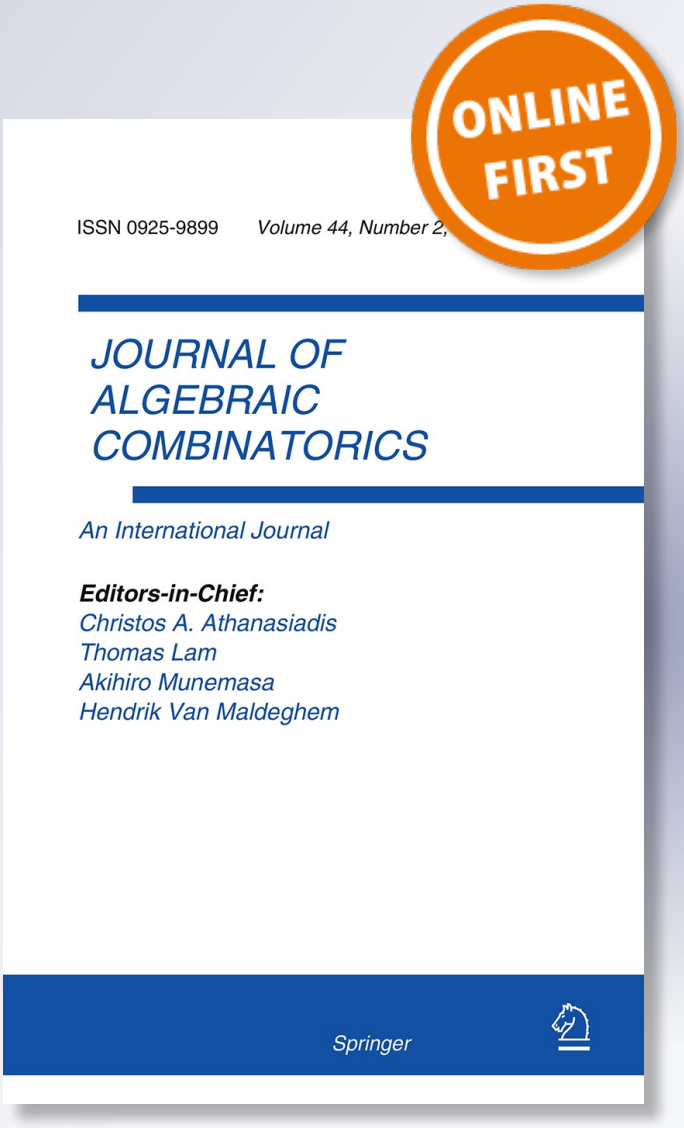
Cartan coherent configurations

Ilia Ponomarenko & Andrey Vasil'ev

Journal of Algebraic Combinatorics
An International Journal

ISSN 0925-9899

J Algebr Comb
DOI 10.1007/s10801-016-0715-5



Springer

J Algebr Comb
DOI 10.1007/s10801-016-0715-5

Cartan coherent configurations

Ilia Ponomarenko[1] · **Andrey Vasil'ev**[2,3]

Received: 23 February 2016 / Accepted: 21 September 2016

Abstract The Cartan scheme $\mathcal{X}$ of a finite group G with a (B, N)-pair is defined to be the coherent configuration associated with the action of G on the right cosets of the Cartan subgroup $B \cap N$ by right multiplication. It is proved that if G is a simple group of Lie type, then asymptotically the coherent configuration $\mathcal{X}$ is 2-separable, i.e., the array of 2-dimensional intersection numbers determines $\mathcal{X}$ up to isomorphism. It is also proved that in this case, the base number of $\mathcal{X}$ equals 2. This enables us to construct a polynomial-time algorithm for recognizing Cartan schemes when the rank of G and the order of the underlying field are sufficiently large. One of the key points in the proof is a new sufficient condition for an arbitrary homogeneous coherent configuration to be 2-separable.

1 Introduction

A well-known general problem in algebraic combinatorics is to characterize an association scheme $\mathcal{X}$ up to isomorphism by a certain set of parameters [3]. A lot of such characterizations are known when $\mathcal{X}$ is the association scheme of a classical

The work of the first and the second authors was partially supported, respectively, by the Grant RFBR No. 14-01-00156 and RFFI Grant No. 13-01-00505.

✉ Ilia Ponomarenko
inp@pdmi.ras.ru

Andrey Vasil'ev
vasand@math.nsc.ru

1 St. Petersburg Department of the Steklov Mathematical Institute, St. Petersburg, Russia

2 Sobolev Institute of Mathematics, Novosibirsk, Russia

3 Novosibirsk State University, Novosibirsk, Russia

Published online: 26 September 2016

distance regular graph [4]. In most cases, the parameters can be chosen as a part of the intersection array of $\mathcal{X}$. However, in general, even the whole array does not determine the scheme $\mathcal{X}$ up to isomorphism. Therefore, it makes sense to consider the m-dimensional intersection numbers, $m \geq 1$, introduced in [12] for an arbitrary coherent configuration (for $m = 1$, these numbers are ordinary intersection numbers; the exact definitions can be found in Sect. 2). It was proved in [12] that every Johnson, Hamming or Grassmann scheme is 2-separable, i.e., is determined up to isomorphism by the array of 2-dimensional intersection numbers.

In a recent paper [1], a generalized notion of distance regularity in buildings was introduced. According to [24], there is a natural 1-1 correspondence between the class of all buildings and the class of special homogeneous coherent configurations called the Coxeter schemes (see also [23, Chapter 12]). In this language, the Tits theorem on spherical buildings says that if $\mathcal{X}$ is a finite Coxeter scheme of rank at least 3 and trivial thin radical, then there exists a group G acting on a set Ω such that

$$\mathcal{X} = \mathrm{Inv}(G, \Omega) \tag{1}$$

where $\mathrm{Inv}(G, \Omega)$ is the coherent configuration of G, i.e., the pair (Ω, S) with $S = \mathrm{Orb}(G, \Omega \times \Omega)$. Moreover, in this case, G is a group with a (B, N)-pair. Thus, a characterization of the coherent configuration (1) with such G by the m-dimensional intersection numbers with small m could be considered as a generalization of the above-mentioned results on the association schemes of classical distance regular graphs to the non-commutative case.

In the present paper, we are interested in coherent configurations (1) in the case where G is a finite group with a (B, N)-pair and $\mathcal{X}$ is a *Cartan scheme of* G in the following sense.

Definition 1.1 The Cartan scheme of G with respect to (B, N) is defined to be the coherent configuration (1), where $\Omega = G/H$ consists of the right cosets of the Cartan subgroup $H = B \cap N$ and G acts on Ω by right multiplication.

Note that the permutation group induced by the action of G is transitive and the stabilizer of the point $\{H\}$ coincides with H. In a Coxeter scheme of rank at least 3, the point stabilizer equals B. Therefore, such a scheme is a quotient of a suitable Cartan scheme.

The separability problem [13] consists of finding the smallest m for which a coherent configuration is m-separable. The separability problem (in particular, for a Cartan scheme) is easy to solve if the group H is trivial. Indeed, in this case, the permutation group induced by G is regular and the corresponding coherent configuration is 1-separable. The following theorem gives a partial solution to the separability problem for Cartan schemes when G is a finite simple group of Lie type and hence with a (B, N)-pair. In what follows, we denote by $\mathcal{L}$ the class of all simple groups of Lie type including all exceptional groups and all classical groups $\Phi(l, q)$, for which $l \geq l_0$ and $q \geq al$, where the values of l_0 and a are given in the last two columns of Table 2.

Theorem 1.2 *The Cartan scheme $\mathcal{X}$ of every finite simple group $G \in \mathcal{L}$ is 2-separable.*

As a byproduct of the proof of Theorem 1.2, we are able to estimate the base number of a Cartan scheme satisfying the hypothesis of this theorem (as to the exact definition, we refer to Sect. 2.2; see also [13] and [2, Sec. 5], where the base number was called the EP-dimension). The base number $b(\mathcal{X})$ of a coherent configuration $\mathcal{X}$ can be thought as a combinatorial analog of the base number of permutation group, which is the minimal number of points such that only identity of the group leaves each of them fixed. In fact, for the coherent configuration (1), we have

$$b(G) \le b(\mathcal{X}), \tag{2}$$

where $b(G)$ is the base number of the permutation group induced by G. Moreover, in this case, obviously, $b(G) = 1$ if and only if $b(\mathcal{X}) = 1$. In general, $b(G)$ can be much smaller than $b(\mathcal{X})$. The following theorem shows that this does not happen for the Cartan schemes in question.

Theorem 1.3 *Let $\mathcal{X}$ be the Cartan scheme of a group $G \in \mathcal{L}$. Then, $b(\mathcal{X}) \le 2$ and $b(\mathcal{X}) = 1$ if and only if the group H is trivial.*

Let us deduce Theorems 1.2 and 1.3 from the results whose proofs occupy most of the paper. Let $\mathcal{X}$ be the Cartan scheme of a group $G \in \mathcal{L}$. Denote by c and k the indistinguishing number and the maximum valency of $\mathcal{X}$, respectively.[1] Translating these invariants into group-theoretic language, we prove in Theorem 4.1 that in our case

$$2c(k-1) < n \tag{3}$$

where $n = |\Omega|$. The proof of this inequality forms the group-theoretic part of the whole proof. The combinatorial part of the proof is to analyze the one-point extension of a homogeneous coherent configuration, for which inequality (3) holds; here, the point extension can be thought as a combinatorial analog of the point stabilizer of permutation group. In this way, we prove Theorem 3.1, which implies that the one-point extension of $\mathcal{X}$ is 1-regular (see Sect. 2.2). Now Theorems 1.2 and 1.3 are immediate consequences of Corollary 2.6 obtained by a combination of two results in [13].

When the rank of a simple group G of Lie type is small, inequality (3) does not generally hold, but the statements of Theorems 1.2 and 1.3 may still be true. For example, if $G = \mathrm{PSL}(2, q)$ with even q, then inequality (3) is not true; however, the following assertion holds.

Theorem 1.4 *Let $\mathcal{X}$ be the Cartan scheme of the group $\mathrm{PSL}(2, q)$, where $q > 3$. Then, $\mathcal{X}$ is 2-separable and $b(\mathcal{X}) = 2$.*

We believe that the Cartan scheme of every simple group of Lie type is 2-separable. Moreover, as in the case of classical distance regular graphs, it might be that in most cases such a scheme is 1-separable, i.e., is determined up to isomorphism by the

[1] In the complete colored graph representing $\mathcal{X}$, k is the maximum number of the monochrome arcs incident to a vertex, and c is the maximum number of triangles with fixed base; the other two sides of which are monochrome arcs.

intersection numbers. In this way, one could probably use more subtle results on the structure of finite simple groups and a combinatorial technique in the spirit of [16].

From the computational point of view, Theorems 1.2 and 1.3 can be used for testing isomorphism and recognizing the Cartan schemes satisfying the hypothesis of Theorem 1.2. To this end, it is convenient to represent a coherent configuration (Ω, S) as a complete colored graph with vertex set Ω such that the color classes of the arcs coincide with the relations of S (the vertex colors match the colors of the loops). It is assumed that the isomorphisms of such colored graphs preserve the colors.

