Алгебра и анализ
Том. 15 (2003), вып. 6

St. Petersburg Math. J.
Vol. 15 (2004), No. 6, Pages 813–835
S 1061-0022(04)00833-7
Article electronically published on November 16, 2004

CIRCULANT GRAPHS: RECOGNIZING AND ISOMORPHISM TESTING IN POLYNOMIAL TIME

S. A. EVDOKIMOV AND I. N. PONOMARENKO

Abstract. An algorithm is constructed for recognizing the circulant graphs and finding a canonical labeling for them in polynomial time. This algorithm also yields a cycle base of an arbitrary solvable permutation group. The consistency of the algorithm is based on a new result on the structure of Schur rings over a finite cyclic group.

§1. Introduction

A finite graph[1] is said to be *circulant* if its automorphism group contains a full cycle,[2] 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, is isomorphic to a Cayley graph over a cyclic group. In particular, any circulant graph can be specified in a compact form by a full cycle automorphism and a neighborhood of some vertex.

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 or not a given graph has an automorphism without fixed points [15].) The first attempt to solve this problem was undertaken in [24], where a polynomial-time algorithm for recognizing circulant tournaments was described. In the subsequent papers [21, 22, 5] several results on recognizing some special classes of circulant graphs were presented, but the general problem remained open up to now. In the present paper we solve this problem completely. 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 for circulant graphs.[3] 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 through the last forty years (see [20]). Most

2000 *Mathematics Subject Classification.* Primary 5C25, 20F65.

Key words and phrases. Regular cycle automorphism group, Cayley graph, polynomial-time algorithm.

Supported by RFBR (grants nos. 01-01-00219 and 03-01-00349). The second author was supported by RFBR, grants nos. 02-01-00093 and NSh-2251.2003.1.

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

[2] In what follows, such an automorphism is said to be *cycle*.

[3] Suppose that associated with each graph belonging to a class $\mathcal{C}$ is a labeling, i.e., a bijection from the set of vertices to an initial interval of the set of nonnegative integers. This labeling is said to be *canonical* provided $\Gamma_1 \cong \Gamma_2$ if and only if $\Gamma_1^{f_1} = \Gamma_2^{f_2}$ for all $\Gamma_1, \Gamma_2 \in \mathcal{C}$, where f_i is the labeling of the graph Γ_i and $\Gamma_i^{f_i}$ is the image of Γ_i under f_i, $i = 1, 2$ (cf. [1]).

papers were aimed at finding efficient necessary and sufficient conditions for isomorphism of Cayley graphs over various special classes of cyclic groups.

The key notion of our approach is a *cycle base* of a finite permutation group G; by definition, this is any set of full cycles in G with the property 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 $\varphi(n)$, where φ is the Euler function, modulo the classification of finite simple groups) where n is the degree of G. A *cycle base of a graph* Γ is defined to be a cycle base of its automorphism group $\mathrm{Aut}(\Gamma)$. As will be shown below (see Theorem 1.2), the problems treated in this paper are reduced efficiently to the problem of finding a cycle base of a graph. In its turn, this problem reduces (see the proof of Theorem 1.1) to a similar problem for cellular rings, and the solution of the latter occupies most of the paper (as to the 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, and let W be the smallest cellular ring containing the adjacency matrix of the graph Γ. It is easy to show 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 by Γ (see Theorem 8.3), we are done. □

The following statement contains the main results of the paper. Though some parts of the proof are folklore, we present all the details in order to make the exposition self-contained.

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

(1) *given a graph $\Gamma \in \mathcal{G}_n$, test whether $\Gamma \in \mathcal{C}_n$, and (if so) find a cycle automorphism of it;*
(2) *given a graph $\Gamma \in \mathcal{C}_n$, find a canonical labeling of it;*
(3) *given graphs $\Gamma, \Gamma' \in \mathcal{C}_n$, test whether $\Gamma \cong \Gamma'$, and (if so) find an isomorphism of them;*
(4) *given a graph $\Gamma \in \mathcal{G}_n$, find a full system of pairwise nonequivalent Cayley representations[4] 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. Therefore, Problem (1) can be solved in time $n^{O(1)}$ by Theorem 1.1. Furthermore, Problem (3) is $O(n)$-reducible to Problem (2). We concentrate on Problems (2) and (4).

Let V be a set of cardinality n. For any full cycle c on V and any element $v \in V$, there exists a unique bijection $f : V \to \{0, \dots, n-1\}$ taking v^{c^i} to i (then c goes to the full 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 Γ under f does not depend on the choice of $v \in V$; we denote it by $\Gamma^{(c)}$. It is easily seen that for any two cycle automorphisms c_1 and c_2 of Γ we have

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

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 $n^{O(1)}$.

[4] 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 said to be equivalent if some isomorphism of the corresponding Cayley graphs belongs to $\mathrm{Aut}(G)$ (see, e.g., [14]).

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

$$\Gamma_1 \cong \Gamma_2 \iff \Gamma_1^{f_1} = \Gamma_2^{f_2}$$

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 $\Gamma \in \mathcal{G}_n$. We treat the set $\{0, \ldots, n-1\}$ of the vertices of the graphs in $\mathcal{C}(\Gamma)$ as the additive group $\mathbb{Z}_n^+$ of the ring $\mathbb{Z}_n = \mathbb{Z}/(n)$. It is easily seen that each graph in $\mathcal{C}(\Gamma)$ 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 the set $\mathcal{C}(\Gamma)$. On the other hand, two elements of $\mathcal{C}(\Gamma)$ are equivalent if and only if there exists an isomorphism between them induced by multiplication 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. □

As we saw in the proof of Theorem 1.1, the problem of finding a cycle base of a graph reduces to the problem of finding a cycle base of a cellular ring, i.e., a cycle base of its automorphism group. To approach the latter problem, we introduce the classes of *quasinormal* and *singular* cellular rings (see §§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 classes are efficiently recognizable. Moreover, the automorphism group of a quasinormal ring has a polynomial-time computable solvable subgroup containing all 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 said to be admissible if it is proper and each of its cycle bases contains a cycle base of the ring.) In a sense, a quasinormal ring can be thought of as a ring covered by normal Cayley rings over cyclic groups (see Definition 3.2). The latter rings 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 has 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, thereby resolving the singularity. Now the algorithm of finding a cycle base of a cellular ring (Main Algorithm) can be outlined as follows (see §7 for the details).

