

I. Ponomarenko, A. Vasil'ev

TESTING ISOMORPHISM OF CENTRAL CAYLEY
GRAPHS OVER ALMOST SIMPLE GROUPS IN
POLYNOMIAL TIME

ABSTRACT. A Cayley graph over a group G is said to be central if its connection set is a normal subset of G . It is proved that for any two central Cayley graphs over explicitly given almost simple groups of order n , the set of all isomorphisms from the first graph onto the second can be found in time $\text{poly}(n)$.

In memory of Sergei Evdokimov

§1. INTRODUCTION

In the present paper, we are interested in a special case of the following restriction of the Graph Isomorphism Problem to the class of Cayley graphs.

Cayley Graph Isomorphism Problem. *For two explicitly given finite groups G and G' and two sets $X \subset G$ and $X' \subset G'$, construct the set $\text{Iso}(\Gamma, \Gamma')$, where $\Gamma = \text{Cay}(G, X)$ and $\Gamma' = \text{Cay}(G, X')$.*

Here the input consists of the multiplication tables of G and G' and the sets X and X' , whereas the output is either empty or given by an element of the set $\text{Iso}(\Gamma, \Gamma')$ and a generating set of the group $\text{Aut}(\Gamma)$ (of size polynomial in the order n of the group G). Obviously, the Luks algorithm [12] solves the Cayley Graph Isomorphism Problem in polynomial time for every group G , whenever the set X is of constant sizes. If G is cyclic, then the problem with no restriction for X is also solvable in polynomial time (see [6] and [13]). It should be noted that if $G = G'$ and G is a so-called CI-group, then an obvious algorithm solves the Cayley Graph Isomorphism Problem in time polynomial in $|\text{Aut}(G)|$ (for details, see [10]).

The aforementioned special case is formed by the two following conditions imposed on the input graphs and groups. First, we assume that Γ is a *central* Cayley graph over G , which means that X is a normal subset

Key words and phrases: Cayley graph, almost simple group, polynomial-time algorithm.

of G , i.e., $X^g = X$ for every $g \in G$. Second, the group G is assumed to be *almost simple*, i.e., the socle of G is a nonabelian simple group. The same conditions are imposed on the graph Γ' and group G' . Even in this rather restrictive case, the problem is still nontrivial; at least the number of possible input graphs is exponential in n .

Example. Let $G = \text{Sym}(m)$ be a symmetric group of degree m . Then the number $N(m)$ of central colored Cayley graphs over G is equal to $2^{p(m)}$, where $p(m)$ is the number of all partitions of the set $\{1, \dots, m\}$. Since $p(m)$ is approximately equal to $2^{\sqrt{m}}$, the number $N(m)$ is exponential in $n = m!$.

By technical reasons, it is more convenient to deal with *colored* Cayley graphs. Such a graph is given by a partition $\mathfrak{P}$ of the group G into $k \geq 2$ classes $X_0, \dots, X_{k-1}$ with $X_0 = \{1\}$, and can be thought as arc-colored complete graph with vertex set G and the i th color class of arcs coinciding with the arc set of the Cayley graph $\text{Cay}(G, X_i)$, $i = 0, \dots, k-1$. We say that $\mathfrak{P}$ is the *Cayley partition* of this graph and denote the latter by $\text{Cay}(G, \mathfrak{P})$. In what follows, all Cayley graphs are assumed to be colored: the graph $\text{Cay}(G, X)$ is treated as $\text{Cay}(G, \mathfrak{P})$ for $k = 3$ and $X_1 = X$.

Theorem 1.1. *For any two central Cayley graphs Γ and Γ' over explicitly given almost simple groups G and G' of order n , the set $\text{Iso}(\Gamma, \Gamma')$ can be found in time $\text{poly}(n)$.*

Corollary 1.2. *The automorphism group of a central Cayley graph over an explicitly given almost simple group of order n can be found in time $\text{poly}(n)$.*

The proof of Theorem 1.1 is a mix of combinatorial and permutation group techniques. Section 2 provides a relevant background for the combinatorial part including coherent configurations and Cayley schemes. In Section 3, we use a classification of regular almost simple subgroups of primitive groups [11] to prove (Lemma 3.2) that except for one special case, if $K \leq \text{Sym}(G)$ is a 2-closed primitive group containing regular almost simple subgroup, then

$$K = \text{Sym}(G) \quad \text{or} \quad K \leq D(2, G), \quad (1)$$

where $D(2, G)$ is the subgroup of $\text{Sym}(G)$ generated by the holomorph of G and the permutation $\sigma : g \mapsto g^{-1}$, $g \in G$. We extend this result to non-primitive groups in Sections 4 and 5 by showing that in this case, either formula (1) holds or K is a nontrivial generalized wreath product

(Theorems 4.1 and 5.1). We apply this fact in Section 6 to the automorphism group K of a central Cayley graph Γ over the group G to establish that

$$K^S = \text{Sym}(S) \quad \text{or} \quad K^S \leq D(2, S), \quad (2)$$

where $S = \text{Soc}(G)$ is the socle of G and K^S is the restriction to S of the setwise stabilizer of S in K . Note that if G is a symmetric group of degree at least 5, then the group $D(2, G)$ is isomorphic to the group $G \wr \text{Sym}(2)$. Thus, as a byproduct of (2), we obtain the following generalization of the result [9, Theorem 1.1] on the automorphism group of the Cayley graph $\text{Cay}(G, X)$, where G is a symmetric group and X is the set of its transpositions.

Theorem 1.3. *Let G be a symmetric group of degree at least 5, X a proper normal subset of $G \setminus \text{Soc}(G)$, and $\Gamma = \text{Cay}(G, X)$. Then $\text{Aut}(\Gamma) = D(2, G)$.*

In Sections 7 and 8, we develop algorithmic tools to find the above structure of the group K with the help of the related Cayley scheme and the group G . The main algorithm providing the proof of Theorem 1.1 is given in Section 9.

Notation.

The diagonal of the Cartesian product $\Omega \times \Omega$ is denoted by 1_Ω .

For $s \subseteq \Omega \times \Omega$, set $s^* = \{(\beta, \alpha) : (\alpha, \beta) \in s\}$.

For $\alpha \in \Omega$ and $s \subseteq \Omega \times \Omega$, set $\alpha s = \{\beta \in \Omega : (\alpha, \beta) \in s\}$.

For $\Delta \subseteq \Omega$ and $s \subseteq \Omega \times \Omega$, set $s_\Delta = s \cap (\Delta \times \Delta)$.

For a partition $\mathfrak{E}$ of a set Ω and $s \subseteq \Omega \times \Omega$, set $s_\mathfrak{E}$ to be the relation consisting of the pairs $(\Delta, \Delta') \in \mathfrak{E} \times \mathfrak{E}$ such that s meets $\Delta \times \Delta'$.

For a set S of binary relations, put $S^\cup$ to be the set of all unions of relations from S .

The symmetric and alternating groups on Ω are denoted by $\text{Sym}(\Omega)$ and $\text{Alt}(\Omega)$, respectively.

For $f \in \text{Sym}(\Omega)$ and $s \subseteq \Omega \times \Omega$, set $s^f = \{(\alpha^f, \beta^f) : (\alpha, \beta) \in s\}$.

For a group G and its subgroup L , set L_{left} and L_{right} to be the subgroups of $\text{Sym}(G)$ induced by left and right multiplications of L , respectively, and $L^* = L_{\text{left}} L_{\text{right}}$.

For a group G , set $D(2, G)$ to be the subgroup of $\text{Sym}(G)$ generated by the group $\text{Hol}(G) = N_{\text{Sym}(G)}(G_{\text{right}})$ and the permutation $\sigma : g \mapsto g^{-1}$.

For a group $K \leq \text{Sym}(G)$ and a set $H \subseteq G$, the restriction to H of the setwise stabilizer of H in K is denoted by K^H .

For an imprimitivity system $\mathfrak{L}$ of a transitive group K , set $K_{\mathfrak{L}}$ and $K^{\mathfrak{L}}$ to be, respectively, the intersection of all K^H with $H \in \mathfrak{L}$ and the permutation group induced by the action of K on $\mathfrak{L}$.

For a group G and a permutation group K , set $\text{Reg}(K, G)$ to be the set of all regular subgroups of K that are isomorphic to G .

§2. COHERENT CONFIGURATIONS AND CAYLEY SCHEMES

This section contains well-known basic facts on coherent configurations. All of them can be found in [7] and papers cited there.

2.1. Main definitions. Let Ω be a finite set and S a partition of $\Omega \times \Omega$. The pair $\mathcal{X} = (\Omega, S)$ is called a *coherent configuration* on Ω if the following conditions hold:

- (C1) $1_{\Omega} \in S^{\cup}$,
- (C2) $S^* = S$,
- (C3) given $r, s, t \in S$, the number $c_{rs}^t = |\alpha r \cap \beta s^*|$ does not depend on the choice of the pair $(\alpha, \beta) \in t$.

The elements of Ω and S , and the numbers c_{rs}^t are called the *points* and *basis relations*, and the *intersection numbers* of $\mathcal{X}$, respectively. The numbers $|\Omega|$ and $|S|$ are called the *degree* and the *rank* of $\mathcal{X}$. The coherent configuration $\mathcal{X}$ is said to be *homogeneous* if $1_{\Omega} \in S$.

Denote by $\Phi = \Phi(\mathcal{X})$ the set of $\Lambda \subseteq \Omega$ such that $1_{\Lambda} \in S$. The elements of Φ are called the *fibers* of $\mathcal{X}$. In view of condition (C1), the set Ω is the disjoint union of all of them. Moreover, for each $s \in S$, there exist uniquely determined fibers Λ and Δ such that $s \subseteq \Lambda \times \Delta$. Note that the coherent configuration $\mathcal{X}$ is homogeneous if and only if $|\Phi| = 1$.