Theorem 1.5 *Let $\mathcal{G}_n$ (resp. $\mathcal{K}_n$) be the class of all colored graphs (resp. the colored graphs of Cartan schemes of the groups in $\mathcal{L}$) with n vertices. Then, the following problems can be solved in polynomial time in n:*

(1) given $D \in \mathcal{G}_n$, test whether $D \in \mathcal{K}_n$, and (if so) find the corresponding groups G, B, and N;
(2) given $D \in \mathcal{K}_n$ and $D' \in \mathcal{G}_n$, find the set $\mathrm{Iso}(D, D')$.

To make the paper possibly self-contained, we cite the basics of coherent configurations in Sect. 2. Theorems 3.1 and 4.1, from which we have deduced Theorems 1.2 and 1.3, are proved in Sects. 3, 4, 5, respectively. Finally, Theorems 1.4 and 1.5 are proved in Sects. 6 and 7, respectively.

Notation. Throughout the paper, Ω denotes a finite set.

The diagonal of the Cartesian product $\Omega \times \Omega$ is denoted by 1_Ω; for any $\alpha \in \Omega$, we set $1_\alpha = 1_{\{\alpha\}}$.

For a relation $r \subset \Omega \times \Omega$, we set $r^* = \{(\beta, \alpha) : (\alpha, \beta) \in r\}$ and $\alpha r = \{\beta \in \Omega : (\alpha, \beta) \in r\}$ for all $\alpha \in \Omega$.

For $S \in 2^{\Omega^2}$, we denote by $S^\cup$ the set of all unions of the elements of S and put $S^* = \{s^* : s \in S\}$ and $\alpha S = \cup_{s \in S} \alpha s$, where $\alpha \in \Omega$.

For $g \in \mathrm{Sym}(\Omega)$, we set $\mathrm{Fix}(g) = \{\alpha \in \Omega : \alpha^g = \alpha\}$; in particular, if χ is the permutation character of a group $G \le \mathrm{Sym}(\Omega)$, then $\chi(g) = |\mathrm{Fix}(g)|$ for all $g \in G$.

The identity of a group G is denoted by e; the set of non-identity elements in G is denoted by $G^\#$.

2 Coherent configurations

2.1 Main definitions

Let Ω be a finite set, and let S be a partition of $\Omega \times \Omega$. The pair $\mathcal{X} = (\Omega, S)$ 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, and $S^\cup$ are called the *points*, *basis relations*, and *relations* of $\mathcal{X}$, respectively. The numbers $|\Omega|$, $|S|$, and c_{rs}^t are called the *degree*, *rank*, and *intersection numbers* of $\mathcal{X}$. The basis relation containing the pair $(\alpha, \beta) \in \Omega \times \Omega$ is denoted by $r(\alpha, \beta)$.

The point set Ω is a disjoint union of *fibers*, i.e., the sets $\Gamma \subseteq \Omega$, for which $1_\Gamma \in S$ For any basis relation $r \in S$, there exist uniquely determined fibers Γ and Δ such that $r \subseteq \Gamma \times \Delta$. Moreover, the number $|\gamma r| = c^t_{rr^*}$ with $t = 1_\Gamma$, does not depend on the choice of $\gamma \in \Gamma$. This number is called the *valency* of r and denoted by n_r. The maximum of all valencies is denoted by $k = k(\mathcal{X})$.

A point $\alpha \in \Omega$ of the coherent configuration $\mathcal{X}$ is called *regular* if

$$|\alpha r| \le 1 \quad \text{for all } r \in S.$$

One can see that the set of all regular points is the union of fibers. If this set is not empty, then the coherent configuration $\mathcal{X}$ is said to be *1-regular*.

The coherent configuration $\mathcal{X}$ is said to be *homogeneous* if $1_\Omega \in S$. In this case, $n_r = n_{r^*} = |\alpha r|$ for all $r \in S$ and $\alpha \in \Omega$. Moreover, the relations

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

hold for all $r, s, t \in S$. We observe that in the homogeneous case, a coherent configuration is 1-regular if and only if it is a thin scheme in the sense of [23].

2.2 Point extensions and the base number

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

$$\mathcal{X} \le \mathcal{X}' \;\Leftrightarrow\; S^\cup \subseteq (S')^\cup.$$

The minimal and maximal elements with respect to this ordering are the *trivial* and *complete* coherent configurations: The basis relations of the former are the reflexive relation 1_Ω and (if $n > 1$) its complement in $\Omega \times \Omega$, whereas the basis relations of the latter are singletons.

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 basis relations of $\mathcal{X}_i$, $i = 1, 2$. This enables us to define the *point extension* $\mathcal{X}_{\alpha,\beta,\dots}$ of a coherent configuration $\mathcal{X} = (\Omega, S)$ with respect to the points $\alpha, \beta, \dots \in \Omega$ as follows:

$$\mathcal{X}_{\alpha,\beta,\dots} = \bigcap_{\mathcal{Y}:\ S \subseteq T^\cup, 1_\alpha, 1_\beta, \dots \in T^\cup} \mathcal{Y},$$

where $\mathcal{Y}$ is the coherent configuration (Ω, T). In other words, $\mathcal{X}_{\alpha,\beta,\dots}$ can be defined as the smallest coherent configuration on Ω that is larger than or equal to $\mathcal{X}$ and has singletons $\{\alpha\}, \{\beta\}, \dots$ as fibers. This configuration can also be considered as the refinement of the color graph associated with $\mathcal{X}$, in which the points of $\alpha, \beta, \dots$

are colored in distinguished new colors. In particular, the extension can be efficiently constructed by the Weisfeiler-Leman algorithm (see Sect. 7).

Definition 2.1 A set $\{\alpha, \beta, \ldots\} \subseteq \Omega$ is a *base* of the coherent configuration $\mathcal{X}$ if the extension $\mathcal{X}_{\alpha,\beta,\ldots}$ with respect to the points $\alpha, \beta, \ldots$ is complete; the smallest cardinality of a base is called the *base number* of $\mathcal{X}$ and denoted by $b(\mathcal{X})$.

It is easily seen that $0 \le b(\mathcal{X}) \le n - 1$, where $n = |\Omega|$, and the equalities are attained for the complete and trivial coherent configurations on Ω, respectively. It is also obvious that $b(\mathcal{X}) \le 1$, whenever the coherent configuration $\mathcal{X}$ is 1-regular.

2.3 Coherent configurations and permutation groups

Two coherent configurations $\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega', S')$ are called *isomorphic* if there exists a bijection $f : \Omega \to \Omega'$ such that the relation $s^f = \{(\alpha^f, \beta^f) : (\alpha, \beta) \in s\}$ belongs to S' for all $s \in S$. The bijection f is called an *isomorphism* from $\mathcal{X}$ onto $\mathcal{X}'$; the set of all of them is denoted by $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$. The group $\mathrm{Iso}(\mathcal{X}, \mathcal{X})$ contains a normal subgroup

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

called the *automorphism group* of $\mathcal{X}$.

Let $G \le \mathrm{Sym}(\Omega)$ be a permutation group, and let S be the set of orbits of the coordinatewise action of G on $\Omega \times \Omega$. Then,

$$\mathrm{Inv}(G) = \mathrm{Inv}(G, \Omega) = (\Omega, S)$$

is a coherent configuration called the *coherent configuration of* G. It is homogeneous if and only if the group G is transitive. From [13, Corollary 3.4], it follows that a coherent configuration $\mathcal{X}$ is 1-regular if and only if $\mathcal{X} = \mathrm{Inv}(G)$, where G is a permutation group having a faithful regular orbit.

Let $G \le \mathrm{Sym}(\Omega)$ be a transitive group, $H = G_\alpha$ the stabilizer of a point α in G, and $\mathcal{X} = \mathrm{Inv}(G)$ the coherent configuration of G. Then, given a basis relation $s \in S$, one can form the set

$$D_s = \{g \in G : (\alpha, \alpha^g) \in s\}, \tag{5}$$

which is, in fact, a double H-coset. It is well known that the mapping $s \mapsto D_s$ is a bijection from the set S of basis relations of $\mathcal{X}$ onto the set of double H-cosets in G. Furthermore, the intersection number c_{rs}^t is equal to the multiplicity, with which an element of D_t enters the product $D_r\, D_s$, divided by $|H|$. It follows that

$$n_s = \frac{|D_s|}{|H|} = \frac{|H|}{|H \cap H^g|} \tag{6}$$

for all $s \in S$ and $g \in D_s$ (the second equality follows from the first one, because $|D_s| = |HgH| = |g^{-1}HgH| = |H^g H|$). In particular, $k = k(\mathcal{X})$ is the ratio between the order of H and the minimal size of the intersection of H with its conjugate.

Lemma 2.2 *Let G be a transitive permutation group and $\mathcal{X} = \mathrm{Inv}(G)$. If $b(\mathcal{X}) \le 2$, then $G = \mathrm{Aut}(\mathcal{X})$.*

Proof Inequality (2) yields $b(G) \le b(\mathcal{X}) \le 2$. It follows that $H \cap H^g = 1$ for some $g \in G$, where $H = G_\alpha$. If s is the basis relation of $\mathcal{X}$ with $D_s = HgH$, then (6) implies that αs is a faithful regular orbit of H. Hence

$$|G| = nk,$$

where n is the cardinality of the underlying set of G. Since $\mathcal{X} = \mathrm{Inv}(G) = \mathrm{Inv}(\mathrm{Aut}(\mathcal{X}))$, inequality (2) also yields $b(\mathrm{Aut}(\mathcal{X})) \le b(\mathcal{X}) \le 2$. So the above equality holds for G replaced by $\mathrm{Aut}(\mathcal{X})$. Thus,

$$|\mathrm{Aut}(\mathcal{X})| = nk = |G|,$$

and we are done, because $G \le \mathrm{Aut}(\mathcal{X})$. □

2.4 Indistinguishing number

Following [16], the sum of all intersection numbers $c^r_{ss^*}$ with fixed r is called the *indistinguishing number* of $r \in S$ and denoted by $c(r)$. It is easily seen that for all pairs $(\alpha, \beta) \in r$, we have

$$c(r) = |\Omega_{\alpha,\beta}|, \text{ where } \Omega_{\alpha,\beta} = \{\gamma \in \Omega : r(\gamma, \alpha) = r(\gamma, \beta)\}. \tag{7}$$

The maximum of the numbers $c(r)$, $r \ne 1_\Omega$, is called the *indistinguishing number* of the coherent configuration $\mathcal{X}$ and denoted by $c(\mathcal{X})$.

The following lemma gives a formula for the indistinguishing number of the coherent configuration of a transitive permutation group. Recall that the fixity $\mathrm{fix}(G)$ of a permutation group G is the maximum number of elements fixed by non-identity permutations [18].

