

The isomorphism problem for circulant graphs via Schur ring theory

Mikhail Muzychuk, Mikhail Klin, and Reinhard Pöschel

ABSTRACT. This paper concerns the applications of Schur ring theory to the isomorphism problem of circulant graphs (Cayley graphs over cyclic groups). A digest of the most important facts about Schur rings presented in the first sections provides the reader with a gentle self-contained introduction to this area. The developed machinery allows us to give proofs of two conjectures (Zibin' 1975 and Toida 1977) about necessary conditions on isomorphisms of the circulants. These new results together with a few new proofs of some known facts show the feasibility of the technique of Schur rings in algebraic combinatorics.

The concluding section contains a short historical and bibliographical survey of various results related to the isomorphism problem for Cayley graphs.

1. Introduction

A circulant graph with n vertices is a Cayley graph over the cyclic group C_n of order n , that is a graph which is invariant with respect to a cyclic rotation of all its vertices.

Circulant graphs form a wide and important class of vertex-transitive (directed or undirected) graphs. Such graphs can be regarded as so-called quasi-random graphs (in the sense of [16]), which means that various graph-theoretical properties can be successfully modelled and investigated within the class of circulants.

Though the history of circulants spans more than a century, modern interest in these graphs did not resurface until the 1960s. In 1967 A. Ádám posed his famous conjecture about a necessary and sufficient isomorphism condition for circulant graphs, thus opening the current wave of interest in the circulants. The history of this conjecture over 20 years can be observed in Pálffy's excellent survey [72].

One of the most successful solutions of the isomorphism problem for circulant graphs is based on the use of Schur rings (S-rings for brevity).

The notion of an S-ring was introduced by I. Schur in 1933 [77]. It was developed and used during a few decades mostly for purely group-theoretical purposes by H. Wielandt and other disciples and followers of I. Schur. In 1972-78 two of the authors (M.K. and R.P.) suggested using S-ring theory in graph theory, namely

1991 *Mathematics Subject Classification.* Primary 05C60, 05E99; Secondary 05C25, 20B25 .
The first author was partially supported by grant of the DAAD.

for the investigation of the symmetry properties of circulant graphs. Most of their results were available, for a long time, only in the form of preprints with a very limited distribution. During the last decade the interest in such application of S-rings was supported by the publications of the first author (M.M.) and a few other mathematicians. It became evident that S-rings give a very suitable and natural way to classify circulants.

The present paper may be regarded as a brief survey of the techniques of S-rings and applications in graph theory. The methodology presented in the paper is illustrated by the unified proofs of a number of known and new criteria for the isomorphism of circulant graphs. In particular, we give complete solutions of two related problems which were posed by D.K. Zibin' (1975) and S. Toida (1977).

During the last two decades circulant graphs found various interesting applications. For example, numerous graph and network models were used for the elaboration of reliable architectures of computers and computer networks. For these purposes one needs to select graphs with certain optimal or quasi-optimal combinations of invariants of a graph such as small diameter, fixed degree, uniformity, redundant paths, short wires, simple routing algorithm, *etc.* [35]. It turns out that rather good solutions of the above-mentioned problems may be found in the class of circulant graphs, see, for example, [10, 9, 27, 90, 75].

We hope that our survey will be of interest not only to the pure experts in the graph isomorphism problem but also to those who are interested in various applications of circulants. This is why we are trying to present here a self-contained gentle introduction to the subject which may be available to a wide mathematical audience.

On the other hand our interest here is limited by the consideration of only one class of Cayley graphs: those over cyclic groups. Other classes of Cayley graphs, as well as purely group-theoretical approaches to the isomorphism problem of Cayley graphs (and circulant graphs in particular) appear only in the context of a general outline of activities, without sufficient details.

The paper consists of seven sections. Section 2 gives a short historical introduction to the isomorphism problem of circulant graphs with a special emphasis on its natural generalization, suggested by L. Babai: the description of Cayley graphs with the Cayley isomorphism property (CI-graphs).

Section 3 presents a self-contained introduction to Schur rings. We start with the main definitions and the characterization of Schur rings as certain subalgebras of group algebras (3.1). Important properties of subgroups appearing as elements of S-rings (first formulated by O. Tamaschke) are given in 3.2. In 3.3 we consider three different sorts of S-ring isomorphisms (algebraic, combinatorial and Cayley), while in 3.4 we explain how isomorphisms of Cayley graphs are related to isomorphisms of S-rings. In 3.5, starting from a classical theorem of Schur, a Galois correspondence between S-rings and permutation groups is established. Example 3.6 provides the reader an opportunity to "play" a little bit with all the above-mentioned notions. We have to admit that Section 3 requires from the reader a certain level of a general algebraic culture.

Section 4 is a short digest of all results about Schur rings over cyclic groups C_n necessary for our presentation. We start from the classical theorem of Schur, claiming that for a non-prime n each non-trivial S-ring over C_n is imprimitive. A number of propositions presented in 4.2 was originally formulated and proved by Muzychuk in [64], a paper mostly aimed at experts in algebra. In this text we try

to find transparent formulations of all claims used, such that they will be clear to a wider mathematical audience.

Section 5 properly concerns the isomorphism problem for circulant graphs. The machinery developed in the previous sections allows us to give short and rather simple proofs of various known and new results. In 5.1 we present the proof of Zibin's conjecture. As an immediate consequence we get the proof of Toida's conjecture and of the theorem about arc-transitive circulants (which recently was proved by C.H. Li with the aid of the Classification of Finite Simple Groups). It is worth mentioning that during the last two decades there appeared many papers dealing with various particular cases of the graph isomorphism problem for circulant graphs. As a rule these results may be reproved by the standard use of S-rings. In 5.2 we illustrate this claim, giving a new proof of the theorem by X. Fang and M. Xu [26] about the so-called double-loop circulants. We conclude Section 5 with a computational example: the solution of the isomorphism problem for 8-vertex circulant graphs. We think that a careful examination of this example will provide the reader with an extra insight, which will help to enter the subject more deeply.

Schur rings are just a particular case of more general structures, commonly treated in Algebraic Combinatorics: association schemes and coherent configurations. A brief outline of such interrelations is given in Section 6, however a deeper consideration of these notions is out of the scope of this paper.

In Sections 1-6 we were tried to avoid a huge amount of information of historical and bibliographical nature. This is why most of such information is concentrated in the final Section 7. Here an interested reader may consider the subject more widely, making a glance on other techniques and other classes of Cayley graphs. Nevertheless we are not pretending to submit in this section a comprehensive survey, being self-restricted by the consideration of only those results which have natural links with the main content of our paper.

2. Genesis of the problem

Let Γ be a (di)graph on n vertices which we identify with the elements of $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. The (di)graph Γ is called **circulant** if it has a cyclic symmetry, i.e., if the permutation $(0, 1, 2, \dots, n-1)$ is an automorphism of the graph. Each circulant graph is completely determined by its **connection set** S which is the set of all points connected to 0 in Γ . Two vertices i and j are Γ -connected if and only if $i - j \in S$ where the difference is taken in the cyclic group $\mathbb{Z}_n$ (additive notation). Thus a circulant graph is a **Cayley graph** over the cyclic group $\mathbb{Z}_n$.

In what follows we shall write $\text{Cay}(\mathbb{Z}_n, S)$ for a circulant graph $\Gamma = (V, E)$ with connection set S , i.e. $V = \mathbb{Z}_n$, $E = \{(x, y) \mid x - y \in S\}$.

The isomorphism problem for circulant graphs is stated as follows:

Given two circulant graphs $\text{Cay}(\mathbb{Z}_n, S)$ and $\text{Cay}(\mathbb{Z}_n, T)$. Find an efficient algorithm which recognizes an isomorphism between these graphs.
--

Let $\mathbb{Z}_n^*$ be the set of all residues modulo n which are relatively prime to n . If $S = mT$ for some $m \in \mathbb{Z}_n^*$, then the permutation $x \mapsto mx$, $x \in \mathbb{Z}_n$ is an isomorphism between the two graphs. In this case we shall say that the connection sets (and the graphs) are **conjugate by multiplier**. In 1967 A. Ádám conjectured that two circulant graphs are isomorphic if and only if they are conjugate by a multiplier [1]. Rather soon it was found that the conjecture is false in general: the minimal

counterexample on 8 vertices was constructed by B. Elspas and J. Turner in 1970 [21]. In general, it was shown by B. Alspach and T.D. Parsons in 1979 [2] and, independently by V.N. Egorov and A.I. Markov [20] that Ádám's conjecture fails if n is divisible by 8 or by a square of an odd prime. On the other hand, it was shown that for specific values of n the conjecture is true (see Section 7 for a detailed survey). This led to the “corrected” Ádám's conjecture formulated by P.P. Pálffy in 1987 [72]:

$$\left| \begin{array}{l} \text{Adam's conjecture holds if and only if 8 does not divide } n \text{ and} \\ p^2 \text{ does not divide } n \text{ for each odd prime number } p. \end{array} \right|$$

Since then, the topic has attracted the attention of many researchers. Two aspects have been considered:

1. To prove the corrected Ádám's conjecture;
2. To find an algorithm which solves the isomorphism problem for some specific values of n which are not covered by the corrected Ádám's conjecture.

An affirmative answer to the corrected Ádám's conjecture was given in 1995-97 by Muzychuk [66, 67]. The proof combines group theory with computations in Schur rings.

There are not many results in the second direction: in 1978, M. Klin and R. Pöschel [46] and, in 1979, B. Alspach and T.D. Parsons [2] gave a complete solution for $n = p^2$. In 1980, Klin and Pöschel solved the isomorphism problem for $n = p^\alpha$, $p > 2$, [43] (in both cases p is a prime).

An important role in the recognition of isomorphisms is played by so-called **layers** of connection sets.

Let d be an arbitrary divisor of n . Then the d -th layer of $S \subseteq \mathbb{Z}_n$ is defined as $(S)_d := S \cap (\mathbb{Z}_n)_d$ where $(\mathbb{Z}_n)_d := \{x \in \mathbb{Z}_n \mid \gcd(x, n) = d\}$. It was shown by Klin and Pöschel [43] that if $n = p^\alpha$, then two circulants $\text{Cay}(\mathbb{Z}_n, S)$ and $\text{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if for each $d|n$ there exist multipliers $m_d \in \mathbb{Z}_n^*$, such that $m_d(T)_d = (S)_d$ and which satisfy some compatibility condition.

The layers and multipliers appeared also in a computer enumeration of small circulants which was done in 1975 by D.K. Zibin' who made the following conjecture.

Zibin's conjecture [88]. If $\text{Cay}(\mathbb{Z}_n, S)$ and $\text{Cay}(\mathbb{Z}_n, T)$ are two isomorphic circulants, then there exist multipliers $m_d \in \mathbb{Z}_n^*$, $d|n$, such that $m_d(S)_d = (T)_d$.

A particular case of this conjecture was independently formulated by S. Toida in 1977:

Toida's conjecture [80]. Let $S \subseteq \mathbb{Z}_n^*$ and $T \subseteq \mathbb{Z}_n$. Then $\text{Cay}(\mathbb{Z}_n, S)$ is isomorphic to $\text{Cay}(\mathbb{Z}_n, T)$ if and only if the connection sets T and S are conjugate by a multiplier.

Inspired by Ádám's conjecture L. Babai started the study of the isomorphism problem of **Cayley combinatorial objects** in 1977 [3]. He showed that the solution of the isomorphism problem for arbitrary Cayley combinatorial objects may be “found” in the automorphism group of the object. To formulate his results we need a few definitions.

Let H be a finite group in multiplicative notation and let

$$\text{Cay}(H, S) := \{(x, y) \in H^2 \mid xy^{-1} \in S\}$$

be an arbitrary Cayley graph over H ($S \subseteq H$). We shall say that two Cayley graphs $\text{Cay}(H, S)$ and $\text{Cay}(H, T)$ are **Cayley isomorphic** if there exists an automorphism $\varphi \in \text{Aut}(H)$ such that $S^\varphi = T$ (S and T are **conjugate** by φ ; $S^\varphi := \{s^\varphi \mid s \in S\}$, where we use the notation $s^\varphi := \varphi(s)$). It is a trivial observation that two Cayley isomorphic Cayley graphs are isomorphic as usual graphs. The converse is not true even for circulants. A subset $S \subseteq H$ is called a **CI-subset** if for each $T \subseteq H$ the graphs $\text{Cay}(H, S)$, $\text{Cay}(H, T)$ are isomorphic if and only if the sets T and S are conjugate by an element from $\text{Aut}(H)$. A group H is called **CI-group** if each subset of H is a CI-subset.