1. While a current ring remains singular, replace it by an admissible extension.
2. If the current ring is not quasinormal, then the cycle base of the input ring is empty.
3. Find a solvable subgroup G of the automorphism group of the 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 (§4), which involves, in particular, the Weisfeiler–Leman algorithm (Subsection 8.3). Steps 2 and 3 are performed by Algorithm A1 (§3). At the first stage of that algorithm we test whether or not the current ring is quasinormal, and if it is, we find a solvable group containing all cycle automorphisms of the current ring. At the second stage we apply the Babai–Luks algorithm to find the group G in question as the intersection of the group mentioned in the preceding sentence and the automorphism group of the current ring. Finally, Step 4 is performed by Algorithm A3 (§6). This algorithm allows us to efficiently find a cycle base of an arbitrary solvable permutation group. The consistency 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 all results concerning permutation groups to be used in the sequel can be found in [28, 29, 4]. To make the paper self-contained, we collect the background material on cellular rings and Schur rings in §8. That section also contains some remarks on algorithms for such rings and for permutation groups.

Notation. As usual, we denote by $\mathbb{Z}$ 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 a usual equivalence relation on V; the set of all such equivalences is denoted by $\mathcal{E}(V)$. 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 put

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

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

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

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

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 we set $\mathrm{Cyc}(V) = \mathrm{Cyc}(\mathrm{Sym}(V))$.

Each bijection $f : V \to V'$ $(v \mapsto v^f)$ naturally determines 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 (respectively, right) multiplications is denoted by G_{left} (respectively, G_{right}).

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

§2. Equivalences in homogeneous cellular rings

This section is of preliminary nature. The material presented here will be used throughout the paper. The relations R on V to be dealt with are assumed to have full support (i.e., $R(v) \cup R^T(v) \neq \varnothing$ for all $v \in V$). Below we fix a homogeneous cellular ring $W \leq \mathrm{Mat}_V$, and we 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. We 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 precisely the connected components of the graph on V with the edge set $R \cup R^T$, so that $\langle R \rangle$ can be constructed efficiently. 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 and 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 $\mathcal{E}$ 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. Therefore, this set has the largest element. We call it the *radical* of R and denote by $\operatorname{rad}(R)$. Obviously, $\operatorname{rad}(R) \subset \langle R\rangle$. Furthermore,

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

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

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

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

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 ($i = 1, 2$ for (5) and $i = 2$ for (6)).

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. For this, we observe that the injectivity follows from the first relation in (4). On the other hand, the second relation 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, obviously, such a path can be chosen to be of length not exceeding 2. This means that $X_1 \cap X_2 \neq \varnothing$ 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 where $E_1, E_2 \in \mathcal{E}$.

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

1) $W^f \geq W_{V/E_1} \otimes W_{V/E_2}$;
2) *if $X_1 \in V/E_1$, then $t_{X_1} \in \operatorname{Iso}(W_{X_1}, W_{V/E_2})$ and $(R_{X_1})^{t_{X_1}} = R_{V/E_2}$ for all $R \in \mathcal{R}$, $R \subset E_1$;*
3) *$t_{X_1,Y_1} \in \operatorname{Iso}(W_{X_1}, W_{Y_1}, \varphi_{X_1,Y_1})$ 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 described in Lemma* 8.1.

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

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

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 from these inclusions. Next, let $R \in \mathcal{R}$, $R \subset E_1$. Then, obviously, $(R_{X_1})^{t_{X_1}} \subset R_{V/E_2}$. Therefore, it suffices to prove the first part of statement 2) only. 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 $R \cap (X_2 \times Y_2) \neq \varnothing$. Thus, for each $X_1 \in V/E_1$ the bijection t_{X_1} induces a bijection $\mathcal{R}(W_{X_1}) \to \mathcal{R}(W_{V/E_2})$, whence $t_{X_1} \in \mathrm{Iso}(W_{X_1}, W_{V/E_2})$. Finally, statement 3) follows from statement 2) and the definition of φ_{X_1,Y_1}. □

Corollary 2.3. *Under 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*

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

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 $g \in \mathrm{Aut}(W)$. Therefore, $G^f \leq G_{V/E_1} \times G_{V/E_2}$. 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

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

and the first relation follows. Since, obviously, $(X_1, v^{t_{X_1}}) = v^f$ for all $v \in X_1$, the second relation is a consequence of the first. □

2.3. Suppose $E_0, E_1 \in \mathcal{E}$ and $E_0 \subset E_1$. We intend to compute the group $\mathrm{Aut}(W)$ in the case where 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 $R \in \mathcal{R}$ such that $R \cap E_1 = \varnothing$.

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 said to be 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 unique permutation of V equal to g_0 on V/E_0 and to g_X on any $X \in V/E_1$. We say that this permutation is *induced* by the pair $(\{g_X\}_{X\in V/E_1}, g_0)$.

We say that an E_1/E_0-admissible pair is *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) $g_0 \in \mathrm{Aut}(W_{V/E_0})$.