Lemma 2.3 *Let $G \le \mathrm{Sym}(\Omega)$ be a transitive group, H a point stabilizer of G, and $\mathcal{X} = \mathrm{Inv}(G)$. Then,*

$$c(\mathcal{X}) = \max_{x \in G \setminus H} |\bigcup_{h \in H} \mathrm{Fix}(hx)|. \tag{8}$$

In particular,

$$c(\mathcal{X}) \le \max_{x \in G \setminus H} \sum_{h \in H} \chi(hx) \le \mathrm{fix}(G) \cdot |H|. \tag{9}$$

Proof Let $r \in S$ and $(\alpha, \beta) \in r$. Then, a point γ belongs to the set $\Omega_{\alpha,\beta}$ defined in (7) if and only if the pairs (γ, α) and (γ, β) belong to the same orbit of the group G acting on $\Omega \times \Omega$, and the latter happens if and only if γ is a fixed point of a permutation $x \in G$ moving α to β. Assuming without loss of generality that $H = G_\alpha$, we conclude that the set of all such x forms an H-coset C. Therefore,

$$c(r) = |\Omega_{\alpha,\beta}| = |\bigcup_{h \in H} \mathrm{Fix}(hx)| \tag{10}$$

for any $x \in C$. Moreover, if $r \neq 1_\Omega$, then $C \neq H$. This proves equality (8). Furthermore, $|\mathrm{Fix}(x)| = \chi(x) \leq \mathrm{fix}(G)$ for any non-identity element $x \in G$. This implies that

$$|\bigcup_{h\in H} \mathrm{Fix}(hx)| \leq \sum_{h\in H} \chi(hx) \leq \mathrm{fix}(G) \cdot |H|.$$

Thus, the second statement of the lemma follows from the first one. □

We complete this subsection by a statement that helps to compute the values of the permutation character of a transitive group.

Lemma 2.4 *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive group, $\alpha \in \Omega$, and $H = G_\alpha$ the point stabilizer of α in G. Then, for every $x \in G$,*

$$\mathrm{Fix}(x) \neq \varnothing \iff x^G \cap H \neq \varnothing. \tag{11}$$

Suppose, additionally, that there is a subgroup N with $H \leq N \leq N_G(H)$ such that every two H-conjugates in G are also conjugate in N. If $x = h_0^{g_0}$, where $h_0 \in H$ and $g_0 \in G$, then

$$\mathrm{Fix}(x) = \{\alpha^g \mid g \in NCg_0\}, \tag{12}$$

where $C = C_G(h_0)$. Furthermore,

$$\chi(x) = \frac{|N : (C \cap N)|\,|C|}{|H|} = \frac{|N : (C \cap N)|\,|\Omega|}{|x^G|}. \tag{13}$$

Proof Clearly, $\alpha^g \in \mathrm{Fix}(x)$ if and only if $Hgx = Hg$, which holds if and only if there is $h \in H$ satisfying $x = h^g$. In particular, this yields (11).

To prove that the left-hand side of (12) is contained in the right-hand side, let $x = h_0^{g_0}$, that is the set $\mathrm{Fix}(x)$ is non-empty. Suppose that g is an arbitrary element of G with $\alpha^g \in \mathrm{Fix}(x)$. Then, there is $h \in H$ such that $h^g = x = h_0^{g_0}$. Put $y = gg_0^{-1}$. Since the elements h_0 and $h = h_0^{y^{-1}}$ are conjugate in G, they are also conjugate in N, so there is $n \in N$ with $h_0^{y^{-1}} = h_0^{n^{-1}}$. It follows that $y = nc$, where $c \in C$. Therefore, $g = ncg_0$, so $\alpha^g \in \mathrm{Fix}(x)$ implies that $g \in NCg_0$. To establish the reverse inclusion, for every $n \in N$, set $h = h_0^{n^{-1}}$. Then, $h^{ncg_0} = h_0^{cg_0} = x$ for every $c \in C$. By the argument of the first paragraph, this proves $\alpha^{NCg_0} \subseteq \mathrm{Fix}(x)$.

Obviously, $|NCg_0| = |N : (C \cap N)||C|$. Now, the first equality in (13) is the direct consequence of (12), because $\alpha^g = \alpha^{g'}$ if and only if $g'g^{-1} \in H$. Since $|C| = |G|/|x^G|$ and $|G|/|H| = |\Omega|$, the second equality follows. □

2.5 Algebraic isomorphisms and m-dimensional intersection numbers

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

$$c_{rs}^t = c_{r's'}^{t'}, \qquad r, s, t \in S. \tag{14}$$

In this case, we say that $\mathcal{X}$ and $\mathcal{X}'$ are *algebraically isomorphic*. Each isomorphism f from $\mathcal{X}$ to $\mathcal{X}'$ naturally induces an algebraic isomorphism between these coherent configurations. The set of all isomorphisms inducing the algebraic isomorphism φ is denoted by $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$. In particular,

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

where id_S is the identity permutation of S. A coherent configuration $\mathcal{X}$ is called *separable* if for any algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$, the set $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ is non-empty.

Saying that coherent configurations $\mathcal{X}$ and $\mathcal{X}'$ have the same intersection numbers, we mean that formula (14) holds for a certain algebraic isomorphism. Thus, the exact meaning of the phrase "the coherent configuration $\mathcal{X}$ is determined up to isomorphism by the intersection numbers" is that $\mathcal{X}$ is separable.

Let $m \geq 1$ be an integer. According to [13], the m-extension of a coherent configuration $\mathcal{X}$ with point set Ω is defined to be the smallest coherent configuration on Ω^m, which contains the Cartesian m-power of $\mathcal{X}$ and for which the set $\mathrm{Diag}(\Omega^m)$ is the union of fibers. The intersection numbers of the m-extension are called the *m-dimensional intersection numbers* of the configuration $\mathcal{X}$. Now, m-separable coherent configurations for $m > 1$ are defined essentially in the same way as for $m = 1$. The exact definition can be found in the survey [13], whereas in the present paper, we need only the following result, which immediately follows from [13, Theorems 3.3 and 5.10].

Theorem 2.5 *Let $\mathcal{X}$ be a coherent configuration admitting a 1-regular extension with respect to $m-1$ points, $m \geq 1$. Then, $\mathcal{X}$ is m-separable.* □

Corollary 2.6 *Let $\mathcal{X}$ be a coherent configuration admitting a 1-regular one-point extension. Then, $\mathcal{X}$ is 2-separable and $b(\mathcal{X}) \leq 2$.* □

3 A sufficient condition for 1-regularity of a point extension

3.1 Main theorem

The aim of this section is to prove the following statement underlying the combinatorial part in the proof of the main results of this paper.

Theorem 3.1 *Let $\mathcal{X}$ be a homogeneous coherent configuration on n points with indistinguishing number c and maximum valency k. Suppose that $2c(k-1) < n$, i.e., inequality (3) holds. Then, every one-point extension of $\mathcal{X}$ is 1-regular.*

The proof of Theorem 3.1 will be given in the end of this section. The idea is to deduce the 1-regularity of the point extension $\mathcal{X}_\alpha$ from Lemma 3.6 stating that inequality (3) implies the connectedness of the binary relations $s_{\max}$ and s_α defined in Sect. 3.2. Note that this condition itself implies that any pair from $s_{\max}$ forms a base of $\mathcal{X}$ (Lemma 3.3).

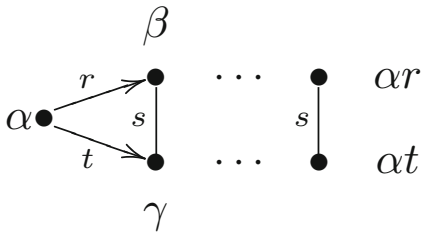


Fig. 1 A part of the relation s_α

3.2 Relations $s_{\max}$ and s_α

Let $\mathcal{X} = (\Omega, S)$. Recall that $k = k(\mathcal{X})$ is the maximal valency of $\mathcal{X}$. Denote by $s_{\max}$ the union of all relations in the set

$$S_{\max} = \{s \in S : \ n_s = k\}.$$

Then, obviously, $s_{\max} \in S^\cup$. Moreover, since $\mathcal{X}$ is homogeneous, we have $n_{s^*} = n_s$ for all $s \in S$, and hence, the relation $s_{\max}$ is symmetric. We are interested in its connectedness, i.e., the connectedness of the graph with vertex set Ω and edge set $s_{\max}$. Note that, in general, this graph is not connected: take $\mathcal{X}$ to be the homogeneous coherent configuration of rank 4 that is associated with a finite projective plane.

With any point $\alpha \in \Omega$, we associate a binary relation $s_\alpha \subseteq \alpha s_{\max} \times \alpha s_{\max}$ that consists of all pairs (β, γ) such that the colored triangle $\{\alpha, \beta, \gamma\}$ is uniquely determined by the side colors $r = r(\alpha, \beta)$, $s = r(\beta, \gamma)$ and $t = r(\alpha, \gamma)$, and one of the sides $\{\alpha, \beta\}$ or $\{\alpha, \gamma\}$, see Fig. 1. More precisely,

$$s_\alpha = \{(\beta, \gamma) \in \alpha s_{\max} \times \alpha s_{\max} : \ c^t_{rs} = 1\},$$

This relation is symmetric. Indeed, we have $n_t = n_r = k$. Since also $n_{r^*} = n_r$, it follows from (4) that $n_t c^t_{rs} = n_{r^*} c^{r^*}_{st^*} = n_r c^r_{ts^*}$. This implies that $c^r_{ts^*} = c^t_{rs} = 1$ and hence $(\gamma, \beta) \in s_\alpha$.

Lemma 3.2 *Suppose that the graph s_α is connected. Denote by T_α the set of all basis relations of the coherent configuration $\mathcal{X}_\alpha$ that are contained in $\alpha s_{\max} \times \alpha s_{\max}$. Then,*

$$|\beta t| = 1 \quad \textit{for all } \ t \in T_\alpha, \ \ \beta \in \alpha s_{\max}. \tag{15}$$

Proof One can see that the set $\alpha s_{\max}$ is the union of fibers of $\mathcal{X}_\alpha$ (see [17, Lemma 2.2]). Therefore,

$$\alpha s_{\max} \times \alpha s_{\max} = \bigcup_{t \in T_\alpha} t. \tag{16}$$

Let $t \in T_\alpha$ and $\beta \in \alpha s_{\max}$. Then, $\beta \in \alpha r$ for some $r \in S_{\max}$. In view of (16), there exists a point $\beta' \in \alpha s_{\max}$ contained in βt. By the connectedness of s_α, there exists a path P in s_α connecting β and β'. If this path has length $l = 1$, then by the definition

of s_α, we have $c^s_{rt'} = 1$, where $t' \in S$ and $s \in S_{\max}$ are unique relations such that $t \subset t'$ and $\beta' \in \alpha s$, respectively. Then, obviously, $\{\beta'\} = \beta t$, as required.

Suppose that $l \geq 2$. Note that if β_1, β_2, and β_3 are successive vertices of P, then they belong to $\alpha s_{\max}$ and

$$\{\beta_2\} = \beta_1 t_1, \ \{\beta_3\} = \beta_2 t_2,$$

where t_1 and t_2 are the basis relations of $\mathcal{X}_\alpha$ that contain (β_1, β_2) and (β_2, β_3), respectively. In particular, $t_1, t_2 \in T_\alpha$ and

$$\{\beta_3\} = \beta_1 t_3,$$

where t_3 is a unique relation of T_α containing the pair (β_1, β_3). This proves the required statement for $l = 2$ and hence for all positive integers l by induction. □

Lemma 3.3 *If $s_{\max}$ and all s_α, $\alpha \in \Omega$, are connected relations, then $\{\alpha, \beta\}$ is a base of the coherent configuration $\mathcal{X}$ for each $\beta \in \Omega$ such that $(\alpha, \beta) \in s_{\max}$.*

Proof Let $\alpha \in \Omega$ and $\beta \in \alpha s_{\max}$. Denote by Γ the set of all points $\gamma \in \Omega$ for which the singleton $\{\gamma\}$ is a fiber of the coherent configuration $\mathcal{X}_{\alpha,\beta}$. Then, obviously $\alpha, \beta \in \Gamma$. We claim that

$$\gamma s_{\max} \subseteq \Gamma \quad \text{or} \quad \gamma s_{\max} \cap \Gamma = \varnothing \tag{17}$$

for all $\gamma \in \Gamma$. Indeed, assume to the contrary that there exist points $\gamma \in \Gamma$ and $\gamma_1, \gamma_2 \in \gamma s_{\max}$ such that $\gamma_1 \in \Gamma$ and $\gamma_2 \notin \Gamma$. Since s_γ is a connected relation, there is an s_γ-path connecting γ_1 and γ_2. Moreover, the definition of s_γ implies that if some point in this path is inside Γ, then the next point in this path must also be inside Γ. Therefore, $\gamma_2 \in \Gamma$, a contradiction.