Babai [3] gave a group-theoretical criterion whether a combinatorial "Cayley structure" has the CI-property. The restriction of his result to Cayley graphs immediately gives the following theorem.

THEOREM 2.1. *A subset $S \subseteq H$ is a CI-subset if and only if every two H -isomorphic¹ regular subgroups of $\text{Aut}(\text{Cay}(H, S))$ are conjugate in $\text{Aut}(\text{Cay}(H, S))$.*

Another, purely combinatorial approach, was suggested by Klin and Pöschel in 1978 [46]. They proposed to look more carefully at the combinatorial invariants of a graph in order to attack the isomorphism problem for Cayley graphs. They found a very strong combinatorial invariant for a Cayley graph: the Schur ring generated by its connection set. The key fact is that an isomorphism between Cayley graphs is also an isomorphism between S-rings generated by their connection sets. Since S-rings are algebraic objects, an isomorphism testing for S-rings is much easier than an isomorphism testing for Cayley graphs. We shall see that for cyclic graphs the structure properties of S-rings yield rather strong necessary conditions for graph isomorphism. To our knowledge there is no group-theoretical way to obtain these conditions. Finally, it is worth mentioning that in some cases the necessary conditions obtained using Schur rings are also sufficient, which leads to an efficient algorithm for recognizing graph isomorphism.

3. Schur rings.

3.1. Basic definitions. Let H be an arbitrary finite multiplicatively written group with identity e . The group algebra $\mathbb{Q}H$ consists of all formal sums $\sum_{h \in H} \alpha_h h$, $\alpha_h \in \mathbb{Q}$ which are multiplied according to the following rule

$$\left(\sum_{h \in H} \alpha_h h\right) \left(\sum_{h \in H} \beta_h h\right) = \sum_{h \in H} \sum_{f \in H} (\alpha_h \beta_f)(fh).$$

The **Schur-Hadamard product** in $\mathbb{Q}H$ is defined as follows:

$$\left(\sum_{h \in H} \alpha_h h\right) \circ \left(\sum_{h \in H} \beta_h h\right) = \sum_{h \in H} (\alpha_h \beta_h) h.$$

For each $m \in \mathbb{Z}$ and $x = \sum_{h \in H} x_h h$ let $x^{(m)} := \sum_{h \in H} x_h h^m$. For a nonempty subset $T \subseteq H$ we set $\underline{T} := \sum_{t \in T} t$. Following [85] elements of this form will be called **simple quantities**. A simple quantity $\underline{T}$ is called **symmetric** if $T^{(-1)} = T$.

A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{Q}H$ is called a **Schur ring**, for short **S-ring**, if it satisfies the following axioms:

- (S1) $\mathcal{A}$ has a basis of simple quantities $\underline{T}_0, \dots, \underline{T}_r$, where $T_0 = \{e\}$,
- (S2) $T_i \cap T_j = \emptyset$ for $i \neq j$, and $\bigcup_{j=0}^r T_j = H$,

¹ H -isomorphic means isomorphic to H

(S3) For each $i \in \{0, 1, \dots, r\}$ there exists $i' \in \{0, 1, \dots, r\}$, such that $T_{i'} = T_i^{(-1)}$

By (S1) and (S2), the basis $\underline{T}_0, \dots, \underline{T}_r$ is unique and it is called the **standard basis** of $\mathcal{A}$. The sets T_i , $0 \leq i \leq r$, are called the **basic sets** of $\mathcal{A}$ and the notation $\mathcal{A} = \langle \underline{T}_0, \dots, \underline{T}_r \rangle$ will be used if $\mathcal{A}$ is an S-ring over H whose basic sets are $T_0, \dots, T_r$. The set of all basic sets is also denoted by $\text{Basic}(\mathcal{A})$. By (S2), every $h \in H$ is contained in exactly one basic set, which will be denoted by $T_{(h)}$. There are two **trivial** S-rings over an arbitrary group H , namely $\langle \underline{e}, \underline{G} \setminus \{e\} \rangle$ and $\mathbb{Q}H$.

The following characterization of Schur rings is folklore (see Section 7 for more details):

THEOREM 3.1. *Let $\mathcal{A} \subseteq \mathbb{Q}H$ be a subalgebra of the group algebra $\mathbb{Q}H$. Then $\mathcal{A}$ is an S-ring over H if and only if $\underline{e} \in \mathcal{A}$, $\underline{H} \in \mathcal{A}$ and $\mathcal{A}$ is closed with respect to $\circ$ and (-1) .*

It follows from this result that the intersection of S-rings over H is an S-ring over the same group. Given $x_1, \dots, x_k \in \mathbb{Q}H$, we define $\langle x_1, \dots, x_k \rangle$ to be the least S-ring which contains the elements $x_1, \dots, x_k$. If $\underline{S}$ is a simple quantity, then we shall write $\langle \underline{S} \rangle$ instead of $\langle \underline{S} \rangle$.

An S-ring $\mathcal{B} \subseteq \mathbb{Q}H$ is called a **fusion** of an S-ring $\mathcal{A} \subseteq \mathbb{Q}H$ (or an **S-subring** of $\mathcal{A}$) if $\mathcal{B} \subseteq \mathcal{A}$. An S-ring $\mathcal{A}$ is called a **fission** of an S-ring $\mathcal{B}$ if $\mathcal{B}$ is a fusion of $\mathcal{A}$. It is a trivial observation that $\mathcal{B}$ is a fusion of $\mathcal{A}$ if and only if each basic set T of $\mathcal{B}$ is the union of some basic sets of $\mathcal{A}$.

The following operation is a useful tool in computing $\langle x_1, \dots, x_k \rangle$. Let $q \in \mathbb{Q}$ be an arbitrary number. Define the mapping $I_q : \mathbb{Q}H \rightarrow \mathbb{Q}H$ by the following formula

$$I_q\left(\sum_{h \in H} x_h h\right) := \sum_{h \in H \wedge x_h = q} h.$$

PROPOSITION 3.2 (SCHUR-WIELANDT PRINCIPLE [85]). *If $\mathcal{A}$ is an S-ring over a group H , then $I_q(x) \in \mathcal{A}$ for each $x \in \mathcal{A}$ and $q \in \mathbb{Q}$.*

We finish this section by a simple example how to calculate $\langle x \rangle$. Let $x = g^1 + g^2 + g^3$ be a simple quantity in the group ring $\mathbb{Z}C_8$. Then $x^2 = g^2 + 2g^3 + 3g^4 + 2g^5 + g^6$. By the Schur-Wielandt principle $g^2 + g^6, g^3 + g^5, g^4 \in \langle x \rangle$. Now $g^3 = x \circ (g^3 + g^5) \in \langle x \rangle$ implies that $\langle x \rangle = \mathbb{Q}C_8$.

3.2. Subgroup properties of S-rings. Let $\mathcal{A} = \langle \underline{T}_0, \dots, \underline{T}_d \rangle$ be an S-ring over a group H . A subgroup $F \leq H$ is called an $\mathcal{A}$ -subgroup [79] if $\underline{F} \in \mathcal{A}$. There are two **trivial** $\mathcal{A}$ -subgroups: $\{e\}$ and H . If $\mathcal{A}$ has a non-trivial $\mathcal{A}$ -subgroup, then $\mathcal{A}$ is called **imprimitive**, otherwise it is called **primitive**. A subgroup $F \leq H$ is an $\mathcal{A}$ -subgroup if and only if it is the union of some basic sets of $\mathcal{A}$.

PROPOSITION 3.3 ([79]). *Let F, G be two arbitrary $\mathcal{A}$ -subgroups. Then $G \cap F$ and $\langle F \cup G \rangle$ are $\mathcal{A}$ -subgroups.*

In other words, the set of all $\mathcal{A}$ -subgroups is a sublattice of the subgroup lattice of H . It is not difficult to show that $\langle T \rangle$ is an $\mathcal{A}$ -subgroup for each $T \in \text{Basic}(\mathcal{A})$.

For each $T \in \text{Basic}(\mathcal{A})$ let

$$\begin{aligned} \text{L}(T) &:= \{h \in H \mid hT = T\} && \text{(left stabilizer),} \\ \text{R}(T) &:= \{h \in H \mid Th = T\} && \text{(right stabilizer),} \\ \text{Sta}(T) &:= \text{L}(T) \cap \text{R}(T) && \text{(stabilizer).} \end{aligned}$$

²We recall that $\langle X \rangle$ denotes a subgroup generated by a subset $X \subseteq G$.

PROPOSITION 3.4 ([85, Prop. 23.5]). *For every $T \in \text{Basic}(\mathcal{A})$, the stabilizers $L(T)$, $R(T)$ and $\text{Sta}(T)$ are $\mathcal{A}$ -subgroups.*

Let F be an $\mathcal{A}$ -subgroup. Define $\mathcal{A}_F := \mathcal{A} \cap \mathbb{Q}F$. It is easy to check that $\mathcal{A}_F$ is an S-ring over the group F and $\text{Basic}(\mathcal{A}_F) = \{T \in \text{Basic}(\mathcal{A}) \mid T \subseteq F\}$. We shall call $\mathcal{A}_F$ an **induced S-subring** of $\mathcal{A}$. If F is an $\mathcal{A}$ -subgroup which is normal in H one can define a **quotient** S-ring $\mathcal{A}/F$ over the factor-group H/F [76], as shown in the next proposition. Notice that the natural homomorphism $\pi : H \rightarrow H/F$ can be canonically extended to an homomorphism $\mathbb{Q}H \rightarrow \mathbb{Q}(H/F)$ that also will be denoted by π .

PROPOSITION 3.5 ([76]). *Let $\mathcal{A}$ be an S-ring over H and $F \trianglelefteq H$ be a normal $\mathcal{A}$ -subgroup. Then the algebra $\mathcal{A}/F := \pi(\mathcal{A})$ is an S-ring over H/F the basic sets of which are given by $\text{Basic}(\mathcal{A}/F) = \{T/F \mid T \in \text{Basic}(\mathcal{A})\}$.³*

3.3. Isomorphisms between S-rings. Two S-rings $\mathcal{A}$ and $\mathcal{B}$ are called **algebraically isomorphic**, notation $\mathcal{A} \cong_{\text{alg}} \mathcal{B}$, if there exists a bijection $g : \text{Basic}(\mathcal{A}) \rightarrow \text{Basic}(\mathcal{B}) : T \mapsto T^g$ such that the map $\underline{T} \mapsto \underline{T}^g$ induces (via $\sum \alpha_i \underline{T}_i \mapsto \sum \alpha_i \underline{T}_i^g$) an isomorphism between the algebras $\mathcal{A}$ and $\mathcal{B}$.

Two S-rings $\mathcal{A} = \langle T_0, \dots, T_r \rangle \subseteq \mathbb{Q}H$ and $\mathcal{B} = \langle S_0, \dots, S_s \rangle \subseteq \mathbb{Q}K$ will be called **combinatorially isomorphic**, notation $\mathcal{A} \cong_{\text{com}} \mathcal{B}$, if $r = s$ and there exists a bijection $f : H \rightarrow K$ such that $\{\text{Cay}(H, T_i)^f \mid i = 0, \dots, r\} = \{\text{Cay}(K, S_i) \mid i = 0, \dots, s\}$. (Here we use the notation $R^f := \{(x^f, y^f) \mid (x, y) \in R\}$ for $R \subseteq H \times H$.) The bijection f is called a **combinatorial isomorphism**. Each combinatorial isomorphism f induces a bijection $f^* : \text{Basic}(\mathcal{A}) \rightarrow \text{Basic}(\mathcal{B})$ given by $\text{Cay}(H, T)^f = \text{Cay}(K, T^{f^*})$ for $T \in \text{Basic}(\mathcal{A})$. A combinatorial isomorphism $f : H \rightarrow K$ is called **normalized**⁴ if $f(e) = e$. If f is a normalized combinatorial isomorphism, then $T^f = T^{f^*}$ holds for each $T \in \text{Basic}(\mathcal{A})$.