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

Theorem 2.5. *Suppose the ring* W *satisfies 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),

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

where $Y = X^g$. Otherwise, we have $R \cap E_1 = \varnothing$, whence $E_0 \subset \mathrm{rad}(R)$ by the conditions of the theorem (see Definition 2.4). Consequently, relation (2) and condition (P2) imply that

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

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 said to be *normal* if G_{right} is a normal subgroup of $\mathrm{Aut}(W)$. We denote by $\mathcal{W}_{\mathrm{norm}}$ the class of all cellular rings strongly isomorphic to a normal Cayley ring over a cyclic group. It is easily seen that a cellular ring belongs to $\mathcal{W}_{\mathrm{norm}}$ if and only if its automorphism group contains a normal regular cyclic subgroup. Any element of $\mathcal{W}_{\mathrm{norm}}$ is called a *normal* ring (over a cyclic group). It can be proved 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, this automorphism group 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 allows us to handle normal rings efficiently (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 $W \in \mathcal{W}_{\mathrm{norm}}$, and (if so) list all elements of the group* $\mathrm{Aut}(W)$;
(2) *given cellular rings $W, W' \in \mathcal{W}_{\mathrm{norm}}$ 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 said to be 1-regular if there exists a regular point, i.e., an element v of V such that $|R(v)| \le 1$ for all $R \in \mathcal{R}(W)$ (see [11, §9]). Next, obviously, if $\varphi : W \to W'$ is a weak isomorphism of cellular rings, then

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

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

Suppose $W \le \mathrm{Mat}_V$ is a cellular ring and $v \in V$. We 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 $v' \in V'$ such that the isomorphism $\varphi_{v,v'}$ does exist. Now, if $W, W' \in \mathcal{W}_{\mathrm{norm}}$, 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 previous paragraph and Theorem 8.3, Problem (2) 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 listed efficiently whenever the ring W_v is 1-regular for all $v \in V$. Since the latter condition is satisfied for any $W \in \mathcal{W}_{\mathrm{norm}}$, we see that Problem (1) is $n^{O(1)}$-reducible to the recognition problem for 1-regular rings. □

3.2. Let $W \leq \mathrm{Mat}_V$ 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 element F of the set $\mathcal{F}(W)$ is called a *flag* of W and will be denoted 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. Therefore, the numbers $|X/E_0|$ and $\mathrm{rk}(W_{X/E_0})$ do not depend on the choice of $X \in V/E_1$; we denote them by $|F|$ and $\mathrm{rk}(W_F)$, respectively. Moreover, 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 said to be *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,

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

for $X \in V/E_1$ 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. 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 $G \leq \mathrm{Aut}(W)$ is a regular cyclic group and $X \in V/E_3$, then, obviously, G_{X/E_0} is a regular cyclic subgroup of $\mathrm{Aut}(W_{X/E_0})$. Applying Corollary 2.3 to the ring W_{X/E_0} and the equivalences $(E_1)_{X/E_0}$ and $(E_2)_{X/E_0}$, we see 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 $\mathcal{F}(W)$. It can be checked that the set $\mathcal{E}(W)$ forms a modular lattice with respect to the operations of intersection and the equivalence closure of a union. Thus, the $\sim$-equivalence corresponds to the projectivity in a modular lattice [2].

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

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

Before stating the main result of the subsection, we need the following technical notion. Let $W \leq \mathrm{Mat}_V$ be a homogeneous cellular ring. By a *majorant* of a group $G \leq \mathrm{Aut}(W)$ 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 $(G_{X/E_0})^{f_X} \le G'$. If $E_0 = \Delta(V)$ and $E_1 = V^2$, then we call G' simply a majorant of G.

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

Proof. We deduce the theorem from the following two lemmas. Below for permutation groups $G_1, \dots, G_s$, $s \ge 0$, we define a permutation group $\mathrm{wr}(G_1, \dots, G_s)$ as follows: this group is $\{1\}$ if $s = 0$; it coincides with G_1 if $s = 1$; with the wreath product of G_1 and G_2 (in imprimitive action) if $s = 2$; and with $\mathrm{wr}(\mathrm{wr}(G_1, \dots, G_{s-1}), G_s)$ if $s \ge 3$.

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

1) $\Delta(V) = E_0 \subset E_1 \subset \cdots \subset E_s = V^2$;
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

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

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

Proof. It is easily seen that $\mathfrak{f}$ is a surjection. Thus, statement 1) follows from the relation $|V| = |E_s/E_0| = \prod_{i=1}^{s} |E_i/E_{i-1}|$. 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

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

On the other hand,

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

(we have used the fact that $V/E_s = \{V\}$). Moreover, it is easy to check 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 deduce that $G^{\mathfrak{f}} \le \mathrm{wr}(\mathrm{wr}(G_1, \dots, G_{s-1}), G_s) = \mathrm{wr}(G_1, \dots, G_s)$. □

Lemma 3.5. *If W is a quasinormal ring, then the group $\mathrm{Aut}_{\mathrm{Cyc}}(W)$ admits a solvable majorant 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 $F_i = E_{i,1}/E_{i,0}$, $i \in [0, s]$, 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 $\mathrm{Aut}_{\mathrm{Cyc}}(W)$ 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, there is no loss of generality in assuming that the flag $F = E_1/E_0$ is subnormal, i.e., it is a subflag of a normal flag $F' = E_1'/E_0'$ of W. For $X, Y \in V/E_1$, we denote by X', Y' the classes of the equivalence E_1' containing X and Y (respectively) and put $\overline{X}' = X'/E_0'$, $\overline{Y}' = Y'/E_0'$. Since $W_{\overline{X}'}, W_{\overline{Y}'} \in \mathcal{W}_{\mathrm{norm}}$, there exists $f \in \mathrm{Iso}(W_{\overline{X}'}, W_{\overline{Y}'}, \varphi_{\overline{X}', \overline{Y}'})$ that takes

