Isomorphism of Coloured Graphs with Slowly Increasing Multiplicity of Jordan Blocks

Sergei Evdokimov [*] **Ilia Ponomarenko** [†]

April, 1995

Abstract

We show that the isomorphism test for n-vertex edge coloured graphs with the multiplicity of Jordan blocks bounded by k can be done in time $(e^{k^2}n)^{O(1)}$.

[*] St.Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia, 199178 St.Petersburg and University of Bonn, 53117 Bonn. E Mail: evdokim@iias.spb.su. Research supported by the Volkswagen-Stiftung Program on Computational Complexity.

[†] St.Petersburg Department of Mathematical Institute of the Academy of Sciences of Russia, 191011 St.Petersburg and University of Bonn, 53117 Bonn. E Mail: ponom-ko@pdmi.ras.ru. Research supported by the Volkswagen-Stiftung Program on Computational Complexity.

1 Introduction

The Graph Isomorphism Problem (ISO) is to recognize whether two given graphs are isomorphic, i.e., whether there is a bijection between their vertex sets preserving the adjacences of edges. The computation complexity status of the ISO is unknown at present and the best general isomorphism test for n-vertex graphs runs in time $n^{O(\sqrt{n})}$ (see [BKL]). It is well-known that the ISO is polynomial-time equivalent to the problem of finding the automorphism group $\mathrm{Aut}(\Gamma)$ of a graph Γ consisting of all isomorphisms from Γ to itself.

The failure in the attempts to find a polynomial-time algorithm for the ISO in the class of all graphs led to the investigation of the problem in some special classes of them. There is a great variety of such results, we mention only some of them. There exist polynomial-time algorithms for graphs with bounded degree [L] and for graphs with bounded eigenvalue multiplicity [BGM]. We also mention a $n^{O(\log n)}$-algorithm for tournaments (directed graphs with exactly one arc between any two distinct vertices) [BL].

Below under a coloured graph we mean an ordered triple $\Gamma = (V, E, c)$ where V is a finite vertex set, $E \subset V \times V$ is an edge set and c is a colouring function on E. For each color i denote by $A_i = A_i(\Gamma)$ the adjacency matrix of the relation $E_i = c^{-1}(i)$. As usual the automorphism group $\mathrm{Aut}(\Gamma)$ of Γ is by definition the group of all permutations of V preserving each color.

One of the oldest approaches to the ISO is due to Weisfeiler and Lehman (see [W]). With each coloured graph Γ it associates an algebra $W(\Gamma)$ (called the cellular algebra of Γ) which is the smallest matrix algebra over $\mathbf{C}$ containing the adjacency matrices $A_i(\Gamma)$, the identity matrix and the matrix whose all the entries are equal to 1, and closed under the Hermitian conjugation and the Hadamard (componentwise) multiplication. They showed that $W(\Gamma)$ is a semisimple algebra over $\mathbf{C}$ and $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(W(\Gamma))$ where the latter group consists by definition of all permutation matrices commuting with all matrices of $W(\Gamma)$. Given a coloured graph Γ the cellular algebra $W(\Gamma)$ can be constructed in polynomial time. This observation reduces the ISO to the problem of constructing the group $\mathrm{Aut}(W)$ where W is a cellular algebra. Throughout the paper we deal exceptionally with this problem.

In [BGM] a $n^{O(k)}$-isomorphism test for the class of all undirected n-vertex graphs with eigenvalue multiplicity bounded by k was described. The question arises: whether the upper bound can be improved by pulling k out of the exponent. Set

$$m(\Gamma) = \min_i m(A_i)$$

where $m(A_i)$ is the maximum multiplicity of a Jordan block of the matrix $A_i = A_i(\Gamma)$. Clearly, $m(\Gamma)$ can be found in polynomial time. We prove the following result.

Theorem 1. *In the class of all coloured n-vertex graphs Γ with $m(\Gamma) \leq k$ a canonical labeling and the automorphism group of Γ can be found in time*

$$f(k)\, n^{O(1)}, \qquad f(k) = k^k J(k)^{2\log_2 k},$$

where $J(k)$ is Jordan's function. (For the strict definition of Jordan's function see the end of section 3.)

Remark. Since $J(k) = k^{O(k^2/\log^2 k)}$ (see [CR]), the running time of our algorithm is bounded by $(e^{k^2} n)^{O(1)}$. In other words the algorithm is polynomial not only for small k but also for $k = O(\sqrt{\log n})$.

As a corollary we give the following answer to the above question.

Theorem 2. *The isomorphism test for n-vertex graphs with eigenvalue multiplicity bounded by k can be done in time $f(k)\, n^{O(1)}$ where $f(k)$ is as above.*

We prove Theorem 1 by reducing it to a theorem for cellular algebras. Let Γ be a graph satisfying the hypothesis of Theorem 1. The cellular algebra $W(\Gamma)$ is a semisimple algebra over $\mathbf{C}$. So the standard matrix representation of $W(\Gamma)$ is a sum of irreducible representations of it. A straightforward checking shows that the multiplicity of each of them is at most k. Thus Theorem 1 follows from the following statement.

Theorem 3 (MAIN THEOREM). *In the class of all cellular algebras W on n points with irreducible representation multiplicity bounded by k a canonical labeling and the automorphism group of W can be found in time $f(k)\, n^{O(1)}$ where $f(k)$ is defined in Theorem 1.*

Remark. It follows from [E] that the class of cellular algebras described above is recognizable in time $n^{O(1)}$.

The proof of the MAIN THEOREM for a primitive W is given in section 4. To reduce the general case to the primitive one we use for cellular algebras an interpretation of the standard permutation group technique. To get the required upper bound we need to control the groups arising throughout the algorithm. To do this we observe that the maximum degree of an irreducible representation of the group $\mathrm{Aut}(W)$ in its standard permutation representation is bounded by k. This implies that $[G : \mathrm{sol}(G)] \leq J(k)^{\log_2 k}$ for each transitive constituent G of $\mathrm{Aut}(W)$ where $\mathrm{sol}(G)$ is the solvable radical of G and $J(k)$ is Jordan's function (see [EP]). Thus the problem is reduced to permutation group computation with solvable groups.

