a long-standing open question whether there exists a polynomial-time algorithm for detecting the Schurity of association schemes; currently, the best known methods for Schurity testing have a subexponential running time [BKL83, BL83]. In this work, we study the notion of *extensibility* of association schemes, which may be regarded as an intuitive measure of how close an association scheme is to being Schurian. As we will see, the problem of computing the extensibility properties of association schemes provides a natural relaxation of the Schurity testing problem.

Phrasing Smith's characterization of Schurity [Smi94, Smi07] in the terminology of extensibility, a partition G of $X \times X$ is group-induced if the pair (X, G) is an association scheme which is extensible to height $(d-2)$, where $d := |X|$ is the order of (X, G). Note here that an association scheme $\mathfrak{X} = (X, G)$ is said to be extensible to height t if $\mathfrak{X}$ is *associated to a height t presuperscheme* (see Section 5.1); the latter notion may be regarded as a higher-dimensional analog of association schemes. In Chapter 5, we formalize the maximal height $t_{\max}(\mathfrak{X})$ of an association scheme $\mathfrak{X} = (X, G)$ as the

largest number $t \in \mathbb{N}$ such that $\mathfrak{X}$ is extensible to height t (we also include the possibility $t_{\max}(\mathfrak{X}) = \infty$, which is equivalent to $t_{\max}(\mathfrak{X}) \geq (d-2)$). The notion of the maximal height fully captures the extensibility properties of association schemes, and specifies our previous remark that the extensibility properties provide a natural measure of how close an association scheme is to being Schurian.

For the purpose of computing the maximal height, we introduce the *association scheme extension algorithm* [AZ12]. On input an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$, the association scheme extension algorithm decides in time $d^{O(t)}$ if the scheme $\mathfrak{X}$ is extensible to height t. In particular, if t is a fixed constant, then the running time of the association scheme extension algorithm is polynomial in the order of $\mathfrak{X}$. The association scheme extension algorithm is used to show that all non-Schurian association schemes up to order 26 are completely inextensible, i.e. they are not extensible to any positive height $t \in \mathbb{N}_{>0}$. Via the tensor product of association schemes, the latter result gives rise to a multitude of infinite families of completely inextensible association schemes.

Apart from its connection to the problem of Schurity testing, the notion of extensibility also plays a major role in the IKS polynomial factoring framework [AIKS12, IKS09]. For the area of research which the latter works fall into, it is of particular interest to gain a more thorough understanding of the combinatorial properties possessed by association schemes which are extensible to a certain height. We discuss this connection in Section 5.1.

1.3 Efficient Matrix Multiplication

As an additional application of (commutative) association schemes to computational complexity, we describe the recent Cohn-Umans [CU12] framework

for *efficient matrix multiplication*. The term 'efficient matrix multiplication' refers to the computational problem of minimizing the number of arithmetic operations necessary to compute the product of two $n \times n$ matrices $A, B \in k^{n \times n}$ with entries in some field k,

$$(AB)_{ik} = \sum_{j=1}^{n} A_{ij} B_{jk}.$$

The asymptotic complexity of matrix multiplication is captured by the *matrix multiplication exponent* ω, which represents the minimum number $\omega \in [2, 3]$ such that the product of two $n \times n$ matrices can be computed using $O(n^{\omega + o(1)})$ arithmetic operations. It is a well known fact that the complexity of many central computational problems (besides matrix multiplication) depend on the exponent ω: For instance, the problem of matrix inversion, computing the determinant, and computing the characteristic polynomial of $n \times n$ matrices each have complexity $O(n^{\omega + o(1)})$ (see [BCS97], Ch. 16 for a comprehensive list of problems whose complexity depend on ω). Determining the exact value of ω is a long-standing barrier in the field of computational algebra, and is widely considered one of the most important open problems in complexity theory as a whole. It is a famous open conjecture to prove that $\omega = 2$; currently, the best known upper bound for the exponent ω stands at $\omega < 2.373$ [VW12].

In this work, we delineate the Cohn-Umans [CU12] *algebra embedding* framework for efficient matrix multiplication. The Cohn-Umans approach relies on the notions of *matrix multiplication tensors* and *tensor rank* to algebraically describe the asymptotic complexity of matrix multiplication (similar to the classical works [Bin80, Sch81, CW87]). In contrast to the latter works, Cohn and Umans [CU12] do not produce explicit tensor calculations to deduce bounds on ω. Rather, they develop a universal method to

embed matrix multiplication tensors into commutative and semisimple complex algebras, thereby relating the complexity of matrix multiplication to properties of purely algebraic objects (see Section 6.2). Their work extends a previous line of research which specialized on embedding matrix multiplication tensors into *group algebras* [CU03, CKSU05, ASU12]. Using the Cohn-Umans group algebra embedding framework, one can show the upper bound $\omega < 2.41$ [CKSU05], not far from the best known $\omega < 2.373$ [VW12].

As a promising candidate class of commutative and semisimple complex algebras to realize matrix multiplication tensors and improve the upper bound on ω, Cohn and Umans [CU12] identify complex adjacency algebras of commutative association schemes. They provide a purely combinatorial condition for association schemes to realize matrix multiplication tensors via their complex adjacency algebra (see Section 6.3). In particular, this approach leads to a natural algebraic-combinatorial conjecture for proving $\omega = 2$ (see Conjecture 6.3.1). Interestingly, Conjecture 6.3.1 subsumes the entirety of the earlier conjectures for $\omega = 2$ of the Cohn-Umans group algebra framework [CU03, CKSU05, ASU12]. Adopting a more global view, the Cohn-Umans [CU12] efficient matrix multiplication framework reflects fittingly the overall idea of the present work – the application of association schemes (as a natural extension of the group concept) as a combinatorial tool in computational complexity.

Chapter 2

Association Schemes

Association schemes are standard combinatorial objects which appear frequently in the realm of algebraic combinatorics [Bai04, BI84, Zie96]. The theory of association schemes is often referred to as "group theory without groups", since it constitutes a natural generalization of the latter notion. In this chapter, we give an introduction to the theory of association schemes and discuss several important and recent results in this area. Our approach to association schemes is of algebraic nature; it utilizes ring theory, representation theory and linear algebra. Note that the results which are discussed in this chapter will be of much importance to the framework for polynomial factoring over finite fields described in Chapters 3 and 4.

The material in this chapter is organized as follows. In §2.1, we introduce the notion of association schemes and look at basic examples. In §2.2, we define the concept of the adjacency algebra of association schemes. §2.3 provides an overview of the character theory of association schemes. §2.4 provides some important results about characters of the complex adjacency algebra. In §2.5, we consider structural results for association schemes of prime order, most notably the Hanaki-Uno Theorem (see Theorem 2.5.4). In

§2.6, we prove a central combinatorial result about association schemes with bounded valencies and indistinguishing numbers (see Theorem 2.6.1).

2.1 Basic Notions

In this section, we discuss the definition of association schemes and look at notable examples. The examples we consider include Schurian association schemes, cyclotomic schemes and strongly regular graphs. Furthermore, we give some basic identities for the intersection numbers of association schemes.

Definition 2.1.1 (Association Scheme)**.** Let X be a finite set and G a partition of $X \times X$. We say that $\mathfrak{X} = (X, G)$ is an **association scheme** if

(A1) G contains the **trivial relation** $1 := \{(x, x) \mid x \in X\}$,

(A2) If $g \in G$, then $g^* := \{(y, x) \mid (x, y) \in g\} \in G$,

(A3) For all $f, g, h \in G$, there exists an **intersection number** $c_{fg}^h \in \mathbb{N}$ such that for all $(\alpha, \beta) \in h$,

$$c_{fg}^h = \left|\{\gamma \in X \mid (\alpha, \gamma) \in f \text{ and } (\gamma, \beta) \in g\}\right|.$$

An element $g \in G$ is called a **relation** (or **color**) of $\mathfrak{X}$. We call $|X|$ the **order** and $|G|$ the **rank** of $\mathfrak{X}$. For each relation $g \in G$, we define its **valency** $n_g := c_{gg^*}^1$ and its **indistinguishing number** $c(g) := \sum_{v \in G} c_{vv^*}^g$. If $c_{fg}^h = c_{gf}^h$ for all $f, g, h \in G$, then we say that $\mathfrak{X}$ is **commutative**.

A classical example of association schemes is provided by *Schurian association schemes*, which arise from the diagonal orbits of transitive permutation groups (see below). In Chapter 3, when we study m-schemes, Schurian schemes will appear as a special case of the more general *orbit m-schemes*.

Example 2.1.2 (Schurian Association Scheme)**.** *Let X be a finite nonempty set and let $\mathcal{G}$ be a transitive permutation group on X. Let $G := \{1, g_1, ..., g_s\}$ denote the set of orbits of $X \times X$ under the diagonal action of $\mathcal{G}$, where $1 := \{(x, x) \mid x \in X\}$ denotes the trivial orbit. Then (X, G) is an association scheme. Schemes which arise from the action of a permutation group in the above-described manner are called* ***Schurian*** *association schemes.* □

Schurian schemes provide copious examples of association schemes, but they do not cover all association schemes. A list of non-Schurian association schemes of small order can be found in Hanaki and Miyamoto's work [HM03]. Examples of infinite families of non-Schurian association schemes can for instance be found in [EP99, FKM94].

Determining whether there exists a polynomial-time algorithm which decides if a given association scheme is Schurian or non-Schurian is a long-standing open problem. The methods introduced in [BKL83, BL83] yield subexponential-time algorithm for testing Schurity of association schemes; this is currently the best known. Recently, Ponomarenko [Pon11] devised an algorithm which decides the Schurity problem for *antisymmetric* association schemes in polynomial time (note that an association scheme $\mathfrak{X} = (Q, \Gamma)$ is called antisymmetric if for all $1 \neq g \in G$, $g^* = \{(y, x) \mid (x, y) \in g\} \neq g$).

Next, we consider the example of *cyclotomic schemes*.

Example 2.1.3 (Cyclotomic Scheme)**.** *Let q be prime power and let $d|(q-1)$. Let $\mathbb{F}_q^*$ denote the multiplicative group of the field $\mathbb{F}_q$. Fix a generator α of $\mathbb{F}_q^*$ and consider the subgroup $\langle \alpha^d \rangle$ generated by α^d. Note that $\langle \alpha^d \rangle$ is a subgroup of index d in $\mathbb{F}_q^*$, the cosets of $\langle \alpha^d \rangle$ in $\mathbb{F}_q^*$ are*

$$\alpha^i \left\langle \alpha^d \right\rangle, \quad i = 1, ..., d.$$

Let $\mathcal{P} := \{P_i \,|\, 0 \leq i \leq d\}$ *be the partition of* $\mathbb{F}_q \times \mathbb{F}_q$ *defined by*

$$P_0 := \{(x, x) \,|\, x \in \mathbb{F}_q\},$$

$$P_i := \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q \,|\, x - y \in \alpha^i \left\langle \alpha^d \right\rangle\}, \quad i = 1, ..., d.$$

Then $(\mathbb{F}_q, \mathcal{P})$ *is an association scheme. Observe that all relations of* $(\mathbb{F}_q, \mathcal{P})$ *are equal in size, i.e.* $|P_i| := \frac{q(q-1)}{d}$ $(i = 1, ..., d)$. *Moreover, observe that the definition of* $(\mathbb{F}_q, \mathcal{P})$ *does not depend on the choice of the generator* α*: If* β *is another generator of* $\mathbb{F}_q^*$, *say* $\beta = \alpha^s$ *for some* $s \in \mathbb{N}$, *then* $\beta^j \left\langle \beta^d \right\rangle \subset \alpha^{js} \left\langle \alpha^d \right\rangle$ $(j = 1, ..., d)$, *and since* $\beta^j \left\langle \beta^d \right\rangle$ *and* $\alpha^{js} \left\langle \alpha^d \right\rangle$ *are equal in size,*

$$\beta^j \left\langle \beta^d \right\rangle = \alpha^{js} \left\langle \alpha^d \right\rangle, \quad j = 1, ..., d.$$

Hence, substituting β *in place of* α *merely permutes the numbering of the relations of* $(\mathbb{F}_q, \mathcal{P})$. *We conclude that the construction of* $(\mathbb{F}_q, \mathcal{P})$ *depends only on the choice of* q *and* d. *We call* $(\mathbb{F}_q, \mathcal{P})$ *the* ***cyclotomic scheme*** *in* (q, d) *and denote it by* $\mathrm{Cyc}(q, d)$. □

An important class of examples of association schemes is constructed from the notion of *strongly regular graphs*. We describe this type of example below.

Example 2.1.4 (Strongly Regular Graph)**.** *A* k*-regular graph* (V, E) *is said to be* ***strongly regular*** *if there exist numbers* $r, s \in \mathbb{N}$ *such that:*

(i) Every two adjacent vertices have r *common neighbors,*

(ii) Every two non-adjacent vertices have s *common neighbors.*

Note that if (V, E) *is a strongly regular graph, then its complement* $(V, \bar{E})$ *is also strongly regular. If we regard* (V, E) *and* $(V, \bar{E})$ *as symmetric digraphs, then we can construct an association scheme* $\mathfrak{X} = (V, G)$ *by defining*

$$G := \{1, E, \bar{E}\},$$

where 1 *denotes the trivial relation. We call* $\mathfrak{X}$ *the association scheme corresponding to the strongly regular graph* (V, E). □

For further examples of association schemes, the reader is referred to the introductory texts [Bai04, BI84]. We conclude this section by listing some fundamental identities for the intersection numbers of association schemes. Note that the identities given below can all be found in [Zie96]; we make repeated use of them in later parts of this work.

Lemma 2.1.5. *Let* (X, G) *be an association scheme and let* $d, e, f \in G$. *The following holds:*

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

2.2 The Adjacency Algebra

Let $\mathfrak{X} = (X, G)$ be an association scheme and let $n := |X|$ be the order of $\mathfrak{X}$. For a relation $g \in G$, we denote its **adjacency matrix** by σ_g. Namely, σ_g is a matrix whose rows and columns are indexed by X and its (x, y)-entry is 1 if $(x, y) \in g$ and 0 otherwise. Let $\Lambda := \{\sigma_g \,|\, g \in G\}$ be the set of all adjacency matrices of G. It follows from Definition 2.1.1 that

(i) $\sum_{g \in G} \sigma_g$ is the $n \times n$ matrix with entries all 1,

(ii) $\sigma_1 \in \Lambda$ is the $n \times n$ identity matrix,

(iii) If $\sigma_g \in \Lambda$, then $\sigma_{g^*} = \sigma_g^T \in \Lambda$,

(iv) For all $f, g, h \in G$, there exists a number $c_{fg}^h \in \mathbb{N}$ such that

$$\sigma_f \sigma_g = \sum_{h \in G} c_{fg}^h \sigma_h.$$

To obtain (iv), note that for $(\alpha, \beta) \in h$, the equation

$$c_{fg}^h = \left|\{\gamma \in X \,|\, (\alpha, \gamma) \in f \text{ and } (\gamma, \beta) \in g\}\right|$$

can also be written as

$$c_{fg}^h = \sum_{\gamma \in X} \left(\sigma_f\right)_{\alpha\gamma} \left(\sigma_g\right)_{\gamma\beta},$$

and the right hand side is $\left(\sigma_f \sigma_g\right)_{\alpha\beta}$ by the definition of matrix multiplication.

Note that a system of 0-1-matrices satisfying the above properties (i)-(iv) and an association scheme constitute the same notion. Moreover, observe that statements (i)-(iv) still hold if we consider the adjacency matrices $\Lambda = \{\sigma_g \,|\, g \in G\}$ as matrices over some commutative ring R with unity. The latter observation gives rise to the definition of the adjacency algebra of association schemes.

Definition 2.2.1 (Adjacency Algebra)**.** Let $\mathfrak{X} = (X, G)$ be an association scheme and let R be a commutative ring with 1. Then we can define an R-algebra (with respect to matrix multiplication)

$$R\mathfrak{X} = \bigoplus_{g \in G} R\sigma_g,$$

where σ_g is considered as a matrix over the coefficient ring R. We call $R\mathfrak{X}$ the **adjacency algebra** of $\mathfrak{X}$ over R.

It is easily seen that the adjacency algebra $R\mathfrak{X}$ is commutative iff the association scheme $\mathfrak{X}$ is commutative. Moreover, we have the following important criterion for the semisimplicity of adjacency algebras:

Theorem 2.2.2. *Let $\mathfrak{X} = (X, G)$ be an association scheme. Let K be a field of characteristic zero. Then the adjacency algebra $K\mathfrak{X}$ is semisimple.*

Proof. It suffices to prove that the Jacobson radical $J(K\mathfrak{X})$ of $K\mathfrak{X}$ is trivial. For the sake of contradiction, suppose there exists $0 \neq \sigma \in J(K\mathfrak{X})$. Choose $\{r_g \in K \mid g \in G\}$ such that

$$\sigma = \sum_{g \in G} r_g \sigma_g.$$

Since σ is nontrivial, we can choose $f \in G$ such that $r_{f^*} \neq 0$. We have

$$tr(\sigma_f \sigma) = \sum_{g \in G} r_g \; tr(\sigma_f \sigma_g) = r_{f^*} \left| f \right|,$$

where tr denotes the trace function. Note that the second equality above follows from

$$\begin{aligned} tr(\sigma_f \sigma_g) &= \sum_{h \in G} c_{fg}^h tr(\sigma_h) = \sum_{h \in G} c_{fg}^h \delta_{1h} \left| X \right| \\ &= c_{fg}^1 \left| X \right| = \delta_{f^* g} \; n_f \left| X \right| = \delta_{f^* g} \left| f \right|. \end{aligned}$$

Now observe that $\sigma_f \sigma$ lies in $J(K\mathfrak{X})$; hence $\sigma_f \sigma$ is nilpotent. It follows that

$$tr(\sigma_f \sigma) = 0.$$

We conclude $r_{f^*} \left| f \right| = 0$. But this contradicts $r_{f^*} \neq 0$. □

Note that there exist many more useful criteria for establishing the semisimplicity of adjacency algebras. The reader may refer to [Zie96], Th. 4.1.3 and [Han00] for further examples of such criteria.

2.3 Character Theory of Association Schemes

In the following, we give a survey of the character theory of association schemes. We begin by recalling the basic definition of characters. Let $\mathcal{A}$ be

an algebra over some field K. Let V be an $\mathcal{A}$-module such that $\dim_K(V) \in \mathbb{N}$. For each $a \in \mathcal{A}$, we have a linear map

$$\varphi_a : V \longrightarrow V, \quad v \longrightarrow va.$$

The linear map defined by

$$\chi_V : \mathcal{A} \longrightarrow K, \quad a \longrightarrow tr(\varphi_a)$$

is called the **character of $\mathcal{A}$ afforded by** V. In case V is an irreducible $\mathcal{A}$-module, we call χ_V an **irreducible** character. The set of all irreducible characters of $\mathcal{A}$ is denoted by $\mathrm{Irr}(\mathcal{A})$.

