Stability of Cayley Graphs and Schur Rings

Ademir Hujdurović István Kovács

Submitted: Aug 23, 2024; Accepted: Jan 17, 2025; Published: Jun 20, 2025

Abstract

A graph Γ is said to be unstable if for the direct product $\Gamma \times K_2$, the group $\mathrm{Aut}(\Gamma \times K_2)$ is not isomorphic to $\mathrm{Aut}(\Gamma) \times \mathbb{Z}_2$. We show that a connected and non-bipartite Cayley graph $\mathrm{Cay}(H, S)$ is unstable if and only if the set $S \times \{1\}$ belongs to a Schur ring over the group $H \times \mathbb{Z}_2$ satisfying certain properties. The S-rings with these properties are characterized if H is a cyclic group of twice odd order. As an application, a necessary and sufficient condition is given for a connected and non-bipartite circulant graph of order $2p^e$ to be unstable, where p is an odd prime and $e \geqslant 1$.

Mathematics Subject Classifications: 05C25, 20B25

1 Introduction

All groups in this paper will be finite and all graphs will be finite, simple, and undirected. If Γ is a graph, then $\mathrm{V}(\Gamma)$, $\mathrm{E}(\Gamma)$ and $\mathrm{Aut}(\Gamma)$ denote its vertex set, edge set and automorphism group, respectively. The direct product $\Gamma \times K_2$ of a graph Γ and the complete graph K_2 on two vertices, also known as the *canonical double cover* of Γ, is defined to have vertex set $\mathrm{V}(\Gamma) \times \{0, 1\}$ and edges $\{(u, 0), (v, 1)\}$, where $\{u, v\} \in \mathrm{E}(\Gamma)$. The graph $\Gamma \times K_2$ admits natural automorphisms, namely the permutation

$$(v, i) \mapsto (v, 1 - i), \text{ where } v \in \mathrm{V}(\Gamma), \ i = 0, 1;$$

and for every $\alpha \in \mathrm{Aut}(\Gamma)$, the permutation

$$(v, i) \mapsto (v^{\alpha}, i), \text{ where } v \in \mathrm{V}(\Gamma), \ i = 0, 1.$$

These permutations can be easily seen to form a group, which is isomorphic to $\mathrm{Aut}(\Gamma) \times \mathbb{Z}_2$. Now, we say that Γ is *stable* if $\mathrm{Aut}(\Gamma \times K_2) \cong \mathrm{Aut}(\Gamma) \times \mathbb{Z}_2$, and *unstable* otherwise. This concept of stability was defined in [14]. Recently, several papers were devoted to the stability of graphs [1, 8, 19, 27], especially to circulant graphs [2, 5, 9, 10, 18, 25].

FAMNIT, University of Primorska, Muzejski trg 2, SI-6000 Koper, Slovenia
IAM, University of Primorska, Glagoljaška ulica 8, SI-6000 Koper, Slovenia
(ademir.hujdurovic@upr.si, istvan.kovacs@upr.si).

Let H be a group with identity element 1_H, and let $S \subseteq H$ be a subset such that $1_H \notin S$ and $x^{-1} \in S$ whenever $x \in S$. The *Cayley graph* $\mathrm{Cay}(H, S)$ is defined to have vertex set H and edges $\{x, sx\}$, where $x \in H$ and $s \in S$. In the case when H is a cyclic group, the term *circulant graph* is commonly used.

The goal of this paper is to propose an approach to the stability of Cayley graphs using Schur rings. A Schur ring (S-ring for short) over a group G is a subring of the integer group ring $\mathbb{Z}G$ satisfying certain conditions. S-rings were defined by Wielandt [24] and studied first by Schur [20] in his investigation of permutation groups. S-rings became an effective tool in algebraic combinatorics [16]. For the exact definition and all the S-ring theoretical concepts, which appear in our results below, we refer to Section 2.

In Section 3, by translating [5, Lemma 2.4] into the language of S-rings, we establish a necessary and sufficient condition for a connected and non-bipartite Cayley graph to be unstable in terms of S-rings. We remark that none of the latter constraints on the given Cayley graph is essential. It is easy to show that any disconnected graph as well as any bipartite graph with a non-trivial automorphism group is unstable (see, e.g., [25]).

Proposition 1. *Let $G = H \times \langle a \rangle$, where H is any finite group and $\langle a \rangle \cong \mathbb{Z}_2$. The following conditions are equivalent for every connected and non-bipartite graph* $\mathrm{Cay}(H, S)$.

(i) $\mathrm{Cay}(H, S)$ *is unstable.*

(ii) There exists a Schurian S-ring $\mathcal{A}$ over G such that $\underline{H}$, $\underline{Sa} \in \mathcal{A}$ and $\underline{\{a\}} \notin \mathcal{A}$.

Proposition 1 suggests the following recipe for finding all connected and non-bipartite unstable graphs $\mathrm{Cay}(H, S)$ on a given group H.

Step 1. Let $G = H \times \langle a \rangle$, where $\langle a \rangle \cong \mathbb{Z}_2$. Describe all S-rings $\mathcal{A}$ over G with $\underline{H} \in \mathcal{A}$ and $\underline{a} \notin \mathcal{A}$.

Step 2. Describe the connected and non-bipartite graphs $\mathrm{Cay}(H, S)$ using the fact that $\underline{Sa} \in \mathcal{A}$ for some S-ring $\mathcal{A}$ described in Step 1.

We explore this idea in the case when H is a cyclic group of order $2p^e$ for an odd prime p and $e \geqslant 1$. To the best of our knowledge, a characterization of the unstable circulant graphs of order n and valency k is known only in some special cases: n is odd [5, 18], $n = 2p$ for a prime p [9], or $k \leqslant 7$ [10]. Recently, the case where n is square-free was solved [2] using one of the results developed in this paper (Theorem 3). Regarding abelian groups of odd order, using elementary techniques, Witte Morris [26] obtained the following theorem (as a demonstration of our approach, we give an alternative proof in Remark 13).

Theorem 2 ([26])**.** *If H is an abelian group of odd order, then every unstable connected graph* $\mathrm{Cay}(H, S)$ *has two vertices with the same neighbours.*

In Section 4, we turn to the S-rings described in Step 1 in the case where H is a cyclic group of twice odd order. The main result of the section is the following theorem.

Theorem 3. *Let $G = H \times \langle a\rangle$, where $H \cong \mathbb{Z}_{2n}$, $n > 1$, n is odd, and $\langle a\rangle \cong \mathbb{Z}_2$. If $\mathcal{A}$ is an S-ring over G with $\underline{H} \in \mathcal{A}$ and $\underline{\{a\}} \notin \mathcal{A}$, then $\{a, ab\}$ is a basic set of $\mathcal{A}$, or*

$$\bigcap_{X\in\mathcal{S}(\mathcal{A}),\, X\cap H_0a\neq\emptyset} \mathrm{rad}(X \cap H_0a) \neq 1,$$

where b is the unique involution of H and H_0 is the subgroup of H of order n.

The above theorem shows that if Γ is a connected and non-bipartite Cayley graph of H (using the notation of Theorem 3), then either Γ is a known example of an unstable Cayley graph (because it is of Wilson type (C.1)), or Γ is stable modulo $\langle b\rangle$. The latter condition implies that every automorphism of $\Gamma \times K_2$ factors to a well-defined automorphism of $(\Gamma/\langle b\rangle) \times K_2$, hence it is contained in the group $\mathrm{Aut}(\Gamma/\langle b\rangle) \times \mathbb{Z}_2$. Based on Theorem 3, we derive the following characterization of unstable connected and non-bipartite circulant graphs of order $2p^e$ for an odd prime p.

Theorem 4. *Let $H \cong \mathbb{Z}_{2p^e}$, where p is an odd prime and $e \geqslant 1$. A connected and non-bipartite graph $\mathrm{Cay}(H, S)$ is unstable if and only if one of the following conditions holds.*

(i) $e > 1$ and $(S \cap H_0)h = S \cap H_0$, where H_0 is the unique subgroup of H of order p^e and $h \in H_0, h \neq 1_G$.

(ii) $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, Sb)$, where b is the unique involution of H.

Remark 5. In fact, the sufficiency part of the theorem follows from known constructions of unstable circulant graphs. The graphs satisfying the condition in case (i) are of Wilson type (C.1) (see [25]), and those satisfying the condition in case (ii) are unstable by [9, Proposition 3.7].

In deriving Theorem 4, besides S-rings, we shall also use generalized multipliers. A brief account on generalized multipliers can be found in Section 5, the proof of Theorem 4 will be presented in Section 6.

2 Schur rings

In this section, we review the necessary Schur ring theory in order to keep our paper self-contained. We begin by setting some notation.

For integers $m \leqslant n$, we use the symbol $[m, n]$ to denote the set $\{i \in \mathbb{Z} \mid m \leqslant i \leqslant n\}$.

For an integer $n > 1$ and a prime number p, n_p and $n_{p'}$ denote the *p-part* and the *p'-part* of n, respectively, i.e., n_p is the largest power of p that divides n, and $n_{p'} = n/n_p$.

For a group G, we denote by 1_G the identity element and by $G^{\#}$ the set of non-identity elements.

For $x \in G$, $o(x)$ denotes the order of x; and for a non-empty subset $X \subseteq G$, let $o(X) = |\langle X\rangle|$. The p-part of $o(x)$ and $o(X)$ are denoted by $o(x)_p$ and $o(X)_p$, respectively.

For an integer $m > 1$ such that m is not divisible by a prime p, we denote by $\sigma_{p^i}(m)$ the *order of* m *modulo* p^i, i.e., the smallest positive integer l satisfying $m^l \equiv 1 \pmod{p^i}$.

If G acts on a set X and $x \in X$, then G_x denotes the *stabiliser* of x in G, $\mathrm{Orb}_G(x)$ denotes the G-*orbit* containing x, and $\mathrm{Orb}(G, X)$ denotes the set of all G-orbits.

For $g \in G$, the *right multiplication* g_r is the permutation of G acting as $x \mapsto xg$ $(x \in G)$. We let

$$G_r = \{x_r \mid x \in G\} \text{ and } \mathrm{Sup}(G) = \{A \leqslant \mathrm{Sym}(G) \mid G_r \leqslant A\}.$$

For a non-empty subset $X \subseteq G$, the element $\sum_{x\in X} x$ in the group ring $\mathbb{Z}G$ is denoted by $\underline{X}$.

2.1 The definition and some properties

Definition 6. (Wielandt [24, Chapter IV]) A subring $\mathcal{A}$ of the group ring $\mathbb{Z}G$ is called a *Schur ring* (*S-ring* for short) if there exists a partition $\mathcal{S}(\mathcal{A})$ of G such that

(i) $\{1_G\} \in \mathcal{S}(\mathcal{A})$.

(ii) If $X \in \mathcal{S}(\mathcal{A})$ then $X^{-1} \in \mathcal{S}(\mathcal{A})$.

(iii) $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} \mid X \in \mathcal{S}(\mathcal{A})\}$.

The subsets in $\mathcal{S}(\mathcal{A})$ are called the *basic sets* of $\mathcal{A}$ and the number $\mathrm{rank}(\mathcal{A}) := |\mathcal{S}(\mathcal{A})|$ is called the *rank* of $\mathcal{A}$. The motivation of the above definition can be explained by the result of Schur [20] stating that for any group $A \in \mathrm{Sup}(G)$, the free $\mathbb{Z}$-module

$$\mathrm{Span}_{\mathbb{Z}}\{\underline{X} \mid X \in \mathrm{Orb}(A_{1_G}, G)\}$$

is a subring of $\mathbb{Z}G$. This ring is an example of an S-ring, which is also called the *transitivity module* over G induced by A and denoted by $V(G, A_{1_G})$. An S-ring $\mathcal{A}$ is called *Schurian* if $\mathcal{A} = V(G, B_{1_G})$ for some permutation group $B \in \mathrm{Sup}(G)$. We remark that not all S-rings are Schurian (see [24]).

