European Journal of Combinatorics 30 (2009) 1456–1476

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Permutation group approach to association schemes

Sergei Evdokimov, Ilia Ponomarenko

Steklov Institute of Mathematics at St. Petersburg, Russian Federation

ARTICLE INFO

Article history:
Available online 9 January 2009

ABSTRACT

We survey the modern theory of schemes (coherent configurations). The main attention is paid to the schurity problem and the separability problem. Several applications of schemes to constructing polynomial-time algorithms, in particular, graph isomorphism tests, are discussed.

1. Introduction

The scheme theory was started independently by Higman in [45] as the theory of coherent configurations (coherent algebras) and by Weisfeiler and Leman in [79] as the theory of stationary graphs (cellular algebras). The motivations were different: in the former case it was a tool for studying permutation groups whereas in the latter one it was the base to attack the Graph Isomorphism Problem. For the next several decades the investigations of schemes were mainly concentrated onto looking for interesting examples of schemes. Within this time the general scheme theory was presented in books [9,13]. However, most of the results were related only to the commutative case.

The situation drastically changed in the 1990s when the permutation group, group-theoretical and linear representation approaches to the scheme theory were developed by the authors of this paper,[1] by P.-H. Zieschang, and by A. Hanaki respectively. It should be noted that in the latter two cases (in contrast to the first one) only homogeneous schemes were taken into consideration. However, we believe that most of the results obtained there can more or less easily be transferred to the general case. Besides, since these parts are presented in this issue, we will concentrate in our survey only onto the permutation group approach. It should be stressed here that the general theory of schemes relates to the theory of homogeneous schemes in the same way as the general permutation group theory relates to the theory of transitive groups.

E-mail addresses: evdokim@pdmi.ras.ru (S. Evdokimov), inp@pdmi.ras.ru (I. Ponomarenko).

[1] The most part of the results on schemes presented here was originally formulated in the cellular algebra language. However, there is a natural bijection between the schemes and the cellular algebras containing the identity matrix that takes respectively isomorphisms and similarities of schemes to strong isomorphisms and weak isomorphisms of cellular algebras (see (2)).

0195-6698/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ejc.2008.11.005

Roughly speaking there are two main problems within the permutation group approach to the scheme theory: the schurity problem and the separability problem. The first of them goes back to H. Wielandt who was interested in necessary and sufficient conditions for a given scheme to be schurian, i.e. to be the scheme of a permutation group. It also includes the question to what degree the scheme can differ from a schurian one. The separability problem is about when the natural invariants of a scheme (like intersection numbers) characterize this scheme up to isomorphism. Since the initial interest of the authors to schemes came from computational complexity theory, this survey contains a section devoted to algorithmic applications of the scheme theory.

2. Schemes in algebra, arithmetic, geometry and combinatorics

2.1. Schemes

Let V be a finite set and $\mathcal{R}$ a partition of V^2. Denote by $\mathcal{R}^*$ the set of all unions of the elements of $\mathcal{R}$.

Definition 2.1. A pair $\mathcal{C} = (V, \mathcal{R})$ is called a *coherent configuration* or a *scheme* on V if the following conditions are satisfied:

(S1) the diagonal $\Delta(V)$ of V^2 belongs to $\mathcal{R}^*$,
(S2) $\mathcal{R}$ is closed with respect to transposition,
(S3) given $R, S, T \in \mathcal{R}$, the number $\{v \in V : (u, v) \in R, (v, w) \in S\}$ does not depend on the choice of $(u, w) \in T$.

The elements of V, $\mathcal{R} = \mathcal{R}(\mathcal{C})$, $\mathcal{R}^* = \mathcal{R}^*(\mathcal{C})$ and the numbers from (S3) denoted by $c_{R,S}^{T}$, are called the *points*, the *basis relations*, the *relations* and the *intersection numbers* of $\mathcal{C}$, respectively. The numbers $|V|$ and $|\mathcal{R}|$ are called the *degree* and the *rank* of $\mathcal{C}$. The scheme $\mathcal{C}$ is called *symmetric* if all relations from $\mathcal{R}$ are symmetric, and *commutative* if $c_{R,S}^{T} = c_{S,R}^{T}$ for all $R, S, T \in \mathcal{R}$.

The set V is the disjoint union of *homogeneity sets*[2] of $\mathcal{C}$, i.e. those $X \subset V$ for which $\Delta(X) \in \mathcal{R}$. The scheme $\mathcal{C}$ is called *homogeneous* if V is a homogeneity set of it. If X is a union of the homogeneity sets, then the restriction of $\mathcal{C}$ to X is defined to be the scheme

$$\mathcal{C}_X = (X, \mathcal{R}_X)$$

where $\mathcal{R}_X$ is the set of all non-empty relations $R \cap X^2$ with $R \in \mathcal{R}$; it is called a *homogeneous component* of $\mathcal{C}$ when X is a homogeneity set.

A homogeneous scheme $\mathcal{C}$ is called *imprimitive* if the set $\mathcal{R}^*$ contains an equivalence relation on V other than $\Delta(V)$ and V^2; otherwise it is called *primitive*. Equivalently, $\mathcal{C}$ is primitive if any of its non-reflexive basis relations is strongly connected.

Two schemes are called *isomorphic* if there exists a bijection between their point sets preserving the basis relations. Any such bijection is called an *isomorphism* of these schemes. The group of all isomorphisms of a scheme $\mathcal{C}$ contains a normal subgroup

$$\mathrm{Aut}(\mathcal{C}) = \{f \in \mathrm{Sym}(V) : R^f = R,\ R \in \mathcal{R}\}$$

called the *automorphism group* of $\mathcal{C}$. If V coincides with a group G and $\mathrm{Aut}(\mathcal{C})$ contains the permutation group G_{right} induced by the right multiplications in G, then $\mathcal{C}$ is called a *Cayley scheme* over G.

Schemes $\mathcal{C}$ and $\mathcal{C}'$ are called *similar* if

$$c_{R,S}^{T} = c_{R^\varphi,S^\varphi}^{T^\varphi}, \quad R, S, T \in \mathcal{R}, \tag{1}$$

for some bijection $\varphi : \mathcal{R} \to \mathcal{R}',\ R \mapsto R^\varphi$ called a *similarity* from $\mathcal{C}$ to $\mathcal{C}'$.[3] The set of all similarities is denoted by $\mathrm{Sim}(\mathcal{C}, \mathcal{C}')$. Each isomorphism f from $\mathcal{C}$ to $\mathcal{C}'$ induces in a natural way a similarity between

[2] We do not use the term "fiber" because D. Higman (who proposed it) used it in different meanings.

[3] The similarity φ induces also a bijection $X \mapsto X^\varphi$ between the homogeneity sets of $\mathcal{C}$ and $\mathcal{C}'$ (and their unions).

these schemes denoted by φ_f. The set of all isomorphisms from $\mathcal{C}$ to $\mathcal{C}'$ inducing a similarity φ is denoted by $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi)$.

In the next subsections we give some examples of schemes arising in algebra, arithmetic, geometry and combinatorics.

2.2. Algebra

A linear subspace $\mathcal{A}$ of the algebra $\mathrm{Mat}_V(\mathbb{C})$ is called a *coherent* algebra [46] if it satisfies the following conditions:

(A1) $\mathcal{A}$ contains the identity matrix I_V and the all-one matrix J_V,
(A2) $\mathcal{A}$ is closed with respect to the ordinary and Hadamard multiplications,
(A3) $\mathcal{A}$ is closed with respect to transposition.

In particular, $\mathcal{A}$ is an algebra with respect to the ordinary and Hadamard multiplications with the identities I_V and J_V respectively. Denote by $\mathcal{M}$ the set of primitive idempotents of $\mathcal{A}$ with respect to the Hadamard multiplication. Then $\mathcal{M}$ is a linear basis of $\mathcal{A}$ consisting of {0,1}-matrices such that

$$\sum_{A\in\mathcal{M}} A = J_V \quad \text{and} \quad A \in \mathcal{M} \;\Leftrightarrow\; A^{\mathrm{T}} \in \mathcal{M}.$$

Thus the coherent algebras are exactly the cellular algebras defined in [78] that contain the identity matrix.

Let $\mathcal{C} = (V, \mathcal{R})$ be a scheme. From the definition of a scheme it follows that the linear span $\mathcal{A}(\mathcal{C})$ of the set $\{A(R) : R \in \mathcal{R}\} \subset \mathrm{Mat}_V$ is a coherent algebra; it is called the *adjacency algebra* of the scheme $\mathcal{C}$.[4] Comparing the definitions of schemes and coherent algebras one can see that the mappings

$$\mathcal{C} \mapsto \mathcal{A}(\mathcal{C}), \qquad \mathcal{A} \mapsto \mathcal{C}(\mathcal{A}) \tag{2}$$

where $\mathcal{C}(\mathcal{A}) = (V, \mathcal{R}(\mathcal{A}))$ with $\mathcal{R}(\mathcal{A}) = \{R \subset V^2 : A(R) \in \mathcal{M}\}$, are reciprocal bijections between the sets of schemes and coherent algebras on V. Here the intersection numbers of a scheme $\mathcal{C}$ coincide with the structure constants of the algebra $\mathcal{A} = \mathcal{A}(\mathcal{C})$ with respect to the basis $\mathcal{M}$. In particular, the scheme $\mathcal{C}$ is commutative if and only if so is the algebra $\mathcal{A}$. Thus scheme is the combinatorial analog of coherent algebra.

Different attempts to remove the standard representation from the definition of coherent algebra produced several generalizations of this notion in the homogeneous case: commutative C-algebras [9], non-commutative C-algebras [34], generalized table algebras [2]. The first generalization including the non-homogeneous case was done recently in [18].

Let G be a finite group. Given a conjugacy class c of it we define a binary relation

$$R_c = \{(x, y) \in G \times G : x^{-1}y \in c\}.$$

Denote by $\mathcal{R}$ the set of all these relations. Then the pair $\mathcal{C} = (G, \mathcal{R})$ is a homogeneous scheme called the *scheme of conjugacy classes of* G. It is easily seen that it is a Cayley scheme over G. Since the adjacency algebra $\mathcal{A}$ of this scheme is isomorphic to the center of the group algebra $\mathbb{C}[G]$, the scheme $\mathcal{C}$ is commutative. It should also be mentioned that the C-algebra dual to $\mathcal{A}$ is known as the character algebra of the group G. It is easily seen that the group $\mathrm{Aut}(\mathcal{C})$ contains the permutation groups induced by the left and right multiplications in G. Since the intersection numbers of the scheme $\mathcal{C}$ are expressed via the values of the character table of G (see [9]), two schemes of conjugacy classes are similar if and only if the corresponding groups have the same character tables.

We complete the subsection by mentioning three more classes of algebraic structures naturally related to schemes. First of them is formed by Schur rings which up to language is nothing else than Cayley schemes; the theory of Schur rings is the subject of paper [69], this issue. The second class consists of the schemes of permutation groups; we consider them in detail in Section 3. Finally, Hecke algebras (algebras of double cosets) are mentioned in Section 3.1, see also [55].

[4] In the commutative case the alternative name for it is the Bose–Mesner algebra.

