Записки научных
семинаров ПОМИ
Том 402, 2012 г.

I. N. Ponomarenko

BASES OF SCHURIAN ANTISYMMETRIC COHERENT CONFIGURATIONS AND ISOMORPHISM TEST FOR SCHURIAN TOURNAMENTS

Abstract. It is known that for any permutation group G of odd order there exists a subset of the permuted set whose stabilizer in G is trivial, and if G is primitive, then there also exists a base of size at most 3. These results are generalized to the coherent configuration of G, that is in this case schurian and antisymmetric. This enables us to construct a polynomial-time algorithm for recognizing and isomorphism testing of schurian tournaments (i.e., arc colored tournaments the coherent configurations of which are schurian).

§1. Introduction

Let $\mathcal{X}$ be a coherent configuration (as for a background of coherent configurations see Sec. 2 and [10]). A *base* of $\mathcal{X}$ is a point set Δ such that the smallest fission of $\mathcal{X}$ in which all points of Δ are fibers, is the complete coherent configuration. The minimal size of Δ is called the *base number* of $\mathcal{X}$ and is denoted by $b(\mathcal{X})$. It is easily seen that $0 \le b(\mathcal{X}) \le n-1$ where n is the degree of $\mathcal{X}$. Besides, if $b(G)$ is the smallest size of a base[1] of a permutation group G, then

$$b(G) \le b(\mathrm{Inv}(G)), \tag{1}$$

where $\mathrm{Inv}(G)$ is the coherent configuration associated with G. Even a weaker upper bound for $b(G)$ was used in [5] to estimate the maximal order of uniprimitive group. As a consequence of Theorem 0.2 of that paper one can obtain that the base number of a nontrivial primitive coherent configuration of degree n is less than $4\sqrt{n}\log n$.

The equality in (1) is obviously attained when the group G is trivial or symmetric. A nontrivial example of the equality was found in [2] for G

Key words and phrases: Coherent configuration, linear group, wreath product, the Weisfeiler–Leman algorithm.

The work was partially supported by RFFI Grant 11-01-00760-a.

[1]A base of a permutation group is a set of permuted points whose pointwise stabilizer is trivial.

being the automorphism group of a cyclotomic scheme over finite field. On the other hand, in general, inequality (1) is strict even for solvable groups: if G is a solvable 2-transitive group of degree n, then $b(G) \leq 4$ by [19], but in this case $\mathrm{Inv}(G)$ is trivial, and hence $b(\mathrm{Inv}(G)) = n - 1$. In contrast to this example we prove here the following theorem.

Theorem 1.1. *Let G be a primitive permutation group of odd order. Then the base number of the coherent configuration* $\mathrm{Inv}(G)$ *is at most* 3.

As an immediate consequence of inequality (1) and Theorem 1.1 we deduce that the base number of a primitive permutation group of odd order is at most 3 (this result have been earlier proved in [13]). In proving Theorem 1.1 we also get a generalization of the Gluck theorem that in any odd order permutation group the stabilizer of some subset of the permuted set is trivial [15]. Namely, a *generalized base* of a coherent configuration $\mathcal{X}$ on Ω is a set $\Pi \subset 2^\Omega$ such that the smallest fission of $\mathcal{X}$ in which any element of Π is a union of some fibers of $\mathcal{X}$, is the complete coherent configuration. The minimal size of the set Π is called the *generalized base number* of $\mathcal{X}$ and is denoted by $gb(\mathcal{X})$. Again, it is easily seen that

$$gb(G) \leq gb(\mathrm{Inv}(G)) \tag{2}$$

where $gb(G)$ is the minimal size of the set Π for which the intersection of all stabilizers $G_{\{\Delta\}}$, $\Delta \in \Pi$, is trivial.

Theorem 1.2. *Let G be a permutation group of odd order. Then the generalized base number of the coherent configuration* $\mathrm{Inv}(G)$ *is at most* 1.

A coherent configuration $\mathcal{X}$ is called *schurian* if there exists a permutation group G such that $\mathcal{X} = \mathrm{Inv}(G)$. Over all coherent configurations schurian ones are relatively rare in occurence. For example, for infinitely many positive integers n there are exponentially many antisymmetric coherent configuration of rank 3 and degree n; on the other hand, such a configuration is schurian if and only if it arises from the Payley tournament on n vertices. In this paper we apply Theorem 1.1 to get the following result.

Theorem 1.3. *Given an antisymmetric coherent configuration $\mathcal{X}$ on n points one can test in time $n^{O(1)}$ whether $\mathcal{X}$ is schurian, and (if so) find the group* $\mathrm{Aut}(\mathcal{X})$.

Antisymmetric coherent configurations are closely related with tournaments (we recall that tournament is a directed graph in which any two

distinct vertices are joined by a unique arc). Indeed, one can easily see that if (Ω, S) is such a configuration and A is a maximal subset of S such that $A \cap A^* = \varnothing$, then the union of relations in A is the arc set of a tournament on Ω. Conversely, the coherent configuration obtained from an arc colored tournament T by means of the Weisfeiler–Leman algorithm[2] is antisymmetric. When this configuration is schurian, we say that the tournament T is *schurian*. In particular, this is always the case when the color classes of arcs are the orbits in the natural action of the group $\mathrm{Aut}(T)$ on pairs of vertices.

Let us turn to the tournament isomorphism problem. It is a special case of the Graph Isomorphism Problem that consists in finding an efficient algorithm to test whether or not two given (arc colored) tournaments are isomorphic. At present, the best result here is the algorithm from [6] testing the isomorphism of two n-vertex tournaments in time $n^{O(\log n)}$ (see also [4]). In this paper we prove the following result.

Theorem 1.4. *Let $\mathcal{T}_n$ be the class of all schurian tournaments on n vertices. Then the following problems can be solved in time $n^{O(1)}$:*

(1) *given a tournament T on n vertices, test whether $T \in \mathcal{T}_n$,*
(2) *given a tournament $T \in \mathcal{T}_n$ find the group $\mathrm{Aut}(T)$,*
(3) *given tournaments $T_1, T_2 \in \mathcal{T}_n$ find a set $\mathrm{Iso}(T_1, T_2)$.*

The proof of Theorem 1.4 is based on Theorem 1.3. In the special case when $\mathcal{X} = \mathrm{Inv}(G)$ for an odd order group G, the group $\mathrm{Aut}(\mathcal{X})$ is by definition the 2-closure of G. Thus our algorithm, in particular, constructs in polynomial time the 2-closure of any odd order permutation group, that generalizes the main result in [9].

For the reader convenience we collect the basic facts on coherent configurations, their bases and linear primitive solvable groups in Sections 2, 3 and 4 respectively. In Sections 5, 6 and 7 we prove some upper bounds for the numbers $b(\mathcal{X})$ and $gb(\mathcal{X})$ when $\mathcal{X}$ is the wreath product or the exponentiation of coherent configurations. In Section 8 we give a sufficient condition for a homogeneous schurian coherent configuration to have a base of size at most 2. This condition is used in Section 9 where we prove that the equality in (1) is attained when G is an affine linear group with irreducible zero stabilizer (Theorem 9.1). Finally, the proofs of Theorems 1.1, 1.2 and 1.4 are given in Section 10.

[2]This algorithm was given in detail in [23]; see also Subsection 2.8.

Notation. Throughout the paper Ω denotes a finite set. The diagonal of the Cartesian product Ω^2 is denoted by 1_Ω.

For $r \subset \Omega^2$ set $r^* = \{(\beta, \alpha) : \ (\alpha, \beta) \in r\}$. For $\Gamma, \Delta \subset \Omega$ set $r_{\Gamma,\Delta} = r \cap (\Gamma \times \Delta)$ and $r_\Gamma = r_{\Gamma,\Gamma}$.

For any $\alpha \in \Omega$ set $1_\alpha = 1_{\{\alpha\}}$ and $\alpha r = \{\beta \in \Omega : \ (\alpha, \beta) \in r\}$.

For $r, s \subset \Omega^2$ set $r \cdot s = \{(\alpha, \beta) \in \Omega^2 : \ (\alpha, \gamma) \in r, \ (\gamma, \beta) \in s \text{ for some } \gamma \in \Omega\}$, and set $r \otimes s = \{(\alpha, \beta) \in \Omega^2 \times \Omega^2 : \ (\alpha_1, \beta_1) \in r \text{ and } (\alpha_2, \beta_2) \in s\}$ where $(\alpha_1, \alpha_2) = \alpha$ and $(\beta_1, \beta_2) = \beta$.

For $S \in 2^{\Omega^2}$ denote by $S^\cup$ the set of all unions of the elements of S, and set $S^* = \{s^* : \ s \in S\}$ and $\alpha S = \bigcup\limits_{s \in S} \alpha s$. For $T \in 2^{\Omega^2}$ set $S \cdot T = \{s \cdot t : \ s \in S, \ t \in T\}$.

For a permutation g set $\mathrm{fix}(g)$ to be the number of points that g leaves fixed. For a set K of permutations set $\mathrm{fix}(K) = \max_g \mathrm{fix}(g)$ and $\mathrm{Fix}(K) = \sum_g \mathrm{fix}(g)$ where g runs over the set $K^\# = K \setminus \{1\}$.

§2. Coherent configurations

Unfortunately up to now there is no commonly used terminology and notations in the coherent configuration theory. In this paper we follow ones from [10] and [24]. All the facts presented below can be found in one of these sources.

2.1. Definitions. A pair $\mathcal{X} = (\Omega, S)$ where Ω is a finite set and S a partition of Ω^2, is called a *coherent configuration* on Ω if $1_\Omega \in S^\cup$, $S^* = S$, and given $r, s, t \in S$, the number

$$c_{rs}^t = |\alpha r \cap \beta s^*|$$

does not depend on the choice of $(\alpha, \beta) \in t$. The elements of Ω, S, $S^\cup$ and the numbers c_{rs}^t are called the *points*, the *basic relations*, the *relations* and the *intersection numbers* of $\mathcal{X}$, respectively. For the intersection numbers the following equalities hold:

$$c_{r^*s^*}^{t^*} = c_{sr}^t \quad \text{and} \quad |t| c_{rs}^{t^*} = |r| c_{st}^{r^*} = |s| c_{tr}^{s^*}, \qquad r, s, t \in S. \tag{3}$$

The numbers $|\Omega|$ and $|S|$ are called the *degree* and the *rank* of $\mathcal{X}$. A unique basic relation containing a pair $(\alpha, \beta) \in \Omega^2$ is denoted by $r_\mathcal{X}(\alpha, \beta)$ or $r(\alpha, \beta)$. The set of basic relations contained in $r \cdot s$ with $r, s \in S^\cup$ is denoted by rs.

2.2. Fibers and homogeneity. The point set Ω is a disjoint union of *fibers* which are the elements of the set

$$\Phi(\mathcal{X}) = \{\Gamma \subset \Omega : \ 1_\Gamma \in S\}.$$

Given a union Γ of fibers we denote by S_Γ the set of all nonempty relations r_Γ with $r \in S$. Then $\mathcal{X}_\Gamma = (\Gamma, S_\Gamma)$ is a coherent configuration, called the *restriction* of $\mathcal{X}$ to Γ.

For any basic relation $r \in S$ there exist uniquely determined fibers Γ and Δ such that $r \subset \Gamma \times \Delta$. Set $t = 1_\Gamma$. Then the number $|\gamma r| = c^t_{rr^*}$ does not depend on the point $\gamma \in \Gamma$. It is called the *valency* of r and denoted n_r. The maximum of all valences is denoted by n_{max}.

The coherent configuration $\mathcal{X}$ is called *homogeneous* or a *scheme* if $1_\Omega \in S$. In this case $n_r = n_{r^*}$ and $|r| = nn_r$ for all $r \in S$ where $n = |\Omega|$. Thus equalities in (3) may be rewritten as follows:

$$c^{t^*}_{r^*s^*} = c^t_{sr} \quad \text{and} \quad n_t c^{t^*}_{rs} = n_r c^{r^*}_{st} = n_s c^{s^*}_{tr}. \tag{4}$$

2.3. Equivalence relations. We define the *support* of a relation $r \subset \Omega^2$ to be the minimal set $\Gamma \subset \Omega$ such that $r \subset \Gamma^2$. Saying that $e \in S^\cup$ is an equivalence relation we mean that e is an equivalence relation on its support; the set of classes of e is denoted by Ω/e. According to [11, Subsection 3.2] any such e is a union of uniform equivalence relations[3] belonging to $S^\cup$ and having pairwise disjoint supports. This implies the following statement to be used in the proof of Corollary 5.2.

Lemma 2.1. *Let $\mathcal{X}$ be a coherent configuration on Ω, $e \in S^\cup$ an equivalence relation and $I \subset \Omega/e$. Suppose that no two classes of e, one in I and another one not in I, have the same size. Then the union of the classes from I belongs to the set $\Phi(\mathcal{X})^\cup$.*

Any coherent configuration has *trivial* equivalence relations in $S^\cup$: 1_Ω and Ω^2. A homogeneous coherent configuration is called *primitive* if there are no other equivalence relations in $S^\cup$; otherwise it is called *imprimitive*.

Let $e \in S^\cup$ be an equivalence relation. Then given $\Gamma \in \Omega/e$ one can construct the *restriction* of $\mathcal{X}$ to Γ that is the coherent configuration

$$\mathcal{X}_\Gamma = (\Gamma, S_\Gamma)$$

[3]An equivalence relation is uniform if all its classes have the same size.

with S_Γ as in Subsection 2.2. The *quotient* of $\mathcal{X}$ modulo e is defined to be the coherent configuration

$$\mathcal{X}_{\Omega/e} = (\Omega/e, S_{\Omega/e})$$

where $S_{\Omega/e}$ is the set of all nonempty relations of the form $\{(\Gamma,\Delta) : s_{\Gamma,\Delta} \neq \varnothing\}$ with $s \in S$.

2.4. Fissions and fusions. There is a natural partial order $\leq$ on the set of all coherent configurations on Ω. Namely, given two coherent configurations $\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega, S')$ we set

$$\mathcal{X} \leq \mathcal{X}' \;\Leftrightarrow\; S^\cup \subset (S')^\cup.$$

In this case $\mathcal{X}$ and $\mathcal{X}'$ are called respectively a *fusion* of $\mathcal{X}'$ and a *fission* of $\mathcal{X}$. This order is preserved under taking the restriction to a set and the quotient modulo an equivalence relation. The minimal and maximal elements with respect to that order are the *trivial* and the *complete* coherent configurations on Ω: the basic relations of the former one are the reflexive relation 1_Ω and (if $n > 1$) its complement in Ω^2, whereas the relations of the latter one are all binary relations on Ω.

Given two coherent configurations $\mathcal{X}_1$ and $\mathcal{X}_2$ on Ω there is a uniquely determined coherent configuration $\mathcal{X}_1 \cap \mathcal{X}_2$ also on Ω, the relation set of which is $(S_1)^\cup \cap (S_2)^\cup$ where S_i is the set of basic relations of $\mathcal{X}_i$, $i = 1, 2$. This enables us to define the smallest fission of a coherent configuration $\mathcal{X}$ on Ω containing a given set $\mathcal{S}$ of binary relations on Ω as follows:

$$\mathrm{Fis}(\mathcal{X}, \mathcal{S}) = \bigcap_{\mathcal{Y}:\ \mathcal{S} \subset T^\cup} \mathcal{Y}$$

where $\mathcal{Y} = (\Omega, T)$ is a coherent configuration. In what follows we will omit $\mathcal{X}$ when it is the trivial coherent configuration. Besides, for $\Pi \subset 2^\Omega$ and $\Gamma \subset \Omega$ we define respectively the Π-*fission* and Γ-*fission* of $\mathcal{X}$ by

$$\mathrm{Fis}(\mathcal{X}, \Pi) = \mathrm{Fis}(\mathcal{X}, \mathcal{S}_\Pi) \quad \text{and} \quad \mathrm{Fis}(\mathcal{X}, \Gamma) = \mathrm{Fis}(\mathcal{X}, \Pi_\Gamma),$$

where $\mathcal{S}_\Pi = \{1_\Delta : \Delta \in \Pi\}$ and $\Pi_\Gamma = \{\{\gamma\} : \gamma \in \Gamma\}$. Sometimes we will also write $\mathcal{X}_{\alpha,\beta,\ldots}$ instead of $\mathrm{Fis}(\mathcal{X}, \{\alpha, \beta, \ldots\})$. One can see that any set in $\Pi^\cup$ is a union of fibers of the Π-fission of $\mathcal{X}$. The following lemma immediately follows from the definitions.