If $\mathcal{A}$ and $\mathcal{B}$ are two S-rings over G, then their usual intersection $\mathcal{A} \cap \mathcal{B}$ is also an S-ring over G (see, e.g., [15, the paragraph following Theorem 4.2]). Moreover, if both $\mathcal{A}$ are $\mathcal{B}$ are Schurian, then $\mathcal{A} \cap \mathcal{B}$ is also Schurian.

Let $\mathcal{A}$ be an S-ring over a group G. A subset $X \subseteq G$ is called an $\mathcal{A}$-*set* if $\underline{X} \in \mathcal{A}$, and a subgroup $H \leqslant G$ is called an $\mathcal{A}$-*subgroup* if $\underline{H} \in \mathcal{A}$. We say that $\mathcal{A}$ is *primitive* if 1 and G are the only $\mathcal{A}$-subgroups of G.

There are two natural $\mathcal{A}$-subgroups associated with an $\mathcal{A}$-set X, namely, $\langle X \rangle$ and the *radical* of X defined as

$$\mathrm{rad}(X) = \{g \in G \mid Xg = X \text{ and } gX = X\}$$

(see [24, Propositions 23.5 and 23.6]). If H and K are two $\mathcal{A}$-subgroups, then it can be easily checked that so are $H \cap K$ and $\langle H \cup K \rangle$.

Let $H \leqslant G$ be an $\mathcal{A}$-subgroup. Then the free $\mathbb{Z}$-module

$$\mathcal{A}_H := \mathrm{Span}_{\mathbb{Z}}\{\underline{X} \mid X \in \mathcal{S}(\mathcal{A}), X \subseteq H\}$$

is an S-ring over H, which is called an *induced S-subring* of $\mathcal{A}$. Furthermore, if $X \in \mathcal{S}(\mathcal{A})$, then there is a positive constant ℓ such that

$$\forall x \in G,\ |Hx \cap X| = 0 \text{ or } \ell. \tag{1}$$

Assume, in addition, that $H \trianglelefteq G$. For an arbitrary non-empty subset $X \subseteq G$, we let X/H denote the subset of the quotient group G/H defined by

$$X/H = \{Hx \mid x \in X\}.$$

It follows that the sets X/H form the basic sets of an S-ring over G/H while X runs over $\mathcal{S}(\mathcal{A})$ (see [23]). The latter S-ring is called *a quotient S-ring* and denoted by $\mathcal{A}_{G/H}$. In what follows, if K, L are two $\mathcal{A}$-subgroups such that $L \trianglelefteq K$, then the more simple notation $\mathcal{A}_{K/L}$ will be used instead of $(\mathcal{A}_K)_{K/L}$. Note that, if $\mathcal{A}$ is Schurian, then so is $\mathcal{A}_{K/L}$.

2.2 Products of S-rings

Definition 7 ([7])**.** Let $\mathcal{A}$ be an S-ring over a group G and $V, W \leqslant G$ be two $\mathcal{A}$-subgroups. The S-ring $\mathcal{A}$ is the *star product* of $\mathcal{A}_V$ with $\mathcal{A}_W$, written as $\mathcal{A} = \mathcal{A}_V \star \mathcal{A}_W$, if the following conditions hold.

(i) $V \cap W \trianglelefteq W$.

(ii) For every $X \in \mathcal{S}(\mathcal{A})$, if $X \subseteq (W \setminus V)$, then X is a union of some $(V \cap W)$-cosets.

(iii) For every $X \in \mathcal{S}(\mathcal{A})$, if $X \subseteq (G \setminus (V \cup W))$, then there exist basic sets $Y, Z \in \mathcal{S}(\mathcal{A})$ such that $Y \subseteq V$, $Z \subseteq W$ and $X = YZ$.

The star product is *non-trivial* if $1 < V < G$. In the special case when $V \cap W = 1$ it is also called the *tensor product* and written as $\mathcal{A}_V \otimes \mathcal{A}_W$.

If $\mathcal{A}$ and $\mathcal{B}$ are two S-rings over G such that $\mathcal{A} \subseteq \mathcal{B}$, then $\mathcal{A}$ is also called an *S-subring* of $\mathcal{B}$. In this case every basic set of $\mathcal{A}$ can be written as a union of basic sets of $\mathcal{B}$.

Definition 8 ([3, 12])**.** Let $\mathcal{A}$ be an S-ring over a group G and let L, U be $\mathcal{A}$-subgroups of G such that $L \leqslant U$. The S-ring $\mathcal{A}$ is the *U/L-wreath product* (also called the *generalised wreath product* of $\mathcal{A}_U$ with $\mathcal{A}_{G/L}$) if the following conditions hold.

(i) $L \trianglelefteq G$.

(ii) For every $X \in \mathcal{S}(\mathcal{A})$, if $X \subseteq G \setminus U$, then X is a union of some L-cosets.

The U/L-wreath product is *non-trivial* if $L \neq 1$ and $U \neq G$. The following simple relation with the star product will be used later, hence we record it here.

Lemma 9. *Let $\mathcal{A}$ be an S-ring over a group G such that $\mathcal{A} = \mathcal{A}_V \star \mathcal{A}_W$ and $V \cap W \trianglelefteq G$. Then $\mathcal{A}$ is the $V/(V \cap W)$-wreath product.*

Proof. Let $X \in \mathcal{S}(\mathcal{A})$ be an arbitrary basic set outside V. We have to show that $V \cap W \leqslant \mathrm{rad}(X)$. This follows from Definition 7(ii) if $X \subseteq W$. Let X be outside W. By Definition 7(iii), there exist basic sets $Y, Z \in \mathcal{S}(\mathcal{A})$ such that $Y \subseteq V$, $Z \subseteq W$ and $X = YZ$. Then $V \cap W \leqslant \mathrm{rad}(Z)$, implying that $V \cap W \leqslant \mathrm{rad}(YZ) = \mathrm{rad}(X)$. □

2.3 S-rings over abelian groups

Let G be a group. For a subset $X \subseteq G$ and integer m, define $X^{(m)} = \{x^m \mid x \in X\}$, and for a group ring element $\eta = \sum_{x \in G} c_x x$, define $\eta^{(m)} = \sum_{x \in G} c_x x^m$. If G is also abelian and d is a divisor of $|G|$, let

$$G[d] = \{x \in G \mid x^d = 1_G\};$$

furthermore, for a prime divisor p of $|G|$, define the subset $X^{[p]} \subseteq G$ as

$$X^{[p]} = \{x^p \mid x \in X \text{ and } |X \cap xG[p]| \not\equiv 0 \pmod{p}\}.$$

Note that $X^{[p]}$ is possibly the empty set.

The next properties are also referred to as Schur's first and second theorem on multipliers, respectively (see [16]).

Theorem 10. *Let $\mathcal{A}$ be an S-ring over an abelian group G.*

(i) ([16, Theorem 3.1]) *If m is an integer coprime to $|G|$ and $\eta \in \mathcal{A}$, then $\eta^{(m)} \in \mathcal{A}$. In particular, $X^{(m)} \in \mathcal{S}(\mathcal{A})$ whenever $X \in \mathcal{S}(\mathcal{A})$.*

(ii) ([16, Theorem 3.3]) *If p is a prime divisor of $|G|$ and X is an $\mathcal{A}$-set, then $X^{[p]}$ is an $\mathcal{A}$-set.*

In the following proposition we consider S-rings over abelian groups having a Sylow q-subgroup of order q. In the case where $q > 2$ and $\mathrm{rank}(\mathcal{A}) > 2$, the statement was derived by Somlai and Muzychuk, see [21, Proposition 3.1].

Proposition 11. *Let $H = P \times Q$, where P is an abelian group of order n and $Q \cong \mathbb{Z}_q$ for a prime q such that $q \nmid n$. Let $\mathcal{A}$ be an S-ring over H and T be a basic set of $\mathcal{A}$ with the property that $T^{(m)} = T$ whenever $q \nmid m$ and $m \equiv 1 \pmod{n}$.[1] Let P_1 be the maximal $\mathcal{A}$-subgroup contained in P and Q_1 be the minimal $\mathcal{A}$-subgroup containing Q. Then*

$$T = S_1 \cup S_{-1} Q^{\#} \cup S_0 Q,$$

where S_1, S_{-1} and S_0 are pairwise disjoint subsets of P, and S_1 and S_{-1} are $\mathcal{A}$-subsets. In addition, the sets S_1, S_{-1} and S_0 satisfy the following conditions.

[1] Subsets with this property are called M_q-invariant in [21].

(i) If $S_1 \neq \emptyset$, then $S_{-1} = S_0 = \emptyset$ and $T \subseteq P_1$.

(ii) If $S_1 = \emptyset$ and $S_{-1} \neq \emptyset$, then $T = S_{-1}(Q_1 \setminus P_1)$.

(iii) If $S_1 = S_{-1} = \emptyset$, then $Q_1 T = T$.

Proof. If $\mathrm{rank}(\mathcal{A}) = 2$, then $T = \{1_H\}$ or $H^{\#}$. If $T = \{1_H\}$, then case (i) holds; and if $T = H^{\#}$, then case (ii) holds with $S_{-1} = \{1_H\}$, $P_1 = 1$, and $Q_1 = H$. For the rest of the proof we assume that $\mathrm{rank}(\mathcal{A}) > 2$.

If $q > 2$, then the statement is true by [21, Proposition 3.1], and therefore, we are left with the case where $q = 2$. In this case it follows immediately that T can be written in the form $T = S_1 \cup S_{-1}Q^{\#} \cup S_0 Q$, where S_1, S_{-1} and S_0 are pairwise disjoint subsets of P. We compute that $T^{[2]} = S_1^{(2)} \cup S_{-1}^{(2)}$.

Suppose that $S_1 \cup S_{-1} \neq \emptyset$. We show that one of cases (i) and (ii) in the proposition holds, and that both sets S_1 and S_{-1} are $\mathcal{A}$-subsets. By the Chinese remainder theorem, there exists an odd integer k satisfying $2k \equiv 1 \pmod{n}$ (note that n is odd as $q \nmid n$). Then,

$$(T^{[2]})^{(k)} = \big(S_1^{(2)} \cup S_{-1}^{(2)}\big)^{(k)} = S_1 \cup S_{-1}.$$

Applying Theorem 10(i)-(ii) to T yields that $S_1 \cup S_{-1}$ is an $\mathcal{A}$-subset. The group $\langle S_1 \cup S_{-1}\rangle$ is an $\mathcal{A}$-subgroup contained in P. It follows that $S_1 \cup S_{-1} \subseteq P_1$. If $S_1 \neq \emptyset$, then the basic set T intersects P_1 non-trivially, implying that $T \subseteq P_1$, since P_1 is an $\mathcal{A}$-subgroup. We conclude that case (i) holds and S_1 is an $\mathcal{A}$-subset.