Denote by Γ_0 the set of all points $\gamma \in \Gamma$ with $\gamma s_{\max} \subseteq \Gamma$. Then, $\alpha \in \Gamma_0$, because in view of (17), the set $\alpha s_{\max}$ contains $\beta \in \Gamma$. Therefore, Γ_0 contains the connected component of $s_{\max}$ that contains α. Since $s_{\max}$ is connected, this implies that $\Gamma_0 = \Omega$ and hence $\Gamma = \Omega$. By the definition of Γ, this means that the fibers of $\mathcal{X}_{\alpha,\beta}$ are singletons. Thus, $\{\alpha, \beta\}$ is a base of $\mathcal{X}$. □

3.3 Connected components of s_α

One can treat s_α also as a graph with vertex set $\alpha s_{\max}$ and edge set s_α. The set of all connected components of this graph which contain a vertex in αu for a fixed $u \in S_{\max}$ is denoted by $C_\alpha(u) = C(u)$.

Lemma 3.4 *Let $u, v \in S_{\max}$. Suppose that $C(u) \cap C(v) \neq \varnothing$. Then, $C(u) = C(v)$ and $|\alpha u \cap C| = |\alpha v \cap C|$ for all $C \in C(u)$.*

Proof Let $C_0 \in C(u) \cap C(v)$. Then, C_0 contains vertices $\beta \in \alpha u$ and $\gamma \in \alpha v$ connected by an s_α-path, say

$$\beta = \beta_0, \beta_1, \ldots, \beta_m = \gamma,$$

where $(\beta_i, \beta_{i+1}) \in s_\alpha$ for $i = 0, \dots, m-1$. By the definition of s_α, this implies that

$$c_{u_i v_i}^{u_{i+1}} = 1 \tag{18}$$

for all i, where $u_i = r(\alpha, \beta_i)$ and $v_i = r(\beta_i, \beta_{i+1})$. Therefore, it is easily seen that for every $C \in C(u)$ given a vertex $\beta' \in C$, there is a unique s_α-path

$$\beta' = \beta'_0, \beta'_1, \dots, \beta'_m = \gamma'$$

such that $\gamma' \in \alpha v$ and $r(\alpha, \beta'_i) = u_i$ and $r(\beta'_i, \beta'_{i+1}) = v_i$ for all i. In view of (18), no vertices β_i and β'_i coincide whenever $\beta \neq \beta'$. Thus, the mapping

$$\alpha u \to \alpha v, \ \beta' \mapsto \gamma'$$

is a bijection. Obviously, the vertex γ' belongs to the component C of the graph s_α that contains β'. Since this is true for all $\beta' \in C$ and all $C \in C(u)$, the required statement follows. □

For a relation $u \in S_{\max}$ and a point $\delta \in \Omega$, denote by $p_u(\delta)$ the number of pairs $(\beta, \gamma) \in \alpha u \times \alpha u$ such that $\beta \neq \gamma$ and $r(\beta, \delta) = r(\gamma, \delta)$. Here, $|\alpha u| = n_u = k$. Therefore, αu contains exactly $k(k-1)$ pairs of distinct elements. Now we are able to estimate from above the sum of $p_u(\delta)$ in terms of the indistinguishing numbers of the corresponding basis relations $c(r(\beta, \gamma))$ as well as the indistinguishing number c of $\mathcal{X}$. Indeed,

$$k(k-1)c \geq \sum_{\beta,\gamma} c(r(\beta, \gamma)) \geq \sum_{\delta \in \Delta} p_u(\delta) \tag{19}$$

for any set $\Delta \subseteq \Omega$. On the other hand, the number $p_u(\delta)$ can be computed by means of the intersection numbers. Namely, if $v = r(\alpha, \delta)$, then, obviously,

$$p_u(\delta) = \sum_{w \in T_{u,v}} c_{uw}^v (c_{uw}^v - 1) \tag{20}$$

where $T_{u,v} = \{w \in u^* v : \ c_{uw}^v > 1\}$ (see Fig. 2). In particular, the number $p_u(\delta)$ does not depend on $\delta \in \alpha v$.

Lemma 3.5 *In the above notation, the following statements hold:*

(1) if either $n_u > n_v$, or $n_u = n_v$ and $C(u) \neq C(v)$, then $p_u(\delta) \geq k$,
(2) if $n_u = n_v$, $C(u) = C(v)$, and $|C(u)| > 1$, then $p_u(\delta) \geq k/2$.

Proof To prove statement (1), suppose that either $n_u > n_v$, or $n_u = n_v$ and $C(u) \neq C(v)$. Then

$$T_{u,v} = u^* v. \tag{21}$$

Indeed, obviously, $T_{u,v} \subseteq u^* v$. The reverse inclusion is true if $n_u > n_v$, because in this case, $c_{uw}^v = n_u c_{v^* u}^{w^*} / n_v > 1$ for all $w \in u^* v$. Let now $C(u) \neq C(v)$. Then, the sets $C(u)$ and $C(v)$ are disjoint (Lemma 3.4). This implies that if $\beta \in \alpha u$ and $\gamma \in \alpha v$,

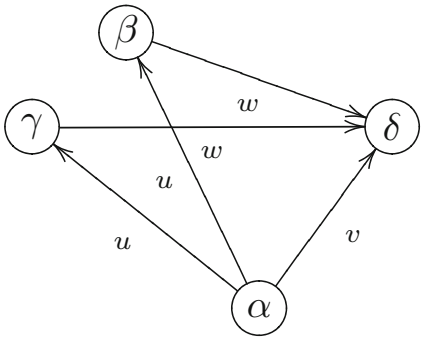


Fig. 2 Relation $w \in T_{u,v}$ with $c^w_{uv} > 1$

then $(\beta, \gamma) \notin s_\alpha$. Therefore, $c^v_{uw} > 1$ for all $w \in u^*v$, whence again $u^*v \subseteq T_{u,v}$. Thus, relation (21) is completely proved. Together with (20), this shows that

$$p_u(\delta) = \sum_{w \in T_{u,v}} c^v_{uw}(c^v_{uw} - 1) \geq \sum_{w \in T_{u,v}} c^v_{uw} = \sum_{w \in u^*v} c^v_{uw} = n_u = k,$$

as required. Observe that the penultimate equality is the well-known identity for homogenous coherent configurations.

To prove statement (2), suppose that $n_u = n_v$, $C(u) = C(v)$, and $|C(u)| > 1$. Let us choose $C \in C(u)$ so that the number $|\alpha u \cap C|$ is the minimum possible. Then,

$$|\alpha u \backslash C| \geq k/2, \tag{22}$$

because $|C(u)| > 1$ and $|\alpha u| = n_u = k$. Next, since $C(u) = C(v)$, we have $C \in C(v)$. Moreover, αv is not contained in C, because $|C(v)| = |C(u)| > 1$. Since $p_u(\delta)$ does not depend on the choice of $\delta \in \alpha v$, we may assume that $\delta \in \alpha v \cap C$. Then, no point $\beta \in \alpha u \backslash C$ belongs to the component of s_α that contains δ. In particular, (δ, β) is not an edge of s_α. Therefore,

$$c^v_{uw} > 1 \quad \text{for all } w \in T,$$

where T is the set of all $w = r(\beta, \delta)$ with $\beta \in \alpha u \backslash C$. By (20) and (22), we obtain

$$p_u(\delta) = \sum_{w \in T_{u,v}} c^v_{uw}(c^v_{uw} - 1) \geq \sum_{w \in T} c^v_{uw} = |\alpha u \cap \delta T^*| \geq |\alpha u \backslash C| \geq k/2,$$

as required. □

3.4 The connectedness of $s_{\max}$ and s_α

Using Lemmas 3.4 and 3.5, we will prove that the hypothesis of Theorem 3.1 gives a sufficient condition for the graphs s_α and $s_{\max}$ to be connected.

Lemma 3.6 *Suppose that* $2c(k-1) < n$ *and* $k \geq 2$. *Then, the graphs* s_α *and* $s_{\max}$ *are connected. Moreover,* $|\alpha s_{\max}| > n/2$.

Proof To prove the first statement, we claim that

$$|C(u)| = 1 \quad \text{for all } u \in S_{\max}. \tag{23}$$

Indeed, if this is not true, then there exists $u \in S_{\max}$ such that $|C(u)| \geq 2$. Lemma 3.5 yields that $p_u(\delta) \geq k/2$ for all points $\delta \in \Omega$. By (19) with $\Delta = \Omega$, this implies that

$$c \geq \frac{1}{k(k-1)} \sum_{\delta \in \Omega} p_u(\delta) \geq \frac{1}{k(k-1)} \frac{|\Omega| k}{2} = \frac{n}{2(k-1)},$$

which contradicts the hypothesis of the lemma . Thus, formula (23) is proved.

Assume to the contrary that the graph s_α is not connected for some $\alpha \in \Omega$. Then, it has a component C containing at most half of the vertices, that is,

$$2|C| \leq |\alpha s_{\max}| < n. \tag{24}$$

By (23), one can find a relation $u \in S_{\max}$ such that $C(u) = C$. Then, for any point $\delta \in \Omega \backslash C$, we have $n_v < n_u$ or $C(v) \neq C(u)$, where $v = r(\alpha, \delta)$ (if $C(v) = C(u) = C$, then $\delta \in C$). By statement (1) of Lemma 3.5, this implies that $p_u(\delta) \geq k$. On the other hand, $2|\Omega \backslash C| \geq n$ by (24). From (19) with $\Delta = \Omega \backslash C$, we obtain

$$c \geq \frac{1}{k(k-1)} \sum_{\delta \in \Omega \backslash C} p_u(\delta) \geq \frac{1}{k(k-1)} |\Omega \backslash C| k \geq \frac{n}{2(k-1)}, \tag{25}$$

which contradicts the hypothesis of the lemma. Thus, the graph s_α is connected.

To prove that the graph $s_{\max}$ is also connected, assume to the contrary that one of its components, say C, has at most $n/2$ points. Let $\alpha \in C$ and $u \in S_{\max}$. Then, $\alpha u \subseteq C$ and $n_u > n_v$ for all $v = r(\alpha, \delta)$ with $\delta \in \Omega \backslash C$. By statement (1) of Lemma 3.5, this implies that $p_u(\delta) \geq k$ for all such δ. Thus, inequality (25) holds again, which contradicts the hypothesis of the lemma.

