Als Manuskript gedruckt

Technische Universität Dresden
Herausgeber: Der Rektor

Isomorphism criteria for circulant graphs*

M. Muzychuk, R. Pöschel

MATH–AL–9–1999 April 1999

*This research was partially supported by the Grant No. I-0333-263.06/93 from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

Isomorphism criteria for circulant graphs

Mikhail Muzychuk Reinhard Pöschel

April 1999

Abstract

The isomorphism problem for circulant graphs over $\mathbb{Z}_n$ is treated for arbitrary $n \in \mathbb{N}$. We show that if two circulant graphs are isomorphic then their layers are conjugate by multipliers (3.3). As a direct consequence of this necessary condition we obtain an affirmative answer to Toida's conjecture. Further, a sufficient isomorphism condition for circulant graphs is given which generalizes known isomorphism criteria for circulant graphs of prime-power and square-free orders (3.8). We conjecture that these conditions also should be necessary. Finally we develop an alternative approach to the isomorphism problem for circulant graphs which is based on the notion of a solving set. Using this notion we reformulate the isomorphism criterion for circulant graphs of prime-power order in a more transparent form (6.6).

Introduction

Circulant graphs are Cayley graphs over a cyclic group. The interest to circulant graphs in graph theory and applications has been grown during the last decade, they appeared in coding theory, VLSI design, Ramsey theory and other areas. The graph isomorphism problem for circulants found particular interest. In 1967 Á. Ádám gave a condition (nowadays a special case of the Cayley isomorphism condition) which was sufficient but not necessary as conjectured for a while. During the last 30 years many experts in algebraic combinatorics (among them B. Alspach, L. Babai, C.Y. Chao, D.Z. Djoković, C.D. Godsil, P.P. Pálfy, T.D. Parsons and J. Turner) made efforts to solve what is called Ádám's problem, i.e., for which n Ádám's conjecture holds for circulants over $\mathbb{Z}_n$. These results were based on deep group theoretical techniques.

Another approach to the isomorphism problem was initiated in 1974-1978 by M. Klin and the second author. The idea was to describe all so-called S-rings over $\mathbb{Z}_n$, to find their automorphism groups and then to use the results for the identification of circulant graphs ([Pös74],[Kli-P81],[Kli-P80],[Gol-N-P85]). This approach was further developed by the first author ([Muz95a], [Muz97], [Muz95b], [Muz96]). The resulting isomorphism criteria are recalled in 3.5 and 3.6 and show that we can attack also those cases which fall outside the scope of Ádám's conjecture (in the terminology introduced in 1.8 this means that there are no Cayley isomorphisms).

However, that results work only for special n (squarefree and prime power). In the present paper we treat the isomorphism problem for circulant graphs over $\mathbb{Z}_n$ for *arbitrary* n. The general background is developed even for Cayley graphs over arbitrary groups in section 1 and specialized to cyclic groups in section 2.

In section 3 we shall give a necessary (3.3) and a sufficient (3.8) condition for isomorphism (the latter being also necessary in the above mentioned special cases).

In sections 4–6 we investigate another attack on the isomorphism problem: we introduce so-called solving sets which – whenever known – solve completely the isomorphism problem for circulant graphs.

A solving set for a circulant graph Γ with vertex set X is a set $P \subseteq \mathsf{Sym}(X)$ of permutations on X such that any other circulant graph Γ' is isomorphic to Γ if and only if there exists an isomorphism in P. In this terminology, Ádám's conjecture for circulant graphs over $X = \mathbb{Z}_n$ says that $\mathbb{Z}_n^*$ is a solving set (for details see 4.1) for the class of all circulant graphs, i.e., one has to test at most $\varphi(n) = |\mathbb{Z}_n^*|$ permutations for detecting whether two circulant graphs are isomorphic or not.

If Ádám's conjecture does not hold then one has to enlarge $\mathbb{Z}_n^*$ in order to get a solving set for all circulant graphs.

However, it turns out, that for $n = p^\alpha$ (prime power) the isomorphism criteria obtained by Klin/Pöschel([Kli-P80]) may be reformulated similiar to Ádám's condition and not increasing essentially its complexity. We have to proceed in two steps.

At first we introduce the *profile* of a graph: this is an easily computable vector $\mathbf{k} = (k_0, k_1, \dots, k_{\alpha-1})$ with components from $\{1, \dots, \alpha\}$ which does not depend on p but only on α. The profile is invariant under graph isomorphisms. Now, in a second step, to each profile $\mathbf{k}$ one can find a solving set of not more (usually much less) than $\varphi(n)$ elements for every circulant graph with profile $\mathbf{k}$. In special cases (depending on the automorphism group of the graph) the indicated solving set even is minimal.

Moreover, in section 7, we explicitly describe the construction of such a solving set for a circulant graph over $\mathbb{Z}_{p^\alpha}$ with profile $\mathbf{k}$. In particular, the size of a minimal solving set can be computed.

1 Schur rings and Cayley graphs

1.1. Group algebras and some notations. Just to fix notations we recall: Let H be some (multiplicatively written) group and $\boldsymbol{Q}$ be a ring (e.g. $\mathbb{Q}$ or $\mathbb{Z}$). The *group algebra* $\boldsymbol{Q}H$ of H over $\boldsymbol{Q}$ is the set of all formal sums $\sum_{i \in I} \alpha_{h_i} h_i$ with finite I and coefficients $\alpha_{h_i} \in \boldsymbol{Q}$, $h_i \in H$ for $i \in I$. These elements also can be written as $\sum_{h \in H} \alpha_h h$ with $\alpha_h = 0$ whenever h is not among the h_i's. Further, $\boldsymbol{Q}H$ is equipped with two operations, addition

$$\sum_{h \in H} \alpha_h h + \sum_{h \in H} \beta_h h := \sum_{h \in H} (\alpha_h + \beta_h) h$$

and multiplication (indicated also by concatenation)

$$(\sum_{h \in H} \alpha_h h)(\sum_{k \in H} \beta_k k) := \sum_{h,k \in H} (\alpha_h \beta_k)(hk) = \sum_{h \in H} (\sum_{k \in H} \alpha_{hk^{-1}} \beta_k) h \ .$$

$\boldsymbol{Q}H$ is also a $\boldsymbol{Q}$-module with scalar multiplication

$$\alpha(\sum_{h\in H} \alpha_h h) := \sum_{h\in H} (\alpha\alpha_h)h \quad \text{for } \alpha \in \boldsymbol{Q}.$$

Dealing with permutation groups we use the notation $\mathsf{Sym}(X)$ for the full symmetric group of all permutations on a set X. If G is a subgroup of H we express this by $G \leq H$. The image $g(x)$ of an element $x \in X$ under a permutation $g \in \mathsf{Sym}(X)$ is also denoted by x^g. According to $x^{gh} := (x^g)^h$, the composition $h \circ g$ of two permutations $g, h \in \mathsf{Sym}(X)$ is written as gh.

1.2. Cayley graphs and isomorphisms. A *Cayley graph* $\Gamma_H(S)$ over a group H is a directed graph defined by a subset $S \subseteq H$ as follows: the vertex set is H and the edge set, also denoted by $\Gamma_H(S)$, is $\{(x,y) \mid xy^{-1} \in S\}$. Two Cayley graphs $\Gamma_H(S)$ and $\Gamma_K(R)$, ($S \subseteq H$, $R \subseteq K$) over the groups H and K, respectively, are called *isomorphic* (notation $\Gamma_K(R) \cong \Gamma_H(S)$), if they are isomorphic in the usual sense, i.e. there exists a bijection $f : H \to K$ such that $xy^{-1} \in S \iff (x^f)(y^f)^{-1} \in R$. Then we have $\Gamma_H(S)^f = \Gamma_K(R)$, where $\Gamma_H(S)^f := \{(x^f, y^f) \mid (x,y) \in \Gamma_H(S)\}$.

If, in addition, f is a group isomorphism, then $\Gamma_H(S)$ and $\Gamma_K(R)$ are called *Cayley isomorphic*, notation $\Gamma_K(R) \cong_{Cay} \Gamma_H(S)$.

1.3. S-rings. Schur-rings over a group H are special subalgebras of the group algebra $\mathbb{Q}H$. They play an important role for the existence of an isomorphism between Cayley graphs.

We need the following notation. For a subset $T \subseteq H$ let $\underline{T} := \sum_{h\in T} h$. Elements (in $\mathbb{Q}H$) of this form will be called *simple quantities* [Wie64]. The identity element of any group usually will be denoted by e.

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

(S1) $\mathcal{A}$ has a basis consisting of simple quantities $\underline{T_0}, \ldots, \underline{T_d}$, where $T_0 = \{e\}$, (S2) $\{T_0, \ldots, T_d\}$ is a partition of H (i.e., $T_i \cap T_j = \emptyset$ for $i \neq j$, and $\bigcup_{j=0}^d T_j = H$),

(S3) For each $i \in \{0, 1, \ldots, d\}$ there exists $i' \in \{0, 1, \ldots, d\}$, such that $T_{i'} = T_i^{-1} := \{t^{-1} \mid t \in T_i\}$.

For given $\mathcal{A}$ the basis $\underline{T_0}, \ldots, \underline{T_d}$ is uniquely determined by (S1) and (S2) and it is called *the (first) standard basis* of $\mathcal{A}$. The sets T_i, $0 \leq i \leq d$, are called the *basic sets* of $\mathcal{A}$ and the notation $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ will be used if $\mathcal{A}$ is an S-ring over H whose basic sets are $T_0, \ldots, T_d$. The set of all basic sets is also denoted by $\mathsf{Basic}(\mathcal{A})$. By (S2), every $x \in H$ is contained in exactly one basic set, which will be denoted by $T_{(x)}$. Moreover, the product $\underline{T_i}\,\underline{T_j}$ of two basic sets must belong to $\mathcal{A}$ and therefore has to be a linear combination of basic sets:

$$\underline{T_i}\,\underline{T_j} = \sum_{k=0}^{d} p_{ij}^k \, \underline{T_k}\,.$$

The elements p_{ij}^d are called the *structure constants* of $\mathcal{A}$.

1.4. Coherent configurations. A *coherent cofiguration* [Hig70, Hig87] or cellular algebra [Wei74] is a relational system $\mathcal{X} = (X, \{R_0, \ldots, R_d\})$ with binary relations R_i on X such that (C1)-(C4) is satisfied (where (C4) is the most important condition) cf. e.g. [Far-K-M94, Chapter 1]:

(C1) $\{R_0, \ldots, R_d\}$ is a partition of $X \times X$,

(C2) the identity relation $\{(x, x) \mid x \in X\}$ is also the union of some R_i's,

(C3) $\forall i \, \exists j : \, R_i^{-1} = R_j$,

(C4) the *structure constants* defined by

$$p_{ij}^k := |\{c \in X \mid (a, c) \in R_i \wedge (c, b) \in R_j\}|$$

for some $(a, b) \in R_k$ are independent of the choice of $(a, b) \in R_k$ $(i, j, k \in \{0, 1, \ldots, d\})$.

A coherent configuration is called *homogeneous* if $\{(x,x) \mid x \in X\} \in \{R_0, \ldots, R_d\}$.

Every S-ring $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ over the group H gives an example of a coherent configuration, namely $\mathsf{Co}(\mathcal{A}) := (H, \{\Gamma_H(T_0), \ldots, \Gamma_H(T_d)\})$ (cf. also [Far-K-M94]). A direct check shows that the structure constants of $\mathsf{Co}(\mathcal{A})$ coincide with the structure constants of $\mathcal{A}$ (see also 1.11 below).

1.5. Algebraic isomorphisms. Two S-rings $\mathcal{A}$ and $\mathcal{B}$ are called *algebraically isomorphic*, notation $\mathcal{A} \cong_{alg} \mathcal{B}$, if there exists a bijection $g : \mathsf{Basic}(\mathcal{A}) \to \mathsf{Basic}(\mathcal{B}) : T \mapsto T^g$ 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 $\mathcal{B}$ (i.e., it has to respect addition – what is satisfied trivially – and multiplication). Instead of $\underline{T^g}$ we also write $\underline{T}^g$.

1.6. Combinatorial isomorphisms and automorphisms. Two S-rings $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle \subseteq \mathbb{Q}H$ and $\mathcal{B} = \langle \underline{S_0}, \ldots, \underline{S_s} \rangle \subseteq \mathbb{Q}K$ will be called *combinatorially isomorphic*, notation $\mathcal{A} \cong_{com} \mathcal{B}$, if there exists a bijection $f : H \to K$ such that $\{\Gamma_H(T_i)^f \mid i = 0, \ldots, d\} = \{\Gamma_K(S_i) \mid i = 0, \ldots, s\}$. Consequently $d = s$ and each combinatorial isomorphism[1] f induces a bijection $f^* : \mathsf{Basic}(\mathcal{A}) \to \mathsf{Basic}(\mathcal{B})$ such that $\Gamma_H(T)^f = \Gamma_K(T^{f^*})$ for $T \in \mathsf{Basic}(\mathcal{A})$.

Given an S-ring $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ over H, the subgroup of $\mathsf{Sym}(H)$ consisting of all combinatorial automorphisms of $\mathcal{A}$ is denoted by $\mathsf{Out}(\mathcal{A})$.

The subgroup of $\mathsf{Out}(\mathcal{A})$ consisting of all automorphisms f which induce the trivial algebraic automorphism of $\mathcal{A}$ (i.e. f^* is the identity) will be denoted by $\mathsf{Aut}(\mathcal{A})$. We have

$$\mathsf{Aut}(\mathcal{A}) = \bigcap_{0 \le i \le d} \mathsf{Aut}(\Gamma_H(T_i)).$$

Clearly, $\mathsf{Aut}(\mathcal{A}) \trianglelefteq \mathsf{Out}(\mathcal{A})$.

Remarks. $\mathsf{Out}(\mathcal{A})$ is the automorphism group of the coherent configuration $\mathsf{Co}(\mathcal{A})$ in the sense of [Zie97] while $\mathsf{Aut}(\mathcal{A})$ is the automorphism group of $\mathsf{Co}(\mathcal{A})$ in the sense of e.g. [Far-K-M94].

[1] in [Kli-P80] called S-isomorphism

Two coherent configurations $(X, \{R_0, \dots, R_d\})$ and $(Y, \{S_0, \dots, S_s\})$ are called isomorphic if $d = s$ and there exists a bijection $h : X \to Y$ such that $\{R_i^h \mid i = 0, \dots, d\} = \{S_i \mid i = 0, \dots, d\}$.
This shows that two S-rings are combinatorially isomorphic if and only if the corresponding coherent configurations (cf. 1.4) are isomorphic.