X/E'_0 to Y/E'_0 (see Subsection 3.1), where $\varphi_{\overline{X'},\overline{Y'}}$ is the weak isomorphism described in Lemma 8.1. Consequently,

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

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 $\mathrm{Aut}_{\mathrm{Cyc}}(W)$) 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. □

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

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

Let W be a commutative cellular ring on n points. We denote by Γ the graph constructed on the set of all primitive flags of W and such that two vertices of Γ are adjacent if and only if 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 found efficiently, it is not hard to test in time $n^{O(1)}$ whether or not two given vertices of Γ are adjacent. 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 if and only if the corresponding vertices of Γ are joined by a path. It is well known that the connected components of a graph and a path joining any two vertices of a connected graph can be found efficiently. Thus, given two primitive flags of W, we can test whether or not 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 $n^{O(1)}$. Therefore, given a primitive flag of W, we can test in time $m^2 n^{O(1)}$ whether it is subnormal by the exhaustive 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 $\mathrm{Aut}_{\mathrm{Cyc}}(W)$ with respect to any given primitive quasinormal flag of W can be found in time $(mn)^{O(1)}$.

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

Step 1. If W is not commutative, then the output G is empty. 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 the output G is empty. Otherwise choose a maximal path $\Delta(V) = E_0 \subset E_1 \subset \cdots \subset E_s = V^2$ of equivalences of W.

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

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

Theorem 3.6. *Algorithm* A1 *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, then it finds a solvable group G such that* $\mathrm{Aut}_{cyc}(W) \leq G \leq \mathrm{Aut}(W)$ *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 if and only if the algorithm terminates before Step 3. This implies that the flags E_i/E_{i-1} $(i \in [s])$ (which, obviously, are primitive) are quasinormal. Moreover, the group G' defined at Step 3 is solvable because it is a wreath product of solvable groups. Thus, the consistency of the algorithm follows from Lemma 3.4 (which implies that $\mathrm{Aut}_{\mathrm{Cyc}}(W)^{\mathfrak{f}} \leq G'$), and from the consistency 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 will be shown below (see Theorem 5.1), every cellular ring admitting a cycle automorphism is quasinormal or has a singularity in the following sense.

Let $W \leq \mathrm{Mat}_V$ be a commutative cellular ring, and let $F = E_1/E_0$ and $F' = E_3/E_2$ be 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 the bijection (5) in 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 said to be *singular* if it has singularity of degree $d \geq 3$ in some pair (F, F').

We shall resolve the singularity by replacing W with the smallest cellular ring $W' = [W, A]$ that contains W, A being the adjacency matrix of a relation of the form

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

where $\mathfrak{F} = \{f_X\}_{X \in V/E_3}$ with $f_X \in \mathrm{Cyc}(X/E_2)$. The next theorem shows that in this case we can control the cycle bases of the rings W and W'. As in [19], we say that a subgroup G' of a permutation group G is *well embedded* 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 $W' \geq W$, without loss of generality we may assume that $\mathrm{Cyc}(\mathrm{Aut}(W)) \neq \varnothing$. Let g be a cycle automorphism of W. Then $(E_3)^g = E_3$, so that $X^{g^k} = X$ 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. Therefore, we can find a permutation $h_X \in \mathrm{Sym}(X/E_2)$ such that $f_X = h_X^{-1}\widetilde{g}_X h_X$. Suppose for a while that there exists $h^* \in \mathrm{Aut}(W)$ such that

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

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

$$\begin{aligned}(Y^{f_X})^{g'} &= (Y^{f_X})^{(h^*)^{-1}gh^*} = (Y^{f_X h_X^{-1}})^{gh^*} = (Y^{h_X^{-1}\widetilde{g}_X})^{gh^*}\\ &= ((Y^{h_X^{-1}})^g)^{\widetilde{g}_{X^g} h_{X^g}} = ((Y^{h_X^{-1}})^g)^{h_{X^g} f_{X^g}} = (Y^{(h^*)^{-1}gh^*})^{f_{X^g}}\\ &= (Y^{g'})^{f_{X^g}},\end{aligned}$$

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

Now we prove the existence of $h^* \in \mathrm{Aut}(W)$ satisfying (13). For this, we observe that the permutation g^l with $l = |V/E_1|$ 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 $Y' = Y^{h_X}$. Obviously, the induced bijection $h_Y : Y \to Y'$ satisfies the following conditions:

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

where $\varphi_{Y,Y'}$ is the weak isomorphism described in 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 next lemma.

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 unique $h^* \in \mathrm{Aut}(W)$ 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 third condition imposed on it. To prove the existence, we take $X \in V/E_3$ and 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 assumption. 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, we 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. Then $h'_X \in \mathrm{Aut}(W_X)$ by Theorem 2.5. Moreover, since $(h'_X)_{X/E_1} = \widetilde{h}_X$, we have $(h'_X)_{X/E_1} = \mathrm{id}_{X/E_1}$. Thus, the pair $(\{h'_X\}, \mathrm{id}_{V/E_1})$ is E_3/E_1-admissible and, therefore, compatible with W. Moreover, the ring W satisfies the E_3/E_1-condition (see (S1)). 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. □

4.2. Below we present an efficient algorithm for recognizing singular rings and for 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 $W \leq \mathrm{Mat}_V$. First, since the equivalences $E_1 \cap E_2$ and $\langle E_1 \cup E_2 \rangle$ can easily be constructed (see Subsection 2.1), we can test efficiently whether or not F' is a multiple of F. Next, since the radical of any relation can easily be found, the E_2/E_0-condition and the E_3/E_1-condition for W can be tested efficiently. Finally, for a given $X \in V/E_3$, the identity in (S2) can also be tested efficiently (e.g., by comparing the basis relations). Thus, the presence of singularity for

W in the pair (F, F') can be tested in time $n^{O(1)}$, where $n = |V|$. We say that an extension W' of W is *admissible* if $\mathrm{Aut}(W')$ is a well-embedded subgroup of $\mathrm{Aut}(W)$ and $W' \neq W$.

