ON SCHUR 2-GROUPS

MIKHAIL MUZYCHUK AND ILYA PONOMARENKO

Abstract. A finite group $G$ is called a Schur group, if any Schur ring over $G$ is the transitivity module of a point stabilizer in a subgroup of $\text{Sym}(G)$ that contains all right translations. We complete a classification of abelian 2-groups by proving that the group $\mathbb{Z}_2 \times \mathbb{Z}_2^n$ is Schur. We also prove that any non-abelian Schur 2-group of order larger than 32 is dihedral (the Schur 2-groups of smaller orders are known). Finally, in the dihedral case, we study Schur rings of rank at most 5, and show that the unique obstacle here is a hypothetical $S$-ring of rank 5 associated with a divisible difference set.

1. Introduction

Following R. Pöschel [26], a finite group $G$ is called a Schur group, if any $S$-ring over $G$ is the transitivity module of a point stabilizer in a subgroup of $\text{Sym}(G)$ that contains all right translations (for the exact definitions, we refer to Section 2). He proved there that if $p \geq 5$ is a prime, then a finite $p$-group is Schur if and only if it is cyclic. For $p = 2$ or 3, a cyclic $p$-group is still Schur, but Pöschel’s theorem is not true: a straightforward computation shows that an elementary abelian group of order 4 or 9 is Schur. In this paper, we are interested in Schur 2-groups.

Recently in [11], it was proved that every finite abelian Schur group belongs to one of several explicitly given families. In particular, from Lemma 5.1 of that paper it follows that all abelian Schur 2-groups are known except for the groups $\mathbb{Z}_2 \times \mathbb{Z}_2^n$, where $n \geq 5$. We prove that all these groups are Schur (Theorem 10.1). As a by-product we can complete the classification of abelian Schur 2-groups.

Theorem 1.1. An abelian 2-group $G$ is Schur if and only if $G$ is cyclic, or elementary abelian of order at most 32, or is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2^n$ for some $n \geq 1$.

Non-abelian Schur groups have been studied in [25] where it was proved that they are metabelian. In particular, from Theorem 4.2 of that paper it follows that non-abelian Schur 2-groups are known except for dihedral groups and groups

(1) \[ M_{2^n} = \langle a, b : a^{2^{n-1}} = b^2 = 1, bab = a^{1+2^{n-2}} \rangle, \]

where $n \geq 4$. In this paper we prove that the latter groups are not Schur (Theorem 11.1). As a by-product we obtain the following statement.

Theorem 1.2. A non-abelian Schur 2-group of order at least 32 is dihedral.

We do not know whether or not a dihedral 2-group of order more than 32 is Schur. A standard technique based on Wielandt’s paper [29] enables us to describe $S$-rings of rank at most 5 as follows (see Subsection 12.2 for a connection between $S$-rings and divisible difference sets).

The work of the second author was partially supported by the RFBR Grant 14-01-00156.
Theorem 1.3. Let be \( A \) an S-ring over a dihedral 2-group. Suppose that \( \text{rk}(A) \leq 5 \). Then one of the following statements is true:

1. \( A \) is isomorphic to an S-ring over \( \mathbb{Z}_2 \times \mathbb{Z}_{2^n} \),
2. \( A \) is a proper dot or wreath product,
3. \( \text{rk}(A) = 5 \) and \( A \) is associated with a divisible difference set in \( \mathbb{Z}_{2^n} \).

S-rings in statement (1) of this theorem are schurian by Theorem 1.1. By induction, this implies that all S-rings in statement (2) are also schurian. Thus, by Theorem 12.4 we obtain the following corollary.

Corollary 1.4. Under the hypothesis of Theorem 1.3, the S-ring \( A \) is not schurian only if \( A \) is associated with a divisible difference set in a cyclic 2-group.

In fact, we do not know whether there exists a non-trivial divisible difference set in a cyclic 2-group that produces an S-ring \( A \) in part (3) of Theorem 1.3. If such a set does exist, then the corresponding dihedral 2-group is not Schur. On the other hand, in Subsection 12.2 we show that using a relative difference set (which is a special case of a divisible one), one can construct an S-ring of rank 6 (over a dihedral 2-group). These difference sets, and, therefore, S-rings, do exist, but are relatively rare. The only known example is the classical \((q + 1, 2, q, (q - 1)/2)\)-difference set where \( q \) is a Mersenne prime. Thus, the question whether a dihedral 2-group is Schur, remains open.

The paper consists of fourteen sections. In Sections 2, 3 and 4 we give a background of S-rings, Cayley schemes\(^1\) and cite some basic facts on S-rings over cyclic and dihedral groups. In Sections 5–10 we develop a theory of S-rings over \( \mathbb{Z}_2 \times \mathbb{Z}_{2^n} \) that is culminated in Theorem 10.1 stating that this group is Schur. In Section 11 we show that the group \( M_{2^n} \) is not Schur for all \( n \geq 4 \) (Theorem 11.1). In Sections 12–14 we study S-rings over a dihedral 2-group: here, we start with constructions based on cyclic divisible difference sets, and then complete the proof of Theorem 1.3.

**Notation.** As usual, by \( \mathbb{Z} \) we denote the ring of rational integers.

The identity of a group \( D \) is denoted by \( e \); the set of non-identity elements in \( D \) is denoted by \( D^\# \).

Let \( X \subseteq D \). The subgroup of \( D \) generated by \( X \) is denoted by \( \langle X \rangle \); we also set \( \text{rad}(X) = \{ g \in D : gX = Xg = X \} \). The element \( \sum_{x \in X} x \) of the group ring \( \mathbb{Z}D \) is denoted by \( X \). The set \( X \) is called regular if the order \( |x| \) of an element \( x \in X \) does not depend on the choice of \( x \).

For a group \( H \leq D \), the quotient epimorphism from \( D \) onto \( D/H \) is denoted by \( \pi_{D/H} \).

The group of all permutations of \( D \) is denoted by \( \text{Sym}(D) \). The set of orbits of a group \( G \leq \text{Sym}(D) \) is denoted by \( \text{Orb}(G) = \text{Orb}(G, D) \). We write \( G \approx G' \) if the groups \( G, G' \leq \text{Sym}(D) \) are 2-equivalent, i.e. have the same orbits in the coordinate-wise action on \( D \times D \).

Given two subgroups \( L \leq U \leq D \), the quotient group \( U/L \) is called the section of \( D \). For a set \( \Delta \subseteq \text{Sym}(D) \) and a section \( S = U/L \) of \( D \) we set

\[
\Delta^S = \{ f^S : f \in \Delta, Sf = S \},
\]

\(^1\)Here, we assume some knowledge of association scheme theory.
where $S' = S$ means that $f$ permutes the right $L$-cosets in $U$ and $f^S$ denotes the bijection of $S$ induced by $f$.

The cyclic group of order $n$ is denoted by $\mathbb{Z}_n$.

2. A BACKGROUND ON S-RING THEORY

In what follows, we use the notation and terminology of [9].

Let $D$ be a finite group. A subring $A$ of the group ring $\mathbb{Z}D$ is called a Schur ring (S-ring, for short) over $D$ if there exists a partition $S = S(A)$ of $D$ such that

- $(S1)$ $\{e\} \in S$,
- $(S2)$ $X \in S \Rightarrow X^{-1} \in S$,
- $(S3)$ $A = \text{Span}(X : X \in S)$.

When $S = \text{Orb}(K,D)$ where $K \leq \text{Aut}(D)$, the S-ring $A$ is called cyclotomic and denoted by $\text{Cyc}(K,D)$. A group isomorphism $f : D \to D'$ is called a Cayley isomorphism from an S-ring $A$ over $D$ to an S-ring $A'$ over $D'$ if $S(A)^f = S(A')$.

