A lower bound for the Weisfeiler-Leman dimension of circulant graphs

Yulai Wu[a] Qing Ren[b] Ilia Ponomarenko[c]

Submitted: Aug 22, 2025; Accepted: Jan 21, 2026; Published: Jun 5, 2026
© The authors. Released under the CC BY-ND license (International 4.0).

Abstract

It is proved that for infinitely many positive integers n, there exists a circulant graph of order n whose Weisfeiler-Leman dimension is at least $c\sqrt{\log n}$ for some constant $c > 0$ not depending on n.

Mathematics Subject Classifications: 20B99, 05E30

1 Introduction

By a circulant graph or a *circulant*, we mean a Cayley graph of a cyclic group. The history of the isomorphism problem for circulants goes back to the case of a group of prime order, studied in several papers in connection with the Ádám conjecture (see [27]). An effective criterion for testing isomorphism suggested by this conjecture has later been proved in [25] for cyclic groups of order n not divisible by 8 or an odd square. Namely, for any two subsets $X, Y \subseteq C_n$,

$$\mathrm{Cay}(C_n, X) \cong \mathrm{Cay}(C_n, Y) \quad \Leftrightarrow \quad Y \in X^{\mathrm{Aut}(C_n)} \tag{1}$$

where $X^{\mathrm{Aut}(C_n)} = \{X^\sigma : \sigma \in \mathrm{Aut}(C_n)\}$. The proof of this result and the results mentioned below are based on the method of Schur rings, first applied to the isomorphism problem for circulants in [20].

For an arbitrary positive integer n, the criterion (1) is not true. In two papers [11] and [26], the isomorphism problem for circulants was completely and independently solved by constructing polynomial-time (in n) algorithms. Although the technique used in these two papers was different, the common ground was the use of permutation groups. A natural generalization of this approach was a polynomial-time algorithm for testing isomorphism of circulant objects in an arbitrary concrete category [28].

[a]School of Mathematics and Statistics, Hainan University, Haikou, China (wuyl@hainanu.edu.cn).
[b]Guangxi Technological College of Machinery and Electricity, Nanning, China (renqing@gxcme.edu.cn). Corresponding author: Qing Ren.
[c]Steklov Institute of Mathematics at St. Petersburg, Russia (inp@pdmi.ras.ru).

In the mid-2000s, at a conference, one of the authors of this paper was asked to briefly describe the idea of an algorithm for testing isomorphism of circulants. This seemed like a difficult task, since the algorithms used (to varying degrees) both the theory of permutation groups and the theory of Schur rings. It was then that the question arose about the existence of a "purely combinatorial" polynomial-time algorithm that does not rely on algebraic methods. As a prototype of such an algorithm, it was natural to consider the multidimensional Weisfeiler-Leman algorithm, see [19].

For a positive integer m and an arbitrary graph $\mathcal{G}$ (directed or undirected), the m-dimensional Weisfeiler-Leman algorithm (m-dim WL algorithm) canonically constructs a special coloring of the m-tuples consisting of vertices of $\mathcal{G}$. Two given graphs are declared isomorphic if the resulting colorings do not distinguish these graphs; in this case, the graphs are said to be WL_m-*equivalent*. The algorithm works correctly if the WL_m-equivalence of the input graphs implies that they are isomorphic. The m-dim WL algorithm is the naive canonical vertex classification in the sense of [2] if $m = 1$, and is the classical Weisfeiler-Leman algorithm [31] if $m = 2$. As one of the key ingredient, the m-dim WL algorithm was used in the Babai quasipolynomial algorithm testing isomorphism of graphs [3].

Following [16], the Weisfeiler-Leman dimension (WL-*dimension*) $\dim_{\mathrm{WL}}(\mathcal{G})$ of a graph $\mathcal{G}$ is defined to be the smallest positive integer m such that any graph which is WL_m-equivalent to the graph $\mathcal{G}$ is isomorphic to $\mathcal{G}$. The isomorphism of any graph of order n and WL-dimension m with any other graph can be tested in time $O(n^{m+1}\log n)$. Now the question we started with can be reformulated as follows (see [29]): whether there exists a positive integer M such that $\dim_{\mathrm{WL}}(\mathcal{G}) \leqslant M$ for every circulant graph $\mathcal{G}$.

It is known that the WL-dimension of a general graph cannot be bounded from above by an absolute constant [4]. On the other hand, it was proved in [29] that if $\mathcal{G}$ is a circulant graph of prime power order, then $\dim_{\mathrm{WL}}(\mathcal{G}) \leqslant 3$. The main result of the present paper (Theorem 1 below) shows that the WL-dimension of a general circulant graph can be arbitrary large. To formulate this result, we refer to Section 10 for the exact definition of ε-expanders, and given a positive integer a, denote by $\mathfrak{B}_a$ the set of all bipartite cubic 3-connected graphs of order a.

Theorem 1. *Let $\varepsilon > 0$ be a real number, and let $a = 2b$ be a positive integer. Assume that there is an ε-expander belonging to $\mathfrak{B}_a$, and let $n = n_1 \cdots n_a$, where each n_i is a product of two distinct primes $\geqslant 5$ and the products $n_1 \cdots n_b$ and $n_{b+1} \cdots n_{2b}$ are coprime. Then there exists a circulant graph of order n the* WL*-dimension of which is at least $\lfloor c \cdot \sqrt{a} \rfloor$, where $c = c(\varepsilon)$ is a constant not depending on a and n.*

The construction underlying Theorem 1 leads to very large graphs. Indeed, for the smallest graph of WL-dimension 3 (the first interesting case) obtained from this construction, one must take $a = 10$ and, say $n_1 = \ldots = n_5 = 5 \cdot 7 = 35$, and $n_6 = \ldots = n_{10} = 11 \cdot 13 = 143$. Therefore, such a graph must have at least $(35 \cdot 143)^5$ vertices.

Graphs satisfying the conditions of Theorem 1 depend on the choice of the even positive integer a, an ε-expander belonging to $\mathfrak{B}_a$, and the numbers $n_1, \ldots, n_a$. It is known that

for any sufficiently large numbers a and a real number ε, there exist cubic ε-expanders [1]. However, we need them to be bipartite and 3-connected. The existence of such graphs can be deduced using the construction of cubic Ramanujan graphs in [23] (see the proof of Theorem 1). The restrictions on the choice of numbers are quite weak; in particular, they can be chosen so that the number n is square free. Thus the algorithm testing isomorphism of circulants on the base of the criterion (1) can be simulated by the m-dim WL algorithm for no constant m independent of n.

Corollary 2. *For infinitely many positive integers n, there exists a circulant graph of order n whose* WL*-dimension is at least $c\sqrt{\log n}$ for some constant $c > 0$ not depending on n.*

Following [33], we define the WL-dimension of a circulant $\mathcal{G}$ with respect to the class of all circulant graphs as the smallest positive integer m such that any circulant graph which is WL_m-equivalent to $\mathcal{G}$ is isomorphic to $\mathcal{G}$. It was proved in [33] that this "relative" WL-dimension of any circulant of order n is at most $O(\log n)$. The question of the tight asymptotic for the maximum relative WL-dimension of circulants remains open. As Corollary 2 shows, it is between $O(\sqrt{\log n})$ and $O(\log n)$.

We conclude the introduction with a brief discussion of the proof of Theorem 1. Our technique is based on theory of coherent configurations [5], see also Section 2. If $\mathcal{G}$ is a graph, then the output $\mathcal{X} = \mathrm{WL}(\mathcal{G})$ of the 2-dim WL-algorithm applied to $\mathcal{G}$ can naturally be viewed as a coherent configuration. The concept of the WL-dimension extends to coherent configurations such that

$$\dim_{\mathrm{WL}}(\mathcal{G}) = \dim_{\mathrm{WL}}(\mathcal{X}),$$

see Section 4. When the graph $\mathcal{G}$ is circulant, the coherent configuration $\mathcal{X}$ naturally corresponds to a Schur ring $\mathcal{A}$ over a cyclic group (a circulant S-ring), see Section 5. Now to find a circulant graph $\mathcal{G}$ with large $\dim_{\mathrm{WL}}(\mathcal{G})$, we construct in Section 9 a circulant S-ring $\mathcal{A}^\star$ such that the corresponding coherent configuration $\mathcal{X}^\star$ has two properties: (a) $\dim_{\mathrm{WL}}(\mathcal{X}^\star)$ is large, and (b) $\mathcal{X}^\star = \mathrm{WL}(\mathcal{G})$ for some circulant graph $\mathcal{G}$. The construction of $\mathcal{A}^\star$ (see below) enables us to verify property (b) more or less easily, see Subsection 10.2.

The construction of the S-ring $\mathcal{A}^\star$ satisfying condition (a) is more subtle. First, we use a theory of multipliers in circulant S-rings, that was developed in [14, 15], see also Section 6. This theory is applied to express the WL_m-equivalence of coherent configurations of circulant graphs in terms of *k-local systems of multipliers* of the corresponding circulant S-rings for $m < \sqrt{k}$, introduced and studied in Section 7. Thus our problem reduces to finding a circulant S-ring having a k-local system of multipliers for enough large k. An explicit construction of such an S-ring is given in Section 9 and is based on two ingredients defined in Section 8.

The first ingredient is a class of coherent configurations, introduced and studied in [9], see Subsection 8.1. For any cubic graph $\mathcal{G}$, one can define a coherent configuration $\mathcal{X} = \mathcal{X}(\mathcal{G})$ of this class so that: if $\mathcal{G}$ has a vertices, then $\mathcal{X}$ has $4a$ points, and if $\mathcal{G}$ is a 3-connected ε-expander, then

$$\dim_{\mathrm{WL}}(\mathcal{X}) \geqslant c' \cdot a \tag{2}$$

for some constant c' depending only on ε.

The second ingredient is a class consisting of special (circulant) S-rings $\mathcal{A}$ over cyclic groups of orders n satisfying the conditions of Theorem 1. The structure of $\mathcal{A}$ depends only on the number n, and is enough simple to describe all possible multipliers. In particular, if we fix a bipartite graph $\mathcal{G}$ from the previous paragraph, then isomorphisms of the coherent configuration $\mathcal{X}$ yield multipliers of $\mathcal{A}$. Now the required S-ring $\mathcal{A}^\star$ is the algebraic fusion of the S-ring $\mathcal{A}$ with respects to the multipliers corresponding the automorphisms of $\mathcal{X}$ (Subsection 9.2). Finally, the inequality (2) enables us to find a k-local system of multipliers of $\mathcal{A}^\star$ for $k = \lfloor c \cdot a \rfloor$ for some constant $c = c(\varepsilon)$.

2 Coherent configurations

In presenting coherent configurations, we follow the monograph [5], which can be consulted for unexplained details.

2.1 Notation

Throughout the paper, Ω denotes a finite set. For a set $\Delta \subseteq \Omega$, the Cartesian product $\Delta \times \Delta$ and its diagonal are denoted by $\mathbf{1}_\Delta$ and 1_Δ, respectively. If $\Delta = \{\alpha\}$, we abbreviate $1_\alpha := 1_{\{\alpha\}}$. For a relation $s \subseteq \mathbf{1}_\Omega$, we set $s^* = \{(\alpha, \beta) : (\beta, \alpha) \in s\}$, $\alpha s = \{\beta \in \Omega : \ (\alpha, \beta) \in s\}$ for all $\alpha \in \Omega$, and define $\langle s \rangle$ as the minimal (with respect to inclusion) equivalence relation on Ω, containing s. The *support* of s is defined to be the smallest set $\Delta \subseteq \Omega$ such that $s \subseteq \mathbf{1}_\Delta$.

For any collection S of relations or sets, we denote by $S^\cup$ the set of all unions of elements of S, and consider $S^\cup$ as a poset with respect to inclusion. The *dot product* of relations $r, s \subseteq \Omega \times \Omega$ is defined by the formula

$$r \cdot s := \{(\alpha, \beta) : \ (\alpha, \gamma) \in r, \ (\gamma, \beta) \in s \text{ for some } \gamma \in \Omega\}.$$

The set of classes of an equivalence relation e on Ω is denoted by Ω/e. For $\Delta \subseteq \Omega$, we set $\Delta/e = \Delta/e_\Delta$, where $e_\Delta = \mathbf{1}_\Delta \cap e$. If the classes of e_Δ are singletons, Δ/e is identified with Δ. Given a relation $s \subseteq \mathbf{1}_\Omega$, we put

$$s_{\Delta/e} = \{(\Gamma, \Gamma') \in \mathbf{1}_{\Delta/e} : \ s_{\Gamma,\Gamma'} \neq \varnothing\}, \tag{3}$$

where $s_{\Gamma,\Gamma'} = s \cap (\Gamma \times \Gamma')$, and abbreviate $s_\Gamma := s_{\Gamma,\Gamma}$. For a fixed s, the set of all equivalence relations e on Ω, such that $e \cdot s = s \cdot e = s$, contains the largest (with respect to inclusion) element which is denoted by $\mathrm{rad}(s)$ and called the *radical* of s. Obviously, $\mathrm{rad}(s) \subseteq \langle s \rangle$.

For a set B of bijections $f : \Omega \to \Omega'$, subsets $\Delta \subseteq \Omega$ and $\Delta' \subseteq \Omega'$, equivalence relations e and e' on Ω and Ω', respectively, we put

$$B^{\Delta/e, \Delta'/e'} = \{f^{\Delta/e} : \ f \in B, \ \Delta^f = \Delta', \ e^f = e'\},$$

where $f^{\Delta/e}$ is the bijection from Δ/e onto Δ'/e', induced by f; we also abbreviate $B^{\Delta/e} := B^{\Delta/e, \Delta'/e}$ if Δ' is clear from context.

By a tuple on Ω, we mean an m-tuple $x = (x_1, \dots, x_m)$ for some $m \geqslant 1$. We put $\Omega(x) := \{x_1, \dots, x_m\}$. For any $1 \leqslant k \leqslant m$, we put $\mathrm{pr}_k(x) = (x_1, \dots, x_k)$ and extend this notation to $\mathrm{pr}_k \mathscr{X}$ for all $\mathscr{X} \subseteq \Omega^m$.

For a finite group G and a set $X \subseteq G$, we treat $\underline{X} = \sum_{x \in X} x$ as an element of the group ring $\mathbb{Z}G$. We put $\mathrm{rad}(X) = \{g \in G : \ gX = Xg = X\}$, denote by $\langle X \rangle$ the subgroup of G generated by X, and set $X^{-1} = \{x^{-1} : \ x \in X\}$.

2.2 Coherent configurations

Let S be a partition of $\mathbf{1}_\Omega$. A pair $\mathcal{X} = (\Omega, S)$ is called a *coherent configuration* on Ω if

(CC1) $1_\Omega \in S^\cup$,

(CC2) $s^* \in S$ for all $s \in S$,

(CC3) given $r, s, t \in S$, the number $c_{rs}^t = |\alpha r \cap \beta s^*|$ does not depend on $(\alpha, \beta) \in t$.

The number $|\Omega|$ is called the *degree* of $\mathcal{X}$. A coherent configuration $\mathcal{X}$ is said to be *trivial* if $S = S(\mathcal{X})$ consists of 1_Ω and its complement (unless Ω is a singleton), *discrete* if S consists of singletons, and *homogeneous* or a *scheme* if $1_\Omega \in S$.

With any permutation group $G \leqslant \mathrm{Sym}(\Omega)$, one can associate a coherent configuration $\mathrm{Inv}(G) = (\Omega, S)$, where S consists of the relations $(\alpha, \beta)^G = \{(\alpha^g, \beta^g) : \ g \in G\}$ for all $\alpha, \beta \in \Omega$. A scheme $\mathcal{X}$ is said to be *regular* if $\mathcal{X} = \mathrm{Inv}(G)$, where the group G is regular, or equivalently, if $|\alpha s| = 1$ for all $\alpha \in \Omega$ and $s \in S$.

2.3 Isomorphisms and algebraic isomorphisms

A *combinatorial isomorphism* or, briefly, *isomorphism* from a coherent configuration $\mathcal{X} = (\Omega, S)$ to a coherent configuration $\mathcal{X}' = (\Omega', S')$ is defined to be a bijection $f : \Omega \to \Omega'$ such that $S^f = S'$. In this case, $\mathcal{X}$ and $\mathcal{X}'$ are said to be *isomorphic*; the set of all isomorphisms from $\mathcal{X}$ to $\mathcal{X}'$ is denoted by $\mathrm{Iso}(\mathcal{X}, \mathcal{X}')$, and by $\mathrm{Iso}(\mathcal{X})$ if $\mathcal{X} = \mathcal{X}'$. The group $\mathrm{Iso}(\mathcal{X})$ contains a normal subgroup

$$\mathrm{Aut}(\mathcal{X}) = \{f \in \mathrm{Sym}(\Omega) : \ s^f = s \text{ for all } s \in S\}$$

called the *automorphism group* of the coherent configuration $\mathcal{X}$.

A bijection $\varphi : S \to S'$ is called an *algebraic isomorphism* from $\mathcal{X}$ to $\mathcal{X}'$ if for all $r, s, t \in S$, we have

$$c_{\varphi(r)\varphi(s)}^{\varphi(t)} = c_{rs}^t.$$

In this case, $|\Omega'| = |\Omega|$ and $|S| = |S'|$. The set of all algebraic isomorphisms from $\mathcal{X}$ to $\mathcal{X}'$ is denoted by $\mathrm{Iso}_{alg}(\mathcal{X}, \mathcal{X}')$, and by $\mathrm{Aut}_{alg}(\mathcal{X})$ if $\mathcal{X} = \mathcal{X}'$.

Every combinatorial isomorphism $f \in \mathrm{Iso}(\mathcal{X}, \mathcal{X}')$ induces the algebraic isomorphism $\varphi_f : \mathcal{X} \to \mathcal{X}'$, $s \mapsto s^f$; we put

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

and abbreviate $\mathrm{Iso}(\mathcal{X}, \varphi) := \mathrm{Iso}(\mathcal{X}, \mathcal{X}, \varphi)$. Note that $\mathrm{Aut}(\mathcal{X}) = \mathrm{Iso}(\mathcal{X}, \mathrm{id}_\mathcal{X})$, where $\mathrm{id}_\mathcal{X}$ is the trivial (identical) algebraic automorphism of $\mathcal{X}$. If $\mathcal{X}$ is a regular scheme, then $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi) \neq \varnothing$ for any φ (see [5, Theorem 2.3.33]).

2.4 Relations and fibers

Let $\mathcal{X} = (\Omega, S)$ be a coherent configuration. The elements of S and of $S^\cup$ are called *basis relations* and *relations* of $\mathcal{X}$. The basis relation containing a pair $(\alpha, \beta) \in \mathbf{1}_\Omega$ is denoted by $r_\mathcal{X}(\alpha, \beta)$ or simply by $r(\alpha, \beta)$. The set of all relations of $\mathcal{X}$ is closed with respect to intersections, unions, and the dot product.

Any set $\Delta \subseteq \Omega$ such that $1_\Delta \in S$ is called a *fiber* of $\mathcal{X}$. In view of condition (CC1), the set $F = F(\mathcal{X})$ of all fibers forms a partition of Ω. Every basis relation is contained in the Cartesian product of two uniquely determined fibers.

Every algebraic isomorphism $\varphi \in \mathrm{Iso}_{alg}(\mathcal{X}, \mathcal{X}')$ can be extended in a natural way to a poset isomorphism $S^\cup \to (S')^\cup$, denoted also by φ; we have $1_{\Omega'} = \varphi(1_\Omega)$. This poset isomorphism respects the set theoretical operations and the dot product. Furthermore, φ induces a poset isomorphism $F^\cup \to (F')^\cup$ which preserves fibers. It takes a set Δ to the set Δ^φ, and is defined by the equality $\varphi(1_\Delta) = 1_{\Delta^\varphi}$.

2.5 Parabolics.

An equivalence relation e on a set $\Delta \subseteq \Omega$ is called a *partial parabolic* of the coherent configuration $\mathcal{X}$ if e is a relation of $\mathcal{X}$; if, in addition, $\Delta = \Omega$, then e is called a *parabolic* of $\mathcal{X}$. Note that the reflexive and transitive closure of any symmetric relation of $\mathcal{X}$ is a partial parabolic.

Let e be a partial parabolic on Ω, and let $\Delta \in \Omega/e$. Denote by $S_{\Omega/e}$ and S_Δ the sets of all non-empty relations

$$s_{\Omega/e} = \{(\Delta, \Gamma) \in \Omega/e \times \Omega/e : \ s_{\Delta,\Gamma} \neq \varnothing\} \quad \text{and} \quad s_\Delta = s_{\Delta,\Delta},$$

respectively, where $s \in S$. Then the pairs $\mathcal{X}_{\Omega/e} = (\Omega/e, S_{\Omega/e})$ and $\mathcal{X}_\Delta = (\Delta, S_\Delta)$ are coherent configurations called the *quotient* of $\mathcal{X}$ modulo e and *restriction* of $\mathcal{X}$ to Δ. Note that if $e = 1_\Delta$ for some $\Delta \in F^\cup$, then $\mathcal{X}_{\Omega/e} = \mathcal{X}_\Delta$.

