A Conjecture about Homogeneous and Antisymmetric m-Schemes

Manuel Arora*

Abstract

We study the notion of matchings in homogeneous and antisymmetric m-schemes, as defined in Ivanyos, Karpinski & Saxena (2009). We give a general conjecture which involves the existence of matchings in homogeneous and antisymmetric m-schemes and prove certain special cases of it. Our results, as part of the general topic of matchings in m-schemes, are closely related to the deterministic time complexity of polynomial factoring over finite fields.

1 Introduction

The topic of *m-schemes*, going back to its origin, is closely related to the computational problem of polynomial factoring over finite fields - a problem with major applications to coding theory and integer factoring, but for which no deterministic polynomial-time algorithm has been found so far. In 2009, Ivanyos, Karpinski and Saxena suggested a new approach to the polynomial factoring problem: They discovered a GRH-based deterministic factoring algorithm (called *IKS-algorithm* in the following) that uses combinatorial schemes in the manipulation of algebraic data generated by the input polynomial (Ivanyos, Karpinski & Saxena [4]). Their new approach entails the definition of m-schemes, and links m-schemes to the deterministic time complexity of polynomial factoring over finite fields. In particular, they showed that the IKS-algorithm computes general instances of the polynomial factoring problem in subexponential time (under GRH), and even has deterministic polynomial running time in the factorization of polynomials of prime degree p, where $(p-1)$ is a constant-smooth number (assuming GRH).

*Hausdorff Center for Mathematics, Bonn, Germany. Email: aroram@cs.uni-bonn.de

In this paper, we pick up the line of research that was started by Ivanyos, Karpinski and Saxena. We consider the types of m-schemes that appear in the IKS-algorithm - namely, *homogeneous* and *antisymmetric* m-schemes - and study combinatorial sub-structures that appear within those m-schemes, called *matchings*. The appearance of matchings in m-schemes is central to our research, as it is directly linked to the deterministic time complexity of polynomial factoring over finite fields (see [4], Theorem 7). As an essential part of our work, we give a general conjecture that involves the existence of matchings in homogeneous and antisymmetric m-schemes and prove certain special cases of it (see Conjecture 3.1). This yields some new results and constitutes some new concepts (see Sections 3, 4).

1.1 Organization

The material in this paper is divided into three parts. In Section 2, we review the existing theory of m-schemes. Amongst other things, we define the notion of m-scheme matchings and explain how matchings relate to the time complexity of the IKS-algorithm. In Section 3, we expand the existing theory of m-schemes by some new concepts. In particular, we introduce the so-called subdegree conjecture for m-schemes, which has important implications for the deterministic time complexity of polynomial factoring over finite fields (see Conjecture 3.1). For the remainder of Section 3, and throughout Section 4, we prove certain special cases of the subdegree conjecture. The results of Section 4 in particular yield some new results about matchings in homogeneous and antisymmetric m-schemes.

2 Definitions and Examples

In the following, we give an overview of the definition of m-schemes and standard notions associated with it. We should remark up front that the term m-scheme refers to an object of purely combinatorial nature; especially, m-schemes are not related to the notion of *schemes* of algebraic geometry. However, m-schemes are closely related to standard objects from algebraic combinatorics, such as *association schemes* (Bannai & Ito [1], Zieschang [7]), *coherent configurations* (Higman [3]), *superschemes* (Smith [5]) and *height t presuperschemes* (Wojdylo [6]).

For reference purposes, the terminology for m-schemes used here is the same as in the paper [4]. The following notions are prerequisite to our discussion of m-schemes.

s-tuples: In the following, let $V = \{v_1, v_2, ..., v_n\}$ be an arbitrary set of n distinct elements. For $1 \leq s \leq n$, we define the *set of s-tuples* by

$$V^{(s)} := \{(v_{i_1}, v_{i_2}, ..., v_{i_s}) \mid \ v_{i_1}, v_{i_2}, ..., v_{i_s} \text{ are } s \text{ distinct elements of } V\}.$$

Projections: For $s > 1$, we define s *projections* $\pi_1^s, \pi_2^s ..., \pi_s^s : V^{(s)} \longrightarrow V^{(s-1)}$ by