Let $S_1 = \emptyset$. Then $S_{-1} \cup T$ is an $\mathcal{A}$-subset, for which $Q \leqslant \mathrm{rad}(S_{-1} \cup T)$. Since $\mathrm{rad}(S_{-1} \cup T)$ is an $\mathcal{A}$-subgroup, it follows that $Q_1 \leqslant \mathrm{rad}(S_{-1} \cup T)$, or equivalently, $(S_{-1} \cup T)Q_1 = S_{-1} \cup T$. It follows from this that $S_{-1}Q_1 \subseteq S_{-1} \cup T$, and hence

$$S_{-1}(Q_1 \setminus P_1) \subseteq S_{-1} \cup T. \tag{2}$$

Now, if $S_{-1}(Q_1 \setminus P_1) \cap S_{-1} \neq \emptyset$, then there exist $s, s' \in S_{-1}$ and $t \in Q_1 \setminus P_1$ such that $st = s'$. But $S_{-1} \subseteq P_1$, implying that $t \in P_1$ as well, a contradiction. Thus $S_{-1}(Q_1 \setminus P_1) \cap S_{-1} = \emptyset$, and we retrieve from (2) that $S_{-1}(Q_1 \setminus P_1) \subseteq T$. On the other hand, as both S_{-1} and $Q_1 \setminus P_1$ are $\mathcal{A}$-subsets, so is $S_{-1}(Q_1 \setminus P_1)$. Since basic sets are minimal $\mathcal{A}$-subsets, it follows that $S_{-1}(Q_1 \setminus P_1) = T$, i.e., case (ii) holds.

Finally, suppose that $S_1 = S_{-1} = \emptyset$. In this case $Q \leqslant \mathrm{rad}(T)$, implying that $Q_1 \leqslant \mathrm{rad}(T)$. Equivalently, $Q_1 T = T$, i.e., case (iii) holds. □

The theorem below was derived by Somlai and Muzychuk [21] for $q > 2$ (part (i) is Corollary 3.2, and parts (ii)–(iv) are Propositions 3.3, 3.4, and 3.5, respectively). The proof relies on Proposition 11 and can be extended to cover also the case where $q = 2$ by copying the arguments in [21]. Therefore, we omit the proof.

Theorem 12. *With the notation given in Proposition 11, let* $\mathrm{rank}(\mathcal{A}) > 2$, $H_1 = P_1 Q_1$, *and* $\mathcal{A}_1 = \mathcal{A}_{H_1}$. *The following statements hold.*

(i) $\mathcal{A}$ is a H_1/Q_1-wreath product.

(ii) P_1 *is an* $\mathcal{A}_1$*-maximal subgroup.*

(iii) *If* $|H_1/P_1| \neq q$*, then* $(\mathcal{A}_1)_{H_1/P_1}$ *has rank* 2 *and* $\mathcal{A}_1 = (\mathcal{A}_1)_{P_1} \star (\mathcal{A}_1)_{Q_1}$*.*

(iv) *If* $|H_1/P_1| = q$ *and* $(\mathcal{A}_1)_{H_1/P_1} = \mathbb{Z}(H_1/P_1)$*, then* $\mathcal{A}_1 = (\mathcal{A}_1)_{P_1} \star (\mathcal{A}_1)_{Q_1}$*.*

Remark 13. One can combine Theorem 12 and Proposition 1 to derive Theorem 2.

Indeed, suppose that H is an abelian group of odd order and $\mathrm{Cay}(H, S)$ is a connected and unstable graph. By Proposition 1, there is a Schurian S-ring $\mathcal{A}$ over $H \times \langle a \rangle$, $\langle a \rangle \cong \mathbb{Z}_2$ such that $\underline{H}, \underline{Sa} \in \mathcal{A}$ and $\underline{\{a\}} \notin \mathcal{A}$. Let us apply Theorem 12 to $\mathcal{A}$ (we let $q = 2$). Recall that P_1 is the maximal $\mathcal{A}$-subgroup of odd order, Q_1 the minimal $\mathcal{A}$-subgroup of even order, $H_1 = P_1 Q_1$, and $\mathcal{A}_1 = \mathcal{A}_{H_1}$. It follows that $P_1 = H$ and $Q_1 > \langle a \rangle$. In particular, $L := P_1 \cap Q_1 \neq 1$. Clearly, $H_1 = P_1 Q_1 = G$, hence $\mathcal{A} = \mathcal{A}_1$ and by Theorem 12(iii)-(iv),

$$\mathcal{A} = \mathcal{A}_{P_1} \star \mathcal{A}_{Q_1}.$$

By Lemma 9, $\mathcal{A}$ is the P_1/L-wreath product. Since Sa is a union of some basic sets of $\mathcal{A}$, all of which are outside P_1, it follows that $L \leqslant \mathrm{rad}(Sa)$. Consequently, as vertices of $\mathrm{Cay}(H, S)$, any two $x, y \in L$ have the same neighbours.

In the remaining part of this subsection we prove two lemmas on S-rings.

Lemma 14. *With the notation given in Proposition 11, let* $q = 2$ *and let* $L = P_1 \cap Q_1$*. Then* $Q_1 \setminus L$ *is a basic set. Furthermore,* $\mathcal{A}$ *is the* P_1/L*-wreath product.*

Proof. Let a be the unique involution of H and T be the basic set of $\mathcal{A}$ containing a. We show now that $T = Q_1 \setminus L$. Clearly, $\underline{L} \in \mathcal{A}$. Consider the S-ring $\mathcal{A}_{Q_1/L}$. We claim that it is primitive. If not, then there was an $\mathcal{A}$-subgroup N such that $L < N < Q_1$. Since $N < Q_1$, N cannot contain a by the minimality of Q_1. Thus $N \leqslant P_1$, so $N \leqslant P_1 \cap Q_1 = L$, contradicting the assumption that $N > L$.

Wielandt showed that every primitive S-ring over an abelian group of composite order with a cyclic Sylow subgroup has rank 2 (see the proof of [24, Theorem 25.4]). Thus $\mathrm{rank}(\mathcal{A}_{Q_1/L}) = 2$, and combining this with (1) yields the existence of a positive number ℓ such that

$$|Lx \cap T| = \ell \text{ for every } x \in Q_1 \setminus L.$$

On the other hand, $\mathcal{A}_{P_1 Q_1} = \mathcal{A}_{P_1} \star \mathcal{A}_{Q_1}$ by Theorem 12(iii)-(iv). This shows that $La \subseteq T$, so $\ell = |L|$, i.e., $T = Q_1 \setminus L$.

Let $X \in \mathcal{S}(\mathcal{A})$ be an arbitrary basic set outside P_1. We have to show that $L \leqslant \mathrm{rad}(X)$. If $X \nsubseteq P_1 Q_1$, then $P_1 Q_1 \neq H$, and $\mathcal{A}$ is a non-trivial $P_1 Q_1/Q_1$-wreath product due to Theorem 12(i), in particular, $L \leqslant Q_1 \leqslant \mathrm{rad}(X)$. If $X \subseteq P_1 Q_1$, then $L \leqslant \mathrm{rad}(X)$ follows from Lemma 9 and Theorem 12(iii)-(iv). □

Lemma 15. *Let* $H = E \times F$ *be an abelian group such that* $E = \langle u, v \rangle \cong \mathbb{Z}_2^2$ *and* $|F|$ *is odd. Suppose that* $\mathcal{A}$ *is a Schurian S-ring over* H *such that* $\underline{F}, \underline{\langle F, v \rangle} \in \mathcal{A}$ *and* $\underline{\{u, uv\}} \in \mathcal{S}(\mathcal{A})$*. Let* $X \in \mathcal{S}(\mathcal{A})$*,* $X \nsubseteq \langle F, v \rangle$*. Then*

$$|X \cap Fu| = |X \cap Fuv|.$$

Furthermore, both sets $X \cap Fu$ and $X \cap Fuv$ are basic sets of a Schurian S-ring $\mathcal{B}$ over H, for which $\mathcal{A} \subset \mathcal{B}$.

Proof. As $\mathcal{A}$ is Schurian, $\mathcal{A} = V(H, A_{1_H})$ for a group $A \in \mathrm{Sup}(H)$. Let K be the kernel of the action of A on the set $[H : F]$ consisting of the F-cosets in H, and let $B = K\langle u_r, v_r\rangle$. Clearly, $B \in \mathrm{Sup}(H)$. Let $\mathcal{B} = V(H, B_{1_H})$.

Since $B < A$, it follows that $\mathcal{B} \supset \mathcal{A}$. The sets $\{u, uv\}/F$ and X/F are basic sets of the S-ring $\mathcal{A}_{H/F}$ whose intersection is non-empty. Thus, they are equal, implying that there are elements $x_1 \in X \cap Fu$ and $x_2 \in X \cap Fuv$.

Let X_i be the basic set of $\mathcal{B}$ containing x_i for $i = 1, 2$. Clearly, X_1 and X_2 are contained in X and belong to different F-cosets. Observe that $A_{1_H} \cap A_{x_1} \leqslant K$. It follows from this that $A_{1_H} \cap A_{x_1} = B_{1_H} \cap B_{x_1}$. Also, $|B| = |K||E| = |A|/2$, and therefore, $|B_{1_H}| = |A_{1_H}|/2$. These together with the orbit-stabilizer lemma yield

$$|X_1| = \frac{|B_{1_H}|}{|B_{1_H} \cap B_{x_1}|} = \frac{|A_{1_H}|}{2|A_{1_H} \cap A_{x_1}|} = |X|/2.$$

The same argument shows that $|X_2| = |X|/2$, and so $|X_1| = |X_2|$ and $X_1 = X \cap Fu$ and $X_2 = X \cap Fuv$. □

2.4 S-rings over cyclic p-groups

The basic sets of S-rings over a cyclic group are described in [15, Theorem 5.9]. In the case where the order of the cyclic group is a p-power for a prime $p > 2$, the description was obtained earlier by Pöschel [17], and in the case where the order is a 2-power, it was derived in [6, 11].

For our purposes, we need to consider the special case where the order of the cyclic group is a power of an odd prime. In order to invoke this description, we need one more concept. Given an S-ring $\mathcal{A}$ over a group H, a basic set $X \in \mathcal{S}(\mathcal{A})$ is called *cyclotomic* if it is a K-orbit for some subgroup $K \leqslant \mathrm{Aut}(H)$.

Proposition 16 ([17, Lemma 4.8])**.** *Let $\mathcal{A}$ be an S-ring over a cyclic p-group H for an odd prime p. For every basic set $X \in \mathcal{S}(\mathcal{A})$, one of the following holds.*

(i) X is cyclotomic.

(ii) $|H| > p$ and $X = F \setminus E$, where $1 \leqslant E < F \leqslant H$ and $|F| > p|E|$.

A constructive characterization of S-rings over a cyclic group was given by Leung and Man [12, 13], which was later refined in [4]. Again, we are content with considering only p-groups, where p is an odd prime.

Proposition 17 (cf. [16, Theorem 4.10])**.** *Let $\mathcal{A}$ be an S-ring over a cyclic p-group H for an odd prime p. Suppose that there is a basic set $X \in \mathcal{S}(\mathcal{A})$ such that $\langle X\rangle = H$ and* $\mathrm{rad}(X) = 1$. *Then $X = H^{\#}$, or $\mathcal{A} = V(H, K)$, where $K \leqslant \mathrm{Aut}(H)$ and $p \nmid |K|$.*

3 Proof of Proposition 1

We keep the notation set in Proposition 1, i.e., $G = H \times \langle a \rangle$, where H is any group and $\langle a \rangle \cong \mathbb{Z}_2$, furthermore, $\mathrm{Cay}(H, S)$ is a connected and non-bipartite graph.

It can be easily seen that $\mathrm{Cay}(H, S) \times K_2 \cong \mathrm{Cay}(G, Sa)$. Moreover, $\mathrm{Cay}(H, S)$ is stable if and only if

$$\mathrm{Aut}(\mathrm{Cay}(G, Sa)) = \mathrm{Aut}(\mathrm{Cay}(H, S)) \times \langle a_r \rangle, \tag{3}$$

where by the latter group we mean the direct product of two permutation groups acting on $G = H \times \langle a \rangle$. We let $A = \mathrm{Aut}(\mathrm{Cay}(G, Sa))$ and write 1 for 1_G. The following claim is a direct consequence of [5, Lemma 3.3]. As the proof is short, we include it here.

