PDMI PREPRINT 03/2003

Recognizing and isomorphism testing circulant graphs in polynomial time

Sergei Evdokimov
St. Petersburg Institute
for Informatics and Automation RAS
evdokim@pdmi.ras.ru *

Ilia Ponomarenko
Steklov Institute of Mathematics
at St. Petersburg
inp@pdmi.ras.ru †

16.05.2003

Abstract

We recognize the circulant graphs and find canonical labeling for them in polynomial time. The algorithm also includes finding a cycle base of an arbitrary solvable permutation group. The correctness of the algorithm is based on a new result on the structure of Schur rings over a finite cyclic group.

*Partially supported by RFFI, grants 01-01-00219, 03-01-00349
†Partially supported by RFFI, grants, 01-01-00219, 02-01-00093, 03-01-00349 NSH-2251.2003.1

1 Introduction

A finite graph[1] is called *circulant* if its automorphism group contains a full cycle, i.e. a permutation the cycle decomposition of which consists of a unique cycle of full length. This means that the graph admits a regular cyclic automorphism group and consequently it is isomorphic to a Cayley graph over a cyclic group. In particular, any circulant graph can be given in a compact form by a full cycle automorphism and the neighbourhood of one of its vertices.

One of the main computational problems concerning circulant graphs is that of finding an efficient algorithm to recognize them. (This problem is a special case of the following NP-complete problem: test whether a given graph has a fixed point free automorphism [15]). The first attempt to solve the problem was undertaken in [24] where a polynomial-time algorithm for recognizing circulant tournaments was described. Since then several results on recognizing some special classes of circulant graphs have appeared [21, 22, 5] but up to now the general problem has been open. In this paper we present a full solution to it. Another problem about circulant graphs is to find an efficient isomorphism test for them. In fact this problem is polynomial-time reducible to the recognition problem because two circulant graphs with the same number of vertices are isomorphic if and only if their disjoint union is a circulant graph. In this paper we present a solution to a more difficult problem of finding a canonical labeling of a circulant graph. It should be mentioned that the isomorphism problem for Cayley graphs over a cyclic group (which is a special case of the isomorphism problem for circulant graphs) has been extensively studied for the last fourty years (see [20]). Most papers were concentrated on finding efficient necessary and sufficient conditions for graphs over various special classes of cyclic groups.

The key notion of our approach is a *cycle base* of a finite permutation group G which is by definition a subset of G consisting of full cycles such that any full cycle of G is conjugate in G to exactly one element of this set. Cycle bases were studied in [19] where it was proved that the cardinality of any cycle base of the group G is at most n (and even $\varphi(n)$ with φ the Euler function assuming the classification of finite simple groups) where n is the degree of G. Let us define a cycle base of a graph Γ as a cycle base of its automorphism group $\mathrm{Aut}(\Gamma)$. As it will be seen below (Theorem 1.2) the problems treated in this paper are efficiently reduced to the problem of finding a cycle base of a graph. The latter in its turn is reduced (see the proof of Theorem 1.1) to a similar problem for cellular rings the solution to which occupies most of the paper (as for cellular rings see Subsection 8.1).

Theorem 1.1 *A cycle base of a graph on n vertices can be found in time $n^{O(1)}$.*

Proof. Let Γ be a graph on n vertices. Denote by W the smallest cellular ring containing the adjacency matrix of the graph Γ. Then it is easy to see that $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(W)$ (see e.g. [27]). From Theorem 7.1 it follows that a cycle base of the ring W (i.e. of the group $\mathrm{Aut}(W)$) can be found in time $n^{O(1)}$. Since the ring W can be efficiently constructed from Γ (see Theorem 8.3), we are done.■

The following statement contains the main results of the paper.

[1]By a graph one can mean an ordinary graph, a digraph or even an edge colored graph.

Theorem 1.2 *Let $\mathcal{G}_n$ (resp. $\mathcal{C}_n$) be the class of all graphs (resp. circulant graphs) with n vertices. Then the following problems can be solved in time $n^{O(1)}$:*

(1) *given $\Gamma \in \mathcal{G}_n$, test whether $\Gamma \in \mathcal{C}_n$, and (if it is so) find a full cycle automorphism of Γ,*

(2) *given $\Gamma \in \mathcal{C}_n$, find a canonical labeling of Γ,*

(3) *given $\Gamma, \Gamma' \in \mathcal{C}_n$, test whether $\Gamma \cong \Gamma'$, and (if it is so) find an isomorphism from Γ onto Γ',*

(4) *given $\Gamma \in \mathcal{G}_n$, find a full system of pairwise nonequivalent Cayley representations[2] of Γ over a cyclic group of order n.*

Proof. Obviously a graph is circulant if and only if every cycle base of it is nonempty. So Problem (1) can be solved in time $n^{O(1)}$ by Theorem 1.1. Furthermore, Problem (3) is $O(n)$-reducible to Problem (2). Let us concentrate on Problems (2) and (4).

Let V be a set of cardinality n. Given a full cycle c on V and $v \in V$, there exists a uniquely determined bijection $f : V \to \{0, \dots, n-1\}$ taking v^{c^i} to i (then c goes to the cycle $(0, \dots, n-1)$). If Γ is a graph on V and $c \in \mathrm{Aut}(\Gamma)$, then obviously the image Γ^f of the graph Γ under f does not depend on the choice of $v \in V$. Denote it by $\Gamma^{(c)}$. Then it is easy to see that given full cycle automorphisms c_1 and c_2 of Γ, we have

$$\Gamma^{(c_1)} = \Gamma^{(c_2)} \ \Leftrightarrow \ c_1 \sim c_2 \tag{1}$$

where $c_1 \sim c_2$ means that c_1 and c_2 are conjugate in the group $\mathrm{Aut}(\Gamma)$. Thus the set $\mathcal{C}(\Gamma) = \{\Gamma^{(c)} : c \in C\}$ does not depend on the choice of a cycle base C of Γ. By Theorem 1.1 this set together with a set of isomorphisms $f : \Gamma \to \Gamma'$, $\Gamma' \in \mathcal{C}(\Gamma)$ (one f for each Γ'), can be found in time $n^{O(1)}$.

Now let $\Gamma \in \mathcal{C}_n$. Then $\mathcal{C}(\Gamma) \neq \emptyset$. Moreover, from the above paragraph it follows that the element Γ' of $\mathcal{C}(\Gamma)$ the adjacency matrix of which is the lexicographical leader among the adjacency matrices of the graphs belonging to $\mathcal{C}(\Gamma)$ as well as the corresponding isomorphism f can be found in time $n^{O(1)}$. The labeling f of Γ is canonical (in the class $\mathcal{C}_n$) because obviously

$$\Gamma_1 \cong \Gamma_2 \ \Leftrightarrow \ \Gamma_1^{(f_1)} = \Gamma_2^{(f_2)}$$

for all $\Gamma_1, \Gamma_2 \in \mathcal{C}_n$ where f_i is the labeling of Γ_i $(i = 1, 2)$. Thus Problem (2) can be solved in time $n^{O(1)}$.

Finally, let $\Gamma \in \mathcal{G}_n$. Let us treat the set $\{0, \dots, n-1\}$ of the vertices of the graphs from $\mathcal{C}(\Gamma)$ as the additive group $\mathbb{Z}_n^+$ of the ring $\mathbb{Z}_n = \mathbb{Z}/(n)$. Then it is easily seen that each graph from $\mathcal{C}(\Gamma)$ is a Cayley representation of Γ over this group. From (1) it follows that every Cayley representation of Γ over $\mathbb{Z}_n^+$ is equivalent to at least one element of $\mathcal{C}(\Gamma)$. On the other hand, two elements of $\mathcal{C}(\Gamma)$ are equivalent if and only if there exists an isomorphism from one to the other induced by an element of the multiplicative group of the ring $\mathbb{Z}_n$. Since the set $\mathcal{C}(\Gamma)$ can be found in time $n^{O(1)}$, this implies that Problem (4) can be solved within the same time.■

[2]By a Cayley representation of a graph Γ over a group G we mean a Cayley graph over G isomorphic to Γ; two such representations are called equivalent if some isomorphism of the corresponding Cayley graphs belong to $\mathrm{Aut}(G)$ (see e.g. [14]).

As we saw in the proof of Theorem 1.1 the problem of finding a cycle base of a graph is reduced to the problem of finding a cycle base of a cellular ring (i.e. that of its automorphism group). To approach the latter problem we introduce the classes of *quasinormal* and *singular* cellular rings (Sections 3 and 4) and prove that each Cayley ring over a cyclic group belongs to one of these classes (Theorem 5.1). We also show that both of the classes are efficiently recognizable. Moreover, the automorphism group of a quasinormal ring has a polynomial-time computable solvable subgroup containing all full cycle automorphisms (Theorem 3.6), whereas a singular ring has a polynomial-time computable *admissible* extension (Theorem 4.4). (An extension of a cellular ring is called admissible if it is proper and every of its cycle bases contains a cycle base of the ring). One can imagine a quasinormal ring as one covered in a sense by normal Cayley rings over cyclic groups (Definition 3.2). The latters were defined and studied in [11]; in fact any such ring is the centralizer ring of a 2-closed subgroup of the holomorph of a cyclic group. On the other hand, each singular ring contains a special subfactor of rank 2 (Definition 4.1); every automorphism of this subfactor can be lifted to an automorphism of the entire ring (Lemma 4.3). When passing to the corresponding admissible extension, we regularize the subfactor and thereby resolve the singularity. Now the algorithm of finding a cycle base of a cellular ring (Main Algorithm) can be described by means of the following scheme (for details see Section 7).

(1) While a current ring is singular, replace it by an admissible extension.

(2) If a current ring is not quasinormal, then a cycle base of the input ring is empty.

(3) Find a solvable subgroup G of the automorphism group of a current ring that contains all full cycle automorphisms.

(4) Find a cycle base of G and reduce it to a cycle base of the input ring.

Step 1 is performed by Algorithm A2 (Section 4) using, in particular, the Weisfeiler-Leman algorithm (Subsection 8.3). Next, Steps 2 and 3 are performed by Algorithm A1 (Section 3). At the first stage of it we test whether or not the current ring is quasinormal, and if it is, we find a solvable group containing all full cycle automorphisms of the current ring. At the second stage we apply the Babai-Luks algorithm to find the group G as the intersection of the latter group and the automorphism group of the current ring. Finally, Step 4 is performed by Algorithm A3 (Section 6). This algorithm efficiently finds a cycle base of an arbitrary solvable permutation group. The correctness of the Main Algorithm follows from Theorem 5.1 based on deep results on the structure of Schur rings over a cyclic group [11, 13].

All undefined terms and results concerning permutation groups can be found in [28, 29, 4]. To make the paper self-contained we cite the background on cellular rings and Schur rings in Section 8. This section also contains some remarks on algorithms for them and for permutation groups.

Notation. As usual by $\mathbb{Z}$ we denote the ring of integers.

Throughout the paper V denotes a finite set. For a (binary) relation R on V we set

$$R^T = \{(u,v) \in V^2 :\ (v,u) \in R\}, \quad \text{and} \quad R(u) = \{v \in V :\ (u,v) \in R\}$$

where $u \in V$.

By an equivalence on V we always mean an ordinary equivalence relation on V and denote by $\mathcal{E}(V)$ the set of all of them. If $E \in \mathcal{E}(V)$, then the set of classes of E is denoted by V/E, and for $X \subset V$ we set $X/E = X/(E \cap X^2)$. If E equals $\Delta(V) = \{(v,v) :\ v \in V\}$, then the set X/E is identified with X.

If R is a relation on V, $X \subset V$ and $E \in \mathcal{E}(V)$, then we set

$$R_{X/E} = \{(Y,Z) \in (X/E)^2 :\ (Y \times Z) \cap R \neq \emptyset\}$$

and treat this set as a relation on X/E.

The ring of all integral matrices whose rows and columns are indexed by the elements of V is denoted by Mat_V, its identity matrix by I_V and the all-one matrix by J_V.

The adjacency matrix of a relation R on V is denoted by $A(R)$; this is a $\{0,1\}$-matrix of Mat_V such that its (u,v)-entry equals 1 iff $(u,v) \in R$.

The group of all permutations of V is denoted by $\mathrm{Sym}(V)$. For $S \subset \mathrm{Sym}(V)$ we denote by $\mathrm{Cyc}(S)$ the set of all full cycles on V belonging to S, and set $\mathrm{Cyc}(V) = \mathrm{Cyc}(\mathrm{Sym}(V))$.

