Automorphism groups of rational circulant graphs

Mikhail Klin

Department of Mathematics, Ben-Gurion University of the Negev
84105 Beer Sheva, Israel

klin@cs.bgu.ac.il

István Kovács*

University of Primorska, UP IAM and UP FAMNIT
Muzejski trg 2, SI6000 Koper, Slovenia

istvan.kovacs@upr.si

Submitted: Apr 29, 2011; Accepted: Jan 23, 2012; Published: Feb 7, 2012
Mathemaical Subject Classifications: 05E18, 05E30, 20B25.

Abstract

The paper concerns the automorphism groups of Cayley graphs over cyclic groups which have a rational spectrum (rational circulant graphs for short). With the aid of the techniques of Schur rings it is shown that the problem is equivalent to consider the automorphism groups of orthogonal group block structures of cyclic groups. Using this observation, the required groups are expressed in terms of generalized wreath products of symmetric groups.

1 Introduction

A circulant graph with n vertices is a Cayley graph over the cyclic group $\mathbb{Z}_n$, i.e., a graph having an automorphism which permutes all the vertices into a full cycle. There is a vast literature investigating various properties of this class of graphs. In this paper we focus on their automorphisms. By the definition, the automorphism groups contain a regular cyclic subgroup. The study of permutation groups with a regular cyclic subgroup goes back to the work of Burnside and Schur. Schur proved that if the group is primitive of composite degree, then it is doubly transitive (see [109]). The complete list of such primitive groups was given recently by the use of the classification of finite simple groups, see [54, 83].

One might expect transparent descriptions of the automorphism groups of circulant graphs by restricting to a suitably chosen family. A natural restriction can be done with

*Supported in part by ARRS – Agencija za raziskovanje Republike Slovenije, program no. P1-0285.

respect to the order n of the graph. For instance, we refer to the papers [32, 68, 76] dealing with the case when n is a square-free number, $n = p^e$ (p is an odd prime), and $n = 2^e$, respectively. In the present paper we choose another natural family by requiring the graphs to have a rational spectrum, i.e., the family of rational circulant graphs.

To formulate our main result some notation is in order. For $n \in \mathbb{N}$, we let $[n]$ denote the set $\{1, \ldots, n\}$, and S_n the group of all permutations of $[n]$. Let $([r], \preceq)$ be a poset on $[r]$. We say that $([r], \preceq)$ is *increasing* if $i \preceq j$ implies $i \leq j$ for all $i, j \in [r]$. Below $\prod_{([r],\preceq)} S_{n_i}$ denotes the generalized wreath product, defined by $([r], \preceq)$ and the groups $S_{n_1}, \ldots, S_{n_r}$, acting on the set $[n_1] \times \cdots \times [n_r]$. For the precise formulation, see Definition 9.3.

Our main result is the following theorem.

Theorem 1.1. *Let G be a permutation group acting on the cyclic group $\mathbb{Z}_n$, $n \geq 2$. The following are equivalent:*

(i) $G = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, Q))$ *for some rational circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, Q)$.

(ii) G is a permutation group, which is permutation isomorphic to a generalized wreath product $\prod_{([r],\preceq)} S_{n_i}$, where $([r], \preceq)$ is an increasing poset, and $n_1, \ldots, n_r$ are in $\mathbb{N}$ satisfying

(a) $n = n_1 \cdots n_r$,

(b) $n_i \geq 2$ *for all* $i \in \{1, \ldots, r\}$,

(c) $(n_i, n_j) = 1$ *for all* $i, j \in \{1, \ldots, r\}$ *with* $i \not\preceq j$.

To the number n_i in (ii) we shall also refer to as the *weight* of node i in the poset $([r], \preceq)$. The following examples serve as illustrations of Theorem 1.1.

Example 1.2. Here $n = 6$. Up to complement, there are four rational circulant graphs:

$$K_6,\ K_2 \times K_3,\ K_{3,3},\ K_{2,2,2}.$$

The corresponding automorphism groups: $S_6, S_2 \times S_3, S_2 \wr S_3$, and $S_3 \wr S_2$.

In part (ii) we get $G = S_6$ for $r = 1$. If $r = 2$, then any choice $n_1, n_2 \in \{2, 3\}$ with $n_1 n_2 = 6$ gives weights of an increasing poset on $\{1, 2\}$. For instance, if $n_1 = 2$, $n_2 = 3$, and $([2], \preceq)$ is an anti-chain, then $G = S_2 \times S_3$, and the same group is obtained if we switch the values of weights. Changing the poset $([2], \preceq)$ to a chain we get the wreath products $S_2 \wr S_3$ and $S_3 \wr S_2$. ∎

Example 1.3. Here $n = 12$. In this example we consider the groups that can be derived from part (ii). We have $G = S_{12}$ if $r = 1$. If $r = 2$, then similarly to the previous example we deduce that G is one of the groups: $S_3 \times S_4$, $S_a \wr S_{n/a}$, $a \in \{2, 3, 4, 6\}$.

Let $r = 3$. The three nodes of $([3], \preceq)$ get weights $2, 2, 3$ by (a)-(b), and because of (c) the two nodes with weight 2 must be related. The possible increasing posets are depicted in Figure 1.

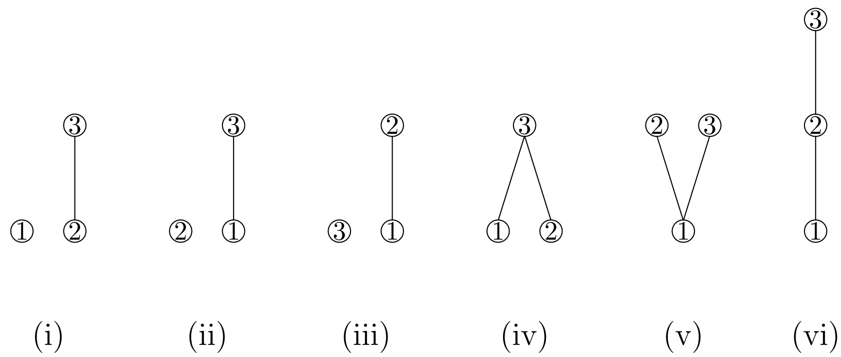

Figure 1: Increasing posets on $\{1, 2, 3\}$.

The weights are unique for posets (i)-(iii). In poset (iv) the only restriction is that $n_3 = 2$, in poset (v) the only restriction is that $n_1 = 2$, and weights are arbitrarily distributed for poset (vi). By Definition 9.3, we obtain the following groups:

- $S_3 \times (S_2 \wr S_2)$ corresponding to posets (i)-(iii),
- $S_2 \wr (S_2 \times S_3)$ corresponding to poset (iv),
- $(S_2 \times S_3) \wr S_2$ corresponding to poset (v),
- $S_3 \wr S_2 \wr S_2$, $S_2 \wr S_3 \wr S_2$ and $S_2 \wr S_2 \wr S_3$ corresponding to poset (vi) (here the group depends also on the weights).

Finally, altogether we obtain exactly 12 possible distinct groups (including the largest S_{12} and the smallest of order 48). Each such group appears exactly ones. (Attribution of the same group of order 48 to three posets is an artifice, which results from the way of the presentation.) Observe that, each of these groups is obtained using iteratively direct or wreath product of symmetric groups. ∎

For larger values of n it is not true that generalized wreath product of symmetric groups may be obtained by an iterative use of direct and wreath products of symmetric groups. An example of such a situation appears for $n = 36$, and it will be discussed later on in the text.

In deriving Theorem 1.1 we follow an approach suggested by Klin and Pöshcel in [67], which is to explore the Galois correspondence between overgroups of the right regular representation $(\mathbb{Z}_n)_R$ in $\mathrm{Sym}(\mathbb{Z}_n)$, and Schur rings (S-rings for short) over $\mathbb{Z}_n$. It turns out that each circulant graph Γ generates a suitable S-ring $\mathcal{A}$, such that $\mathrm{Aut}(\Gamma)$ coincides with $\mathrm{Aut}(\mathcal{A})$. If in addition Γ is a rational circulant graph, then the corresponding S-ring $\mathcal{A}$ is also rational.

Rational S-rings over cyclic groups were classified by Muzychuk in [88]. Therefore, in principle, knowledge of [88] is enough in order to deduce our main results. Nevertheless, it is helpful and natural to interpret groups of rational circulant graphs as the automorphism groups of orthogonal group block structures on $\mathbb{Z}_n$. This implies interest to results of Bailey et al. about such groups (see [6, 13, 9]). Consideration of orthogonal group block structures as well as of crested products (see [12]) makes it possible to describe generalized wreath products as formulas over the alphabet with words "crested", "direct", "wreath", and "symmetric group". Finally, the reader will be hopefully convinced that the simultaneous use of a few relatively independent languages, like S-rings, lattices, association schemes, posets, orthogonal block structures in conjunction with suitable group theoretical concepts leads naturally to the understanding of the entire picture as well as to a rigorous proof of the main results.

The rest of the paper is organized as follows. Section 3 serves as a brief introduction to S-rings, while in sections 4 and 5 we pay attention to the particular case of rational S-rings over $\mathbb{Z}_n$. We conclude these sections by crucial Corollary 5.4, which reduces the problem to the consideration of the automorphism groups of rational S-rings over $\mathbb{Z}_n$. In Section 6 an equivalent language of block structures on $\mathbb{Z}_n$ is introduced. Section 7 provides the reader an opportunity to comprehend all main ideas on a level of simple examples. In Section 8 crested products are introduced and it is shown that their use is, in principle, enough for the recursive description of all required groups. In Section 9 poset block structures are linked with generalized wreath products, while Section 10 provides a relatively self-contained detailed proof of the main Theorem 1.1.

A number of interesting by-product results, which follow almost immediately from the consideration are presented in Section 11. Finally, in Section 12 we enter to a discussion of diverse historical links between all introduced languages and techniques, though not aiming to give a comprehensive picture of all details.

2 Preliminaries

In this section we collect all basic definitions and facts needed in this paper.

2.1 Permutation groups

The group of all permutations of a set X is denoted by $\mathrm{Sym}(X)$. We let $g \in \mathrm{Sym}(X)$ act on the right, i.e., x^g is written for the image of x under action of g, and further we have $x^{g_1 g_2} = (x^{g_1})^{g_2}$. For a group K, let K_R denote the *right regular representation* of K acting on itself, i.e., $x^k = xk$ for all $x, k \in K$. Two permutation groups $K_1 \leq \mathrm{Sym}(X_1)$ and $K_2 \leq \mathrm{Sym}(X_2)$ are *permutation isomorphic* if there is a bijection $f\colon X_1 \to X_2$, and an isomorphism $\varphi : K_1 \to K_2$ such that, $f(x_1^{k_1}) = f(x_1)^{\varphi(k_1)}$ for all $x_1 \in X_1$, $k_1 \in K_1$.

Two operations over permutations groups will play a basic role in the sequel. The *permutation direct product* $K_1 \times K_2$ of groups $K_i \leq \mathrm{Sym}(X_i)$, $i = 1, 2$, is the permutation representation of $K_1 \times K_2$ on $X_1 \times X_2$ acting as:

$$(x_1, x_2)^{(k_1,k_2)} = (x_1^{k_1}, x_2^{k_2}),\ (x_1, x_2) \in X_1 \times X_2,\ (k_1, k_2) \in K_1 \times K_2.$$

Note that the direct product is commutative and associative.

Let $A \leq \mathrm{Sym}(X_1)$ and $C \leq \mathrm{Sym}(X_2)$ be two permutation groups. The *wreath product* $A \wr C$ is the subgroup of $\mathrm{Sym}(X_1 \times X_2)$ generated by the following two groups: the *top group* T, which is a faithful permutation representation of A on $X_1 \times X_2$, acting as:

$$(x_1, x_2)^a = (x_1^a, x_2) \text{ for } (x_1, x_2) \in X_1 \times X_2,\ a \in A,$$

and the *base group* B, which is the representation of the group C^{X_1} on $X_1 \times X_2$, acting as:

$$(x_1, x_2)^f = (x_1, x_2^{f(x_1)}),\ (x_1, x_2) \in X_1 \times X_2,\ f \in C^{X_1},$$

where $f(x_1)$ is the component (belonging to C) of f, corresponding to $x_1 \in X_1$. (Here C^{X_1} denotes the group of all functions from X_1 to C, with group operation $(fg)(x_1) = f(x_1) \cdot g(x_1)$ for $x_1 \in X,\ f, g \in C^{X_1}$.) The group T normalizes B, $|B \cap T| = 1$, therefore $\langle B, T\rangle = B \rtimes T$. Clearly, the group $A \wr C$ has order $|A \wr C| = |T| \cdot |B| = |A| \cdot |C|^{|X_1|}$. Each element $w \in A \wr C$ admits a unique decomposition $w = tb$, where $t \in T$ and $b \in B$. Also element w may be denoted as $w = [a, f(x_1)]$, called the *table form* of w (note that here x_1 is a symbol for a variable). By definition, $(x_1, x_2)^w = (x_1^a, x_2^{f(x_1)})$. Note that, sometimes in wreath product $A \wr C$ the group A is called *active*, while C *passive* groups. The wreath product is associative, but not commutative. We remark that our notation for wreath product follows, e.g., [40], and it has opposite direction in comparison with traditions accepted in modern group theory.

A permutation group $K \leq \mathrm{Sym}(X)$ acts canonically on $X \times X$ by letting $(x_1, x_2)^k = (x_1^k, x_2^k)$. The corresponding orbits are called the *2-orbits* of K, the set of which we denote by 2-Orb(K). The 2-*closure* $K^{(2)}$ of K is the unique maximal subgroup of $\mathrm{Sym}(X)$ that has the same 2-orbits as K. Clearly, $K \leq K^{(2)}$, and we say that K is 2-*closed* if $K^{(2)} = K$.

2.2 Cayley graphs and circulant graphs

By a *(directed) graph* we mean a pair $\Gamma = (X, R)$, where X is a nonempty set, and R is a binary relation on X. In the particular case when $(x, y) \in R$ if and only if $(y, x) \in R$ for all $(x, y) \in X \times X$, Γ is also called an *undirected graph*, and then $\{x, y\}$ is said to be an (undirected) edge of Γ, which substitutes $\{(x, y), (y, x)\}$. The *automorphism group* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}((X, R))$ is the group of all permutations g in $\mathrm{Sym}(X)$ that preserve R, i.e., $(x^g, y^g) \in R$ if and only if $(x, y) \in R$ for all $x, y \in X$.

The *adjacency matrix* $A(\Gamma)$ of the graph $\Gamma = (X, R)$ is the X-by-X complex matrix defined by

$$A(\Gamma)_{x,y} = \begin{cases} 1 & \text{if } (x, y) \in R \\ 0 & \text{otherwise.} \end{cases}$$

The *eigenvalues* of Γ are defined to be the eigenvalues of $A(\Gamma)$, and Γ is called *rational* if all its eigenvalues are rational. Note that, since the characteristic polynomial of $A(\Gamma)$ has integer coefficients and leading coefficient ± 1, if its eigenvalues are rational numbers, then these are in fact integers.

For a subset $Q \subseteq K$, the *Cayley graph* $\mathrm{Cay}(K, Q)$ over K with *connection set* Q is the graph (X, R) defined by

$$X = K, \text{ and } R = \{(x, qx) \mid x \in K, q \in Q\}.$$

Two immediate observations: the graph $\mathrm{Cay}(K, Q)$ is undirected if and only if $Q = Q^{-1} = \{q^{-1} \mid q \in Q\}$; and the right regular representation K_R is a group of automorphisms of $\mathrm{Cay}(K, Q)$. Cayley graphs over cyclic groups are briefly called *circulant graphs*.

2.3 Schur rings

Let H be a group written with multiplicative notation and with identity e. Denote $\mathbb{Q}H$ the group algebra of H over the field $\mathbb{Q}$ of rational numbers. The group algebra $\mathbb{Q}H$ consists of the formal sums $\sum_{x \in H} a_x x$, $a_x \in \mathbb{Q}$, equipped with entry-wise addition $\sum_{x \in H} a_x x + \sum_{x \in H} b_x x = \sum_{x \in H} (a_x + b_x) x$, and multiplication

$$\sum_{x \in H} a_x x \cdot \sum_{x \in H} b_x x = \sum_{x, y \in H} (a_y b_{y^{-1}x}) x.$$

Given $\mathbb{Q}H$-elements $\eta_1, \ldots, \eta_r$, the subspace generated by them is denoted by $\langle \eta_1, \ldots, \eta_r \rangle$. For a subset $Q \subseteq H$ the *simple quantity* $\underline{Q}$ is the $\mathbb{Q}H$-element $\sum_{x \in H} a_x x$ with $a_x = 1$ if $x \in Q$, and $a_x = 0$ otherwise (see [123]). We shall also write $\underline{q_1, \ldots, q_k}$ for the simple quantity $\underline{\{q_1, \ldots, q_k\}}$. The *transposed* of $\eta = \sum_{x \in H} a_x x$ is defined as $\eta^\top = \sum_{x \in H} a_x x^{-1}$.

A subalgebra $\mathcal{A}$ of $\mathbb{Q}H$ is called a *Schur ring* (for short *S-ring*) of *rank* r over H if the following axioms hold:

(SR1) $\mathcal{A}$ (as a vector space) has a linear basis of simple quantities: $\mathcal{A} = \langle \underline{T_1}, \ldots, \underline{T_r} \rangle$, $T_i \subseteq H$ for all $i \in \{1, \ldots, r\}$.

(SR2) $T_1 = \{e\}$, and $\sum_{i=1}^{r} \underline{T_i} = \underline{H}$.

(SR3) For every $i \in \{1, \ldots, r\}$ there exists $j \in \{1, \ldots, r\}$ such that $\underline{T_i}^\top = \underline{T_j}$.

The simple quantities $\underline{T_1}, \ldots, \underline{T_r}$ are called the *basic quantities* of $\mathcal{A}$, the corresponding sets $T_1, \ldots, T_r$ the *basic sets* of $\mathcal{A}$. We set the notation $\mathsf{Basic}(\mathcal{A}) = \{T_1, \ldots, T_r\}$.

2.4 Posets and partitions

A *partially ordered set* (for short a *poset*) is a pair $(X, \preceq)$, where X is a nonempty set, and $\preceq$ is a relation on X which is reflexive, antisymmetric and transitive. We write $x \prec y$ if $x \preceq y$ but $x \neq y$. For a subset $L \subseteq X$ we say an element $m \in L$ is *maximal* in L if $m \preceq l$ implies $l = m$ for all $l \in L$. Similarly, $m \in L$ is *minimal* in L if $l \preceq m$ implies $l = m$ for all $l \in L$. Further, we say that $i \in X$ is the *infimum* of L if $i \preceq l$ for all $l \in L$, and if for some $i' \in X$ we have $i' \preceq l$ for all $l \in L$, then $i' \preceq i$. Similarly, we say that $s \in X$ is the *supremum* of L if $l \preceq s$ for all $l \in L$, and if for some $s' \in X$ we have $l \preceq s'$ for all

$l \in L$, then $s \preceq s'$. We set the notations: $i = \bigwedge L$ and $s = \bigvee L$. The infimum (supremum, respectively) does not always exist, but if this is the case, it is determined uniquely.

The poset $(X, \preceq)$ is called a *lattice* if each pair of elements in X has infimum and supremum. Then we have binary operations $x \wedge y = \wedge\{x, y\}$ and $x \vee y = \vee\{x, y\}$. The lattice $(X, \preceq)$ is *distributive* if for all x, y, z in X,

$$\begin{aligned} x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z), \\ x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z). \end{aligned}$$

If $(X, \preceq)$ is a lattice, and a subset $X' \subset X$ is closed under both $\wedge$ and $\vee$, then $(X', \preceq)$ is also a lattice, it is called a *sublattice* of $(X, \preceq)$.

Let F be a partition of a set X. We denote by R_F the equivalence relation corresponding to F, and by $A(F)$ the adjacency matrix $A(R_F)$. We say that two partitions E and F of X are *orthogonal* if for their adjacency matrices $A(E)A(F) = A(F)A(E)$ (see [10, Section 6.2] for a nice discussion of this concept). The set of all partitions of X is partially ordered by the relation $\sqsubseteq$, where $E \sqsubseteq F$ (E is a *refinement* of F) if any class of E is contained in a class of F. The resulting poset is a lattice, where $E \wedge F$ is the partition whose classes are the intersection of E-classes with F-classes; and $E \vee F$ is the partition whose classes are the minimal subsets being union of E-classes and F-classes. The smallest element in this lattice is the *equality partition* E_X, the classes of which are the singletons; the largest is the *universal partition* U_X consisting of only the whole set X.