Let $e \in S^{\cup}$ be an equivalence relation and $\mathfrak{E}$ the set of its classes. Given $\Delta \in \mathfrak{E}$ denote by S_{Δ} the set of all nonempty relations s_{Δ} with $s \in S$. Then the pair

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

is a coherent configuration called the *restriction* of $\mathcal{X}$ to Δ . This enables to define the restriction of $\mathcal{X}$ to a set $\Lambda \in \Phi^{\cup}$: the corresponding equivalence relation is equal to the union of $\Delta \times \Delta$, where Δ runs over the fibers contained in Λ . Another coherent configuration associated with e is obtained as follows. Denote by $S_{\mathfrak{E}}$ the set of all nonempty relations $s_{\mathfrak{E}}$, $s \in S$. Then

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

is a coherent configuration called the *quotient* of $\mathcal{X}$ modulo e .

2.2. Combinatorial and algebraic isomorphisms. A bijection $f : \Omega \rightarrow \Omega'$ is called the (combinatorial) *isomorphism* from $\mathcal{X}$ onto a coherent configuration $\mathcal{X}' = (\Omega', S')$ if the set S' contains the relation s^f for each $s \in S$. The set of all isomorphisms f is denoted by $\text{Iso}(\mathcal{X}, \mathcal{X}')$. The group of all isomorphisms of $\mathcal{X}$ to itself contains a normal subgroup

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

called the *automorphism group* of $\mathcal{X}$. Conversely, let $G \leq \text{Sym}(\Omega)$ be a permutation group, and let S be the set of orbits of the component-wise action of G on $\Omega \times \Omega$. Then the pair $\mathcal{X} = (\Omega, S)$ is a coherent configuration; we say that $\mathcal{X}$ is *associated* with G and denote it by $\text{Inv}(G)$.

According to Wielandt [17], a permutation group G on Ω is said to be *2-closed* if it is equal to its *2-closure*

$$G^{(2)} = \text{Aut}(\text{Inv}(G)),$$

or, equivalently, if G is an automorphism group of a family of binary relations on Ω (such a family can always be chosen as the set of basis relations of a coherent configuration on Ω). If G is 2-closed and $\mathfrak{L}$ is an imprimitivity system of G , then the group $G_{\mathfrak{L}}$ is 2-closed. However, the group $G^{\mathfrak{L}}$ is not always 2-closed.

A bijection $\varphi : S \rightarrow S', r \mapsto r'$, is called an *algebraic isomorphism* from $\mathcal{X}$ onto $\mathcal{X}'$ if

$$c_{rs}^t = c_{r's'}^{t'}, \quad r, s, t \in S. \quad (3)$$

In this case, $\mathcal{X}$ and $\mathcal{X}'$ are said to be *algebraically isomorphic*. Each isomorphism f from $\mathcal{X}$ onto $\mathcal{X}'$ induces an algebraic isomorphism $\varphi_f : r \mapsto r^f$ between these configurations. The set of all isomorphisms inducing the algebraic isomorphism φ is denoted by $\text{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$. In particular,

$$\text{Iso}(\mathcal{X}, \mathcal{X}, \text{id}_S) = \text{Aut}(\mathcal{X}), \quad (4)$$

where id_S is the identity mapping on S .

An algebraic isomorphism φ induces a bijection from $S^{\cup}$ onto $(S')^{\cup}$: the union $r \cup s \cup \dots$ of basis relations of $\mathcal{X}$ is taken to $r' \cup s' \cup \dots$. This bijection is also denoted by φ . It preserves the equivalence relations $e \in S^{\cup}$; moreover, the equivalence relations e and $\varphi(e)$ have the same number of classes as well as the same multiset of their sizes. In this case, if $\mathfrak{E}$ and $\mathfrak{E}'$ are the sets of classes of e and $\varphi(e)$, respectively, and $\Delta \in \mathfrak{E}$, then φ induces the algebraic isomorphisms

$$\varphi_{\Delta} : \mathcal{X}_{\Delta} \rightarrow \mathcal{X}'_{\Delta'}, \quad s \mapsto \varphi(s)_{\Delta'}, \quad \text{and} \quad \varphi_{\mathfrak{E}} : \mathcal{X}_{\mathfrak{E}} \rightarrow \mathcal{X}'_{\mathfrak{E}'}, \quad s_{\mathfrak{E}} \mapsto \varphi(s)_{\mathfrak{E}'}$$

for a suitable $\Delta' \in \mathfrak{E}'$.

2.3. Direct sum and wreath product. Let $\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega', S')$ be coherent configurations. Denote by $\Omega \sqcup \Omega'$ the disjoint union of Ω and Ω' , and by $S \boxplus S'$ the union of the set $S \sqcup S'$ and the set of all relations $\Delta \times \Delta'$ and $\Delta' \times \Delta$ with $\Delta \in \Phi(\mathcal{X})$ and $\Delta' \in \Phi(\mathcal{X}')$. Then the pair

$$\mathcal{X} \boxplus \mathcal{X}' = (\Omega \sqcup \Omega', S \boxplus S')$$

is a coherent configuration called the *direct sum* of $\mathcal{X}$ and $\mathcal{X}'$. The automorphism group of this configuration equals the direct product $\text{Aut}(\mathcal{X}) \times \text{Aut}(\mathcal{X}')$ acting on the set $\Omega \sqcup \Omega'$. Furthermore, if φ is an algebraic isomorphism from $\mathcal{X} \boxplus \mathcal{X}'$ to another coherent configuration, then the latter is also the direct sum $\mathcal{Y} \boxplus \mathcal{Y}'$ and φ induces algebraic isomorphisms $\mathcal{X} \rightarrow \mathcal{Y}$ and $\mathcal{X}' \rightarrow \mathcal{Y}'$ coinciding with the restrictions of φ on Ω and Ω' , respectively.

Let $\mathcal{X}$ be a homogeneous coherent configuration, $e \in S^\cup$ an equivalence relation, and $\mathfrak{E}$ the set of classes of e . We say that $\mathcal{X}$ is the *wreath product* with respect to e if for each $s \in S$ such that $s \not\subseteq e$,

$$s = \bigcup_{(\Lambda, \Delta) \in s_{\mathfrak{E}}} \Lambda \times \Delta.$$

In what follows, we always assume that the classes of e can be identified with the help of a family of the isomorphisms $f_{\Lambda, \Delta} : \mathcal{X}_\Lambda \rightarrow \mathcal{X}_\Delta$, $\Lambda, \Delta \in \mathfrak{E}$, such that

$$(s_\Lambda)^{f_{\Lambda, \Delta}} = s_\Delta, \quad s \in S. \quad (5)$$

In this case, $\mathcal{X}$ is isomorphic to the usual wreath product $\mathcal{X}_\Delta \wr \mathcal{X}_{\mathfrak{E}}$ for all $\Delta \in \mathfrak{E}$ (see [15, p.45]). The automorphism group of this coherent configuration is permutation isomorphic to the wreath product $\text{Aut}(\mathcal{X}_\Delta) \wr \text{Aut}(\mathcal{X}_{\mathfrak{E}})$ in imprimitive action.

Furthermore, if φ is an algebraic isomorphism from the wreath product $\mathcal{X}$ with respect to e to another coherent configuration, then the latter is also the wreath product $\mathcal{X}'$ with respect to $e' = \varphi(e)$ and φ induces algebraic isomorphisms $\mathcal{X}_\Delta \rightarrow \mathcal{X}'_{\Delta'}$ and $\mathcal{X}_{\mathfrak{E}} \rightarrow \mathcal{X}'_{\mathfrak{E}'}$ coinciding with the restrictions of φ on Δ and $\mathfrak{E}$, respectively, where $\mathfrak{E}'$ is the set of classes of e' and $\Delta' \in \mathfrak{E}'$.

2.4. Cayley schemes. A coherent configuration $\mathcal{X} = (\Omega, S)$ is called the *Cayley scheme* over a group G if

$$\Omega = G \quad \text{and} \quad G_{\text{right}} \leq \text{Aut}(\mathcal{X}).$$

In this case, $\mathcal{X}$ is homogeneous and each basis relation s is the set of arcs of the Cayley graph $\text{Cay}(G, X)$, where X is the neighborhood of the identity of G in the relation s . In particular, $\mathcal{X}$ can be treated as a color graph $\text{Cay}(G, \mathfrak{P})$, where the classes of the Cayley partition $\mathfrak{P}$ are the neighborhoods of the identity of G in the basis relations of $\mathcal{X}$.

The class of Cayley schemes is closed with respect to taking restrictions and quotients. Namely, if $\mathcal{X}$ is a Cayley scheme over a group G and $e \in S^\cup$ is an equivalence relation, then the class H of e containing the identity of G is a subgroup of G . Moreover, the set $\mathfrak{E}$ of classes of e coincides with the right H -cosets of G . It follows that

$$\mathcal{X}_H = \text{Cay}(H, \mathfrak{E}_H) \quad \text{and} \quad \mathcal{X}_{\mathfrak{E}} = \text{Cay}(G/H, \mathfrak{E}_{G/H}),$$

with

$$\mathfrak{E}_H = \{X \in \mathfrak{E} : X \subset H\} \quad \text{and} \quad \mathfrak{E}_{G/H} = \{\pi(X) : X \in \mathfrak{E}\},$$

where in the latter case, H is a normal subgroup of G and $\pi : G \rightarrow G/H$ is the canonical epimorphism.

Assume that the Cayley scheme $\mathcal{X}$ is the *wreath product* with respect to an equivalence relation $e \in S^\cup$. Then for any two classes $\Lambda, \Delta \in \mathfrak{E}$, there exists a permutation $f \in G_{\text{right}}$ taking Λ to Δ ; set $f_{\Lambda, \Delta}$ to be the restriction of f to Λ . Since all these f are automorphisms of $\mathcal{X}$, the family $\{f_{\Lambda, \Delta}\}_{\Lambda, \Delta \in \mathfrak{E}}$ satisfies conditions (5).