The paper consists of five sections. Section 2 contains the definition of a cellular algebra and related concepts as well as the basic notations used along the paper. It also contains statements concerning algebraic properties of cellular algebras. In section 3 we prove a proposition concerning the computation of a canonical labeling and the automorphism group of a cellular algebra with respect to the permutation group of a special kind. The case of a primitive cellular algebra is treated in section 4. In section 5 we completely prove the MAIN THEOREM and deduce Theorem 1 from it.

Notations. As usual by $\mathbf{C}$ we denote the field of all complex numbers. If L is a linear space over $\mathbf{C}$, then the set of all linear operators on L is denoted by $\mathrm{End}(L)$.

If G is a group, then $H \leq G$ means that H is a subgroup of G. The index of H in G is denoted by $[G : H]$. If $S_i \subset G$, $i = 1, \ldots, l$, we use notation $< S_1, \ldots, S_l >$ for the subgroup of G generated by all S_i.

Troughout the paper V denotes a finite set with $n = |V|$ elements. The group of all permutations of V is denoted by $\mathrm{Sym}(V)$. By relations on V me mean subsets of $V \times V$. If R is a relation on V, then for $g \in \mathrm{Sym}(V)$

$$R^g = \{(u^g, v^g)|\ (u, v) \in R\}.$$

If E is an equivalence (i.e. reflexive, symmetric and transitive relation) on V, then V/E denotes the set of all equivalence classes modulo E.

For a positive integer l by $[1, l]$ we denote the set $\{1, \ldots, l\}$.

2 Cellular algebras and their representations

Denote by L_V a linear space over $\mathbf{C}$ with the set V as a base. For any subset $U \subset V$ the linear space L_U can naturally be viewed as a subspace of L_V (spanned by U). If E is an equivalence on V, then there is a natural linear injection

$$i_E : L_{V/E} \to L_V, \quad U \mapsto \sum_{v \in U} v \quad (U \in V/E).$$

Thus $L_{V/E}$ is isomorphic to a subspace of L_V. Below we identify L_U and $L_{V/E}$ with the above subspaces of L_V.

Let $\mathrm{Mat}_V = \mathrm{Mat}_V(\mathbf{C})$ be the algebra of all complex $n \times n$ matrices whose rows and columns are indexed by the elements of V. By a *cellular algebra* W on V we mean a subalgebra of Mat_V containing the identity matrix I_V, the matrix J_V whose all the entries are equal to 1, and closed under the Hermitian conjugation and the Hadamard (componentwise) multiplication denoted by $\circ$ below. The algebra Mat_V naturally acts on the linear space L_V. The restriction of this action to W defines a faithful linear representation

$$\Delta^W_{\mathrm{stand}} : W \to \mathrm{End}(L_V)$$

called the *standard representation* of W. It is completely reducible over $\mathbf{C}$ due to the fact that W is a semisimple algebra (see [W]).

Since W is closed under the Hadamard multiplication, it has a uniquely determined linear space basis $\mathcal{R} = \mathcal{R}(W)$ consisting of $\{0,1\}$-matrices such that

$$\sum_{R\in\mathcal{R}} R = J_V \qquad \text{and} \qquad R \in \mathcal{R} \Leftrightarrow R^T \in \mathcal{R}$$

where R^T is the transpose of R. This basis is called the *standard basis* of W. We write $W = (V, \mathcal{R})$ to emphasize that W is given by V and $\mathcal{R}$. The $\{0,1\}$-matrices belonging to $\mathcal{R}$ and their sums can be viewed as adjacency matrices of some relations on V. For convenience's sake we identify the matrices with the corresponding relations.

It follows from $I_V \in W$ that there exists a uniquely determined decomposition $I_V = \sum_{i=1}^{s} I_{V_i}$ with $I_{V_i} \in \mathcal{R}$ for some $V_i \subset V$. Thus

$$V = \bigcup_{i=1}^{s} V_i \qquad \text{(disjoint partition).}$$

Any such V_i is called a *cell* of W. The set of all of them is denoted by $\mathrm{Cel}(W)$. For each $R \in \mathcal{R}$ there exist uniquely determined integers $i, j \in [1, s]$ (depending on R) such that $R \subset V_i \times V_j$. It is well-known (see [W]) that the number of 1's in the uth row (resp. vth column) of the matrix R does not depend on $u \in V_i$ (resp. $v \in V_j$). This number is denoted by $d_{\mathrm{out}}(R)$ (resp. $d_{\mathrm{in}}(R)$).

Let W be a cellular algebra on V with $|\,\mathrm{Cel}(W)| = 1$. We say that W is *primitive* if the only equivalences belonging to W are I_V and J_V. Otherwise, W is called *imprimitive.* Up to the language this definition coincides with that of [W].

The set of all cellular algebras on V is ordered by inclusion. The algebra Mat_V is obviously the greatest element of the set. We write $W \le W'$ if W is a subalgebra of W'. If $A_1, \ldots, A_m \in \mathrm{Mat}_V$, then the intersection of all cellular algebras on V containing W and all the matrices A_i is also a cellular algebra on V. It is denoted by $W[A_1, \ldots, A_m]$. It is known (see [W]) that the standard basis of this algebra can be constructed in polynomial time from W and $A_1, \ldots, A_m$.

The natural action of $\mathrm{Sym}(V)$ on V induces actions of this group on the algebra Mat_V and the linear space L_V. Clearly, the actions respect the algebraic operations on Mat_V and L_V and

$$(Ax)^g = A^g x^g, \qquad A \in \mathrm{Mat}_V,\ x \in L_V.$$

Two cellular algebras W_1 and W_2 on V are called *isomorphic* ($W_1 \cong W_2$), if $W_1^g = W_2$ as sets for some permutation $g \in \mathrm{Sym}(V)$ (called an *isomorphism* from W_1 to W_2).

Clearly, g induces a bijection between the sets of the basis relations of W_1 and W_2. For a cellular algebra W on V we set

$$\mathrm{Aut}(W) = \{g \in \mathrm{Sym}(V) |\ A^g = A \ \text{ for all } \ A \in W\}.$$

This group is called the *automorphism group* of W.