The next proposition shows that beeing combinatorially isomorphic implies being algebraically isomorphic. It is a special case of a more general result for coherent configurations (see [Wei74]).

1.7. Proposition. *If f is a combinatorial isomorphism between two S-rings $\mathcal{A}$ and $\mathcal{B}$ (over groups H and K as in* 1.5*), then f^* is an algebraic isomorphism between them.*

Proof. For each $T \in \mathsf{Basic}(\mathcal{A})$ we define an $H \times H$-matrix $A(T) = (A(T)_{xy})$ as follows[2]:

$$A(T)_{xy} := \begin{cases} 1 \text{ if } xy^{-1} \in T \\ 0 \text{ if } xy^{-1} \notin T \end{cases}, \quad (x, y) \in H \times H \ .$$

It is well known that the vector space $\mathsf{Span}\{A(T) \mid T \in \mathsf{Basic}(\mathcal{A})\}$ over $\mathbb{Q}$ spanned by the matrices $A(T)$ is closed under matrix multiplication. Moreover, the mapping $\underline{T} \mapsto A(T)$ induces an isomorphism between the algebra $\mathcal{A}$ and $\mathsf{Span}\{A(T) \mid T \in \mathsf{Basic}(\mathcal{A})\}$.
Analogously, $\mathcal{B}$ is isomorphic to the algebra $\mathsf{Span}\{B(U) \mid U \in \mathsf{Basic}(\mathcal{B})\}$ of $K \times K$-matrices, where

$$B(U)_{xy} = \begin{cases} 1 \text{ if } xy^{-1} \in U \\ 0 \text{ if } xy^{-1} \notin U \end{cases}, \quad (x, y) \in K \times K \ .$$

Let P_f be the $H \times K$-matrix defined as follows:

$$(P_f)_{xy} = \begin{cases} 1 & \text{if } y = x^f \\ 0 & \text{otherwise} \end{cases}, \quad (x, y) \in H \times K \ .$$

Since $\Gamma_H(T)^f = \Gamma_K(T^{f^*})$, we have $B(T^{f^*}) = P_f^{-1} A(T) P_f$. Now the claim easily follows since matrix conjugation preserves matrix multiplication. □

[2] $A(T)$ is the adjacency matrix of $\Gamma_H(T)$

1.8. Cayley isomorphisms. Two S-rings are called *Cayley isomorphic*, notation $\mathcal{A} \cong_{Cay} \mathcal{B}$, if there exists a combinatorial isomorphism $f : H \to K$ 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:

$$\mathcal{A} \cong_{Cay} \mathcal{B} \quad \Longrightarrow \quad \mathcal{A} \cong_{com} \mathcal{B} \quad \Longrightarrow \quad \mathcal{A} \cong_{alg} \mathcal{B},$$

But the respective converses are not true in general:

$$\mathcal{A} \cong_{Cay} \mathcal{B} \;\not\Longleftarrow\; \mathcal{A} \cong_{com} \mathcal{B} \;\not\Longleftarrow\; \mathcal{A} \cong_{alg} \mathcal{B}.$$

For a subset $S \subseteq H$ let $\langle\langle S \rangle\rangle$ denote the least S-ring that contains $\underline{S}$. Then, obviously, S must be a union of basic sets of $\langle\langle S \rangle\rangle$. The following Theorem clarifies the connection between $\langle\langle S \rangle\rangle$ and S with respect to isomorphisms.

1.9. Theorem. *Let $f : H \to K$ be an isomorphism between the Cayley graphs $\Gamma_H(S)$ and $\Gamma_K(R)$. Then we have:*

(1) *f is a combinatorial isomorphism between $\langle\langle S \rangle\rangle$ and $\langle\langle R \rangle\rangle$. In particular* $|\mathsf{Basic}(\langle\langle S \rangle\rangle)| = |\mathsf{Basic}(\langle\langle B \rangle\rangle)|$;

(2) $\langle\langle S \rangle\rangle \cong_{alg} \langle\langle R \rangle\rangle$;

(3) *Let $S = \bigcup\{B \mid B \in I\}$ be the decomposition of S into a disjoint union of basic sets of $\langle\langle S \rangle\rangle$ ($I \subseteq \mathsf{Basic}(\mathcal{A})$), then $R = \bigcup\{B^{f^*} \mid B \in I\}$.*

PROOF. (1) follows from Chapter M of [Wei74]. (2) follows from (1) and 1.7. Finally, (3) follows from the following equalities: $\Gamma_K(R) = (\Gamma_H(S))^f = (\bigcup\{\Gamma_H(B) \mid B \in I\})^f = \bigcup\{\Gamma_H(B)^f \mid B \in I\} = \bigcup\{\Gamma_K(B^{f^*}) \mid B \in I\}$. □

1.10. Cayley configurations. The automorphism group of the coherent configuration $\mathsf{Co}(\mathcal{A})$ associated with an S-ring $\mathcal{A}$ over a group H contains a regular subgroup isomorphic to H. More precisely, H acts on itself by right multiplications. We say that a coherent configuration $\mathcal{X} = (X; \{R_0, \ldots, R_d\})$ is a *Cayley configuration* if $\mathsf{Aut}(\mathcal{X})$ contains a subgroup H that acts regularly on X. In the remainder of this section we show how to reconstruct a Schur ring from a given Cayley configuration.

Let $H \leq \mathsf{Sym}(X)$ be a regular permutation group and let $R \subseteq X^2$ be a relation invariant under the group H. For $x \in X$ we define the *Schur projection* $\mathsf{spr}_{H,x}(R)$ of R on H at x by

$$\mathsf{spr}_{H,x}(R) := \{h \in H \mid (x^h, x) \in R\}\,.$$

Since R is H-invariant, R is completely determined by $\mathsf{spr}_{H,x}(R)$. More precisely, $R = \{(x^{h_1}, x^{h_2}) \mid h_1 h_2^{-1} \in \mathsf{spr}_{H,x}(R)\}$.

Let $\mathcal{X} = (X, \{R_0, \ldots, R_d\})$ be an H-invariant coherent configuration and let x be a fixed element of X. Let $T_i := \mathsf{spr}_{H,x}(R_i)$, $i = 0, ..., d$. The following properties are easy to check.

(1) $\{T_0, \ldots, T_d\}$ is a partition of H with $T_0 = \{e\}$.

(2) If $R_i^{-1} = R_j$ then $T_i^{-1} = T_j$.

(3) $\mathsf{spr}_{H,x^h}(R_i) = h^{-1}\,(\mathsf{spr}_{H,x}(R_i))\,h$.

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

1.11. Proposition. *Let $\mathcal{X}$ and T_i be as in* 1.10. *Further let p_{ij}^k be the structure constants of $\mathcal{X}$ and let $\mathcal{A}$ be the $\mathbb{Z}$-submodule of $\mathbb{Z}H$ spanned by the simple quantities T_i, $i \in \{0, \ldots, d\}$. Then we have:*

(1) *$\mathcal{A}$ is an S-ring over H where* $\underline{T_i}\,\underline{T_j} = \sum_{k=0}^{d} p_{ij}^k \underline{T_k}\,.$

(2) *The coherent configurations $\mathsf{Co}(\mathcal{A})$ and $\mathcal{X}$ are isomorphic.*

Proof. (1): We have to show that the structure constants of $\mathcal{A}$ equal p_{ij}^k, i.e., for an arbitrary $h^* \in T_k$ we have to show that the

number of solutions of the equation $h_1 h_2 = h^*$, where $h_1 \in T_i$ and $h_2 \in T_j$, is equal to p_{ij}^k.
By definition, $h^* \in T_k$ implies $(x^{h^*}, x) \in R_k$. Thus the set

$$Y = \{y \in X \mid (x^{h^*}, y) \in R_i \wedge (y, x) \in R_j\}$$

contains exactly p_{ij}^k elements (cf. 1.4). Since $\{y \mid (y,x) \in R_j\} = \{x^h \mid h \in T_j\}$, we get

$$Y = \{x^h \mid (x^{h^*}, x^h) \in R_i \wedge h \in T_j\}.$$

Since H is regular we have

$$\begin{aligned} p_{ij}^k &= |Y| \\ &= |\{h \in T_j \mid (x^{h^*}, x^h) \in R_i\}| = |\{h \in T_j \mid (x^{h^* h^{-1}}, x) \in R_i\}| \\ &= |\{h \in T_j \mid h^* h^{-1} \in T_i\}| = |\{(h_1, h_2) \in T_i \times T_j \mid h_1 h_2 = h^*\}|, \end{aligned}$$

as desired.
(2): Since H is regular, for each $y \in X$ there exists a unique $h_y \in H$ such that $x^{h_y} = y$. Thus we have a bijection $y \mapsto h_y$ between X and H. We claim that this map is an isomorphism between $\mathcal{X}$ and $\mathsf{Co}(\mathcal{A})$. Indeed,

$$\begin{aligned} (y,z) \in R_i &\iff (x^{h_y}, x^{h_z}) \in R_i \iff (x^{h_y h_z^{-1}}, x) \in R_i \\ &\iff h_y h_z^{-1} \in T_i \iff (h_y, h_z) \in \Gamma_H(T_i). \qquad \square \end{aligned}$$

1.12. Transitivity module. Let $G \leq \mathsf{Sym}(X)$ be a transitive permutation group and $\mathcal{X} = (X, \{R_0, \ldots, R_d\})$ be the coherent configuration of the 2-orbits of G. If G contains a regular subgroup H, then $H \leq G \leq \mathsf{Aut}(\mathcal{X})$ and the sets $\mathsf{spr}_{H,x}(R_i), i = 0, ..., d$ are the basic sets of an S-ring over H. Following [Wie64] we call it the *transitivity module* of G and denote it by $V(H, G_x)$.

1.13. Remarks. The notation $V(H, G_x)$ is motivated by the observation that the basic sets of $V(H, G_x)$ are just the 1-orbits of the stabilizer $G_x := \{g \in G \mid x^g = x\}$; in fact $\mathsf{spr}_{H,x}(R)$ of a 2-orbit $R = (y,x)^G$ of G equals (via the correspondence $y \leftrightarrow h_y$) the 1-orbit y^{G_x} of G_x.

Further,

$$V(H, G_x) \cong_{com} V(K, G_x)$$

for any regular subgroup H and K of G. In fact, with the notations from 1.12 and according to 1.11, $\mathsf{Co}(V(H, G_x))$ and $\mathcal{X}$ are isomorphic as coherent configurations, *i.e.*, there exists a map $\psi : X \mapsto H$ which induces a bijection between the relations of $\mathsf{Co}(V(H, G_x))$ and $\mathcal{X}$. If G contains another regular subgroup, say K, then $\mathsf{Co}(V(K, G_x))$ is isomorphic to $\mathcal{X}$ via some $\varphi : X \mapsto K$. Hence $\varphi \circ \psi^{-1} : H \mapsto K$ is an isomorphism between the coherent configurations $\mathsf{Co}(V(H, G_x))$ and $\mathsf{Co}(V(K, G_x))$.

2 Schur rings over cyclic groups

In this section we compile a list of properties of Schur rings over cyclic groups which will be useful later.

2.1. Some notations. Let C_n be a cyclic group of order n with a generator g_0. We write the group operation multiplicatively (by dot "$\cdot$" or concatenation), the identity element is denoted by e. 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 $m \in \mathbb{Z}_n^*$ 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 $x^{(m)}$ shall denote the element $\sum_{g \in C_n} x_g g^m$. For $T \subseteq C_n$, $g \in C_n$ and $m \in \mathbb{Z}_n^*$ let $T \cdot g := \{tg \mid t \in T\}$ and $T^{(m)} := \{t^m \mid t \in T\}$. Clearly, $\underline{T}^{(m)} = \underline{T^{(m)}}$.

The proof of the following claim can be found in [Wie64].

2.2. Proposition. *Let $\mathcal{A}$ be an S-ring over C_n and let $m \in \mathbb{Z}_n^*$. Then*

$$T \in \mathsf{Basic}(\mathcal{A}) \iff T^{(m)} \in \mathsf{Basic}(\mathcal{A})\,. \qquad \square$$

2.3. Conjugates, traces and stabilizers. Let $\mathcal{A}$ be an S-ring over C_n. Two subsets $S, T \subseteq C_n$ are called *conjugate*, notation

$S \sim T$, if $T = S^{(m)}$ for some $m \in \mathbb{Z}_n^*$. The relation $\sim$ is an equivalence relation on $\mathsf{Basic}(\mathcal{A})$. Given a basic set $T \in \mathsf{Basic}(\mathcal{A})$ or, more generally, a simple quantity $\underline{T} \in \mathcal{A}$, we define its *trace* $\mathring{T}$, $\mathbb{Z}_n^*$*-stabilizer* $\mathsf{Stab}_*(T)$ and C_n*-stabilizer* $\mathsf{Stab}_+(T)$ respectively, as follows:

$$\begin{aligned} \mathring{T} &:= \bigcup\{T^{(m)} \mid m \in \mathbb{Z}_n^*\}, \\ \mathsf{Stab}_*(T) &:= \{m \in \mathbb{Z}_n^* \mid T^{(m)} = T\}, \\ \mathsf{Stab}_+(T) &:= \{g \in C_n \mid T \cdot g = T\}. \end{aligned}$$

Clearly we have $\mathsf{Stab}_*(T) \leq \mathbb{Z}_n^*$ and $\mathsf{Stab}_+(T) \leq C_n$. (The notation becomes more intuitive if we switch from C_n to the additive group $\mathbb{Z}_n$, then we have a multiplicative stabilizer $\mathsf{Stab}_*()$ and an additive one, $\mathsf{Stab}_+()$, see Table 1.)

2.4. Theorem ([Muz95a, (Thm. 1.1')]). *Let $\lambda : \mathcal{A} \to \mathcal{B}$ be an algebraic isomorphism between two S-rings $\mathcal{A}$ and $\mathcal{B}$ over C_n and let $T \in \mathsf{Basic}(\mathcal{A})$. Then $\underline{T}^\lambda = \underline{T}^{(m)}$ for some $m \in \mathbb{Z}_n^*$.* □

Remarks: a) The isomorphisms used in [Muz95a] coincide with the algebraic isomorphisms in the sense of 1.5.
b) Notice that the exponent m may depend on the basic set T.