Claim. $\mathrm{Cay}(H, S)$ *is stable if and only if* $a_r\alpha = \alpha a_r$ *for every* $\alpha \in A_1$.

Proof of the claim. The implication "$\Rightarrow$" is clear by (3).

For the implication "$\Leftarrow$", assume that $a_r\alpha = \alpha a_r$ for every $\alpha \in A_1$, where A_1 is the stabilizer of 1 in A. The graph $\mathrm{Cay}(G, Sa)$ is bipartite with colour classes H and Ha. Since $\mathrm{Cay}(H, S)$ is connected and non-bipartite, it follows that $\mathrm{Cay}(G, Sa)$ is also connected. Therefore, the partition of G into H and Ha is A-invariant. Let $\alpha \in A_1$. Then $H^\alpha = H$. Let β be the permutation of H induced by α. Then for every $x \in H$, $(xa)^\alpha = x^{a_r\alpha} = x^{\alpha a_r} = x^\beta a$. This means that $\alpha \in \mathrm{Sym}(H) \times \langle a_r \rangle$. We show now that $\beta \in \mathrm{Aut}(\mathrm{Cay}(H, S))$.

Pick an arbitrary edge $\{x, sx\}$ of $\mathrm{Cay}(H, S)$. Then $\{x, sax\} \in \mathrm{E}(\mathrm{Cay}(G, Sa))$, and since $\alpha \in A_1$, it follows that

$$(sax)^\alpha = s'ax^\alpha \text{ for some } s' \in S.$$

On the other hand, $(sax)^\alpha = (sx)^\beta a$ and $s'ax^\alpha = s'x^\beta a$. We obtain that β maps the edge $\{x, sx\}$ to the edge $\{x^\beta, s'x^\beta\}$, so $\beta \in \mathrm{Aut}(\mathrm{Cay}(H, S))$. We showed that $A_1 \leqslant \mathrm{Aut}(\mathrm{Cay}(H, S)) \times \langle a_r \rangle$. Using this, together with the fact that $A = A_1G_r$ and (3), we deduce that $\mathrm{Cay}(H, S)$ is stable. □

Assume first that $\mathrm{Cay}(H, S)$ is unstable. It is sufficient to show that the S-ring $\mathcal{A} = V(G, A_{1_G})$ satisfies all the conditions in Proposition 1(ii). i.e.,

$$\underline{H},\ \underline{Sa} \in \mathcal{A} \text{ and } \underline{\{a\}} \notin \mathcal{A}. \tag{4}$$

It is clear that $\underline{Sa} \in \mathcal{A}$. It has been shown above that H and Ha form an A-invariant partition. This implies that $\underline{H} \in \mathcal{A}$. Finally, due to the claim, $a_r\alpha \neq \alpha a_r$ for some $\alpha \in A_1$. Thus $(ga)^\alpha \neq g^\alpha a$ for some $g \in G$. Using that $a \in Z(G)$, this can be rewritten as $(ag)^\alpha (g^\alpha)^{-1} \neq a$. Letting $a' = (ag)^\alpha (g^\alpha)^{-1}$ and $\alpha' = g_r\alpha \cdot ((g^\alpha)^{-1})_r$, we find that $1^{\alpha'} = 1$ and $a^{\alpha'} = a' \neq a$, showing that $\underline{\{a\}} \notin \mathcal{A}$.

Now assume that there is a Schurian S-ring $\mathcal{A}$ over G satisfying all conditions in (4). Then $\mathcal{A} = V(G, B_{1_G})$ for some permutation group $B \in \mathrm{Sup}(G)$. Observe that, as

$\underline{Sa} \in \mathcal{A}$, $B \leqslant A$. Assume to the contrary that $\mathrm{Cay}(H,S)$ is stable. Then $\alpha a_r = a_r\alpha$ for every $\alpha \in A_1$ due to the claim above, hence

$$\mathrm{Orb}_{B_1}(a) = \left\{\, 1^{a_r x} \mid x \in B_1 \,\right\} = \left\{\, 1^{x a_r} \mid x \in B_1 \,\right\} = \{a\}.$$

This, however, contradicts the condition that $\underline{\{a\}} \notin \mathcal{A}$. The proof of Proposition 1 is completed.

4 Proof of Theorem 3

For this section we set the following assumptions.

Hypothesis 18. *H is an abelian group of twice odd order with a unique involution b and $H_0 < H$ is the unique subgroup of H of order $|H|/2$ and $|H| > 2$. Furthermore,*

$\mathcal{A}$ is an S-ring over $G = H \times \langle a\rangle$, where $\langle a\rangle \cong \mathbb{Z}_2$ such that $\underline{H} \in \mathcal{A}$.

T is the basic set of $\mathcal{A}$ containing a.

K is the largest $\mathcal{A}$-subgroup of odd order.

The proof of Theorem 3 will be given in the end of the section following four preparatory lemmas.

The following simple fact will be used a couple of times hence we record it here. If $A, B \leqslant G$ are any subgroups and $S \subseteq G$ is any non-empty subset, then

$$AB/B \leqslant \mathrm{rad}(S/B) \implies A \leqslant \mathrm{rad}(SB). \tag{5}$$

Lemma 19. *Assuming Hypothesis 18, suppose that $\underline{Kab} \in \mathcal{A}$ and $La \subseteq T$ for some $\mathcal{A}$-subgroup L, $L \leqslant H_0$. Then*

$$L \leqslant \bigcap_{X \in \mathcal{S}(\mathcal{A}),\, X \not\subseteq H \cup Kab} \mathrm{rad}(X).$$

Proof. Fix a basic set $X \in \mathcal{S}$ such that $X \not\subseteq H \cup Kab$. We show now that $L \leqslant \mathrm{rad}(X)$. As $\underline{L} \in \mathcal{A}$, there is a positive number ℓ such that $|X \cap Lx| = 0$ or ℓ for every $x \in G$, see (1). As $X \not\subseteq H$, X can be expressed as

$$X = X_1 a \cup X_2 ab \cup X_3 a \cup X_3 ab,$$

where X_1, X_2 and X_3 are pairwise disjoint subsets of H_0.

Assume first that $X_1 \cup X_2 = \emptyset$. Then $b \in \mathrm{rad}(X)$, hence $Q \leqslant \mathrm{rad}(X)$, where Q is the least $\mathcal{A}$-subgroup containing b. Let us consider the S-ring $\mathcal{A}_{G/Q}$. Then G/Q has twice odd order and T/Q is a basic set of $\mathcal{A}_{G/Q}$ containing the unique involution of G/Q. It follows from Lemma 14 that

$$T/Q = \langle T\rangle Q/Q \setminus H/Q \text{ and } \langle T\rangle Q/Q \cap H/Q \leqslant \mathrm{rad}(X/Q).$$

The group $\langle T\rangle Q/Q \cap H/Q = (\langle T\rangle \cap HQ)Q/Q$. Using (5), we obtain $\langle T\rangle \cap HQ \leqslant \mathrm{rad}(XQ) = \mathrm{rad}(X)$. As $La \subseteq T$, $L \leqslant \langle T\rangle \cap HQ$, so $L \leqslant \mathrm{rad}(X)$.

Now assume that $X_1 \cup X_2 \neq \emptyset$, Then $X^{[2]} = (X_1 \cup X_2)^{(2)}$. Due to Theorem 10(ii), the latter set is an $\mathcal{A}$-set, which is clearly contained in K. As $|K|$ is odd, there is an integer m such that $\gcd(m, |K|) = 1$ and $2m \equiv 1 \pmod{|K|}$. Using Theorem 10(i), we conclude that $X_1 \cup X_2 = (X_1 \cup X_2)^{(2m)}$ is also an $\mathcal{A}$-set. If $X_2 \neq \emptyset$, then $X \cap Kab \neq \emptyset$, hence $X \subseteq Kab$. This is impossible by our assumption that $X \not\subseteq Kab$, thus $X_2 = \emptyset$ and $X_1 \neq \emptyset$. Then $\underline{X} \cdot \underline{X_1^{(-1)}} \in \mathcal{A}$. We have $\underline{X} \cdot \underline{X_1^{(-1)}} = \sum_{x\in G} \alpha_x x$ for some non-negative integers α_x's. It is easy to see that $\alpha_a = |X_1|$. Also, $\alpha_y = \alpha_a$ for every $y \in T$ because T is a basic set and $a \in T$. In particular, as $La \subseteq T$, we obtain that

$$\sum_{y\in La} \alpha_y = |X_1| \cdot |L|.$$

Now fix $x \in X_1$. Denote by ν_x the number of elements $x' \in X$ such that $x'x^{-1} \in La$. We find that $\nu_x = |X \cap Lax| = \ell$ because $ax \in X$. Then we can write that

$$|X_1| \cdot |L| = \sum_{y\in La} \alpha_y = \sum_{x\in X_1} \nu_x = |X_1| \cdot \ell.$$

This shows that $\ell = |L|$, so $L \leqslant \mathrm{rad}(X)$. □

Lemma 20. *Assuming Hypothesis 18, suppose that $ab \in T$ and $La \subseteq T$ for some $\mathcal{A}$-subgroup L, $L \leqslant H_0$. Then $\mathcal{A}$ is the H/L-wreath product.*

Proof. Assume to the contrary that there is a basic set X, $X \not\subseteq H$ and $L \not\leqslant \mathrm{rad}(X)$. Due to (1), there is a constant ℓ, $0 < \ell < |L|$ such that $|X \cap Lx| = 0$ or ℓ for every $x \in G$. Since $|L|$ is odd, it is possible to choose X so that $\ell < |L|/2$.

As $X \not\subseteq H$, $X = X_1a \cup X_2ab \cup X_3a \cup X_3ab$, where X_1, X_2 and X_3 are pairwise disjoint subsets of H_0. If $X_1 \cup X_2 = \emptyset$, then the argument, used in the proof of the previous lemma, yields that $L \leqslant \mathrm{rad}(X)$. This is impossible, hence $X_1 \cup X_2 \neq \emptyset$.

Consequently, $X_1 \cup X_2$ is a non-empty $\mathcal{A}$-set, and the product $\underline{X} \cdot \underline{X_1^{(-1)} \cup X_2^{(-1)}}$ belongs to $\mathcal{A}$. Write it as $\sum_{x\in G} \alpha_x x$. It is easy to see that $\alpha_a = |X_1|$ and $\alpha_{ab} = |X_2|$. Since $ab \in T$, $\alpha_a = \alpha_{ab}$, so $|X_1| = |X_2|$. As $La \subseteq T$, we obtain

$$\sum_{y\in La} \alpha_y = |X_1| \cdot |L|.$$

Now fix $x \in X_1 \cup X_2$ and denote by ν_x the number of elements $x' \in X$ such that $x'x^{-1} \in aL$. Notice that $\nu_x = |X \cap Lax|$, and so $\nu_x = 0$ or ℓ for every $x \in X_1 \cup X_2$. Then we can write

$$|X_1| \cdot |L| = \sum_{y\in La} \alpha_y = \sum_{x\in X_1\cup X_2} \nu_x \leqslant (|X_1| + |X_2|) \cdot \ell = |X_1| \cdot 2\ell.$$

This contradicts our assumption that $\ell < |L|/2$. □

Lemma 21. *Assuming Hypothesis 18, suppose that $T = La \cup Lab$ for some subgroup $L \leqslant H_0$, $L \neq 1$, and L contains no non-trivial $\mathcal{A}$-subgroup. Then $\mathcal{A}$ is the H/M-wreath product, where $M = \langle b, L\rangle$.*

Proof. Observe that $\langle T\rangle = \langle a, b\rangle L$. Thus $\langle T\rangle \cap H = M$, in particular, $\underline{M} \in \mathcal{A}$ because both $\langle T\rangle$ and H are $\mathcal{A}$-subgroups. Let N be a minimal non-trivial $\mathcal{A}$-subgroup contained in $M = \langle L, b\rangle$. Then $\mathcal{A}_N$ is a primitive S-ring. As $N \nleqslant L$, $\langle b\rangle$ is a Sylow 2-subgroup of N. By a result of Wielandt (see [24, Theorem 25.4]), $\mathcal{A}_N$ has rank 2, and we have that $N^\#$ is a basic set.