Equivalently, characters can be defined via the notion of matrix representations. Recall that a **matrix representation** of $\mathcal{A}$ is a K-algebra homomorphism from $\mathcal{A}$ into a full matrix ring over K,

$$\mathbf{X} : \mathcal{A} \longrightarrow M_n(K), \quad a \longrightarrow X(a).$$

Given a matrix representation $\mathbf{X}$ of $\mathcal{A}$, the map

$$\chi : \mathcal{A} \longrightarrow K, \quad \sigma \longrightarrow tr(X(\sigma)).$$

constitutes a character of $\mathcal{A}$, i.e. $\chi = \chi_V$ for some $\mathcal{A}$-module V such that $\dim_K(V) \in \mathbb{N}$ (note that the $\mathcal{A}$-module V which affords χ is determined uniquely up to isomorphism). In the above situation, we call χ the **character of $\mathcal{A}$ afforded by $\mathbf{X}$**. Furthermore, we call V a **representation module** for χ.

In the following, let $\mathfrak{X} = (X, G)$ be an association scheme and let K be a field of characteristic 0. Note that we may regard integers $a \in \mathbb{Z}$ as elements of K by identifying $a = a \cdot 1_K$. We will study the characters of the adjacency algebra $K\mathfrak{X}$. Consider the following examples.

Example 2.3.1 (Trivial Character)**.** *Consider the $K\mathfrak{X}$-representation*

$$\boldsymbol{X} : K\mathfrak{X} \longrightarrow K, \quad \sigma_g \longrightarrow n_g.$$

This is indeed a representation, since for all $e, f \in G$, it holds that

$$\boldsymbol{X}(\sigma_e\sigma_f) = \sum_{g\in G} c_{ef}^g \boldsymbol{X}(\sigma_g) = \sum_{g\in G} c_{ef}^g n_g = n_e n_f = \boldsymbol{X}(\sigma_e)\boldsymbol{X}(\sigma_f)$$

*(see Lemma 2.1.5 (iv)). Let 1_G denote the character afforded by $\boldsymbol{X}$. We call 1_G the **trivial character** of $K\mathfrak{X}$. Explicitly, we have*

$$1_G(\sigma_g) = n_g$$

for all $g \in G$. Moreover, since $\dim_K(T) = 1$ for any representation module T of $\boldsymbol{X}$, the trivial character 1_G is irreducible. □

Example 2.3.2 (Principal Character)**.** *Let $\chi_{K\mathfrak{X}}$ denote the character of $K\mathfrak{X}$ which is afforded by $K\mathfrak{X}$ as a module. We call $\chi_{K\mathfrak{X}}$ the **principal character** of $K\mathfrak{X}$. Explicitly, we have*

$$\chi_{K\mathfrak{X}}(\sigma_g) = \sum_{v\in G} c_{vg}^v$$

for all $g \in G$. □

Example 2.3.3 (Standard Representation, Standard Character)**.** *Denote by $n := |X|$ the order of $\mathfrak{X}$. We define the **standard representation $\boldsymbol{Y}$** of $K\mathfrak{X}$ by*

$$\boldsymbol{Y} : K\mathfrak{X} \longrightarrow M_n(K), \quad \sigma_g \longrightarrow \sigma_g.$$

*Let γ denote the character afforded by $\boldsymbol{Y}$. We call γ the **standard character** of $K\mathfrak{X}$. Explicitly, we have*

$$\gamma(\sigma_g) = \delta_{1g} n$$

for all $g \in G$, where δ denotes the Kronecker delta. □

In the following, let $\mathfrak{X} = (X, G)$ be an association scheme and let K be a field of characteristic 0. By Theorem 2.2.2, the adjacency algebra $K\mathfrak{X}$ is semisimple. Especially, there are finitely many isomorphism types $S_1, ..., S_k$ of irreducible $K\mathfrak{X}$-modules. Further, for any $K\mathfrak{X}$-module V such that $\dim_K(V) \in \mathbb{N}$, we have an **irreducible decomposition**

$$V \cong \lambda_1 S_1 \oplus \cdots \oplus \lambda_k S_k,$$

where $\lambda_1, ..., \lambda_k \in \mathbb{N}$ are some multiplicities. For the character χ_V of $K\mathfrak{X}$ afforded by V, this translates to the **irreducible character decomposition**

$$\chi_V = \sum_{i=1}^{k} \lambda_i \chi_i,$$

where χ_i denotes the irreducible character corresponding to the module S_i. Especially, note that the standard character γ of $K\mathfrak{X}$ can be written as a linear combination of irreducible characters. Since this constitutes an important special case, we settle for the following convention.

Definition 2.3.4 (Multiplicity)**.** Let γ be the standard character of $K\mathfrak{X}$ and let

$$\gamma = \sum_{\chi \in \mathrm{Irr}(K\mathfrak{X})} m_\chi \chi$$

be the irreducible character decomposition of γ, where m_χ denotes the multiplicity corresponding to the irreducible character χ. We refer to m_χ simply as the **multiplicity** of χ.

The multiplicities $\{m_\chi \in \mathbb{N} \,|\, \chi \in \mathrm{Irr}(K\mathfrak{X})\}$ can be calculated explicitly via the *orthogonality relations*, which are provided below.

Theorem 2.3.5 (Orthogonality Relations)**.** *Let $\phi, \psi \in \mathrm{Irr}(K\mathfrak{X})$. We have the following:*

(i) For each $g \in G$,

$$\sum_{e\in G}\sum_{f\in G}\frac{c^f_{g^*e}}{|e^*|}\phi(\sigma_{e^*})\psi(\sigma_f) = \delta_{\phi\psi}\frac{\phi(\sigma_{g^*})}{m_\phi}.$$

(ii) We have

$$\sum_{g\in G}\frac{1}{|g^*|}\phi(\sigma_{g^*})\psi(\sigma_g) = \delta_{\phi\psi}\frac{\phi(\sigma_1)}{m_\phi}.$$

The above version of the orthogonality relations, alongside a proof, can be found in [Zie96] (Th. 4.1.5). Bailey's book (see [Bai04], Th. 2.12 and Cor. 2.14, 2.15) gives a similar treatment of the subject, while Bannai and Ito (see [BI84], Th. II.3.5) only consider the orthogonality relations in the case of commutative association schemes.

As a consequence of Theorem 2.3.5, we obtain the following corollary:

Corollary 2.3.6. *The trivial character $1_G \in \mathrm{Irr}(K\mathfrak{X})$ has multiplicity $m_{1_G} = 1$ in the standard character γ.*

Proof. Using the second orthogonality relation, we infer

$$\sum_{g\in G}\frac{1}{|g^*|}1_G(\sigma_{g^*})1_G(\sigma_g) = \frac{1_G(\sigma_1)}{m_{1_G}}.$$

By the definition of the trivial character (see Example 2.3.2), this yields

$$\sum_{g\in G}\frac{1}{|g|}n_g^2 = \frac{1}{m_{1_G}},$$

and the left side is 1 by the identity $n_g\,|X| = |g|$. □

2.4 Characters of the Complex Adjacency Algebra

In the following, let $\mathfrak{X} = (X, G)$ be an association scheme and let $\mathbb{C}\mathfrak{X}$ denote the complex adjacency algebra. We discuss some basic lemmas about

characters of $\mathbb{C}\mathfrak{X}$ which will be of importance throughout the remainder of this chapter. The results described below are used to prove structural results about association schemes of prime order (see Section 2.5).

The following lemma provides an apt character-theoretic description of the concept of commutativity of association schemes. Moreover, it gives the irreducible character decomposition of the principal character of the complex adjacency algebra.

Lemma 2.4.1. *Let $\chi_{\mathbb{C}\mathfrak{X}}$ denote the principal character of $\mathbb{C}\mathfrak{X}$ and let 1 be the unity in $\mathbb{C}\mathfrak{X}$. The following holds:*

(i) We have

$$\sum_{\chi\in\mathrm{Irr}(\mathbb{C}\mathfrak{X})} \chi(1) \leq \sum_{\chi\in\mathrm{Irr}(\mathbb{C}\mathfrak{X})} \chi(1)^2 = |G|\,,$$

and equality holds if and only if $\mathfrak{X}$ is commutative.

(ii) We have

$$\chi_{\mathbb{C}\mathfrak{X}} = \sum_{\chi\in\mathrm{Irr}(\mathbb{C}\mathfrak{X})} \chi(1)\chi.$$

Proof. Note that

$$\chi_V(1) = tr(id_V) = \dim_{\mathbb{C}}(V)$$

for any character χ_V afforded by a $\mathbb{C}\mathfrak{X}$-module V with $\dim_{\mathbb{C}}(V) \in \mathbb{N}$. Using the above identity, statements (i), (ii) are simple corollaries of Wedderburn's Theorem (see [NT89], Th. I. 8.5). □

Next, consider the following basic preliminary lemma.

Lemma 2.4.2. *Let $\boldsymbol{X}$ be matrix representation of $\mathbb{C}\mathfrak{X}$,*

$$\boldsymbol{X} : \mathbb{C}\mathfrak{X} \longrightarrow M_k(\mathbb{C}), \quad \sigma \longrightarrow Y(\sigma).$$

Then for all $\sigma \in \mathbb{C}\mathfrak{X}$, every eigenvalue of $\boldsymbol{X}(\sigma)$ is also an eigenvalue of σ.

Proof. Put $n := |X|$. Let $f(x) = \sum_{i=1}^{n} a_i x^i$ be the characteristic polynomial of σ and let λ be some eigenvalue of $\mathbf{X}(\sigma)$. It suffices to show $f(\lambda) = 0$. For this purpose, note that

$$\sum_{i=1}^{n} a_i \sigma^i = 0$$

by Cayley-Hamilton's Theorem. Applying $\mathbf{X}$ to both sides of this equation yields

$$\sum_{i=1}^{n} a_i \mathbf{X}(\sigma)^i = 0.$$

Thus, if $0 \neq v \in \mathbb{C}^k$ is some eigenvector of $\mathbf{X}(\sigma)$ associated with λ, we have

$$\sum_{i=1}^{n} a_i \mathbf{X}(\sigma)^i v = 0 \Longrightarrow \sum_{i=1}^{n} a_i \lambda^i v = 0 \Longrightarrow f(\lambda)v = 0 \Longrightarrow f(\lambda) = 0,$$

from which the assertion follows. □

We obtain the following important result:

Lemma 2.4.3. *Let χ be a character of $\mathbb{C}\mathfrak{X}$. Then the character values $\{\chi(\sigma_g) \,|\, g \in G\}$ are algebraic integers.*

Proof. Let $\mathbf{X}$ be a matrix representation of $\mathbb{C}\mathfrak{X}$ that affords χ. For $g \in G$, every eigenvalue of $\mathbf{X}(\sigma_g)$ is also an eigenvalue of σ_g (see Lemma 2.4.2). But σ_g is an integral matrix; thus, the eigenvalues of σ_g are algebraic integers. Hence, $\chi(\sigma_g) = tr(\mathbf{X}(\sigma_g))$ is a sum of algebraic integers and therefore an algebraic integer itself. □

For the next result, let $\chi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})$. Let K be a finite normal extension of the rational number field $\mathbb{Q}$ such that the character values $\{\chi(\sigma_g) \,|\, g \in G\}$ are contained in K and $K\mathfrak{X}$ is a split K-algebra (for the existence of K, see [Bos06] (Ch. 3.5) or [NT89] (Ch. II. 3)). We denote by $Gal(K/\mathbb{Q})$ the Galois group of this extension. The following holds:

Lemma 2.4.4. *In the above situation, for each $\tau \in Gal(K/\mathbb{Q})$, there exists a character χ^τ of $\mathbb{C}\mathfrak{X}$ such that*

$$\chi^\tau(\sigma_g) = \chi(\sigma_g)^\tau$$

for all $g \in G$. Moreover, the character χ^τ is irreducible.

Proof. Let U be an irreducible $\mathbb{C}\mathfrak{X}$-module which affords χ. Then by [CR88], Th. 29.21 there exists an irreducible $K\mathfrak{X}$-module V such that

$$\mathbb{C} \otimes_K V \cong U.$$

For $\tau \in Gal(K/\mathbb{Q})$, let σ^τ denote the (entrywise) image of $\sigma \in K\mathfrak{X}$ under τ. We exchange the original scalar product on V with the slightly modified

$$V \times K\mathfrak{X} \longrightarrow V, \quad (v, \sigma) \longrightarrow v\sigma^\tau;$$

the resulting $K\mathfrak{X}$-module we denote by V^τ. Clearly, V^τ is an irreducible $K\mathfrak{X}$-module (this follows from the irreducibility of V). Consequently,

$$\mathbb{C} \otimes_K V^\tau =: U^\tau$$

is an irreducible $\mathbb{C}\mathfrak{X}$-module (see [CR88], Th. 29.21). Moreover, it is evident from the above construction that the character χ^τ of $\mathbb{C}\mathfrak{X}$ afforded by U^τ satisfies

$$\chi^\tau(\sigma_g) = \chi(\sigma_g)^\tau$$

for all $g \in G$. This completes the proof. □

Using the notation of Lemma 2.4.4, we can define a group action of $Gal(K/\mathbb{Q})$ on the set $\mathrm{Irr}(\mathbb{C}\mathfrak{X})$ of irreducible characters of $\mathbb{C}\mathfrak{X}$,

$$Gal(K/\mathbb{Q}) \times \mathrm{Irr}(\mathbb{C}\mathfrak{X}) \longrightarrow \mathrm{Irr}(\mathbb{C}\mathfrak{X}), \quad (\tau, \chi) \longrightarrow \chi^\tau.$$

In the following, we call two characters $\chi, \varphi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})$ **algebraically conjugate** if they lie in the same orbit by this action. Note that this definition does not depend on the choice of K, which the reader may prove himself by using the fact that the restriction homomorphism

$$Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Gal(K/\mathbb{Q}), \quad \tau \longrightarrow \tau|_K$$

is surjective (see [Bos06], Ch. 4.1). Using the above terminology, we prove the following important lemma:

Lemma 2.4.5. *Let χ be an irreducible character of $\mathbb{C}\mathfrak{X}$. Let Φ be the sum of all algebraic conjugates of χ. Then the Φ-values $\{\Phi(\sigma_g) \,|\, g \in G\}$ are rational integers.*

Proof. We use the same notation as in Lemma 2.4.4. Define by

$$I := \{\tau \in Gal(K/\mathbb{Q}) \,|\, \chi^\tau = \chi\}$$

the stabilizer group of χ in $Gal(K/\mathbb{Q})$. Clearly, $\big|Gal(K/\mathbb{Q}) : I\big| < \infty$. Put

$$Gal(K/\mathbb{Q}) = I\tau_1 \cup \cdots \cup I\tau_r$$

a coset decomposition of $Gal(K/\mathbb{Q})$. Then

$$\{\chi^\tau \,|\, \tau \in Gal(K/\mathbb{Q})\} = \{\chi^{\tau_1}, ..., \chi^{\tau_r}\}.$$

Consequently,

$$\Phi = \sum_{i=1}^{r} \chi^{\tau_i}.$$

For $g \in G$, it follows that $\Phi(\sigma_g)^\tau = \Phi(\sigma_g)$ for all $\tau \in Gal(K/\mathbb{Q})$. Hence, $\Phi(\sigma_g) \in \mathbb{Q}$. But $\Phi(\sigma_g)$ is an algebraic integer (see Lemma 2.4.3), so we even have $\Phi(\sigma_g) \in \mathbb{Z}$. This completes the proof. □

2.5 Association Schemes of Prime Order

In this section, we consider structural theorems for association schemes of prime order. In particular, we discuss the Hanaki-Uno Theorem [HU06] and certain results related to this topic. Given an association scheme $\mathfrak{X} = (X, G)$ of prime order $p := |X|$, we prove that the multiplicities of all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$ coincide, i.e. there exists $k \in \mathbb{N}$ such that $k = m_\chi$ for all $1_G \neq \chi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})$. Moreover, we show that $k = n_g$ for all $1 \neq g \in G$, i.e. all nontrivial valencies coincide with k. Furthermore, we show that for all relations $1 \neq g \in G$, the indistinguishing number is $c(g) = (k-1)$. In addition, we obtain that the scheme $\mathfrak{X}$ is commutative.

We begin by proving some basic preliminary lemmas. In the following, let $p \in \mathbb{N}$ be a prime number and let F be a field of characteristic p. Let $\mathfrak{X} = (X, G)$ be an association scheme of order $|X| = p$. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the image of a under the canonical projection $\pi : \mathbb{Z} \longrightarrow F$. We use the same notation for polynomials $f(x) \in \mathbb{Z}[x]$ and matrices $\alpha \in M_p(\mathbb{Z})$ whose coefficients/entries are reduced under π (i.e. $\overline{f}(x)$ and $\overline{\alpha}$, respectively). We regard $\mathbb{Z}\mathfrak{X}$ as a subring of $M_p(\mathbb{Z})$ and denote by E the $p \times p$ identity matrix in characteristic zero.

Lemma 2.5.1. *Let $\alpha \in \mathbb{Z}\mathfrak{X}$. If $\overline{\alpha}^2 = \overline{\alpha}$, then $\overline{\alpha}$ is either 0 or $\overline{E}$.*

Proof. For the sake of contradiction, suppose $\overline{\alpha}^2 = \overline{\alpha}$ and $\overline{\alpha} \neq 0$ and $\overline{\alpha} \neq \overline{E}$. Observe that since $\overline{\alpha}^2 = \overline{\alpha}$, every eigenvalue of $\overline{\alpha}$ is either 0 or 1. Since we assume $\overline{\alpha} \neq 0$ and $\overline{\alpha} \neq \overline{E}$, we have $tr(\overline{\alpha}) \neq 0$. However, since $\alpha \in \mathbb{Z}\mathfrak{X}$, all entries on the diagonal of α coincide. Especially, $p | tr(\alpha)$. This is a contradiction. □

Note that the following result was first proven by Hanaki [Han02]. The proof given below, which constitutes a significant simplification of the original

proof, was communicated via personal correspondence by Hanaki [Han10].

Lemma 2.5.2 ([Han02, Han10])**.** *Let $p \in \mathbb{N}$ be a prime. Let F be a field of characteristic p and let $\mathfrak{X} = (X, G)$ be an association scheme of order $|X| = p$. For $g \in G$, the matrix $\overline{\sigma_g}$ has the unique eigenvalue $\overline{n_g}$ in F.*

Proof. Let $f(x)$ be the characteristic polynomial of σ_g. Then $\overline{f}(x) \in F[x]$ is the characteristic polynomial of $\overline{\sigma_g}$. For the sake of contradiction, suppose there exists an eigenvalue of $\overline{\sigma_g}$ which is not equal to $\overline{n_g}$. Then there exists a polynomial $\overline{g}(x) \in F[x]$ such that $\overline{f}(x) = (x - \overline{n_g})^e \overline{g}(x)$, where $0 \leq e < p$ and $\overline{g}(\overline{n_g}) \neq 0$. Since $F[x]$ is a principal ideal domain, there exists polynomials $\overline{s}(x), \overline{t}(x) \in F[x]$ such that

$$(x - \overline{n_g})^e \overline{s}(x) + \overline{g}(x)\overline{t}(x) = 1.$$

Now one can easily check that $(\overline{\sigma_g} - \overline{n_g})^e \overline{s}(\overline{\sigma_g})$ and $\overline{g}(\overline{\sigma_g})\overline{t}(\overline{\sigma_g})$ are nonzero idempotents and

$$(\overline{\sigma_g} - \overline{n_g})^e \overline{s}(\overline{\sigma_g}) + \overline{g}(\overline{\sigma_g})\overline{t}(\overline{\sigma_g}) = \overline{E}.$$

This contradicts Lemma 2.5.1. □

We can now prove the following crucial lemma.