As a consequence of this Theorem and Proposition 2.2 we obtain:

2.5. Theorem([Muz95a, (Thm. 1.1)]). *Any two algebraically isomorphic S-rings over C_n coincide.* □

The theorems 2.4 and 2.5 imply the following one:

2.6. Theorem. *Let $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ be an S-ring over C_n and let $\lambda : \mathsf{Basic}(\mathcal{A}) \to \mathsf{Basic}(\mathcal{A})$ be an algebraic automorphism of $\mathcal{A}$. Then for every $T \in \mathsf{Basic}(\mathcal{A})$ 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 $(m_T)_{T \in \mathsf{Basic}(\mathcal{A})}$ but not vice versa, since each m_T may be replaced by any product $m_T c$ with $c \in \mathsf{Stab}_*(T)$. Moreover, an arbitrary choice of $(m_T)_{T\in\mathsf{Basic}(\mathcal{A})}$ may not correspond to an algebraic 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 result.

2.7. Lemma ([Muz95a, (Prop. 3.1)]). *Let $f : \mathcal{A} \to \mathcal{B}$ be an algebraic isomorphism between two S-rings. 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) $\mathsf{Stab}_*(\underline{T}^f) = \mathsf{Stab}_*(\underline{T})$. □

2.8. Definition. For a divisor $d|n$ and a subset $S \subseteq C_n$ let S_d denote the set of all elements in S of order $r := \dfrac{n}{d}$. In particular, $(C_n)_d$ contains all elements of order r. We call $S_d = S \cap (C_n)_d$ a *layer* of S.

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

Proof. Fix an arbitrary $T \in \mathsf{Basic}(\mathcal{A})$ with $T \cap (C_n)_d \neq \emptyset$. By 2.6 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 nontrivially $(C_n)_d$, then there exists $m \in \mathbb{Z}_n^*$ with $T^{(m)} \cap T' \neq \emptyset$. Therefore $T' = T^{(m)}$. By Lemma 2.7, $T'^f = (T^{(m)})^f = (T^f)^{(m)} = (T^{(m_T)})^{(m)} = T^{(m_T m)} = T^{(m m_T)} = T'^{(m_T)}$. To finish the proof it is enough to put $m_d := m_T$. □

The following theorem gives a necessary isomorphism condition for Cayley graphs over a cyclic group.

2.10. Theorem. *Let $\Gamma_{C_n}(S)$ and $\Gamma_{C_n}(R)$ be two isomorphic Cayley graphs. Then for each $d|n$ there exists $m_d \in \mathbb{Z}_n^*$ such that $S_d^{(m_d)} = R_d$.*

PROOF. Let $f : C_n \to C_n$ be an isomorphism between $\Gamma_{C_n}(S)$ and $\Gamma_{C_n}(R)$. Then, by Theorem 1.9(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 $\mathsf{B}_S := \mathsf{Basic}(\langle\langle S\rangle\rangle)$ and $\mathsf{B}_R := \mathsf{Basic}(\langle\langle R\rangle\rangle)$. By 1.9(3) we have

$$R = \bigcup\{T^{f^*} \mid T \in \mathsf{B}_S \text{ and } T \subseteq S\}\,.$$

Therefore for arbitrary $d|n$ we obtain

$$\begin{aligned}
R_d &= \bigcup\{T^{f^*} \cap (C_n)_d \mid T \in \mathsf{B}_S \text{ and } T \subseteq S\} \\
&\overset{(2.6)}{=} \bigcup\{T^{(m_T)} \cap (C_n)_d \mid T \in \mathsf{B}_S \text{ and } T \subseteq S\} \\
&= \bigcup\{(T \cap (C_n)_d)^{(m_T)} \mid T \in \mathsf{B}_S \text{ and } T \subseteq S\} \\
&= \bigcup\{(T \cap (C_n)_d)^{(m_T)} \mid T \in \mathsf{B}_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\} \\
&\overset{(2.9)}{=} \bigcup\{(T \cap (C_n)_d)^{(m_d)} \mid T \in \mathsf{B}_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\} \\
&= \left(\bigcup\{(T \cap (C_n)_d) \mid T \in \mathsf{B}_S, T \subseteq S, T \cap (C_n)_d \neq \emptyset\}\right)^{(m_d)} \\
&= S_d^{(m_d)}\,.
\end{aligned}$$

□

3 Isomorphism criteria for circulant graphs

In this section we recall and investigate some necessary and/or sufficient conditions for two circulant graphs $\Gamma_n(S)$ and $\Gamma_n(R)$ to be isomorphic, $S, R \subseteq \mathbb{Z}_n$ (see 3.2 below). We start with some preliminary remarks.

3.1. Multiplicative versus additive notation. Instead of the multiplicatively written cyclic group C_n, one may alternatively take the additively written cyclic group $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with addition modulo n. In order to avoid confusion with the addition operation in S-rings up to now we used the multiplicative notation.

multiplicative		additive	
$a, b \in C_n$	$(= \{e, g_0, g_0^2, \ldots, g_0^{n-1}\})$	$a, b \in \mathbb{Z}_n$	$(= \{0, 1, 2, \ldots, n-1\})$
$a \cdot b$		$a + b$	
a^{-1}		$-a$	
a^m		ma	(for $m \in \mathbb{Z}$)
$S^{(m)}$	(for $S \subseteq C_n$)	mS	$(= \{ms \mid s \in S\}$ for $S \subseteq \mathbb{Z}_n)$
$S \cdot a$		$S + a$	
$(C_n)_d$	(for $d \mid n$)	$(\mathbb{Z}_n)_d$	$(= \{x \in \mathbb{Z}_n \mid \gcd(x, n) = d\})$
$(C_n)_1$		$\mathbb{Z}_n^*$	
S_d	$(= S \cap (C_n)_d)$	S_d	$(= \{x \in S \mid \gcd(x, n) = d\})$
$\Gamma_{C_n}(S)$		$\Gamma_n(S)$	
$a \mapsto a^m$	$(m \in \mathbb{Z}_n^* \cong \mathsf{Aut}(C_n))$	$a \mapsto ma$	action of $m \in \mathbb{Z}_n^* \cong \mathsf{Aut}(\mathbb{Z}_n)$
$\mathsf{Stab}_*(S)$	$(= \{m \in \mathbb{Z}_n^* \mid S^{(m)} = S\})$	$\mathsf{Stab}_*(S)$	$(= \{m \in \mathbb{Z}_n^* \mid mS = S\})$
$\mathsf{Stab}_+(S)$	$(= \{g \in C_n \mid S \cdot g = S\})$	$\mathsf{Stab}_+(S)$	$(= \{m \in \mathbb{Z}_n \mid S + m = S\})$

Table 1: Multiplicative and additive notation

Dealing with circulant graphs, usually one prefers the additive notation. Therefore, in Table 1 we give a “dictionary” for both notations. In particular, we write $\Gamma_n(S)$ for the Cayley graph $\Gamma_{\mathbb{Z}_n}(S)$.

3.2. Circulant graphs. Let $H \leq \mathsf{Sym}(X)$ be a regular cyclic permutation group acting on X and let g_0 be a generating element, fixed from now on. A graph Γ with vertex set X is called *circulant*, if $g_0 \in \mathsf{Aut}(\Gamma)$. Usually one identifies both H and X with $\mathbb{Z}_n$ for $n = |X|$, and takes $g_0 = (0, 1, \ldots, n-1)$ (cyclic shift $g_0 : x \mapsto x+1$) as generating cycle. For a circulant graph Γ, the set $S := \{x \in \mathbb{Z}_n \mid (x, 0) \in E\}$ is called the *connection set* of Γ.
We observe: *The set of all such circulant graphs*, which we shall denote by $\mathsf{Circ}(H; X)$ or simply by $\mathsf{Circ}(\mathbb{Z}_n)$, *is just the set of all Cayley graphs over the group* $H = \mathbb{Z}_n$ (cf. 1.2).
In fact: According to 1.2 (and Table 1), $\{(x, y) \mid x - y \in S\}$ is the set of edges of the Cayley graph $\Gamma_n(S)$. Thus the cycle g_0 is obviously an automorphism of $\Gamma_n(S)$. Conversely, let $\Gamma = (\mathbb{Z}_n, E)$ be a circulant graph with edge set $E \subseteq \mathbb{Z}_n \times \mathbb{Z}_n$, $g_0 \in \mathsf{Aut}(\Gamma)$ and connection set S. From $(x, y) \in E \iff (x^{g_0^{n-y}}, y^{g_0^{n-y}}) = (x - y, 0) \in E$ it follows that $\Gamma = \Gamma_n(S)$. $\square$

Now we investigate isomorphism criteria for circulant graphs over $\mathbb{Z}_n$. From 2.10 we immediately get:

3.3. A necessary condition for arbitrary *n*. If $\Gamma_n(S) \cong \Gamma_n(R)$, then:

For all $d|n$, there exist $m_d \in \mathbb{Z}_n^*$, such that $m_d S_d = R_d$. $\quad (^\circ)$

In particular, the "layer graphs" $\Gamma_n(S_d)$ and $\Gamma_n(R_d)$ are isomorphic since the mapping $x \mapsto m_d x$ (for $m_d \in \mathbb{Z}_n^*$) is an isomorphism between these layers whenever $m_d S_d = R_d$. Thus we obtain as a corollary of Theorem 2.10 the following result (which for $d = 1$, i.e. $S \subseteq \mathbb{Z}_n^* = (\mathbb{Z}_n)_1$, sometimes is called the Toida Conjecture, [Toi77]), here in additive notation:

3.4. Theorem. *Let $\Gamma_n(S)$ and $\Gamma_n(R)$ be two circulant graphs. Assume that $S \subseteq (\mathbb{Z}_n)_d$ for some $d|n$. Then we have*

$$\Gamma_n(S) \cong \Gamma_n(R) \iff \exists\, m \in \mathbb{Z}_n^* : mS = R \quad (\iff \langle\!\langle S \rangle\!\rangle \cong_{Cay} \langle\!\langle R \rangle\!\rangle).$$
□

In view of 3.3 it is natural to ask if it is possible to add some additional conditions to the multipliers m_d in order to get a condition which is both necessary *and* sufficient. The simplest condition would be the possibility to choose all m_d equal to a single multiplier m. This is exactly the famous ***Àdàm's conjecture*** saying that the connection sets S and R of isomorphic graphs satisfy $mS = R$ for some $m \in \mathbb{Z}_n^*$, that is in our terminology: isomorphic Cayley graphs over $\mathbb{Z}_n$ are also Cayley isomorphic (cf. 1.2, note $\mathbb{Z}_n^* = \mathsf{Aut}(\mathbb{Z}_n)$).

It turned out soon that Àdàm's conjecture is true only in very special cases. In the context of our general approach, Àdàm's conjecture holds for $\mathbb{Z}_n$ if for every combinatorial isomorphism $f : \mathcal{A} \to \mathcal{B}$ between two S-rings (over $\mathbb{Z}_n$) one can find a Cayley isomorphism g with the same action on the basic sets, i.e., $T^{f^*} = T^{g^*}$ for $T \in \mathsf{Basic}(\mathcal{A})$.

We report here the following two results that show the answer to the above general question about additional conditions for the m_d's in case of (twice) squarefree n (here Àdàm's conjecture holds) and for odd prime power n.

3.5. Isomorphism criterion for (twice) square-free n ([Muz95b]).
Let $n \in \mathbb{Z}$ be *square-free* or *twice square-free*, resp., i.e. $n = cp_1p_2 \dots p_m$ is a product of pairwise distinct prime numbers with the additional factor $c = 1$ or $c = 2$, resp. Then we have:

Two circulant graphs $\Gamma_n(S)$ and $\Gamma_n(R)$ $(S, R \subseteq \mathbb{Z}_n)$ are isomorphic if and only if there exists $m \in \mathbb{Z}_n^*$ such that $R = mS$.

3.6. Isomorphism criterion for prime power n ([Kli-P80]).
Let $n = p^\alpha$ be a prime power $(p \neq 2)$. For $S \subseteq \mathbb{Z}_n$ we introduce the simplified layer notation

$$S_i := \{x \in S \mid \gcd(x, n) = p^i\}$$

instead of S_{p^i} (cf. 2.8).

Two circulant graphs $\Gamma_n(S)$ and $\Gamma_n(R)$ $(S, R \subseteq \mathbb{Z}_n)$ are isomorphic if and only if there exist $m_0, \dots, m_{\alpha-1} \in \mathbb{Z}_n^*$ such that $R_i = m_i S_i$, $0 \leq i \leq \alpha - 1$ and the following "equality conditions" are satisfied for all pairs $0 \leq i < j \leq \alpha - 1$:

If $(1 + p^{j-i})S_i \neq S_i$, then

$$(*)_i^j \quad \begin{cases} m_i & \equiv & m_{i+1} & \pmod{p^{j-i}}\,, \\ & \vdots & & \\ m_t & \equiv & m_{t+1} & \pmod{p^{j-t}}\,, \\ & \vdots & & \\ m_{j-1} & \equiv & m_j & \pmod{p}\,. \end{cases}$$

3.7. Decomposition of $\mathbb{Z}_n$. Some notations.
Let $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ be the prime number decomposition of $n \in \mathbb{N}$ where $p_i \neq p_j$ for $i \neq j$. Then $\mathbb{Z}_n$ is isomorphic to the direct sum of primary cyclic groups:

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}\,,$$

and with respect to this decomposition we also have

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{\alpha_1}}^* \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}^*\,.$$

Thus every $z \in \mathbb{Z}_n$ can be represented as

$$z = [\![z_1, \ldots, z_k]\!] \quad \text{with} \quad z_i \in \mathbb{Z}_{p_i^{\alpha_i}}, \tag{1}$$

where addition and multiplication in $\mathbb{Z}_n$ can be done componentwise in each $\mathbb{Z}_{p_i^{\alpha_i}}$ (if, more generally, appear arbitrary entries z_i then they must be taken modulo $p_i^{\alpha_i}$, e.g. $z_i = p_i^{\alpha_i} \equiv 0$). The special brackets $[\![\ldots]\!]$ are used to remind that we have to deal not with arbitrary k-tuples but with elements of $\mathbb{Z}_n$. Moreover, every element $x \in \mathbb{Z}_{p^\alpha}$ admits a unique decomposition of the following form:

$$x = \sum_{i=0}^{\alpha-1} x_i p^i, \tag{2}$$

where $x_i \in \{0, 1, ..., p-1\}$ and all arithmetic is done modulo p^α. To simplify notation (and to avoid double indices) we write $n = p^\alpha \cdot \cdots \cdot q^\beta$ and $z = [\![x, \ldots, y]\!]$ instead of (1). Then (1) and (2) together give a presentation of each $z \in \mathbb{Z}_n$ in the form

$$z = [\![\sum_{i=0}^{\alpha-1} x_i p^i, \ldots, \sum_{j=0}^{\beta-1} y_j q^j)]\!]. \tag{3}$$