3 More about S-rings

Let H be a finite group written with multiplicative notation and with identity e. The *Schur-Hadamard product* $\circ$ on the group algebra $\mathbb{Q}H$ is defined by

$$\sum_{x \in H} a_x\, x \circ \sum_{x \in H} b_x\, x := \sum_{x \in H} a_x b_x\, x.$$

The following alternative characterization of S-rings over H is a folklore (cf. [96, Theorem 3.1]): a subalgebra $\mathcal{A}$ of $\mathbb{Q}H$ is an S-ring if and only if $\underline{e}, \underline{H} \in \mathcal{A}$, and $\mathcal{A}$ is closed with respect to $\circ$ and $^\top$. By this it is easy to see that the intersection of two S-rings is also an S-ring, in particular, given a subset $\mathcal{A}'$ of $\mathbb{Q}H$, denote by $\langle\langle \mathcal{A}' \rangle\rangle$ the S-ring defined as the intersection of all S-rings $\mathcal{A}$ that $\mathcal{A}' \subseteq \mathcal{A}$. For $Q \subseteq H$ we shall also write $\langle\langle Q \rangle\rangle$ instead of $\langle\langle \underline{Q} \rangle\rangle$, calling $\langle\langle Q \rangle\rangle$ the S-ring *generated* by Q. For two S-rings $\mathcal{A}$ and $\mathcal{B}$ over H, we say that $\mathcal{B}$ is an *S-subring* of $\mathcal{A}$ if $\mathcal{B} \subseteq \mathcal{A}$. It can be seen that this happens exactly when every basic set of $\mathcal{B}$ is written as the union of some basic sets of $\mathcal{A}$.

Let $\mathcal{A}$ be an S-ring over H. A subset $Q \subseteq H$ (subgroup $K \leq H$, respectively) is an $\mathcal{A}$*-subset* ($\mathcal{A}$*-subgroup*, respectively) if $\underline{Q} \in \mathcal{A}$ ($\underline{K} \in \mathcal{A}$, respectively). If $Q \subseteq H$ is an $\mathcal{A}$-subset, then $\langle Q \rangle$ is an $\mathcal{A}$-subgroup (see [123, Proposition 23.6]). By definition, the trivial subgroups $\{e\}$ and H are $\mathcal{A}$-subgroups, and for two $\mathcal{A}$-subgroups E and F, also

$E \cap F$ and $\langle E, F\rangle$ are $\mathcal{A}$-subgroups. In other words, the $\mathcal{A}$-subgroups form a sublattice of the subgroup lattice of H. Let K be an $\mathcal{A}$-subgroup. Define $\mathcal{A}_K = \mathcal{A} \cap \mathbb{Q}K$. It is easy to check that $\mathcal{A}_K$ is an S-ring over K and

$$\mathsf{Basic}(\mathcal{A}_K) = \{T \in \mathsf{Basic}(\mathcal{A}) \mid T \subseteq K\}.$$

We shall call $\mathcal{A}_K$ an *induced S-subring* of $\mathcal{A}$.

Following [67], by an *automorphism* of an S-ring $\mathcal{A} = \langle \underline{T}_1, \ldots, \underline{T}_r\rangle$ over H we mean a permutation $f \in \mathrm{Sym}(H)$ which is an automorphism of all *basic graphs* $\mathrm{Cay}(H, T_i)$. Thus the automorphism group of $\mathcal{A}$ is

$$\mathrm{Aut}(\mathcal{A}) = \bigcap_{i=1}^{r} \mathrm{Aut}(\mathrm{Cay}(H, T_i)).$$

The simplest examples of an S-ring are the whole group algebra $\mathbb{Q}H$, and the subspace $\langle \underline{e}, \underline{H \setminus \{e\}}\rangle$. The latter is called the *trivial S-ring* over H. Further examples are provided by permutation groups G which are overgroups of H_R in $\mathrm{Sym}(H)$ (i.e., $H_R \leq G \leq \mathrm{Sym}(H)$). Namely, letting $T_1 = \{e\}, T_2, \ldots, T_r$ be the orbits of the stabilizer G_e of e in G, it follows that the subspace $\langle \underline{T}_1, \ldots, \underline{T}_r\rangle$ is an S-ring over H (see [123, Theorem 24.1]). This fact was proved by Schur, and the resulting S-ring is also called the *transitivity module* over H induced by the group G_e, notation $V(H, G_e)$. It turns out that not every S-ring over H arises in this way, and we call therefore an S-ring $\mathcal{A}$ *Schurian* if $\mathcal{A} = V(H, G_e)$ for a suitable overgroup G of H_R in $\mathrm{Sym}(H)$. The connection between permutation groups and S-rings is reflected in the following proposition (see [96, Theorem 3.13]).

Proposition 3.1. *Let $\mathcal{A}$ and $\mathcal{B}$ be arbitrary S-rings over H, and let G and K be arbitrary overgroups of H_R in $\mathrm{Sym}(H)$. Then*

(i) $\mathcal{A} \subseteq \mathcal{B} \Rightarrow \mathrm{Aut}(\mathcal{A}) \geq \mathrm{Aut}(\mathcal{B})$.

(ii) $G \leq K \Rightarrow V(H, G_e) \supseteq V(H, K_e)$.

(iii) $\mathcal{A} \subseteq V(H, \mathrm{Aut}(\mathcal{A})_e)$.

(iv) $G \leq \mathrm{Aut}(V(H, G_e))$.

The above proposition describes a *Galois correspondence* between S-rings over H and overgroups of H_R in $\mathrm{Sym}(H)$. We remark that it is a particular case of a Galois correspondence between coherent configurations and permutation groups (cf. [121, 38]).

The starting point of our approach toward Theorem 1.1 is the following consequence of the Galois correspondence, which is formulated implicitly in [121].

Theorem 3.2. *Let H be a finite group and $Q \subseteq H$. Then*

$$\mathrm{Aut}(\mathrm{Cay}(H, Q)) = \mathrm{Aut}(\langle\langle Q \rangle\rangle).$$

4 Rational S-rings over cyclic groups

In this section we turn to S-rings over cyclic groups. Our goal is to provide a description of those S-rings $\mathcal{A}$ that $\mathcal{A} = \langle\langle Q \rangle\rangle$ for some rational circulant graph $\mathrm{Cay}(\mathbb{Z}_n, Q)$.

Throughout the paper the cyclic group of order n is given by the additive cyclic group $\mathbb{Z}_n$, written as $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$. Note that, we have switched from multiplicative to additive notation. For a positive divisor d of n, Z_d denotes the unique subgroup of $\mathbb{Z}_n$ of order d, i.e.,

$$Z_d = \langle m \rangle = \big\{ xm \mid x \in \{0, \dots, d-1\} \big\}, \text{ where } n = dm.$$

Let $\mathbb{Z}_n^* = \{i \in \mathbb{Z}_n \mid \gcd(i, n) = 1\}$, i.e., the multiplicative group of invertible elements in the ring $\mathbb{Z}_n$. (By some abuse of notation $\mathbb{Z}_n$ stands parallel for both the ring and also its additive group.) For $m \in \mathbb{Z}_n^*$, and a subset $Q \subseteq \mathbb{Z}_n$, define $Q^{(m)} = \{mq \mid q \in Q\}$. Two subsets $R, Q \subseteq \mathbb{Z}_n$ are said to be *conjugate* if $Q = R^{(m)}$ for some $m \in \mathbb{Z}_n^*$. The *trace* $\overset{\circ}{Q}$ of Q is the union of all subsets conjugate to Q, i.e.,

$$\overset{\circ}{Q} = \bigcup_{m \in \mathbb{Z}_n^*} Q^{(m)}.$$

The elements m in $\mathbb{Z}_n^*$ act on $\mathbb{Z}_n$ as automorphisms by sending x to mx. We have corresponding orbits

$$(\mathbb{Z}_n)_d = \big\{ x \in \mathbb{Z}_n \mid \gcd(x, n) = d \big\}, \tag{1}$$

where d runs over the set of positive divisors of n. The *complete S-ring of traces* is the transitivity module

$$V(\mathbb{Z}_n, \mathbb{Z}_n^*) = \langle \underline{(\mathbb{Z}_n)_d} \mid d \mid n \rangle.$$

By the *rational* (or *trace*) S-rings over $\mathbb{Z}_n$ we mean the S-subrings of $V(\mathbb{Z}_n, \mathbb{Z}_n^*)$. For an S-ring $\mathcal{A}$ over $\mathbb{Z}_n$ its *rational closure* $\overset{\circ}{\mathcal{A}}$ is the S-ring defined as $\overset{\circ}{\mathcal{A}} = \mathcal{A} \cap V(\mathbb{Z}_n, \mathbb{Z}_n^*)$, and thus $\mathcal{A}$ is rational if and only if $\mathcal{A} = \overset{\circ}{\mathcal{A}}$.

Recall that a circulant graph $\mathrm{Cay}(\mathbb{Z}_n, Q)$ is rational if it has a rational spectrum. The following result describes its connection set Q in terms of the generated S-ring $\langle\langle Q \rangle\rangle$ (cf. [23]).

Theorem 4.1. *A circulant graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_n, Q)$ is rational if and only if the generated S-ring $\langle\langle Q \rangle\rangle$ is a rational S-ring over $\mathbb{Z}_n$.*

It follows from the theorem that Q is a union of some sets of the form $(\mathbb{Z}_n)_d$. In particular, exactly $2^{\tau(n)-1}$ subsets of $\mathbb{Z}_n$ define a rational circulant graph without loops (i.e., $0 \notin Q$). Here $\tau(n)$ denotes the number of positive divisors of n. As we shall see in 11.1, the resulting graphs are pairwise non-isomorphic.

5 Properties of rational S-rings over cyclic groups

Denote $L(n)$ the lattice of positive divisors of n endowed with the relation $x \mid y$ (x divides y). For two divisors x and y, we write $x \wedge y$ for their greatest common divisor, and $x \vee y$ for their least common multiple. Note that, the lattice $L(n)$ is distributive, and if L is any set of positive divisors of n, then the poset $(L, |)$ is a sublattice of $L(n)$ if and only if L is closed with respect to $\wedge$ and $\vee$. By some abuse of notation we shall denote by L this sublattice as well.

For a sublattice L of $L(n)$, and $m \in L$, we define the sets

$$L_{[m]} = \{x \in L \mid x \mid m\}, \text{ and } L^{[m]} = \{x \in L \mid m \mid x\}.$$

It is not hard to see that these are sublattices of $L(n)$.

The following classification of rational S-rings over $\mathbb{Z}_n$ is due to Muzychuk (see [88, Main Theorem]).

Theorem 5.1.

(i) Let L be a sublattice of $L(n)$ such that $1, n \in L$. Then the vector space $\mathcal{A} = \langle \underline{Z_l} \mid l \in L \rangle$ is an S-ring over $\mathbb{Z}_n$, which is rational.

(ii) Let $\mathcal{A}$ be a rational S-ring over $\mathbb{Z}_n$. Then there exists a sublattice L of $L(n)$, $1, n \in L$, such that $\mathcal{A} = \langle \underline{Z_l} \mid l \in L \rangle$.

We remark that if $\mathcal{A} = \langle \underline{Z_l} \mid l \in L \rangle$ is the S-ring in part (i) above, then the simple quantities $\underline{Z_l}$ form a basis of the vector space $\mathcal{A}$, where l runs over the set L. This basis we shall also call the *group basis* of $\mathcal{A}$. It is also true that all $\mathcal{A}$-subgroups appear in this basis, i.e., for any subgroup $Z_k \leq \mathbb{Z}_n$, we have $\underline{Z_k} \in \mathcal{A}$ if and only if $k \in L$. The basic quantities of the rational S-ring $\mathcal{A}$ are easily obtained from its group basis, namely $\mathsf{Basic}(\mathcal{A})$ consists of the sets:

$$\widehat{Z}_l = Z_l \setminus \bigcup_{d \in L_{[l]}, d < l} Z_d, \quad l \in L. \tag{2}$$

In the rest of this section we are going to prove that rational S-rings over $\mathbb{Z}_n$ are generated by subsets of $\mathbb{Z}_n$. More formally, that every rational S-ring $\mathcal{A}$ over $\mathbb{Z}_n$ satisfies $\mathcal{A} = \langle\langle Q \rangle\rangle$, where Q is a suitable subset $Q \subseteq \mathbb{Z}_n$. Notice that, the corresponding circulant graph $\mathrm{Cay}(\mathbb{Z}_n, Q)$ is rational (see Theorem 4.1), and its automorphism group $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, Q)) = \mathrm{Aut}(\mathcal{A})$ (see Theorem 3.2).

We start with an auxiliary lemma, for which the authors thank Muzychuk (see [94]).

Lemma 5.2. *Let L be a sublattice of $L(n)$, $1, n \in L$. Let m be a maximal element of the poset $(L \setminus \{n\}, |)$, and s be the smallest number in the set $L \setminus L_{[m]}$. Then*

$$L \setminus L_{[m]} = \Big\{ x \, \frac{s}{m \wedge s} \mid x \in (L_{[m]})^{[m \wedge s]} \Big\}.$$

Proof. Define the mapping

$$f\colon L \setminus L_{[m]} \to L_{[m]},\ l \mapsto m \wedge l.$$

Let $l \in L \setminus L_{[m]}$. As m is maximal, $l \vee m = s \vee m = n$. By distributive law, $(l \wedge s) \vee m = (l \vee m) \wedge (s \vee m) = n$. Thus $l \wedge s \in L \setminus L_{[m]}$, and by the choice of s, $s \leq l \wedge s$, hence $s \mid l$, $(m \wedge s) \mid f(l)$, and $f(l) \in (L_{[m]})^{[m \wedge s]}$.

On the other hand, choose $x \in (L_{[m]})^{[m\wedge s]}$. Then $l = s \vee x$ is in $L \setminus L_{[m]}$, and we find $f(l) = m \wedge l = (m \wedge s) \vee (m \wedge x) = (m \wedge s) \vee x = x$. Also, $f(L \setminus L_{[m]}) = (L_{[m]})^{[m \wedge s]}$.

For each $l \in L \setminus L_{[m]}$,

$$s \vee f(l) = s \vee (m \wedge l) = (s \vee m) \wedge (s \vee l) = n \wedge l = l. \tag{3}$$

The lemma follows as

$$L \setminus L_{[m]} = \Big\{ s \vee f(l) \ \mid \ l \in L \setminus L_{[m]} \Big\} = \Big\{ s \vee x = \frac{s}{m \wedge s}\, x \ \mid \ x \in (L_{[m]})^{[m \wedge s]} \Big\},$$

here we use the property $x \wedge s = m \wedge s$. ∎

Proposition 5.3. *Let $\mathcal{A}$ be a rational S-ring over $\mathbb{Z}_n$. Then there exists a subset $Q \subseteq \mathbb{Z}_n$ such that $\mathcal{A} = \langle\langle \underline{Q} \rangle\rangle$.*

Proof. We proceed by induction on n. The case $n = 1$ is trivially true. Let $n > 1$. By (ii) of Theorem 5.1,

$$\mathcal{A} = \langle \underline{Z_l} \ \mid \ l \in L \rangle, \tag{4}$$

where L is a sublattice of $L(n)$, $1, n \in L$. Let m be a maximal element in the poset $(L \setminus \{n\}, |)$, and s be the smallest number in the set $L \setminus L_{[m]}$. Apply the induction hypothesis to the induced S-subring $\mathcal{A}|_{Z_m} = \mathcal{A} \cap \mathbb{Q}Z_m$. This results in a subset $R \subseteq Z_m$ such that $\mathcal{A}|_{Z_m} = \langle\langle \underline{R} \rangle\rangle$. Pick the basic set $\widehat{Z}_s \in \mathsf{Basic}(\mathcal{A})$, see (2). By the choice of s we get

$$\widehat{Z}_s = Z_s \setminus \bigcup_{d \in L_{[s]}, d < s} Z_d = Z_s \setminus Z_{m \wedge s}.$$

Let

$$Q = R \cup \widehat{Z}_s, \text{ and } \mathcal{A}' = \langle\langle \underline{Q} \rangle\rangle.$$

It is clear that Q equals its trace $\overset{\circ}{Q}$, so $\mathcal{A}'$ is a rational S-ring. We complete the proof by showing that in fact $\mathcal{A} = \mathcal{A}'$.

As $\underline{\widehat{Z}_s} \in \mathcal{A}$, $\underline{Q} \in \mathcal{A}$, hence $\mathcal{A}' \subseteq \mathcal{A}$. By (4), to have $\mathcal{A} \subseteq \mathcal{A}'$ it is enough to show that, for any positive divisor l of n,

$$l \in L \implies \underline{Z_l} \in \mathcal{A}'. \tag{5}$$

We show first that $\underline{Z_s} \in \mathcal{A}'$. Let $T \in \mathsf{Basic}(\mathcal{A}')$ such that $(\mathbb{Z}_n)_{n/s} \subseteq T$. Consider the subgroup $\langle T \rangle$, and let $\langle T \rangle = Z_t$. As $\mathcal{A}' \subseteq \mathcal{A}$, $\underline{T} \in \mathcal{A}$, and therefore $\underline{Z_t}$ is in $\mathcal{A}$. This gives $t \in L$. Clearly, $t \in L \setminus L_{[m]}$, and hence $t = s \vee (m \cap t)$, see (3). It follows from the description of basic sets in (2) that T contains a generator of $\langle T\rangle = Z_t$. Thus if $t \neq s$, then $T \cap (\mathbb{Z}_n \setminus Z_m \setminus Z_s) \neq \emptyset$. But, $T \subseteq Q$ and $Q \subseteq Z_m \cup Z_s$, implying that $t = s$, and so $\underline{Z_s}$ is in $\mathcal{A}'$.

Thus $\underline{Q \setminus Z_s} = \underline{R \setminus Z_s} \in \mathcal{A}'$. Let $s < n$. We may further assume that $R \cap (\mathbb{Z}_n)_{n/m} \neq \emptyset$, otherwise replace R with its complement in $Z_m \setminus \{0\}$. Thus we find $\underline{Z_m} = \underline{\langle R \setminus Z_s\rangle} \in \mathcal{A}'$. If $s = n$ and $m > 1$ then we may assume that $(Z_m \setminus R) \cap (\mathbb{Z}_n)_{n/m} \neq \emptyset$. From this $\underline{Z_m} = \underline{\langle \mathbb{Z}_n \setminus Q\rangle} \in \mathcal{A}'$. Then

$$\mathcal{A}|_{Z_m} = \langle\langle \underline{R} \rangle\rangle \subseteq \mathcal{A}'|_{Z_m} \subseteq \mathcal{A}|_{Z_m},$$

from which $\mathcal{A}|_{Z_m} = \mathcal{A}'|_{Z_m}$. We conclude that (5) holds if $l \in L_{[m]}$.

Let $l \in L \setminus L_{[m]}$. By (3) we can write $l = s \vee l'$, where $l' = m \wedge l$ is in $L_{[m]}$. Then $Z_l = \langle Z_{l'}, Z_s\rangle$. As both $\underline{Z_{l'}} \in \mathcal{A}'$ and $\underline{Z_s} \in \mathcal{A}'$, $\underline{Z_l} \in \mathcal{A}'$ follows, and this completes the proof of (5). ∎

By Theorems 3.2, 4.1 and Proposition 5.3, we obtain the following equivalence.

Corollary 5.4. *Let G be a permutation group acting on the cyclic group $\mathbb{Z}_n$. The following are equivalent:*

(i) $G = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, Q))$ *for a suitable rational circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, Q)$.

(ii) $G = \mathrm{Aut}(\mathcal{A})$ *for some rational S-ring* $\mathcal{A}$ *over* $\mathbb{Z}_n$.

6 From rational S-rings to block (partition) structures

A *block structure* $\mathcal{F}$ on a set X is simply a collection of partitions of X. A partition F of X is *uniform* if all classes of F are of the same cardinality. Block structure $\mathcal{F}$ is called *orthogonal* (see e.g. [10]) if the following axioms hold:

(OBS1) $E_X, U_X \in \mathcal{F}$.

(OBS2) Every $F \in \mathcal{F}$ is uniform.

(OBS3) Every two $E, F \in \mathcal{F}$ are orthogonal.

(OBS4) For every two $E, F \in \mathcal{F}$, both $E \wedge F \in \mathcal{F}$ and $E \vee F \in \mathcal{F}$.

Note that, if $\mathcal{F}$ is orthogonal, then the poset $(\mathcal{F}, \sqsubseteq)$ is a lattice, where $\sqsubseteq$ is the refinement relation defined on the set of partitions of X. Below we say that $\mathcal{F}$ is *distributive* if the lattice $(\mathcal{F}, \sqsubseteq)$ is distributive.

The following example of a block structure is crucial in the sequel.