The Cayley scheme $\mathcal{X}$ is said to be *central* if $G_{\text{left}} \leq \text{Aut}(\mathcal{X})$ which is by definition of a Cayley scheme is equivalent to $G^* \leq \text{Aut}(\mathcal{X})$. One can see that $\mathcal{X}$ is central if and only if the colored Cayley graph associated with $\mathcal{X}$ is central.

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

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

The minimal and maximal elements with respect to this order are, respectively, the *trivial* and *discrete* coherent configurations. The first one is a unique coherent configuration $\mathcal{T}_\Omega$ with at most two basis relations: 1_Ω and its complement to $\Omega \times \Omega$ (if Ω consists of at least two points). Every basis relation of the discrete configuration is a singleton. With respect to this order, the direct sum $\mathcal{X} \boxplus \mathcal{X}'$ is the minimal coherent configuration

on $\Omega \sqcup \Omega'$, the restrictions of which to Ω and Ω' are equal to $\mathcal{X}$ and $\mathcal{X}'$, respectively.

One can prove that given a set $T \subseteq 2^{\Omega \times \Omega}$, there exists a unique minimal coherent configuration $\mathcal{X}'$ such that every relation of T is the union of some basis relations of $\mathcal{X}'$. This coherent configuration is called the *coherent closure* of T and can be constructed by the well-known Weisfeiler–Leman algorithm (WL-algorithm) [15, Section B] in time polynomial in sizes of T and Ω . To stress this fact, the coherent closure of T is denoted by $\text{WL}(T)$. For a color graph Γ with the set S of color classes, we set

$$\text{WL}(\Gamma, T) = \text{WL}(S \cup T)$$

and write $\text{WL}(\Gamma)$ instead of $\text{WL}(\Gamma, \emptyset)$. It is important to note that the automorphism group of the coherent configuration $\text{WL}(\Gamma, T)$ is equal to the subgroup of $\text{Aut}(\Gamma)$ leaving each relation of T fixed (as a set). This implies that if Γ is a Cayley graph over G , then the coherent configuration $\text{WL}(\Gamma)$ is a Cayley scheme over G . Since any coherent configuration $\mathcal{X}$ can be considered as a color graph, we extend our notation to write $\text{WL}(\mathcal{X}, T)$. Concerning the following statement, we refer to [14, Theorem 2.4].

Theorem 2.1. *Let S and S' be m -sets of binary relations on an n -element set. Then given a bijection $\psi : S \rightarrow S'$, one can check in time $mn^{O(1)}$ whether or not there exists an algebraic isomorphism $\varphi : \text{WL}(S) \rightarrow \text{WL}(S')$ such that $\varphi|_S = \psi$. Moreover, if φ does exist, then it can be found within the same time.*

§3. ALMOST SIMPLE GROUPS

In this section, we collect several known facts on finite almost simple groups and deduce some auxiliary results to be used throughout the paper.

Lemma 3.1. *Let G be an almost simple group of order n . Then*

- (i) $|G/L| \leq \log n$, where $L = \text{Soc}(G)$,
- (ii) $|\text{Reg}(K, G)| = n^{O(1)}$ for every $K \leq \text{Sym}(G)$ containing G as a normal regular subgroup.

Proof. From the description of the automorphism groups of simple groups (see, e.g., [4, Introduction]), it follows that $|\text{Aut}(L)/L| \leq \log |L|$. Therefore, statement (i) is a consequence of the inclusions $L \leq G \leq \text{Aut}(G) \leq \text{Aut}(L)$. The inclusions also imply that $|\text{Aut}(G)| \leq n \log n$. Since the centralizer of G in $\text{Sym}(G)$ is of order n [16, Exercise 4.5], we have

$$|K| \leq |N_{\text{Sym}(G)}(G)| \leq |C_{\text{Sym}(G)}(G)| \cdot |\text{Aut}(G)| \leq n^2 \log n.$$

On the other hand, the group G is 3-generated [5]. Thus, the number of regular subgroups of K isomorphic to G is at most $\binom{K}{3}$ and statement (ii) follows. $\square$

In the following statement, we use the classification of regular almost simple subgroups of a primitive group [11, Theorem 1.4].

Lemma 3.2. *Let G be an almost simple group and $G^* \leq K \leq \text{Sym}(G)$. Suppose that K is primitive. Then one of the following holds:*

- (i) $K \geq \text{Alt}(G)$,
- (ii) $G = \text{Soc}(G)$ and $K \leq D(2, G)$,
- (iii) $G = \text{Sym}(5)$ and $K = \text{Sp}_8(2)$ is 2-transitive.

Proof. Without loss of generality, we assume that neither $K \geq \text{Alt}(G)$, nor $G = \text{Soc}(G)$ and $K \leq D(2, G)$. Then by aforementioned classification, exactly one of the following pairs $(G, \text{Soc}(K))$ occurs:

- (a) $(\text{Alt}(p^2 - 2), \text{Alt}(p^2 + 1))$, where $p = 3 \pmod{4}$ is prime,
- (b) $(\text{Sym}(p - 2), \text{Alt}(p))$ or $(\text{Sym}(p - 2), \text{Alt}(p + 1))$, where $p \geq 7$ is prime,
- (c) the twelve pairs in the table below.

No.	G	$\text{Soc}(K)$	No.	G	$\text{Soc}(K)$
1	$\text{Alt}(5)$	$L_2(59)$	7	$\text{Sym}(5)$	$\Omega_8^+(2)$
2	$\text{Alt}(7)$	$\text{Alt}(11)$	8	$\text{Sym}(5)$	$\text{Sp}_8(2)$
3	$\text{Alt}(7)$	$\text{Alt}(12)$	9	$L_2(16).4$	$\text{Sp}_6(4)$
4	$\text{Sym}(5)$	$\text{Alt}(9)$	10	$L_2(16).4$	$\Omega_8^+(4)$
5	$\text{Sym}(5)$	$\text{Sp}_4(4)$	11	$L_3(4).2$	M_{23}
6	$\text{Sym}(5)$	$\text{Sp}_6(2)$	12	$L_3(4).2$	M_{24}

The assumption $G^* \leq K$, in particular, implies that $|G|^2 \leq |K|$. By straightforward check this excludes cases (a) with $p > 3$, (b) with $p > 7$, and cases 11 and 12 from the table. Similarly, the remaining cases in (a) and (b) as well as cases 1–4, and 9 are impossible because $|G|^2$ must divide $|K|$.

In cases 5, 6, 7, and 10 from the table, we check the maximal subgroups of K and show that none of them includes the subgroup isomorphic to G^* . Indeed, in cases 5 and 6 none of the maximal subgroups contains $\text{Alt}(5) \times \text{Alt}(5)$ [2, Tables 8.14, 8.28, 8.29]. In case 10, information from [11, Table 2] shows that K is an extension of $\Omega_8^+(4)$ by a field automorphism.

This group contains the only (up-to conjugation) maximal subgroup with section isomorphic to $L_2(16) \times L_2(16)$ [2, Table 8.50], but the order of this subgroup is less than $|G^*|$. In case 7, we make use of [11, Table 2] to see that $K = \Omega_8^+(2)$. Again this group includes up to conjugation the only maximal subgroup M with section isomorphic to $\text{Alt}(5) \times \text{Alt}(5)$ (see [2, Table 8.50]). However, $|M| = |G^*|$ but $M \simeq D(2, \text{Alt}(5))$ is not isomorphic to $G^* \simeq \text{Sym}(5) \times \text{Sym}(5)$.

This leaves us with case 8 of the table where $\text{Soc}(K) = \text{Sp}_8(2) = K$ and we arrive at case (iii) of the conclusion of the lemma. $\square$

§4. THE STRUCTURE OF AUTOMORPHISM GROUPS: THE PRINCIPAL SECTION

4.1. Preliminaries. Let G be a finite group. The automorphism group of every central Cayley graph over G contains a subgroup G^* (see Notation). In this section, we establish some basic facts on the permutation groups K satisfying the following condition:

$$G^* \leq K \leq \text{Sym}(G), \quad (6)$$

where G is an almost simple group. We use concept of the *generalized wreath product* of permutation groups introduced and studied in [8]. Namely, a transitive group K is the generalized wreath product if it has two imprimitivity systems $\mathfrak{L}$ and $\mathfrak{U}$ such that every block of $\mathfrak{L}$ is contained in a block of $\mathfrak{U}$ and

$$K_{\mathfrak{L}} = \prod_{X \in \mathfrak{U}} (K_X)^X.$$

The generalized wreath product is said to be *trivial* if either $\mathfrak{L}$ consists of singletons or $\mathfrak{U} = \{\Omega\}$. When $\mathfrak{L} = \mathfrak{U}$, the group K is permutation isomorphic to the wreath product $K^X \wr K^{\mathfrak{L}}$ in imprimitive action, where $X \in \mathfrak{U}$.

Theorem 4.1. *Let G be an almost simple group, and let K be a 2-closed group satisfying condition (6). Then one of the following statements holds:*

- (i) $K = \text{Sym}(G)$ or $G^* \trianglelefteq K$,
- (ii) K is a nontrivial generalized wreath product.

The proof of Theorem 4.1 is given in the end of Section 6.

4.2. The minimal block. Let K satisfy condition (6) and X be the K -block containing the identity of G . Since K is a permutation group on G that contains G_{right} , the block X is a subgroup of G [16, Theorem 24.12]. Taking into account that G_{left} also lies in K , we conclude that X is normal. Denote by L the intersection of all non-singleton K -blocks containing the identity of the group G . Then L is a K -block and we call it the *minimal block* of K .

Lemma 4.2. *Let K satisfy condition (6) and L the minimal block of K . Then L is normal subgroup of G including $\text{Soc}(G)$. In particular, L is an almost simple group such that $\text{Soc}(L) = \text{Soc}(G)$.*

Proof. According to the above remark, every K -block containing the identity of G is a normal subgroup of G . If the block is not a singleton, then this normal subgroup is nontrivial and hence contains $\text{Soc}(G)$, because the group G is almost simple. Thus, the minimal block L being the intersection of nontrivial normal subgroups of G is a normal subgroup and contains $\text{Soc}(G)$. $\square$

Denote by $\mathfrak{L}$ the imprimitivity system containing L . Obviously,

$$\text{Orb}(L^*, G) = \mathfrak{L}.$$

Recall that according to the definition, $K_{\mathfrak{L}}$ is a normal subgroup of K leaving each block of $\mathfrak{L}$ fixed (as a set), and given $X \in \mathfrak{L}$, the group $(L^*)^X \leq \text{Sym}(X)$ is induced by right multiplications of L .