Let $d = p^{a(d)} \cdot \cdots \cdot q^{b(d)}$ be an arbitrary divisor of n. Then, by definition, $(\mathbb{Z}_n)_d$ consists of all elements of the form $\mu \cdot [\![p^{a(d)}, \ldots, q^{b(d)}]\!]$ with $\mu \in \mathbb{Z}_n^*$. For $\emptyset \neq S_d \subseteq (\mathbb{Z}_n)_d$ the stabilizer $\mathsf{Stab}_+(S_d)$ is a subgroup of $\mathbb{Z}_n$ (cf. 2.3) of order, say $\dfrac{n}{\hat{d}}$. Thus it is generated by an element of that order, e.g. by $[\![p^{a(\hat{d})}, \ldots, q^{b(\hat{d})}]\!]$ (where $\hat{d} = p^{a(\hat{d})} \cdot \cdots \cdot q^{b(\hat{d})}$), and we have

$$\mathsf{Stab}_+(S_d) = \langle [\![p^{a(\hat{d})}, \ldots, q^{b(\hat{d})}]\!] \rangle = \{ \lambda \cdot [\![p^{a(\hat{d})}, \ldots, q^{b(\hat{d})}]\!] \mid \lambda \in \mathbb{Z}_n \}.$$

Moreover, we claim that

$$a(d) < a(\hat{d}), \ldots, b(d) < b(\hat{d}).$$

whenever $a(d) < \alpha, \ldots, b(d) < \beta$, respectively. Indeed, if $a(d) \geq a(\hat{d})$, then we have for any $\mu \cdot [\![p^{a(d)}, \ldots, q^{b(d)}]\!] \in S_d$ ($\mu \in \mathbb{Z}_n^*$):

$$\mu \cdot [\![p^{a(d)}, \ldots, q^{b(d)}]\!] + \mu \cdot [\![(p-1) p^{a(d)-a(\hat{d})}, 1, \ldots, 1]\!] \cdot [\![p^{a(\hat{d})}, \ldots\, q^{b(\hat{d})}]\!] \\ \in S_d + \mathsf{Stab}_+(S_d) \subseteq S_d.$$

On the other hand,

$$\mu\cdot[\![p^{a(d)},\dots,q^{b(d)}]\!]+\mu\cdot[\![(p-1)p^{a(d)-a(\hat d)},1,\dots,1]\!]\cdot[\![p^{a(\hat d)},\dots q^{b(\hat d)}]\!] \\ =\mu\cdot[\![p^{a(d)+1},\dots]\!]\notin S_d\,,$$

since $S_d\subseteq(\mathbb{Z}_n)_d$, a contradiction. This proves the claim.

Remark: The tuple $(a(\hat d),\dots,b(\hat d))$ can be defined equivalently to be the least[3] tuple satisfying

$$S_d+[\![p^{a(\hat d)},\dots,q^{b(\hat d)}]\!]=S_d\,.$$

This characterization also gives a practicable method to determine the values $a(\hat d),\dots,b(\hat d)$. The case $d=n$ is not excluded but trivial, since $(\mathbb{Z}_n)_n=\{0\}$ and thus circulants with $S_n\neq\emptyset$ are just circulants with loops.

3.8. A sufficient condition for arbitrary *n*. In addition to the necessary condition in 3.3, we now present a sufficient condition. We shall use the same notations as in 3.7.

Assume that for two Cayley graphs $\Gamma_n(S)$ and $\Gamma_n(R)$, $S,R\subseteq\mathbb{Z}_n$, $n=p^\alpha\cdot\dots\cdot q^\beta$ the following condition $(^{\circ\circ})$ is satisfied:

$$\left[\begin{array}{l}\text{There exist elements } \mu_i\in\mathbb{Z}_{p^\alpha},\dots,\nu_j\in\mathbb{Z}_{q^\beta}\ (0\le i\le\alpha-1,\\ \dots,\ 0\le j\le\beta-1) \text{ such that the following holds: For every}\\ d|n \text{ with } d=p^{a(d)}\cdot\dots\cdot q^{b(d)} \text{ we have}\\ \begin{array}{rcll} R_d &=& m_dS_d & \text{where}\quad m_d:=[\![\mu_{a(d)},\dots,\nu_{b(d)}]\!],\\ \mu_ip^i &\equiv& \mu_{a(d)}p^i & \pmod{p^{a(\hat d)}}\quad \text{for}\quad a(d)\le i<a(\hat d)\,,\\ & \vdots & & \\ \nu_jq^j &\equiv& \nu_{b(d)}q^j & \pmod{q^{b(\hat d)}}\quad \text{for}\quad b(d)\le j<b(\hat d)\end{array}\\ (\text{where } \hat d \text{ is defined in } 3.7).\end{array}\right] \qquad (^{\circ\circ})$$

Then we have $\Gamma_n(S)\cong\Gamma_n(R)$.

[3] with respect to the componentwise natural order in $\mathbb{Z}_{p^\alpha}\oplus\dots\oplus\mathbb{Z}_{q^\beta}$.

PROOF. Assume $(^{\circ\circ})$. For simplicity let $a = a(d)$, $b = b(d)$, $\hat{a} = a(\hat{d})$, $\hat{b} = b(\hat{d})$. A routine check shows that the mapping $f : \mathbb{Z}_n \to \mathbb{Z}_n$ defined by

$$z^f := [\![\sum_{i=0}^{\alpha-1} \mu_i x_i p^i, \ldots, \sum_{j=0}^{\beta-1} \nu_j y_j q^j]\!]$$

for $z = [\![\sum_{i=0}^{\alpha-1} x_i p^i, \ldots, \sum_{j=0}^{\beta-1} y_j q^j]\!]$ is a permutation. We are going to show that f is an isomorphism from $\Gamma_n(S)$ onto $\Gamma_n(R)$. Moreover it is even an isomorphism between the layers graphs $\Gamma_n(S_d)$ onto $\Gamma_n(R_d)$.

Thus let $z - z' \in S$, i.e. $z - z' \in S_d$ for some $d|n$. We have to prove $z^f - z'^f \in R_d$. In fact, $z - z' \in S_d$ implies (by definition of S_d) $x_i = x_i', \ldots, y_j = y_j'$ for $i \in \{0, 1, \ldots, a-1\}, \ldots, j \in \{0, 1, \ldots, b-1\}$ and we obtain (using $(^{\circ\circ})$):

$$\begin{aligned}
z^f - z'^f &= [\![\sum_{i=0}^{\alpha-1} \mu_i (x_i - x_i') p^i, \ldots, \sum_{j=0}^{\beta-1} \nu_j (y_j - y_j') q^j]\!] \\
&= [\![\sum_{i=a}^{\hat{a}-1} \mu_i (x_i - x_i') p^i, \ldots, \sum_{j=b}^{\hat{b}-1} \nu_j (y_j - y_j') q^j]\!] \\
&\qquad + [\![\sum_{i=\hat{a}}^{\alpha-1} \mu_i (x_i - x_i') p^i, \ldots, \sum_{j=\hat{b}}^{\beta-1} \nu_j (y_j - y_j') q^j]\!] \\
&= [\![\sum_{i=a}^{\hat{a}-1} \mu_a (x_i - x_i') p^i, \ldots, \sum_{j=b}^{\hat{b}-1} \nu_b (y_j - y_j') q^j]\!] \\
&\qquad\qquad + \lambda \cdot [\![p^{\hat{a}}, \ldots, q^{\hat{b}}]\!] \\
&\in [\![\mu_a, \ldots, \nu_b]\!] \cdot [\![\sum_{i=a}^{\hat{a}-1} (x_i - x_i') p^i, \ldots, \sum_{j=b}^{\hat{b}-1} (y_j - y_j') q^j]\!] \\
&\qquad\qquad + \langle [\![p^{\hat{a}}, \ldots, q^{\hat{b}}]\!] \rangle \\
&= m_d \cdot (z - z') + \langle [\![p^{\hat{a}}, \ldots, q^{\hat{b}}]\!] \rangle \\
&= m_d \Big((z - z') + \langle [\![p^{\hat{a}}, \ldots, q^{\hat{b}}]\!] \rangle \Big)
\end{aligned}$$

$$= m_d\left((z - z') + \mathsf{Stab}_+(S_d)\right)$$
$$\subseteq m_d\left(S_d + \mathsf{Stab}_+(S_d)\right) = m_d S_d = R_d\,,$$

(for suitable $\lambda \in \mathbb{Z}_n$). Empty sums appear if e.g. $a = \alpha$, then the sum equals 0. □

3.9. Open problem. The condition 3.8($^{\circ\circ}$) turns out to be equivalent to the conditions in 3.5 (simply take $m := [\![\mu_0, \ldots, \nu_0]\!]$) and 3.6 (see proof of 6.3) for the square-free and prime power cases. Thus there is some hope that the condition is close to necessary, also (cf. also 4.7). We formulate this as an open problem:
Prove or disprove that condition 3.8($^{\circ\circ}$) is a necessary and sufficient condition for circulant graphs to be isomorphic ($n \in \mathbb{Z}$ arbitrary).

4 Solving sets for circulant graphs: General case

In this section we investigate another attack on the isomorphism problem: we introduce and investigate so-called solving sets which – whenever known – solve completely the isomorphism problem for circulant graphs. The subsequent sections deal with special cases of this general approach.

4.1. Solving sets. A set $P \subseteq \mathsf{Sym}(X)$ is called a *solving set* for a class $\mathcal{K} \subseteq \mathsf{Circ}(H;X)$ of circulant graphs (cf. 3.2), if any two graphs $\Gamma \in \mathcal{K}$ and $\Gamma' \in \mathsf{Circ}(H;X)$ are isomorphic if and only if there exists a $g \in P$ such that $\Gamma^g = \Gamma'$. In the case when $\mathcal{K}$ consists of a single graph Γ we shall say that P is a solving set for Γ.

A solving set P for $\mathcal{K}$ is called *minimal* if it is a solving set of a minimal cardinality (in particular, no proper subset is a solving set).

Thus every solving set resolves the isomorphism problem for circulant graphs in $\mathcal{K}$. Note that in this terminology Ádám's conjecture holds for $\mathbb{Z}_n$ if and only if $\mathbb{Z}_n^*$ (considered as subgroup of $\mathsf{Sym}(\mathbb{Z}_n)$, cf. 2.1) is a solving set for $\mathsf{Circ}(\mathbb{Z}_n)$, and a graph is a CI-graph if $\mathbb{Z}_n^*$ is a solving set for it.

4.2. Cycle bases. By $[H, \mathsf{Sym}(X)] := \{G \le \mathsf{Sym}(X) \mid H \le G\}$ we denote the set of all *overgroups* of H in $\mathsf{Sym}(X)$ (interval in the subgroup lattice of $\mathsf{Sym}(X)$).

A subset C of a group $G \in [H, \mathsf{Sym}(X)]$ is called a *cycle base* ([Pon]) of G if every *full cycle* $g \in G$ (i.e. a cycle of length $n = |X|$ and therefore of the form $g_0^s := s^{-1}g_0 s$ for some $s \in \mathsf{Sym}(X)$) is conjugate in G to exactly one element from C. Thus $|C|$ is equal to the number of conjugacy classes of full cycles in G.

The next Proposition 4.3 motivates the following definition: A subset $P \subseteq \mathsf{Sym}(X)$ is called a *solving set for a group* $G \in [H, \mathsf{Sym}(X)]$ if $\{g_0^{g^{-1}} \mid g \in P\} = \{gg_0g^{-1} \mid g \in P\}$ contains at least one cycle base of G, and P is called *minimal* if $\{gg_0g^{-1} \mid g \in P\}$ is a cycle base of G.

The following Proposition may be easily derived from [Als-P79] and [Bab77] (see also [MuzXX]) but we add a proof here for completeness:

4.3. Proposition. *Let* $\Gamma \in \mathsf{Circ}(H; X)$*. Then the following conditions are equivalent:*

(i) *P is a solving set (minimal solving set, resp.) for* Γ*,*

(ii) *P is a solving set (minimal solving set, resp.) for* $\mathsf{Aut}(\Gamma)$*.*

PROOF. (i) $\Longrightarrow$ (ii). Let $r \in \mathsf{Aut}(\Gamma)$ be a full cycle. Then $r = g_0^{f^{-1}}$ for some $f \in \mathsf{Sym}(X)$. Then $g_0 \in \mathsf{Aut}(\Gamma^f)$, *i.e.*, $\Gamma^f \in \mathsf{Circ}(H; X)$. Therefore, by (i), $\Gamma^f = \Gamma^p$ for some $p \in P$ implying $g := pf^{-1} \in \mathsf{Aut}(\Gamma)$. Therefore $r = g_0^{p^{-1}g}$ from which it follows that $r^G \cap \{g_0^{p^{-1}} \mid p \in P\} \neq \emptyset$.

(ii) $\Longrightarrow$ (i) Let $\Gamma' \in \mathsf{Circ}(H; X)$ be a circulant graph isomorphic to Γ, *i.e.*, $\Gamma' = \Gamma^f$ for a suitable $f \in \mathsf{Sym}(X)$. Since $g_0 \in \mathsf{Aut}(\Gamma') = \mathsf{Aut}(\Gamma)^f$ we have $g_0^{f^{-1}} \in \mathsf{Aut}(\Gamma)$. Further, since P is a solving set for $\mathsf{Aut}(\Gamma)$ and $g_0^{f^{-1}}$ is a full cycle there must exist $g \in \mathsf{Aut}(\Gamma)$ and $p \in P$ such that $g_0^{f^{-1}} = (g_0^{p^{-1}})^g$. Therefore $f^{-1}g^{-1}p$ centralizes g_0. Hence $f^{-1}g^{-1}p = g_0^k$ for some $k \in \mathbb{Z}$. Now we obtain $\Gamma^p = \Gamma^{g^{-1}p} = \Gamma^{fg_0^k} = \Gamma'^{g_0^k} = \Gamma'$ which implies that P is a solving set for Γ. $\square$

Proposition 4.3 in particular implies that the number of distinct circulant graphs isomorphic to a given one equals the number of conjugacy classes of full cycles in $\mathsf{Aut}(\Gamma)$. Elementary arguments show that the number of such classes does not exceed $|X|-1$. This upper bound can be improved to $\varphi(|X|)$ (by using the classification of finite simple groups in the general case and by more elementary methods for prime powers $|X|$, see [Muz97], [MuzXX]).