It follows from (S3) that given $X, Y \in S(A)$ there exist non-negative integers $c_{XY}^Z$, $Z \in S(A)$, such that

$$XY = \sum_{Z \in S(A)} c_{XY}^Z Z.$$

One can see that $c_{XY}^Z$ equals the number of different representations $z = xy$ with $(x, y) \in X \times Y$ for a fixed (and hence for all) $z \in Z$. It is a well-known fact that

$$c_{XY}^{Z^{-1}} = c_{X^{-1}Y^{-1}}^Z$$

and

$$|Z|c_{XY}^{Z^{-1}} = |X|c_{YZ}^{X^{-1}} = |Y|c_{XZ}^{Y^{-1}}$$

for all $X, Y, Z$. A ring isomorphism $\varphi : A \to A'$ is said to be algebraic if for any $X \in S(A)$ there exists $X' \in S(A')$ such that $\varphi(X) = X'$.

The classes of the partition $S$ and the number $\text{rk}(A) = |S|$ are called the basic sets and the rank of the S-ring $A$, respectively. Any union of basic sets is called an $A$-subset of $D$ or $A$-set. The set of all of them is closed with respect to taking inverse and product. Given an $A$-set $X$, we denote by $A_X$ the submodule of $A$ spanned by the elements $Y$ where $Y$ belongs to the set

$$S(A)_X = \{Y \in S(A) : Y \subseteq X\}.$$

Any subgroup of $D$ that is an $A$-set, is called an $A$-subgroup of $D$ or $A$-group. With each $A$-set $X$, one can naturally associate two $A$-groups, namely $(X)$ and $\text{rad}(X)$ (see Notation). The following useful lemma was proved in [8] p.21.

**Lemma 2.1.** Let $A$ be an S-ring over a group $D$ and $H \leq D$ an $A$-group. Then given $X \in S(A)$, the cardinality of the set $X \cap xH$ does not depend on $x \in X$.

A section $S = U/L$ of the group $D$ is called an $A$-section, if both $U$ and $L$ are $A$-groups. In this case, the module

$$A_S = \text{Span}\{\pi_S(X) : X \in S(A)_U\}$$

is an S-ring over the group $S$, the basic sets of which are exactly the sets $\pi_S(X)$ from the right-hand side of the formula.

The S-ring $A$ is called primitive if the only $A$-groups are $e$ and $D$, otherwise this ring is called imprimitive. One can see that if $H$ is a minimal $A$-group, then the

\[\text{ord}(H) = \text{ord}(D/H)\]
S-ring $A_H$ is primitive. The classical results on primitive S-rings over abelian and dihedral groups were obtained in papers [28, 16, 29]. A careful analysis of the proofs shows that the schurity assumption there was superfluous. Therefore, in the first part of the following statement, we formulate the corresponding results in slightly more general form.

**Theorem 2.2.** Let $D$ be a 2-group which is cyclic, dihedral, or isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2^n$. Then any primitive S-ring over $D$ is of rank 2. In particular, if $A$ is an S-ring over $D$ and $H \leq D$ is a minimal $A$-group, then $H^\#$ is a basic set of $A$.

Let $S = U/L$ be an $A$-section of the group $D$. The S-ring $A$ is called the *generalized S-wreath product* if the group $L$ is normal in $D$ and $L \leq \text{rad}(X)$ for all basic sets $X$ outside $U$; in this case we write

$$A = A_U \wr_S A_{D/L},$$

and omit $S$ if $U = L$. When the explicit indication of $S$ is not important, we use the term *generalized wreath product*. The generalized S-wreath product is proper if $L \neq e$ and $U \neq D$. When $U = L$, the generalized S-wreath product coincides with the ordinary wreath product.

Let $D = D_1 \times D_2$, where $D_1$ and $D_2$ are trivially intersecting subgroups of $D$. If $A_1$ and $A_2$ are S-rings over the groups $D_1$ and $D_2$ respectively, then the module

$$A = \text{Span}\{X_1 \cdot X_2 : X_1 \in S(A_1), X_2 \in S(A_2)\}$$

is an S-ring over the group $D$ whenever $A_1$ and $A_2$ are commute with each other. In this case, $A$ is called the *dot product* of $A_1$ and $A_2$, and denoted by $A_1 \cdot A_2$ [19]. When $D = D_1 \times D_2$, the dot product coincides with the *tensor product* $A_1 \otimes A_2$.

The following statement was proved in [11].

**Lemma 2.3.** Let $A$ be an S-ring over an abelian group $D = D_1 \times D_2$. Suppose that $D_1$ and $D_2$ are $A$-groups. Then $A = A_{D_1} \otimes A_{D_2}$ whenever $A_{D_1} = \mathbb{Z}D_1$ or $A_{D_2} = \mathbb{Z}D_2$.

The following two important theorems go back to Schur and Wielandt (see [30, Ch. IV]). The first of them is known as the Schur theorem on multipliers, see [8].

**Theorem 2.4.** Let $A$ be an S-ring over an abelian group $D$. Then given an integer $m$ coprime to $|D|$, the mapping $X \mapsto X^{(m)}$, $X \in S(A)$, where

$$X^{(m)} = \{x^m : x \in X\},$$

is a bijection. Moreover, $x \mapsto x^m$, $x \in D$, is a Cayley automorphism of $A$.

Given a subset $X$ of an abelian group $D$, denote by $\text{tr}(X)$ the trace of $X$, i.e. the union of all $X^{(m)}$ over the integers $m$ coprime to $|D|$. We say that $X$ is rational if $X = \text{tr}(X)$. When $\text{tr}(X) = \text{tr}(Y)$ for some $Y \subseteq D$, the sets $X$ and $Y$ are called *rationally conjugate*. For an S-ring $A$ over $D$, the module

$$\text{tr}(A) = \text{Span}\{\text{tr}(X) : X \in S(A)\}$$

is also an S-ring; it is called the *rational closure* of $A$. Finally, the S-ring is *rational* if it coincides with its rational closure, or equivalently, if each of its basic sets is rational.

---

3In [19], the term *wedge product* was used.
In general, Theorem 2.4 is not true when \( m \) is not coprime to the order of \( D \). However, the following weaker statement holds.

**Theorem 2.5.** Let \( A \) be an S-ring over an abelian group \( D \). Then given a prime divisor \( p \) of \(|D|\), the mapping \( X \mapsto X[p] \), \( X \in 2^D \), where

\[
X[p] = \{x^p : x \in X, |X \cap Hx| \neq 0 \text{ (mod } p)\}
\]

with \( H = \{g \in D : g^p = 1\} \), takes an \( A \)-set to an \( A \)-set.

We complete the section by the theorem on separating subgroup that was proved in [6].

**Theorem 2.6.** Let \( A \) be an S-ring over a group \( D \). Suppose that \( X \in S(A) \) and \( H \leq D \) are such that

\[
X \cap H \neq \emptyset \quad \text{and} \quad X \setminus H \neq \emptyset \quad \text{and} \quad (X \cap H) \leq \text{rad}(X \setminus H).
\]

Then \( X = \langle X \rangle \setminus \text{rad}(X) \) and \( \text{rad}(X) \leq H \leq \langle X \rangle \).

## 3. S-rings and Cayley schemes

In this section, we freely use the language of association scheme theory; in our exposition, we follow [7, 21].

### 3.1. The 1-1 correspondence.

For a group \( D \), denote by \( R(D) \) the set of all binary relations on \( D \) that are invariant with respect to the group \( D \)-right (consisting of the permutations of the set \( D \) induced by the right multiplications in the group \( D \)). Then the mapping

\[
2^D \to R(D), \quad X \mapsto R_D(X)
\]

where \( R_D(X) = \{(g, xg) : g \in D, x \in X\} \), is a bijection. If \( A \) is an S-ring over the group \( D \), then the pair

\[
\mathcal{X} = (D, S),
\]

where \( S = R_D(S(A)) \), is an association scheme. Moreover, it is a Cayley scheme over \( D \), i.e. \( D_{\text{right}} \leq \text{Aut}(\mathcal{X}) \). Each basis relation \( s \in S \) of this scheme, is a Cayley digraph over \( D \) the connection set of which is equal to \( es = \{g \in D : (e, g) \in s\} \). Conversely, given a Cayley scheme \( \mathcal{X} \) the module

\[
\mathcal{A} = \text{Span}\{es : s \in S\}
\]

is an S-ring over \( D \).