Each bijection $f : V \to V'$ $(v \mapsto v^f)$ naturally defines a bijection $R \mapsto R^f$ from the relations on V onto the relations on V', a ring isomorphism $A \mapsto A^f$ from Mat_V onto $\mathrm{Mat}_{V'}$ and a group isomorphism $g \mapsto g^f$ from $\mathrm{Sym}(V)$ onto $\mathrm{Sym}(V')$. For $X \subset V$ and $E \in \mathcal{E}(V)$ the bijection f induces a bijection $f_{X/E} : X/E \to X'/E'$ where $X' = X^f$ and $E' = E^f$.

For a group G the permutation group on the set G defined by the left (resp. right) multiplications is denoted by G_{left} (resp. G_{right}).

For integers l, m the set $\{l, l+1, \ldots, m\}$ is denoted by $[l,m]$. We write $[m]$ instead of $[1,m]$.

2 Equivalences in homogeneous cellular rings

This section is a preliminary one. Its contents will be used throughout the paper. The relations we deal here with are assumed to have full support (i.e. $R(v) \cup R^T(v) \neq \emptyset$ for all $v \in V$). Below we fix a homogeneous celular ring $W \leq \mathrm{Mat}_V$ and set $\mathcal{R} = \mathcal{R}(W)$, $\mathcal{R}^* = \mathcal{R}^*(W)$, $\mathcal{E} = \mathcal{E}(W)$ and $\mathcal{B} = \mathcal{B}(W)$ (see Subsection 8.1).

2.1. Let R be a relation on V. Denote by $\langle R \rangle$ the smallest equivalence on V containing R and call it the *equivalence closure* of R:

$$\langle R \rangle = \bigcap_{E \in \mathcal{E}(V), E \supset R} E.$$

It is easily seen that the classes of $\langle R \rangle$ are exactly the connected components of the graph on V with the edge set $R \cup R^T$ and so $\langle R \rangle$ can be efficiently constructed. If $E_1, E_2 \in \mathcal{E}(V)$, then obviously $\langle E_1 \cup E_2 \rangle$ is the smallest equivalence on V the classes of which are unions of classes of E_1 as well as classes of E_2. A routine check shows that if $R \in \mathcal{R}^*$, then $\langle R \rangle \in \mathcal{E}$. This implies that every $E \in \mathcal{E} \setminus \{\Delta(V)\}$ is of the form $E = \langle E_1 \cup R \rangle$ where E_1 is a maximal element of the set $\{E' \in \mathcal{E} :\ E' \subset E,\ E' \neq E\}$ and $R \in \mathcal{R}$. Therefore, the elements of the set $\mathcal{E}$ can be listed in polynomial time in $|V|$ and $|\mathcal{E}|$.

Let R be a relation on V. It is easily seen that the set of all equivalences $E \in \mathcal{E}(V)$ such that

$$R = \bigcup_{(X,Y)\in R_{V/E}} X \times Y \tag{2}$$

is closed with respect to taking the equivalence closure of a union. So this set has the largest element. We call it the *radical* of R and denote by $\mathrm{rad}(R)$. Obviously, $\mathrm{rad}(R) \subset \langle R \rangle$. Furthemore,

$$\mathrm{rad}(R) = \mathrm{Eq}(R) \cap \mathrm{Eq}(R^T) \tag{3}$$

where for a relation S on V we set $\mathrm{Eq}(S) = \{(u,v) \in V^2 : \ S(u) = S(v)\}$. Indeed, from the definitions it follows that $\mathrm{rad}(R) \subset \mathrm{Eq}(R) \cap \mathrm{Eq}(R^T)$. On the other hand, it is easy to show that the equivalence $E = \mathrm{Eq}(R) \cap \mathrm{Eq}(R^T)$ satisfies (2). Equality (3) implies that $\mathrm{rad}(R)$ can be found in polynomial time in $|V|$. Now, if $R \in \mathcal{R}^*$, then $\mathrm{Eq}(R), \mathrm{Eq}(R^T) \in \mathcal{E}$ (see [6, p.94]), so that $\mathrm{rad}(R) \in \mathcal{E}$ by (3).

2.2. Let $E_1, E_2 \in \mathcal{E}(V)$ be such that

$$E_1 \cap E_2 = \Delta(V), \qquad \langle E_1 \cup E_2 \rangle = V^2. \tag{4}$$

The first condition enables us to define the mapping

$$f : V \to V/E_1 \times V/E_2, \quad v \mapsto (X_1, X_2), \tag{5}$$

and for $X_1 \in V/E_1$ the mapping

$$t_{X_1} : X_1 \to V/E_2, \quad v \mapsto X_2, \tag{6}$$

where X_i is the class of the equivalence E_i containing v ($i = 1, 2$ in the first case whereas $i = 2$ in the second one).

Lemma 2.1 *The mappings f and t_{X_1} are bijections whenever the matrices $A(E_1)$ and $A(E_2)$ commute.*

Proof. It suffices to prove the bijectivity of f. To do this we observe that the injectivity follows from the first equality of (4). On the other hand, the second equality implies that any two vertices of the graph on V with the edge set $E_1 \cup E_2$ are connected by a path. If $A(E_1)A(E_2) = A(E_2)A(E_1)$, then such a path can be chosen of length at most 2. This means that $X_1 \cap X_2 \neq \emptyset$ for all $X_1 \in V/E_1$ and $X_2 \in V/E_2$, i.e. the mapping f is surjective.■

The following theorem describes the properties of the mappings f and t_{X_1} in the case when $E_1, E_2 \in \mathcal{E}$.

Theorem 2.2 *Let the ring W be commutative and let $E_1, E_2 \in \mathcal{E}$ be equivalences satisfying (4). Then the mappings f and t_{X_1}, $X_1 \in V/E_1$, are bijections and the following statements hold:*

(1) $W^f \geq W_{V/E_1} \otimes W_{V/E_2}$,

(2) *given* $X_1 \in V/E_1$, *we have* $t_{X_1} \in \mathrm{Iso}(W_{X_1}, W_{V/E_2})$ *and* $(R_{X_1})^{t_{X_1}} = R_{V/E_2}$ *for all* $R \in \mathcal{R}$, $R \subset E_1$,

(3) $t_{X_1,Y_1} \in \mathrm{Iso}(W_{X_1}, W_{Y_1}, \varphi_{X_1,Y_1})$ *for all* $X_1, Y_1 \in V/E_1$, *where* $t_{X_1,Y_1} = t_{X_1} \circ t_{Y_1}^{-1}$ *and* φ_{X_1,Y_1} *is the weak isomorphism from Lemma 8.1.*

Proof. The bijectivity of f and t_{X_1} follows from Lemma 2.1. Let us prove statement (1). A straightforward check shows that $A(E_1)^f = I_{V/E_1} \otimes J_{V/E_2}$ and

$$(\sum_{R\in\mathcal{R},R_{V/E_2}=R_2} A(R))^f = I_{V/E_1} \otimes A(R_2)$$

for all $R_2 \in \mathcal{R}(W_{V/E_2})$. This implies that $W^f \geq \{I_{V/E_1}\} \otimes W_{V/E_2}$. Similarly, $W^f \geq W_{V/E_1} \otimes \{I_{V/E_2}\}$. Thus, statement (1) follows. Next, let $R \in \mathcal{R}$, $R \subset E_1$. Then obviously $(R_{X_1})^{t_{X_1}} \subset R_{V/E_2}$. So it suffices to prove only the first part of statement (2). Since the matrices $A(E_1)$ and $A(E_2)$ commute, we have

$$R \cap (X_2 \times Y_2) = E_1 \cap (X_2 \times Y_2)$$

for all $X_2, Y_2 \in V/E_2$ such that $R \cap (X_2 \times Y_2) \neq \emptyset$. So for each $X_1 \in V/E_1$ the bijection t_{X_1} induces a bijection $\mathcal{R}(W_{X_1}) \to \mathcal{R}(W_{V/E_2})$, so that $t_{X_1} \in \mathrm{Iso}(W_{X_1}, W_{V/E_2})$. Finally, statement (3) follows from statement (2) and the definition of φ_{X_1,Y_1}.∎

Corollary 2.3 *In the conditions of Theorem 2.2 suppose that* $G \leq \mathrm{Aut}(W)$ *is a regular abelian group. Then the equivalences* E_1 *and* E_2 *are* G*-invariant, and*

$$G^f = G_{V/E_1} \times G_{V/E_2} \quad \text{and} \quad (G_{X_1})^{t_{X_1}} = G_{V/E_2}$$

for all $X_1 \in V/E_1$.

Proof. From statement (1) of Theorem 2.2 it follows that $g^f = (g_{V/E_1}, g_{V/E_2})$ for all $g \in \mathrm{Aut}(W)$. So $G^f \leq G_{V/E_1} \times G_{V/E_2}$. On the other hand, since G is regular and abelian, so are the groups G^f, G_{V/E_1} and G_{V/E_2}. This implies that

$$|G^f| = |V^f| = |V/E_1| \cdot |V/E_2| = |G_{V/E_1}| \cdot |G_{V/E_2}| = |G_{V/E_1} \times G_{V/E_2}|$$

whence the first equality follows. Since obviously $(X_1, v^{t_{X_1}}) = v^f$ for all $v \in X_1$, the second equality is the consequence of the first one.∎

2.3. Let $E_0, E_1 \in \mathcal{E}$ and $E_0 \subset E_1$. We intend to compute the group $\mathrm{Aut}(W)$ providing that W satisfies the E_1/E_0-condition in the sense of the following definition (see also [5]).

Definition 2.4 *We say that the ring* W *satisfies the* E_1/E_0*-condition if* $E_0 \subset \mathrm{rad}(R)$ *for all* $R \in \mathcal{R}$, $R \cap E_1 = \emptyset$.

Suppose we are given a permutation $g_0 \in \mathrm{Sym}(V/E_0)$ that respects the equivalence E_1, and for each $X \in V/E_1$ a bijection $g_X : X \to Y$ where $Y \in V/E_1$. The pair $(\{g_X\}_{X\in V/E_1}, g_0)$ is called *E_1/E_0-admissible* if $(g_X)_{X/E_0} = (g_0)_{X/E_0}$ for all $X \in V/E_1$. In this case there exists a uniquely determined permutation of V equal g_0 on V/E_0 and equal g_X on any $X \in V/E_1$. We say that it is induced by the pair $(\{g_X\}_{X\in V/E_1}, g_0)$.

An E_1/E_0-admissible pair is called *compatible* with W if the following conditions are satisfied:

(P1) $g_X \in \mathrm{Iso}(W_X, W_Y, \varphi_{X,Y})$ for all $X \in V/E_1$,

(P2) $g_0 \in \mathrm{Aut}(W_{V/E_0})$.

Denote by $\mathcal{P}(W, E_1/E_0)$ the set of all permutations induced by E_1/E_0-admissible pairs compatible with W.

Theorem 2.5 *Let the ring W satisfy the E_1/E_0-condition for some $E_0, E_1 \in \mathcal{E}$ such that $E_0 \subset E_1$. Then* $\mathrm{Aut}(W) = \mathcal{P}(W, E_1/E_0)$.

Proof. The inclusion $\mathrm{Aut}(W) \subset \mathcal{P}(W, E_1/E_0)$ is clear because any $g \in \mathrm{Aut}(W)$ is induced by the pair $(\{g_X\}_{X\in V/E_1}, g_{V/E_0})$ which is obviously compatible with W. Conversely, suppose that g is induced by an E_1/E_0-admissible pair $(\{g_X\}_{X\in V/E_1}, g_0)$ compatible with W. Then $R^g = R$ for all $R \in \mathcal{R}$. Indeed, if $R \subset E_1$, then by condition (P1) we have

$$R^g = \bigcup_{X\in V/E_1} (R_X)^{g_X} = \bigcup_{X\in V/E_1} (R_X)^{\varphi_{X,Y}} = \bigcup_{X\in V/E_1} R_Y = R$$

where $Y = X^g$. Otherwise, $R \cap E_1 = \emptyset$ and hence $E_0 \subset \mathrm{rad}(R)$ by the theorem hypothesis (see Definition 2.4). So equality (2) and condition (P2) imply that

$$R^g = (\bigcup_{(X_0,Y_0)\in R_0} X_0 \times Y_0)^g = \bigcup_{(X_0,Y_0)\in R_0} (X_0)^g \times (Y_0)^g = \bigcup_{(X_0,Y_0)\in R_0} (X_0)^{g_0} \times (Y_0)^{g_0} =$$

$$\bigcup_{(X_0,Y_0)\in R_0^{g_0}} X_0 \times Y_0 = \bigcup_{(X_0,Y_0)\in R_0} X_0 \times Y_0 = R$$

where $R_0 = R_{V/E_0}$.■

3 Quasinormal cellular rings

3.1. Let W be a Cayley ring over a group G (see Subsection 8.2). In accordance with [11] the ring W is called *normal* if G_{right} is a normal subgroup of $\mathrm{Aut}(W)$. We denote by $\mathcal{W}_{norm}$ the class of all cellular rings each of which is strongly isomorphic to a normal Cayley ring over a cyclic group. It is easily seen that a cellular ring belongs to $\mathcal{W}_{norm}$ iff its automorphism group contains a normal regular cyclic subgroup. Any element of $\mathcal{W}_{norm}$ is called a *normal* ring (over a cyclic group). One can prove that the automorphism group of a normal ring is isomorphic to a subgroup of the holomorph of a cyclic group (see [11, Theorem 4.5]). In particular, it is solvable. Furthermore, from [11, Theorem 6.6] it follows that every weak isomorphism of normal rings is induced by a strong isomorphism. The following result enables us efficiently handle with normal rings (see also [5]).