Let $\varphi \in \mathrm{Iso}_{alg}(\mathcal{X}, \mathcal{X}')$ be an algebraic isomorphism and e a (partial) parabolic of $\mathcal{X}$. Then $\varphi(e)$ is a (partial) parabolic of $\mathcal{X}'$ with the same number of classes. Moreover,

$$\varphi(\langle s \rangle) = \langle \varphi(s) \rangle \quad \text{and} \quad \varphi(\mathrm{rad}(s)) = \mathrm{rad}(\varphi(s)). \tag{4}$$

The algebraic isomorphism φ induces the algebraic isomorphism

$$\varphi_{\Omega/e} : \mathcal{X}_{\Omega/e} \to \mathcal{X}'_{\Omega'/e'}, \ s_{\Omega/e} \mapsto s'_{\Omega'/e'}, \tag{5}$$

where $e' = \varphi(e)$ and $s' = \varphi(s)$. Now let $\Delta \in \Omega/e$ and $\Delta' \in \Omega/e'$. Assume that there is $\Gamma \in F$ such that $\Delta \cap \Gamma \neq \varnothing \neq \Delta' \cap \Gamma'$, where $\Gamma' = \Gamma^\varphi$. Then φ induces an algebraic isomorphism

$$\varphi_{\Delta,\Delta'} : \mathcal{X}_\Delta \to \mathcal{X}'_{\Delta'}, \ s_\Delta \mapsto s'_{\Delta'}. \tag{6}$$

This algebraic isomorphism always exists for all Δ and Δ' if $\mathcal{X}$ (and hence $\mathcal{X}'$) is a scheme.

2.6 Tensor and wreath product.

Let $\mathcal{X} = (\Omega, S)$ and $\mathcal{X}' = (\Omega', S')$ be two coherent configurations. Denote by $S \otimes S'$ the set of all relations

$$s \otimes s' = \left\{((\alpha, \alpha'), (\beta, \beta')) \in (\Omega \times \Omega')^2 : \ (\alpha, \beta) \in s, \ (\alpha', \beta') \in s'\right\},$$

where $s \in S$ and $s' \in S'$. Then the pair $\mathcal{X} \otimes \mathcal{X}' = (\Omega \times \Omega', S \otimes S')$ is a coherent configuration called the *tensor product* of $\mathcal{X}$ and $\mathcal{X}'$. One can easily prove that $\mathrm{Aut}(\mathcal{X} \times \mathcal{X}') = \mathrm{Aut}(\mathcal{X}) \times \mathrm{Aut}(\mathcal{X}')$.

Assume that the coherent configurations $\mathcal{X}$ and $\mathcal{X}'$ are schemes. Denote by T and T' the sets of all relations

$$s \otimes 1_{\Omega'}, \ s \in S, \qquad \text{and} \qquad \mathbf{1}_\Omega \otimes s', \ 1_{\Omega'} \neq s' \in S',$$

respectively. Then the pair $\mathcal{X} \wr \mathcal{X}' = (\Omega \times \Omega', T \cup T')$ is also a scheme. It is called the *wreath product* of $\mathcal{X}$ and $\mathcal{X}'$. The mapping $\mathrm{Aut}(\mathcal{X} \wr \mathcal{X}') \to \mathrm{Aut}(\mathcal{X}')$, $f \mapsto f^{\Omega'}$, is an epimorphism the kernel of which is equal to the direct product of $|\Omega'|$ copies of the group $\mathrm{Aut}(\mathcal{X})$.

3 Binary schemes

In the proof of our main result, we will need schemes for which every "correct" bijection between point tuples of bounded arity lifts to an automorphism. The automorphism groups of these schemes are the binary permutation groups in sense of [7].

Let $\mathcal{X}$ be a scheme on Ω. For any integer $m \geqslant 1$ and a tuple $x \in \Omega^m$, we define the $m \times m$ array

$$R_{\mathcal{X},m}(x) = (r_{\mathcal{X}}(x_i, x_j) : \ 1 \leqslant i, j \leqslant m). \tag{7}$$

The scheme $\mathcal{X}$ is said to be *binary* if for any m and any two tuples $x, y \in \Omega^m$ such that $R_{\mathcal{X},m}(x) = R_{\mathcal{X},m}(y)$, there exists an automorphism of $\mathcal{X}$, that takes x to y. In this case, the group $\mathrm{Aut}(\mathcal{X})$ is transitive, and acts transitively on each basis relation of $\mathcal{X}$.

The main goal of this section is to prove that any scheme constructed from regular schemes using tensor and wreath products is binary.

Theorem 3. *The class of binary schemes contains all regular schemes and is closed with respect to tensor and wreath products.*

Proof. Below, $\mathcal{X}$ is a scheme on Ω, $m \geqslant 1$ is an integer, and $x, y \in \Omega^m$ are such that the arrays $R(x)$ and $R(y)$ with $R = R_{\mathcal{X},m}$ are equal. First, assume that the scheme $\mathcal{X}$ is regular (see Subsection 2.2). Then there exists a unique automorphism $f \in \mathrm{Aut}(\mathcal{X})$ such that ${x_1}^f = y_1$. Let $1 \leqslant i \leqslant m$. By the assumption, y_i is the unique point for which $r(x_1, x_i) = r(y_1, y_i)$, where $r = r_{\mathcal{X}}$. Since $r(x_1, x_i)^f = r(y_1, x_i^f)$, this shows that $y_i = {x_i}^f$. Thus $y = x^f$ and $\mathcal{X}$ is binary.

Let $\mathcal{X} = \mathcal{X}_1 \otimes \mathcal{X}_2$, where $\mathcal{X}_1$ and $\mathcal{X}_2$ are binary schemes on Ω_1 and Ω_2, respectively. Denote by $\mathrm{pr}_i : \Omega_1 \times \Omega_2 \to \Omega_i$ the natural projection, $i = 1, 2$. Identifying in a natural way

the sets $(\Omega_1 \times \Omega_2)^m$ and $\Omega_1^m \times \Omega_2^m$, we can write $x = (\mathrm{pr}_1 x, \mathrm{pr}_2 x)$ and $y = (\mathrm{pr}_1 y, \mathrm{pr}_2 y)$. By the definition of tensor product, we have

$$R_1(\mathrm{pr}_1 x) = R_1(\mathrm{pr}_1 y) \quad \text{and} \quad R_2(\mathrm{pr}_2 x) = R_2(\mathrm{pr}_2 y),$$

where $R_1 = R_{\mathcal{X}_1,m}$, and $R_2 = R_{\mathcal{X}_2,m}$. Since the scheme $\mathcal{X}_i$ is binary, there exists an automorphism $f_i \in \mathrm{Aut}(\mathcal{X}_i)$ such that $\mathrm{pr}_i y = (\mathrm{pr}_i x)^{f_i}$, $i = 1, 2$. It follows that the permutation $f := (f_1, f_2)$ of $\Omega_1 \times \Omega_2$ belongs to the group $\mathrm{Aut}(\mathcal{X}_1) \times \mathrm{Aut}(\mathcal{X}_2) = \mathrm{Aut}(\mathcal{X})$. Thus,

$$x^f = (\mathrm{pr}_1 x, \mathrm{pr}_2 x)^{(f_1,f_2)} = ((\mathrm{pr}_1 x)^{f_1}, (\mathrm{pr}_2 x)^{f_2}) = (\mathrm{pr}_1 y, \mathrm{pr}_2 y) = y,$$

and the scheme $\mathcal{X}$ is binary.

Now let $\mathcal{X} = \mathcal{X}_1 \wr \mathcal{X}_2$. Then $e = \mathbf{1}_{\Omega_1} \otimes 1_{\Omega_2}$ is a parabolic of the scheme $\mathcal{X}$. Each class of e is of the form $\bar{\alpha} = \Omega_1 \times \{\alpha\}$, where $\alpha \in \Omega_2$. The bijection $\Omega_2 \to \Omega/e$, $\alpha \mapsto \bar{\alpha}$, $\alpha \in \Omega_2$, is an isomorphism from the scheme $\mathcal{X}_2$ to the quotient scheme $\bar{\mathcal{X}} = \mathcal{X}_{\Omega/e}$; in particular, the scheme $\bar{\mathcal{X}}$ is binary.

$$\bar{R}(\bar{x}) = \bar{R}(\bar{y}),$$

where $\bar{R} = R_{\bar{\mathcal{X}},m}$, $\bar{x} = (\overline{x_1}, \dots, \overline{x_m})$, and $\bar{y} = (\overline{y_1}, \dots, \overline{y_m})$. Thus there exists an automorphism $\bar{f} \in \mathrm{Aut}(\bar{\mathcal{X}})$ such that $\bar{y} = \bar{x}^{\bar{f}}$. Because the natural homomorphism $\mathrm{Aut}(\mathcal{X}) \to \mathrm{Aut}(\bar{\mathcal{X}})$ is surjective (see [5, Theorem 3.4.6.]), one can find an automorphism $g \in \mathrm{Aut}(\mathcal{X})$ such that $g^{\Omega/e} = \bar{g}$. Replacing x by x^g and taking into account that $R(x^g) = R(x)$, we may assume that

$$\overline{x_i} = \overline{y_i}, \qquad i = 1, \dots, m. \tag{8}$$

Let $\Delta \in \Omega/e$. Let the integer $k \geqslant 1$ and indices $1 \leqslant i_1 < \dots < i_k \leqslant m$ be such that $\{x_{i_1}, \dots x_{i_k}\} = \Omega(x) \cap \Delta$. Put $x_\Delta = (x_{i_1}, \dots, x_{i_k})$. In a similar way, we define the integer $\ell \geqslant 1$ and ℓ-tuple y_Δ. Since $R(x) = R(y)$, formula (8) implies that $k = \ell$ and

$$R_\Delta(x_\Delta) = R_\Delta(y_\Delta),$$

where $R_\Delta = R_{\mathcal{X}_\Delta,k}$. Because the scheme $\mathcal{X}_\Delta = \mathcal{X}_1$ is binary, there exists an automorphism $f_\Delta \in \mathrm{Aut}(\mathcal{X}_\Delta)$ such that $y_\Delta = (x_\Delta)^{f_\Delta}$. Let us define a permutation $f \in \mathrm{Sym}(\Omega)$ such that $f^\Delta = f_\Delta$ for all $\Delta \in \Omega/e$. Then obviously $x^f = y$. To complete the proof, it remains to note that $f \in \mathrm{Aut}(\mathcal{X})$, because the kernel of the homomorphism $\mathrm{Aut}(\mathcal{X}) \to \mathrm{Aut}(\overline{\mathcal{X}})$ coincides with the direct product of $|\Omega/e|$ copies of the group $\mathrm{Aut}(\mathcal{X}_\Delta)$. □

4 WL-dimension of graphs and coherent configurations

4.1 Definitions

Let $\mathscr{R}$ be a linear ordered set of binary relations on Ω, and let $m \geqslant 1$ be an integer. The Weisfeiler-Leman algorithm (the m-dim WL) constructs a coloring $c = c_{m,\mathscr{R}}$ assigning a color $c(x)$ to each m-tuple $x \in \Omega^m$. The coloring is canonical in the sense that for any bijection $f : \Omega \to \Omega'$, the induced bijection $\Omega^m \to \Omega'^m$ takes the coloring $c_{m,\mathscr{R}}$ to the

coloring $c_{m,\mathscr{R}'}$, where $\mathscr{R}' = \{s^f : s \in \mathscr{R}\}$. More details (including the exact definition of the m-dim WL) can be found in [16] (see also [18]).

The color classes of the coloring $c_{m,\mathscr{R}}$ form a partition $\mathrm{WL}_m(\mathscr{R})$ of the Cartesian power Ω^m,[1] which is an m-ary coherent configuration in the sense of [3]; for $m = 2$, the m-ary coherent configurations are just the coherent configurations in the sense of Subsection 2.2. We do not need to give here the exact definition of m-ary coherent configurations or their algebraic isomorphisms; the interested reader can find them in [29, Section 3]. Let us make just a few remarks about projections.

Let $\mathfrak{X}$ be an m-ary coherent configuration and $1 \leqslant k \leqslant m$. The collection of the projections $\mathrm{pr}_k\, \mathscr{X}$, $\mathscr{X} \in \mathfrak{X}$, forms a partition of Ω^k, that is a k-ary coherent configuration; we denote it by $\mathrm{pr}_k\, \mathfrak{X}$. The projections are respected by algebraic isomorphisms. More precisely, any algebraic isomorphism $\widehat{\varphi} : \mathfrak{X} \to \mathfrak{X}'$ of m-ary coherent configurations induces the algebraic isomorphism $\widehat{\varphi}_k : \mathrm{pr}_k\, \mathfrak{X} \to \mathrm{pr}_k\, \mathfrak{X}'$ of k-ary coherent configurations such that $\mathrm{pr}_k\, \widehat{\varphi}(\mathscr{X}) = \widehat{\varphi}_k(\mathrm{pr}_k\, \mathscr{X})$ for all $\mathscr{X} \in \mathfrak{X}$.

At this point, we assume that $m \geqslant 2$. For a (2-ary) coherent configuration $\mathcal{X}$, denote by $\mathrm{WL}_m(\mathcal{X})$ the m-ary coherent configuration $\mathrm{WL}_m(\mathscr{R})$ with $\mathscr{R} = S(\mathcal{X})$. Following [29], we say that two coherent configurations $\mathcal{X}$ and $\mathcal{X}'$ are WL_m-*equivalent* with respect to an algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$ if there exists an algebraic isomorphism $\hat{\varphi} : \mathrm{WL}_m(\mathcal{X}) \to \mathrm{WL}_m(\mathcal{X}')$ such that its 2-projection $\hat{\varphi}_2$ extends φ, i.e., $\hat{\varphi}_2(s) = \varphi(s)$ for all $s \in S(\mathcal{X})$. (Note that we always have $\mathrm{pr}_2\, \mathrm{WL}_m(\mathcal{X}) \geqslant \mathcal{X}$ and $\mathrm{pr}_2\, \mathrm{WL}_m(\mathcal{X}') \geqslant \mathcal{X}'$.)

The m-dim WL algorithm *identifies* a coherent configuration $\mathcal{X}$ if for any algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$ with respect to which $\mathcal{X}$ and $\mathcal{X}'$ are WL_m-equivalent, the set $\mathrm{Iso}(\mathcal{X}, \mathcal{X}', \varphi)$ is not empty. The WL-*dimension* $\dim_{\mathrm{WL}}(\mathcal{X})$ of the coherent configuration $\mathcal{X}$ is defined to be the smallest positive integer $m \geqslant 2$ such that the m-dim WL algorithm identifies $\mathcal{X}$.

With any graph $\mathcal{G}$, we associate the coherent configuration $\mathrm{WL}(\mathcal{G}) = \mathrm{WL}_2(\mathscr{R})$, where the set $\mathscr{R}$ is the singleton consisting of the edge set of $\mathcal{G}$. Let us define the WL-dimension of $\mathcal{G}$ by the formula

$$\dim_{\mathrm{WL}}(\mathcal{G}) = \dim_{\mathrm{WL}}(\mathrm{WL}(\mathcal{G})). \tag{9}$$

It should be noted that our definition of the WL-dimension of a graph differs somewhat from the generally accepted one. However, both definitions give the same value of the WL-dimension when the graph in question is of WL-dimension at least 2 in the conventional sense. Therefore, the difference in the definitions of the WL-dimension does not affect the validity of the main result of our paper.

4.2 Pebble games

It is convenient to express the WL_m-equivalence of coherent configurations $\mathcal{X}$ and $\mathcal{X}'$ with respect to an algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$ in terms of the pebbling game $\mathscr{C}_m(\varphi)$, see [6, 33]. The idea and the main result of this subsection go back to a fundamental paper [4].

[1] Though the coloring $c_{m,\mathscr{R}}$ depends on the linear order of $\mathscr{R}$, the partition $\mathrm{WL}_m(\mathscr{R})$ does not.

There are two players, called Spoiler and Duplicator, and m pairwise distinct pebbles, each given in duplicate. The game consists of rounds and each round consists of two parts. At the first part, Spoiler chooses a set A' of points belonging to $\mathcal{X}$ or $\mathcal{X}'$. Duplicator responds with a set A in the other coherent configuration, such that $|A| = |A'|$ (if this is impossible, then Duplicator loses). At the second part, Spoiler places one of the pebbles[2] on a point in A. Duplicator responds by placing the copy of the pebble on some point of A'.

The configuration after a round is determined by a bijection $f : \Delta \to \Delta'$, where $\Delta \subseteq \Omega$ (respectively, $\Delta' \subseteq \Omega'$) is the set of points in $\mathcal{X}$ (respectively, in $\mathcal{X}'$), covered by pebbles, and any two points $\alpha \in \Delta$ and $\alpha^f \in \Delta'$ are covered by the copies of the same pebble. Duplicator wins the round if

$$(s_\Delta)^f = \varphi(s)_{\Delta'}$$

for all basis relations $s \in S$ such that $s_\Delta \neq \varnothing$. Spoiler wins if Duplicator does not win.

The game starts from an initial configuration (which is considered as the configuration after zero rounds), i.e., a pair $(x, x') \in \Omega^k \times \Omega'^k$ for which $k \leqslant m$ and the points x_i and x'_i are covered with copies of the same pebble, $i = 1, \ldots, k$. We say that Duplicator has a winning strategy for the game $\mathscr{C}_m(\varphi)$ on $\mathcal{X}$ and $\mathcal{X}'$ with initial configuration (x, x') if, regardless of Spoiler's actions, Duplicator wins after any number of rounds.

Lemma 4. *Let $\mathcal{X}$ and $\mathcal{X}'$ be coherent configurations on, respectively, Ω and Ω', and let $\varphi : \mathcal{X} \to \mathcal{X}'$ be an algebraic isomorphism. Assume that an integer $m \geqslant 2$ and a bijection $f : \Omega^m \to \Omega'^m$ are such that for each $x \in \Omega^m$, Duplicator has a winning strategy in the game $\mathscr{C}_{m+1}(\varphi)$ on $\mathcal{X}$ and $\mathcal{X}'$ with initial configuration (x, x'), where $x' = x^f$. Then $\mathcal{X}$ and $\mathcal{X}'$ are WL_m-equivalent with respect to φ.*

Proof. Let $T \subseteq \Omega^m \times \Omega'^m$ consist of all pairs (x, x') such that Duplicator has a winning strategy in the pebble game $\mathscr{C}_{m+1}(\varphi)$ on $\mathcal{X}$ and $\mathcal{X}'$ with initial configuration (x, x'). By the assumption, T contains each pair (x, x^f), $x \in \Omega^m$. Since f is a bijection, the relation T has full support. This completes the proof, because, by [33, Theorem 3.3], $\mathcal{X}$ and $\mathcal{X}'$ are WL_m-equivalent with respect to φ if and only if T has full support. □

5 S-rings and Cayley schemes

In this section, we give a short background concerning S-rings and Cayley schemes; in our presentation, we mainly follow [10, 14].

5.1 S-rings

Let G be a finite group. A free $\mathbb{Z}$-submodule $\mathcal{A}$ of the group ring $\mathbb{Z}G$ is called a *Schur ring* (*S-ring*, for short) over G if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of G such that $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : X \in \mathcal{S}\}$ and

[2] It is allowed to move previously placed pebbles to other vertices and place more than one pebble on the same vertex.

(S1) $\{1_G\} \in \mathcal{S}$,

(S2) $X^{-1} \in \mathcal{S}$ for all $X \in \mathcal{S}$,

(S3) $\underline{X}\,\underline{Y} = \sum_{Z\in\mathcal{S}} c^Z_{X,Y}\underline{Z}$ for all $X, Y \in \mathcal{S}$ and some nonnegative integers $c^Z_{X,Y}$.

The elements of $\mathcal{S}$ and the number $\mathrm{rk}(\mathcal{A}) = |\mathcal{S}|$ are called, respectively, the *basic sets* and *rank* of $\mathcal{A}$. The integer $c^Z_{X,Y}$ is equal to the number of representations $z = xy$ with $x \in X$ and $y \in Y$ for a fixed $z \in Z$. For any subgroup $M \leqslant \mathrm{Aut}(G)$, the set $\{x^M : x \in G\}$ of all M-orbits forms a partition $\mathcal{S}(\mathcal{A})$ for some S-ring $\mathcal{A}$ over G; we denote this S-ring by $\mathrm{cyc}(M, G)$ and call it *cyclotomic*.

The partial order $\leqslant$ on the S-rings over G is induced by inclusion. Thus, $\mathcal{A} \leqslant \mathcal{A}'$ if and only if any basic set of $\mathcal{A}$ is a union of some basic sets of $\mathcal{A}'$; in this case, we say that $\mathcal{A}'$ is an *extension* of $\mathcal{A}$. The least and greatest elements with respect to $\leqslant$ are, respectively, the *trivial* S-ring spanned by $\underline{1_G}$ and $\underline{G}$, and the group ring $\mathbb{Z}G$. For any $X \subseteq G$, we denote by $\mathrm{WL}_G(\underline{X})$ the smallest S-ring over G, that contains the element $\underline{X}$.