2.3. Arithmetic

Let R be a finite commutative ring with identity and K a subgroup of its multiplicative group $R^{\times}$. Denote by $\mathrm{Rel}(K,R)$ the set of all binary relations $S_r = \{(x,y) \in R \times R : \ y - x \in rK\}$ where $r \in R$. Then the pair

$$\mathrm{Cyc}(K,R) = (R, \mathrm{Rel}(K,R))$$

is a homogeneous scheme called a *cyclotomic scheme over* R [38]. Clearly, $\mathrm{Cyc}(K,R)$ is the scheme of the group of all permutations on R taking x to $ax + b$ where $a \in K$ and $b \in R$ (see Section 3). In particular, it is a Cayley scheme over the additive group R^{+} of the ring R or a translation scheme in the sense of [13]. The automorphism groups of cyclotomic schemes over rings were studied in [22].

Cyclotomic schemes over rings generalize cyclotomic schemes over finite fields that were introduced by P. Delsarte in 1973 in the framework of coding theory. Let $R = \mathbb{F}$ be a field of order q and K a subgroup of $\mathbb{F}^{\times}$ of index m. Then the intersection number of the scheme $\mathrm{Cyc}(K,\mathbb{F})$ that corresponds to the relations S_a, S_b, S_c with $a, b, c \neq 0$ equals the number of solutions $\xi, \eta \in \{0, 1, \ldots, (q-1)/m - 1\}$ of the equation $ag^{m\xi} + b = cg^{m\eta}$ where g is a primitive element of $\mathbb{F}$. The explicit evaluation of these integers called the cyclotomic numbers is a hard number-theoretic problem (see [62, p.305]).

The notion of cyclotomic scheme can be analogously defined for the algebraic structures other than rings; for instance, in [7] the cyclotomic schemes over finite near-fields are considered.

2.4. Geometry

There is a lot of schemes that can be obtained from incidence geometries in the sense of [14]. In this subsection we consider only one source of schemes, namely partial geometries. As for the connections of schemes with buildings, spherical designs and knots we refer to [81,8,71] respectively.

Let P be a non-empty finite set and let L be a non-empty set of P-subsets; the elements of P and L will be called the points and the lines. Suppose that

(1) any two distinct points belong to at most one common line,
(2) there exists an integer $t \geq 1$ such that any point belongs to exactly $t+1$ lines,
(3) there exists an integer $s \geq 1$ such that any line consists of exactly $s+1$ points.

The pair $\mathcal{G} = (P, L)$ is called a *partial geometry* with parameters (s,t,α) where α is a non-negative integer, if

$$|\{(q,m) \in P \times L : \ p \in m, \ q \in l \cap m\}| = \alpha$$

for all $(p,l) \in P \times L$ with $p \notin l$ (see [14, p. 441]). The partial geometries with $\alpha = 1, \alpha \in \{s+1, t+1\}$ and $\alpha = t$ are the generalized quadrangles, the Steiner 2-designs and their duals, and the Bruck nets of order $s+1$ and degree $t+1$ respectively.

For an arbitrary partial geometry $\mathcal{G}$ let us define the following sets of relations on $V = P \cup L$:

$$\mathcal{R}_X = \{\Delta(X), R_X, R'_X\}, \quad X \in \{P, L\},$$
$$\mathcal{R}_{X,Y} = \{I_{X,Y}, I'_{X,Y}\}, \quad \{X, Y\} = \{P, L\}$$

where R_X is the relation consisting of all pairs of non-equal points on a common line for $X = P$ and all pairs of non-equal lines with a common point for $X = L$, $R'_X = (X \times X) \setminus (\Delta(X) \cup R_X)$, and $I_{X,Y}$ and $I'_{X,Y}$ are the incidence and non-incidence relations respectively. It was proved by D. Higman in [46,47] that

$$\mathcal{R} = (\mathcal{R}_P \cup \mathcal{R}_L \cup \mathcal{R}_{P,L} \cup \mathcal{R}_{L,P}) \setminus \{\emptyset\}$$

is the set of basis relations of a scheme on V; we call it the *scheme of the partial geometry* $\mathcal{G}$. This scheme has two homogeneity sets P and L and the corresponding homogeneous components are of rank 2 or 3. Moreover, the schemes of partial geometries $\mathcal{G}$ and $\mathcal{G}'$ are similar if and only if $(s,t,\alpha) = (s',t',\alpha')$. Other examples of schemes can be constructed on flags of generalized polygons [48].

In the case $s = t = \alpha - 1$ the partial geometry $\mathcal{G}$ is a *finite projective plane* of order $q = t$. Then $|P| = |L| = q^2 + q + 1$, $\mathrm{rk}(\mathcal{C}) = 8$ and each of two homogeneous components of $\mathcal{C}$ is of rank 2 where $\mathcal{C}$ is the scheme of $\mathcal{G}$. Moreover, $\mathcal{C}$ has a non-trivial similarity φ of order 2 interchanging $\Delta(P)$ and $\Delta(L)$. Therefore $\{R \cup R^{\varphi} : R \in \mathcal{R}\}$ is the set of basis relations of a homogeneous scheme of rank 4 on the set V. We call this scheme the *homogeneous scheme* of the plane $\mathcal{G}$.

In the case $s+1 = t = \alpha$ the partial geometry $\mathcal{G}$ is a *finite affine plane* of order $q = t$. Then $|P| = q^2$, $|L| = q^2 + q$ and there exist exactly $q + 1$ classes $B_1, \ldots, B_{q+1}$ of pairwise parallel lines with $|B_i| = q$ for all i. The scheme of $\mathcal{G}$ is of rank 9 and its homogeneous component of rank 3 has an equivalence relation with classes B_i's. Let us define one more scheme associated with $\mathcal{G}$. Set $R_0 = \Delta(P)$ and

$$R_i = \{(p_1, p_2) \in P^2 : l(p_1, p_2) \in B_i\}, \quad i = 1, \ldots, q + 1,$$

where $l(p_1, p_2)$ is the line containing p_1 and p_2. Then the pair $(P, \mathcal{R})$ with $\mathcal{R} = \{R_i : i = 0, \ldots, q+1\}$, is a symmetric scheme of rank $q+2$ [39]. The group of similarities of this scheme is isomorphic to the symmetric group $\mathrm{Sym}(q + 1)$.

2.5. Combinatorics

Let P be a finite set with n elements, $1 \le k \le n$, and B a set of k-subsets of P. The elements of P and B will be called points and blocks respectively. The pair (P, B) is called a 2-(n, k, λ) *design*, if any two distinct points belong to λ common blocks. Set

$$V = P \cup B, \qquad C = \{|b \cap b'| : b, b' \in B\}$$

and define the partition $\mathcal{R} = \bigcup_{i,j=1}^{2} \mathcal{R}_{i,j}$ of the set V^2 as follows:

$$\mathcal{R}_{1,1} = \{\Delta(P), P^2 \setminus \Delta(P)\}, \qquad \mathcal{R}_{1,2} = \{R, (P \times B) \setminus R\},$$
$$\mathcal{R}_{2,1} = \{R^{\mathrm{T}}, (B \times P) \setminus R^{\mathrm{T}}\}, \qquad \mathcal{R}_{2,2} = \{R_c : c \in C\}$$

where $R = \{(p, b) \in P \times B : p \in b\}$ and $R_c = \{(b, b') \in B^2 : |b \cap b'| = c\}$. In certain cases the pair $\mathcal{C} = (V, \mathcal{R})$ is a scheme (with two homogeneity sets P and B). For example, this is always true when the design is symmetric ($|C| = 2$) or quasi-symmetric ($|C| = 3$) [46]. It should be noted that some of these designs are partial geometries but any design which is a partial geometry, is a Steiner 2-design (i.e. $\lambda = 1$). Examples of schemes with more than 2 homogeneity sets arise from systems of linked designs introduced and studied in [16]. In fact, it was proved there than any such system produces a scheme.

Under the *scheme* of a graph Γ with vertex set V and edge set E we mean the minimal scheme $\mathcal{C} = \mathcal{C}(\Gamma) = (V, \mathcal{R})$ such that $E \in \mathcal{R}^*$ (as for the partial order on the set of all schemes on V see Section 3.2). One can see that $\mathrm{Aut}(\mathcal{C}) = \mathrm{Aut}(\Gamma)$. The basis relations of $\mathcal{C}$ have especially simple form when the graph Γ is *distance-regular* (see [13]). In this case denote by d the diameter of it and set

$$R_i = \{(u, v) \in V^2 : d(u, v) = i\}, \quad i = 0, \ldots, d,$$

where $d(u, v)$ is the distance between u and v in Γ. Then $R_0 = \Delta(V)$, $R_1 = E$ and

$$\mathcal{R} = \{R_i : i = 0, \ldots, d\}.$$

It follows that the scheme of a distance-regular graph is symmetric and hence commutative. Moreover, the intersection numbers of this scheme are uniquely determined by the numbers $c_{R_1,R_i}^{R_{i-1}}$ and $c_{R_1,R_{i-1}}^{R_i}$ for $i = 1, \ldots, d$, that are called the parameters of Γ.

A *Latin square* of order n is an $n \times n$ matrix containing n copies of each of n symbols, so that no symbol is repeated in any row or column. There are several constructions of schemes related to Latin squares [44]. Here we consider only one of them; another one is based on the 1–1 correspondence between the Latin squares of order n and the Brook nets of order n and degree 3 that were mentioned in Section 2.4. Let A be a Latin square of order $n > 2$. Then the graph (V, E) with

$$V = \{1, \ldots, n\}^2, \quad E = \{(u, v) \in V^2 : u_1 = v_1 \text{ or } u_2 = v_2 \text{ or } A_u = A_v\}$$

is strongly regular, i.e. distance-regular of diameter 2. The corresponding scheme $\mathcal{C}$ of rank 3 is called the *scheme* of A. When A is the multiplication table of a finite group G, the scheme $\mathcal{C}$ is a Cayley scheme over the group $G \times G$. In this case one can prove that the schemes of the Latin squares corresponding to groups G and G' are isomorphic if and only if G is isomorphic to G' (see [1, Theorem 2] and [66, Lemma 3]). On the other hand, one can see that the schemes corresponding to Latin squares of the same order are always similar.

3. Schemes and permutation groups

3.1. Galois correspondence

Given a permutation group $\Gamma \leq \mathrm{Sym}(V)$ set $\mathrm{Orb}_2(\Gamma) = \mathrm{Orb}(\Gamma, V^2)$ where the latter is the set of orbits in the coordinatewise action of Γ on V^2. Then the pair

$$\mathrm{Inv}(\Gamma) = (V, \mathrm{Orb}_2(\Gamma))$$

is a scheme; we call it the *scheme of the group* Γ. One can see that $\Gamma \leq \mathrm{Aut}(\mathcal{C})$ where $\mathcal{C} = \mathrm{Inv}(\Gamma)$. It is also clear that the homogeneity sets of $\mathcal{C}$ coincide with the orbits of Γ; in particular, the scheme $\mathcal{C}$ is homogeneous if and only if the group Γ is transitive. Moreover, $\mathcal{C}$ is primitive (resp. of rank 2) if and only if Γ is primitive (resp. 2-transitive).