Theorem 3.1 *The following problems for cellular rings on n points can be solved in time $n^{O(1)}$:*

(1) *given a cellular ring W test whether $W \in \mathcal{W}_{norm}$, and (if it is so) list all elements of the group* $\mathrm{Aut}(W)$*,*

(2) *given cellular rings $W, W' \in \mathcal{W}_{norm}$ and a weak isomorphism $\varphi : W \to W'$, list all elements of the set* $\mathrm{Iso}(W, W', \varphi)$*.*

Proof. First we recall that a cellular ring $W \le \mathrm{Mat}_V$ is called *1-regular* if there exists a regular point of W, i.e. an element v of V such that $|R(v)| \le 1$ for all $R \in \mathcal{R}(W)$ (see [11, Section 9]). Next, if $\varphi : W \to W'$ is a weak isomorphism of cellular rings, then obviously

$$R^{\varphi}(v^f) = R(v)^f, \quad f \in \mathrm{Iso}(W, W', \varphi),$$

for every point v of W. It follows that if v is a regular point of W, then any such isomorphism f is uniquely determined (and can be efficiently constructed) by v^f. In particular, $|\mathrm{Iso}(W, W', \varphi)| \le n$ and the elements of this set can be listed in time $n^{O(1)}$.

Let $W \le \mathrm{Mat}_V$ be a cellular ring and $v \in V$. Set $W_v = [W, I_v]$ where $I_v = A(\{(v, v)\})$ (see Subsection 8.1). If $\varphi : W \to W'$ is a weak isomorphism and $v' \in V'$ where V' is the point set of W', then obviously there exists at most one weak isomorphism $\varphi_{v,v'} : W_v \to W'_{v'}$ that coincides with φ on W and takes I_v to $I_{v'}$. Moreover, it is easy to show that

$$\mathrm{Iso}(W, W', \varphi) = \bigcup_{v' \in S'} \mathrm{Iso}(W_v, W'_{v'}, \varphi_{v,v'})$$

where S' is the set of all $v' \in V'$ for which the isomorphism $\varphi_{v,v'}$ does exist. Now, if $W, W' \in \mathcal{W}_{norm}$, then from [11, Theorem 6.1] it follows that the cellular rings W_v and $W'_{v'}$ are 1-regular for all $v \in V$ and $v' \in V'$. So by the above paragraph and Theorem 8.3 the second problem can be solved in time $n^{O(1)}$. Since $\mathrm{Aut}(W) = \mathrm{Iso}(W, W, \mathrm{id}_W)$, the same argument shows that the elements of this group can be efficiently listed whenever the ring W_v is 1-regular for all $v \in V$. Taking into account that the latter condition is satisfied for any $W \in \mathcal{W}_{norm}$ we see that the first problem is $n^{O(1)}$-reducible to the recognition problem for 1-regular rings.∎

3.2. Let $W \le \mathrm{Mat}_V$ be a homogeneous cellular ring. Set

$$\mathcal{F}(W) = \{F = (E_0, E_1) : \ E_0, E_1 \in \mathcal{E}(W), \ E_0 \subset E_1\}.$$

Any above element F of $\mathcal{F}(W)$ is called a *flag* of W and will be denoted below by E_1/E_0. From Lemma 8.1 it follows that the cellular rings W_{X/E_0}, $X \in V/E_1$, are pairwise weakly isomorphic. So the numbers $|X/E_0|$ and $\mathrm{rk}(W_{X/E_0})$ do not depend on the choice of $X \in V/E_1$; denote them by

$|F|$ and $\mathrm{rk}(W_F)$ respectively. Also all the rings W_{X/E_0} are primitive or not simultaneously. In the former case we say that the flag F is *primitive*. The flag F is called *normal* if W_{X/E_0} is a normal ring for all $X \in V/E_1$. We say that F is a subflag of a flag $F' = E'_1/E'_0$ if $E_1 \subset E'_1$, $E_0 \supset E'_0$. In this case, obviously,

$$\mathrm{Aut}(W)_{X/E_0} \le \mathrm{Aut}(W_{X'/E'_0})_{X/E_0} \tag{7}$$

for all $X \in V/E_1$ and $X' \in V/E'_1$ with $X \subset X'$ (we identify X/E_0 with $(X/E'_0)/(E_0)_{X/E'_0}$).

Now suppose that the ring W is commutative and let $F = E_1/E_0$ and $F' = E_3/E_2$ be flags of W. We say that F' is a *multiple* of F if $E_0 = E_1 \cap E_2$ and $E_3 = \langle E_1 \cup E_2 \rangle$. In this case, if $G \le \mathrm{Aut}(W)$ is a regular cyclic group and $X \in V/E_3$, then obviously G_{X/E_0} is a regular cyclic subgroup of $\mathrm{Aut}(W_{X/E_0})$. So from Corollary 2.3 applied to the ring W_{X/E_0} and the equivalences $(E_1)_{X/E_0}$ and $(E_2)_{X/E_0}$ it follows that

$$(G_{X_1/E_0})^{t_{X_1/E_0}} = G_{X/E_2}, \quad X_1 \in X/E_1, \tag{8}$$

where t_{X_1/E_0} is the bijection (6). Denote by $\sim$ the equivalence closure of the relation "to be a multiple" on the set $\mathcal{F}(W)$. One can prove that the set $\mathcal{E}(W)$ forms a modular lattice with respect to the intersection and the equivalence closure of union. Thus, the $\sim$-equivalence corresponds to the projectivity in a modular lattice (see [2]).

Definition 3.2 *A flag of a commutative cellular ring W is called subnormal if it is a subflag of a normal flag of W; the flag is called quasinormal if it is $\sim$-equivalent to a subnormal one. We say that the ring W is quasinormal if every primitive flag of W is quasinormal.*

Obviously, each normal cellular ring is quasinormal. The converse statement is not true. Indeed, let W be the centralizer ring of the wreath product of two groups of prime order p. Then obviously the ring W is not normal for $p \ge 3$. On the other hand, W is quasinormal because any primitive subfactor of it is isomorphic to the centralizer ring of a regular group of order p and consequently is normal. One can prove that there exists a quasinormal ring not every primitive flag of which is subnormal.

Before stating the main result of the subsection we need the following technical notion. Let $W \le \mathrm{Mat}_V$ be a homogeneous cellular ring. By a *majorant* of a group $G \le \mathrm{Aut}(W)$ with respect to a flag $E_1/E_0 \in \mathcal{F}(W)$ we mean a permutation group G' on a set V' together with a family of bijections $f_X : X/E_0 \to V'$, $X \in V/E_1$, such that $(G_{X/E_0})^{f_X} \le G'$. We say that it is a majorant of G if $E_0 = \Delta(V)$ and $E_1 = V^2$.

Theorem 3.3 *Let W be a quasinormal cellular ring. Then there exists a solvable majorant of the group $\mathrm{Aut}_{cyc}(W)$ generated by all full cycle automorphisms of W. In particular, the group $\mathrm{Aut}_{cyc}(W)$ is solvable.*

Proof. We deduce the theorem from the following two lemmas. Below for permutation groups $G_1, \ldots, G_s$, $s \ge 0$, we define $\mathrm{wr}(G_1, \ldots, G_s)$ to be $\{1\}$ if $s = 0$, G_1 if $s = 1$, the wreath product of G_1 and G_2 in imprimitive action if $s = 2$, and $\mathrm{wr}(\mathrm{wr}(G_1, \ldots, G_{s-1}), G_s)$ if $s \ge 3$.

Lemma 3.4 *Let $W \le \mathrm{Mat}_V$ be a homogeneous cellular ring and $G \le \mathrm{Sym}(V)$. Suppose that equivalences $E_0, \ldots, E_s \in \mathcal{E}(W)$ satisfy the following conditions:*

(1) $\Delta(V) = E_0 \subset E_1 \subset \ldots \subset E_s = V^2$,

(2) *for each $i \in [s]$ we are given a majorant $(G_i, V_i, \{f_X\}_{X \in V/E_i})$ of the group G with respect to the flag E_i/E_{i-1}.*

Then the mapping

$$\mathfrak{f} : V \to \prod_{i=1}^{s} V_i, \quad v \mapsto (\ldots, f_{X_i}(X_{i-1}), \ldots) \tag{9}$$

is a bijection where X_i is the class of E_i containing v, and $G^{\mathfrak{f}} \le \mathrm{wr}(G_1, \ldots, G_s)$.

Proof. It is easily seen that $\mathfrak{f}$ is a surjection. Thus the first statement follows from the equality $|V| = |E_s/E_0| = \prod_{i=1}^{s} |E_i/E_{i-1}|$. To prove the second statement we assume (without loss of generality) that $s > 0$. Let $X \in V/E_{s-1}$. Then for every $i \in [s-1]$ the triple $(G_i, V_i, \{f_Y\}_{Y \in V/E_{i,X}})$ with $E_{i,X} = E_i \cap X^2$, is a majorant of the group $G_X \le \mathrm{Aut}(W_X)$ with respect to the flag $E_{i,X}/E_{i-1,X} \in \mathcal{F}(W_X)$. By induction for the bijection $\mathfrak{f}_X : X \to \prod_{i=1}^{s-1} V_i$ we have

$$(G_X)^{\mathfrak{f}_X} \le \mathrm{wr}(G_1, \ldots, G_{s-1}). \tag{10}$$

On the other hand,

$$(G_{V/E_{s-1}})^{f_V} \le G_s \tag{11}$$

(we used the fact that $V/E_s = \{V\}$). Besides, it is easily seen that $(G^{\mathfrak{f}})_{X^{\mathfrak{f}_X}} = (G_X)^{\mathfrak{f}_X}$ for all $X \in V/E_{s-1}$, and $(G^{\mathfrak{f}})_{V^{\mathfrak{f}}/(E_{s-1})^{\mathfrak{f}}} = (G_{V/E_{s-1}})^{f_V}$ (we identify $V^{\mathfrak{f}}/(E_{s-1})^{\mathfrak{f}}$ with V_s). Thus from (10) and (11) we conclude that $G^{\mathfrak{f}} \le \mathrm{wr}(\mathrm{wr}(G_1, \ldots, G_{s-1}), G_s) = \mathrm{wr}(G_1, \ldots, G_s)$.$\blacksquare$

Lemma 3.5 *Let W be a quasinormal ring. Then there exists a solvable majorant of the group $\mathrm{Aut}_{cyc}(W)$ with respect to any given primitive flag of W.*