Lemma 4.3. *For any $X \in \mathfrak{L}$, the group $(K_{\mathfrak{L}})^X$ is primitive and contains $(L^*)^X$.*

Proof. The normality of L in G implies that the orbits of the action of L^* on G coincide with the L -cosets. It follows that the permutation group induced by this action is contained in $K_{\mathfrak{L}}$. This proves the second statement. To prove the first statement, in view of the transitivity of K , we may assume that $X = L$.

Assume on the contrary that the group $K' = (K_{\mathfrak{L}})^L$ is not primitive. Then there exists a minimal non-singleton K' -block $L' < L$. Taking into account that $K' \trianglelefteq K^L$, we conclude that $L'' = (L')^k$ is a also K' -block for every $k \in K$ [16, Proposition 6.2]. The imprimitivity system $\mathfrak{L}'$ of the group K' that contains L' coincides with the imprimitivity system containing L'' , for otherwise by the minimality of L' and Lemma 4.2 applied

for the group K' , one can choose the block L'' so that

$$1 = L' \cap L'' \supseteq \text{Soc}(L) = \text{Soc}(G) \supsetneq 1,$$

a contradiction. Thus, $\mathfrak{L}'$ is an imprimitivity system of the group K^L . Consequently, L' is a non-singleton K -block strictly contained in L , which is impossible by the definition of L . $\square$

4.3. The wreath decomposition of $K_{\mathfrak{L}}$. For every two sets $X, X' \in \mathfrak{L}$, we write $X \sim X'$ if the restriction epimorphisms

$$(K_{\mathfrak{L}})^{X \cup X'} \rightarrow (K_{\mathfrak{L}})^X \quad \text{and} \quad (K_{\mathfrak{L}})^{X \cup X'} \rightarrow (K_{\mathfrak{L}})^{X'} \quad (7)$$

are isomorphisms. In particular, the groups $(K_{\mathfrak{L}})^X$ and $(K_{\mathfrak{L}})^{X'}$ are isomorphic. It is easily seen that $\sim$ is an equivalence relation on $\mathfrak{L}$. This relation is K -invariant, because $K_{\mathfrak{L}}$ is a normal subgroup of K . Denote by U the union of L -cosets belonging to the class of $\sim$ that contains L . Then U is obviously a K -block and hence is a normal subgroup of G . Thus,

$$L \trianglelefteq U \trianglelefteq G.$$

The imprimitivity system of the group K that contains the block U is denoted by $\mathfrak{U}$. We say that U/L is the *principal K -section* of G , and $\mathfrak{U}$ and $\mathfrak{L}$ are the *associated partitions*.

Theorem 4.4. *Let G be an almost simple group, K a 2-closed group satisfying condition (6), and $\mathfrak{U}, \mathfrak{L}$ are the partitions associated with the principal K -section. Then the coherent configuration $\text{Inv}(K_{\mathfrak{L}})$ is the direct sum of the coherent configurations $\text{Inv}(K_{\mathfrak{L}})_Y$, where $Y \in \mathfrak{U}$. In particular,*

$$K_{\mathfrak{L}} = \prod_{Y \in \mathfrak{U}} (K_{\mathfrak{L}})^Y, \quad (8)$$

i.e., K is generalized wreath product.

Proof. The subgroup $K_{\mathfrak{L}}$ of 2-closed group K is 2-closed too (see Subsection 2.2). Therefore, equality (8) follows from the first statement of the theorem, because the automorphism group of the direct sum equals the direct product of the summands (see Subsection 2.3). To prove the first statement, it suffices to verify that given $X, X' \in \text{Orb}(K_{\mathfrak{L}}, G)$,

$$X \not\sim X' \quad \Rightarrow \quad X \times X' \in \text{Orb}(K_{\mathfrak{L}}, X \times X'). \quad (9)$$

To this end, we note that the group $(K_{\mathfrak{L}})^{X \cup X'}$ is the subdirect product of the transitive constituents $M = (K_{\mathfrak{L}})^X$ and $M' = (K_{\mathfrak{L}})^{X'}$. Therefore,

there exist uniquely determined normal subgroups H and H' of M and M' , respectively, and a group isomorphism $\varphi : M/H \rightarrow M'/H'$ such that

$$(K_{\mathfrak{L}})^{X \cup X'} = \{(k, k') \in M \times M' : \varphi(k) = k'\}. \quad (10)$$

Now if $X \not\sim X'$, then at least one of the epimorphisms (7) is not an isomorphism. Therefore, one of the groups H and H' , say H , is nontrivial. It follows that H being a normal subgroup of the primitive group M (Lemma 4.3) acts transitively on X . By (10), this implies that $(K_{\mathfrak{L}})^{X \cup X'}$ contains the subgroup $H \times 1$. Thus,

$$(x, x')^{H \times 1} = X \times \{x'\}$$

for all $x' \in X'$ and hence the group $(K_{\mathfrak{L}})^{X \cup X'}$ is transitive on the set $X \times X'$. $\square$

§5. THE NORMALIZER OF $\text{Soc}(G)^*$ IN $\text{Sym}(G)$

The goal of this section is to prove the following theorem that shows (as we will see) that the case $U = G$ is very similar to the case where the group K is primitive.

Theorem 5.1. *Let G be an almost simple group, $S = \text{Soc}(G)$, and $N = N_{\text{Sym}(G)}(S^*)$. Then*

$$N = D(2, G). \quad (11)$$

Clearly, N is a proper subgroup of $\text{Sym}(G)$ and condition (6) is satisfied for $K = N$. In particular, the minimal block of N coincides with S .

Lemma 5.2. *In the above notation, $C_{\text{Sym}(G)}(S^*) = 1$.*

Proof. Set $C = C_{\text{Sym}(G)}(S^*)$. Then obviously, $C = C_N(S^*)$. Since N is transitive and C is normal in N , the orbits of C form an imprimitivity system of N . Denote by X the block of this system that contains the identity of G . We may assume that the block X is not a singleton, for otherwise $C = 1$ and we are done. Then $S \subseteq X$, because S is the minimal N -block. Since C is transitive on X and S is a block of C^X , there exists $c \in C$ such that $S^c = S$ and $c^S \neq 1$. However, the latter is impossible, because c^S centralizes the subgroups S_{left} and S_{right} . $\square$

Proof of Theorem 5.1. By Lemma 5.2, there exists a monomorphism from $N = N_{\text{Sym}(G)}(S^*)$ to $\text{Aut}(S^*)$. Since the latter is isomorphic to

the wreath product $W = \text{Aut}(S) \wr \text{Sym}(2)$, this monomorphism induces a monomorphism

$$\varphi : N \rightarrow W.$$

Clearly, φ can be chosen so that the subgroups S_{left} and S_{right} of the group N go to the subgroup $\text{Inn}(S) \times 1$ of the group $A = \text{Aut}(S) \times 1$ and to the subgroup $1 \times \text{Inn}(S)$ of the group $B = 1 \times \text{Aut}(S)$, respectively. Set

$$W_1 = \text{im}(\varphi) \quad \text{and} \quad W_0 = \text{im}(\varphi) \cap (A \times B).$$

Then since the index of $A \times B$ in W equals 2 and W_1 is not contained in $A \times B$, we conclude that

$$|W_1 : W_0| = 2. \quad (12)$$

Note that the centralizer of the group $\varphi(S_{\text{right}}) \leq B$ in the group W_0 is contained in A , because the group B is almost simple with the socle $\varphi(S_{\text{right}})$. Since the group $G_{\text{left}} \leq N$ centralizes S_{right} , this proves the first of the two following inclusions (the second one can be proved in a similar way):

$$\varphi(G_{\text{left}}) \leq A \quad \text{and} \quad \varphi(G_{\text{right}}) \leq B.$$

The first inclusion implies that $\varphi(G_{\text{left}}) \leq W_0 \cap A$. The reverse inclusion follows from the fact that the centralizer of G_{left} in $\text{Sym}(G)$ is equal to G_{right} [16, Proposition 4.3]. Thus, we obtain the equalities:

$$\varphi(G_{\text{left}}) = W_0 \cap A \quad \text{and} \quad \varphi(G_{\text{right}}) = W_0 \cap B. \quad (13)$$

This immediately implies that $\varphi(G_{\text{left}})$ and $\varphi(G_{\text{right}})$ are normal in W_0 . This group has trivial center and hence can be identified with a subgroup of the direct product of the groups $A' = \text{Aut}(\varphi(G_{\text{left}}))$ and $B' = \text{Aut}(\varphi(G_{\text{right}}))$ (isomorphic to $\text{Aut}(G)$). It follows that

$$\overline{W}_0 = W_0 / \varphi(G^*) \leq \overline{A'} \times \overline{B'},$$

where $\overline{A'} = A' / \varphi(G_{\text{left}})$ and $\overline{B'} = B' / \varphi(G_{\text{right}})$. Moreover in view of formulas (13), the group $\overline{W}_0$ intersects each of the groups $\overline{A'}$ and $\overline{B'}$ trivially. Therefore,

$$|\overline{W}_0| = |\text{Aut}(G)/G|. \quad (14)$$

Now, the inclusion $\varphi(\text{Aut}(G)) \leq W_0$ and formula (14) show that $W_0 = \varphi(\text{Hol}(G))$. Formula (12) yields that $|N : \text{Hol}(G)| = 2$. Since the permutation $\sigma : g \mapsto g^{-1}$ lies in N , formula (11) holds. $\square$

§6. SYMMETRIC AND NORMAL TYPES OF THE AUTOMORPHISM GROUP

Let G be an almost simple group, K be a 2-closed group satisfying condition (6), and U/L the principal K -section of G . Then the group L is almost simple (Lemma 4.2) and K^L is primitive (Lemma 4.3). We say that K is of *symmetric type* if either $K^L \geq \text{Alt}(L)$, or $G = \text{Sym}(5)$ and $K = \text{Sp}_8(2)$ is 2-transitive; if $L = \text{Soc}(L)$ and $K^L \leq D(2, L)$, the group K is said to be of *normal type*. The following statement is a straightforward consequence of Lemma 3.2 and the above definitions.