Let U be a union of cells of W. The subalgebra $I_U W I_U \subset W$ invariantly acts on the subspace $L_U = I_U L_V \subset L_V$. So it can be viewed as a subalgebra of Mat_U. Clearly, it is closed under the Hermitian conjugation and the Hadamard multiplication and contains I_U and J_U. Thus it is a cellular algebra on U called the *restriction* of W to U and denoted by W_U.

Let $E \in W$ be an equivalence on V. The subalgebra $QWQ \subset W$ with $Q = \sum_{U \in V/E} J_U/|U|$ invariantly acts on the subspace $L_{V/E} = QL_V \subset L_V$. So it can be viewed as a subalgebra of $\mathrm{Mat}_{V/E}$. Denote it by W/E. Clearly, W/E contains $I_{V/E}$, $J_{V/E}$ and is closed under the Hermitian conjugation. For two basis relations $R, S \in \mathcal{R}$ we write $R \overset{E}{\sim} S$ if S enters the decomposition of QRQ in the standard basis of W (we make use of the fact that $Q \in W$). It easily follows that $\overset{E}{\sim}$ is an equivalence relation on $\mathcal{R}$. If $QRQ = \sum_{S \in \mathcal{R}} c_S^R S$, then clearly, the set $\{S \in \mathcal{R} |\ c_S^R \neq 0\}$ coincides with the equivalence class containing R and $c_S^R = c_R^R$ does not depend on S with $c_S^R \neq 0$. So if $QR_1Q \circ QR_2Q \neq 0$ for $R_1, R_2 \in \mathcal{R}$, then $QR_1Q = (c_{R_1}^{R_1}/c_{R_2}^{R_2})QR_2Q$. It follows that the algebra W/E is closed under the Hadamard multiplication. Thus W/E is a cellular algebra on V/E called the *cellular factoralgebra* of W modulo E. Clearly, given W and E the standard basis of W/E can be constructed in polynomial time.

Remark. When each equivalence class modulo E is contained in a cell of W the notion of cellular factoralgebra was introduced in [W]. Our definition coincides with that of [W] in this case and can be viewed as its generalization.

The following statement is straightforward from definitions.

Lemma 2.1 *Let W be a cellular algebra on V, U be a union of cells of W and $E \in W$ be an equivalence on V. Then the representation $\Delta_{\mathrm{stand}}^{W_U}$ (resp. $\Delta_{\mathrm{stand}}^{W/E}$) is equivalent to the representation*

$$\Delta_Q : QWQ \to \mathrm{End}(QL_V), \quad Q = I_U \ \ (\textit{resp. } Q = \sum_{U \in V/E} J_U/|U|)$$

induced by $\Delta_{\mathrm{stand}}^W$.■

Let $\Delta : W \to \mathrm{End}(L)$ be a representation of a semisimple algebra W over $\mathbf{C}$ on a linear space L. Denote by $\mathrm{Spec}\,(W)$ the set of all primitive central idempotents of the algebra W. For each $P \in \mathrm{Spec}\,(W)$ the restriction of Δ to the subspace $PL \subset L$ is a multiple of an irreducible representation of W. Denote its multiplicity by $m(P,\Delta)$ and set

$$m(\Delta)=\max_{P\in\mathrm{Spec}\,(W)} m(P,\Delta).$$

If W is a cellular algebra, set

$$m(P,W)=m(P,\Delta^W_{\mathrm{stand}}),\quad m(W)=m(\Delta^W_{\mathrm{stand}})$$

where $\Delta^W_{\mathrm{stand}}$ is the standard representation of W. We call $m(W)$ the *multiplicity* of W.

Proposition 2.2 *Let W be a cellular algebra on a set V. Then*

(1) if $W'\geq W$, then $m(W')\leq m(W)$;

(2) if U is a union of cells of W, then $m(W_U)\leq m(W)$;

(3) if $E\in W$ is an equivalence on V, then $m(W/E)\leq m(W)$.

Proof. Since $\Delta^W_{\mathrm{stand}}$ is equivalent to the restriction of $\Delta^{W'}_{\mathrm{stand}}$ to W, statement (1) is clear. Statements (2) and (3) follow by Lemma 2.1 from the following lemma.

Lemma 2.3 *Let $\Delta: W\to \mathrm{End}(L)$ be a linear representation of a semisimple algebra W over $\boldsymbol{C}$, Q be an idempotent of W and $\Delta_Q: QWQ\to\mathrm{End}(QL)$ be the representation of the algebra QWQ induced by Δ. Then $m(\Delta_Q)\leq m(\Delta)$. Moreover, if $P\in\mathrm{Spec}\,(W)$, then the following statement holds: either $PQ=0$, or $PQ\in\mathrm{Spec}\,(QWQ)$ and*

$$m(PQ,\Delta_Q)=m(P,\Delta).$$

Each element of $\mathrm{Spec}\,(QWQ)$ is uniquely written in the form PQ with $P\in\mathrm{Spec}\,(W)$.

Proof. Let $P\in\mathrm{Spec}\,(W)$ and $PQ\neq 0$. Since the idempotent P is primitive, the algebra PW is simple, isomorphic to $\mathrm{End}(\mathbf{C}^r)$ for some positive integer r. Then it follows from $PQ\neq 0$ that the image of PQ with respect to the above isomorphism is a non-trivial idempotent T of $\mathrm{End}(\mathbf{C}^r)$. So $PQWQ$ is isomorphic to $\mathrm{End}(T\mathbf{C}^r)$. Thus $PQ\in\mathrm{Spec}\,(QWQ)$ and $m(PQ,\Delta_Q)=m(P,\Delta)$. It follows that if $1=\sum_{P\in\mathrm{Spec}\,(W)}P$ is the decomposition of unity of W, then $Q=\sum_{P,PQ\neq 0}PQ$ is the decomposition of unity of QWQ and

$$m(\Delta_Q)=\max_{P,PQ\neq 0} m(PQ,\Delta_Q)\leq\max_P m(P,\Delta)=m(\Delta).\blacksquare$$

3 Canonical labeling of a cellular algebra

Below by a cellular algebra on V we mean one with a linear order on the set of its basis relations. By isomorphisms of such algebras we mean those preserving orders of their basis relations. We say that cellular algebras W_1 and W_2 on V are equal ($W_1 = W_2$), if the identity map of V is an isomorphism from one to the other. It should be noted that the order on the set $\mathcal{R}(W)$ of the basis relations of a cellular algebra W induces a natural linear order on the set of all relations of W. If $E \in W$ is an equivalence on V (resp. U is a union of cells of W), then it also induces a linear order on the set $\mathcal{R}(W/E)$ (resp. $\mathcal{R}(W_U)$). For $W = (V, \mathcal{R})$ and $g \in \mathrm{Sym}(V)$ we define $W^g = (V, \mathcal{R}^g)$ as a cellular algebra on V with the standard basis

$$\mathcal{R}^g = \{R^g \mid R \in \mathcal{R}\}$$

and the linear order induced by that of W. Clearly, $g : W \to W^g$ is a cellular algebra isomorphism.