**Theorem 3.1.** [15] The mappings \( A \mapsto \mathcal{X}, \mathcal{X} \mapsto A \) form a 1-1 correspondence between the S-rings and Cayley schemes over the group \( D \).

It should be mentioned that the above correspondence preserves the inclusion. Moreover, the mapping \( [X] \mapsto [X] \) induces a ring isomorphism from \( A \) onto the adjacency algebra of the Cayley scheme \( \mathcal{X} \) associated with \( A \). It follows that \( c_{XY}^Z = c_{rs}^t \), for all \( X, Y, Z \in S(A) \), where \( r = R_D(X) \), \( s = R_D(Y) \) and \( t = R_D(Z) \). In particular, the number \(|X|\) is equal to the valency \( n_r \) of the relation \( r \), and the S-ring \( A \) is commutative if and only if so is the Cayley scheme \( \mathcal{X} \).
3.2. Isomorphisms and schurity. We say that S-rings $\mathcal{A}$ and $\mathcal{A}'$ are (combinatorial) isomorphic if the Cayley schemes associated with $\mathcal{A}$ and $\mathcal{A}'$ are isomorphic. Any isomorphism between these schemes is called the isomorphism of $\mathcal{A}$ and $\mathcal{A}'$. The group $\text{Iso}(\mathcal{A})$ of all isomorphisms from $\mathcal{A}$ to itself has a normal subgroup

$$\text{Aut}(\mathcal{A}) = \{ f \in \text{Iso}(\mathcal{A}) : R_D(X)^f = R_D(X) \text{ for all } X \in S(\mathcal{A}) \};$$

any such $f$ is called a (combinatorial) automorphism of the S-ring $\mathcal{A}$. In particular, if $\mathcal{A} = \mathbb{Z}D$ (resp. $\text{rk}(\mathcal{A}) = 2$), then $\text{Aut}(\mathcal{A}) = D_{\text{right}}$ (resp. $\text{Aut}(\mathcal{A}) = \text{Sym}(D)$).

The S-ring $\mathcal{A}$ is called schurian (resp. normal) if so is the Cayley scheme associated with $\mathcal{A}$. Thus, $\mathcal{A}$ is schurian if and only if $S(\mathcal{A}) = \text{Orb}(\text{Aut}(\mathcal{A})_e, D)$, and normal if and only if $D_{\text{right}} \trianglelefteq \text{Aut}(\mathcal{A})$.

From our definitions, it follows that $\mathcal{A} = \mathcal{A}_1 \cdot \mathcal{A}_2$ if and only if $\mathcal{X} = \mathcal{X}_1 \cdot \mathcal{X}_2$ where $\mathcal{X}, \mathcal{X}_1$ and $\mathcal{X}_2$ are the Cayley schemes associated with the S-rings $\mathcal{A}, \mathcal{A}_1$ and $\mathcal{A}_2$ respectively. Similarly, $\mathcal{A} = \mathcal{A}_1 \cdot \mathcal{A}_2$ if and only if $\mathcal{X} = \mathcal{X}_1 \circ \mathcal{X}_2$. On the other hand, the tensor and wreath product of association schemes (and permutation groups) are special cases of the crested product introduced and studied in [1]. Thus, Theorem 3.2 below immediately follows from Remark 23 of that paper and Theorems 21 and 22 proved there.

**Theorem 3.2.** Let $\mathcal{A} = \mathcal{A}_1 * \mathcal{A}_2$, where $* \in \{ \cdot, \circ \}$. Then $\mathcal{A}$ is schurian if and only if so are $\mathcal{A}_1$ and $\mathcal{A}_2$. Moreover,

$$\text{Aut}(\mathcal{A}_1 \cdot \mathcal{A}_2) = \text{Aut}(\mathcal{A}_1) \cdot \text{Aut}(\mathcal{A}_2) \quad \text{and} \quad \text{Aut}(\mathcal{A}_1 \cdot \mathcal{A}_2) = \text{Aut}(\mathcal{A}_1) \times \text{Aut}(\mathcal{A}_2).$$

The following simple statement is an obvious consequence of the definition of wreath product and Theorem 3.2.

**Corollary 3.3.** Let $\mathcal{A}$ be an S-ring over a group $D$ and $H$ an $\mathcal{A}$-group such that $\text{rk}(\mathcal{A}) = \text{rk}(\mathcal{A}_H) + 1$. Then $\mathcal{A}$ is isomorphic to the wreath product of $\mathcal{A}_H$ by an S-ring of rank 2 over the group $\mathbb{Z}[D/H]$. Moreover, $\mathcal{A}$ is schurian if and only if so is $\mathcal{A}_H$.

3.3. Quasi-thin S-rings. An S-ring $\mathcal{A}$ is called quasi-thin if any of its basic sets consists of at most two elements. Thus, $\mathcal{A}$ is quasi-thin if and only if the Cayley scheme associated with $\mathcal{A}$ is quasi-thin (the latter means that the valency of any its basic relation is at most 2).

**Lemma 3.4.** Let $\mathcal{A}$ be an S-ring over an abelian group $D$. Suppose that $X \in S(\mathcal{A})$ is such that $|X| = 2$ and $\langle X \rangle = D$. Then $\mathcal{A}$ is quasi-thin.

**Proof.** The Cayley scheme $\mathcal{X}$ associated with $\mathcal{A}$ is commutative, because the group $D$ is abelian. Moreover, the relation $r = R_D(X)$ corresponding to the set $X$, is of valency $|X| = 2$. Thus, the equality $\langle X \rangle = D$ implies that $\mathcal{X}$ is a 2-cyclic scheme generated by the tightly attached relation $r$ in the sense of [12]. So, by Proposition 3.11 of that paper, $\mathcal{X}$ is a quasi-thin scheme. Therefore, the S-ring $\mathcal{A}$ is also quasi-thin.

Following the theory of quasi-thin schemes in [22], we say that a basic set $X \neq \{e\}$ of a quasi-thin S-ring $\mathcal{A}$ is an orthogonal if $X \subseteq Y Y^{-1}$ for some $Y \in S(\mathcal{A})$.

**Lemma 3.5.** Any commutative quasi-thin S-ring $\mathcal{A}$ is schurian. Moreover, if it has at least two orthogonals, then the group $\text{Aut}(\mathcal{A})_e$ has a faithful regular orbit.
Proof. The first statement immediately follows from [22, Theorem 1.2]. To prove the second one, denote by $X$ the Cayley scheme associated with the S-ring $\mathcal{A}$. Then from [22, Corollary 6.4] it follows that the group $\text{Aut}(X)_e$ is trivial for some $x \in D$. This means that $x^{\text{Aut}(X)_e}$ is a faithful regular orbit of the group $\text{Aut}(\mathcal{A})_e$. $lacksquare$

4. S-rings over cyclic and dihedral groups

4.1. Cyclic groups. Let $C$ be a cyclic group of order $2^n$, $n \geq 1$. Then the group $\text{Aut}(C)$ consists of permutations $\sigma_m : x \mapsto x^m$, $x \in C$, where $m$ is an odd integer. In what follows, $c_1$ denotes the unique involution in $C$.

Lemma 4.1. Let $X \in \text{Orb}(K, C)$, where $K \subseteq \text{Aut}(C)$. Then

1. $\text{rad}(X) = e$ if and only if $X$ is a singleton, or $n \geq 3$ and $X = \{x, \varepsilon x^{-1}\}$ where $x \in X$ and $\varepsilon \in \{e, c_1\}$,
2. if $K \supseteq \{\sigma_m : m = 1 \pmod{2^{n-k}}\}$, then $2^k$ divides $|\text{rad}(X)|$.