Consider the S-ring $\mathcal{A}_{G/N}$. Then G/N has twice odd order and T/N is the basic set containing the unique involution. It follows from Lemma 14 that

$$T/N = \langle T\rangle/N \setminus H/N \text{ and } \langle T\rangle/N \cap H/N \leqslant \mathrm{rad}(X/N),$$

where $X \in \mathcal{S}(\mathcal{A})$, $X \nsubseteq H$. The group $\langle T\rangle/N \cap H/N = M/N$, and by (5), $M \leqslant \mathrm{rad}(NX)$. This shows that it is sufficient to show that $N \leqslant \mathrm{rad}(X)$ for every basic set $X \in \mathcal{S}(\mathcal{A})$, $X \nsubseteq H$.

Assume to the contrary that there is a basic set X such that $X \nsubseteq H$ and $N \nleqslant \mathrm{rad}(X)$. Due to (1), there is a constant ℓ, $0 < \ell < |N|$ such that $|X \cap Nx| = 0$ or ℓ for every $x \in G$. It is possible to choose X such that $\ell \leqslant |N|/2$.

As $X \nsubseteq H$, $X = X_1a \cup X_2ab \cup X_3a \cup X_3ab$, where X_1, X_2 and X_3 are pairwise disjoint subsets of H_0. Let us consider the product $\underline{X} \cdot \underline{X^{(-1)}}$, which is in $\mathcal{A}$. Write it as $\sum_{x\in G} \alpha_x x$. It is easy to see that $\alpha_b = 2|X_3|$. As $N^\#$ is a basic set, we obtain

$$\sum_{y\in N^\#} \alpha_y = 2|X_3| \cdot (|N| - 1).$$

Now fix $x \in X$. If ν_x denotes the number of elements $x' \in X$ such that $x'x^{-1} \in N^\#$, then we find that $\nu_x = |X \cap Nx| - 1 = \ell - 1$, and so we obtain that

$$2|X_3| \cdot (|N| - 1) = \sum_{y\in N^\#} \alpha_y = \sum_{x\in X} \nu_x = |X| \cdot (\ell - 1). \tag{6}$$

This combined with the fact that $|X| = 2|X_3| + |X_1| + |X_2|$ and the assumption that $\ell \leqslant |N|/2$ yield that

$$2|X_3| < |X_1| + |X_2|. \tag{7}$$

In particular, $X_1 \cup X_2 \neq \emptyset$.

Let us consider the product $\underline{X} \cdot \underline{(X_1^{(-1)} \cup X_2^{(-1)})} = \sum_{x\in G} \beta_x x$. Computing the value $\sum_{y\in Na} \beta_y$ in two ways as in the proof of Lemma 20, we deduce that

$$|X_1| \cdot |N| = |X_1| \cdot 2\ell.$$

We show next that $\ell = 1$, and hence $N = \langle b\rangle$.

Choose $y, z \in X_1a \cup X_2ab$ such that $y \neq z$, and assume for the moment that $My = Mz$. If $y, z \in X_1a$ or $y, z \in X_2ab$, then $yz^{-1} \in M \cap \langle X_1 \cup X_2\rangle$. If $y \in X_1a$ and $z \in X_2ab$, then as $b \in M$, $bz \in X_2a$, and we get $y(bz)^{-1} \in M \cap \langle X_1 \cup X_2 \rangle$. Note that $y \neq bz$ because $X_1 \cap X_2 = \emptyset$. The set $X_1 \cup X_2$ is an $\mathcal{A}$-set and we obtain that $\langle X_1 \cup X_2 \rangle \cap M$ is a non-trivial $\mathcal{A}$-subgroup. But, as the latter subgroup is contained in $L = H_0 \cap M$, this contradicts our initial assumption that no such subgroup exists. Thus, $My \neq Mz$. This implies that $Ny \neq Nz$ also holds, therefore, if $\ell > 1$, then we can write that

$$|X_1| + |X_2| \leqslant \sum_{x \in X_1a \cup X_2ab} |Nx \cap (X_3a \cup X_3ab)| \leqslant 2|X_3|.$$

This contradicts (7), and we conclude that $\ell = 1$.

Substituting this in (6) gives us that $X_3 = \emptyset$. We have shown above that $M \leqslant \mathrm{rad}(NX)$. Let $x \in X$. Using also that $N = \langle b \rangle$ and $X = X_1a \cup X_2ab$, we find that

$$\begin{aligned} |M| &= |Mx \cap NX| = |Mx \cap (X \cup Xb)| = |Mx \cap X| + |Mx \cap Xb| \\ &= 2|Mx \cap X| = 2|Mx \cap (X_1a \cup X_2ab)|, \end{aligned}$$

where the third equality is true because $X \cap Xb = \emptyset$ and the fourth equality follows as $b \in M$. Finally, then $|Mx \cap (X_1a \cup X_2ab)| = |M|/2 = |L| > 1$, which contradicts our previous observation that $My \neq Mz$ for any distinct elements $y, z \in X_1a \cup X_2ab$. □

In our last lemma before the proof of Theorem 3 we describe the basic set T when H is a cyclic group.

Lemma 22. *Assuming Hypothesis 18, suppose that H is a cyclic group. Then*

$$T \in \big\{La,\ La \cup Lab \mid 1 \leqslant L \leqslant H_0\big\} \ \cup\ \big\{Ma \cup (M \setminus L)ab \mid 1 \leqslant L < M \leqslant H_0\big\}. \quad (8)$$

Proof. We proceed by induction on $|H_0|$. Suppose first that $|H_0| = p$ for a prime p. For every integer k such that $\gcd(k, 2p) = 1$, $a^k = a$, and thus $T^{(k)} = T$ due to Theorem 10(i). It follows that T is one of the following sets:

$$\{a\},\ \{a, ab\},\ \{a\} \cup H_0^{\#}ab,\ \{a\} \cup H_0ab,\ H_0a,\ H_0a \cup \{ab\},\ H_0a \cup H_0^{\#}ab,\ H_0a \cup H_0ab.$$

Thus (8) holds unless $T = \{a\} \cup H_0^{\#}ab$ or $\{a\} \cup H_0ab$ or $H_0a \cup \{ab\}$. In each of the latter cases, $H_0 = \langle T^{[2]} \rangle$, so $\underline{H_0} \in \mathcal{A}$ by Theorem 10(ii). Then, however, $|T \cap H_0a| \neq |T \cap H_0ab|$, contradicting the identity in (1). This shows that the lemma holds if $|H_0|$ is a prime.

Now assume that $|H_0|$ is a composite number. Let $R = \mathrm{rad}(T)$. If $R \neq 1$ and $|R|$ is odd, then the lemma follows from the induction hypothesis applied to $\mathcal{A}_{G/R}$. Whereas if $|R|$ is even, then the lemma follows from Lemma 14 applied to $\mathcal{A}_{G/R}$. For the rest of the proof let $R = 1$. We are going to show that $T = M\{a, ab\} \setminus \{ab\}$ for some $1 \leqslant M \leqslant H_0$, in particular, (8) holds in this case as well.

Write T as

$$T = T_1a \cup T_2ab \cup T_3a \cup T_3ab,$$

where T_1, T_2 and T_3 are pairwise disjoint subsets of H_0. Note that $T_1 \cup T_2 \neq \emptyset$ because $R = 1$. Using also that $T_1 \cup T_2 \subseteq K$, we find that $K \neq 1$. Fix a prime divisor p of $|K|$

and consider the set $T^{[p]}$. Since $R = 1$ and H_0 is a cyclic group, it follows that $T^{[p]} \neq \emptyset$. Let $N = \langle T^{[p]} \rangle$. It is clear that $N < G$ and $\underline{N} \in \mathcal{A}$ by Theorem 10(ii). If $\langle a, b\rangle \leqslant N$, then the induction hypothesis can be applied to $\mathcal{A}_N$, and this yields $T = M\{a, ab\} \setminus \{ab\}$ for some $1 \leqslant M \leqslant H_0$. Therefore, we may assume that $|\langle a, b\rangle \cap N| = 2$.

Now if $a \in N$, then we can apply Lemma 14 to $\mathcal{A}_N$ and conclude that $T = \{a\}$ because $\mathrm{rad}(T) = 1$.

It remains to consider the case when $ab \in N$ but $a \notin N$. We show that these conditions give rise to a contradiction. Using Lemma 14 and the fact that $\underline{H} \in \mathcal{A}$, we find that the basic set of $\mathcal{A}$ containing ab is equal to Lab for some subgroup $L \leqslant H_0$. Since Lab is a basic set, it follows that $KLab = Kab$ is an $\mathcal{A}$-subset. It is clear that $Kab \cap T = \emptyset$. Using also that $T_1 \cup T_2 \subseteq K$, we find that $T_2 = \emptyset$. On the other hand, the condition that $a \notin N$ shows that $P \leqslant \mathrm{rad}(T_1 \cup T_3)$, where P is the subgroup of K of order p. Choose an element $t \in T_1$. As $T_1 \subseteq K$, $Pt \subseteq K$. Thus, if $Pt \cap T_3 \neq \emptyset$, then $Ptab \cap T_3ab \neq \emptyset$, implying that $Kab \cap T \neq \emptyset$, which is impossible. We conclude in turn that $P \leqslant \mathrm{rad}(T_1)$, $P \leqslant \mathrm{rad}(T_3)$, and eventually that $P \leqslant \mathrm{rad}(T) = R$, contradicting our assumption that $R = 1$. □

We are ready to prove Theorem 3.

Proof of Theorem 3. Let us keep all the symbols $H, H_0, G, a, b, \mathcal{A}, T, K$ set in Hypothesis 18, and assume, in addition, that H is a cyclic group and $\underline{\{a\}} \notin \mathcal{A}$. Define the subgroup

$$V = \bigcap_{X \in \mathcal{S}(\mathcal{A}),\, X \cap H_0 a \neq \emptyset} \mathrm{rad}(X \cap H_0 a).$$

We have to show that $V \neq 1$ provided that $T \neq \{a, ab\}$. We distinguish three cases according to the possibilities for T mentioned in Lemma 22.

Case 1. $T = La$, $1 \leqslant L \leqslant H_0$.

Since $\{a\}$ is not a basic set of $\mathcal{A}$ due to one of the assumptions in Theorem 3, it follows that $L > 1$. Let $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap H_0 a \neq \emptyset$. It is sufficient to show that $L \leqslant \mathrm{rad}(X)$. Notice that $\langle T, K\rangle = \langle a, K\rangle$ is an $\mathcal{A}$-subgroup. Applying Lemma 14 to $\mathcal{A}_{\langle a,K\rangle}$, we obtain that $L \leqslant \mathrm{rad}(X)$ if $X \subseteq Ka$. Assume that $X \nsubseteq Ka$. Let T' be the basic set containing ab. By Lemma 22, $T' = Mab$ or $Nab \cup (N \setminus M)a$ for some subgroups $1 \leqslant M < N \leqslant H_0$. In the former case $M \leqslant K$ and $\underline{Kab} \in \mathcal{A}$. As $X \nsubseteq H \cup Kab$, $L \leqslant \mathrm{rad}(X)$ due to Lemma 19. In the latter case $\langle T'\rangle \setminus (H \cup T') = Ma$, implying that $\underline{Ma} \in \mathcal{A}$. Thus $L \leqslant M$, and so $Lab \subseteq T'$. As $X \nsubseteq H \cup Ka$, $L \leqslant \mathrm{rad}(X)$ follows after applying Lemma 19 with T' and ab playing the role of T and a, respectively, in Lemma 19.