PROPOSITION 3.6 ([69]). *If f is a combinatorial isomorphism between two S-rings $\mathcal{A}$ and $\mathcal{B}$, then f^* is an algebraic isomorphism between them.*

Two S-rings are called **Cayley isomorphic**, notation $\mathcal{A} \cong_{\text{Cay}} \mathcal{B}$, if there exists a combinatorial isomorphism $f : H \rightarrow K$ which is simultaneously an isomorphism from the group H onto K . The connection between the three types of isomorphisms is given by the following implications:

$$\mathcal{A} \cong_{\text{Cay}} \mathcal{B} \implies \mathcal{A} \cong_{\text{com}} \mathcal{B} \implies \mathcal{A} \cong_{\text{alg}} \mathcal{B}.$$

But the converse is not true in general:

$$\mathcal{A} \cong_{\text{Cay}} \mathcal{B} \not\Leftarrow \mathcal{A} \cong_{\text{com}} \mathcal{B} \not\Leftarrow \mathcal{A} \cong_{\text{alg}} \mathcal{B}.$$

We shall give a simple example which shows that $\mathcal{A} \cong_{\text{Cay}} \mathcal{B} \not\Leftarrow \mathcal{A} \cong_{\text{com}} \mathcal{B}$. Let $H = \mathbb{Z}_4$ and $K = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be two abelian groups of order 4 written additively. Take the following Schur rings $\mathcal{A} = \langle 0, 2, 1, 3 \rangle \subseteq \mathbb{Q}\mathbb{Z}_4$, $\mathcal{B} = \langle (0, 0), (1, 0), (1, 1), (0, 1) \rangle \subseteq \mathbb{Q}[\mathbb{Z}_2 \oplus \mathbb{Z}_2]$. These S-rings cannot be Cayley isomorphic, since $\mathbb{Z}_4 \not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. On the other hand the bijection $0 \mapsto (0, 0)$, $1 \mapsto (0, 1)$, $2 \mapsto (1, 0)$, $3 \mapsto (1, 1)$ is a combinatorial isomorphism between them.

Let $\mathcal{A} \subseteq \mathbb{Q}H$ and $\mathcal{B} \subseteq \mathbb{Q}K$ be two S-rings over the groups H and K respectively. We shall write $\text{Iso}_{\text{Cay}}(\mathcal{A}, \mathcal{B})$, $\text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{B})$, $\text{Iso}_{\text{alg}}(\mathcal{A}, \mathcal{B})$ for the sets of all Cayley,

³Here T/F stands for the set of left F -cosets: $T/F := \{tF \mid t \in T\}$.

⁴S-isomorphisms in [47]

combinatorial and algebraic isomorphisms, respectively, between $\mathcal{A}$ and $\mathcal{B}$. If $\mathcal{A} = \mathcal{B}$, then

$$\begin{aligned}\text{Aut}_{\text{Cay}}(\mathcal{A}) &:= \text{Iso}_{\text{Cay}}(\mathcal{A}, \mathcal{A}) \leq \text{Sym}(H); \\ \text{Aut}_{\text{com}}(\mathcal{A}) &:= \text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{A}) \leq \text{Sym}(H); \\ \text{Aut}_{\text{alg}}(\mathcal{A}) &:= \text{Iso}_{\text{alg}}(\mathcal{A}, \mathcal{A}) \leq \text{Sym}(\text{Basic}(\mathcal{A})).\end{aligned}$$

The subgroup of $\text{Aut}_{\text{com}}(\mathcal{A})$ consisting of all automorphisms f which induce the trivial algebraic automorphism of $\mathcal{A}$ (i.e. f^* is the identity) will be denoted by $\text{Aut}(\mathcal{A})$. We call these automorphisms **strong automorphisms** of a Schur ring (cf. with similarly defined notions in [22]). If $\text{Basic}(\mathcal{A}) = \{T_0, \dots, T_r\}$, then

$$\text{Aut}(\mathcal{A}) = \bigcap_{0 \leq i \leq r} \text{Aut}(\text{Cay}(H, T_i)).$$

We have $\text{Aut}(\mathcal{A}) \trianglelefteq \text{Aut}_{\text{com}}(\mathcal{A})$.

The symmetric group $\text{Sym}(H)$ contains two natural copies of H , namely H_R and H_L defined as follows:

$$\begin{aligned}H_R &:= \{h_R \mid h \in H\}, \quad x^{h_R} := xh, \quad x \in H, \\ H_L &:= \{h_L \mid h \in H\}, \quad x^{h_L} := h^{-1}x, \quad x \in H.\end{aligned}$$

Since H_R is a subgroup of the automorphism group of an arbitrary Cayley graph $\text{Cay}(H, S)$, we have $H_R \leq \text{Aut}(\mathcal{A})$ for each S-ring $\mathcal{A} \subseteq \mathbb{Q}H$.

The group $\text{Aut}_{\text{Cay}}(\mathcal{A})$ is a subgroup of the normalizer of H_R in $\text{Sym}(H)$ which is isomorphic to the holomorph $H \rtimes \text{Aut}(H)$ of H and acts on H by the following rule: $x^{(h, \varphi)} = x^\varphi h$. More precisely $\text{Aut}_{\text{Cay}}(\mathcal{A}) = H \rtimes \Phi$ where $\Phi \leq \text{Aut}(H)$ consists of all automorphisms which satisfy

$$T^\varphi = T \text{ for all } T \in \text{Basic}(\mathcal{A}).$$

An S-ring $\mathcal{A}$ over a group H is called **CI-S-ring** if for arbitrary S-ring $\mathcal{B}$ over H and any $f \in \text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{B})$ there exists an automorphism $g \in \text{Aut}(H)$ such that $T^{f^*} = T^g$ for each $T \in \text{Basic}(\mathcal{A})$. If $f \in \text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{B})$ is a combinatorial isomorphism, then fh_R is also a combinatorial isomorphism between the same Schur rings, and, moreover $f^* = (fh_R)^*$. If $h = f(e)^{-1}$, then fh_R will be a normalized combinatorial isomorphism. Therefore an S-ring $\mathcal{A}$ is a CI-S-ring if and only if for each normalized combinatorial isomorphism $f \in \text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{B})$ there exists an automorphism $\varphi \in \text{Aut}(H)$ such that $T^f = T^\varphi$ for each $T \in \text{Basic}(\mathcal{A})$.

3.4. S-rings and Cayley graphs. Given a Cayley graph $\text{Cay}(H, S)$, $S \subseteq H$, we can associate the S-ring $\langle\langle S \rangle\rangle$ generated by its connection set. It turns out that there exists a deep connection between the properties of S and $\langle\langle S \rangle\rangle$. In what follows we shall write $\langle\langle S \rangle\rangle$ instead of $\langle\langle S \rangle\rangle$.

THEOREM 3.7 ([69]). *Let $f : H \rightarrow K$ be an isomorphism between the Cayley graphs $\text{Cay}(H, S)$ and $\text{Cay}(K, R)$. Then*

- (1) *f is a combinatorial isomorphism between $\langle\langle S \rangle\rangle$ and $\langle\langle R \rangle\rangle$. In particular $|\text{Basic}(\langle\langle S \rangle\rangle)| = |\text{Basic}(\langle\langle R \rangle\rangle)|$;*
- (2) *$\langle\langle S \rangle\rangle \cong_{\text{alg}} \langle\langle R \rangle\rangle$;*
- (3) *Let $S = \bigcup \{B \mid B \in I\}$ be the decomposition of S into a disjoint union of basic sets of $\langle\langle S \rangle\rangle$ ($I \subseteq \text{Basic}(\mathcal{A})$), then $R = \bigcup \{B^{f^*} \mid B \in I\}$.*

In a particular case, namely when $H = K$ and $S = T$ we have a stronger result which is very useful in computing of the automorphism group of a Cayley graph.

THEOREM 3.8 ([69]). *Let $f \in \text{Sym}(H)$ be an automorphism of a Cayley graph $\text{Cay}(H, S)$. Then $f \in \text{Aut}(\langle\langle S \rangle\rangle)$ and $f^* \in \text{Aut}_{\text{alg}}(\langle\langle S \rangle\rangle)$.*

As a consequence we can easily obtain the following useful statement:

THEOREM 3.9. *A subset $S \subseteq H$ is a CI-subset if and only if $\langle\langle S \rangle\rangle$ is a CI-S-ring over H .*

PROOF. Let S be an CI-subset, $\mathcal{A} := \langle\langle S \rangle\rangle$ and $f \in \text{Iso}_{\text{com}}(\mathcal{A}, \mathcal{B})$ be an arbitrary combinatorial isomorphism between $\mathcal{A}$ and some S-ring $\mathcal{B}$. W.l.o.g. we may assume that f is normalized. Let $S = \bigcup_{i \in I} S_i$ be a decomposition of S into basic sets of $\mathcal{A}$. Then $\text{Cay}(H, S_i)^f = \text{Cay}(H, S_i^{f^*})$ and $\text{Cay}(H, S)^f = \text{Cay}(H, T)$, where $T = \bigcup_{i \in I} S_i^{f^*}$. Since S is a CI-subset, there exists $g \in \text{Aut}(H)$ such that $T = S^g$. Therefore $fg^{-1} \in \text{Aut}(\text{Cay}(H, S))$. By Theorem 3.7, $fg^{-1} \in \text{Aut}(\mathcal{A})$, implying $R^{(fg^{-1})^*} = R$ for each $R \in \text{Basic}(\mathcal{A})$. Since fg^{-1} is normalized, $R^{fg^{-1}} = R$ implying that $R^{f^*} = R^f = R^g$ for each $R \in \text{Basic}(\mathcal{A})$, as desired.

Assume now that $\mathcal{A} := \langle\langle S \rangle\rangle$ is a CI-S-ring and let $\text{Cay}(H, T)$ be a Cayley graph isomorphic to $\text{Cay}(H, S)$. Let f be an arbitrary isomorphism between $\text{Cay}(H, S)$ and $\text{Cay}(H, T)$, i.e., $\text{Cay}(H, S)^f = \text{Cay}(H, T)$. Then, by Theorem 3.7, f is a combinatorial isomorphism between the S-rings $\mathcal{A}$ and $\mathcal{B} := \langle\langle T \rangle\rangle$. Since $\mathcal{A}$ is a CI-S-ring there exists $g \in \text{Aut}(H)$ such that $fg^{-1} \in \text{Aut}(\mathcal{A})$. Then $R^{f^*} = R^g$ holds for each $R \in \text{Basic}(\mathcal{A})$ and our claim follows easily from part (3) of Theorem 3.7. $\square$

The following result is a direct analogue to Theorem 2.1:

THEOREM 3.10. *An S-ring $\mathcal{A}$ over a group H is a CI-S-ring if and only if any two regular H -isomorphic subgroups of $\text{Aut}(\mathcal{A})$ are conjugate in $\text{Aut}(\mathcal{A})$.*

We shall say that an algebraic isomorphism $f : \mathcal{A} \rightarrow \mathcal{B}$ is **induced by a group automorphism** if there exists a group automorphism $\varphi \in \text{Aut}(H)$ such that $T^f = T^\varphi$ for each basic set T of $\mathcal{A}$. The following claim is a direct consequence of the definition of an CI-S-ring and gives a sufficient condition for being a CI-S-ring which easily can be verified.

THEOREM 3.11. *Let $\mathcal{A}$ be an S-ring over a group H . Assume that for every S-ring $\mathcal{B} \subseteq \mathbb{Q}H$ algebraically isomorphic to $\mathcal{A}$ each algebraic isomorphism $f \in \text{Iso}_{\text{alg}}(\mathcal{A}, \mathcal{B})$ is induced by a group automorphism. Then $\mathcal{A}$ is a CI-S-ring.*

3.5. S-rings and permutation groups. As we have seen before, the automorphism group of a Cayley graph $\text{Cay}(H, S)$ contains the subgroup H_R which is a regular subgroup of the symmetric group $\text{Sym}(H)$. Consider an arbitrary group $G \leq \text{Sym}(H)$ which contains H_R as a subgroup. Let $\{e\} = T_0, T_1, \dots, T_r$ be all the orbits of G_e . The vector space spanned by the simple quantities T_i ($i \in \{0, \dots, r\}$) is called the **transitivity module** of G and is denoted by $\mathcal{S}(H, G_e)$. The following result was proved by I. Schur in 1933.