Proof. Statement (1) follows from [5, Lemma 5.1], whereas statement (2) is straightforward. $lacksquare$

Let $\mathcal{A}$ be an S-ring over the group $C$. By the Schur theorem on multipliers, the group $\text{rad}(X)$ does not depend on a set $X \in \mathcal{S}(\mathcal{A})$ that contains a generator of $C$. This group is called the radical of $\mathcal{A}$ and denoted by $\text{rad}(\mathcal{A})$. Since $C$ is a 2-group, from [5, Lemma 6.4] it follows that if $\text{rad}(\mathcal{A}) = e$, then either $n \geq 2$ and $\text{rk}(\mathcal{A}) = 2$, or $\mathcal{A} = \text{Cyc}(K, C)$, where $K \subseteq \text{Aut}(C)$ is the group generated by the automorphism taking a generator $x$ of $C$ to an element in $\{x, x^{-1}, c_1x^{-1}\}$ (see also statement (1) of Lemma 4.1). In any case, $\mathcal{A}$ is, obviously, schurian. In fact, the latter statement holds for any S-ring over a cyclic p-group [10].

For any basic set $X$ of the S-ring $\mathcal{A}$, one can form an $\mathcal{A}$-section $S = \langle X \rangle / \text{rad}(X)$. Then the radical of the S-ring $\mathcal{A}_S$ is trivial. Since in our case, $|S|$ is a 2-group, the result in previous paragraph shows that either the S-ring $\mathcal{A}_S$ is cyclotomic or $|S|$ is a composite number and $\text{rk}(\mathcal{A}_S) = 2$. In the former case, $X$ is an orbit of an automorphism group of $C$, whereas in the latter case, $X = \langle X \rangle / \text{rad}(X)$. Thus, any basic set of $\mathcal{A}$ is either regular or equals the set difference of two distinct $\mathcal{A}$-groups.

Lemma 4.2. Let $\mathcal{A}$ be a cyclotomic S-ring over a cyclic 2-group. Suppose that $\text{rad}(\mathcal{A}) = e$. Then $\text{rad}(\mathcal{A}_S) = e$ for any $\mathcal{A}$-section $S$ such that $|S| \neq 4$.

Proof. Follows from [10, Theorem 7.3]. $lacksquare$

The following auxiliary lemma will be used in Section 9.

Lemma 4.3. Let $C$ be a cyclic 2-group, and let $X$ and $Y$ be orbits of some subgroups of $\text{Aut}(C)$. Suppose that $\langle X \rangle \neq \langle Y \rangle$ and $\text{rad}(X) = \text{rad}(Y) = e$. Then the product $XY$ contains no coset of $\langle c_1 \rangle$.

Proof. Without loss of generality, we can assume that $\langle Y \rangle$ is a proper subgroup of $\langle X \rangle$. Then from statement (1) of Lemma 4.1 it follows that $X = \{x\}$ or $\{x, \varepsilon x^{-1}\}$, and $Y = \{y\}$ or $\{y, \varepsilon y^{-1}\}$ where $|x| > |y|$. Therefore, the required statement trivially holds whenever $X$ or $Y$ is a singleton. Thus, we can assume that $|X| = |Y| = 2$, and hence $|x| > |y| \geq 8$. Furthermore,

$$XY = \{xy, \varepsilon xy^{-1}, \varepsilon x^{-1} y, \varepsilon'' x^{-1} y^{-1}\},$$
where $e'' = e' e'$. Suppose on the contrary, that this product contains a coset of $\langle c_1 \rangle$. Then, obviously, $c_1 x y = e' x y^{-1}$ or $c_1 x y^{-1} y = e'' x y^{-1}$. In any case, $y^2 \in \{ e, c_1 \}$ and hence $|y| \leq 4$. Contradiction. 

4.2. Dihedral groups. Throughout this subsection, $D$ is a dihedral group and $C$ is the cyclic subgroup of $D$ such that all the elements in $D \setminus C$ are involutions. A set $X \subseteq D$ is called mixed if the sets $X_0 = X \cap C$ and $X \setminus X_0$ are not empty. For an element $s \in D \setminus C$, we denote by $X_1 = X_{1,s}$ the subset of $C$ for which $X = X_0 \cup X_1 s$.

The following statement (in the other notation) was proved in [29].

Lemma 4.4. Let $A$ be an $S$-ring over the dihedral group $D$ and $X$ a mixed basic set of $A$. Then

1. the sets $X_0$, $X_1 s$ and $X$ are symmetric, and $X_0$ commutes with $X_1 s$,
2. given an integer $m$ coprime to $|D|$, there exists a unique $Y \in S(A)$ such that $(X_0)^{(m)} = Y_0$.

When it does not lead to confusion, the set $Y$ from statement (2) of Lemma 4.3 will be also denoted by $X^{(m)}$; for $X \subseteq C$, this notation is consistent with [3]. For any $A$-set $X$ such that $X_0 \neq \emptyset$, one can define its trace $\text{tr}(X)$ to be the union of sets $X^{(m)}$, where $m$ runs over all integers coprime to $|D|$. The following statement was also proved in [29].

Lemma 4.5. Let $A$ be an $S$-ring over the dihedral group $D$. Suppose that $X_0 \neq \emptyset$ for all $X \in S(A)$. Then given an integer $m$ coprime to $|D|$, the mapping $X \mapsto X^{(m)}$ induces an algebraic isomorphism of $A$; in particular, $|X^{(m)}| = |X|$.

The algebraic fusion of the $S$-ring $A$ from Lemma 4.5 with respect to the group of all algebraic isomorphisms defined in this lemma, is an $S$-ring any basic set of which is of the form $\text{tr}(X)$ where $X \in S(A)$. This $S$-ring is called the rational closure of $A$ and denoted by $\text{tr}(A)$. It should be stressed that this notation has sense only if the hypothesis of Lemma 4.5 is satisfied.

5. S-rings over $D = \mathbb{Z}_2 \times \mathbb{Z}_2^*$: basic sets containing involutions

In what follows, $C \subseteq D$ is a cyclic group of order $2^n$ and $E$ is the Klein subgroup of $D$. The non-identity elements of this subgroup are the involution $c_1 \in C$ and the other two involutions $s \in D \setminus C$ and $c_1 s$. For an $S$-ring over $D$ and an element $t \in E$, we denote by $X_t$ the basic set that contains $t$. Then by the Schur theorem on multipliers (Theorem 2.4), this set is rational. In this section we completely describe the sets $X_t$’s.

Theorem 5.1. Let $A$ be an $S$-ring over the group $D$. Then the set $H = \bigcup_{t \in E} X_t$ is an $A$-group and for a suitable choice of $s$ one of the following statements holds with $U = \langle X_{c_1} \rangle$:

1. $X_{c_1} = X_s = X_{sc_1} = U \setminus e$,
2. $X_{c_1} = U \setminus e$ and $X_s = X_{sc_1} = H \setminus U$,
3. $X_{c_1} = X_{sc_1} = U \setminus \langle s \rangle$ and $X_s = \{ s \}$,
4. $X_{c_1} = U \setminus e$, $X_s = \{ s \}$ and $X_{sc_1} = s X_{c_1}$.

The proof of Theorem 5.1 will be given later. The following auxiliary statement is, in fact, a consequence of the Schur theorem on multipliers. Below, we fix an $S$-ring $A$ over the group $D$. 

Lemma 5.2. Suppose that $X \in S(A)$ contains two elements $x$ and $y$ such that $|x| > |y| \geq 2$. Then $x\{e, c_1\} \subseteq X$.

Proof. Set $m = 1 + |x|/2$. Then by Schur’s theorem on multipliers, $Y := X^{(m)}$ is a basic set of $A$. On the other hand, since $|x| > |y|$, we have $y^m = y$. Thus, $y^m \in X$. This implies that $X = Y$, and hence $x^m \in X$. Since $|x| > 2$ and $x^m = xc_1$, we conclude that $x\{e, c_1\} \subseteq X$ as required.