To prove the second statement, denote by V the union of all $v \in S$ with $n_v < k$, and fix $u \in S_{\max}$. Then, by statement (1) of Lemma 3.5, we have $p_u(\delta) \geq k$ for all $\delta \in \Omega$ such that $r(\alpha, \delta) \in V$. This implies that

$$\sum_{\delta \in \alpha V} p_u(\delta) \geq k |\alpha V|.$$

Since there are $k(k-1)$ pairs of different points in αu, at least for one of such pairs, say (α, β), we obtain

$$c \geq c(u) = |\Omega_{\alpha,\beta}| \geq \frac{1}{k(k-1)} \sum_{\delta \in \alpha V} p_u(\delta) \geq \frac{k\,|\alpha V|}{k(k-1)} = \frac{|\alpha V|}{k-1}.$$

By the hypothesis of the lemma, this implies that $2\frac{|\alpha V|}{k-1}(k-1) < n$, whence $|\alpha V| < n/2$. Since $|\alpha V| + |\alpha s_{\max}| = n$, we are done. □

3.5 Proof of Theorem 3.1

Obviously, we may assume that $k \geq 2$. Let $\alpha \in \Omega$. It suffices to prove that each $\beta \in \alpha s_{\max}$ is a regular point of the coherent configuration $\mathcal{X}_\alpha$. Assume to the contrary that this is not true for some β. Then, $\mathcal{X}_\alpha$ has a basis relation v such that $|\beta v| \geq 2$. Therefore, there exist distinct points γ_1 and γ_2 such that

$$r(\beta, \gamma_1) = v = r(\beta, \gamma_2). \tag{26}$$

Let T_α be the set defined in Lemma 3.2. Then, in view of (15), $v \notin T_\alpha$. Therefore, neither γ_1 nor γ_2 belongs to $\alpha s_{\max}$.

Let us verify that formula (26) holds with β replaced by an arbitrary $\beta' \in \alpha s_{\max}$ and suitable distinct points γ_1 and γ_2. By virtue of (15), the relation $u \in T_\alpha$ containing the pair (β, β') is of the form

$$u = \{(\delta, \delta^g) : \delta \in \Delta\}$$

for some bijection $g : \Delta \to \Delta'$, where Δ and Δ' are the fibers of $\mathcal{X}_\alpha$ containing β and β', respectively. Define a permutation $f \in \mathrm{Sym}(\Omega)$ by

$$\omega^f = \begin{cases} \omega^g & \text{if } \omega \in \Delta, \\ \omega^{g^{-1}} & \text{if } \omega \in \Delta', \\ \omega & \text{otherwise.} \end{cases}$$

Then, the graph of f is the union of basis relations of $\mathcal{X}_\alpha$, each of which is of valency 1. One can see that in this case, f takes any basis relation of $\mathcal{X}_\alpha$ to another basis relation. This implies that f is an isomorphism of the coherent configuration $\mathcal{X}_\alpha$ to itself. Therefore, by equality (26), we have

$$r(\beta', \gamma_1) = r(\beta^f, \gamma_1^f) = r(\beta^f, \gamma_2^f) = r(\beta', \gamma_2),$$

and the claim is proved. Thus, the set $\Omega_{\gamma_1,\gamma_2}$ contains $\alpha s_{\max}$. By the hypothesis of the theorem and second statement of Lemma 3.6, this implies that

$$c \geq |\Omega_{\gamma_1,\gamma_2}| \geq |\alpha S_{\max}| > n/2.$$

However, then, $n > 2c(k-1) > n(k-1)$, which is impossible for $k > 1$. □

4 Inequality (3) in simple groups of Lie type

The main purpose of the following two sections is to prove Theorem 4.1 below, from which Theorems 1.2 and 1.3 were deduced in Introduction. In this section, we reduce the proof to Lemma 4.3, which will be proved in the next section.

Theorem 4.1 *For the Cartan scheme $\mathcal{X}$ of every group $G \in \mathcal{L}$, inequality (3) holds.*

We generally follow the notation of well-known Carter's book [6] with some exceptions that we explain below inside parentheses. If Φ_l is a simple Lie algebra of rank l, then $\Phi_l(q)$ is the simple Chevalley group of rank l over a field of order q. Let B, N, and $H = B \cap N$ be a Borel, monomial, and Cartan subgroups of a simple Chevalley group $\Phi_l(q)$ as in [6], while $W = N/H$ be the corresponding Weyl group. Then, [6, Proposition 8.2.1] implies that the subgroups B and N form a (B, N)-pair of $\Phi_l(q)$. If τ is a symmetry of the Dynkin diagram of Φ_l of order t, then ${}^t\Phi_l(q)$ is the simple twisted group of Lie type (in [6] such a group is denoted as ${}^t\Phi_l(q^t)$).[2] Again B, N, and $H = B \cap N$ stand for Borel, monomial, and Cartan subgroups of a simple twisted group of Lie type, and $W = N/H$ is the Weyl group (in [6], they are denoted by B^1, N^1, and so on). It follows from [6, Theorem 13.5.4] that in this case, B and N form a (B, N)-pair of ${}^t\Phi_l(q)$ again. For the sake of brevity, we will use notation ${}^t\Phi_l(q)$ for all simple groups of Lie type, assuming that t is the empty symbol in the case of untwisted groups. Recall also that the order w of the Weyl group W does not depend on the order of the underlying field.

Let G be a finite simple group of Lie type, and let $\mathcal{X} = (\Omega, S)$ be the Cartan scheme of G, where the corresponding (B, N)-pair is as in the previous paragraph (see Definition 1.1). In particular, $\Omega = G/H$ and $S = \mathrm{Orb}(G, \Omega^2)$. Put $n = |\Omega|$, $k = k(\mathcal{X})$, and $c = c(\mathcal{X})$.

Lemma 4.2 *There exists an element $g_0 \in G$ such that $H \cap H^{g_0} = 1$. In particular,*

$$k = \max_{s \in S} n_s = |H|. \tag{27}$$

Proof It is well known that $B = U \rtimes H$ is the semidirect product of U and H, where U is the unipotent radical of B. By [7, Propositions 5.1.5 and 5.1.7], there exists a unipotent element $u \in U$ such that $C_G(u) \le U$ (in fact, u can be chosen as a regular unipotent element fixed by an appropriate Frobenius map of the corresponding algebraic group). It follows that $[h, u] \ne 1$ for every $h \in H^{\#}$. On the other hand, if $h \in H \cap H^u$, then $[h, u] \in H \cap U = 1$, so $h = 1$, and $g_0 = u$ is the desired element of G.[3] Now, in view of (6),

$$k = \max_{s \in S} n_s = \max_{g \in G} \frac{|H|}{|H \cap H^g|} = \frac{|H|}{|H \cap H^{g_0}|} = |H|.$$

□

[2] In the case of Suzuki and Ree groups, $q = 2^{2\alpha+1}$ for ${}^2B_2(q)$ and ${}^2F_4(q)$, and $q = 3^{2\alpha+1}$ for ${}^2G_2(q)$, where $\alpha > 1$ is an integer.

[3] The alternative way to establish the same is to apply Zenkov's theorem [22]. It yields that since H is abelian, there is an element $g_0 \in G$ such that $H \cap H^{g_0}$ lies in the Fitting subgroup of G, which is trivial if the group G is simple.

Observe that G satisfies the hypotheses of Lemmas 2.3 and 2.4. Indeed, the transitivity of the action of G on Ω is evident, while the monomial subgroup N of G satisfies the additional condition from Lemma 2.4 due to [6, Proposition 8.4.5]. This enables us to estimate the indistinguishing number c and get the required inequality (3) with the help of Lemma 4.3 below, which is proved in the next section.

In what follows, for a coset $\overline{y} = Hy$, set $M_{\overline{y}} = \{u \in \overline{y} : u^G \cap H \neq \varnothing\}$. Note that all elements of $M_{\overline{y}}$ are semisimple. For an integer m, set

$$M_{\overline{y},m} = \{u \in M_{\overline{y}} : |u^G| \geq m\}, \quad \text{and} \quad M'_{\overline{y},m} = M_{\overline{y}} \backslash M_{\overline{y},m}.$$

Put

$$r_m = \max_{y \in G \backslash H} |M'_{\overline{y},m}| \quad \text{and} \quad m_0 = \min_{\varnothing \neq y^G \cap H \neq y^G} |y^G|.$$

Lemma 4.3 *In the above notation, there exists a positive integer m such that*

$$\frac{k}{m} + \frac{r_m}{m_0} \leq \frac{1}{2wk} \tag{28}$$

for all groups $G \in \mathcal{L}$.

Proof of Theorem 4.1 Immediately follows from Lemma 4.3 and Lemma 4.4 below. □

Lemma 4.4 *Let G be a simple group of Lie type. Suppose that there exists an integer m such that inequality (28) holds. Then, for the Cartan scheme $\mathcal{X}$ of G, inequality (3) is satisfied.*

Proof It follows from Lemma 2.3 that

$$c \leq \max_{y \in G \backslash H} \sum_{h \in H} \chi(hy) \leq \max_{y \in G \backslash H} \sum_{x \in M_{\overline{y}}} \chi(x), \tag{29}$$

where χ is the permutation character of the group induced by the action of G on Ω. Let $x \in M_{\overline{y}}$. Then, by the definition of $M_{\overline{y}}$, $\mathrm{Fix}(x) \neq \varnothing$, i.e., there are $h_0 \in H$ and $g_0 \in G$ such that $x = h_0^{g_0}$. In the notation of Lemma 2.3, we have $\chi(x) = |N : (C \cap N)|\,|\Omega|/|x^G|$. Furthermore, $|N : (C \cap N)| \leq |N/H| = |W| = w$, because $H \leq C \cap N$. We conclude that

$$\chi(x) \leq \frac{w\,n}{|x^G|}. \tag{30}$$

Let m be a positive integer from Lemma 4.3. Our definitions imply that $|x^G| \geq m$ for all $x \in M_{\overline{y},m}$ and $|x^G| \geq m_0$ for all $x \in M_{\overline{y}}$. Taking into account $|M_{\overline{y}}| \leq |H| = k$ and formula (30), we obtain

$$\sum_{x\in M_{\overline{y}}}\chi(x)\le w\,n\sum_{x\in M_{\overline{y}}}\frac{1}{|x^G|}\le w\,n\left(\sum_{x\in M_{\overline{y},m}}\frac{1}{|x^G|}+\sum_{x\in M'_{\overline{y},m}}\frac{1}{|x^G|}\right)$$
$$\le w\,n\left(\frac{|M_{\overline{y},m}|}{m}+\frac{|M'_{\overline{y},m}|}{m_0}\right)\le w\,n\left(\frac{k}{m}+\frac{r_m}{m_0}\right).$$

By inequality (28), this implies

$$\sum_{x\in M_{\overline{y}}}\chi(x)\le wn\cdot\frac{1}{2wk}=\frac{n}{2k}$$

for any $y\in G\backslash H$. In view of (29), it immediately follows that $2ck\le n$, and inequality (3) holds. □

5 Proof of Lemma 4.3

First, suppose that G is a simple exceptional group. We prove that relation (28) holds for $m=m_0$. Note that the size of the conjugacy class of a non-identity semisimple element of G can be estimated from below by means of results in [9,10] (for all exceptional groups other than the Ree and Suzuki groups, this was done in [20]). The corresponding lower bounds for m_0 are listed in the second column of Table 1. The values from the third and forth columns are well known. Using this table, one can easily check that

$$m_0\ge 2wk^2, \tag{31}$$

which is equivalent to inequality (28) for $m=m_0$, because $r_{m_0}=0$ in this case.