Proof. Let F be a primitive flag of W. Then the quasinormality of W implies that there exist flags $F_i = E_{i,1}/E_{i,0}$ of W, $i \in [0, s]$, such that $F_0 = F$, the flag F_s is subnormal and for every $i \in [s]$ one of the flags F_{i-1}, F_i is a multiple of the other. From (8) it follows that if $(G', V', \{f_X\}_{X \in V/E_{i,1}})$ is a majorant of the group $\mathrm{Aut}_{cyc}(W)$ with respect to F_i, then $(G', V', \{\widetilde{t}_X \circ f_X\}_{X \in V/E_{i-1,1}})$ is a majorant of the same group with respect to F_{i-1} where $\widetilde{t}_X = t_{X/E_{i,0}}$ if F_{i-1} is a multiple of F_i and $\widetilde{t}_X = t_{X/E_{i,0}}^{-1}$ otherwise. Thus without loss of generality the flag $F = E_1/E_0$ can be assumed to be subnormal, i.e. a subflag of a normal flag $F' = E_1'/E_0'$ of W. For $X, Y \in V/E_1$ denote by X', Y' the classes of the equivalence E_1' containing X and Y respectively and set $\overline{X}' = X'/E_0'$ and $\overline{Y}' = Y'/E_0'$. Since $W_{\overline{X}'}, W_{\overline{Y}'} \in \mathcal{W}_{norm}$, there exists $f \in \mathrm{Iso}(W_{\overline{X}'}, W_{\overline{Y}'}, \varphi_{\overline{X}',\overline{Y}'})$ taking X/E_0' to Y/E_0' (see Subsection 3.1) where $\varphi_{\overline{X}',\overline{Y}'}$ is the weak isomorphism from Lemma 8.1. It follows that

$$(\mathrm{Aut}(W_{\overline{X}'})_{\overline{X}})^{f_{\overline{X}}} = \mathrm{Aut}(W_{\overline{Y}'})_{\overline{Y}}$$

where $\overline{X} = X/E_0$, $\overline{Y} = Y/E_0$ and $f_{\overline{X}} : \overline{X} \to \overline{Y}$ is the bijection induced by f. Then by (7) for a fixed $\overline{Y}$ the triple $(\overline{G}, \overline{Y}, \{f_{\overline{X}}\}_{X \in V/E_1})$ is a majorant of $\mathrm{Aut}(W)$ (and hence of $\mathrm{Aut}_{cyc}(W)$) with respect to F where $\overline{G} = \mathrm{Aut}(W_{\overline{Y}'})_{\overline{Y}}$. Since the group $\overline{G}$ is solvable (see Subsection 3.1), we are done.■

Now to prove the theorem choose equivalences $E_0, \ldots, E_s$ of W so that they satisfy condition (1) of Lemma 3.4 and the flag $F_i = E_i/E_{i-1}$ be primitive for all $i \in [s]$. By Lemma 3.5 there exists a solvable majorant $(G_i, V_i, \{f_X\}_{X \in V/E_i})$ of the group $\mathrm{Aut}_{cyc}(W)$ with respect to the flag F_i for all i. Set $G' = \mathrm{wr}(G_1, \ldots, G_s)$, $V' = \prod_{i=1}^{s} V_i$. Then by Lemma 3.4 the triple $(G', V', \{\mathfrak{f}\})$ where $\mathfrak{f}$ is bijection (9), is a majorant of the group $\mathrm{Aut}_{cyc}(W)$. Since the wreath product of solvable groups is solvable, we are done.■

3.3. In this subsection we describe an algorithm for recognizing the quasinormal cellular rings. Before doing this we make some remarks concerning computation with flags.

Let W be a commutative cellular ring on n points. Denote by Γ the graph on the set of all primitive flags of W such that two vertices of Γ are adjacent iff one of the corresponding flags is a multiple of the other. Since the intersection of equivalences and the equivalence closure of their union can be efficiently found, one can test whether two given vertices of Γ are adjacent in time $n^{O(1)}$. Since the set $\mathcal{E}(W)$ can be found in time $(mn)^{O(1)}$ where $m = |\mathcal{E}(W)|$ (see Subsection 2.1), the graph Γ can be constructed within the same time. Moreover, two primitive flags are $\sim$-equivalent iff the corresponding vertices of Γ are connected by a path. It is well known that the connected components of a graph and a path connecting any two vertices of a connected graph can be efficiently found. Thus given two primitive flags of W one can test whether they are $\sim$-equivalent and (if they are) find an appropriate sequence of flags in time $(mn)^{O(1)}$. Next, from statement (1) of Theorem 3.1 it follows that the normality of any flag of W can be tested in time $n^{O(1)}$. So given a primitive flag of W one can test if it is subnormal in time $m^2 n^{O(1)}$ by the exaustive search over the set of all normal flags of W. This enables us to efficiently recognize the primitive quasinormal flags. Finally, from the proof of Lemma 3.5 and Theorem 3.1 it follows that a solvable majorant of the group $\mathrm{Aut}_{cyc}(W)$ with respect to any given primitive quasinormal flag of W can be found in time $(mn)^{O(1)}$.

Algorithm A1
Input: a cellular ring $W \leq \mathrm{Mat}_V$.
Output: a solvable group G such that $\mathrm{Aut}_{cyc}(W) \leq G \leq \mathrm{Aut}(W)$ if W is a quasinormal ring, or $G = \emptyset$ otherwise.

Step 1. If W is not commutative, then output $G = \emptyset$. Otherwise construct the graph Γ on the set of all primitive flags of W (see above) and the set $\mathcal{F}$ of all subnormal flags of W.

Step 2. If none of the vertices of some connected component of Γ belongs to $\mathcal{F}$, then output $G = \emptyset$. Otherwise choose a maximal path $\Delta(V) = E_0 \subset E_1 \subset \ldots \subset E_s = V^2$ of equivalences of W.

Step 3. Find a solvable majorant $(G_i, V_i, \{f_X\}_{X\in V/E_i})$ of the group $\mathrm{Aut}_{cyc}(W)$ with respect to the flag E_i/E_{i-1}, $i \in [s]$ (see above), the group $G' = \mathrm{wr}(G_1, \ldots, G_s)$ and the bijection $\mathfrak{f}$ defined by (9).

Step 4. Output the group $G = \mathrm{Aut}(W) \cap (G')^{\mathfrak{f}^{-1}}$ found by the Babai-Luks algorithm (see Theorem 8.4).■

Theorem 3.6 *Algorithm A1 correctly tests the quasinormality of the ring W in time $(mn)^{O(1)}$ where $m = |\mathcal{E}(W)|$ and $n = |V|$. Moreover, if W is quasinormal it finds a solvable group G such that* $\mathrm{Aut}_{cyc}(W) \le G \le \mathrm{Aut}(W)$ *within the same time.*

Proof. From the definitions of a quasinormal ring and the graph Γ it follows that W is not a quasinormal ring iff the algorithm terminates before Step 3. This implies that the flags E_i/E_{i-1} ($i \in [s]$) being, obviously, primitive, are quasinormal. Besides, the group G' defined at Step 3 is solvable as the wreath product of solvable groups. Thus the correctness of the algorithm follows from Lemma 3.4 (implying that $\mathrm{Aut}_{cyc}(W)^{\mathfrak{f}} \le G'$) and from the correctness of the Babai-Luks algorithm. The required time bound follows from Theorem 8.4 and the remarks before the algorithm.■

4 Singular rings

4.1. As it will be shown below (see Theorem 5.1), every cellular ring admitting a full cycle automorphism is quasinormal or has a singularity in the following sense.

Let $W \le \mathrm{Mat}_V$ be a commutative cellular ring and $F = E_1/E_0$ and $F' = E_3/E_2$ flags of W. Suppose that F' is a multiple of F and the following conditions are satisfied (see Subsection 2.3):

(S1) W satisfies both the E_2/E_0-condition and the E_3/E_1-condition,

(S2) $W_{X/E_0} = W_{X/E_1} \otimes W_{X/E_2}$ for all $X \in V/E_3$.

(The set X/E_0 is identified with $X/E_1 \times X/E_2$ with the help of bijection (5) of Lemma 2.1 applied to $V = X/E_0$.) We observe that $\mathrm{rk}(W_F) = \mathrm{rk}(W_{F'})$ by statement (2) of Theorem 2.2.

Definition 4.1 *We say that the ring W has singularity in the pair (F, F') if* $\mathrm{rk}(W_F) = 2$. *In this case the number $d = |F| = |F'|$ is called the singularity degree. The ring W is called singular if it has singularity of degree $d \ge 3$ in some pair (F, F').*

We will resolve the singularity by changing W for the smallest cellular ring $W' = [W, A]$ containing W and the adjacency matrix A of a relation of the form

$$R(\mathfrak{F}) = \bigcup_{X\in V/E_3} \bigcup_{Y\in X/E_2} Y \times Y^{f_X}, \tag{12}$$

with $\mathfrak{F} = \{f_X\}_{X\in V/E_3}$ where $f_X \in \mathrm{Cyc}(X/E_2)$. The next theorem shows that in this case we can control the cycle bases of the rings W and W'. Below following [19] we will say that a subgroup G' of a permutation group G is a *well-embedded* one, if every cycle base of G' contains a cycle base of G, or, equivalently, if every full cycle of G is conjugate in G to some full cycle of G'.

Theorem 4.2 *In the above notation, for any family $\mathfrak{F}$ the group* $\mathrm{Aut}(W')$ *is a well-embedded subgroup of* $\mathrm{Aut}(W)$.

Proof. Let $\mathfrak{F}=\{f_X\}_{X\in V/E_3}$ where $f_X\in\mathrm{Cyc}(X/E_2)$. Since $W'\ge W$, without loss of generality we assume that $\mathrm{Cyc}(\mathrm{Aut}(W))\ne\emptyset$. Let g be a full cycle automorphism of W. Then $(E_3)^g=E_3$ and so $X^{g^k}=X$ for all $X\in V/E_3$ where $k=|V/E_3|$. It is easily seen that $\widetilde{g}_X=(g^k)_{X/E_2}$ is a full cycle on X/E_2. So one can find a permutation $h_X\in\mathrm{Sym}(X/E_2)$ such that $f_X=h_X^{-1}\widetilde{g}_Xh_X$. Suppose for a while that there exists $h^*\in\mathrm{Aut}(W)$ for which

$$(h^*)_{X/E_2}=h_X,\quad X\in V/E_3. \tag{13}$$

Then obviously the permutation $g'=(h^*)^{-1}gh^*$ belongs to $\mathrm{Cyc}(\mathrm{Aut}(W))$. Furthermore, for $X\in V/E_3$ and $Y\in X/E_2$ we have

$$(Y^{f_X})^{g'}=(Y^{f_X})^{(h^*)^{-1}gh^*}=(Y^{f_Xh_X^{-1}})^{gh^*}=(Y^{h_X^{-1}\widetilde{g}_X})^{gh^*}=$$

$$=((Y^{h_X^{-1}})^g)^{\widetilde{g}_{X^g}h_{X^g}}=((Y^{h_X^{-1}})^g)^{h_{X^g}f_{X^g}}=(Y^{(h^*)^{-1}gh^*})^{f_{X^g}})=(Y^{g'})^{f_{X^g}},$$

whence

$$R^{g'}=\bigcup_{X\in V/E_3}\bigcup_{Y\in X/E_2}Y^{g'}\times(Y^{f_X})^{g'}=\bigcup_{X\in V/E_3}\bigcup_{Y\in X/E_2}Y^{g'}\times(Y^{g'})^{f_{X^g}}=R,$$

where $R=R(\mathfrak{F})$. So $g'\in\mathrm{Cyc}(\mathrm{Aut}(W'))$. Since g is conjugate in $\mathrm{Aut}(W)$ to g', we are done.

Let us prove the existence of $h^*\in\mathrm{Aut}(W)$ satisfying (13). To do this we observe that the permutation g^l where $l=|V/E_1|$ induces the identical permutation of X/E_1 and a full cycle of X/E_2. This implies that for each $Y\in X/E_2$ there exists a power of this permutation that takes Y to $Y'=Y^{h_X}$. The induced bijection $h_Y:Y\to Y'$ obviously satisfies the following conditions:

$$h_Y\in\mathrm{Iso}(W_Y,W_{Y'},\varphi_{Y,Y'}),\qquad (h_Y)_{Y/E_0}=t_{Y/E_0,Y'/E_0} \tag{14}$$

where $\varphi_{Y,Y'}$ is the weak isomorphism from Lemma 8.1 and $t_{Y/E_0,Y'/E_0}$ is the bijection defined in statement (3) of Theorem 2.2. Thus the required statement follows from the lemma below.