Lemma 2.2. *Let $\mathcal{X} = (\Omega, S)$ be a coherent configuration and $\alpha \in \Omega$. Then for all $r, s, t \in S$ we have*

$$\alpha r \in (\Phi_\alpha)^\cup \quad \textit{and} \quad t_{\alpha r, \alpha s} \in (S_\alpha)^\cup$$

where Φ_α and S_α are the sets of fibers and basic relations of the coherent configuration $\mathcal{X}_\alpha$. Moreover, $|\beta t_{\alpha r,\alpha s}| = c^s_{rt}$ for all $\beta \in \alpha r$.

2.5. Isomorphisms and schurity. Two coherent configurations $\mathcal{X}_1$ and $\mathcal{X}_2$ are called *isomorphic* if there exists a bijection between their point sets that induces a bijection between their sets of basic relations. Such a bijection is called an *isomorphism* between $\mathcal{X}_1$ and $\mathcal{X}_2$; the set of all of them is denoted by $\mathrm{Iso}(\mathcal{X}_1, \mathcal{X}_2)$.

The group of all isomorphisms of a coherent configuration $\mathcal{X} = (\Omega, S)$ to itself contains a normal subgroup

$$\mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : \ s^f = s, \ s \in S\}$$

called the *automorphism group* of $\mathcal{X}$ where $s^f = \{(\alpha^f, \beta^f) : \ (\alpha, \beta) \in s\}$. Coversely, let G be a permutation group on Ω and S be the set of orbits of the componentwise action of G on Ω^2. Then $\mathrm{Inv}(G) := (\Omega, S)$ is a coherent configuration; it is called the *coherent configuration of* G. This coherent configuration is homogeneous if and only if the group G is transitive. One can also see that

$$\mathcal{X} \le \mathcal{X}' \ \Rightarrow \ \mathrm{Aut}(X) \ge \mathrm{Aut}(\mathcal{X}') \quad \text{and} \quad G \le G' \ \Rightarrow \mathrm{Inv}(G) \ge \mathrm{Inv}(G').$$

A coherent configuration $\mathcal{X}$ is called *schurian* if $\mathcal{X} = \mathrm{Inv}(G)$ for some permutation group G. In this case the group G can be always replaced by $\mathrm{Aut}(\mathcal{X})$. Moreover, the schurity of $\mathcal{X}$ implies the schurity of all its restrictions and quotients. An important example of a schurian scheme is a *cyclotomic scheme* over a finite field $\mathbb{F}$; in this case G is an affine[4] subgroup of $\mathrm{AGL}(1, \mathbb{F})$. In this paper we also deal with the scheme of a primitive solvable group. The structure of such a group is given in the following statement proved in [21, Section 4].

Theorem 2.3. *Let $G \le \mathrm{Sym}(\Omega)$ be a primitive solvable permutation group. Then $|\Omega| = p^d$ for a prime p and integer $d \ge 1$. Moreover the set Ω can be identified with a linear space of dimension d over field of order p so that*

$$G \le \mathrm{AGL}(d, p) \quad \textit{and} \quad K \le \mathrm{GL}(d, p)$$

where K is the stabilizer of zero point in G; the group G is affine and the group K is irreducible.

[4]In what follows saying that G is an affine (sub)group we mean that G contains all the translations of the underlying linear space.

2.6. Algebraic isomorphisms. Let $\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega', S')$ be coherent configurations. A bijection $\varphi : S \to S'$, $r \mapsto r'$ is called an *algebraic isomorphism* from $\mathcal{X}$ to $\mathcal{X}'$ if

$$c_{rs}^t = c_{r's'}^{t'}, \qquad r, s, t \in S; \tag{5}$$

we say that $\mathcal{X}$ and $\mathcal{X}'$ are *algebraically isomorphic*. In this case they have the same degree and rank. Moreover, φ induces a bijection from $S^\cup$ onto $(S')^\cup$ such that

$$(r \cup s)^\varphi = r^\varphi \cup s^\varphi, \qquad r, s \in S.$$

This bijection preserves reflexive and equivalence relations. In particular, we can define a bijection from $\Phi(\mathcal{X})^\cup$ onto $\Phi(\mathcal{X}')^\cup$ so that $(1_\Gamma)^\varphi = 1_{\Gamma^\varphi}$. Finally, given a set $\Gamma \in \Phi(\mathcal{X})^\cup$ and an equivalence relation $e \in S^\cup$ we have the induced algebraic isomorphisms

$$\varphi_\Gamma : \mathcal{X}_\Gamma \to \mathcal{X}'_{\Gamma'} \quad \text{and} \quad \varphi_{\Omega/e} : \mathcal{X}_{\Omega/e} \to \mathcal{X}'_{\Omega'/e'}$$

where $\Gamma' = \Gamma^\varphi$ and $e' = e^\varphi$.

Any isomorphism $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ induces an algebraic isomorphism $r \mapsto r^f$ from $\mathcal{X}$ to $\mathcal{X}'$. The set of all isomorphisms inducing the algebraic isomorphism φ is denoted by $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$. Clearly,

$$\mathrm{Iso}(\mathcal{X}, \mathcal{X}, \mathrm{id}_S) = \mathrm{Aut}(\mathcal{X})$$

where id_S is the identity on S. Let us give another example of algebraic isomorphism. Suppose that the scheme $\mathcal{X}$ is imprimitive and $e \in S^\cup$ an equivalence relation. Then given any two sets $\Gamma, \Gamma' \in \Omega/e$ the mapping

$$\varphi_{\Gamma,\Gamma'} : \mathcal{X}_\Gamma \to \mathcal{X}_{\Gamma'}, \ s_\Gamma \to s_{\Gamma'} \tag{6}$$

is an algebraic isomorphism (here s runs over the set of all basic relations of $\mathcal{X}$ that are contained in e).

2.7. Antisymmetric and 1-regular coherent configurations. A coherent configuration $\mathcal{X}$ is called *antisymmetric* if

$$s \in S \quad \text{and} \quad s = s^* \quad \Rightarrow \quad s \subset 1_\Omega,$$

or equivalently if the cardinality of any basic relation of $\mathcal{X}$ is an odd number. The latter condition implies that the valences of $\mathcal{X}$ are odd and that the coherent configuration $\mathrm{Inv}(G)$ is antisymmetric if and only if G is the group of odd order. One can prove that the class of antisymmetric coherent configurations is closed with respect to taking fissions, restrictions and quotients. In particular, the automorphism group of antisymmetric coherent configuration has odd order.

A coherent configuration $\mathcal{X}$ is called 1-*regular* if it has a *regular* point; by definition a point $\alpha \in \Omega$ is regular in $\mathcal{X}$, if

$$r \in S \ \Rightarrow \ |\alpha r| \le 1. \tag{7}$$

The set Γ of all regular points is a union of fibers and any basic relation of the coherent configuration $\mathcal{X}_\Gamma$ has valency 1. When $\Omega = \Gamma$, the coherent configuration $\mathcal{X}$ is called *semiregular*, and *regular* in homogeneous case. Thus regular schemes are exactly *thin schemes* in the sense of [24]. One can also define such a scheme by the condition that any basic relation r of it is *thin*, i.e. that

$$|\alpha r| \le 1 \quad \text{and} \quad |\alpha r^*| \le 1$$

for all $\alpha \in \Omega$. We note that the set of all thin relations on the same set is closed with respect to $*$ and $\cdot$.

2.8. The Weisfeiler–Leman algorithm. From the algorithmic point of view a coherent configuration $\mathcal{X}$ on n points is given by the set S of its basic relations. In this representation one can check in time $n^{O(1)}$ whether $\mathcal{X}$ is homogeneous or imprimitive. Moreover, within the same time one can list the fibers of $\mathcal{X}$, and find a nontrivial equivalence relation $e \in S^\cup$ (if it exists) as well as the quotient of $\mathcal{X}$ modulo e.

The well-known Weisfeiler–Leman algorithm is described in detail in [23, Section B]. The input of it is a set $\mathcal{S}$ of binary relations on a set Ω, and the output is the coherent configuration $\mathcal{X} = \mathrm{Fis}(\mathcal{S})$. The running time of the algorithm is polynomial in sizes of $\mathcal{S}$ and Ω. The canonical version of the Weisfeiler–Leman algorithm have been studied in Section M of the above book (under the name "simultaneous stabilization"), where, in fact, the following statement was proved.

Theorem 2.4. *Let $\mathcal{S}_i$ be a set of m binary relations on a set of size n, $i = 1, 2$. Then given a bijection $\psi : \mathcal{S}_1 \to \mathcal{S}_2$ one can check in time $mn^{O(1)}$ whether or not there exists an algebraic isomorphism $\varphi : \mathrm{Fis}(\mathcal{S}_1) \to \mathrm{Fis}(\mathcal{S}_2)$ such that $\varphi|_{\mathcal{S}_1} = \psi$. Moreover, if φ does exist, it can be found within the same time.*

§3. Bases of a coherent configuration

3.1. Generalized base. A set $\Pi \subset 2^\Omega$ is called a *generalized base* of a coherent configuration $\mathcal{X}$ if the Π-fission of the latter is complete. When Π consists of singletons, we identify Π with the corresponding subset of Ω, and say that Π is a *base* of $\mathcal{X}$. It is easily seen that Π is a generalized base

of any fission of $\mathcal{X}$, and that any $\Pi' \subset 2^\Omega$ that contains Π is a generalized base of $\mathcal{X}$. It is also clear that replacing some elements of Π by their complements in Ω produces a generalized base of $\mathcal{X}$. The following simple statement will be used in Section 7.

Lemma 3.1. *Let $\mathcal{X}$ be a coherent configuration on Ω, Π a generalized base of $\mathcal{X}$ and $\alpha \in \Omega$. Set $\mathcal{X}' = (\mathcal{X}_\alpha)_{\Omega'}$ and $\Pi' = \{\Gamma' : \Gamma \in \Pi\}$ where $\Gamma' = \Gamma \setminus \{\alpha\}$ for all $\Gamma \subset \Omega$. Then Π' is a generalized base of $\mathcal{X}'$.*

Proof. Denote by $\mathcal{Y}$ the *direct sum* of the one-point coherent configuration on $\{\alpha\}$ and Π'-fission of $\mathcal{X}'$; namely, $\mathcal{Y}$ is the smallest coherent configuration on Ω such that

$$\{\alpha\} \in \Phi(\mathcal{Y}) \quad \text{and} \quad \mathcal{Y}_{\Omega'} = \mathrm{Fis}(\mathcal{X}', \Pi').$$

Then obviously $\mathcal{Y} \geq \mathcal{X}_\alpha$ and $\Pi \subset \Phi(\mathcal{Y})^\cup$. Therefore

$$\mathcal{Y} \geq \mathrm{Fis}(X_\alpha, \Pi) \geq \mathrm{Fis}(\mathcal{X}, \Pi).$$

Since Π is a generalized base of $\mathcal{X}$, it follows that $\mathrm{Fis}(\mathcal{X}, \Pi)$, and hence $\mathcal{Y}$, is a complete coherent configuration. This implies that so is $\mathcal{Y}_{\Omega'} = \mathrm{Fis}(\mathcal{X}', \Pi')$. Thus Π' is a generalized base of $\mathcal{X}'$. □

3.2. Generalized base number. Denote by $gb(\mathcal{X})$ the smallest cardinality of a generalized base of the coherent configuration $\mathcal{X}$; this number is called the *generalized base number* of $\mathcal{X}$. The *base number* $b(\mathcal{X})$ of $\mathcal{X}$ is defined in a similar way. Obviously,

$$gb(\mathcal{X}) \leq b(\mathcal{X}). \tag{8}$$

Since any fiber of $\mathcal{X}$ is a union of fibers in any fission of $\mathcal{X}$, we also have

$$gb(\mathcal{X}) \leq \max_{\Gamma \in \Phi} gb(\mathcal{X}_\Gamma) \quad \text{and} \quad b(\mathcal{X}) \leq \sum_{\Gamma \in \Phi} b(\mathcal{X}_\Gamma) \tag{9}$$

where $\Phi = \Phi(\mathcal{X})$. Moreover, from the remark made in Subsection 3.1 it immediately follows that

$$\mathcal{X}' \geq \mathcal{X} \quad \Rightarrow \quad gb(\mathcal{X}') \leq gb(\mathcal{X}) \quad \text{and} \quad b(\mathcal{X}') \leq b(\mathcal{X}).$$

It was observed in [2] that any regular point of a coherent configuration forms a base of it. Thus $b(\mathcal{X}) \leq 1$ for any 1-regular coherent configuration $\mathcal{X}$. In the following statement we will use the fact that the equality

$$b(\mathcal{X}) = b(\mathrm{Aut}(\mathcal{X})) \tag{10}$$

holds for any cyclotomic scheme $\mathcal{X}$ (statement (2) of [2, Theorem 1.2]).

Theorem 3.2. *Let $\mathcal{X}$ be an antisymmetric cyclotomic scheme over a finite field. Then $gb(\mathcal{X}) \le 1$ and $b(\mathcal{X}) \le 3$.*

Proof. We note that any antisymmetric scheme of degree > 1 has rank at least 3. By the hypothesis this implies that $\mathcal{X}$ is a proper cyclotomic scheme in the sense of paper [2]. Therefore by the McConnel theorem (inclusion (1) of that paper) this implies that $\mathrm{Aut}(\mathcal{X}) \le \mathrm{A\Gamma L}(1,\mathbb{F})$ where $\mathbb{F}$ is the underlying finite field. Thus due to (10) we have

$$b(\mathcal{X}) = b(\mathrm{Aut}(\mathcal{X})) \le b(\mathrm{A\Gamma L}(1,\mathbb{F})) \le 3.$$

To prove that $gb(\mathcal{X}) \le 1$ set $b = b(\mathcal{X})$. Without loss of generality we can assume that $b = 2$ or $b = 3$. Denote by $\mathcal{Y}$ the Π-fission of $\mathcal{X}$ with $\Pi = \{B\}$ where $B = \{\alpha_0, \dots, \alpha_{b-1}\}$ is a base of $\mathcal{X}$. Then it suffices to verify that

$$B \notin \Phi(\mathcal{Y}). \tag{11}$$

Indeed, in this case the set B must be the union of b fibers, because the size of any fiber of antisymmetric configuration is of odd cardinality. But then $\mathcal{Y} = \mathrm{Fis}(\mathcal{X}, B)$ is the complete configuration. Thus Π is a generalized base of $\mathcal{X}$ and we are done.