In the following lemma, we keep the notation of Theorem 5.1.

Lemma 5.3. Either $X_{c_1} = U \setminus e$, or $H$ is an $A$-group and statement (3) of Theorem 5.1 holds.

Proof. The statement is trivial if the set $X := X_{c_1}$ is contained in $E$. So, we can assume that $X$ contains at least one element of order greater than two. Then $x\{e, c_1\} \subseteq X$ for each $x \in X$ with $|x| > 2$ (Lemma 5.2). Thus, $c_1 \in \text{rad}(X \setminus E)$.

We observe that $X \cap E$ is equal to one of the following sets:

$$
\{c_1\} \text{ or } \{c_1, s, sc_1\} \text{ or } \{c_1, t\},
$$

where $t \in \{s, sc_1\}$. In the first two cases, $c_1 \in \text{rad}(X \setminus \{c_1\})$. So by Theorem 2.6 with $H = \langle c_1 \rangle$, we conclude that $X = \langle X \setminus \text{rad}(X) \rangle$ and $c_1 \notin \text{rad}(X)$. However, the only non-trivial subgroups of $D$ not containing $c_1$, are $\langle s \rangle$ and $\langle sc_1 \rangle$. Since none of them equals $\text{rad}(X)$, we conclude that $\text{rad}(X) = e$ and $X = U \setminus e$.

In the remaining case, $X \cap E = \{c_1, t\}$, and hence $|c_1 X \cap X| = |X| - 2$. Since $c_1 \in X$, this implies that the latter number equals $c_{X/X}^{X}$ (see Section 2). Therefore, $|x^{-1}X \cap X| = |X| - 2$ for each $x \in X$. On the other hand, the set $\{c_1, t\}t = \{c_1t, e\}$ does not intersect $X$. Thus, $t(X \setminus E) = X \setminus E$, and hence

$$
\text{rad}(X \setminus E) = E.
$$

By Theorem 2.6 with $H = E$, we conclude that $X = \langle X \setminus \text{rad}(X) \rangle$ and $E \setminus \text{rad}(X)$ is contained in $X$. Therefore, $\text{rad}(X) = \langle t' \rangle$, where $t'$ is the element of $\{s, sc_1\}$ other than $t$. Thus, $X = U \setminus \langle t' \rangle$, $H = U$ is an $A$-group and we are done.

Proof of Theorem 5.1 By Lemma 5.3 we can assume that $X := X_{c_1} = U \setminus e$. If, in addition, $X$ contains $s$ or $sc_1$, then $H = U$ is an $A$-group and statement (1) of the theorem holds. Thus, we can also assume that $X \neq X_t$ for each $t \in \{s, sc_1\}$. Suppose first that $X_s = X_{sc_1}$: denote this set by $Y$. Then $Y \cap E = \{s, sc_1\}$, and hence $c_1 \in \text{rad}(Y)$ (Lemma 5.2). Since $X = U \setminus e$, this implies that $U \leq \text{rad}(Y)$. Thus, $H = \langle Y \rangle$ is an $A$-group, $X_s = X_{sc_1} = Y = H \setminus U$ and statement (2) holds.

Let now $X_s \neq X_{sc_1}$ and $t \in \{s, sc_1\}$. Then $Y \cap E = \{t\}$ where $Y = X_t$. It follows that $|c_1 Y \cap Y| = |Y| - 1$, and hence

$$
Y^2 = |Y|e + (|Y| - 1)X + \cdots,
$$

where the omitted terms in the right-hand side contain neither $e$ nor elements of $X$ with non-zero coefficients. However, $|X|c_{Y}^{X} = |Y|c_{Y}^{X}$ because $X = X^{-1}$ and $Y = Y^{-1}$. Since $c_{Y}^{X} = |Y| - 1$, this implies that $|X|$ is divided by $|Y|$. If, in addition, $|Y| = 1$, then we have $\{X_s, X_{sc_1}\} = \{\{t\}, tX_{c_1}\}$ and $H = U \cup tU$ is an $A$-group. So statement (4) holds. If $|Y| \neq 1$, equality (7) implies that $|Y| = |X| = |U| - 1$ and $Y^2 = |Y|e + (|Y| - 1)X$. It follows that $c_{Y}^{X} = |X| - 1$. Therefore,

$$
|tU \cap Y| = |X| - 1 = |U| - 2.
$$
This is true for \( t = c_1 \) and \( t = sc_1 \). On the other hand, \( sU = sc_1U \) and the sets \( X_s \) and \( X_{sc_1} \) are disjoint. Thus,
\[
|U| = |tU| \geq |sU \cap X_s| + |sc_1U \cap X_{sc_1}| = 2(|U| - 2).
\]
It follows that \( |U| = 2 \) or \( |U| = 4 \). In the former case, \( H = E \) and statement (4) trivially holds. In the latter one, \( |X| = |X_s| = 3 \) and \( |sU \cap Y| = 2 \). Therefore, there exists a unique \( x \in X_s \) outside \( sU \). It follows that \( |xU \cap X_s| = 1 \) which is impossible by Lemma 2.1.

6. S-rings over \( D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n} \): Non-regular case

A set \( X \subseteq D \) is said to be highest (in \( D \)) if it contains an element of order \( 2^n \). Given an S-ring \( \mathcal{A} \) over \( D \), denote by \( \text{rad}(\mathcal{A}) \) the group generated by the groups \( \text{rad}(X) \), where \( X \) runs over the highest basic sets of \( \mathcal{A} \). Clearly, \( \text{rad}(\mathcal{A}) \) is an \( \mathcal{A} \)-group, and it is equal to \( e \) if and only if each highest basic set of \( \mathcal{A} \) has trivial radical. In what follows, we say that \( \mathcal{A} \) is regular, if each highest basic set of \( \mathcal{A} \) is regular. Now, the main result of this section can be formulated as follows.

**Theorem 6.1.** Let \( \mathcal{A} \) be an S-ring over the group \( D \). Suppose that \( \text{rad}(\mathcal{A}) = e \). Then \( \mathcal{A} \) is either regular or rational. Moreover, in the latter case, \( \mathcal{A} = \mathcal{A}_H \otimes \mathcal{A}_L \), where \( \text{rk}(\mathcal{A}_H) = 2 \) and \( |L| \leq 2 \leq |H| \); in particular, \( \mathcal{A} \) is schurian.

The proof of Theorem 6.1 will be given in the end of the section. The key point of the proof is the following statement.

**Theorem 6.2.** Let \( \mathcal{A} \) be an S-ring over the group \( D \). Then any non-regular basic set of \( \mathcal{A} \) either intersects \( E \), or has a non-trivial radical.

**Proof.** Let \( X \) be a non-regular basic set of \( \mathcal{A} \) that does not intersect \( E \). Then the minimal order of an element in \( X \) equals \( 2^m \) for some \( m \geq 2 \). Denote by \( X_m \) the set of all elements in \( X \) of order \( 2^m \). Clearly, each of the sets \( X \setminus X_m \) and \( X_m \) is non-empty. Suppose, towards a contradiction, that \( \text{rad}(X) = e \). Then \( c_1 \notin \text{rad}(X) \), and \( c_1 \in \text{rad}(X \setminus X_m) \) (Lemma 5.2). It follows that
\[
(8) \quad c_1 \notin \mathcal{A},
\]
because otherwise \( c_1X \) is a basic set other than \( X \) that intersects \( X \).