Example 6.1. (*Group block structure.*) Let H be an arbitrary group, and K be a subgroup of H. Denote by F_K the partition of H into right cosets of K. A *group block structure* on H is a block structure $(H, \{F_K \mid K \in \mathcal{K}\})$ where $\mathcal{K}$ is a set of subgroups of H satisfying the following axioms:

(GBS1) The trivial subgroup $\{e\}$ is in $\mathcal{K}$.

(GBS2) For every two $K_1, K_2 \in \mathcal{K}$, $K_1K_2 = K_2K_1$, and $K_1K_2 \in \mathcal{K}$.

It follows that the group block structure $(H, \{F_K \mid K \in \mathcal{K}\})$ is orthogonal if and only if $H \in \mathcal{K}$, and $(\mathcal{K}, \leq)$ is a sublattice of the subgroup lattice of H. ∎

In this context Theorem 5.1 can be rephrased as follows.

Theorem 6.2.

(i) Let $\mathcal{F}$ be an orthogonal group block structure on $\mathbb{Z}_n$. Then the vector space $\mathcal{A} = \langle \underline{Z_l} \mid F_{Z_l} \in \mathcal{F}\rangle$ is an S-ring over $\mathbb{Z}_n$.

(ii) Let $\mathcal{A}$ be a rational S-ring over $\mathbb{Z}_n$. Then there exists an orthogonal group block structure $\mathcal{F}$ on $\mathbb{Z}_n$ such that $\mathcal{A} = \langle \underline{Z_l} \mid F_{Z_l} \in \mathcal{F}\rangle$ (here again equality means equality of vector spaces).

For $i = 1, 2$, let $\mathcal{F}_i$ be a block structure on X_i. Following [9], a *weak isomorphism* from $\mathcal{F}_1$ to $\mathcal{F}_2$ is a bijection $f \colon X_1 \to X_2$ such that there exists an induced bijection $g \colon \mathcal{F}_1 \to \mathcal{F}_2$ for which $(x_1, y_1) \in R_F$ if and only if $(x_1^f, y_1^f) \in R_{F^g}$ for all $x_1, y_1 \in X_1$, and $F \in \mathcal{F}_1$. The mapping f is also called a *strong isomorphism with respect to a prescribed* g, or simply a *strong isomorphism* if g is understood. In particular, a *weak automorphism* of $\mathcal{F}$ is a weak isomorphism of $\mathcal{F}$ onto itself, and a *strong automorphism* (or an *automorphism*) is a weak automorphism which is strong with respect to the identity. The *automorphism group* $\mathrm{Aut}(\mathcal{F})$ of $\mathcal{F}$ is therefore the permutation group (see also [6])

$$\mathrm{Aut}(\mathcal{F}) = \bigcap_{F \in \mathcal{F}} \mathrm{Aut}((X, R_F)).$$

Proposition 6.3. *Let $\mathcal{A}$ be a rational S-ring over $\mathbb{Z}_n$, and $\mathcal{F}$ be the orthogonal group block structure on $\mathbb{Z}_n$ such that $\mathcal{A} = \langle \underline{Z_l} \mid F_{Z_l} \in \mathcal{F}\rangle$. Then* $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{F})$.

Proof. Let L be the sublattice of $L(n)$ corresponding to $\mathcal{F}$. To ease notation, we write R_l for the relation $R_{F_{Z_l}}$, where $l \in L$. Then $\mathcal{A}$ has basic sets $\widehat{Z}_l$, $l \in L$, see (2). Let $\widehat{R}_l$ be the relation on $\mathbb{Z}_n$ that is given by the arc set of $\mathrm{Cay}(\mathbb{Z}_n, \widehat{Z}_l)$, i. e., $\mathrm{Cay}(\mathbb{Z}_n, \widehat{Z}_l) = (\mathbb{Z}_n, \widehat{R}_l)$. Thus for $l \in L$,

$$\widehat{R}_l = R_l \setminus \bigcup_{d \in L_{[l]}, d < l} R_d, \text{ and } R_l = \bigcup_{d \in L_{[l]}} \widehat{R}_d.$$

Thus for $g \in \mathrm{Aut}(\mathcal{A})$, $R_l^g = \cup_{d \in L_{[l]}} \widehat{R}_d^{\,g} = \cup_{d \in L_{[l]}} \widehat{R}_d = R_l$, and so $g \in \mathrm{Aut}(\mathcal{F})$. Similarly, if $g \in \mathrm{Aut}(\mathcal{F})$, then $\widehat{R}_l^g = R_l^g \setminus \cup_{d \in L_{[l]}, d<l} R_d^g = R_l \setminus \cup_{d \in L_{[l]}, d<l} R_d = \widehat{R}_l$, implying $g \in \mathrm{Aut}(\mathcal{A})$. Therefore $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{F})$. ∎

We remark that the above correspondence in Theorem 6.2 is a particular case of a correspondence between orthogonal block structures and association schemes, see the discussion in 11.2.

By Corollary 5.4, Theorem 6.2, and Proposition 6.3, we obtain the following equivalence.

Corollary 6.4. *Let G be a permutation group acting on the cyclic group $\mathbb{Z}_n$. The following are equivalent:*

(i) $G = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, Q))$ *for some rational circulant graph* $\mathrm{Cay}(\mathbb{Z}_n, Q)$*.*

(ii) $G = \mathrm{Aut}(\mathcal{F})$ *for some orthogonal group block structure* $\mathcal{F}$ *on* $\mathbb{Z}_n$*.*

7 Simple examples

We interrupt the main line of the presentation, exposing a few simple examples. The goal is to provide the reader additional helpful context. Recall that according to the previous propositions each rational S-ring over $\mathbb{Z}_n$ is uniquely determined by a suitable sublattice of the lattice $L(n)$, or in equivalent terms, by a suitable block structure on $\mathbb{Z}_n$. Moreover, for each rational S-ring a Cayley graph may be found which generates the S-ring in certain prescribed sense. Nevertheless, in many cases consideration of several Cayley graphs in role of generators allows to better comprehend the considered S-ring. Each time in this section we intentionally abuse notation, identifying lattices with their S-rings as well as the automorphism group $\mathrm{Aut}(L)$ of a lattice L with the group $\mathrm{Aut}(\mathcal{A})$, where $\mathcal{A}$ is the rational S-ring defined by L.

Our first example refines Example 1.2.

Example 7.1. Here $n = 6$, we first depict lattice $L = L(6)$. Clearly L has 3 sublattices containing 1 and 6 as shown in Figure 2. $\mathrm{Aut}(L_0) = S_6$. The sublattice L_1 is generated by the point 3, which may be regarded as partition $\{\{0, 2, 4\}, \{1, 3, 5\}\}$. $\mathrm{Aut}(L_1)$ is recognized as the wreath product $S_2 \wr S_3$ of order $2! \cdot (3!)^2 = 72$. Similarly, $\mathrm{Aut}(L_2)$ is the wreath product of order $3! \cdot (2!)^3 = 48$. A significant message is that, for lattice L we have $\mathrm{Aut}(L) = \mathrm{Aut}(L_1) \cap \mathrm{Aut}(L_2) = S_3 \times S_2$, a transitive group of order 12, containing $(\mathbb{Z}_6)_R$ as a subgroup. ∎

Next two rules appear as natural generalization of the observations learned from Example 7.1. Recall that a partition E is a refinement of partition F if each class of E is a part of some class of F.

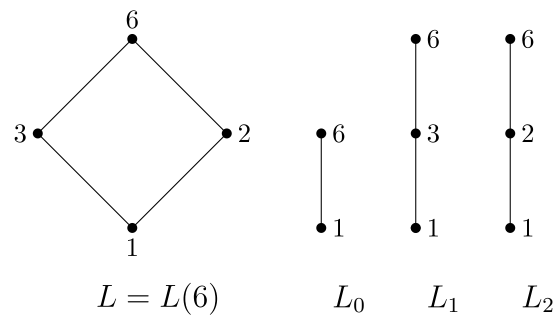

Figure 2: Sublattices of $L(6)$.

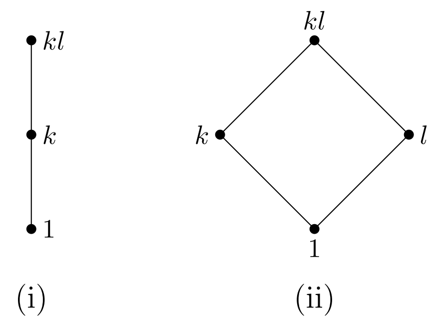

Figure 3: Rules 1 and 2.

Rule 1. The partition defined by node k is a refinement of the partition defined by node kl, see part (i) of Figure 3. This is also called *nesting* of partitions (see [12]). In this case $\mathrm{Aut}(L) = S_l \wr S_k$.

Rule 2. Let $\gcd(k, l) = 1$. Each class of the partition defined by node kl is union of classes defined by nodes k and l, respectively, such that the latter partitions have classes intersecting in at most one element, see part (ii) of Figure 3. This is also called *crossing* of partitions (see [12]). In this case $\mathrm{Aut}(L) = S_k \times S_l$.

The following simple reductions rules are clear generalizations of the above Rules 1 and 2.

Reduction rule 1. This falls into two cases: either each partition defined by node $i, i \neq lm$, is a refinement of the partition defined by node m, see (i) of Figure 4; or the partition defined by node l is a refinement of each partition defined by node $i, i \neq 1$, see (ii) of Figure 4. In the first case $\mathrm{Aut}(L) = S_l \wr \mathrm{Aut}(L_1)$, and in the second case $\mathrm{Aut}(L) = \mathrm{Aut}(L_1) \wr S_l$.

Reduction rule 2. Here $n = ij, \gcd(i, j) = 1$, and $L = L_1 \times L_2$ is a *direct product* of sublattices L_1 of $L(i)$ and L_2 of $L(j)$. An essential property of such situation is that the entire lattice L contains a sublattice, isomorphic to (ii) in Figure 3. (This fact is conditionally depicted in (iii) of Figure 4. Note that, in fact we mean that both L_1 and L_2 contain also 1.) In this case $\mathrm{Aut}(L) = \mathrm{Aut}(L_1) \times \mathrm{Aut}(L_2)$.

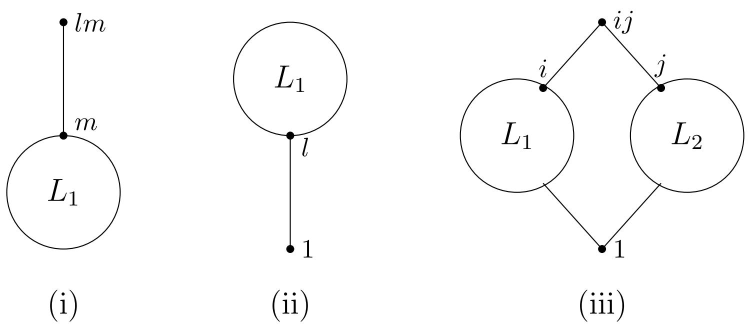

Figure 4: Reduction rules 1 and 2.

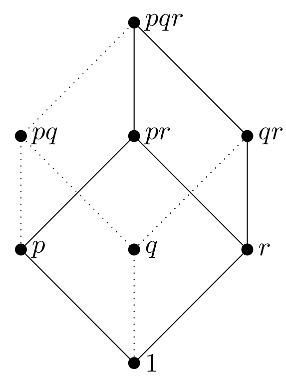

Figure 5: Sublattice L of $L(pqr)$.

The created small toolkit of rules proves immediately its efficiency.

Example 7.2. Here $n = p^e$, p is a prime number. In this case each sublattice of $L(p^e)$ forms a chain, hence can be constructed with using only Reduction rule 1. Thus the automorphism group of each sublattice of $L(p^e)$ is an iterated wreath product of symmetric groups. ∎

Example 7.3. Here $n = pqr$, p, q, and r are distinct primes. One can case by case describe possible sublattices of $L(pqr)$ and in each case to express corresponding automorphism group with the aid of operations of direct and wreath products.

For example, for the sublattice L in Figure 5 we easily obtain $\mathrm{Aut}(L) = (S_q \wr S_r) \times S_p$. (Indeed, here L is a direct product of two chains with 2 and 3 nodes.)

∎

We refer to Section 11.4 for a more rigorous consideration of the reduction rules.

It is not true however that such an easy life is possible for arbitrary value of n. A simple case of a failure is provided by $n = p^2q^2$, where p, q are distinct primes. To make presentation more clear and visible let us consider a concrete sublattice L of $L(36)$.

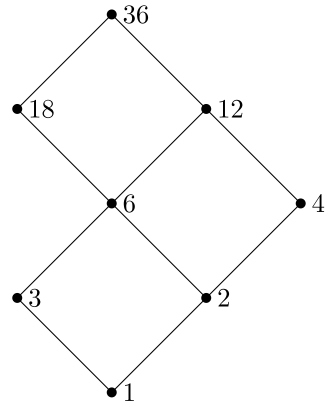

Figure 6: Sublattice L of $L(36)$.

Example 7.4. Here $n = 36$, and let L be the sublattice of $L(36)$ given in Figure 6.

At this stage we wish to describe the automorphism group of L, using simple naive arguments of a computational nature, avoiding however more rigorous justification. We note that we will return to the lattice L in this example a few times in our further presentation. It may be convenient for us to identify the group $\mathrm{Aut}(L)$ with the group $\mathrm{Aut}(\Gamma)$, for a suitable Cayley graph Γ. Recall that as a rule, one may find several possibilities to reach such graph (cf. Section 5). We however wish to use first a more dogmatic (in a sense naive) approach, which is based completely on the paper [89]. Basing on this text, we easily identify the unique rational S-ring which corresponds to L. (We admit that our theoretical reasonings were, in addition, confirmed independently with the aid of a computer via the use of COCO (see [39]).) Thus we reach that the S-ring defined by L has rank 8 with the basic sets B_k as follows (see also (2)):

$$Q_{36},\ Q_2 \cup Q_4,\ Q_3,\ Q_6,\ Q_9,\ Q_{12},\ Q_{18},\ Q_1,$$

where Q_d stands for the set $Q_d = (\mathbb{Z}_{36})_d = \{x \in L(36) \mid \gcd(x, 36) = d\}$. Our goal is to describe

$$G = \bigcap_{k=1}^{7} \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{36}, B_k))$$

as the permutation group preserving each of 7 non-trivial basic Cayley graphs. It turns out however that we may avoid consideration of all 7 basic graphs. (We refer the reader to the texts [40, 69, 123] for discussion of corresponding tools, in particular Galois correspondence between S-rings and permutation groups as well as the Schur-Wielandt principle.)

Thus, acting in such a spirit, we observe that it is possible to disregard basic sets Q_1, Q_{18}, Q_{12}, and Q_9. Therefore now we define G as group which preserves three Cayley graphs Γ_i, $i = 1, 2, 3$, over $\mathbb{Z}_{36}$ defined by basic sets $Q_2 \cup Q_4$, Q_6 and Q_3, respectively. These three graphs are conditionally depicted on the three diagrams below (see also discussion of the rules of the game accepted in these figures). We admit that ad hoc reasonings are playing a significant role in the ongoing exposition.

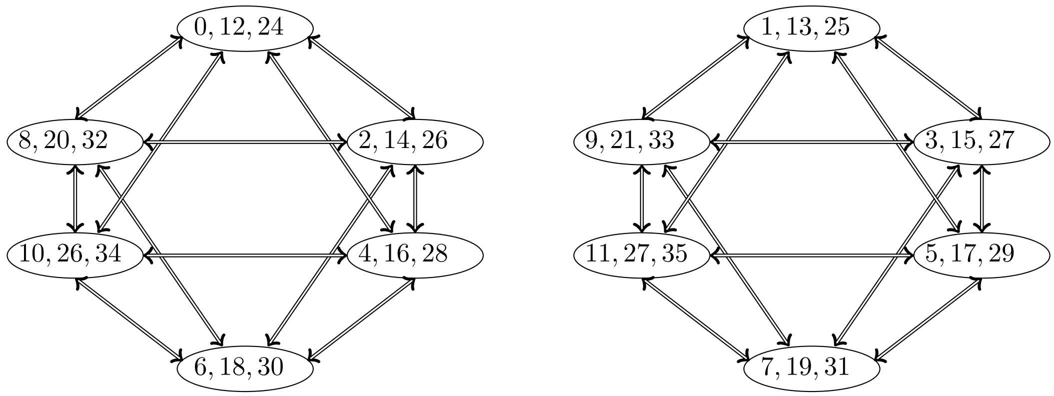

Figure 7: $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{36}, Q_2 \cup Q_4)$.

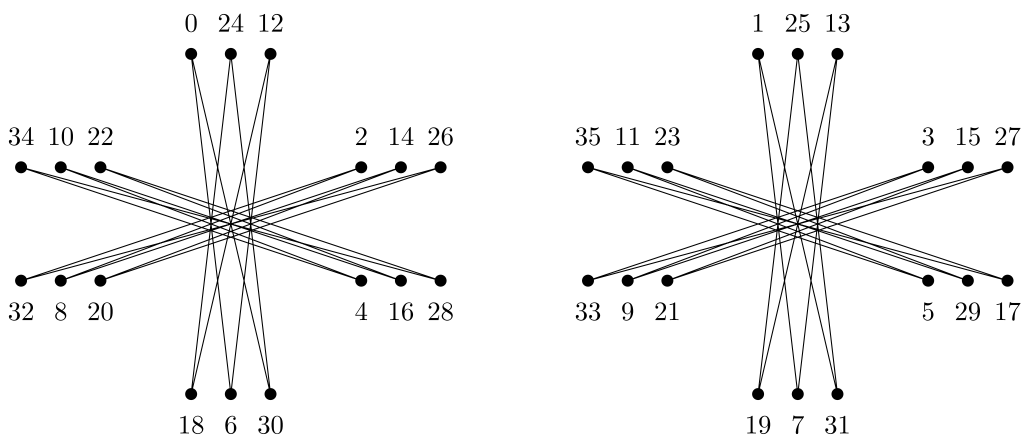

Figure 8: $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{36}, Q_6)$.

Graph Γ_1 is nothing else but a regular graph of valency 12, which has a quotient graph $\widetilde{\Gamma}_1$ on 12 metavertices, see Figure 7. Each metavertex consists of subsets $\{i, 12+i, 24+i\}$, where $i \in \mathbb{Z}_{12}$. Each metaedge substitutes 9 edges in complete bipartite graphs $K_{3,3}$. The graphs Γ_1 and $\widetilde{\Gamma}_1$ have two connectivity components corresponding to even and odd elements of $\mathbb{Z}_{36}$. An easy way to describe isomorphism type of the components of $\widetilde{\Gamma}_1$ is $\overline{3 \circ K_2}$, the complement of a 1-factor on 6 points.

Graph Γ_2 is a disconnected graph of the form $6 \circ C_6$, see Figure 8. Each cycle C_6 is defined on two metavertices from Γ_1. Correspondence is observed from diagram.

Graph Γ_3 has a more sophisticated nature. It has three connectivity components defined by the value of $x \in \mathbb{Z}_{36}$ modulo 3, one of them is depicted in Figure 9. Each connectivity component is a bipartite graph with bipartition to odd and even elements. In addition, each component is 3-partite with the parts visible on the picture. Thus finally it may be convenient to regard edge set of a connectivity component as union of edges from 6 disjoint quadrangles.

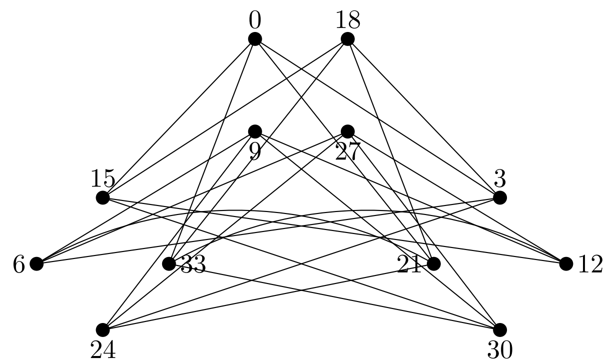

Figure 9: A connectivity component of $\Gamma_3 = \mathrm{Cay}(\mathbb{Z}_{36}, Q_3)$.