5.2 Isomorphisms

For any set $X \subseteq G$, one can define a Cayley (di)graph $\mathrm{Cay}(G, X)$ with vertex set G and the arcs (x, y) with $yx^{-1} \in X$. The automorphism group of this graph contains a regular subgroup G_{right} of the symmetric group $\mathrm{Sym}(G)$, induced by right multiplications of G.

Let $\mathcal{A}$ and $\mathcal{A}'$ be S-rings over groups G and G', respectively, and let $f : G \to G'$ be a bijection. We say that f is a *(combinatorial) isomorphism* from $\mathcal{A}$ to $\mathcal{A}'$ if for each $X \in \mathcal{S}(\mathcal{A})$, there is $X' \in \mathcal{S}(\mathcal{A}')$ such that f is a graph isomorphism from $\mathrm{Cay}(G, X)$ to $\mathrm{Cay}(G', X')$, i.e.,

$$y\,x^{-1} \in X \quad \Leftrightarrow \quad y'\,x'^{-1} \in X'$$

for all $x, y \in G$, where $x' = x^f$ and $y' = y^f$.[3] The isomorphism f is said to be *normalized* if $f(1_G) = 1_{G'}$. Note that the S-rings $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic if and only if there is a normalized isomorphism from $\mathcal{A}$ to $\mathcal{A}'$.

The group of all isomorphisms from the S-ring $\mathcal{A}$ to itself is denoted by $\mathrm{Iso}(\mathcal{A})$. It has a normal subgroup $\mathrm{Aut}(\mathcal{A})$, the *automorphism group* of $\mathcal{A}$, that is equal to the intersection of the groups $\mathrm{Aut}(\mathrm{Cay}(G, X))$, $X \in \mathcal{S}$. In particular,

$$G_{right} \leqslant \mathrm{Aut}(\mathcal{A}) \leqslant \mathrm{Aut}(\mathrm{Cay}(G, X)) \tag{10}$$

for each X. Thus, $f \in \mathrm{Aut}(\mathcal{A})$ if and only if for all $x, y \in G$ and all $X \in \mathcal{S}$, the elements $y\,x^{-1}$ and $y'\,x'^{-1}$ belong or do not belong to X simultaneously. Note that if $f \in \mathrm{Aut}(G)$ or f is a normalized isomorphism of $\mathcal{A}$, then $f \in \mathrm{Aut}(\mathcal{A})$ if and only if f leaves every basic set of $\mathcal{A}$ fixed.

[3] This condition means exactly that $(Xx)^f = X'x'$ for all $X \in \mathcal{S}$ and $x \in G$.

5.3 $\mathcal{A}$-sets

Any union of basic sets is called an $\mathcal{A}$-*set*. The set $\mathcal{S}^\cup$ of all of them is closed with respect to taking inverse, product, and standard set-theoretical operations. An $\mathcal{A}$-set which is a subgroup of G is called an $\mathcal{A}$-*subgroup*. For example, if X is an $\mathcal{A}$-set, then the groups $\langle X\rangle$ and $\mathrm{rad}(X)$ are $\mathcal{A}$-subgroups.

The following important theorem goes back to I. Schur and H. Wielandt (see [32, Ch. IV]); as to the formulation given here we refer to [13, Theorem 2.3]. Below for a subset X of an abelian group G, an integer m, and a prime p, we put

$$X^{(m)} = \{x^m :\ x \in X\}, \quad X^{[p]} = \{x^p :\ x \in X,\ |xH \cap X| \not\equiv 0 \mod p\}$$

where $H = \{g \in G :\ g^p = 1\}$.

Theorem 5. *Let $\mathcal{A}$ be an S-ring over an abelian group of order n, and $\mathcal{S} = \mathcal{S}(\mathcal{A})$. Then*

(1) *$X^{(m)} \in \mathcal{S}$ for any integer m coprime to n and any $X \in \mathcal{S}$,*

(2) *$X^{[p]} \in \mathcal{S}^\cup$ for any prime p dividing n and any $X \in \mathcal{S}^\cup$.*[4]

5.4 Tensor and wreath products

Let $\mathcal{A}_1$ and $\mathcal{A}_2$ be S-rings over groups G_1 and G_2, respectively. The *tensor product* $\mathcal{A}_1 \otimes \mathcal{A}_2$ and the *wreath product* $\mathcal{A}_1 \wr \mathcal{A}_2$ are defined to be the S-rings over the direct product $G = G_1 \times G_2$, such that

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

where $\mathcal{S}_1 = \mathcal{S}(\mathcal{A}_1)$ and $\mathcal{S}_2 = \mathcal{S}(\mathcal{A}_2)$, and

$$\mathcal{S}(\mathcal{A}_1 \wr \mathcal{A}_2) = \{X_1 \times \{1_{G_2}\} : X_1 \in \mathcal{S}_1\} \cup \{G_1 \times X_2 : 1_{G_2} \neq X_2 \in \mathcal{S}_2\},$$

respectively. If $H_1 \leqslant G_1$ and $H_2 \leqslant G_2$ are, respectively, $\mathcal{A}_1$- and $\mathcal{A}_2$-subgroups, then H_1H_2 is an $(\mathcal{A}_1 \otimes \mathcal{A}_2)$-subgroup, whereas H_1 and G_1H_2 are $(\mathcal{A}_1 \wr \mathcal{A}_2)$-subgroups. If, in addition, the group $G_1 \times G_2$ is cyclic, then these are the only $(\mathcal{A}_1 \otimes \mathcal{A}_2)$- and $(\mathcal{A}_1 \wr \mathcal{A}_2)$-subgroups, respectively.

5.5 Sections

Let U and L be $\mathcal{A}$-subgroups and also L a normal subgroup of U. The group $\mathfrak{s} = U/L$ is called an $\mathcal{A}$-*section*; the set of all $\mathcal{A}$-sections is denoted by $\mathfrak{S}(\mathcal{A})$. Furthermore, let $\pi : U \to U/L$ be the natural epimorphism. The set

$$\mathcal{S}_\mathfrak{s} = \{\pi(X) :\ X \in \mathcal{S},\ X \subseteq U\}$$

[4] Though Lemma 2.1 in [12] requires X to be the basic set of $\mathcal{A}'$, the proof of the lemma remains true under a weaker assumption that X is an $\mathcal{A}'$-set.

forms a partition of the group $\mathfrak{s}$, and the elements $\pi(X)$ span an S-ring over $\mathfrak{s}$; it is denoted by $\mathcal{A}_\mathfrak{s}$ and is called the *restriction* of $\mathcal{A}$ to $\mathfrak{s}$. If $U = \langle X \rangle$ and $L = \mathrm{rad}(X)$ for some $X \in \mathcal{S}$, then the section $\mathfrak{s}$ is said to be *principal* and is denoted by $\mathfrak{s}_X$. In this case, setting $\mathfrak{s} = \mathfrak{s}_X$, $\pi_\mathfrak{s} = \pi$, and $X_\mathfrak{s} = \pi(X)$, we have

$$X = {\pi_\mathfrak{s}}^{-1}(X_\mathfrak{s}). \tag{11}$$

For any $x \in U$, we put $x_\mathfrak{s} = \pi_\mathfrak{s}(x)$.

Let $\mathfrak{s} = U/L$ and $\mathfrak{t} = U'/L'$ be $\mathcal{A}$-sections. We say that $\mathfrak{s}$ is a *subsection* of $\mathfrak{t}$ if $U \leqslant U'$ and $L \geqslant L'$; in this case, we write $\mathfrak{s} \preceq \mathfrak{t}$. This defines a partial order on the set $\mathfrak{S}(\mathcal{A})$. The greatest element in it is $G/1$; every minimal element is of the form H/H, where H is an $\mathcal{A}$-subgroup.

5.6 Projective equivalence

An $\mathcal{A}$-section $\mathfrak{t} = U'/L'$ is called a *multiple* of the section $\mathfrak{s} = U/L$ if

$$L = U \cap L' \quad \text{and} \quad U' = UL'. \tag{12}$$

The *projective equivalence* relation on the set $\mathfrak{S}(\mathcal{A})$ of all $\mathcal{A}$-sections is defined to be the symmetric transitive closure of the relation "to be a multiple"; we write $\mathfrak{s} \sim \mathfrak{t}$ if the sections $\mathfrak{s}$ and $\mathfrak{t}$ are projectively equivalent. Any two projectively equivalent sections are obviously isomorphic as groups. Moreover, if $\mathfrak{s} \sim \mathfrak{t}$, then there is a group isomorphism $f = f_{\mathfrak{s},\mathfrak{t}}$ from $\mathfrak{s}$ to $\mathfrak{t}$ belonging to $\mathrm{Iso}(\mathcal{A}_\mathfrak{s}, \mathcal{A}_\mathfrak{t})$ and such that $(\gamma^\mathfrak{s})^f = \gamma^\mathfrak{t}$ for all normalized automorphisms $\gamma \in \mathrm{Aut}(\mathcal{A})$, where $\gamma^\mathfrak{s}$ and $\gamma^\mathfrak{t}$ are the restriction of γ to $\mathfrak{s}$ and to $\mathfrak{t}$, respectively (see Subsection 2.1).

5.7 Algebraic isomorphisms

Let $\mathcal{A}$ and $\mathcal{A}'$ be S-rings over groups G and G', respectively. A ring isomorphism $\varphi : \mathcal{A} \to \mathcal{A}'$ is called an *algebraic isomorphism* from $\mathcal{A}$ to $\mathcal{A}'$, if for any $X \in \mathcal{S}(\mathcal{A})$, there exists $X' \in \mathcal{S}(\mathcal{A}')$ such that

$$\varphi(\underline{X}) = \underline{X'}.$$

Each normalized isomorphism $f : \mathcal{A} \to \mathcal{A}'$ *induces* an algebraic isomorphism for which $X' = X^f$. However not every algebraic isomorphism is induced by an isomorphism.

From the definition, it follows that the mapping $X \mapsto X'$ is a bijection from $\mathcal{S}(\mathcal{A})$ onto $\mathcal{S}(\mathcal{A}')$. This bijection is naturally extended to a bijection between the $\mathcal{A}$- and $\mathcal{A}'$-sets, with respect to which the $\mathcal{A}$-subgroups go to $\mathcal{A}'$-subgroups. Moreover, if the groups G and G' are abelian, then the last bijection can be extended to the bijection between the $\mathcal{A}$- and $\mathcal{A}'$-sections. The images of an $\mathcal{A}$-set X and an $\mathcal{A}$-section $\mathfrak{s}$ under the corresponding bijections are denoted by X^φ and $\mathfrak{s}^\varphi$, respectively. For any such $\mathfrak{s}$, the algebraic isomorphism φ induces an algebraic isomorphism

$$\varphi_\mathfrak{s} : \mathcal{A}_\mathfrak{s} \to \mathcal{A}'_{\mathfrak{s}'},\ \pi_\mathfrak{s}(X) \mapsto \pi_{\mathfrak{s}'}(X'),$$

where $\mathfrak{s}' = \mathfrak{s}^\varphi$.

The above bijection between the $\mathcal{A}$- and $\mathcal{A}'$-sets is in fact an isomorphism of the corresponding lattices. Furthermore, given an $\mathcal{A}$-set X, we have

$$\langle X^\varphi \rangle = \langle X \rangle^\varphi \quad \text{and} \quad \mathrm{rad}(X^\varphi) = \mathrm{rad}(X)^\varphi. \tag{13}$$

Let $f : G \to G'$ be a bijection taking the identity of G to that of G'. Then f is a normalized isomorphism from $\mathcal{A}$ to $\mathcal{A}'$ if and only if there exists an algebraic isomorphism $\varphi : \mathcal{A} \to \mathcal{A}'$ such that $X^\varphi = X^f$ for all $X \in \mathcal{S}(\mathcal{A})$. In this case, we say that f *induces* φ. The set of all normalized isomorphisms that induce a fixed φ is denoted by $\mathrm{Iso}(\mathcal{A}, \mathcal{A}', \varphi)$; we abbreviate $\mathrm{Iso}(\mathcal{A}, \varphi) = \mathrm{Iso}(\mathcal{A}, \mathcal{A}, \varphi)$.

5.8 Circulant S-rings

An S-ring $\mathcal{A}$ over a cyclic group G is said to be *circulant*. Any basic set of $\mathcal{A}$, containing a generator of G, is said to be *highest*. The class of circulant S-rings is closed with respect to tensor product and wreath product (if the underlying groups of the factors are of coprime orders).

As was shown in [24], any two algebraically isomorphic circulant S-rings are isomorphic, and are equal if they have the same underlying groups. Therefore, in what follows, we focus on algebraic automorphisms and isomorphisms of a circulant S-ring to itself, rather than general algebraic and combinatorial isomorphisms. The fact that any two nonisomorphic subgroups of a cyclic group G have different orders, implies that if $\mathcal{A}$ is an S-ring over G and H is an $\mathcal{A}$-subgroup, then $H = H^\varphi = H^f$ for all algebraic automorphisms φ of $\mathcal{A}$ and all normalized isomorphisms f of $\mathcal{A}$ to itself.

The general theory of circulant S-rings (see, for example, [10]) shows that each such ring is obtained by generalized wreath and tensor products from trivial and normal circulant rings (the normal S-rings are defined below). For the purposes of this paper, there is no need to give this theory in detail. Instead, we define in Subsection 5.10 a class of totally normal S-rings that is contained in the intersection of the classes of quasinormal and quasidense rings studied in papers [11, 33] and [14], respectively. This will allow us to freely use the results of those papers without further specification.

5.9 Coset closure

An S-ring $\mathcal{A}$ over a group G is called a *coset* S-ring if each of its basic set is a coset of some $\mathcal{A}$-subgroup of G. The class of coset S-rings contains all group rings and is closed with respect to tensor and wreath products.

Let $\mathcal{A}$ be a *quasidense* circulant S-ring, i.e., $\mathcal{A}$ satisfies the following condition: if $\mathfrak{s}$ is an $\mathcal{A}$-section and the S-ring $\mathcal{A}_\mathfrak{s}$ is trivial, then the group $\mathfrak{s}$ is of prime order. In accordance with paper [14], the *coset closure* $\mathcal{A}_0$ of $\mathcal{A}$ is defined to be the intersection of all coset S-rings over G, that contain $\mathcal{A}$. The ring $\mathcal{A}_0$ is a coset S-ring and $\mathfrak{S}(\mathcal{A}_0) = \mathfrak{S}(\mathcal{A})$, see Theorems 8.5 and 10.7 *ibid*. Denote by $\mathfrak{S}_0(\mathcal{A})$ the set of all $\mathcal{A}$-sections $\mathfrak{s}$ such that $\mathfrak{s}$ is a subsection of some $\mathcal{A}$-section projectively equivalent to a principal $\mathcal{A}$-section. Then

$$\mathfrak{S}_0(\mathcal{A}) \subseteq \{\mathfrak{s} \in \mathfrak{S}(\mathcal{A}) : \ (\mathcal{A}_0)_\mathfrak{s} = \mathbb{Z}\mathfrak{s}\} = \mathfrak{S}_0(\mathcal{A}_0), \tag{14}$$

see formula (37) and Corollary 10.10 *ibid.*

5.10 Normal and totally normal S-rings

An S-ring $\mathcal{A}$ over a group G is said to be *normal* if the subgroup G_{right} is normal in $\mathrm{Aut}(\mathcal{A})$. The class of normal S-rings contains all group rings and is closed with respect to extensions and tensor products. A complete classification of normal circulant S-rings was obtained in [10]. In particular, it was proved there that every normal circulant S-ring is cyclotomic and the following lemma holds true.

Lemma 6. *Let $\mathcal{A}$ be a normal circulant S-ring over a group G of odd order. Then*

(1) $\mathrm{WL}_G(\underline{X}) = \mathcal{A}$ *for any highest basic set* $X \in \mathcal{S}(\mathcal{A})$,

(2) $\mathrm{Iso}(\mathcal{A}) \leqslant \mathrm{Aut}(G)$,

(3) $\mathcal{A} = \mathrm{cyc}(M, G)$ *for a unique* $M \leqslant \mathrm{Aut}(G)$, *and also* $\mathrm{Aut}(\mathcal{A}) = G \rtimes M$.

Proof. The assumption that the group G is of odd order implies that, in terms of the paper [10], the S-ring $\mathcal{A}$ has trivial radical. Thus the first two statements follow from Lemma 6.7 of that paper and the proof of it, whereas the third statement is a consequence of Theorem 6.1 and Corollary 6.3 *ibid.* □

An $\mathcal{A}$-section $\mathfrak{s}$ of a circulant S-ring $\mathcal{A}$ is said to be *normal* if the S-ring $\mathcal{A}_\mathfrak{s}$ is normal. Any $\mathcal{A}$-section projectively equivalent to a normal section is normal. However, in general, a subsection of a normal section is not necessarily normal.

A circulant S-ring $\mathcal{A}$ is said to be *totally normal* if any subsection of a principal $\mathcal{A}$-section is normal, or, equivalently, any section belonging to $\mathfrak{S}_0(\mathcal{A})$ is normal. Obviously, any circulant coset S-ring is totally normal, because the restriction of it to any principal section is a group ring (which is always normal). In general, an $\mathcal{A}$-section $\mathfrak{s}$ of a circulant S-ring $\mathcal{A}$ is said to be totally normal if the S-ring $\mathcal{A}_\mathfrak{s}$ is totally normal.

Any totally normal circulant S-ring $\mathcal{A}$ is quasidense. Indeed, otherwise, there is an $\mathcal{A}$-section $\mathfrak{s}$ of composite order and such that the S-ring $\mathcal{A}_\mathfrak{s}$ is trivial. But then $\mathfrak{s}$ is a subsection of a principal section. Since $\mathfrak{s}$ is not normal, we arrive at a contradiction.

From the above mentioned classification of normal circulant S-rings, it follows that any nontrivial circulant S-ring over a group of prime order is also totally normal. Note also that the class of totally normal circulant S-rings is closed with respect to tensor products such that the underlying groups of the factors are of coprime orders.

5.11 Cayley schemes and S-rings

Let G be a group. A coherent configuration $\mathcal{X} = (\Omega, S)$ is called a *Cayley scheme* over G if

$$\Omega = G \quad \text{and} \quad G_{right} \leqslant \mathrm{Aut}(\mathcal{X}).$$

Each relation $s \in S$ is the arc set of the Cayley graph $\mathrm{Cay}(G, X)$, where $X = X(s)$ is the neighborhood of the identity of G in the relation s. The neighborhoods $X(s)$, $s \in S$, form

a partition $\mathcal{S}$ of the group G. Moreover, this partition satisfies conditions (S1), (S2), and (S3). Thus, every Cayley scheme over G is associated with an S-ring $\mathcal{A} = \mathcal{A}(\mathcal{X})$ over G, such that $\mathcal{S}(\mathcal{A}) = \mathcal{S}$.

Conversely, let $\mathcal{A}$ be an S-ring over G. For each $X \in \mathcal{S}(\mathcal{A})$, denote by s_X the arc set of the Cayley graph $\mathrm{Cay}(G, X)$. Then the relations s_X, $X \in \mathcal{S}(\mathcal{A})$, form a partition S of the Cartesian square Ω^2, where $\Omega = G$. Moreover, this partition satisfies conditions (CC1), (CC2), and (CC3). Thus, every S-ring $\mathcal{A}$ over G is associated with a Cayley scheme $\mathcal{X} = \mathcal{X}(\mathcal{A})$ over G, such that $S(\mathcal{X}) = S$.

For any group G, the above mappings

$$\mathcal{X} \mapsto \mathcal{A}(\mathcal{X}) \quad \text{and} \quad \mathcal{A} \mapsto \mathcal{X}(\mathcal{A}) \tag{15}$$

define a one-to-one correspondence between the Cayley schemes over G and the S-rings over G. This correspondence preserves the corresponding partial orders on the schemes and S-rings. Moreover, it is functorial in the sense that for any Cayley schemes $\mathcal{X}$ and $\mathcal{X}'$, we have

$$\mathrm{Iso}(\mathcal{X}, \mathcal{X}') = \mathrm{Iso}(\mathcal{A}, \mathcal{A}'),$$

where $\mathcal{A} = \mathcal{A}(\mathcal{X})$ and $\mathcal{A}' = \mathcal{A}(\mathcal{X}')$. Furthermore, there is a one-to-one correspondence between algebraic isomorphisms, in which an algebraic isomorphism $\varphi : \mathcal{X} \to \mathcal{X}'$, $s \mapsto s'$, corresponds to the algebraic isomorphism $\tilde{\varphi} : \mathcal{A} \to \mathcal{A}'$, $X(s) \mapsto X(\varphi(s))$. In what follows, we denote $\tilde{\varphi}$ just by φ.