Lemma 4.3 *In the notation of the theorem suppose that for every $X\in V/E_3$ we are given a permutation $h_X\in\mathrm{Sym}(X/E_2)$ and for every $Y\in X/E_2$ a bijection $h_Y:Y\to Y'$ satisfying (14) where $Y'=Y^{h_X}$. Then there exists a uniquely determined $h^*\in\mathrm{Aut}(W)$ such that $(h^*)_{X/E_2}=h_X$, $(h^*)_{X/E_1}=\mathrm{id}_{X/E_1}$ and $(h^*)_Y=h_Y$ for all X and Y.*

Proof. The uniqueness of h^* follows from the last condition on it. To prove the existence let $X\in V/E_3$. Denote by $\widetilde{h}_X$ the permutation of the set $X/E_0=X/E_1\times X/E_2$ taking (X_1,X_2) to $(X_1,X_2^{h_X})$. Then the pair $(\{h_Y\},\widetilde{h}_X)$ is $(E_2/E_0)_X$-admissible where $(E_2/E_0)_X=(E_2)_X/(E_0)_X$ (see Subsection 2.3) because $(h_Y)_{Y/E_0}=t_{Y/E_0,Y'/E_0}=(\widetilde{h}_X)_{Y/E_0}$ for all $Y\in X/E_2$. Moreover, it is compatible with the ring W_X. Indeed, condition (P1) is satisfied by the lemma hypothesis. Next, since $\mathrm{rk}(W_{X/E_2})=2$, condition (S2) implies that $\widetilde{h}_X\in\mathrm{Aut}(W_{X/E_0})$. Thus condition (P2) is also satisfied. Now set h'_X to be the permutation of X induced by the pair $(\{h_Y\},\widetilde{h}_X)$. Then

$h'_X \in \mathcal{P}(W_X, (E_2/E_0)_X)$. On the other hand, condition (S1) implies that the ring W_X satisfies the $(E_2/E_0)_X$-condition. Thus $h'_X \in \mathrm{Aut}(W_X)$ by Theorem 2.5. Moreover, since $(h'_X)_{X/E_1} = \widetilde{h}_X$, we have $(h'_X)_{X/E_1} = \mathrm{id}_{X/E_1}$. So the pair $(\{h'_X\}, \mathrm{id}_{V/E_1})$ is E_3/E_1-admissible and hence compatible with W. Besides W satisfies the E_3/E_1-condition (see (S1)). Thus by Theorem 2.5 the permutation h^* of V induced by this pair belongs to $\mathrm{Aut}(W)$. Since $(h^*)_X = h'_X$ for all $X \in V/E_3$, we are done.$\blacksquare$

4.2. Below we present an efficient algorithm for recognizing singular rings and resolving their singularities. We start with some preliminary remarks. Let $F = E_1/E_0$ and $F' = E_3/E_2$ be flags of a commutative cellular ring $W \le \mathrm{Mat}_V$. First, since the equivalences $E_1 \cap E_2$ and $\langle E_1 \cup E_2 \rangle$ can be easily constructed (see Subsection 2.1), one can efficiently test whether F' is a multiple of F. Next, since the radical of any relation can be easily found, the E_2/E_0-condition and the E_3/E_1-condition can be efficiently tested for W. Finally, given $X \in V/E_3$, the equality in (S2) also can be efficiently tested (e.g. by comparing basis relations). Thus, one can test whether the ring W has singularity in the pair (F, F') in time $n^{O(1)}$ where $n = |V|$. Below we call an extension W' of W *admissible* if $\mathrm{Aut}(W')$ is a well-embedded subgroup of $\mathrm{Aut}(W)$ and $W' \ne W$.

Algorithm A2
Input: a cellular ring $W \le \mathrm{Mat}_V$.
Output: an admissible extension W' of W if W is singular or $W' = \emptyset$ otherwise.

> **Step 1.** If W is not commutative, then output $W' = \emptyset$. Otherwise construct the set $\mathcal{E}(W)$ (see Subsection 2.1) and then the set $\mathcal{F}(W)$.
>
> **Step 2.** Find the set $\mathcal{P}$ of all pairs $(F, F') \in \mathcal{F}(W)^2$ such that W has singularity of degree at least 3 in (F, F') (see above).
>
> **Step 3.** If $\mathcal{P} = \emptyset$, then output $W' = \emptyset$. Otherwise choose $(F, F') \in \mathcal{P}$.
>
> **Step 4.** Output $W' = [W, A]$ where A is the adjacency matrix of the relation (12) with an arbitrarily chosen family $\mathfrak{F}$.$\blacksquare$

Theorem 4.4 *Algorithm A2 correctly tests the singularity of the ring W in time $(mn)^{O(1)}$ where $m = |\mathcal{E}(W)|$ and $n = |V|$. Moreover, if W is singular, then it finds an admissible extension W' of it within the same time.*

Proof. The correctness of the algorithm is the consequence of Theorem 4.2, the definition of a singular ring and the fact that at Step 4 $W' \ne W$ because W has singularity of degree at least 3 in (F, F'). Since the set $\mathcal{E}(W)$ can be constructed in time $(mn)^{O(1)}$ (see Subsection 2.1), the required time bound follows from Theorem 8.3 and the remarks before the algorithm.$\blacksquare$

In this paper Algorithm A2 will be applied only when $m \le n$ and so in this case its complexity is bounded by $n^{O(1)}$. In the general case one can modify the algorithm to attain the same time upper bound. Indeed, if W has singularity in (F, F'), then it can be proved that $E_1 \setminus E_0 \in \mathcal{R}(W)$ and E_2 equals the equivalence closure of the union of all $R \in \mathcal{R}(W)$ such that $\langle R \rangle \cap E_1 \subset E_0$.

5 Quasinormal and singular Cayley rings over a cyclic group

In this section we deal with quasinormal and singular rings as introduced in Sections 3 and 4, belonging to the class of Cayley rings over a cyclic group. The main result can be formulated as follows.

Theorem 5.1 *Every cellular ring admitting a full cycle automorphism is either quasinormal or singular.*

Proof. Let W be a cellular ring such that $\mathrm{Cyc}(\mathrm{Aut}(W)) \neq \emptyset$. Without loss of generality we can assume that W is a Cayley ring over a cyclic group G (see Subsection 8.2). We observe that by Theorem 8.2 the lattice $\mathcal{E} = \mathcal{E}(W)$ of equivalences of W is isomorphic to a sublattice of the lattice of subgroups of the group G which is isomorphic by the cyclicity of G to the lattice of divisors of the integer $n = |G|$.[3] According to [2] the latter lattice is distributive and hence so is the lattice $\mathcal{E}$. Let $\mathcal{C}$ be a class of $\sim$-equivalence on the set of all flags of the ring W (see Subsection 3.2). Below an element of $\mathcal{C}$ is called the *least* (resp. the *greatest*) one if every element of this class is a multiple of it (resp. it is a multiple of every element of this class).

Lemma 5.2 *Each class of the $\sim$-equivalence on the set $\mathcal{F}(W)$ of all flags of W contains the least element and the greatest element.*

Proof. Since the notion of $\sim$-equivalence is selfdual, we only verify the existence of the least element. From the transitivity of the relation "to be a multiple" and the definition of the $\sim$-equivalence it follows that it suffices to prove that if F_3 is a multiple of both F_1 and F_2, then there exists F_0 such that both F_1 and F_2 are multiples of F_0 (here $F_i \in \mathcal{F}(W)$ for all i). Let $F_i = E_{i1}/E_{i0}$ $(i = 1, 2, 3)$. Set $F_0 = E_{01}/E_{00}$ where $E_{0j} = E_{1j} \cap E_{2j}$ $(j = 1, 2)$. Then

$$E_{00} = E_{01} \cap E_{00} = E_{01} \cap E_{i0} \cap E_{0i'} = (E_{01} \cap E_{i0}) \cap (E_{i'1} \cap E_{30}) = E_{01} \cap E_{i0}$$

and due to the distributivity of the lattice $\mathcal{E}$ also

$$E_{i1} = E_{31} \cap E_{i1} = (E_{i'1}E_{30}) \cap E_{i1} = (E_{i'1} \cap E_{i1})(E_{30} \cap E_{i1}) = E_{01}E_{i0}$$

where $i' = 3 - i$ $(i = 1, 2)$. Thus both F_1 and F_2 are multiples of F_0.■

Suppose that the ring W is not quasinormal. Then there exists a class $\mathcal{C}$ of the $\sim$-equivalence on the set of all primitive flags of W that contains no subnormal flags. Let $F = E_1/E_0$ and $F' = E_3/E_2$ be the least and greatest elements of $\mathcal{C}$. Then the theorem is the consequence of the proposition below.

Proposition 5.3 *The ring W has singularity of degree $d \geq 4$ in the pair (F, F').*

[3] Below for $E_1, E_2 \in \mathcal{E}$ we write E_1E_2 instead of $\langle E_1 \cup E_2 \rangle$.

Proof. First we observe that $d = |F| = |F'| \ge 4$, for otherwise the flags F and F' have to be normal. Next, it is easy to see that the ring W_{X/E_0} is strongly isomorphic to a Cayley ring over a cyclic group for all $X \in G/E_1$. Since it is primitive, Theorem 2.10.5 of [3] implies that either its rank equals 2 or its degree is a prime. In the latter case the rank also equals 2 for otherwise the ring W_{X/E_0} be normal by Theorem 12.7.5 of [3]. Thus it suffices to verify conditions (S1) and (S2).

Set $\mathcal{A} = W^{\rho^{-1}}$ and $H_i = E_i^{\rho^{-1}}$, $i = 0,1,2,3$, where $\rho = \rho_G$ is monomorphism (24). Then $\mathcal{A}$ is an S-ring over the group G, $H_i \in \mathcal{H}(\mathcal{A})$ for all i and $H_0 = H_1 \cap H_2$, $H_3 = H_1H_2$ (here and below we freely use the notation and the facts of Subsection 8.2). Since obviously $\mathrm{rad}(R) = \mathrm{rad}(X)^\rho$ for all $R \in \mathcal{R}^*(W)$ where $X = R^{\rho^{-1}}$, the cellular ring W satisfies the E_{i+2}/E_i-condition iff the S-ring $\mathcal{A}$ satisfies the H_{i+2}/H_i-condition ($i = 0,1$). Furthermore, the correspondence between the Cayley rings and the S-rings respects tensor product. Thus it suffices to verify that

(S1$'$) $\mathcal{A}$ satisfies both the H_2/H_0-condition and the H_3/H_1-condition,

(S2$'$) $\mathcal{A}_{H_3/H_0} = \mathcal{A}_{H_1/H_0} \otimes \mathcal{A}_{H_2/H_0}$.

To do this let $X \in \mathcal{S}(\mathcal{A})$. Then it suffices to verify that $\mathrm{rad}(X) \ge H_i$ whenever $X \subset G \setminus H_{i+2}$, $i = 0,1$ (condition (S1$'$)), and $XH_0 = X_1H_0 \cdot X_2H_0$ for some $X_i \in \mathcal{S}(\mathcal{A}_{H_i})$, $i = 1,2$, whenever $X \subset H_3$ (condition (S2$'$)). We will verify the both conditions simultaneously. Suppose first that $X \subset H_2$ or $\mathrm{rad}(X) \ge H_1$. Then as to condition (S1$'$) there is nothing to verify. Next, condition (S2$'$) is trivially satisfied for $X \subset H_2$. If $\mathrm{rad}(X) \ge H_1$, then $X \not\subset H_3$ for otherwise the image of the basic set X with respect to the natural epimorphism $H_3 \to H_1/H_0$ equals H_1/H_0 which is not a basic set of the ring $\mathcal{A}_{H_1/H_0}$. So in this case condition (S2$'$) is also satisfied. Thus without loss of generality we can assume that

$$X \not\subset H_2, \quad \mathrm{rad}(X) \not\ge H_1. \tag{15}$$

Then the required conditions are satisfied due to the following lemma.

Lemma 5.4 *In the above notation and assumptions we have $H_0 \le \mathrm{rad}(X)$ and $X \subset H_3$. Moreover, $X = X_1X_2$ where $X_1 = H_1 \setminus H_0$ and $X_2 \in \mathcal{S}^*(\mathcal{A}_{H_2})$ with $X_2H_0 = X_2$.*

Proof. Using the results of Subsection 8.2 we transfer from the Cayley rings to the S-rings the notions of flag, subflag, multiple and $\sim$-equivalence, and also of normality, subnormality and quasinormality of a flag. We observe that a flag U/L of the S-ring $\mathcal{A}$ is normal iff the S-ring $\mathcal{A}_{U/L}$ is normal in the sense of [11] (i.e. the cellular ring $(\mathcal{A}_{U/L})^{\rho_{U/L}}$ is normal). Besides, from the definition of H_i ($i = 0,1,2,3$) it follows that the flag H_3/H_2 is a multiple of H_1/H_0 and no flag in the class of the $\sim$-equivalence containing both of them is subnormal. Moreover, the flags H_1/H_0 and H_3/H_2 are the least element and the greatest element of this class respectively.