Proposition 6.1. *Let G be an almost simple group, and let $K \leq \text{Sym}(G)$ be a 2-closed group containing G^* . Then K is of symmetric or normal type.*

Let us study a group of symmetric and normal types in detail. As the following statement shows, any group of symmetric type is, in fact, the wreath product in imprimitive action. In what follows, $\mathfrak{U}$ and $\mathfrak{L}$ are the partitions associated with the principal K -section of G .

Theorem 6.2. *Let K be a group of symmetric type. Then*

$$\mathfrak{L} = \mathfrak{U} \quad \text{and} \quad (K_{\mathfrak{L}})^L = \text{Sym}(L).$$

In particular, K is permutation isomorphic to the wreath product $\text{Sym}(L) \wr K^{\mathfrak{L}}$ in imprimitive action.

Proof. Let $X, X' \in \mathfrak{L}$ and $X \sim X'$. We claim that there exists a bijection $f : X \rightarrow X'$, for which

$$s_f \in \text{Orb}(K_{\mathfrak{L}}, X \times X'), \tag{15}$$

where $s_f = \{(\alpha, \alpha f) : \alpha \in X\}$ is the graph of f . Indeed, consider the group $M = (K_{\mathfrak{L}})^{X \cup X'}$. Since $X \sim X'$, the group M acts faithfully on X and X' . As the group K is of symmetric type, each of these actions is 2-transitive. However, M has a unique faithful 2-transitive representation of degree $d = |X|$: this is obvious if $M \geq \text{Alt}(d)$ and follows from the classification of 2-transitive groups if $M = \text{Sp}_8(2)$ (see, e.g., [3, Table 7.4]). Consequently, among $2d$ point stabilizers M_{β} , $\beta \in X \cup X'$, there are exactly d distinct, and also $M_{\beta} \neq M_{\gamma}$ whenever β and γ are distinct points in X . Therefore, for every $\alpha \in X$ there is the only $\alpha' \in X'$ such that

$$M_{\alpha} = M_{\alpha'} = M_{\alpha, \alpha'}.$$

Thus, the required bijection f takes α to α' .

To prove that $\mathfrak{L} = \mathfrak{U}$, assume on the contrary that U contains a block $X \in \mathfrak{L}$ other than L . Denote by $f : L \rightarrow X$ the bijection defined in the above claim for $X = L$ and $X' = X$. Then by the assumption, the element $f(1)$, where 1 is the identity of the group G , does not belong to L . The binary relation s_f is invariant with respect to the group $K_{\mathfrak{L}} \geq L^*$ and hence for all $x \in L$,

$$(x, f(1)x) = (1, f(1))^{x_r} = (x, f(x)) = (1, f(1))^{x_l} = (x, xf(1)),$$

where x_r and x_l are the permutations of L^* induced by the right and left multiplication by x . This implies that the element $f(1) \in X \subset U$ centralizes L . However, this is impossible, because $f(1) \neq 1$ and the group U is almost simple.

Let us prove the second equality. The 2-closedness of K implies that $K_{\mathfrak{L}}$ is 2-closed. Furthermore, in view of the 2-transitivity of the group $(K_{\mathfrak{L}})^X$ its 2-closure equals $\text{Sym}(X)$. By Theorem 4.4 and equality $\mathfrak{L} = \mathfrak{U}$, this implies that

$$K_{\mathfrak{L}} = (K_{\mathfrak{L}})^{(2)} = \left(\prod_{X \in \mathfrak{L}} (K_{\mathfrak{L}})^X \right)^{(2)} = \prod_{X \in \mathfrak{L}} ((K_{\mathfrak{L}})^X)^{(2)} = \prod_{X \in \mathfrak{L}} \text{Sym}(X).$$

Thus, $(K_{\mathfrak{L}})^X = \text{Sym}(X)$ for all $X \in \mathfrak{L}$ and we are done. $\square$

Theorem 6.2 shows that in the case of symmetric type, the group $K^U = \text{Sym}(U)$ is the largest possible. In the normal type case, the group K^U is quite small. More exactly, the following statement holds.

Theorem 6.3. *Let K be a group of normal type. Then $K^U \leq D(2, U)$.*

Proof. By the hypothesis of the theorem, $L = \text{Soc}(L)$ and $K^L \leq D(2, L)$. By Lemma 4.2, the first equality implies that $L = \text{Soc}(G)$ and hence

$$L = \text{Soc}(U). \quad (16)$$

The second inclusion implies that $(L^*)^X$ is a characteristic subgroup of the group $(K_{\mathfrak{L}})^X$ for all $X \in \mathfrak{L}$. By the definition of U , this implies that $(L^*)^U$ is a characteristic subgroup of the group $(K_{\mathfrak{L}})^U$. However, the latter group is normal in K^U . Thus,

$$(L^*)^U \trianglelefteq K^U.$$

It follows that K^U is contained in the normalizer of $(L^*)^U$ in $\text{Sym}(U)$. However, this normalizer is contained in $D(2, U)$ by Theorem 5.1 applied for $G = U$ with taking into account equality (16). $\square$

Proof of Theorem 4.1. Let U/L be the principal K -section of the group G . By Proposition 6.1, the group K is of symmetric or normal type. Suppose first that $U = G$. Then statement (i) of Theorem 4.1 holds. Indeed, if K is of symmetric type, then $K = \text{Sym}(G)$ (Theorem 6.2), whereas if K is of normal type, then $K \leq D(2, G)$ (Theorem 6.3) and the required statement follows from the fact that G^* is normal in $D(2, G)$. Finally, if $U < G$, then statement (ii) of Theorem 4.1 holds by Theorem 4.4. $\square$

Proof of Theorem 1.3. First, assume that the group $K = \text{Aut}(\Gamma)$ is a nontrivial generalized wreath product. Note that $S = \text{Soc}(G)$ is a unique proper normal subgroup in G and $|G/S| = 2$. Therefore the generalized wreath product must be a usual one and the group K is permutation isomorphic to the wreath product $M \wr C_2$ in imprimitive action for some group $M \leq \text{Sym}(S)$. It follows that $G \setminus S$ is an orbit of the point stabilizer K_α , where α is the identity of G . Since $X \subset G \setminus S$ is a union of some orbits of K_α , we conclude that $X = G \setminus S$, a contradiction.

The group K is 2-closed as the automorphism group of a graph. The normality of X implies that K satisfies condition (6) with $G = \text{Sym}(m)$ for $m \geq 5$. Finally, K is not a nontrivial generalized wreath product by above, and $K \neq \text{Sym}(G)$, because the graph Γ is neither complete nor empty. Thus, by Theorem 4.1, the group G^* is normal in K and

$$G^* \leq K \leq D(2, G),$$

hence $K = G^*$ or $K = D(2, G)$, because $|D(2, G) : G^*| = 2$. However, since X is a normal subset of a symmetric group, we have $X = X^{-1}$, so the graph Γ has the automorphism $\sigma : g \mapsto g^{-1}$, $g \in G$. Thus, $K = \langle G^*, \sigma \rangle = D(2, G)$, as required. $\square$

§7. FINDING THE PRINCIPAL SECTION IN A CAYLEY SCHEME

7.1. The main result. Let $\mathcal{X}$ be a central Cayley scheme over an almost simple group G . Then the group $K = \text{Aut}(\mathcal{X})$ is 2-closed and satisfies condition (6). Therefore, K is of symmetric or normal type by Proposition 6.1. In this section, we develop an algorithmic technique to determine (with no K in hand) which of these cases occurs for the scheme $\mathcal{X}$. The main result here is Theorem 7.1 below which immediately follows from Corollaries 7.3 and 7.5 proved in Subsections 7.2 and 7.3, respectively.

Theorem 7.1. *Given a central Cayley scheme $\mathcal{X}$ over an almost simple group G of order n , one can determine the type of $K = \text{Aut}(\mathcal{X})$ and find the principal K -section of G in time $\text{poly}(n)$.*

7.2. The case of symmetric type. For a group $H \leq G$, denote by $\mathfrak{H}$ and $\text{WL}(\mathcal{X}, \mathfrak{H})$ the partition of G into the right H -cosets and the Cayley scheme $\text{WL}(\mathcal{X}, T)$ with $T = \{1_X : X \in \mathfrak{H}\}$, respectively. Recall that $\mathcal{T}_X$ is the trivial coherent configuration on X . Denote by $\mathcal{H}_0$ the set of groups H such that $\text{Soc}(G) \leq H \leq G$ and

$$\text{WL}(\mathcal{X}, \mathfrak{H}) = \bigsqcup_{X \in \mathfrak{H}} \mathcal{T}_X. \quad (17)$$

Lemma 7.2. *In the above notation, the following statements hold:*

- (i) *if the group K is of symmetric type, then the set $\mathcal{H}_0$ is nonempty and the minimal block L of K is the largest (by inclusion) element of $\mathcal{H}_0$,*
- (ii) *K is of symmetric type if and only if $\mathcal{H}_0$ contains $S = \text{Soc}(G)$.*

Proof. To prove statement (i), assume that the group K is of symmetric type. Set $\mathfrak{U}$ and $\mathfrak{L}$ to be the partitions associated with the principal K -section of G . Then by Theorem 6.2, we have $\mathfrak{L} = \mathfrak{U}$ and $\text{Inv}(K^X) = \mathcal{T}_X$ for all $X \in \mathfrak{L}$. By Theorem 4.4, this implies that

$$\text{Inv}(K_{\mathfrak{L}}) = \bigsqcup_{X \in \mathfrak{L}} \mathcal{T}_X. \quad (18)$$

The minimality of the direct sum implies that $\text{WL}(\mathcal{X}, \mathfrak{L}) = \text{Inv}(K_{\mathfrak{L}})$, which proves formula (17) for $H = L$ and $\mathfrak{H} = \mathfrak{L}$, in particular, $\mathcal{H}_0$ is nonempty. If L is not the largest element of $\mathcal{H}_0$, then there exists $H \in \mathcal{H}_0$ such that $H \setminus L \neq \emptyset$. It follows that

$$K \geq \text{Sym}(H) \times \text{id}_{G \setminus H},$$

where $\text{id}_{G \setminus H}$ is the identity subgroup of $\text{Sym}(G \setminus H)$. Hence there is a permutation $k \in K$ that moves the identity of G to $H \setminus L$ and leaves all non-identity elements of L fixed. But this is impossible, because L is a K -block.