To prove (11) suppose on the contrary that $B \in \Phi(\mathcal{Y})$. Then $b = 3$ because any antisymmetric scheme, and hence $\mathcal{Y}_B$, has odd degree. However, up to isomorphism there is a unique antisymmetric scheme of degree 3, namely, the scheme of a regular group of order 3. This implies that $r_{\mathcal{Y}}(\alpha_0, \alpha_1) = r_{\mathcal{Y}}(\alpha_0, \alpha_2)^*$, and hence

$$r(\alpha_0, \alpha_1) = r(\alpha_0, \alpha_2)^* \tag{12}$$

On the other hand, by the transitivity of the group $\mathrm{Aut}(\mathcal{X})$ without loss of generality we can assume that $\alpha_0 = 0_{\mathbb{F}}$. Then given $\alpha \in \Omega$ the set of fixed points of the two-point stabilizer $\mathrm{Aut}(\mathcal{X})_{\alpha_0,\alpha}$, is an additive subgroup of $\mathbb{F}$. Due to (10) this implies that the set $\{\alpha_0, \alpha_1', \alpha_2'\}$ with $\alpha_i' \in \{\alpha_i, -\alpha_i\}$, is also a base of $\mathcal{X}$. Thus the points α_1 and α_2 can be chosen so that

$$r(\alpha_0, \alpha_1) \ne r(\alpha_0, \alpha_2)^*.$$

However, this contradicts (12). □

3.3. Bases of size at most 2. A symmetric relation $s \in S^{\cup}$ is called *connected* if any two distinct points in Ω are joined by a path in the graph (Ω, s). It is well-known that a scheme $\mathcal{X}$ is primitive if and only if any nonreflexive relation $s \cup s^*$, $s \in S$, is connected.

Theorem 3.3. *Let $\mathcal{X}$ be a coherent configuration and $s \in S^{\cup}$ a connected relation. Suppose that for any point $\alpha \in \Omega$ the coherent configuration $(\mathcal{X}_\alpha)_{\alpha s}$ is semiregular. Then any pair of distinct points in s forms a base of $\mathcal{X}$. In particular, $b(\mathcal{X}) \le 2$.*

Proof. Without loss of generality we can assume that $s \cap 1_\Omega = \varnothing$. Let $(\alpha, \beta) \in s$. Set $\Gamma = \{\gamma \in \Omega : \ \{\gamma\} \in \Phi(\mathcal{X}_{\alpha,\beta})\}$. Then obviously $\alpha, \beta \in \Gamma$. Moreover, given $\gamma \in \Gamma$ we have

$$\gamma s \subset \Gamma \quad \text{or} \quad \gamma s \cap \Gamma = \varnothing. \tag{13}$$

Indeed, suppose on the contrary that there are $\gamma \in \Gamma$ and $\gamma_1, \gamma_2 \in \gamma s$ such that $\gamma_1 \in \Gamma$ and $\gamma_2 \notin \Gamma$. Since the coherent configuration $(\mathcal{X}_\gamma)_{\gamma s}$ is semiregular this implies that $\{\gamma_2\} \in \Phi(\mathcal{X}_{\gamma,\gamma_1})$. However, the coherent configuration $\mathcal{X}_{\gamma,\gamma_1}$ is a fusion of $\mathcal{X}_{\alpha,\beta}$ because $\gamma, \gamma_1 \in \Gamma$. Therefore $\{\gamma_2\} \in \Phi(\mathcal{X}_{\alpha,\beta})$, and hence $\gamma_2 \in \Gamma$. Contradiction.

Denote by Γ_0 the set of all points $\gamma \in \Gamma$ for which $\gamma s \subset \Gamma$. Then $\alpha \in \Gamma_0$ because $(\alpha, \beta) \in s$, $\beta \in \Gamma$ and the coherent configuration $(\mathcal{X}_\alpha)_{\alpha s}$ is semiregular. By (13) this implies that Γ_0 is the connectivity component of the graph (Ω, s) that contains the vertex α. Since this graph is connected, this implies that $\Gamma_0 = \Omega$. Therefore $\Gamma = \Omega$. By the definition of Γ this means that any fiber of the coherent configuration $\mathcal{X}_{\alpha,\beta}$ is singleton, and hence this configuration is complete. Thus $\{\alpha, \beta\}$ is a base of $\mathcal{X}$. □

The following special statement will be used in the proof of Lemma 9.4. Below given a nonnegative integer m and relations $r, s \in S$ we denote by $r \circ_m s$ the set of all $t \in r^* s$ such that $c^s_{rt} \le m$.

Lemma 3.4. *Let $\mathcal{X}$ be an antisymmetric primitive schurian scheme and $r \in S$ a nonreflexive relation such that $|r \circ_2 r \cup r \circ_2 r^*| > 2n_r/3$ and $r \circ_2 r^* \ne \varnothing$. Then $b(\mathcal{X}) \le 2$.*

Proof. By the hypothesis $s = r \cup r^*$ is a connected non-reflexive relation of $\mathcal{X}$. So by Theorem 3.3 it suffices to verify that the coherent configuration $\mathcal{X}_0 = (\mathcal{X}_\alpha)_{\alpha s}$ is semiregular for all $\alpha \in \Omega$. However, from the schurity of $\mathcal{X}$ it follows that

$$\alpha r, \alpha r^* \in \Phi(\mathcal{X}_0).$$

Denote by S_1 and S_2 the set of thin relations in $(S_0)_{\alpha r, \alpha r^*}$ and in $(S_0)_{\alpha r}$ respectively. Then one can see that the coherent configuration $\mathcal{X}_0$ is semiregular if and only if the following inequalities hold:

$$|S_1| > 0 \quad \text{and} \quad |S_2| > n_r/3. \tag{14}$$

Let $u \in r \circ_2 r^*$. Since $n_u = n_{u^*}$, from (4) we obtain that $u^* \in r^* \circ_2 r$. This implies that any point in αr has at most two neighbors in the relation $u' = u_{\alpha r^*, \alpha r}$. On the other hand, the valences of $\mathcal{X}_0$ are odd. Thus by Lemma 2.2 the relation u' contains a relation from S_1. This proves the first inequality in (14). Let now $v \in r \circ_2 r$. Then again any point in αr has at most two neighbors in $v' = v_{\alpha r, \alpha r}$, and the above argument shows that v contains a relation from S_2. Thus by the lemma hypothesis we have

$$|S_1| + |S_2| \geq |r \circ_2 r \cup r \circ_2 r^*| > 2n_r/3.$$

Therefore either S_1 or S_2 contains more that $n_r/3$ elements. In the latter case the second inequality in (14) is clear, whereas in the former case it follows because S_2 contains a set $t \cdot S_1^*$ where t is an arbitrary element from S_1. □

3.4. Bases and isomorphisms. The following statement shows how bases are used to find isomorphisms between coherent configurations.

Theorem 3.5. *Let $\mathcal{X}$ and $\mathcal{X}'$ be coherent configurations of degree n. Then given an algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$ all the elements in the set $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ can be listed in time $(bn)^{O(b)}$ where $b = b(\mathcal{X})$.*

Proof. By exhaustive search in time $n^{O(b)}$ one can find a base B of the coherent configuration $\mathcal{X}$ that contains exactly b points. Obviously, any isomorphism from $\mathcal{X}$ onto $\mathcal{X}'$ takes this base to a base of $\mathcal{X}'$. Therefore

$$\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi) = \bigcup_{B'} \bigcup_{g} \mathrm{Iso}_g(\mathcal{X}, \mathcal{X}', \varphi)$$

where B' runs over all b-subsets of the point set of $\mathcal{X}'$, g runs over all bijections from B onto B', and $\mathrm{Iso}_g(\mathcal{X}, \mathcal{X}', \varphi)$ consists of all $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ such that $f|_B = g$. Since there are at most $(bn)^{O(b)}$ possibilities for a pair (B', g), only we need is to find in time $n^{O(1)}$ the set $\mathrm{Iso}_g(\mathcal{X}, \mathcal{X}', \varphi)$ for fixed B' and g. To do this set

$$\mathcal{S} = S \cup \{1_{\{\alpha\}} : \ \alpha \in B\} \quad \text{and} \quad \mathcal{S}' = S' \cup \{1_{\{\alpha'\}} : \ \alpha' \in B'\}$$

where S and S' are the sets of basic relations of $\mathcal{X}$ and $\mathcal{X}'$ respectively. Then obviously the coherent configurations

$$\mathrm{Fis}(\mathcal{S}) = \mathrm{Fis}(\mathcal{X}, B) \quad \text{and} \quad \mathrm{Fis}(\mathcal{S}') = \mathrm{Fis}(\mathcal{X}', B')$$

are complete. So any algebraic isomorphism between them is induced by exactly one bijection between their fiber sets. Thus the required statement

immediately follows from Theorem 2.4 for the bijection $\psi : \mathcal{S} \to \mathcal{S}'$ such that $\psi|_S = \varphi$ and $\psi(1_{\{\alpha\}}) = 1_{\{\alpha^g\}}$ for all $\alpha \in B$. □

The following technical notion was introduced in [3, Sec. 3.2]. Let $\mathcal{X}$ be a scheme and $e_0, e_1 \in S^\cup$ two equivalence relations such that $e_0 \subset e_1$. Set

$$\Omega_0 = \{\Gamma_1/e_0 : \ \Gamma_1 \in \Omega/e_1\}.$$

By a *majorant* of the group $G = \mathrm{Aut}(\mathcal{X})$ with respect to the pair (e_0, e_1) we mean a permutation group H on a set Δ together with a family of bijections $f_\Gamma : \Gamma \to \Delta$ where $\Gamma \in \Omega_0$, such that

$$(G^\Gamma)^{f_\Gamma} \le H \tag{15}$$

where $G^\Gamma = G^{\Gamma_1/e_0}$ is the permutation group induced by the natural action of the setwise stabilizer $G_{\{\Gamma_1\}}$ on the set Γ_1/e_0.

Corollary 3.6. *In the above notation let Γ be an element of Ω_0. Suppose that*

$$\mathrm{Iso}(\mathcal{X}_\Gamma, \mathcal{X}_{\Gamma'}, \varphi_{\Gamma,\Gamma'}) \ne \varnothing \quad \text{for all} \quad \Gamma' \in \Omega_0 \tag{16}$$

where $\varphi_{\Gamma,\Gamma'}$ is the algebraic isomorphism (6) *for $\mathcal{X} = \mathcal{X}_{\Omega/e_0}$. Then the group $\mathrm{Aut}(\mathcal{X}_\Gamma)$ together with any family of bijections $f_{\Gamma'} \in \mathrm{Iso}(\mathcal{X}_\Gamma, \mathcal{X}_{\Gamma'}, \varphi_{\Gamma,\Gamma'})$, $\Gamma' \in \Omega_0$, is a majorant of $\mathrm{Aut}(\mathcal{X})$ with respect to the pair (e_0, e_1). Moreover, it can be constructed in time $(bn)^{O(b)}$ where $n = |\Gamma|$ and $b = b(\mathcal{X}_\Gamma)$.*

Proof. For any $\Gamma' \in \Omega_0$ we obviously have inclusion $G^{\Gamma'} \le \mathrm{Aut}(\mathcal{X}_{\Gamma'})$. On the other hand, given a bijection $f_{\Gamma'} \in \mathrm{Iso}(\mathcal{X}_\Gamma, \mathcal{X}_{\Gamma'}, \varphi_{\Gamma,\Gamma'})$, we have

$$\mathrm{Aut}(\mathcal{X}_{\Gamma'})^{f_{\Gamma'}} = \mathrm{Aut}(\mathcal{X}_{\Gamma'}^{f_{\Gamma'}}) = \mathrm{Aut}(\mathcal{X}_\Gamma).$$

Thus inclusion (15) holds for $\Delta = \Gamma$ and $H = \mathrm{Aut}(\mathcal{X}_\Gamma)$. This proves the first statement. The second one follows from Theorem 3.5. □

§4. Primitive linear groups of odd order

The structure of a finite solvable linear primitive group is well-known, see [17, 21]. The following theorem is just a specialization of [22, Theorem 2.2] for the groups of odd order.

Theorem 4.1. *Let $K \le \mathrm{GL}(d, p)$ be a primitive group of odd order. Then every normal abelian subgroup of K is cyclic, and K has a series of normal subgroups $1 < U \le F \le A \le K$ such that the following statements hold:*

(P1) $\mathrm{Span}(U) = \mathrm{GF}(p^a)$ *where a is a divisor of d,*

(P2) $C_K(F) \le F \le \mathrm{Fit}(K)$ *and* $|F : U| = e^2$ *for some integer* e *such that each prime divisor of* e *divides* $p^a - 1$,
(P3) $A = C_K(U)$ *and* A/F *is isomorphic to a completely reducible subgroup of the group* $\prod_{i=1}^m \mathrm{Sp}(2n_i, p_i)$ *where* n_i *and* p_i *are defined from the prime power decomposition* $e = \prod_{i=1}^m p_i^{n_i}$,
(P4) $|K : A|$ *divides* a *and* ae *divides* d.

By statements (P1) and (P4) we have $|U| \le u_{a,p}$ and $|K : A| \le a_0$ where $u_{a,p}$ and a_0 are the maximal odd divisors of $p^a - 1$ and a respectively. Thus

$$|K| \le u_{a,p} \cdot e^2 \cdot s_e \cdot a_0 \tag{17}$$

where s_e is the maximal order of the group A/F for a fixed e (see statement (P3)). The following two lemmas collect some special facts on the group K from Theorem 4.1 that are contained in papers [12,13] or obtained by means of computer package GAP [14].

Lemma 4.2. *Let* e *be the number from Theorem* 4.1. *Then one of the following statements hold:*

(1) $e = 1$ *and* $K \le \Gamma\mathrm{L}(1, p^d)$,
(2) $e \in \{5, 9, 11, 13\}$ *and* $s_5 \le |K : F| = 3$, $s_9, s_{11} \le 5$, $s_{13} \le 7$,
(3) $e \ge 15$ *is an odd integer and* $s_e \le e^2/2$.

Proof. Suppose first that $e = 1$. Then from (P1) and (P2) it follows that $U = F$ is a normal abelian self-centralizing subgroup of K. By [17, Lemma 2.2] this implies that F is irreducible. Thus by [17, Theorem 2.1] we conclude that $K \le \Gamma\mathrm{L}(1, p^d)$ which proves the second part of statement (1). For $e \ge 15$ the required inequality immediately follows from the fact that any completely reducible odd order subgroup of the group $\mathrm{Sp}(2n_i, p_i)$ has a regular orbit on the underground linear space (see [12, Theorem A]). To deal with the case $1 < e < 15$ we start with some observation.

Suppose that e is an odd prime. We claim that the group K/F has an irreducible representation in $\mathrm{GL}(2, e)$. Indeed, by statement (1) of [22, Theorem 2.2] the group F is a central product of U and a characteristic subgroup E of K that contains an extraspecial subgroup E_0 of order e^3 and exponent e. In particular, $Z = E \cap U$ is a central subgroup of F, $E/Z \cong F/U$ and $|E_0 \cap Z| \le e$. Therefore by statement (P2) this implies that $|E : Z| = |F : U| = e^2$, and

$$F/U \cong E_0/(E_0 \cap Z) \cong \mathbb{Z}_e \times \mathbb{Z}_e. \tag{18}$$

However, by statement (2) of [22, Theorem 2.2] the group F/U is a completely reducible K/F-module. Therefore K/F has a representation in $\mathrm{GL}(2,e)$. Suppose that this representation is not irreducible. Then one can find a group $E' > Z$ such that $|E : E'| = e$ and the group E'/Z is K/F-invariant. But then obviously E' is a normal abelian subgroup of K. Moreover from (18) it follows that $|E' \cap E_0| = e^2$. Therefore E' contains an elementary abelian subgroup of order e^2. Thus E' is normal abelian non-cyclic subgroup of K, which is impossible by Theorem 4.1. The claim is proved.