Denote by \( K \) the setwise stabilizer of \( X \) in the group \( G \cong \mathbb{Z}_{2^n}^* \) of all permutations \( x \mapsto x^m \), \( x \in D \), where \( m \) is an odd integer. Then by Schur’s theorem on multipliers, \( X_m \) is the union of at most two \( K \)-orbits (one inside \( C \) and the other outside). The radicals of these orbits must be trivial, because \( \text{rad}(X) = e \) and \( c_1 \in \text{rad}(X \setminus X_m) \). Thus, by statement (1) of Lemma 4.1, we have
\[
(9) \quad X_m = \{x\} \text{ or } \{x, x^{-1} \varepsilon\} \text{ or } \{x, y\} \text{ or } \{x, x^{-1} \varepsilon, y, y^{-1} \varepsilon s\},
\]
where \( x, y \in X_m \) are such that \( \{x\} = \{y\} \), and \( \varepsilon \in \{e, c_1\} \). It should be mentioned that \( x \neq \varepsilon y \), for otherwise \( \varepsilon s \in \text{rad}(X) \).

Let us define \( \mathcal{A} \)-groups \( U \) and \( H \) as in Theorem 5.1. Then \( X \subseteq D \setminus H \), because \( X \) does not intersect \( E \). By the definition of \( H \), this implies that it does not contain elements of order \( 2^m \). Since \( U \leq H \), we conclude that \( xU \cap X \subseteq X_m \) for each \( x \in X_m \). Therefore, \( X_m \) is a disjoint union of some sets \( xU \cap X \) with such \( x \). However, by Lemma 2.1 the number \( \lambda := |xU \cap X| \) doesn’t depend on a choice of
Thus, \( \lambda \) divides \(|X_m|\). By (9) this implies that \( \lambda \in \{1, 2, 4\} \). Moreover, setting \( Y \) to be the basic set containing \( c_1 \), we have

\[
(10) \quad c_{XY}^X = \lambda - 1,
\]

because \( U = Y \setminus e \) or \( U = Y \setminus (\varepsilon s) \), and \( x \neq \varepsilon y \).

Denote by \( \alpha \) the number of \( z \in X_m \) for which \( c_1 z \notin X_m \). If \( \alpha = 1 \), then from Theorem 2.5 it follows that \( S(A) \) contains \( X^{[2]} = \{z^2\} \) for an appropriate \( z \in X_m \). Since \( z \notin E \), this implies that \( c_1 \in A \) in contrast to (8). Thus, \( \alpha \neq 1 \). Therefore, \( \alpha \) is an even number less or equal than \(|X_m| \leq 4 \) (see (9)). Moreover, it is not zero, because otherwise \( c_1 \in \text{rad}(X) \). Besides, from (10) it follows that

\[
(11) \quad |X|(\lambda - 1) = |X|c_{XY}^X = |Y|c_{XY}^Y = |Y| \quad |c_1 X \cap X| = |Y| (|X| - \alpha).
\]

Since \(|X| > |X_m| \geq \alpha \), this implies that the right-hand side of the equality is not zero. Thus, \( \lambda \neq 1 \), and finally

\[
(12) \quad \lambda, \alpha \in \{2, 4\}.
\]

**Lemma 6.3.** In the above notation \(|X| \geq 2|X_m|\), and the equality holds only if

1. \( X_m \) is a union of two \( K \)-orbits and \( X \setminus X_m \) is a \( K \)-orbit,
2. any element in \( X \setminus X_m \) is of order \( 2^{m+1} \).

**Proof.** By the Schur theorem on multipliers, the stabilizers of an element \( x \in X \) in the groups \( K \) and \( G \), coincide. However, the stabilizer in \( G \) consists of raising to power \( 1+i|x| \), where \( i = 0, 1, \ldots, 2^n/|x| - 1 \). Therefore, \(|K_x| = 2^n/|x| \). For \( x \in X_m \) and \( y \in X \setminus X_m \), this implies that \(|K_x| \geq 2|K_y|\), and hence

\[
|x^K| = \frac{|G|}{|K_x|} \leq \frac{|G|}{2|K_y|} = \frac{|y^K|}{2}.
\]

Taking into account that \( X_m \) is a disjoint union of at most two \( K \)-orbits, we obtain that

\[
|X| - |X_m| \geq |y^K| \geq 2|x^K| \geq |X_m|
\]

as required. Since the equality holds only if the second and third inequalities in the above formula are equalities, we are done.

We observe that \(|Y| \neq \lambda - 1\): indeed, for \( \lambda = 2 \), this follows from (5) whereas for \( \lambda = 4 \), the assumption \(|Y| = \lambda - 1 \) implies by (11) an impossible equality \(|X| = |X| - \alpha \). Thus, by (11) and Lemma 6.3 we have

\[
\frac{\alpha |Y|}{|Y| - (\lambda - 1)} = |X| \geq 2|X_m| \geq 2\alpha.
\]

Furthermore, if \( \lambda = 2 \), then \(|Y| = 2 \) and \(|X| = 2\alpha \). On the other hand, if \( \lambda = 4 \), then \( \lambda - 1 < |Y| \leq 6 \) and \(|Y| \in \{2^a - 1, 2^a - 2\} \) for some \( a \) (Theorem 5.1); but then \(|Y| = 6 \) and \(|T| = 2\alpha \). Thus, by (12) there are exactly four possibilities:

1. \( \alpha = 2, \lambda = 2, |Y| = 2, |X| = 4, |X_m| = 2, \)
2. \( \alpha = 4, \lambda = 2, |Y| = 2, |X| = 8, |X_m| = 4, \)
3. \( \alpha = 2, \lambda = 4, |Y| = 6, |X| = 4, |X_m| = 2, \)
4. \( \alpha = 4, \lambda = 4, |Y| = 6, |X| = 8, |X_m| = 4. \)
In all cases, \(|X| = 2|X_m|\). Therefore, by Lemma 6.3 and (9), we conclude that
\(X_m = \{x, ys\}\) in cases (1) and (3), and \(X_m = \{x, x^{-1}\varepsilon, sy, sy^{-1}\varepsilon\}\) in cases (2) and (4). Moreover, since the number \(|Y|\) is even, \(U \setminus Y\) is a group of order two. Without loss of generality, we assume that it is \(\langle s \rangle\).

Let \(\pi\) be the quotient epimorphism from \(D\) to \(D' = D/U\). Then the group \(D'\) is cyclic, the S-ring \(A' = A_{D'}\) is circulant\(\textsuperscript{4}\) and \(X' = \pi(X)\) is a non-regular basic set of it (the elements in \(X_m = \pi(X_m)\) and in \(X' \setminus X'_m\) have different orders). However, any non-regular basic set of a circulant S-ring over a 2-group is a set difference of two its subgroups (see Subsection 4.1). Therefore, \(X' = \langle X' \rangle \setminus \text{rad}(X')\).

Since \(X' \neq X'_m\), this implies that \(|X'| \geq 3\). On the other hand, \(|X'| = |X|/\lambda\) by the definition of \(\lambda\). Thus, we can exclude cases (1), (3) and (4). In case (2) let \(|\text{rad}(X')| = 2^i\) for some \(i \geq 0\). Then \(4 = |X'| = 2^{i+2} - 2^i = 32^i\). Contradiction.

Any basic set \(X\) of an S-ring \(A\) over \(D\) that intersects the group \(E\), must contain an involution. Therefore, such \(X\) is rational. By Theorem 6.2 this proves the following statement.

**Corollary 6.4.** Let \(X\) be a basic set of an S-ring over \(D\). Suppose that \(\text{rad}(X) = e\). Then \(X\) is either regular or rational.

**Proof of Theorem 6.1** Suppose that \(A\) is not regular. Then there exists a highest set \(X \in S(A)\) that is not regular. Since \(\text{rad}(X) = e\), we conclude by Theorem 6.2 that the set \(X \cap E\) is not empty. Therefore, \(X\) is contained in the \(A\)-group \(H \geq E\) defined in Theorem 5.1. But then \(H = D\), because the set \(X\) is highest. Now, the first statement follows, because the S-ring \(A_H = A\) is, obviously, rational. Moreover, statements (2) and (3) of Theorem 5.1 do not hold, because \(\text{rad}(A_H) = \text{rad}(A) = e\). Thus, the second statement of our theorem is true for \(L = e\) (resp. \(L = \langle s \rangle\)) if statement (1) (resp. statement (4)) of Theorem 5.1 holds.