The adjacency algebra of the scheme $\mathcal{C}$ is nothing else than the *centralizer algebra* of the permutation group Γ; we denote it by $\mathcal{Z}(\Gamma)$. It is easily seen that

$$\mathcal{Z}(\Gamma) = \{A \in \mathrm{Mat}_V : A^g = A,\ g \in \Gamma\}.$$

If the group Γ is transitive, then this algebra is isomorphic to the *Hecke algebra* of the group Γ by a point stabilizer (the isomorphism takes the basis matrices to the double cosets). Conversely, any Hecke algebra of a finite group Γ by its subgroup Δ can be obtained in the above way from the permutation group induced by the right action of Γ on the set of its left cosets by Δ.

There is a natural partial order $\leq$ on the set of all schemes on V. Namely, given two such schemes $\mathcal{C}$ and $\mathcal{C}'$ we set

$$\mathcal{C} \leq \mathcal{C}' \;\Leftrightarrow\; \mathcal{R}^*(\mathcal{C}) \subset \mathcal{R}^*(\mathcal{C}').$$

In this case $\mathcal{C}'$ is called an *extension* of $\mathcal{C}$.[5] The minimal and maximal elements with respect to that order are the schemes of the symmetric and identical groups on V respectively. The latter scheme contains all binary relations on V and is called *trivial*.

One can see that the mappings

$$\mathcal{C} \mapsto \mathrm{Aut}(\mathcal{C}), \qquad \Gamma \mapsto \mathrm{Inv}(\Gamma) \tag{3}$$

from the set of all schemes on V to the set of all permutation groups on V and conversely, reverse the partial orders on these sets and

$$\mathrm{Inv}(\mathrm{Aut}(\mathcal{C})) \geq \mathcal{C}, \qquad \mathrm{Aut}(\mathrm{Inv}(\Gamma)) \geq \Gamma$$

for all $\mathcal{C}$ and Γ. Therefore these mappings form a Galois correspondence. The closed objects under this correspondence are, respectively, the 2-closed groups and the schurian schemes discussed in Section 4.1.

3.2. Point extensions

It is easily seen that the set of coherent algebras on the same set is closed under intersection. Therefore given two schemes $\mathcal{C}_1$ and $\mathcal{C}_2$ on V there is a uniquely determined scheme $\mathcal{C}_1 \cap \mathcal{C}_2$ on V such that

[5] In the homogeneous case $\mathcal{C}$ is also called a fusion of $\mathcal{C}'$, and $\mathcal{C}'$ a fission of $\mathcal{C}$.

$$\mathcal{R}^*(\mathcal{C}_1 \cap \mathcal{C}_2) = \mathcal{R}^*(\mathcal{C}_1) \cap \mathcal{R}^*(\mathcal{C}_2).$$

This enables us to define the combinatorial analogs of setwise and pointwise stabilizers of permutation groups as follows. Given sets $\mathcal{R}_1, \ldots, \mathcal{R}_s$ of binary relations on V, the scheme

$$[\mathcal{R}_1, \ldots, \mathcal{R}_s] = \bigcap_{\mathcal{C}:\ \mathcal{R} \subset \mathcal{R}^*(\mathcal{C})} \mathcal{C}$$

where $\mathcal{R}$ is the union of all $\mathcal{R}_i$'s, is the smallest scheme on V containing all relations from $\mathcal{R}$. If $\mathcal{R}_i$ coincides with $\mathcal{R}(\mathcal{C}_i)$ for some scheme $\mathcal{C}_i$ on V or with $\{\Delta(X_i)\}$ for some set $X_i \subset V$, then instead of $\mathcal{R}_i$ we write $\mathcal{C}_i$ and X_i respectively.

Given a scheme $\mathcal{C}$ and a set $X \subset V$, the scheme

$$\mathcal{C}_{\{X\}} = [\mathcal{C}, X]$$

is called a *set extension* of $\mathcal{C}$. We have

$$\mathrm{Aut}(\mathcal{C}_{\{X\}}) = \mathrm{Aut}(\mathcal{C})_{\{X\}}$$

where the right-hand side is the setwise stabilizer of the set X in the group $\mathrm{Aut}(\mathcal{C})$. Thus the scheme $\mathcal{C}_{\{X\}}$ can be treated as a combinatorial analog of this setwise stabilizer.

Similarly, for $X = \{v_1, \ldots, v_s\}$ with some of v_i's possibly equal, set

$$\mathcal{C}_{(X)} = [\mathcal{C}, \{v_1\}, \ldots, \{v_s\}]$$

(for the latter scheme we also use notation $\mathcal{C}_{v_1,\ldots,v_s}$). Then

$$\mathrm{Aut}(\mathcal{C}_{(X)}) = \mathrm{Aut}(\mathcal{C})_{(X)}$$

where the right-hand side is the pointwise stabilizer of the set X in the group $\mathrm{Aut}(\mathcal{C})$. The scheme $\mathcal{C}_{(X)}$ can be treated as a combinatorial analog of this pointwise stabilizer. Any such scheme will be called a *point extension* or, more specifically, *s-point extension* of $\mathcal{C}$.

The concepts of set and point extensions of a scheme go back to [78]. However, they were not used intensively in the scheme theory because in the most part of investigations only homogeneous schemes were considered whereas with exception of trivial cases any set or point extension is a non-homogeneous scheme. We observe that a one-point extension $\mathcal{C}_v$ of a homogeneous scheme $\mathcal{C}$ is closely related to its Terwilliger algebra $\mathcal{T}_v$ with respect to the point v [77]. In fact, we have

$$\mathcal{Z}(\mathrm{Aut}(\mathcal{C})_v) \supset \mathcal{A}(\mathcal{C}_v) \supset \mathcal{T}_v \tag{4}$$

with both inclusions not always equalities. It should also be noted that in general the algebra $\mathcal{T}_v$ is not coherent.

The point extension concept enables us to define the *base number* of a scheme which is the combinatorial analog for the base number of a permutation group (i.e. the minimal number of points the pointwise stabilizer of which in this group is trivial).

Definition 3.1. The base number $b(\mathcal{C})$ of a scheme $\mathcal{C}$ is the minimal integer s for which some of its s-point extensions is trivial.

Obviously, $0 \le b(\mathcal{C}) \le n - 1$ where n is the degree of $\mathcal{C}$. Besides, the base number of a scheme is less than or equal to the distinguishing number for it which was used in [3] to estimate the maximal order of a uniprimitive (i.e. primitive but not 2-transitive) permutation group. Thus from the result proved there it immediately follows the statement below.

Theorem 3.2. *Let $\mathcal{C}$ be a primitive scheme of degree n and rank at least 3. Then $b(\mathcal{C}) < 4\sqrt{n}\log n$.*

The upper bound from Theorem 3.2 can be improved to $O(\log n)$ for the schemes of Hadamard matrices [61] and for the schemes of Latin squares [66] of order n. Another upper bound for the base number of a primitive scheme was obtained in [23] by using the natural linear representation invariants of its adjacency algebra.

3.3. Regularity

A special role in the scheme theory play schemes satisfying some regularity conditions. In accordance with [24] a scheme $\mathcal{C}$ on a set V is called *1-regular* if there exists a point $v \in V$ such that

$$|R_{out}(v)| \le 1, \quad R \in \mathcal{R}(\mathcal{C}),$$

where $R_{out}(v) = \{u \in V : (v, u) \in R\}$. Any such point is called a *regular point* of the scheme $\mathcal{C}$. One can see that the set of all regular points is a union of homogeneity sets of $\mathcal{C}$. Besides, the scheme of a permutation group is 1-regular if the base number of it is at most 1, or equivalently if this group has a faithful regular orbit. The class of 1-regular schemes contain all trivial schemes and is closed with respect to extensions and tensor products.

Theorem 3.3 (*[24]*). *Any 1-regular scheme is schurian and separable.*[6]

A scheme is called *semi-regular* if it is 1-regular and the set of all regular points of it coincides with its point set; a homogeneous semi-regular scheme is called *regular*. From Theorem 3.3 it follows that any semi-regular (resp. regular) scheme is the scheme of a semi-regular (resp. regular) permutation group. Moreover, any schurian scheme is a quotient of an appropriate semi-regular scheme.

Corollary 3.4. *The mappings* (3) *define a bijection between 1-regular schemes and permutation groups with base number at most 1. Under this bijection semi-regular (resp. regular) schemes correspond to semi-regular (resp. regular) permutation groups.*

Any 1-regular scheme has a regular homogeneous component (any homogeneity set contained in the set of regular points gives such a component). A scheme is called *quasi-regular* if each of its homogeneous components is regular [25]. As above, one can see that the scheme of a permutation group Γ is quasi-regular if and only if so is Γ. An interesting special class of quasi-regular schemes is the class of *simple spectrum* schemes, i.e. those any irreducible representation of the adjacency algebra of which is of multiplicity one. The characteristic property of a simple spectrum scheme is that any homogeneous component of it is regular and commutative. It was stated in [37] that any simple spectrum scheme is schurian. However, the proof contains a gap and a family of non-schurian simple spectrum schemes all the homogeneity sets of which are of cardinality 4 was found in [26].

4. Schurity and separability

4.1. Schurity problem

One of the most important concepts in the modern scheme theory is that of a schurian scheme defined as follows.

Definition 4.1. A scheme $\mathcal{C}$ is *schurian* if it is the scheme of some permutation group, or equivalently, if $\mathcal{C} = \mathrm{Inv}(\mathrm{Aut}(\mathcal{C}))$.

As we saw above the mappings (3) establish a bijection between the schurian schemes and the 2-closed groups. The simplest examples of schurian schemes are schemes of minimal and maximal rank. Another example is the scheme of conjugacy classes of a group G: indeed, one can see that the 2-closure of the group $\langle G_{left} G_{right} \rangle$ coincides with the automorphism group of the scheme. It is also easily seen that the scheme of a distance-regular graph is schurian if and only if the graph is distance-transitive. This shows, in particular, that most of schemes are non-schurian.

Problem. Given a class $\mathcal{K}$ of schemes identify all schurian schemes in $\mathcal{K}$.

[6] The definition of a separable scheme is given in Section 4.

In general, the schurity problem (even for a class consisting of only one scheme) is quite difficult. For example, let $\mathcal{K}$ be the class of *quasi-thin* schemes: by definition any such scheme is homogeneous and each basis relation of it is of valency at most two [50]. The following statement is one of the oldest results in the scheme theory.

Theorem 4.2 (*[78]*).[7] *Any primitive quasi-thin scheme is schurian.*

We observe that the class $\mathcal{K}$ contains any regular (thin) scheme which is schurian by Theorem 3.3. Therefore, at first it was conjectured that every quasi-thin scheme is schurian. However, then a non-schurian quasi-thin scheme of degree 28 was found (for details see [56]). At present, the schurity problem for $\mathcal{K}$ is far from being completed. Some partial results can be found in [51,70].

Let $\mathcal{K}$ be the class of *circulant* schemes; by definition any scheme in $\mathcal{K}$ is isomorphic to a Cayley scheme over a cyclic group. The schurity problem for $\mathcal{K}$ goes back to I. Schur who had been conjecturing for a long time that every Cayley scheme is schurian, [80, p. 54]; for cyclic groups this statement was known as the Schur–Klin hypothesis. It was confirmed for cyclic groups the order of which is a prime power [73,40] or the product of two distinct primes [57]. Only in 2002 the authors of this paper found that the Schur–Klin hypothesis is false.

Theorem 4.3 (*[27]*). *There exists an infinite family of non-schurian circulant schemes.*

Later it was proved in [24] that any *normal* circulant scheme is schurian (see also [69]). At present the schurity problem for the class $\mathcal{K}$ is open.