Set $U = \langle X \rangle$ and $L = \mathrm{rad}(X)$. Let us show that

$$H_1/H_0 \sim H_1L/H_0L, \quad H_3/H_2 \sim (H_3 \cap U)/(H_2 \cap U). \tag{16}$$

Since both equivalences can be proved along the same lines, we prove, for instance, the second one. First, we observe that the flag H_3U/H_2U is not a multiple of H_3/H_2. (Otherwise, $U \le H_3$

due to the maximality of the latter flag. Since also $H_3 \cap H_2U = H_2$, we have $H_2U = H_2$, which contradicts the first relation of (15).) So $H_2 < H_3 \cap (H_2U)$ and then $H_3 \cap (H_2U) = H_3$ because $\mathrm{rk}(\mathcal{A}_{H_3/H_2}) = 2$. Therefore, $H_3 \le H_2U$ whence

$$H_0(H_1 \cap U) = (H_1 \cap H_2)(H_1 \cap U) = H_1 \cap (H_2U) = H_1$$

by the distributivity of the lattice $\mathcal{H}(\mathcal{A})$. This implies that H_1/H_0 is a multiple of $(H_1 \cap U)/(H_0 \cap U)$ and hence $H_1 \le U$ by the minimality of the flag H_1/H_0. So $H_3 \ge (H_3 \cap U)H_2 \ge H_1H_2 = H_3$, and hence $(H_3 \cap U)H_2 = H_3$. Since obviously $(H_3 \cap U) \cap H_2 = H_2 \cap U$, this implies that H_3/H_2 is a multiple of $(H_3 \cap U)/(H_2 \cap U)$.

From (16) and the fact that H_1/H_0 and H_3/H_2 are the least and greatest elements respectively it follows that the flags H_1L/H_0L and $(H_3 \cap U)/(H_2 \cap U)$ are subflags of U/L. Let us prove that there exist groups $H, H' \in \mathcal{H}(\mathcal{A})$ such that $L \le H, H' \le U$ and

$$H_1L/H_0L \sim H/L, \quad (H_3 \cap U)/(H_2 \cap U) \sim U/H', \quad \mathcal{A}_{U/L} = \mathcal{A}_{H/L} \otimes \mathcal{A}_{H'/L}. \tag{17}$$

To do this we observe that the image of X in U/L has trivial radical. Then from [17, Theorem 3.1] and the definition of U it follows that it contains a generator of the group U/L. So the S-ring $\mathcal{A}_{U/L}$ has trivial radical in the sense of [11]. By [11, Corollary 6.4] this implies that there exist groups $U_i \in \mathcal{H}(\mathcal{A})$, $L \le U_i \le U$ $(i = 0, \ldots, s)$, such that

$$\mathcal{A}_{U/L} = \bigotimes_{i=0}^{s} \mathcal{A}_{U_i/L}, \tag{18}$$

where $\mathcal{A}_{U_0/L}$ is a normal S-ring and $\mathrm{rk}(\mathcal{A}_{U_i/L}) = 2$ for all $i > 0$. It is easy to see that every group belonging to $\mathcal{H}(\mathcal{A}_{U/L})$ is of the form $\prod_{i=0}^{s} U'_i/L$ where $U'_0 \in \mathcal{H}(\mathcal{A})$, $L \le U'_0 \le U_0$, and $U'_i \in \{U_i, L\}$ for $i > 0$. So every subflag F of U/L such that $\mathrm{rk}(\mathcal{A}_F) = 2$ is $\sim$-equivalent either to a subflag of U_0/L or both to the flags U_i/L and U/U'_i for some $i > 0$ where U'_i is the product of U_j with $j \ne i$. On the other hand, the flags H_1L/H_0L and $(H_3 \cap U)/(H_2 \cap U)$ are not quasinormal because so are not the flags H_1/H_0 and H_3/H_2 (see (16)). Thus by the normality of the ring $\mathcal{A}_{U_0/L}$ the first case is impossible for them. So there exists $i > 0$ such that $H_1L/H_0L \sim U_i/L$ and $(H_3 \cap U)/(H_2 \cap U) \sim U/U'_i$. Therefore, (17) is true for $H = U_i$ and $H' = U'_i$ (see (18)).

To complete the proof of the lemma we observe that the first part of it follows from the equivalences (16) and (17) because the flags H_1/H_0 and H_3/H_2 are the least and greatest elements of the $\sim$-equivalence class containing both of them respectively. Next, equality (17) implies that $X = X_1X_2$ for some $X_1 \in \mathcal{S}^*(\mathcal{A}_H)$ and $X_2 \in \mathcal{S}^*(\mathcal{A}_{H'})$ such that $X_i = X_iL$ $(i = 1, 2)$. Thus the second part of the lemma is the consequence of the first part of it and the equality $X_1 = (H_1 \setminus H_0)L$.■

6 Cycle base of a solvable group

6.1. In this section we construct a polynomial-time algorithm for finding a cycle base of an arbitrary solvable permutation group. First we treat a slightly different problem.

Let $G \le \mathrm{Sym}(V)$ be a permutation group and let $c \in \mathrm{Sym}(V)$ normalize G. Suppose that $V_0, \ldots, V_{m-1}$ are pairwise disjoint subsets of V such that

$$V = \bigcup_{i=0}^{m-1} V_i, \quad (V_i)^G = V_i, \quad (V_i)^c = V_{i+1} \quad \text{for all } i \tag{19}$$

(here and below the addition of indices is meant modulo m). Denote by G_i the permutation group induced by the action of G on V_i. Then since $G^c = c^{-1}Gc = G$, from (19) it follows that $(G_i)^c = G_{i+1}$ for all i (we write c instead of c_{V_i} in brief). Given $X \subset G$ and $S \subset [0, m-1]$ set $X_S = \varphi_S(X)$ where

$$\varphi_S : G \to \prod_{i \in S} G_i, \quad g \mapsto (\ldots, g_i, \ldots)$$

is the homomorphism induced by the natural epimorphisms $G \to G_i$ ($i \in S$). If $S = \{i\}$, we write X_i and φ_i instead of X_S and φ_S respectively. Obviously, φ_S is a monomorphism for $S = [0, m-1]$. Concerning computation with permutation groups in the algorithm below see Subsection 8.3.

Auxiliary algorithm A3′
Input: a group $G \le \mathrm{Sym}(V)$ and a permutation $c \in \mathrm{Sym}(V)$ as above.
Output: a set $X \subset Gc$ (given as the list of elements) such that $Gc = \bigcup_{g \in G} X^g$.

Step 1. If $G = \{1\}$, then output $X = \{c\}$. Otherwise, using the normal closure algorithm find a maximal c^m-invariant normal subgroup K_0 of G_0.

Step 2. Set $G^{(0)} = G$. For $i = 0, \ldots, m-1$ successively by the sift procedure find the group $G^{(i+1)} = G^{(i)} \cap \varphi_i^{-1}(K_i)$ where $K_i = (K_0)^{c^i}$.

Step 3. By the sift procedure find the maximal number $l \in [0, m-1]$ for which $[G : G^{(i+1)}] = \prod_{j=0}^{i} [G_j : K_j]$, and then a transversal T of the group $G^{(m)}$ in the group $G^{(l)}$.

Step 4. For each $t \in T$ recursively find the set $X_t =$A3′(H, tc) where $H = G^{(m)}$. Output $X = \bigcup_{t \in T} X_t$.■

Theorem 6.1 *Algorithm A3′ correctly finds a set $X \subset Gc$ such that $Gc = \bigcup_{g \in G} X^g$ in time $(nr)^{O(1)}$ where $n = |V|$ and $r = |G_0|$. Moreover, $|X| \le |G_0|$.*

Proof. We prove the theorem by induction on r. If $r = 1$, then $G = \{1\}$ and we are done (see Step 1). Suppose that $r > 1$.

To prove the correctness of the algorithm first let us verify that each pair (H, tc) where $t \in T$ with H and T found at Steps 2 and 3, is an admissible input of the algorithm. Indeed, since $H \le G$, equalities (19) imply that $(V_i)^H = V_i$ and $(V_i)^{tc} = V_{i+1}$ for all i. Furthemore, K_i is a normal subgroup of G_i and $(K_i)^c = K_{i+1}$ (see Steps 1 and 2), whence it follows that $H^{tc} = H$.

Next, in accordance with Steps 1 and 3 we have $H_0 \leq K_0 < G_0$ where $H_0 = \varphi_0(H)$. So by the induction hypothesis

$$Htc = \bigcup_{h \in H} (X_t)^h, \quad t \in T, \tag{20}$$

where the set X_t is found at Step 4. To complete the proof of the correctness let $fc \in Gc$. Then for every $g \in G$ we have

$$(g^{-1} f g^{c^{-1}})_i = g_i^{-1} f_i (g_{i+1})^{c^{-1}}, \quad 0 \leq i \leq m-2.$$

On the other hand, from the definition of l at Step 3 it follows that the natural homomorphism $G \to \prod_{j=0}^{l}(G_j/K_j)$ is in fact an epimorphism. So g can be chosen in such a way that the right-hand side of the last equality belong to K_i for all $i \in [0, l-1]$. Then $g^{-1} f g^{c^{-1}} \in G^{(l)}$ (see Step 2) and hence the element $(fc)^g$ (equal to $g^{-1} f c g = (g^{-1} f g^{c^{-1}})c$) belongs to $G^{(l)}$. Thus,

$$Gc = \bigcup_{g \in G} (G^{(l)} c)^g = \bigcup_{g \in G} (HTc)^g$$

which by equality (20) implies that

$$Gc = \bigcup_{g \in G} \bigcup_{t \in T} (Htc)^g = \bigcup_{g \in G} \bigcup_{t \in T} \bigcup_{h \in H} (X_t)^{hg} = \bigcup_{g \in G} (\bigcup_{t \in T} X_t)^g = \bigcup_{g \in G} X^g.$$

The correctness is proved.

For the rest of the proof we need the following lemma.

Lemma 6.2 *In the notation of the algorithm,* $[G^{(l)} : H] \leq [G_0 : H_0]$ *where* $H_0 = \varphi_0(H)$.

Proof. We have

$$[G^{(l)} : G^{(l+1)}] = [G_l : K_l] = [G_0 : K_0] \leq [G_0 : H_0].$$

So it suffices to prove that $H = G^{(l+1)}$. To do this we observe that the kernel of the natural epimorphism $G \to \prod_{j=0}^{l}(G_j/K_j)$ equals $G^{(l+1)}$ and contains H. Thus we only have to show that the induced epimorphism

$$G/H \to \prod_{j=0}^{l} (G_j/K_j) \tag{21}$$

is in fact an isomorphism. By the definition of H it suffices to verify that $(G^{(i)})_i \leq K_i$ for all $i \in [l+1, m-1]$. Without loss of generality we assume that $l < m-1$. Since obviously $(G^{(i)})_i$ is a normal c^m-invariant subgroup of G_i and $K_i = (K_0)^{c^i}$ for all i, the statement for $i = l+1$ follows from the choice of K_0 at Step 1 and l at Step 3. Suppose that it is true for some $i \in [l+1, m-2]$. Then

$$(G^{(i+1)})_{i+1} = (\varphi_{[0,i]}^{-1}(\prod_{j=0}^{i} K_j))_{i+1} \leq (\varphi_{[1,i]}^{-1}(\prod_{j=1}^{i} K_j))_{i+1} =$$

$$((\varphi^{-1}_{[0,i-1]}(\prod_{j=0}^{i-1} K_j))_i)^c = ((G^{(i)})_i)^c \le (K_i)^c = K_{i+1},$$

and we are done.■

To estimate $|X|$ we observe that $|X_t| \le |H_0|$ for all $t \in T$ by the induction hypothesis. On the other hand, from Lemma 6.2 it follows that $|T| = [G^{(l)} : H] \le [G_0 : H_0]$. Thus,

$$|X| = \sum_{t \in T} |X_t| \le |T||H_0| \le [G_0 : H_0]|H_0| = |G_0|.$$

To estimate the complexity denote by $t(G,c)$ the running time of the algorithm applied to the pair (G,c). From the inequality $[G^{(i-1)} : G^{(i)}] \le r$, $i \in [m]$, and Lemma 6.2 it follows that Steps 1-3 can be done in time $(nr)^{O(1)}$ (see Subsection 8.3). The same lemma implies that the number of recursion calls at Step 4 is at most $\overline{r} = [G_0 : K_0] \le [G_0 : H_0]$. So by the induction hypothesis we have

$$t(G,c) \le (nr)^{O(1)} + \overline{r}(nr/\overline{r})^{O(1)},$$

which completes the proof of the theorem.■

6.2. Let us describe the main algorithm of this section. Let $c = (v_1, \ldots, v_n)$ and $c' = (v'_1, \ldots, v'_n)$ be full cycles on V. Then it is easily seen that

$$\{g \in \mathrm{Sym}(V) :\ g^{-1}cg = c'\} = \langle c \rangle g_0 \tag{22}$$

where g_0 is the permutation of V taking v_i to v'_i for all i. Thus if $G \le \mathrm{Sym}(V)$ is an $n^{O(1)}$-recognizable permutation group [4] then by checking whether or not $c^i g_0 \in G$ for some $i \in [n]$ one can test in time $n^{O(1)}$ whether or not c and c' are G-conjugate. In particular, if $Y \subset \mathrm{Cyc}(V)$, then the family $\mathfrak{F}_G(Y)$ of all G-conjugacy classes of Y (and then a transversal of $\mathfrak{F}_G(Y)$) can be found in time $(n|Y|)^{O(1)}$.