Given a cellular algebra W on V and $A \in \mathrm{Mat}_V$, we put in order the set of the basis relations of the algebra $W[A]$ according to Weisfeiler-Lehman's canonical algorithm, so that the following holds (see [W], Ch.M):

(W-L) if $g \in \mathrm{Sym}(V)$ is an isomorphism from W to W' and $A^g = A'$, then g is also an isomorphism from $W[A]$ to $W'[A']$.

The standard basis of $W[A]$ (with the order) can be constructed in polynomial time from W and A.

Let $G \leq \mathrm{Sym}(V)$. We say that cellular algebras W_1 and W_2 are *G-isomorphic* ($W_1 \cong_G W_2$), if there exists $h \in G$ such that $W_1^h = W_2$. Let $g \in \mathrm{Sym}(V)$ and $\mathcal{W}$ be a class of cellular algebras on V closed under $< g, G >$-isomorphisms. Following [BL] we define for $\mathcal{W}$ the notion of *canonical labeling* with respect to the coset gG.

A map $\mathrm{CF} : \mathcal{W} \to \mathcal{W}$ is called canonical with respect to the coset gG if the following conditions hold:

(C1) $\forall W \in \mathcal{W} : \quad \mathrm{CF}(W) \cong_G W^g$;

(C2) $\forall W_1, W_2 \in \mathcal{W} : \quad W_1^g \cong_G W_2^g \Leftrightarrow \mathrm{CF}(W_1) = \mathrm{CF}(W_2)$.

It follows that for any $W \in \mathcal{W}$ there exists $h = h(W) \in gG$ such that $\mathrm{CF}(W) = W^h$. Any such h is called a *canonical labeling* of the algebra W with respect to the coset gG.

The algebra $\mathrm{CF}(W)$ is called the *canonical form* of W with respect to gG. We do not refer to gG if $G = \mathrm{Sym}(V)$.

Let G be a finite group. Denote by $\mathrm{sol}(G)$ the maximal normal solvable subgroup of G. Clearly, if $G = G_1 \times G_2$, then $[G : \mathrm{sol}(G)] = [G_1 : \mathrm{sol}(G_1)] \cdot [G_2 : \mathrm{sol}(G_2)]$, and if H is a subgroup of or a homomorphic image of G, then $[H : \mathrm{sol}(H)] \leq [G : \mathrm{sol}(G)]$.

Proposition 3.1 *Let $\mathcal{W}$ be a class of cellular algebras on a linearly ordered set V, closed under $< g, G >$-isomorphisms where $G \leq \mathrm{Sym}(V)$ and $g \in \mathrm{Sym}(V)$. Assume that for some positive integer t the group G satisfies the following condition:*

(*) if H is a transitive constituent of G, then $[H : \mathrm{sol}(H)] \leq t$

Then the group $\mathrm{Aut}(W^g) \cap G$ and a canonical labeling of $W \in \mathcal{W}$ with respect to gG can be found in time $t^2 n^{O(1)}$.

Proof. Let the basis relations of W be labeled by the elements of $[1, l]$. We associate with W the map $s = s(W) : V \times V \to [1, l]$ where $s(u, v)$ is the label of the basis relation of W^g containing (u, v) (such maps will be called strings on $V \times V$). Following [BL] we reduce the canonization problem for $\mathcal{W}$ with respect to gG to that one for the class $\mathcal{S}_{\mathcal{W}} = \{s(W) | \, W \in \mathcal{W}\}$ of strings on $V \times V$ with respect to the group $G' \leq \mathrm{Sym}(V \times V)$ coinciding with the natural action of G on $V \times V$. The problem includes finding a canonical labeling of a string s as well as constructing the subgroup $A(s, G')$ of G' preserving equal labels. It should be noted that if U_1 and U_2 are orbits of G then $U_1 \times U_2$ is a G'-invariant set. Thus if H' is a transitive constituent of G', then H' is a homomorphic image of a subgroup of the group $H_1 \times H_2$ where H_1 and H_2 are some transitive constituents of G. Now by (*) we conclude that $[H' : \mathrm{sol}(H')] \leq t^2$.

Following [BL] the canonization problem for strings of $\mathcal{S}_{\mathcal{W}}$ can in polynomial time be reduced to the case of a transitive group G'. In this case the above argument shows that $[G' : \mathrm{sol}(G')] \leq t^2$.

Let G' be transitive. Construct the group $H = \mathrm{sol}(G')$ and a decomposition

$$G' = \bigcup_{j=1}^{r} g_j H$$

of G' into a disjoint union of cosets. By [KL] it can be done in time $n^{O(1)}$. Apply the algorithm of [BL] to find for a string $s \in \mathcal{S}_{\mathcal{W}}$ the group $A(s, H)$, a canonical labeling h with respect to H and a canonical labeling h_j with respect to the coset $g_j H$ for all j. Set $T = \{j = 1, \ldots, r \mid s^{h_j} = s^h\}$. Clearly, $h_j h^{-1} \in A(s, G')$ for all $j \in T$. Conversely,

$g' \in A(s,G')$ implies $g' \in A(s,G') \cap g_j H$ for some j. Then s^{g_j} is H-isomorphic to s and so $j \in T$. Moreover, $hh_j^{-1}g' \in A(s,H)$. Thus

$$A(s,G') =< A(s,H),\ \{h_j h^{-1}\}_{j\in T} > .$$

Let $W^{h_{j_0}} = \min_{j\in[1,r]} W^{h_j}$ according to the lexicographic order on the set of all strings. Take h_{j_0} as a canonical labeling of s with respect to G'.