We complete the subsection by remarking that the mappings (15) respect the tensor and wreath products, namely,

$$\mathcal{A}(\mathcal{X}_1 \otimes \mathcal{X}_2) = \mathcal{A}(\mathcal{X}_1) \otimes \mathcal{A}(\mathcal{X}_2) \quad \text{and} \quad \mathcal{A}(\mathcal{X}_1 \wr \mathcal{X}_2) = \mathcal{A}(\mathcal{X}_1) \wr \mathcal{A}(\mathcal{X}_2).$$

6 Multipliers of totally normal circulant S-rings

Throughout this section, $\mathcal{A}$ is a totally normal circulant S-ring over a (cyclic) group G, $\mathcal{S} = \mathcal{S}(\mathcal{A})$, and $\mathfrak{S}_0 = \mathfrak{S}_0(\mathcal{A})$. We denote by $\mathcal{A}_0$ the coset closure of $\mathcal{A}$ and put $\mathcal{S}_0 = \mathcal{S}(\mathcal{A}_0)$. Finally, we denote by $\mathrm{Iso}_{\mathcal{A}}(\mathcal{A}_0)$ the set of all isomorphisms $f \in \mathrm{Iso}(\mathcal{A}_0)$ such that $\mathcal{A}^f = \mathcal{A}$, and put

$$\mathrm{Aut}_{\mathcal{A}}(\mathfrak{s}) = \mathrm{Aut}(\mathcal{A}_{\mathfrak{s}}) \cap \mathrm{Aut}(\mathfrak{s})$$

for each $\mathfrak{s} \in \mathfrak{S}_0$.

6.1 Outer multipliers

Suppose that for every section $\mathfrak{s} \in \mathfrak{S}_0$, we are given a coset $\mathfrak{c}_{\mathfrak{s}} = \sigma_{\mathfrak{s}} \cdot \mathrm{Aut}_{\mathcal{A}}(\mathfrak{s}) = \mathrm{Aut}_{\mathcal{A}}(\mathfrak{s}) \cdot \sigma_{\mathfrak{s}}$, where $\sigma_{\mathfrak{s}} \in \mathrm{Aut}(\mathfrak{s})$. Following [15], the family

$$\mathfrak{c} = \{\mathfrak{c}_{\mathfrak{s}} : \ \mathfrak{s} \in \mathfrak{S}_0\} \tag{16}$$

is called an *outer $\mathcal{A}$-multiplier* if the following conditions are satisfied for all sections $\mathfrak{s}, \mathfrak{t} \in \mathfrak{S}_0$:

$$\mathfrak{s} \succeq \mathfrak{t} \ \Rightarrow \ (\mathfrak{c}_{\mathfrak{s}})^{\mathfrak{t}} = \mathfrak{c}_{\mathfrak{t}} \qquad \text{and} \qquad \mathfrak{s} \sim \mathfrak{t} \ \Rightarrow \ (\mathfrak{c}_{\mathfrak{s}})^{f_{\mathfrak{s},\mathfrak{t}}} = \mathfrak{c}_{\mathfrak{t}}, \tag{17}$$

where $(\mathfrak{c}_\mathfrak{s})^\mathfrak{t} = \{f^\mathfrak{t} : f \in \mathfrak{c}_\mathfrak{s}\}$ and $f_{\mathfrak{s},\mathfrak{t}}$ is the projective isomorphism from $\mathfrak{s}$ onto $\mathfrak{t}$ (defined in Subsection 5.6). The restriction $\mathfrak{c}_\mathfrak{T}$ of the outer multiplier $\mathfrak{c}$ to a subset $\mathfrak{T} \subseteq \mathfrak{S}_0$ is defined to be the family $\{\mathfrak{c}_\mathfrak{s} : \mathfrak{s} \in \mathfrak{T}\}$.

The set of all outer $\mathcal{A}$-multipliers forms a group $\mathfrak{C}(\mathcal{A})$ with respect to componentwise multiplication. By [15, Theorem 3.4], there is an isomorphism $\mathfrak{c} \mapsto \varphi_\mathfrak{c}$, $\mathfrak{c} \in \mathfrak{C}(\mathcal{A})$, from the group $\mathfrak{C}(\mathcal{A})$ onto the group of all algebraic automorphisms of the S-ring $\mathcal{A}$. Here the algebraic automorphism $\varphi = \varphi_\mathfrak{c}$ is defined as follows. Let $X \in \mathcal{S}(\mathcal{A})$ and let $\mathfrak{s} = \mathfrak{s}_X$ be the principal section associated with X. Then we put X^φ to be the $\pi_\mathfrak{s}$-preimage of the set $(X_\mathfrak{s})^{\sigma_\mathfrak{s}}$, see formula (11). Thus,

$$(X_\mathfrak{s})^{\varphi_\mathfrak{s}} = (X_\mathfrak{s})^{\mathfrak{c}_\mathfrak{s}} = (X_\mathfrak{s})^{\sigma_\mathfrak{s}}. \tag{18}$$

6.2 Inner multipliers

Suppose that for every section $\mathfrak{s} \in \mathfrak{S}_0$, we are given an automorphism $\mathfrak{m}_\mathfrak{s} \in \mathrm{Aut}(\mathfrak{s})$. Following [15], the family

$$\mathfrak{m} = \{\mathfrak{m}_\mathfrak{s} : \mathfrak{s} \in \mathfrak{S}_0\} \tag{19}$$

is called an *inner $\mathcal{A}$-multiplier* if the conditions (17) are satisfied for the cosets $\mathfrak{c}_\mathfrak{s}$ replaced by the singletons $\{\mathfrak{m}_\mathfrak{s}\}$. The restriction $\mathfrak{m}_\mathfrak{T}$ of the inner multiplier $\mathfrak{m}$ to a subset $\mathfrak{T} \subseteq \mathfrak{S}_0$ is defined to be the family $\{\mathfrak{m}_\mathfrak{s} : \mathfrak{s} \in \mathfrak{T}\}$.

The set of all inner $\mathcal{A}$-multipliers forms a subgroup $\mathfrak{M}(\mathcal{A})$ of the direct product of the groups $\mathrm{Aut}(\mathfrak{s})$, $\mathfrak{s} \in \mathfrak{S}_0$. For a subgroup $\mathfrak{M} \leqslant \mathfrak{M}(\mathcal{A})$ and a set $\mathfrak{T} \subseteq \mathfrak{S}_0$, we put $\mathfrak{M}_\mathfrak{T} = \{\mathfrak{m}_\mathfrak{T} : \mathfrak{m} \in \mathfrak{M}\}$ and abbreviate $\mathfrak{M}_\mathfrak{s} := \mathfrak{M}_{\{\mathfrak{s}\}}$ for $\mathfrak{s} \in \mathfrak{S}_0$. Clearly, $\mathfrak{M}_\mathfrak{T}$ is a group with respect to componentwise product. For any inner $\mathcal{A}$-multiplier $\mathfrak{m}$ and any outer $\mathcal{A}$-multiplier $\mathfrak{c}$, we write $\mathfrak{m}_\mathfrak{T} \leqslant \mathfrak{c}_\mathfrak{T}$ if $\mathfrak{m}_\mathfrak{s} \in \mathfrak{c}_\mathfrak{s}$ for all $\mathfrak{s} \in \mathfrak{T}$. When $\mathfrak{T} = \mathfrak{S}_0$, we abbreviate $\mathfrak{m} \leqslant \mathfrak{c}$.

Lemma 7. *For each inner $\mathcal{A}$-multiplier $\mathfrak{m} \in \mathfrak{M}(\mathcal{A})$, there exists a normalized isomorphism $f_\mathfrak{m} \in \mathrm{Iso}_\mathcal{A}(\mathcal{A}_0)$ such that for all $X \in \mathcal{S}$, we have*

$$X_\mathfrak{s}{}^{(f_\mathfrak{m})^\mathfrak{s}} = X_\mathfrak{s}{}^{\mathfrak{m}_\mathfrak{s}}, \tag{20}$$

where $\mathfrak{s} = \mathfrak{s}_X$ (see Subsection 5.5).

Proof. By [15, Lemma 5.2], the family of the singletons $\{\mathfrak{m}_\mathfrak{s}\}$, $\mathfrak{s} \in \mathfrak{S}_0$, is an outer $\mathcal{A}_0$-multiplier. By [15, Theorem 3.4], there exists a uniquely determined algebraic automorphism φ of the S-ring $\mathcal{A}_0$ such that

$$X_\mathfrak{s}{}^{\varphi_\mathfrak{s}} = X_\mathfrak{s}{}^{\mathfrak{m}_\mathfrak{s}}, \qquad X \in \mathcal{S}, \tag{21}$$

where $\mathfrak{s} = \mathfrak{s}_X$. By [14, Theorem 9.1], every algebraic automorphism of $\mathcal{A}_0$ is induced by an isomorphism. Consequently, there exists a normalized isomorphism $f \in \mathrm{Iso}(\mathcal{A}_0, \varphi)$. By virtue of (21), we have

$$X_\mathfrak{s}{}^{f^\mathfrak{s}} = X_\mathfrak{s}{}^{\varphi_\mathfrak{s}} = X_\mathfrak{s}{}^{\mathfrak{m}_\mathfrak{s}},$$

which proves formula (20) for $f_\mathfrak{m} = f$.

To prove that $f \in \mathrm{Iso}_{\mathcal{A}}(\mathcal{A}_0)$, we need to verify that $X^f \in \mathcal{S}$ for all $X \in \mathcal{S}$. The principal section $\mathfrak{s} = \mathfrak{s}_X$ belongs to the set $\mathfrak{S}_0$. By formula (11),

$$X^f = (\pi^{-1}(X_{\mathfrak{s}}))^f = \pi^{-1}(X_{\mathfrak{s}}{}^{f^{\mathfrak{s}}}) = \pi^{-1}(X_{\mathfrak{s}}{}^{\mathfrak{m}_{\mathfrak{s}}}),$$

where $\pi = \pi_{\mathfrak{s}}$. Put $Y = X^{\mathfrak{m}'}$, where $\mathfrak{m}' \in \mathrm{Aut}(G)$ is such that $(\mathfrak{m}')^{\mathfrak{s}} = \mathfrak{m}_{\mathfrak{s}}$. By Theorem 5(1), we have $Y \in \mathcal{S}$. Furthermore, $\langle X \rangle = \langle Y \rangle$ and $\mathrm{rad}(X) = \mathrm{rad}(Y)$. Therefore, $\mathfrak{s} = \mathfrak{s}_X = \mathfrak{s}_Y$ and $Y_{\mathfrak{s}} = X_{\mathfrak{s}}{}^{\mathfrak{m}_{\mathfrak{s}}}$. Thus,

$$X^f = \pi^{-1}(X_{\mathfrak{s}}{}^{\mathfrak{m}_{\mathfrak{s}}}) = \pi^{-1}(Y_{\mathfrak{s}}) = Y \in \mathcal{S},$$

and $\mathcal{A}^f = \mathcal{A}$, as required. □

Each normalized isomorphism $f \in \mathrm{Iso}(\mathcal{A})$ leaves every $\mathcal{A}$-subgroup fixed (because the S-ring $\mathcal{A}$ is circulant). This yields the restriction isomorphism $f^{\mathfrak{s}} \in \mathrm{Iso}(\mathcal{A}_{\mathfrak{s}})$ for every $\mathcal{A}$-section $\mathfrak{s}$. Note that the collection $\mathfrak{m}_f = \{f^{\mathfrak{s}} : \ \mathfrak{s} \in \mathfrak{S}_0\}$ is not necessarily an inner $\mathcal{A}$-multiplier (because $f^{\mathfrak{s}}$ does not always belong to $\mathrm{Aut}(\mathfrak{s})$). Put

$$\mathfrak{M}_{aut}(\mathcal{A}) = \{\mathfrak{m}_f \in \mathfrak{M}(\mathcal{A}) : \ f \in \mathrm{Aut}(\mathcal{A})\}.$$

Assume that the group G is of odd order. Let $\mathfrak{s} \in \mathfrak{S}_0$. Since the S-ring $\mathcal{A}$ is totally normal, the S-ring $\mathcal{A}_{\mathfrak{s}}$ is normal and by Lemma 6(2), the isomorphism $f^{\mathfrak{s}}$ belongs to $\mathrm{Aut}(\mathfrak{s})$. Thus, $\mathfrak{m}_f \in \mathfrak{M}(\mathcal{A})$ and $\mathfrak{M}_{aut}(\mathcal{A})$ is a subgroup of $\mathfrak{M}(\mathcal{A})$.

6.3 Algebraic fusions

Let $\mathcal{A}$ be a coset S-ring, i.e., $\mathcal{A} = \mathcal{A}_0$, and let $\mathfrak{M}$ be a group of inner $\mathcal{A}$-multipliers. This group acts on the basic sets of $\mathcal{A}$, namely, if $X \in \mathcal{S}$ and $\mathfrak{m} \in \mathfrak{M}$, then

$$X^{\mathfrak{m}} := \pi_{\mathfrak{s}}^{-1}(X_{\mathfrak{s}}{}^{\mathfrak{m}_{\mathfrak{s}}}), \tag{22}$$

where $\mathfrak{s} = \mathfrak{s}_X$. We define the *algebraic fusion* of $\mathcal{A}$ with respect to the group $\mathfrak{M}$ as an S-ring $\mathcal{A}^{\mathfrak{M}}$ over G with the basic sets

$$X^{\mathfrak{M}} = \bigcup_{\mathfrak{m} \in \mathfrak{M}} X^{\mathfrak{m}}, \qquad X \in \mathcal{S}. \tag{23}$$

In the sense of [5, Subsection 2.3.3], the Cayley scheme $\mathcal{X}(\mathcal{A}^{\mathfrak{M}})$ is the algebraic fusion of the Cayley scheme $\mathcal{X}(\mathcal{A})$ with respect to the group of the algebraic automorphisms $\varphi_{\mathfrak{c}_{\mathfrak{m}}}$ corresponding to the outer $\mathcal{A}$-multiplier $\mathfrak{c}_{\mathfrak{m}} = \{\{\mathfrak{m}_{\mathfrak{s}}\} : \ \mathfrak{s} \in \mathfrak{S}_0\}$, $\mathfrak{m} \in \mathfrak{M}$. Since the S-ring $\mathcal{A}$ is a coset S-ring, formula (14) implies that

$$(\mathcal{A}^{\mathfrak{M}})_{\mathfrak{s}} = (\mathcal{A}_{\mathfrak{s}})^{\mathfrak{M}_{\mathfrak{s}}} = (\mathbb{Z}\mathfrak{s})^{\mathfrak{M}_{\mathfrak{s}}} = \mathrm{cyc}(\mathfrak{M}_{\mathfrak{s}}, \mathfrak{s}) \tag{24}$$

for all $\mathfrak{s} \in \mathfrak{S}_0$.

Obviously, $\mathcal{A}^{\mathfrak{M}} \leqslant \mathcal{A}$. Therefore each $\mathcal{A}^{\mathfrak{M}}$-subgroup is an $\mathcal{A}$-subgroup. Conversely, if H is an $\mathcal{A}$-subgroup, then by Lemma 7, we have $H^{\mathfrak{m}} = H^{f_{\mathfrak{m}}} = H$ for all $\mathfrak{m} \in \mathfrak{M}$, and

hence H is an $\mathcal{A}^{\mathfrak{M}}$-subgroup. Thus the S-rings $\mathcal{A}$ and $\mathcal{A}^{\mathfrak{M}}$ have the same $\mathcal{A}$-subgroups and

$$\mathfrak{S}(\mathcal{A}) = \mathfrak{S}(\mathcal{A}^{\mathfrak{M}}). \tag{25}$$

Moreover, it is not hard to see that the relations $\preceq$ and $\sim$ on the $\mathcal{A}$- and $\mathcal{A}^{\mathfrak{M}}$-sections are the same.

Lemma 8. *In the above notation, assume that G is of odd order and the S-ring* $\mathrm{cyc}(\mathfrak{M}_{\mathfrak{s}}, \mathfrak{s})$ *is normal for all $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$. Then $\mathfrak{M} \leqslant \mathfrak{M}_{aut}(\mathcal{A}^{\mathfrak{M}})$ and*

$$\mathfrak{S}_0(\mathcal{A}^{\mathfrak{M}}) = \mathfrak{S}_0(\mathcal{A}) \quad \textit{and} \quad (\mathcal{A}^{\mathfrak{M}})_0 = \mathcal{A}. \tag{26}$$

Proof. To prove the first inclusion, we need to verify that for each $\mathfrak{m} \in \mathfrak{M}$, there exists $f \in \mathrm{Aut}(\mathcal{A}^{\mathfrak{M}})$ such that $\mathfrak{m} = \mathfrak{m}_f$. To this end, denote by f the isomorphism $f_{\mathfrak{m}} \in \mathrm{Iso}(\mathcal{A})$ from Lemma 7 (note that in our case, $\mathcal{A} = \mathcal{A}_0$). Then $\mathfrak{m} = \mathfrak{m}_f$. Moreover, for all $X \in \mathcal{S}$, we have

$$(X^{\mathfrak{M}})^f = \Big(\bigcup_{\mathfrak{n}\in\mathfrak{M}} X^{\mathfrak{n}}\Big)^f = \Big(\bigcup_{\mathfrak{n}\in\mathfrak{M}} \pi_{\mathfrak{s}}^{-1}(X_{\mathfrak{s}}{}^{\mathfrak{n}_{\mathfrak{s}}})\Big)^f = \bigcup_{\mathfrak{n}\in\mathfrak{M}} \pi_{\mathfrak{s}}^{-1}(X_{\mathfrak{s}}{}^{\mathfrak{n}_{\mathfrak{s}}\mathfrak{m}_{\mathfrak{s}}})$$
$$= \bigcup_{\mathfrak{n}\in\mathfrak{M}} \pi_{\mathfrak{s}}^{-1}(X_{\mathfrak{s}}{}^{(\mathfrak{n}\mathfrak{m})_{\mathfrak{s}}}) = \bigcup_{\mathfrak{n}'\in\mathfrak{M}} \pi_{\mathfrak{s}}^{-1}(X_{\mathfrak{s}}{}^{(\mathfrak{n}')_{\mathfrak{s}}}) = \bigcup_{\mathfrak{n}'\in\mathfrak{M}} X^{\mathfrak{n}'} = X^{\mathfrak{M}},$$

where $\mathfrak{s} = \mathfrak{s}_X$, see formulas (22) and (23). Thus, $f \in \mathrm{Aut}(\mathcal{A}^{\mathfrak{M}})$, as required.

First, we prove that $\mathfrak{S}_0(\mathcal{A}) \subseteq \mathfrak{S}_0(\mathcal{A}^{\mathfrak{M}})$. Since the relations $\preceq$ and $\sim$ on the $\mathcal{A}$- and $\mathcal{A}^{\mathfrak{M}}$-sections are the same, it suffices to verify that every principal $\mathcal{A}$-section $\mathfrak{s}$ is a principal $\mathcal{A}^{\mathfrak{M}}$-section. Suppose that $\mathfrak{s} = \mathfrak{s}_X$ for some $X \in \mathcal{S}$. Then obviously $\langle X\rangle = \langle X^{\mathfrak{M}}\rangle$ and $\mathrm{rad}(X) \leqslant \mathrm{rad}(X^{\mathfrak{M}})$. Suppose on the contrary that $\mathrm{rad}(X) \neq \mathrm{rad}(X^{\mathfrak{M}})$. Then the radical of the set $(X^{\mathfrak{M}})_{\mathfrak{s}} \leqslant \mathfrak{s}$ is nontrivial. Since the group $\mathfrak{s}$ is of odd order and $(X^{\mathfrak{M}})_{\mathfrak{s}}$ is a highest basic set of the S-ring $(\mathcal{A}^{\mathfrak{M}})_{\mathfrak{s}} = \mathrm{cyc}(\mathfrak{M}_{\mathfrak{s}}, \mathfrak{s})$, this S-ring is not normal by [10, Theorem 6.1], a contradiction.

From formula (14), it follows that $\mathfrak{S}_0(\mathcal{A}^{\mathfrak{M}}) \subseteq \mathfrak{S}_0((\mathcal{A}^{\mathfrak{M}})_0)$. On the other hand, $\mathcal{A}$ is a coset S-ring containing $\mathcal{A}^{\mathfrak{M}}$. Therefore, $(\mathcal{A}^{\mathfrak{M}})_0 \leqslant \mathcal{A}$. It follows that $\mathfrak{S}_0((\mathcal{A}^{\mathfrak{M}})_0) \subseteq \mathfrak{S}_0(\mathcal{A})$. Consequently, $\mathfrak{S}_0(\mathcal{A}^{\mathfrak{M}}) \subseteq \mathfrak{S}_0(\mathcal{A})$. Together with the inclusion in the above paragraph, this proves the first equality in (26). Furthermore, the above argument shows that $\mathfrak{S}_0((\mathcal{A}^{\mathfrak{M}})_0) = \mathfrak{S}_0(\mathcal{A})$. Hence the coset S-rings $(\mathcal{A}^{\mathfrak{M}})_0$ and $\mathcal{A}$ have the same principal sections. Thus they are equal which proves the second equality in (26). □

7 Local system of multipliers

Let $\mathcal{A}$ be a circulant S-ring, $\mathfrak{c}$ an outer $\mathcal{A}$-multiplier, and $k \geqslant 2$ an integer. Denote by $\mathfrak{S}_k = \mathfrak{S}_k(\mathcal{A})$ the set of all subsets consisting of no more than k principal $\mathcal{A}$-sections. Assume that for each $\mathfrak{S} \in \mathfrak{S}_k$, we are given an inner $\mathcal{A}$-multiplier $\mathfrak{m}(\mathfrak{S})$. A family

$$\{\mathfrak{m}(\mathfrak{S}) \in \mathfrak{M}(\mathcal{A}) :\ \mathfrak{S} \in \mathfrak{S}_k\} \tag{27}$$

is called a *k-local system of inner $\mathcal{A}$-multipliers* with respect to $\mathfrak{c}$ if the following two conditions are satisfied for all subsets $\mathfrak{S}, \mathfrak{S}' \in \mathfrak{S}_k$ and some inner $\mathcal{A}$-multipliers $\mathfrak{m}(\mathfrak{S}, \mathfrak{S}') \in \mathfrak{M}_{aut}(\mathcal{A})$:

$$\mathfrak{m}(\mathfrak{S})_{\mathfrak{S}} \leqslant \mathfrak{c}_{\mathfrak{S}} \quad \text{and} \quad \mathfrak{m}(\mathfrak{S})_{\mathfrak{S}\cap\mathfrak{S}'} = \mathfrak{m}(\mathfrak{S}')_{\mathfrak{S}\cap\mathfrak{S}'} \cdot \mathfrak{m}(\mathfrak{S}, \mathfrak{S}')_{\mathfrak{S}\cap\mathfrak{S}'}. \tag{28}$$

The main result of this section is the following theorem.