THEOREM 3.12 ([85, Theorem 24.1]). *The transitivity module $\mathcal{S}(H, G_e)$ is an S-ring over H .*

Not every S-ring is the transitivity module of some permutation group. An S-ring which is the transitivity module of some group G , $H_R \leq G \leq \text{Sym}(H)$, is called a **Schurian S-ring** ([73]).

Let $\Phi \leq \text{Aut}(H)$ be an arbitrary subgroup. The group $G := H \rtimes \Phi$ acts on H by the following rule: $x^{(h, \varphi)} = x^\varphi h$. Since G contains H_R , the transitivity module

$S(H, G_e)$ is an S-ring. The basic sets of this S-ring are exactly the orbits of Φ on H . It may be characterized as the subspace of $\mathbb{Q}H$ which consists of all elements fixed by Φ . We denote this S-ring by $S(H, \Phi)$.

The connection between permutation groups and Schur rings is reflected in the following theorem.

THEOREM 3.13. *Let $\mathcal{A}$ and $\mathcal{B}$ be arbitrary S-rings over a group H and let G and K be arbitrary overgroups of H_R in $\text{Sym}(H)$. Then*

- (1) $\mathcal{A} \subseteq \mathcal{B} \implies \text{Aut}(\mathcal{A}) \geq \text{Aut}(\mathcal{B})$,
- (2) $G \leq K \implies S(H, G_e) \supseteq S(H, K_e)$,
- (3) $\mathcal{A} \subseteq S(H, \text{Aut}(\mathcal{A})_e)$,
- (4) $G \leq \text{Aut}(S(H, G_e))$.

This statement describes a Galois correspondence between S-rings over H and overgroups of the regular permutation group H_R in $\text{Sym}(H)$. It is a particular case of a Galois correspondence between coherent configurations and permutation groups [23, 25]. Theorem 3.13 implies that an S-ring $\mathcal{A}$ is Schurian if and only if $\mathcal{A} = S(H, \text{Aut}(\mathcal{A})_e)$.

3.6. An example. In this subsection we show by example how to use S-ring theory for proving that a certain group is a CI-group. We take the quaternion group Q_8 which is known to be a CI-group (see, for example, [54]). We use the standard notation for the elements of Q_8 : $1, i, j, k, -1, -i, -j, -k$ where $i^2 = j^2 = k^2 = ijk = -1$.

The complete list of all S-rings over Q_8 can be found e.g. by the computer package COCO [24]. There are 24 non-trivial S-rings over Q_8 which are spread into 10 Cayley-isomorphism classes. We give a list of representatives of these classes:

$$\mathcal{A}_1 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3}, \underline{T_4}, \underline{T_5} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{k\}, T_2 = \{-1\}, T_3 = \{-k\}, T_4 = \{i, -i\}, T_5 = \{j, -j\};$$

$$\mathcal{A}_2 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3}, \underline{T_4} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{-1\}, T_2 = \{i, -i\}, T_3 = \{j, k\}, T_4 = \{-j, -k\};$$

$$\mathcal{A}_3 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3}, \underline{T_4} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{-1\}, T_2 = \{i, -i\}, T_3 = \{j, -j\}, T_4 = \{k, -k\};$$

$$\mathcal{A}_4 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3}, \underline{T_4} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{k\}, T_2 = \{-1\}, T_3 = \{-k\}, T_4 = \{i, -i, j, -j\};$$

$$\mathcal{A}_5 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{-1\}, T_2 = \{k, -k\}, T_3 = \{i, -i, j, -j\};$$

$$\mathcal{A}_6 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2}, \underline{T_3} \rangle \quad \text{with}$$

$$T_0 = \{1\}, T_1 = \{-1\}, T_2 = \{i, j, k\}, T_3 = \{-i, -j, -k\};$$

$$\mathcal{A}_7 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2} \rangle \quad \text{with} \quad T_0 = \{1\}, T_1 = \{k, -1, -k\}, T_2 = \{i, j, -i, -j\};$$

$$\mathcal{A}_8 = \langle \underline{T_0}, \underline{T_1}, \underline{T_2} \rangle \quad \text{with} \quad T_0 = \{1\}, T_1 = \{-1\}, T_2 = \{i, j, k, -i, -j, -k\};$$

$$\mathcal{A}_9 = \langle \underline{T_0}, \underline{T_1} \rangle \quad \text{with} \quad T_0 = \{1\}, T_1 = \{-1, i, j, k, -i, -j, -k\};$$

$$\mathcal{A}_{10} = \mathbb{Q}Q_8.$$

Our goal is to show that each S-ring in the list is a CI-S-ring. By Theorem 3.11 it is sufficient to show that each algebraic isomorphism between two S-rings is induced by a group automorphism. Thus we have to study algebraic isomorphisms between the enumerated S-rings. Two algebraically isomorphic S-rings not only have the same number of basic sets, but also have the same multisets of basic set cardinalities. Using this observation we can easily find that all S-rings $\mathcal{A}_1 - \mathcal{A}_{10}$ are pairwise non-isomorphic algebraically. Thus each algebraic isomorphism between two S-rings is, in fact, an algebraic automorphism of one of the S-rings $\mathcal{A}_i$, $i = 1, \dots, 8$. There are S-rings the non-trivial basic sets of which are of distinct cardinalities (S-rings $\mathcal{A}_5, \mathcal{A}_7, \mathcal{A}_8, \mathcal{A}_9$); $\mathcal{A}_{10}$ is a trivial S-ring and therefore it is an CI-S-ring. Therefore their groups of algebraic automorphisms are trivial and the corresponding S-rings are CI. We consider the remaining cases.

S-ring $\mathcal{A}_1$: There is only one basic set X which satisfies $X^2 = T_0$, namely T_2 . Therefore $T_2^f = T_2$ for each $f \in \text{Aut}_{\text{alg}} \mathcal{A}_1$. Analogously, the equation $X^2 = T_2$ has two solutions: T_1 and T_3 . Hence $\{T_1, T_3\}^f = \{T_1, T_3\}$ for every $f \in \text{Aut}_{\text{alg}} \mathcal{A}_1$. As we mentioned before, an algebraic automorphism preserves the cardinality of basic sets. Therefore $\{T_4, T_5\}^f = \{T_4, T_5\}$ and, finally, $\text{Aut}_{\text{alg}} \mathcal{A}_1 \leq \{1, (13), (45), (13)(45)\}$. On the other hand, a direct check shows $(\text{Aut}_{\text{Cay}} \mathcal{A}_1)^* = \{1, (13), (45), (13)(45)\}$. By Theorem 3.11, $\mathcal{A}_1$ is a CI-S-ring.

S-ring $\mathcal{A}_2$: Since T_1 is the unique non-trivial basic set of cardinality 1, $T_1^f = T_1$ for each $f \in \text{Aut}_{\text{alg}} \mathcal{A}_1$. T_2 is the unique symmetric basic set of cardinality 2. Therefore $T_2^f = T_2$ for each $f \in \text{Aut}_{\text{alg}} \mathcal{A}_1$. Thus $\text{Aut}_{\text{alg}} \mathcal{A}_2 \leq \{1, (34)\}$. Together with $(\text{Aut}_{\text{Cay}} \mathcal{A}_2)^* = \{1, (34)\}$ we obtain that $\mathcal{A}_2$ is a CI-S-ring.

In the same fashion one can show that every S-ring in our list has the property $(\text{Aut}_{\text{Cay}} \mathcal{A}_i)^* = \text{Aut}_{\text{alg}} \mathcal{A}_i$, $i = 1, \dots, 10$. Thus, by Theorem 3.11, every S-ring over Q_8 is a CI-S-ring and, therefore, Q_8 is a CI-group.

4. Schur rings over a cyclic group

In order to avoid confusion between addition in the group algebra and addition in $\mathbb{Z}_n$ we shall use multiplicative notation for the cyclic group of order n . Thus C_n will stand for a cyclic group of order n , the identity element will be denoted by e , and by g_0 we denote a generator of the group. The automorphism group of C_n will be identified with $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid \gcd(x, n) = 1\}$, where the action of $m \in \mathbb{Z}_n^*$ on C_n is defined by $g \mapsto g^m$. If $X = \sum_{g \in C_n} x_g g$ is an arbitrary element of $\mathbb{Q}C_n$, then for an integer m let $X^{(m)}$ denote the element $\sum_{g \in C_n} x_g g^m$. The mapping $X \mapsto X^{(m)}$ is bijective if and only if $\gcd(m, n) = 1$. For $T \subseteq C_n$ and an integer m let $T^{(m)} := \{t^m \mid t \in T\}$. If $\gcd(m, n) = 1$, then $\underline{T}^{(m)} = \underline{T}^{(m)}$. For an arbitrary subset $S \subseteq C_n$ we define two groups: $\text{Sta}_+(S) := \{g \in C_n \mid gS = S\} \leq C_n$ and $\text{Sta}_*(S) := \{m \in \mathbb{Z}_n^* \mid S^{(m)} = S\} \leq \mathbb{Z}_n^*$.

4.1. Classical results. The first result about the structure of S-rings over a cyclic group was obtained by I. Schur in 1933.

THEOREM 4.1 ([77]). *If n is not prime, then each non-trivial S-ring over C_n is imprimitive.*

If n is prime, then each S-ring over C_n will be primitive. The classification of all S-rings over a cyclic group of prime order p can be easily obtained (see the references in Section 7).

THEOREM 4.2. *Let p be a prime number. Then each S -ring over C_p coincides with $\mathcal{S}(C_p, \Phi)$ for some $\Phi \leq \mathbb{Z}_n^*$.*

The following statement is very useful for the study of S -rings over cyclic groups.

PROPOSITION 4.3. [85] *Let $\mathcal{A}$ be an S -ring over C_n . Then, for each $m \in \mathbb{Z}_n^*$, we have $T \in \text{Basic}(\mathcal{A}) \iff T^{(m)} \in \text{Basic}(\mathcal{A})$.*

Two basic sets S and T of $\mathcal{A}$ are called **conjugate** if there exists an $m \in \mathbb{Z}_n^*$ such that $S^{(m)} = T$. It is easy to see that conjugacy is an equivalence relation on $\text{Basic}(\mathcal{A})$. The set $\hat{T} := \bigcup \{T^{(m)} \mid m \in \mathbb{Z}_n^*\}$ is called the **trace** of T . Let $\hat{\mathcal{A}}$ denote the vector space spanned by the simple quantities $\hat{T}$, $T \in \text{Basic}(\mathcal{A})$. Since $\hat{\mathcal{A}} = \mathcal{A} \cap \mathcal{S}(C_n, \mathbb{Z}_n^*)$, $\hat{\mathcal{A}}$ is an S -ring over C_n which is a fusion of $\mathcal{A}$. An S -ring is called **rational** (or an **S -ring of traces**) if $\mathcal{A} = \hat{\mathcal{A}}$.

4.2. Algebraic isomorphisms between S -rings over a cyclic group. We start with the following theorem.

THEOREM 4.4 ([64, Theorem 1.1']). *Let $\lambda : \mathcal{A} \rightarrow \mathcal{B}$ be an algebraic isomorphism between two S -rings $\mathcal{A}$ and $\mathcal{B}$ over C_n and let $\underline{T}$ be a basic quantity of $\mathcal{A}$. Then $(\underline{T})^\lambda = \underline{T}^{(m)}$ for some $m \in \mathbb{Z}_n^*$.*

REMARK. Notice that the exponent m may depend on the basic set T .

As a consequence of this theorem and Proposition 4.3 we obtain:

THEOREM 4.5. ([64, Theorem 1.1]) *Any two algebraically isomorphic S -rings over C_n coincide.*

Theorem 4.4 and Theorem 4.5 imply the following theorem.