From the proof of Theorem 6.1 it follows that if one of the highest basic sets of \(A\) is not regular, then all highest basic sets are rational. This implies the following statement.

**Corollary 6.5.** Let \(A\) be an S-ring over the group \(D\). Suppose that \(\text{rad}(A) = e\). Then either every highest basic set of \(A\) is regular, or every highest basic set of \(A\) is rational.

**7. S-rings over \(D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}\): regular case**

Throughout this section, \(C = C_n\) is a cyclic subgroup of \(D = D_n\) that is isomorphic to \(\mathbb{Z}_{2^n}\). We denote by \(c_1, c_2\) and \(s\), respectively, the unique involution in \(C\), one of the two elements of \(C\) of order 4, one of the two involutions in \(D \setminus C\). The main result is given by the following theorem.

**Theorem 7.1.** Let \(A\) be a regular S-ring over the group \(D\). Suppose that \(\text{rad}(A) = e\). Then \(A\) is a cyclotomic S-ring. More precisely, \(A = \text{Cyc}(K, D)\), where \(K \leq \text{Aut}(D)\) is one of the groups listed in Table 7.
### Corollary 7.2
Under the assumptions of Theorem 7.1, let $K = K_i$, where $i = 1, \ldots, 11$. Then the following statements hold:

1. $\langle c_1 \rangle$ is an $A$-group,
2. $C$ is an $A$-group if and only if $i \leq 5$,
3. $\langle \varepsilon s \rangle$ with $\varepsilon \in \{e, c_1\}$, is an $A$-group if and only if $i \in \{1, 2, 3, 8, 9\}$.

In what follows, given a basic set $X \in S(A)$, we denote by $X_0$ and $X_1$ the uniquely determined subsets of $C$ for which $X = X_0 \cup sX_1$.

**Proof of Theorem 7.1**
Let $X$ be a highest basic set of the S-ring $A$. Then it is regular by the theorem hypothesis. By the Schur theorem on multipliers, this implies that if the set $X_a$ is not empty for some $a \in \{0, 1\}$, then $X_a$ is an orbit of the group $\text{Aut}(C)(X_a)$. Therefore, $X_a$ is of the form given in statement (1) of Lemma 4.1. The rest of the proof consists of Lemmas 7.3, 7.6 and 7.10 below: in the first one, $X_0$ or $X_1$ is empty, and in the other two, both $X_0$ and $X_1$ are not empty and $|X_0| = 2$ or 1, respectively.

**Lemma 7.3.** Let $X_0 = \emptyset$ or $X_1 = \emptyset$. Then $A = \text{Cyc}(K_i, D)$ with $i \in \{1, 2, 3, 4, 5\}$.

**Proof.** Without loss of generality, we can assume that $n \geq 3$ and $X_1 = \emptyset$. Then $X = X_0$ generates $C$. Therefore, $C$ is an $A$-group and $X$ is a highest basic set of a circulant S-ring $A_C$. Since $\text{rad}(X) = e$, this implies that $\text{rad}(A_C) = e$. If, in addition, $(s)$ is an $A$-group, then $A = A_C \otimes A_{(s)}$ by Lemma 7.3 and hence $A = \text{Cyc}(K_i, D)$ with $i = 1, 2, 3$. Thus, we can assume that

$$s \notin A.$$ (13)

Let us prove by induction on $n$ that $A = \text{Cyc}(K_i, D)$ with $i = 4$ or 5. For $n = 3$ this statement can be verified by a computer computation. Let $n > 3$. Denote by $X'$ the basic set of $A$ that contains $x' = xs$, where $x \in X$ is a generator of $C$. Then by the theorem hypothesis, $X'$ is a regular set with trivial radical. It follows that $C' = \langle X' \rangle$ is the order $2^n$ cyclic subgroup of $D$ other than $C$. In particular,

$$\text{rad}(A_{C'}) = \text{rad}(X') = e.$$
Besides, since $C^2 = (C')^2$, the S-rings $A_C$ and $A_{C'}$ have the same basic sets inside the group $C^2$; in particular, $|X| = |X'|$. Moreover, these S-rings are not Cayley isomorphic. Indeed, otherwise $X' = sY$, where $Y = X^{(m)}$ for some odd $m$. Then $s$ is the only element that appears in the product $Y^{-1}X'$ with multiplicity $|X|$. However, in this case $s \in A$, contrary to (12). Thus,

$$X = \{x, \varepsilon x^{-1}\} \quad \text{and} \quad X' = \{sx, sc_1 \varepsilon x^{-1}\}.$$ 

(14) Set $i = 4$ or $5$ depending on $\varepsilon = e$ or $c_1$, respectively. Then from (13) and the Schur theorem on multipliers, it follows that the S-rings $A$ and $\text{Cyc}(K_i, D)$ have the same highest basic sets. We also observe that $D_{n-1}$ is an $A$-group.

Since the S-ring $A_C$ is cyclotomic, it follows from (13) that $Y = \{x^2, x^{-2}\}$ is a basic set of $A$. Denote by $Y'$ the basic set containing $sx^2$. Then, obviously,

$$Y' \subseteq X' = \{sx^2, sc_1 x^{-2}, s, sc_1\}.$$ 

However, $|sx^2| \geq 8$, because $n \geq 4$. Thus, $Y' \subseteq \{sx^2, sc_1 x^{-2}\}$: otherwise $Y \cap E$ is not empty and from Theorem 5.1 it follows that $|Y'| > 4$. Therefore, $Y'$ is regular and $\text{rad}(Y') = e$. Since also $\text{rad}(Y) = e$ and $Y, Y'$ are highest basic sets of the S-ring $A_{D_{n-1}}$, the latter satisfies the hypothesis of Lemma 7.3. By the induction, we conclude that $A_{D_{n-1}} = \text{Cyc}(K_4, D_{n-1})$. Thus, $A = \text{Cyc}(K_i, D)$ as required. \hfill \Box

Lemma 7.4. Let $|X_0| = 2$ and $X_1 \neq \emptyset$. Then $A = \text{Cyc}(K_i, D)$ with $i \in \{6, 7\}$.

Proof. By statement (1) of Lemma 2.1 we have $X_0 = \{x, \varepsilon x^{-1}\}$. Since $X$ is regular, this implies that

$$X = \{x, \varepsilon x^{-1}, sy, s \varepsilon y^{-1}\}$$

(15) for some generator $y$ of the group $C$. For $n = 3$, we tested in the computer that no S-ring over $D$ has a highest basic set $X$ such that $X_0 = \{x, \varepsilon x^{-1}\}$ and $X_1 \neq \emptyset$. Suppose that $n \geq 4$. Let us prove that the lemma statement holds for $i = 6$ or $i = 7$ depending on $\varepsilon = e$ or $\varepsilon = c_1$, respectively. For $n = 4$, we tested this statement in the computer. Thus, in what follows, we can assume that $n \geq 5$.

Lemma 7.5. In the above notations, the following statements hold:

1. $C_{n-1}$ is an $A$-group whereas $\langle s \rangle$ and $\langle sc_1 \rangle$ are not,

2. $Y_x = \{x^{\pm 2}, c_1 x^{\pm 2}\}$ and $Z_x = \{sx^{\pm 2}\}$ are $A$-sets,

3. $y = xc_2$ for a suitable choice of $y$ and $c_2$.