Table 1 Exceptional groups

${}^t\Phi_l$	m_0	$\lvert H\rvert$	$\lvert W\rvert$
E_8	q^{112}	$(q-1)^8$	$2^{14}\cdot 3^5\cdot 5^2\cdot 7$
E_7	$(1/2)q^{64}$	$(q-1)^7/(2,q-1)$	$2^{10}\cdot 3^4\cdot 5\cdot 7$
E_6	$(1/3)q^{30}$	$(q-1)^6/(3,q-1)$	$2^7\cdot 3^4\cdot 5$
${}^2E_6$	$(1/3)q^{30}$	$(q-1)^4(q+1)^2/(3,q+1)$	$2^7\cdot 3^2$
F_4	q^{16}	$(q-1)^4$	$2^7\cdot 3^2$
G_2	$q^3(q^3-1)$	$(q-1)^2$	$2^2\cdot 3$
${}^3D_4$	q^{16}	$(q-1)(q^3-1)$	$2^2\cdot 3$
${}^2F_4$	$q^6(q-1)(q^3+1)$	$(q-1)^2$	2^4
${}^2G_2$	$q^2(q^2+q+1)$	$q-1$	2
${}^2B_2$	$q^2(q-1)$	$q-1$	2

Table 2 Classical groups I

${}^t\Phi_l$	Conditions	m_0	$\lvert H\rvert$	$\lvert W\rvert$	l_0	a
A_l		$\frac{q^{2l}}{2}$	$\frac{(q-1)^l}{(l+1,q-1)}$	$(l+1)!$	7	4
${}^2A_l$	l odd	$\frac{q^{4l-3}}{2(q+1)}$	$\frac{(q-1)^{\frac{l+1}{2}}(q+1)^{\frac{l-1}{2}}}{(l+1,q+1)}$	$2^{\frac{l+1}{2}}\frac{l+1}{2}!$	6	4
${}^2A_l$	l even	$\frac{q^{2l+1}}{2(q+1)}$	$\frac{(q-1)^{\frac{l}{2}}(q+1)^{\frac{l}{2}}}{(l+1,q+1)}$	$2^{\frac{l}{2}}\frac{l}{2}!$	6	4
B_l	$\frac{l(q-1)}{2}$ odd	$\frac{q^{4l-1}}{4(q+1)}$	$\frac{(q-1)^l}{2}$	$2^l l!$	4	4
B_l	$\frac{l(q-1)}{2}$ even	$\frac{q^{2l+1}}{4(q+1)}$	$\frac{(q-1)^l}{2}$	$2^l l!$	4	4
C_l		$\frac{q^{4l-4}}{2}$	$\frac{(q-1)^l}{(2,q-1)}$	$2^l l!$	3	4
D_l		$\frac{q^{4l-3}}{4(q+1)}$	$\frac{(q-1)^l}{(4,q^l-1)}$	$2^{l-1}l!$	4	2
${}^2D_l$		$\frac{q^{4l-3}}{4(q+1)}$	$\frac{(q-1)^{l-1}(q+1)}{(4,q^l+1)}$	$2^{l-1}l!$	4	2

Now G is a simple classical group. Our main source for estimating the size of a conjugacy class of G is [5].[4] Let V be a natural module over a field $\mathbb{F}_{q^v}$, where $v = 2$ in the case of unitary groups and $v = 1$, otherwise, such that $G \leq PSL(V)$, and let $\widetilde{G}$ be the preimage of G in $SL(V)$. If $x \in G$ and $X \leq G$, then $\widetilde{x}$ and $\widetilde{X}$ are preimages of x and X in $\widetilde{G}$. We also agree to fix a basis of the vector space V so that the preimage $\widetilde{H}$ of the Cartan subgroup H consists of diagonal matrices. Following [5, Definition 3.16], for any $x \in G$, we denote by $\nu(x)$ the codimension of largest eigenspace of $\widetilde{x}$ on $\overline{V} = V \otimes K$, where K is the algebraic closure of $\mathbb{F}_q$. For elements x conjugated to elements of H, which are of prime interest for our purposes, $\nu(x)$ is equal to the difference between the dimension of V and the maximum eigenvalue multiplicity of the diagonal matrix $\widetilde{h}$ with $x = h^g$. We gather in Table 2 the lower bounds m_0 on the sizes of conjugacy classes from [5, Table 3.7–3.9][5] as well as the numbers $|H|$ and $|W|$. This table also contains the numbers l_0 and a defining the class $\mathcal{L}$. We also suppose that q is odd in the case of the groups $B_l(q)$ due to the well-known isomorphism $B_l(q) \cong C_l(q)$ for even q.

Now, we are ready to define the number m for simple classical groups. Denote by m_1 the lower bound for $|x^G|$ with $\nu(x) \geq 2$ that was found in [5, Tables 3.7–3.9]; the relevant values of m_1 are collected in the third column of Table 3. Set

$$m = \begin{cases} m_0, & \text{if } \nu(h) \geq 2 \text{ for all } h \in H^{\#}, \\ m_1, & \text{otherwise.} \end{cases} \tag{32}$$

[4] It is worth noting that in 'an asymptotical sense' the required lower bounds can be taken from [15, Lemma 3.4]. We choose to use the results of the later paper [5] in order to obtain the numerical values of l_0 and a.

[5] It is worth mentioning that despite [5, Tables 3.7–3.9] contain the bounds on the sizes of conjugacy classes in the group $\mathrm{Inndiag}(G)$ rather than G itself, the bounds for m_0 in Table 5 are correct, because $|G : C_G(h)| = |\mathrm{Inndiag}(G) : C_{\mathrm{Inndiag}(G)}(h)|$ for every $h \in H$ (see, e.g., the definition of the diagonal automorphism in [6, Sec. 12.2]).

Table 3 Classical groups II

${}^t\Phi_l$	Conditions	m_1	r_m
A_l		$\frac{q^{4(l-1)}}{2}$	$\frac{l(l+1)(q-1)^2}{2} - 1$
${}^2A_l$	l even	$\frac{q^{4l-3}}{2(q+1)}$	$\frac{(l+1)(q+1)^2}{2} + q$
B_l	$\frac{l(q-1)}{2}$ even	$\frac{q^{4l-1}}{4(q+1)}$	$\frac{l(q-3)}{2} + 1$

Note that for any coset $\overline{y} = Hy$ distinct from H, $M_{\overline{y},m} = \{x \in M_{\overline{y}} \mid \nu(x) \geq 2\}$ and $M'_{\overline{y},m}$ consist of all elements $x \in M_{\overline{y}}$ such that $\nu(x) = 1$. Recall that $r_m = \max_{y \in G \setminus H} |M'_{\overline{y},m}|$.

Lemma 5.1 *In the above notation, the following statements hold.*

(1) If G is one of the groups A_l, ${}^2A_l$ with l even, and B_l with $l(q-1)/2$ even, then the number r_m does not exceed the number in the fourth column of the corresponding row of Table 3.

(2) If G is one of the other simple classical groups, then $\nu(h) \geq 2$ for every $h \in H^{\#}$.

Proof It is well known and easily verified that the diagonal subgroup of a perfect classical matrix group contains an element h with $\nu(h) = 1$ only if G is one of the groups in statement (1). Therefore, we need only to estimate r_m in these cases.

We claim that in any case,

$$r_m \leq |\{h \in H^{\#} : \ \nu(h) \leq 2\}| =: u. \tag{33}$$

Indeed, let y and $z = hy$ be distinct elements of $M'_{\overline{y},m}$. Then, $\nu(y) = \nu(z) = 1$. Therefore, each of the matrices $\widetilde{y}$ and $\widetilde{z}$ has an eigenvalue of multiplicity $\dim(V) - 1$. Since these matrices are conjugate to diagonal matrices, this implies that the matrix $\widetilde{h} = \widetilde{y}(\widetilde{z})^{-1}$ has an eigenvalue of multiplicity at least $\dim(V) - 2$. Therefore, $\nu(h) \leq 2$. Since this is true for all $z \in M'_{\overline{x},m}$, we are done.

Let $G = A_l$. Then, the required statement immediately follows from (33) with the help of direct estimation of the number u from above by the number of diagonal matrices in $\mathrm{SL}(l+1, q)$ with at least $l-1$ equal diagonal entries.

Suppose that $G = {}^2A_l$ and l is even. To check the required upper bound on the number u, we observe that the basis of V can be chosen so that any matrix $\widetilde{h} \in \widetilde{H}$ is of the form

$$\widetilde{h} = \mathrm{diag}(\lambda_1, \ldots, \lambda_r, \lambda_0, \lambda_1^{-q}, \ldots, \lambda_r^{-q}),$$

where $r = l/2$, $\lambda_i \in \mathbb{F}_{q^2}$ for all i, $(\lambda_0)^{q+1} = 1$, and $\lambda_0(\lambda_1)^{1-q} \cdots (\lambda_r)^{1-q} = 1$. If, in addition, $\nu(h) \leq 2$ and $l \geq 6$, then either

$$\widetilde{h} = \mathrm{diag}(\lambda, \ldots, \lambda, \lambda_0, \lambda, \ldots, \lambda),$$

where $\lambda^{q+1} = 1$ and $\lambda_0\lambda^l = 1$, or

$$\widetilde{h} = \mathrm{diag}(\lambda, \ldots, \lambda, \mu, \lambda, \ldots, \lambda, \lambda_0, \lambda, \ldots, \lambda, \mu^{-q}, \lambda, \ldots, \lambda),$$

where $\lambda = \lambda_0$, $\lambda^{l-1}\mu^{1-q} = 1$, and μ takes an arbitrary jth of the first r positions (so μ^{-q} takes the $(r+1+j)$th position). The rest is routine.

Let $G = B_l$ and $l(q-1)/2$ be even. Then $G = \widetilde{G} = \Omega_{2l+1}(q)$. To estimate u from above, choose the basis of V so that any matrix $h \in H$ is of the form

$$h = \mathrm{diag}(\xi^{k_1}, \ldots, \xi^{k_l}, \xi^{-k_1}, \ldots, \xi^{-k_l}, 1),$$

where ξ is a primitive element of the field $\mathbb{F}_q$, and the number $k_1 + \ldots + k_l$ is even. If, in addition, $\nu(h) \leq 2$ and $l \geq 3$, then either

$$h = \mathrm{diag}(-1, \ldots, -1, 1)$$

(recall that $l(q-1)/2$ is even), or

$$h = \mathrm{diag}(1, \ldots, 1, \mu, 1, \ldots, 1, \mu^{-1}, 1, \ldots, 1),$$

where μ is a nonzero square in $\mathbb{F}_q$ and takes an arbitrary jth of the first l positions (so μ^{-1} takes the $(l+j)$th position). Thus, $u \leq l(q-3)/2 + 1$. □

To complete the proof, we verify inequality (28) for the number m defined by (32). Observe that, due to (32) and Lemma 5.1, the number r_m equals 0 in all cases when $m = m_0$. In the latter case, it suffices to verify inequality (31). We proceed further case by case.