Algorithm A3
Input: a permutation group $G \le \mathrm{Sym}(V)$.
Output: a cycle base C of G.

Step 1. If G is not transitive, then output $C = \emptyset$.

Step 2. If $|V| = 1$, then output $C = G$. Otherwise, find a minimal element E in the set of all G-invariant equivalences on V other than $\Delta(V)$.

Step 3. Construct the groups $G_{V/E}$ and $G_E = \{g \in G :\ g_{V/E} = \mathrm{id}_{V/E}\}$. Recursively find the set $\overline{C}$ =A3$(G_{V/E})$.

[4] The group G is not assumed to be given by generators.

Step 4. For each $\overline{c} \in \overline{C}$ find $c \in G$ such that $c_{V/E} = \overline{c}$, and then the set $X_c = \mathrm{A3}'(G_E, c)$ (decomposition (19) is given by the classes of E).

Step 5. Output as C a transversal of the family $\mathfrak{F}_G(\mathrm{Cyc}(X))$ where $X = \bigcup_{\overline{c} \in \overline{C}} X_c$.■

Theorem 6.3 *Algorithm A3 correctly finds a cycle base of the group G. If G is solvable, then this algorithm runs in time $n^{O(1)}$ where n is the degree of G.*

Proof. To prove the correctness of the algorithm it suffices to verify that if the group G is transitive, then every full cycle of G is conjugate in G to some element of C. Let $c' \in \mathrm{Cyc}(G)$. Then $c'_{V/E} \in \mathrm{Cyc}(G_{V/E})$ whence by induction it follows that $c'_{V/E}$ is conjugate in $G_{V/E}$ to some element $\overline{c} \in \overline{C}$. This implies that c' is conjugate in G_E to some element of $G_E c$ and consequently to some element of X_c by Theorem 6.1. Thus, c' is conjugate in G to some element of C by the choice of C at Step 5.

Let us estimate the running time $t(G)$ of the algorithm applied to a solvable group G. First, we observe that Steps 1 and 2 can be easily done in time $n^{O(1)}$. The running time of Step 3 is $t(G_{V/E}) + n^{O(1)}$. By Theorem 6.1 the running time of Step 4 is $|\overline{C}|(n^{O(1)} + (n|G_0|)^{O(1)})$ where $G_0 = (G_E)_{V_0}$ with V_0 a fixed class of E. Finally, Step 5 can be done in time $(n|X|)^{O(1)}$ (see the remark before the algorithm). From the minimality of E it follows that the group G_{V_0} is primitive. So $|G_{V_0}| \le |V_0|^4$ due to the upper bound for the order of a primitive solvable group proved in [23]. Next, $|X_c| \le |G_0|$ for each $\overline{c} \in \overline{C}$ by Theorem 6.1. Thus, $|X| \le |\overline{C}||V_0|^4 \le n^4$ because $G_0 \le G_{V_0}$ and $|\overline{C}| \le |V/E|$ (see Section 1). Summing up all we said in this paragraph we obtain

$$t(G) \le n^{O(1)} + t(G_{V/E})$$

which completes the proof.■

7 Cycle base of a cellular ring

Let W be a homogeneous cellular ring on V. Set

$$\mathcal{E}_0(W) = \{\langle R\rangle : \ R \in \mathcal{R}(W)\}.$$

Then $\mathcal{E}_0(W) \subset \mathcal{E}(W)$ (see Subsection 2.1). If W is a Cayley ring over a cyclic group G, then $\mathcal{E}_0(W) = \mathcal{E}(W)$. Indeed, let $E \in \mathcal{E}(W)$. Then $E = H^{\rho_G}$ for some $H \in \mathcal{H}(\mathcal{A})$ where $\mathcal{A}$ is the S-ring over G corresponding to W (see Theorem 8.2). So $E = \langle R\rangle$ for $R = X^{\rho_G}$ where X is the basic set of $\mathcal{A}$ containing a generator of H. Generally, however, $\mathcal{E}_0(W) \ne \mathcal{E}(W)$. But then one can find two distinct relations $R, S \in \mathcal{R}(W)$ such that the equivalence $\langle R \cup S\rangle$ does not belong to $\mathcal{E}_0(W)$. Thus the equality $\mathcal{E}_0(W) = \mathcal{E}(W)$ can be tested in time $n^{O(1)}$ where $n = |V|$.

Main Algorithm
Input: a cellular ring W on V.
Output: a cycle base C of W.

Step 1. Set $W_0 = W$ and $W' = W$.

Step 2. While $W' \neq \emptyset$ repeat the following: if W' is not homogeneous or $\mathcal{E}_0(W') \neq \mathcal{E}(W')$, then output $C = \emptyset$, else set $W = W'$ and find W' =A2(W).

Step 3. Find G =A1(W). If $G = \emptyset$, then output $C = \emptyset$.

Step 4. Find C' =A3(G). Output as C a transversal of the family $\mathfrak{F}_{\mathrm{Aut}(W_0)}(C')$ (see Subsection 6.2).∎

Theorem 7.1 *Given a cellular ring W on n points, the Main Algorithm correctly finds a cycle base of W in time $n^{O(1)}$.*

Proof. Let us prove the correctness of the algorithm. First, suppose that $\mathrm{Cyc}(\mathrm{Aut}(W)) = \emptyset$. Then we can assume that the algorithm terminates at Step 4. Since the cellular ring at Step 3 contains the input ring, we have $\mathrm{Cyc}(G) = \emptyset$ where G is the group found at Step 3. Thus the correctness of the algorithm follows from that of Algorithm A3 (Theorem 6.3). Let now $\mathrm{Cyc}(\mathrm{Aut}(W)) \neq \emptyset$. Then at each iteration of Step 2 $\mathrm{Aut}(W')$ is a well-embedded subgroup of $\mathrm{Aut}(W)$ by Theorem 4.4 and hence W' is a homogeneous ring with $\mathcal{E}_0(W') = \mathcal{E}(W')$ (see the beginning of the section). So at Step 3 $\mathrm{Aut}(W)$ is a well-embedded subgroup of the automorphism group of the input ring (equal to $\mathrm{Aut}(W_0)$). On the other hand, the ring W at the same step is not singular. Thus from Theorem 5.1 it follows that the ring W is quasinormal. By Theorem 3.6 this implies that the group G found at Step 3 is a well-embedded subgroup of $\mathrm{Aut}(W)$ and hence of $\mathrm{Aut}(W_0)$. This means that every cycle base of G contains a cycle base of the input ring. Therefore again the correctness of the algorithm follows from that of Algorithm A3 (Theorem 6.3).

Let us estimate the running time of the algorithm. First we observe that the number of iterations at Step 2 is at most n by Theorem 4.4. So this step can be done in time $n^{O(1)}$ by the same theorem and the remark in the beginning of the section. Thus the required time bound follows from Theorems 3.6 and 6.3, the remark in the beginning of Subsection 6.2 and the fact that the group $\mathrm{Aut}(W_0)$ at Step 4 is obviously $n^{O(1)}$-recognizable.∎

8 Appendix

In this section we cite the background on cellular rings, Schur rings and related algorithms. The notions of a cellular ring and a Schur ring go back to [12, 26] and [25, 28] respectively. Below we follow [11].

8.1. Cellular rings. A subring W of Mat_V is called a *cellular ring* on V if it has a (uniquely determined) $\mathbb{Z}$-base consisting of {0,1}-matrices $A(R)$ where R runs over a family $\mathcal{R} = \mathcal{R}(W)$ of pairwise disjoint nonempty relations on V such that

$$\Delta(V) \in \mathcal{R}^*, \quad \bigcup_{R\in\mathcal{R}} R = V^2 \quad \text{and} \quad R \in \mathcal{R} \Rightarrow R^T \in \mathcal{R}$$

where $\mathcal{R}^* = \mathcal{R}^*(W)$ is the set of all unions of the elements of $\mathcal{R}$. The elements of V and $\mathcal{R}$ are called the *points* and the *basis relations* of W respectively; the numbers $\deg(W) = |V|$ and $\mathrm{rk}(W) = |\mathcal{R}|$ are called the *degree* and the *rank* of W. The ring W is called *homogeneous* if $\Delta(V) \in \mathcal{R}$. In this case each basis relation can be treated as the set of arcs of a regular digraph on V. Every commutative cellular ring is homogeneous. The set of all equivalences on V belonging to $\mathcal{R}^*$ is denoted by $\mathcal{E} = \mathcal{E}(W)$; the set of all classes of all of them is denoted by $\mathcal{B} = \mathcal{B}(W)$. Obviously, $\Delta(V), V^2 \in \mathcal{E}$. A homogeneous ring W is called *primitive* if $\deg(W) > 1$ and $\mathcal{E} = \{\Delta(V), V^2\}$.

Cellular rings W on V and W' on V' are called *strongly isomorphic* if $W^f = W'$ for some bijection $f : V \to V'$ called a *strong isomorphism* from W to W'. If $W = W'$, then the group of all of them contains a normal subgroup

$$\mathrm{Aut}(W) = \{f \in \mathrm{Sym}(V) :\ A^f = A,\ A \in W\}$$

called the *automorphism group* of W. The rings W and W' are called *weakly isomorphic* if there exists a $\mathbb{Z}$-module isomorphism $\varphi : W \to W'$ preserving both the matrix and Hadamard (componentwise) multiplications. Any such isomorphism is called a *weak isomorphism* from W to W'. From [9, Lemma 2.2] it follows that φ induces a bijection from $\mathcal{R}^*(W)$ onto $\mathcal{R}^*(W')$, $R \mapsto R^\varphi$, such that $\varphi(A(R)) = A(R^\varphi)$. Moreover, this bijection maps $\mathcal{R}(W)$ onto $\mathcal{R}(W')$ and $\mathcal{E}(W)$ onto $\mathcal{E}(W')$ with $(R^\varphi)^T = (R^T)^\varphi$ and $|R| = |R^\varphi|$ for all $R \in \mathcal{R}^*(W)$. Each strong isomorphism from W to W' induces a weak isomorphism between these rings. For a weak isomorphism $\varphi : W \to W'$ we set

$$\mathrm{Iso}(W, W', \varphi) = \{f \in \mathrm{Iso}(W, W') :\ \varphi_f = \varphi\}$$

where $\mathrm{Iso}(W, W')$ is the set of all strong isomorphisms from W to W' and φ_f is the weak isomorphism induced by f. In particular, $\mathrm{Iso}(W, W', \mathrm{id}_W) = \mathrm{Aut}(W)$.

Let W be a homogeneous ring on V and $X \in \mathcal{B}$, $E \in \mathcal{E}$. Then the submodule W_X of Mat_X spanned by the matrices $A(R_X)$, $R \in \mathcal{R}$, is a cellular ring on X (see [11]) and the submodule W/E of $\mathrm{Mat}_{V/E}$ spanned by the matrices $A(R_{V/E})$, $R \in \mathcal{R}$, is a cellular ring on V/E (see [7, Section 2.2]). We observe that $E_X \in \mathcal{E}(W_X)$, $X/E \in \mathcal{B}(W/E)$ and $W_X/E_X = (W/E)_{X/E}$. The latter cellular ring on X/E is denoted by $W_{X/E}$. One can see that

$$\mathcal{R}(W_{X/E}) = \{R_{X/E} :\ R \in \mathcal{R},\ R \cap X^2 \neq \emptyset\}. \tag{23}$$

It is easy to see that the ring $W_{X/E}$ is homogeneous, and it is commutative whenever W is. The following statement is a special case of [8, Lemma 2.6].