Now we are prepared to claim that the desired group G has the following structure:

$$G = \mathbb{Z}_2^6 \centerdot \big((S_3 \wr S_3) \centerdot \mathbb{Z}_2 \big),$$

and thus it has order $2^6 \cdot 6^4 \cdot 2 = 2^{11} \cdot 3^4$. To justify this claim, we will present concrete automorphisms from G, will comment their action on the basic graphs, and will count the order of the group, generated by these permutations. First we wish to describe 64 permutations from G, which preserve each metavertex of Γ_1 and each connectivity component of Γ_2. (Of course, in addition, they preserve the remaining graph, this time Γ_3.) In fact, we restrict ourselves by list of 3 permutations which are corresponding to the connectivity component of Γ_3 given in Figure 9.

$$\begin{aligned} g_1^{(1)} &= (3,15)(6,30)(12,24)(21,33), \\ g_2^{(1)} &= (0,12)(18,30)(9,21)(3,27), \\ g_3^{(1)} &= (0,24)(6,18)(9,33)(15,27). \end{aligned}$$

Similarly, two more sets of permutations $g_1^{(i)}, g_2^{(i)}, g_3^{(i)}, i = 2, 3$, are defined with the aid of the remaining two components of Γ_3. Altogether, involutions from three groups, isomorphic to $(\mathbb{Z}_2)^2$ are listed. Direct product of these three groups provides group $(\mathbb{Z}_2)^6$, forming first factor in description of G.

Now we wish to justify part of the formula $S_3 \wr S_3$. It is helpful to think about the group acting faithfully on the set of 9 anti-cliques of size 4 visible from the diagram of Γ_3. First, consider permutations on $\mathbb{Z}_{36}$ defined as

$$\begin{aligned} g_4 &: \quad x \mapsto x + 4, \text{ and} \\ g_5 &= (0)(1,35)(2,34)(3,33)\cdots(17,19)(18). \end{aligned}$$

Clearly, these permutations generate a subgroup, which acts as S_3 on the connected components of Γ_3 and preserves odd and even parts. On next step, consider

$$\begin{aligned} g_6^{(1)} &= (0,6,12,18,24,30)(3,9,15,21,27,33), \text{ and} \\ g_7^{(1)} &= g_1^{(1)} = (3,15)(6,30)(12,24)(21,33). \end{aligned}$$

Check that $\langle g_6^{(1)}, g_7^{(1)}\rangle$ acts as S_3 on the connected component of Γ_3 given in Figure 9, it preserves other components, and of course it is an automorphism group of two remaining basic graphs. Similarly, two more sets of permutations $\langle g_6^{(i)}, g_7^{(i)}\rangle, i = 2, 3$, are defined. Notice that, all permutations, presented till this moment, preserve the sets of odd and even vertices. Last natural permutation on $\mathbb{Z}_{36}$ is defined as $g_8 \colon x \mapsto x + 1$, which clearly interchanges odd and even vertices, thus justifying last ingredient $\mathbb{Z}_2$ in our formula for the group G.

We suggest the reader to check that the permutations $g_1^{(i)}, g_2^{(i)}, \ldots, g_8$ exposed above (which belong to G indeed) generate the group of the desired order $2^{11} \cdot 3^4$. It is a standard (and helpful) exercise in computational algebraic graph theory to confirm that we already encountered the entire group G. ∎

In next sections group G will appear again, though in different incarnations, thus helping the reader again and again to build a bridge between our theoretical reasonings and practical ad hoc computations.

8 Crested products

In this section (in order to make our presentation as self-contained as possible) we provide a short digest of the paper [12], which is adopted essentially for the purposes of the current presentation. We refer to [12] for accurate proofs of the claims presented below, while ongoing level of rigor follows the intuitive style of the previous section.

Recall that our foremost goal is to investigate and to extend the possibility to build arbitrary sublattice L of $L(n)$ from trivial lattices using only simple reduction rules. The *trivial sublattice* of $L(n)$ consists of only the elements 1 and n, and it will be denoted by T_n. We may prove that such an "easy life" (cf. Section 7) is possible if and only if $n = p^e$ or $n = p^e q$ or $n = pqr$ for distinct primes p, q and r (see Section 11). We wish to define binary operation $\otimes_d, d \in \mathbb{N}$, for lattices with the following goals in mind.

- Special cases of $\otimes_d$ give back simple reduction rules.
- Every sublattice L of $L(n)$ such that $1, n \in L$ can be built from trivial lattices using only operations $\otimes_d$.
- If L is built from trivial lattices as

$$L = T_{d_k} \otimes_{d_{k-1}} \Big(T_{d_{k-1}} \otimes_{d_{k-2}} (\cdots \otimes_{d_2} (T_{d_2} \otimes_{d_1} T_{d_1}) \cdots)\Big),$$

then $\mathrm{Aut}(L)$ can be nicely described in terms of symmetric groups $\mathrm{Aut}(T_{d_i}) = S_{d_i}$.

In what follows this desired operation $\otimes_d$ will be called *crested product*. The word "crested", suggested in [12], is a mixture of "crossed" and "nested", and is also cognate with the meaning of "wreath" in "wreath product". Due to the existence of the bijections between S-rings of traces over $\mathbb{Z}_n$, sublattices of $L(n)$, rational association schemes (invariant with respect to regular cyclic groups) and orthogonal group block structures on $\mathbb{Z}_n$, the desired new operation may be translated in a few corresponding diverse languages. We prefer to start with orthogonal block structures (see [12, Definition 3]).

For $i = 1, 2$, let F_i be a partition of X_i. Define $F_1 \times F_2$ to be the partition of $X_1 \times X_2$ whose adjacency matrix $A(F_1 \times F_2)$ is the Kronecker product $A(F_1) \otimes A(F_2)$ (cf. 2.4).

Definition 8.1. For $i = 1, 2$, let $\mathcal{F}_i$ be an orthogonal block structure on a set X_i, and let $F_i \in \mathcal{F}_i$. The *(simple) crested product* of $\mathcal{F}_1$ and $\mathcal{F}_2$ with respect to F_1 and F_2 is the following set $\mathcal{P}$ of partitions of $X_1 \times X_2$:

$$\mathcal{P} = \left\{ P_1 \times P_2 \;\middle|\; P_1 \in \mathcal{F}_1, P_2 \in \mathcal{F}_2, P_1 \sqsubseteq F_1 \text{ or } P_2 \sqsupseteq F_2 \right\}.$$

It can be proved that the crested product, as just defined, is an orthogonal block structure. The reader may be easily convinced that indeed, crossing and nesting are special cases of the crested product. An important subclass of orthogonal block structures consists of the poset block structures (see, e.g. [10]), for a definition see Section 9. It can be proved that crested products of poset block structures remain poset block structures. Moreover, every poset block structure can be attained from trivial block structures by a repeated use of crested products. Thus it can be proved that the crested products satisfy the above three goals. (Note that our claim about the fulfillment of the above goals literally is actual for the poset block structures on $\mathbb{Z}_n$. We avoid discussion of difficulties, which may appear in more general cases.)

The formal definition of crested product $\otimes_d$ (adopted for the orthogonal group block structures on $\mathbb{Z}_n$) is as follows.

Definition 8.2. For $i = 1, 2$, let $n_i \in \mathbb{N}$, L_i be a sublattice of $L(n_i)$ such that $1, n_i \in L(n_i)$, and d be in L_2 such that $\gcd(n_1, n_2/d) = 1$. Then the sublattice $L_1 \otimes_d L_2$ of $L(n_1 n_2)$ is defined as

$$L_1 \otimes_d L_2 = \left\{ l_1 l_2 \;\middle|\; l_1 = 1, l_2 \in L_2, \text{ or } l_1 \in L_1, l_2 \in L_2 \text{ with } d \mid l_2 \right\}.$$

The fact that the set $L_1 \otimes_d L_2$ is indeed a sublattice of $L(n_1 n_2)$ is proven below.

Proposition 8.3. *For $i = 1, 2$, let $n_i \in \mathbb{N}$, L_i be a sublattice of $L(n_i)$ such that $1, n_i \in L(n_i)$, and d be in L_2 such that $\gcd(n_1, n_2/d) = 1$. Then the set*

$$L = \left\{ l_1 l_2 \;\middle|\; l_1 = 1, l_2 \in L_2, \textit{ or } l_1 \in L_1, l_2 \in L_2 \textit{ with } d \mid l_2 \right\}$$

is a sublattice of $L(n_1 n_2)$.

Proof. It is clear that each element in L is a divisor of $n_1 n_2$, and that $1, n_1 n_2 \in L$. We have to show that L is closed under the operations $\wedge$ and $\vee$, i.e., $x \wedge y \in L$ and $x \vee y \in L$ for all $x, y \in L$. These are clearly true if both $x \in L_2$ and $y \in L_2$, and hence we may assume that at least one of them is from $L \setminus L_2$.

First, let both x and y be from $L \setminus L_2$. Then $x = x_1x_2$ and $y = y_1y_2$ for some $x_1, y_1 \in L_1$ and $x_2, y_2 \in L_2$; furthermore, $x_2 = dx_2'$, $y_2 = dy_2'$. Since $n_1 \wedge \frac{n_2}{d} = 1$, we find $x_1 \wedge x_2' = x_1 \wedge y_2' = y_1 \wedge x_2' = y_1 \wedge y_2' = 1$. Using these,

$$x \wedge y = x_1x_2 \wedge y_1y_2 = d(x_1x_2' \wedge y_1y_2') = d(x_1 \wedge y_1)(x_2' \wedge y_2') = (x_1 \wedge y_1)(d(x_2' \wedge y_2')),$$

which is in L. Then

$$x \vee y = \frac{xy}{x \wedge y} = \frac{x_1dx_2' \cdot y_1dy_2'}{(x_1 \wedge y_1)d(x_2' \wedge y_2')} = (x_1 \vee y_1)(d(x_2' \vee y_2')) \in L \setminus L_2.$$

Second, let $x \in L_2$ and $y \in L \setminus L_2$, $y = y_1y_2$ for some $y_1 \in L_1$ and $y_2 \in L_2$ with $y_2 = dy_2'$. Then

$$x \wedge y = x \wedge (y_1dy_2') = (x \wedge d)\Big(\frac{x}{x \wedge d} \wedge \frac{y_1dy_2'}{x \wedge d}\Big).$$

As $\frac{x}{x \wedge d} \wedge y_1 = 1$, the above is reduced to

$$(x \wedge d)\Big(\frac{x}{x \wedge d} \wedge \frac{y_2}{x \wedge d}\Big) = x \wedge y_2 \in L_2 \subseteq L.$$

Therefore,

$$x \vee y = \frac{xy}{x \wedge y} = \frac{xy_1y_2}{x \wedge y_2} = y_1(x \vee y_2).$$

As $y_1 \in L$, and $x \vee y_2 = x \vee dy_2'$ is in L_2 which is in addition divisible by d, it follows that $x \vee y = y_1(x \vee y_2) \in L$. The proposition is proved. ∎

Notice that, operations $\otimes_d$ include simple reduction rules 1 and 2 as special cases. Namely, in case $d = n_2$, and $L_1 = T_{n_1}$ or $L_2 = T_{n_2}$ we get reduction rule 1, and in case $d = 1$ reduction rule 2.

Consider the orthogonal group block structure on $\mathbb{Z}_{n_1n_2}$ corresponding to the lattice $L_1 \otimes_d L_2$. This is weakly isomorphic to the crested product of the block structure on $\mathbb{Z}_{n_1}$ corresponding to L_1 and that one on $\mathbb{Z}_{n_2}$ corresponding to L_2 with respect to partitions F_{Z_1} and F_{Z_d} in the sense of Definition 8.1, justifying the name "crested product" for $\otimes_d$. (We once more refer to [10, 12] for a justification of all necessary intermediate claims.)

Example 8.4. (*Example 7.4 revised.*) Let L be the sublattice of $L(36)$ given in Figure 6. To each of 8 nodes in diagram for L naturally corresponds a partition of $\mathbb{Z}_{36}$. Because L is a lattice, we get a corresponding orthogonal block structure on $\mathbb{Z}_{36}$. Naive description of nodes of L looks as follows: consider all nodes in L and take into consideration those ones which are in $L_{[18]}$ or are multiples of $d = 2$. Let $L_1 = \{1, 2\}$ on $\mathbb{Z}_2$ and $L_2 = L_{[18]} = \{1, 2, 3, 6, 18\}$ on $\mathbb{Z}_{18}$. Then by Definition 8.2 we obtain

$$L = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 3, 1 \cdot 6, 1 \cdot 18, 2 \cdot 2, 2 \cdot 6, 2 \cdot 18\} = L_1 \otimes_2 L_2.$$

Moreover, using properly notation for the crested product of lattices, the product $L_1 \otimes_2 L_2$ is depicted in Figure 10.

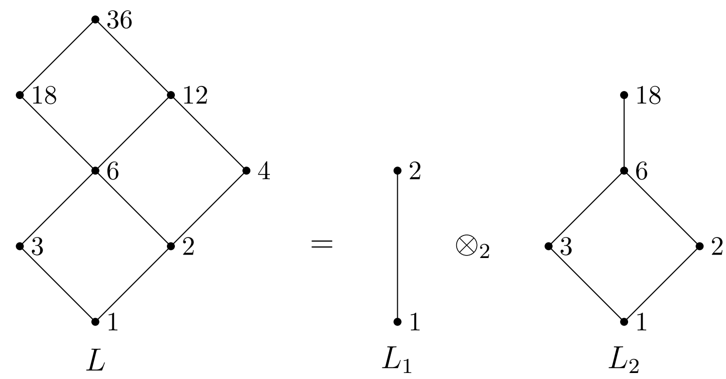

Figure 10: Decomposition $L = L_1 \otimes_2 L_2$.

We now easily interpret L with the aid of Definition 8.1 as crested product. Namely, consider subgroups $Z_m \leq \mathbb{Z}_{36}$ for $m = 2, 4$ and 18. We have $Z_2 = \{0, 18\}$, $Z_4 = \{0, 9, 18, 27\}$, and write the quotient group Z_4/Z_2 as $Z_4/Z_2 = \{Z_2, Z_2 + 9\}$. As the $\mathbb{Z}_{36}$-elements 0 and 9 form a complete set of coset representatives of the subgroup Z_{18} in $\mathbb{Z}_{36}$, every element x in $\mathbb{Z}_{36}$ can be written uniquely as a sum

$$x = x_1 + x_2, \text{ where } x_1 \in \{0, 9\}, x_2 \in Z_{18},$$

and addition is in $\mathbb{Z}_{36}$. Therefore, we can define the bijective mapping

$$f \colon \mathbb{Z}_{36} \to Z_4/Z_2 \times Z_{18},\, x \mapsto (Z_2 + x_1, x_2).$$

Let d be an arbitrary element in L, and let Γ denote the graph defined by the equivalence relation corresponding to the partition of $\mathbb{Z}_{36}$ into its Z_d-cosets (here and later on we freely identify partitions with the graphs defined by the corresponding equivalence relations). The bijection f maps Γ to a graph Γ^f on $V = Z_4/Z_2 \times Z_{18}$. The graph Γ^f is described as follows.

If $d \in L_{[18]}$, then for any two $(x, y), (x', y') \in V$,

$$(x, y) \sim_{\Gamma^f} (x', y') \iff x = x' \text{ and } y \sim_\Sigma y',$$

where Σ is the graph on Z_{18} corresponding to the partition of Z_{18} defined by $d \in L_{[18]}$. We obtain Γ^f as a direct product $\Gamma^f = K_2^c \times \Sigma$, where K_2^c is the complement of the complete graph K_2.

Suppose next that $d \in L \setminus L_{18}$. Then for $(x, y), (x', y') \in V$,

$$(x, y) \sim_{\Gamma^f} (x', y') \iff y \sim_\Sigma y',$$

this time Σ denotes the graph on Z_{18} corresponding to the partition of Z_{18} defined by $d/2 \in L_{[18]}$. In this case $\Gamma^f = K_2 \times \Sigma$. Notice also that, now $d/2$ does not run over the whole lattice $L_{[18]}$, but the sublattice $\left(L_{[18]}\right)^{[2]}$. Since the direct product of graphs corresponds to the Kronecker product of partitions, we conclude by Definition 8.1 that the partitions, corresponding to the graphs Γ^f, comprise actually a suitable crested product. Namely, it is the crested product of the block structure on Z_4/Z_2 defined by L_1 and the block structure on Z_{18} defined by L_2 with respect to the partition F_1 and F_2, where F_1 is the trivial partition of Z_4/Z_2, and F_2 is the partition of Z_{18} into Z_2-cosets. In other words, f is a weak isomorphism from $L = L_1 \otimes_2 L_2$ to the latter crested product.

Eventually, notice that simple reduction rules apply to L_2. We obtain that $L_2 = T_3 \otimes_6 (T_2 \otimes_1 T_3)$, therefore, L actually decomposes as

$$L = T_2 \otimes_2 (T_3 \otimes_6 (T_2 \otimes_1 T_3)).$$

■

In the rest of the section we turn to the group $\mathrm{Aut}(L_1 \otimes_d L_2)$. It remains to translate everything to the language of association schemes, and after that the one of permutation groups, with the goal that finally $\mathrm{Aut}(L_1 \otimes_d L_2)$ is described in terms of $\mathrm{Aut}(L_1)$ and $\mathrm{Aut}(L_2)$. We refer again to the paper [12], where such goal is fulfilled to a certain extent. Namely, it is proved that for the case of poset block structures one gets that crested product of $\mathrm{Aut}(L_1)$ and $\mathrm{Aut}(L_2)$ preserves the crested product of L_1 and L_2. Instead of a discussion of corresponding precise definitions and formulations, we prefer to play again on the level of our striking example.

Example 8.5. (*Continuation of Example 8.4.*) We again use freely the possibility to switch at any moment between languages of lattices, S-rings, and association schemes. In the above notation we get $L_1 = \{1, 2\}$ on $\mathbb{Z}_2$, $L_2 = \{1, 2, 3, 6, 18\}$ on $\mathbb{Z}_{18}\}$ and $L = \{1 \cdot 1, 1 \cdot 2, 1 \cdot 3, 1 \cdot 6, 1 \cdot 18, 2 \cdot 1, 2 \cdot 2, 2 \cdot 6, 2 \cdot 18\}$ on $\mathbb{Z}_{36}$.

In our previous attempt it was natural and convenient to consider automorphism groups of basic graphs (regarded as rational circulant graphs). We proceeded finally with three such graphs. At the current stage we see $G = \mathrm{Aut}(L)$ with the aid of group basis in the corresponding S-ring (cf. [23, 88]). Clearly, each element of a group basis corresponds to a partition of $\mathbb{Z}_{36}$ into cosets of a suitable subgroup. Therefore, now we get

$$G = \bigcap_{l \in L} \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{36}, Z_m)),$$

where Z_m is the unique subgroup of $\mathbb{Z}_{36}$ of order m. Thus we have immediately that in fact G is the automorphism group of four partitions defined by Z_m, namely $m = 2, 3, 4$ and 18. We again describe this group, using a suitable diagram (see Figure 11) which exhibits simultaneously all the partitions.

Comments about the diagram. First partition $2 \circ K_{18}$ (due to Z_{18}) is presented by division to left and right part (even and odd numbers). Horizontal lines represent $9 \circ K_4$ (due to Z_4). Finally, we have 6 connected components of size 6. Columns of all such components entirely provide $12 \circ K_3$ (due to Z_3), while rows give $18 \circ K_2$ (due to Z_2).

We now describe the automorphism group G as an extension $G = \widetilde{G} \mathbin{.} S_2$, where $\widetilde{G}$ is the stabilizer of left part of the picture (clearly left and right parts may be exchanged).

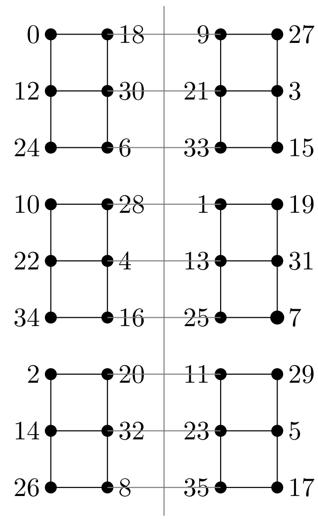

Figure 11: Coset-partitions of $\mathbb{Z}_{36}$ defined by Z_m for $m = 2, 3, 4, 18$.

The stabilizer of the left part is a wreath product of the groups of the three components. Thus we get $G = (S_3 \wr \widehat{G}) \centerdot S_2$, where $\widehat{G}$ is the stabilizer of a component. Stabilizer of left upper component, according to simple rule, is $S_2 \times S_3$, and in addition, an independent copy of S_2 transposes columns in corresponding right part of the upper component. We have thus obtained the formula

$$G = (S_3 \wr ((S_3 \times S_2) \times S_2)) \centerdot S_2,$$

with the order $|G| = 2 \cdot 3! \cdot 24^3 = 2^{11} \cdot 3^4$. We expect that the reader will admit that the current arguments are more transparent and straightforward, however, we again are depending on the use of ad hoc tricks of geometrical and combinatorial nature.