Let now $1 < e < 15$. By means of GAP we find that (a) there are no odd order irreducible subgroups in $\mathrm{GL}(2,e)$ for $e = 3, 7$, (b) the maximal order of an irreducible odd order subgroup in $\mathrm{GL}(2,e)$ for $e = 5, 11, 13$ equals respectively to $3, 15$ and 21, and (c) the irreducible subgroups in $\mathrm{GL}(2,11)$ of order 15 and in $\mathrm{GL}(2,13)$ of order 21 are not subgroups of $\mathrm{Sp}(2,11)$ and $\mathrm{Sp}(2,13)$ respectively. Thus the required statement immediately follows from the above claim unless $e = 9$. In the remaining case the same argument as in the claim shows that K/F has a representation in $\mathrm{GL}(4,e)$. Since up to conjugacy the latter group has a unique irreducible odd order subgroup and the order of it is 5, it suffices to verify that the above representation is irreducible. Suppose that this is not true. Then as in the above claim one can check that there is no K/F-invariant subgroup of E/Z of order e. Therefore such a subgroup has order e^2. But this is impossible by statement (a) with $e = 3$. □

Lemma 4.3. *In the notation of Theorem* 4.1 *we have* $\mathrm{fix}(K) \le p^{\lfloor 4d/9 \rfloor}$. *Moreover, if g is an element of K of prime order q, then*

(1) $\mathrm{fix}(g) \le p^{\lfloor d/q \rfloor}$ *for* $g \in F$,
(2) $\mathrm{fix}(g) \le p^{\lfloor d/3 \rfloor}$ *for* $g \notin F$ *and* $q \ne 3$.

Proof. Follows from Lemma 1.3 of [12] and the proof of it. □

§5. Bases of the wreath product

In this section we fix a coherent configuration $\mathcal{X}_i = (\Omega_i, S_i)$, $i = 1, 2$. The *wreath product* $\mathcal{X}_1 \wr \mathcal{X}_2$ can be defined as the smallest coherent configuration $\mathcal{X} = (\Omega, S)$ with $\Omega = \Omega_1 \times \Omega_2$ such that the set $S^\cup$ contains the equivalence relation e with classes $\Omega_\alpha = \Omega_1 \times \{\alpha\}$, $\alpha \in \Omega_2$, and

$$(\mathcal{X}_{\Omega_\alpha})^{\pi_\alpha} = \mathcal{X}_1, \qquad \mathcal{X}^\pi = \mathcal{X}_2$$

where $\pi_\alpha : \Omega_\alpha \to \Omega_1$ and $\pi : \Omega \to \Omega_2$ are the natural projections. In particular, $\pi_\alpha \in \mathrm{Iso}(\mathcal{X}_{\Omega_\alpha}, \mathcal{X}_1)$ and $\mathcal{X}_{\Omega/e} = \mathcal{X}_2$. When the coherent configuration $\mathcal{X}$ is homogeneous, we have

$$S = \{s_1 \otimes 1_{\Omega_2} : \ s_1 \in S_1\} \cup \{\Omega_1^2 \otimes s_2 : \ s_2 \in S_2, \ s_2 \neq 1_{\Omega_2}\}. \tag{19}$$

Any imprimitive schurian scheme is isomorphic to a fission of the wreath product of two smaller schemes. In general case the set $\Phi(\mathcal{X})$ consists of all sets $\Gamma_1 \times \Gamma_2$ where $\Gamma_1 \in \Phi(\mathcal{X}_1)$ and $\Gamma_2 \in \Phi(\mathcal{X}_2)$, and

$$\mathcal{X}_{\Gamma_1 \times \Gamma_2} = (\mathcal{X}_1)_{\Gamma_1} \wr (\mathcal{X}_1)_{\Gamma_2}. \tag{20}$$

Lemma 5.1. *Let $\mathcal{X} = \mathcal{X}_1 \wr \mathcal{X}_2$ and $\Pi \subset 2^\Omega$. Suppose that*

(1) *$\Pi_\alpha = \{\Gamma \cap \Omega_\alpha : \ \Gamma \in \Pi\}$ is a generalized base of $\mathcal{X}_{\Omega_\alpha}$ for all $\alpha \in \Omega_2$,*
(2) *$\Pi_{\Omega/e} = \{\Gamma^\pi : \ \Gamma \in \Pi\}$ is a generalized base of $\mathcal{X}_2$.*

Then Π is a generalized base of $\mathcal{X}$.

Proof. Set $\mathcal{Y} = \mathrm{Fis}(\mathcal{X}, \Pi)$. Then obviously $\mathcal{Y}^\pi \geq \mathrm{Fis}(\mathcal{X}_2, \Pi_2)$ is a complete configuration by condition (2). So $\Omega_\alpha \in \Phi(\mathcal{Y})^\cup$ for all $\alpha \in \Omega_2$. It follows that $\Gamma \cap \Omega_\alpha \in \Phi(\mathcal{Y})^\cup$ for all $\Gamma \in \Pi$. Therefore $\mathcal{Y}_{\Omega_\alpha} \geq \mathrm{Fis}(\mathcal{X}_{\Omega_\alpha}, \Pi_\alpha)$ is a complete configuration for all α. Consequently, any fiber of $\mathcal{Y}$ is a singleton, which means that the coherent configuration $\mathcal{Y}$ is complete. Thus Π is a generalized base of $\mathcal{X}$. □

Let Π be a generalized base of the coherent configuration $\mathcal{X}$. We say that Π is *proper* if there exists a set $\Gamma \in \Pi$ such that $\Gamma \cap \Omega_\alpha$ is a proper subset of Ω_α for all $\alpha \in \Omega_2$. Clearly, such a base can exist only if $|\Omega_2| > 1$.

Theorem 5.2. *Let $\mathcal{X} = \mathcal{X}_1 \wr \mathcal{X}_2$ and $b = \max\{gb(\mathcal{X}_1), gb(\mathcal{X}_2)\}$. Suppose that $\mathcal{X}_1$ is antisymmetric. Then $gb(\mathcal{X}) \leq b$. Moreover, if $b > 0$, then there exists a proper generalized base of $\mathcal{X}$ of size b.*

Proof. Without loss of generality we can also assume that $|\Omega_1| > 1$ and $b > 0$, and that the coherent configurations $\mathcal{X}_1$, $\mathcal{X}_2$, and hence $\mathcal{X}$, are homogeneous (see the first inequality in (9) and equality (20)). Let Π_i be a generalized base of $\mathcal{X}_i$ of size b, $i = 1, 2$. The assumption implies that the set Π_1 contains a proper subset of Ω_1. Let us choose a bijection $\Gamma_1 \mapsto \Gamma_2$ from Π_1 onto Π_2, and denote by Π the set of all

$$\Gamma = \Gamma_1 \times \Gamma_2 \ \cup \ \Gamma_1' \times \Gamma_2' \tag{21}$$

with $\Gamma_1 \in \Pi_1$ where Γ_i' is the complement to Γ_i in Ω_i, $i = 1, 2$. Then $|\Pi| = b$. So it suffices to verify that Π is a generalized base of $\mathcal{X}$ (in this case Π is proper because Π_1 contains a proper subset of Ω_1).

One can see that conditions (1) and (2) of Lemma 5.1 are satisfied for the union of Π and $\Pi' = \{\Gamma_1 \times \Gamma_2 : \ \Gamma_1 \in \Pi_1\}$. So by this lemma the union is a generalized base of $\mathcal{X}$. Thus we have to verify only that $\mathrm{Fis}(\mathcal{X}, \Pi \cup \Pi')$ is a fission of $\mathcal{Y} = \mathrm{Fis}(\mathcal{X}, \Pi)$, or, equivalently, that

$$\Gamma_1 \times \Gamma_2 \in \Phi(\mathcal{Y})^{\cup} \tag{22}$$

for all $\Gamma_1 \in \Pi_1$. To do this denote by e' the equivalence relation on the set Γ such that $\Gamma/e' = I \cup I'$ with

$$I = \{\Gamma \cap \Omega_\alpha : \ \alpha \in \Gamma_2\} \quad \text{and} \quad I' = \{\Gamma \cap \Omega_\alpha : \ \alpha \in \Gamma_2'\}.$$

Then from (21) it follows that $e' = \Gamma^2 \cap e$ is also a relation of $\mathcal{Y}$. Besides, since $\mathcal{X}_1$ is antisymmetric, exactly one of the numbers Γ_1 and Γ_1' is odd. This implies that the hypothesis of Lemma 2.1 is satisfied for $\mathcal{X} = \mathcal{Y}$ and $e = e'$. By this lemma the union of all elements of I belongs to the set $\Phi(\mathcal{Y})^{\cup}$. Since the union is obviously equal to $\Gamma_1 \times \Gamma_2$, we conclude that (22) holds. □

Let Π be a proper generalized base of the coherent configuration $\mathcal{X}$. We say that Π is *thin* if $|\Gamma \cap \Omega_\alpha| \le 1$ for all $\Gamma \in \Pi$ and $\alpha \in \Omega_2$. The following statements will be used in Section 7 to estimate the base number of the exponentiation of schemes.

Theorem 5.3. *Let $\mathcal{X} = \mathcal{X}_1 \wr \mathcal{X}_2$. Suppose that $\mathcal{X}_1$ is antisymmetric. Then $\mathcal{X}$ has a thin generalized base of size $b = b_1 + \max\{0, b_2 - \lceil b_1/2 \rceil\}$ where $b_1 = b(\mathcal{X}_1)$ and $b_2 = gb(\mathcal{X}_2)$.*

Proof. Let Π_1 be a base of $\mathcal{X}_1$ of size b_1, and Π_2 a generalized base of $\mathcal{X}_2$ of size b_2. Suppose first that $2b_2 \ge b_1$. Then $b = \lfloor b_1/2 \rfloor + b_2$. Without loss of generality we can assume that b_1 is even (otherwise we add an extra point to Π_1). Let us fix

- a point $\delta \in \Omega_1$,
- a decomposition $\Pi_1 = B \cup B'$ into two disjoint sets of equal size,
- a fixed point free involution $\beta \mapsto \beta'$ on Ω_1 taking B to B',
- an injection $B \to \Pi_2$, $\beta \mapsto \Gamma_\beta$, and set Π_2' to be the complement to its image.

Denote by Π the family of sets Γ and Γ' defined below for all $\beta \in B$, and sets $\{\delta\} \times \Gamma_2$ for all $\Gamma_2 \in \Pi_2'$,

$$\Gamma = \{\beta\} \times \Gamma_\beta \ \cup \ \{\beta'\} \times \Gamma_\beta' \quad \text{and} \quad \Gamma' = \{\beta'\} \times \Gamma_\beta \ \cup \ \{\beta\} \times \Gamma_\beta'. \tag{23}$$

Since $|B| = b_1/2$ and $|\Pi_2'| = b_2 - b_1/2$, the family Π is of size $b = b_1/2 + b_2$. To complete the proof we will verify that Π is a generalized base of $\mathcal{X}$ (in this case Π is thin just by the definition).

To prove that the coherent configuration $\mathcal{Y} = \mathrm{Fis}(\mathcal{X}, \Pi)$ is complete, we note that $\Phi(\mathcal{Y})^\cup$ contains the sets $\Gamma^* = \Gamma \cup \Gamma'$ where Γ and Γ' are defined by (23). We claim that

$$\{\beta\} \times \Gamma_\beta \in \Phi(\mathcal{Y})^\cup \tag{24}$$

for all $\beta \in B$. Then obviously $\{\beta'\} \times \Gamma'_\beta \in \Phi(\mathcal{Y})^\cup$. This implies that conditions (1) and (2) of Lemma 5.1 are satisfied for $\mathcal{X}$ and Π^* where the latter consists of all sets $\{\beta\} \times \Gamma_\beta$, $\{\beta'\} \times \Gamma'_\beta$ and $\{\delta\} \times \Gamma_2$. So by this lemma Π^* is a generalized base of $\mathcal{X}$. Thus the coherent configuration $\mathcal{Y} \geq \mathrm{Fis}(\mathcal{X}, \Pi^*)$ is complete and we are done.

To prove (24) suppose on the contrary that there is a set $\Delta \in \Phi(Y)$ such that

$$\beta\alpha,\ \beta'\alpha' \in \Delta \tag{25}$$

for some $\beta \in B$, $\alpha \in \Gamma_\beta$ and $\alpha' \in \Gamma'_\beta$, where $\beta\alpha = (\beta, \alpha)$ and $\beta'\alpha' = (\beta', \alpha')$. Denote by e^* the equivalence relation on Γ^* with classes $\Gamma^* \cap \Omega_\gamma = \{\beta, \beta'\} \times \{\gamma\}$ where $\gamma \in \Omega_2$. Then $e^* = e \cap (\Gamma^*)^2$ is a relation of $\mathcal{Y}$. Therefore the set $\Delta' = \Delta e^*$ belongs to $\Phi(\mathcal{Y})^\cup$. Since the relation $u := e^* \setminus 1_{\Gamma^*}$ is thin, this implies that Δ' is a fiber of Y and $u_{\Delta,\Delta'}$ is a basic relation of $\mathcal{Y}$. Thus from (25) we obtain that

$$r_{\mathcal{Y}}(\beta\alpha, \beta'\alpha) = r_{\mathcal{Y}}(\beta'\alpha', \beta\alpha') = u_{\Delta,\Delta'}.$$

However, in this case $r_{\mathcal{X}_1}(\beta, \beta') = r_{\mathcal{X}_1}(\beta', \beta)$ which is impossible because the coherent configuration $\mathcal{X}_1$ is antisymmetric.

Let now $2b_2 < b_1$. Then $b = b_1$. In this case take two disjoint sets $B, B' \subset \Pi_1$ of the same size b_2, choose a bijection from $B \to \Pi_2$, $\beta \mapsto \Gamma_\beta$, and set Π_2' to be the family of $b_1 - 2b_2$ sets $\{\beta\} \times \Omega_2$ where β runs over the set $\Pi_1 \setminus (B \cup B')$. Then the rest of the proof is completely analogous to the previous case. □

§6. Exponentiation

Let Γ be a finite set, m a positive integer and $\Delta = \{1, \dots, m\}$. Given a set $T \subset 2^{\Gamma \times \Gamma}$ denote by $T^{\otimes_m}$ the set of all relations $t_1 \otimes \cdots \otimes t_m$ with $t_i \in T$ for all i. For a coherent configuration $\mathcal{Y} = (\Gamma, T)$ the pair

$$\mathcal{Y}^{\otimes_m} = (\Gamma^m, T^{\otimes_m})$$

is also a coherent configuration (the Cartesian m-power of $\mathcal{Y}$). Any permutation group $L \le \mathrm{Sym}(\Delta)$ has the natural action on $\Omega = \Gamma^m$: a permutation $l \in L$ moves a point $\alpha = (\dots, \alpha_i, \dots)$ to the point $\alpha^l = (\dots, \alpha_j, \dots)$ with $j^l = i$ (and hence a relation $t = \cdots \otimes t_i \otimes \cdots$ to the relation $t^l = \cdots \otimes t_j \cdots \otimes$). Denote by $T \uparrow L$ the set of all relations $t^L = \cup_{l \in L} t^l$ with $t \in T^{\otimes_m}$. Then according to paper [1] the pair

$$\mathcal{X} = \mathcal{Y} \uparrow L = (\Omega, T \uparrow L) \tag{26}$$

is a coherent configuration called the *exponentiation* of $\mathcal{Y}$ by L.[5] It was also proved in that paper that $\mathcal{X}$ is schurian if and only if so is $\mathcal{Y}$, and that $\mathcal{X}$ is primitive if and only if L is transitive and $\mathcal{Y}$ is primitive and non-regular. It is easily seen that $\mathcal{X} = \mathcal{Y}$ whenever $m = 1$.