There are non-trivial classes of schemes for which the schurity problem is completely solved, e.g. the schemes of algebraic forests[8] and 1-regular schemes are schurian (see [33] and Theorem 3.3 here). The schurity problem in the class of Coxeter schemes was studied in [82] where a sufficient condition for a Coxeter scheme to be schurian was found.

An interesting open problem is to characterize the schurian schemes of partial geometries. Probably, the first step was done in [17] where it was proved that the scheme of a Latin square (or Bruck net of degree 3) of order at least 3 is schurian if and only if it is the multiplication table of an elementary abelian 2-group or a cyclic group of order 3 or 5. Also we have the following result proved in [28].

Theorem 4.4. *The scheme (homogeneous or not) of a projective plane $\mathcal{P}$ is schurian if and only if $\mathcal{P}$ is isomorphic to a Galois plane.*[9]

4.2. Separability problem

It is an old problem in permutation group theory to characterize a permutation group up to isomorphism by its combinatorial invariants, e.g. by subdegrees [49]. A similar problem arises in different parts of combinatorics where one would like to characterize up to isomorphism a combinatorial structure, for instance a design, by its parameters [12]. To deal with problems of such a kind it is convenient to give the following definition [28].

Definition 4.5. A scheme $\mathcal{C}$ is separable with respect to a class $\mathcal{K}$ of schemes if $\mathrm{Iso}(\mathcal{C}, \mathcal{C}', \varphi) \neq \emptyset$ for all similarities $\varphi : \mathcal{C} \to \mathcal{C}'$ where $\mathcal{C}' \in \mathcal{K}$. If $\mathcal{K}$ is the class of all schemes, we say that $\mathcal{C}$ is separable.

[7] In fact, in [78, p. 71,72] it was proved that any primitive quasi-thin scheme is the scheme of a directed or undirected cycle of prime length.

[8] Examples of algebraic forests are trees, interval graphs and cographs.

[9] The projective plane formed by the lines and the planes of a 3-dimensional linear space over a Galois field, is called a *Galois plane*.

Thus any separable scheme is characterized up to isomorphism by the intersection numbers. In this sense Higman's characterization results mentioned above mean that the schemes of certain permutation groups are separable with respect to the class of schurian schemes. As in the schurity case the simplest examples of separable schemes are schemes of minimal and maximal rank. On the other hand, it is easily seen that the scheme of a distance-regular graph is separable if and only if the graph is uniquely determined by its parameters in the sense of [13].

Problem. Given classes $\mathcal{K}_1$ and $\mathcal{K}_2$ of schemes identify all schemes in $\mathcal{K}_1$ that are separable with respect to $\mathcal{K}_2$.

Let $\mathcal{K}_1 = \mathcal{K}_2 = \mathcal{K}$ be the class of schemes any element of which is the scheme of conjugacy classes of a finite group. Then we have the following statement (see Section 2.2).

Theorem 4.6. *A scheme belonging to $\mathcal{K}$ is separable with respect to $\mathcal{K}$ if the underlying group is determined up to isomorphism by its character table.*

Let $\mathcal{K}$ be the class of schemes of distance-regular graphs (resp. partial geometries, designs). Then one can prove that any scheme similar to a scheme in $\mathcal{K}$, also belongs to $\mathcal{K}$. Therefore the separability problem with $\mathcal{K}_1 = \mathcal{K}_2 = \mathcal{K}$ is equivalent to the separability problem with $\mathcal{K}_1 = \mathcal{K}$ and $\mathcal{K}_2$ the class of all schemes. In any case, the solution consists in identifying all distance-regular graphs (resp. partial geometries, designs) which are uniquely determined by its parameters.

Let $\mathcal{K}$ be the class of circulant schemes. An old construction [35, p.75] shows that there exist non-schurian schemes of rank 3 and prime degree that are not in $\mathcal{K}$ but similar to Paley schemes. Since any Paley scheme of prime degree is schurian and circulant, not all schemes in $\mathcal{K}$ are separable. In fact, this statement can be considerably strengthened.

Theorem 4.7 *([27]). There exists an infinite family of circulant schemes that are not separable with respect to $\mathcal{K}$.*

At present the separability problem with $\mathcal{K}_1 = \mathcal{K}_2 = \mathcal{K}$ is open. On the other hand, it was proved in [24] that any normal circulant scheme is separable with respect to $\mathcal{K}$. Thus the separability problem with $\mathcal{K}_1$ being the class of normal schemes belonging to $\mathcal{K}$ and $\mathcal{K}_2 = \mathcal{K}$ is completely solved.

There are non-trivial classes of schemes for which the separability problem is completely solved, e.g. the schemes of algebraic forests and 1-regular schemes are separable (see [33] and Theorem 3.3 here). On the other hand, the separability problem for schemes of partial geometries (or designs) is closely related to the characterization of them up to isomorphism. For instance, in the case of projective planes it is easily seen that the non-homogeneous (resp. homogeneous) schemes of projective planes $\mathcal{P}$ and $\mathcal{P}'$ of order q are always similar, but they are isomorphic if and only if $\mathcal{P}$ is isomorphic to $\mathcal{P}'$ (resp. to $\mathcal{P}'$ or to the plane dual to $\mathcal{P}'$). It is a well-known fact (see [14]) that given a composite prime power q there is a unique projective plane of order q for $q < 9$, and there are at least two non-isomorphic projective planes of order q (one of which is the Galois plane) for $q \geq 9$. This proves the following statement.

Theorem 4.8. *Let q be a composite prime power and $\mathcal{C}$ the (homogeneous or not) scheme of a projective plane of order q. Then $\mathcal{C}$ is separable if and only if $q < 9$.*

When q is prime the separability of the scheme $\mathcal{C}$ is closely related to the open problem on the existence of a non-Galois projective plane of order q.

We complete the section by remarking that the classes of schurian and separable schemes are invariant with respect to direct sums, tensor product and wreath product [18].

5. Higher schurity and higher separability

5.1. Multi-dimensional extensions of a scheme

The key point of the Wielandt method of invariant relations [80] is to study a permutation group $\Gamma \leq \mathrm{Sym}(V)$ by means of the permutation groups $\widehat{\Gamma}^{(m)}$ induced by the coordinatewise action of Γ on

Cartesian m-fold products of V. A realization of this idea for the scheme theory goes back to [78] where a combinatorial analog of the coordinatewise action was introduced under the name of "daughter system". Since then several multi-dimensional constructions have been studied [37,64,75], but in all these cases the resulting objects were not schemes. To avoid this disbalance the authors introduced in [21,26] the concept of m-extension of a scheme. One of the ideas was to find the scheme analog of the following equality

$$\widehat{\Gamma}^{(m)} = (\Gamma^m)_{\{\Delta_m\}}$$

(see Section 3.2) where $\Delta_m = \Delta_m(V)$ is the diagonal of the set V^m and Γ^m is the permutation group induced by the coordinatewise action of the m-fold direct product of Γ on this set.

Let $\mathcal{C}$ be a scheme on V and m a positive integer. Denote by $\mathcal{C}^m$ the m-fold tensor product of $\mathcal{C}$. Set

$$\widehat{\mathcal{C}}^{(m)} = (C^m)_{\{\Delta_m\}}.$$

Thus $\widehat{\mathcal{C}}^{(m)}$ is a scheme on V^m that is a set extension of the scheme $\mathcal{C}^m$.

Definition 5.1. The scheme $\widehat{\mathcal{C}}^{(m)}$ is called the *m-extension* of $\mathcal{C}$.

Clearly, the 1-extension of $\mathcal{C}$ coincides with $\mathcal{C}$. For $m \geq 2$ we have $\Delta_m \neq V^m$ whenever V is not a singleton. Therefore in this case the m-extension is a non-homogeneous scheme. Moreover, the number of its homogeneity sets grows rapidly as m grows. It is easily seen, that any invariant binary relation with respect to the group $\widehat{\Gamma}^{(m)}$ with $\Gamma = \mathrm{Sym}(V)$, is a relation of the scheme $\widehat{\mathcal{C}}^{(m)}$. Moreover,

$$\mathrm{Aut}(\widehat{\mathcal{C}}^{(m)}) = \widehat{\mathrm{Aut}(\mathcal{C})}^{(m)}, \quad \mathrm{Inv}(\widehat{\mathrm{Aut}(\mathcal{C})}^{(m)}) \geq \widehat{\mathcal{C}}^{(m)}.$$

In many cases the latter inclusion is in fact equality, and hence the m-extension is schurian, e.g. this is true for all m whenever $\mathrm{rk}(\mathcal{C}) = 2$ or $\mathcal{C}$ is a regular scheme. It is much more non-trivial to prove that this is also so when $\mathcal{C}$ is a cyclotomic scheme over a field [24]. On the other hand, in [29] the 2-extension of the homogeneous (as well as non-homogeneous) scheme $\mathcal{C}$ of a finite projective plane of order q was found. It turned out that for sufficiently large q the scheme $\widehat{\mathcal{C}}^{(2)}$ is not schurian and its rank does not depend on q. Generally, only the following result holds (Theorems 3.3 and 5.10) and it cannot be substantially improved (Theorem 5.13).

Theorem 5.2. *The m-extension of a scheme on n-points is schurian whenever $m \geq n$.*

Any permutation group $\Gamma \leq \mathrm{Sym}(V)$ is isomorphic (as a permutation group) to the restriction of the group $\widehat{\Gamma}^{(m)}$ to the set Δ_m; the natural isomorphism is induced by the bijection $\delta : v \mapsto (v, \ldots, v)$, $v \in V$. In the scheme case the situation is more complicated. Nevertheless, for a scheme $\mathcal{C}$ on V, Δ_m is a union of the homogeneity sets of its m-extension $\widehat{\mathcal{C}}^{(m)}$. Therefore one can define a scheme

$$\overline{\mathcal{C}}^{(m)} = ((\widehat{\mathcal{C}}^{(m)})_{\Delta_m})^{\delta^{-1}}$$

on V which is the translation of the scheme $(\widehat{\mathcal{C}}^{(m)})_{\Delta_m}$ along the bijection δ^{-1}. In other words any basis relation of $\overline{\mathcal{C}}^{(m)}$ is of the form

$$R^{\delta^{-1}} = \{(u, v) \in V^2 : (u^\delta, v^\delta) \in R\}$$

where R is a basis relation of $\widehat{\mathcal{C}}^{(m)}$ contained in $(\Delta_m)^2$. The scheme $\overline{\mathcal{C}}^{(m)}$ is called the *m-closure* of $\mathcal{C}$. One can prove (Theorem 5.11) that

$$\mathcal{C} \leq \overline{\mathcal{C}}^{(m)} \leq \overline{\mathcal{C}}^{(\infty)} \tag{5}$$

where $\overline{\mathcal{C}}^{(\infty)} = \mathrm{Inv}(\mathrm{Aut}(\mathcal{C}))$ is the schurian closure of $\mathcal{C}$.

Definition 5.3. A scheme $\mathcal{C}$ is called m-closed if $\mathcal{C} = \overline{\mathcal{C}}^{(m)}$.