It turns out that the above argumentation may be modified into certain nice formal rule with the aid of the use of crested product, taking into account the decomposition formula presented for the lattice L in the consideration, that is $L = L_1 \otimes_2 L_2$.

Regarding as sets, let $\mathbb{Z}_{36} = \mathbb{Z}_2 \times \mathbb{Z}_{18}$. In definition of crested product first ingredient corresponds to active while second to passive groups. Thus in our case G is regarded as a subgroup of the wreath product $\mathrm{Aut}(L_1) \wr \mathrm{Aut}(L_2) = G_1 \wr G_2$ or more precisely as $B \rtimes G_1$, where B is base group and G_1 is top group. Note that at this stage B is just a subgroup of the base group, corresponding to the usual wreath product. Using our toolkit of simple rules, we obtain that

$$G_1 = \mathrm{Aut}(L_1) = S_2, \text{ and } G_2 = \mathrm{Aut}(L_2) = S_3 \wr (S_2 \times S_3).$$

We have to understand the structure of the base group. Recall that in our case B is subgroup of group $G_2^{\mathbb{Z}_2}$. To describe B we refer to the partition $F_2 = F_{Z_2}$ of $\mathbb{Z}_{18}$, which is preserved by G_2. Clearly, this partition F_2 is of the kind $9 \circ K_2$. Note that we have also a trivial partition $F_1 = F_{Z_1}$ of kind $2 \circ K_1$ which is preserved by G_1. Now we are looking

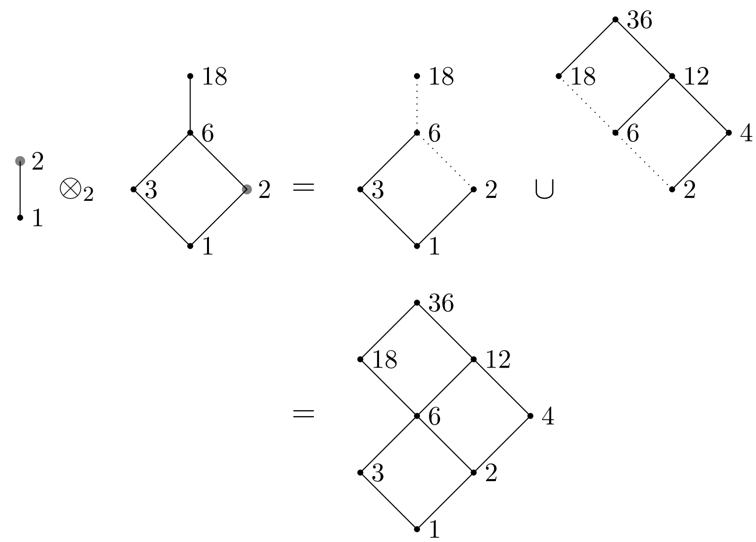

Figure 12: "Amalgamation of lattices".

for the subgroup N of group G_2 which fixes each part of the partition F_2. Clearly, in our case N is isomorphic to S_2^3.

It turns out (see [12] for general justification) that the base group B is generated by N^{F_1} and G_2. Here N^{F_1} is embedded in $G_2^{\mathbb{Z}_2}$ as the set of functions which are constant on the classes of F_1 and take values diagonally. G_2 is embedded diagonally. G_2 normalizes N^{F_1}, therefore their product is a group, while intersection is N. Thus we obtain that

$$|B| = \frac{|N^{F_1}| \cdot |G_2|}{|N|} = \frac{|N|^2 \cdot G_2}{|N|} = |N| \cdot |G_2|.$$

Finally we get the order of the group $G = B \rtimes G_1$ as $|G_1| \cdot |N| \cdot |G_2| = 2 \cdot 8 \cdot 3!(2 \cdot 3)^3 = 2^{11} \cdot 3^4$, as desired. (In fact, again we first obtain that the automorphism group of L has order at least $2^{11} \cdot 3^4$. After that, exactly like in Example 7.4, we have to check that $B \rtimes G_1$ indeed coincides with the entire group G.) ∎

Remark. We wish to use an extra chance to explain the role of index 2 in our notation for the used version of crested product. Hopefully, the following pictorial explanation (see Figure 12) may help. Here selected node in L_2 is origin of the index. We multiply part of L_1 strictly below the index on L_2, after that L_1 on the part of L_2 above the index and amalgamate the two products.

In our eyes the formulated goal to create for the reader a context with the aid of an example is fulfilled. In principle, based on the earned experience, one can go ahead and prove that the leads formulated above are completely fulfilled with the aid of the crested product. However, this will not be done in the current paper. Instead, we refer the reader to the recent papers [36, 37] (cf. Section 12.7). We finish the deviation, developed in Sections 7-8, and return to the main stream of the presentation, aiming to exploit another classical generalization of the operation wreath product.

9 Generalized wreath products

Let $(I, \preceq)$ be a poset. A subset $J \subseteq I$ is called *ancestral* if $i \in J$ and $i \preceq j$ imply that $j \in J$ for all $i, j \in I$. For $i \in I$, we put A_i for the ancestral subset

$$A_i = \{j \in I \mid i \prec j\}.$$

We denote the set of all ancestral subsets of I by $\text{Anc}((I, \preceq))$. For each $i \in I$, fix a set X_i of cardinality at least 2, and let $X = \prod_{i \in I} X_i$. We write elements x in X as $x = (x_i)_{i \in I}$ or simply as $x = (x_i)$. For $J \subseteq I$, let $\sim_J$ be the equivalence relation on X given as

$$(x_i) \sim_J (y_i) \iff x_j = y_j \text{ for all } j \in J,$$

and denote by $\Pi(J)$ the corresponding partition of X. Now, the *poset block structure* defined by the poset $(I, \preceq)$ and the sets X_i is the block structure on X consisting of all partitions $\Pi(J)$ that $J \in \text{Anc}((I, \preceq))$. Denote by $\mathcal{F}$ this block structure. Let $J, J' \in \text{Anc}((I, \preceq))$. Both sets $J \cap J'$ and $J \cup J'$ are ancestral, and we have

$$\Pi(J) \wedge \Pi(J') = \Pi(J \cup J') \text{ and } \Pi(J) \vee \Pi(J') = \Pi(J \cap J').$$

Thus the poset block structure $\mathcal{F}$ is an orthogonal block structure. Further, the equivalence $\Pi(J) \sqsubseteq \Pi(J') \iff J' \subseteq J$ holds, and the mapping $J \mapsto \Pi(J)$ is an anti-isomorphism from the lattice $(\text{Anc}((I, \preceq)), \subseteq)$ to the lattice $(\mathcal{F}, \sqsubseteq)$ (thus these have Hasse diagrams dual to each other). The lattice $(\text{Anc}((I, \preceq)), \subseteq)$ is obviously distributive, and by the previous remarks so is $\mathcal{F}$. The following converse is due to Bailey and Speed [114] (see also [6, Theorem 5]).

Theorem 9.1. *An orthogonal block structure is distributive if and only if it is weakly isomorphic to a poset block structure.*

Note that, in particular, the orthogonal group block structures on $\mathbb{Z}_n$ are poset block structures. We continue consideration of our striking example.

Example 9.2. (*Example 7.4 revised.*) Let L be the sublattice of $L(36)$ given in Figure 6. As before, L will simultaneously denote the orthogonal block structure on $\mathbb{Z}_{36}$ consisting of coset-partitions of $Z_l, l \in L$.

In order to obtain L as a poset block structure we start with the poset $N = ([4], \preceq)$ depicted in part (i) of Figure 13. The dual lattice of ancestral subsets of N has Hasse diagram shown in part (ii) of Figure 13. This is indeed isomorphic to our lattice L. Next, let us choose sets $X_1 = [3]$, $X_2 = [2]$, $X_3 = [3]$ and $X_4 = [2]$. We define the mapping $f \colon X_1 \times X_2 \times X_3 \times X_4 \to \mathbb{Z}_{36}$ as

$$(x_1, x_2, x_3, x_4) \mapsto 12x_1 + 18x_2 + 2x_3 + 9x_4 \pmod{36}.$$

The reader is invited to work out that f is a bijection, and that f is a weak isomorphism from the poset block structure defined by N and the sets X_i to our block structure L. ■

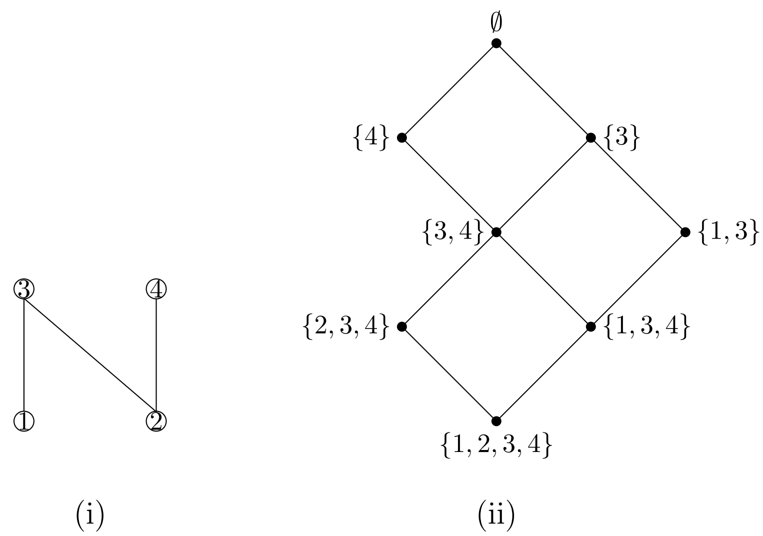

Figure 13: Poset N and the dual lattice of its ancestral subsets.

Now we are approaching the group-theoretical concept, crucial for the current presentation. Let $\mathcal{F}$ be a poset block structure defined by a poset $(I, \preceq)$ and sets X_i $(i \in I)$. Recall that $A_i = \{j \in I \mid i \prec j\}$ is uncestral for all $i \in I$. We set

$$^{i}H = \prod_{j \in A_i} X_j = \prod_{i \prec j} X_j,$$

and π^i for the *projection* of $X = \prod_{i \in I} X_i$ onto ^{i}H. The following construction can be found in [13].

Definition 9.3. Let $(I, \preceq)$ be a poset, X_i be a set $(i \in I)$, $|X_i| \geq 2$, and K_i be a permutation group $K_i \leq \mathrm{Sym}(X_i)$. The *generalized wreath product* $\prod_{(I,\preceq)} K_i$ defined by $(I, \preceq)$ and the groups K_i, is the complexus product

$$P = \prod_{i \in I} P_i,$$

where P_i is the permutation representation of the group $K_i^{\,^{i}H}$ on X acting by the rule

$$(x^f)_j = \begin{cases} x_j^{f(\pi^i(x))} & \text{if } i = j \\ x_j & \text{if } i \neq j \end{cases}, \; x = (x_j) \in X, \; f \in K_i^{\,^{i}H},$$

where $x_j^{f(\pi^i(x))}$ means the image of x_j under the action of $f(\pi^i(x))$.

Clarification of the notation $f(\pi^i(x))$ follows below. We remark that, the fact that the above complexus product is indeed a group was proved in [13]. This construction has a very interesting history, see Section 12.

Let $I = [r] = \{1, \ldots, r\}$ in Definition 9.3. We write $x = (x_1, \ldots, x_r)$ for $x \in X = \prod_{i=1}^{r} X_i$. Every $f \in P$ is presented uniquely as the product $f = f_1 \cdots f_r$, where each $f_i \in P_i$. Analogously to the ordinary wreath product (see 2.1), we shall also write f in the *table form*

$$f = \left[\ f_1(\pi^1(x)), \ldots, f_r(\pi^r(x))\ \right].$$

By definition, $(x_1, \ldots, x_r)^f = \left(x_1^{f_1(\pi^1(x))}, \ldots, x_r^{f_r(\pi^r(x))}\right)$. It is not hard to see that the group $P = \prod_{([r],\preceq)} K_i$ has order

$$\Big|\prod_{([r],\preceq)} K_i\Big| = \prod_{i=1}^{r} |K_i|^{m_i}, \tag{6}$$

where $m_i = 1$ if $\{i\} \in \mathrm{Anc}((I, \preceq))$, and $m_i = \prod_{j \in A_i} |X_j|$ otherwise. The generalized wreath product gives back the ordinary direct and wreath product. Namely, in case $r = 2$ and the poset is an anti-chain the group $P = K_1 \times K_2$, and if the poset is a chain with $1 \prec 2$, then $P = K_2 \wr K_1$.

The following result about the automorphism group of a poset block structure was proved by Bailey et al. (see [13, Theorem A]). We say that a poset $(I, \preceq)$ satisfies the *maximal condition* if any subset $J \subseteq I$ contains a maximal element.

Theorem 9.4. *Let $(I, \preceq)$ be a poset having the maximal condition, X_i be a set of cardinality at least 2 for all $i \in I$, and $\mathcal{F}$ be the poset block structure on X defined by $(I, \preceq)$ and the sets X_i. Then* $\mathrm{Aut}(\mathcal{F}) = \prod_{(I,\preceq)} \mathrm{Sym}(X_i)$.

Of course, if the set I is finite, then $(I, \preceq)$ satisfies the maximal condition. In particular, the above theorem applies to the orthogonal group block structures on $\mathbb{Z}_n$, and hence we observe that their automorphism groups are certain generalized wreath products. As an illustration of the above ideas, we determine once more the automorphism group of a rational circulant graph, corresponding to our lattice L, in terms of generalized wreath product.

Example 9.5. Let Γ be the rational circulant graph $\mathrm{Cay}(\mathbb{Z}_{36}, Q)$, where

$$\begin{aligned} Q &= \{2, 3, 4, 6, 8, 10, 14, 15, 16, 20, 21, 22, 26, 28, 30, 32, 33, 34\} \\ &= (\mathbb{Z}_{36})_2 \cup (\mathbb{Z}_{36})_3 \cup (\mathbb{Z}_{36})_4 \cup (\mathbb{Z}_{36})_6. \end{aligned}$$

Because of Theorem 3.2 the group $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\langle\!\langle Q \rangle\!\rangle)$, where $\langle\!\langle Q \rangle\!\rangle$ is the S-ring over $\mathbb{Z}_{36}$ generated by Q. S-ring $\langle\!\langle Q \rangle\!\rangle$ is rational, hence by Theorem 5.1, $\langle\!\langle Q \rangle\!\rangle = \langle \underline{Z_d} \mid d \in L \rangle$ for a sublattice L of $L(36)$. After some simple reasonings we see that L is our sublattice in Figure 5. Thus

$$\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\langle\!\langle Q \rangle\!\rangle) = \mathrm{Aut}(L).$$

As shown in Example 9.2, the orthogonal block structure L is weekly isomorphic to the poset block structure $\mathcal{F}$ defined by the poset $N = ([4], \preceq)$ and sets $X_i = [n_i], i \in \{1, \ldots, 4\}$. Therefore, $\mathrm{Aut}(L)$ is permutation isomorphic to the group $\mathrm{Aut}(\mathcal{F})$. By Theorem 9.4, the latter group $\mathrm{Aut}(\mathcal{F}) = \prod_N S_{n_i}$ (we may get order once more using formula (6) as $|\prod_N S_{n_i}| = (3!)^3 \cdot (2!)^6 \cdot 3! \cdot 2! = 2^{11} \cdot 3^4$.) ∎

We converge with the consideration of our striking example. Simultaneously, in principle, the main goals of the paper are fulfilled. Combination of all presented results implies that the automorphism groups of rational circulant graphs are described by the groups as they appear in Theorem 9.4. Nevertheless, at this stage we are willing to justify much more precise formulation, as it is presented in the main Theorem 1.1, as well as to provide its self-contained proof.

10 Proof of Theorem 1.1

Let $P = ([r], \preceq)$ be a poset, and $n_1, \ldots, n_r$ be in $\mathbb{N}$ such that $n_i \geq 2$ for all $i \in \{1, \ldots, r\}$. We denote by $\mathsf{PBS}(P; n_1, \ldots, n_r)$ the poset block structure defined by P and the sets $[n_i]$. We recall that $P = ([r], \preceq)$ is increasing if $i \preceq j$ implies $i \leq j$ for all $i, j \in [r]$.

The final step toward Theorem 1.1 is the following statement.

Proposition 10.1.

(i) Let $P = ([r], \preceq)$ be an increasing poset and $n_1, \ldots, n_r$ be in $\mathbb{N}$ satisfying

(a) $n = n_1 \cdots n_r$,

(b) $n_i \geq 2$ for all $i \in \{1, \ldots, r\}$,

(c) $(n_i, n_j) = 1$ for all $i, j \in \{1, \ldots, r\}$ with $i \not\preceq j$.

Then $\mathsf{PBS}(P; n_1, \ldots, n_r)$ is weakly isomorphic to an orthogonal group block structure on $\mathbb{Z}_n$.

(ii) Let $\mathcal{F}$ be an orthogonal group block structure on $\mathbb{Z}_n$. Then exists an increasing poset $P = ([r], \preceq)$ and $n_1, \ldots, n_r$ in $\mathbb{N}$ satisfying (a)-(c) in (i) such that $\mathcal{F}$ is weakly isomorphic to $\mathsf{PBS}(P; n_1, \ldots, n_r)$.

To settle the proposition we first prove two preparatory lemmas. For $J \subset [r]$ we set the notation $\overline{J} = [r] \setminus J$.

Lemma 10.2. *Let $P = ([r], \preceq)$ be an increasing poset and $n_1, \ldots, n_r$ be in $\mathbb{N}$ satisfying (a)-(c) in (i) of Proposition 10.1. Then the set $L = \left\{ \prod_{j \in \overline{J}} n_j \mid J \in \operatorname{Anc}(P) \right\}$ is a sublattice of $L(n)$.* [1]

Proof. We prove the lemma by induction on r. If $r = 1$ then $L = \{1, n\}$. Suppose that $r > 1$ and let $n' = n_1 \cdots n_{r-1}$. Let $P' = ([r-1], \preceq)$ be the poset on $[r-1]$ induced by $\preceq$. The induction hypothesis applies to P' and numbers $n_1, \ldots, n_{r-1}$. Thus we get sublattice L_2 of $L(n')$ as

$$L_2 = \Big\{ \prod_{j \in \overline{J}} n_j \mid J \in \operatorname{Anc}(P') \Big\}.$$

[1] If $J \in \operatorname{Anc}(P)$ is the whole set $[r]$, then we set $\prod_{j \in \overline{J}} n_j = 1$.

Here by $\overline{J}$ we mean the complement of J in $[r-1]$.

Since P is increasing, r is a maximal element in P. Thus for any $J \subseteq [r-1]$,

$$J \in \mathrm{Anc}(P') \iff J \cup \{r\} \in \mathrm{Anc}(P). \tag{7}$$

Let $J_* = \{j \in [r-1] \mid j \not\preceq r\}$. Then $J_* \in \mathrm{Anc}(P)$. Further, for any $J \subseteq [r-1]$,

$$J \in \mathrm{Anc}(P) \iff J \in \mathrm{Anc}(P') \text{ and } J \subseteq J_*. \tag{8}$$

Put $d = \prod_{j \in \overline{J_*}} n_j$. Clearly, $d \in L_2$. Let $J \in \mathrm{Anc}(P')$ such that $d \mid \prod_{j \in \overline{J}} n_j$. Suppose that J is not contained in J_*, and pick an element $j \in J \cap \overline{J_*}$. Since $d \mid \prod_{j \in \overline{J}} n_j$, the weight n_j divides the product $\prod_{i \in J_* \setminus J} n_i$. This implies that there exsits a node $j' \in J_* \setminus J$ such that $n_{j'} \wedge n_j \neq 1$. Thus $j \preceq j'$ or $j' \preceq j$. Since J is ancestral, $j \in J$ and $j' \notin J$, we obtain that $j' \preceq j$. But, $j \notin J_*$, i.e., $j \preceq r$, implying that $j' \preceq r$, contradicting that $j' \in J_*$. We proved the following property.

$$\text{For any } J \in \mathrm{Anc}(P') \text{ if } d \mid \prod_{j \in \overline{J}} n_j, \text{ then } J \subseteq J_*. \tag{9}$$

Now, $n'/d = \prod_{j \in [r-1], j \not\preceq r} n_j$, hence condition (c) in (i) of Proposition 10.1 implies that $n'/d \wedge n_r = 1$. Thus we can use Definition 8.2 to form the crested product $L_1 \otimes_d L_2$, where $L_1 = \{1, n_r\}$. Then

$$\begin{aligned} L_1 \otimes_d L_2 &= \left\{ l_1 l_2 \mid l_1 = 1, l_2 \in L_2, \text{ or } l_1 \in L_1, l_2 \in L_2 \text{ with } d \mid l_2 \right\} \\ &= L_2 \cup \left\{ n_r l_2 \mid l_2 \in L_2 \text{ with } d \mid l_2 \right\}. \end{aligned}$$

Now, we use (7), (8) and (9) to find

$$\begin{aligned} L &= \left\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \text{ and } r \in J \right\} \cup \left\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \text{ and } r \notin J \right\} \\ &= L_2 \cup \left\{ l_2 n_r \mid l_2 \in L_2 \text{ with } d \mid l_2 \right\} = L_1 \otimes_d L_2. \end{aligned}$$

Thus L is a sublattice of $L(n)$, as required. ∎

We show next the converse to Lemma 10.2.