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

Permutations: The symmetric group on s elements $Symm_s$ acts on $V^{(s)}$ in a natural way by permuting the coordinates of the s-tuples. More accurately, the action of $\tau \in Symm_s$ on $(v_1, ..., v_i, ..., v_s) \in V^{(s)}$ is defined as

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

m-Collection: For $1 \leq m \leq n$, an *m-collection* on V is a set Π of partitions $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m$ of $V^{(1)}, V^{(2)}, ..., V^{(m)}$ 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 $\equiv_{\mathcal{P}_s}$. The elements of $\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m$ are referred to as the *colors* of Π.

The notion of m-schemes arises from the notion of m-collections in a natural way. To give a brief description: An m-scheme is an m-collection $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ on a set $V = \{v_1, v_2, ..., v_n\}$ that satisfies some natural properties which are inherently connected to the routine of the IKS-algorithm (see [4], Sec. 3). Amongst those properties are, for example, *compatibility* and *invariance*. We give a brief summary of these properties: An m-collection $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is called compatible if for all $1 < s \leq m$, the relation $\bar{u} \equiv_{\mathcal{P}_s} \bar{v}$ implies $\pi_i^s(\bar{u}) \equiv_{\mathcal{P}_{s-1}} \pi_i^s(\bar{v})$, for all $1 \leq i \leq s$ and $\bar{u}, \bar{v} \in V^{(s)}$. Moreover, Π is called invariant if for all $1 \leq s \leq m$, $P \in \mathcal{P}_s$ and $\tau \in Symm_s$,

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

Some m-schemes satisfy the additional property of antisymmetry, which is related to invariance: We say that Π is *antisymmetric* if for all $1 < s \leq m$, $P \in \mathcal{P}_s$ and $id \neq \tau \in Symm_s$, we have $P^\tau \neq P$. As we noted before, the m-schemes that appear in the IKS-algorithm are always antisymmetric. For an in-depth discussion of the properties of m-schemes and their role in the IKS-algorithm, the reader is referred to the paper [4].

Consider the following example of m-schemes. Let $V = \{v_1, v_2, ..., v_n\}$ be a set of n distinct elements and $G \leq Symm_V$ a permutation group on V.

Assume $1 \leq m \leq n$. Then for all $1 \leq s \leq m$, the set of orbits that arise from the componentwise action of G on $V^{(s)}$ form a partition $\mathcal{P}_s$ of $V^{(s)}$. It is easily shown that the set of partitions $\Pi := \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ which arise in this way form an m-scheme on V; the reader may check himself that all the m-scheme properties (as defined in [4], Sec. 2) are satisfied. m-schemes that are constructed from permutation groups in the above-described way are called *orbit m-schemes*.

In the above example, note that if G is transitive, then $\mathcal{P}_1 = \{V\}$. In general, m-schemes that satisfy this triviality property at the lowest level are said to be *homogeneous*. As we noted before, the m-schemes that appear in the IKS-algorithm are always homogeneous. Also note in the above example, it can be shown that the orbit m-scheme $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ is antisymmetric if and only if $gcd(m!, |G|) = 1$; we leave the proof as an exercise to the reader. It is important to remark that so far, the only examples of homogeneous and antisymmetric m-schemes that are known (when $m \geq 3$) stem from the class of orbit m-schemes.

To complete our survey of m-scheme definitions, we will now explain the notion of subdegrees and matchings, concepts which appear frequently in our discussion of m-schemes. In the following, let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$ be an m-scheme on $V = \{v_1, v_2, ..., v_n\}$.

Subdegree: It follows from the m-scheme properties (see [4], Sec. 2) that for all $1 < s \leq m$, $P \in \mathcal{P}_s$ and $1 \leq i \leq s$, the cardinality of the color $Q := \pi_i^s(P) \in \mathcal{P}_{s-1}$ is a divisor of the cardinality of P. Especially, this gives rise to the definition of the *subdegree of P over Q* as the positive integer $\frac{|P|}{|Q|}$.

Matching: A color $P \in \mathcal{P}_s$ at any level $1 < s \leq m$ is called a *matching* if there exists $1 \leq i < j \leq s$ such that $\pi_i^s(P) = \pi_j^s(P)$ and $|\pi_i^s(P)| = |P|$.