Case 2. $T = La \cup Lab$, $1 \leqslant L \leqslant H_0$.

If $L = 1$, then $T = \{a, ab\}$. Assume that $L \neq 1$. Then it follows from Lemmas 20 and 21 that $\mathcal{A}$ is the H/N-wreath product, where $1 < N \leqslant L$ or $N = \langle L, b\rangle$. In either case, $1 < N \cap H_0 \leqslant V$, in particular, $V \neq 1$.

Case 3. $Ma \cup (M \setminus L)ab$, $1 \leqslant L < M \leqslant H_0$.

Then $\langle T\rangle \setminus (H \cup T) = Lab$, implying that $\underline{Lab} \in \mathcal{A}$. By Lemma 22, the basic set containing ab is equal to the coset Nab for some subgroup $1 \leqslant N \leqslant L$.

If $N = 1$, then $\{ab\}$ is a basic set. Then so is $Tab = Mb \cup (M \setminus L)$. Observe that if $X \in \mathcal{S}(\mathcal{A})$ such that $X \cap H_0 a \neq \emptyset$, then Xab is also basic, it is contained in H and has non-empty intersection with $H_0 b$. By Lemma 14, $L \leqslant \mathrm{rad}(Xab)$, so $L \leqslant \mathrm{rad}(X)$, and this yields that $1 < L \leqslant V$.

Now assume that $N \neq 1$. Let $X \in \mathcal{S}(\mathcal{A})$ be a basic set such that $X \cap H_0 a \neq \emptyset$. Then $X \not\subseteq Kab$, and $N \leqslant \mathrm{rad}(X)$ holds by Lemma 19. All these yield that $1 < N \leqslant V$. □

5 Generalized multipliers

Generalized multipliers of $\mathbb{Z}_n$ were introduced by Muzychuk [15], who used them in his solution to the isomorphism problem for circulant graphs. For our purposes, we consider the particular case where $n = p^e$ for a prime p.

In what follows, for a cyclic group H and a positive divisor d of $|H|$, we denote by H_d the unique subgroup of H of order d.

5.1 Generalized multipliers

Definition 23. Let p be a prime and $e \geqslant 1$ be an integer. A *generalised multiplier* of $\mathbb{Z}_{p^e}$ is an e-tuple $\vec{m} = (m_1, \ldots, m_e)$ of positive integers such that $\gcd(m_i, p) = 1$ for every $i \in [1, e]$.

The set of all generalized multipliers of $\mathbb{Z}_{p^e}$ is denoted by $\mathbb{Z}_{p^e}^{**}$.

Definition 24. Let $\vec{m} \in \mathbb{Z}_{p^e}^{**}$ and $H = \langle h\rangle \cong \mathbb{Z}_{p^e}$. Define the mapping $f_{\vec{m}} : H \to H$ as

$$\forall x \in \mathbb{Z}_{p^e},\ (h^x)^{f_{\vec{m}}} = h^{x'},$$

where $x = \sum_{i=0}^{e-1} x_i p^i$ is the *p-adic expansion* of x, i.e., $0 \leqslant x_i \leqslant p-1$ for every $i \in [0, e-1]$; and $x' = \sum_{i=0}^{e-1} m_{e-i} x_i p^i$.

It is not hard to show that the mapping $f_{\vec{m}}$ in the above definition is bijective. In the next definition we extend $f_{\vec{m}}$ to a permutation of a cyclic group $\widehat{H}$ of order $2p^e$, where $p > 2$. For this purpose we use the fact that any element $x \in \widehat{H}$ admits a unique factorization $x = x_1 x_2$, where $x_1 \in \widehat{H}_{p^e}$ and $x_2 \in \widehat{H}_2$.

Definition 25. Let $\vec{m} \in \mathbb{Z}_{p^e}^{**}$ and $\widehat{H} \cong \mathbb{Z}_{2p^e}$, where p is an odd prime. Define the mapping $\widehat{f}_{\vec{m}} : \widehat{H} \to \widehat{H}$ as

$$\forall x \in \widehat{H}_{p^e}, \forall y \in \widehat{H}_2,\ (xy)^{\widehat{f}_{\vec{m}}} = x^{f_{\vec{m}}} y.$$

If $\vec{m} \in \mathbb{Z}_{p^e}^{**}$ and S is an inverse-closed subset of $\widehat{H} \cong \mathbb{Z}_{2p^2}$ not containing $1_{\widehat{H}}$, then Muzychuk [15] gave a sufficient condition for $\widehat{f}_{\vec{m}}$ to be an isomorphism of $\mathrm{Cay}(\widehat{H}, S)$. This condition is formulated in terms of so called primary keys.

5.2 Primary keys

Definition 26. Let p be a prime and $e \geqslant 1$ be an integer. The *key space* $\mathbf{K}_{p^e}$ consists of the e-tuples $\mathbf{k} = (k_1, \ldots, k_e)$ of integers such that

(K1) If $1 \leqslant i \leqslant e$, then $0 \leqslant k_i \leqslant i - 1$,

(K2) If $2 \leqslant i \leqslant e$, then $k_{i-1} \leqslant k_i$.

The e-tuples in $\mathbf{K}_{p^e}$ are called *primary keys*.

Definition 27. Let $\mathbf{k} = (k_1, \ldots, k_e) \in \mathbf{K}_{p^e}$ and $H \cong \mathbb{Z}_{p^e}$. The *key partition* $\Pi_H(\mathbf{k})$ is the partition of H defined as

$$\Pi_H(\mathbf{k}) = \left\{ H_{\omega(x)}x \mid x \in H \right\},$$

where the mapping $\omega : H \to \{p^i \mid i \in [0, e]\}$ is defined as

$$\forall x \in H,\ \omega(x) = \begin{cases} 1 & \text{if } \ x = 1_H, \\ p^{k_t} & \text{if } \ o(x) = p^t > 1. \end{cases}$$

The above definition can be extended naturally to cyclic groups of order $2p^e$, where $p > 2$.

Definition 28. Let $\mathbf{k} \in \mathbf{K}_{p^e}$ for a prime $p > 2$ and $\widehat{H} \cong \mathbb{Z}_{2p^e}$. The *key partition* $\Pi_{\widehat{H}}(\mathbf{k})$ is the partition of $\widehat{H}$ defined as

$$\Pi_{\widehat{H}}(\mathbf{k}) = \left\{ Xy \mid X \in \Pi_{\widehat{H}_{p^e}}(\mathbf{k}),\, y \in \widehat{H}_2 \right\}.$$

For a primary key $\mathbf{k} \in \mathbf{K}_{p^e}$, let $\mathbb{Z}_{p^e}^{**}(\mathbf{k}) \subseteq \mathbb{Z}_{p^e}^{**}$ be the subset defined by $\mathbb{Z}_p^{**}(\mathbf{k}) := \mathbb{Z}_p^{**}$ (i.e., $e = 1$), and if $e > 1$, then

$$\mathbb{Z}_{p^e}^{**}(\mathbf{k}) := \left\{ \vec{m} = (m_1, \ldots, m_e) \in \mathbb{Z}_{p^e}^{**} \mid \forall i \in [2, e],\ m_i \equiv m_{i-1} \pmod{p^{i-1-k_i}} \right\}. \tag{9}$$

If $\vec{m} = (m_1, \ldots, m_e) \in \mathbb{Z}_{p^e}^{**}(\mathbf{k})$] such that m_i is odd for every $i \in [1, e]$ and $\widehat{H} \cong \mathbb{Z}_{2p^e}$, then $\widehat{f}_{\vec{m}}$ permutes the $\Pi_{\widehat{H}}(\mathbf{k})$-classes. Moreover, $\widehat{f}_{\vec{m}}$ induces an isomorphism of $\mathrm{Cay}(\widehat{H}, X)$ for every class $X \in \Pi_{\widehat{H}}(\mathbf{k})$, $X \neq \{1_{\widehat{H}}\}$.

Proposition 29 ([15, case (2) in Proposition 2.4 and Proposition 2.5])**.** *Let $\mathbf{k} \in \mathbf{K}_{p^e}$ for a prime $p > 2$, $\vec{m} = (m_1, \ldots, m_e) \in \mathbb{Z}_{p^e}^{**}(\mathbf{k})$ be a generalized multiplier such that m_i is odd for every $i \in [1, e]$, and let $\widehat{H} \cong \mathbb{Z}_{2p^e}$. Then for every $X \in \Pi_{\widehat{H}}(\mathbf{k})$, if $X \neq \{1_{\widehat{H}}\}$ and $o(X) = p^i$ or $2p^i$, then*

$$\mathrm{Cay}(\widehat{H}, X)^{\widehat{f}_{\vec{m}}} = \mathrm{Cay}(\widehat{H}, X^{(m_i)}).$$

We say that a subset $S \subseteq \widehat{H}$, where $\widehat{H} \cong \mathbb{Z}_{2p^e}$, is a $\Pi_{\widehat{H}}(\mathbf{k})$-*subset*, if S is a union of $\Pi_{\widehat{H}}(\mathbf{k})$-classes. As a corollary of Proposition 29, we have the following sufficient condition for $\widehat{f}_{\vec{m}}$ ($\vec{m} \in \mathbb{Z}_{p^e}^{**}$) to be an isomorphism of a Cayley graph $\mathrm{Cay}(\widehat{H}, S)$.

Corollary 30. *Let $\vec{m} = (m_1, \ldots, m_e) \in \mathbb{Z}_{p^e}^{**}$, where p is an odd prime, such that m_i is odd for every $i \in [1, e]$, $\widehat{H} \cong \mathbb{Z}_{2p^e}$ and $\Gamma = \mathrm{Cay}(\widehat{H}, S)$. If there exists a primary key $\mathbf{k} \in \mathbb{Z}_{p^e}^{**}$ such that $\vec{m} \in \mathbb{Z}_{p^e}^{**}(\mathbf{k})$ and S is a $\Pi_{\widehat{H}}(\mathbf{k})$-subset, then $\widehat{f}_{\vec{m}}$ is an isomorphism from Γ to $\mathrm{Cay}(\widehat{H}, S^{\widehat{f}_{\vec{m}}})$.*

5.3 Primary keys and S-rings

Definition 31. Let $H \cong \mathbb{Z}_{p^e}$ for an odd prime p and $e \geqslant 1$, and $\mathcal{A}$ be an S-ring over H. For $i \in [1, e]$, let $X_i \in \mathcal{S}(\mathcal{A})$ be a basic set containing an element of order p^i.[2] We define the e-tuple $\mathbf{k}(\mathcal{A}) := (k_1, \ldots, k_e)$ as

$$\forall i \in [1, e],\ p^{k_i} = \left|\operatorname{rad}(X_i \cap (H_{p^i} \setminus H_{p^{i-1}}))\right|.$$

For every S-ring $\mathcal{A}$ over H, it is not hard to show that the e-tuple $\mathbf{k}(\mathcal{A})$ is a primary key. It is obvious that axiom (K1) holds, i.e., $k_i \leqslant i - 1$. One can use Propositions 16 and 17 to verify that axiom (K2) holds too, i.e., $k_{i-1} \leqslant k_i$ whenever $i > 1$.