Lemma 2.5.3 ([HU06, Han10])**.** *Let $\mathfrak{X} = (X, G)$ be an association scheme of prime order $p := |X|$. Let χ be a nontrivial irreducible character of $\mathbb{C}\mathfrak{X}$ and let Φ be the sum of all algebraic conjugates of χ. Then there exist rational integers $\{u_g \mid g \in G\}$ such that*

$$\Phi(\sigma_g) = n_g \Phi(1) - u_g p.$$

Proof. Let K be a finite extension of the rational number field $\mathbb{Q}$ such that for each $g \in G$, all eigenvalues of σ_g are contained in K. Then by

[NT89] (Ch. I. 13), there exists a valuation ring R of K with maximal ideal π such that $F := R/\pi$ is a field of characteristic p and

$$\pi \cap \mathbb{Z} = (p).$$

As a valuation ring, R is integrally closed (see [Mat06], Th. 10.3). Especially, for each $g \in G$, all eigenvalues of σ_g are contained in R. Moreover, observe the following:

(i) $\Phi(\sigma_g)$ is a sum of $\Phi(1)$ eigenvalues of σ_g (see Lemma 2.4.2),

(ii) All eigenvalues of σ_g are congruent to n_g modulo π (see Lemma 2.5.2).

Together, this yields

$$\Phi(\sigma_g) \equiv n_g\Phi(1) \pmod{\pi}.$$

Since $\Phi(\sigma_g) - n_g\Phi(1) \in \mathbb{Z}$ by Lemma 2.4.5, we conclude

$$\Phi(\sigma_g) - n_g\Phi(1) \in \pi \cap \mathbb{Z} = (p).$$

The assertion follows. □

We can now prove the main result of this section, the *Hanaki-Uno Theorem*, which provides a strong structural result for association schemes of prime order.

Theorem 2.5.4 ([HU06])**.** *Let $\mathfrak{X} = (X, G)$ be an association scheme of prime order $p := |X|$. Then all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$ are algebraically conjugate. Especially, their multiplicities coincide.*

Proof. Let 1_G be the trivial character of $\mathbb{C}\mathfrak{X}$ and let χ be a nontrivial irreducible character of $\mathbb{C}\mathfrak{X}$. Let Φ be the sum of all algebraic conjugates of χ, and let Ψ be the sum of all nontrivial irreducible characters which are not

algebraically conjugate to χ. If Ψ is zero, then the assertion holds, so we assume $\Psi \neq 0$.

By Lemma 2.5.3, there exist rational integers $\{u_g \mid g \in G\}$ such that

$$\Phi(\sigma_g) = n_g\Phi(1) - u_g p.$$

Similarly, there exist rational integers $\{v_g \mid g \in G\}$ such that

$$\Psi(\sigma_g) = n_g\Psi(1) - v_g p.$$

By the orthogonality relation (Theorem 2.3.5 (ii)),

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g} 1_G(\sigma_{g^*})\Phi(\sigma_g) = \sum_{g\in G} \Phi(\sigma_g) \\ &= \sum_{g\in G} \big(n_g\Phi(1) - u_g p\big) = p\left(\Phi(1) - \sum_{g\in G} u_g\right). \end{aligned}$$

Hence, $\sum_{g\in G} u_g = \Phi(1)$. Similarly, one can show $\sum_{g\in G} v_g = \Psi(1)$.

Again by the orthogonality relation,

$$\begin{aligned} 0 &= \sum_{g\in G} \frac{1}{n_g}\Phi(\sigma_{g^*})\Psi(\sigma_g) = \sum_{g\in G} \frac{1}{n_g}\big(\Phi(1)n_{g^*} - u_{g^*}p\big)\big(\Psi(1)n_g - v_g p\big) \\ &= \sum_{g\in G} \Phi(1)\Psi(1)n_g - \sum_{g\in G} \Phi(1)v_g p - \sum_{g\in G} \Psi(1)u_{g^*}p + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2 \\ &= p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) - p\Phi(1)\Psi(1) + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2 \\ &= -p\Phi(1)\Psi(1) + \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p^2. \end{aligned}$$

We conclude

$$\Phi(1)\Psi(1) = \sum_{g\in G} \frac{1}{n_g} u_{g^*}v_g p.$$

However, $\Phi(1)\Psi(1)$ is relatively prime to p (because $\Phi(1), \Psi(1) < p$), whereas the right hand side is divisible by p (because n_g and p are relatively prime for all $g \in G$). This is a contradiction. □

The combinatorial significance of Theorem 2.5.4 becomes apparent when considering the next result. The proof given below follows after the works of Blau [Bla10] and Muzychuk-Ponomarenko [MP12].

Theorem 2.5.5. *Let $\mathfrak{X} = (X, G)$ be an association scheme. Assume that all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$ have the same multiplicity, i.e. there exists $k \in \mathbb{N}$ such that $k = m_\chi$ for all $1_G \neq \chi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})$. Then:*

(i) The association scheme $\mathfrak{X}$ is commutative,

(ii) The valency of any relation $1 \neq g \in G$ is $n_g = k$,

(iii) The indistinguishing number of any relation $1 \neq g \in G$ is $c(g) = (k-1)$.

Proof. We begin by proving statement (ii). Let γ denote the standard character of $\mathbb{C}\mathfrak{X}$ and let

$$\Phi := \sum_{1_G \neq \chi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})} \chi$$

denote the sum of all nontrivial irreducible characters of $\mathbb{C}\mathfrak{X}$. Observe the following:

$$|X| = \gamma(1) = 1 + k\Phi(1),$$

$$0 = \gamma(\sigma_g) = n_g + k\Phi(\sigma_g), \quad g \in G.$$

Choose $1 \neq f \in G$ such that n_f is the smallest valency of a relation in G. Then

$$k(-\Phi(\sigma_f))(|G| - 1) = n_f(|G| - 1) \leq |X| - 1 = k\Phi(1) \leq k(|G| - 1).$$

Since $(-\Phi(\sigma_f))$ is a positive integer, the above inequality implies $(-\Phi(\sigma_f)) = 1$. We conclude that equality holds at every point in the above inequality. Especially, $k(|G| - 1) = n_f(|G| - 1) = |X| - 1$. Since n_f is the smallest valency of a relation in G, we conclude $k = n_g$ for all $1 \neq g \in G$.

This proves statement (ii). Moreover, since $\Phi(1) = (|G| - 1)$, we conclude that $\mathfrak{X}$ is commutative (see Lemma 2.4.1 (i)). This proves statement (i).

What remains is to prove statement (iii). Let $\chi_{\mathbb{C}\mathfrak{X}}$ denote the principal character of $\mathbb{C}\mathfrak{X}$. Note that by Lemma 2.1.5 and statement (ii), we have

$$\chi_{\mathbb{C}\mathfrak{X}}(\sigma_g) = \sum_{v \in G} c_{vg}^{v} = c(g)$$

for all $1 \neq g \in G$. Now observe that since $\mathfrak{X}$ is commutative, we have $\chi(1) = 1$ for all irreducible characters $\chi \in \mathrm{Irr}(\mathbb{C}\mathfrak{X})$ (see Lemma 2.4.1). Consequently, by Lemma 2.4.1 (ii), for all $1 \neq g \in G$,

$$\chi_{\mathbb{C}\mathfrak{X}}(\sigma_g) = k + \Phi(\sigma_g).$$

Now observe that for all $1 \neq g \in G$,

$$k(k - \chi_{\mathbb{C}\mathfrak{X}}(\sigma_g)) = -k\Phi(\sigma_g) = k - \gamma(\sigma_g) = k;$$

especially, $\chi_{\mathbb{C}\mathfrak{X}}(\sigma_g) = (k - 1)$. This yields statement (iii). □

2.6 Association Schemes with Bounded Valencies and Indistinguishing Numbers

In the following, we concern ourselves with association schemes $\mathfrak{X} = (X, G)$ whose valencies and indistinguishing numbers of nontrivial relations $g \in G$ are confined to a certain range (see Theorem 2.6.1). In simple terms, we prove that there exist *small* intersection numbers in such association schemes. Note that association schemes of prime order are easily seen to belong to the class of association schemes considered in this section (see Theorem 2.5.5). Moreover, note that the results of this section will be of much importance in Chapters 3 and 4, when they are applied to a general framework for the computational problem of polynomial factoring over finite fields.

Theorem 2.6.1 ([AIKS12])**.** *Let (X, G) be an association scheme. Assume there exist $c, k, \ell \in \mathbb{N}$ and $0 < \delta_1, \delta_1', \delta_2' \leq 1$ with $1 < \ell < (\delta_1^2/\delta_1') \cdot k$ such that for all $1 \neq g \in G$,*

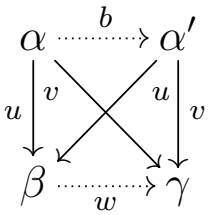
$$\delta_1 \cdot k \leq n_g \leq \delta_1' \cdot k \quad \text{and} \quad c(g) \leq \delta_2' \cdot c.$$

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

Proof. 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_{bu}^u choices for $\alpha' \in X$ such that $(\alpha, \alpha') \in b$ and $(\alpha', \beta) \in u$. Moreover, after choosing α', there are exactly $c_{vv^*}^b$ choices for $\gamma \in X$ such that $(\alpha, \gamma), (\alpha', \gamma) \in v$. Thus, $|S_v| = \sum_{b \in G} c_{bu}^u \cdot c_{vv^*}^b$. In particular,

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

where the last inequality follows from Lemma 2.1.5 (3).

For the sake of contradiction, assume that for all $v \in G \setminus \{1, u\}$ we have either $c_{u^*v}^w = 0$ or $c_{u^*v}^w \geq \ell$ 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 $c^u_{vw^*} \geq c^w_{u^*v} \cdot \frac{\delta_1}{\delta'_1}$ for all $w \in W_v$ by Lemma 2.1.5 (1), (2). Since we assume that $c^w_{u^*v} \geq \ell$ for all except at most one relation $w \in W_v$ we conclude

$$|S_v| \geq \frac{\delta_1}{\delta'_1} \cdot \sum_{w \in W_v} c^w_{u^*v}(c^w_{u^*v} - 1) \geq \frac{\delta_1}{\delta'_1} \cdot \left((\ell - 1) \cdot \sum_{w \in W_v} c^w_{u^*v} - \frac{\ell^2}{4} \right).$$

Note that the last inequality follows from the summand-wise inequality: $(\ell - 1)c^w_{u^*v} - c^w_{u^*v}(c^w_{u^*v} - 1) \leq (\ell^2/4)$. From $\sum_{w \in W_v} c^w_{u^*v} \cdot n_w = n_{u^*} \cdot n_v$ (see Lemma 2.1.5 (4)) it follows that $\sum_{w \in W_v} c^w_{u^*v} \geq (\delta_1^2/\delta'_1) \cdot k$. Moreover, using the assumption $1 < \ell < (\delta_1^2/\delta'_1) \cdot k$, we deduce

$$|S_v| \geq \frac{\delta_1}{\delta'_1} \cdot (\ell - 1) \cdot \left(\frac{\delta_1^2}{\delta'_1} \cdot k - \frac{\ell^2}{4(\ell - 1)} \right) > \frac{\delta_1^3}{2(\delta'_1)^2} \cdot (\ell - 1)k.$$

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 $\delta'_1\delta'_2 \cdot ck > (|G| - 2) \cdot \frac{\delta_1^3}{2(\delta'_1)^2} \cdot (\ell - 1)k$, from which we conclude $2(\delta'_1/\delta_1)^3\delta'_2 \cdot \frac{c}{\ell - 1} + 2 > |G|$. This is a contradiction. □

Theorem 2.6.1 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. Applying this result to association schemes of prime order (see Theorems 2.5.4 and 2.5.5) yields the following corollary.

Corollary 2.6.2 ([AIKS12]). *Let (X, G) be an association scheme of prime order $p := |X|$. Let $k \in \mathbb{N}$ be such that for all $1 \neq g \in G$, $k = n_g$. Let $\ell \in \mathbb{N}_{>1}$. If $|G| \geq \frac{2(k-1)}{\ell-1} + 2$ then there exist nontrivial relations $u \neq v$, $w \neq w' \in G$ such that $0 < c_{u^*v}^{w} \leq c_{u^*v}^{w'} < \ell$.*

It is possible to prove that, in a certain sense, the result achieved in Corollary 2.6.2 is optimal. The example of the cyclotomic scheme below shows that the conditions of Corollary 2.6.2 cannot be relaxed (up to constant factors).

In the following, let p be a prime and fix $d|(p-1)$. Let $\mathrm{Cyc}(p, d) = (\mathbb{F}_p, \mathcal{P})$ denote the cyclotomic scheme in (p, d) and let $k := (p-1)/d$. For nontrivial relations $P_r, P_s, P_t \in \mathcal{P}$ and $(x, y) \in P_t$, we have

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

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

By the Hasse-Weil bound [Wei76, Voi05], we have

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

from which it follows that

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

To make the 'error' term small, we fix p and d such that $d = k^{1/3}/c \succeq p^{1/4}$ for a large enough constant $c \in \mathbb{N}$ (note that there are infinitely many primes p for which there exists such d by [For08], Theorem 7). Now $(p+1)/d^2 \geq 2\sqrt{p}$ and we can estimate

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

Moreover, we have $|G| > d \geq k/(ck^{2/3})$. Thus, we have an association scheme where both the number of relations and the intersection numbers are large, i.e. in the range $k^{\frac{1}{3}}$ and $k^{\frac{2}{3}}$, respectively. This matches the parameters of Corollary 2.6.2 exactly.

Chapter 3

m-Schemes

In this chapter, we introduce the notion of m-schemes, combinatorial objects which may be regarded as higher-dimensional analogs of the concept of association schemes. m-Schemes were first defined in the paper [IKS09], where they appear naturally in connection with an algebraic-combinatorial approach to the computational problem of polynomial factoring over finite fields (the polynomial factoring approach of [IKS09] is delineated in Chapter 4). If we denote $[n] := \{1, ..., n\}$, then an m-scheme can be described as a partition of the set $[n]^s$, for each $1 \leq s \leq m$, which satisfies certain natural properties called compatibility, regularity and invariance (see Section 3.1). Note that m-schemes are closely related to association schemes (see Section 3.2) and are connected to various other notions of combinatorial schemes, such as presuperschemes [Woj01a, Woj98, Woj01b], superschemes [Smi94, Smi07], coherent configurations [Hig70], cellular algebras [WL68] and Krasner algebras [Kra38].

The material in this chapter is organized as follows. In §3.1, we define m-schemes and discuss certain natural properties associated with this notion. In §3.2, we describe the connection of m-schemes and association schemes.

§3.3 provides a discussion of orbit m-schemes, a class of m-schemes which may be regarded as a higher-dimensional analog of Schurian association schemes. §3.4 introduces the notion of matchings, generalizing the concept of thin relations (i.e. relations of valency 1) from association schemes to the higher dimensions of m-schemes. §3.5 provides a discussion of the schemes conjecture, which concerns the existence of matchings in homogeneous and antisymmetric m-schemes and holds great significance for the polynomial factoring framework described in Chapter 4. In §3.6, we prove the currently best known bound for the existence of matchings in homogeneous and antisymmetric m-schemes.

3.1 Basic Notions

In this section, we introduce the notion of m-schemes. The terminology used here follows after the works [IKS09, AIKS12].

s-Tuples: Throughout this section, let V be an arbitrary set of n distinct elements. For $1 \leq s \leq n$, 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 each $s > 1$, we define s *natural projections*

$$\pi_1^s, \pi_2^s, \ldots, \pi_s^s : V^{(s)} \longrightarrow V^{(s-1)}$$
$$\pi_i^s : (v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_s) \longrightarrow (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_s).$$

Furthermore, for $1 \leq i_1 < \ldots < i_k \leq s$ we define

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

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. For all

$(v_1, \ldots, v_i, \ldots, v_s) \in V^{(s)}$ and $\tau \in \mathrm{Symm}_s$, define

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

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

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

Next, we discuss some natural properties of m-collections which are relevant to us in the future. In the following, let $\Pi = \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ 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 $1 \leq i \leq s$, 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 $P \in \mathcal{P}_s$,

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

Fibers: We call the tuples in $P \cap (\pi_i^s)^{-1}(\bar{u})$ the *π_i^s-fibers of $\bar{u}$ in P*. Using this terminology, the property of regularity just 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 an s-color P over an $(s-k)$-color Q* as $s(P, Q) := \frac{|P|}{|Q|}$, assuming

$\pi^s_{i_1,\ldots,i_k}(P) = Q$ for some $1 \leq i_1 < \ldots < i_k \leq s$ and that Π is regular at all levels $2, \ldots, s$.

P3 (Invariance): We say that Π is *invariant* at level $1 < s \leq m$, if for every $P \in \mathcal{P}_s$ and $\tau \in \mathrm{Symm}_s$,

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

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

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

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

P6 (Symmetry): We say that Π is *symmetric* at level $1 < s \leq m$, 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*, *antisymmetric*, or *symmetric* if it is at every level $1 < s \leq m$, compatible, regular, invariant, antisymmetric, or symmetric respectively.

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

To familiarize ourselves with the above definitions, we prove an easy non-existence lemma for m-schemes. Note that the lemma below rephrases the combinatorial argument of [Rón88] in m-scheme terminology.

Lemma 3.1.1 ([IKS09])**.** *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 $m \geq r$, clearly every m-scheme contains an r-scheme. 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 $V = \{v_1, v_2, \ldots, v_n\}$. By definition, $\mathcal{P}_r$ partitions

$n(n-1)\cdots(n-r+1)$ 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, $r!n|n(n-1)\cdots(n-r+1)$. But this implies $r!|(n-1)\cdots(n-r+1)$, which contradicts $r|n$. Therefore, Π cannot exist. □

In the following sections, we describe the relationship between m-schemes and association schemes and discuss the example of orbit m-schemes.

3.2 3-Schemes from Association Schemes

The notion of m-schemes is closely related to the concept of association schemes. In this section, we show that the notion of homogeneous 3-schemes and association schemes are essentially equivalent. The next lemma shows that the first two levels of any homogeneous 3-scheme constitute an association scheme (up to containment of the identity relation).

Lemma 3.2.1. *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 $\big(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\}\big)$ 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 $\mathcal{S} \subseteq \mathcal{P}_3$ 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

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

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

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

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

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

Since the above equation is independent of the choice of $(\alpha,\beta)\in P_k$, it follows that $\big(\mathcal{P}_1,\mathcal{P}_2\cup\{1\}\big)$ is an association scheme. □

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

Lemma 3.2.2. *Let $(\mathcal{P}_1,\mathcal{P}_2)$ 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 $\{\mathcal{P}_1,\mathcal{P}_2-\{1\},\mathcal{P}_3\}$ is a 3-scheme.

Proof. It is an easy exercise to show that $\{\mathcal{P}_1,\mathcal{P}_2-\{1\},\mathcal{P}_3\}$ satisfies compatibility, regularity and invariance. □

3.3 Orbit m-Schemes

In this section, we introduce *orbit m-schemes*, a class of m-schemes which is constructed from the action of permutation groups. Orbit m-schemes can be regarded as a higher-level analog of the notion of Schurian association schemes (see Example 2.1.2). Throughout this section, let $V = \{v_1, v_2, ..., v_n\}$ be a set of n distinct elements and $G \leq Symm_V$ a permutation group. Consider the following theorem.