The canonicity of the algorithm follows from that of [BL]. Since H is a solvable group, finding h, h_j and $A(s,H)$ can be done in time $n^{O(1)}$. Besides, by condition (*) $r \le t^2$. Thus $A(s,G')$ can be constructed in time $(t^2 n)^{O(1)}$.■

We will use Proposition 3.1 for $G = \mathrm{Aut}(W)$ where W is a cellular algebra with $m(W) \le k$. In this case the multiplicities of irreducible representations of W in its standard representation coincide with the degrees of irreducible representations of the subalgebra of Mat_V centralizing W (see [We]). This implies that the degree of each irreducible representation of the group G entering its standard permutation representation is bounded by k. So the hypothesis of Proposition 3.1 is satisfied for $t = J(k)^{\log_2 k}$ by the following result.

Theorem 3.2.([EP]) *Let G be a transitive permutation group. If the degree of each irreducible representation of G in its permutation representation is at most k, then*

$$[G : \mathrm{sol}(G)] \le J(k)^{\log_2 k}$$

where $J(k)$ is Jordan's function.■

Remark. Jordan's function is defined as follows: for a positive integer k

$$J(k) = \sup_G \min_{A\subset G} [G : A]$$

where G runs over all finite groups G having a faithful linear representation over $\mathbf{C}$ of degree k and A runs over all normal Abelian subgroups of G. By Jordan's theorem $J(k) < +\infty$ for all k (see [CR]).

4 The case of a primitive cellular algebra

Here we prove Theorem 3 for primitive cellular algebras. Throughout the section the algebra $W[I_{\{v_1\}},\ldots,I_{\{v_l\}}]$ with $v_1,\ldots,v_l \in V$ is denoted by $W_{v_1,\ldots,v_l}$. We also assume that V is a linearly ordered set.

Denote by $\mathcal{W}_{\mathrm{prim}}$ the class of all primitive cellular algebras on V. For $W \in \mathcal{W}_{\mathrm{prim}}$ set

$$\delta = \delta(W) = \min_{R\in\mathcal{R}(W)\setminus I_V} d_{\mathrm{out}}(R), \qquad \mu = \mu(W) = \min_{P\in\mathrm{Spec}(W)\setminus\frac{1}{n}J_V} m(P).$$

where $m(P) = m(P,W)$ (see section 2). If $|V| = 1$, we set $\delta(W) = \mu(W) = 1$.

Theorem 4.1 *For the class $\mathcal{W}_{\rm prim}$ the following two statements hold:*

(1) if $W \in \mathcal{W}_{\rm prim}$, then $|\operatorname{Aut}(W)| \le \delta^{\mu-1}n$;

(2) for $W \in \mathcal{W}_{\rm prim}$ a canonical labeling of W and all the elements of the group $\operatorname{Aut}(W)$ can be found in time $\delta^{\mu-1}n^{O(1)}$.

Proof. Theorem's statements are trivial for $n = 1$. So we assume $n > 1$. We start by the description of the algorithm.

Input: $W \in \mathcal{W}_{\rm prim}$, $|V| > 1$.

Output: a canonical labeling of W and the list of all the elements of $\operatorname{Aut}(W)$.

Step 1. Find the minimal basis relation $R \in \mathcal{R}(W) \setminus I_V$ such that $d_{\rm out}(R) = \delta(W)$.

Step 2. Construct a set S consisting of all tuples $(v_1, \dots, v_l) \in V^l, l = 1, 2, \dots$ such that:

(i) $(v_i, v_{i+1}) \in R$ for $i \in [1, l-1]$;

(ii) $\{v_{i+1}\} \notin \operatorname{Cel}(W_{v_1,\dots,v_i})$ for $i \in [1, l-1]$;

(iii) $W_{v_1,\dots,v_l} = \operatorname{Mat}_V$.

Step 3. For each $s = (v_1, \dots, v_l) \in S$ find the ordering of $\mathcal{R}(W_{v_1,\dots,v_l})$ applying (W-L) canonical algorithm. Denote by $\varphi_s : V \to [1, n]$ the bijection respecting the corresponding linear order on the basis relations $I_{\{v\}}$ of the algebra $W_s = W_{v_1,\dots,v_l}$.

Step 4. Let $W^{\varphi_{s_0}}$ be lexicographically minimal among all W^{φ_s} with $s \in S$. Set

$$S_0 = \{s \in S |\ W^{\varphi_s} = W^{\varphi_{s_0}}\}, \qquad G = \{\varphi_s\varphi_{s_0}^{-1} |\ s \in S_0\}.$$

Let $h \in \operatorname{Sym}(V)$ be such that the h-image of the ith element of V with respect to the original order on V equals $\varphi_{s_0}^{-1}(i)$.

Step 5. Output G as $\operatorname{Aut}(W)$ and h as a canonical labeling of W.

Let us prove the correctness of the above algorithm. It follows from the primitivity of W that the graph (V, R) is strongly connected (see [W]). Thus $S \ne \emptyset$. Besides, it is clear from Step 4 that $G \le \operatorname{Aut}(W)$. Let $g \in \operatorname{Aut}(W)$. Then from the definition of S at Step 2 and (W-L) we conclude that $s = s_0^g \in S$. Moreover, it follows from (W-L) that $g : W_{s_0} \to W_s$ is an isomorphism. So $g\varphi_{s_0} = \varphi_s$ by the definition of φ_s at Step 3. Therefore, $s \in S_0$ and $g \in G$. Thus $G = \operatorname{Aut}(W)$.

Let us prove that h is a canonical labeling. If $g : W \to W'$ is an isomorphism, then $S^g = S'$ and $\varphi_s = g\varphi_{s^g}$. Thus, $\{W^{\varphi_s}\}_{s\in S} = \{W'^{\varphi_{s'}}\}_{s'\in S'}$ and $\mathrm{CF}(W) = \mathrm{CF}(W')$.

To prove the required upper bound and the inequality it suffices to prove that $(v_1, \ldots, v_l) \in S$ implies $l \le \mu$. Then $|S| \le n\delta^{\mu-1}$ (see (i) at Step 2) and we are done. We start by two lemmas.