Note also that, if $x \in H$ with $o(x) = p^i$ and $X \in \mathcal{S}(\mathcal{A})$ is the basic set containing x, then $H_{p^{k_i}} x \subseteq X$, where $\mathbf{k}(\mathcal{A}) = (k_1, \ldots, k_e)$; in other words, X is a $\Pi_H(\mathbf{k})$-subset.

A key step in the proof of Theorem 4 will be a construction of a particular generalized multiplier contained in $\mathbb{Z}_{p^e}^{**}(\mathbf{k}(\mathcal{A}))$, where $\mathcal{A}$ is an S-ring over a cyclic group of order p^e, $p > 2$. In this construction we shall use two facts from elementary number theory.

Fix an odd prime p. We denote by $\mathbb{Z}_{p^e}^*$ the multiplicative group of integers modulo p^e. It is well-known that $\mathbb{Z}_{p^e}^* \cong \mathbb{Z}_{p^{e-1}(p-1)}$. For $j \in [0, e-1]$, the unique subgroup of $\mathbb{Z}_{p^e}^*$ of order p^j can be can be written in the form $\{xp^{e-j} + 1 \mid x \in [0, p^j - 1]\}$, which coincides with the coset $H_{p^j} + 1$, where $H = \mathbb{Z}_{p^e}$ and H_{p^j} is the subgroup of H of order p^j. Also, if $L \leqslant \mathbb{Z}_{p^e}^*$ is the subgroup of order $p - 1$, then acting on $\mathbb{Z}_{p^e}$, $L_x = 1$ for every $x \in \mathbb{Z}_{p^e}, x \neq 0$. More generally, the following lemma holds.

Lemma 32. *Let $H \cong \mathbb{Z}_{p^e}$ for an odd prime p and $e \geqslant 1$, let $x \in H$ and let $K \leqslant \operatorname{Aut}(H)$.*

(i) If $p \nmid |K|$ and $x \neq 1_H$, then $|\operatorname{Orb}_K(x)| = |K|$.

(ii) If $o(x) = p^i$ for some $i \in [0, e]$ and $|K| = p^j$ for some $j \in [0, e-1]$, then

$$\operatorname{Orb}_K(x) = H_{p^{j-\min(j,e-i)}} x.$$

Proof. Part (i) follows directly from the paragraph preceding the lemma.

For part (ii), one can see that $\operatorname{Orb}_K(x)$ is a coset of some subgroup of H of p-power order, and hence it only remains to find the length of the orbit $\operatorname{Orb}_K(x)$. It is not hard to show that $|\operatorname{Aut}(H)_x| = p^{e-i}$. As $|\operatorname{Orb}_K(x)| = |K|/|K \cap \operatorname{Aut}(H)_x|$, we compute that $|\operatorname{Orb}_K(x)| = p^{j-\min(j,e-i)}$. □

Recall that, for an integer $m > 1$ such that m is not divisible by a prime p, $\sigma_{p^i}(m)$ denotes the order of m modulo p^i, i.e., the smallest positive integer l satisfying $m^l \equiv 1 \pmod{p^i}$. Equivalently, $\sigma_{p^i(m)} = o(m)$, where m is regarded as an element of $\mathbb{Z}_{p^i}^*$, or in other words, $\sigma_{p^i(m)} = |\langle m \rangle|$.

[2]Note that, it may happen that $X_i = X_j$ for some $i \neq j$. Also, if X' is any basic set containing an element of order p^i, then it follows from Theorem 10(i) that $X' = X_i^{(m)}$ for some integer m not divisible by p. This implies that $\operatorname{rad}(X' \cap (H_{p^i} \setminus H_{p^{i-1}})) = \operatorname{rad}(X_i \cap (H_{p^i} \setminus H_{p^{i-1}}))$, and this shows that $\mathbf{k}(\mathcal{A})$ is well-defined.

Lemma 33. *Let m be a positive integer not divisible by an odd prime p such that $\sigma_{p^i}(m)$ is not divisible by p for $i > 1$. Then $\sigma_{p^{i-1}}(m) = \sigma_{p^i}(m)$.*

Proof. We regard m as an element of $\mathbb{Z}_{p^i}^*$ and let $M = \langle m \rangle \leqslant \mathbb{Z}_{p^i}^*$. Then $\sigma_{p^i}(m) = |M|$. Consider the homomorphism $\varphi : \mathbb{Z}_{p^i}^* \to \mathbb{Z}_{p^{i-1}}^*$ that satisfies $\varphi(1) = 1$ (in the right side 1 stands for an element in $\mathbb{Z}_{p^{i-1}}^*$). Then $\sigma_{p^{i-1}}(m) = |\varphi(M)|$. It is well known that $|\operatorname{Ker}(\varphi)| = p$. Using also the assumption that $p \nmid |M|$, we obtain that the restriction of φ to M is injective, by which $|\varphi(M)| = |M|$, and so $\sigma_{p^{i-1}}(m) = \sigma_{p^i}(m)$. □

Lemma 34. *Let $H \cong \mathbb{Z}_{p^e}$ for an odd prime p, $e \geqslant 1$, and $\mathcal{A}$ be an S-ring over H. There exists a generalized multiplier $\vec{m} = (m_1, \ldots, m_e) \in \mathbb{Z}_{p^e}^{**}(\mathbf{k}(\mathcal{A}))$ such that for every $i \in [1, e]$, m_i is odd, and for every cyclotomic basic set $X \in \mathcal{S}(\mathcal{A})$, $X \neq \{1_H\}$,*

$$o(X) = p^i \implies \sigma_{p^i}(m_i) = |X|/|\operatorname{rad}(X)|. \tag{10}$$

Proof. Assume first that $e = 1$. Then $\mathcal{A} = V(\mathbb{Z}_p, K)$ for a subgroup $K \leqslant \operatorname{Aut}(H)$ (see Proposition 17). The lemma holds after letting $\vec{m}$ to be (m_1), where m_1 is a positive integer coprime with $2p$ and satisfying $\sigma_p(m_1) = |K|$.

Let $e > 1$ and let $\mathbf{k}(\mathcal{A}) = \mathbf{k} = (k_1, \ldots, k_e)$. For every $i \in [1, e]$, fix a a basic set X_i containing an element of order p^i. We define $\vec{m} = (m_1, \ldots, m_e)$ recursively starting with its e-th entry.

- Let m_e be a positive integer such that it is coprime with $2p$, and if X_e is cyclotomic, then $\sigma_{p^e}(m_e) = |X_e|/|\operatorname{rad}(X_e)|$.
- Let $i \in [2, e]$ and suppose that m_i is already defined. If X_{i-1} is cyclotomic and $k_i = i - 1$, then let m_{i-1} be a positive integer coprime with $2p$ and satisfying $\sigma_{p^{i-1}}(m_{i-1}) = |X_{i-1}|/|\operatorname{rad}(X_{i-1})|$; and let $m_{i-1} = m_i$ otherwise.

It can be easily checked that $\vec{m} \in \mathbb{Z}_{p^e}^{**}(\mathbf{k})$.

We finish the proof by showing that (10) holds. Let X be an arbitrary cyclotomic basic set of $\mathcal{A}$ with $o(X) = p^i > 1$. By Theorem 10(i), $X = X_i^{(l)}$ for some integer $l > 1$ not divisible by p. Consequently, X_i is cyclotomic and

$$|X|/|\operatorname{rad}(X)| = |X_i|/|\operatorname{rad}(X_i)|. \tag{11}$$

Assume for the moment that $o(X)$ is maximal among all cyclotomic basic sets X of $\mathcal{A}$. If $i = e$, then (10) holds because of (11) and the definition of m_e. Suppose that $i < e$. Then X_{i+1} is not cyclotomic, hence it follows from Proposition 16 that $k_{i+1} = i$. Then (10) holds because of (11) and the definition of m_i.

Therefore, we may assume that (10) holds for every cyclotomic basic set X' with $o(X') > o(X)$. As above, (10) holds if $k_{i+1} = i$, hence let $k_{i+1} < i$. It follows from Proposition 16 that X_{i+1} is cyclotomic. According to the definition of $\vec{m}$, we have that $m_i = m_{i+1}$.

Then $\langle X_{i+1}\rangle = H_{p^{i+1}}$ and $\mathrm{rad}(X_{i+1}) = H_{p^{k_{i+1}}}$, hence the latter subgroups are $\mathcal{A}$-subgroups. It follows from Proposition 17 that $\mathcal{A}_{H_{p^{i+1}}/H_{p^{k_{i+1}}}} = V(H_{p^{i+1}}/H_{p^{k_{i+1}}}, L)$ such that $L \leqslant \mathrm{Aut}(H_{p^{i+1}}/H_{p^{k_{i+1}}})$ and

$$|L| = |X_{i+1}/H_{p^{k_{i+1}}}| = |X_{i+1}|/|\,\mathrm{rad}(X_{i+1})| = \sigma_{p^{i+1}}(m_{i+1}) = \sigma_{p^{i+1}}(m_i), \tag{12}$$

where the last but one equation follows from the assumption that (10) holds for X_{i+1}.

Now, $X_i/H_{p^{k_{i+1}}}$ is a basic set of $\mathcal{A}_{H_{p^{i+1}}/H_{p^{k_{i+1}}}}$, so it is an L-orbit. As $p \nmid |L|$, by Lemma 32(i),

$$|X_i/H_{p^{k_{i+1}}}| = |L|. \tag{13}$$

We show next that

$$|X_i/H_{p^{k_{i+1}}}| = |X_i|/|\,\mathrm{rad}(X_i)|. \tag{14}$$

Fix an arbitrary element $x \in X_i$ and let $\ell = |X_i \cap H_{p^{k_{i+1}}}x|$. It follows from (1) that $|X_i/H_{p^{k_{i+1}}}| = |X_i|/\ell$. Since X_i is cyclotomic, $X_i = \mathrm{Orb}_K(x)$ for some subgroup $K \leqslant \mathrm{Aut}(H)$. Lemma 32 and the assumption that $k_{i+1} < i$ yield in turn that, if $x' \in X_i \cap H_{p^{k_{i+1}}}x$, then x' is in the orbit of x under the Sylow-p-subgroup of K, $x' \in \mathrm{rad}(X_i)x$, and so $\ell \leqslant |\,\mathrm{rad}(X_i)|$. On the other hand, as $\mathrm{rad}(X_i) = H_{p^{k_i}}$ and $k_i \leqslant k_{i+1}$, we also obtain that $\ell \geqslant |\,\mathrm{rad}(X_i)|$, by which (14) holds.

Finally, $\sigma_{p^{i+1}}(m_i) = \sigma_{p^i}(m_i)$ due to Lemma 33; and combining this with the identities (11)–(14), yields that $\sigma_{p^i}(m_i) = |X|/|\,\mathrm{rad}(X)|$, what is required in (10). □

Corollary 35. *With the notation in Lemma 34, for every $X \in \mathcal{S}(\mathcal{A})$, if $o(X) = p^i$ for some $i \in [1, e]$, then $X^{(m_i)} = X$.*

6 Proof of Theorem 4

We keep the notation set in Theorem 4, i.e., $H \cong \mathbb{Z}_{2p^e}$ for some odd prime p and $e \geqslant 1$ and $\mathrm{Cay}(H, S)$ is a connected and non-bipartite graph. Let b be the unique involution of H and H_0 be the unique subgroup of H of order p^e. In view of Remark 5, we may assume that $\mathrm{Cay}(H, S)$ is unstable. To settle Theorem 4, we have to show that,

$$(S \cap H_0)h = S \cap H_0 \text{ for some } h \in H_0, h \neq 1_H, \tag{15}$$

or

$$\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, Sb). \tag{16}$$

By Proposition 1, there is a Schurian S-ring $\mathcal{A}$ over G such that $\underline{H}, \underline{Sa} \in \mathcal{A}$ and $\underline{\{a\}} \notin \mathcal{A}$. Let

$$V = \bigcap_{X \in \mathcal{S}(\mathcal{A}),\, X \cap H_0 a \neq \emptyset} \mathrm{rad}(X \cap H_0 a).$$

Then $S \cap H_0 \neq \emptyset$ because $\mathrm{Cay}(H, S)$ is non-bipartite. It follows that $Sa \cap H_0 a \neq \emptyset$ and $(Sa \cap H_0 a)h = Sa \cap H_0 a$ for every $h \in V$. This shows that (15) holds if $V \neq 1$. For the rest of the section we assume that $V = 1$.