Let $G = C_l(q)$. Here, $m = m_0$ and we need to prove that $m_0 \geq 2wk^2$. According to Table 2, this is true if

$$\frac{q^{4l-4}}{2} \geq 2^{l+1} l!(q-1)^{2l}$$

for $l \geq 3$ and $q \geq 4l$. For $l = 3$, this inequality is straightforward. If $l \geq 4$, then $q^{2l-4} \geq 4(2l)^l \geq 2^{l+2} l!$, and we are done.

Let $G = D_l(q)$ or $G = {}^2D_l(q)$. Then, $m = m_0$ and inequality (31) is true if

$$\frac{q^{4l-3}}{4(q+1)} \geq 2^l l!(q-1)^{2l-2}(q+1)^2$$

for $l \geq 4$ and $q \geq 2l$. However, since $(q-1)^{2l-2}(q+1)^3 < q^{2l+1}$ for all these l and q, it suffices to prove that $q^{2l-4} \geq 2^{l+2} l!$. For $l = 4$, this is verified directly, while for $l > 4$, we have $q^{2l-4} \geq 4(2l)^l \geq 2^{l+2} l!$.

Let $G = A_l(q)$. We may assume $l \geq 7$ and $q \geq 4l$. By Lemma 5.1,

$$r_m \leq \frac{l(l+1)(q-1)^2}{2} - 1 \leq \frac{q^4}{32}.$$

Thus, the left-hand side of (28) can be estimated as follows:

$$\frac{k}{m}+\frac{r_m}{m_0}\le\frac{2(q-1)^l}{q^{4l-1}}+\frac{2q^4}{32q^{2l}}\le\frac{2}{q^{4l-3}}+\frac{1}{16q^{2l-4}}\le\frac{1}{8q^{2l-4}}. \tag{34}$$

On the other hand, $(l+1)!\le 4^{l-3}l^{l-4}$ for $l\ge 7$: This is verified directly for $7\le l\le 9$, and follows from the obvious inequalities $(l+1)!<l^l<4^{l-3}l^{l-4}$ for $l\ge 10$. Therefore, in our case, we get the following lower bound for the right-hand side of (28):

$$\frac{1}{2wk}\ge\frac{1}{2(q-1)^l(l+1)!}\ge\frac{1}{2q^l4^{l-3}l^{l-4}}\ge\frac{1}{2q^l4q^{l-4}}=\frac{1}{8q^{2l-4}}. \tag{35}$$

Thus, the required statement follows from (34) and (35).

For each of the remaining two series of classical groups, the expression on the left-hand side of (28) for $m=m_0\le m_1$ does not exceed the same expression for $m=m_1$ (see Tables 2 and 3). Since the expression on the right-hand side in both cases does not depend on whether $m=m_0$ or not, it suffices to verify (28) for $G={}^2A_l(q)$ (resp., $G=B_l(q)$) independently of the parity of l (resp., $l(q-1)/2$), where m_0 and m are taken as in the case of even l (resp. even $l(q-1)/2$).

Let $G={}^2A_l(q)$. We may assume $l\ge 6$ and $q\ge 4l$. Lemma 5.1 yields that

$$r_m\le\frac{(l+1)(q+1)^2}{2}+q\le\frac{q^3}{6}.$$

Put $b=\lfloor l+1/2\rfloor$. Now, the left-hand side and right-hand side of (28) can be estimated as follows:

$$\frac{k}{m}+\frac{r_m}{m_0}\le\frac{2(q-1)^b(q+1)^{\lfloor\frac{l}{2}\rfloor+1}}{q^{4l-3}}+\frac{2q^3(q+1)}{6q^{2l+1}}\le\frac{2q^l(q+1)}{q^{4l-3}}+\frac{q^3(q+1)}{3q^{2l+1}} \tag{36}$$

and

$$\frac{1}{2wk}\ge\frac{1}{2(q-1)^b(q+1)^{\frac{l}{2}}2^bb!}\ge\frac{1}{2q^l2^bb!}. \tag{37}$$

By (36) and (37), it suffices to verify that

$$2^bb!\le\frac{3q^{2l-3}}{2(q+1)(q^{l-1}+6)}. \tag{38}$$

However, one can easily check that $2(q+1)(q^{l-1}+6)\le 3q^l$ and $2^bb!\le q^{l-3}$ for all $q\ge 4l\ge 25$. Therefore, (38) holds, and we are done.

Let $G=B_l(q)$. We may assume $l\ge 4$ and $q\ge 4l$. By Lemma 5.1,

$$r_m\le\frac{l(q-3)}{2}+1\le\frac{q^2}{8}.$$

Now, the left-hand side and right-hand side of (28) can be estimated as follows:

$$\frac{k}{m}+\frac{r_m}{m_0}\le\frac{4q^l(q+1)}{2q^{4l-1}}+\frac{4q^2(q+1)}{8q^{2l+1}}=\frac{(q+1)(q^l+4)}{2q^{3l-1}}$$

and

$$\frac{1}{2wk}\ge\frac{1}{2^l l!(q-1)^l}\ge\frac{1}{2^l l!q^{l-1}(q-1)}.$$

Thus, it suffices to verify that

$$(q^l+4)2^l l!\le 2q^{2l-2}.$$

This is straightforward for $l=4$. Since $q\ge 4l$, the required inequality holds whenever $l!\le 2^{l-4}l^{l-2}$, which can easily be checked for $5\le l\le 10$. Finally, if $l\ge 11$, then $l!\le l^l\le 2^{l-4}l^{l-2}$. This completes the proof of the lemma.

6 Proof of Theorem 1.4

Let $G=\mathrm{PSL}(2,q)$ with $q>3$, H the Cartan subgroup of G, and $\mathcal{X}=\mathrm{Inv}(G,\Omega)$, where $\Omega=G/H$. If q is odd, then the required statement follows from Theorem 3.1 and Corollary 2.6, because inequality (3) is satisfied. Indeed, in this case,

$$|G|=\frac{q(q^2-1)}{2},\qquad |H|=\frac{q-1}{2},\qquad |\Omega|=|G:H|=q^2+q,$$

so it suffices to verify that $c<(q^2+q)/(q-3)$. However, if χ is the permutation character of the action of G on Ω and $\chi(x)\ne 0$ for some $x\in G\backslash H$, then $\chi(x)=2$ by Lemma 2.4, because $|C_G(x)|=|C_G(h_0)|$ and in our case $C_G(h_0)=H$. Thus, $\mathrm{fix}(G)=2$. By Lemma 2.3, this implies that $c\le 2k=q-1<(q^2+q)/(q-3)$, as required.

Let now q be even. Then, $G=\mathrm{SL}(2,q)$ and

$$|G|=q(q^2-1),\qquad |H|=q-1,\qquad |\Omega|=|G:H|=q^2+q. \tag{39}$$

First, we study the structure of $\mathcal{X}$ in terms of double H-cosets (see Sect. 2.3).

One can see that the group $N=N_G(H)$ is the disjoint union of two double H-cosets, namely H and $HiH=Hi$, where

$$i=\begin{pmatrix}0&1\\1&0\end{pmatrix}$$

Denote by s_1 and s_i the basis relations of $\mathcal{X}$, for which $D_{s_1}=H$ and $D_{s_i}=HiH$ (see (5)). Clearly, $s_1=1_\Omega$.

Lemma 6.1 *Let S be the set of basis relations of the coherent configuration $\mathcal{X}$. Then, given $s \in S$, we have*

$$n_s = \begin{cases} 1 & \text{if } s \in \{s_1, s_i\}, \\ q-1 & \text{otherwise.} \end{cases}$$

In particular, $|S| = q + 4$ and $|S_{\max}| = q + 2$.

Proof It is easy to verify that $H^x \cap H = 1$ for all $x \in G \backslash N$ and $N = H \cup Hi$. Thus, the required statements follow from formula (6). □

Denote by U and V the subgroups (in G) of unipotent upper triangular and lower triangular matrices, respectively. Since, obviously, $H \le N_G(U) \cap N_G(V)$, we conclude that

$$HuH = HU^{\#} = U^{\#}H \quad \text{and} \quad HvH = HV^{\#} = V^{\#}H \tag{40}$$

for all $u \in U^{\#}$ and $v \in V^{\#}$. Denote by s_u and s_v the basis relations of $\mathcal{X}$, for which $D_{s_u} = HuH$ and $D_{s_v} = HvH$, respectively. In view of (40), these relations do not depend on the choice of the matrices

$$u = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad v = \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix},$$

where x and y are nonzero elements of the field $\mathbb{F}_q$. Again by (40), we have $(s_u)^* = s_u$ and $(s_v)^* = s_v$.

Lemma 6.2 *In the above notation, let $s \in S$. Then,*

(1) $c_{s_u s}^{s_v} = 0$ if $s = s_1$ or s_i, and $c_{s_u s}^{s_v} = 1$ otherwise,
(2) if $s \notin \{s_1, s_i, s_u, s_v\}$, then $c_{s_u s_v}^{s} = 1$ or $c_{s_v s_u}^{s} = 1$.

Proof It is straightforward to check that $c_{s_u s_1}^{s_v} = c_{s_u s_i}^{s_v} = 0$. By Lemma 6.1, we may assume that $s \in S_{\max}$, and hence, $n_s = q - 1 = n_{s_v}$. Therefore, $c_{s_u s}^{s_v} = c_{s_u s_v}^{s}$. The number $|H|\, c_{s_u s_v}^{s}$ is equal to the multiplicity, with which an element $w \in D_s$ enters the product

$$D_{s_u}\, D_{s_v} = HuH\, HvH = HU^{\#}\, HV^{\#} = HH(U^{\#}V^{\#})$$

(see (40)). Thus, to prove statement (1), it suffices to verify that no two elements in UV belong to the same H-coset. For this aim, suppose that $u_1 v_1 h = u_2 v_2$ for some $u_1, u_2 \in U$, $h \in H$, and $v_1, v_2 \in V$. Then, the group U of unipotent upper triangular matrices contains the element

$$u_2^{-1} u_1 \;\; = v_2\, h^{-1} v_1^{-1},$$

which is a lower triangular matrix. It follows that $u_1 = u_2$, $v_1 = v_2$, $h = 1$, and we are done.

To prove statement (2), it suffices to verify that the complement to the set $D_{s_u}D_{s_v} \cup D_{s_v}D_{s_u}$ in G is equal to $D_{s_1} \cup D_{s_i} \cup D_{s_u} \cup D_{s_v}$. In view of equalities (40), this is equivalent to

$$G\backslash(HU^{\#}V^{\#} \cup HV^{\#}U^{\#}) = N \cup HU^{\#} \cup HV^{\#}. \tag{41}$$

To prove this relation, we observe that general elements of the sets $U^{\#}V^{\#}$ and $V^{\#}U^{\#}$ are, respectively,

$$\begin{pmatrix} 1+xy & x \\ y & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & x \\ y & 1+xy \end{pmatrix},$$

where x and y are nonzero elements in $\mathbb{F}_q$. Therefore, there are at least $q-1$ elements in $V^{\#}U^{\#}$, which do not belong to $U^{\#}V^{\#}$ (they correspond to nonzero elements xy). By the statement proved in the previous paragraph, it follows that the set $HU^{\#}V^{\#} \cup HV^{\#}U^{\#}$ is the disjoint union of $(q-1)^2$ distinct cosets of H contained in $HU^{\#}V^{\#}$ and at least $q-1$ distinct cosets of H contained in $HV^{\#}U^{\#}$. Since none of all these cosets is contained in $N \cup HU^{\#} \cup HV^{\#}$, we have

$$\begin{aligned}(q-1)^2q &= q(q+1)(q-1) - 2(q-1) - 2(q-1)^2 \\ &= |G\backslash(N \cup HU^{\#} \cup HV^{\#})| \geq |HU^{\#}V^{\#} \cup HV^{\#}U^{\#}| \\ &\geq (q-1)^2(q-1) + (q-1)(q-1) = (q-1)^2q,\end{aligned}$$

which proves formula (41). □

Let us verify that the coherent configuration $\mathcal{X}_\alpha$ is 1-regular for $\alpha = H$. Indeed, in this case, Theorem 1.4 follows from Corollary 2.6.