Theorem 9. *Let $\mathcal{A}$ be a totally normal circulant S-ring and $k \geqslant 2$ an integer. Assume that*

(1) *the scheme $\mathcal{X}(\mathcal{A}_0)$ is binary,*

(2) *there is a k-local system of inner $\mathcal{A}$-multipliers with respect to an outer multiplier $\mathfrak{c} \in \mathfrak{C}(\mathcal{A})$.*

Then for each $2 \leqslant m < \sqrt{k}$, the scheme $\mathcal{X}(\mathcal{A})$ is WL_m-equivalent to itself with respect to the algebraic isomorphism $\varphi_{\mathfrak{c}}$.

We prove Theorem 9 at the end of the section. In what follows, G is a cyclic group underlying the S-ring $\mathcal{A}$, $\mathcal{X} = \mathcal{X}(\mathcal{A})$ is the Cayley scheme associated with $\mathcal{A}$, and $\varphi = \varphi_{\mathfrak{c}}$. Fix an integer ℓ such that

$$2 \leqslant \ell \leqslant \lfloor \sqrt{k} \rfloor, \tag{29}$$

and fix a k-local system (27) of inner $\mathcal{A}$-multipliers with respect to the outer multiplier $\mathfrak{c}$.

Denote by $\mathcal{R}_\ell = \mathcal{R}_\ell(\mathcal{X})$ the partition of the Cartesian power G^ℓ into the classes of the equivalence relation $\sim_\ell$ defined as follows: $x \sim_\ell y$ if and only if $R_\ell(x) = R_\ell(y)$, where $R_\ell(\cdot) = R_{\mathcal{X},\ell}(\cdot)$ is the $\ell \times \ell$-array defined in formula (7). In particular, each class $\mathscr{X} \in \mathcal{R}_\ell$ is a maximal subset of G^ℓ such that the array $R_\ell(x)$ does not depend on the choice of the ℓ-tuple $x \in \mathscr{X}$. In accordance with [6, Subsection 3.1], we have

$$\mathrm{WL}_\ell(\mathcal{X}) \geqslant \mathcal{R}_\ell(\mathcal{X}), \tag{30}$$

i.e., each class of the partition $\mathcal{R}_\ell(\mathcal{X})$ is a union of some classes of the partition $\mathrm{WL}_\ell(\mathcal{X})$. Furthermore, the algebraic isomorphism φ (of $\mathrm{WL}_\ell(\mathcal{X})$ to itself) induces a permutation of $\mathcal{R}_\ell(\mathcal{X})$, that takes $\mathscr{X}$ to $\mathscr{X}^\varphi = \{y \in G^\ell :\ R(y) = R(x)^\varphi\}$, where $R(x)^\varphi = (r(x_i, x_j)^\varphi)$ and $x \in \mathscr{X}$. In particular,

$$\mathcal{R}_\ell(\mathcal{X})^\varphi = \mathcal{R}_\ell(\mathcal{X}). \tag{31}$$

Let $\mathscr{X}$ be a class of the partition $\mathcal{R}_\ell$, and let $1 \leqslant i, j \leqslant \ell$. The basis relation $s = r(x_i, x_j)$ of the scheme $\mathcal{X}$ does not depend on the ℓ-tuple $x \in \mathscr{X}$. Denote by X_{ij} the basic set of the S-ring $\mathcal{A}$, corresponding to s (see Subsection 5.11). Clearly, $x_j {x_i}^{-1} \in X_{ij}$ for all $x \in \mathscr{X}$. The set

$$\mathfrak{S}(\mathscr{X}) = \{\mathfrak{s}_{X_{ij}} :\ 1 \leqslant i, j \leqslant \ell\} \tag{32}$$

consists of at most $\ell^2 \leqslant k$ principal $\mathcal{A}$-sections $\mathfrak{s}_{X_{ij}}$ and hence $\mathfrak{S}(\mathscr{X}) \in \mathfrak{S}_k$. Denote by $\mathfrak{m}(\mathscr{X})$ the inner $\mathcal{A}$-multiplier $\mathfrak{m}(\mathfrak{S})$ belonging to the family (27) for $\mathfrak{S} = \mathfrak{S}(\mathscr{X})$, and by $f_{\mathscr{X}}$ the isomorphism $f_{\mathfrak{m}(\mathscr{X})} \in \mathrm{Iso}_{\mathcal{A}}(\mathcal{A}_0)$ in Lemma 7 for $\mathfrak{m} = \mathfrak{m}(\mathscr{X})$.

Lemma 10. *In the above notation, the mapping*

$$f : G^\ell \to G^\ell,\ x \mapsto x^{f_{\mathscr{X}}},$$

is a bijection, where $\mathscr{X} \in \mathcal{R}_\ell(\mathcal{X})$ is the class containing the ℓ-tuple x and $x^{f_{\mathscr{X}}}$ denotes the ℓ-tuple $(x_1^{f_{\mathscr{X}}}, \dots, x_\ell^{f_{\mathscr{X}}})$. Moreover,

$$\mathcal{R}_\ell(\mathcal{X})^f = \mathcal{R}_\ell(\mathcal{X}) \quad \textit{and} \quad \mathrm{WL}_\ell(\mathcal{X})^f = \mathrm{WL}_\ell(\mathcal{X}). \tag{33}$$

Proof. First we prove that f is a bijection and the first equality holds true. By equality (31), it suffices to verify that for any $\mathscr{X} \in \mathcal{R}_\ell(\mathcal{X})$, we have $\mathscr{X}^f = \mathscr{X}^\varphi$. To do this, we need to show that $R_\ell(x^f) = R_\ell(x)^\varphi$, or, equivalently, that $r({x_i}^f, {x_j}^f) = r(x_i, x_j)^\varphi$ for all $1 \leqslant i, j \leqslant \ell$. Since $f_{\mathscr{X}}$ is a normalized isomorphism of the S-ring $\mathcal{A}$, we have

$$x_j {x_i}^{-1} \in X_{ij} \quad \Leftrightarrow \quad {x_j}^{f_{\mathscr{X}}} ({x_i}^{f_{\mathscr{X}}})^{-1} \in (X_{ij})^{f_{\mathscr{X}}}.$$

However, $(X_{ij})^{f_{\mathscr{X}}} = {X_{ij}}^\varphi$ by the first condition in (28), and we are done.

To prove the second equality in (33), we need to verify that $\mathscr{X}^f \in \mathrm{WL}_\ell(\mathcal{X})$ for each class $\mathscr{X} \in \mathrm{WL}_\ell(\mathcal{X})$. Note that by virtue of (30), there is a class $\mathscr{X}' \in \mathcal{R}_\ell(\mathcal{X})$ containing $\mathscr{X}$. Therefore, $\mathscr{X}^f = \mathscr{X}^{f_{\mathscr{X}'}}$. Since $f_{\mathscr{X}'} \in \mathrm{Iso}(\mathcal{X})$, we conclude that $\mathscr{X}^{f_{\mathscr{X}'}} \in \mathrm{WL}_\ell(\mathcal{X})$. Thus, $\mathscr{X}^f \in \mathrm{WL}_\ell(\mathcal{X})$, as required. □

The following lemma is a key point in the proof of Theorem 9. Below, for an ℓ-tuple x, we put $x \cdot \alpha = (x_1, \dots, x_\ell, \alpha)$ for all $\alpha \in G$. For any set $\mathscr{X} \subseteq G^{\ell+1}$, we put $\mathrm{Res}_x \mathscr{X} = \{\alpha \in G :\ x \cdot \alpha \in \mathscr{X}\}$.

Lemma 11. *Assume that $m < \lfloor \sqrt{k} \rfloor$. Then given a tuple $x \in G^m$, there is a permutation $\theta \in \mathrm{Sym}(G)$ such that for all $\alpha \in G$*

$$R(x^f \cdot \alpha^\theta) = R(x \cdot \alpha)^\varphi, \tag{34}$$

where $R = R_{m+1}$ and f is the bijection from Lemma 10 for $\ell = m$.

Proof. Denote by $\hat{f} : G^{m+1} \to G^{m+1}$ the bijection f defined in Lemma 10 for $\ell = m + 1$; note that by the assumption on m, we have $\ell \leqslant \lfloor \sqrt{k} \rfloor$. It suffices to prove that if $\hat{\mathscr{X}} \in \mathcal{R}_{m+1}(\mathcal{X})$ and $x \in \mathrm{pr}_m \hat{\mathscr{X}}$, then there exists a bijection $\theta_{\hat{\mathscr{X}}} : \mathrm{Res}_x \hat{\mathscr{X}} \to \mathrm{Res}_{x^f} \hat{\mathscr{X}}^{\hat{f}}$ such that

$$R(x^f \cdot \alpha^{\theta_{\hat{\mathscr{X}}}}) = R(x \cdot \alpha)^\varphi \quad \text{for all } \alpha \in \mathrm{Res}_x \hat{\mathscr{X}}. \tag{35}$$

Indeed, G is a disjoint union of those sets $\mathrm{Res}_x \hat{\mathscr{X}}$ for which $\hat{\mathscr{X}} \in \mathcal{R}_{m+1}(\mathcal{X})$ and $x \in \mathrm{pr}_m \hat{\mathscr{X}}$. Moreover, assuming the existence of the bijections $\theta_{\hat{\mathscr{X}}}$, we see that

$$\mathrm{Res}_{x^f} \hat{\mathscr{X}}^{\hat{f}} \neq \varnothing \quad \Leftrightarrow \quad \mathrm{Res}_x \hat{\mathscr{X}} \neq \varnothing.$$

Thus the required bijection $\theta : G \to G$ can be defined as follows: $\theta(\alpha) = \alpha^{\theta_{\hat{\mathscr{X}}}}$, where $\hat{\mathscr{X}}$ is the class containing the tuple $x \cdot \alpha$.

To prove formula (35), fix $\alpha \in \mathrm{Res}_x\, \hat{\mathscr{X}}$ and put $\mathscr{X} = \mathrm{pr}_m\, \hat{\mathscr{X}}$. Let $\hat{\mathfrak{S}} = \mathfrak{S}(\hat{\mathscr{X}})$ and $\mathfrak{S} = \mathfrak{S}(\mathscr{X})$ be the sets of principal $\mathcal{A}$-sections, defined by formula (32). Then $\mathfrak{S} \subseteq \hat{\mathfrak{S}}$, and $\mathfrak{S}, \hat{\mathfrak{S}} \in \mathfrak{S}_k$ by the choice of m. Since $x \in \mathscr{X}$ and $x \cdot \alpha \in \hat{\mathscr{X}}$, this implies that

$$x^f = x^{f_{\mathscr{X}}} \quad \text{and} \quad (x \cdot \alpha)^{\hat{f}} = (x \cdot \alpha)^{\hat{f}_{\hat{\mathscr{X}}}} = x^{\hat{f}_{\hat{\mathscr{X}}}} \cdot \alpha^{\hat{f}_{\hat{\mathscr{X}}}}. \tag{36}$$

According to our definition, $f_{\mathscr{X}} = f_{\mathfrak{m}(\mathscr{X})}$ and $\hat{f}_{\hat{\mathscr{X}}} = f_{\mathfrak{m}(\hat{\mathscr{X}})}$ are the isomorphisms of the S-ring $\mathcal{A}$, inducing the inner $\mathcal{A}$-multipliers $\mathfrak{m}(\mathfrak{S})$ and $\mathfrak{m}(\hat{\mathfrak{S}})$, respectively. Now the left-hand side of formula (28) implies that

$$\hat{f}^{\mathfrak{s}_{ij}} = \mathfrak{m}(\mathfrak{S}')_{\mathfrak{s}_{ij}} \in \mathfrak{c}_{\mathfrak{s}_{ij}}$$

for all principal $\mathcal{A}$-sections $\mathfrak{s}_{ij} = \mathfrak{s}_{X_{ij}}$ belonging to the subset $\hat{\mathfrak{S}}$. This implies that $(X_{ij})^{\hat{f}} = \varphi(X_{ij})$. By the right-hand side of formula (36), this yields

$$R(x^{\hat{f}} \cdot \alpha^{\hat{f}}) = R(x \cdot \alpha)^{\varphi} \quad \text{for all } \alpha \in \mathrm{Res}_x\, \hat{\mathscr{X}}. \tag{37}$$

At this point, we need an auxiliary statement concerning the array $R_0(\cdot) = R_{\mathcal{X}_0,m}(\cdot)$ defined by formula (7), where $\mathcal{X}_0 = \mathcal{X}(\mathcal{A}_0)$ is the Cayley scheme associated with the S-ring $\mathcal{A}_0$ (recall that $\mathcal{A}_0$ is the coset closure of $\mathcal{A}$).

Claim 12. *Let $h = h(\mathfrak{S}, \hat{\mathfrak{S}})$ be the automorphism of the S-ring $\mathcal{A}$, corresponding to the inner $\mathcal{A}$-multiplier $\mathfrak{m}(\mathfrak{S}, \hat{\mathfrak{S}}) \in \mathfrak{M}_{aut}(\mathcal{A})$ on the right-hand side of formula* (28)*. Then*

$$R_0(x^{\hat{f}}) = R_0(x^{fh}).$$

Proof. We need to verify that for all $1 \leqslant i, j \leqslant m$, the relations $r_0((x^{\hat{f}})_i, (x^{\hat{f}})_j)$ and $r_0((x^{fh})_i, (x^{fh})_j)$ are equal, where $r_0 = r_{\mathcal{X}_0}$. Recall that $\hat{f}_{\hat{\mathscr{X}}} \in \mathrm{Iso}_{\mathcal{A}}(\mathcal{A}_0)$ and hence $\hat{f}_{\hat{\mathscr{X}}} \in \mathrm{Iso}(\mathcal{X}_0)$. Therefore,

$$r_0((x^{\hat{f}})_i, (x^{\hat{f}})_j) = r_0({x_i}^{\hat{f}_{\hat{\mathscr{X}}}}, {x_j}^{\hat{f}_{\hat{\mathscr{X}}}}) = r_0(x_i, x_j)^{\hat{f}_{\hat{\mathscr{X}}}} = r_0(x_i, x_j)^{\hat{f}}. \tag{38}$$

Similarly, since $f_{\mathscr{X}}$ and $h_{\mathscr{X}}$ are also isomorphisms of the scheme $\mathcal{X}_0$, we have

$$r_0((x^{fh})_i, (x^{fh})_j) = r_0(x_i, x_j)^{fh}. \tag{39}$$

It remains to verify that the relations on the right-hand sides of formulas (38) and (39) coincide. Denote by X_0 the basic set of the S-ring $\mathcal{A}_0$ that corresponds to the basis relation $r_0(x_i, x_j)$. Then X_0 contains the element $x_0 = x_j x_i^{-1}$. The element $\bar{x}_0 = (x_0)_{\mathfrak{s}}$ belongs to the set X_{ij} that generates the cyclic group $\mathfrak{s} = \mathfrak{s}_{X_{ij}}$. Since the S-ring $\mathcal{A}$ is totally normal, the S-ring $\mathcal{A}_{\mathfrak{s}}$ is normal and hence every element of X_{ij} is a generator of $\mathfrak{s}$; in particular, $\mathfrak{s} = \langle x_0 \rangle$. It follows that $\mathfrak{s} = \mathfrak{s}_{X_0}$. Consequently,

$$\bar{x}_0{}^{(\hat{f}_{\hat{\mathscr{X}}})^{\mathfrak{s}}} = \bar{x}_0{}^{\hat{\mathfrak{m}}_{\mathfrak{s}}} = \bar{x}_0{}^{\mathfrak{m}_{\mathfrak{s}}\mathfrak{n}_{\mathfrak{s}}} = \bar{x}_0{}^{(f_{\mathscr{X}})^{\mathfrak{s}}(h_{\mathscr{X}})^{\mathfrak{s}}} = \bar{x}_0{}^{(f_{\mathscr{X}} h_{\mathscr{X}})^{\mathfrak{s}}},$$

where $\hat{\mathfrak{m}} = \mathfrak{m}(\hat{\mathfrak{S}})$, $\mathfrak{m} = \mathfrak{m}(\mathfrak{S})$, $\mathfrak{n} = \mathfrak{m}(\mathfrak{S}, \hat{\mathfrak{S}})$, and the equality $\hat{\mathfrak{m}}_{\mathfrak{s}} = m_{\mathfrak{s}} n_{\mathfrak{s}}$ follows from the second equality in (28). Therefore,

$$X_0{}^{\hat{f}} = (\pi^{-1}(\bar{x}_0))^{\hat{f}} = \pi^{-1}(\bar{x}_0{}^{(\hat{f}_{\hat{\mathscr{X}}})^{\mathfrak{s}}}) = \pi^{-1}(\bar{x}_0{}^{(f_{\mathscr{X}} h_{\mathscr{X}})^{\mathfrak{s}}}) = (\pi^{-1}(\bar{x}_0))^{fh} = X_0{}^{fh},$$

where $\pi = \pi_{\mathfrak{s}}$. Thus, $X_0{}^{\hat{f}} = X_0{}^{fh}$, as required. □

By theorem condition, the scheme $\mathcal{X}_0$ is binary. Besides, $R_0(x^{\hat{f}}) = R_0(x^{fh})$ by Claim 12, where $h \in \mathrm{Aut}(\mathcal{A})$. Thus there exists $h_0 \in \mathrm{Aut}(\mathcal{X}_0) \leqslant \mathrm{Aut}(\mathcal{X})$ such that $x^{\hat{f}h_0} = x^{fh}$. Then

$$(x^{\hat{f}} \cdot \alpha^{\hat{f}})^{h_0} = x^{\hat{f}h_0} \cdot \alpha^{\hat{f}h_0} = x^{fh} \cdot \alpha^{\hat{f}h_0h^{-1}h} = (x^f \cdot \alpha^{\hat{f}h_0h^{-1}})^h. \tag{40}$$

Note that $x^{\hat{f}} \cdot \alpha^{\hat{f}} \in \hat{\mathscr{X}}^{\hat{f}}$ by the choice of α. Since h_0 and h^{-1} are automorphisms of the scheme $\mathcal{X}$, this implies that $x^f \cdot \alpha^{\theta_{\hat{\mathscr{X}}}} \in \hat{\mathscr{X}}^{\hat{f}}$, where $\theta_{\hat{\mathscr{X}}} = \hat{f}h_0h^{-1}$ is the composition of isomorphisms of $\mathcal{X}$. In particular,

$$\alpha^{\theta_{\hat{\mathscr{X}}}} \in \mathrm{Res}_{x^f}\, \hat{\mathscr{X}}^{\hat{f}}.$$

To complete the proof, we recall that the point α was chosen in $\mathrm{Res}_x\, \hat{\mathscr{X}}$ arbitrarily. Moreover, none of the isomorphisms $\hat{f}$, h_0, and h depends on α, and the mapping $\theta_{\hat{\mathscr{X}}} : \mathrm{Res}_x\, \hat{\mathscr{X}} \to \mathrm{Res}_{x^f}\, \hat{\mathscr{X}}^{\hat{f}}$ is a bijection. Finally, by formulas (37) and (40) and because of $h_0, h \in \mathrm{Aut}(\mathcal{X})$, we have

$$R(x \cdot \alpha)^{\varphi} = R(x^{\hat{f}} \cdot \alpha^{\hat{f}}) = R(x^{\hat{f}} \cdot \alpha^{\hat{f}})^{h_0h^{-1}} = R(x^f \cdot \alpha^{\hat{f}h_0h^{-1}}) = R(x^f \cdot \alpha^{\theta_{\hat{\mathfrak{X}}}})$$

which proves formula (35). □

Poof of Theorem 9. By Lemma 4, to prove that the scheme $\mathcal{X}$ is WL_m-equivalent to itself with respect to the algebraic isomorphism φ, it suffices to verify that the bijection f defined in Lemma 10 for $\ell = m$ satisfies the condition of Lemma 4. In other words, we need to verify that if $x \in G^m$ and $x' = x^f$, then Duplicator has a winning strategy in the pebble game $\mathscr{C}_{m+1}(\varphi)$ on the scheme $\mathcal{X}$ with initial configuration (x, x'). Let Spoiler choose a set $B \subseteq G$. Duplicator responds with the set $A = B^\theta$, where θ is the bijection defined in Lemma 11. Spoiler places one of the pebbles on a point $\alpha \in A$. Duplicator places the corresponding pebble to the point $b = \alpha^\theta$ and wins, because $R(x \cdot \alpha)^\varphi = R(x' \cdot b)$ by formula (34). □

8 Two ingredients for the main construction

In the sequel, $a = 2b$ is a positive integer and V is a set of cardinality a. We fix a simple graph $\mathcal{G} = (V, E)$ belonging to the class $\mathfrak{B}_a$ defined in Section 1; in particular, $|E| = 3a/2$. It is assumed that $V = \{v_1, \ldots, v_a\}$. The vertices of the parts V_1 and V_2 of the (bipartite) graph $\mathcal{G}$ are denoted by $u_1 := v_1, \ldots, u_b := v_b$ and $w_1 := v_{b+1}, \ldots, w_b := v_a$, respectively.