Then $\{a, ab\}$ is a basic set of $\mathcal{A}$ due to Theorem 3 and hence $E := \langle a, ab\rangle$ is an $\mathcal{A}$-subgroup. Let

$$\mathbf{k} = \mathbf{k}(\mathcal{A}_{G/E}) = (k_1, \ldots, k_e)$$

and $\vec{m} = (m_1, \ldots, m_e)$ be a generalized multiplier defined for $\mathcal{A}_{G/E}$ in Lemma 34.

Fix a basic set $X \in \mathcal{S}(\mathcal{A})$ such that $X \not\subseteq H$, $X \neq \{a, ab\}$. As $\langle b\rangle = E \cap H$ and E, H are $\mathcal{A}$-subgroups, so is $\langle b\rangle$. It follows from this and (1) that

$$X = X_1 a \cup X_2 ab,$$

where $X_1, X_2 \subseteq H_0$ and either $X_1 = X_2$ or $X_1 \cap X_2 = \emptyset$. Since $X \not\subseteq H$, it follows that the order $o(X) = |\langle X\rangle|$ is even. We show that

$$o(X) = 2p^i \implies X^{(m_i)} = Xb. \tag{17}$$

The group G is in the form $G = E \times H_0$. In what follows, we identify G/E with H_0 and regard $\mathcal{A}_{G/E}$ as an S-ring over H_0; in particular, $X_1 \cup X_2$ is a basic set of $\mathcal{A}_{G/E}$. By Corollary 35, $(X_1 \cup X_2)^{(m_i)} = X_1 \cup X_2$. This implies that $X^{(m_i)} \subseteq X \cup Xb$. Thus (17) holds if $X_1 = X_2$, and we may assume that $X_1 \cap X_2 = \emptyset$. As $\{b\} \in \mathcal{S}(\mathcal{A})$, $Xb = X_1 ab \cup X_2 a$ is also a basic set of $\mathcal{A}$. On the other hand, so is $X^{(m_i)}$, see Theorem 10(i), and therefore, $X^{(m_i)} = X$ or Xb. It is sufficient to show that $X^{(m_i)} \neq X$.

Observe that $\langle X^{[2]}\rangle = \langle X_1 \cup X_2\rangle$. The former subgroup is an $\mathcal{A}$-subgroup, so the latter is also and Lemma 15 can be applied to the Schurian S-ring $\mathcal{A}_{E\langle X_1 \cup X_2\rangle}$. As a result, we obtain that X_1 and X_2 are basic sets of an S-ring over the group $\langle X_1 \cup X_2\rangle \leqslant H_0$, and $|X_1| = |X_2|$. According to Proposition 16, if X_1 is not cyclotomic, then $|X_1| = p^i - p^j$, where $i > j + 1$, and hence $|X_1 \cup X_2| = 2(p^i - p^j)$. Regarding that $X_1 \cup X_2 \in \mathcal{S}(\mathcal{A}_{G/E})$, this is impossible. We deduce that each of X_1, X_2 and $X_1 \cup X_2$ is cyclotomic. This means that $X_1 \cup X_2 = \mathrm{Orb}_K(x)$ for some subgroup $K \leqslant \mathrm{Aut}(H_0)$ and X_1 and X_2 are the L-orbits contained in X, where $L < K$, $|K| = 2|L|$, say

$$X_1 = \mathrm{Orb}_L(x_1) \text{ and } X_2 = \mathrm{Orb}_L(x_2).$$

Due to Lemma 34, $\sigma_{p^i}(m_i) = |X_1 \cup X_2|/|\operatorname{rad}(X_1 \cup X_2)|$, which is equal to $|K|_{p'}$. Using also that $o(x_1) = p^i$, this implies that $x_1^{m_i} \notin \mathrm{Orb}_L(x_1) = X_1$. Therefore, $x_1^{m_i} \in X_2$, $(x_1 a)^{m_i} \in X_2 a$, so $X^{(m_i)} \neq X$, and by this (17) holds.

We show next that $Xa = X_1 \cup X_2 b$ is a $\Pi_H(\mathbf{k})$-subset (recall that X was fixed to be an arbitrary basic set of $\mathcal{A}$ such that $X \not\subseteq H$, $X \neq \{a, ab\}$). If $X_1 = X_2$, then this follows from the fact that $X_1 \cup X_2$ is a $\Pi_{H_0}(\mathbf{k})$-subset. If $X_1 \neq X_2$, then we have seen that $X_1 \cup X_2 = \mathrm{Orb}_K(x)$ for a subgroup $K \leqslant \mathrm{Aut}(H_0)$. Thus the $\Pi_{H_0}(\mathbf{k})$-class containing x is equal to the orbit $\mathrm{Orb}_{K_p}(x)$, where K_p is the Sylow p-subgroup of K. Clearly, $K_p \leqslant L$, and this yields that $\mathrm{Orb}_{K_p}(x) \leqslant X_1$ if $x \in X_1$ and $\mathrm{Orb}_{K_p}(x)b \leqslant X_2 b$ if $x \in X_2$. This shows that Xa is a $\Pi_H(\mathbf{k})$-subset, as required.

Consequently, since $\underline{Sa} \in \mathcal{A}$, it follows that S is a $\Pi_H(\mathbf{k})$-subset, and hence $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, S^{\widehat{f}_{\vec{m}}})$ due to Corollary 30. We derive (16) by showing that

$$S^{\widehat{f}_{\vec{m}}} = Sb. \tag{18}$$

Fix an arbitrary element $x \in S$ and let X be the basic set of $\mathcal{A}$ containing xa. Note that $X \subseteq Sa$, and hence $X \neq \{a, ab\}$. Suppose that $o(x) = p^i$ or $2p^i$ and let $Y = H_{p^{k_i}}x$. Then $Y \in \Pi_H(\mathbf{k})$ and $Ya \subseteq X$. By Proposition 29, $Y^{\widehat{f}_{\vec{m}}} = Y^{(m_i)}$. All these together with (17) yield that

$$x^{\widehat{f}_{\vec{m}}}a \in Y^{(m_i)}a = (Ya)^{(m_i)} \subseteq X^{(m_i)} = Xb \subseteq Sab.$$

This shows that $x^{\widehat{f}_{\vec{m}}} \in Sb$, and as x was chosen arbitrarily from S, (18) follows.

Acknowledgements

The authors are grateful to the reviewer for the valuable comments and suggestions, which helped to improve the paper considerably.

Ademir Hujdurović received support from the Slovenian Research Agency (research program P1-0404 and research projects N1-0140, N1-0102, J1-1691, N1-0159, J1-2451, N1-0208, and J1-4084). István Kovács received support from the Slovenian Research Agency (research program P1-0285 and the research projects J1-1695, N1-0140, J1-2451, N1-0208, and J1-3001).

References

[1] M. Ahanjideh, I. Kovács, and K. Kutnar. Stability of Rose Window graphs. *J. Graph Theory*, 127: 810–832, 2024.

[2] B. Bychawski. Classification of unstable circulants of square-free order. arXiv:2410.00701v1, 2024.

[3] S. Evdokimov and I. Ponomarenko. On a family of Schur rings over a finite cyclic group. *Algebra i Analiz*, 13: 139–154, 2001. English translation in *St. Petersburg Math. J.*, 13: 441–451, 2002.

[4] S. Evdokimov and I. Ponomarenko. Characterization of cyclotomic schemes and normal Schur rings over a finite cyclic group. *Algebra i Analiz*, 14: 11–55, 2002. English translation in *St. Petersburg Math. J.*, 14: 189–221, 2003.

[5] B. Fernandes and A. Hujdurović. Canonical double covers of circulants. *J. Combin. Theory Ser. B*, 154: 49–59, 2022.

[6] Ja. Ju. Golfand, N. L. Neimark, and R. Pöschel. The structure of S-rings over Z_{2^m}. *Akad. der Wiss, der DDR Ins. für Math.*, Preprint P-MATH-01/85, 1985.

[7] M. Hirasaka and M. Muzychuk. An elementary abelian group of rank 4 is a CI-group. *J. Combin. Theory Ser. A*, 94: 339–362, 2001.

[8] A. Hujdurović and D. Mitrović. Some conditions implying stability of graphs. *J. Graph Theory*, 105: 98–109, 2024.

[9] A. Hujdurović, D. Mitrović, and D. Witte Morris. On automorphisms of the double cover of a circulant graph. *Electron. J. Combin.*, 28: #P4.43, 2021.

[10] A. Hujdurović, D. Mitrović, and D. Witte Morris. Automorphisms of the double cover of a circulant graph of valency at most 7. *Algebr. Comb.*, 6: 1235–1271, 2023.

[11] M. Ch. Klin, N. L. Neimark, and R. Pöschel. Schur rings over Z_{2^m}. *Akad. der Wiss, der DDR Ins. für Math.*, Preprint P-MATH-14/81, 1981.

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

[13] K. H. Leung and S. H. Man. On Schur rings over cyclic groups. *Isr. J. Math.*, 106: 251–267, 1998.

[14] D. Marušič, R. Scapellato, and N. Zagaglia Salvi. A characterization of particular symmetric (0,1) matrices. *Linear Algebra Appl.*, 119: 153–162, 1989.

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

[16] M. Muzychuk and I. Ponomarenko. Schur rings. *European J. Combin.*, 30: 1526–1539, 2009.

[17] R. Pöschel. Untersuchungen von S-Ringen, insbesondere im Gruppenring von p-Gruppen. *Math. Nachr.*, 60: 1–27, 1974.

[18] Y. L. Qin, B. Xia, and S. Zhou. Stability of circulant graphs. *J. Combin. Theory Ser. B*, 136: 154–169, 2019.

[19] Y. L. Qin, B. Xia, and S. Zhou. Canonical double covers of generalized Petersen graphs, and double generalized Petersen graphs. *J. Graph Theory*, 97: 70–81, 2021.

[20] I. Schur. Zur Theorie der einfach transitiven Permutationgruppen. *S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl.*, 18: 598–623, 1933.

[21] G. Somlai and M. Muzychuk. The Cayley isomorphism property for $\mathbb{Z}_p^3 \times \mathbb{Z}_q$. *Algebr. Comb.*, 4: 289–299, 2021.

[22] D. B. Surowski. Stability of arc-transitive graphs. *J. Graph Theory*, 38: 95–110, 2001.

[23] O. Tamaschke. A generalization of conjugacy in groups. *Rend. Sem. Mat. Univ. Padova*, 40: 408–427, 1968.

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

[25] S. Wilson. Unexpected symmetries in unstable graphs. *J. Combin. Theory Ser. B*, 98: 359–383, 2008.

[26] D. Witte Morris. On automorphisms of direct products of Cayley graphs on abelian groups. *Electron. J. Combin.*, 28: #P3.5, 2021.

[27] D. Witte Morris. Automorphisms of the canonical double cover of a toroidal grid. *Art Discrete Appl. Math.*, 6: #P3.07, 2023.