As we noted before, matchings are of great importance to the time complexity of the IKS-algorithm. It was shown in [4], Sec. 4.1 that under a plausible conjecture about m-scheme matchings, the so-called *schemes conjecture*, the IKS-algorithm has polynomial running time in the factorization of polynomials over finite fields (assuming GRH). In this paper, we consider a conjecture about m-schemes which is slightly weaker than the schemes conjecture, but which would nevertheless imply a new best known running time for polynomial factoring over finite fields (see Conjecture 3.1). We introduce this slightly weaker conjecture, which we refer to as the *subdegree conjecture*, in the following section.

3 The Subdegree Conjecture

For the remainder of this work, let us fix some conventions. For brevity of notation, we omit the level indices of the projections $\pi_1^s, \pi_2^s ..., \pi_s^s$ $(s > 1)$ in the future; the corresponding projection level will be clear from context. In addition, we establish the following terminology and notations for m-schemes:

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.

Subdegree: For colors $G \in \mathcal{P}_s$ and $H \in \mathcal{P}_{s-1}$ such that $\pi_i(G) = H$ for some $1 \leq i \leq s$ we denote the subdegree of G over H by $s(G, H) := \frac{|G|}{|H|}$.

We now state the conjecture that will be central in the whole of this work.

Conjecture 3.1 (Subdegree Conjecture)**.** *Let $\Pi = \{\mathcal{P}_1, ..., \mathcal{P}_m\}$ be a homogeneous, antisymmetric m-scheme on $n > m!$ points. Then either there exists a matching in Π or there exist colors $S \in \mathcal{P}_m$ and $P \in \mathcal{P}_{m-1}$ such that $s(S, P) \leq \frac{n}{m!}$ and at least two of the sets $\pi_1(S), \pi_2(S), ..., \pi_m(S)$ equal P.*

The above conjecture is easily proven for $m = 2$ (see [4], Lemma 8):

Theorem 3.2. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2\}$ be a homogeneous, antisymmetric 2-scheme on $V = \{v_1, v_2, ..., v_n\}$, where $n > 2$. Then there exists a color $P \in \mathcal{P}_2$ such that $s(P, V) \leq \frac{n}{2}$. Especially, if $s(P, V) = 1$, then P is a matching.*

From the above theorem it follows by [4], Theorem 7 that a polynomial of degree n over $\mathbb{F}_p$ can be factored deterministically in time $poly(n^{\log n}, \log p)$. Note that the bound $poly(n^{\log n}, \log p)$ for polynomial factoring over finite fields was obtained earlier by Evdokimov (see [2]) and is currently still the best known bound.

By [4], Theorem 7 a complete proof of Conjecture 3.1 would imply an improvement in the deterministic time complexity of polynomial factoring over finite fields to $poly(n^{o(\log n)}, \log p)$ - this would mark the first improvement in time complexity since Evdokimov's paper. A first step towards proving Conjecture 3.1 was undertaken in the paper [4] (see Lemma 10); the methods used there rely on some highly non-trivial results derived from the theory of adjacency matrices of association schemes. In our present paper, we give an

alternative and arguably easier proof of the result that was obtained there (see Theorem 3.3). In addition, we prove Conjecture 3.1 in the case $m = 4$; this is a new result and constitutes some new concepts (see Theorem 4.2).

The following theorem was first proven in [4] (see Lemma 10). It implies Conjecture 3.1 in the case $m = 3$. Moreover, we obtain from this theorem an explicit level bound for matchings in homogeneous and antisymmetric m-schemes (see Corollary 3.4 below).