Clearly, $\overline{\mathcal{C}}^{(1)} = \mathcal{C}$; thus any scheme is 1-closed. However, not all schemes are 2-closed. The minimal homogeneous scheme which is not 2-closed is the non-symmetric scheme of degree 15 and rank 3 (see [43]). On the other hand, any schurian scheme is m-closed for all m (see (5)). However, not each m-closed scheme is schurian, for $m = 2$ this follows from Theorems 4.4 and 5.4 below.

Theorem 5.4 (*[29]*). *The homogeneous and non-homogeneous schemes of any projective plane are 2-closed.*

5.2. *Stable partitions*

It seems reasonable to compare the concept of m-extension with multi-dimensional constructions from [78,75] (concerning the construction from [37] we refer to [21]). Despite the fact that formally none of them is a scheme, each of them produces a stable partition of the set V^m in the sense of the following definition proposed in [26] (a similar notion was introduced in unpublished preprint [54]).

Definition 5.5. A partition Π of a set V^M with $M = \{1, \ldots, m\}$ is stable if the following conditions are satisfied:

(P1) given $L \subset M$ the diagonal $\Delta(V^L)$ is a union of the elements from $\pi_L(\Pi)$,
(P2) Π is invariant with respect to the group $\mathrm{Sym}(M)$,
(P3) given $T \in \Pi, L \subset M$ and $S \in \pi_L(\Pi)$ the number $|\pi_L^{-1}(u) \cap T|$ does not depend on $u \in S$

where $\pi_L : V^M \to V^L$ is a natural projection and $\pi_L(\Pi) = \{\pi_L(T) : T \in \Pi\}$.

The comparison with the definition of a scheme shows that the projections to V^2 of stable partitions of V^3 are in 1–1 correspondence with the schemes on V. Besides, given a group $\Gamma \le \mathrm{Sym}(V)$ the elements of the set $\mathrm{Orb}_m(\Gamma) = \mathrm{Orb}(\widehat{\Gamma}^{(m)})$ form a stable partition of V^m for all m.

A superscheme defined in [75] is a compatible family $\{\Pi_m\}_{m=1}^{\infty}$ where Π_m is a stable partition of V^m, such that $\mathcal{C} = (V, \Pi_2)$ is a homogeneous scheme. It was proved there that

$$\Pi_m = \mathrm{Orb}_m(\Gamma)$$

for all m where $\Gamma = \mathrm{Aut}(\mathcal{C})$. Thus this approach can be applied only to schurian schemes $\mathcal{C}$. On the other hand, given a scheme $\mathcal{C}$ denote respectively by $\Pi_m(\mathcal{C})$ and $\mathcal{R}_m(\mathcal{C})$ the partitions of the sets V^m and V^{2m} into the homogeneity sets and the basis relations of the m-extension of $\mathcal{C}$. It was proved in [26] that these partitions are stable. Moreover, it was shown there that the m-dim Weisfeiler–Leman method [78,15] applied to the scheme $\mathcal{C}$ leads to a natural stable partition of V^m; we denote it by $\mathrm{WL}_m(\mathcal{C})$.

Theorem 5.6. *Given a scheme $\mathcal{C}$ and a positive integer m the following statements hold:*

$$\mathrm{WL}_m(\mathcal{C}) \le \Pi_m(\mathcal{C}), \qquad \mathcal{R}_m(\mathcal{C}) \le \pi_{2m}(\mathrm{WL}_{3m}(\mathcal{C}))$$

where $\le$ denotes the natural partial order on the set of partitions of a set.

One can see that the m-extension has rather reach structure. For example, any permutation of coordinates induces an isomorphism of this scheme. The adjacency algebra of it is closed with respect to some convolutions two of which are the ordinary and Hadamard multiplications. It would be interesting to describe all convolutions with respect to which the adjacency algebra is invariant.

5.3. *Multi-dimensional extensions of a similarity*

The m-extension gives a powerful tool to study automorphisms of a scheme. To study similarities of schemes the m-extension of a similarity was introduced in [26]. The theories of multi-dimensional extensions of similarities and schemes can be developed in parallel.

Let $\varphi : \mathcal{C} \to \mathcal{C}'$ be a similarity. Denote by φ^m the m-fold tensor power of φ, i.e. the similarity from $\mathcal{C}^m$ to $(\mathcal{C}')^m$ induced by φ.

Definition 5.7. A similarity $\psi : \widehat{\mathcal{C}}^{(m)} \to \widehat{\mathcal{C}}'^{(m)}$ is called an *m-extension* of φ if the following conditions are satisfied:

(1) $(\Delta^{(m)})^{\psi} = (\Delta')^{(m)}$,
(2) $R^{\psi} = R^{\varphi^m}$ for all $R \in \mathcal{R}(\mathcal{C}^m)$.

It is easily seen that the m-extension of φ is uniquely determined; it is denoted by $\widehat{\varphi}^{(m)}$. Clearly, $\widehat{\varphi}^{(1)} = \varphi$ for all φ. However, for $m \ge 2$ not each similarity has m-extension. For example, a computation shows that the similarity of the homogeneous non-symmetric scheme of degree 15 and rank 3 that is induced by transposition has no 2-extension.

Definition 5.8. A similarity is called m-similarity if it has m-extension.

The set of all m-similarities from $\mathcal{C}$ to $\mathcal{C}'$ is denoted by $\mathrm{Sim}_m(\mathcal{C},\mathcal{C}')$; clearly, $\mathrm{Sim}_1(\mathcal{C},\mathcal{C}') = \mathrm{Sim}(\mathcal{C},\mathcal{C}')$. The above example shows that a similarity is not necessarily an m-similarity even for $m = 2$. On the other hand, for any positive integer m and any isomorphism f from $\mathcal{C}$ to $\mathcal{C}'$ the similarity φ_f (see Section 2.1) has m-extension; it coincides with $\varphi_{\widehat{f}}$ where $\widehat{f}$ is the isomorphism from $\widehat{\mathcal{C}}^{(m)}$ to $\widehat{\mathcal{C}}'^{(m)}$ induced by f. Therefore

$$\mathrm{Sim}_\infty(\mathcal{C},\mathcal{C}') \subset \mathrm{Sim}_m(\mathcal{C},\mathcal{C}') \subset \mathrm{Sim}(\mathcal{C},\mathcal{C}')$$

where $\mathrm{Sim}_\infty(\mathcal{C},\mathcal{C}') = \{\varphi_f : f \in \mathrm{Iso}(\mathcal{C},\mathcal{C}')\}$. It follows that any similarity induced by an isomorphism is an m-similarity for all m. However, there exist m-similarities not induced by isomorphism, for $m = 2$ this follows from Theorems 4.8 and 5.9 below.

Theorem 5.9 ([29]). *Any similarity between the homogeneous (or non-homogeneous) schemes of projective planes is a 2-similarity.*

5.4. Schurity and separability numbers

The following statement shows that for a sufficiently large m the m-extension of any scheme contains the scheme of a regular action of its automorphism group. Thus asymptotically the theory of m-extensions reduces to permutation group theory.

Theorem 5.10 ([24]). *Let $\mathcal{C}$ be a scheme and $m \geq 1$. Suppose that some of the $(m-1)$-point extensions of $\mathcal{C}$ is 1-regular. Then the scheme $\widehat{\mathcal{C}}^{(m)}$ is also 1-regular.*

We note that the assumption of Theorem 5.10 is not restrictive in the sense that such an m always exists, e.g. the degree of $\mathcal{C}$ will do. In fact, one can take even $m = b(\mathcal{C})+1$. However, always $m \geq b(\mathcal{C})$.

From Theorems 3.3 and 5.10 it follows that the scheme $\widehat{\mathcal{C}}^{(m)}$ is schurian and separable for any m satisfying the assumption of the latter theorem. This implies that the scheme $\overline{\mathcal{C}}^{(m)}$ is schurian and that any m-similarity from $\mathcal{C}$ to another scheme is induced by isomorphism. Using these facts one can prove the following important result [28].

Theorem 5.11. *Given schemes $\mathcal{C}$ and $\mathcal{C}'$ of degree n we have*

$$\mathcal{C} = \overline{\mathcal{C}}^{(1)} \leq \cdots \leq \overline{\mathcal{C}}^{(n)} = \cdots = \overline{\mathcal{C}}^{(\infty)}, \tag{6}$$

$$\mathrm{Sim}(\mathcal{C},\mathcal{C}') = \mathrm{Sim}_1(\mathcal{C},\mathcal{C}') \supset \cdots \supset \mathrm{Sim}_n(\mathcal{C},\mathcal{C}') = \cdots = \mathrm{Sim}_\infty(\mathcal{C},\mathcal{C}'). \tag{7}$$

This theorem shows that the larger an integer m is, the more an m-closed scheme and an m-similarity look like a schurian scheme and a similarity induced by isomorphism respectively. In fact, some non-trivial facts from permutation group theory can be generalized even to 2-closed schemes (for details see [23]).

Definition 5.12 ([28]). A scheme $\mathcal{C}$ is called *m-schurian* if $\overline{\mathcal{C}}^{(m)} = \overline{\mathcal{C}}^{(\infty)}$, it is called *m-separable* if $\mathrm{Sim}_m(\mathcal{C},\mathcal{C}') = \mathrm{Sim}_\infty(\mathcal{C},\mathcal{C}')$ for all schemes $\mathcal{C}'$.

From (6) and (7) it follows that the property of a scheme to be m-schurian (or m-separable) is preserved as m grows. Moreover, any scheme of degree n is n-schurian and n-separable. Set

$$t(\mathcal{C}) = \min\{m : \mathcal{C} \text{ is } m\text{-schurian}\}, \qquad s(\mathcal{C}) = \min\{m : \mathcal{C} \text{ is } m\text{-separable}\}.$$

These numbers are called the *schurity number* and the *separability number* of the scheme $\mathcal{C}$. From Theorem 5.11 it follows that

$$1 \leq t(\mathcal{C}) \leq n, \qquad 1 \leq s(\mathcal{C}) \leq n$$

for all schemes $\mathcal{C}$. Obviously, $t(\mathcal{C}) = 1$ (resp. $s(\mathcal{C}) = 1$) if and only if the scheme $\mathcal{C}$ is schurian (resp. separable). It is more interesting that the upper bounds are asymptotically optimal [26,18].

Theorem 5.13. *There exist schemes with arbitrarily large schurity and separability numbers. Moreover,*

$$\limsup_{n(\mathcal{C})\to\infty} \frac{t(\mathcal{C})}{n(\mathcal{C})} > 0, \qquad \limsup_{n(\mathcal{C})\to\infty} \frac{s(\mathcal{C})}{n(\mathcal{C})} > 0,$$

where $\mathcal{C}$ runs over the class of all schemes and $n(\mathcal{C})$ is the degree of $\mathcal{C}$. Both inequalities remain true in the case when $\mathcal{C}$ runs over the class of all homogeneous schemes, and for the second inequality even schurian homogeneous schemes.

Generally, given a scheme it is difficult to find the exact values of its schurity and separability numbers. On the other hand, for direct sums and tensor and wreath products the problem is reduced to the same problem for operands [26,28,18]. The following result proved in [28] connects these numbers with the corresponding numbers of certain extensions.