Theorem 3.3.1. *Fix some integer $2 \leq m \leq n$. For $1 \leq s \leq m$, let $\mathcal{P}_s$ be the partition on $V^{(s)}$ such that for any two s-tuples $(u_1, u_2, ..., u_s)$ and $(v_1, v_2, ..., v_s)$, we have $(u_1, u_2, ..., u_s) \equiv_{\mathcal{P}_s} (v_1, v_2, ..., v_s)$ if and only if*

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

Then $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is an m-scheme on V. Moreover:

(i) $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is homogeneous if and only if G is transitive,

(ii) $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is antisymmetric if and only if $gcd(m!, |G|) = 1$.

Proof. We prove statement (ii) and leave the remaining assertions as an exercise to the reader. First, suppose $gcd(m!, |G|) = 1$. Assume for the sake of contradiction that $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is not antisymmetric at some level $1 < s \leq m$. Then there exists $(u_1, u_2, ..., u_s) \in V^{(s)}$ such that

$$(u_1, u_2, ..., u_s) \equiv_{\mathcal{P}_s} (u_{1^\tau}, u_{2^\tau}, ..., u_{s^\tau})$$

for some $id \neq \tau \in Symm_s$. By the definition of $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$, this means there exists $\sigma \in G$ such that

$$(\sigma(u_1), \sigma(u_2), ..., \sigma(u_s)) = (u_{1^\tau}, u_{2^\tau}, ..., u_{s^\tau}).$$

Choose an index $j \in \{1, ..., s\}$ such that $\sigma(u_j) \neq u_j$. Then there exists an integer k such that $2 \leq k \leq s$ and

$$\sigma^k(u_j) = u_j.$$

Clearly, k divides the order of σ, which in turn divides the order of G. Hence $gcd(m!, |G|) > 1$, a contradiction.

Now consider the converse: Suppose $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is antisymmetric. Assume for the sake of contradiction that $gcd(m!, |G|) > 1$. By Sylow's Theorem, there exists $\sigma \in G$ such that $\sigma^k = id$ for some $k \leq m$. We can now easily obtain a contradiction by reversing the proof of the opposite direction. The details are left to the reader. □

We call m-schemes which arise from the action of permutation groups as described in Theorem 3.3.1 **orbit m-schemes**. Currently, all examples of homogeneous and antisymmetric m-schemes with $m \geq 4$ which we know of stem from the class of orbit m-schemes.

It is known that every $(n-1)$-scheme on n points is an orbit scheme (see Theorem 5.1.2). Moreover, the important schemes conjecture (see Section 3.5) is already proven for orbit m-schemes. We will study the above issues in more detail at a later point.

3.4 Matchings

We now introduce the notion of *matchings*, certain special colors of m-schemes which have important applications for the polynomial factoring framework described in Chapter 4. Note that matchings generalize the concept of *thin relations* (i.e. relations of valency 1) from the theory of association schemes to the higher-dimensional setting of m-schemes. In

the following, 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 $1 < s \leq m$ is called a *matching* if for some positive integer k there exists $1 \leq i_1 < \ldots < i_k \leq s$ and $1 \leq j_1 < \ldots < j_k \leq s$ 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 $\left|\pi^s_{i_1,\ldots,i_k}(P)\right| = |P|$.

Note that the paper [IKS09] 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. Also note that under the identification of homogeneous 3-schemes and association schemes (see Lemmas 3.2.1 and 3.2.2), matchings at level 2 correspond simply to thin relations (i.e. relations of valency 1).

The next theorem gives an important sufficient condition for the existence of matchings in m-schemes.

Theorem 3.4.1 ([AIKS12])**.** *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$ be an m-scheme on $V = \{v_1, v_2, \ldots, v_n\}$. 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 $1 \leq i \leq t$ such that $1 < s(P_t, P_{t-1}) = \frac{|P_t|}{|P_{t-1}|} \leq \ell$ and $m \geq t - 1 + \log_2 \ell$, where $\ell \in \mathbb{N}$. Then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$.*

Proof. Wlog, 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

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

Evidently, if $s(P_{t+1}, P_t) = 1$ then P_{t+1} is a matching. Otherwise, if $s(P_{t+1}, P_t) > 1$ then 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. □

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

Corollary 3.4.2. *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 $m \geq \log_2 n$ then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m\}$.*

In Section 3.6, we show how combinatorial arguments can further improve the bound $m \geq \log_2 n$ of Corollary 3.4.2. It is conjectured that $m \geq c$ (where $c \geq 4$ is some constant) is sufficient to guarantee the existence of matchings in homogeneous and antisymmetric m-schemes. We discuss this conjecture in the next section.

3.5 The Schemes Conjecture

In Corollary 3.4.2 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 $c \geq 4$ that could replace the above $\log_2 n$-bound.

Conjecture 3.5.1 (Schemes Conjecture)**.** *There exists a constant $c \geq 4$ such that every homogeneous, antisymmetric m-scheme with $m \geq c$ contains a matching.*

In Chapter 4, we revisit a theorem from [IKS09, AIKS12], which states that under GRH, the correctness of the schemes conjecture implies a de-

terministic polynomial time algorithm for the factorization of polynomials over finite fields (see Theorem 4.3.1). The schemes conjecture is especially motivated by the fact that it is known to be true for orbit m-schemes.

Theorem 3.5.2 (Schemes Conjecture for Orbit m-Schemes)**.** *For $m \geq 4$, every homogeneous, antisymmetric orbit m-scheme contains a matching.*

Proof. This is shown in [IKS09], Section 4.1. □

Drawing on the association scheme results from Section 2.6, we can prove the schemes conjecture for m-schemes $\Pi = \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ on a prime number of points which have 'large' number of relations at level 2. This is provided in the following theorem.

Theorem 3.5.3 ([AIKS12])**.** *Let $\Pi = \{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ be a homogeneous, antisymmetric m-scheme on V, where $p := |V|$ is a prime number. Let $k \in \mathbb{N}$ denote the valency of every nontrivial relation of the association scheme $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$. Assume that $m \geq 2\log_2 \ell + 3$ and $|\mathcal{P}_2| \geq \frac{2(k-1)}{\ell-1} + 1$ for some $\ell \in \mathbb{N}_{>1}$. Then there exists a matching in Π.*

Proof. By Corollary 2.6.2, there exist nontrivial relations $u \neq v, w \neq w' \in \mathcal{P}_2$ such that $0 < c^w_{u^*v} \leq c^{w'}_{u^*v} < \ell$. 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, $|P|/|v| = |P|/|u| \leq c^w_{u^*v} \cdot c^{w'}_{u^*v} \leq \ell^2$, 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 follows that at least one of the subdegrees $s(P, Q), s(Q, v)$ is both at least 2 and at most ℓ^2. Especially, we get a matching in Π by suitably invoking Theorem 3.4.1. □

In Chapter 4, we describe how Theorem 3.5.3 translates to an important result concerning the factorization of prime-degree polynomials over finite fields (see Theorem 4.4.1). It is a good example of how progress towards the schemes conjecture translates into improvements in the realm of polynomial factoring through the IKS-framework.

3.6 An Improved Matching Bound

In this section, we strengthen the criterion for matchings in homogeneous and antisymmetric given in Corollary 3.4.2. For the remainder of this chapter, we omit the level indices of the projections $\pi_1^s, \pi_2^s ..., \pi_s^s$ $(s > 1)$, we assume that the corresponding level will be clear from context. In addition, we establish the following terminology.

Underlying Color Sequence: Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme, where $m \geq 3$. Then we define the *underlying color sequence* of a color $C \in \mathcal{P}_3$ as the tuple

$$(\pi_1(C), \pi_2(C), \pi_3(C)),$$

which gives us the information to which colors C projects at the second level.

The following result was shown in [IKS09] (see Lemma 10). It gives an improvement of the bound for the existence of matchings in homogeneous and antisymmetric m-schemes over Corollary 3.4.2.

Theorem 3.6.1 ([IKS09])**.** *Let* $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ *be a homogeneous* m*-scheme on* $V = \{v_1, v_2, ..., v_n\}$*. Assume that* Π *is antisymmetric at the first three levels. Moreover, assume that* $m \geq \frac{2}{3} \log_2 n$*. Then there exists a matching in* $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$*.*

We will see next that it is possible to further improve the bound $m \geq \frac{2}{3}\log_2 n$ of Theorem 3.6.1. The discussion below leads to new results and manifests some new concepts. First, we prove the following preliminary lemma.

Lemma 3.6.2 ([Aro11])**.** *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ be a homogeneous, antisymmetric 3-scheme on $V = \{v_1, v_2, ..., v_n\}$. Assume that $\mathcal{P}_2$ contains exactly 2 colors, say $\mathcal{P}_2 = \{P, Q\}$, where $Q = P^{(1,2)}$. Then the following holds:*

(i) There exists a color $C \in \mathcal{P}_3$ with underlying color sequence (P, P, P),

(ii) There exists a color $D \in \mathcal{P}_3$ with underlying color sequence (P, Q, P),

(iii) There exists a color $S \in \mathcal{P}_3$ with $s(S, P) \leq \frac{n}{12}$ and $\pi_1(S) = \pi_3(S) = P$.

Proof. (i) First, observe that the set

$$A := \{\bar{v} \in V^{(3)} \mid \pi_2(\bar{v}), \pi_3(\bar{v}) \in P\}$$

is a nontrivial union of $\mathcal{P}_3$-colors that have underlying color sequence either (P, P, P) or (Q, P, P). Second, observe that if a color $S \in \mathcal{P}_3$ has underlying color sequence (Q, P, P), then its associated color $T := S^{(2,3)}$ has underlying color sequence (P, P, P). Together, this implies that there exists at least one color $C \in \mathcal{P}_3$ with underlying color sequence (P, P, P).

(ii) Recall that since $|\mathcal{P}_2| = 2$ there are exactly 8 possibilities of underlying color sequences for colors in $\mathcal{P}_3$. We can partition these 8 possibilities into two sets

$$\{(P, P, P),\ (P, P, Q),\ (P, Q, Q),\ (Q, Q, Q),\ (Q, Q, P),\ (Q, P, P)\},$$

$$\{(P, Q, P),\ (Q, P, Q)\}$$

which constitute the two different options for the set of underlying color sequences that a set of associated colors $\{F^\sigma \,|\, \sigma \in Symm_3\}$ $(F \in \mathcal{P}_3)$ can have. Now observe that

$$\left|\{\bar{v} \in V^{(3)} \,|\, \pi_1(\bar{v}), \pi_2(\bar{v}), \pi_3(\bar{v}) \in P\}\right| = \frac{|A|}{2} = \frac{n \cdot (n-1) \cdot (n-3)}{8} \quad (3.6.1)$$

and hence the combined size of all colors having one of the underlying color sequences

$$(P,P,P),\ (P,P,Q),\ (P,Q,Q),\ (Q,Q,Q),\ (Q,Q,P),\ (Q,P,P)$$

is $6 \cdot \frac{n\cdot(n-1)\cdot(n-3)}{8}$, which is strictly smaller than $\left|V^{(3)}\right|$. So there must exist colors in $\mathcal{P}_3$ whose underlying color sequence is not one of the above six, but rather one of

$$(P,Q,P),\ (Q,P,Q).$$

This completes the proof of statement (ii).

(iii) Consider the set

$$Z := \{\bar{v} \in V^{(3)} \,|\, \pi_1(\bar{v}), \pi_3(\bar{v}) \in P\}.$$

The above set can be partitioned into $Z = X \sqcup Y$, where

$$X := \{\bar{v} \in V^{(3)} \,|\, \pi_1(\bar{v}), \pi_2(\bar{v}), \pi_3(\bar{v}) \in P\},$$

$$Y := \{\bar{v} \in V^{(3)} \,|\, \pi_1(\bar{v}), \pi_3(\bar{v}) \in P,\ \pi_2(\bar{v}) \in Q\}.$$

For the cardinalities of Z and X, we have

$$|Z| = \frac{n \cdot (n-1) \cdot (n-3)}{4}\ , \quad |X| = \frac{n \cdot (n-1) \cdot (n-3)}{8};$$

the latter one was computed in Equation (3.6.1). From this we obtain the cardinality of Y,

$$|Y| = |Z| - |X| = \frac{n \cdot (n-1) \cdot (n-3)}{8}. \quad (3.6.2)$$

We now show that there are at least 3 colors in $\mathcal{P}_3$ which are subsets of Z. For this purpose, choose a color $D \in \mathcal{P}_3$ with underlying color sequence (P, Q, P). Next, observe that there are exactly 3 colors in $\{D^\sigma \mid \sigma \in Symm_3\}$ which have underlying color sequence (P, Q, P). Hence there are at least 3 colors in $\mathcal{P}_3$ which are subsets of Z. Consequently, there exists a color $S \in \mathcal{P}_3$ such that $S \subset Z$ and

$$s(S, P) \leq \frac{|Z|/3}{|P|} < n/12;$$

the latter inequality can be deduced using Equation (3.6.2). This completes the proof. □

Using Lemma 3.6.2, we can now prove the main result of this section. Theorem 3.6.1 yields an improved level bound for matchings in homogeneous and antisymmetric m-schemes (which is currently the best known).

Theorem 3.6.3. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be a homogeneous m-scheme on $V = \{v_1, v_2, ..., v_n\}$. Assume that Π is antisymmetric at the first three levels. Moreover, assume $m \geq \frac{2}{\log_2 12} \log_2 n + 2 \approx 0.559 \log_2 n + 2$. Then there exists a matching in $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$.*

Proof. By Lemma 3.6.2 (iii), for any color $P_t \in \mathcal{P}_t$ $(1 < t \leq m-2)$ which has subdegree ℓ over $P_{t-1} := \pi_t(P_t) \in \mathcal{P}_{t-1}$, we either find a color $P_{t+2} \in \mathcal{P}_{t+2}$ such that $\pi_{t+2}(P_{t+2}) = \pi_t(P_{t+2})$ and $s(P_{t+2}, \pi_{t+2}(P_{t+2})) < \frac{\ell}{12}$, or we find a color $P_{t+1} \in \mathcal{P}_{t+1}$ such that $\pi_{t+1}(P_{t+1}) = \pi_t(P_{t+1})$ and $s(P_{t+1}, \pi_t(P_{t+1})) < \frac{\ell}{4}$. Using this observation, iteration yields the desired bound. □

Chapter 4

GRH-Based Deterministic Polynomial Factoring

In this chapter, we discuss the IKS-framework for polynomial factoring over finite fields [IKS09, AIKS12], which is based on the assumption of the generalized Riemann hypothesis (GRH). The IKS-framework relies on the theory of m-schemes, which provides a natural tool to codify the algebraic-combinatorial information which occurs in the process of polynomial factoring. The IKS-algorithm 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 $\mathcal{A}^{\otimes s}$ $(1 \leq s \leq m)$. 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 $\mathcal{A}^{\otimes s}$ $(1 \leq s \leq m)$. It is not difficult to prove that the IKS-algorithm always finds a zero divisor in $\mathcal{A}$ if we choose m large enough (viz. in the range $\log n$), which implies that the IKS-algorithm deterministically factors $f(x)$ in time $\text{poly}(n^{\log n}, \log q)$. Moreover, it is conjectured that even choosing m as

constant, say $m = c$ where $c \geq 4$, 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. The latter result would follow from the correctness of the schemes conjecture (see Section 3.5).

The IKS-framework subsumes several earlier approaches to GRH-based polynomial factoring. Given a degree n polynomial $f(x) \in \mathbb{F}_q$ which has n distinct roots in $\mathbb{F}_q$, the IKS-algorithm finds a nontrivial factor of $f(x)$ in time $\text{poly}(n^{\log n}, \log q)$, matching the best known time-bound of Evdokimov [Evd94]. Moreover, if the degree n of the polynomial $f(x)$ is constant-smooth, then the IKS-algorithm factors $f(x)$ in polynomial time, matching an earlier result of Rónyai [Rón88] (which used a framework less general than that of m-schemes). Concerning the factorization of prime-degree polynomials - a notoriously complicated case - the IKS-algorithm offers significant improvements over the earlier methods. It was shown in [IKS09] 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 4.4, we delineate the advances of [AIKS12], which extend 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 $\text{poly}(n, \log q)$.

The material in this chapter is organized as follows. In §4.1, we provide the necessary algebraic prerequisites for the discussion of the IKS-framework for polynomial factoring over finite fields. In §4.2, we give a description of the IKS-algorithm. §4.3 delineates how certain properties of m-schemes relate to the problem of polynomial factoring via the IKS-framework. §4.4 describes

how structural results for m-schemes on a prime number of points translate to improvements for factoring certain classes of prime-degree polynomials. In §4.5, we take a closer look at specific classes of prime numbers for which our structural results make progress.

4.1 Algebraic Prerequisites

In this section, we discuss algebraic prerequisites for the description of the IKS-algorithm. Below, we revisit some of the basic concepts of polynomial factoring over finite fields.

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 $\mathbb{F}_q$ which have n distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{F}_q$ [Ber67, Ber70]. 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*

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

The algebra $\mathcal{A}$ is isomorphic to k^n, the direct product of n copies of the one-dimensional algebra k. 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 $\mathcal{A}$: Observe that for nonzero polynomials $y(x), z(x) \in \mathcal{A}$, if $y(x)z(x) = 0$ 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, as shown in the following lemma.

Lemma 4.1.1. *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 can be partitioned as*

$$V = \mathit{Supp}(I_1) \sqcup \cdots \sqcup \mathit{Supp}(I_t).$$

Tensor powers of $\mathcal{A}$: For $1 \leq m \leq n$, we denote by $\mathcal{A}^{\otimes m}$ the m-th tensor power of $\mathcal{A}$ (regarded as k-modules). We may interpret $\mathcal{A}^{\otimes m}$ as the algebra of all functions from V^m to k. In this interpretation, the rank one tensor element $h_1 \otimes \cdots \otimes h_m$ corresponds to a function 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 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 4.1.1 can be generalized as follows:

Lemma 4.1.2. *For $s \leq n$, 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 $V^{(s)}$ can be partitioned as*

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

Connection with GRH: The IKS-algorithm relies on the assumption of the generalized Riemann hypothesis (GRH) [Rie59, Cho65, BCRW08]. 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 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 > 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 [Rón92] 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. Rónyai's result [Rón92] relies on the ability of efficiently computing *radicals* (r-th roots for prime r) in finite fields, which is known to be possible under GRH as shown by Huang [Hua84]. Hence, the assumption of GRH is an artifact of Huang's result. The motivating case of a prime field and $r = 2$ can be easily explained by Ankeny's theorem [Ank52] on the smallest primitive root.

4.2 Description of the IKS-algorithm

In the following, we describe the routine of the IKS-algorithm. Throughout this section, let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree n having n dis-

tinct 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. For algorithmic purposes, we assume $\mathcal{A}$ is given by structure constants with respect to some basis $b_1, \ldots, b_n$. Below, we recall below a result from [IKS09] which delineates a deterministic algorithm for computing the essential parts $\mathcal{A}^{(s)}$ $(1 \leq s \leq n)$.

Lemma 4.2.1. *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* $\mathrm{poly}(\log |k|, n^m)$.