Theorem 3.3. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$ be a homogeneous, antisymmetric 3-scheme on $V = \{v_1, v_2, ..., v_n\}$, where $n > 8$. Then either there exists a matching in Π or there exist colors $P \in \mathcal{P}_2$ and $S \in \mathcal{P}_3$ such that $s(S, P) \leq \frac{n}{8}$ and at least two of the sets $\pi_1(S), \pi_2(S), \pi_3(S)$ equal P.*

Proof. Assume there are more than 2 colors in $\mathcal{P}_2$. Then by antisymmetry at level 2 there are at least 4 colors in $\mathcal{P}_2$. Hence we find a color $P \in \mathcal{P}_2$ of subdegree smaller than $\frac{n}{4}$ over $V \in \mathcal{P}_1$. Now if $s(P, V) = 1$ then P is a matching; if on the other hand $s(P, V) > 1$ then by Theorem 3.2 applied on $\{\pi_1(\mathcal{P}_2), \pi_1(\mathcal{P}_3)\}$ (which is easily seen to be a 2-scheme) we find a color $S \in \mathcal{P}_3$ such that $\pi_2(S) = \pi_3(S) = P$ and $s(S, P) \leq \frac{n}{8}$ (subdegree is halved). We conclude that the theorem holds in this case.

Now assume there are exactly 2 colors in $\mathcal{P}_2$; say $\mathcal{P}_2 = \{P, Q\}$, where $Q = P^{(1,2)}$. By Theorem 3.2 applied on $\{\pi_1(\mathcal{P}_2), \pi_1(\mathcal{P}_3)\}$ we find a color $T \in \mathcal{P}_3$ such that $s(T, P) \leq \frac{n}{4}$ (subdegree is halved). By construction, the cardinality of T is less than $n \cdot \frac{n}{2} \cdot \frac{n}{4} = \frac{n^3}{8}$. By antisymmetry at level 3, this means that there are at least 12 colors in $\mathcal{P}_3$. Consequently, we find in $\mathcal{P}_3$ at least two colors C, D which are not associated colors (under the action of $Symm_3$).

Let us consider the different types of underlying color sequences that C, D can have. Observe 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

$$\{(P,P,P),\ (P,P,Q),\ (P,Q,Q),\ (Q,Q,Q),\ (Q,Q,P),\ (Q,P,P)\},\quad \text{and}$$

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

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; this can be verified as an easy exercise. Since C, D are not associated colors, we may assume wlog that each C, D have underlying color sequence either (P, P, P) or (P, Q, P).

Here let us consider the case that C and D both have underlying color sequence (P, P, P) (the other cases are similar). In this case, the set

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

covers at least 4 colors (as each $\{C^\sigma \mid \sigma \in Symm_3\}$ and $\{D^\sigma \mid \sigma \in Symm_3\}$ contain two colors which are subsets of A). Accordingly, we find a color $S \subset A$ such that

$$s(S, P) \leq \frac{|A|/4}{|P|} < n/8;$$

here we used $|P| = n \cdot \frac{(n-1)}{2}$ and $|A| = n \cdot \frac{(n-1)}{2} \cdot \frac{(n-3)}{2}$. So the assumption is true in this case. The other cases are shown analogously. □

From the above lemma we see that within three levels we are able to reduce the subdegree to a fraction of 2^{-3}. This immidiately gives us the following level bound for matchings in homogeneous and antisymmetric m-schemes (see [4], Corollary 11):

Corollary 3.4. *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 $\{\mathcal{P}_1, \mathcal{P}_2, ..., \mathcal{P}_m\}$.*

4 A Proof for the Case $m = 4$ of the Subdegree Conjecture

We now turn to the proof of the case $m = 4$ of Conjecture 3.1. This represents a new result and manifests some new concepts. In order to prove this case, we need the following preliminary lemma:

Lemma 4.1. *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).

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

$$\{(P,P,P),\ (P,P,Q),\ (P,Q,Q),\ (Q,Q,Q),\ (Q,Q,P),\ (Q,P,P)\},\quad \text{and}$$

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

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

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

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

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

From this the assertion follows immediately. □

We use the above lemma to prove Conjecture 3.1 in the case $m = 4$. The proof given below is of purely combinatorial nature; it requires only basic m-scheme theory.