In this paper, we will use the exponentiation construction for the scheme of a primitive solvable permutation group. The structure of such a group is described in Theorem 2.3. Depending on whether the group K from this theorem is primitive (as a linear group) or not we will say that the scheme $\mathcal{X} = \mathrm{Inv}(G)$ is *linearly primitive* or *linearly imprimitive*. In both cases $\mathcal{X}$ is schurian and the following statement holds.

Theorem 6.1. *The scheme $\mathcal{X}$ has a (possibly trivial) fusion isomorphic to $\mathcal{Y} \uparrow L$ where $\mathcal{Y}$ is a linearly primitive scheme and L is a transitive group. Moreover, if $\mathcal{X}$ is antisymmetric, then $\mathcal{Y}$ is antisymmetric and L has odd order.*

Proof. Without loss of generality we can assume that the group K is imprimitive. Then the linear space Ω is a direct sum of the subspaces belonging the set

$$\Delta = \{\Gamma^k : \ k \in K\}$$

where Γ is a proper subspace of Ω, and K is isomorphic to a subgroup of the wreath product of the group $K^U = (K_{\{U\}})^U \le \mathrm{GL}(U)$ and the transitive permutation group $K^\Delta \le \mathrm{Sym}(\Delta)$ induced by the action of K on Δ, [21, Section 15.2]. According to [9, Proposition 4.1] this implies that G can be identified with a subgroup of the wreath product $G^U \uparrow K^\Delta$ of permutation groups G^U and K^Δ in primitive action. On the other hand, by [16, p.212] we have

$$\mathrm{Inv}(G^U \uparrow K^\Delta) = \mathrm{Inv}(G^U) \uparrow K^\Delta.$$

[5] It is a special case of the general construction of the exponentiation introduced in [1].

Thus the scheme $\mathcal{X} = \mathrm{Inv}(G)$ has a fusion $\mathcal{Y} \uparrow L$ where $\mathcal{Y} = \mathrm{Inv}(G^U)$ and $L = K^\Delta$. Moreover, if the scheme $\mathcal{Y}$ is linear imprimitive, then by the above it has a fusion $Y' \uparrow L'$ for some scheme $\mathcal{Y}' = \mathrm{Inv}(G')$ where G' is a primitive solvable permutation group and L' is a transitive group. So by [9, Proposition 3.3] the scheme $\mathcal{X}$ has a fusion $(\mathcal{Y}' \uparrow L') \uparrow L = \mathcal{Y}' \uparrow (L' \wr L)$ and the first statement follows. To prove the second statement it suffices to note that if the scheme $\mathcal{X}$ is antisymmetric, then the group K has odd order. □

§7. Bases of the exponentiation.

The following theorem gives upper bounds for the maximal sizes of generalized and ordinary bases of the exponentiation (26) when the coherent configuration $\mathcal{Y}$ is antisymmetric. The former bound is the best possible whereas the latter one definitely not. Nevertheless, even this rather weak bound is sufficient for the purpose of the paper.

Theorem 7.1. *Let $\mathcal{Y}$ be an antisymmetric coherent configuration and let L be a transitive permutation group of odd order. Then*

$$gb(\mathcal{Y} \uparrow L) \le \max\{gb(\mathcal{Y}), b\},$$

where $b = gb(\mathrm{Inv}(L))$. Moreover, if $\mathcal{Y}$ is not complete, then

$$b(\mathcal{Y} \uparrow L) \le b(\mathcal{Y}) + \max\{0, b - \lceil (b(\mathcal{Y}) - 1)/2 \rceil\}.$$

The proof of Theorem 7.1 will be given in the end of this section. Let us fix some notations. Let $\mathcal{X} = (\Omega, S)$ be the coherent configuration defined by (26). For any $i \in \{0, \dots, m\}$ set

$$r_i = \{(\alpha, \beta) \in \Gamma^m \times \Gamma^m : \ d(\alpha, \beta) = i\}$$

where $d(\alpha, \beta)$ is the number of all $j \in \Delta$ such that $\alpha_j \ne \beta_j$. One can see that r_i is the union of the relations from $T^{\otimes m}$ in which i factors are equal to 1_Γ and the other $m - i$ factors are $\Gamma^2 \setminus 1_\Gamma$. Therefore $r_i \in S^\cup$ for all i (which means that $\mathcal{X}$ is a fission of a Hamming scheme). In what follows we set $r_{-1} = \varnothing$ and $r = r_1$.

Let us fix a point $\gamma_0 \in \Gamma$, and set $\alpha = \alpha(\gamma_0)$ to be the point of Ω with all coordinates equal to γ_0. Then the neighborhood αr of α in r is the disjoint union of the sets

$$\Gamma_i = \{\beta \in \Omega : \ d(\alpha, \beta) = 1 \text{ and } \beta_i \ne \gamma\}, \qquad i \in \Delta. \tag{27}$$

They are the classes of an equivalence relation on αr that is denoted by e. It is easily seen that $e = 1_{\alpha r} \cup r_{\alpha r}$. Therefore e is a relation of the coherent configuration $\mathcal{X}_0 = (\mathcal{X}_\alpha)_{\alpha r}$. The following two lemmas are key ingredients in our proof.

Lemma 7.2. *The mapping* $\rho : \Omega \to 2^{\alpha r}$, $\beta \mapsto \beta r_{d-1} \cap \alpha r$ *where* $d = d(\alpha, \beta)$, *is an injection and*

$$\mathrm{Im}(\rho) = \{\Lambda \subset \alpha r : \ |\Lambda \cap \Gamma_i| \le 1 \text{ for all } i \in \Delta\}.$$

In particular, the set αr *is a base of the coherent configuration* $\mathcal{X}_\alpha$.

Proof. Given $\beta \in \Omega$ and $i \in \Delta$ such that $\beta_i \ne \gamma_0$ set $\beta^{(i)}$ to be the unique point in Γ_i the ith coordinate of which is equal to β_i. Then obviously

$$d(\beta, \beta^{(i)}) = d(\beta, \alpha) - 1.$$

Therefore $\beta^{(i)} \in \rho(\beta)$. On the other hand, let $\delta \in \rho(\beta)$. Then $d(\delta, \beta) = d-1$. So the points δ and β have exactly $m - d + 1$ equal coordinates. At least $m-d$ of them equal γ_0. But β has exactly $m-d$ such coordinates. Therefore there is $i \in \Delta$ such that $\beta_i \ne \gamma_0$ and $\beta_i = \delta_i$. This means that $\delta = \beta^{(i)}$. Thus

$$\rho(\beta) = \{\beta^{(i)} : \ i \in \Delta, \ \beta_i \ne \gamma\} \tag{28}$$

which proves the first statement. To prove the second one it suffices to note that no two points β and β' with $\rho(\beta) \ne \rho(\beta')$ belong the same fiber of the coherent configuration $\mathrm{Fis}(\mathcal{X}_\alpha, \alpha r)$. □

Set $\Gamma_0 = \Gamma \setminus \{\gamma_0\}$. Let us define the mapping $f : \Gamma_0 \times \Delta \to \alpha r$ taking a pair (γ, i) to the unique point $\beta \in \Gamma_i$ for which $\beta_i = \gamma$. Then obviously f is a bijection and the f-image of the set $\Gamma_0 \times \{i\}$ coincides with Γ_i for all $i \in \Delta$.

Lemma 7.3. *Set* $\mathcal{Y}_0$ *to be the restriction of* $\mathcal{Y}_{\gamma_0}$ *to* Γ_0. *Then* $\mathcal{X}_0^{f^{-1}} \ge \mathcal{Y}_0 \wr \mathrm{Inv}(L)$.

Proof. Denote by T_0 the set of all relations t_{Γ_0} with $t \in T$ (we recall that T is the set of basic relations of $\mathcal{Y}$). Then it is easily seen that $\mathcal{Y}_0 = \mathrm{Fis}(T_0)$. So by the definition of wreath product it suffices to verify that for all $t_0 \in T_0$ and all orbits $u \in \mathrm{Orb}(L, \Delta^2)$ we have

$$(t_0 \otimes 1_\Delta)^f, \ (\Gamma_0^2 \otimes u)^f \in S_0^\cup \tag{29}$$

where S_0 is the set of basic relations of $\mathcal{X}_0$. To do this let $t_0 \in T_0$. Then $t_0 = t_{\Gamma_0}$ for some $t \in T$. By the definition of the exponentiation and the

transitivity of L the set S contains the relation

$$(t\otimes 1_\Delta\otimes\cdots\otimes 1_\Delta)^L=(t\otimes 1_\Delta\otimes\cdots\otimes 1_\Delta)\cup\cdots\cup(1_\Delta\otimes\cdots\otimes 1_\Delta\otimes t). \quad (30)$$

Denote by s the restriction of this relation to αr. Then $s\in S_0^\cup$ by Lemma 2.2. On the other hand, given $i\in\Delta$ denote by s_i the summand in the right-hand side of (30) with t being at the ith position. Then a straightforward computation shows that $(s_i)_{\alpha r}$ coincides with the f-image of $t_0\otimes 1_{\{i\}}$. It follows that the relation

$$(t_0\otimes 1_\Delta)^f=\bigcup_{i\in\Delta}(t_0\otimes 1_{\{i\}})^f=\bigcup_{i\in\Delta}s_i=s$$

belongs to $S_0^\cup$ which proves the first part of (29). To prove the second part let $u\in\mathrm{Orb}(L,\Delta^2)$. Then $S^\cup$ contains the union of relations $u_{ij}=s_1\otimes\cdots\otimes s_m$ with $s_i=u$, $s_j=u^*$ and $s_k=1_\Gamma$ for all $k\ne i,j$. Denote by s the restriction of this relation to αr. Then $s\in S_0^\cup$ by Lemma 2.2. On the other hand, a straightforward computation shows that given $(i,j)\in u$ the set $s_{ij}=(u_{ij})_{\alpha r}$ coincides with the f-image of the relation $(\gamma_0 u\times\{i\})\times(\gamma_0 u^*\times\{j\})$. It follows that $e\cdot s_{ij}\cdot e=\Gamma_i^2\cup\Gamma_j^2\cup\Gamma_i\times\Gamma_j$. Thus the relation

$$\Big(\Gamma_0^2\otimes u)^f=\bigcup_{(i,j)\in u}((\Gamma_0\times\{i\})\times(\Gamma_0\times\{j\})\Big)^f$$
$$=\Big(\bigcup_{(i,j)\in u}e\cdot s_{ij}\cdot e\Big)\setminus e=(e\cdot s\cdot e)\setminus e$$

belongs to $S_0^\cup$, and we are done. □

Proof of Theorem 7.1. To prove the first statement without loss of generality we can assume that $b>0$, for otherwise, $|\Delta|=1$ and $\mathcal{Y}\uparrow L=\mathcal{Y}$. Besides, by Lemma 3.1 we have $gb(\mathcal{Y}_0)\le gb(\mathcal{Y})$ where $\mathcal{Y}_0$ is the coherent configuration defined in Lemma 7.3 with arbitrarily chosen point γ_0. Thus by Theorem 5.2 the coherent configuration $\mathcal{Y}_0\wr\mathrm{Inv}(L)$ has a proper generalized base Π_0 of size

$$b_0\le\max\{gb(\mathcal{Y}_0),b\}\le\max\{gb(\mathcal{Y}),b\}.$$

By Lemma 7.3 this implies that the coherent configuration $\mathcal{X}_0=(\mathcal{X}_\alpha)_{\alpha r}$ with $\alpha=\alpha(\gamma_0)$, has a generalized base Π of size b_0 that contains an element Λ_0 such that

$$0<|\Lambda_0\cap\Gamma_i|<|\Gamma_i|\quad\text{for all } i\in\Delta, \quad (31)$$

where the sets Γ_i are defined in (27). By the second statement of Lemma 7.2 the set Π is a generalized base of the coherent configuration $\mathcal{X}_\alpha$. Set Φ be the fiber of $\mathrm{Fis}(\mathcal{X},\Pi)$ that contains α. Then it suffices to verify that $\Phi=\{\alpha\}$ (indeed, in this case $\mathrm{Fis}(\mathcal{X},\Pi)\ge\mathrm{Fis}(\mathcal{X}_\alpha,\Pi)$ and we are done). To do this suppose that $\beta\in\Phi$. Then since $\alpha\in\Phi$, $\Lambda_0\subset\alpha r$ and Λ_0 is the union of fibers of $\mathrm{Fis}(\mathcal{X},\Pi)$, we have

$$\Lambda_0\subset\beta r. \tag{32}$$

Then obviously $d(\alpha,\beta)\le 2$. So without loss of generality we can assume that

$$\alpha_1=\gamma\ne\beta_1 \quad\text{and}\quad \alpha_3=\gamma=\beta_3 \tag{33}$$

(since L is a transitive group of odd order, we can assume that $m\ge 3$). However, by (31) there exists a point $\delta\in\Lambda_0\cap\Gamma_3$. Then by (33) we have $d(\delta,\beta)\ge 2$. So $\delta\notin\beta r$ which contradicts (32).

To prove the second statement suppose that the coherent configuration $\mathcal{Y}$ is not complete. Then the point $\gamma_0\in\Gamma$ can be chosen to belong a base of $\mathcal{Y}$ of size $b(\mathcal{Y})$. By Lemma 3.1 this implies that the coherent configuration $\mathcal{Y}_0$ has a base of size at most $b(\mathcal{Y})-1$. So by Theorem 5.3 the coherent configuration $\mathcal{Y}_0\wr\mathrm{Inv}(L)$ has a thin generalized base of size

$$b_0\le(b(\mathcal{Y})-1)+\max\{0,b-\lceil(b(\mathcal{Y})-1)/2\rceil\}. \tag{34}$$

By Lemma 7.3 this implies that the coherent configuration $\mathcal{X}_0$ has a generalized base Π of size b_0 such that $|\Lambda\cap\Gamma_i|\le 1$ for all $\Lambda\in\Pi$. By Lemma 7.2 any such Λ is of the form $\rho(\beta)$ for uniquely determined point $\beta=\beta(\Lambda)$ in Ω. Set

$$B_0=\{\beta(\Lambda):\ \Lambda\in\Pi\}.$$

Then $\mathrm{Fis}(\mathcal{X}_\alpha,B_0)\ge\mathrm{Fis}(\mathcal{X}_\alpha,\Pi)$ because $\rho(\beta)$ is a union of fibers of the coherent configuration $\mathcal{X}_{\alpha,\beta}$ for all $\beta\in B_0$. Now, the second statement of Lemma 7.2 shows that B_0 is a base of the coherent configuration $\mathcal{X}_\alpha$. Thus the set $B=B_0\cup\{\alpha\}$ is a base of $\mathcal{X}$. Moreover, $|B|=|\Pi|+1=b_0+1$ and the required statement follows from (34). □

§8. Indistinguishing number and base number

Let $\mathcal{X}=(\Omega,S)$ be a scheme. For points $\alpha,\beta\in\Omega$ denote by $\Omega_{\alpha,\beta}$ the set of all $\gamma\in\Omega$ such that $r(\alpha,\gamma)=r(\beta,\gamma)$. Set $s=r(\alpha,\beta)$. Then the number

$$|\Omega_{\alpha,\beta}|=\sum_{t\in S}c_{tt^*}^s \tag{35}$$

does not depend on the choice of $(\alpha,\beta)\in s$ and is denoted by $c(s)$; in [18] it was called the *indistinguishing number* of s. The maximal indistinguishing number of a non-reflexive basic relation of $\mathcal{X}$ is denoted by $c=c(\mathcal{X})$. It is easily seen that $c\geq 0$ and the equality is attained if and only if the scheme $\mathcal{X}$ is regular.