Proof. Define embeddings μ_i $(1 \leq i \leq m)$ of $\mathcal{A}$ into $\mathcal{A}^{\otimes m}$ as follows:

$$\mu_i : \mathcal{A} \longrightarrow \mathcal{A}^{\otimes m}, \quad a \longrightarrow 1 \otimes \cdots \otimes 1 \otimes \underset{\substack{\uparrow \\ i\text{-th factor}}}{a} \otimes 1 \otimes \cdots \otimes 1.$$

In the functional interpretation, $\mu_i(\mathcal{A})$ corresponds to those functions on $V^{(m)}$ which depend only on the i-th coordinate of the tuples. For $1 \leq i < j \leq m$, we define

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

Observe that $\Delta_{i,j}^m$ is the ideal of $\mathcal{A}^{\otimes m}$ consisting of the functions which are zero on every tuple $(v_1, v_2, ..., v_m) \in V^m$ with $v_i \neq v_j$. A basis for $\Delta_{i,j}^m$ 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). Since $\mathcal{A}^{(m)}$ is just the annihilating ideal of $\sum_{1 \leq i < j \leq m} \Delta_{i,j}^m$,

$$\mathcal{A}^{(m)} = \{c \in \mathcal{A}^{\otimes m} \mid bc = 0 \ \text{ for every } b \in \textstyle\sum_{1 \leq i < j \leq m} \Delta_{i,j}^m\},$$

we can compute $\mathcal{A}^{(m)}$ in $poly(n^m)$ field operations. The assertion follows. □

We now proceed to give an overview of the routine of the IKS-algorithm. We delineate how an m-scheme can be obtained from the ideal decompositions of the essential parts $\mathcal{A}^{(s)}$ $(1 \leq s \leq n)$. For referential purposes, let us quickly recall 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 $1 < m \leq n$ is given, and we can assume that we have the smallest field extension $k \supseteq \mathbb{F}_q$ having s-th nonresidues for all $1 \leq s \leq m$ (computing k will take $\text{poly}(\log q, m^m)$ 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 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 $\mathcal{A}^{(s)}$ $(1 < s \leq m)$ of the tensor powers of $\mathcal{A}$ (this takes $\text{poly}(\log q, n^m)$ time by Lemma 4.2.1).

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

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

is an algebra automorphism of $\mathcal{A}^{(s)}$. By [Rón92], 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 $I_{s,1}, \ldots, I_{s,t_s}$ $(t_s \geq 2)$ of $\mathcal{A}^{(s)}$ such that

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

By Lemma 4.1.2, this decomposition of $\mathcal{A}^{(s)}$ induces a partition $\mathcal{P}_s$ on $V^{(s)}$:

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

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 $1 < s \leq m$ we have s natural algebra embeddings $\iota_1^s, \ldots, \iota_s^s : \mathcal{A}^{\otimes(s-1)} \longrightarrow \mathcal{A}^{\otimes s}$ which map $b_{i_1} \otimes \cdots \otimes b_{i_{s-1}}$ to $b_{i_1} \otimes \cdots \otimes b_{i_{j-1}} \otimes 1 \otimes b_{i_j} \otimes \cdots \otimes b_{i_{s-1}}$ 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 j-th coordinate.

The algorithm is now best described by explaining the five kinds of refinement procedures which 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 $I_{s,i'}$ 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 $1 < s \leq m$, 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 $I_{s-1,i}$ 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 $1 < s \leq m$ 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 $1 < s \leq m$, for some ideal $I_{s,i}$ and for some $\tau \in \mathrm{Symm}_s \backslash \{id\}$, we have $I_{s,i}^{\tau} = I_{s,i}$, then τ is an algebra automorphism of $I_{s,i}$. By [Rón92], 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 $\mathcal{A}^{(s)}$ $(1 \leq s \leq m)$ 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 $\mathrm{poly}(\log q, n^m)$.

4.3 From m-Schemes to Factoring

In the last section, we described how to either find a nontrivial factor of a given polynomial $f(x)$ or construct an m-scheme on the n roots of $f(x)$. In the following, we explain how to deal with the 'bad case', when we get a homogeneous, antisymmetric m-scheme instead of a nontrivial factor. We show 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 extends the argument of [IKS09], Theorem 7 to our general notion of matchings).

Theorem 4.3.1 ([AIKS12])**.** *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 ei-*

ther 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 described in Section 4.2. 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 $1 \leq i_1 < \ldots < i_k \leq s$ and $1 \leq j_1 < \ldots < j_k \leq s$ 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 $\left|\pi^s_{i_1,\ldots,i_k}(P)\right| = |P|$. 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 implies 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 [Rón92], 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 and Corollary 3.4.2, 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 [Evd94], which is based on a framework less general than that of m-schemes described above. Note that any progress towards the schemes conjecture (Section 3.5) 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 4.3.1 never occurs. This is discussed in the following section.

4.4 Factoring Prime Degree Polynomials

Following after the work [AIKS12], 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 $s|(n-1)$ and all prime factors of s are smaller than r (the exact relationship between ℓ, r and the time is described in Theorem 4.4.1). 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 [IKS09]. The results given in this section 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 the structural results about association schemes of prime order described in Sections 2.5 and 2.6.

Theorem 4.4.1 ([AIKS12])**.** *Let $f(x)$ be a polynomial of prime degree n over $\mathbb{F}_q$. Assume $(n-1)$ has an r-smooth divisor s, with $s \geq \sqrt{n/\ell}+1$ 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.*

Proof. 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 4.2) and by Theorem 4.3.1 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 $\text{poly}(\log q, n^m)$. Suppose for the sake of contradiction that the latter case occurs.

Clearly, $(\mathcal{P}_1, \mathcal{P}_2 \cup \{1\})$ is an association scheme of prime order n, where 1 denotes the trivial relation. Thus, by Hanaki-Uno's theorem [HU06] there exists $k|(n-1)$ 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 $|\mathcal{P}_2| = (n-1)/k \geq s \geq \sqrt{2n/(\ell'-1)} + 1$. Thus, $k < \sqrt{n(\ell'-1)/2} = \sqrt{2n/(\ell'-1)} \cdot (\ell'-1)/2 \leq (s-1)(\ell'-1)/2$, implying $|\mathcal{P}_2| \geq s > 1 + \frac{2k}{\ell'-1}$. In particular, Π contains a matching by Theorem 3.5.3, 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 $V' := \{\alpha \in V \,|\, (\alpha_1, \alpha) \in P_0\}$. Furthermore, define an r-collection $\Pi' = \{\mathcal{P}'_1, \ldots, \mathcal{P}'_r\}$ on V' such that for all $1 \leq i \leq r$ and for each color $P \in \mathcal{P}_{i+1}$, we put a color $P' \in \mathcal{P}'_i$ such that

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

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 3.1.1. □

Naturally, one asks if there exist infinitely many primes n for which Theorem 4.4.1 is a significant improvement. A well-known number theory conjecture concerning primes in arithmetic progressions is connected to this question (Section 4.5). Under the conjecture that $L = 2$ is admissible for Linnik's constant [Lin44], we prove that there exist infinitely many primes n

for which the time complexity in Theorem 4.4.1 is polynomial. Even simply under GRH the factoring algorithm has an improved time complexity over the best known ones, for infinitely many n.

4.5 Connection to Linnik's Constant

Linnik's theorem in number theory answers a natural question about primes in arithmetic progressions. For coprime integers a, s such that $1 \leq a \leq s-1$, 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 [Xyl11]. It has been conjectured numerous times that $L \leq 2$ [SS58, Kan63, Kan64, HB92] as noted below.

Conjecture 4.5.1. *There exists $c > 0$ such that for all coprime integers a, s with $1 \leq a \leq s-1$, 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 best known under GRH is $p(a, s) < 2(s \log s)^2$ (see [BS96], Theorem 5.3). In the following corollary, we consider how the primes of the type described in Theorem 4.4.1 relate to $p(1, s)$.

Corollary 4.5.2 ([AIKS12])**.** *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 $\mathrm{poly}(\log q, n)$.

Proof. 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 [BS96], Theorem 5.3 there exists a prime $n = p(1, s) < 2(s \log s)^2$. Thus,

$$s > \sqrt{n/2}/\log s \geq (\sqrt{n/2}/\log n) + 1 = \sqrt{n/(2\log^2 n)} + 1.$$

It follows that we can generate infinitely many primes n such that Theorem 4.4.1 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 4.5.1. Let $r \in \mathbb{N}_{>1}$ be a constant and $s \in \mathbb{N}$ a (large enough) r-smooth number. By the conjecture there exists a prime $n = p(1, s) < cs^2$. Thus,

$$s > \sqrt{n/c} \geq \sqrt{n/(c+1)} + 1.$$

It follows that we can generate infinitely many primes n such that Theorem 4.4.1 applies for $\ell := (c + 1)$, and proves a time complexity of $\mathrm{poly}(\log q, n)$. □

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 [Evd94].

Naturally, one asks if it is possible to further relax the conditions which Theorem 4.4.1 places on the prime number n (i.e. the degree of the polynomial we want to factor). In our current framework, this translates to asking

to which extent we can relax the conditions for the existence of small intersection numbers in schemes of bounded valency and indistinguishing number (see Theorem 2.6.1). However, we saw in Section 2.6 from the example of the cyclotomic scheme that the conditions of Theorem 2.6.1 cannot be relaxed (up to constant factors). On the other hand, this does not rule out improvements of the following kind: If $\mathfrak{X} = (X, G)$ is an association scheme of prime order $p := |X|$ and we assume $|G| \approx k/\log k$, where $k \in \mathbb{N}$ is such that $k = n_g$ for all $1 \neq g \in G$, then there exist at least two constant-small intersection numbers in $\mathfrak{X}$ (note that in this case, the argument involving the Hasse-Weil bound from Section 2.6 produces too large an 'error' in order to restrict the intersection numbers). This would be enough to give an infinite family of primes n for which Theorem 4.4.1 has a polynomial time complexity (only assuming GRH).

Chapter 5

Extensibility of Association Schemes

In this chapter, we introduce the notion of extensibility of association schemes, a concept which was first defined in [AZ12]. An association scheme which is associated to a height t presuperscheme [Woj98, Woj01a, Woj01b] is said to be extensible to height t. Smith [Smi94, Smi07] showed that an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ is Schurian iff $\mathfrak{X}$ is extensible to height $(d-2)$. We formalize the maximal height $t_{\max}(\mathfrak{X})$ of an association scheme $\mathfrak{X}$ as the largest number $t \in \mathbb{N}$ such that $\mathfrak{X}$ is extensible to height t (we also include the possibility $t_{\max}(\mathfrak{X}) = \infty$, which is equivalent to $t_{\max}(\mathfrak{X}) \geq (d-2)$). Intuitively, the maximal height provides a natural measure of how close an association scheme is to being Schurian.

For the purpose of computing the maximal height, we introduce the association scheme extension algorithm. On input an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$, the association scheme extension algorithm decides in time $d^{O(t)}$ if the scheme $\mathfrak{X}$ is extensible to height t. In particular, if t is a fixed constant, then the

running time of the association scheme extension algorithm is polynomial in the order of $\mathfrak{X}$. The association scheme extension algorithm is used to show that all non-Schurian association schemes up to order 26 are completely inextensible, i.e. they are not extensible to any positive height $t \in \mathbb{N}_{>0}$.

Apart from its connection to the Schurity problem, the notion of extensibility of association schemes is deeply related to the IKS-framework for polynomial factoring over finite fields (see Chapter 4). In the language of m-schemes, the concept of extensibility formalizes the property that a homogeneous 3-scheme $\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ on a set V is part of a larger m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_m\}$ on V, where $m > 3$ (see Section 5.1). For the line of research started in [IKS09, AIKS12], it is of particular interest to gain a more thorough understanding of the combinatorial properties possessed by association schemes which are extensible to a certain height. The present chapter provides an algorithmic starting point for this discussion.

The material in this chapter is organized as follows. §5.1 introduces the notion of t-preschemes and defines the concept of extensibility of association schemes. In §5.2, we define adjacency tensors of t-preschemes and delineate in which sense they express a central combinatorial property of t-preschemes (see Theorem 5.2.3). In §5.3, we give a description of the association scheme extension algorithm. §5.4 lists the computational results obtained through the application of the algorithm.

5.1 Height t Presuperschemes

In this section, we introduce the notion of *height t presuperschemes* (short: *t-preschemes*), which may be regarded as a higher-dimensional analog of the notion of association schemes. In the following, let Q be a finite nonempty

set. For each $n \in \mathbb{N}_{>1}$, define a projection

$$\mathrm{pr}_n : Q^n \longrightarrow Q^{n-1}$$
$$(x_1, ..., x_{n-1}, x_n) \longrightarrow (x_1, ..., x_{n-1})$$

(the projection pr_n eliminates the last coordinate from tuples in Q^n). The inverse image of a set $C \subseteq Q^{n-1}$ under pr_n is denoted by $\mathrm{pr}_n^{-1}(C)$. Throughout this work, we omit the index n (we assume it is clear from context) and just write pr instead of pr_n. For each $n \in \mathbb{N}$, observe that the symmetric group on n elements Symm_n acts on the set of tuples Q^n by permuting the coordinates. For all $\bar{u} := (u_1, ..., u_n) \in Q^n$ and $\tau \in \mathrm{Symm}_n$, define

$$\bar{u}^\tau := (u_{\tau(1)}, ..., u_{\tau(n)}).$$

Furthermore, we fix the following convention:

$$\mathbb{N}_t := \{n \in \mathbb{N} \,|\, n \leq t\}, \quad \mathbb{N}_t^2 := \{(m, n) \in \mathbb{N}^2 \,|\, m + n \leq t\}.$$

The definition of height t presuperschemes given below is equivalent to the definition given by Wojdyło [Woj98, Woj01a, Woj01b].

Definition 5.1.1 (Height t Presuperscheme)**.** Let Q be a finite nonempty set and let $t \in \mathbb{N}$. A **height t presuperscheme** (Q, Γ^*) on Q is a family of sets $\{\Gamma^n\}_{n \in \mathbb{N}_t}$, where each set $\Gamma^n = \{C_1^n, ..., C_{s_n}^n\}$ is a partition of the direct power Q^{n+2} (note that all C_i^n are assumed to be nonempty), such that:

(P1) (Identity Relation) $C_1^0 := \{(x, x) \,|\, x \in Q\}$;

(P2) (Projection) $\forall n \in \mathbb{N}_t - \{0\}$, $\forall C_j^n \in \Gamma^n$,

$$\mathrm{pr}(C_j^n) := \{\mathrm{pr}(\bar{u}) \,|\, \bar{u} \in C_j^n\} \in \Gamma^{n-1};$$

(P3) (Invariance) $\forall n \in \mathbb{N}_t$, $\forall C_j^n \in \Gamma^n$, $\forall \tau \in \mathrm{Symm}_{n+2}$,

$$(C_j^n)^\tau := \{\bar{u}^\tau \,|\, \bar{u} \in C_j^n\} \in \Gamma^n;$$

(P4) (Intersection) $\forall (m,n) \in \mathbb{N}_t^2$, $\forall C_i^m \in \Gamma^m$, $\forall C_j^n \in \Gamma^n$, $\forall C_k^{m+n} \in \Gamma^{m+n}$, $\exists c(i,j,k;m,n) \in \mathbb{N}$. $\forall (x_0,...,x_m,y_0,...,y_n) \in C_k^{m+n}$,

$$\left|\{z \in Q \mid (x_0,...,x_m,z) \in C_i^m,\ (z,y_0,...,y_n) \in C_j^n\}\right| = c(i,j,k;m,n).$$

For brevity, we refer to height t presuperschemes simply as **t-preschemes**. We call the elements of Γ^n $(0 \leq n \leq t)$ the **relations at height** n. We refer to the numbers $c(i,j,k;m,n)$ as the **intersection numbers** of (Q,Γ^*).

Property (P2) interrelates the different layers $\{\Gamma^n\}_{n\in\mathbb{N}_t}$ of a t-prescheme, while Properties (P3), (P4) may be regarded as higher-dimensional analogs of Properties (A2), (A3) of association schemes, respectively (see Definition 2.1.1). From Definition 5.1.1 it is clear that a 0-prescheme and an association scheme constitute the exact same notion.

If (Q,Γ^*) is a t-prescheme, then (Q,Γ^0) is an association scheme. We say that the association scheme (Q,Γ^0) is **associated** to the t-prescheme (Q,Γ^*). If an association scheme $\mathfrak{X}$ is associated to a t-prescheme (Q,Γ^*), we call $\mathfrak{X}$ **extensible to height** t. In this case, we refer to the t-prescheme partitions $\{\Gamma^n\}_{1\leq n\leq t}$ as a **t-Extension** of $\mathfrak{X}$. Note that by definition, every association scheme is extensible to height 0.

We define the **maximal height** $t_{\max}(\mathfrak{X})$ of an association scheme $\mathfrak{X}$ as the largest number $t \in \mathbb{N}$ such that $\mathfrak{X}$ is extensible to height t. If $\mathfrak{X}$ is extensible to arbitrary heights (meaning that for all $t \in \mathbb{N}$, $\mathfrak{X}$ is extensible to height t), we say that $\mathfrak{X}$ has maximal height ∞. In case $t_{\max}(\mathfrak{X}) = 0$, we say that $\mathfrak{X}$ is **completely inextensible**.

For an association scheme $\mathfrak{X} = (Q,\Gamma)$ of order $d := |Q|$, it is easily proven that $t_{\max}(\mathfrak{X}) = \infty$ iff $\mathfrak{X}$ is extensible to height $(d-2)$. A fundamental result by Smith connects the concept of extensibility to the notion of Schurity of association schemes.

Theorem 5.1.2 (Smith [Smi94, Smi07])**.** *An association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ is Schurian iff $\mathfrak{X}$ is extensible to height $(d-2)$.*

Note that Theorem 5.1.2 may also be phrased as follows: An association scheme $\mathfrak{X}$ is Schurian iff $t_{\max}(\mathfrak{X}) = \infty$. Moreover, observe that if an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ is non-Schurian, then $0 \leq t_{\max}(\mathfrak{X}) < (d-2)$.

We end this section with a remark about the relationship of t-preschemes and m-schemes (the latter notion was introduced in Chapter 3). We saw in Section 3.2 that there exists a natural correspondence between homogeneous 3-schemes and association schemes (which we may regard as 0-preschemes). A simple extension of Lemmas 3.2.1 and 3.2.2 shows that more generally, homogeneous m-schemes (where $m \geq 3$) naturally correspond to preschemes of height $(m-3)$. Especially, the concept of extensibility can be phrased in m-scheme terminology as follows: An association scheme $\mathfrak{X}$ is said to be extensible to height t if the homogeneous 3-scheme corresponding to $\mathfrak{X}$ constitutes the first three levels of a $(t+3)$-scheme. As we will see in the following sections, the advantage of using the notion of preschemes is that certain scheme-theoretic properties can be phrased in a more algebraic and computational way in this framework.

In the same context, we also want to mention the following result, which is a variation of Theorem 5.1.2 (it is the m-scheme version of the theorem). We cite it here for completeness.