Lemma 10.3. *Let L be a sublattice of $L(n), n \geq 2$ such that $1, n \in L$. Then $L = \left\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \right\}$, where $P = ([r], \preceq)$ is an increasing poset and $n_1, \ldots, n_r$ are in $\mathbb{N}$ satisfying (a)-(c) in (i) of Proposition 10.1.*

Proof. We proceed by induction on n. The statement is clear if $L = \{1, n\}$. Suppose $L \neq \{1, n\}$, and let m be a maximal element in the poset induced by $L \setminus \{n\}$. Induction applies to sublattice $L_{[m]}$, and we can write

$$L_{[m]} = \left\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P') \right\}$$

with a suitable poset $P' = ([r-1], \preceq)$ and numbers $n_1, \ldots, n_{r-1}$ in $\mathbb{N}$. Now, let s be the smallest number in the set $L \setminus L_{[m]}$. Since $m \wedge s \in L_{[m]}$, we have a subset $J_* \in \mathrm{Anc}(P')$ for which $m \wedge s = \prod_{j \in \overline{J}_*} n_j$. Define the poset P on $[r]$ as the extension of P' to $[r]$ by setting $r \not\preceq x$ for all $x \in [r-1]$, and

$$x \preceq r \iff x \notin J_*.$$

We claim that P is the required poset and $n_1, \ldots, n_{r-1}, n_r = n/m$ are the required numbers.

First, poset P is obviously increasing, $n_1 \cdots n_r = n$, and $n_i \geq 2$ for all $i \in [r]$. Let $i, j \in [r]$ with $i < j$ and $i \not\preceq j$. It is clear that $n_i \wedge n_j = 1$ if $j \neq r$. Let $j = r$. Then

$$n_r = \frac{n}{m} = \frac{s}{m \wedge s}, \text{ and } \prod_{k \not\preceq r} n_k = \prod_{k \in J_*} n_k = \frac{m}{m \wedge s}.$$

This shows that $n_i \wedge n_r = 1$ holds as well, and so $n_1, \ldots, n_r$ satisfy (a)-(c) in (i) of Proposition 10.1.

By (7), (8) and (9),

$$\begin{aligned}
\Big\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \Big\} &= \Big\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \text{ and } r \in J \Big\} \cup \\
&\quad \Big\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \text{ and } r \notin J \Big\} \\
&= L_{[m]} \cup \big\{ x n_r \mid x \in (L_{[m]})^{[m \wedge s]} \big\}.
\end{aligned}$$

Now, we use Lemma 5.2 to conclude

$$L_{[m]} \cup \Big\{ x \frac{s}{m \wedge s} \mid x \in (L_{[m]})^{[m \wedge s]} \Big\} = L_{[m]} \cup (L \setminus L_{[m]}) = L.$$

∎

Proof of Proposition 10.1. Let $P = ([r], \preceq)$ be an increasing poset and $n_1, \ldots, n_r$ be in $\mathbb{N}$ satisfying (a)-(c) in (i) of Proposition 10.1. Let $L = \big\{ \prod_{j \in \overline{J}} n_j \mid J \in \mathrm{Anc}(P) \big\}$ be the sublattice of $L(n)$. In view of Lemmas 10.2 and 10.3 it remains to prove that $\mathsf{PBS}(P; n_1, \ldots, n_r)$ is weakly isomorphic to the orthogonal group block structure on $\mathbb{Z}_n$ defined by L.

Let $J \in \mathrm{Anc}(P)$, $J \neq [n]$, and $x_j, y_j \in [n_j]$ for each $j \in \overline{J}$. We claim that

$$\sum_{j \in \overline{J}} \Big(\prod_{i \in [r], i \not\preceq j} n_i \Big) x_j \equiv \sum_{j \in \overline{J}} \Big(\prod_{i \in [r], i \not\preceq j} n_i \Big) y_i \pmod{n} \implies \forall j \in \overline{J} : x_j = y_j. \tag{10}$$

We proceed by induction on r. Let $r = 1$. Then $J = \emptyset$, the assumption in (10) reduces to $x_1 \equiv y_1 \pmod{n}$ for $x_1, y_1 \in [n]$, and from this $x_1 = y_1$.

Let $r > 1$. Let $n' = n/n_r$ and P' be the poset induced by $[r-1]$. First, let $r \in J$, and put $J' = J \setminus \{r\}$. By (7), $J' \in \mathrm{Anc}(P')$. The assumption in (10) can be rewritten in the form

$$\sum_{j \in \overline{J'}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) n_r x_j \equiv \sum_{j \in \overline{J'}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) n_r y_i \pmod{n},$$

where $\overline{J'}$ is written for $[r-1] \setminus J'$. From this

$$\sum_{j \in \overline{J'}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) x_j \equiv \sum_{j \in \overline{J'}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) y_i \pmod{n'},$$

and hence, by induction, $x_j = y_j$ for each $j \in \overline{J'}$, and (10) holds. Second, let $r \notin J$. Put $n_r^* = \prod_{i \in [r], j \not\preceq r} n_j$. Notice that $n_r \wedge n_r^* = 1$ (see (c) in (i) of Proposition 10.1). The assumption in (10) can be rewritten as

$$\sum_{j \in \overline{J}, j \neq r} \Big(n_r \prod_{i \in [r-1], i \not\preceq j} n_i \Big) x_j + n_r^* x_r \equiv \sum_{j \in \overline{J}, j \neq r} \Big(n_r \prod_{i \in [r-1], i \not\preceq j} n_i \Big) y_i + n_r^* y_r \pmod{n}.$$

From this $n_r^*(x_r - y_r) \equiv 0 \pmod{n_r}$. And as $n_r \wedge n_r^* = 1$, $x_r = y_r$. By (8), $J \in \mathrm{Anc}(P')$. Regarded J as an ancestral subset of P', we find

$$\sum_{j \in \overline{J}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) x_j \equiv \sum_{j \in \overline{J}} \Big(\prod_{i \in [r-1], i \not\preceq j} n_i \Big) \pmod{n'}.$$

Thus, by induction, $x_j = y_j$ for each $j \in [r-1] \setminus J$, and so (10) holds.

Let $X = [n_1] \times \cdots \times [n_r]$. Define the mapping

$$f\colon X \to \mathbb{Z}_n,\ (x_i) \mapsto \sum_{i=1}^{r} \big(\prod_{j \in [r], j \not\preceq i} n_j \big) x_i \pmod{n}.$$

We claim that f is a weak isomorphism from $\mathsf{PBS}(P; n_1, \ldots, n_s)$ to L. First, that f is a bijection can be seen from (10) by substituting $J = \emptyset$. Let $J \in \mathrm{Anc}(P)$, and fix an element $(x_i) = (x_1, \ldots, x_r) \in X$. The class of $\Pi(J)$ containing (x_i) is the set

$$C = \big\{ \ (y_i) \in X \ \mid \ x_j = y_j \ \text{ for all } \ i \in J \ \big\}.$$

Put $m = \sum_{j \in J} \big(\prod_{i \in [r], i \not\preceq j} n_i \big) x_j$ in $\mathbb{Z}_n$. Then f maps the class C to the set

$$m + \Big\{ \ \sum_{j \in \overline{J}} \big(\prod_{i \in [r], i \not\preceq j} n_i \big) y_j \ \mid \ j \in \overline{J},\ y_j \in [n_j] \ \Big\}.$$

Observe that $i \not\preceq j$ for any $j \in \overline{J}$ and $i \in J$. Thus the product $\prod_{j \in J} n_j$ divides the numbers in the above set, and hence

$$m + \Big\{ \ \sum_{j \in \overline{J}} \big(\prod_{i \in [r], i \not\preceq j} n_i \big) y_j \ \mid \ j \in \overline{J},\ y_j \in [n_j] \ \Big\} \subseteq m + \big\langle \ \prod_{j \in J} n_j \ \big\rangle = m + Z_d,$$

where $d = \prod_{j\in\overline{J}} n_j$, and thus C is mapped into the coset $m + Z_d$. The number of classes of $\Pi(J)$ is equal to $\prod_{j\in J} n_j$, which is the index of Z_d in $\mathbb{Z}_n$. This together with the fact that f is a bijection imply that f maps C onto the coset $m + Z_d$, and so the partition $\Pi(J)$ to the coset-partition F_{Z_d}. This completes the proof of the proposition. ∎

Proof of Theorem 1.1.

$(i) \Rightarrow (ii)$ Let $\mathrm{Cay}(\mathbb{Z}_n, Q)$ be a rational circulant graph with $G = \mathrm{Aut}(\mathrm{Cay}\ (\mathbb{Z}_n, Q))$. By Corollary 6.4, $G = \mathrm{Aut}(\mathcal{F})$, where $\mathcal{F}$ is an orthogonal group block structure on $\mathbb{Z}_n$. By (ii) of Proposition 10.1, $\mathcal{F}$ is weakly isomorphic to the poset block structure $\mathsf{PBS}(P; n_1, \dots, n_r)$ for suitable poset $P = ([r], \preceq)$ and numbers $n_1, \dots, n_r$. Theorem 9.4 gives that G is permutation isomorphic to $\Pi_P S_{n_i}$.

$(ii) \Rightarrow (i)$ Let $G = \Pi_P S_{n_i}$, where $P = ([r], \preceq)$ is an increasing poset and $n_1, \dots, n_r$ are in $\mathbb{N}$ satisfying (a)-(c) in (ii) of Proposition 10.1. Because of Theorem 9.4 the group G equals the automorphism group of the poset block structure $\mathsf{PBS}(P; n_1, \dots, n_r)$. By (i) of Proposition 10.1, $\mathsf{PBS}(P; n_1, \dots, n_r)$ is weakly isomorphic to an orthogonal group block structure $\mathcal{F}$ on $\mathbb{Z}_n$, hence G is permutation isomorphic to $\mathrm{Aut}(\mathcal{F})$. Finally, Corollary 6.4 shows that there is a rational circulant graph $\mathrm{Cay}(\mathbb{Z}_n, Q)$ such that $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, Q)) = \mathrm{Aut}(\mathcal{F})$. ∎

11 Miscellany

We conclude the paper by a collection of miscellaneous topics related to rational circulant graphs and their automorphisms.

11.1 Enumeration of rational circulant graphs

Let $\mathrm{Cay}(\mathbb{Z}_n, Q)$ be a rational graph. By Theorem 4.1, Q follows to be the union of some of the sets

$$(\mathbb{Z}_n)_d = \{x \in \mathbb{Z}_n \mid \gcd(x, n) = d\},$$

where d is a divisor of n. Conversely, any set in such a form is a connection set of a rational graph. In particular, up to isomorphism, we have at most $2^{\tau(n)-1}$ rational Cayley graphs (without loops) over $\mathbb{Z}_n$.

To investigate, which of these graphs are pairwise non-isomorphic, we refer to the following Zibin's conjecture for arbitrary circulant graphs, which follows easily from the results in [89] (see also [95] and [96, Theorem 5.1]).

Theorem 11.1. (Zibin's conjecture.) *Let* $\mathrm{Cay}(\mathbb{Z}_n, Q)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, R)$ *be two isomorphic circulant graphs. Then for each* $d \mid n$ *there exists a multiplier* $m_d \in \mathbb{Z}_n^*$ *such that* $Q_d^{(m_d)} = R_d$.

Here for arbitrary subset $Q \subseteq \mathbb{Z}_n$, we define $Q_d = Q \cap (\mathbb{Z}_n)_d$.

Corollary 11.2. *Let* $\mathrm{Cay}(\mathbb{Z}_n, Q)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, R)$ *be two rational circulant graphs. Then these are isomorphic if and only if* $Q_d = R_d$ *for all* $d \mid n$*. Moreover, for each* $d \mid n$ *the common set* $Q_d = R_d$ *is equal to* $\emptyset$ *or to* $(\mathbb{Z}_n)_d$*.*

Corollary 11.3. *The number of non-isomorphic rational circulant graphs (without loops) of order* n *is* $2^{\tau(n)-1}$*, where* $\tau(n)$ *is the number of positive divisors of* n*.*

We should mention that the above statement was given as a conjecture by So [112, Conjecture 7.3].

Remark 1. We refer to the sequence A100577 (starting with $1, 2, 2, 4, 2, 8, 2, 8, 4, 8, 2, 32$) in the famous Sloane's On-Line Encyclopedia of Integer Sequences, see [98], which consists of the numbers $2^{\tau(n)-1}, n \in \mathbb{N}$.

Remark 2. For a given n let X be an arbitrary subset of the set $L(n) \setminus \{n\}$. Let $Q = \cup_{d \in X}(\mathbb{Z}_n)_d$, $\Gamma = \mathrm{Cay}(\mathbb{Z}_n, Q)$. Clearly, Γ is a presentation of an arbitrary rational circulant with n vertices. According to the presented theory, one may start with the simple quantity $\underline{Q}$ to construct the rational S-ring $\mathcal{A} = \langle\langle \underline{Q} \rangle\rangle$, and to express $\mathcal{A}$ with the aid of a suitable sublattice L of the lattice $L(n)$. Then $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(L)$. In Example 9.5 for X presented there the corresponding lattice L coincides with our striking sublattice.

A question of elaboration of a simple direct procedure to recognize L from an arbitrary subset X is of a definite independent interest, though it is out of the scope in the current text.

11.2 Association schemes

Though we have managed to arrange the main line of the presentation without the evident use of association schemes, it is now time to consider explicitly this concept.

Let X be a nonempty finite set, and let Δ_X denote the *diagonal relation* on X, i. e., $\Delta_X = \{(x, x) \mid x \in X\}$. For a relation $R \subseteq X \times X$, its *transposed* R^t is defined by $R^t = \{(y, x) \mid (x, y) \in R\}$. For a set $\{R_0, R_1, \ldots, R_d\}$ of relations on X the pair $\mathcal{X} = (X, \{R_0, \ldots, R_d\})$ is called an *association scheme* on X if the following axioms hold (see [14]):

(AS1) $R_0 = \Delta_X$, and $R_0, R_1, \ldots, R_d$ form a partition of $X \times X$.

(AS2) For every $i \in \{0, \ldots, d\}$ there exists $j \in \{0, \ldots, d\}$ such that $R_i^t = R_j$.

(AS3) For every triple $i, j, k \in \{0, \ldots, d\}$ and for $(x, y) \in R_k$, the number, denoted by $p_{i,j}^k$, of elements $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ does not depend on the choice of the pair $(x, y) \in R_k$.

The relations R_i are called the *basic relations* of $\mathcal{X}$, the corresponding graphs (X, R_i) the *basic graphs* of $\mathcal{X}$. The automorphism group of $\mathcal{X}$ is the permutation group

$$\mathrm{Aut}(\mathcal{X}) := \bigcap_{i=0}^{r} \mathrm{Aut}((X, R_i)).$$

Let $\mathcal{F}$ be an orthogonal block structure on X. For $F \in \mathcal{F}$, define the *color relation* C_F on X as

$$(x,y) \in C_F \iff F = \bigwedge \{E \in \mathcal{F} \mid (x,y) \in R_E\}.$$

It is immediately clear that for each $F \in \mathcal{F}$, C_F is a symmetric relation and the set of relations $\{C_F, F \in \mathcal{F}\}$ forms a partition of $X \times X$. It turns out that we can claim more.

The relational system $(X, \{C_F \mid F \in \mathcal{F}\})$ is a symmetric association scheme on X (see [9, Theorem 4]). Recall that in a *symmetric* association scheme $R_i^t = R_i$ for all $i \in \{0, 1, \dots d\}$. This we denote by $\mathrm{As}(\mathcal{F})$. Observe that, if $\mathcal{F}$ is the orthogonal group block structure on $\mathbb{Z}_n$ given in Proposition 6.3, then the color relations are $\widehat{R_l}$ defined in the proof of Proposition 6.3.

11.3 Schurity of rational S-rings over cyclic groups

Let $\mathcal{A}$ be a rational S-ring over $\mathbb{Z}_n$, and $\mathcal{F}$ be the corresponding orthogonal group block structure on $\mathbb{Z}_n$. Recall that $\mathcal{A}$ is Schurian if $\mathcal{A} = V(\mathbb{Z}_n, \mathrm{Aut}(\mathcal{A})_e)$. It is not hard to see that this is equivalent to saying that the basic relations of the association scheme $\mathrm{As}(\mathcal{F})$ are the 2-orbits of $\mathrm{Aut}(\mathcal{A})$, the latter group is the same as $\mathrm{Aut}(\mathcal{F}) = \mathrm{Aut}(\mathrm{As}(\mathcal{F})))$.

The following result is due to Bailey et al. (see [13, Theorem C]), which in particular also answers the Schurity of rational S-rings over $\mathbb{Z}_n$ in the positive.

Theorem 11.4. *Let $(I, \preceq)$ be a finite poset, X_i be a finite set of cardinality at least 2 for each $i \in I$, $X = \prod_{i \in I} X_i$, and $\mathcal{F}$ be the poset block structure on X defined by $(I, \preceq)$ and the sets X_i. Then the association scheme $\mathrm{As}(\mathcal{F})$ is Schurian, i. e., $\mathrm{As}(\mathcal{F}) = (X, \text{2-Orb}(\mathrm{Aut}(\mathrm{As}(\mathcal{F}))))$.*

Corollary 11.5. *Every rational S-ring over $\mathbb{Z}_n$ is Schurian.*

Let us remark that it has been conjectured that all S-rings over the cyclic groups $\mathbb{Z}_n$ are Schurian (known also as the Schur-Klin conjecture). The conjecture was denied recently by Evdokimov and Ponomarenko [35].

11.4 Simple reduction rules

We say that *simple reduction rules* apply to the group $\mathbb{Z}_n$ if every sublattice L of $L(n)$ such that $1, n \in L$, is obtained from trivial lattices via an iterative use of reduction rules 1 and 2. For instance, simple reduction rules apply to $\mathbb{Z}_{12}$, but not to $\mathbb{Z}_{36}$ (see the striking example). We already discussed informally which are the orders n that simple reduction rules apply to $\mathbb{Z}_n$.

The question is closely related to simple block structures introduced by Nelder [97]. Next we recall shortly the definition and some properties following [9].

For $i = 1, 2$, let F_i be a partition of a set X_i. Define the partition (F_1, F_2) of $X_1 \times X_2$ by setting the corresponding equivalence relation $R_{(F_1,F_2)}$ as

$$\big(\, (x_1,x_2), (y_1,y_2) \,\big) \in R_{(F_1,F_2)} \iff (x_1,y_1) \in R_{F_1} \wedge (x_2,y_2) \in R_{F_2}.$$

Let $\mathcal{F}_i$ be a block structure on X_i $(i = 1, 2)$. Their *crossing product* is the block structure on $X_1 \times X_2$ defined by

$$\mathcal{F}_1 * \mathcal{F}_2 = \big\{(F_1, F_2) \mid F_1 \in \mathcal{F}_1,\ F_2 \in \mathcal{F}_2\big\},$$

and their *nesting product* is the block structure on $X_1 \times X_2$ defined by

$$\mathcal{F}_1/\mathcal{F}_2 = \big\{(F_1, U_2) \mid F_1 \in \mathcal{F}_1\big\} \cup \big\{(E_1, F_2) \mid F_2 \in \mathcal{F}_2\big\}.$$

For the automorphism groups we have $\mathrm{Aut}(\mathcal{F}_1 * \mathcal{F}_2) = \mathrm{Aut}(\mathcal{F}_1) \times \mathrm{Aut}(\mathcal{F}_2)$, and $\mathrm{Aut}(\mathcal{F}_1/\mathcal{F}_2) = \mathrm{Aut}(\mathcal{F}_1) \wr \mathrm{Aut}(\mathcal{F}_2)$. Note that, if in addition both $\mathcal{F}_i$ are orthogonal, then so are $\mathcal{F}_1 * \mathcal{F}_2$ and $\mathcal{F}_1/\mathcal{F}_2$. The *trivial block* structure on a set X is the one formed by the partitions E_X and U_X. The *simple* orthogonal block structures are defined recursively as follows:

- Every trivial block structure is simple of depth 1.
- If for $i = 1, 2$, $\mathcal{F}_i$ is a simple orthogonal block structures of depth s_i on a set X_i, $|X_i| \geq 2$, then $\mathcal{F}_1 * \mathcal{F}_2$ and $\mathcal{F}_1/\mathcal{F}_2$ are simple orthogonal block structures of depth $s_1 + s_2$.