To prove the necessity for statement (ii), let K be of symmetric type. Then formula (18) holds. Therefore, if $\mathfrak{S}$ is the partition of G into the cosets of S , then $\mathfrak{S}$ refines $\mathfrak{L}$ and hence

$$\text{WL}(\mathcal{X}, \mathfrak{S}) = \text{WL}(\text{WL}(\mathcal{X}, \mathfrak{L}), \mathfrak{S}) = \bigsqcup_{X \in \mathfrak{L}} \text{WL}(\mathcal{T}_X, \mathfrak{S}_X) = \bigsqcup_{X \in \mathfrak{S}} \mathcal{T}_X,$$

where $\mathfrak{S}_X$ is the partition of X induced by $\mathfrak{S}$. Consequently, $S \in \mathcal{H}_0$. Conversely, assume on the contrary that K is of normal type. Then $K^U \leq D(2, U)$ by Theorem 6.3. Therefore $K^S \leq \text{Hol}(S)$. On the other hand, since $S \in \mathcal{H}_0$, we have $\text{Sym}(S) = K^S \leq \text{Hol}(S)$, a contradiction. $\square$

From statement (i) of Lemma 3.1, it follows that the number of groups $H \leq G$ containing $\text{Soc}(G)$ is at most $\log n$, where n is the order of G ; in particular, $|\mathcal{H}_0| \leq \log n$. Moreover, for each H , the coherent configuration $\text{WL}(\mathcal{X}, \mathfrak{H})$ can be efficiently found by the WL-algorithm and condition (17) can be verified by checking at most $|\mathfrak{H}|^2 \leq n^2$ basis relations. Therefore, the set $\mathcal{H}_0$ can be found in time $\text{poly}(n)$. By statement (ii) of Lemma 7.2, this is enough to test efficiently whether or not K is of symmetric type, and if it so, then to find the minimal block $L = U$ of the group K (statement (i) of the same lemma).

Corollary 7.3. *Given a central Cayley scheme $\mathcal{X}$ over an almost simple group G of order n , one can test in time $\text{poly}(n)$ whether the group $\text{Aut}(\mathcal{X})$ is of symmetric type, and (if so) find the principal section of $\text{Aut}(\mathcal{X})$ within the same time.*

7.3. The case of normal type. In view of Corollary 7.3 and Proposition 6.1, one can efficiently test whether the automorphism group K of a central Cayley scheme $\mathcal{X}$ is of normal type. Denote by $\mathcal{H}_1$ the set of all groups H such that $\text{Soc}(G) \leq H \leq G$ and

$$H^* \times \text{id}_{G \setminus H} \leq K, \quad (19)$$

where the left-hand side denotes the subgroup of $\text{Sym}(G)$ that leaves each point of $G \setminus H$ fixed and coincides with H^* on H .

Lemma 7.4. *Suppose that the group K is of normal type and U/L is the principal K -section of G . Then $L = \text{Soc}(G)$, the set $\mathcal{H}_1$ is nonempty, and U is the smallest element of $\mathcal{H}_1$.*

Proof. Lemma 3.2 yields that $L = \text{Soc}(G)$. From Theorem 4.4, it is easily follows that $U \in \mathcal{H}_1$. Assume on the contrary that the group U is not the smallest in $\mathcal{H}_1$. Then there is a group $V \in \mathcal{H}_1$ such that $L \leq U \cap V < U$. Take a non-identity element $w \in U \cap V$ and denote by k_U (respectively, k_V) the permutation on G acting on U (respectively, V) by right multiplication by w and acting trivially outside U (respectively, V). Then $k_U, k_V \in K$, the permutation

$$k = k_U k_V^{-1}$$

is not identity on U , and $U^k = U$ and $k^{U \cap V} = \text{id}_{U \cap V}$. Clearly, k^U belongs to K^U , and hence to $D(2, U)$ because K is of normal type. However, as is easily seen, the identity element is the only element of $D(2, U)$ that leaves all points of $L \leq U \cap V$ fixed, a contradiction. $\square$

Again from statement (i) of Lemma 3.1 it follows that the number of groups H such that $\text{Soc}(G) \leq H \trianglelefteq G$ is at most $\log n$, and so is $|\mathcal{H}_1|$. For every H and each $k \in H^* \times \text{id}_{G \setminus H}$ one can efficiently test whether k is an automorphism of $\mathcal{X}$. Thus, Lemma 7.4 immediately implies the following statement.

Corollary 7.5. *Given a central Cayley scheme $\mathcal{X}$ over an almost simple group G of order n , one can test in time $\text{poly}(n)$ whether the group $\text{Aut}(\mathcal{X})$ is of normal type, and (if so) find the principal section of $\text{Aut}(\mathcal{X})$ within the same time.*

§8. A MAJORANT FOR THE COSET OF ISOMORPHISMS

Throughout this section, we assume that $\mathcal{X}$ is a central Cayley scheme over an almost simple group G and $K = \text{Aut}(\mathcal{X})$. The principal K -section of G and the associated partitions are denoted by U/L and $\mathfrak{U}$ and $\mathfrak{L}$, respectively. The equivalence relations corresponding to the partitions $\mathfrak{U}$ and $\mathfrak{L}$, are denoted by $e_{\mathfrak{U}}$ and $e_{\mathfrak{L}}$. Let φ be an algebraic isomorphism from $\mathcal{X}$ onto a Cayley scheme $\mathcal{X}'$ over an almost simple group G' . Assume that

$$\varphi(e_{\mathfrak{U}}) = e_{\mathfrak{U}'} \quad \text{and} \quad \varphi(e_{\mathfrak{L}}) = e_{\mathfrak{L}'}, \quad (20)$$

where in what follows, the group K' , the principal section U'/L' , the partitions $\mathfrak{U}'$ and $\mathfrak{L}'$, and the equivalence relations $e_{\mathfrak{U}'}$ and $e_{\mathfrak{L}'}$ are defined for the scheme $\mathcal{X}'$ in a similar way.

Lemma 8.1. *In the above notation, $|\mathfrak{U}| = |\mathfrak{U}'|$ and $|\mathfrak{L}| = |\mathfrak{L}'|$. Moreover, the groups K and K' either both of symmetric type, or both of normal type.*

Proof. The first statement follows from assumption (20). To prove the second one, we note that by Lemma 7.2 the group K is of symmetric type if and only if the scheme $\mathcal{X}$ is isomorphic to the wreath product $\mathcal{T}_U \wr \mathcal{Y}$, where $\mathcal{Y}$ is the quotient of $\mathcal{X}$ modulo the equivalence relation $e_{\mathfrak{L}}$. Since algebraic isomorphisms respect wreath products, we are done. $\square$

For all $Y \in \mathfrak{U}$ and $Y' \in \mathfrak{U}'$, the algebraic isomorphism φ induces an algebraic isomorphism

$$\varphi_{Y, Y'} : \mathcal{X}_Y \rightarrow \mathcal{X}'_{Y'},$$

that takes a relation s_Y to the relation $s'_{Y'}$ for all basis relations $s \subseteq e_{\mathfrak{U}}$ of the scheme $\mathcal{X}$, where $s' = \varphi(s)$. It follows that if $\mathcal{X}' = \mathcal{X}$ and φ is trivial, then $\varphi_{Y,Y}$ is trivial for all $Y \in \mathfrak{U}$.

For each $Y \in \mathfrak{U}$, set

$$D_Y = \begin{cases} \text{Sym}(Y) & \text{if } K \text{ is of symmetric type,} \\ D(2, U^Y) \cap \text{Aut}(\mathcal{X}_Y) & \text{otherwise,} \end{cases}$$

where, for brevity, U^Y denotes the restriction of the permutation group U_{right} to the set Y . Note that the form of the group D_Y does not depend on $Y \in \mathfrak{U}$, and D_Y contains K^Y for all Y (Theorems 6.2 and 6.3). Furthermore, if $Z \in \mathfrak{U}$, then any permutation of G^* taking Y to Z induces a permutation isomorphism from the group D_Y onto the group D_Z .

Lemma 8.2. $(D_Y)^f = D_{Y^f}$ for all $Y \in \mathfrak{U}$ and all $f \in \text{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$.

Proof. Without loss of generality, we may assume that both K and K' are of normal types (Lemma 8.1). Let $Y \in \mathfrak{U}$ and $f \in \text{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$. Then in view of (20),

$$\text{Aut}(\mathcal{X}_Y)^f = \text{Aut}(\mathcal{X}'_{Y'}), \quad (21)$$

where $Y' = Y^f$. Thus, it suffices to verify that $D(2, V)^f = D(2, V')$, where $V = U^Y$ and $V' = (U')^{Y'}$. However, by the definition of $\mathfrak{U}$, we have $V = Ug$ for suitable $g \in G$ and

$$D(2, V) = D(2, U^{g_r}),$$

where $g_r : U \rightarrow V$ is the bijection induced by right multiplication by g . A similar statement holds for V' , U' , and a suitable bijection $(g')_r$. Therefore, without loss of generality, we may assume that $Y = U$ and $Y' = U'$.