The number $n-c$ where $n=|\Omega|$, was called in paper [5] the distinguishing number of the scheme $\mathcal{X}$. It was proved there that if $\mathcal{X}$ is primitive and $|S|\geq 3$, then $b(\mathcal{X})\leq 4\sqrt{n}\log n$. In the following theorem we are interested in the base number when $\mathcal{X}$ is not necessarily primitive and c is rather small.

Theorem 8.1. *In the above notation suppose that* $4c(m-1)<n$ *where* $m=n_{max}$. *Then for any* $\alpha\in\Omega$ *the coherent configuration* $\mathcal{X}_\alpha$ *is* 1*-regular. In particular,* $b(\mathcal{X})\leq 2$.

Proof. Without loss of generality we can assume that $m\geq 2$, for otherwise the scheme $\mathcal{X}$ is regular, and the statement is obvious. Let $\alpha\in\Omega$ and $r\in S$. Given $\beta\in\Omega$ denote by Ω_β the set of all pairs $(\delta,\gamma)\in\alpha r\times\alpha r$ such that $\delta\neq\gamma$ and $\beta\in\Omega_{\delta,\gamma}$. Then it is easily seen that

$$|\Omega_\beta|=\sum_{s\in S}c_{rs}^t(c_{rs}^t-1)\geq\sum_{s\notin r\circ t}c_{rs}^t=\sum_{s\in S}c_{rs}^t-|r\circ t|=n_r-|r\circ t|$$

where $t=r(\alpha,\beta)$ and $r\circ t=\{s\in r^*t:\ c_{rs}^t=1\}$. This implies that if $\beta\in\alpha S_r'$ where S_r' is the set of all $t'\in S$ with $|r\circ t'|<n_r/2$, then the set Ω_β has at least $n_r/2$ elements. Therefore

$$|\alpha S_r'|\cdot\frac{n_r}{2}\leq\sum_{\beta\in\alpha S_r'}|\Omega_\beta|\leq|T| \tag{36}$$

where T is the union of all sets $\Omega_\beta\times\{\beta\}$ with $\beta\in\alpha S_r'$. However, for each pair $(\delta,\gamma)\in\alpha r\times\alpha r$ with $\delta\neq\gamma$ there are at most c points β such that $(\delta,\gamma)\in\Omega_\beta$. So the set T has at most $n_r(n_r-1)c$ elements. By (36) and the lemma hypothesis this implies that $|\alpha S_r'|\leq 2(n_r-1)c\leq 2(m-1)c<n/2$. Thus

$$|\alpha S_r|=n-|\alpha S_r'|>\frac{n}{2} \tag{37}$$

where $S_r=\{t\in S:\ |r\circ t|>n_r/2\}$ is the complement to S_r'.

To complete the proof we will show that any $\beta\in\Omega$ for which the relation $r=r(\alpha,\beta)$ is of valency m, is a regular point of the coherent

configuration $\mathcal{X}_\alpha$, i.e., that

$$\beta\, r_{\mathcal{X}_\alpha}(\beta,\gamma) = \{\gamma\} \tag{38}$$

for all $\gamma \in \Omega$. To do this set $u = r(\alpha,\gamma)$. Then inequality (37) implies that $|\alpha S_r| > n/2$ and $|\alpha S_u| > n/2$. Therefore the sets S_r and S_u contain a common relation, say v. It follows that neither $r \circ v$ nor $u \circ v$ is empty; take $s_\beta \in r \circ v$ and $s_\gamma \in u \circ v$. Then by the definition of $\circ$ one can find points β' and γ' in αv such that

$$\beta' s_\beta^* \cap \alpha r = \{\beta\} \quad \text{and} \quad \gamma' s_\gamma^* \cap \alpha u = \{\gamma\}. \tag{39}$$

Moreover, we have $|r \circ v| > n_r/2$ because $v \in S_r$. Therefore one can find two relations t_β and t_γ in $r \circ v$ such that

$$\beta' t_\beta^* \cap \alpha r = \{\delta\} = \gamma' t_\gamma^* \cap \alpha r \tag{40}$$

for some point $\delta \in \alpha r$. The obtained configuration is represented at Fig. 1. By Lemma 2.2 the set $(S_\alpha)^\cup$ contains the relations

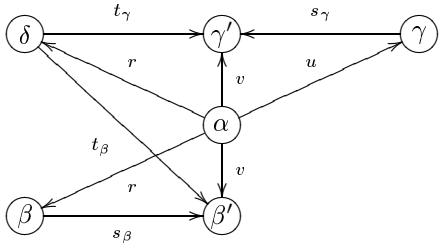

Fig. 1

$$a_1 = (s_\beta)_{\alpha r,\alpha v}, \quad a_2 = (t_\beta^*)_{\alpha v,\alpha r}, \quad a_3 = (t_\gamma)_{\alpha r,\alpha v}, \quad a_4 = (s_\gamma^*)_{\alpha v,\alpha u},$$

and hence the relation $a = a_1 \cdot a_2 \cdot a_3 \cdot a_4$. On the other hand, since $n_r = m$ and $v \in S_r$, from (4) it follows that $n_v = m$. This implies that $s_\beta^*, t_\beta^*, t_\gamma^* \in S(v,r)$. Therefore due to (39) and (40) we obtain that

$$\beta\, a_1 = \{\beta'\}, \quad \beta' a_2 = \{\delta\}, \quad \delta\, a_3 = \{\gamma'\}, \quad \gamma' a_4 = \{\gamma\}. \tag{41}$$

Thus $\beta\, r_{\mathcal{X}_\alpha}(\beta,\gamma) \subset \beta a = \{\gamma\}$ whence (38) follows. □

Corollary 8.2. *Let $G \le \mathrm{AGL}(\Omega)$ be an affine group acting on a linear space Ω over a finite field, and K a one point stabilizer of G. Suppose that*

$$4(k-1)\,\mathrm{Fix}(K) < n. \tag{42}$$

where $n = |\Omega|$ and $k = |K|$. Then $b(\mathrm{Inv}(G)) \le 2$. In particular, this is always true whenever $4k(k-1)f < n$ where $f = \mathrm{fix}(K)$.

Proof. Let α be the zero vector of the space Ω. Choose a point β of the scheme $\mathcal{X} = \mathrm{Inv}(G)$ such that

$$c = c(s) = |\Omega_{\alpha,\beta}| \tag{43}$$

where $s = r(\alpha, \beta)$. Obviously, α and β are in the same orbit of G_γ for all $\gamma \in \Omega_{\alpha,\beta}$. Therefore any such γ is a fixed point of an appropriate permutation belonging to the set $G_{\alpha\to\beta} = \{a \in G : \ \alpha^a = \beta\}$. It follows that

$$|\Omega_{\alpha,\beta}| \le \mathrm{Fix}(G_{\alpha\to\beta}). \tag{44}$$

On the other hand, any $a \in G_{\alpha\to\beta}$ is an affine mapping on Ω, say $x \mapsto hx + x_0$ where $h \in G_\alpha$ and $x_0 = \beta - h\alpha$. So the numbers $\mathrm{fix}(a)$ and $\mathrm{fix}(h)$ are equal respectively to the numbers of solutions of linear equation systems $(e-h)x = x_0$ and $(e-h)x = 0$ where e is the identity matrix. When $h \ne e$, the latter two numbers are equal. Therefore the right-hand side of (44) coincides with $\mathrm{Fix}(G_\alpha) = \mathrm{Fix}(K)$ (the latter is because G_α and K are conjugate in G). Thus by(43) and (44) we have

$$c \le \mathrm{Fix}(K). \tag{45}$$

Besides, by the definition of $\mathcal{X}$ the set αr with $r \in S$, is an orbit of the group G_α. Therefore $n_r = |\alpha r| \le |G_\alpha| = k$, and hence $m = n_{max} \le k$. By (45) and (42) this implies that

$$4(m-1)c \le 4(k-1)\,\mathrm{Fix}(K) < n.$$

Thus the required statements follow from Theorem 8.1 and obvious inequality $\mathrm{Fix}(K) \le (k-1)f$. □

§9. Base of linearly primitive antisymmetric scheme

In this section, we will prove that, in fact, the base number of a linearly primitive antisymmetric scheme coincides with the base number of its automorphism group. The proof given here does not use the fact that the latter number is at most 3.

Theorem 9.1. *The base number of a linearly primitive antisymmetric scheme is at most* 3 *and the equality is attained only when the scheme is cyclotomic.*

In what follows we fix an affine group $G \le \mathrm{AGL}(d,p)$ such that the scheme $\mathcal{X} = \mathrm{Inv}(G)$ is antisymmetric and linearly primitive. By Theorem 2.3 the zero stabilizer in G is an irreducible primitive group $K \le \mathrm{GL}(d,p)$ of odd order. For this group we keep the notation of Theorem 4.1. In the following three lemmas we will verify that

$$e > 1 \;\Rightarrow\; b(\mathcal{X}) \le 2. \tag{46}$$

Along the proof we will subsequently exclude by means of Lemma 3.4 and Corollary 8.2 the values of e for which the implication could be violate.

Lemma 9.2. *The implication* (46) *holds unless the quadruple* (e,a,d,p) *is one of the following:*

(E1) $(e,a,d) = (9,1,9)$ *and* $p \in \{7,13,19,31,37,43\}$,
(E2) $(e,a,d,p) = (5,4,20,3)$, $(5,3,15,11)$ *or* $(5,2,10,11)$,
(E3) $(e,a,d) = (5,1,5)$ *and* $p \in \{11,\dots,5591\}$, $p = 1 \mod 5$.

Proof. Suppose that the parameters e,a,d,p of the group K do not form a quadruple from the lemma statement. By Corollary 8.2 it suffices to verify that $p^d > 4k^2 f$ where $k = |K|$ and $f = \mathrm{fix}(K)$. However, $f \le p^{\lfloor 4d/9 \rfloor}$ by Theorem 4.3. Therefore due to (17) the required inequality is a consequence of the following one:

$$p^d > 4 \cdot (u_{a,p} \cdot e^2 \cdot s_e \cdot a_0)^2 \cdot p^{\lfloor 4d/9 \rfloor}. \tag{47}$$

Here $ae \le d$ by statement (P4) of Theorem 4.1. Therefore $a_0 \le a \le d/e$ and $2u_{a,p} \le p^a \le p^{d/e}$. Besides, by the second and the third statements of Lemma 4.2 we have $s_e \le e^2/2$. Consequently, $4 \cdot u_{a,p} \cdot s_e \cdot a_0 \le p^{d/e} \cdot d \cdot e$. Thus to check inequality (47) it suffices to verify that

$$4 \cdot p^{d - \lfloor 4d/9 \rfloor} > p^{2d/e} \cdot d^2 e^6. \tag{48}$$

A direct computation shows that $4 \cdot 3^{14d/27} > d^8$ for all $d \ge 54$. Therefore for all integers $e \ge 54$ and all primes $p \ge 3$ the inequality

$$4 \cdot p^{d - \lfloor 4d/9 \rfloor - 2d/e} \ge 4 \cdot 3^{(5/9 - 2/54)d} = 4 \cdot 3^{14d/27} > d^8 \ge d^2 e^6.$$

holds for all $d \ge e$. This proves the required statement for all $e \ge 54$.

Denote by $d(e,p)$ the minimal positive integer d for which inequality (48) holds for a fixed e and p, and by $p(a,e)$ the minimal element in the set $P(a,e)$ of all odd primes q such that each prime divisor of e divides $q^a - 1$. Then by statements (P2) and (P4) of Theorem 4.1 and by Lemma 4.2 without loss of generality we can assume that

(C1) $e \in \{5,\dots,53\}$ is an odd integer other than 7,

(C2) when e is fixed, $a \in \{1, \dots, \lfloor d_0/e \rfloor\}$ where $d_0 = d(e,3)$,
(C3) when e and a are fixed, $p \in P(a,e)$.

For each e satisfying (C1) we list in the Table 1 below the values of the function $d_3 = d(e,3)$ (the second row), the possible values for the integer a (the third row), and for a fixed a also the values of the functions $p_a = p(a,e)$ and $d_p = d(e,p_a)$ (the fourth and the fifth rows, respectively).[6]

Table 1

e	53	51	49	47	45	43	41	39	37	35
	33	31	29	27	25					
d_3	54	54	53	53	53	53	52	52	52	51
	51	51	50	50	50					
a	1	1	1	1	1	1	1	1	1	1
	1	1	1	1	1,2					
p_a	107	103	29	283	31	173	83	79	149	71
	67	311	59	7	11					
d_p	12	12	16	10	16	10	12	12	10	12
	12	9	12	27	22					

e	33	31	29	27	25	23	21		19	
d_3	51	51	50	50	50	49	49		49	
a	1	1	1	1	1,2	1,2	1	2	1	2
p_a	67	311	59	7	11	47	43	13	191	37
d_p	12	9	12	27	22	13	13	20	9	14

e	17		15		13		11	9		5
d_3	49		49		50		51	55		103
a	1	2	1,3	2	1,2	**3**	**1**,2,3,4	**1**,**3**,5	**2**,4,6	1..20
p_a	103	67	31	11	53	3	23	7	5	3,11
d_p	10	12	14	21	12	50	16	29	36	55,43

From the above definitions it follows that for a fixed pair (e,a) satisfying conditions (C1) and (C2) and such that $d(e,p_a) \le ea$, inequality (48) holds for all $d \ge ae$ and $p \in P(a,e)$. This enables us to find all the pairs for which

[6] When $e = 5$, we have $p_a = 3$ and $d(e,p_a) = 55$ for $a = 0 \mod 4$, and $p_a = 11$ and $d(e,p_a) = 43$ otherwise.

inequality (48) does not hold for at least one $p \in P(a,e)$ (the corresponding values of a in Table 1 are written in bold script):

- $(e,a) = (13,3)$ or $(11,1)$,
- $e = 9$ and $a \in \{1,2,3\}$,
- $e = 5$ and $a \in \{1,\dots,8\}$.

For each of these pairs we have to check inequality (47) for all positive integers $d \le d(e,3)$ which is a multiple of ae. The *available* triples (e,a,d), i.e. those that are obtained in this way, are listed in the first three rows of Table 2 below.[7] In the fourth and the fifth rows of this table we give respectively the values $p = p(a,e)$ and $q = q(e,a,d)$ where the latter number is equal to the minimal prime in $P(a,e)$ for which

$$q^{d-\lfloor 4d/9 \rfloor} > 4 \cdot ((q^a - 1)/t_a \cdot e^2 \cdot s_e \cdot a_0)^2; \tag{49}$$

Here the integer t_a is defined as follows: if a is odd, then $t_a = 2$, otherwise $t_a = 2^{t+2}$ where t is the maximal positive integer such that 2^t divides a. Then obviously t_a divides $p^a - 1$ for any odd prime p, and hence $u_{a,p} \le (p^a - 1)/t_a$. Thus the required inequality (47) follows from (49). In the computation of q we used the values of s_e (and in cases $(e,a,d) = (5,3,15)$ and $(5,5,25)$ also the equality $|K : F| = 3$) given in the second statement of Lemma 4.2.