Clearly, if $\mathcal{F}$ is simple, then $\mathrm{Aut}(\mathcal{F})$ is obtained using iteratively direct or wreath product of symmetric groups. The equivalence follows.

Corollary 11.6. *Simple reduction rules apply to $\mathbb{Z}_n$ if and only if every orthogonal group block structure on $\mathbb{Z}_n$ is simple.*

Corollary 11.7. *Simple reduction rules apply to $\mathbb{Z}_n$ if and only if $n = pqr$, or $n = p^e q$, or $n = p^e$, where p, q and r are distinct primes.*

Proof. In view of the previous corollary we only need to check if there exists an orthogonal group block structure $\mathcal{F}$ on $\mathbb{Z}_n$ which is not simple. By Proposition 10.1, $\mathcal{F}$ is weakly isomorphic to $\mathsf{PBS}(P; n_1, \ldots, n_r)$, where $P = ([r], \preceq)$ is a non-increasing poset with suitable weights n_i. Let N be the poset given in part (i) of Figure 13. It is proved that $\mathcal{F}$ is not simple if and only if P contains a subposet isomorphic to N (see [9, pp. 64]). Let m_i, $1 \leq i \leq 4$, be the weights of this subposet. Then $m_1 m_2 m_3 m_4 \mid n$, and hence $n \neq pqr$ for distinct primes p, q and r. Let $n = p^e q$ or $n = p^e$. Then q appears as a factor in at most one of the numbers m_i, and so $(m_1, m_2) > 1$ or $(m_3, m_4) > 1$. This contradicts (c) in (ii) of Theorem 1.1. These yield implication '$\Leftarrow$' in the statement.

For implication '$\Rightarrow$' assume that n is none of the numbers $pqr, p^e q$, or p^e, where p, q and r are distinct primes. We leave for the reader to check that in this case it is possible to assign weights n_i to N satisfying (a)-(c) in (ii) of Theorem 1.1. The arising orthogonal group block structure on $\mathbb{Z}_n$ is therefore not simple, and by this the proof is completed. ∎

11.5 Style of the paper

This paper is deliberately intended for a quite wide audience: from graduate students to mature experts on one hand, and to readers working in many diverse areas of mathematics and its applications on the other hand. The established style of the paper necessarily implies that different readers may hopefully be satisfied by one facet of the presentation, while be concerned with other ones. Two concrete examples are mentioned below.

The reduction rules appear in the text in different level of rigor: from very naive and intuitive consideration of examples in Section 7 to a quite formal presentation in Section 11.4. Similarly, we believe that a student, having certain background in computational group theory, will enjoy the striking (in our eyes) exercise outlined in Example 7.4, while it is difficult to expect the same enthusiasm from a mature expert in abstract algebra.

Last but not least, it is worthy to mention that Section 10 is in a sense a “paper inside of the entire paper”. The reader with a high level of culture of mathematical formalisms in group theory may skip in the text a reasonable portion of material, besides Section 10.

12 Historical digest

This paper objectively carries certain interdisciplinary features. Indeed, the main concepts we discuss may be attributed to such areas as association schemes, S-rings, group theory, design of statistical experiments, spectral graph theory, lattice theory, etc. While for the authors there exists an evident natural impact of ideas borrowed from many diverse areas, it is difficult to expect similar experience from each interested reader. Nevertheless, at least brief acquaintance with the roots of the many facets of rational circulants, may create an extra helpful context for the reader. This is why we provide in the final section a digest of historical comments. We did not try to make it comprehensive, hoping to come once more in a forthcoming paper to discuss the plethora of all detected lines with more detail.

12.1 Schur rings

The concept of an S-ring goes back to the seminal paper of Schur [109], the abbreviation S-ring was coined and used by R. Kochendörfer and H. Wielandt [123]. For a few decades S-rings were used exclusively in permutation group theory in framework of very restricted area of interests. Books [110, 30] provide a nice framework, showing evolution in attention of modern experts to this concept. (Indeed, while S-rings occupy a significant position in [110], the authors of [30] avoid to use the term itself, though still present the background of the classical applications of S-rings to so-called B-groups, B stands for Burnside.)

On the dawn of algebraic graph theory, the interest to S-rings was revived due to their links with graphs and association schemes, admitting a regular group as a subgroup of the full automorphism group. In this context paper [27] by C. Y. Chao definitely deserves credit for pioneering contribution. More evident combinatorial applications of S-rings stem from [102, 67]. Tendencies of modern trends for attention to the use of S-rings in graph theory still are not clear enough. On one hand, a number of experts do not even try to hide their fearful feelings toward S-rings, regarding their ability to avoid "heavy use of Schur rings" (see [55]) as a definite positive feature of their presentation. On other hand, S-rings form a solid part of a background for high level monographs, though under alternative names like translation association scheme [25] or blueprint [10].

12.2 Schur rings over $\mathbb{Z}_n$

Practical application of established theory by Schur [109] originally was consideration of S-rings over finite cyclic groups. As a consequence, he proved that every primitive overgroup of a regular cyclic group of composite order n in symmetric group S_n is doubly transitive. Further generalizations of this result are discussed in [123]. Nowadays, the group theoretical results of such flavor are obtained with the aid of classification of finite simple groups (CFSG), see e. g. [83]. Schur himself did not try to describe all S-rings over $\mathbb{Z}_n$. First such serious attempt was done by Pöschel [102] on suggestion of L. A. Kalužnin, disciple of Schur. In [102] all S-rings over cyclic groups of odd prime-power order were classified. Classification of S-rings over group $\mathbb{Z}_{2^e}$ was fulfilled by joint efforts of Ja. Ju. Gol'fand, M. H. Klin, N. L. Naimark and R. Pöschel (1981-1985), see references in [96, 75]. First attempts of description of automorphism groups of circulants of order n, their normalizers in S_n and, as a result, a solution of isomorphism problem for circulants can be traced to [67]. K. H. Leung, S. L. Ma and S. H. Man reached complete recursive description of S-rings over $\mathbb{Z}_n$ in [80, 81, 82]. An alternative approach was established by Muzychuk, see e.g. [89, 90]. The results of Leung and Ma were rediscovered by S. A. Evdokimov and I. N. Ponomarenko [35]. In fact, in [35] a much more advanced result was presented: evident description of infinite classes of non-Schurian S-rings over $\mathbb{Z}_n$.

In 1967 A. Ádám [1] posed a conjecture: two circulants of order n are isomorphic if and only if they are conjugate with the aid of a suitable multiplier from $\mathbb{Z}_n^*$. A number of mathematicians more or less immediately presented diverse counterexamples to this conjecture. Nevertheless, a more refined question was formulated: for which values of n the conjecture is true, see [99] and references in it. A complete solution of this problem was given in [91]. Later on Muzychuk [92] provided a necessary and sufficient condition for two circulants of order n to be isomorphic. This monumental result (as well as previous publications) of Muzychuk is based on skillful combination of diverse tools, including deep use of S-rings. Schur rings were also used for the analytical enumeration of circulant graphs, see [66, 85]. Current ongoing efforts for the description of the automorphism groups of circulant graphs are also based on the use of S-rings. For n equal to odd prime-power and $n = 2^e$ the problem is completely solved, see [61, 62, 74, 68, 76]. A polynomial time algorithm which returns the automorphism group of an arbitrary circulant graph was recently constructed by Ponomarenko [103].

For about four decades investigation of Schur rings over cyclic groups is serving for generation of mathematicians as a challenging training polygon in development of algebraic graph theory. This supports the author's enthusiasm to further promote combinatorial applications of S-rings and to expose this theory to a wider audience.

12.3 Rational S-rings and integral graphs

Original name coined by Schur was S-ring of traces. It seems that Wielandt [123] was the first who suggested to use adjective rational for this class of S-rings. The complete rational S-ring $\mathcal{A}_n$ over $\mathbb{Z}_n$ appears as the transitivity module of the holomorph of $\mathbb{Z}_n$, which is isomorphic to $\mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. Its basic quantities are orbits of the multiplicative action of $\mathbb{Z}_n^*$ on $\mathbb{Z}_n$. It was already Schur who noticed that in a similar way $\mathbb{Z}_n^*$ acts multiplicatively on an arbitrary finite abelian group H of exponent n. Thus also in this case it is possible to consider the transitivity module of $H \rtimes \mathbb{Z}_n^*$. The resulting S-ring is exactly the complete rational S-ring over H. W. G. Bridges and R. A. Mena rediscovered in [23] (in a different context) the algebra $\mathcal{A}_n$ and exposed a lot of its significant properties. Only later on, in [24], they realized (due to hint of E. Bannai) existence of links of their generalization of $\mathcal{A}_n$ for arbitrary finite abelian groups with the theory of S-rings. A crucial contribution, exploited in [23, 24], was the use of the group basis in the complete rational S-ring over H. Implicitly or explicitly the algebras $\mathcal{A}_n$ and $V(H, \mathbb{Z}_n^*)$ were investigated later on again and again, basing on diverse motivation see e.g. [106, 46, 48, 15].

As was mentioned, Muzychuk's classification of rational S-rings over $\mathbb{Z}_n$ [88] forms a cornerstone for the background of the current paper. In turn, solutions for two particular cases, that is n is a prime-power [102] and n is square-free [48] created a helpful starting context for Muzychuk. Essential tools exploited in [88] are use of group basis and possibility to work with so-called pseudo-S-rings (those which do not obligatory include $\underline{e}$ and $\underline{H}$). In fact, pseudo-S-rings were used a long time ago by Wielandt [123]. This, in conjunction with the classical techniques of Schur ring theory, allows to obtain transparent proofs of main results. For example, Zibin's conjecture (and its particular case Toida's conjecture) were proved in [96] with the aid of S-rings based on earlier results of Muzychuk. An alternative approach developed in [31] depends on the use of CFSG.

F. Harary and A. J. Schwenk [50] suggested to call a graph Γ *integral* if every eigenvalue of Γ is integer. Since their pioneering paper a lot of interesting results about such graphs were obtained. A very valuable survey appears in [100, Chapter 5]. More fresh results are discussed in [120]. It was proved in [2] that integral graphs are quite rare, that is, only a fraction of $2^{-\Omega(n)}$ of the graphs on n vertices have an integral spectrum. Recent serious applications of integral graphs for designing the network topology of perfect state transfer networks (see e.g. references in [2]) imply new wave of interest to these graphs. In the context of the current paper, our interest to integral graphs is strictly restricted by regular graphs. A significant source of regular integral graphs is provided by basic graphs of symmetric association schemes and in particular by distance regular and strongly regular graphs [14, 25, 100]. A serious attempt to establish a more strict approach to algebraic properties of integral graphs is presented in [118]. Clearly, rational circulants form an interesting particular case of regular integral graphs. Investigation of these graphs usually is based on the amalgamation of techniques from number theory, linear algebra and combinatorics. Even a brief glance on such recent contributions as [112, 108, 2, 71] shows a promising potential to use for the same purposes also S-rings.

Let us now consider a very particular infinite series of rational circulants $X_n = \mathrm{Cay}(\mathbb{Z}_n, \mathbb{Z}_n^*)$, that is, the basic graph of the complete rational circulant association scheme, containing edge $\{0, 1\}$. As in [29], we will call such graphs *unitary* circulant graphs. Different facets of interest to the unitary circulants may be traced from [47, 70, 3, 105, 33]. A problem of description of $\mathrm{Aut}(X_n)$ was posed in [70] and solved in [3]. Clearly, the reader will understand that the answer was in fact known for a few decades in framework of the approach presented in this paper. Similarly, one sets complete answer on the Problem 2 from [70].

12.4 Designed experiments: a bridge from and to statisticians

I. Schur and R. C. Bose are now commonly regarded as the two most influential forrunners of the theory of association schemes, a significant part of algebraic combinatorics, see e.g. [14, 69, 10].

A geometer by initial training, Bose (1901-1987) was in a sense recruited by P. C. Mahalanobis to start from the scratch research in the area of statistics at a newly established statistical laboratory at Calcutta (now the Indian Statistical Institute). Fruitful influence of R. A. Fischer and F. Levi (during 1938 - 1943 and later on) turned out to become a great success not only for Bose himself, but also for all growing new area of mathematics, see [19]. As a result, within about two decades, theory of association schemes was established by Bose et al., see [21, 22, 20, 18] for most significant cornerstone contributions on this long way. Being in a sense a mathematical bilingual, Bose was perfectly feeling in the two areas which were created and developed via his very essential contributions: design of statistical experiments and association schemes.

Unfortunately, over the theory of association schemes was recognized as an independent area of mathematics, in particular after death of Bose, close links of algebraic combinatorics to experimental statistics became less significant, especially in the eyes of pure mathematicians. Sadly this divergence still continues. Nevertheless, mainly to the efforts of R. A. Bailey, a hope for the future reunion is becoming during the last years more realistic. The book [10] is the most serious messenger in this relation. Being also bilingual (Bailey got initial deep training in classical group theory), during last three decades she systematically promotes better understanding of foundations of association schemes by statisticians. Referring to [10] for more detail, we wish just to cite here such papers as [6, 114, 8] and especially [9].

These contributions, became in turn, very significant for pure mathematics. Indeed, initial ideas of Nelder [97], equivalent in a sense to the use of simple reduction rules, in hands of Bailey et al. were transformed to the entire theory of orthogonal partitions, group poset structures and crested products. Note also that our striking example appears in [10] as Example 9.1 in surprising clothes of designed experiment for bacteria search in a milk laboratory.

12.5 Lattices and finite topological spaces

For a square free number n Gol'fand established in [48] bijection between rational S-rings over $\mathbb{Z}_n$ and finite topologies on a k-element set, here n has exactly k distinct prime factors. This is a particular case of a bijection between rational S-rings over $\mathbb{Z}_n$ and sublattices of $L(n)$ for arbitrary n. Here we face another impact of diverse techniques from algebraic combinatorics, general algebra, group theory, experimental designs, etc. Such references as [116, 49, 17, 34, 73, 107, 101] provide a possibility to make a brief glance of the top of this iceberg. We pay also a particular attention to the theory of posets in its entire development, say from [115] to [117], with its own terminology, not obligatorily coinciding with the one in our paper.

12.6 Generalized wreath products

The operation of wreath product has a long history, which goes back to such names as A. Cauchy, C. Jordan, E. Netto and Gy. Pólya. E. Specht was one of the first experts who considered it in a rigorous algebraic context, see [113]. A new wave of interest and applications of wreath products was initiated by L. A. Kalužnin. The Kalužnin-Krasner Theorem (see [77]) is nowadays commonly regarded as a classical result in the beginning course of group theory. Less known is a calculus for iterated wreath product of cyclic groups, the outline of which was created by Kalužnin during the period 1941-45 (at the time he was imprisoned in a nazi concentration camp), see [119]. After the war the results, shaped mathematically, were reported on the Bourbaki seminar, and published in a series of papers, see e.g. [56]. A few decades later on this calculus was revived, extended and exploited in hands of L. A. Kalužnin, V. I. Sushchanskii and their disciples, cf. [59]. The notation, used in current paper is inherited from the texts of Kalužnin et al.

The generalized wreath product, the main tool in the reported project, was created independently, more or less at the same time by two experts. The approach of V. Feĭnberg (other spelling is Fejnberg) has purely combinatorial origins, first it was presented on the IX All Union Algebraic Colloquium (Homel, 1968, see [41]). Details are given in a series of papers [42, 43, 44, 45]. Feĭnberg traces roots of his approach to the ideas of Kalužnin [57]. The book [58] provides a helpful detailed source for the wide scope of diverse ideas, related to different versions of wreath products, its generalizations and applications. It seems that as an entity this stream of investigations is overlooked by modern experts.

W. Ch. Holland submitted his influential paper [52] on January 11, 1968. Though his interests are of a purely algebraic origin and the suggested operation is less general (in comparison with one considered by Feĭnberg), his ideas got much more lucky fate. The paper [52] is noticed already in [122] and exploited in spirit of group posets in [111] (both authors cite also [44]). It was Bailey who realized in [6] that the approach of Holland is well suited for the description of the automorphism groups of poset block structures. With more detail all necessary main ideas may be detected from [13], while [104, 26] stress extra helpful information. Our paper is strongly influenced by presentation in [10, 11].

12.7 Other products

The crucial input in [11] is that the generalized wreath product of permutation groups is considered in conjunction with the wreath product of association schemes, and lines between the two concepts are investigated. The crested product is a particular case of generalized wreath products, which may be alternatively explained in terms of iterated use of crested product. Note that the crested product for a particular case of S-rings was considered in [51] under the name *star product*. As we now are aware, the considered operations are enough in order to classify rational S-rings over cyclic groups.

A more general product operation, the wedge product of association schemes, was recently introduced and investigated in [93]. The term goes back to [81, 82], where it was used for a recursive classification of S-rings over cyclic groups. Muzychuk also investigates the automorphism groups of his wedge product of association schemes. It should be mentioned that, as observed in [93], the crested product for association schemes (and hence for S-rings) is reduced to tensor and wedge products.

In a similar situation Evdokimov and Ponomarenko [35] are speaking about wreath product of S-rings. The reader should notice that their terminology does not coincide with the one accepted in our paper. As the authors recently realized from [37], the approach developed by Evdokimov and Ponomarenko has its independent roots, which go back to the school of D. K. Faddeev at Leningrad. No doubt that in the future the history of all the exploited concepts must be investigated more carefully and systematically. Note also that Theorem 1.2 in [36] in conjunction with some results in [37] provides an independent background for the understanding of the structure of the automorphism groups of rational S-rings.

For a particular case of S-rings over cyclic groups of prime-power order these groups coincide with the subwreath product in a sense of [62, 68, 74, 76]. A few other operations over association schemes (semi-direct product and exponentiation) are also of a definite interest, see references in [93], though out of scope in this paper.

12.8 More references

It is a pleasure to admit that S-rings are proving their efficiency in algebraic graph theory. As was mentioned, sometimes they may substitute the use of CFSG. One more such example is provided by the classification of arc-transitive circulants. This problem was solved for a particular case in [124], and in general in [84]. Both papers rely on a description of 2-transitive groups (a well known consequence of CSFG). In fact, the entire result in [84] is a consequence of [89], the proof runs in the same fashion as the one for Zibin's conjecture. Note that, in fact the author of [84] does not cite [89], however, relies on a presentation in [35]. Moreover, the same text [35] was used e.g. in [92].

It is worth to mention that in [54] all doubly transitive groups, containing a regular cyclic subgroup, are classified, also with the aid of CFSG. We do not know if the same result may be obtained, avoiding the use of CFSG.

Below is a small sample of other situations when knowledge of S-ring theory turn out to be quite helpful.

- Rational circulants, satisfying $A^m = dI + \lambda J$ [78, 86].
- Isomorphisms and automorphisms of circulants [53, 60].
- Classification of distance regular circulants [87].
- Commuting decompositions of complete graphs [4].

For purely presentational purposes we also recall one more old example. Arasu et al. posed in [5] a question about the existence of a Payley type Cayley strongly regular graph Γ which does not admit regular elementary abelian subgroups of automorphisms. Such an example on 81 points was presented in [63] as a simple exercise via the use of rational S-ring over group $\mathbb{Z}_9^2$, it has automorphism group of order 1944. An infinite series of similar examples, using alternative techniques, was given [28], automorphism groups were not considered. Complete classification of such strongly regular graphs over $\mathbb{Z}_n^2$ with the aid of S-rings, is given in [79] for $n = p^k$. In our eyes the problem of classification of partial difference sets (that is, Cayley strongly regular graphs) over groups $\mathbb{Z}_n^2, n \in \mathbb{N}$ is a nice training task for innovative applications of S-rings and association schemes.

12.9 Concluding remarks

This project has been started in 1994 at the time of a visit of M. Klin to Freiburg. During years 1994-96 Klin was discussing with O. H. Kegel diverse aspects of the use of S-rings and simple reduction rules. These discussions as well as ongoing numerous conversations with Muzychuk shaped the format of the project. Starting from year 2003, Kovács joined Klin, and by year 2006, in principle, the full understanding of the automorphism groups of the rational circulants was achieved, and presented in [64]. At that time we became familiar with [12, 11] and were convinced that the crested products is a necessary additional brick which allows to create a clear and transparent vision of the entire subject. Finally, a more ambitious lead was attacked; the authors were striving to make presentation reasonably available to a wide mathematical audience. Our goal is not only to solve a concrete problem but also to promote use of S-rings and to stimulate interdisciplinary dialogue between the experts from diverse areas, who for many decades were working in a relative isolation, being not aware of the existence of worlds "parallel" to their efforts.