Recall that U is an almost simple group with $\text{Soc}(U) = L$, and also $U^* \leq K^U$. Therefore, $\text{Soc}(K^U) = L^*$. The same is true with K , U , and L , replaced by K' , U' , and L' , respectively. Taking into account that f takes K^U to $(K')^{U'}$, we conclude that

$$(L^*)^f = (L')^*.$$

This implies that f takes the normalizer of the group $L^* \leq \text{Sym}(U)$ to the normalizer of the group $(L')^* \leq \text{Sym}(U')$. However by Theorem 5.1, these normalizers are equal to $D(2, U)$ and $D(2, U')$. Thus, f takes the first of these groups to the second, and we are done. $\square$

Definition 8.3. Denote by $C_\varphi(\mathcal{X}, \mathcal{X}')$ the set of all bijections $f : G \rightarrow G'$ taking $\mathfrak{U}$ to $\mathfrak{U}'$ and satisfying the following conditions for every $Y \in \mathfrak{U}$:

$$f^Y \in \text{Iso}(\mathcal{X}_Y, \mathcal{X}'_{Yf}, \varphi_{Y, Yf}) \quad \text{and} \quad (D_Y)^f = D_{Yf}. \quad (22)$$

Let us find the explicit form of the set $C = C_\varphi(\mathcal{X}, \mathcal{X}')$ when $\mathcal{X} = \mathcal{X}'$ and $\varphi = \text{id}$. In this case, C is obviously a subgroup of $\text{Sym}(G)$ preserving the partition $\mathfrak{U}$. Condition (22) means that f^Y belongs to the intersection of $\text{Aut}(\mathcal{X}_Y)$ and the normalizer of D_Y in $\text{Sym}(Y)$ for all $f \in C_{\mathfrak{U}}$. This proves the first of the equalities

$$\prod_{Y \in \mathfrak{U}} D_Y = C_{\mathfrak{U}} \quad \text{and} \quad C^{\mathfrak{U}} = \text{Sym}(\mathfrak{U});$$

the second equality follows from the fact that any $g \in G$ induces the permutation isomorphism from D_Y onto D_{Yg} that induces $\varphi_{Y, Yg}$. Thus, the group C is permutation isomorphic to the wreath product $D_U \wr \text{Sym}(\mathfrak{U})$ (in imprimitive action). For arbitrary $\mathcal{X}'$ and φ , and for each $f \in C_\varphi(\mathcal{X}, \mathcal{X}')$, we obviously have

$$C_\varphi(\mathcal{X}, \mathcal{X}') = C_{\text{id}}(\mathcal{X}, \mathcal{X}')f. \quad (23)$$

Thus if the set $C_\varphi(\mathcal{X}, \mathcal{X}')$ is not empty, then it can be given by a generator set of the group $C = C_{\text{id}}(\mathcal{X}, \mathcal{X})$ and the bijection f . In the sense of the following statement, the set $C_\varphi(\mathcal{X}, \mathcal{X}')$ can be called a *majorant* of $\text{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$.

Theorem 8.4. $\text{Iso}(\mathcal{X}, \mathcal{X}', \varphi) \subseteq C_\varphi(\mathcal{X}, \mathcal{X}')$. Moreover, the set $C_\varphi(\mathcal{X}, \mathcal{X}')$ can be found in time $\text{poly}(n)$.

Proof. The first statement immediately follows from Lemma 8.2. To prove the second one, it suffices to find the set

$$C_0 = \{f_0 \in \text{Iso}_\psi(\mathcal{X}_U, \mathcal{X}'_{U'}) : (D_U)^{f_0} = D_{U'}\},$$

where $\psi = \varphi_{U, U'}$. Indeed, if this set is empty, then obviously so is the majorant $C_\varphi(\mathcal{X}, \mathcal{X}')$. On the other hand, if $f_0 \in C_0$, then to construct the majorant given by formula (23) it suffices to find D_U and the bijection f defined as follows:

$$f^Y = (g_Y)^{-1} f_0 g'_{Y'}, \quad Y \in \mathfrak{U},$$

where $Y \mapsto Y'$ is an arbitrary bijection from $\mathfrak{U}$ onto $\mathfrak{U}'$ taking U to U' , and the bijections $g_Y : U \rightarrow Y$ and $g'_{Y'} : U' \rightarrow Y'$ are induced by the right multiplications by the elements $g \in G$ and $g' \in G'$ such that $Y = Ug$ and $Y' = U'g'$.

To find the sets D_U and C_0 , assume first that K is of symmetric type (recall that this can efficiently be checked by Theorem 7.1). Then the coherent configurations $\mathcal{X}_U$ and $\mathcal{X}'_{U'}$ are trivial. Thus, $D_U = \text{Sym}(U)$ and for any bijection $f_0 : U \rightarrow U'$,

$$C_0 = \text{Sym}(U)f_0.$$

Let now K be of normal type. Then $D_U \leq D(2, U)$ and $D_{U'} \leq D(2, U')$. In particular, $D_U = D(2, U) \cap \text{Aut}(\mathcal{X}_U)$ can be found in time $\text{poly}(n)$. Furthermore, every element $f_0 \in C_0$ takes D_U to $D_{U'}$ (Lemma 8.2), and induces a permutation group isomorphism from U_{right} onto a group

$$V' \in \text{Reg}(D_{U'}, U').$$

By statement (ii) of Lemma 3.1, the set $\text{Reg}(D_{U'}, U')$ is of cardinality at most $|U'|^c \leq n^c$ for some constant $c > 0$, and all its elements can be found by exhaustive search of all 3-generated subgroups of the group $D_{U'}$. Since for a fixed V' , there are at most $|\text{Aut}(V')| \leq n^c$ distinct elements $f_0 \in C_0$ taking U_{right} to V' , one can test in time $\text{poly}(n)$, whether the set C_0 is not empty and (if so) find it in the form

$$C_0 = D_U f_0$$

with arbitrary $f_0 \in C_0$. □

§9. PROOF OF THEOREM 1.1

9.1. Reduction to Cayley schemes. Let Γ be a central Cayley graph over an almost simple group G , $\{e_i : i \in I\}$ the set of color classes of Γ , and $K = \text{Aut}(\Gamma)$. The principal K -section of G and the associated partitions are denoted by U/L and $\mathfrak{U}$ and $\mathfrak{L}$, respectively. Set

$$\mathcal{X} = \text{WL}(\Gamma, \{e_{\mathfrak{U}}, e_{\mathfrak{L}}\}),$$

where $e_{\mathfrak{U}}$ and $e_{\mathfrak{L}}$ are the equivalence relations corresponding to the partitions $\mathfrak{U}$ and $\mathfrak{L}$. For other central Cayley graphs Γ' , we use similar notation, e.g., G' and K' denote the underlying group and the automorphism group of Γ' , respectively.

Lemma 9.1. *Given central Cayley graphs Γ and Γ' over almost simple groups G and G' , respectively, one can construct in time $\text{poly}(n)$ the Cayley schemes $\mathcal{X}$ and $\mathcal{X}'$ over the same underlying groups and check whether there exists a (unique) algebraic isomorphism $\varphi : \mathcal{X} \rightarrow \mathcal{X}'$ such that*

$$\varphi(e_i) = e'_i \text{ for all } i \in I \quad \text{and} \quad \varphi(e_{\mathfrak{U}}) = e_{\mathfrak{U}'}, \quad \varphi(e_{\mathfrak{L}}) = e_{\mathfrak{L}'}, \quad (24)$$

and (if so) find φ within the same time. Moreover, $K = \text{Aut}(\mathcal{X})$, $K' = \text{Aut}(\mathcal{X}')$, and also

$$\text{Iso}(\Gamma, \Gamma') = \text{Iso}(\mathcal{X}, \mathcal{X}', \varphi). \quad (25)$$

Proof. By Theorem 7.1, the principal sections and hence the equivalence relations $e_{\mathcal{U}}$, $e_{\mathcal{L}}$ and $e_{\mathcal{U}'}$, $e_{\mathcal{L}'}$ can be found in time $\text{poly}(n)$. Therefore the first part of the statement immediately follows from Theorem 2.1. To prove the second one, we observe that every $f \in \text{Iso}(\Gamma, \Gamma')$ takes the group K to the group K' . By the definition of the minimal block (Subsection 4.2) this implies that f takes $e_{\mathcal{L}}$ to $e_{\mathcal{L}'}$ and hence takes $e_{\mathcal{U}}$ to $e_{\mathcal{U}'}$. Thus, the isomorphism f induces φ . This means that $f \in \text{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ and hence the left-hand side of (25) is contained in the right-hand side. Since the reverse inclusion is obvious, equality (25) is completely proved. Next, if $\Gamma' = \Gamma$, then $\varphi = \text{id}$ and equality (25) shows that $K = \text{Aut}(\mathcal{X})$. Similarly, $K' = \text{Aut}(\mathcal{X}')$. $\square$

9.2. Determining the coset of isomorphisms. Denote by π the canonical epimorphism from G onto $\overline{G} = G/L = \mathfrak{L}$. Then π induces a map taking the set $\mathcal{S}$ of basis relations of the Cayley scheme $\mathcal{X}$ over G to the set $\overline{\mathcal{S}}$ of basis relations of the quotient Cayley scheme $\overline{\mathcal{X}}$ over $\overline{G}$. In particular, π takes $\mathcal{S}^{\cup}$ to $\overline{\mathcal{S}}^{\cup}$. Set $\overline{\Gamma}$ to be the Cayley graph over $\overline{G}$ with color classes $\pi(e_i)$, $i \in I$. For any set C of the bijections $f : G \rightarrow G'$ taking $e_{\mathcal{U}}$ to $e_{\mathcal{U}'}$ and $e_{\mathcal{L}}$ to $e_{\mathcal{L}'}$, we denote by $\overline{C}$ the set of bijections $\overline{f} : \overline{G} \rightarrow \overline{G}'$ induced by $f \in C$.