Table 2

e	13	11	9	9	9	9	5	5	5
a	3	1	1	1	3	2	4	4	8
d	39	11	**9**	18	27	18	**20**	40	40
p	3	23	7	7	7	5	3	3	3
q	3	23	61	5	5	5	7	3	3
e	5	5	5	5	5	5	5	5	5
a	1	1	2	2	3	3	5	6	7
d	**5**	10	**10**	20	**15**	30	25	30	35
p	11	11	11	11	11	11	11	11	11
q	5641	11	19	3	31	3	11	7	11

It follows from the definition of q that if (e,a,d) is one of the available triples and $q \le p$, then inequality (47) holds for all $p \in P(a,e)$. The

[7] We did not cited in the table some available triples, like (e,a,d) with $d \ge 22$ and $(e,a) = (11,1)$, because if the inequality (49) holds for some d, then it holds also for largest d's.

remaining 5 triples are the following: $(9,1,9)$, $(5,4,20)$, $(5,1,5)$, $(5,2,10)$ and $(5,3,15)$ (the corresponding values of d in Table 2 are written in bold script). For any of them the inequality (47) does not hold only for those quadruples (e,a,d,p) in which

$$p \in P(a,e) \cap \{1,\dots,q-1\}.$$

A straightforward check shows that these quadruples are exactly those listed in the lemma statement. □

Lemma 9.3. *The implication* (46) *holds unless* $(e,a,d) = (9,1,9)$ *and* $p \in \{7,19\}$, *or* $(e,a,d) = (5,1,5)$ *and* $p \in \{11,31,41,61,71,101,151,181,271\}$.

Proof. Given a prime q denote by k_q the number of all non-identity elements $g \in K$ the order of which is a power of q; the maximum of $\mathrm{fix}(g)$ over all these elements g is denoted by f_q. Clearly, this maximum is achieved on the elements of order q. The number $f_{q'}$ is defined in a similar way: the maximum is taken over all non-identity elements $g \in K$ the order of which is not a power of q. Then it is easily seen that $\mathrm{Fix}(K) \le k_q f_q + (k-k_q) f_{q'}$. So by Corollary 8.2 it suffices to prove that the inequality

$$p^d > 4(k-1)(k_q f_q + (k-k_q) f_{q'}). \tag{50}$$

holds for an appropriate prime divisor q of $k = |K|$. By Lemma 9.2 it suffices to check this inequality only for those groups K the parameters (e,a,d,p) of which are listed in the statement of this lemma.

Let $(e,a,d) = (9,1,9)$ and $p \in \{13,31,37,43\}$. Then from Theorem 4.1 it follows that $K = A$, $|F:U| = 3^4$ and U is a central subgroup of K. Besides, by Lemma 4.2 we also have $|A:F| = s_e = 5$. Thus

$$k = |F| \cdot 5 \quad \text{divides} \quad p_0 := \frac{p-1}{2} \cdot 3^4 \cdot 5.$$

It follows that the order of a Sylow 5-subgroup of K is 5 or 25 depending on whether $p \in \{13,37,43\}$ or $p = 31$; in the former case $k_5 = 4 \cdot 3^4$, whereas in the latter one $k_5 = 20 \cdot 3^4$. Moreover, in any case one can easily deduce from Lemma 4.3 that $f_5 \le p^{\lfloor d/5 \rfloor} = p$ and $f_{5'} \le p^{d/3} = p^3$. Thus

$$k_5 f_5 + (k-k_5) f_{5'} \le k_5 p + (p_0 - k_5) p^3.$$

A straightforward computation shows that the right-hand side of this inequality is less than $p^9/4(k-1)$ for $p \in \{13,31,37,43\}$. This proves required inequality (50) in our case.

A similar argument works when the quadruple (e,a,d,p) is equal to $(5,4,20,3)$, $(5,3,15,11)$ or $(5,2,10,11)$. In all these cases $|K:F|=3$ by Lemma 4.2. From now on we always assume that the group U is the maximal odd subgroup of the multiplicative subgroup of $\mathrm{Span}(U)=\mathrm{GF}(p^a)$ (the base of a scheme is not decreased under taking a fusion). Then from Theorem 4.1 and Lemma 4.3 it follows that $k=75\cdot u$ with $u=|U|$, $f_3\le p^{\lfloor 4d/9\rfloor}$ and

- if $(e,a,d,p)=(5,4,20,3\ )$, then $u=5$, $k_3=5^2\cdot 2$ and $f_{3'}\le p^4$,
- if $(e,a,d,p)=(5,3,15,11)$, then $u=35\cdot 19$, $k_3\le 7\cdot 19\cdot 5^2\cdot 2$ and $f_{3'}\le p^3$,
- if $(e,a,d,p)=(5,2,10,11)$, then $u=15$, $k_3=5^2\cdot 6$ and $f_{3'}\le p^2$.

In all these cases inequality (50) with $q=3$ follows by a straightforward computation (for $d=15$ we have even more strong inequality in which the summand $(k-k_q)f_{q'}$ is replaced by $kf_{q'}$).

Let $(e,a,d)=(5,1,5)$ and p belongs to the set $\mathcal{P}_0$ of all primes $q\le 5591$ such that $q=1\,(\mathrm{mod}\ 5)$. In this case as before we have: $K=A$, $|A:F|=3$, $|F:U|=5^2$ and U is a central subgroup of K (Theorem 4.1 and Lemma 4.2). Thus

$$k=|F|\cdot 3 \quad \text{divides} \quad \frac{p-1}{2}\cdot 5^2\cdot 3. \tag{51}$$

A straightforward computation for all $p\in\mathcal{P}_0$ shows that the order of a Sylow 3-subgroup of the group K equals to 3^{t_p} where $1\le t_p\le 6$. By Lemma 4.3 we have

$$k_3=25(3^{t_p}-3^{t_p-1}),\quad f_3\le p^{\lfloor 4d/9\rfloor}=p^2,\quad f_{3'}\le p^{\lfloor d/3\rfloor}=p \tag{52}$$

Next, given a positive integer t denote by $p_0=p_0(t)$ the minimal prime in $\mathcal{P}_0$ for which 3^{t-1} divides $(p_0-1)/2$, and by $p_1=p_1(t)$ the maximal real root of the polynomial

$$g_t(x)=x^5-4\cdot(x'-1)\cdot(t'x^2+(x'-t')x).$$

where $x'=75(x-1)/2$ and $t'=25(3^t-3^{t-1})$. When $t=t_p$ and $x=p$, we obtain from (51) and (52) that $x'\ge k$ and $t'=k_3$. Therefore

$$p^5\ge p^5-g_{t_p}(p)\ge 4\cdot(k-1)\cdot(k_3f_3+(k-k_3)f_{3'}).$$

On the other hand, it is easily seen that $g_t(p)>0$ for all $t\ge 1$ and all $p>p_1(t)$. Thus inequality (50) does not hold only if $t\in\{1,\dots,6\}$ and $p\in\mathcal{P}_0$ is such that $p_0(t)\le p\le p_1(t)\}$. In the Table 3 we present computed values of the functions $p_0(t)$ and $p_1(t)$. It follows that the required inequality

does not hold only if (p,t) is one of the following pairs: $(271,4)$, $(181,3)$, $\{31,61,151\}\times\{2\}$ and $\{11,41,71,101\}\times\{1\}$. Thus the proof in this case is completely done. □

Table 3

t	1	2	3	4	5	6
p_0	11	31	181	271	811	4861
$\lfloor p_1 \rfloor$	113	166	269	455	782	1351

Lemma 9.4. *The implication* (46) *holds for all* $e>1$.

Proof. We recall that the set Ω is identified with a d-dimensional linear space over a field $\mathrm{GF}(p)$ and the group G contains the translation group of Ω. Denote by α the zero vector of Ω. Then given $r\in S$ and $\beta\in\alpha r$ the intersection number c^r_{ts} is equal to the number of all $\gamma\in\alpha t$ for which $r(\gamma,\beta)=s$. Besides, it is easily seen that $r(\gamma,\beta)=r(\gamma',\beta)$ if and only if $\gamma-\beta\in(\gamma'-\beta)^K$ for all γ'. Thus

$$c^r_{ts}=|\Delta_\beta(t)| \tag{53}$$

where $\Delta_\beta(t)$ the set of all sets $(\gamma-\beta)^K\cap(\alpha t-\beta)$ with $\gamma\in\alpha t$ and $\alpha t-\beta$ is the set of all vectors $\gamma'-\beta$ with $\gamma'\in\alpha t$. Then using (53) for $t=r$ and $t=r^*$ we can compute the numbers $r\circ_2 r$ and $|r\circ_2 r^*|$ defined before Lemma 3.4 as follows:

$$|r\circ_2 r|=|\{\Delta\in\Delta_\beta(r):\ |\Delta|\le 2\}|=:a_r$$

and

$$|r\circ_2 r^*|=|\{\Delta\in\Delta_\beta(r^*):\ |\Delta|\le 2\}|=:b_r$$

(in the second case we used equalities $c^{r^*}_{rs}=c^r_{s^*r^*}=c^r_{r^*s^*}$ that follow from (4)). Our goal is to find a relation $r\in S$ such that

$$a_r+b_r>2n_r/3. \tag{54}$$

Then Lemma 3.4 implies that $b(\mathcal{X})\le 2$, and we are done. To find such r we can assume that (e,a,d,p) is one of the quadruples listed in the statement of Lemma 9.3.

Suppose first that $(d,p)=(9,7)$. Denote by E an extraspecial group of order 3^5 and exponent 3. Then $K=A$ is isomorphic to a semidirect product $K_0=E.5$ in which the group of order 5 acts irreducibly on $E/Z(E)$.

By means of GAP we found that K_0 is uniquely determined up to isomorphism (there is a unique non-nilpotent group of order $3^5 \cdot 5$ with a nonabelian Sylow 3-subgroup). Moreover, up to equivalence there are exactly two classes of irreducible d-dimensional K_0-modules over $\mathrm{GF}(p)$. For both of them we constructed in GAP generators for the corresponding primitive subgroup of $\mathrm{GL}(d,p)$ isomorphic to K (see Section 4). Then we fixed a standard linear base $\{e_1,\dots,e_d\}$ in $\mathrm{GF}(p)^d$ and took

$$\beta = e_1 + e_2 + e_5 \quad \text{and} \quad r = r(\alpha,\beta).$$

A straightforward computation shows that in both cases $n_r = |\beta^K| = |K| = 1215$, $a_r = 1035$ and $b_r \geq 754$. Therefore inequality (54) do hold and we are done.

The computation in each of the remaining case is essentially the same as in the above case $(d,p) = (9,7)$. The minor differences are the following. In the case $(d,p) = (9,19)$ we have $K = \langle K_0, \xi_p I_d\rangle$ where I_d is the identity matrix in $\mathrm{GL}(d,p)$, and $\xi_p \in \mathrm{GF}(p)$ is a generator of the maximal multiplicative $2'$-subgroup in $\mathrm{GF}(p)$ (in our case, the subgroup of order 9). In the case $(5,p)$ the group E is an extraspecial group of order 5^3 and exponent 5, K_0 is a semidirect product $E.3$ in which the group of order 3 acts irreducibly on $E/Z(E)$, and $K = \langle K_0, \xi_p I_d\rangle$. The computation results cited in the Table 4 below

Table 4

	$(9,9,1)$		$(5,5,1)$								
p	7	19	11	31	41	61	71	101	151	181	271
β	$e_1+e_2+e_5$		e_1+e_2								
n_r	1215	3645	375	1125	375	1125	2625	1875	5625	3375	10125
a_r	1035	3483	199	987	361	1061	2413	1755	5221	3199	9421
b_r	754	1697	99	469	160	526	1181	853	2585	1563	4685
N	2	2	4	12	4	12	4	4	12	12	12

show that inequality (54) holds in all the cases (in the last row in the table we gives the number of the classes of irreducible d-dimensional K_0-modules over $\mathrm{GF}(p)$; the values a_r and b_r correspond to the K_0-module with minimal sum $a_r + b_r$). □

Proof of Theorem 9.1. Let $\mathcal{X} = \mathrm{Inv}(G)$ where $G \leq \mathrm{AGL}(d,p)$ is an affine group with primitive zero stabilizer $K \leq \mathrm{GL}(d,p)$ of odd order,

p is an odd prime. Then from Lemmas 9.4 and 4.2 it follows that K is contained in the unique Hall $2'$-subgroup K^* of the group $\Gamma\mathrm{L}(1,p^d)$. It is easily seen that $\mathrm{Orb}(K^*,\Omega)=\mathrm{Orb}(K',\Omega)$ where K' is the maximal odd order multiplicative group of the field $\mathbb{F}=\mathrm{GF}(p^d)$. Thus

$$\mathcal{X}=\mathrm{Inv}(G)\geq\mathrm{Inv}(G^*)=\mathrm{Inv}(G')=:\mathcal{X}' \tag{55}$$

where $G^*=AK^*$ and $G'=AK'$ with A being the translation group of the linear space Ω. However, $\mathcal{X}'$ is a cyclotomic scheme over the field $\mathbb{F}$. Therefore $b(\mathcal{X}')\leq 3$ by Theorem 3.2. Thus by (55) we conclude that $b(\mathcal{X})\leq b(\mathcal{X}')\leq 3$ which completes the proof. □

§10. The proofs of Theorems 1.1, 1.2 and 1.4

10.1. Proof of Theorem 1.2. We argue by induction on the degree of a schurian antisymmetric coherent configuration $\mathcal{X}=\mathrm{Inv}(G)$. By the first inequality in (9), we can assume that it is homogeneous. Suppose that $\mathcal{X}$ is imprimitive. Then there is a nontrivial equivalence relation $e\in S^{\cup}$. The schemes $\mathcal{X}_1=\mathcal{X}_\Gamma$ where $\Gamma\in\Omega/e$, and $\mathcal{X}_2=\mathcal{X}_{\Omega/e}$ are obviously antisymmetric and schurian. Moreover, $\mathcal{X}$ is isomorphic to a fission of the scheme $\mathcal{X}_1\wr\mathcal{X}_2$. By Corollary 5.2 this implies that

$$gb(\mathcal{X})\leq gb(\mathcal{X}_1\wr\mathcal{X}_2)\leq\max\{gb(\mathcal{X}_1),gb(\mathcal{X}_2)\}$$

and we are done by induction.

Suppose that the scheme $\mathcal{X}$ is primitive. Then by Theorem 2.3 it is either linearly imprimitive or linearly primitive. In the former case $\mathcal{X}$ has a nontrivial fusion isomorphic to $\mathcal{Y}\uparrow L$ where $\mathcal{Y}$ is a linearly primitive antisymmetric scheme and L is a transitive group of odd order (Theorem 6.1). Thus by induction and Theorem 7.1 we have

$$gb(\mathcal{X})\leq gb(\mathcal{Y}\uparrow L)\leq\max\{gb(\mathcal{Y}),gb(\mathrm{Inv}(L))\}\leq 1.$$

To complete the proof suppose that $\mathcal{X}$ is linearly primitive. If it is cyclotomic, then we are done by Theorem 3.2. Otherwise by Theorem 9.1 it has a base $B=\{\alpha,\beta\}$ where α and β are two (possibly equal) points in Ω. In this case

$$\mathrm{Fis}(\mathcal{X},\{B\})=\mathcal{X}_{\alpha,\beta}$$

because the scheme $\mathcal{X}$ is antisymmetric. Thus $gb(\mathcal{X})\leq 1$ and we are done. □

10.2. Proof of Theorem 1.1. By Theorem 2.3 the scheme $\mathcal{X} = \mathrm{Inv}(G)$ is either linearly imprimitive or linearly primitive. In the latter case we are done by Theorem 9.1. In the former case $\mathcal{X}$ has a nontrivial fusion isomorphic to $\mathcal{Y} \uparrow L$ where $\mathcal{Y}$ is a linearly primitive antisymmetric scheme and L is a transitive group of odd order (Theorem 6.1). In particular, the scheme $\mathcal{Y}$ is not complete. Besides, $b(\mathcal{Y}) \le 3$ by Theorem 9.1 and $b := gb(\mathrm{Inv}(L)) = 1$ by Theorem 1.2. This implies by Theorem 7.1 that

$$b(\mathcal{X}) \le b(\mathcal{Y} \uparrow L) \le b(\mathcal{Y}) + \max\{0, 1 - \lceil (b(\mathcal{Y}) - 1)/2 \rceil\}.$$

When $b(\mathcal{Y}) = 1, 2, 3$, the right-hand side of the above inequality is equal respectively to $2, 2, 3$. In any case $b(\mathcal{X}) \le 3$, and we are done. □

10.3. Algorithm. We will deduce Theorem 1.4 from Theorem 1.3 proved below. The algorithm constructed in the proof of the latter theorem is, in a sense, a combinatorial version of the Babai–Luks algorithm from [6]. The following statement to be used in the proof of Theorem 1.3 is a special case of Corollary 3.6 of that paper. In what follows we always assume that any permutation group on the input or output of an algorithm is given by a generator set of polynomial size in the degree of the group.