THEOREM 4.6 ([64]). *Let $\mathcal{A} = \langle \underline{T}_0, \dots, \underline{T}_r \rangle$ be an S -ring over C_n and let $\lambda : \text{Basic}(\mathcal{A}) \rightarrow \text{Basic}(\mathcal{A})$ be an algebraic automorphism of $\mathcal{A}$. Then for every $T \in \text{Basic}(\mathcal{A})$ there exists $m_T \in \mathbb{Z}_n^*$ such that $T^\lambda = T^{(m_T)}$.*

Thus each algebraic automorphism of $\mathcal{A}$ is uniquely determined by the data $(m_T)_{T \in \text{Basic}(\mathcal{A})}$ but not vice versa, since each m_T may be replaced by any product m_{Tc} with $c \in \text{Sta}_*(T)$. On the other hand, an arbitrary choice of $(m_T)_{T \in \text{Basic}(\mathcal{A})}$ may not correspond to a combinatorial automorphism of $\mathcal{A}$, since there may be some dependencies between the exponents m_T . To show the simplest connections between the exponents we need the following statement.

LEMMA 4.7 ([64, Prop. 3.1]). *Let f be an algebraic automorphism of an S -ring $\mathcal{A}$ over C_n . Then for every simple quantity $\underline{T} \in \mathcal{A}$ and $m \in \mathbb{Z}_n^*$ we have*

- (1) $(\underline{T}^{(m)})^f = (\underline{T}^f)^{(m)}$,
- (2) $\text{Sta}_*(\underline{T}^f) = \text{Sta}_*(\underline{T})$.

For $d|n$, let $(C_n)_d$ denote the set of all elements in C_n of order n/d . Given $S \subseteq C_n$ we define the **layer**

$$(S)_d := S \cap (C_n)_d.$$

LEMMA 4.8 ([69]). *Let f be an algebraic automorphism of an S -ring $\mathcal{A}$ over C_n . Then for each $d|n$ there exists an $m_d \in \mathbb{Z}_n^*$ such that $T^f = T^{(m_d)}$ for all $T \in \text{Basic}(\mathcal{A})$ with $(T)_d \neq \emptyset$.*

PROOF. Fix an arbitrary $T \in \text{Basic}(\mathcal{A})$ with $T \cap (C_n)_d \neq \emptyset$. By Theorem 4.6 we know that $T^f = T^{(m_T)}$ for some $m_T \in \mathbb{Z}_n^*$. If T and T' are two basic sets of $\mathcal{A}$ which intersect non-trivially $(C_n)_d$, then there exists an $m \in \mathbb{Z}_n^*$ with $T^{(m)} \cap T' \neq \emptyset$. Therefore $T' = T^{(m)}$. By Lemma 4.7, $T'^f = (T^{(m)})^f = (T^f)^{(m)} = (T^{(m_T)})^{(m)} = T^{(m_T m)} = T^{(m m_T)} = T'^{(m_T)}$. Thus we can choose $m_d := m_T$. $\square$

5. Application of Schur rings to the isomorphism problem for circulants

5.1. Proofs of Zibin's and Toida's conjectures.

THEOREM 5.1 (ZIBIN'S CONJECTURE [69]). *Let $\text{Cay}(C_n, S)$ and $\text{Cay}(C_n, R)$ be two isomorphic circulant graphs. Then for each $d|n$ there exists $m_d \in \mathbb{Z}_n^*$ such that $(S)_d^{(m_d)} = (R)_d$.*

PROOF. Let $f : C_n \rightarrow C_n$ be an isomorphism between the Cayley graphs $\text{Cay}(C_n, S)$ and $\text{Cay}(C_n, R)$. Then, by Theorem 3.7(1)-(2), f is a combinatorial isomorphism between $\langle\langle S \rangle\rangle$ and $\langle\langle R \rangle\rangle$ which induces an algebraic isomorphism f^* between $B_S := \text{Basic}(\langle\langle S \rangle\rangle)$ and $B_R := \text{Basic}(\langle\langle R \rangle\rangle)$. By 3.7(3) we have $R = \bigcup \{T^{f^*} \mid T \in B_S \text{ and } T \subseteq S\}$. Therefore

$$\begin{aligned}
 (R)_d &= \bigcup \{T^{f^*} \cap (C_n)_d \mid T \in B_S \text{ and } T \subseteq S\} \\
 &\stackrel{(4.6)}{=} \bigcup \{T^{(m_T)} \cap (C_n)_d \mid T \in B_S \text{ and } T \subseteq S\} \\
 &= \bigcup \{(T \cap (C_n)_d)^{(m_T)} \mid T \in B_S \text{ and } T \subseteq S\} \\
 &= \bigcup \{(T \cap (C_n)_d)^{(m_T)} \mid T \in B_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\} \\
 &\stackrel{(4.8)}{=} \bigcup \{(T \cap (C_n)_d)^{(m_d)} \mid T \in B_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\} \\
 &= \left(\bigcup \{(T \cap (C_n)_d) \mid T \in B_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\} \right)^{(m_d)} \\
 &= (S)_d^{(m_d)}.
 \end{aligned}$$

$\square$

Since Toida's conjecture is a partial case of Zibin's conjecture, the above result implies the following:

THEOREM 5.2 (TOIDA'S CONJECTURE). *Every $S \subseteq \mathbb{Z}_n^*$ is a CI-subset of $\mathbb{Z}_n$.*

Another class of CI-subsets of the cyclic group is described in the following statement which is a direct consequence of Theorem 4.6.

THEOREM 5.3. *If a subset $T \subset C_n$ is a basic set of some S -ring over C_n , then T is a CI-subset. In particular, this is true if the circulant $\text{Cay}(C_n, T)$ is arc-transitive.*

REMARK. It was shown by C.H. Li [57] that an arc-transitive circulant graph $\text{Cay}(C_n, T)$ is a CI-graph. His proof is purely group-theoretical and relies on the classification of finite simple groups.

5.2. Isomorphism problem for double-loop circulants. As an illustration of the previous results we shall solve the isomorphism problem for a special class of circulant graphs, so-called double-loop circulants. Following [82] a **double-loop circulant graph** is (in the original additive notation) a circulant $\text{Cay}(\mathbb{Z}_n, S)$

with $S = \{a, -a, b, -b\}$, $|S| = 4$. The isomorphism problem for double-loop circulants was considered in several publications [26, 60, 62]. It was shown in [26] that S is a CI-subset of $\mathbb{Z}_n$. We give a short proof of this result based on S-ring theory.

THEOREM 5.4. *Every 4-element subset $S = \{a, -a, b, -b\}$, $|S| = 4$ of $\mathbb{Z}_n$ is a CI-subset.*

PROOF. First we switch to the multiplicative notation. Let $H = C_n$, $S = \{a, a^{-1}, b, b^{-1}\}$ and $\mathcal{A} := \langle\langle S \rangle\rangle$. Without loss of generality we may assume that the graph $\text{Cay}(C_n, S)$ is connected. If S is a basic set of $\mathcal{A}$, then S is a CI-subset by Theorem 5.3. Assume the contrary, i.e., let S be a union of at least two basic sets. By Theorem 3.9 we have to show that $\mathcal{A}$ is a CI-S-ring. The simple quantity $\underline{S}$ belongs to the vector space $\mathcal{B} := \text{Span}_{\mathbb{Q}}\{g + g^{-1} \mid g \in C_n\}$. Since $\mathcal{B} = \mathcal{S}(C_n, \Phi)$ for $\Phi = \{1, -1\} \leq \mathbb{Z}_n^*$, it is a Schur ring over C_n . Therefore $\mathcal{A} \subseteq \mathcal{B}$ and each basic set of $\mathcal{A}$ is symmetric. But there is a unique way to split S into a union of symmetric subsets of C_n : $S = \{a, a^{-1}\} \cup \{b, b^{-1}\}$. Therefore $A := \{a, a^{-1}\}$ and $B := \{b, b^{-1}\}$ are basic sets of $\mathcal{A}$. Since the graph $\text{Cay}(C_n, S)$ is connected, $\langle a, b \rangle = C_n$.

To prove that $\mathcal{A}$ is a CI-S-ring it is sufficient to show that each algebraic automorphism of $\mathcal{A}$ is induced by some automorphism of C_n . Let λ be an algebraic automorphism of $\mathcal{A}$. Then by Theorem 4.6 there exist $m_a, m_b \in \mathbb{Z}_n^*$ such that $A^\lambda = A^{(m_a)}$, $B^\lambda = B^{(m_b)}$. We have to show that there exists an automorphism $m \in \mathbb{Z}_n^*$ such that $A^{(m_a)} = A^{(m)}$ and $B^{(m_b)} = B^{(m)}$. Since the group $\langle a, b \rangle$ is cyclic, the automorphisms $x \mapsto x^{m_a}$, $x \in \langle a \rangle$, and $x \mapsto x^{m_b}$, $x \in \langle b \rangle$, are induced by an automorphism of $\langle a, b \rangle$ if and only if they agree on the intersection $F = \langle a \rangle \cap \langle b \rangle$. Thus we have to show that the automorphisms m_a and m_b may be chosen in such a way that their restrictions to F induce the same automorphism, i.e., $x^{m_a} = x^{m_b}$ for each $x \in F$. Let s, t be natural numbers such that $f := a^s = b^t \in F$ and f generates F .

The elements $A^{(k)}$, $B^{(k)}$ ($k \geq 1$) satisfy the recurrences $AA^{(k)} = A^{(k-1)} + A^{(k+1)}$, $BB^{(k)} = B^{(k-1)} + B^{(k+1)}$. Therefore, by induction on k , we obtain

$$\begin{aligned} (A^{(k)})^\lambda &= (A^{(k)})^{(m_a)}, \\ (B^{(k)})^\lambda &= (B^{(k)})^{(m_b)} \end{aligned}$$

In particular,

$$(a^t + a^{-t})^\lambda = (a^t + a^{-t})^{(m_a)},$$

and

$$(b^s + b^{-s})^\lambda = (b^s + b^{-s})^{(m_b)}.$$

Together with

$$(a^t + a^{-t})^\lambda = (b^s + b^{-s})^\lambda$$

we obtain $b^{sm_b} \in \{a^{tm_a}, a^{-tm_a}\}$. Replacing m_b by $-m_b$, if necessary, we obtain $b^{sm_b} = a^{tm_a}$, or, equivalently, $f^{m_a} = f^{m_b}$. Since m_a and m_b agree on the intersection $\langle a \rangle \cap \langle b \rangle$, there exists an $m \in \mathbb{Z}_n^*$ such that the restrictions of m onto the subgroups $\langle a \rangle$, $\langle b \rangle$ coincide with m_a and m_b respectively. $\square$

5.3. Solution of the isomorphism problem for $\mathbb{Z}_8$. In previous subsections we dealt only with necessary conditions for being a CI-subset. Here we shall apply S-rings to get a solution for the isomorphism problem for a particular cyclic group, namely the cyclic group of order 8. In this subsection, instead of C_8 we use the additive notation $\mathbb{Z}_8$ for the cyclic group.

We start with a complete list of S-rings over $\mathbb{Z}_8$ which was obtained in [32, 33, 44]. It contains the following S-rings:

$$\mathcal{A}_1 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2 \rangle \quad \text{with} \quad T_0 = \{0\}, T_1 = \{1, 2, 3, 4, 5, 6, 7\};$$

$$\mathcal{A}_2 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2 \rangle \quad \text{with} \quad T_0 = \{0\}, T_1 = \{1, 3, 5, 7\}, T_2 = \{2, 6, 4\};$$

$$\mathcal{A}_3 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2 \rangle \quad \text{with} \quad T_0 = \{0\}, T_1 = \{1, 3, 5, 7, 2, 6\}, T_2 = \{4\};$$

$$\mathcal{A}_4 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3 \rangle \quad \text{with} \quad T_0 = \{0\}, T_1 = \{1, 3, 5, 7\}, T_2 = \{2, 6\}, T_3 = \{4\};$$

$$\mathcal{A}_5 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3, \underline{T}_4 \rangle \quad \text{with} \\ T_0 = \{0\}, T_1 = \{1, 3, 5, 7\}, T_2 = \{2\}, T_3 = \{6\}, T_4 = \{4\};$$

$$\mathcal{A}_6 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3, \underline{T}_4, \underline{T}_5 \rangle \quad \text{with} \\ T_0 = \{0\}, T_1 = \{1, 5\}, T_2 = \{3, 7\}, T_3 = \{2\}, T_4 = \{6\}, T_5 = \{4\};$$

$$\mathcal{A}_7 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3, \underline{T}_4 \rangle \quad \text{with} \\ T_0 = \{0\}, T_1 = \{1, 5\}, T_2 = \{3, 7\}, T_3 = \{2, 6\}, T_4 = \{4\};$$

$$\mathcal{A}_8 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3, \underline{T}_4 \rangle \quad \text{with} \\ T_0 = \{0\}, T_1 = \{1, 3\}, T_2 = \{5, 7\}, T_3 = \{2, 6\}, T_4 = \{4\};$$

$$\mathcal{A}_9 = \langle \underline{T}_0, \underline{T}_1, \underline{T}_2, \underline{T}_3, \underline{T}_4 \rangle \quad \text{with} \\ T_0 = \{0\}, T_1 = \{1, 7\}, T_2 = \{3, 5\}, T_3 = \{2, 6\}, T_4 = \{4\};$$

$$\mathcal{A}_{10} = \mathbb{Q}\mathbb{Z}_8.$$

Our goal is to find all non-CI-S-rings among this list. We shall use the sufficient condition formulated in Theorem 3.11 which means that we have to study algebraic isomorphisms between the enumerated S-rings.