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

> **Step 1.** If W is not commutative, then the output W' is empty. 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 $\mathcal{P} = \varnothing$, then the output W' is empty. Otherwise choose $(F, F') \in \mathcal{P}$.
> **Step 4.** Take $W' = [W, A]$ as the output, where A is the adjacency matrix of relation (12) with a family $\mathfrak{F}$ chosen arbitrarily. □

Theorem 4.4. *Algorithm* A2 *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* W *within the same time.*

Proof. The consistency of the algorithm is a consequence of Theorem 4.2, the definition of a singular ring, and the fact that at Step 4 we have $W' \neq W$ 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. □

In this paper, Algorithm A2 will be applied only in the case where $m \leq n$, so that in this case its complexity is bounded by $n^{O(1)}$. In the general case, this algorithm can be modified so as to achieve the same time upper bound. Indeed, it can be proved that if W has singularity in (F, F'), then $E_1 \setminus E_0 \in \mathcal{R}(W)$ and E_2 coincides with 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 (see §§3 and 4) that are 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 $\mathrm{Cyc}(\mathrm{Aut}(W)) \neq \varnothing$. Without loss of generality we may 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, by the cyclicity of G, is isomorphic to the lattice of divisors of the integer $n = |G|$.[5] In accordance with [2], the latter lattice is distributive; consequently, 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. We say that an element of $\mathcal{C}$ is a *smallest* (respectively, a *greatest*) one if every element of this class is a multiple of it (respectively, 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 a smallest element and a greatest element.*

[5] In what follows, for $E_1, E_2 \in \mathcal{E}$ we write E_1E_2 instead of $\langle E_1 \cup E_2 \rangle$.

Proof. Since the notion of $\sim$-equivalence is self-dual, we only verify the existence of a smallest element. The transitivity of the relation "to be a multiple" and the definition of the $\sim$-equivalence show 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 $F_i = E_{i1}/E_{i0}$ $(i = 1, 2, 3)$. We 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, by the distributivity of the lattice $\mathcal{E}$,

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

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. There exists a class $\mathcal{C}$ of the $\sim$-equivalence on the set of all primitive flags of W such that $\mathcal{C}$ contains no subnormal flags. Let $F = E_1/E_0$ and $F' = E_3/E_2$ be a smallest and a greatest elements of $\mathcal{C}$. Theorem 5.1 is a consequence of the proposition below.

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

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

We set $\mathcal{A} = W^{\rho^{-1}}$ and $H_i = E_i^{\rho^{-1}}$, $i = 0, 1, 2, 3$, where $\rho = \rho_G$ is the 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 if and only if 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 the tensor product. Thus it suffices to check the following:

(S1′) $\mathcal{A}$ satisfies both the H_2/H_0-condition and the H_3/H_1-condition;
(S2′) $\mathcal{A}_{H_3/H_0} = \mathcal{A}_{H_1/H_0} \otimes \mathcal{A}_{H_2/H_0}$.

For this, let $X \in \mathcal{S}(\mathcal{A})$. Then it suffices to verify that $\mathrm{rad}(X) \geq H_i$ whenever $X \subset G \setminus H_{i+2}$, $i = 0, 1$ (condition (S1′)), and that $XH_0 = X_1H_0 \cdot X_2H_0$ for some $X_i \in \mathcal{S}(\mathcal{A}_{H_i})$, $i = 1, 2$, whenever $X \subset H_3$ (condition (S2′)). We shall check both conditions simultaneously. First, suppose that $X \subset H_2$ or $\mathrm{rad}(X) \geq H_1$. Then in condition (S1′) there is nothing to check. Next, condition (S2′) is satisfied trivially for $X \subset H_2$. If $\mathrm{rad}(X) \geq H_1$, then $X \not\subset H_3$, for otherwise the image of the basic set X under the natural epimorphism $H_3 \to H_1/H_0$ would be equal to 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 may assume that

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

Then the required conditions are satisfied by the following lemma.

Lemma 5.4. *In the above notation and under the above assumptions, we have $H_0 \leq \mathrm{rad}(X)$ and $\langle X \rangle \subset H_3$. 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 the notions of a flag, subflag, multiple, and $\sim$-equivalence, and also of normality, subnormality, and quasinormality of a flag, from the Cayley rings to the S-rings. We observe that a flag U/L of the S-ring $\mathcal{A}$ is normal if and only if 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). Moreover, 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 that 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 smallest and the greatest element of this class, respectively. Putting $U = \langle X\rangle$ and $L = \mathrm{rad}(X)$, we 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 the proofs of both equivalences are similar, we prove the second for instance. We start with the observation that the flag H_3U/H_2U is not a multiple of H_3/H_2. (Otherwise, $U \le H_3$ because the latter flag is maximal. Since also $H_3 \cap H_2U = H_2$, we have $H_2U = H_2$, which contradicts the first relation in (15).) Therefore, $H_2 < H_3 \cap (H_2U)$, whence $H_3 \cap (H_2U) = H_3$ because $\mathrm{rk}(\mathcal{A}_{H_3/H_2}) = 2$. Thus, $H_3 \le H_2U$, and we obtain