How does one find a solving set for $\mathsf{Circ}(H;X)$? Obviously one may proceed as follows:

Take the automorphism groups of all graphs from the class $\mathsf{Circ}(H;X)$, and for each of them find a cycle base and (using Proposition 4.3) build a minimal solving set for each $\Gamma \in \mathsf{Circ}(H;X)$. Clearly, the union of all "individual" solving sets will give a solving set for the complete class $\mathsf{Circ}(H;X)$. This approach seems intractable, since it requires the knowledge of all automorphism groups of circulant graphs. Fortunately however, one can reduce the set of required groups using the simple observation given in the next Proposition 4.5 below.

4.4. Cycle complete embeddings. Let F, G be two subgroups belonging to $[H, \mathsf{Sym}(X)]$. We say that F is *cycle complete embedded* into G (called *well embedded* in [MuzXX]), notationally $F \preceq G$, if $F \leq G$ and if for every regular cyclic subgroup $E \leq G$ there exists a $g \in G$ such that $E^g \leq F$. It can be shown easily that $\preceq$ is a partial ordering on $[H, \mathsf{Sym}(X)]$.

4.5. Proposition. *If $F \preceq G$, then any solving set for F is a solving set for G as well.*

Proof. It follows directly from the definition of $\preceq$ that each cycle base of F is a cycle base of G as well. Now the claim follows from the definition of a solving set for a permutation group (cf. 4.2). □

4.6. Due to Proposition 4.5 we need to analyze only the $\preceq$-minimal subgroups of $[H, \mathsf{Sym}(X)]$. To illustrate how this approach works we consider circulant graphs with $|X| = p^\alpha$ vertices, where p is a prime (for more details see sections 6 and 5).

From Sylow's theorems it follows that a Sylow p-subgroup P of an arbitrary $G \in [H, \mathsf{Sym}(X)]$ is cycle complete embedded in G provided that $P \in [H, \mathsf{Sym}(X)]$. So, in order to find a solving set for circulant graphs Γ it is sufficient to find such a set for the Sylow p-subgroups of $\mathsf{Aut}(\Gamma)$ only. The automorphism groups of circulant graphs have a very strong property, namely they are 2-closed.

Recall that the 2-*closure* of a permutation group (G, X) is defined by

$$G^{(2)} := \bigcap \{\mathsf{Aut}(\Gamma) \mid \Gamma \text{ is a graph on } X \text{ with } G \leq \mathsf{Aut}(\Gamma)\}.$$

We note that for any group G containing H as regular subgroup holds $V(H, G_0) = V(H, (G^{(2)})_0)$ and $G^{(2)} = \mathsf{Aut}(V(H, G_0))$.

A Sylow p-subgroup of 2-closed permutation group is also 2-closed (see Proposition 5.2). Therefore, we have to analyze 2-closed p-groups from the class $[H, \mathsf{Sym}(X)]$. It turns out that for $p > 2$ the number of these groups does not depend on p but only on α (more precisely, it is the α^{th} Catalan number which we shall denote by c_α). Since a minimal solving set for every p-group $P \in [H, \mathsf{Sym}(X)]$ does not exceed $\varphi(p^\alpha) = |\mathbb{Z}_{p^\alpha}^*|$, the resulting solving set contains at most $\mathsf{c}_\alpha \cdot (p^\alpha - p^{\alpha-1})$ permutations, i.e., it has cardinality less than $|X|^2$.

4.7. The isomorphism problem for circulant graphs: Conjecture. Let $P_1 \subseteq \mathsf{Sym}(\mathbb{Z}_{p_1^{a_1}}), \ldots, P_m \subseteq \mathsf{Sym}(\mathbb{Z}_{p_m^{a_m}})$ be arbitrary sets of permutations, then $P_1 \times \cdots \times P_m$ has a natural action on the set $\mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{a_m}}$:

$$(x_1, \ldots, x_m)^{(\pi_1, \ldots, \pi_m)} = (x_1^{\pi_1}, \ldots, x_m^{\pi_m}).$$

In what follows we identify $P_1 \times \cdots \times P_m$ with the corresponding subset of $\mathsf{Sym}(\mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{a_m}})$.

Now we can formulate the following conjecture which reduces the isomorphism problem to the prime power case.

Conjecture. *If, for every $i \in \{1, \ldots, m\}$, $P_i \subseteq \mathsf{Sym}(\mathbb{Z}_{p_i^{a_i}})$ is a solving set for the circulant graphs in $\mathsf{Circ}(\mathbb{Z}_{p_i^{a_i}})$, then $P_1 \times \cdots \times P_m$ is a solving set for the circulant graphs in $\mathsf{Circ}(\mathbb{Z}_n)$* (using the decomposition $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{a_1}} \oplus \cdots \oplus \mathbb{Z}_{p_m^{a_m}}$, cf. 3.7).

If this conjecture were true then, as a corollary, Problem 3.9 would be solved, i.e. condition 3.8($^{\circ\circ}$) would be a necessary and sufficient condition for $\Gamma_n(S) \cong \Gamma_n(R)$.

4.8. Proposition. *Let $G \leq \mathsf{Sym}(\mathbb{Z}_n)$ be a 2-closed permutation group that contains the full cycle $g_0 = (0, 1, \ldots, n-1)$. If, for some permutation $\hat{f} : i \mapsto a_i$ $(i \in \mathbb{Z}_n)$, the full cycle $\hat{f}^{-1} g_0 \hat{f} = (a_0, ..., a_{n-1})$ belongs to G, then $\hat{f}$ belongs to $\mathsf{Out}(V(\mathbb{Z}_n, G_0))$. In particular, $\hat{f}$ normalizes G.*

Proof. Let $f := \hat{f}^{-1} g_0 \hat{f}$. Both, $F := \langle f \rangle$ and $\mathbb{Z}_n = \langle g_0 \rangle$, are regular subgroups of G. Thus we have (cf. 1.13)

$$V(\mathbb{Z}_n, G_0) \cong_{com} V(F, G_0)\,.$$

Let $\mathsf{Basic}(V(\mathbb{Z}_n, G_0)) = \{T_0, ..., T_d\}$. Thus there are also d basic set of $V(F, G_0)$ and their images under the isomorphism $F \to \mathbb{Z}_n : f^j \mapsto j$ $(j \in \mathbb{Z}_n)$ will be denoted by S_i, $i \in \{0, \ldots, d\}$. Then

$$\langle \underline{S_0}, ..., \underline{S_d} \rangle \cong_{Cay} V(F, G_0) \cong_{com} V(\mathbb{Z}_n, G_0).$$

Therefore $\langle \underline{S_0}, ..., \underline{S_d} \rangle \cong_{com} \langle \underline{T_0}, ..., \underline{T_d} \rangle$, whence, by 1.8 and 2.5, $\langle \underline{S_0}, ..., \underline{S_d} \rangle = \langle \underline{T_0}, ..., \underline{T_d} \rangle$.

Any T_α equals some S_β for a suitable β and we obtain:

$$\begin{aligned}
\Gamma_n(T_\alpha)^{\hat{f}} &= \{(i,j) \mid i,j \in \mathbb{Z}_n \ \wedge \ i-j \in T_\alpha\}^{\hat{f}} \\
&= \{(a_i, a_j) \mid i,j \in \mathbb{Z}_n \ \wedge \ i-j \in T_\alpha\} \\
&= \{(a_0^{f^i}, a_0^{f^j}) \in \mathbb{Z}_n^2 \mid i-j \in T_\alpha\} \\
&= \{(a_0^{f^i}, a_0^{f^j}) \mid i,j \in \mathbb{Z}_n \ \wedge \ i-j \in S_\beta\}\,.
\end{aligned}$$

The last line shows that $\Gamma_n(T_\alpha)^{\hat{f}}$ is a 2-orbit of G (cf. 1.10 and 1.12, 1.13). Hence, $\Gamma_n(T_\alpha)^{\hat{f}} = \Gamma_n(T_\gamma)$ for some $\gamma \in \{0, ..., d\}$. Thus, $\hat{f}$ permutes the 2-orbits of G, and therefore $\hat{f} \in \mathsf{Out}(V(\mathbb{Z}_n, G_0))$. Taking into account that $G = \mathsf{Aut}(V(\mathbb{Z}_n, G_0))$ (since G is 2-closed) we obtain that $\hat{f}$ normalizes G (cf. 1.6). $\square$

4.9. Transversals. For the next result we need the following definition. Let A be a normal subgroup of a group B. A subset $T \subseteq B$ is called *(A, B)-transversal* if T intersects each A-coset in exactly one element.

4.10. Theorem. *Let $G \leq \mathsf{Sym}(\mathbb{Z}_n)$ be a 2-closed permutation group, $\mathbb{Z}_n \leq G$ and let $\mathcal{A} := V(\mathbb{Z}_n, G_0)$. For an arbitrary set $P \subseteq \mathsf{Sym}(\mathbb{Z}_n)$ of permutations on $\mathbb{Z}_n$ the following conditions are equivalent:*

(i) *P is a minimal solving set for $G := \mathsf{Aut}(\mathcal{A})$* (cf. 4.2),

(ii) *P is an $(\mathsf{Aut}(\mathcal{A}), \mathsf{Out}(\mathcal{A}))$-transversal.*

PROOF. (i) $\Longrightarrow$ (ii): Since P is a minimal solving set for G, $\{pg_0p^{-1} \mid p \in P\}$ forms a cycle base of G (here $g_0 = (0, ..., n-1)$), cf. 4.3. By 4.8, we have $p^{-1} \in \mathsf{Out}(\mathcal{A})$ for $p \in P$. Hence $P \subset \mathsf{Out}(\mathcal{A})$. Consider the mapping $p \mapsto Gp \in \mathsf{Out}(\mathcal{A})/\mathsf{Aut}(\mathcal{A})$. It is injective, since $Gp_1 = Gp_2$ implies $p_1p_2^{-1} \in G$, therefore $p_1g_0p_1^{-1}$ and $p_2g_0p_2^{-1}$ are conjugate in G which is possible only if $p_1 = p_2$.

To finish the proof of this part it remains to show that the mapping $p \mapsto Gp$ is surjective. Take any $u \in \mathsf{Out}(\mathcal{A})$. Then ug_0u^{-1} is a full cycle in G and is, therefore, conjugate to exactly one element of the form pg_0p^{-1}; thus there exists $g \in G$ such that $gug_0u^{-1}g^{-1} = pg_0p^{-1}$. Consequently, the element $p^{-1}gu$ centralizes g_0. But $C_{\mathsf{Sym}(\mathbb{Z}_n)}(g_0) = \langle g_0 \rangle \leq G$. Therefore $G = Gp^{-1}gu$, and, by $G \trianglelefteq \mathsf{Out}(\mathcal{A})$, we obtain $Gp = Gu$.

(ii) $\Longrightarrow$ (i): Let P be an $(\mathsf{Aut}(\mathcal{A}), \mathsf{Out}(\mathcal{A}))$-transversal. Clearly, $pg_0p^{-1} \in \mathsf{Aut}(\mathcal{A})$ for every $p \in P$. Moreover, routine arguments show that pg_0p^{-1} $(p \in P)$ are pairwise non-conjugate in G.

It remains to show that each full cycle $u \in \mathsf{Aut}(\mathcal{A})$ is conjugate to one of the elements pg_0p^{-1} $(p \in P)$. Take $v \in \mathsf{Sym}(\mathbb{Z}_n)$ such that $u = vg_0v^{-1}$. By Proposition 4.8 we have $v^{-1} \in \mathsf{Out}(\mathcal{A})$, hence $v^{-1} = pg$ for some $g \in \mathsf{Aut}(\mathcal{A}), p \in P$, and therefore u is conjugate in G to pg_0p^{-1}. □

5 2-closed p-groups and p-S-rings

As mentioned in 4.6, solving sets for 2-closed p-groups play a crucial role in the general case of arbitrary n (cf. also 4.7). We start with some permutation group theoretic results on p-groups.

5.1. Proposition. *Let $G \leq \mathsf{Sym}(X)$ be a p-group, p a prime. Then its 2-closure $G^{(2)} \leq \mathsf{Sym}(X)$* (cf. 4.6) *is a p-group as well.*

In [Wie69] this proposition is left to the reader as Exercise 5.28. Nevertheless, for sake of completeness, we give here a
PROOF. If G is intransitive, then $G^{(2)}$ is a subdirect product of the 2-closures of the transitive components of G. So it is sufficient to prove our claim for transitive $G \leq \mathsf{Sym}(X)$. Let $G \leq \mathsf{Sym}(X)$ be a transitive p-group of degree p^α. We shall proceed by induction on α.
If G is abelian, then it acts regularly on X, and its 2-closure coincides with G. So we may assume that G is non-abelian. In this case its center $Z(G)$ is intransitive, since otherwise, the stabilizer G_x would be trivial and $G = Z(G)$. Because of $Z(G) \trianglelefteq G$, the $Z(G)$-orbits, say $\Delta_1, ..., \Delta_{p^\beta}$, $\beta < \alpha$, form a G-invariant partition of X. Then G induces a permutation group $G^\Delta \leq \mathsf{Sym}(\Delta)$ on the set $\Delta := \{\Delta_1, ..., \Delta_{p^\beta}\}$ of orbits where $G^\Delta \cong G/G_\Delta$ with $G_\Delta := \{g \in G \mid \forall_{0 \leq i \leq \beta}\, (\Delta_i^g = \Delta_i)\}$. Since G^Δ is a p-group, by induction hypothesis, $(G^\Delta)^{(2)}$ is a p-group and therefore also the subgroup $(G^{(2)})^\Delta \leq (G^\Delta)^{(2)}$ does. Because of $(G^{(2)})^\Delta \cong G^{(2)}/(G^{(2)})_\Delta$ and therefore $|G^{(2)}| = |(G^{(2)})_\Delta| \cdot |(G^{(2)})^\Delta|$, it remains to prove that $(G^{(2)})_\Delta$ is also a p-group.

First we note that $Z(G) \leq Z(G^{(2)})$. Indeed, for every $z \in Z(G)$ the relation $\varrho := \{(x, x^z) \mid x \in X\}$ is G-invariant. Therefore it is also invariant for every permutation $g \in G^{(2)}$, i.e., $(x^g, (x^z)^g) \in \varrho$. Consequently $(x^g)^z = (x^z)^g$ and thus $gz = zg$.