First we note that $\mathcal{A}_1$ and $\mathcal{A}_{10}$ are CI, since they are trivial S-rings. By Theorem 4.5 two distinct S-rings over $\mathbb{Z}_8$ are pairwise non-isomorphic algebraically. Therefore, each algebraic isomorphism between two S-rings is, in fact, an algebraic automorphism of one of the S-rings $\mathcal{A}_i$, $i = 1, \dots, 10$.

Let now $\mathcal{A}$ be one of the above S-rings and let f be one of its algebraic automorphisms. Since $T_0^f = T_0$ and f preserves the cardinalities of basic sets, those S-rings where all non-identical basic sets have distinct cardinalities have a trivial group $\text{Aut}_{\text{alg}}\mathcal{A}$, and, therefore, are CI-S-rings. This excludes S-rings $\mathcal{A}_1 - \mathcal{A}_4$ from being non-CI-S-rings.

The S-rings $\mathcal{A}_7, \mathcal{A}_8, \mathcal{A}_9$ have a unique non-trivial basic set of cardinality one: $\{4\}$. Therefore $\{4\}^f = \{4\}$ for each $f \in \text{Aut}_{\text{alg}}\mathcal{A}$. Furthermore, $\{2, 6\}$ is the unique symmetric basic set T of $\mathcal{A}$ which satisfies $T + T = \{4\}$. Therefore $\{2, 6\}^f = \{2, 6\}$ for each $f \in \text{Aut}_{\text{alg}}\mathcal{A}$. Thus each algebraic automorphism of $\mathcal{A}$ fixes T_0, T_3 and T_4 . Thus either it is trivial or it swaps T_1 and T_2 . In both cases it is induced by a group automorphism of $\mathbb{Z}_8$.

Thus $\mathcal{A}_6$ is the remaining candidate for a non-CI-S-ring. Take an arbitrary $f \in \text{Aut}_{\text{alg}}\mathcal{A}$. Since T_3 and T_4 are the only basic sets which satisfy the equation $X + X + X = T_0$, either $T_3^f = T_3, T_4^f = T_4$ or $T_3^f = T_4, T_4^f = T_3$. As f preserves the cardinalities of basic sets, $\{T_1, T_2\}$ and $\{T_3, T_4, T_5\}$ are f -invariant sets. Combining these results we obtain that f must be one of the following four permutations: $\text{id}, (3, 4), (1, 2), (3, 4)(1, 2)$. A direct check shows that each of this permutations is

an algebraic automorphism of $\mathcal{A}_6$. The automorphism group of $\mathbb{Z}_n$ contains four permutations $x \mapsto x$, $x \mapsto 5x$, $x \mapsto 3x$, $x \mapsto 7x$. Each of these permutes the basic sets of $\mathcal{A}_6$, and, therefore, induces an algebraic automorphism of $\mathcal{A}_6$. The first two permutations act trivially on $\{T_0, T_1, \dots, T_5\}$. The two others induce the permutation $(3, 4)(1, 2)$. Therefore the algebraic automorphisms $(3, 4)$ and $(1, 2)$ are not induced by a group automorphism. If they are not induced by a combinatorial automorphism, then $\mathcal{A}_6$ also would be a CI-S-ring. In fact, it is sufficient to check one of them, say $(3, 4)$. So we are faced with the following question:

Does there exist a permutation $g \in \text{Sym}(\mathbb{Z}_8)$ such that

$$(*) \quad \begin{cases} \text{Cay}(\mathbb{Z}_8, T_1)^g = \text{Cay}(\mathbb{Z}_8, T_1), & \text{Cay}(\mathbb{Z}_8, T_2)^g = \text{Cay}(\mathbb{Z}_8, T_2), \\ \text{Cay}(\mathbb{Z}_8, T_3)^g = \text{Cay}(\mathbb{Z}_8, T_4), & \text{Cay}(\mathbb{Z}_8, T_4)^g = \text{Cay}(\mathbb{Z}_8, T_3), \\ \text{Cay}(\mathbb{Z}_8, T_5)^g = \text{Cay}(\mathbb{Z}_8, T_5)? \end{cases}$$

It turns out that the answer to this question is affirmative! Each element $x \in \mathbb{Z}_8$ has a unique presentation in the form $x = x_0 + 2x_1$ where $x_0 \in \{0, 1\}$, $x_1 \in \{0, 1, 2, 3\}$ and all arithmetic is done modulo 8. Define the permutation $g \in \text{Sym}(\mathbb{Z}_8)$ as follows $(x_0 + 2x_1)^g = x_0 + 6x_1$. A direct check shows that g satisfies $(*)$! Thus $\mathcal{A}_6$ is not a CI-S-ring. To build a non-CI-subset it is sufficient to find a union of basic sets of $\mathcal{A}_6$ which generates the whole S-ring. For this purpose we can examine the list of S-rings over $\mathbb{Z}_8$. The set $S = T_1 \cup T_3 = \{1, 5, 2\}$ does not appear as a union of basic sets of any S-ring except $\mathcal{A}_6$. Therefore $\langle\langle S \rangle\rangle = \mathcal{A}_6$. Using Theorem 3.9 we obtain that $\{1, 5, 2\}$ is a non-CI-subset. It should be mentioned that $\{1, 5, 2\}$ was the first known example of a non-CI-subset of a cyclic group ([21]).

Our detailed analysis of S-rings yields the complete solution of the isomorphism problem for $\mathbb{Z}_8$. In fact, any two isomorphic circulants on 8 points are either conjugate by a multiplier or an isomorphism between them may be realized as a product of g (as defined above) and a multiplier from $\mathbb{Z}_8^*$.

6. Schur rings and association schemes

S-rings were introduced by I. Schur in a purely group-theoretical way. Much later it was understood that S-rings are a special case of more general combinatorial objects known as association schemes. The aim of this section is to give a short introduction to the connection between these two objects. We start with the definition of an association scheme.

Let X be a finite set. A set $\mathcal{R} = \{R_0, \dots, R_r\}$ of binary relations forms an **association scheme** on X ([6]) if it satisfies the following conditions

AS1. $R_0 = I_X$, and $X^2 = R_0 \cup \dots \cup R_r$ is a disjoint union;

AS2. $\forall 0 \leq i \leq r \exists 0 \leq i' \leq r : R_i^\top = R_{i'};$ ⁵

AS3. For each triple $i, j, k \in \{0, \dots, r\}$ and arbitrary $(u, v) \in R_k$ the cardinality p_{ij}^k of the set $\{y \in X \mid (u, y) \in R_j \text{ and } (y, v) \in R_k\}$ depends on the triple (i, j, k) only and does not depend on the choice of the pair $(u, v) \in R_k$.

The numbers p_{ij}^k are called the **intersection numbers** of the association scheme $(X, \mathcal{R})$. The relations R_k are called **basic relations** of the association scheme. The (di)graphs $\Gamma_i = (X, R_i)$ are called **basic graphs** of the association scheme.

The **Bose-Mesner algebra** of an association scheme $(X, \mathcal{R})$ is the matrix algebra $\mathcal{W}$ the basis of which consists of the adjacency matrices A_i of the graphs

⁵Here $R^\top := \{(y, x) \mid (x, y) \in R\}$.

Γ_i , $i \in \{0, \dots, r\}$. This basis of adjacency matrices is called the **standard basis** of the Bose-Mesner algebra.

The **automorphism group** $\text{Aut}(\mathcal{W})$ of an association scheme $\mathcal{W} = (X, \mathcal{R})$ is defined as the intersection of the automorphism groups of all basic graphs Γ_i .

Every S-ring $\mathcal{A} = \langle \underline{T}_0, \dots, \underline{T}_r \rangle$ over a group H yields an association scheme on H the basic relations of which are the Cayley graphs $\text{Cay}(H, T_i)$, $i \in \{0, \dots, r\}$. We shall denote it by $\text{As}(\mathcal{A}) = (H; \{\text{Cay}(H, T_i)\}_{i=0}^r)$. A direct check shows that the structure constants of $\text{As}(\mathcal{A})$ coincide with the structure constants of $\mathcal{A}$. A combinatorial isomorphism between S-rings as introduced in Section 2 is a particular case of an association scheme isomorphism. More precisely, two S-rings $\mathcal{A} = \langle \underline{T}_0, \dots, \underline{T}_r \rangle \subseteq \mathbb{Q}H$ and $\mathcal{B} = \langle \underline{S}_0, \dots, \underline{S}_r \rangle \subseteq \mathbb{Q}F$ are combinatorially isomorphic if and only if the corresponding association schemes are isomorphic in the usual way. It is well-known that the automorphism group $\text{Aut}(\mathcal{A})$ as defined in Section 2 coincides with the automorphism group of the association scheme $\text{As}(\mathcal{A})$. As we have seen before, $\text{Aut}(\mathcal{A})$ contains the subgroup H_R , the right regular representation of the group H . Thus $\text{Aut}(\text{As}(\mathcal{A}))$ contains a regular subgroup isomorphic to H . This property characterizes the S-rings among the association schemes. Let $(X, \mathcal{R})$ ($\mathcal{R} = \{R_0, \dots, R_r\}$) be an association scheme on a set X . We say that $(X, \mathcal{R})$ is a **Cayley association scheme** over a group H if $\text{Aut}(\mathcal{R})$ contains a regular subgroup isomorphic to H .

Let $(X, \mathcal{R})$ be a Cayley association scheme, let H be a regular subgroup of $\text{Aut}(X, \mathcal{R})$ and let $x \in X$ be an arbitrary point. We define the **Schur projection** of a basic relation $R_i \in \mathcal{R}$ on H at $x \in X$ by

$$\text{Spr}_{H,x}(R_i) := \{h \in H \mid (x^h, x) \in R_i\}$$

Let $T_i := \text{Spr}_{H,x}(R_i)$ for $i \in \{0, 1, \dots, r\}$. Then the following properties are easy to check:

- (1) $\{T_0, \dots, T_r\}$ is a partition of H with $T_0 = \{e\}$;
- (2) If $R_i^T = R_j$ then $T_j = T_i^{(-1)}$;
- (3) $\text{Spr}_{H,x^h}(R_i) = h^{-1} \text{Spr}_{H,x}(R_i) h$.

Every $y \in X$ is of the form x^h for some uniquely determined $h \in H$. Thus by (3), if H is abelian, then $\text{Spr}_{H,x}(R_i)$ does not depend on the choice of $x \in X$.

The following theorem follows directly from the definitions.

THEOREM 6.1. *The vector space $\mathcal{A} := \langle \underline{T}_0, \dots, \underline{T}_r \rangle$ is an S-ring over H . The association schemes $(X, \mathcal{R})$ and $\text{As}(\mathcal{A})$ are isomorphic (as association schemes).*

Moreover, the above S-ring has the same structure constants as $(X, \mathcal{R})$ does:

$$\underline{T}_i \underline{T}_j = \sum_{k=0}^r p_{ij}^k \underline{T}_k.$$

In many cases the automorphism group of $(X, \mathcal{A})$ may contain more than one regular subgroup. The following result is a direct analogue to Babai's Theorem 2.1.