Lemma 8.1 *Let W be a homogeneous cellular ring on V and $E \in \mathcal{E}(W)$. Then given $X, Y \in V/E$ there exists a uniquely determined weak isomorphism $\varphi_{X,Y} : W_X \to W_Y$ taking $A(R_X)$ to $A(R_Y)$ for all $R \in \mathcal{R}(W)$. In particular, $|X| = |Y|$.* ■

If W_1 and W_2 are cellular rings on V_1 and V_2 respectively, then the subring $W_1 \otimes W_2$ of the ring $\mathrm{Mat}_{V_1} \times \mathrm{Mat}_{V_2} = \mathrm{Mat}_{V_1 \times V_2}$ is a cellular ring on $V_1 \times V_2$ with

$$\mathcal{R}(W_1 \otimes W_2) = \{R_1 \otimes R_2 :\ R_1 \in \mathcal{R}(W_1),\ R_2 \in \mathcal{R}(W_2)\}$$

where $R_1 \otimes R_2 = \{((u_1,u_2),(v_1,v_2)) :\ (u_1,v_1) \in R_1,\ (u_2,v_2) \in R_2\}$. It is called the *tensor product* of W_1 and W_2. Obviously, $\mathrm{Aut}(W_1 \otimes W_2) = \mathrm{Aut}(W_1) \times \mathrm{Aut}(W_2)$.

The set of all cellular rings on V is partially ordered by inclusion and closed under intersection. The largest and the smallest elements of this set are respectively the full matrix ring Mat_V and the ring with $\mathbb{Z}$-base $\{I_V, J_V\}$. We write $W \le W'$ and call W' an *extension* of W if $W \subset W'$. Given subsets $\mathcal{M}_1,\ldots,\mathcal{M}_s$ of Mat_V, their *cellular closure*, i.e. the smallest cellular ring on V containing all of them is denoted by $[\mathcal{M}_1,\ldots,\mathcal{M}_s]$. If $\mathcal{M}_i = \{A_i\}$, we omit the braces.

8.2. S-rings and Cayley rings. Let G be a finite group. A subring $\mathcal{A}$ of the group ring $\mathbb{Z}[G]$ is called a *Schur ring* (briefly *S-ring*) over G if it has a (uniquely determined) $\mathbb{Z}$-base consisting of elements $\xi(X) = \sum_{x\in X} x$ where X runs over a family $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of pairwise disjoint nonempty subsets of G such that

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X\in\mathcal{S}} X = G \quad \textit{and} \quad X \in \mathcal{S} \ \Rightarrow\ X^{-1} \in \mathcal{S}.$$

We call the elements of $\mathcal{S}$ *basic* sets of $\mathcal{A}$ and denote by $\mathcal{S}^*(\mathcal{A})$ the set of all unions of them and by $\mathcal{H}(\mathcal{A})$ the set of all subgroups of G belonging to $\mathcal{S}^*(\mathcal{A})$. The number $\mathrm{rk}(\mathcal{A}) = \dim_{\mathbb{Z}}(\mathcal{A})$ is called the *rank* of $\mathcal{A}$.

Let $H, K \in \mathcal{H}(\mathcal{A})$, K a normal subgroup of H, and $i : H \to G$ and $\pi : H \to H/K$ natural homomorphisms. Then the ring $\mathcal{A}_{H/K} = \pi(i^{-1}(\mathcal{A}))$ is an S-ring over the group H/K with

$$\mathcal{S}(\mathcal{A}_{H/K}) = \{\pi(X) :\ X \in \mathcal{S}(\mathcal{A}),\ X \subset H\}$$

(we save notation i and π also for the induced homomorphisms of the corresponding group rings).

If $\mathcal{A}_1$ and $\mathcal{A}_2$ are S-rings over groups G_1 and G_2 respectively, then the subring $\mathcal{A}_1 \otimes \mathcal{A}_2$ of the ring $\mathbb{Z}[G_1] \times \mathbb{Z}[G_2] = \mathbb{Z}[G_1 \times G_2]$ is an S-ring over the group $G_1 \times G_2$ with

$$\mathcal{S}(\mathcal{A}_1 \otimes \mathcal{A}_2) = \{X_1 \times X_2 :\ X_1 \in \mathcal{S}(\mathcal{A}_1),\ X_2 \in \mathcal{S}(\mathcal{A}_2)\}.$$

It is called the *tensor product* of $\mathcal{A}_1$ and $\mathcal{A}_2$.

For $g \in G$ denote by P_g the permutation matrix corresponding to the left multiplication by g. Then the mapping

$$\rho_G : \mathbb{Z}[G] \to \mathrm{Mat}_G, \qquad g \mapsto P_g, \tag{24}$$

is a ring monomorphism the image of which is the enveloping ring of the group G_{left}. This monomorphism induces a bijection $X \mapsto X^{\rho_G}$ between the subsets of G and the G_{right}-invariant relations on G such that $A(X^{\rho_G}) = \rho_G(\xi(X))$ for all X. If $\mathcal{A}$ is an S-ring over G, then $W = \mathcal{A}^{\rho_G}$ is a cellular ring on G for which $G_{right} \le \mathrm{Aut}(W)$. Any such cellular ring is called a *Cayley ring* over G. It is always homogeneous, and it is commutative whenever G is. The following statement can be found in [11].

Theorem 8.2 *The mapping (24) defines a bijection $\mathcal{A} \mapsto W$ between the S-rings over G and the Cayley rings over G. Moreover, $\mathcal{S}(\mathcal{A})^{\rho_G} = \mathcal{R}(W)$, $\mathcal{S}^*(\mathcal{A})^{\rho_G} = \mathcal{R}^*(W)$, $\mathcal{H}(\mathcal{A})^{\rho_G} = \mathcal{E}(W)$, and for $H, K \in \mathcal{H}(\mathcal{A})$ with K normal in H, we have $G/E = \{Hg :\ g \in G\}$ and $\rho_{H/K}(\mathcal{A}_{H/K}) = W_{H/E'}$ where $E = H^{\rho_G}$ and $E' = K^{\rho_G}$.* ■

Given $X \subset G$ the group $\mathrm{rad}(X) = \{g \in G : \ gX = Xg = X\}$ is called the *radical* of X. It is the largest subgroup of G such that X is a union of the left as well as right cosets by this subgroup. If $\mathrm{rad}(X)$ is normal in G, then the image of X under the natural epimorphism from G to $G/\mathrm{rad}(X)$ has trivial radical. If $X \in \mathcal{S}^*(\mathcal{A})$ where $\mathcal{A}$ is an S-ring over G, then $\mathrm{rad}(X) \in \mathcal{H}(\mathcal{A})$. If $H, K \in \mathcal{H}(\mathcal{A})$ and $K \leq H$, then we say that $\mathcal{A}$ satisfies the *H/K-condition* if $K \leq \mathrm{rad}(X)$ for all $X \in \mathcal{S}(\mathcal{A})$ with $X \subset G \setminus H$.

8.3. Algorithmic tools. A cellular ring W on n points will be always given by the set of basis relations (or their adjacency matrices). In this representation in time $n^{O(1)}$ one can test its homogeneity, commutativity and primitivity, and given $X \in \mathcal{B}(W)$ and $E \in \mathcal{E}(W)$ construct the cellular ring $W_{X/E}$. As for the cellular closure of a set of matrices we observe that historically the first method of finding it was described in [26] and in more details in [27] where in fact the following statement was proved.

Theorem 8.3 *Given a finite set $\mathcal{M} \subset \mathrm{Mat}_V$, the basis relations of the cellular closure of $\mathcal{M}$ can be found in time $mn^{O(1)}$ where $m = |\mathcal{M}|$ and $n = |V|$. Moreover, if $\varphi : \mathcal{M} \to \mathcal{M}'$ is a bijection where $\mathcal{M}' \subset \mathrm{Mat}_{V'}$, then within the same time one can test whether there exists a weak isomorphism from this ring onto the cellular closure of $\mathcal{M}'$ that coincides with φ on $\mathcal{M}$, and find it if it does exist.*■

The permutation group algorithms used in this paper are standard and mostly are based on the sift procedure (for details see [16]). Here we only make some remarks. A permutation group G on n points will be always given by a strong generating set (of at most n^2 generators). In this representation one can test the membership in G and find the order of G in time $n^{O(1)}$. Moreover, within the same time one can find any $n^{O(1)}$-recognizable subgroup of G of index at most n^c where $c > 0$, and consequently any permutation group $G_{X/E} = \{g_{X/E} : \ g \in G, \ X^g = X\}$ and the setwise stabilizer of X in G where E is a G-invariant equivalence and X is a block of G. If K is a permutation group on the same set as G, then the normal closure of G with respect to K can also be found in time $n^{O(1)}$. Finally, the following statement to be used in Section 3 is a special case of [1, Corollary 3.6].

Theorem 8.4 *Let $G \leq \mathrm{Sym}(V)$ be a solvable group. Then given a cellular ring $W \leq \mathrm{Mat}_V$ the group $\mathrm{Aut}(W) \cap G$ can be found in time $n^{O(1)}$ where $n = |V|$.*■

References

[1] L. Babai, and E. M. Luks, *Canonical labeling of graphs*, Proc. 15th ACM STOC, (1983), 171–183.

[2] G. Birkhoff, *Lattice Theory*, Providence, Rhode Island, 1967.

[3] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer, Berlin, 1989.

[4] J. D. Dixon, B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, No. 163, Springer-Verlag New York, 1996.

[5] S. Evdokimov, M. E. Muzychuk, I. Ponomarenko, G. Tinhofer, *Recognizing Certain Cayley Graphs in Polynomial Time*, 2003, submitted to Electronic Journal of Combinatorics.

[6] S. Evdokimov, I. Ponomarenko, *Two inequalities for the parameters of a cellular algebra*, Zapiski Nauchnykh Seminarov POMI, **240** (1997), 82–95.

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

[8] S. Evdokimov, M. Karpinski, I. Ponomarenko, *On a New High Dimensional Weisfeiler-Leman Algorithm*, Journal of Algebraic Combinatorics, **10** (1999), 29–45.

[9] S. Evdokimov, I. Ponomarenko, *Separability Number and Schurity Number of Coherent Configurations*, Electronic Journal of Combinatorics, **7** (2000), #R31.

[10] S. Evdokimov, I. Ponomarenko, *On a family of Schur rings over a finite cyclic group*, Algebra and Analysis, **13** (2001), 3, 139–154.

[11] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra and Analysis, **14** (2002), 2, 11–55.

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

[13] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups, II*, J. Algebra, **183** (1996), 273–285.

[14] C. H. Li, *On isomorphisms of finite Cayley graphs – a survey*, Discrete Mathematics, **256** (2002), 301–334.

[15] A. Lubiw, *Some NP-complete problems similar to graph isomorphism*, SIAM J. Comput., **10** (1981), 11–21.

[16] E. M. Luks, *Permutation groups and polynomial-time computation*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **11** (1993), 139–175.

[17] Muzychuk M. E., *On the structure of basic sets of Schur rings over cyclic groups*, J. Algebra, **169** (1994), 655-678.

[18] M. Muzychuk, *Ádám's conjecture is true in the square-free case*, J. Combin. Theory Ser. A, **72** (1995), 118–134.

[19] M. Muzychuk, *On the isomorphism problem for cyclic combinatorial objects*, Discr. Math., **197/198** (1999), 589–606.

[20] M. Muzychuk, M. Klin, R. Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, **56** (2001), 241–264.

[21] M. E. Muzychuk, G. Tinhofer, *Recognizing circulant graphs of prime order in polynomial time*, Electronic J. of Combinatorics, **5** (1998), #R25.

[22] M. E. Muzychuk, G. Tinhofer, *Recognizing circulant graphs in polynomial time: An application of association schemes*, Electronic J. of Combinatorics, **8**, (2001), #R26.

[23] P. P. Palfy, *A polynomial bound for the orders of primitive solvable groups*, J. Algebra, **77** (1982), 127–137.

[24] I. Ponomarenko, *Polynomial-time algorithms for recognizing and isomorphism testing of cyclic tournaments*, Acta Appl. Math., **29** (1992), 139–160.

[25] I. Schur, *Zür Theorie der einfach transitiven Permutationgruppen*, S.-B. Preus Akad. Wiss. Phys.-Math. Kl., (1933), 598–623.

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

[27] B. Weisfeiler (editor), *On construction and identification of graphs*, Springer Lecture Notes, 558, 1976.

[28] H. Wielandt, *Finite permutation groups*, Academic press, New York - London, 1964.

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