Each permutation $g \in (G^{(2)})_\Delta$ can be represented as a product $g = g_1 \cdot ... \cdot g_{p^\beta}$ with $g_i \in \mathsf{Sym}(\Delta_i)$. The restriction $Z(G)^{\Delta_i} \leq \mathsf{Sym}(\Delta_i)$ of $Z(G)$ on the orbit Δ_i (a so-called transitive constituent) is transitive and abelian. Since $Z(G)$ commutes with g elementwise, $Z(G)^{\Delta_i}$ centralizes g_i. Consider the subgroup $Q \leq \mathsf{Sym}(\Delta_i)$ generated by

$Z(G)^{\Delta_i}$ and g_i. Clearly, Q is abelian and transitive on Δ_i. Therefore, it is regular, from which it follows that $|Q| = |\Delta_i| = |Z(G)^{\Delta_i}|$. Hence $Q = Z(G)^{\Delta_i}$, or, equivalently, $g_i \in Z(G)^{\Delta_i}$. Thus $(G^{(2)})_\Delta$ is a subdirect product of the groups $Z(G)^{\Delta_i}, i = 1, ..., p^\beta$. Since each $Z(G)^{\Delta_i}$ is an abelian p-group, $(G^{(2)})_\Delta$ is an abelian p-group as well. Thus both $(G^{(2)})_\Delta$ and $(G^{(2)})^\Delta$ are p-groups, hence $G^{(2)}$ is also a p-group. □

Remark. Proposition 5.1 is a special case of the more general fact that the automorphism group of p-valenced association scheme is a p-group (see [Zie97] for definition and properties of a p-valenced scheme).
We mention in addition, that the 2-closure of a nilpotent group is also nilpotent.

A straight consequence of 5.1 is:

5.2. Corollary. *A Sylow p-subgroup of a 2-closed group is 2-closed.* □

5.3. p-S-rings. As in 3.2 let $H = \mathbb{Z}_n$, $X = \mathbb{Z}_n$ and let $p > 2$ be a prime number. An S-ring $\mathcal{A}$ over $\mathbb{Z}_n$ is called *p-S-ring* if the cardinality of each basic set $T \in \mathsf{Basic}(\mathcal{A})$ is a power of p (where $p^0 = 1$ is also allowed).

For example, the transitivity module $\mathcal{A} = V(\mathbb{Z}_n, G_0)$ of a 2-closed p-group $G \in [H, \mathsf{Sym}(X)]$ is a p-S-ring (and we have $G = \mathsf{Aut}(\mathcal{A})$).

We now restrict to the case $n = p^\alpha$ for which we explicitly can construct solving sets (see Theorem 6.5 and 6.6). However we believe that this approach can be generalized also to arbitrary n.

A complete classification of S-rings over $\mathbb{Z}_{p^\alpha}$ was given in [Pös74] (see also [Kli-P80]). From this description we obtain immediately the following characterization of p-S-rings over $\mathbb{Z}_{p^\alpha}$:

5.4. Theorem. *Let $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ be a p-S-ring over $\mathbb{Z}_{p^\alpha}$, $p > 2$. Then $\underline{\langle p^i \rangle} \in \mathcal{A}$ for each $i \in \{0, \ldots, \alpha - 1\}$ (recall $\langle p^i \rangle = \{\lambda \cdot p^i \mid \lambda \in \mathbb{Z}\} = \mathbb{Z}_{p^\alpha} \cdot p^i$) and there exists a vector $\mathbf{k} = (k_0, k_1, \ldots, k_{\alpha-1}) \in \{1, \ldots, \alpha\}^\alpha$ such that*

(i) $i < k_i \le \alpha$ *for all* $i \in \{0, 1, \ldots, \alpha - 1\}$*;*

(ii) $\mathbf{k}$ *is non-decreasing, i.e.,* $k_i \le k_{i+1}$*;*

(iii) *The basic sets of* $\mathcal{A}$ *are* $g + \langle p^{k_i} \rangle$*, where* $g \in \langle p^i \rangle \setminus \langle p^{i+1} \rangle$ *and* $0 \le i < \alpha$*.*

Conversely, each vector $\mathbf{k} = (k_0, k_1, \ldots, k_{\alpha-1})$ *that satisfies the conditions* (i)-(ii)*, defines an S-ring the basic sets of which are given by* (iii)*.* $\square$

5.5. Profile vectors. According to 5.4, each p-S-ring $\mathcal{A}$ over $\mathbb{Z}_{p^\alpha}$ is uniquely determined by a vector $\mathbf{k}$ satisfying (i) and (ii); we shall call such vectors *profile vectors*, in particular $\mathbf{k}$ is called the *profile* of $\mathcal{A}$. Therefore, there exists a one-to-one correspondence between p-S-rings and their profiles. Consequently, also 2-closed p-groups $P \in [H, \mathsf{Sym}(X)]$ are characterizable by profile vectors.

We also introduce here the profile for a single circulant graph as follows.

Let $S \subseteq \mathbb{Z}_{p^\alpha}$ be the connection set of a circulant graph $\Gamma_{p^\alpha}(S)$. As in 3.6 we decompose S into the disjoint union of its layers:

$$S = \bigcup_{i=0}^{\alpha-1} S_i \,.$$

Let p^{q_i} generate the cyclic subgroup $\mathsf{Stab}_+(S_i) \le \mathbb{Z}_{p^\alpha}$, $i \in \{0, \ldots, \alpha - 1\}$. Clearly, $i < q_i$ if $S_i \neq \emptyset$ (otherwise we set $q_i = 0$). Let $k_i := \max\{i + 1, q_0, q_1, \ldots, q_i\}$. Then $i < k_i$ and $k_i \le k_{i+1}$. Thus the vector $\mathbf{k} := (k_0, ..., k_{\alpha-1})$ is a profile vector called the *profile of the graph* $\Gamma_{p^\alpha}(S)$.

Remarks. Let $\Gamma_n(S)$ be a circulant graph with profile $\mathbf{k}$ and let $\mathcal{A}$ be the p-S-ring defined by this profile vector. Then we have $\langle\!\langle S \rangle\!\rangle \subseteq \mathcal{A}$ and therefore $\mathsf{Aut}(\langle\!\langle S \rangle\!\rangle) = \mathsf{Aut}(\Gamma(S)) \supseteq \mathsf{Aut}(\mathcal{A})$.

A predecessor of the profile vector can be found already (as "μ-values") in the "S-systems" defined in [Pös74, (4.11)].

5.6. Example. Let $p = 3$, $n = p^6 = 729$. We determine the profile of the circulant graph $\Gamma := \Gamma_{p^6}(S)$ with

$$\begin{aligned} S &= \{1 + \lambda p^3 \mid \lambda \in \mathbb{Z}_{p^3}\} \cup \{p + \lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\} \cup \{p^3 + \lambda p^5 \mid \lambda \in \mathbb{Z}_p\} \\ &= \{1, 28, 55, \ldots, 703\} \cup \{3, 84, 165, \ldots, 651\} \cup \{27, 270, 513\}\,. \end{aligned}$$

Then we have (cf. 5.5):

$$\begin{array}{llll} S_0 = \{1 + \lambda p^3 \mid \lambda \in \mathbb{Z}_{p^3}\}, & \mathsf{Stab}_+(S_0) = \langle p^3 \rangle, & q_0 = 3, & k_0 = 3, \\ S_1 = \{p + \lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\}, & \mathsf{Stab}_+(S_1) = \langle p^4 \rangle, & q_1 = 4, & k_1 = 4, \\ S_2 = \emptyset, & \mathsf{Stab}_+(S_2) = \langle p^0 \rangle, & q_2 = 0, & k_2 = 4, \\ S_3 = \{p^3 + \lambda p^5 \mid \lambda \in \mathbb{Z}_p\}, & \mathsf{Stab}_+(S_3) = \langle p^5 \rangle, & q_3 = 5, & k_3 = 5, \\ S_4 = \emptyset, & \mathsf{Stab}_+(S_4) = \langle p^0 \rangle, & q_4 = 0, & k_4 = 5, \\ S_5 = \emptyset, & \mathsf{Stab}_+(S_5) = \langle p^0 \rangle, & q_5 = 0, & k_5 = 6\,. \end{array}$$

Consequently, $\mathbf{k} = (3, 4, 4, 5, 5, 6)$ is the profile of Γ.

6 Solving sets for circulant graphs over $\mathbb{Z}_{p^\alpha}$

The conjecture in 4.7 gives an additional motivation to ask for solving sets for circulant graphs with $n := p^\alpha$ vertices. Due to 3.6 the isomorphism problem is solved in this case and we are going to interpret the solution 3.6 in terms of a solving set.

6.1. The permutations $f_{\mathbf{m}}$ and the set $P(p^\alpha)$. For each multiplier sequence $\mathbf{m} = (m_0, ..., m_{\alpha-1})$, $m_i \in \mathbb{Z}_n^*$, we define a map $f_{\mathbf{m}} : \mathbb{Z}_n \to \mathbb{Z}_n$ by

$$f_{\mathbf{m}}(x) := \sum_{i=0}^{\alpha-1} m_i x_i p^i\,,$$

where $x_i \in \{0, ..., p-1\}$ are defined by the decomposition $x = \sum_{i=0}^{\alpha-1} x_i p^i$ (and all arithmetic is to be done within $\mathbb{Z}_n$, i.e., modulo $n = p^\alpha$). This map is well-defined, since the decomposition of x is unique (cf. 3.7). A direct check shows that the map $f_{\mathbf{m}}$ is also a permutation on $\mathbb{Z}_n$. Let $P(p^\alpha)$ be the set of all such permutations.

6.2. Remarks. Notice that different multiplier sequences, say $\mathbf{m}$ and $\mathbf{n}$, may give the same permutation. Indeed, if $m_i p^i \equiv n_i p^i \pmod{p^\alpha}$ for all $i = 0, ..., \alpha - 1$, then $f_{\mathbf{m}}(x) = f_{\mathbf{n}}(x)$ for all $x \in \mathbb{Z}_n$. Therefore, the sequences $\mathbf{m}$ with $m_i \in \{1, ..., p^{\alpha-i} - 1\} \cap \mathbb{Z}_n^*$ exhaust the whole set $P(p^\alpha)$. The number of such permutations is $\prod_{j=1}^{\alpha}(p^j - p^{j-1}) = (p-1)^\alpha p^{\frac{\alpha(\alpha-1)}{2}}$. Thus the cardinality $|P(p^\alpha)|$ is about $n^{c \log n}$.

6.3. Theorem. *$P(p^\alpha)$ is a solving set for* $\mathsf{Circ}(H, X)$, *($H = \mathbb{Z}_{p^\alpha} = X$, cf. 3.2).*

Proof. We use the same notations as in 3.6. Let $n := p^\alpha$ and let $\Gamma_n(S) \cong \Gamma_n(R)$ be two isomorphic circulant graphs. We are going to show that there exists an isomorphism $f_{\mathbf{m}}$ in $P(n)$.
By 3.6 there exist $m_0, m_1, \ldots, m_{\alpha-1} \in \mathbb{Z}_n^*$ with $m_i S_i = R_i$ satisfying the conditions $(*)_j^i$ whenever $(1 + p^{j-i})S_i \neq S_i$. For $a \in \{0, 1, \ldots, \alpha - 1\}$ with $S_a \neq \emptyset$ let $\hat{a}$ be the least number in $\{1, \ldots, \alpha\}$ such that $S_a + p^{\hat{a}} = S_a$. (Equivalently, $\hat{a}$ can be defined such that $\mathsf{Stab}_+(S_a) = \langle p^{\hat{a}} \rangle$, cf. 3.7). In the case of $S_a = \emptyset$ we put $\hat{a} := a + 1$. By definition of $\hat{a}$ we have $S_a + p^{\hat{a}-1} \neq S_a$. The latter is equivalent to $(1 + p^{\hat{a}-1-a})S_a \neq S_a$ since, otherwise, we would have $S_a + \langle p^{\hat{a}-1} \rangle = S_a$, i.e. $p^{\hat{a}-1} \in \mathsf{Stab}_+(S_a)$ in contradiction to the definition of $\hat{a}$.
Consequently the conditions $3.6(*)_a^{\hat{a}-1}$ hold which can be rewritten (by multiplying with p^{t+1} both sides and the module, cf. 3.6) as follows:

$$\begin{aligned}
m_a p^{a+1} &\equiv m_{a+1} p^{a+1} \pmod{p^{\hat{a}}} \\
m_{a+1} p^{a+2} &\equiv m_{a+2} p^{a+2} \pmod{p^{\hat{a}}} \\
&\vdots \\
m_t p^{t+1} &\equiv m_{t+1} p^{t+1} \pmod{p^{\hat{a}}} \\
&\vdots \\
m_{\hat{a}-2} p^{\hat{a}-1} &\equiv m_{\hat{a}-1} p^{\hat{a}-1} \pmod{p^{\hat{a}}}
\end{aligned}$$

But this implies $m_a p^t \equiv m_t p^t \pmod{p^{\hat{a}}}$ for $a \le t < \hat{a}$; this, however, is just the sufficient condition $(^{\circ\circ})$ in 3.8 in case of $n = p^\alpha$ with

$\mu_i := m_i$. From the proof in 3.8 we conclude that $x \mapsto f_{\mathbf{m}}(x) = \sum_{i=0}^{\alpha-1} m_i x_i p^i$ is an isomorphism. $\square$

We now come to a crucial point of our approach. Instead of looking for a solving set for all circulant graphs altogether, we divide $\mathsf{Circ}(\mathbb{Z}_n)$ in a preprocessing step into several classes defined by the profile vectors. If two graphs belong to different classes then they are not isomorphic. If they do belong to the same class (i.e., if they have the same profile) then we can provide a solving set of a size that does not exceed the size $\varphi(n) = |\mathbb{Z}_n^*|$ which is not more than in the case that Ádám's conjecture holds.

We already discussed this appproach in Section 4 (in particular 4.6) classifying circulant graphs by their automorphism groups (more precisely by their Sylow p-subgroups). This was the motivation to investigate p-S-rings. We start with the description of solving sets for the automorphism group of p-S-rings since in this case we are able to indicate even a *minimal* solving set.

Let us fix an arbitrary p-S-ring $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ over $\mathbb{Z}_{p^\alpha}$, or, equivalently (see 5.5), a profile vector $\mathbf{k} = (k_0, k_1, \ldots, k_{\alpha-1})$.