The graph $\mathcal{G}$ being cubic and bipartite admits a 1-factorization $F_\mathcal{G}$ (see [8, Theorem 5.9(1)]), i.e., the set of three pairwise disjoint matchings the union of which is equal to E. It is convenient to index the matchings of $F_\mathcal{G}$ by the nonidentity elements of the Klein group $K = C_2 \times C_2$; we set $F_\mathcal{G} = \{E_k : k \in K^\#\}$, where $K^\# = K \setminus \{1\}$ and E_k is the matching indexed by k.

8.1 A coherent configuration associated with $\mathcal{G}$

With each vertex $v \in V$ of the graph $\mathcal{G}$, we associate a copy Ω_v of the Klein group K and, for a subset $V' \subseteq V$, we denote by $\Omega_{V'}$ the union of Ω_v, $v \in V'$. When $V' = \{v, v'\}$, we abbreviate $\Omega_{v,v'} := \Omega_{\{v,v'\}}$.

For any $v \in V$ and any $k \in K$, we denote by $\bar{k}_v$ the permutation $x \mapsto xk$, $x \in K$, on the copy Ω_v of the group K. The set $\bar{K}_v = \{\bar{k}_v : \ k \in K\}$ is a permutation group on Ω_v, that is isomorphic to K. The direct product

$$K_V = \prod_{v \in V} \bar{K}_v,$$

is a permutation group on the set $\Omega = \Omega_V$; the orbits of K_V are the sets Ω_v. It was proved in [9, Section 5] that there exists a coherent configuration $\mathcal{X} = \mathcal{X}(\mathcal{G}, F_{\mathcal{G}}) = (\Omega, S)$ that satisfies the following conditions:

(K1) $F(\mathcal{X}) = \{\Omega_v : \ v \in V\}$, and also $\mathrm{Aut}(\mathcal{X})^{\Omega_v} = \bar{K}_v$ for all v,

(K2) the group of all $f \in \mathrm{Iso}(\mathcal{X})$ such that ${\Omega_v}^f = \Omega_v$ and $f^{\Omega_v} \in \bar{K}_v$ for all $v \in V$, coincides with K_V,

(K3) $\mathrm{Aut}(\mathcal{X})^{\Omega_{v,v'}} = \bar{K}_v \times \bar{K}_{v'}$ for all distinct $v, v' \in V$ nonadjacent in $\mathcal{G}$,

(K4) if $\{v, v'\} \in E_k$ for some $k \in K^{\#}$, then

$$\mathrm{Aut}(\mathcal{X})^{\Omega_{v,v'}} = \{(x, x') \in \bar{K}_v \times \bar{K}_{v'} : \ \bar{\rho}_v(x) = \bar{\rho}_{v'}(x')\},$$

where $\bar{\rho}_v : \bar{K}_v \to \mathrm{Sym}(2)$ and $\bar{\rho}_{v'} : \bar{K}_{v'} \to \mathrm{Sym}(2)$ are the natural epimorphisms with kernels $\langle \bar{k}_v \rangle$ and $\langle \bar{k}_{v'} \rangle$, respectively,

(K5) if $\{u, w\} \in E$ and $\psi \in \mathrm{Sym}(S)$ are such that $\psi(s) \neq s$ if and only if $s \subseteq (\Omega_u \times \Omega_w) \cup (\Omega_w \times \Omega_u)$, then ψ is an algebraic automorphism of $\mathcal{X}$.

The details concerning the construction and other properties of the coherent configuration $\mathcal{X}$ can also be found in [5, Subsections 4.1.3 and 4.2.1], where $\mathcal{X}$ is defined as a special case of a cubic Klein configuration.

To state the main fact about the coherent configuration $\mathcal{X}$, that we need later, we fix an edge $e_0 \in E$ and set $\psi = \psi_{e_0}$ to be the algebraic isomorphism in condition (K5) for $e = e_0$. Next, for an integer $m \geqslant 1$, we put

$$F_m = F_m(\mathcal{X}) = \{\Omega_{V'} : \ |V'| \leqslant m\}.$$

A family $\{f_\Delta \in K_V : \Delta \in F_m\}$ is called an *m-local system of isomorphisms for $\mathcal{X}$* with respect to ψ if for all $\Delta, \Delta' \in F_m$, we have

$$(f_\Delta)^\Delta \in \mathrm{Iso}(\mathcal{X}_\Delta, \psi_\Delta) \quad \text{and} \quad (f_\Delta {f_{\Delta'}}^{-1})^{\Delta \cap \Delta'} \in \mathrm{Aut}(\mathcal{X})^{\Delta \cap \Delta'},$$

where $\mathcal{X}_\Delta$ and ψ_Δ are the restrictions of $\mathcal{X}$ and ψ to Δ, respectively.

Lemma 13. *In the above notation, assume that each separator*[5] *of the graph $\mathcal{G}$ has cardinality greater than $3m$. Then $\mathrm{Iso}(\mathcal{X}, \psi) = \varnothing$ and there is an m-local system of isomorphisms for the coherent configuration $\mathcal{X}$ with respect to the algebraic isomorphism ψ.*

Proof. Follows from Lemma 4.2.6 in [5] and its proof. □

8.2 A coset S-ring associated with the graph $\mathcal{G}$

Let a and b be the integers as above, and let n be as in Theorem 1. We define an S-ring over the group $G = C_n$ as the tensor product of two iterated wreath products of the group rings of cyclic groups,

$$\mathcal{A} = (\mathbb{Z}C_{n_1} \wr \mathbb{Z}C_{n_2} \wr \cdots \wr \mathbb{Z}C_{n_b}) \otimes (\mathbb{Z}C_{n_{b+1}} \wr \mathbb{Z}C_{n_{b+2}} \wr \cdots \wr \mathbb{Z}C_{n_{2b}}), \tag{41}$$

where the numbers n_i are as in Theorem 1. For any vertex $v \in V$ of the graph $\mathcal{G}$, we denote by G_v the (cyclic) subgroup of G such that

$$|G_v| = \begin{cases} n_1 \cdot \ldots \cdot n_i & \text{if } v = u_i \text{ with } 1 \leqslant i \leqslant b, \\ n_{b+1} \cdot \ldots \cdot n_{b+j} & \text{if } v = w_j \text{ with } 1 \leqslant j \leqslant b. \end{cases}$$

Clearly, $G = G_{u_b} \times G_{w_b}$ and $\mathcal{A}$ is the tensor product of the two iterated wreath products in formula (41). The statement below immediately follows from remarks in Subsection 5.9) and Theorem 3.

Lemma 14. *The S-ring $\mathcal{A}$ is a coset S-ring and the (circulant) scheme $\mathcal{X}(\mathcal{A})$ is binary.*

We enlarge the bipartition sets V_1 and V_2 by adding to them new elements u_0 and w_0, respectively, and set $G_{u_0} = G_{w_0} = 1$. Then G_v is an $\mathcal{A}$-subgroup for each v, including these new elements. Moreover,

$$G_{u_0} < G_{u_1} < \ldots < G_{u_b} \quad \text{and} \quad G_{w_0} < G_{w_1} < \ldots < G_{w_b}. \tag{42}$$

We sometimes identify the subgroups G_{u_i} and $G_{u_i} \times G_{w_0}$, and G_{w_j} with $G_{u_0} \times G_{w_j}$. Below, for any vertex v of the graph $\mathcal{G}$, we define a section $\mathfrak{s}_v$ of the group G as follows:

$$\mathfrak{s}_v = \begin{cases} G_{u_i}/G_{u_{i-1}} & \text{if } v = u_i \text{ with } 1 \leqslant i \leqslant b, \\ G_{w_j}/G_{w_{j-1}} & \text{if } v = w_j \text{ with } 1 \leqslant j \leqslant b. \end{cases}$$

Lemma 15.

(1) *Each $\mathcal{A}$-subgroup is of the form $U \times W$, where $G_{u_{i-1}} \leqslant U \leqslant G_{u_i}$ and $G_{w_{j-1}} \leqslant W \leqslant G_{w_j}$ for some $1 \leqslant i, j \leqslant b$,*

[5] A separator of the graph $\mathcal{G}$ is a subset $V' \subset V$ satisfying the following condition: each connected component of the graph obtained from $\mathcal{G}$ by removing all the vertices of V' contains at most half vertices of $\mathcal{G}$.

(2) $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$ *if and only if* $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$ *for some* $u \in V_1$ *and* $w \in V_2$, *where* $\mathfrak{s}_{u,w} = \mathfrak{s}_u \times \mathfrak{s}_w$.

Proof. Let $u = u_b$ and $w = w_b$. Since the group $G = G_u \times G_w$ is cyclic, any subgroup $H \leqslant G$ is the direct product of two subgroups $U := H \cap G_u$ and $W := H \cap G_w$. Assume that H is an $\mathcal{A}$-subgroup. Since obviously G_u and G_w are also $\mathcal{A}$-subgroups, so is U and hence it is an $\mathcal{A}_{G_u}$-subgroup. By the first part of formula (42), there is the smallest $i \in \{1, \dots, b\}$ such that $U \leqslant G_{u_i}$. Without loss of generality, we assume that $U \neq 1$. Then U is an $(\mathcal{A}_{i-1} \wr \mathbb{Z}C_{n_i})$-subgroup, where $\mathcal{A}_{i-1}$ is the restriction of $\mathcal{A}$ to $G_{u_{i-1}}$. The minimality of i implies that $U \geqslant G_{u_{i-1}}$ (see Subsection 5.4). Thus, $G_{u_{i-1}} \leqslant U \leqslant G_{u_i}$. Similarly, one can prove that $G_{w_{j-1}} \leqslant W \leqslant G_{w_j}$ for some $1 \leqslant j \leqslant b$. Statement (1) is proved.

To prove statement (2), let $u \in V_1$ and $w \in V_2$ be arbitrary. The necessity is a consequence of the fact that $\mathfrak{s}_{u,w}$ is a principal section. Conversely, let $\mathfrak{s}$ be an $\mathcal{A}$-section. By statement (1), there exist subgroups $U' \leqslant U \leqslant G_{u_b}$ and $W' \leqslant W \leqslant G_{w_b}$ such that

$$\mathfrak{s} = (U \times W)/(U' \times W') = (U/U') \times (W/W'),$$

It follows that $\mathfrak{s} = \mathfrak{s}_1 \times \mathfrak{s}_2$, where $\mathfrak{s}_1 = U/U'$ and $\mathfrak{s}_2 = W/W'$. Assume that $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$. Let us verify that $\mathfrak{s}_1 \preceq \mathfrak{s}_u$ for some $u \in V_1$; the fact that $\mathfrak{s}_2 \preceq \mathfrak{s}_w$ for some $w \in V_2$, is proved similarly.

By [14, Theorem 8.3], we have $\mathcal{A}_{\mathfrak{s}} = \mathbb{Z}\,\mathfrak{s}$ and hence $\mathcal{A}_{\mathfrak{s}_1} = \mathbb{Z}\,\mathfrak{s}_1$. Without loss of generality, we may assume that $U \neq 1$ (otherwise one can take $u = 1$). Then $G_{u_{i-1}} < U \leqslant G_{u_i}$ for some $1 \leqslant i \leqslant b$. Now if $U' < G_{u_{i-1}}$, then setting $\mathfrak{t} = G_{u_{i-1}}/U'$ and $\mathfrak{t}' = U/G_{u_{i-1}}$, we obtain

$$\mathbb{Z}\,\mathfrak{s}_1 = \mathcal{A}_{\mathfrak{s}_1} = \mathcal{A}_{\mathfrak{t}} \wr \mathcal{A}_{\mathfrak{t}'} \neq \mathbb{Z}\,\mathfrak{s}_1,$$

a contradiction. Thus, $G_{u_{i-1}} \leqslant U' \leqslant U \leqslant G_{u_i}$, and we are done with $v = u_i$. □

In the following lemma, we show that the inner $\mathcal{A}$-multipliers are in a one-to-one correspondence with the elements of the direct product of the groups $\mathrm{Aut}(\mathfrak{s}_v)$, $v \in V$.

Lemma 16. *Put* $\mathfrak{S} = \{\mathfrak{s}_v : v \in V\}$ *and* $\mathfrak{M} = \mathfrak{M}(\mathcal{A})$. *Then*

(1) $\bar{\mathfrak{m}} \in \mathfrak{M}_{\mathfrak{S}}$ *if and only if* $\bar{\mathfrak{m}} = \{\sigma_v \in \mathrm{Aut}(\mathfrak{s}_v) : v \in V\}$,

(2) *the mapping* $\mathfrak{M} \to \mathfrak{M}_{\mathfrak{S}}$, $\mathfrak{m} \mapsto \mathfrak{m}_{\mathfrak{S}}$, *is a group monomorphism.*

Proof. The necessity in statement (1) is trivial. To prove the sufficiency, we need to find an inner $\mathcal{A}$-multiplier $\mathfrak{m}$ such that $\mathfrak{m}_{\mathfrak{S}} = \bar{m}$. First, put

$$\mathfrak{m}_{\mathfrak{s}_{u,w}} = (\sigma_u, \sigma_w) \tag{43}$$

for all $u \in V_1$ and $w \in V_2$. Now let section $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$ be arbitrary. By Lemma 15(2), there exist u and w such that $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$. Put

$$\mathfrak{m}_{\mathfrak{s}} := (\mathfrak{m}_{\mathfrak{s}_{u,w}})^{\mathfrak{s}}. \tag{44}$$

We claim that $\mathfrak{m}_\mathfrak{s}$ does not depend on the choice of u and w for which $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$. Indeed, let $\mathfrak{s} \preceq \mathfrak{s}_{u',w'}$ for some u' and w' such that $u \neq u'$ or $w \neq w'$. Then either $u = u'$ and $w \neq w'$, or $u \neq u'$ and $w = w'$ (because the sections $\mathfrak{s}_{u,w}$ and $\mathfrak{s}_{u',w'}$ have no common subsections if $u \neq u'$ and $w \neq w'$). Assume the first case occurs (in the second case the proof is similar). Then $\mathfrak{s} = \mathfrak{t} \times \mathfrak{t}'$ where $\mathfrak{t} \preceq \mathfrak{s}_u$ and $\mathfrak{t}'$ is a trivial subsection of both $\mathfrak{s}_w$ and $\mathfrak{s}_{w'}$. It follows that

$$(\mathfrak{m}_{\mathfrak{s}_{u,w}})^\mathfrak{s} = ({\sigma_u}^\mathfrak{t}, {\sigma_w}^{\mathfrak{t}'}) = ({\sigma_u}^\mathfrak{t}, \mathrm{id}_{\mathfrak{t}'}) = ({\sigma_{u'}}^\mathfrak{t}, {\sigma_{w'}}^{\mathfrak{t}'}) = (\mathfrak{m}_{\mathfrak{s}_{u',w'}})^\mathfrak{s},$$

which proves the claim.

From the above, it follows that the family $\mathfrak{m}$ defined by formulas (43) and (44) satisfies the first condition in (17) and the equality $\bar{\mathfrak{m}} = \mathfrak{m}_\mathfrak{S}$. To prove that $\mathfrak{m}$ is an inner $\mathcal{A}$-multiplier, we need to verify the second condition in (17). Let $\mathfrak{s}$ and $\mathfrak{t}$ be projectively equivalent $\mathcal{A}$-sections belonging to $\mathfrak{S}_0(\mathcal{A})$. Without loss of generality we may assume that both $\mathfrak{s}$ and $\mathfrak{t}$ are subsections of a section $\mathfrak{s}_{u,w}$ for some u and w. The automorphism $\mathfrak{m}_{\mathfrak{s}_{u,w}}$ of the cyclic group $\mathfrak{s}_{u,w}$ acts by raising to a certain integer power λ. Hence the automorphisms $\mathfrak{m}_\mathfrak{s} = (\mathfrak{m}_{\mathfrak{s}_{u,w}})^\mathfrak{s}$ and $\mathfrak{m}_\mathfrak{t} = (\mathfrak{m}_{\mathfrak{s}_{u,w}})^\mathfrak{t}$ act by raising to the powers $\lambda \pmod{|\mathfrak{s}|}$ and $\lambda \pmod{|\mathfrak{t}|}$, respectively. Since $|\mathfrak{s}| = |\mathfrak{t}|$ and the isomorphism $f_{\mathfrak{s},\mathfrak{t}} : \mathfrak{s} \to \mathfrak{t}$ preserves raising to a power, we conclude that $(\mathfrak{m}_\mathfrak{s})^{f_{\mathfrak{s},\mathfrak{t}}} = \mathfrak{m}_\mathfrak{t}$, as required.

To prove statement (2), assume that $\mathfrak{m} \in \mathfrak{M}$ is such that $\mathfrak{m}_\mathfrak{s} = \mathrm{id}_\mathfrak{s}$ for all $\mathfrak{s} \in \mathfrak{S}$. Note that if $u \in V_1$ and $w \in V_2$, then $\mathfrak{m}_{\mathfrak{s}_{u,w}} = (\mathfrak{m}_{\mathfrak{s}_u}, \mathfrak{m}_{\mathfrak{s}_w}) = \mathrm{id}_{\mathfrak{s}_{u,w}}$. Now let $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$. By Lemma 15(2), we have $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$ for some u and w. By the first condition in (17), this implies that

$$\mathfrak{m}_\mathfrak{s} = (\mathfrak{m}_{\mathfrak{s}_{u,w}})^\mathfrak{s} = (\mathrm{id}_{\mathfrak{s}_{u,w}})^\mathfrak{s} = \mathrm{id}_\mathfrak{s}\,.$$

Thus the $\mathfrak{m}$ is the trivial inner $\mathcal{A}$-multiplier and we are done. □

The basic sets of the S-ring $\mathcal{A}$ can conveniently be divided into parts parameterized by the $\mathcal{A}$-sets defined below; this parameterization will be used in Section 10. Namely, by Lemma 15, for any two indices $1 \leqslant i, j \leqslant b$, there is an $\mathcal{A}$-subgroup $G_{i,j} = G_{u_i} \times G_{w_j}$. It follows that the difference

$$D_{i,j} = G_{i,j} \setminus G_{i-1,j-1} \tag{45}$$

is an $\mathcal{A}$-set. Since any nonidentity element of G belongs to some of these differences, the union of all of them is equal to $G^\#$ and each nonidentity set $X \in \mathcal{S}(\mathcal{A})$ is contained in at least one of them. Moreover, it is not hard to verify that

$$X \subseteq D_{i,j} \quad \Leftrightarrow \quad X = \pi_{i,j}^{-1}(x) \text{ for some } 1 \neq x \in \mathrm{im}(\pi_{i,j}), \tag{46}$$

where $\pi_{i,j} : G_{i,j} \to G_{i,j}/G_{i-1,j-1}$ is the natural epimorphism.

8.3 Inner $\mathcal{A}$-multipliers associated with $\mathcal{G}$

Let $v = v_i$ be a vertex of the graph $\mathcal{G}$, $1 \leqslant i \leqslant a$. Then $\mathfrak{s}_v = C_{n_i}$ is a (cyclic) group of order $n_i = p_i q_i$, where p_i and q_i are distinct odd primes, $p_i < q_i$. It follows that the group

$$\mathrm{Aut}(\mathfrak{s}_v) = \mathrm{Aut}(C_{p_i}) \times \mathrm{Aut}(C_{q_i})$$

has a uniquely determined Klein subgroup $K_v = \{k_v : \ k \in K\}$. For definiteness, we assume that for a fixed $k \in K^{\#}$ exactly one of the conditions

$$k_{v_i} \in \mathrm{Aut}(C_{p_i}) \quad \text{or} \quad k_{v_i} \in \mathrm{Aut}(C_{q_i}) \quad \text{or} \quad k_{v_i} \notin \mathrm{Aut}(C_{p_i}) \text{ and } k_{v_i} \notin \mathrm{Aut}(C_{q_i})$$

is satisfied simultaneously for $i = 1, \ldots, a$; in the latter case, k_{v_i} is equal to the product of two involutions, one in $\mathrm{Aut}(C_{p_i})$ and another in $\mathrm{Aut}(C_{q_i})$. Clearly, the mapping

$$\pi_v : \bar{K}_v \to K_v, \ \bar{k}_v \mapsto k_v, \tag{47}$$

is a group isomorphism for all $v \in V$. The lemma below immediately follows from Lemma 16.