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

by the distributivity of the lattice $\mathcal{H}(\mathcal{A})$. This implies that H_1/H_0 is a multiple of $(H_1 \cap U)/(H_0 \cap U)$, so that $H_1 \le U$ by the minimality of the flag H_1/H_0. It follows that $H_3 \ge (H_3 \cap U)H_2 \ge H_1H_2 = H_3$, and, consequently, $(H_3 \cap U)H_2 = H_3$. Obviously, since $(H_3 \cap U) \cap H_2 = H_2 \cap U$, 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 smallest and the greatest element, respectively, it follows that the flags H_1L/H_0L and $(H_3 \cap U)/(H_2 \cap U)$ are subflags of U/L. We prove that there exist groups $H, H' \in \mathcal{H}(\mathcal{A})$ such that $L \le H, H' \le U$ and

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

For this, we observe that the radical of the image of X in U/L is trivial. Then from [17, Theorem 3.1] and the definition of U it follows that this image contains a generator of the group U/L. So, the S-ring $\mathcal{A}_{U/L}$ has a trivial radical in the sense of [11]. By [11, Corollary 6.4], this implies the existence of groups $U_i \in \mathcal{H}(\mathcal{A})$, $L \le U_i \le U$ $(i = 0, \dots, s)$, 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 easily seen 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 $i > 0$. Therefore, every subflag F of U/L with $\mathrm{rk}(\mathcal{A}_F) = 2$ is $\sim$-equivalent either to a subflag of U_0/L or to both flags U_i/L and U/U_i' for some $i > 0$, where U_i' is the product of the 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 the flags H_1/H_0 and H_3/H_2 are not quasinormal (see (16)). Thus, by the normality of the ring $\mathcal{A}_{U_0/L}$, the first case is impossible for the former two flags. We conclude that 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 (respectively) the smallest and the greatest element of the $\sim$-equivalence class containing both of them. Next, (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 a consequence of the first part and the relation $X_1 = (H_1 \setminus H_0)L$. □

§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 $G \leq \mathrm{Sym}(V)$ 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

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

(here and below, addition of indices is meant modulo m). We 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 (for brevity, we write c instead of c_{V_i}). Given $X \subset G$ and $S \subset [0, m-1]$, we 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.

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

Step 1. If $G = \{1\}$, then the output X is equal to $\{c\}$. Otherwise, use the normal closure algorithm to 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, use the sift procedure to 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 maximum 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 $H = G^{(m)}$. The output X equals $\bigcup_{t \in T} X_t$.

Theorem 6.1. *Algorithm A3′ 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, $|X| \leq |G_0|$.*

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

In order to prove the consistency of the algorithm, we first verify that if H and T are found at Steps 2 and 3, then each pair (H, tc) with $t \in T$ is an admissible input of the algorithm. Indeed, since $H \leq G$, relations (19) imply that $(V_i)^H = V_i$ and $(V_i)^{tc} = V_{i+1}$ for all i. Furthermore, K_i is a normal subgroup of G_i, and $(K_i)^c = K_{i+1}$ (see Steps 1 and 2), whence $H^{tc} = H$. Next, in accordance with Steps 1 and 3, we have $H_0 \leq K_0 < G_0$, where $H_0 = \varphi_0(H)$. Therefore, by the induction hypothesis,

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

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

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

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. This allows us to choose g in such a way that the right-hand side of the above identity belongs to K_i for all $i \in [0, l-1]$. Then $g^{-1}fg^{c^{-1}} \in G^{(l)}$ (see Step 2), which shows that the element $(fc)^g$ (equal to $g^{-1}fcg = (g^{-1}fg^{c^{-1}})c$) belongs to $G^{(l)}c$. Thus, we have

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

By (20), this implies that

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

completing the consistency proof.

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

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

Proof. Since

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

it suffices to check that $H = G^{(l+1)}$. For 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 need 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 $(G^{(i)})_i \le K_i$ for all $i \in [l+1, m-1]$. Without loss of generality, we may 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 claim for $i = l+1$ follows from the choice of K_0 at Step 1 and l at Step 3. Suppose that the claim is true for some $i \in [l+1, m-2]$. Then

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

and we are done. □

To estimate $|X|$, 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 complexity, we 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. We describe the main algorithm of this section. Let $c = (v_1, \dots, v_n)$ and $c' = (v'_1, \dots, v'_n)$ be full cycles on V. 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,[6] then, by checking whether or not $c^i g_0 \in G$ for some $i \in [n]$, we 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 that family) 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 $C = \varnothing$.
    Step 2. If $|V| = 1$, then $C = G$. 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($G_{V/E}$).
    Step 4. For each $\overline{c} \in \overline{C}$, find $c \in G$ such that $c_{V/E} = \overline{c}$ and then the set $X_c$ =A3′($G_E, c$) (the decomposition (19) is given by the classes of $E$).
    Step 5. As the output $C$, take 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 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. For the proof of consistency 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 it follows by induction 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.

We estimate the running time $t(G)$ of the algorithm applied to a solvable group G. First, we observe that Steps 1 and 2 can easily be 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 $G_0 = (G_E)_{V_0}$ and V_0 is 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. Therefore, we have $|G_{V_0}| \le |V_0|^4$, by 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 §1). Summarizing, we obtain

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

which completes the proof. □

[6] Here the group G is not assumed to be given by generators.

§7. Cycle base of a cellular ring

Let W be a homogeneous cellular ring on V. We 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). Therefore, $E = \langle R\rangle$ with $R = X^{\rho_G}$, where X is the basic set of $\mathcal{A}$ containing a generator of H. However, $\mathcal{E}_0(W) \neq \mathcal{E}(W)$ in general. But then we can find two different 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 identity $\mathcal{E}_0(W) = \mathcal{E}(W)$ 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 $W' \neq \varnothing$, repeat the following: if W' is not homogeneous or $\mathcal{E}_0(W') \neq \mathcal{E}(W')$, then the output C is empty, else set $W = W'$ and find $W' =$A2(W).