Due to Theorem 6.3, a solving set for the group $\mathsf{Aut}(\mathcal{A})$ may be described by means of permutations $f_{\mathbf{m}}$ as defined in 6.1. However, we do not need all these permutations. Those that are needed for a solving set may be specified in more detail, because the structure of $\mathbf{m}$ is influenced by the profile vector $\mathbf{k}$.

6.4. The sets $M(\mathbf{k})$. Let $M(\mathbf{k})$ be the set of all multiplier sequences $\mathbf{m} = (m_0, \ldots, m_{\alpha-1})$ that satisfy the following two properties:

(P1) $\forall_{0\le i\le \alpha-1} \left(m_i \in \{0, ..., p^{k_i - i}\} \cap \mathbb{Z}_{p^\alpha}^*\right);$

(P2) $\forall_{0\le i\le j\le \alpha-1} \left(m_i p^j \equiv m_j p^j \pmod{p^{k_i}}\right).$

Then we have:

6.5. Theorem. *Let $\mathcal{A}$ be a p-S-ring over $\mathbb{Z}_{p^\alpha}$ with profile vector $\mathbf{k}$. Then $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ (cf. 6.1) is an $(\mathsf{Aut}(\mathcal{A}), \mathsf{Out}(\mathcal{A}))$-transversal and therefore a minimal solving set for $\mathsf{Aut}(\mathcal{A})$ (cf. 4.10).*

PROOF. Arguing as in the proof of Theorem 6.3 one can easily show that each permutation $f_{\mathbf{m}}$ ($\mathbf{m} \in M(\mathbf{k})$) is a combinatorial automorphism of the S-ring $\mathcal{A}$ defined by the profile vector $\mathbf{k}$ and that

$$(\Gamma_n(T))^{f_{\mathbf{m}}} = \Gamma_n(m_i T) \text{ for } T \in \mathsf{Basic}(\mathcal{A}),$$

where i is uniquely defined by $T \subset \langle p^i \rangle \setminus \langle p^{i+1} \rangle$. In other words, $f_{\mathbf{m}} \in \mathsf{Out}(\mathcal{A})$.

Let $\mathbf{m}, \mathbf{n} \in M(\mathbf{k})$ be two arbitrary multiplier sequences that induce the same algebraic automorphism of $\mathcal{A}$ (i.e., $f^*_{\mathbf{m}} = f^*_{\mathbf{n}}$, cf. 1.6). Then for each $0 \le i \le \alpha - 1$ it holds that

$$m_i(p^i + \langle p^{k_i} \rangle) = n_i(p^i + \langle p^{k_i} \rangle)$$

implying $m_i \equiv n_i \pmod{p^{k_i - i}}$, $0 \le i \le \alpha - 1$. Since $m_i, n_i \in \{0, ..., p^{k_i - i} - 1\}$, these congruences imply $\mathbf{m} = \mathbf{n}$. Therefore, $f_{\mathbf{m}}$ and $f_{\mathbf{n}}$ are in different $\mathsf{Aut}(\mathcal{A})$-cosets whenever $\mathbf{n} \neq \mathbf{m}$.

Now, take an arbitrary $f \in \mathsf{Out}(\mathcal{A})$. Then, by 1.7,

$$\forall_{T \in \mathsf{Basic}(\mathcal{A})} \ \left(\Gamma_n(T)^f = \Gamma_n(T^{f^*})\right)$$

where f^* is the algebraic isomorphism induced by f. By 2.9 there exist $m_0, ..., m_{\alpha-1} \in \mathbb{Z}^*_{p^\alpha}$ such that

$$T^{f^*} = m_i T \text{ for } T \in \mathsf{Basic}(\mathcal{A}) \text{ with } T \subset \langle p^i \rangle \setminus \langle p^{i+1} \rangle.$$

At first we show that the m_i's satisfy (P2). We shall do this by induction on $j - i$ (cf. 6.4). The case of $j - i = 0$ is trivial, so we shall start from $j - i = 1$ as the base of the induction. For an element X in the group ring $\mathbb{Z}\mathbb{Z}_n$ and $m \in \mathbb{Z}$ let $m \bullet X$ be the m-fold sum $X + \cdots + X$ (where $+$ stands for the addition in the group ring), recall that for λX the λ just denotes the coefficient (cf. 1.1) while mT is meant as in Table 1 (cf. 3.1). For the basic set $T = p^i + \langle p^{k_i} \rangle$ of $\mathcal{A}$ we have

$$(p \bullet \underline{T})^{f^*} = p \bullet (\underline{T}^{f^*}).$$

By direct calculations one obtains $p \bullet \underline{T} = (p^{(\alpha - k_i)(p-1)})\underline{S}$ where $S = p^{i+1} + \langle p^{k_i} \rangle$. Thus,

$$(p \bullet \underline{T})^{f^*} = p^{(\alpha - k_i)(p-1)} \underline{S}^{f^*} = p^{(\alpha - k_i)(p-1)} (\underline{m_{i+1} p^{i+1} + \langle p^{k_i} \rangle}).$$

On the other hand,

$$p \bullet (\underline{T}^{f^*}) = p \bullet (\underline{m_i T}) = p^{(\alpha-k_i)(p-1)}(\underline{m_i p^{i+1} + \langle p^{k_i}\rangle}).$$

Therefore $m_{i+1}p^{i+1} \equiv m_i p^{i+1} \pmod{p^{k_i}}$, *i.e.*, P2 is proved for $j = i+1$.

Let now $i+1 < j$. Then $m_{j-1}p^j \equiv m_j p^j \pmod{p^{k_{j-1}}}$ and $m_{j-1}p^{j-1} \equiv m_i p^{j-1} \pmod{p^{k_i}}$. Since $i < j-1$, $k_i \le k_{j-1}$ and we can write $m_{j-1}p^j \equiv m_j p^j \pmod{p^{k_i}}$. Together with

$$m_{j-1}p^{j-1} \equiv m_j p^{j-1} \pmod{p^{k_i}} \implies m_{j-1}p^j \equiv m_j p^j \pmod{p^{k_i}}$$

we obtain $m_i p^j \equiv m_j p^j \pmod{p^{k_i}}$, as desired.

Let $n_i \in \{0, ..., p^{k_i - i} - 1\}$ be the remainder of m_i modulo $p^{k_i - i}$. Then $n_i p^i \equiv m_i p^i \pmod{p^{k_i}}$, and, therefore, the congruence

$$n_i p^j \equiv n_j p^j \pmod{p^{k_i}}$$

holds for every $j \ge i$. Hence $f_{\mathbf{n}} \in \mathsf{Out}(\mathcal{A})$ and $\Gamma_n(T)^{f_{\mathbf{n}}} = \Gamma_n(n_i T)$ where i is determined by the inclusion $T \subset \langle p^i\rangle \setminus \langle p^{i+1}\rangle$. Since every basic set T with $T \subset \langle p^i\rangle \setminus \langle p^{i+1}\rangle$ is of the form $T = xp^i + \langle p^{k_i}\rangle, x \in \mathbb{Z}_{p^\alpha}^*$, we have $n_i T = m_i T$. Therefore $f_{\mathbf{n}}G = f_{\mathbf{m}}G = fG$ for $G = \mathsf{Aut}(\mathcal{A})$. □

According to 4.3, Theorem 6.5 provides a minimal solving set for every circulant graph $\Gamma_n(S)$ with automorphism group $\mathsf{Aut}(\mathcal{A})$, in other word, for which the generated S-ring $\langle\langle S\rangle\rangle$ is a p-S-ring. The next theorem shows that if $\langle\langle S\rangle\rangle$ is not a p-S-ring then we still are able to provide a "relatively small" solving set (which in general, however, is no longer minimal). It is even a solving set for the class of all circulant graphs with the same profile (cf. 5.5).

6.6. Theorem.

(i) *If two circulant graphs over $\mathbb{Z}_{p^\alpha}$ have different profiles then they are not isomorphic.*

(ii) *Let $\mathbf{k}$ be a profile vector. Then $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ is a solving set for the class of all circulant graphs over $\mathbb{Z}_{p^\alpha}$ with profile $\mathbf{k}$.*

PROOF. (i): It follows from 3.6 that isomorphic circulant graphs must have the same profile.
(ii): Let $\Gamma_{p^\alpha}(S)$ be a circulant graph with profile $\mathbf{k}$, and let $\Gamma_{p^\alpha}(T)$ be a circulant graph isomorphic to $\Gamma_{p^\alpha}(S)$. Then there exist $m_i \in \mathbb{Z}^*_{p^\alpha}$, $i = 0, ..., \alpha - 1$, which satisfy the conditions $(*)^j_i$ in 3.6. According to Theorem 3.6 and the proof of 6.3, the permutation $f_{\mathbf{m}}$ with $\mathbf{m} = (m_0, \dots, m_{\alpha-1})$ realizes an isomorphism between these two graphs. Moreover, the conditions in Theorem 3.6 show that $\mathbf{m} \in M(\mathbf{k})$ (cf. 6.4). $\square$

The size and a more explicite characterization of the above solving set $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ will be considered in the next section.

7 Enumeration of the permutations $f_{\mathbf{m}}$

Once we know (by Theorems 6.5 and 6.6) that the permutations $f_{\mathbf{m}}$ form solving sets and thus resolves the isomorphism problem for circulant graphs $\Gamma \in \mathsf{Circ}(\mathbb{Z}_{p^\alpha})$, there arises the problem to calculate these permutations, in particular to find the size of such solving sets. This problem we shall treat in this section by describing the multiplier sequences $\mathbf{m}$ via a corresponding matrix M.

7.1. The matrices in $\mathsf{Mat}(\mathbf{k})$. Let $\mathbf{k} = (k_0, k_1, \dots, k_{\alpha-1})$ be a fixed profile vector, i.e., according to 5.4, $\mathbf{k}$ satisfies

$$\begin{aligned} i < k_i \leq \alpha \ &(\text{for } i \in \{0, \dots, \alpha-1\}) \text{ and} \\ k_i \leq k_{i+1} \ &(\text{for } i \in \{0, \dots, \alpha-2\})\,. \end{aligned}$$

For $\mathbf{m} = (m_0, \dots, m_{\alpha-1}) \in M(\mathbf{k})$ we define M_{ij} by $m_i = \sum_{j=0}^{\alpha-1} M_{ij} p^j$ (cf. 3.7(2)). In particular we have $M_{ij} \in \{0, 1, \dots, p-1\}$ and $M_{s0} \neq 0$ for $s \in \{0, 1, \dots, \alpha-1\}$. Thus $\mathbf{m}$ is uniquely determined by the matrix $M = (M_{ij})_{i,j \in \{0,\dots,\alpha-1\}}$:

$$\mathbf{m} = \begin{pmatrix} m_0 \\ m_1 \\ \vdots \\ m_{\alpha-1} \end{pmatrix} = M \begin{pmatrix} 1 \\ p \\ \vdots \\ p^{\alpha-1} \end{pmatrix}$$

Let $\mathsf{Mat}(\mathbf{k})$ denote the set of all matrices obtained in this way. The conditions (P1) and (P2) characterizing $\mathbf{m} \in M(\mathbf{k})$ can be reformulated as follows: A matrix $M = (M_{ij})_{ij \in \{0,\dots,\alpha-1\}}$ belongs to $\mathsf{Mat}(\mathbf{k})$ if and only if it satisfies the following conditions:

(P1′) For all $s \in \{0, 1, \dots, \alpha-1\} : M_{s0} \neq 0 \wedge (\forall_{k_s - s \leq t \leq \alpha-1} M_{st} = 0)$.

(P2′) For all $i \in \{0, 1, \dots, \alpha-1\}, i \leq j \leq \alpha-1 : (\forall_{0 \leq t \leq k_i - j} M_{it} = M_{jt})$.

This gives the following construction procedure for the matrices in $\mathsf{Mat}(\mathbf{k})$: For each $t \in \{0, 1, \dots, \alpha - 1\}$ let $W_t := \{s \mid k_s - s > t\}$ and $U_t := \bigcup\{[s, k_s - 1 - t] \mid s \in W_t\}$. Then W_t and U_t are either empty or U_t can be represented as a disjoint union of closed intervals (built from the overlapping intervals $[s, k_s - 1 - t]$, cf. Example 7.2). Put $M_{st} = 0$ whenever $s \notin W_t$ (this ensures (P1′)). Further, for every of the disjoint intervals I in U_t a value $x \in \{0, 1, , \dots, p - 1\}$ can be chosen arbitrarily and assigned to every M_{it} for $i \in I$ (this ensures (P2′) since (P2′) can be reformulated demanding $M_{it} = M_{jt}$ whenever $s \leq i \leq j \leq k_s - 1 - t$ for some $s \in W_t$). Using an indeterminate x instead of a concrete value we get a generic matrix describing all possible $M \in \mathsf{Mat}(\mathbf{k})$. We shall demonstrate this in the following example.