THEOREM 6.2. *Let $(X, \mathcal{R})$ be a Cayley association scheme and let H, K be two regular subgroups of $\text{Aut}(\mathcal{R})$. Then the Schur projections of $(X, \mathcal{R})$ on H and K are Cayley isomorphic if and only if H and K are conjugate in $\text{Aut}(\mathcal{R})$.*

Finally it should be mentioned that association schemes are a particular case of **coherent configurations** introduced by D. Higman [36, 37]. The shortest way to

define them is to drop the requirement that the diagonal relation is one of the basic relations of a scheme. Equivalent algebraic objects known as **cellular algebras** were introduced by B. Weisfeiler and A. Leman [83, 84].

7. Concluding remarks

7.1. Circulant matrices. Circulants have a long history. One of the first references is attributed to a paper by E. Catalan in 1846. In the 19th century, the theory of circulants was developed within the origins of matrix theory and especially determinants theory. The book [17] by Ph.J. Davis gives a vivid description of the place of circulants in matrix theory from the beginning of the century to the 1970's. It also introduces the reader to the powerful methods of spectral analysis of circulant matrices. These methods may be reformulated in modern terms of the so-called second standard basis in commutative coherent algebras, cf. [6, 25].

7.2. Different approaches to Ádám's conjecture. It is worth mentioning that the dates of the publications sometimes do not give exact attribution to the time when the corresponding result became known to experts. For example, [29] and [72] were available as preprints many years before the corresponding papers appeared, results of [46, 43] were reported in [45], etc. (We refer to the final note in [5], which cites already in August 1977 several of the above-mentioned results.)

7.3. Conjectures of Zibin' and Toida. The authors are much obliged to D.K. Zibin' (Riga) – an expert in technical cybernetics –, who attracted the attention of Klin and Pöschel to the isomorphism problem of circulant graphs. The computer experiments, arranged by him and his colleagues have played a very stimulative role. In fact, his conjecture was formulated on a less rigorous level, as an empirical observation based on the analysis of the experimental results. Toida's conjecture was independently considered and attacked in [15] by C.Y. Chao. However, the proof of the conjecture presented there contains a gap, namely: in the proof of the main result the author wrote (page 95, line 2) that, ω denoting the n -th root of unity, $\omega^0, \omega^1, \dots, \omega^{n-1}$ are linearly independent over $\mathbb{Q}$ contrary to the well-known identity $\omega^0 + \omega^1 + \dots + \omega^{n-1} = 0$. This error makes the whole proof incorrect.

7.4. Schur rings. Schur's method as a tool in group theory was known to experts for a long time due to its detailed presentation in [85, 50, 78]. As a combinatorial tool, it is still unpopular and has the reputation of a "heavy technique" (cf. [41]). One can mention a number of publications, where Schur's methodology was rediscovered, for example in the framework of the description of strongly regular circulant graphs (partial difference sets over cyclic groups) [61]. In the encyclopedical monograph [12], objects equivalent to S-rings are called translation association schemes.

Theorem 3.1 was implicitly used by many authors, see for example [11, 18]. In explicit form it was formulated in [63].

7.5. Circulants with a prime number of vertices. In explicit form all S-rings over $\mathbb{Z}_p$, p a prime, were first described in [73]. Much earlier, in 1965, B. Gordon introduced in [34] α -partitions of a group H , which are equivalent to S-rings. He also determined all α -partitions over $\mathbb{Z}_p$.

Chao used the method of Schur rings in [13] as a tool for the classification of vertex-transitive graphs. J. Turner in [81] proved Adam's conjecture for p -vertex circulant graphs (though the conjecture itself is not mentioned in this paper). There is a number of other interesting publications (see for example references in [42] which are devoted to the circulants with a prime and a prime-power number of vertices), however their consideration does not fit the framework of our survey.

7.6. Schur rings over cyclic groups. The problem of complete enumeration of S-rings over the cyclic group of order n was first raised in [73], see also Chapter 8 of the book [74] (this chapter was written jointly with Klin). Although the isomorphism problem of circulants was the main application of S-rings, the enumeration problem was also studied as an interesting combinatorial problem by itself. The first enumeration results were obtained by M. Klin, Ja. Gol'fand, N. Naimark and R. Pöschel during 1974-85 in [73, 46, 74, 32, 44, 33]. They gave a complete list of all S-rings over $\mathbb{Z}_n$ if n is a prime power or a product of two distinct primes. Their results were used for a solution of the isomorphism problem for circulants. All S-rings over $\mathbb{Z}_n$ for several small values of n were enumerated by V.A. Zaichenko in [87], using a computer. The results of an attempt to enumerate all S-rings over $\mathbb{Z}_n$ where n is a product of three distinct primes were reported in [28]. The rational S-rings over the cyclic group of square-free order were classified Ja. Gol'fand in 1985 ([31]). This result was generalized by Muzychuk for a cyclic group of arbitrary order, [63]. All S-rings over the cyclic group of square-free order were classified by Muzychuk in 1993, see [65]. It should be mentioned that although the latter classification was not used directly for proving the corrected Ádám's conjecture, the Schur ring theory was an important ingredient of its proof.

A beautiful survey of some results on enumeration of S-rings is presented in [51]. An important classification result about Schur rings over a cyclic group was obtained in [52, 53]. It claims that each S-ring over $\mathbb{Z}_n$ is either a tensor or a so-called wedge product of two S-rings over cyclic groups of smaller orders. We are not aware of any attempts to apply these results to the study of the algebraic and combinatorial isomorphisms of Schur rings.

7.7. Isomorphism criteria for circulant graphs. Just a few results are known in the case where Adam's conjecture is not true. Klin and Pöschel presented in [45, 46, 74, 47] isomorphism criteria for $n = p^2$, p a prime. The proof is based on the following "complete scheme":

- enumeration of S-rings,
- description of the automorphism groups,
- finding the normalisers of the automorphism groups in the symmetric group,
- formulation of an isomorphism criterion.

In [43] necessary and sufficient isomorphism conditions for p^m -vertex circulant graphs, p an odd prime, were obtained on the base of the classification of S-rings in [73]. In all these papers the multiplier approach was used.

7.8. Multipliers. It turns out that the multiplier approach can be used as a universal tool for the classification of combinatorial objects with cyclic symmetry. The main idea of the multiplier approach may be formulated as follows. If two cyclic objects are not conjugate by one multiplier, then we may take a set of multipliers and use them to construct an isomorphism between these objects which will be a local multiplier isomorphism, i.e. a multiplier isomorphism on each "section" of $\mathbb{Z}_n$

(of course, the notion of section must be rigorously defined simultaneously with the exact definition of a combinatorial object). This idea was successfully implemented for cyclic codes in [39, 40]. Concerning circulant graphs, this approach was used in [2, 43]. It follows from Theorem 5.1 that the layers of the connection sets of two isomorphic circulants are conjugate by multipliers. The main problem now is to find necessary and sufficient conditions which allow us to reconstruct an isomorphism between the graphs from a list of multipliers. Another approach to the isomorphism problem for cyclic combinatorial objects was suggested in [68, 70] in the framework of so-called solving sets.

A very surprising fact is that the origins of this method go back to the beginning of the century (S. Bays, P. Lambossy), when it was used for the isomorphism testing of circulant Steiner systems.

7.9. The isomorphism problem for Cayley graphs. As already mentioned, the isomorphism problem for circulants is a particular case of the general isomorphism problem for Cayley graphs. The main open problem in this area is to classify all CI-groups. During the last decade C.H. Li and his colleagues, using the classification of finite simple groups, made significant progress towards a complete solution of the problem. They found a very narrow list of groups which still remain as candidates for being CI. The main problem now is to check which of these groups are really CI. In general, it is a rather hard problem to show that a concrete group is a CI-group. In almost all known cases the proof of being CI either essentially exploits S-ring theory or may be simplified by using calculations in S-rings. For this reason, we are sure that a combination of group-theoretical techniques with S-ring theory will be helpful in order to make a further progress in the area.

7.10. Coherent algebras. Coherent (cellular) algebras from the beginning were considered by representatives of the Soviet school as a tool for the solution of the isomorphism problem for all graphs. The minimal coherent algebra $W(A)$ which contains an adjacency matrix A of a given graph Γ is a source of various important invariants of Γ .

In [71] coherent algebras together with S-rings are used for the solution of the recognition problem for circulant graphs with prime number of vertices. We refer to [48, 49] for the description of other applications of coherent algebras in isomorphism testing.

7.11. Towards further progress. One can modify the “complete scheme” (see Subsection 7.7) proposed by Klin and Pöschel in order to make it suitable for a solution of the isomorphism problem for Cayley graphs over an arbitrary group. In the original “complete scheme” approach we enumerate all S-rings over a given group. But for the Cayley graph isomorphism problem we need only Schurian S-rings. This observation together with rather elementary group-theoretical arguments lead sometimes to an essential reduction of the enumeration part. For example such ideas led to a proof that $\mathbb{Z}_p^4$ is a CI-group [38].

8. Acknowledgements

We thank a referee and Alyssa Sankey for helpful remarks and linguistic improvements.

References

- [1] A. Ádám, *Research problem 2-10*, J. Combin. Theory **2**(1967), 393.
- [2] B. Alspach, T.D. Parsons, *Isomorphism of circulant graphs and digraphs*, Discrete Math. **25**(1979), 97-108.
- [3] L. Babai, *Isomorphism problem for a class of point-symmetric structures*, Acta Math. Acad. Sci. Hungar. **29**(1977), 329-336.
- [4] L. Babai, P. Frankl, *Isomorphism of Cayley graphs I*, in: Colloq. Math. Soc. J. Bolyai **18**. Combinatorics, Keszthely, 1976, North - Holland, Amsterdam, 1978, 35-52.
- [5] L. Babai, P. Frankl, *Isomorphism of Cayley graphs II*, Acta Math. Acad. Sci. Hungar. **34**(1979), 177-183.
- [6] E. Bannai, T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.
- [7] E. Bannai, Song-Sung-Yell, *Character tables of fission schemes*, European J. of Combin. **14**(1993), no. 5, 385-396.
- [8] J.-C. Bermond, G. Illiades, C. Peyrat, *An optimization problem in distributing loop computer networks*, Annals New York Acad. Sci. **555**(1989), 45-55.
- [9] F.T. Boesch, J.-F. Wang, *Reliable circulant networks with minimum transmission delay*, IEEE Trans. on circ. and syst. **C32**(1985), 1286-1291.
- [10] J.E. Boilatt, *Fast load balancing in Cayley graphs and in circuits*, Lect. Nites in Comp. Science **790**(1994), 315-326.
- [11] W.G. Bridges, R.A. Mena, *Rational G -matrices with rational eigenvalues*, J. of Combin. Theory A **108**(1982), no. 6, 264-280.
- [12] A.E. Brouwer, A.E. Cohen, A. Neumaier, *Distance-regular graphs*, Springer Verlag, 1989.
- [13] C.Y. Chao, *Some applications of a theorem of Schur to graphs and to a class of endomorphisms*, Portugaliae Math. **26**(1967), 505-523.
- [14] C.Y. Chao, *On a type of circulants*, Linear Algebra and Appl. **6**(1973), 241-248.
- [15] C.Y. Chao, *On digraphs with circulant adjacency matrices*, Arch. Math. **54**(1990), 93-104.
- [16] F.P.K. Chung, R.L. Graham, *Quasi-random subsets of $\mathbb{Z}_n$* , J. Comb. Theory (A) **61**(1992), 64-86.
- [17] Ph. J. Davis, *Circulant matrices*, John Wiley & Sons. New York, 1979.
- [18] Ph. Delsarte, *Regular schemes over a finite Abelian group*, Geom. Dedicatae **8**(1979), 477-490.
- [19] D.Ž. Djoković, *Isomorphism problem for a special class of graphs*, Acta Math. Acad. Sci. Hung. **21**(1970), 267-270.
- [20] V.N. Egorov, A.I. Markov, *On Ádám's conjecture for graphs with circulant adjacency matrices*, Soviet Math. Dokl. **20**(1979), 1292-1296. (Russian)
- [21] B. Elspas, J. Turner, *Graphs with circulant adjacency matrices*, J. Combin. Theory **9**(1970), 297-307.
- [22] S. Evdokimov, I. Ponomarenko, *On highly closed cellular algebras and highly closed isomorphism*, Electron. J. Comb. **6**(1999), # R18.
- [23] I.A. Faradžev, A.A. Ivanov, M.H. Klin, *Galois correspondence between permutation groups and cellular rings (association schemes)*, Graphs and Combinatorics **6**(1990), 303-332.
- [24] I.A. Faradžev, M.H. Klin, *Computer package for computations with coherent configurations*, Proc. of the 1991 Intern. Symp. on Symb. and Algebr. Computations, ISSAC'91 (Bonn, July 15-17, 1991), ACM press, 219-223.
- [25] I.A. Faradžev, M.H. Klin, M.E. Muzichuk, *Cellular rings and groups of automorphisms of graphs*, In: Investigations on Algebraic Theory of Combinatorial Objects. Mathematics and Its Applications (Soviet Series), I.A. Faradžev, A.A. Ivanov, M.H. Klin, A.J. Woldar (eds.), Kluwer Acad. Publ. **84**(1993), 1-152.
- [26] Xingui Fang, Mingyao Xu, *On isomorphisms of Cayley graphs of small valency*, Algebra Colloq. **1:1**(1994), 67-76.
- [27] C.M. Fiduccia, R.W. Foreade and G.S. Zito, *Geometry and diameter bounds of directed Cayley graphs on abelian groups*, SIAM Journal of Disc. Math. **11**(1998), 157-167.
- [28] A.G. Ganushkin, *Schur rings over cyclic groups of order pqr* , In: Sixth All-Union Conference in group theory. Abstracts, Kiev, 1978, p. 15. (Russian)
- [29] C.D. Godsil, *On Cayley graphs isomorphism*, Ars Combinatoria **15**(1983), 231-246.
- [30] C. D. Godsil, *On the full automorphism group of Cayley graphs*, Combinatorica **1**(1981) 243-256.