Step 3. Find $G =$A1(W). If $G = \varnothing$, then the output C is emply.

Step 4. Find $C' =$A3(G). As the output C, take 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 finds a cycle base of W in time $n^{O(1)}$.*

Proof. For the proof of consistency, first we suppose that $\mathrm{Cyc}(\mathrm{Aut}(W)) = \varnothing$. Then we may assume that the algorithm terminates at Step 4. Since the cellular ring at Step 3 contains the input ring, we have $\mathrm{Cyc}(G) = \varnothing$, where G is the group found at Step 3. Thus, the consistency of the Main Algorithm follows from that of Algorithm A3 (Theorem 6.3). Now, let $\mathrm{Cyc}(\mathrm{Aut}(W)) \neq \varnothing$. Then, at each iteration of Step 2, $\mathrm{Aut}(W')$ is a well-embedded subgroup of $\mathrm{Aut}(W)$ by Theorem 4.4; consequently, W' is a homogeneous ring with $\mathcal{E}_0(W') = \mathcal{E}(W')$ (see the beginning of the section). Therefore, at Step 3, $\mathrm{Aut}(W)$ is a well-embedded subgroup of the automorphism group of the input ring (which is equal to $\mathrm{Aut}(W_0)$). On the other hand, the ring W at the same step is not singular. By Theorem 5.1, it follows that this 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 consistency of the algorithm in question follows from that of Algorithm A3 (see Theorem 6.3).

We 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. Therefore, this step can be done in time $n^{O(1)}$ by the same theorem and the remark at the beginning of the section. Thus, the required time bound follows from Theorems 3.6 and 6.3, the remark at the beginning of Subsection 6.2, and the fact that, obviously, the group $\mathrm{Aut}(W_0)$ at Step 4 is $n^{O(1)}$-recognizable. □

§8. Cellular rings, Cayley rings, Schur rings, and permutation groups

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. 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

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

Here $\mathcal{R}^* = \mathcal{R}^*(W)$ is the set of all unions of 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*. The ring W is said to be *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, $\Delta(V)$ and V^2 belong to $\mathcal{E}$. A homogeneous ring W is *primitive* if $\deg(W) > 1$ and $\mathcal{E} = \{\Delta(V), V^2\}$.

We say that cellular rings W on V and W' on V' are *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 strong isomorphisms contains the 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 said to be *weakly isomorphic* if there exists a $\mathbb{Z}$-module isomorphism $\varphi : W \to W'$ preserving both the matrix and the 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 let $X \in \mathcal{B}$, $E \in \mathcal{E}$. 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, Subsection 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 $W_{X/E}$. It can be shown that

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

It is easily seen that the ring $W_{X/E}$ is homogeneous, and it is commutative whenever so is W. 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 let $E \in \mathcal{E}(W)$. For any $X, Y \in V/E$ there exists a unique 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 $\mathrm{Mat}_{V_1} \otimes \mathrm{Mat}_{V_2} = \mathrm{Mat}_{V_1\times V_2}$ is a cellular ring on $V_1 \times V_2$, and

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

where $R_1 \otimes R_2 = \{((u_1, u_2), (v_1, v_2)) : (u_1, v_1) \in R_1,\ (u_2, v_2) \in R_2\}$. The ring $W_1 \otimes W_2$ 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 is 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 $W \subset W'$. If $\mathcal{M}_1, \dots, \mathcal{M}_s$ are subsets of Mat_V, then their *cellular closure*, i.e., the smallest cellular ring on V containing all of them, is denoted by $[\mathcal{M}_1, \dots, \mathcal{M}_s]$. 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, an *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

$$\{1\} \in \mathcal{S}, \quad \bigcup_{X \in \mathcal{S}} X = G \qquad \text{and} \quad X \in \mathcal{S} \implies X^{-1} \in \mathcal{S}.$$

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

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

(we keep the 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 $G_1 \times G_2$, and

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

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

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

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

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, and $A(X^{\rho_G}) = \rho_G(\xi(X))$ for all X. If $\mathcal{A}$ is an S-ring over G, then $W = \mathcal{A}^{\rho_G}$ is a cellular ring on G such that $G_{\mathrm{right}} \le \mathrm{Aut}(W)$. 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) *determines 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 $E' = K^{\rho_G}$.*

Let $X \subset G$; 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 left as well as right cosets by this subgroup. If this subgroup is normal in G, then the image of X under the natural epimorphism from G to $G/\mathrm{rad}(X)$ has a 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 $K \le H$, then we say that $\mathcal{A}$ satisfies the *H/K-condition* if $K \le \mathrm{rad}(X)$ for all $X \in \mathcal{S}(\mathcal{A})$ with $X \subset G \setminus H$.

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

Theorem 8.3. *For 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 we 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; mostly, they are based on the sift procedure (for the details, see [16]). Here we only make some remarks. A permutation group G on n points will always be determined by a strong generating set (of at most n^2 generators). In this representation, the membership in G can be tested and the order of G can be found in time $n^{O(1)}$. Moreover, within the same time we 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 §3) is a special case of [1, Corollary 3.6].

Theorem 8.4. *Let $G \leq \mathrm{Sym}(V)$ be a solvable group. For 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*, Annual ACM Symposium on Theory of Computing (Proc. 15th Annual ACM Symposium on Theory of Computing), ACM Press, New York, NY, 1983, pp. 171–183.