Theorem 5.1.3. *Every homogeneous $(n-1)$-scheme on n points is an orbit scheme.*

Proof. A simple comparison of definitions shows that every homogeneous $(n-1)$-scheme on n points can be regarded as a superscheme (in the sense

of [Smi07]). The assertion then follows from [Smi07], Th. 8.5. □

5.2 Adjacency Tensors

In this section, we introduce the notion of *adjacency tensors*. The concept of adjacency tensors of t-preschemes naturally generalizes the notion of adjacency matrices of association schemes (see Section 2.2). Analogously, adjacency tensors describe the intersection property of t-preschemes in simple algebraic terms (see Theorem 5.2.3). Note that we apply the concept of adjacency tensors in Section 5.3, when we describe the association scheme extension algorithm.

As a first step, we introduce *tensors of order k* (short: *k-tensors*) and discuss certain natural operations associated with this notion. Note that k-tensors constitute a natural generalization of the concept of square matrices.

Definition 5.2.1 (k-Tensor)**.** For $k \geq 2$, a **k-tensor** with entries in $\mathbb{Z}$ is a function

$$T : \{1, ..., d\}^k \longrightarrow \mathbb{Z}.$$

We refer to the number k as the order of the tensor T. We denote by $T_{i_1 \cdots i_k}$ the image of $(i_1, ..., i_k)$ under T. We call $T_{i_1 \cdots i_k}$ the $(i_1, ..., i_k)$-*entry* of T.

Throughout this work, tensors are regarded simply as multidimensional arrays. For $k = 2$, the notion of k-tensors with entries in $\mathbb{Z}$ coincides with the notion of $d \times d$ matrices with entries in $\mathbb{Z}$. For a more general (algebraic) treatment of tensors, the reader is referred to [CL03, Dim02].

In the following, we define some basic operations for k-tensors. These operations naturally generalize the standard matrix operations from linear algebra. For two k-tensors $S, T : \{1, ..., d\}^k \longrightarrow \mathbb{Z}$, we define their **sum**

$U = S + T$ as the k-tensor $U : \{1, ..., d\}^k \longrightarrow \mathbb{Z}$ with entries

$$U_{i_1 \cdots i_k} = S_{i_1 \cdots i_k} + T_{i_1 \cdots i_k}.$$

For an element $c \in \mathbb{Z}$ and a k-tensor $S : \{1, ..., d\}^k \longrightarrow \mathbb{Z}$, we define their **scalar product** $V = c \cdot S$ as the k-tensor $V : \{1, ..., d\}^k \longrightarrow \mathbb{Z}$ with entries

$$V_{i_1 \cdots i_k} = c \cdot S_{i_1 \cdots i_k}.$$

For a m-tensor $E : \{1, ..., d\}^m \longrightarrow \mathbb{Z}$ and a n-tensor $F : \{1, ..., d\}^n \longrightarrow \mathbb{Z}$, we define their **inner product** $W = EF$ as the order $(m + n - 2)$ tensor $W : \{1, ..., d\}^{(m+n-2)} \longrightarrow \mathbb{Z}$ with entries

$$W_{i_1 \cdots i_{m+n-2}} = \sum_{j=1}^{d} E_{i_1 \cdots i_{m-1} j} \cdot F_{j i_m \cdots i_{m+n-2}}.$$

The above operations generalize the standard addition, scalar multiplication and inner multiplication of matrices. It is easily verified that addition and inner multiplication of tensors are associative, distributive and compatible with scalar multiplication.

Next, we define the notion of adjacency tensors, boolean tensors which indicate membership to subsets of direct powers of $Q := \{1, ..., d\}$.

Definition 5.2.2 (Adjacency Tensor)**.** Let $Q := \{1, ..., d\}$ and let $C \subseteq Q^n$, where $n \geq 2$. We define the **adjacency tensor** corresponding to the subset C as the n-tensor $A(C) : \{1, ..., d\}^n \longrightarrow \mathbb{Z}$ such that the entry $[A(C)]_{x_1 \cdots x_n}$ is 1 if $(x_1, ..., x_n) \in C$ and 0 otherwise.

Let (Q, Γ^*) be a t-prescheme on $Q := \{1, ..., d\}$. We denote the **adjacency tensor of a relation** $C_i^m \in \Gamma^m$ $(m \in \mathbb{N}_t)$ as the $(m + 2)$-tensor $A_i^m : \{1, ..., d\}^{m+2} \longrightarrow \mathbb{Z}$, where $(A_i^m)_{x_1 \cdots x_{m+2}}$ is 1 if $(x_1, ..., x_{m+2}) \in C_i^m$ and 0 otherwise. Adjacency tensors can be used to express the intersection property of t-preschemes in algebraic terms (analogously to adjacency matrices in the case of association schemes, see [BI84, Zie05]).

Theorem 5.2.3 ([AZ12]). *Let (Q, Γ^*) be a t-prescheme on $Q := \{1, ..., d\}$. Then for all $(m, n) \in \mathbb{N}_t^2$, $C_i^m \in \Gamma^m$ and $C_j^n \in \Gamma^n$, it holds that*

$$A_i^m A_j^n = \sum_{k=1}^{s_{m+n}} c(i, j, k; m, n) A_k^{m+n},$$

where A_i^m, A_j^n and A_k^{m+n} denote the adjacency tensors of C_i^m, C_j^n and $C_k^{m+n} \in \Gamma^{m+n}$, respectively, and $c(i, j, k; m, n) \in \mathbb{N}$ denote the intersection numbers. Furthermore, the above statement is equivalent to the intersection property of t-preschemes (see Definition 5.1.1 (P4)).

Proof. Recall the intersection property of t-preschemes: For all $(m, n) \in \mathbb{N}_t^2$, $C_i^m \in \Gamma^m$, $C_j^n \in \Gamma^n$, $C_k^{m+n} \in \Gamma^{m+n}$ and $(x_0, ..., x_m, y_0, ..., y_m) \in C_k^{m+n}$, it holds that

$$c(i, j, k; m, n) = \left| \{ z \in Q \mid (x_0, ..., x_m, z) \in C_i^m,\ (z, y_0, ..., y_m) \in C_j^n \} \right|.$$

Note that the above equation can also be written as

$$c(i, j, k; m, n) = \sum_{z=1}^{d} (A_i^m)_{x_0 \cdots x_m z} \left(A_j^n \right)_{z y_0 \cdots y_m}$$

where the right-hand side is $\left(A_i^m A_j^n \right)_{x_0 \cdots x_m y_0 \cdots y_m}$ by the definition of the inner product of tensors. From this the assertion follows immediately. □

5.3 The Association Scheme Extension Algorithm

In this section, we describe the *association scheme extension algorithm* [AZ12]. On input an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d - 2)$, the association scheme extension algorithm decides in time $d^{O(t)}$ if $\mathfrak{X}$ is extensible to height t. Furthermore, if

$\mathfrak{X}$ is extensible to height t, then the algorithm outputs its unique coarsest t-extension $\mathfrak{X}_t$, which represents the most 'basic' way in which $\mathfrak{X}$ can be extended to a t-prescheme. We apply the association scheme extension algorithm to determine that all non-Schurian association schemes up to order 26 are completely inextensible (see Theorem 5.4.1). Via the tensor product of association schemes, the latter result gives rise to a multitude of infinite families of completely inextensible association schemes (see Section 5.4).

Description of the Algorithm

We now describe the association scheme extension algorithm. On input an association scheme $\mathfrak{X} = (Q, \Gamma)$ on $Q := \{1, ..., d\}$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$, the algorithm begins with trivial partitions $\Gamma^s := \{Q^{s+2}\}$ $(1 \leq s \leq t)$ and then gradually refines these partitions according to a set of rules derived from the properties of t-extensions (see Definition 5.1.1). Via this refinement process, the partitions Γ^s $(1 \leq s \leq t)$ either turn into a t-extension of $\mathfrak{X}$, or they provide combinatorial justification for the conclusion that $\mathfrak{X}$ cannot be extended to height t.

Input: An association scheme $\mathfrak{X} = (Q, \Gamma)$ on $Q := \{1, ..., d\}$, and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$.

Output: A t-extension $\{\Gamma^s\}_{1 \leq s \leq t}$ of $\mathfrak{X}$, or the decision that $\mathfrak{X}$ is not extensible to height t.

Initialization. For each $1 \leq s \leq t$, let $\Gamma^s := \{Q^{s+2}\}$ be the trivial partition of Q^{s+2}.

Step 1. For each $1 \leq s \leq t$, refine the partition Γ^s of Q^{s+2} according to the projection property of t-preschemes (see Definition 5.1.1 *(P2)*). That is, for each $C \in \Gamma^s$, determine if the set $\mathrm{pr}(C)$ can be written as a union of relations

in Γ^{s-1}, i.e. if

$$\mathrm{pr}(C) = C_{i_1}^{s-1} \cup \cdots \cup C_{i_k}^{s-1}$$

for some $C_{i_1}^{s-1}, ..., C_{i_k}^{s-1} \in \Gamma^{s-1}$.

If YES. Replace in Γ^s the set $C \in \Gamma^s$ with the pairwise disjoint sets

$$C \cap \mathrm{pr}^{-1}(C_{i_1}^{s-1}), ..., C \cap \mathrm{pr}^{-1}(C_{i_k}^{s-1}).$$

ELSE. Distinguish between the following two cases:

(a) If $s > 1$. Replace in Γ^{s-1} each set $C' \in \Gamma^{s-1}$ such that $C' \cap \mathrm{pr}(C) \neq \emptyset$ with the two disjoint sets $C' \cap \mathrm{pr}(C)$ and $C' \setminus \mathrm{pr}(C)$.

(b) If $s = 1$. Terminate the algorithm and output: $\mathfrak{X}$ *is not extensible to height* t.

Step 2. For each $1 \leq s \leq t$, refine the partition Γ^s of Q^{s+2} according to the invariance property of t-preschemes (see Definition 5.1.1 *(P3)*). That is, for each $C \in \Gamma^s$ and each $\tau \in Symm_{s+2}$, replace in Γ^s each set $C' \in \Gamma^s$ such that $C' \cap C^\tau \neq \emptyset$ with the two disjoint sets $C' \cap C^\tau$ and $C' \setminus C^\tau$.

Step 3. For each $1 \leq s \leq t$, refine the partition Γ^s of Q^{s+2} according to the intersection property of t-preschemes (see Theorem 5.2.3). That is, for each $m, n \in \mathbb{N}$ such that $s = (m + n)$, and each pair of sets $C_i^m \in \Gamma^m$ and $C_j^n \in \Gamma^n$, compute the inner product

$$P := A_i^m A_j^n,$$

where A_i^m, A_j^n denote the adjacency tensors of C_i^m, C_j^n, respectively (see Section 5.2). The entries of P are integers in the range from 0 to d. For each $r = 0, ..., d$ define

$$P^{-1}(r) := \{(i_1, ..., i_{s+2}) \in Q^{s+2} \mid P_{i_1 \cdots i_{s+2}} = r\}$$

and replace in Γ^s each set $C \in \Gamma^s$ such that $C \cap (P^{-1}(r)) \neq \emptyset$ with the two disjoint sets $C \cap (P^{-1}(r))$ and $C \setminus (P^{-1}(r))$.

Repeat Steps 1-3. If none of them yields any further refinement of the partitions Γ^s $(1 \leq s \leq t)$, then terminate the algorithm and output $\{\Gamma^s\}_{1 \leq s \leq t}$. □

Correctness of the Algorithm

We now prove the correctness of the association scheme extension algorithm. We need the following preliminary lemma.

Lemma 5.3.1 ([AZ12])**.** *Let $\mathfrak{X} = (Q, \Gamma)$ be an association scheme on the set $Q := \{1, ..., d\}$ and let $t \in \mathbb{N}$ be such that $1 \leq t \leq (d-2)$. The following holds:*

(1) On input $\mathfrak{X}$ and t, the association scheme extension algorithm terminates after at most $d^{O(t)}$ steps.

(2) On input $\mathfrak{X}$ and t, if the association scheme extension algorithm outputs a set of partitions $\{\Gamma^s\}_{1 \leq s \leq t}$, then these partitions constitute a t-extension of $\mathfrak{X}$.

Proof. (1) Note that the algorithm can make at most $(d^3 + ... + d^{t+2})$ refinements to the partitions $\{\Gamma^s\}_{1 \leq s \leq t}$ before it must terminate. Moreover, observe that the algorithm goes through at most $d^{O(t)}$ elementary operations in between two refinements. From this the assertion follows directly.

(2) Note that the algorithm outputs a set of partitions $\{\Gamma^s\}_{1 \leq s \leq t}$ only if Steps 1-3 of the algorithm do not yield any further refinement of $\{\Gamma^s\}_{1 \leq s \leq t}$. The latter condition implies that Definition 5.1.1 *(P2)-(P4)* hold for $\mathfrak{X}$ and $\{\Gamma^s\}_{1 \leq s \leq t}$ (see Theorem 5.2.3). This in turn implies that the partitions $\{\Gamma^s\}_{1 \leq s \leq t}$ constitute a t-extension of $\mathfrak{X}$. □

Let us fix some terminology. Let X be a finite, nonempty set and let $\mathcal{P}, \mathcal{R}$ be partitions of X. If for each $P \in \mathcal{P}$ there exist sets $R_1, ..., R_n \in \mathcal{R}$ such that $P = \cup_{i=1}^{n} R_i$, then we call $\mathcal{P}$ a **fusion** of $\mathcal{R}$. We use this convention in the proof of correctness of the association scheme extension algorithm given below.

Theorem 5.3.2 ([AZ12])**.** *The association scheme extension algorithm works correctly, and its running time is* $d^{O(t)}$.

Proof. Let $\mathfrak{X} = (Q, \Gamma)$ be an association scheme on $Q := \{1, ..., d\}$ and let $t \in \mathbb{N}$ be such that $1 \leq t \leq (d-2)$. First, assume $\mathfrak{X}$ is not extensible to height t. Then by Lemma 5.3.1 (1), (2) it follows that on input $\mathfrak{X}$ and t, the algorithm correctly outputs the decision that $\mathfrak{X}$ is not extensible to height t, in time $d^{O(t)}$.

Now consider the converse: Assume we are given as input an association scheme $\mathfrak{X} = (Q, \Gamma)$ on $Q := \{1, ..., d\}$ and a number $t \in \mathbb{N}$ with $1 \leq t \leq (d-2)$ such that $\mathfrak{X}$ is extensible to height t. Choose an arbitrary t-extension $\{\tilde{\Gamma}^s\}_{1 \leq s \leq t}$ of $\mathfrak{X}$. Observe the following facts about the partitions $\{\Gamma^s\}_{1 \leq s \leq t}$ which appear in the algorithm:

(i) For each $1 \leq s \leq t$, the partition Γ^s is trivially a fusion of $\tilde{\Gamma}^s$ at the initialization step.

(ii) For each $1 \leq s \leq t$, the partition Γ^s remains a fusion of $\tilde{\Gamma}^s$ over the whole course of the algorithm (this follows from Properties *(P2), (P3), (P4)* of Definition 5.1.1 applied on $\mathfrak{X}$ and $\{\tilde{\Gamma}^s\}_{1 \leq s \leq t}$). Especially, the algorithm never terminates during the execution of Step 1.

From statement (ii) and Lemma 5.3.1 (1) we conclude that on input $\mathfrak{X}$ and t, the algorithm outputs a set of partitions $\{\Gamma^s\}_{1 \leq s \leq t}$. Consequently, by Lemma 5.3.1 (2), the output $\{\Gamma^s\}_{1 \leq s \leq t}$ constitutes a t-extension of $\mathfrak{X}$. □

Recall that in the proof of Theorem 5.3.2, the t-extension $\{\tilde{\Gamma}^s\}_{1\leq s\leq t}$ of $\mathfrak{X}$ was chosen arbitrarily. Hence we obtain the following corollary.

Corollary 5.3.3 ([AZ12]). *On input an association scheme $\mathfrak{X} = (Q, \Gamma)$ and a number $t \in \mathbb{N}$ with $1 \leq t \leq (d-2)$ such that $\mathfrak{X}$ is extensible to height t, the association scheme extension algorithm outputs the* ***unique coarsest t-extension*** *$\mathfrak{X}_t := \{\Gamma^s\}_{1\leq s\leq t}$ of $\mathfrak{X}$. That is, for any t-extension $\{\tilde{\Gamma}^s\}_{1\leq s\leq t}$ of $\mathfrak{X}$, for each $1 \leq s \leq t$, the partition Γ^s is a fusion of $\tilde{\Gamma}^s$.*

5.4 Computational Results

In this section, we discuss computational results obtained through the application of the association scheme extension algorithm. More precisely, we determine the extensibility properties of all non-Schurian association schemes up to order 26. Note that there are exactly 142 non-Schurian schemes of order less or equal to 26 (see [HM98a, HM98b, HM03, HM09]).

Theorem 5.4.1 ([Aro12], [AZ12]). *All non-Schurian association schemes $\mathfrak{X} = (Q, \Gamma)$ of order $|Q| \leq 26$ are completely inextensible.*

Proof. We created a program of the association scheme extension algorithm with fixed parameter $t = 1$ in the input, written in "C". We applied our program to all non-Schurian association schemes of order less or equal to 26; for this we relied on the classification of non-Schurian association schemes of small order by Hanaki and Miyamoto [HM98a, HM98b, HM03, HM09]. The reader can download an organized version of the C-programs and their output online [Aro12]. □

Let us fix some convention. For an association scheme $\mathfrak{X} = (Q, \Gamma)$, we denote the equivalence relation on $Q \times Q$ corresponding to the partition Γ

by $\equiv_\Gamma$. Recall the definition of the **tensor product** of association schemes. For two association schemes $\mathfrak{X}_1 = (Q_1, \Gamma_1)$ and $\mathfrak{X}_2 = (Q_2, \Gamma_2)$, the tensor product $\mathfrak{X}_1 \otimes \mathfrak{X}_2$ is defined as the association scheme $(Q_1 \times Q_2, \Gamma_1 \otimes \Gamma_2)$ such that for all $x_1, x_1', y_1, y_1' \in Q_1$ and $x_2, x_2', y_2, y_2' \in Q_2$,

$$\begin{aligned}&((x_1, x_2), (x_1', x_2')) \equiv_{\Gamma_1 \otimes \Gamma_2} ((y_1, y_2), (y_1', y_2'))\\ \Longleftrightarrow &(x_1, x_1') \equiv_{\Gamma_1} (y_1, y_1') \text{ and } (x_2, x_2') \equiv_{\Gamma_2} (y_2, y_2').\end{aligned}$$

Given a number $t \in \mathbb{N}$, it is easily seen that the tensor product $\mathfrak{X}_1 \otimes \mathfrak{X}_2$ is extensible to height t iff both $\mathfrak{X}_1$ and $\mathfrak{X}_2$ are extensible to height t. Via the above construction, Theorem 5.4.1 gives rise to a multitude of examples of infinite families of completely inextensible association schemes. Especially, we have the following corollary.

Corollary 5.4.2 ([AZ12])**.** *There exist infinitely many completely inextensible association schemes.*

Chapter 6

Efficient Matrix Multiplication using Association Schemes

The topic of this chapter is a new approach, suggested by Cohn and Umans [CU03, CU12], to efficient matrix multiplication, i.e. the problem of minimizing the number of arithmetic operations necessary to multiply two matrices with entries in some field k. We outline here why the problem is considered to be central in computational algebra and theoretical computer science as a whole, describe some of the past breakthroughs in obtaining upper bounds on the exponent of matrix multiplication ω, and delineate in detail the Cohn-Umans *algebra embedding* approach and the progress it has made towards the famous open conjecture $\omega = 2$. In addition, we describe how association schemes and their adjacency algebras pertain to the Cohn-Umans fast matrix multiplication framework, and delineate in which way they could help to improve the state of efficient matrix multiplication.