Theorem 5.14. *Let $\mathcal{C}$ be a scheme on V. Then*

(1) $s(\mathcal{C}) \le s(\mathcal{C}_v) + 1$ *for all* $v \in V$,
(2) *if* $\mathcal{C}_v$ *is* $t(\mathcal{C}_v)$*-separable for some point* $v \in V$, *then* $t(\mathcal{C}) \le t(\mathcal{C}_v) + 1$,
(3) $s(\mathcal{C}) \le m\, s(\widehat{\mathcal{C}}^{(m)})$, $t(\mathcal{C}) \le m\, t(\widehat{\mathcal{C}}^{(m)})$ *for all* $m \ge 1$.

From Theorems 3.3 and 5.10 and statement (3) of Theorem 5.14 we obtain the first statement of the theorem below. The second statement follows from the first one because the existence of an s-point extension of a scheme $\mathcal{C}$ implies that $b(\mathcal{C}) \le s + 1$.

Theorem 5.15. *Let $\mathcal{C}$ be a scheme. Then*

(1) $t(\mathcal{C}) \le m$ *and* $s(\mathcal{C}) \le m$ *whenever some of the* $(m-1)$*-point extensions of* $\mathcal{C}$ *is 1-regular,*
(2) $t(\mathcal{C}) \le b(\mathcal{C}) + 1$ *and* $s(\mathcal{C}) \le b(\mathcal{C}) + 1$.

We observe that for the schemes which were used to prove Theorem 5.13, the upper bounds from statement (2) of Theorem 5.15 are asymptotically optimal. On the other hand, for a scheme $\mathcal{C}$ of rank 2 and degree n we have $t(\mathcal{C}) = s(\mathcal{C}) = 1$, whereas $b(\mathcal{C}) = n - 1$.

The developed theory enables us to obtain non-trivial upper bounds for schurity and separability numbers in certain classes of schemes. For example, for a primitive scheme one can use Theorem 3.2 and statement (2) of Theorem 5.15 to prove the following result.

Corollary 5.16. *Let $\mathcal{C}$ be a primitive non-rank 2 scheme of degree n. Then $t(\mathcal{C}) < 4\sqrt{n}\log n + 1$ and $s(\mathcal{C}) < 4\sqrt{n}\log n + 1$.*

Other examples are considered below.

5.5. Explicit upper bounds

In this subsection we study the schurity and separability numbers of schemes from several well-known classes. In most cases these schemes are schurian, i.e. the schurity number of any of them equals one. Therefore more attention will be paid to the separability problem.

Let $\mathcal{C}$ be a scheme. Below by saying that the *intersection numbers of $\mathcal{C}$ and another scheme $\mathcal{C}'$ are the same* we mean that a similarity

$$\varphi : \mathcal{C} \to \mathcal{C}'$$

is given. Thus the scheme $\mathcal{C}$ is characterized by the intersection numbers if and only if $s(\mathcal{C}) = 1$. This look at the problem of characterization of schemes is adequate to the point of view adopted in book [13]. Next, we could call the intersection numbers of the scheme $\widehat{\mathcal{C}}^{(m)}$ the *m-dim intersection numbers* of $\mathcal{C}$. Then it is natural to say that the *m-dim intersection numbers of $\mathcal{C}$ and $\mathcal{C}'$ are the same* if the intersection numbers of $\mathcal{C}$ and $\mathcal{C}'$ are the same and the corresponding similarity φ has an m-extension, i.e.

$$\varphi \in \mathrm{Sim}_m(\mathcal{C}, \mathcal{C}').$$

Thus $\mathcal{C}$ is characterized by the m-dim intersection numbers if and only if $s(\mathcal{C}) \le m$.

The following statement proved in [28] shows that the schemes of distance-regular graphs with classical parameters are characterized by the 2-dim intersection numbers.

Theorem 5.17. *Let $\mathcal{C}$ be either the scheme of a distance-regular graph with parameters of the Johnson or Hamming graph, or the Grassmann scheme. Then $t(\mathcal{C}) \le 2$ and $s(\mathcal{C}) \le 2$.*

The proof of this theorem is based on the well-known characterizations of distance-regular graphs with classical parameters cited in book [13]. In fact, if $\mathcal{C}$ is the Johnson, Hamming or Grassmann scheme, then obviously $t(\mathcal{C}) = 1$. Moreover, in the first two cases $s(\mathcal{C}) = 1$ if and only if $\mathcal{C}$ is not the scheme of a Chang or Doob graph for which the both numbers equal 2. It would be interesting to generalize Theorem 5.17 to the scheme of a distance-regular graph with parameters of the Grassmann graph, by using the characterization of the Grassmann graph given in [65].

Let $\mathcal{C}$ be the homogeneous or non-homogeneous scheme of a finite projective plane of order q. The following rough upper bound for the schurity and separability numbers of $\mathcal{C}$ was proved in [28]:

$$t(\mathcal{C}) \le 5 + \log_2 \log_2 q, \qquad s(\mathcal{C}) \le 5 + \log_2 \log_2 q.$$

As we saw in Section 4 (Theorems 4.8 and 4.1) in most cases $t(\mathcal{C}) > 1$ and $s(\mathcal{C}) > 1$. In [29] the 2-extension of $\mathcal{C}$ was explicitly found and as a consequence the following unexpected result was proved.

Theorem 5.18. *Let $\mathcal{C}$ be the homogeneous or non-homogeneous scheme of a finite projective plane $\mathcal{P}$. Then $t(\mathcal{C}) \ne 2$ and $s(\mathcal{C}) \ne 2$. Moreover, if $\mathcal{P}$ is a Galois plane, then $s(\mathcal{C}) \le 3$.*

Let $\mathcal{C}$ be a cyclotomic scheme over a field $\mathbb{F}$. Then obviously $t(\mathcal{C}) = 1$. Moreover, it was proved in [63] that

$$\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{F}) \tag{8}$$

whenever $\mathrm{rk}(\mathcal{C}) > 2$. On the other hand, in contrast to many classical schemes the intersection numbers of a cyclotomic scheme do not characterize it up to isomorphism. For example, there is a lot of pairwise non-isomorphic schemes arising from the conference and Hadamard matrices having the same intersection numbers as Paley schemes which are exactly cyclotomic schemes of rank 3.

Since any scheme of rank 2 is separable, the following theorem together with inclusion (8) shows that any cyclotomic scheme is characterized by its 3-dim intersection numbers.

Theorem 5.19 (*[24]*). *Let $\mathcal{C}$ be a cyclotomic scheme. Then $s(\mathcal{C})$ does not exceed the base number of the group* $\mathrm{Aut}(\mathcal{C})$. *In particular, $s(\mathcal{C}) \le 3$.*

The proof of Theorem 5.19 is based on the fact that a one-point extension of a normal Cayley scheme over a cyclic group is 1-regular. This implies, in particular, that any point extension (as well as any multi-dimensional extension) of a cyclotomic scheme $\mathcal{C}$ is schurian. It follows that the first of inclusions (4) is in fact the equality $\mathcal{Z}(\mathrm{Aut}(\mathcal{C})_v) = \mathcal{A}(\mathcal{C}_v)$. On the other hand, as it was observed in [53] the question whether or not the Terwilliger algebra $\mathcal{T}_v$ coincides with $\mathcal{Z}(\mathrm{Aut}(\mathcal{C})_v)$ is reduced to a difficult number theoretical problem.

Any cyclotomic scheme is 3/2-*homogeneous* which means that it is homogeneous and all its non-reflexive basis relations have the same cardinality. It is easily seen that the scheme of a non-regular permutation group is 3/2-homogeneous if and only if the group is 3/2-transitive. It is known that any imprimitive 3/2-transitive group is a Frobenius group [72, Theorem 8.1], and hence the base number of its one-point stabilizer is 1. A combinatorial analog of this statement is that any one-point extension of an imprimitive 3/2-homogeneous scheme is 1-regular [23]. By Theorem 5.15 this implies the following result.

Theorem 5.20 (*[28]*). *If $\mathcal{C}$ is an imprimitive* 3/2-*homogeneous scheme, then $t(\mathcal{C}) \le 2$ and $s(\mathcal{C}) \le 2$.*

There is a lot of schemes satisfying the assumption of Theorem 5.20. Apart from imprimitive regular schemes, these include, in particular, the schemes of finite affine planes defined in Section 2.4 and the schemes of imprimitive Frobenius groups. It should be noted that the latter are just those non-regular imprimitive 3/2-homogeneous schemes $\mathcal{C}$ for which $t(\mathcal{C}) = 1$.

6. Schemes and computation

6.1. Enumeration of schemes

The most part of computational problems concerning schemes can be attributed to one of two big topics: computer-aided computations and the design of algorithms efficient from the theoretical point of view. The first topic is the subject of this subsection. In the other subsections we give some ideas how to apply schemes in the computational complexity theory.

The enumeration problem is to construct the complete list of explicitly given pairwise non-isomorphic schemes in a given class. One of the first results of this type appeared in [59] where all schemes on at most 7 points were enumerated. Since then a lot of results have been obtained for special classes of schemes mostly arising from certain combinatorial objects like distance-regular graphs [13] or incidence graphs of block designs [12]. At present, the most complete list of homogeneous schemes of small degree can be found in [43]. This list shows that the smallest degree of a non-schurian homogeneous scheme equals 15; in the non-homogeneous case the corresponding number is unknown.

At present there are two special packages for computations with schemes. The first of them called COCO (COherent COnfigurations) was designed for arbitrary schemes of rank at most 256 [36]. The second one works mostly with homogeneous schemes of any rank and is implemented as a package of the computer system GAP [42].

We complete the subsection by mentioning one of the basic tools in computing with schemes. It is the Weisfeiler–Leman polynomial-time algorithm for finding the basis relations of the smallest scheme containing a given family of binary relations [79,78]. The first efficient implementation of it can be found in [5].

Theorem 6.1. *Given a family $\mathcal{R}$ of binary relations on a set V the set of basis relations of the scheme $[\mathcal{R}]$ can be found in time $O(mn^2 \log n + n^3 \log n)$ where $m = |\mathcal{R}|$ and $n = |V|$.*

Two other efficient implementations of the Weisfeiler–Leman algorithm as well as some comparison results can be found in [10,6].

6.2. Graph isomorphism

Two graphs are called isomorphic if there is a bijection of their vertex sets preserving the adjacency of vertices.

Graph Isomorphism Problem (ISO). Given two graphs test whether or not they are isomorphic.

At present the ISO is one of the most famous problem of the computational complexity theory for which neither NP-completeness is proved, nor a polynomial-time algorithm is known. In fact, the running time of the best general isomorphism test is moderately exponential and the proof of this estimate is based on the classification of finite simple groups. A more detailed discussion of the topic can be found in [4].

As we said in Section 1 there is a relationship between schemes and the ISO [78]. In the modern language the idea is as follows. Let Γ and Γ' be graphs with vertex sets V and V', and edge sets E and E' respectively. Then any isomorphism of them induces a similarity[10]

$$\varphi : \mathcal{C}(\Gamma) \to \mathcal{C}(\Gamma'), \qquad E^{\varphi} = E' \tag{9}$$

where $\mathcal{C}(\Gamma)$ and $\mathcal{C}(\Gamma')$ are the schemes of the graphs Γ and Γ' (see Section 2.5). On the other hand, with the help of the Weisfeiler–Leman algorithm one can easily test whether such a similarity φ exists. Thus the ISO is reduced to the following problem.

[10] This similarity does not depend on the choice of the isomorphism.

Problem. Given a similarity $\varphi : \mathcal{C} \to \mathcal{C}'$ test whether or not $\varphi \in \mathrm{Sim}_\infty(\mathcal{C}, \mathcal{C}')$.