[2] G. Birkhoff, *Lattice theory*, Amer. Math. Soc. Colloq. Publ., vol. 25, Amer. Math. Soc., Providence, RI, 1967. MR0227053 (37:2638)

[3] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-regular graphs*, Ergeb. Math. Grenzgeb. (3), vol. 18, Springer-Verlag, Berlin–New York, 1989. MR1002568 (90e:05001)

[4] J. D. Dixon and B. Mortimer, *Permutation groups*, Grad. Texts in Math., vol. 163, Springer-Verlag, New York, 1996. MR1409812 (98m:20003)

[5] S. Evdokimov, M. E. Muzychuk, I. Ponomarenko, and G. Tinhofer, *Recognizing certain Cayley graphs in polynomial time* (submitted to Electron. J. Combin.).

[6] S. A. Evdokimov and I. N. Ponomarenko, *Two inequalities for parameters of a cellular algebra*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **240** (1997), 82–95; English transl., J. Math. Sci. **96** (1999), no. 5, 3496–3504. MR1691640 (2000c:20017)

[7] ———, *Isomorphism of coloured graphs with slowly increasing multiplicity of Jordan blocks*, Combinatorica **19** (1999), 321–333. MR1723252 (2001h:05070)

[8] S. Evdokimov, M. Karpinski, and I. Ponomarenko, *On a new high-dimensional Weisfeiler–Leman algorithm*, J. Algebraic Combin. **10** (1999), 29–45. MR1701282 (2001i:05110)

[9] S. Evdokimov and I. Ponomarenko, *Separability number and schurity number of coherent configurations*, Electron. J. Combin. **7** (2000), no. 1, Res. Paper 31. MR1763969 (2001g:05108)

[10] ———, *On a family of Schur rings over a finite cyclic group*, Algebra i Analiz **13** (2001), no. 3, 139–154; English transl., St. Petersburg Math. J. **13** (2002), no. 3, 441–452. MR1850191 (2002i:16036)

[11] ———, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra i Analiz **14** (2002), no. 2, 11–55; English transl., St. Petersburg Math. J. **14** (2003), no. 2, 189–221. MR1925880 (2003h:20005)

[12] D. G. Higman, *Coherent configurations.* I, Rend. Sem. Mat. Univ. Padova **44** (1970), 1–25. MR0325420 (48:3767)

[13] K. H. Leung and S. H. Man, *On Schur rings over cyclic groups.* II, J. Algebra **183** (1996), 273–285. MR1399027 (98h:20009)

[14] C. H. Li, *On isomorphisms of finite Cayley graphs—a survey*, Discrete Math. **256** (2002), 301–334. MR1927074 (2003i:05067)

[15] A. Lubiw, *Some NP-complete problems similar to graph isomorphism*, SIAM J. Comput. **10** (1981), 11–21. MR0605600 (82f:03036)

[16] E. M. Luks, *Permutation groups and polynomial-time computation*, Groups and Computation (New Brunswick, NJ, 1991), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 11, Amer. Math. Soc., Providence, RI, 1993, pp. 139–175. MR1235801 (94h:20005)

[17] M. E. Muzychuk, *On the structure of basic sets of Schur rings over cyclic groups*, J. Algebra **169** (1994), 655-678. MR1297167 (95i:20004)

[18] ______, *Ádám's conjecture is true in the square-free case*, J. Combin. Theory Ser. A **72** (1995), 118–134. MR1354970 (96m:05141)

[19] ______, *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198** (1999), 589–606. MR1674890 (2000e:05165)

[20] M. Muzychuk, M. Klin, and R. Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory*, Codes and Association Schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 241–264. MR1816402 (2002g:05128)

[21] M. E. Muzychuk and G. Tinhofer, *Recognizing circulant graphs of prime order in polynomial time*, Electron. J. Combin. **5** (1998), no. 1, Res. Paper 25. MR1618814 (99c:05186)

[22] ______, *Recognizing circulant graphs in polynomial time: an application of association schemes*, Electron. J. Combin. **8** (2001), no. 1, Res. Paper 26. MR1855867 (2002j:05141)

[23] P. P. Palfy, *A polynomial bound for the orders of primitive solvable groups*, J. Algebra **77** (1982), 127–137. MR665168 (84c:20007)

[24] I. Ponomarenko, *Polynomial-time algorithms for recognizing and isomorphism testing of cyclic tournaments*, Acta Appl. Math. **29** (1992), 139–160. MR1192837 (94f:05142)

[25] I. Schur, *Zür Theorie der einfach transitiven Permutationsgruppen*, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. **18/20** (1933), 598–623.

[26] B. Yu. Weisfeiler and A. A. Leman, *Reduction of a graph to a canonical form and an algebra which appears in the process*, Nauchno-Tekhn. Inform. Sb. VINITI Ser. 2 **1968**, no. 9, 12–16. (Russian)

[27] B. Weisfeiler (ed.), *On the construction and identification of graphs*, Lecture Notes in Math., vol. 558, Springer-Verlag, Berlin etc., 1976. MR0543783 (58:27590)

[28] H. Wielandt, *Finite permutation groups*, Acad. Press, New York–London, 1964. MR0183775 (32:1252)

[29] ______, *Permutation groups through invariant relations and invariant functions*, Lecture Notes Dept. Math., Ohio State Univ., Columbus, Ohio, 1969.

St. Petersburg Institute for Informatics and Automation RAS, St. Petersburg, Russia
E-mail address: evdokim@pdmi.ras.ru

St. Petersburg Branch, Steklov Mathematical Institute, Russian Academy of Sciences, Fontanka 27, St. Petersburg 191023, Russia
E-mail address: inp@pdmi.ras.ru

Received 15/MAY/2003

Translated by THE AUTHORS