Lemma 4.2 *Let W be a cellular algebra on V. For $A \in \mathrm{Mat}_V$ set*

$$\mathrm{Eq}(A) = \{(u, v) \in V \times V |\ Au = Av \ne 0\}.$$

Then $A \in W$ implies $\mathrm{Eq}(A) \in W$.

Proof. Since

$$\mathrm{Eq}\Big(\sum_{R\in\mathcal{R}(W)} \alpha(R)R\Big) = \sum_{U\in\mathrm{Cel}(W)} \mathrm{Eq}\Big(\sum_{R\subset V\times U} \alpha(R)R\Big) = \sum_{U\in\mathrm{Cel}(W)} \bigcap_{\alpha\ne 0} \mathrm{Eq}\Big(\sum_{R\subset V\times U,\alpha(R)=\alpha} R\Big),$$

it suffices to prove Lemma for a nonzero $A = \sum_R R$ where R runs over a subset of the set $\mathcal{R}_U(W) = \{R \in \mathcal{R}(W)|\ R \subset V \times U\}$ for some $U \in \mathrm{Cel}(W)$. Then for such an A

$$A^T A = d_{\mathrm{in}}(A)\,\mathrm{Eq}(A) + B,$$

where $d_{\mathrm{in}}(A) = \sum_R d_{\mathrm{in}}(R)$ and $B = (B_{u,v}) \in \mathrm{Mat}_V$ with $0 \le B_{u,v} < d_{\mathrm{in}}(A)$ for all $u, v \in V$ and $B \circ \mathrm{Eq}(A) = 0$. It follows that $\mathrm{Eq}(A) \in W$.■

Lemma 4.3 *Let W be a cellular algebra on V and $A \in W$ with* $\mathrm{Eq}(A) = I_V$. *Then $Av \in \sum_{i=1}^h Wv_i$ implies $\{v\} \in \mathrm{Cel}(W_{v_1,\ldots,v_h})$ where $v, v_1, \ldots, v_h \in V$. Besides, $Av \ne 0$ for all $v \in V$.*

Proof. The second statement follows from the definition of $\mathrm{Eq}(A)$. Let $B \in \mathrm{Mat}_V$ be defined by

$$Bu = \begin{cases} Av, & \text{if } u \in \{v_1, \ldots, v_h\}; \\ Au, & \text{otherwise.} \end{cases}$$

It is easy to see that $B \in W_{v_1,\ldots,v_h}$. By Lemma 4.2 $\mathrm{Eq}(B) \in W_{v_1,\ldots,v_h}$. From $\mathrm{Eq}(A) = I_V$ it follows that the equivalence class modulo $\mathrm{Eq}(B)$ containing v_1 coincides with the set $\{v_1, \ldots, v_h, v\}$. Denote by U the cell of $W_{v_1,\ldots,v_h}$ containing v. Then $\{v_1\} \times U \in \mathcal{R}(W_{v_1,\ldots,v_h})$. Thus $U \subset \{v_1, \ldots, v_h, v\}$, whence $U = \{v\}$.■

Now we are ready to complete the proof of Theorem 4.1. Let $(v_1, \ldots, v_l) \in S$. Denote by P a primitive central idempotent of W with $m(P) = \mu$ different from $\frac{1}{n}J_V$. It follows from the primitivity of W and Lemma 4.2 that $\mathrm{Eq}(P) = I_V$. Set

$$L_h = \sum_{i=1}^{h} WPv_i, \qquad h \in [0, l].$$

Then L_h is a W-module and

$$\{0\} = L_0 \subset L_1 \subset \cdots \subset L_l \subset PL_V.$$

Now Lemma 4.3 with $A = P$ and condition (ii) of the definition of S imply $L_{i-1} \neq L_i$ for all $i \in [1, l]$. It follows that $l \leq m(P)$, whence $l \leq \mu$.∎

To apply Theorem 4.1 in section 5 we need the following statement.

Lemma 4.4 *If W is a primitive cellular algebra on V, then*

$$\delta(W) \leq m(W), \qquad \mu(W) \leq m(W)$$

where $m(W) = \max\limits_{P \in \mathrm{Spec}\,(W)} m(P)$ is the multiplicity of W (see section 2).

Proof. First of all we recall that

$$\dim_{\mathbf{C}}(W) = \sum_{R \in \mathcal{R}(W)} d_{\mathrm{out}}(R) = \sum_{P \in \mathrm{Spec}\,(W)} n(P)^2$$

where $n(P)$ is the degree of an irreducible representation of the algebra W corresponding to the idempotent P. For $n = 1$ Lemma is clear. If $n \geq 2$, then

$$\delta(W)(\dim_{\mathbf{C}}(W) - 1) \leq \sum_{R \in \mathcal{R}(W) \setminus I_V} d_{\mathrm{out}}(R) = n - 1 =$$

$$= \sum_{P \in \mathrm{Spec}\,(W)} m(P)n(P) - 1 = 1 + \sum_{P \in \mathrm{Spec}\,(W) \setminus \frac{1}{n}J_V} m(P)n(P) - 1 \leq$$

$$\leq m(W) \sum_{P \in \mathrm{Spec}\,(W) \setminus \frac{1}{n}J_V} n(P)^2 = m(W)(\dim_{\mathbf{C}}(W) - 1).$$

(We made use of the fact that $m(P) = n(P) = 1$ for $P = \frac{1}{n}J_V$.) Thus, $\delta(W) \leq m(W)$. The second inequality is trivial.∎

5 Proofs of Theorems

In this section we prove Theorem 3 and deduce Theorem 1 from it. The set V is assumed to be linearly ordered.

Proof of Theorem 3. We start by describing the corresponding procedure.

Input: a cellular algebra W on V.

Output: the group $\mathrm{Aut}(W)$ and a canonical labeling of W.