We remark that the main intention of this chapter is to give an exposition of the Cohn-Umans approach, delineating a further application of combinatorial schemes to computational complexity. We will not provide a full

introduction to the subject of fast matrix multiplication - for this purpose, the reader is referred to the classical introductory text [BCS97].

6.1 The Exponent of Matrix Multiplication

We consider the problem of multiplying two $n \times n$ matrices $A, B \in k^{n \times n}$ with entries in some field k, i.e. computing the product

$$(AB)_{ik} = \sum_{j=1}^{n} A_{ij} B_{jk}. \tag{6.1.1}$$

Matrix multiplication is one of the most fundamental problems in algebraic complexity, with hosts of applications to various algorithms used by mathematicians, computer scientists, physicists and engineers today. We are interested in the algorithmic complexity of matrix multiplication – more specifically, in answering the following question: What is the minimum value $\omega(k) \in [2, 3]$ such that the product of two $n \times n$ matrices over the field k can be computed using less than $n^{\omega(k)+o(1)}$ arithmetic operations? Note here that the lower bound $\omega(k) \geq 2$ follows because each entry of the $n \times n$ matrices to be multiplied must be considered at least once, and the upper bound $\omega(k) \leq 3$ is obtained from the complexity of the naive method of computation computation of the matrix product (plainly following Equation (6.1.1) - which takes $O(n^3)$ arithmetic operations). The quantity $\omega(k)$ is often referred to as the **exponent of matrix multiplication**, possibly depending on the underlying field k (although $\omega(k)$ depends, if at all, on the characteristic of k, since $\omega(.)$ is invariant under field extensions [Sch81]). In the following, we just write ω instead of $\omega(k)$, as the methods mentioned here are not exclusive to any specific characteristic.

It is well-known that the exponent of matrix multiplication ω measures the asymptotic complexity of several central computational problems besides

matrix multiplication. For example, the problem of computing the determinant, the characteristic polynomial and the inverse of an $n \times n$ matrix each have asymptotic complexity $n^{\omega+o(1)}$ (see [BCS97], Ch. 16 for an exposition of problems whose complexity depends on ω). In particular, the complexity of any algorithm which depends on the multiplication, determinant, characteristic polynomial or inversion of 'large' rectangular matrices benefits from improvements on the upper bound of ω. This may shed additional light on why determining the exact value of ω is considered to be one of the most important open problems in algebraic complexity.

In the following, we give a brief summary of the history of upper bounds obtained on the exponent ω. The first nontrivial upper bound on ω was achieved by Strassen [Str69], who showed $\omega < 2.81$; a result which essentially started the field of efficient matrix multiplication. Among the most important milestones since Strassen, one has to count the work of Bini *et al.* [BCRL79] and Bini [Bin80], who obtained the upper bound $\omega < 2.78$ by introducing the notion of *border rank* of tensors. Another milestone was achieved by Schönhage [Sch81], who used his *asymptotic sum inequality* (which relates ω to the border rank of direct sums of independent matrix multiplication tensors) to obtain $\omega < 2.55$. Further milestone improvements came - once again - from Strassen [Str87], who introduced the *laser method*, by which he obtained $\omega < 2.48$, and Coppersmith and Winograd [CW87], who extended the laser method and achieved $\omega < 2.376$. By pushing Coppersmith and Winograd's ideas a little further, Stothers [Sto11] obtained $\omega < 2.374$ and Vassilevska Williams [VW12] obtained $\omega < 2.373$, which is currently the best known. (For a more detailed history from Strassen (1969) to Coppersmith-Winograd (1987), see [BCS97], §15.13). Nowadays, it is a widely believed conjecture among complexity theorists that $\omega = 2$. The correctness of this

conjecture would imply that asymptotically, multiplying two $n \times n$ matrices does not require much more computational effort than simply looking at each of the matrices' components once.

6.2 The Cohn-Umans Approach

The Cohn-Umans *algebra embedding* approach [CU03, CU12] subsumes many of the earlier works on efficient matrix multiplication. It provides an algebraic-combinatorial framework in which properties of certain algebras correspond to upper bounds on the matrix multiplication exponent ω. In the following, we assume some familiarity with tensorial notation (see [BCS97] for an introduction to tensors). We adopt the standard convention of representing tensors as multilinear forms.

Let k be a field. Recall that the **matrix multiplication tensor** $\langle \ell, m, n \rangle$ is the tensor $\sum_{i=1}^{\ell} \sum_{j=1}^{m} \sum_{k=1}^{n} \hat{x}_{ij} \hat{y}_{jk} \hat{z}_{ki}$, where $\hat{x}_{ij}, \hat{y}_{jk}, \hat{z}_{ki}$ are formal variables. The tensor $\langle \ell, m, n \rangle$ naturally corresponds to the matrix multiplication $k^{\ell \times m} \times k^{m \times n} \longrightarrow k^{\ell \times n}$ (see [BCS97], Prop. 14.15). It is a well-known fact that

$$\omega = \inf\{\tau \in \mathbb{R} \mid R(\langle n, n, n \rangle) = O(n^{\tau})\}, \tag{6.2.1}$$

where $R(.)$ is the **tensor rank** (see [BCS97], §15.1). Recall that the **support** $\mathrm{supp}(T)$ of a tensor T is the set of monomials that have nonzero coefficients (in the case of $\langle \ell, m, n \rangle$, these are exactly the monomials of the form $\hat{x}_{ij} \hat{y}_{jk} \hat{z}_{ki}$). Cohn and Umans [CU12] define the ***s*-rank** $R_s(T)$ of a tensor T as the minimum rank of a tensor T' for which $\mathrm{supp}(T) = \mathrm{supp}(T')$. Moreover, they define the notion of ***s*-rank exponent of matrix multiplication**

$$\omega_s := \inf\{\tau \in \mathbb{R} \mid R_s(\langle n, n, n \rangle) = O(n^{\tau})\}. \tag{6.2.2}$$

It is easily seen that $2 \leq \omega_s \leq \omega$. Moreover, it can be proven that $\omega_s \leq 2 + \epsilon \Rightarrow \omega \leq 2 + \frac{3}{2}\epsilon$ (see [CU12], Th. 3.6), which means $\omega_s = 2$ implies $\omega = 2$; a crucial observation. Furthermore, it was shown in [CU12], Prop. 3.5 that

$$(\ell mn)^{\omega_s/3} \leq R_s(\langle \ell, m, n \rangle). \tag{6.2.3}$$

Following the work [CU12], we define next what it means for an r-dimensional complex algebra A to realize a matrix multiplication tensor $\langle \ell, m, n \rangle$. Let $U := \{u_1, ..., u_r\}$ be a basis of A and let $(\lambda_{ijk})_{i,j,k}$ denote the **structure constants** defined by $u_i u_j = \sum_k \lambda_{ijk} u_k$. We say that A **realizes** $\langle \ell, m, n \rangle$ if there exist three injective functions

$$\alpha : [\ell] \times [m] \longrightarrow [r], \quad \beta : [m] \times [n] \longrightarrow [r], \quad \gamma : [n] \times [\ell] \longrightarrow [r]$$

such that $\lambda_{\alpha(a,b'),\beta(b,c'),\gamma(c,a')} \neq 0$ iff $a = a'$, $b = b'$ and $c = c'$. For group algebras $A = \mathbb{C}G$, where G is a group, the property that A realizes $\langle \ell, m, n \rangle$ naturally leads to the notion of the *triple product property* of groups [ASU12, CKSU05, CU03]. The above-mentioned works constitute a line of research in which certain properties of groups satisfying the triple product property are related to upper bounds on ω. Using this group-theoretic framework, one can show the upper bound $\omega < 2.41$ [CKSU05], not far from the best known $\omega < 2.373$ [VW12]. Furthermore, the works [ASU12, CKSU05, CU03] give a discussion of group-theoretic and combinatorial conjectures which would imply $\omega = 2$. In the following, we delineate the more general approach of [CU12], in which the aforementioned conjectures appear as a special case of a universal conjecture for $\omega = 2$.

As before, assume that A is an r-dimensional complex algebra. Let $U := \{u_1, ..., u_r\}$, $V := \{v_1, ..., v_r\}$ and $W := \{w_1, ..., w_r\}$ be any three bases of A and let $(c_{ijk})_{i,j,k}$ be the coefficients defined by $u_i v_j = \sum_k c_{ijk} w_k$. We

call

$$T_A := \sum_{i,j,k} c_{ijk} \hat{x}_i \hat{y}_j \hat{z}_k$$

the **structural tensor of A with respect to the bases** U, V, W, or simply the *structural tensor of* A (since different choices of bases U, V, W all yield isomorphic structural tensors). If A realizes $\langle \ell, m, n \rangle$, then it holds that $R_s(\langle \ell, m, n \rangle) \leq R(T_A)$ (see [CU12], Prop. 4.2). Moreover, if A is semisimple, then there exist $d_1, ..., d_t \in \mathbb{N}$ such that $A \cong \mathbb{C}^{d_1 \times d_1} \times \cdots \times \mathbb{C}^{d_t \times d_t}$, in which case $T_A \cong \langle d_1, d_1, d_1 \rangle \oplus \cdots \oplus \langle d_t, d_t, d_t \rangle$. If additionally we assume A to be commutative, then $d_i = 1$ for all $1 \leq i \leq t$ and hence $R(T_A) = r$. Thus, we obtain the following theorem:

Theorem 6.2.1 ([CU12])**.** *If A is an r-dimensional, semisimple and commutative complex algebra which realizes $\langle \ell, m, n \rangle$, then $R_s(\langle \ell, m, n \rangle) \leq r$.*

The above theorem gives reason to hope that 'suitable' semisimple and commutative complex algebras may be helpful in obtaining nontrivial upper bounds on $R_s(\langle \ell, m, n \rangle)$ (which in turn may translate to nontrivial upper bounds on ω_s by Equation (6.2.3)). This intuition will be made precise in the following.

6.3 Connection to Association Schemes

As a promising class of commutative algebras to realize matrix multiplication tensors and obtain upper bounds on ω_s, Cohn and Umans [CU12] identify adjacency algebras of commutative association schemes (note that their paper actually uses the term *commutative coherent configurations*, which is synonymous). Efficient matrix multiplication constitutes yet another important computational problem to which the theory of association schemes is closely

related - for problems such as polynomial factoring over finite fields [AIKS12, Evd94, IKS09] and graph isomorphism [CFI92, EKP99, Wei76, WL68], the connection to combinatorial schemes has been known for a long time.

In the following, let $\mathfrak{X} = (X, G)$ be an association scheme and let $\mathbb{C}\mathfrak{X}$ denote the complex adjacency algebra of $\mathfrak{X}$ (see Chapter 2). Note that the structure constants of the algebra $\mathbb{C}\mathfrak{X}$ with respect to the basis consisting of the adjacency matrices of $\mathfrak{X}$ are simply the intersection numbers of the association scheme $\mathfrak{X}$. Moreover, note that the adjacency algebra $\mathbb{C}\mathfrak{X}$ is semisimple (see Theorem 2.2.2), and it is commutative iff the association scheme (X, G) is commutative. Finally, observe that the rank of $\mathbb{C}\mathfrak{X}$ equals $|G|$.

It is essential to discern the structural conditions placed on association schemes in order for their adjacency algebra to realize a matrix multiplication tensor $\langle \ell, m, n \rangle$. Cohn and Umans [CU12] have started this discussion by introducing the following notion: An association scheme $\mathfrak{X} = (X, G)$ of rank r is said to **realize** $\langle \ell, m, n \rangle$ if there exist three injective functions

$$\alpha : [\ell] \times [m] \longrightarrow [r], \quad \beta : [m] \times [n] \longrightarrow [r], \quad \gamma : [n] \times [\ell] \longrightarrow [r]$$

such that the intersection number $\lambda_{\alpha(a,b'),\beta(b,c'),\gamma(c,a')}$ is nonzero iff $a = a'$, $b = b'$ and $c = c'$. Clearly, if an association scheme $\mathfrak{X} = (X, G)$ realizes $\langle \ell, m, n \rangle$, then $\mathbb{C}\mathfrak{X}$ realizes $\langle \ell, m, n \rangle$ as an algebra. Exemplary, Cohn and Umans describe the condition which Schurian association schemes must satisfy in order to realize a matrix multiplication tensor $\langle \ell, m, n \rangle$ (see [CU12], Prop. 4.7); we omit the details of this special case here.

As one would hope, applying the Cohn-Umans algebra embedding approach from Section 6.2 to adjacency algebras of 'suitable' commutative association schemes yields bounds on the s-rank exponent of matrix multiplication ω_s. In [CU12], Theorem 5.6 we find commutative association schemes

$\mathfrak{X} = (X, G)$ which - via the adjacency algebra $\mathbb{C}\mathfrak{X}$ - prove the s-rank exponent bounds $\omega_s \leq 2.48$, $\omega_s \leq 2.41$, and $\omega_s \leq 2.376$, respectively. (Note that it is no coincidence that the upper bound $\omega_s \leq 2.376$ equals the upper bound on ω obtained by Coppersmith-Winograd [CW87] - it is due to a construction of the latter work being transferred into the Cohn-Umans [CU12] framework). Moreover, the approach described by Cohn-Umans [CU12] naturally leads to the following conjecture for proving $\omega_s = 2$ (and hence $\omega = 2$):

Conjecture 6.3.1 ([CU12])**.** *There exist commutative association schemes* $\mathfrak{X}_n = (X_n, G_n)$ *realizing* $\langle n, n, n\rangle$ *and of rank* $|G_n| = n^{2+o(1)}$.

Notably, the latter conjecture subsumes all of the earlier conjectures for $\omega = 2$ of the 'group-algebra embedding' approach [ASU12, CKSU05, CU03] (for an explanation of this fact, the reader is referred to [CU12], §5). Principally, this makes the above conjecture the 'easiest' among all conjectures associated with the Cohn-Umans approach for proving $\omega = 2$.

Chapter 7

Conclusion

In Chapter 4, we studied the computational problem of polynomial factoring over finite fields (assuming GRH). Our approach was based on algebraic-combinatorial techniques introduced in Chapters 2 and Chapters 3. These techniques proved to be very effective when the polynomial has a prime degree (Theorem 4.4.1). We were able to give an infinite family of prime degrees for which our analysis is much better than the known techniques (Corollary 4.5.2). It is a central open problem to extend the methods described in this work to factor all prime degree polynomials efficiently. The key to this problem lies in studying the underlying m-scheme that the factoring algorithm gets 'stuck' with. Its 3-subscheme has a convenient structure - it is an equivalenced association scheme. Since the intersection numbers, and other deeper representation theory invariants, manifest in the higher levels of the m-scheme, the schemes conjecture (Section 3.5) might be within reach.

Another open problem is to 'slightly' improve Corollary 2.6.2. We showed that it cannot be improved to an arbitrary extent (Section 2.6), but this does not rule *small* improvements of the following kind: There exist at least two constant-small intersection numbers in prime-order association schemes

$\mathfrak{X} = (X, G)$ which satisfy $|G| \approx k/\log k$, where $k \in \mathbb{N}$ is such that $k = n_g$ for all $1 \neq g \in G$. As we remarked before, the possibility for this improvement arises because the argument involving the Hasse-Weil bound from Section 2.6 produces too large an 'error' in order to restrict the intersection numbers in this case. Note that an improvement of the above kind would be enough to give an infinite family of primes n so that Theorem 4.4.1 has a polynomial time complexity (only assuming GRH).

It is also open to extend Theorem 2.6.1, so that it becomes applicable to composite-order association schemes. Improvements there would likely translate to new results in the domain of polynomial factoring, especially concerning the factorization of additional classes of composite-degree polynomials. This question connects to a more general open problem: We proved in Theorem 3.6.3 that a homogeneous, antisymmetric m-scheme on n points always contains a matching if $m \geq 0.559 \log_2 n + 2$, beating the previously best known bound $m \geq \frac{2}{3}n$. In generalizing the (purely combinatorial) methods of Section 3.6, the bound $m = o(\log n)$ for the existence of matchings in homogeneous and antisymmetric m-schemes on n points seems approachable. The latter result would already translate to an improved time complexity for the general case of polynomial factoring over finite fields (assuming GRH).

In Chapter 5, we introduced the notion of extensibility of association schemes. We defined for an association scheme $\mathfrak{X} = (X, G)$ the notion of the maximal height $t_{\max}(\mathfrak{X})$ and - assuming that $\mathfrak{X}$ is extensible to height t - the concept of the unique coarsest t-extension $\mathfrak{X}_t$. We delineated in which sense the maximal height may be regarded as an intuitive measure of how close an association scheme is to being Schurian. Moreover, we saw that the concept of extensibility - phrased in the language of m-schemes - can also be used to formalize the property that a homogeneous 3-scheme $\{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ on

a set V is part of a larger m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_m\}$ on V, where $m > 3$. The latter observation connects the notion of extensibility to the topic of m-schemes and the IKS polynomial factoring framework (Chapters 3 and 4). For the IKS-framework, it is of particular interest to gain a more thorough understanding of the combinatorial properties possessed by association schemes which are extensible to a certain height. The present work provided an algorithmic starting point for this discussion.

In Section 5.3, we described the association scheme extension algorithm, which on input an association scheme $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$ and a number $t \in \mathbb{N}$ such that $1 \leq t \leq (d-2)$, decides in time $d^{O(t)}$ if $\mathfrak{X}$ is extensible to height t. We used the association scheme extension algorithm to determine that all non-Schurian association schemes up to order 26 are completely inextensible, i.e. they have maximal height 0. It is evident that computing the maximal height of an association scheme $\mathfrak{X} = (Q, \Gamma)$ with the association scheme extension algorithm may require time exponential in $|Q|$ in the worst case. A central open question is whether there exists an algorithm for computing the maximal height which achieves a better worst-case running time (for instance, in the subexponential range). A relaxation of this question would be to ask whether there exist 'thresholds' $t(d) \in \mathbb{N}$ such that for all association schemes $\mathfrak{X} = (Q, \Gamma)$ of order $d := |Q|$, deciding if $\mathfrak{X}$ is extensible to height $t(d)$ can be done more efficiently than using the association scheme extension algorithm. Apart from this, we note that it is currently an open problem to identify the smallest order $d \in \mathbb{N}$ for which there exists a non-Schurian association scheme of positive maximal height. We leave the above questions to future research.