Lemma 17. *Let $\mathfrak{M} = \mathfrak{M}(\mathcal{A})$ and $f \in K_V$. Then there is a unique inner $\mathcal{A}$-multiplier $\mathfrak{m}_f \in \mathfrak{M}$ such that $(\mathfrak{m}_f)_{\mathfrak{s}_v} = \pi_v(f_v)$ for all $v \in V$, Moreover, the mapping*

$$\mu : K_V \to \mathfrak{M}, \ f \mapsto \mathfrak{m}_f,$$

is a group monomorphism and $\mathrm{im}(\mu) = \{\mathfrak{m} \in \mathfrak{M} : \ \mathfrak{m}_{\mathfrak{s}_v} \in K_v\}$.

9 The construction

9.1 The main theorem

In this section, we construct an S-ring $\mathcal{A}^\star$ and a set of $\mathcal{A}^\star$-multipliers. They will be used to prove Theorem 1 in Section 10. The relevant properties of $\mathcal{A}^\star$ are given in the theorem below.

Theorem 18. *Let $\mathcal{G} \in \mathfrak{B}_a$ and k a positive integer. Assume that each separator of the graph $\mathcal{G}$ has cardinality greater than k. Then there exist*

(1) *a totally normal circulant S-ring $\mathcal{A}^\star$ of degree n defined as in Theorem 1, such that the scheme $\mathcal{X}((\mathcal{A}^\star)_0)$ is binary,*

(2) *an outer $\mathcal{A}^\star$-multiplier $\mathfrak{c}$ such that $\mathrm{Iso}(\mathcal{A}^\star, \varphi_{\mathfrak{c}}) = \varnothing$, and*

(3) *a $\lfloor k/6 \rfloor$-local system of inner $\mathcal{A}^\star$-multipliers with respect to $\mathfrak{c}$.*

The proof will be given in the end of the section. In what follows, we keep notation of Section 8.

9.2 Construction of the S-ring $\mathcal{A}^\star$

Let $\mathcal{X}$ be the coherent configuration defined in Subsection 8.1. By the condition (K3), we have $\mathrm{Aut}(\mathcal{X}) \leqslant K_V$. Let

$$\mathfrak{M} = \mu(\mathrm{Aut}(\mathcal{X})),$$

where μ is the monomorphism defined in Lemma 17. As a consequence of conditions (K1), (K3), and (K4), and Lemma 17, we have the following statement, in which we abbreviate $\mathfrak{M}_v := \mathfrak{M}_{\mathfrak{s}_v}$ and $\mathfrak{M}_{v,v'} := \mathfrak{M}_{\{\mathfrak{s}_v, \mathfrak{s}_{v'}\}}$ for all $v, v' \in V$, and denote by $\rho_v : K_v \to \mathrm{Sym}(2)$ the natural epimorphism with kernel $\langle k_v \rangle$.

Lemma 19. *In the above notation, $\mathfrak{M}_v = K_v$ for all $v \in V$. Furthermore, if $v' \in V$, then*

$$\mathfrak{M}_{v,v'} = \begin{cases} \{(x,y) \in K_v \times K_{v'} : \ \rho_v(x) = \rho_{v'}(y)\} & \text{if } (v,v') \in E, \\ K_v \times K_{v'} & \text{otherwise.} \end{cases}$$

Let $\mathcal{A}$ be the S-ring defined in Subsection 8.2. Denote by $\mathcal{A}^\star$ the algebraic fusion of $\mathcal{A}$ with respect to the subgroup $\mathfrak{M} \leqslant \mathfrak{M}(\mathcal{A})$,

$$\mathcal{A}^\star = \mathcal{A}^{\mathfrak{M}}.$$

Since $\mathcal{A}$ and $\mathcal{A}^\star$ have the same $\mathcal{A}$-subgroups (formula (25)), the subsets $D_{i,j}$ defined by formula (45) are $\mathcal{A}^\star$-sets for all i, j.

Let $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$ for some $u \in V_1$ and $w \in V_2$. Then from Lemma 19, it follows that

$$\mathfrak{M}_{\mathfrak{s}} \leqslant (K_u)^{\mathfrak{s}} \times (K_w)^{\mathfrak{s}} \leqslant \mathrm{Aut}(\mathfrak{s}).$$

Since the group $\mathfrak{s}$ is of odd order whereas the groups $(K_u)^{\mathfrak{s}}$ and $(K_w)^{\mathfrak{s}}$ are of order at most 4, the cyclotomic S-ring $\mathrm{cyc}(\mathfrak{M}_{\mathfrak{s}}, \mathfrak{s})$ is normal by [10, Theorem 6.1]. By Lemma 8, this implies that

$$\mathfrak{S}_0(\mathcal{A}^\star) = \mathfrak{S}_0(\mathcal{A}) \quad \text{and} \quad (\mathcal{A}^\star)_0 = \mathcal{A}. \tag{48}$$

Lemma 20. *The S-ring $\mathcal{A}^\star$ is totally normal.*

Proof. Let $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A}^\star)$. Then $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A})$ by the left-hand side of formula (48). By Lemma 15(2), this implies that $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$ for some $u \in V_1$ and $w \in V_2$. Since by the above, the S-ring $(\mathcal{A}^\star)_{\mathfrak{s}} = \mathrm{cyc}(\mathfrak{M}_{\mathfrak{s}}, \mathfrak{s})$ is normal, we are done. □

9.3 An outer multiplier

In the notation of Subsection 8.1, fix an arbitrary edge $e_0 = \{u_{i_0}, w_{j_0}\}$ of the graph $\mathcal{G}$ and the algebraic automorphism $\psi = \psi_{e_0}$ of the coherent configuration $\mathcal{X}$. From condition (K4), it follows that the group $\mathrm{Aut}(\mathcal{X})^{\Omega_{e_0}}$ has index 2 in the group $\bar{K}_{u_{i_0}} \times \bar{K}_{w_{j_0}}$. Choose any permutation $\bar{k}_0$ of this group, not belonging to $\mathrm{Aut}(\mathcal{X})^{\Omega_{e_0}}$, and define the permutation $k_0 \in \mathrm{Aut}(\mathfrak{s}_{e_0})$ by the conditions

$$(k_0)_{\mathfrak{s}_u} = \pi_u((\bar{k}_0)_u) \quad \text{and} \quad (k_0)_{\mathfrak{s}_w} = \pi_w((\bar{k}_0)_w),$$

where $u = u_{i_0}$ and $w = w_{j_0}$. The definition of the monomorphism μ implies that if $f \in K_V$ and $f^{e_0} = \bar{k}_0$, then $(\mu(f))_{e_0} = k_0$.

Let $u \in V_1$ and $w \in V_2$. Then the section $\mathfrak{s} = \mathfrak{s}_{u,w}$ belongs to $\mathfrak{S}_0(\mathcal{A})$, see Lemma 15(2). By formula (48), this implies that $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A}^\star)$. Let us define a coset $\mathfrak{c}_{\mathfrak{s}}$ of the subgroup $\mathfrak{M}_{\mathfrak{s}} \leqslant \mathrm{Aut}(\mathfrak{s})$ by the formula

$$\mathfrak{c}_{\mathfrak{s}} = \begin{cases} k_0 \cdot \mathfrak{M}_{\mathfrak{s}} & \text{if } \mathfrak{s} = \mathfrak{s}_{e_0}, \\ \mathfrak{M}_{\mathfrak{s}} & \text{otherwise,} \end{cases} \tag{49}$$

where $\mathfrak{s}_{e_0} = \mathfrak{s}_{u',w'}$ with $u' = u_{i_0}$ and $w' = w_{j_0}$. We extend this definition to all sections $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A}^\star)$ by setting $\mathfrak{c}_\mathfrak{s} = \mathfrak{c}_{\mathfrak{s}_{u,w}}$ for suitable u, w (see Lemma 15(2) and formula (48)). Furthermore, by formula (24), we have

$$(\mathcal{A}^\star)_\mathfrak{s} = \mathrm{cyc}(\mathfrak{M}_\mathfrak{s}, \mathfrak{s}).$$

This S-ring is normal by Lemma 20 and hence $\mathfrak{M}_\mathfrak{s} = \mathrm{Aut}_{\mathcal{A}^\star}(\mathfrak{s})$ by Lemma 6(3). Using arguments in the proof of Lemma 16, one can verify that the family $\mathfrak{c} := \mathfrak{c}(e_0)$ of the cosets $\mathfrak{c}_\mathfrak{s}$, $\mathfrak{s} \in \mathfrak{S}_0(\mathcal{A}^\star)$, is an outer $\mathcal{A}^\star$-multiplier.

In the following statement, we establish a relationship between the isomorphisms of the coherent configuration $\mathcal{X}$, the corresponding inner multipliers in $\mathfrak{M}$, and the outer multiplier $\mathfrak{c}$.

Lemma 21. *Let $f \in K_V$ and $e = \{v, v'\}$, where $v, v' \in V$ and $v \neq v'$. Then*

$$f^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e}) \quad \Leftrightarrow \quad \text{either } e \notin E \text{ or } (\mathfrak{m}_f)_e \in \mathfrak{c}_e, \tag{50}$$

where $\mathfrak{m}_f = \mu(f)$ with μ as in Lemma 17, $(\mathfrak{m}_f)_e = (\mathfrak{m}_f)_{\mathfrak{s}_e}$, and $\mathfrak{c}_e = \mathfrak{c}_{\mathfrak{s}_e}$.

Proof. We note that if $e \notin E$, then $\mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e}) = \bar{K}_v \times \bar{K}_{v'}$ and $f^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e})$ by condition (K5). Assume that $e \in E$.

Let $e \neq e_0$. Then $\mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e}) = \mathrm{Aut}(\mathcal{X}_{\Omega_e})$ by condition (K4). Therefore, $f^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e})$ if and only if

$$(\mathfrak{m}_f)_e \in \mu_e(\mathrm{Aut}(\mathcal{X}_{\Omega_e})) = \mathfrak{M}_e = \mathfrak{M}_{\mathfrak{s}_{v,v'}} = \mathfrak{c}_{\mathfrak{s}_{v,v'}} = \mathfrak{c}_e,$$

see Lemma 19, where μ_e is the restriction of the monomorphism μ to e.

Finally, let $e = e_0$, i.e., $\{v, v'\} = \{u_{i_0}, w_{j_0}\}$. Then by condition (K4), the group $\mathrm{Aut}(\mathcal{X}_{\Omega_e})$ has index 2 in the group $\bar{K}_{u_{i_0}} \times \bar{K}_{w_{j_0}}$. By virtue of condition (K5), we have

$$\mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e}) = \bar{k}_0 \cdot \mathrm{Aut}(\mathcal{X}_{\Omega_e}),$$

where $\bar{k}_0$ is the permutation chosen at the beginning of this subsection. Thus, $f^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e})$ if and only if

$$(\mathfrak{m}_f)_e \in \mu_e(\bar{k}_0 \cdot \mathrm{Aut}(\mathcal{X}_{\Omega_0})) = \mathfrak{M}_{e_0} = \mathfrak{M}_{\mathfrak{s}_{u,w}} = \mathfrak{c}_{\mathfrak{s}_{u,w}} = \mathfrak{c}_{e_0},$$

as required, where $\Omega_0 = \Omega_{e_0}$, $u = u_{i_0}$ and $w = w_{j_0}$. □

9.4 Proof of Theorem 18

Let $\mathcal{A}^\star$ be the S-ring over the group G, defined in Subsection 9.2. By Lemma 20, this S-ring is totally normal. By formula (48), we have $(\mathcal{A}^\star)_0 = \mathcal{A}$. Hence the scheme $\mathcal{X}((\mathcal{A}^\star)_0)$ associated with the S-ring $(\mathcal{A}^\star)_0$ is binary by Lemma 14. Thus it suffices to verify that statements (2) and (3) of the theorem in question hold true for the outer $\mathcal{A}^\star$-multiplier $\mathfrak{c}$ defined in Subsection 9.3.

To prove statement (2), assume on the contrary that there is $g \in \mathrm{Iso}(\mathcal{A}^\star, \varphi_{\mathfrak{c}})$. Without loss of generality, we may assume that the isomorphism g is normalized. Since the group G is of odd order and the S-ring $\mathcal{A}^\star$ is totally normal, the family

$$\mathfrak{m} = \{g^{\mathfrak{s}} : \ \mathfrak{s} \in \mathfrak{S}_0(\mathcal{A}^\star)\}$$

is an inner $\mathcal{A}^\star$-multiplier, see the end of Subsection 6.2. Furthermore, $\mathfrak{m}$ is an inner $\mathcal{A}$-multiplier by the first equality in (48). In addition, $\mathfrak{m} \leqslant \mathfrak{c}$ and hence

$$\mathfrak{m}_{\mathfrak{s}_v} = g^{\mathfrak{s}_v} \in \mathfrak{c}_{\mathfrak{s}_v} = \mathfrak{M}_{\mathfrak{s}_v} = K_v \qquad v \in V.$$

By Lemma 17, this shows that $f = \mu^{-1}(\mathfrak{m})$ is an isomorphism of the coherent configuration $\mathcal{X}$, belonging to the group K_V. Furthermore, let $e = \{v, v'\}$, where $v, v' \in V$ and $v \neq v'$. Then

$$(\mathfrak{m}_f)_e = (\pi_v(f_v), \pi_{v'}(f_{v'})) = (g_v, g_{v'}) = \mathfrak{m}_e \in \mathfrak{c}_e,$$

where π_v and $\pi_{v'}$ are the isomorphisms defined in formula (47). By Lemma 21, this implies that $f^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e})$. It follows that $f \in \mathrm{Iso}(\mathcal{X}, \psi)$, which contradicts Lemma 13.

Let us prove statement (3). Put $m = \lfloor k/6 \rfloor$. The graph $\mathcal{G}$ has no separators of cardinality at most $3 \cdot (2m) \leqslant k$. By Lemma 13, there exists an $(2m)$-local system

$$\{f_\Delta \in K_V : \Delta \in F_{2m}(\mathcal{X})\} \tag{51}$$

of isomorphisms for the coherent configuration $\mathcal{X}$ with respect to the algebraic isomorphism ψ.

Let $\mathfrak{S} \subseteq \mathfrak{S}_m$, where $\mathfrak{S}_m = \mathfrak{S}_m(\mathcal{A}^\star)$. By formula in (48) and Lemma 15(2), there is a minimal (by inclusion) subset $\bar{V} = \bar{V}(\mathfrak{S})$ of the set V such that if $\mathfrak{s} \in \mathfrak{S}$, then $\mathfrak{s} \preceq \mathfrak{s}_{u,w}$ for some $u \in V_1 \cap \bar{V}$ and $w \in V_2 \cap \bar{V}$. Clearly,

$$|\bar{V}| \leqslant 2 \cdot |\mathfrak{S}| \leqslant 2 \cdot m$$

and hence $\Omega_{\bar{V}} \in F_{2m}(\mathcal{X})$. Thus the $(2m)$-local system (51) contains an isomorphism $f_\Delta \in K_V$ of the coherent configuration $\mathcal{X}$, where $\Delta = \Omega_{\bar{V}}$. Denote by $\mathfrak{m}(\mathfrak{S})$ the inner $\mathcal{A}$-multiplier $\mu(f_\Delta)$.

To complete the proof, it suffices to verify that the family

$$\{\mathfrak{m}(\mathfrak{S}) \in \mathfrak{M}(\mathcal{A}^\star) : \ \mathfrak{S} \in \mathfrak{S}_m\}$$

is an m-local system of inner $\mathcal{A}^\star$-multipliers with respect to the outer $\mathcal{A}^\star$-multiplier $\mathfrak{c}$.

To verify the first relation in (28), let $\mathfrak{S} \in \mathfrak{S}_m$ and $\mathfrak{s} \in \mathfrak{S}$. By Lemma 15(2), we may assume without loss of generality that $\mathfrak{s} = \mathfrak{s}_{u,w}$ for some vertices $u \in V_1 \cap \bar{V}$ and $w \in V_2 \cap \bar{V}$, where $\bar{V} = \bar{V}(\mathfrak{S})$. Since $u, w \in \bar{V}$, we have $\Omega_{u,w} \subseteq \Omega_{\bar{V}} := \Delta$. By the definition of f_Δ, this implies that $(f_\Delta)^{\Omega_e} \in \mathrm{Iso}(\mathcal{X}_{\Omega_e}, \psi_{\Omega_e})$, where $e = \{u, w\}$. By Lemma 21, either $e \notin E$, or $e \in E$ and

$$\mathfrak{m}(\mathfrak{S})_{\mathfrak{s}} = \mu(f_\Delta)_{\mathfrak{s}} = \mu(f_\Delta)_{\mathfrak{s}_e} \in \mathfrak{c}_e = \mathfrak{c}_{\mathfrak{s}}.$$

Finally, if $e \notin E$, then $\mathfrak{m}(\mathfrak{S})_{\mathfrak{s}} \in K_u \times K_w = \mathfrak{c}_{\mathfrak{s}}$.

To verify the second relation in (28), let $\mathfrak{S}, \mathfrak{S}' \in \mathfrak{S}_m$. Put $\Delta = \Omega_{\bar{V}}$ and $\Delta' = \Omega_{\bar{V}'}$, where $\bar{V} = \bar{V}(\mathfrak{S})$ and $\bar{V}' = \bar{V}(\mathfrak{S}')$. As above, we have $\Delta, \Delta' \in F_{2m}(\mathcal{X})$. By the definition of $(2m)$-local system, this implies that

$$(f_\Delta {f_{\Delta'}}^{-1})^{\Delta\cap\Delta'} = (h_{\Delta,\Delta'})^{\Delta\cap\Delta'}$$

for some $h_{\Delta,\Delta'} \in \mathrm{Aut}(\mathcal{X})$. It follows that $f_\Delta {f_{\Delta'}}^{-1} = f_{\Delta,\Delta'} h_{\Delta,\Delta'}$, where the isomorphism $f_{\Delta,\Delta'} := f_\Delta {f_{\Delta'}}^{-1} h_{\Delta,\Delta'}^{-1}$ belongs to K_V and is identical on $\Delta \cap \Delta'$. Applying the monomorphism μ from Lemma 17 to the last equality, we obtain

$$\mathfrak{m}(\mathfrak{S})\mathfrak{m}(\mathfrak{S}')^{-1} = \mu(f_{\Delta,\Delta'} h_{\Delta,\Delta'}) = \mu(f_{\Delta,\Delta'})\mu(h_{\Delta,\Delta'}). \tag{52}$$

By Lemma 8, the inner $\mathcal{A}^\star$-multiplier $\mathfrak{m}(\mathfrak{S}, \mathfrak{S}') := \mu(h_{\Delta,\Delta'})$ belongs to the group $\mathfrak{M} \leqslant \mathfrak{M}_{aut}(\mathcal{A}^\star)$. Moreover, the inner $\mathcal{A}^\star$-multiplier $\mu(f_{\Delta,\Delta'})$ is identical on $\mathfrak{S} \cap \mathfrak{S}'$. Thus, taking restriction of the equality (52) to $\mathfrak{S} \cap \mathfrak{S}'$, we get

$$\mathfrak{m}(\mathfrak{S})_{\mathfrak{S}\cap\mathfrak{S}'} = \mathfrak{m}(\mathfrak{S}')_{\mathfrak{S}\cap\mathfrak{S}'}(\mathfrak{m}(\mathfrak{S}, \mathfrak{S}'))_{\mathfrak{S}\cap\mathfrak{S}'},$$

as required.

10 Proof of Theorem 1 and Corollary 2

10.1 Reduction from S-rings to graphs

Let $\mathcal{G} \in \mathfrak{B}_a$ be an ε-expander for some real $\varepsilon > 0$. This means that for every vertex subset Δ containing at most half of the vertices of $\mathcal{G}$, we have $|\partial\Delta| \geqslant \varepsilon|\Delta|$, where $\partial\Delta$ is the set of all vertices outside Δ, each adjacent to at least one vertex of Δ. It is not hard to prove (see, e.g., [5, Lemma 4.2.7]) that each separator of the graph $\mathcal{G}$ has cardinality greater than $k = \lfloor c_\varepsilon \cdot 2a \rfloor + 1$, where $c_\varepsilon = \frac{\varepsilon}{4+\varepsilon}$.