Obviously, this problem becomes trivial whenever the scheme $\mathcal{C}$ (or $\mathcal{C}'$) is separable, because in this case any $\varphi \in \mathrm{Sim}(\mathcal{C}, \mathcal{C}')$ is induced by an isomorphism.

The direct application of the above approach solves the isomorphism problem for algebraic forests defined in [33]. This class of graphs includes trees, interval graphs, cographs, directed path graphs, etc. As it was mentioned in Section 4.2 the scheme of an algebraic forest is separable. Thus by Theorem 6.1 we obtain the following result.

Theorem 6.2. *The isomorphism of two n-vertex algebraic forests can be tested in time* $O(n^3 \log n)$.

For an integer $m \geq 1$ denote by $\mathcal{K}_m$ the class of all graphs Γ such that $s(\mathcal{C}) \leq m$ where $\mathcal{C} = \mathcal{C}(\Gamma)$. As we saw above for $m = 1$ the isomorphism of n-vertex graphs $\Gamma, \Gamma' \in \mathcal{K}_m$ can be tested within time polynomial in n. In the general case, for these graphs we have

$$\mathrm{Sim}_m(\mathcal{C}, \mathcal{C}') = \mathrm{Sim}_\infty(\mathcal{C}, \mathcal{C}')$$

where $\mathcal{C} = \mathcal{C}(\Gamma)$ and $\mathcal{C}' = \mathcal{C}(\Gamma')$. Therefore to test isomorphism of them it suffices to check whether similarity (9) exists and if so whether it has the m-extension

$$\widehat{\varphi}^{(m)} : \widehat{\mathcal{C}}^{(m)} \to \widehat{\mathcal{C}}'^{(m)}.$$

Since the degrees of the schemes $\widehat{\mathcal{C}}^{(m)}$ and $\widehat{\mathcal{C}}'^{(m)}$ equal n^m, this can be done in time $n^{O(m)}$ by the Weisfeiler–Leman algorithm.

Theorem 6.3. *The isomorphism of two n-vertex graphs from* $\mathcal{K}_m$ *can be tested in time* $n^{O(m)}$.

Bearing in mind Theorem 6.3 it would be interesting to find natural classes of graphs contained in the class $\mathcal{K}_m$ for a fixed m. Of a special interest are graphs with bounded multiplicity of spectra, graphs of bounded genus and graphs of bounded degree [4]. In the first two cases some results from [23, 41] can be useful. For instance, in the former paper it was in fact proved that any graph Γ with the multiplicity of spectra bounded by m is contained in $\mathcal{K}_{m+1}$ whenever the scheme of Γ is primitive.

The discussed technique is not a unique way to use the scheme theory for designing efficient graph isomorphism tests. For example, the combinatorial part of algorithms from papers [30,31] is based on the analysis of primitive schemes arising in the reduction process. Another example is the isomorphism test for strongly regular graphs from [76] the key point of which is the use of Neumaier's claw bound. Finally, the scheme theory is the essential part of the polynomial-time isomorphism tests for circulant graphs proposed independently in [67,32]; the former one is discussed in [69], this issue, whereas the second is the subject of the next subsection.

6.3. Circulants

A finite graph (or a scheme) is said to be *circulant* if its automorphism group contains a full cycle, i.e., a permutation the cycle decomposition of which consists of a unique cycle of full length. Certainly, a circulant scheme is isomorphic to a Cayley scheme over a cyclic group.

It is an old problem to recognize whether or not a given graph Γ is circulant, and if so to construct a full cycle in $\mathrm{Aut}(\Gamma)$. In fact, for circulant graphs the ISO is polynomial-time reducible to the recognition problem, because two circulant graphs with the same number of vertices are isomorphic if and only if their disjoint union is a circulant graph. Here, the isomorphism can also be easily found (if it exists), e.g. for connected graphs any full cycle of the automorphism group of the disjoint union produces an isomorphism between them.

Theorem 6.4 ([32]). *The recognition and isomorphism problems for circulant graphs can be solved in time* $n^{O(1)}$ *where n is the number of vertices of input graphs.*

The main difficulty in proving Theorem 6.4 is to control the set of full cycles in a permutation group. In this connection the following notion is useful.

Definition 6.5. A cycle base of a finite permutation group G is a subset of G consisting of full cycles such that any full cycle of G is conjugate in G to exactly one element of this set.

Cycle bases were studied in [68] where it was proved that the cardinality of any cycle base of the group G is at most n (and even $\varphi(n)$ with φ the Euler function assuming the classification of finite simple groups) where n is the degree of G. We note that given a cycle base of the automorphism group of an n-vertex graph, one can explicitly construct a full system of pairwise non-equivalent Cayley representations of it over a given cyclic group of order n [32].

Let Γ be a graph and $\mathcal{C} = \mathcal{C}(\Gamma)$. Then obviously Γ is a circulant graph if and only if a cycle base of the group $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{C})$ is non-empty. Thus a polynomial-time solution to the recognition problem for circulant graphs is the direct consequence of the following result, where under a cycle base of a scheme we mean a cycle base of its automorphism group.

Theorem 6.6 (*[32]*). *A cycle base of a scheme on n points can be found in time $n^{O(1)}$.*

Let us briefly discuss the idea of the proof of Theorem 6.6. The theory of circulant schemes developed in [32] shows that given a scheme $\mathcal{C}$ we have the following alternative: either the group $\mathrm{Aut}(\mathcal{C})$ is solvable, or there exists a scheme $\mathcal{C}' > \mathcal{C}$ such that at least one cycle base of $\mathcal{C}'$ is that of $\mathcal{C}$. Moreover, this alternative is resolved in polynomial time: the group $\mathrm{Aut}(\mathcal{C})$ in the former case and the scheme $\mathcal{C}'$ in the latter one can be found in time $n^{O(1)}$ where n is the degree of $\mathcal{C}$. This reduces the problem of finding a cycle base of $\mathcal{C}$ to that of finding a cycle base of a solvable permutation group. However, the latter problem can be efficiently solved by means of standard algorithms in computational permutation group theory.

6.4. Factorization of polynomials

The factorization problem for a polynomial over a finite field was intensively studied in computational complexity theory (see papers [19,52,60] where polynomial-time algorithms for special classes of polynomials were constructed). However, only two strong enough results for the factorization of an arbitrary degree n polynomial over a field of order $q = p^m$ with p prime were known:

- the Berlekamp algorithm [11] of complexity $(nmp)^{O(1)}$,
- the Rónyai algorithm [74] of complexity $(n^n m \log p)^{O(1)}$ (under the *Generalized Riemann Hypothesis*[11]).

A substantial progress in the factorization problem was made in [20] where the following theorem was proved.

Theorem 6.7. *Under the Generalized Riemann Hypothesis the irreducible factors of a degree n polynomial over an explicitly given finite field of order q can be found in time $(n^{\log n} \log q)^{O(1)}$.*

A careful analysis of the algorithm of Theorem 6.7 revealed unexpected deep connections between the factorization of polynomials and the theory of multi-dimensional extensions of schemes (see Section 5). The key point here is the notion of *odd* scheme.

Definition 6.8. A scheme is called odd if the cardinality of any of its basis relations is odd.

It immediately follows from the definition that a homogeneous scheme is odd if and only if the degrees of it and of all of its basis relations are odd. One can prove that the class of odd schemes is closed with respect to taking extensions and factors as well as direct sums and tensor and wreath products [18]. Moreover, the automorphism group of an odd scheme is of odd cardinality and hence

[11] This hypothesis states that the L-series of an algebraic number field K with the Dirichlet character χ has no zeros in the right half-plane $\mathrm{Re}(s) > 1/2$ for all K and χ [58].

is solvable by the Feit–Thompson theorem. (It is interesting to note that the latter theorem can be reformulated in the scheme theory language as follows: any odd regular scheme of composite degree has a non-trivial equivalence relation the adjacency matrix of which belongs to the adjacency algebra of the scheme).

For a positive integer n denote by $\mathcal{K}_n$ the class of all schemes $\mathcal{C}$ of degree n such that $\mathcal{C} \geq \mathcal{C}'$ for some primitive odd scheme $\mathcal{C}'$. Set

$$t_n = \max_{\mathcal{C}\in\mathcal{K}_n} t(\mathcal{C}).$$

Theorem 6.9 (*[18]*). *Under the Generalized Riemann Hypothesis the irreducible factors of a degree n polynomial over an explicitly given finite field of order q can be found in time $(n^{t_n}\log q)^{O(1)}$.*

By Theorems 3.2 and 5.15 we have $t_n < 4\sqrt{n}\log n + 1$. Getting a stronger upper bound for the number t_n (based on deeper investigations of primitive odd schemes) could lead to an improvement of the running time estimate for the factorization algorithm.

Acknowledgements

The first author's work was partially supported by RFFI Grants 07-01-00485 and 06-01-00471 and the second author's work was partially supported by RFFI Grants 07-01-00485, 08-01-00379 and 08-01-00640.

References

[1] A.A. Albert, Quasigroups. I, Trans. Amer. Math. Soc. 54 (3) (1943) 507–519.

[2] Z. Arad, E. Fisman, M. Muzychuk, Generalized table algebras, Israel J. Math. 114 (1999) 29–60.

[3] L. Babai, On the order of uniprimitive permutation groups, Ann. Math. 113 (1981) 553–568.

[4] L. Babai, Automorphism groups, isomorphism, reconstruction, in: Handbook Of Combinatorics, vol. 2, Elsevier Science, 1995, pp. 1447–1541.

[5] L. Babel, Computing coherent configurations, Technische Universität München, TUM-M0204, März 2002.

[6] L. Babel, I.V. Chuvaeva, M. Klin, D.V. Pasechnik, Algebraic combinatorics in mathematical chemistry II. Program implementation of the Weisfeiler–Leman algorithm, Technische Universität München, TUM-M9701, Januar 1997.

[7] J. Bagherian, I. Ponomarenko, A. Rahnamai Barghi, On cyclotomic schemes over finite near-fields, J. Algebraic Combin. 27 (2008) 173–185.

[8] E. Bannai, E. Bannai, A survey on spherical designs and algebraic combinatorics on spheres, this volume.

[9] E. Bannai, T. Ito, Algebraic combinatorics. I, Benjamin/Cummings, Menlo Park, CA, 1984.

[10] O. Bastert, New ideas for canonically computing graph algebras, Technische Universität München, TUM-M9803, Juni 1998.

[11] E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. 24 (1970) 713–735.

[12] T. Beth, D. Jungnickel, H. Dieter, Design theory, in: Encyclopedia of Mathematics and Its Applications, 69, Cambridge University Press, Cambridge, 1999.

[13] A.E. Brouwer, A.M. Cohen, A. Neumaier, Distance-regular graphs, in: Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 3. Folge, 18. Berlin etc., 1989.

[14] F. Buekenhout (Ed.), Handbook of incidence geometry, in: Buildings and foundations, North-Holland, Amsterdam, 1995.

[15] J.Y. Cai, M. Fürer, N. Immerman, An optimal lower bound on the number of variables for graph identification, Combinatorica 12 (1992) 389–410.

[16] P.J. Cameron, On groups with several doubly-transitive permutation representations, Math. Z. 128 (1972) 1–14.