Step 1. Let W have at least two cells, $\mathrm{Cel}(W) = \{V_1, \ldots, V_s\}$, $s > 1$. Following [BL] reduce the canonization problem with respect to $\mathrm{Sym}(V)$ to that one with respect to $\prod_{i=1}^{s} \mathrm{Sym}(V_i)$. Apply the algorithm recursively to the cellular algebra W_{V_i} to find its canonical labeling $g_i \in \mathrm{Sym}(V_i)$ and the group $\mathrm{Aut}(W_{V_i})$, $i \in [1, s]$. Set

$$G = \prod_{i=1}^{s} \mathrm{Aut}(W_{V_i}^{g_i}), \quad g = (g_1, \ldots, g_s) \in \prod_{i=1}^{s} \mathrm{Sym}(V_i).$$

Applying the algorithm of Proposition 3.1 find the group $\mathrm{Aut}(W^g) = \mathrm{Aut}(W^g) \cap G$ and a canonical labeling h of the algebra W with respect to the coset gG. Output $\mathrm{Aut}(W)$ and h as a canonical labeling of W.

Step 2. Let $|\,\mathrm{Cel}(W)| = 1$ and W be imprimitive. Perform steps 2.1 – 2.4.

Step 2.1. Find the minimal equivalence $E \in W$ (with respect to the order on the relations of W defined above) such that $\widetilde{W} = W/E$ is primitive. The set V/E is ordered according to the lexicographic order on 2^V induced by the linear order on V. Recursively find a canonical labeling of the algebra $\widetilde{W}$ and the group $\mathrm{Aut}(\widetilde{W})$. Put in order the set V/E according to this labeling, so that $V/E = \{U_1, \ldots, U_r\}$.

Step 2.2. For each $i \in [1, r]$ construct the cellular algebra

$$W_i = W[I_{U_i}]_{U_i}.$$

Apply the algorithm recursively to the algebra W_i to find its canonical labeling g_i and the group $\mathrm{Aut}(W_i)$, $i \in [1, r]$. By analogy with Step 1 reduce the canonization problem with respect to $\mathrm{Sym}(V)$ to that one with respect to its maximal subgroup G fixing E. (Below we identify V with $U \times [1, r]$ where U is an "etalon" copy of an equivalence class modulo E so that U_i is identified with $U \times \{i\}$. The group G is identified with the wreath product of $\mathrm{Sym}(U)$ and $\mathrm{Sym}([1, r])$ so that the action of $g \in G$ on V is given by

$$(u, i)^g = (u^{g_i}, i^h), \quad u \in U,\ i \in [1, r]$$

where $g = (g_1, \ldots, g_r; h)$ with $g_i \in \mathrm{Sym}(U)$, $h \in \mathrm{Sym}([1, r])$. According to above W_i (resp. $\widetilde{W}$) can naturally be viewed as a cellular algebra on U (resp. on $[1, r]$)).

Step 2.3. Set

$$W^{(h)} = W[I_{U_{1^h}}, \ldots, I_{U_{r^h}}], \quad h \in \mathrm{Aut}(\widetilde{W}).$$

(We successively add the relations $I_{U_{1^h}}, \ldots, I_{U_{r^h}}$ to W applying at each stage Weisfeiler-Lehman's canonical algorithm). Set

$$G^{(h)} = \prod_{i=1}^{r} \mathrm{Aut}(W_{i^h}^{g_{i^h}}), \quad g^{(h)} = (g_1, \ldots, g_r; h^{-1}) \in G.$$

Applying the algorithm of Proposition 3.1 find $\mathrm{Aut}(W^{(h)}) = \mathrm{Aut}(W^{(h)}) \cap g^{(h)}G^{(h)}g^{(h)^{-1}}$ and a canonical labeling of the algebra $W^{(h)}$ with respect to the coset $g^{(h)}G^{(h)}$.

Step 2.4. Let h_0 be a permutation for which the canonical form of $W^{(h_0)}$ is minimal among the canonical forms of $W^{(h)}$, $h \in \mathrm{Aut}(\widetilde{W})$. (Though h_0 is not uniquely determined, the output of Step 2.4 is.) For each h using the canonical labeling of $W^{(h)}$, find (if it exists) an isomorphism $W^{(h_0)} \to W^{(h)}$. Denote by S the set of all these permutations of V. Output the group $< \mathrm{Aut}(W^{(h_0)}), S >$ as $\mathrm{Aut}(W)$ and the canonical labeling of $W^{(h_0)}$ with respect to $g^{(h_0)}G^{(h_0)}$ as a canonical labeling of W.

Step 3. Let W be a primitive cellular algebra. Apply the algorithm from section 4 to find $\mathrm{Aut}(W)$ and a canonical labeling of W.■

We prove the correctness of the procedure applying the induction on the number l of its recursive calls. If $l = 0$, then the procedure terminates at Step 3 and the correctness follows from Theorem 4.1 and Lemma 4.4. If $l > 0$ we consider two cases according to the Step (1 or 2) at which the procedure terminates.

Let the procedure terminate at Step 1 and W be isomorphic to W' with respect to $\prod_{i=1}^{s} \mathrm{Sym}(V_i)$. It follows that W_{V_i} is isomorphic to W'_{V_i} for all i. By the induction hypothesis $W_{V_i}^{g_i} = {W'_{V_i}}^{g'_i}$. So W^g and $W'^{g'}$ are G-isomorphic. Thus the correctness follows from that of the algorithm of Proposition 3.1.

Let the procedure terminate at Step 2. First we prove the canonicity of the labeling of the algebra W defined at Step 2.4. Let g be a G-isomorphism from W to W' (the group G is defined at Step 2.2). Since $E^g = E$, g induces an isomorphism $\tilde{g} \in \mathrm{Sym}([1,r])$ from $\widetilde{W}$ to $\widetilde{W}'$. According to Step 2.1 $\widetilde{W}$ and $\widetilde{W}'$ coincide with their canonical forms. So $\widetilde{W} = \widetilde{W}'$ and $\tilde{g} \in \mathrm{Aut}(\widetilde{W})$. By (W-L) g is also an isomorphism from $W^{(h)}$ to $W'^{(h')}$ for all $h \in \mathrm{Aut}(\widetilde{W})$ where $h' = h\tilde{g}$. Set

$$c^{(h)} = g^{(h)^{-1}} g\, g'^{(h')}.$$

It follows from the definitions that $c^{(h)} \in \prod_{i=1}^{r} \mathrm{Sym}(U_i)$, i.e. $c^{(h)} = (c_1, \ldots, c_r; 1)$ where $c_i \in \mathrm{Sym}(U)$. By (W-L) c_i is an isomorphism from $W_{i^h}^{g_{i^h}}$ to ${W'_{i^{h'}}}^{g'_{i^{h'}}}$ (see Step 2.3). So $W_{i^h}^{g_{i^h}} = {W'_{i^{h'}}}^{g'_{i^{h'}}}$ and $c_i \in \mathrm{Aut}(W_{i^h}^{g_{i^h}})$ for all i, whence $c^{(h)} \in G^{(h)}$. Thus by Proposition 3.1 the canonical form of $W^{(h)}$ with respect to $g^{(h)}G^{(h)}$ coincides with that of $W'^{(h')}$ with respect to $g'^{(h')}G'^{(h')}$. If h runs over $\mathrm{Aut}(\widetilde{W})$, then h' also runs over $\mathrm{Aut}(\widetilde{W})$. Therefore, the corresponding canonical forms of $W^{(h_0)}$ and $W'^{(h'_0)}$ coincide. So do the canonical forms of W and W' defined at Step 2.4.