Let $\mathcal{A}^\star$ be the totally normal S-ring over a cyclic group G of order n and $\varphi^\star = \varphi_{\mathfrak{c}}$ the algebraic isomorphism of $\mathcal{A}^\star$, that were defined in Theorem 18; in particular, $\mathcal{A}^\star$ admits a $\lfloor k/6 \rfloor$-local system of inner $\mathcal{A}^\star$-multipliers with respect to $\mathfrak{c}$ and $\mathrm{Iso}(\mathcal{A}^\star, \varphi^\star) = \varnothing$. Then

$$\mathrm{Iso}(\mathcal{X}^\star, \varphi^\star) = \varnothing, \tag{53}$$

where $\mathcal{X}^\star = \mathcal{X}(\mathcal{A}^\star)$ is the Cayley scheme associated with the S-ring $\mathcal{A}^\star$. Furthermore, from Theorem 9, it follows that the scheme $\mathcal{X}^\star$ is WL_m-equivalent to itself with respect to the algebraic isomorphism $\varphi^\star$, where $m = \lfloor \sqrt{\lfloor k/6 \rfloor - 1} \rfloor = c \cdot \sqrt{a}$ for a certain real constant $0 < c < 1$. This fact together with relation (53) shows that

$$\dim_{\mathrm{WL}}(\mathcal{X}^\star) \geqslant c \cdot \sqrt{a}, \tag{54}$$

see Section 4. In the rest of this section, we construct a circulant graph $\mathcal{G}^\star$ over the group G and verify that

$$\mathrm{WL}(\mathcal{G}^\star) = \mathcal{X}^\star. \tag{55}$$

This is enough to complete the proof. Indeed, in accordance with formulas (9) and (54), we then have $\dim_{\mathrm{WL}}(\mathcal{G}^\star) = \dim_{\mathrm{WL}}(\mathcal{X}^\star) \geqslant c \cdot \sqrt{a}$, as required.

10.2 The definition of the graph $\mathcal{G}^\star$

To construct the graph $\mathcal{G}^\star$, for any two indices $1 \leqslant i, j \leqslant b$, we choose an arbitrary basic set $X_{i,j} \in \mathcal{S}(\mathcal{A}^\star)$ contained in the difference $D_{i,j}$ defined by formula (45) and such that $\bar{X} = (X_{i,j})_{\mathfrak{s}_{i,j}}$ is a highest basic set of the S-ring $\mathcal{A}_{\mathfrak{s}_{i,j}}$, where the section $\mathfrak{s}_{i,j} := \mathfrak{s}_{u_i,w_j}$ is as in Lemma 15.

Recall that $|\bar{X}|$ is equal to $|K_{u_i}|$ if $j = 1$, and to $|K_{w_j}|$ if $i = 1$; in any of these cases $|\bar{X}| = 4$. Furthermore, by Lemma 19, $|\bar{X}| = |K_{u_i}| \cdot |K_{w_j}| / 2 = 8$ if $i, j > 1$ and $\{u_i, w_j\} \in E$, or $|\bar{X}| = |K_{u_i}| \cdot |K_{w_j}| = 16$ otherwise. It follows that

$$|X_{i,j}| = |\pi_{i,j}^{-1}(\bar{X})| = |G_{i-1,j-1}| \cdot \begin{cases} 4 & \text{if } i = 1 \text{ or } j = 1, \\ 8 & \text{if } i, j > 1 \text{ and } \{u_i, w_j\} \in E, \\ 16 & \text{otherwise,} \end{cases} \tag{56}$$

where $G_{i-1,j-1}$ and $\pi_{i,j}$ are as in formulas (45) and (46), respectively. Denote by $X^\star$ the union of all these basic sets $X_{i,j}$. Then the Cayley graph

$$\mathcal{G}^\star = \mathrm{Cay}(G, X^\star)$$

is circulant of order n.

10.3 Proof of equality (55)

The scheme $\mathrm{WL}(\mathcal{G}^\star)$ is a Cayley scheme over the group G. It is associated with the S-ring $\mathcal{A}' = \mathrm{WL}_G(\underline{X^\star})$. Since $X^\star$ is also an $\mathcal{A}^\star$-set, we have $\mathcal{A}^\star \geqslant \mathcal{A}'$. It remains to prove the reverse inclusion

$$\mathcal{A}^\star \leqslant \mathcal{A}', \tag{57}$$

i.e., that each basic set of $\mathcal{A}^\star$ is an $\mathcal{A}'$-set. To do this, we need several auxiliary statements.

Claim 22. *G_{u_b} and G_{w_b} are $\mathcal{A}'$-groups.*

Proof. We prove the statement for G_{u_b} only; the statement for G_{w_b} is proved similarly. Recall that the number n_1 is a product of two distinct primes, say p_1 and q_1. We apply Theorem 5(2) for $\mathcal{A} = \mathcal{A}'$ and $X = X^\star$. Note that if $x \in X^\star$ and H the subgroup defined before that theorem, then $xH \subseteq X^\star$ unless x belongs to the union of all $X_{i,j}$ with $i = 0, 1$. Therefore,

$$((X^\star)^{[p_1]})^{[q_1]} = \Big(\bigcup_{i,j=0}^{b} (X_{i,j})^{[p_1]}\Big)^{[q_1]} = \Big(\bigcup_{j=0}^{b} (X'_{0,j} \cup X'_{1,j})\Big)^{[q_1]} = \bigcup_{j=0}^{b} X''_{0,j},$$

where for all i, j, we set $X'_{i,j} = \sum_{x \in X_{i,j}} x^{p_1}$ and $X''_{i,j} = \sum_{x \in X'_{i,j}} x^{q_1}$. The right-hand side is contained in G_{u_b} and contains the set $X''_{0,b}$ generating G_{u_b}. Thus, G_{u_b} is an $\mathcal{A}'$-group. □

Claim 23. *G_{u_i} and G_{w_i} are $\mathcal{A}'$-groups, $i = 1, \ldots, b$.*

Proof. From Claim 22, it follows that $X := X^\star \cap G_{u_b}$ is an $\mathcal{A}'$-set. Note that $X = X_{0,0} \cup X_{1,0} \cup \ldots \cup X_{b,0}$ and $X_{i,0} \subseteq D_{i,0}$ for $i = 0, 1, \ldots, b$. Since each $X_{i,0}$ is a basic set of the S-ring $\mathcal{A}^\star$, we have

$$(\underline{X} \cdot \underline{X}) \circ \underline{X} = \sum_{i=0}^{b} a_i \underline{X_{i,0}} \tag{58}$$

for some nonnegative integers a_i, where $\circ$ denotes the componentwise product in $\mathbb{Z}G$. The integer a_i is equal to the number of pairs $(y, z) \in X \times X$ such that $yz = x$ for an arbitrary fixed $x \in X_{i,0}$.

Let $y \in D_{i',0}$, where $0 \leqslant i' \leqslant b$. Assume that $i' > i$. Then $y^{-1}x \in y^{-1}G_{i,0} \subseteq X$, and $x = yz$ with $z := y^{-1}x$. Similarly, if $i' < i$, then $x = yz$ for some $z \in X$. Now suppose that $i' = i$. In this case, if $i > 0$, then the set $(X_{\mathfrak{s}_{i,0}}) \cdot (X_{\mathfrak{s}_{i,0}})$ contains no element of $X_{\mathfrak{s}_{i,0}}$ (this follows from the assumption that $|\mathfrak{s}_{i,0}| \geqslant 5$). Thus,

$$a_i = |X| - |X_{i,0}|, \quad i = 1, \ldots b.$$

Besides, $a_0 = |X|$. Together with formula (56), this shows that the integers $a_0, a_1 \ldots, a_b$ are pairwise distinct. It easily follows that $X_{i,0}$ is an $\mathcal{A}'$-set for all i. Therefore, $G_{u_i} = \langle X_{i,0} \rangle$ is an $\mathcal{A}'$-group, $i = 1, \ldots, b$. In a similar way, one can prove that so is the group $G_{w_j} = \langle X_{0,j} \rangle$, $j = 1, \ldots, b$. □

Corollary 24. *Let $0 \leqslant i, j \leqslant b - 1$. Then $\mathfrak{s}_{i,j} \in \mathfrak{S}(\mathcal{A}')$ and $D_{i,j}, X_{i,j} \in \mathcal{S}(\mathcal{A}')^\cup$.*

Proof. By Claim 23, $G_{i,j} = G_{u_i} \times G_{w_j}$ is an $\mathcal{A}'$-group for all i, j. Then obviously $\mathfrak{s}_{i,j}$ is an $\mathcal{A}'$-section and $D_{i,j}$ is an $\mathcal{A}'$-set. Moreover, so is the subset $X_{i,j} = X^\star \cap D_{i,j}$. □

Let X be a nonidentity basic set of $\mathcal{A}^\star$. Then there are indices $0 \leqslant i, j \leqslant b - 1$ such that $X \subseteq D_{i,j}$. Put $\mathfrak{s} = \mathfrak{s}_{i,j}$. From Lemma 20, it follows that $(\mathcal{A}^\star)_\mathfrak{s}$ is a normal S-ring over $\mathfrak{s}$. By the choice of the basic set $X_{i,j}$, Lemma 6 implies that $(\mathcal{A}^\star)_\mathfrak{s}$ is the smallest S-ring over $\mathfrak{s}$ that contains $(X_{i,j})_\mathfrak{s}$. By Corollary 24, this implies that $(\mathcal{A}')_\mathfrak{s} \geqslant (\mathcal{A}^\star)_\mathfrak{s}$. Therefore,

$$X_\mathfrak{s} \in \mathcal{S}(\mathcal{A}^\star_\mathfrak{s})^\cup \subseteq \mathcal{S}(\mathcal{A}'_\mathfrak{s})^\cup.$$

By formula (46), this shows that $X = \pi_{i,j}^{-1}(X_\mathfrak{s})$ is an $\mathcal{A}'$-set, which proves inclusion (57).

10.4 Proof of Corollary 2

Recall (see, e.g., [21] and references therein) that a k-regular graph $\mathcal{G}$ is *Ramanujan* if all of its nontrivial eigenvalues lie between $-2\sqrt{k-1}$ and $2\sqrt{k-1}$. Any such graph is an ε-expander with $2\varepsilon = 1 - \lambda/k$, where λ is the second largest (in absolute value) eigenvalue of the adjacency matrix of $\mathcal{G}$. By Theorem 1, it suffices to find an infinite family of bipartite cubic 3-connected Ramanujan graphs.

Let $d \in \mathbb{N}$ be even. Denote by $\mathcal{G}$ a connected cubic Ramanujan graph on $2^{3d} - 2^d$ vertices, constructed in [23, Theorem 5.13]. Note that it is a Cayley graph of the group $\mathrm{PSL}(2, 2^d)$. Let $\mathcal{G}_d$ be the 2-cover of the graph $\mathcal{G}$, i.e., the vertex set of $\mathcal{G}_d$ is the disjoint union of the vertex sets of two copies of $\mathcal{G}$ and two vertices of $\mathcal{G}_d$ are adjacent if they

lie in different copies and the corresponding vertices of $\mathcal{G}$ are adjacent. Obviously, the graph $\mathcal{G}_d$ is cubic and bipartite. Moreover, it is a Ramanujan graph (see, e.g., a remark in [22, p. 311]).

It remains to verify that the graph $\mathcal{G}_d$ is 3-connected. From the fact that $\mathcal{G}$ is a Cayley graph, it easily follows that the graph $\mathcal{G}_d$ is vertex transitive. The connectivity of it can be equal neither 1 (because it contains at least one vertex which is not a cut point), nor 2 (because any vertex transitive graph of connectivity 2 is a polygon [30, Corollary 3A]). Thus the (cubic) graph $\mathcal{G}_d$ is 3-connected.

Acknowledgements

The authors would like to thank Professor Gang Chen for his helpful discussions and valuable suggestions. This work was partly supported by Hainan Province Natural Science Foundation of China (grant No. 120RC452) and National Science Foundation of China (grant No. 12371019).

References

[1] N. Alon, *Explicit expanders of every degree and size*, Combinatorica, **41** (2021), no. 4, 447–463.

[2] L. Babai, *Monte-Carlo algorithms in graph isomorphism testing*, Tech. Report Tech. Rep. 79–10, Université de Montréal, 1979, http://people.cs.uchicago.edu/~laci/lasvegas79.pdf.

[3] L. Babai, *Group, Graphs, Algorithms: the Graph Isomorphism Problem*, Proceedings of the International Congress of Mathematicians (ICM 2018), vol. 3, WORLD SCIENTIFIC, 2019, pp. 3319–3336; see also L. Babai, *Graph Isomorphism in Quasipolynomial Time* (2016), arXiv:1512.03547v2 [cs.DS]).

[4] J. Y. Cai, M. Fürer, and N. Immerman, *An optimal lower bound on the number of variables for graph identification*, Combinatorica, **12** (1992), 389–410.

[5] G. Chen and I. Ponomarenko, *Coherent configurations*, Central China Normal University Press, 2019, the updated version is available at http://www.pdmi.ras.ru/~inp/ccNOTES.pdf.

[6] G. Chen, Q. Ren, and I. Ponomarenko, *On the Weisfeiler algorithm of depth-1 stabilization*, Theoretical Computer Science, **1054** (2025), no. 3, 115460.

[7] G. Cherlin, *Sporadic homogeneous structures*, The Gelfand Mathematical Seminars, 1996–1999, Gelfand Math. Sem., Birkhäuser Boston, Boston, MA, 2000, pp. 15–48.

[8] C. J. Colbourn (ed.) and J. H. Dinitz (ed.), *The CRC handbook of combinatorial designs. 2nd ed.*, Boca Raton, FL: Chapman & Hall/CRC (2007).

[9] S. Evdokimov and I. Ponomarenko, *On highly closed cellular algebras and highly closed isomorphisms*, Electronic J. Combin., **6** (1999), #R18, 1–31.

[10] S. Evdokimov and I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, St. Petersburg Math. J. **14** (2003), no. 2, 189–221.

[11] S. Evdokimov and I. Ponomarenko, *Recognizing and isomorphism testing circulant graphs in polynomial time*, St. Petersburg Math. J. **15** (2004), no. 6, 813–835.

[12] S. Evdokimov and I. Ponomarenko, *A new look at the Burnside-Schur theorem*, Bull. London Math. Soc. **37** (2005), 535–546.

[13] S. Evdokimov and I. Ponomarenko, *Schur rings over a product of Galois rings*, Beitr. Algebra Geom. **55** (2014), no. 1, 105–138.

[14] S. Evdokimov and I. Ponomarenko, *Coset closure of a circulant S-ring and schurity problem*, J. Algebra Appl., **15** (2016), no. 4, 1650068, 49.

[15] S. Evdokimov and I. Ponomarenko, *On the separability problem for circulant S-rings*, St. Petersburg Math. J., **28** (2017), no. 1, 21–35.

[16] M. Grohe, *Descriptive complexity, canonisation, and definable graph structure theory*, Cambridge University Press, 2017.

[17] M. Grohe and D. Neuen, *Recent advances on the graph isomorphism problem*, Surveys in combinatorics 2021, London Math. Soc. Lecture Note Ser., vol. 470, Cambridge Univ. Press, Cambridge, 2021, pp. 187–234.

[18] H. Helfgott, J. Bajpai, and D. Dona, *Graph isomorphisms in quasi-polynomial time*, 2017, arXiv:1710.04574, pp. 1–67.

[19] S. Kiefer, *The Weisfeiler-Leman algorithm: an exploration of its power*, ACM SIGLOG News, **7** (2020), no. 3, 5–27.

[20] M. H. Klin and R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Colloq. Math. Soc. J.Bolyai, **25** (1978), 405–434.

[21] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica, **8** (1988), no. 3, 261–277.

[22] A. W. Marcus, D. A. Spielman, and N. Srivastava, *Interlacing families I: Bipartite Ramanujan graphs of all degrees*, Ann. of Math. (2), **182** (2015), no. 1, 307–325.

[23] M. Morgenstern, *Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q*, J. Combin. Theory Ser. B, **62** (1994), no. 1, 44–62.

[24] M. Muzychuk, *On the structure of basis sets of Schur rings over cyclic groups*, J. Algebra **169** (1994), 655–678.

[25] M. Muzychuk, *On Adam's conjecture for circulant graphs*, Discrete Math. **176** (1997), 285–298.

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

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

[28] M. Muzychuk and I. Ponomarenko, *Testing isomorphism of circulant objects in polynomial time*, J. Combin. Theory Ser. A **169** (2020), 105128, 10.

[29] I. Ponomarenko, *On the WL-dimension of circulant graphs of prime power order*, Algebraic Combinatorics **6** (2023), no. 6, 1469–1490.

[30] M. Watkins, *Connectivity of transitive graphs*, J. Combin. Theory **8** (1970), 23–29.

[31] B. Yu. Weisfeiler and A. A. Leman, *The reduction of a graph to canonical form and the algebra which appears therein*, NTI, Ser. 2 **9** (1968), 12–16. English translation is available at https://www.iti.zcu.cz/wl2018/pdf/wl_paper_translation.pdf.

[32] H. Wielandt, *Finite permutation groups*, Academic Press, New York and London, 1964.

[33] Yu. Wu and I. Ponomarenko, *On the Weisfeiler-Leman dimension of circulant graphs*, Algebra Analiz, **37**, no. 2, 1–27 (2025).

Corrigendum - Added October 9, 2026

Thanks to an anonymous volunteer who identified the following problems: the definition of $D_{i,j} = G_{i,j} \setminus G_{i-1,j-1}$ in formula (45) does not isolate the intended level pair (i, j). As a consequence, formula (46) is false. Also, the connection sets $X_{i,j}$ on page 33 are defined only for $1 \leqslant i, j \leqslant b$. Consequently, $X^\star \cap G_{u_b}$ and $X^\star \cap G_{w_b}$ are empty. These failures leave the reverse inclusion in (57), and hence equality (55), unproved. The observations above do not show that Theorem 1 or Corollary 2 is false; the purpose of this corrigendum is to provide corrected form for formula (46) and indicate the necessary changes in Subsection 10.2.

In what follows, we use the notation from the original paper. We also adopt the convention $G_{u_0} = G_{w_0} = \{1\}$, and for all $0 \leqslant i, j \leqslant b$, we set $G_{i,j} := G_{u_i} \times G_{w_i}$. We replace the definition of $D_{i,j}$ in formula (45) with the following:

$$D_{i,j} = (G_{u_i} \setminus G_{u_{i-1}}) \times (G_{w_j} \setminus G_{w_{j-1}}), \;\; 1 \leqslant i, j \leqslant b.$$

$$D_{i,0} = (G_{u_i} \setminus G_{u_{i-1}}) \times 1,\; D_{0,i} = 1 \times (G_{w_i} \setminus G_{w_{i-1}}),\; 1 \leqslant i \leqslant b.$$

With this corrected definition, for any nonidentity basic set $X \in \mathcal{S}(\mathcal{A})$, there exist i, j such that $X \subseteq D_{i,j}$ and also

$$X \subseteq D_{i,j} \quad \Leftrightarrow \quad X = \pi_{i,j}^{-1}(x) \text{ for some } 1 \neq x \in \mathrm{im}(\pi_{i,j}),$$

where $\pi_{i,j} : G_{i,j} \to G_{i,j}/G_{i-1,j-1}$ is the natural epimorphism. The formula (46) is now valid.

We redefine $X_{i,j}$ and $X^\star$ in Subsection 10.2 as follows: for each $1 \leqslant i, j \leqslant b$, choose a basic set $X_{i,j} \in \mathcal{S}(\mathcal{A}^\star)$ contained in $D_{i,j}$ such that the projection of $X_{i,j}$ to the section $\mathfrak{s}_{i,j} := \mathfrak{s}_{u_i,u_j}$ is a highest basic set of $\mathcal{A}_{s_{i,j}}$. Additionally, for each $1 \leqslant i \leqslant b$, choose a basic set $X_{i,0} \in \mathcal{S}(\mathcal{A}^\star)$ contained in $D_{i,0}$ such that its projection to $\mathfrak{s}_{u_i}$ is a highest basic set. Similarly, for each $1 \leqslant j \leqslant b$, choose a basic set $X_{0,j} \in \mathcal{S}(\mathcal{A}^\star)$ contained in $D_{0,j}$ such that its projection to $\mathfrak{s}_{w_j}$ is a highest basic set.

It is necessary to correct the indices at the paragraph preceding formula (56) as follows. Set $\bar{X} = (X_{i,j})_{\mathfrak{s}_{i,j}}$. Note that $|\bar{X}|$ is equal to $|K_{u_i}|$ if $j = 0$, and to $|K_{w_j}|$ if $i = 0$; in any of these cases $|\bar{X}| = 4$. Furthermore, let $i \geqslant 1$ and $j \geqslant 1$, by Lemma 19, $|\bar{X}| = |K_{u_i}| \cdot |K_{w_j}|/2 = 8$ if $\{u_i, w_j\} \in E$, or $|\bar{X}| = |K_{u_i}| \cdot |K_{w_j}| = 16$ otherwise. Define

$$X^\star = \bigcup_{\substack{0 \leqslant i,j \leqslant b \\ (i,j) \neq (0,0)}} X_{i,j}.$$

This corrected definition ensures that $X^\star \cap G_{u_b}$ and $X^\star \cap G_{w_b}$ are nonempty, as required for the proof of Claim 23 to be correct.