A preliminary version of this paper was published as preprint in arXiv (August 4, 2010), see [65]. Since that time a few new publications, related to the topic of the current presentation, became available, in particular [16, 72] and the above cited significant paper [37].

Acknowledgements

A visit of the second author at Ben-Gurion University of the Negev in November 2006 helped us to proceed with the paper, the second author thanks Ben-Gurion University of the Negev for supporting his trip. The authors are much obliged to Otto Kegel and

Misha Muzychuk for a long-standing fruitful cooperation. We thank Ilia Ponomarenko for helpful discussions and Andy Woldar for permanent stimulating interest to diverse facets of S-ring theory. We also thank Gareth Jones and Valery Liskovets for helpful remarks. Finally, we are much grateful to the anonymous referee, whose comprehensive report helped to improve the quality of the presentation.

References

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

[2] O. Ahmadi, N. Alon, I. F. Blake, and I. E. Shparlinski, Graphs with integral spectrum, *Linear Algebra Appl.* **430** (2009), 547–552.

[3] R. Akhtar, M. Bogess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel, and D. Pritikin, On the unitary Cayley graph of a finite ring, *Electron. J. Combin.* **16** (2009), R117.

[4] S. Akbari and A. Herman, Commuting decompositions of complete graphs, *J. Combin. Des.* **15** (2007), 133–142.

[5] K. T. Arasu, D. Jungnickel, S. L. Ma, and A. Pott, Strongly regular Cayley graphs with $\lambda - \mu = -1$, *J. Combin. Theory Ser. A* **67** (1994), 116–125.

[6] R. A. Bailey, Distributive block structures and their automorphisms, Combinatorial Mathematics VIII (K. L. McAvaney, ed.), Springer-Verlag, Berlin, Lecture Notes in Mathematics, Vol. 884 (1981), 115–124.

[7] R. A. Bailey, Quasi-complete Latin squares: construction and randomization, *J. Royal Stat. Soc., Ser. B* **46** (1984), 323–334.

[8] R. A. Bailey, Nesting and crossing in design, In *Encyclopedia of statistical sciences* (eds. S. Kotz and N. L. Johnson), J. Wiley, New York (1985), 181–185.

[9] R. A. Bailey, Orthogonal partitions in designed experiments, *Des. Codes Cryptogr.* **8** (1996), 45–77.

[10] R. A. Bailey, Association schemes. Designed experiments, algebra and combinatorics, Cambridge Studies in Advanced Mathematics, 84, Cambridge University Press, Cambridge 2004.

[11] R. A. Bailey, Generalized wreath product of association schemes, Europ. J. Combin. **27** (2006), 428–435.

[12] R. A. Bailey and P. J. Cameron, Crested products of association schemes, *J. London Math. Soc.* (2) **72** (2005), 1–24.

[13] R. A. Bailey, C. E. Praeger, C. A. Rowley and T. P. Speed, Generalized wreath products of permutation groups, *Proc. London Math. Soc.* **47** (1983), 69–82.

[14] E. Bannai and T. Ito, Algebraic combinatorics I: Association schemes, W. A. Benjamin, Menlo Park, CA 1984.

[15] S. Bang and S-Y. Song, Characterization of maximal rational circulant association schemes, In: Codes and designs (eds. K. T. Arasu and Á. Seress), Walter de Grujter, Berlin, New York, 2002, 37–48.

[16] M. Bašić and A. Ilić, On the automorphism group of integral circulant graphs, *Electronic J. Combin.* **18** (2011), #P68.

[17] R. Belding, Structures characterizing partially ordered sets, and their automorphism groups, *Discrete Math.* **27** (1979), 117–126.

[18] R. C. Bose, Strongly regular graphs, partial geometries and partially balanced designs, *Pacific J. Math.* **13** (1963), 389–419.

[19] R. C. Bose, Autobiography of a mathematical statistician, The making of statisticians (ed. J. Gani), Springer-Verlag, New York 1982.

[20] R. C. Bose and D. L. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Ann. Math. Statist.* **30** (1959), 21–38

[21] R. C. Bose and K. R. Nair, Partially balanced incomplete block designs, *Sankhya* **4** (1939), 337–372.

[22] R. C. Bose and T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two assiciate classes, *J. Amer. Stat. Assn.* **47** (1952), 151–84.

[23] W. G. Bridges and R. A. Mena, Rational circulants with rational spectra and cyclic strongly regular graphs, *Ars Combin.* **8** (1979), 143–161.

[24] W. G. Bridges and R. A. Mena, Rational G-matrices with rational eigenvalues, *J. Combin. Theory Ser. A* **108** (1982), 264–280.

[25] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin 1989.

[26] P. J. Cameron, Regular orbits of permutation groups on the power set, *Discrete Math.* **62** (1986), 307–309.

[27] C. Y. Chao, Some applications of a theorem of Schur to graphs and to a class of endomorphisms, *Portugal. Math.* **26** (1967), 505–523.

[28] J. A. Davis, Partial difference sets in p-groups, *Archiv Math.* **63** (1994), 103–110.

[29] I. J. Dejter and R. E. Giudici, On unitary Cayley graphs, *J. Combin. Math. Combin. Comput.* **18** (1995), 121–124.

[30] J. D. Dixon and B. Mortimer, Permutation Groups, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.

[31] E. Dobson and J. Morris, Toida's conjecture is true, *Electronic J. Combin.* **9** (1) (2002), R35.

[32] E. Dobson and J. Morris, On automorphism groups of circulant digraphs of square-free order, *Discrete Math.* **299** (2005), 79–98.

[33] P. A. Droll, A classification of Ramanujan unitary Cayley graphs, *Electronic. J. Combin.* **17** (2010), N29.

[34] V. Duquenne, What can lattices do for experimental designs, *Math. Social. Sci.* **11** (1986), 243–281.

[35] S. A. Evdokimov and I. N. Ponomarenko, On a family of Schur rings over a finite cyclic group, *St. Petersburg Math. J.* vol 13 (2002), No. 3, 1–11.

[36] S. A. Evdokimov and I. N. Ponomarenko, Schur rings over a product of Galois rings, preprint arXiv:0912.1559v2 [math.CO] (2009), http://arxiv.org/abs/0912.1559 (to appear in Algebra and Analysis, 2012).

[37] S. A. Evdokimov and I. N. Ponomarenko, Schurity of S-rings over a cyclic group and generalized wreath product of permutation groups, preprint arXiv:1012.5393v2 [math.CO] (2011), http://arxiv.org/abs/1012.5393.

[38] I. A. Faradžev, A. A. Ivanov, and M. H. Klin, Galois correspondence between permutation groups and cellular rings (association schemes), *Graphs and Combin.* **6** (1990), 303–332.

[39] I. A. Faradžev and M. H. Klin, Computer package for computations with coherent configurations, Proc. ISSAC-91, ACM Press (1991), 219–223.

[40] I. A. Faradžev, M. H. Klin, and M. E. Muzichuk, Cellular rings and automorphism groups of graphs, In Investigations on Algebraic Theory of Combinatorial Objects, Mathematics and its Applications (Soviet Series), vol. **84** (eds. I. A. Faradžev, A. A. Ivanov, M. H. Klin, A. J. Woldar), Kluwer Acad. Publ., 1994.

[41] V. Z. Feĭnberg, Automorphisms of some partially ordered sets and wreath products of groups, in: IX All-Union algebraic colloquium. Abstracts of talks, July 1968, Homel, 1968, pp. 191–192.

[42] V. Z. Feĭnberg, Unary algebras and their automorphism groups (in Russian), *DAN BSSR,* **13** (1969), 17–21.

[43] V. Z. Feĭnberg, Automorphism groups of tress (in Russian), *DAN BSSR,* **13** (1969), 1065–1967.

[44] V. Z. Feĭnberg, Wreath products of permutation groups with respect to partially ordered sets and filters (in Russian), *Vesci Akad. Navuk BSSR Ser. Fiz. Mat.* Navuk (1971), No. 6, 26–38.

[45] V. Z. Feĭnberg, On wreath product of semigroups of mappings by partially ordered sets and filters I, II (in Russian), *Vesci Akad. Navuk BSSR Ser. Fiz. Mat.* Navuk (1973), No. 1, 1–27; No. 3, 5–15.

[46] P. A. Ferguson and A. Turull, Algebraic decompositions of commutative association schemes, *J. Algebra* **96** (1985), 211–229.

[47] E. D. Fuchs, Longest induced cycles in circulant graphs, *Electron. J. Combin.* **12** (2005), RP52.

[48] Ja. Ju. Golfand, A description of subrings in $V(S_{p_1} \times \cdots \times S_{p_m})$, Investigations in the algebraic theory of combinatorical objects, Proc. Seminar Inst. System Studies,

Moscow, 1985, 65–76 (Russian); English trans. in: Investigations on algebraic theory of combinatorical objects, Mathematics and its applications (Soviet series) (Eds. I. A. Faradžev, A. A. Ivanov, M. H. Klin, A. J. Woldar), Kluwer Acad. Publ. **84** (1994), 209–223.

[49] L. H. Harper, The morphology of partially ordered sets, *J. Combin. Theory Ser. A* **17** (1974), 44–57.

[50] F. Harary and A. J. Schwenk, Which graphs have integral spectra? In *Graphs and combinatorics* (Ed. R. Bari and F. Harary), Springer-Verlag, Berlin, 1974, 45–51.

[51] M. Hirasaka and M. H. Muzychuk. An elementary abelian group of rank 4 is a CI-Group, *J. Combin. Theory Series A* **94** (2001), 339-362.

[52] W. C. Holland, The characterization of generalized wreath products, *J. Algebra* **13** (1969), 152–172.

[53] Q. X. Huang and J. X. Meng, On the isomorphisms and automorphism groups of circulants, *Graphs Combin.* **12** (1996), 179–187.

[54] G. Jones, Cyclic regular subgroups of primitive permutation groups, *J. Group Theory* **5** (4) (2002), 403–407.

[55] A. Joseph, The isomorphism problem for Cayley digraphs on groups of prime-squared order, *Discrete Math.* **141** (1995), 173–183.

[56] L. Kaloujnine, La structure des p-groupes de Sylow de groupes symetriques finis, *Ann. sci. École Normale Supérieure, Sér. 3* **65** (1948), 239–276.

[57] L. A. Kaluzhnin, A generalization of the Sylow p-subgroups of symmetric groups, *Acta. Math. Acad. Sci. Hungar.* **2** (1951), 197–221. (Russian; German summary)

[58] L. A. Kalužnin, P. M. Beleckij and V. Z. Fejnberg, Kranzprodukte, Teubner-Texte zur Matematik, B. G. Teubner, Leipzig 1987.

[59] L. A. Kaluzhnin and V. I. Sushchanskii, Wreath products of abelian groups, *Trudy Moskov. Mat. Obshch.* **29** (1973) 147–163; English trans. *Trans. Moscow Math. Soc.* **29** (1973).

[60] B. Kerby, Automorphism groups of Schur rings, preprint arXiv:0905.1898v1, http://arx- hiv.org/abs/0905.1898, 2009.

[61] M. H. Klin, Automorphism groups of circulant graphs, in: Tagungsbericht of the conference Applicable Algebra, Oberwolfach, 14–20 Februar, 1993, p. 12.

[62] M. H. Klin, Automorphism groups of p^m-vertex circulant graphs. The First China-Japan International Simposium on Algebraic Combinatorics. Beijing, October 11–15, 1994, Abstracts, 56–58.

[63] M. H. Klin, Rational S-rings over abelian groups, presented at the seminar in the University of Delaware, April 1994.

[64] M. H. Klin and I. Kovács, Automorphism groups of rational circulant graphs, In 1020th AMS meeting, American Mathematical Society, Ohio, USA, Abstracts, 2006, p. 41.

[65] M. H. Klin and I. Kovács, Automorphism groups of rational circulant graphs through the use of Schur rings, preprint arXiv:1008.0751v1 [math.CO] (2010), http://arxiv.org/abs/1008.0751.

[66] M. H. Klin, V. Liskovets and R. Pöschel, Analytical enumeration of circulant graphs with prime-squared number of vertices, *Sèm. Lotharing. Combin.* **36** (B36d) (1996), 1–36.

[67] M. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings, In: "Algebraic Methods in Graph Theory, Szeged, 1978", Colloq. Math. Soc. János Bolyai, Vol. 25, North-Holland, Amsterdam (1981), 405–434.

[68] M. Klin and R. Pöschel, Circulant graphs via Schur ring theory, II. Automorphism groups of circulant graphs on p^m vertices, p an odd prime, manuscript.

[69] M. Klin, Ch. Rücker, G. Rücker and G. Tinhofer, Algebraic combinatorics in mathematical chemistry. *Match.* **40** (1999), 7–138.

[70] W. Klotz and T. Sander, Some properties of unitary Cayley graphs, *Electronic. J. Combin.* **14** (2007), R45.

[71] W. Klotz and T. Sander, Integral Cayley graphs over abelian groups, *Electronic. J. Combin.* **17** (2010), R81.

[72] W. Klotz and T. Sander, Integral Cayley graphs defined by greatest common divisors, *Electronic. J. Combin.* **18** (2011), P94.

[73] Y. Koda, The numbers of finite lattices and finite topologies, *Bull. Inst. Combin. Appl.* **10** (1994), 83–89.

[74] I Kovács, On the automorphisms of circulants on p^m vertices, p an odd prime, *Linear Algebra Appl.* **356** (2002), 231–252.

[75] I. Kovács, The number of indecomposable S-rings over a cyclic 2-group, *Sèm. Lotharing. Combin.* **51** (2005), Article B51h.

[76] I. Kovács, A construction of the automorphism groups of indecomposable S-rings over Z_{2^n}, *Beiträge zur Algebra und Geometrie* **52** (2011), 83–103.

[77] M. Krasner and L. Kaloujnine, Produit complet des groupes de permutations et problème d'extension de groupes I, II, III, *Acta Sci. Math. Szeged* **13** (1950), 208–230; **14** (1951), 39–66, 69-82.

[78] C. W. H. Lam, On rational circulants satisfying $A^m = dI + \lambda J$, *Linear Algebra Appl.* **12** (1975), 139–150.

[79] Y. I. Leifman and M. E. Muzychuk, Strongly regular Cayley graphs over the group $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$, *Discrete Math.* **305** (2005), 219–239.

[80] K. H. Leung and S. L. Ma, The structure of Schur rings over cyclic groups, *J. Pure and Appl. Algebra* **66** (1990), 287–302.

[81] K. H. Leung and S. L. Man, On Schur rings over cyclic groups II, *J. Algebra* **183** (1996), 273–285.

[82] K. H. Leung and S. L. Man, On Schur rings over cyclic groups, *Israel J Math.* **106** (1998), 251–267.

[83] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc.* **87** (2003), 725–748.

[84] C. H. Li, Permutation groups with a cyclic regular subgroup and arc transitive circulants, *J. Algebraic Combin.* **21** (2005), 131–136.

[85] V. Liskovets and R. Pöschel, Counting circulant graphs of prime-power order by decomposing into orbit enumeration problems, *Discrete Math.* **214** (2000), 173–191.

[86] S. L. Ma, On rational circulants satisfying $A^m = dI + \lambda J$, *Linear Algebra Appl.* **62** (1984), 155–161.

[87] Š. Miklavič and P. Potočnik, Distance-regular circulants, *Europ. J. Combin.* **24** (2003), 777-784.

[88] M. E. Muzychuk, The structure of rational Schur rings over cyclic groups, *Europ. J. Combin.* **14** (1993), 479–490.

[89] M. E. Muzychuk, On the structure of basic sets of Schur rings over cyclic groups, *J. Algebra.* **169** (1994), no. 2., 655–678.

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

[91] M. Muzychuk, On Ádám's conjecture for circulant graphs, *Discrete Math.* **197** (1997), 285–298.

[92] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, *Proc. London Math. Soc.* (3) **88** (2004), 1–41.

[93] M. Muzychuk, A wedge product of association schemes, *Europ. J. Combin.* **30** (2009), 705–715.

[94] M. Muzychuk, Private communication.

[95] M. Muzychuk and R. Pöschel, Isomorphism criteria for circulant graphs, Technische Universität Dresden, Preprint MATH-AL-9-1999 (1999) 1–43.

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

[97] J. A. Nelder, The analysis of randomized experiments with orthogonal block structures, *Proc. Royal Soc., Ser. A,* Vol. **283** (1965), 147–178.

[98] The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences.

[99] P. P. Pálfy, Isomorphism problem for rational structures with a cyclic automorphism, *Europ. J. Combin.* **8** (1987), 35–43.

[100] M. Petrović and Z. Radosavljević, Spectrally constrained graphs, Faculty of Science, University of Kragujevac, 2001.

[101] G. Pfeiffer, Counting transitive relations, *J. Integer Sequences* **7** (2004), Article 04. 3. 2.

[102] R. Pöschel, Untersuchungen von S-ringen, insbesondere im Gruppring von p-Gruppen, *Math. Nachr.* **60** (1974), 1–27.

[103] I. N. Ponomarenko, Determination of the automorphism group of a circulant association scheme in polynomial time (Russian), Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **321** (2005), Vopr. Teor. Predst. Algebr. i Grupp. **12**, 251–267, 301; English trans. in: *J. Math. Sciences* **136** (2006), 3972–3979.

[104] C. E. Praeger, C. A. Rowley, T. P. Speed, A note on generalized wreath product, *J. Aust. Math. Soc. (Series A)* **39** (1985), 415–420.

[105] H. N. Ramaswamy and C. R. Veena, On the energy of unitary Cayley graphs, *Electron. J. Combin.* **16** (2009), N24.

[106] S. B. Rao, D. K. Ray-Chaudhuri, and N. M. Singhi, On imprimitive association schemes, Combinatorics and Applications (Calcutta, 1982), Indian Statist. Inst., Calcutta, 1984, 273–291.

[107] P. Renteln, On the enumeration of finite topologies, *J Combin. Inf. Syst. Sciences* **19** (1994), 201–206.

[108] N. Saxena, S Severini, and I. E. Shparlinski, Parameters of integral circulant graphs and periodic quantum dinamycs, *Int. J. Quant. Inf.* **5** (2007), 417–430.

[109] I. Schur, Zur Theorie der einfach transitiven Permutationsgruppen, *Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl.* (1933), 598–623.

[110] W. R. Scott. Group theory, Prentice-Hall, 1964.

[111] H. L. Silcock, Generalized wreath products and the lattice of normal subgroups of a group, *Algebra Universalis,* **7** (1977), 361–372.

[112] W. So, Integral circulant graphs, *Discrete Math.* **306** (2006), 153–158.

[113] W. Specht, Eine Verallgemeinerung der Permutationsgruppen, *Math. Z.* **37** (1933), 321–341.

[114] T. P. Speed and R. A. Bailey, On a class of association schemes derived from lattices of equivalence relations, In *Algebraic Structures and Applications* (eds. P. Schultz, C. E. Praeger and R. P. Sullivan), Marcell Dekker, New York (1982), 55–74.

[115] R. P. Stanley, Structure of incidence algebras and their automorphism groups, *Bull. Amer. Math. Soc.* **76** (1970), 1236–1239.

[116] R. P. Stanley, On the number of open sets in finite topologies, *J. Combin. Theory* **10** (1971), 74–79.

[117] R. P. Stanley, Enumerative combinatorics. Volume I, Cambridge studies in advance mathematics, v. 49., Cambridge University Press, 2002.

[118] D. Stevanović, N. M. M. de Abreu, M. M. A. de Freitas, and R. Del-Vecchio, Walks and regular integral graphs, *Linear Algebra Appl.* **423** (2007), 119–135.

[119] V. I. Sushchanskii, M. H. Klin, F. G. Lazebnik, R. Pöschel, V. A. Ustimenko, and V. A. Vyshenskii, Lev Arkad'evich Kalužnin (1914-1990), Algebra and combinatorics: interactions and applications, Königstein, 1994, *Acta Appl. Math.* **52** (1998), 5–18.

[120] L. Wang, A survey of results on integral trees and integral graphs, Memorandum. No. 1763, Department of Applied Mathematics, University of Twente, Twente (2005), 1–22.

[121] B. J. Weisfeiler (ed.), On construction and identification of graphs, Lecture Notes in Math. 558, Springer, Berlin 1976.

[122] C. Wells, Some applications of the wreath product construction, *Amer. Math. Monthly* **83** (1976), 317–338.

[123] H. Wielandt, Finite permutation groups, Academic Press, New York 1964.

[124] M. Y. Xu, Y-G. Baik, H-S. Sim, Arc-transitive circulant digraphs of odd prime-power order, *Discrete Math.* **287** (2004), 113–119.