Theorem 4.2. *Let $\Pi = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \mathcal{P}_4\}$ be a homogeneous, antisymmetric 4-scheme on $V = \{v_1, v_2, ..., v_n\}$, where $n > 24$. Then either there exists a matching in Π or there exist colors $T \in \mathcal{P}_3$ and $S \in \mathcal{P}_4$ such that $s(S,T) \leq \frac{n}{24}$ and at least two of the sets $\pi_1(S), \pi_2(S), \pi_3(S), \pi_4(S)$ equal T.*

Proof. Assume there are more than 2 colors in $\mathcal{P}_2$. Then by antisymmetry at level 2 there are at least 4 colors in $\mathcal{P}_2$. Hence we find a color $P \in \mathcal{P}_2$ of subdegree smaller than $\frac{n}{4}$ over $V \in \mathcal{P}_1$. Now if $s(P,V) = 1$ then P is a matching; if on the other hand $s(P,V) > 1$ then according to Theorem 3.3 applied on $\{\pi_1(\mathcal{P}_2), \pi_1(\mathcal{P}_3), \pi_1(\mathcal{P}_4)\}$ (which is easily seen to be a 3-scheme)

we either find a matching in $\mathcal{P}_3$ or we find colors $S \in \mathcal{P}_4$ and $T \in \mathcal{P}_3$ such that $s(S,T) \leq \frac{n}{32}$ and $\pi_i(S) = \pi_j(S) = T$ for some $1 \leq i < j \leq 4$. We conclude that the above assumption holds in this case.

Now assume there are exactly 2 colors in $\mathcal{P}_2$; say $\mathcal{P}_2 = \{P, Q\}$, where $Q = P^{(1,2)}$. Recall that $|\mathcal{P}_2| = 2$ implies there are exactly 8 possibilities of underlying color sequences for colors in $\mathcal{P}_3$. We can partition these 8 possibilities into two sets

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

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. The proof now follows a simple counting argument. 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 (1). From this we obtain the cardinality of Y,

$$|Y| = |Z| - |X| = \frac{n \cdot (n-1) \cdot (n-3)}{8}. \tag{2}$$

We now show that there are at least 3 colors in $\mathcal{P}_3$ which are subsets of Y. First, recall that by Lemma 4.1 (ii) there exists $D \in \mathcal{P}_3$ with underlying color sequence (P,Q,P). Second, observe that there are exactly 3 colors in $\{D^\sigma \,|\, \sigma \in Symm_3\}$ that have underlying color sequence (P,Q,P). Hence there are at least 3 colors in $\mathcal{P}_3$ which are subsets of Y. Consequently, there exists a color $T \subset Y$ such that

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

the latter inequality can be deduced using Equation (2). Now if $s(T,P) = 1$ then T is a matching; if on the other hand $s(T,P) > 1$ then by Theorem 3.2 applied on $\{\pi_1(\mathcal{P}_3), \pi_1(\mathcal{P}_4)\}$ (which is easily seen to be a 2-scheme) we find colors $S \in \mathcal{P}_4$ and $T \in \mathcal{P}_3$ such that $\pi_3(S) = \pi_4(S) = T$ and $s(S,T) \leq \frac{n}{24}$ (subdegree is halved). This completes our proof. □

Acknowledgments

I want to thank my doctoral advisers Nitin Saxena and Marek Karpinski for their generous support and guidance. Also, I want to thank the Bonn International Graduate School for Mathematics and the Hausdorff Center for Mathematics, Bonn, for their kind support and for research funding.

References

[1] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin-Cummings (1984).

[2] S. A. Evdokimov, *Factorization of Polynomials over Finite Fields in Subexponential Time Under GRH*, Lecture Notes in Computer Science 877 (1994), 209-219.

[3] D. G. Higman, *Coherent Configurations I*, Rend. Mat. Sem. Univ. Padova 44 (1970), 1-25.

[4] G. Ivanyos, M. Karpinski, N. Saxena, *Schemes for Deterministic Polynomial Factoring*, 34th Int. Symposium on Symbolic and Algebraic Computation (2009), 191-198.

[5] J. D. H. Smith, *Association Schemes, Superschemes, and Relations Invariant Under Permutation Groups*, European Journal of Combinatorics 15 (1994), 285-291.

[6] J. Wojdyło, *An Inextensible Association Scheme Associated With a 4-Regular Graph*, Garphs and Combinatorics 17/1 (2001), 185-192.

[7] P. H. Zieschang, Theory of Association Schemes, Springer (2005).