Now we prove that the group obtained at Step 2.4 coincides with $\mathrm{Aut}(W)$. Let $g \in \mathrm{Aut}(W)$. Denote by $\tilde{g}$ the permutation of V/E induced by g. By (W-L) g is an isomorphism from $W^{(h_0)}$ to $W^{(h_0\tilde{g})}$. So g is of the form $g = g_1g_2$ where $g_1 \in \mathrm{Aut}(W^{(h_0)})$ and $g_2 \in S$. Thus $g \in < \mathrm{Aut}(W^{(h_0)}), S >$. The inverse inclusion is obvious.

Let us estimate the running time $t(W)$ of the procedure applied to a cellular algebra W on n points with $m(W) \leq k$. Denote by $t(k,n)$ the maximum of $t(W)$ taken over all such W. We will prove by induction on n that $t(k,n) = k^k J(k)^{2\log_2 k} n^{O(1)}$. If the procedure terminates at Step 3, then it follows from Theorem 4.1 and Lemma 4.4 that for some constant c_1

$$t(W) \leq k^k n^{c_1}. \tag{1}$$

Let the procedure terminate at Step 1. By Proposition 2.2 $m(W_{V_i}) \leq m(W) \leq k$ for all $i \in [1,s]$. So $\mathrm{Aut}(W_{V_i})$ and the canonical labeling g_i of W_{V_i} can be found in time $t(k,|V_i|)$. By Theorem 3.2 $[H : \mathrm{sol}(H)] \leq J(k)^{\log_2 k}$ for each transitive constituent H of $\mathrm{Aut}(W_{V_i})$. So by Proposition 3.1 the group $\mathrm{Aut}(W)$ and the canonical labeling of W with respect to gG can be found in time $J(k)^{2\log_2 k} n^{c_2}$ for some constant c_2. Therefore

$$t(W) \leq \sum_{i=1}^{s} t(k,|V_i|) + J(k)^{2\log_2 k} n^{c_2} + n^{O(1)}. \tag{2}$$

Let the procedure terminate at Step 2. By Proposition 2.2 $m(\widetilde{W}) \leq m(W) \leq k$ and $m(W_i) \leq m(W) \leq k$ for all $i \in [1,r]$. So the group $\mathrm{Aut}(W_i)$ and the canonical labeling $\underset{\sim}{g_i}$ of W_i can be found in time $t(k,n/r)$. The group $\mathrm{Aut}(\widetilde{W})$ and the canonical labeling of $\widetilde{W}$ can be found in time $k^k r^{c_1}$ due to Theorem 4.1 and Lemma 4.4. By Proposition 3.1 and Theorem 3.2 the group $\mathrm{Aut}(W^{(h)})$ and the canonical labeling of $W^{(h)}$ for $h \in \mathrm{Aut}(\widetilde{W})$ can be found in time $J(k)^{2\log_2 k} n^{c_2}$ where c_2 is as above. Besides, $|\mathrm{Aut}(\widetilde{W})| \leq k^k r$ by Theorem 4.1 and Lemma 4.4. Therefore,

$$t(W) \leq k^k r^{c_1} + r\, t(k,n/r) + k^k r \cdot J(k)^{2\log_2 k} n^{c_2} + n^{O(1)}. \tag{3}$$

It follows from (1), (2), (3) by induction that there exists a constant c for which

$$t(k,n) \leq k^k J(k)^{2\log_2 k} n^c.$$

Theorem 3 is completely proved.■

Proof of Theorem 1. Denote by $W(\Gamma)$ the cellular algebra generated by all the matrices A_i. Then $m(W(\Gamma)) \leq m(A_i)$ for all i. Thus by the hypothesis of the theorem

$$m(W(\Gamma)) \leq \min_i m(A_i) = m(\Gamma) \leq k.$$

Now Theorem 1 follows from Theorem 3, since $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(W(\Gamma))$ (see [W]).■

References

[BGM] Babai, L., Grigoriev, D.Y., Mount, D.M, *Isomorphism of graphs with bounded eigenvalue multiplicity*, Proc. 14th ACM STOC, (1982), 310-324.

[BKL] Babai, L., Kantor, W.M., Luks, E.M., *Computation complexity and the classification of finite simple groups*, Proc. 24th FOCS, (1983), 162-171.

[BL] Babai, L., Luks, E.M., *Canonical labeling of graphs*, Proc. 15th ACM STOC, (1983), 1-15.

[CR] Curtis, C.W., Reiner, I., *Representation theory of finite groups and associative algebras*, 1962.

[E] Eberly, W., *Decomposition of algebras over* **R** *and* **C**, Computational Complexity, 1 (1991), 211-234.

[EP] Evdokimov, S.A., Ponomarenko, I.N., *Transitive groups with irreducible representations of bounded degree* , to appear in Zapiski Nauch. Semin. POMI, 1995.

[L] Luks, E.M., *Isomorphism of graphs of bounded valence can be tested in polynomial time*, J. Comp. Sys. Sci., v.25, (1982), 42-65.

[KL] Kantor, W.M., Luks, E.M., *Computing in quotient groups*, Proc. 22nd ACM STOC, (1990), 524-534.

[W] Weisfeiler, B. (editor), *On the construction and identification of graphs*, Lect. Notes Math., v.558, 1976.

[We] Weyl, H., *Classical groups. Their invariants and representations*, 1939.