7.2. Example. Let $\alpha = 6$ and consider the following profile vector $\mathbf{k} = (k_0, \dots, k_5) := (3, 4, 4, 5, 5, 6)$. Then we have:

$$
\begin{aligned}
&t = 0: \\
&W_0 = \{0,1,2,3,4,5\}, \quad U_0 = \overset{s=0}{[0,2]} \cup \overset{s=1}{[1,3]} \cup \overset{s=2}{[2,3]} \cup \overset{s=3}{[3,4]} \cup \overset{s=4}{[4,4]} \cup \overset{s=5}{[5,5]} \\
&\phantom{W_0 = \{0,1,2,3,4,5\}, \quad U_0} = [0,4] \cup [5,5]\ ; \\
&t = 1: \\
&W_1 = \{0,1,2,3\}, \qquad U_1 = [0,1] \cup [1,2] \cup [2,2] \cup [3,3] \\
&\phantom{W_1 = \{0,1,2,3\}, \qquad U_1} = [0,2] \cup [3,3]\ ; \\
&t = 2: \\
&W_2 = \{0,1\}, \qquad U_2 = [0,0] \cup [1,1]\ ; \\
&3 \leq t \leq 5: \\
&W_3 = W_4 = W_5 = \emptyset, \quad U_3 = U_4 = U_5 = \emptyset\,.
\end{aligned}
$$

The corresponding generic matrix for $\mathsf{Mat}(\mathbf{k})$ has the following form

$$(M_{st})_{s,t\in\{0,1,\dots,5\}} = \begin{array}{cc} \begin{matrix} t=0 & 1 & 2 & 3 & 4 & 5 \end{matrix} & \\ \begin{pmatrix} x & y & z & 0 & 0 & 0 \\ x & y & u & 0 & 0 & 0 \\ x & y & 0 & 0 & 0 & 0 \\ x & v & 0 & 0 & 0 & 0 \\ x & 0 & 0 & 0 & 0 & 0 \\ w & 0 & 0 & 0 & 0 & 0 \end{pmatrix} & \begin{matrix} s=0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{matrix} \end{array}$$

where $x, w \in \{1, ..., p-1\}$, while $y, z, u, v \in \{0, ..., p-1\}$. The cardinality of the solving set is therefore

$$|\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}| = |M(\mathbf{k})| = |\mathsf{Mat}(\mathbf{k})| = (p-1)^2 p^4 \,.$$

According to 7.1 the vectors $\mathbf{m} \in M(\mathbf{k})$ are of the form

$$\mathbf{m} = (x + yp + zp^2, x + yp + up^2, x + yp, x + vp, x, w)\,.$$

The corresponding permutations $f_{\mathbf{m}}$ (cf. 6.1) are given by

$$\begin{aligned} f_{\mathbf{m}}&(x_0 + x_1 p + x_2 p^2 + x_3 p^3 + x_4 p^4 + x_5 p^5) \\ &= (x + yp + zp^2)x_0 + (x + yp + up^2)x_1 p + (x + yp)x_2 p^2 \\ &\quad + (x + vp)x_3 p^3 + x x_4 p^4 + w x_5 p^5 \\ &= x x_0 + (y x_0 + x x_1)p + (z x_0 + u x_1 + x x_2)p^2 \\ &\quad + (u x_1 + y x_2 + x x_3)p^3 \\ &\quad + (v x_3 + x x_4)p^4 + w x_5 p^5 \pmod{p^6} \end{aligned} \tag{*}$$

(with x, w, y, z, u, v as above). Note that all arithmetic is done modulo p^6, i.e., the coefficients of p^i may contribute also to coefficients of higher poewers of p; however, the coefficients x_i are given as elements of $\{0, 1, \dots, p-1\}$, cf. 3.7.

By Theorem 6.5 the set of these $f_{\mathbf{m}}$ is a minimal solving set for the group $G = \mathsf{Aut}(\mathcal{A})$ where $\mathcal{A}$ is the p-S-ring over $\mathbb{Z}_{p^6}$ determined by the profile vector $\mathbf{k}$ (cf. 5.4). The following sets are basic sets of $\mathcal{A}$:

$$\begin{aligned}
T_{(0)} &= \{0\} \\
T_{(1)} &= 1 + \langle p^{k_0} \rangle &&= \{1 + \lambda p^3 \mid \lambda \in \mathbb{Z}_{p^3}\} \\
T_{(p)} &= p + \langle p^{k_1} \rangle &&= \{p + \lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\} \\
T_{(p^2)} &= p^2 + \langle p^{k_2} \rangle &&= \{p^2 + \lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\} \\
T_{(p^3)} &= p^3 + \langle p^{k_3} \rangle &&= \{p^3 + \lambda p^5 \mid \lambda \in \mathbb{Z}_{p}\} \\
T_{(p^4)} &= p^4 + \langle p^{k_4} \rangle &&= \{p^4 + \lambda p^5 \mid \lambda \in \mathbb{Z}_{p}\} \\
T_{(p^5)} &= p^5 + \langle p^{k_5} \rangle &&= \{p^5\}
\end{aligned}$$

All other basic sets of $\mathcal{A}$ can be obtained from these by multiplying with some $m \in \mathbb{Z}_{p^6}^*$, e.g., if $g = mp^i$ with $m \in \mathbb{Z}_{p^6}^*$ then $T_{(g)} = mT_{(p^i)}$ is the base set containing g.

Because of Theorem 4.3 the above set $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ of permutations is a minimal solving set for all circulant graphs $\Gamma_{p^\alpha}(S)$ with $\mathsf{Aut}(\Gamma) = \mathsf{Aut}(\mathcal{A})$.

The automorphism group G of $\mathcal{A}$ is the intersection of the automorphism groups of the Cayley graphs $\Gamma_{\mathbb{Z}_{p^6}}(T)$ for $T \in \mathsf{Basic}(\mathcal{A})$ (one can show that it suffices to take into account only the above mentioned basic sets $T_{(p^i)}$ $(i = 0, \ldots, 5)$ only). One can also show that the circulant graph with connection set $S := T_{(1)} \cup T_{(p)} \cup T_{(p^2)} \cup T_{(p^3)} \cup T_{(p^4)} \cup T_{(p^5)}$ has automorphism group G.

The structure of such automorphism groups is described in [Kli-P99] as (sub-)wreath products of cyclic groups and their cartesian powers but we shall not describe it here in detail (with the notations from [Kli-P99] we have $\mathsf{Aut}(\mathcal{A}) = \left[((\mathbb{Z}_p)^{p^3} \bullet \mathbb{Z}_p) \bullet \mathbb{Z}_{p^5}\right] \wr \mathbb{Z}_p)$.

Further, due to Theorem 6.6, the above set $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ of permutations is at the same time a solving set (not necessarily minimal) for all graphs with profile $\mathbf{k}$.

For instance, take the graph $\Gamma_{\mathbb{Z}_{p^6}}(S)$ from Example 5.6 with $p = 3$ and $S := T_{(1)} \cup T_{(p)} \cup T_{(p^3)}$. As shown in 5.6 its profile is $\mathbf{k} = (3, 4, 4, 5, 5, 6)$.

The circulant graphs $\Gamma_{\mathbb{Z}_{p^6}}(S')$ and $\Gamma_{\mathbb{Z}_{p^6}}(S'')$ with $S' := T_{(1)} \cup T_{(2p)} \cup T_{(p^3)} = \{1+\lambda p^3 \mid \lambda \in \mathbb{Z}_{p^3}\} \cup \{2p+\lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\} \cup \{p^3+\lambda p^5 \mid \lambda \in \mathbb{Z}_p\}$

and $S'' := T_{(1)} \cup T_{(2p)} \cup T_{(p^3)} = \{1 + \lambda p^3 \mid \lambda \in \mathbb{Z}_{p^3}\} \cup \{p + \lambda p^4 \mid \lambda \in \mathbb{Z}_{p^2}\} \cup \{4p^3 + \lambda p^5 \mid \lambda \in \mathbb{Z}_p\}$ obviously have the same profile (since $\mathsf{Stab}_+(S_i) = \mathsf{Stab}_+(S_i') = \mathsf{Stab}_+(S_i''))$.

$\Gamma_{\mathbb{Z}_{p^6}}(S')$ is not isomorphic to $\Gamma_{\mathbb{Z}_{p^6}}(S)$ as it can be checked directly with 3.6 ($m_0 \equiv m_1 \bmod p$ contradicts $S_0' = S_0$ and $S_1' = 2 \cdot S_1$).

But $\Gamma_{\mathbb{Z}_{p^6}}(S'')$ is isomorphic to $\Gamma_{\mathbb{Z}_{p^6}}(S)$ (take $m_0 = m_1 = 1$ and $m_3 = 1 + p = 4$ in 3.6). Consequently, there also exists $f_{\mathbf{m}}$ with $\Gamma(S)^{f_{\mathbf{m}}} = \Gamma(S'')$, namely $f_{\mathbf{m}}$ with $\mathbf{m} = (1, 1, 1, 4, 1, 1)$.

The solving set $\{f_{\mathbf{m}} \mid \mathbf{m} \in M(\mathbf{k})\}$ contains $(p-1)^2 p^4 = 324$ permutations. It is not a minimal solving set for $\Gamma(S)$. But note that even if Ádám's conjecture would hold one would have to check $|\mathbb{Z}_{p^6}^*| = \varphi(3^6) = 486$ cases.

Acknowledgements

Our thanks are due to Mikhail Klin for encouraging the authors to write this paper and for helpful discussions and hints. We gratefully acknowledge partial support by the Grant No. I-0333-263.06/93 from the G.I.F., the German-Israeli Foundation for Scientific Research and Development.

References

[Ada69] A. Ádám. Research problem 2-10. *J. Combin. Theory 2(1967), p.393.*

[Als-P79] B. Alspach, T.D. Parsons. Isomorphism of circulant graphs and digraphs. *Discrete Math. 25 (1979), pp.97-108.*

[Bab77] L. Babai. Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar., 29 (1977), pp. 329-336.*

[Bab-F78] L. Babai and P. Frankl. Isomorphism of Cayley graphs I, in *Colloq. Math. Soc. J. Bolyai, 18. Combinatorics, Keszthelv, 1976, North - Holland, Amsterdam, 1978, pp. 35-52.*

[Bab-F79] L. Babai and P. Frankl. Isomorphism of Cayley graphs II. *Acta Math. Acad. Sci. Hungar., 34 (1979), pp. 177-183.*

[Bay31] S. Bays. Sur les systemes cycliques de triples de Steiner differents pour N premier (on puissance de nombre premier) de la forme $6n+1$, II-III.*Comment. Math. Helv., 3 (1931), pp. 22-41.*

[Bra85] N. Brand. Some combinatorial isomorphism theorems. *Congressus Numer., 50 (1985), pp. 155-163.*

[Bra89] N. Brand. Isomorphisms of cyclic combinatorial objects. *Disc. Math., 78 (1989),pp. 1-2.*

[Bra91] N. Brand. Polynomial isomorphisms of combinatorial object. *Graphs and Comb., v. 7 (1991), pp. 7-14.*

[Djo70] D.Ź. Djoković. Isomorphism problem for a special class of graphs. *Acta Math. Acad. Sci. Hung. 21(1970), pp. 267-270.*

[Els-T70] B. Elspas, J. Turner. Graphs with circulant adjacency matrices. *J. Combin. Theory 9(1970), pp. 297-307.*

[Far-K-M94] I.A.Faradžev, M.H. Klin and M.E. Muzychuk. Cellular rings and automorphism groups of graphs In: Investigations on Algebraic Theory of Combinatorial Objects. Mathematics and Its Applications (Soviet Series), v. 84, I.A. Faradžev, A.A.Ivanov, M.H.Klin, A.J.Woldar(Eds), Kluwer Acad. Publ., 1994.

[Gol-N-P85] J.J. Gol'fand, N.L. Najmark, R. Pöschel, The structure of S-rings over $\mathbb{Z}_{2^m}$. *Techn. Report P-MATH-01/85, Akad. der Wiss. der DDR, Inst. f. Math., Berlin, 1980.*

[Gor72] D. Gorenstein. Finite Simple Groups. Plenum Press. New York, 1972.

[Hig70] D.G. Higman. Coherent configurations, I. *Rend. Sem. Mat. Univ. Padova,* **44***(1970), 1-25.*

[Hig87] D.G. Higman. Coherent algebras. *Linear algebra and its applications, v.93, 1987, pp. 209-239.*

[Huf-J-P93] W.G. Huffman, A. Job and V. Pless. Multipliers and generalized multipliers of cyclic objects and cyclic codes. *J. of Comb. Th. (A), 62, No. 2 (1993), pp. 183-215.*

[Huf96] W.C. Huffman. The equivalence of two cyclic objects on pq elements. *Discrete Math., 154 (1996) 103-127.*

[Kal-K72] L.A. Kalužnin and M.H. Klin. On some maximal subgroups of symmetric and alternating groups. *Mat. Sbornik., 87 (1972), pp. 91-121 (in Russian).*

[Kal-P82] L.A. Kalužnin and R. Pöschel. Zur Darstellung und Behandlung Algebraisch-Kombinatorischer Objecte. *EIK, 22 (1986), pp. 5-24.*

[Kal-S-U82] L.A. Kalužnin, V.I. Sushchanskii and V.A. Ustimenko. Application of computers in permutation group theory and its applications. *Kibernetika, 1982, No 6, pp. 83-94 (in Russian).*

[Kli-P80] M.Ch. Klin and R. Pöschel. The isomorphism problem for circulant graphs and digraphs with p^n vertices. *Techn. Report P-34/80, Akad. der Wiss. der DDR, ZIMM, Berlin, 1980.*

[Kli-P99] M. Klin, R. Pöschel, Automorphism groups of circulant graphs on p^m vertices, p an odd prime. Manuscript (Techn. Report to appear 1999)

[Kli-P81] 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; pp. 405-434.

[Lam31] P. Lambossy. Sur une maniere de differedcier les functions cycliques d'un form donnee.*Commen. Math. Helv., 3 (1931), pp. 69-102.*

[Muz95a] M. Muzychuk. On the structure of basic sets of Schur rings over cyclic groups. *Journal of Algebra, v.169, 2, 1994, pp. 655-678.*

[Muz95b] M. Muzychuk. Ádám's conjecture is true in the square-free case. *J. of Combin. Th. (A), 72, No. 1 (1995), pp. 118-134.*

[Muz96] M. Muzychuk. On the number of cyclic combinatorial objects isomorphic to a given one. Preprint MATH-AL-16-1996, Technische Universität Dresden 1996.

[Muz97] M. Muzychuk. On Ádám's conjecture for circulant graphs. *Discrete Math. v. 176 (1997), pp. 285-298.*

[MuzXX] M. Muzychuk. On the isomorphism problem for cyclic combinatorial objects. To appear in Disc. Math.

[Pal87] P.P. Pálfy. Isomorphism problem for relational structures with a cyclic automorphism. *Europ. J. Combinatorics, 8 (1987), pp. 35-43.*

[Pon] I. Ponomarenko. Private communication.

[Pös74] R. Pöschel, Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen. *Math. Nachr.,* **60** *(1974), 1-27.*

[Toi77] S. Toida. A note on Ádám's conjecture. *J.Combin. Theory (B), 23(1977), pp. 239-246.*

[Wei74] B. Weisfeiler. On construction and identification of graphs. LNM v. 558, 1974.

[Wie64] H. Wielandt. Finite Permutation Groups. *Academic Press, 1964, Berlin.*

[Wie69] H. Wielandt. Permutation groups through invariant relations and invariant functions. Ohio State University 1969.

[Zie97] P.-H. Zieschang. An algebraic approach to association schemes. LNM, 1628, 1997

Authors' addresses:

Mikhail Muzychuk
Department of Mathematics
& Computer Science,
Bar Ilan University
52900 Ramat Gan,
Israel
e-mail: `muzychuk@bimacs.cs.biu.ac.il`

Reinhard Pöschel
Institut für Algebra
Technische Universität Dresden
D – 01062 Dresden
Germany
e-mail: `poeschel@math.tu-dresden.de`