Theorem 10.1. *Let $G \le \mathrm{Sym}(\Omega)$ be a solvable group of degree n. Then given a coherent configuration $\mathcal{X}$ on Ω, the group $\mathrm{Aut}(\mathcal{X}) \cap G$ can be found in time $n^{O(1)}$.*

To apply Theorem 10.1 we have to be able to construct the group G. This will be done by means of Corollary 3.6 and the following statement proved in [3, Lemma 3.4]. Below for permutation groups $G_1, \dots, G_s$, $s \ge 1$, we define the group $\mathrm{Wr}(G_1, \dots, G_s)$ to be the iterated wreath product $(\cdots (G_1 \wr G_2) \wr \cdots) \wr G_s$ in imprimitive action.

Lemma 10.2. *Let $\mathcal{X}$ be a scheme and $1_\Omega = e_0 \subset e_1 \subset \ldots \subset e_s = \Omega^2$ a series of equivalence relations in $S^\cup$. Suppose that for $i = 1, \dots s$ a permutation group G_i on a set Δ_i and a family of bijections $f_\Gamma : \Gamma \to \Delta_i$ where $\Gamma \in \Omega_i$ with $\Omega_i = \{\Gamma'/e_{i-1} : \Gamma' \in \Omega/e_i\}$, form a majorant of $\mathrm{Aut}(\mathcal{X})$ with respect to the pair (e_{i-1}, e_i). Then the mapping*

$$f : \Omega \to \prod_{i=1}^{s} \Delta_i, \quad \alpha \mapsto (\dots, f_i(\Gamma_{i-1}), \dots)$$

is a bijection and $\mathrm{Aut}(\mathcal{X})^f \le \mathrm{Wr}(G_1, \dots, G_s)$ where $f_i = f_{\Gamma_i}$ and Γ_{i-1} and Γ_i are respectively the classes of e_{i-1} and e_i containing α.

Proof of Theorem 1.3. To describe the algorithm we need the auxiliary procedure $\mathrm{Test}(\mathcal{X}, G)$ that given a coherent configuration $\mathcal{X} = (\Omega, S)$ and a group $G \le \mathrm{Sym}(\Omega)$ output G or empty set depending whether or not $\mathcal{X} = \mathrm{Inv}(G)$. Since the latter equality exactly means that $S = \mathrm{Orb}(G, \Omega^2)$, the procedure can be implemented in polynomial time in $|\Omega|$ by means of a standard algorithm finding the orbits of a permutation group (see e.g. [20]).

Schurity Recognition Algorithm

Input: an antisymmetric coherent configuration $\mathcal{X}$.
Output: the group $\mathrm{Aut}(\mathcal{X})$, or $\mathcal{X}$ is not schurian.

Step 1. If $\mathcal{X}$ is not homogeneous, then recursively apply the algorithm to the coherent configuration $\mathcal{X}_1 = \mathcal{X}_{\Delta_1}$ and $\mathcal{X}_2 = \mathcal{X}_{\Delta_2}$ where Δ_1 is a fiber of $\mathcal{X}$ and Δ_2 is its complement. If either $\mathcal{X}_1$ or $\mathcal{X}_2$ is not schurian, then so is $\mathcal{X}$, else output $\mathrm{Test}(\mathcal{X}, H)$ where $H \le \mathrm{Sym}(\Omega)$ is the group found by the algorithm of Theorem 10.1 for $G = \mathrm{Aut}(\mathcal{X}_1) \times \mathrm{Aut}(\mathcal{X}_2)$.

Step 2. Find a maximal series of equivalence relations as in the hypothesis of Lemma 10.2. If there exist $i \in \{1, \dots, s\}$ and $\Gamma, \Gamma' \in \Omega_i$ such that

$$b(\mathcal{X}_\Gamma) > 3 \quad \text{or} \quad \mathrm{Iso}(\mathcal{X}_\Gamma, \mathcal{X}_{\Gamma'}, \varphi_{\Gamma,\Gamma'}) = \varnothing \tag{56}$$

where $\varphi_{\Gamma,\Gamma'}$ is the algebraic isomorphism (6) for $\mathcal{X} = \mathcal{X}_{\Omega/e_{i-1}}$, then $\mathcal{X}$ is not schurian.

Step 3. By the algorithm of Corollary 3.6 find a majorant of $\mathrm{Aut}(\mathcal{X})$ with respect to (e_{i-1}, e_i), say $G_i \le \mathrm{Sym}(\Delta_i)$ and $\{f_\Gamma\}_{\Gamma \in \Omega_i}$ for $i = 1, \dots s$.

Step 4. Output $\mathrm{Test}(\mathcal{X}, H)$ where $H = \mathrm{Aut}(\mathcal{X}) \cap G^{f^{-1}}$ is the group found by the algorithm of Theorem 10.1 with $G = \mathrm{Wr}(G_1, \dots, G_s)$ and f as in Lemma 10.2.

To prove the correctness of the algorithm suppose first that the coherent configuration $\mathcal{X}$ is not homogeneous. Then it is schurian only if so are the coherent configurations $\mathcal{X}_1$ and $\mathcal{X}_2$ found at Step 1, and, moreover,

$$\mathrm{Aut}(\mathcal{X}) \le \mathrm{Aut}(\mathcal{X}_1) \times \mathrm{Aut}(\mathcal{X}_2)$$

where the group in the right-hand side has odd order. Thus the correctness in this case follows from Theorem 10.1. Let $\mathcal{X}$ be homogeneous. Then it is schurian only if for all Γ and Γ' defined at Step 2 we have

$$\mathcal{X}_\Gamma = \mathrm{Inv}(\mathrm{Aut}(\mathcal{X})^\Gamma) \quad \text{and} \quad \mathrm{Aut}(\mathcal{X})_{\Gamma \to \Gamma'} \subset \mathrm{Iso}(\mathcal{X}_\Gamma, \mathcal{X}_{\Gamma'}, \varphi_{\Gamma,\Gamma'})$$

where $\mathrm{Aut}(\mathcal{X})_{\Gamma\to\Gamma'}$ is the set of all bijections from Γ onto Γ' induced by the automorphisms of $\mathcal{X}$. On the other hand, the maximality condition in choosing e_i's implies that under the schurity assumption each scheme $\mathcal{X}_\Gamma$ is also primitive. Therefore by Theorem 1.1 in our case $b(\mathcal{X}_\Gamma)\le 3$ for all Γ. Thus the relations (56) imply that $\mathcal{X}$ is not schurian, and the output of Step 3 is correct. Now, the correctness of the output at Step 4 follows from Lemma 10.2. Finally a polynomial bound for the running time of the algorithm follows from Theorem 10.1 and Corollary 3.6. □

10.4. Proof of Theorem 1.4. Given a colored tournament T denote by $\mathcal{X}=\mathcal{X}(T)$ the coherent configuration $\mathcal{X}(T)=\mathrm{Fis}(\mathcal{S})$ where $\mathcal{S}$ is the set of color classes of the arc set of T. Then T is schurian if and only if the coherent configuration $\mathcal{X}$ is schurian. Since the latter can be constructed in time $n^{O(1)}$ where n is the number of vertices of T (see Subsection 2.8), statements (1) and (2) immediately follow from Theorem 1.3.

To prove statement (3) let T_i be a colored schurian tournament, $\mathcal{S}_i$ the set of color classes of the arc set of T_i and $\mathcal{X}_i=\mathcal{X}(T_i)$, $i=1,2$. Then by Theorem 2.4 without loss of generality we can assume that there exists an algebraic isomorphism $\varphi:\mathcal{X}_1\to\mathcal{X}_2$ such that

$$\mathcal{S}_1^\varphi=\mathcal{S}_2 \tag{57}$$

(for otherwise $\mathrm{Iso}(T_1,T_2)=\varnothing$). In this case $\mathrm{Iso}(T_1,T_2)=\mathrm{Iso}(\mathcal{X}_1,\mathcal{X}_2,\varphi)$. To construct the latter set take a copy $\mathcal{X}_3$ of the coherent configuration $\mathcal{X}_2$. Set

$$\mathcal{W}=\{\mathcal{X}_i\}_{i=1}^3 \quad\text{and}\quad \Psi=\{\psi_{i,j}\}_{i,j=1}^3$$

where $\psi_{i,j}:\mathcal{X}_i\to\mathcal{X}_j$ is an algebraic isomorphism defined as follows (below S_i denotes the set of basic relations of $\mathcal{X}_i$):

- $\psi_{i,j}=\mathrm{id}_{S_i}$ if $i=j$ or $\{i,j\}=\{2,3\}$,
- $\psi_{i,j}=\varphi$ if $1=i\ne j$,
- $\psi_{i,j}=\varphi^{-1}$ if $i\ne j=1$.

According to [8, Definition 7.1] there exists the smallest coherent configuration $\mathcal{X}$ on the disjoint union $\Omega=\Omega_1\cup\Omega_2\cup\Omega_3$ where Ω_i is the point set of $\mathcal{X}_i$, such that

$$\mathcal{X}_{\Omega_i}=\mathcal{X}_i \quad\text{and}\quad \mathcal{X}_{\Omega/e}=\mathrm{Inv}(G)$$

where $i=1,2,3$, $e=\Omega_1^2\cup\Omega_2^2\cup\Omega_3^2$ and G is the cyclic subgroup of $\mathrm{Sym}(3)$. It was also proved there (see [8, Corollary 7.9]) that $\mathcal{X}$ is schurian if and only if $\mathcal{X}_i$ is schurian for all i and the algebraic isomorphism $\psi_{i,j}$ is induced by an isomorphism for all i,j. In our case the former condition is

obviously satisfied, whereas the latter one is satisfied if and only if the set $\mathrm{Iso}(\mathcal{X}_1, \mathcal{X}_2, \varphi)$ is not empty.

To complete the proof we note that the coherent configuration $\mathcal{X}$ is antisymmetric. Therefore by Theorem 1.3 one can test whether or not $\mathcal{X}$ is schurian and (if so) find the group $\mathrm{Aut}(\mathcal{X})$ in time $n^{O(1)}$. Now, if $\mathcal{X}$ is not schurian, then by the above

$$\mathrm{Iso}(\mathcal{X}_1, \mathcal{X}_2, \varphi) = \varnothing.$$

On the other hand, if $\mathcal{X}$ is schurian, then by means of standard permutation group algorithms (see e.g. [20]) one can efficiently find an element $g \in \mathrm{Aut}(\mathcal{X})$ such that $\Omega_1^g = \Omega_2$, and the setwise stabilizer H of the set Ω_1 in the group $\mathrm{Aut}(\mathcal{X})$. Since in this case obviously

$$\mathrm{Iso}(\mathcal{X}_1, \mathcal{X}_2, \varphi) = \{h^{\Omega_1} g_{\Omega_1} : \ h \in H\}$$

where h^{Ω_1} is the restriction of h on Ω_1, and $g_{\Omega_1} : \Omega_1 \to \Omega_2$ is the bijection induced by g, we are done. □

References

1. С. Евдокимов, И. Пономаренко, *О примитивных клеточных алгебрах.* — Зап. научн. семин. ПОМИ **256** (1999), 38–68.
2. С. Евдокимов, И. Пономаренко, *Характеризация циклотомических схем и нормальные кольца Шура над циклической группой.* — Алгебра и анализ **14** (2002), no. 2, 11–55.
3. С. Евдокимов, И. Пономаренко, *Распознавание и проверка изоморфизма циркулянтных графов за полиномиальное время.* — Алгебра и анализ **15** (2003), no. 6, 1–34.
4. V. Arvind, B. Das, P. Mukhopadhyay, *Isomorphism and canonization of tournaments and hypertournaments.* — J. Computer and System Sciences **76** (2010), 509–523.
5. L. Babai, *On the order of uniprimitive permutation groups.* — Ann. Math. **113** (1981), 553–568.
6. L. Babai, E. M. Luks, *Canonical labeling of graphs.* — In: Proc. 15th ACM STOC, (1983), 171–183.
7. R. F. Bailey, P. J. Cameron, *Base size, metric dimension and other invariants of groups and graphs.* — Bull. London Math. Soc. **43** (2011), 209–242.
8. S. Evdokimov, I. Ponomarenko, *On highly closed cellular algebras and highly closed isomorphisms.* — Electr. J. Combin. **6** (1999), #R18, 1–31.
9. S. Evdokimov, I. Ponomarenko, *Two-closure of odd permutation group in polynomial time.* — Discr. Math. **235/1-3** (2001), 221–232.
10. S. Evdokimov, I. Ponomarenko, *Permutation group approach to association schemes.* — European J. Combin. **30** (2009), no. 6, 1456–1476.

11. S. Evdokimov, I. Ponomarenko, G. Tinhofer, *Forestal algebras and algebraic forests (on a new class of weakly compact graphs).* — Discr. Math. **225** (2000), 149–172.
12. A. Espuelas, *Regular orbits on symplectic modules.* — J. Algebra, **138** (1991), 1–12.
13. A. Espuelas, *Large character degrees of groups of odd order.* — Illinois J. Math. **35** (1991), 499–505.
14. The GAP Group, GAP-4-Groups, Algorithms, and Programming, Version 4.4.5, 2005, `http://www.gap-system.org`.
15. D. Gluck, *Trivial set-stabilizers in finite permutation groups.* — Can. J. Math. **XXXV** (1983), 59–67.
16. G. A. Jones, M. Klin, Y. Moshe, *Primitivity of Permutation Groups, Coherent Algebras and Matrices.* — J. Combin. Theory **A98** (2002), 210–217.
17. O. Manz, T. Wolf, *Representations of solvable groups.* — London Math. Soc. Lect. Note Ser. vol. 185, Cambridge Univ. Press, Cambridge (1993).
18. M. Muzychuk, I. Ponomarenko, *On Pseudocyclic Association Schemes.* — Ars Math. Contemporanea **5** (2012), no. 1, 1–25.
19. A. Seress, *The minimal base size of primitive solvable permutation groups.* — J. London Math. Soc. **53** (1996), 243–255.
20. A. Seress, *Permutation Group Algorithms.* Cambridge Univ. Press, 2002.
21. D. A. Suprunenko, *Matrix Groups*, Amer. Math. Soc., Providence, RI, 1976.
22. Yong Yang, *Regular orbits of finite primitive solvable groups.* — J. Algebra **323** (2010), 2735–2755.
23. B. Weisfeiler (editor), *On construction and identification of graphs.* Springer Lect. Notes 558, 1976.
24. P.-H. Zieschang, *Theory of Association Schemes.* Springer, Berlin & Heidelberg, 2005.

St.Petersburg Department
of Steklov Mathematical Institute RAS
Fontanka 27, St.Petersburg 191023, Russia
E-mail: `inp@pdmi.ras.ru`

Поступило 7 мая 2012 г.