- [31] Ja.Ju. Gol'fand, *A description of subrings in $V(S_{p_1} \times \dots \times S_{p_m})$* , Investigations in the algebraic theory of combinatorial objects, Proc. Seminar Inst. System Studies, Moscow, 1985, 65-76. (Russian); English translation in: Investigations on Algebraic Theory of Combinatorial Objects, Mathematics and Its Applications (Soviet Series), I.A. Faradžev, A.A. Ivanov, M.H. Klin, A.J. Woldar (Eds), Kluwer Acad. Publ. **84**(1994), 209-223.
- [32] Ja.Ja. Gol'fand, M.H. Klin, N.L. Naimark, *The structure of S -rings over $\mathbb{Z}_2^m$* , In: "Sixteenth All-Union Algebraic Conference", part 2, Leningrad, 1981, 195-196.
- [33] Ja.Ju. Gol'fand, N.L. Naimark, R. Pöschel, *Schur rings over $\mathbb{Z}_2^m$* , Preprint P-MATH-01/85 Akad. der Wiss. der DDR, ZIMM, Berlin, 1985.
- [34] B. Gordon, *A generalization of the coset decomposition of a finite group*, Pacif. J. Math. **15**(1965), 503-509.
- [35] W.D. Hillis, *The Connection Machine*, The MIT Press, Cambridge, 1986.
- [36] D.G. Higman, *Coherent configurations I*, Rend. Sem. Mat. Univ. Padova **44**(1970), 1-25.
- [37] D.G. Higman, *Coherent algebras*, Linear algebra and its applications **93**(1987), 209-239.
- [38] M. Hirasaka, M. Muzychuk, *The elementary abelian group of rank 4 is a CI-group*, J. of Combin. Theory, accepted.
- [39] W.G. Huffman, A. Job, V. Pless, *Multipliers and generalized multipliers of cyclic objects and cyclic codes*, J. of Comb. Th. (A) **62**(1993), no. 2, 183-215.
- [40] W.C. Huffman, *The equivalence of two cyclic objects on pq elements*, Discrete Math. **154**(1996), 103-127.
- [41] A. Joseph, *The isomorphism problem for Cayley digraphs on graphs of prime-squared order*, Discrete Math. **141**(1995), no. 1-3, 173-183.
- [42] M. Klin, V. Liskovets, R. Pöschel, *Analytical enumeration of circulant graphs with prime-squared number of vertices*, Semin. Lothar. Comb. **36**(1996), B36d.
- [43] M.Ch. Klin, R. Pöschel, *The isomorphism problem for circulant digraphs with p^n vertices*, Preprint P-34/80 Akad. der Wiss. der DDR, ZIMM, Berlin, 1980.
- [44] M.Ch. Klin, N.L. Naimark, R. Pöschel, *Schur rings over $\mathbb{Z}_2^m$* , Preprint P-MATH-14/81 Akad. der Wiss. der DDR, ZIMM, Berlin, 1981.
- [45] M.H. Klin, Pöschel, *The isomorphism problem for cyclic graphs with p^2 or pq vertices*, Abstract presented at the A.A.Zykov's Seminar on Graph Theory, Odessa, 1975. (Russian)
- [46] M.Ch. Klin, R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the characterization of Schur rings*, Preprint AdWd DDR, ZIMM, Berlin, March 1978.
- [47] M.H. Klin, R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Colloq. Math. Soc. J. Bolyai **25**, Algebraic methods in graph theory, Szeged, 1978. North-Holland, Amsterdam, 1981; 405-434.
- [48] M. Klin, Ch. Rücker, G. Rücker, G. Tinhofer, *Algebraic combinatorics in mathematical chemistry. Methods and algorithms. I. Permutation groups and coherent (cellular) algebras*, MATCH **40**(1999), 7-138.
- [49] M. Klin, G. Tinhofer, *Algebraic combinatorics in mathematical chemistry. Methods and algorithms. III. Graph invariants and stabilization methods*, Technical report TUM-M9902. Technische Universität München, März 99, 64 pp.
- [50] R. Kochendörfer, *Lehrbuch der Gruppentheorie unter besonder Berücksichtigung der endlichen Gruppen*, Akad. Verlagsgesellschaft, Leipzig, 1966.
- [51] K.H. Leung, S.L. Ma, *The structure of Schur rings over cyclic groups*, J. Pure Appl. Algebra **66**(1990), 287-302.
- [52] K.H. Leung, S.H. Man, *On Schur rings over cyclic groups*, Israel J. Math. **106**(1998), 251-267.
- [53] K.H. Leung, S.H. Man, *On Schur rings over cyclic groups, II*, J. of Algebra **183**(1996), no. 2, 273-285.
- [54] C.H. Li, M. Conder, *On the isomorphisms of finite Cayley graphs*, Europ. J. Combin. **19**(1998), no. 8, 911-919.
- [55] C.H. Li, C.E. Praeger, M.Y. Xu, *On finite groups with Cayley isomorphism property*, J. of Graph Theory **27**(1998), 1-11.
- [56] C.H. Li, *On isomorphism of connected Cayley graphs*, Discrete Math. **178**(1998), 109-122.
- [57] C.H. Li, *Permutation groups and circulant graphs*, Manuscript 1999.
- [58] C.H. Li, *The finite groups with the 2-DCI-property*, Comm. in Algebra **24**(1996), 1749-1757.
- [59] C.H. Li, *On isomorphism of connected Cayley graphs II*, J. Combin. Theory (B) **74**(1998), 28-34.

- [60] B. Litow, B. Mans, *On the Ádám property for circulant graphs*, Tech. Report of the Dept. of Comp. Science, James Cook Univ., TR-96-11 (1996), 1-8.
- [61] S.L. Ma, *On association schemes, Schur rings, strongly regular graphs and partial difference sets*, Ars Combinatoria **27**(1989), 211-220.
- [62] B. Mans, F. Pappalardi, I. Shparlinski, *On Ádám's conjecture on circulant graphs*, Lect. Notes in Comp. Science **1449**(1998), 260-285.
- [63] M. Muzychuk, *The structure of rational Schur rings over cyclic groups*, Europ. J. of Combin. **14**(1993), 479-490.
- [64] M. Muzychuk, *On the structure of basic sets of Schur rings over cyclic groups*, J. of Algebra **169**(1994), no. 2, 655-678.
- [65] M. Muzychuk, *The structure of Schur rings over cyclic groups of square-free order*, Acta Appl. Math. **52**(1998), 163-181.
- [66] M. Muzychuk, *Ádám's conjecture is true in the square-free case*, J. of Combin. Th. (A) **72**(1995), no. 1, 118-134.
- [67] M. Muzychuk, *On Ádám's conjecture for circulant graphs*, Discrete Math. **176**(1997), 285-298.
- [68] M. Muzychuk, *On the number of cyclic combinatorial objects isomorphic to a given one*, Preprint Math-AL-16-1996, Technische Universität Dresden 1996.
- [69] M. Muzychuk, R. Pöschel, *Isomorphism criterion for circulant graphs*, Preprint Math-AL-9-1999, Technische Universität Dresden, 1999.
- [70] M. Muzychuk, *On the isomorphism problem for cyclic combinatorial objects*, Discrete Math. **197/198**(1999), 589-606.
- [71] M. Muzychuk, G. Tinhofer, *Recognizing circulant graphs of prime order in polynomial time*, Electron. J. Comb. **5**(1998), Research paper R25, 28 pp.
- [72] P.P. Pálffy, *Isomorphism problem for relational structures with a cyclic automorphism*, Europ. J. Comb. **8**(1987), 35-43.
- [73] R. Pöschel, *Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen*, Math. Nachr. **60**(1974), 1-27.
- [74] R. Pöschel, L.A. Kalužnin, *Funktionen- und Relationenalgebren*, Birkhäuser Verlag, Basel u. Stuttgart, and Deutscher Verlag der Wissenschaften, Berlin, 1979.
- [75] S.T. Schibell, R.M. Stafford, *Processor interconnection networks from Cayley graphs*, Disc. Appl. Math. **40**(1992), 333-357.
- [76] Wai-Chee Shiu, *Algebraic structure of Schur rings*, Chinese Journal of Math. **21**(1993), no. 1, 55-71.
- [77] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, S.-B. Preuss. Akad. Wiss. phys.-math. Kl. **18/20**(1933), 598-623.
- [78] W.R. Scott, *Group Theory*, Prentice-Hall, 1964.
- [79] O. Tamaschke, *A generalization of conjugacy in groups*, Rendiconti del Seminario Matematico dell'Università di Padova **40**(1968), 408-427.
- [80] S. Toida, *A note on Ádám's conjecture*, J. Combin. Theory (B), **23**(1977), 239-246.
- [81] J. Turner, *Point symmetric graphs of prime order*, J. Combin. Theory **3**(1967), 136-145.
- [82] J.L.A. Vebra, M.A. Fiol, P. Morillo, I. Alegre, *The diameter of undirected graphs associated to plane tessellations*, Ars Combinatoria **20 B**(1985), 159-171.
- [83] B. Ju. Weisfeiler, A.A. Leman, *Reduction of a graph to a canonical form and an algebra arising during this reduction*, Nauchno-Technicheskaya Informatsia **9** Seria 2, (1968), 12-16. (Russian)
- [84] B. Weisfeiler (editor), *On the construction and identification of graphs*, Lect. Notes in Math. **558**(1976).
- [85] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964, Berlin.
- [86] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, Lect. Notes., Dept. Math.m Ohio St. Univ, Colimbus, 1969.
- [87] V.A. Zaichenko, *An algorithmic approach to the construction of combinatorial objects and to computations in permutation groups based on the method of invariant relations*, Ph.D. Thesis, Moscow, MPhTI, 1981. (Russian)
- [88] D.K. Zibin', Private communication, August 1975.
- [89] P.H. Lieschang, *An Algebraic Approach to Association Schemes*, Springer, LNM 1628.
- [90] J. Žerovnik, T. Pisanski, *Computing the diameter in multiple-loop networks*, J. of Algorithms **14**(1993), 226-243.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, NETANYA ACADEMIC COLLEGE, 16
KIBUTZ GALUYOT ST., 42365 NETANYA, ISRAEL

E-mail address: muzy@Netanya.ac.il

DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, 84105 BEER-
SHEVA, ISRAEL,

E-mail address: klin@cs.bgu.ac.il

INSTITUT FÜR ALGEBRA, TECHNISCHE UNIVERSITÄT DRESDEN, D - 01062 DRESDEN, GERMANY

E-mail address: poeschel@math.tu-dresden.de