To prove the 1-regularity of $\mathcal{X}_\alpha$, we check that every point $\beta \in \alpha s_{\max}$ is regular. However, if t is a basis relation of $\mathcal{X}_\alpha$, then t is contained in a basis relation s of $\mathcal{X}$. If $s \in \{s_1, s_i\}$, then by Lemma 6.1, we have

$$|\beta t| \leq |\beta s| = n_s = 1.$$

Thus, by the same lemma, we may assume that $s \in S_{\max}$, and hence, t belongs to the set T_α defined in Lemma 3.2. The latter lemma proves that β is regular if the graph s_α is connected.

Let us prove the connectedness of s_α. Suppose that the pair $(\gamma, \delta) \in \alpha u \times \alpha v$, belongs to the basis relation s. Then, obviously, $c_{s_u s}^{s_v} \neq 0$. Thus, by statement (1) of Lemma 6.2 and the definition of s_α, the points γ and δ are adjacent in s_α. From statement (2) of Lemma 6.2, it follows that any other vertex $\beta \in \alpha s$ with $s \in S_{\max}$, has at least one neighbor in the set $\alpha s_u \cup \alpha s_v$, i.e.,

$$\beta s_\alpha \cap (\alpha s_u \cup \alpha s_v) \neq \varnothing.$$

Thus, s_α is connected, and we are done.

7 Proof of Theorem 1.5

We make use of the well-known Weisfeiler-Leman algorithm described in detail in [21, Section B]. The input of it is a set $\mathcal{S}$ of binary relations on a set Ω, and the output is the smallest coherent configuration

$$\mathrm{WL}(\mathcal{S}) = (\Omega, S)$$

such that $\mathcal{S} \subset S^{\cup}$. The running time of the algorithm is polynomial in the cardinalities of $\mathcal{S}$ and Ω. The proof of the following statement is based on the Weisfeiler-Leman algorithm and can be found in [17, Theorem 3.5].

Theorem 7.1 *Let $\mathcal{X}$ and $\mathcal{X}'$ be coherent configurations on n points. Then given an algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$, all the elements of the set* $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ *can be listed in time $(bn)^{O(b)}$, where $b = b(\mathcal{X})$.*

To solve the recognition problem, we recognize first the colored graphs D of Cartan schemes of G with respect to (B, N)-pairs of rank at least 2. In this case, from the corollary of the main theorem in [8], it follows that B is the normalizer $N_G(P)$ of a group $P \in \mathrm{Syl}_p(G)$ such that

$$H \cap P = 1, \qquad H \le N_G(P), \qquad |N_G(P)| = |H|\,|P|, \tag{42}$$

where p is the characteristic of the ground field. By [19], one can also see that apart from finitely many exceptional groups, $N = N_G(H)$ for every group from $\mathcal{L}$. Thus, the correctness of the algorithm below is obtained as a consequence of Theorems 1.3 and 7.1.

In what follows, we denote by Ω the vertex set of the graph $D \in \mathcal{G}_n$, by $\mathcal{S}$ the set of its color classes, and by $\mathcal{S}_{\alpha,\beta}$ the union of $\mathcal{S}$ and the set of two one-element relations $\{(\alpha, \alpha)\}$ and $\{(\beta, \beta)\}$.

Recognizing Cartan schemes (the rank of (B, N) is at least **2**)

Step 1. Find the coherent configuration $\mathcal{X} = \mathrm{WL}(\mathcal{S})$.
Step 2. If there are no distinct points α, β such that the coherent configuration $\mathcal{X}_{\alpha,\beta} = \mathrm{WL}(\mathcal{S}_{\alpha,\beta})$ is complete, then $b(\mathcal{X}) > 2$ and $D \notin \mathcal{K}_n$.
Step 3. Find all the elements of the group $G = \mathrm{Iso}(\mathcal{X}, \mathcal{X}, \mathrm{id})$ by the algorithm of Theorem 7.1. If G is not simple, then $D \notin \mathcal{K}_n$.
Step 4. Analyzing the number $|G|$, check that $G \in \mathcal{L}$. If not, then $D \notin \mathcal{K}_n$; otherwise, set p to be the characteristic of the ground field associated with G.
Step 5. Fix a point stabilizer H of G and find $P \in \mathrm{Syl}_p(G)$, for which relations (42) hold. If there is no such P, then $D \notin \mathcal{K}_n$.
Step 6. Now, $D \in \mathcal{K}_n$ and $\mathcal{X}$ is the Cartan scheme of G with respect to (B, N), where $B = N_G(P)$ and $N = N_G(H)$. □

Let us estimate the running time of the algorithm. At Steps 1 and 2, we apply the Weisfeiler-Leman algorithm $n(n-1)+1$ times. Thus, the complexity of these

steps is at most $n^{O(1)}$. At Step 3, the time is polynomially bounded by Theorem 7.1 and the fact that a group is simple if and only if no non-trivial conjugacy class of it generates a proper subgroup (given the multiplication table of G, the conjugacy classes of this group can be found efficiently). Step 4 requires polynomially many arithmetic operations involving the number $|G|$ written in the unary system. Here, we use the fact based on CFSG that except for known cases, any finite simple group is uniquely determined by its order (see Theorem 5.1 and Lemma 2.5 in [14]). Since Steps 5 and 6 can obviously be implemented in polynomial time for the group G given by the multiplication table, we conclude that the running time of the algorithm is at most $n^{O(1)}$.

The first four steps of the algorithm remain the same as before if we do not assume that the rank of (B, N) is at least 2. But in this case, one can find a 2-transitive representation of the group G; here, a complete classification of all 2-transitive groups is useful (see, e.g., [11, Sec. 7.7]). This enables us to find the groups B and N.

To solve the isomorphism problem, let $D \in \mathcal{K}_n$ and $D' \in \mathcal{G}_n$. Denote by $\mathcal{S}$ and $\mathcal{S}'$ the sets of color classes of D and D', respectively. Without loss of generality, we may assume that there is a color preserving bijection $\psi : \mathcal{S} \to \mathcal{S}'$. Then, one can apply the canonical version of the Weisfeiler-Leman algorithm presented in [21, Section M], where, in fact, the following statement was proved.

Theorem 7.2 *Let $\mathcal{S}$ and $\mathcal{S}'$ be m-sets of binary relations on an n-element set. Then, given a bijection $\psi : \mathcal{S} \to \mathcal{S}'$ one can check in time $mn^{O(1)}$ whether or not there exists an algebraic isomorphism $\varphi : \mathrm{WL}(\mathcal{S}) \to \mathrm{WL}(\mathcal{S}')$ such that $\varphi|_{\mathcal{S}} = \psi$. Moreover, if φ does exist, then it can be found within the same time.* □

Clearly, the original graphs D and D' are not isomorphic if there is no algebraic isomorphism φ from Theorem 7.2. Assuming the existence of φ, we can find the set

$$\mathrm{Iso}(D, D') = \mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$$

in time $(bn)^{O(b)}$ by Theorem 7.1, where $\mathcal{X} = \mathrm{WL}(\mathcal{S})$, $\mathcal{X}' = \mathrm{WL}(\mathcal{S}')$, and $b = b(\mathcal{X})$. Since $b \leq 2$ (Theorem 1.3), we are done.

References

1. Abramenko, P., Parkinson, J., Van Maldeghem, H.: Distance regularity in buildings and structure constants in Hecke algebras. arXiv:1508.03912 [math.CO] 1–23 (2015)
2. Bailey, R.F., Cameron, P.J.: Base size, metric dimension, and other invariants of groups and graphs. Bull. Lond. Math. Soc. **43**, 209–242 (2011)
3. Bannai, E., Ito, T.: Algebraic Combinatorics. I Benjamin/Cummings, Menlo Park, CA (1984)
4. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 3, 18th edn. Springer, Berlin (1989)
5. Burness, T.C.: Fixed point ratios in actions of finite classical groups, II. J. Algebra **309**, 80–138 (2007)
6. Carter, R.W.: Simple Groups of Lie Type. Wiley, London (1972)
7. Carter, R.W.: Finite Groups of Lie Type. Conjugacy Classes and Complex Characters. Wiley, London (1985)
8. De Medts, T., Haot, F., Tent, K., Van Maldeghem, H.: Split BN-pairs of rank at least 2 and the uniqueness of splittings. J. Group Theory **8**(1), 1–10 (2005)

9. Deriziotis, D.: The centralizers of semisimple elements of the Chevalley groups E_7 and E_8. Tokyo J. Math. **6**(1), 191–216 (1983)
10. Deriziotis, D.: Conjugacy classes and centralizers of semisimple elements in finite groups of Lie type, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen, Heft 11 (1984)
11. Dixon, J.D., Mortimer, B.: Permutation Groups, Graduate Texts in Mathematics. Springer, New York (1996)
12. Evdokimov, S., Ponomarenko, I.: Separability number and schurity number of coherent configurations. Electron. J. Comb. **7**, R31 (2000)
13. Evdokimov, S., Ponomarenko, I.: Permutation group approach to association schemes. Eur. J. Comb. **30**, 1456–1476 (2009)
14. Kimmerle, W., Lyons, R., Sandling, R., Teague, D.N.: Composition factors from the group ring and Artin's theorem on orders of simple groups. Proc. Lond. Math. Soc. Ser. **60**(1), 89–122 (1990)
15. Liebeck, M.W., Shalev, A.: Simple groups, permutation groups, and probability. J. Am. Math. Soc. **12**(2), 497–520 (1999)
16. Muzychuk, M., Ponomarenko, I.: On Pseudocyclic association schemes. Ars Math. Contemp. **5**(1), 1–25 (2012)
17. Ponomarenko, I.: Bases of schurian antisymmetric coherent configurations and isomorphism test for schurian tournaments. J. Math. Sci. **192**(3), 316–338 (2013)
18. Saxl, J., Shalev, A.: The fixity of permutation groups. J. Algebra **174**, 1122–1140 (1995)
19. Veldkamp, F.D.: Roots and maximal tori in finite forms of semisimple algebraic groups. Math. Ann. **207**, 301–314 (1974)
20. Vdovin, E.P.: On intersections of solvable Hall subgroups in finite simple exceptional groups of Lie type. Proc. Steklov Institute Math. **285**(1), S1–S8 (2014)
21. Weisfeiler, B. (ed.): On Construction and Identification of Graphs, Springer Lecture Notes in Mathematics, **558** (1976)
22. Zenkov, V.I.: Intersection of abelian subgroups in finite groups. Math. Notes **56**(2), 869–871 (1994)
23. Zieschang, P.-H.: Theory of Association Schemes. Springer, Berlin (2005)
24. Zieschang, P.-H.: Trends and lines of development in scheme theory. Eur. J. Comb. **30**, 1540–1563 (2009)