[17] H. Enomoto, Strongly regular graphs and finite permutation groups of rank 3, J. Math. Kyoto Univ. 11 (1971) 381–397.

[18] S. Evdokimov, Schurity and separability of association schemes, Thesis (2004) (in Russian).

[19] S.A. Evdokimov, Factorization of a solvable polynomial over finite fields and the generalized Riemann hypothesis, Zapiski Nauchnykh Seminarov POMI 176 (1989) 104–117. (Prepublication in 1986). English translation: J. Soviet Math. 59 (3) (1992) 842–849.

[20] S. Evdokimov, Factorization of polynomials over finite fields in subexponential time under GRH, in: Algorithmic number theory (Ithaca, NY, 1994), in: Lecture Notes in Comput. Sci., 877, Springer, Berlin, 1994, pp. 209–219.

[21] S. Evdokimov, M. Karpinski, I. Ponomarenko, On a new high dimensional Weisfeiler–Leman algorithm, J. Algebraic Combin. 10 (1999) 29–45.

[22] S. Evdokimov, I. Ponomarenko, Normal cyclotomic schemes over a finite commutative ring, Algebra and Analysis 19 (2007) 59–85. English translation: St. Petersburg Math. J. 19 (2008), 911-929.

[23] S. Evdokimov, I. Ponomarenko, On primitive cellular algebras, Zapiski Nauchnykh Seminarov POMI 256 (1999) 38–68. English translation: J. Math. Sci., New York, 107 (5) (2001) 4172–4191.

[24] S. Evdokimov, I. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, Algebra and Analysis 14 (2) (2002) 11–55. English translation: St. Petersburg Math. J. 14 (2) (2003) 189–221.

[25] S. Evdokimov, I. Ponomarenko, Two inequalities for the parameters of a cellular algebra, Zapiski Nauchnykh Seminarov POMI 240 (1997) 82–95. English translation: J. Math. Sci., New York 96 (5) (1999) 3496-3504.

[26] S. Evdokimov, I. Ponomarenko, On highly closed cellular algebras and highly closed isomorphisms, European. J. Combin. 6 (1999) #R18.

[27] S. Evdokimov, I. Ponomarenko, On a family of Schur rings over a finite cyclic group, Algebra and Analysis 13 (3) (2001) 139–154. English translation: St. Petersburg Math. J. 13 (3) (2002) 441–451.

[28] S. Evdokimov, I. Ponomarenko, Separability number and schurity number of coherent configurations, Electron. J. Combin. 7 (2000) #R31.

[29] S. Evdokimov, I. Ponomarenko, Schemes of a finite projective plane and their extensions, accepted in Algebra and Analysis, (2008). PDMI Preprint, 14 (2007), 1–34.

[30] S. Evdokimov, I. Ponomarenko, On the geometric graph isomorphism problem, J. Pure Appl. Algebra 117–118 (1997) 253–276.

[31] S. Evdokimov, I. Ponomarenko, Isomorphism of coloured graphs with slowly increasing multiplicity of Jordan blocks, Combinatorica 19 (1999) 321–333.

[32] S. Evdokimov, I. Ponomarenko, Recognizing and isomorphism testing circulant graphs in polynomial time, Algebra and Analysis 15 (6) (2003) 1–34. English translation: St. Petersburg Math. J. 15 (6) (2004) 813–835.

[33] S. Evdokimov, I. Ponomarenko, G. Tinhofer, Forestal algebras and algebraic forests (on a new class of weakly compact graphs), Discrete Math. 225 (2000) 149–172.

[34] S.A. Evdokimov, I.N. Ponomarenko, A.M. Vershik, Algebras in Plancherel duality and algebraic combinatorics, Funct. Anal. Appl. 31 (4) (1997) 34–46.

[35] I.A. Faradžev, M.H. Klin, M.E. Muzychuk, Cellular rings and groups of automorphisms of graphs, in: I.A. Faradžev (Ed.), Investigations In Algebraic Theory Of Combinatorial Objects, Kluwer Acad. Publ, Dordrecht, 1994, pp. 1–152.

[36] I.A. Faradžev, M.H. Klin, Computer package for computations with coherent configurations, Proc. Conf. ISSAC-91. Bonn, July 1991.

[37] S. Friedland, Coherent algebras and the graph isomorphism problem, Discrete Appl. Math. 25 (1989) 73–98.

[38] R.W. Goldbach, H.L. Claasen, Cyclotomic schemes over finite rings, Indag. Math. (N.S.) 3 (1992) 301–312.

[39] J.Y. Gol'fand, M.H. Klin, Amorphic cellular rings I, in: Investigations in Algebraic Theory of Combinatorial Objects, VNIISI, Institute for System Studies, Moscow, 1985, pp. 32–38 (in Russian).

[40] Y.Y. Gol'fand, M.H. Klin, N.L. Naimark, The structure of S-rings over $\mathbb{Z}_{2^m}$, XVI All Union Algebraic Conference, Part 2, (Leningrad 1981), LOMI, 1981, 195–196 (in Russian).

[41] M. Grohe, Isomorphism testing for embeddable graphs through definability, Proc. of the 32nd ACM Ann. Symp. on Theory of Computing, 2000, 63–72.

[42] A. Hanaki, Elementary functions for association schemes on GAP, 2007 http://kissme.shinshu-u.ac.jp/as/gap/association_scheme.pdf.

[43] A. Hanaki, I. Miyamoto, Classification of association schemes with small vertices, published on web http://kissme.shinshu-u.ac.jp/as/.

[44] A. Heinze, M. Klin, Loops, Latin Squares and Strongly Regular Graphs: An algorithmic approach via Algebraic Combinatorics, 2008.

[45] D.G. Higman, Coherent configurations 1, Rend. Mat. Sem. Padova 44 (1970) 1–25.

[46] D.G. Higman, Coherent algebras, Linear Algebra Appl. 93 (1987) 209–239.

[47] D.G. Higman, Strongly regular designs and coherent configurations of type $\begin{bmatrix}3 & 2\\ & 3\end{bmatrix}$, European J. Combin. 9 (1988) 411–422.

[48] D.G. Higman, Invariant relations, coherent configurations and generalized polygons, in: Combinatorics (Proc. Advanced Study Inst., Breukelen, 1974), Part 3: Combinatorial group theory, in: Math. Centre Tracts, 57, Math. Centrum, Amsterdam, 1974, pp. 27–43.

[49] D.G. Higman, Characterization of families of rank 3 permutation groups by the subdegree I, II, Arch. Math. 21 (1970) 151–156. 353–361.

[50] M. Hirasaka, On quasi-thin association schemes with odd number of points, J. Algebra 240 (2001) 665–679.

[51] M. Hirasaka, M. Muzychuk, On quasi-thin association schemes, J. Combin. Theory A98 (2002) 17–32.

[52] M.-D.A. Huang, Riemann hypothesis and finding roots over finite fields, Proc. 17th ACM Symp. on Theory of Computing (STOC) New York, (1985), 121–130.

[53] H. Ishibashi, T. Ito, M. Yamada, Terwilliger algebras of cyclotomic schemes and jacobi sums, European J. Combin. 20 (1999) 397–410.

[54] G. Ivanyos, On the combinatorics of Evdokimov's deterministic factorization method, Draft preprint, 1997.

[55] M.Kh. Klin, The axiomatics of cellular rings, Investigations in the algebraic theory of combinatorial objects, 6–32, Vsesoyuz. Nauchno-Issled. Inst. Sistem. Issled., Moscow, 1985 (in Russian).

[56] M. Klin, M. Muzychuk, C. Pech, A. Woldar, P.-H. Zieschang, Association schemes on 28 points as mergings of a half-homogeneous coherent configurations, European J. C. 28 (2007) 1994–2025.

[57] M.Kh. Klin, R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings, in: Algebraic Methods in Graph Theory. vol. 1, 2 (Szeged, 1978), in: Colloq. Math. Soc. János Bolyai, 25, North-Holland, Amsterdam, New York, 1981, pp. 405–434.

[58] J.C. Lagarias, H.L. Montgomery, A.M. Odlyzko, A bound for the least prime ideal in the Chebotarev density theorem, Invent. Math. 54 (1979) 271–296.

[59] A.A Leman, On automorphisms of certain classes of graphs, Avtomat. Telemeh. 2 (1970) 75–82. English translation: Automat. Remote Control (1970) 235–242.

[60] H.W. Lenstra Jr., Finding isomorphisms between finite fields, Math. Comp. 56 (1991) 329–347.

[61] J.S. Leon, An algorithm for computing the automorphism group of a hadamard matrix, J. Combin. Theory A27 (1979) 289–306.

[62] R. Lidl, H. Niedereiter, Introduction To Finite Fields And Their Applications, Cambridge University Press, 1986.

[63] R. McConnel, Pseudo-ordered polynomials over a finite field, Acta Arith. 8 (1963) 127–151.

[64] D.M. Mesner, P. Bhattacharya, Association schemes on triples and a ternary algebra, J. Combin. Theory A55 (1990) 204–234.

[65] K. Metsch, A characterization of grassmann graphs, European J. Combin. 16 (1995) 639–644.

[66] G.L. Miller, On the $n^{\log n}$ isomorphism technique, The 10th Annual ACM Symposium on the Theory of Computing, 1978, 51–58.

[67] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, Proc. London Math. Soc. 88 (2004) 1–41.

[68] M. Muzychuk, On the isomorphism problem for cyclic combinatorial objects, Discrete Math. 197–198 (1999) 589–606.

[69] M. Muzychuk, I. Ponomarenko, Schur rings, European J. Combin., in this issue (doi:10.1016/j.ejc.2008.11.006).

[70] M. Muzychuk, P.-H. Zieschang, On association schemes all elements of which have valency 1 or 2, Discrete Math 308 (2008) 3097–3103.

[71] K. Nomura, Spin models and bose-mesner algebras, European J. Combin. 20 (1999) 691–700.

[72] D. Passman, Permutation Groups, W. A. Benjamin, Inc., New York, Amsterdam, 1968.

[73] P. Pöschel, Untersuchungen von S-ringen insbesondere im gruppenring von p-gruppen, Math. Nachr. 60 (1974) 1–27.

[74] L. Rónyai, Factoring polynomials over finite fields, Proc. 28th IEEE Symp. on Foundations of Computer Science (FOCS) New York, (1987), 132–137.

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

[76] D. Spielman, Faster isomorphism testing of strongly regular graphs, in: Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing, 1996, Philadelphia, PA, ACM, New York, 1996, pp. 576–584.

[77] P. Terwilliger, The subconstituent algebra of an association scheme, J. Algebraic Combin. 1 (Part I) (1992) 363–388. (Part II) 2 (1993), 73–103; (Part III) 2 (1993), 177–210.

[78] B. Weisfeiler (Ed.), On construction and identification of graphs, in: Lecture Notes in Math. 558, 1976.

[79] B.Ju. Weisfeiler, A.A. Leman, Reduction of a graph to a canonical form and an algebra which appears in the process, NTI, Ser.2 9 (1968) 12–16.

[80] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lect. Notes Dept. Math. Ohio St. Univ., Columbus, 1969.

[81] P.-H. Zieschang, Homogeneous coherent configurations as generalized groups and their relationship to buildings, J. Algebra 178 (1995) 677–709.

[82] P.-H. Zieschang, The exchange condition for association schemes, Israel J. Math. 151 (2006) 357–380.