In Chapter 6, we described the Cohn-Umans algebra embedding approach to efficient matrix multiplication, which relates the exponent of matrix mul-

tiplication ω to combinatorial properties of association schemes and their adjacency algebras. The logical centerpiece for further research on the Cohn-Umans approach is the identification of suitable 'candidate' classes of association schemes (X, G), which - via the framework described in Section 6.2 - could help improve the upper bound $\omega_s \leq 2.376$ [CU12]. As a first step, it is essential to discern the structural conditions placed on various classes of association schemes in order for their adjacency algebra to realize a matrix multiplication tensor $\langle \ell, m, n \rangle$. Cohn and Umans [CU12] started this discussion by describing the condition which Schurian association schemes must satisfy in order to realize a matrix multiplication tensor $\langle \ell, m, n \rangle$ (see [CU12], Prop. 4.7). Moreover, they used ideas from earlier works on efficient matrix multiplication (such as [CW87, CU03]) to design explicit constructions of commutative association schemes which yield nontrivial upper bounds on ω_s (see [CU12], §6). It is evident that the algebraic-combinatorial discussion of the concept of realization of matrix multiplication tensors in association schemes (Section 6.3) is still in the beginning stages, and much 'groundwork' is required with regards to the question of how association schemes and their adjacency algebras can be of use in the Cohn-Umans fast matrix multiplication framework. Apart from the central goal, establishing a theory whose ultimate consequence will be an improvement of the upper bound of the s-rank exponent ω_s (and thereby to gain ground on the conjecture $\omega = 2$), there are many more worthwhile objectives at hand, e.g. finding the correct place of the 'main' Cohn-Umans conjecture (see [CU12], Conject. 5.7) within the field of algebraic combinatorics. The above issues represent natural topics for further research.

Acknowledgments

The task of finding an ideal Ph.D. adviser exhibits distinctive traits often associated with certain *computationally hard* problems: While there seems to be no practical method for selecting ideal advisers, it is quite easy to determine whether a selection is ideal after it was made. I was outrageously lucky to work with and be advised by Nitin Saxena and Marek Karpinski during my doctoral studies, both of whom I am infinitely indebted to. Above all, I am grateful for their generous support, continuous encouragement, and truly invaluable advice. Their dedication to research continues to be a great source of inspiration, and I look back in gratitude to the countless hours they spent discussing mathematical ideas with me. I could not have wished for more ideal Ph.D. advisers.

I owe many thanks to Paul-Hermann Zieschang for sharing his knowledge of association schemes with me, and for hosting me at the University of Texas in 2011 and 2012. It was both a privilege and a pleasure to work with him, and I profited in several ways from his careful mentoring. I am honored and grateful also that he agreed to serve on my thesis committee.

I am thankful to Ilya Ponomarenko for the many interesting and fruitful discussions at MPI Bonn and Steklov Institute St. Petersburg. His results provided a valuable resource for this thesis, and he was generous in offering explanations and pointers when I needed them.

I am grateful that I had the chance to work with Gábor Ivanyos in February of 2012. (Gábor was also generous in reducing my Erdös number to three). Moreover, I am thankful to Mikhail Muzychuk, Akihide Hanaki, and Sergei Evdokimov for several stimulating conversations, some of which were crucial to this thesis. In addition, I owe Heiko Röglin my gratitude for agreeing to serve on my thesis committee.

My heartfelt thanks to HCM Bonn and BIGS, which provide an excellent environment for mathematical research. I owe a big *Dankeschön* to the helpful administrative staff, especially Dr. Michael Meier, Karen Bingel, Sabine George, and Rosa Manthey. Also, I am grateful to my fellow Ph.D. students and office neighbors Johannes Mittmann, Richard Schmied, and Claus Viehmann, who were quite generous with their time and shared many valuable insights.

It was a pleasure and one of the best things during graduate school to attend well-organized workshops at HCM Bonn, Princeton University, and Steklov Institute St. Petersburg. Many thanks to the organizers, and to the participants which I had the opportunity of meeting there!

At last, some personal acknowledgments: I am deeply grateful to Dr. Sibille Beerbaum, Friedrich Buckel, and Siegfried Zak for igniting my interest for mathematics when I was a child. I owe them more than they might imagine.

I am forever indebted to my family and friends, both at home and abroad. This work would not have been possible without them. *I dedicate this thesis to my grandparents.*

Bibliography

[AIKS12] M. Arora, G. Ivanyos, M. Karpinski, and N. Saxena. Deterministic polynomial factoring and association schemes. *Manuscript*, 2012. arXiv: 1205.5653.

[AMM77] L. Adleman, K. Manders, and G. Miller. On taking roots in finite fields. In *Proc. 18th FOCS*, pages 175–178, 1977.

[Ank52] N. C. Ankeny. The least quadratic non residue. *Annals of Mathematics*, 55(1):65–72, 1952.

[Aro10] M. Arora. *Theory of m-Schemes and Applications to Polynomial Factoring.* Diploma Thesis, Mathematisch-Naturwissenschaftliche Fakultät der Universität Bonn, 2010.

[Aro11] M. Arora. A conjecture about homogeneous and antisymmetric m-schemes. Technical report, CS-Report 85320, 2011.

[Aro12] M. Arora. Extensibility of association schemes of small order. 2012. Published online: `http://theory.cs.uni-bonn.de/info5/ase/`.

[ASU12] N. Alon, A. Shpilka, and C. Umans. On sunflowers and matrix multiplication. In *Proc. 27th IEEE CCC*, 2012.

[AZ12] M. Arora and P.-H. Zieschang. An algorithmic approach to the extensibility of association schemes. *Manuscript*, 2012. arXiv: 1209.6312.

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

[BCRL79] D. Bini, M. Capovani, F. Romani, and G. Lotti. $O(n^{2.7799})$ complexity for matrix multiplication. *Inf. Process. Lett.*, 8(5):234–235, 1979.

[BCRW08] P. Borwein, S. Choi, B. Rooney, and A Weirathmueller, editors. *The Riemann Hypothesis: A Resource for the Afficionado and Virtuoso Alike*. CMS Books in Mathematics. Springer, 2008.

[BCS97] P. Bürgisser, M. Clausen, and M. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997.

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

[Ber70] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24:713–735, 1970.

[BI84] E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes*. Benjamin-Cummings, 1984.

[Bin80] D. Bini. Relation between exact and approximate bilinear algorithms. Applications. *Calcolo*, 17:87–97, 1980.

[BKL83] L. Babai, W. M. Kantor, and E. M. Luks. Computational complexity and the classification of finite simple groups. In *Proc. 24th IEEE FOCS*, pages 162–171, 1983.

[BL83] L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proc. 15th ACM STOC*, pages 171–183, 1983.

[Bla10] H. I. Blau. Association schemes, fusion rings, C-algebras, and reality-based algebras where all nontrivial multiplicities are equal. *Journal of Algebraic Combinatorics*, 31(4):491 – 499, 2010.

[Bos06] S. Bosch. *Algebra*. Springer, 2006.

[BS96] E. Bach and J. Sorenson. Explicit bounds for primes in residue classes. *Mathematics of Computation*, 65(216):1717–1735, 1996.

[BvzGL01] 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.

[Cam83] P. Camion. A deterministic algorithm for factorizing polynomials of $\mathbb{F}_q[x]$. *Ann. Discr. Math.*, 17:149–157, 1983.

[CFI92] J.-Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12:389–410, 1992.

[CH00] Q. Cheng and M. A. Huang. Factoring polynomials over finite fields and stable colorings of tournaments. In *Proc. 4th ANTS*, pages 233–246, 2000.

[Cho65] S. Chowla. *The Riemann Hypothesis and Hilbert's Tenth Problem*. Gordon and Breach, 1965.

[CKSU05] H. Cohn, R. Kleinberg, B. Szegedy, and C. Umans. Group-theoretic algorithms for matrix multiplication. In *Proc. 46th IEEE FOCS*, pages 379–388, 2005.

[CL03] M. J. Cloud and L. P. Lebedev. *Tensor Analysis*. World Scientific, 2003.

[CR88] C. W. Curtis and I. Reiner. *Representation Theory of Finite Groups and Associative Algebras*. Wiley Classics Library, 1988.

[CU03] H. Cohn and C. Umans. A group-theoretic approach to fast matrix multiplication. In *Proc. 44th IEEE FOCS*, pages 438–449, 2003.

[CU12] H. Cohn and C. Umans. Fast matrix multiplication using coherent configurations. *Manuscript*, 2012. arXiv: 1207.6528.

[CW87] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. In *Proc. 19th ACM STOC*, pages 1–6, 1987.

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

[Dim02] Y. I. Dimitrienko. *Tensor Analysis and Nonlinear Tensor Functions*. Kluwer Acad. Publ., 2002.

[EKP99] S. A. Evdokimov, M. Karpinski, and I. N. Ponomarenko. On a new high dimensional Weisfeiler-Lehman algorithm. *Journal of Algebraic Combinatorics*, 10:29–45, 1999.

[EP99] S. A. Evdokimov and I. N. Ponomarenko. On primitive cellular algebras. *Zapiski Nauchnykh Seminarov POMI*, 256:38–68, 1999. English translation in J. Math. Sci. 107/5 (2001), 4172-4191.

[Evd89] S. A. Evdokimov. Factorization of a solvable polynomial over finite fields and the generalized Riemann hypothesis. *Zapiski Nauchnyck Seminarov LOMI*, 176:104–117, 1989.

[Evd94] 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, 1994.

[FKM94] I. A. Faradžev, M. H. Klin, and M. E. Muzychuk. Cellular rings and groups of automorphisms of graphs. *In: I. Faradžev et. al (eds.), Investigations in Algebraic Theory of Combinatorial Objects*, pages 1–152, 1994. (Translation from Russian edition 1985).

[For08] K. Ford. The distribution of integers with a divisor in a given interval. *Annals of Math.*, 168:367–433, 2008.

[Gao01] S. Gao. On the deterministic complexity of factoring polynomials. *Journal of Symbolic Computation*, 31(1-2):19–36, 2001.

[Han00] A. Hanaki. Semisimplicity of adjacency algebras of association schemes. *Journal of Algebra*, 225:124–129, 2000.

[Han02] A. Hanaki. Locality of a modular adjacency algebra of an association scheme of prime power order. *Archiv der Mathematik*, 79:167–170, 2002.

[Han10] A. Hanaki. Private communication. 2010.

[HB92] D. R. Heath-Brown. Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression. *Proceedings of the London Mathematical Society*, 64(3):265–338, 1992.

[Hig70] D. G. Higman. Coherent configurations I. *Rend. Mat. Sem. Univ. Padova*, 44:1–25, 1970.

[HM98a] A. Hanaki and I. Miyamoto. Classification of association schemes with 16 and 17 vertices. *Kyushu J. Math.*, 52(2):383–395, 1998.

[HM98b] A. Hanaki and I. Miyamoto. Classification of association schemes with 18 and 19 vertices. *Korean J. Comput. Appl. Math.*, 5(3):543–551, 1998.

[HM03] A. Hanaki and I. Miyamoto. Classification of association schemes of small order. *Discrete Mathematics*, 264:75–80, 2003.

[HM09] A. Hanaki and I. Miyamoto. Classification of association schemes with small vertices. 2009. Published online: `http://kissme.shinshu-u.ac.jp/as/`.

[HU06] A. Hanaki and K. Uno. Algebraic structure of association schemes of prime order. *Journal of Algebraic Combinatorics*, 23(2):189–195, 2006.

[Hua84] M. A. Huang. Factorization of polynomials over finite fields and factorization of primes in algebraic number fields. In *Proceedings of the 16th annual ACM Symposium on Theory of Computing (STOC)*, pages 175–182, 1984.

[Hua91] M. A. Huang. Generalized Riemann hypothesis and factoring polynomials over finite fields. *Journal of Algorithms*, 12(3):464–481, 1991.

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

[IKS09] G. Ivanyos, M. Karpinski, and N. Saxena. Schemes for deterministic polynomial factoring. In *Proc. 34th International Symposium on Symbolic and Algebraic Computation*, pages 191–198, 2009.

[Kan63] H. J. Kanold. Elementare Betrachtungen zur Primzahltheorie. *Archiv der Mathematik*, 14:147–151, 1963.

[Kan64] H. J. Kanold. Über Primzahlen in Arithmetischen Folgen. *Mathematische Annalen*, 156:393–395, 1964.

[Kra38] M. Krasner. Une généralisation de la notion de corps. *J. Math. Pures Appl.*, 17:367–385, 1938.

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

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

[Lin44] Y. V. Linnik. On the least prime in an arithmetic progression I. the basic theorem. *Rec. Math. (Mat. Sbornik) N.S.*, 15(57):139–178, 1944.

[Mat06] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 2006.

[Moe77] R. T. Moenck. On the efficiency of algorithms for polynomial factoring. *Mathematics of Computation*, 31:235–250, 1977.

[MP12] M. E. Muzychuk and I. N. Ponomarenko. On pseudocyclic association schemes. *ARS Mathematica Contemporanea*, 5:1–25, 2012.

[MS88] M. Mignotte and C. P. Schnorr. Calcul déterministe des racines d'un polynôme dans un corps fini. *Comptes Rendus Académie des Sciences*, 306:467–472, 1988.

[NT89] H. Nagao and Y. Tsushima, editors. *Representations of Finite Groups*. Academic Press, 1989.

[Pon11] I. N. Ponomarenko. Bases of schurian antisymmetric coherent configurations and isomorphism test for schurian tournaments. *Manuscript*, 2011. arXiv:1108.5645.

[Rab80] M. O. Rabin. Probabilistic algorithms in finite fields. *SIAM Journal on Computing*, 9:273–280, 1980.

[Rie59] B. Riemann. Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monatsberichte der Berliner Akademie*, 1859.

[Rón88] L. Rónyai. Factoring polynomials over finite fields. *Journal of Algorithms*, 9:391–400, 1988.

[Rón89] L. Rónyai. Factoring polynomials modulo special primes. *Combinatorica*, 9:199–206, 1989.

[Rón92] L. Rónyai. Galois groups and factoring polynomials over finite fields. *SIAM Journal on Discrete Mathematics*, 5(3):345–365, 1992.

[Sah08] C. Saha. Factoring polynomials over finite fields using balance test. In *25th STACS*, pages 609–620, 2008.

[Sch81] A. Schönhage. Partial and total matrix multiplication. *SIAM J. Comp.*, 10:434–455, 1981.

[Smi94] J. D. H. Smith. Association schemes, superschemes, and relations invariant under permutation groups. *European J. Combin.*, 15(3):285–291, 1994.

[Smi07] J. D. H. Smith. *An Introduction to Quasigroups and Their Representations*. Chapman & Hall/CRC, 2007.

[SS58] A. Schinzel and W. Sierpinski. Sur certaines hypothèses concernant les nombres premiers. *Acta Arithmetica*, 4:345–365, 1958.

[Sto11] A. Stothers. *On the complexity of matrix multiplication*. PhD Thesis, University of Edinburgh, 2011.

[Str69] V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13(4):354–356, 1969.

[Str87] V. Strassen. Relative bilinear complexity and matrix multiplication. *J. Reine Angew. Math.*, 375 & 376:406–443, 1987.

[Voi05] J. Voight. Curves over finite fields with many points: an introduction. In Tanush Shaska, editor, *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Series on Computing*, pages 124–144. World Scientific, Hackensack, NJ, 2005.

[VW12] V. Vassilevska-Williams. Multiplying matrices faster than Coppersmith-Winograd. In *Proc. 44th ACM STOC*, pages 887–898, 2012.

[vzG87] J. von zur Gathen. Factoring polynomials and primitive elements for special primes. *Theoretical Computer Science*, 52:77–89, 1987.

[vzGS92] J. von zur Gathen and V. Shoup. Computing frobenius maps and factoring polynomials. *Computational Complexity*, 2:187–224, 1992.

[Wei76] B. Weisfeiler, editor. *On Construction and Identification of Graphs*, volume 558. Lecture Notes in Mathematics, 1976.

[WL68] B. Weisfeiler and A. Lehman. Reduction of a graph to a canonical form and an algebra which appears in this process (in russian). *Scientific-Technological Investigations*, 9(2):12–16, 1968.

[Woj98] J. Wojdyło. Relation algebras and t-vertex condition graphs. *European Journal of Combinatorics*, 19:981–986, 1998.

[Woj01a] J. Wojdyło. An inextensible association scheme associated with a 4-regular graph. *Graphs and Combinatorics*, 1(17):185–192, 2001.

[Woj01b] J. Wojdyło. Presuperschemes and colored directed graphs. *JCMCC*, 38:45–54, 2001.

[Xyl11] 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.

[Zie96] P.-H. Zieschang. *An Algebraic Approach to Association Schemes*, volume 1628. Lecture Notes in Mathematics, 1996.

[Zie05] P.-H. Zieschang. *Theory of Association Schemes.* Springer, 2005.

Index

Adjacency algebra (of an association scheme), 20, 92
Adjacency matrix (of an association scheme relation), 19
Adjacency tensor (of an n-ary relation), 79
Algebraically conjugate (characters), 29, 32
Association scheme, 16, 73
  Antisymmetric, 17
  Commutative, 16, 34, 92
  Completely inextensible, 76, 85
  Cyclotomic, 17, 38
  Non-Schurian, 17, 85
  Schurian, 17, 77
Association scheme extension algorithm, 80

Cellular algebra, 8
Character (of an algebra), 22
  Irreducible, 22, 32
Coherent configuration, 8, 92
m-Collection, 43, 63
  Antisymmetric, 44, 65
  Compatible, 43, 64
  Homogeneous, 44, 65
  Invariant, 44, 64
  Regular, 43, 64
  Symmetric, 44

Dirichlet character, 61
Dirichlet L-function, 61

Efficient matrix multiplication, 87
Extensibility (of an association scheme), 73, 80
t-Extension (of an association scheme), 76, 85

Finite field, 17, 38, 59
Fusion (of an association scheme), 84

Galois group (of a field extension), 27
Generalized Riemann hypothesis (GRH), 61, 65, 69
Graph isomorphism problem, 8
Group algebra, 14, 91

Hanaki-Uno theorem, 32
Hasse-Weil bound, 38, 71
Height t presuperscheme (*short:* t-prescheme), 75, 80

Ideal decomposition (of an algebra), 60
IKS-Algorithm, 61, 65–66
Indistinguishing number (in an association scheme), 16, 34
Intersection number (in a presuperscheme), 76
Intersection number (in an association scheme), 16, 35
Irreducible character (of an algebra), 22, 32

Krasner algebra, 8

Linnik constant, 69

Matching (in an m-scheme), 49, 51, 55, 65–66
Matrix multiplication exponent, 88, 94
Matrix multiplication tensor, 90
Matrix representation (of an algebra), 22
Maximal height (of an association scheme), 76
Multiplicative group (of a finite field), 17
Multiplicity, 24, 32

Non-Schurian (association scheme), 17, 85

Orbit m-scheme, 47, 77
Order (of a tensor), 78
Order (of an association scheme), 16, 32, 38
Orthogonality relations, 24

Polynomial factoring over finite fields, 57
Presuperscheme (*short:* Prescheme), 75, 80
Principal Character, 23

Rank (of a tensor), 90
Rank (of an association scheme), 16

Realization (of a matrix multiplication tensor in a finite-dimensional algebra), 91
Realization (of a matrix multiplication tensor in an association scheme), 93
Representation (of an algebra), 22

m-Scheme, 44, 65–66
Orbit, 47, 77
Schemes conjecture, 50
Schurian (association scheme), 17, 77
Semisimple (algebra), 21, 92
Standard Character, 23
Standard Representation, 23
Strongly regular graph, 18
Structural tensor (of a finite-dimensional algebra), 92
Subdegree (of an m-scheme relation), 43, 49
Superscheme, 8, 77

Tensor, 78, 90
Trivial Character, 23

Unique coarsest t-extension (of an association scheme), 85

Valency (of an association scheme relation), 16, 34