Theorem 9.2. *Let Γ and Γ' be central Cayley graphs over almost simple groups G and G' , respectively. Assume that the algebraic isomorphism φ from Theorem 9.1 does exist. Then*

$$\text{Iso}(\Gamma, \Gamma') = \pi^{-1}(\overline{C} \cap B), \quad (26)$$

where $B = \text{Iso}(\overline{\Gamma}, \overline{\Gamma}')$, $C = C_{\varphi}(\mathcal{X}, \mathcal{X}')$, and the right-hand side consists of all $f \in C$ for which $\overline{f} \in B$.

Proof. To prove that the left-hand side of (26) is contained in the right-hand side, let $f \in \text{Iso}(\Gamma, \Gamma')$. Then the uniqueness of the principal sections implies that

$$(e_{\mathcal{U}})^f = e_{\mathcal{U}'} \quad \text{and} \quad (e_{\mathcal{L}})^f = e_{\mathcal{L}'}$$

Therefore, the isomorphism f induces the algebraic isomorphism φ . By Theorem 8.4, this implies that $f \in C$. Consequently, the induced bijection

$\bar{f} : \bar{G} \rightarrow \bar{G}'$ belongs to the set $\bar{C}$. Since obviously $\bar{f} \in B$, we conclude that f belongs to the right-hand side of (26), as required.

Conversely, let f belong to the right-hand side of (26). By formula (25) in Lemma 9.1, it suffices to verify that f induces φ . To this end, let $s \in \mathcal{S}$. Assume first that $s \subseteq e_{\mathfrak{U}}$. Then s equals the union of s_Y , $Y \in \mathfrak{U}$. Therefore since $f \in C$, conditions (22) are satisfied for all Y and hence

$$s^f = \left(\bigcup_{Y \in \mathfrak{U}} s_Y \right)^f = \bigcup_{Y \in \mathfrak{U}} (s_Y)^f = \bigcup_{Y \in \mathfrak{U}} \varphi_{Y,Yf}(s_Y) = \varphi(s).$$

Now assume that s is outside the equivalence relation $e_{\mathfrak{U}}$. Let us prove that

$$s = \bigcup_{\substack{X, Y \in \mathfrak{L}, \\ (X, Y) \in \bar{s}}} X \times Y \quad \text{and} \quad s^f = \bigcup_{\substack{X', Y' \in \mathfrak{L}', \\ (X', Y') \in \bar{s}'}} X' \times Y', \quad (27)$$

where $\bar{s} = \pi(s)$ and $\bar{s}' = \pi'(s^f)$. Since $(e_{\mathfrak{U}})^f = e_{\mathfrak{U}'}$, the relation s^f is outside the equivalence relation $e_{\mathfrak{U}'}$. Therefore, it suffices to verify the first equality of (27); denote the right-hand side of this equality by t . Clearly, $s \subseteq t$. Conversely, let $(X, Y) \in t$ for some $(X, Y) \in \bar{s}$. Since s is outside $e_{\mathfrak{U}}$, we conclude that $X \times Y$ is a basis relation of the coherent configuration $\text{Inv}(K_{\mathfrak{L}})$ (Theorem 4.4). Since $\text{Inv}(K_{\mathfrak{L}}) \geq \mathcal{X}$, it follows that this basis relation is contained in a basis relation of $\mathcal{X}$ which equals s , because $(X, Y) \in \bar{s}$. Therefore, $t \subseteq s$. This completes the proof of (27) implying $s = \pi^{-1}(\bar{s})$ and $s^f = (\pi')^{-1}(\bar{s}')$.

On the other hand, the graph isomorphism $\bar{f} \in B \cap \bar{C}$ induces an algebraic isomorphism $\bar{\varphi} : \bar{\mathcal{X}} \rightarrow \bar{\mathcal{X}'}$ that coincides with the restriction of the algebraic isomorphism φ modulo $e_{\mathfrak{L}}$. Thus,

$$\varphi(s) = \varphi(\pi^{-1}(\bar{s})) = (\pi')^{-1}(\bar{\varphi}(\bar{s})) = (\pi')^{-1}((\bar{s})^{\bar{f}}) = (\pi')^{-1}(\bar{s}') = s^f,$$

as required. $\square$

9.3. The algorithm. In the algorithm below, the input is given by two central Cayley graphs Γ and Γ' over almost simple groups G and G' , respectively. It is assumed that these groups are presented by the multiplication tables. The output consists of the set $\text{Iso}(\Gamma, \Gamma')$, which is either empty or equals the set $\text{Aut}(\Gamma)f$ for some $f \in \text{Iso}(\Gamma, \Gamma')$. Here, the group $\text{Aut}(\Gamma)$ is presented by a generating set.

Central Cayley graph isomorphism test

Step 1. Find the principal sections of the automorphism groups of the (central Cayley) schemes $\text{WL}(\Gamma)$ and $\text{WL}(\Gamma')$ (Theorem 7.1); denote by $\mathfrak{U}$, $\mathfrak{L}$ and $\mathfrak{U}'$, $\mathfrak{L}'$ the associated partitions of G and G' , respectively.

Step 2. Find the schemes $\mathcal{X} = \text{WL}(\Gamma, \{e_{\mathfrak{U}}, e_{\mathfrak{L}}\})$ and $\mathcal{X}' = \text{WL}(\Gamma', \{e_{\mathfrak{U}'}, e_{\mathfrak{L}'}\})$ and the algebraic isomorphism φ satisfying condition (24); if φ does not exist, output $\text{Iso}(\Gamma, \Gamma') = \emptyset$.

Step 3. Find the set $C = C_{\varphi}(\mathcal{X}, \mathcal{X}')$ (Theorem 8.4).

Step 4. Using the graph isomorphism and coset intersection algorithms from [1], find the set $B = \text{Iso}(\overline{\Gamma}, \overline{\Gamma}')$ and then the set $B' = B \cap \overline{C}$.

Step 5. Output $\text{Iso}(\Gamma, \Gamma') = \pi^{-1}(B')$. □

To complete the proof of Theorem 1.1, we show that the above algorithm correctly finds the set $\text{Iso}(\Gamma, \Gamma')$ in time $\text{poly}(n)$. Note that every graph isomorphism $f \in \text{Iso}(\Gamma, \Gamma')$ induces an algebraic isomorphism φ satisfying condition (24). Therefore, the output at Step 2 is correct. Thus, the correctness of the output at Step 5 and hence of the algorithm immediately follows from Theorem 9.2.

To estimate the running time, we note that all the steps except for Step 4 run in polynomial time (Theorem 7.1, Lemma 9.1, and Theorem 8.4). Furthermore, the graph isomorphism and coset intersection algorithms from [1] are applied at Step 4 to graphs with $m = |\mathfrak{L}|$ vertices and to the cosets contained in $\text{Sym}(m)$, respectively. Each of these algorithms runs in time at most $\exp((\log m)^c \sqrt{m})$. Since $m \leq \log n$, the complexity of this step does not exceed

$$\exp((\log m)^c \sqrt{m}) \leq \exp((\log \log n)^c (\log n)^{1/2}) \leq \exp(\log n) \leq n$$

for sufficiently large n and a suitable constant $c > 0$. Thus, the running time of the algorithm is polynomial in n , as required. □

REFERENCES

1. L. Babai, W. Kantor, E. M. Luks, *Computational complexity and the classification of finite simple groups*, — in: Proceedings of the 24th Ann. Symp. Found. Comput. Sci. (1983), 162–171.
2. J. Bray, J. Holt, D. Roney-Dougal, *The Maximal Subgroups of the Low-Dimensional Finite Classical Groups*, Cambridge University Press, Cambridge (2013).
3. P. J. Cameron, *Permutation Groups*, Cambridge University Press (1999).
4. J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *An ATLAS of Finite Groups*, Oxford University Press, Oxford (1985).

5. F. Dalla Volta, A. Lucchini, *Generation of almost simple groups*, — J. Algebra, **178**, No. 1 (1995), 194–223.
6. S. Evdokimov, I. Ponomarenko, *Recognizing and isomorphism testing circulant graphs in polynomial time*, — Algebra Analiz, **15**, No. 6 (2003), 1–34.
7. S. Evdokimov, I. Ponomarenko, *Permutation group approach to association schemes*, — Eur. J. Combin., **30** (2009), 1456–1476.
8. S. Evdokimov, I. Ponomarenko, *Schurity of S -rings over a cyclic group and generalized wreath product of permutation groups*, — Algebra Analiz, **24**, No. 3 (2012), 84–127.
9. A. Ganesan, *Automorphism group of the complete transposition graph*, — J. Algebr. Combin., **42**, No. 3 (2015), 793–801.
10. C. H. Li, *On isomorphisms of finite Cayley graphs – a survey*, — Discrete Math., **256** (2002), 301–334.
11. M. W. Liebeck, Ch. E. Praeger, J. Saxl, *Regular subgroups of primitive permutation groups*, — Memoirs Amer. Math. Soc., **203**, No. 952 (2010), 1–88.
12. E. M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, — J. Comp. Sys. Sci., **25** (1982), 42–65.
13. M. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, — Proc. London Math. Soc., **88** (2004), 1–41.
14. I. Ponomarenko, *Bases of Schurian antisymmetric coherent configurations and isomorphism test for Schurian tournaments*, — J. Math. Sci., **192**, No. 3 (2013), 316–338.
15. B. Weisfeiler (editor), *On Construction and Identification of Graphs*, Lecture Notes Math., **558** (1976).
16. H. Wielandt, *Finite Permutation Groups*, Academic press, New York-London (1964).
17. H. Wielandt, *Permutation Groups Through Invariant Relations and Invariant Functions*, Lect. Notes Dept. Math. Ohio St. Univ., Columbus (1969).

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

Поступило 10 апреля 2017 г.

Sobolev Institute of Mathematics,
Novosibirsk, Russia
Novosibirsk State University,
Novosibirsk, Russia
E-mail: `vasand@math.nsc.ru`