Proof. Since $n \geq 5$, we have $x^2 \neq x^{-2}$ and $y^2 \neq y^{-2}$. Besides, since neither $s$ nor $sc_1$ belongs to $\text{rad}(X)$, we have $x^2 \neq y^{\pm 2} \neq x^{-2}$. Thus,

$$|\{x^2, x^{-2}, y^2, y^{-2}\}| = 4.$$ 

(16) However, $X^{[2]} = \{x^2, x^{-2}, y^2, y^{-2}\}$ and $X^{[2]}$ is an $A$-set by Theorem 2.5. Thus, the first part of statement (1) holds, because $C_{n-1} = \langle X^{[2]} \rangle$. To prove the second part of statement (1), suppose on the contrary that $L := \langle \varepsilon \rangle$ is an $A$-group for some $\varepsilon' \in \{e, c_1\}$. Then the circulant S-ring $A_{D/L}$ has a basic set $\pi(X) = \{\pi(x), \pi(\varepsilon x^{-1}), \pi(y), \pi(\varepsilon y^{-1})\}$,

where $\pi : D \to D/L$ is the quotient epimorphism. However, from (16) it easily follows that $|\text{rad}(\pi(X))| \geq 2$. Therefore, one of the quotients $\pi(x)/\pi(\varepsilon x^{-1})$,

\footnote{One can interchange $y$ and $y^{-1}$, and $c_2$ and $c_2^{-1}$.}
\[ \pi(x)/\pi(y) \text{ or } \pi(x)/\pi(\varepsilon y^{-1}) \text{ has order 2.} \] This implies, respectively, that the order of \( \pi(x) \) is 8, \( \pi(x) = \pi(c_1)\pi(y) \), and \( \pi(x) = \pi(c_1)\pi(\varepsilon y^{-1}) \). The former case is impossible, because \( n \geq 5 \), whereas in the other two, we have \( x \in c_1 y L \) and \( x \in c_1 \varepsilon y^{-1} L \) which is impossible due to \[ \text{(16)}. \]

To prove the second part of statement (2), we observe that \( C_{n-1} \cup \text{tr}(X) \) is an \( \mathcal{A} \)-set. But the complement to it in \( D \) coincides with \( sC_{n-1} \). Thus, it is also an \( \mathcal{A} \)-set. Besides,

\[ X^2 \circ sC_{n-1} = 2 sX', \]

where \( X' = \{(xy)^{\pm 1}, \varepsilon(xy^{-1})^{\pm 1}\} \). Therefore, \( sX' \) is an \( \mathcal{A} \)-set. However, it is easily seen that \( |xy| \neq |\varepsilon xy^{-1}| \). Moreover, \( |xy| = 2^{n-1} \) or \( |\varepsilon xy^{-1}| = 2^{n-1} \), because \( x \) and \( y \) are generators of the group \( C \) and \( n \geq 3 \). Thus, the elements \( sxy \) and \( \varepsilon xy^{-1} \) cannot belong to the same basic set of \( \mathcal{A} \). Indeed, otherwise assuming \( |xy| = 2^{n-1} \), we conclude by Lemma \[ \text{(15)} \] that this basic set contains \( sxy c_1 \). Then \( xy c_1 \in X' \), and hence \( xy c_1 \in \{(xy)^{\pm 1}, \varepsilon xy^{-1}\} \). Consequently, \( (xy)^2 = c_1 \) or \( x^2 = c_1 \varepsilon \). In any case, \( n - 1 \leq 2 \). Contradiction. A similar argument leads to a contradiction when \( |\varepsilon xy^{-1}| = 2^{n-1} \). In the same way, one can verify that no two elements, one in \( \{s(xy)^{\pm 1}\} \) and the other one in \( \{s\varepsilon(xy^{-1})^{\pm 1}\} \), cannot belong to the same basic set of \( \mathcal{A} \). Thus, \( sX' \) is a disjoint union of two \( \mathcal{A} \)-sets of the form \( \{sz^{\pm 1}\} \) with \( z \in C \), and one of them consists of elements of order \( 2^{n-1} \). This implies that \( Z_x \) is an \( \mathcal{A} \)-set, as required.

To prove statement (3), suppose on the contrary that \( x^4 \neq y^{\pm 4} \). Then since \( Y := X^{[2]} \), \( Z_x \), and \( Z_y \) are \( \mathcal{A} \)-sets, the S-ring \( \mathcal{A} \) contains the element

\[ (YZ_x) \circ (YZ_y) = 2s(2e + x^{\pm 2}y^{\pm 2}). \]

Since \( n \geq 3 \), this implies that only \( s \) appears in the right-hand side with multiplicity 4. By the Schur-Wielandt principle, this implies that \( s \in \mathcal{A} \). However, this contradicts the second part of statement (1).

To complete the proof, we note that by statement (3), we have \( Y_x = X^{[2]} \). Since \( X^{[2]} \) is an \( \mathcal{A} \)-set, the first part of statement (2) follows. \[ \blacksquare \]

Let us continue the proof of Lemma \[ \text{(72)} \]. Denote by \( \mathcal{A}_i \) the minimal S-ring over \( D \) that contains \( X \) as a basic set; we recall that \( i = 6 \) or \( i = 7 \) depending on \( \varepsilon = e \) or \( \varepsilon = c_1 \). We claim that

\[ \mathcal{A}_i = \text{Cyc}(K_i, D). \]

Indeed, from statements (2) and (3) of Lemma \[ \text{(75)} \] it follows that the sets \( X, Y_x, \) and \( Z_x \) are orbits of the group \( K_i \) (see Table \[ \text{(4)} \] where the generic orbits of the group \( K_i \) contained inside \( C_{n-1} \) and \( sC_{n-1} \) are given). Therefore, by the Schur theorem on multipliers, we have

\[ (\mathcal{A}_i)_{D \setminus D_n} = \text{Cyc}(K_i, D)_{D \setminus D_{n-2}}. \]

Next, \( C' := (Z_x) \) is a cyclic \( \mathcal{A} \)-group of order \( 2^{n-1} \) other than \( C_{n-1} \). Moreover, \( Z_x \) is a highest basic set of the circulant S-ring \( (\mathcal{A}_i)_{C'} \). Therefore, this S-ring has trivial radical. From the results discussed just after Lemma \[ \text{(73)} \] it follows that it is the cyclotomic S-ring \( \text{Cyc}(K', C') \), where \( K' \) is the subgroup of \( \text{Aut}(C') \) that has \( Z_x \) as an orbit. Since \( \text{Orb}(K_i, C') = \text{Orb}(K', C') \), we conclude that

\[ (\mathcal{A}_i)_{C_{n-2}} = \text{Cyc}(K_i, D)_{C_{n-2}}. \]
Let us complete the proof of (18). To do this, taking into account that \( \varepsilon(e + c_1) = e + c_1 \), we find that

\[
Y_x \cdot Z_x = sx^\pm 4(e + c_1) + 2s(e + c_1). \tag{21}
\]

Moreover, since \( n \geq 5 \), the elements \( x^\pm 1, sx^\pm 4 \) appear in the right-hand side with coefficient 1. By the Schur-Wielandt principle, this implies that \( \{s, sc_1\}x^\pm 4 \) and \( \{s, sc_1\} \) are \( A \)-sets. Thus,

\[
(22) \quad (A_i \cdot c_n \setminus c_{n-1}) = \text{Cyc}(K_i, D)_x c_m \setminus c_{m-1} \quad \text{and} \quad (A_i \cdot c_1) = \text{Cyc}(K_i, D)_x c_1,
\]

where \( m = n - 2 \). For all \( m = n - 3, \ldots, 2 \) the first equality is proved in a similar way by the induction on \( m \); the sets \( Y_x \) and \( Z_x \) in equation (21) are replaced by the \( A \)-sets \( \{x^\pm 2^{m+1}\} \) and \( \{e + c_1\}\{x^\pm 2^{m+1}\} \), respectively. Thus, the claim follows from (19), (20) and (22).

Let us continue the proof of Lemma 7.4. Now, since obviously, \( A \geq A_i \), we conclude by (18) that \( A \geq \text{Cyc}(K_i, D) \). To verify the converse inclusion, we have to prove that every \( K_i \)-orbit \( Z' \) belongs to \( S(A) \). Suppose on the contrary that some \( Z' \) properly contains a set \( Z \in S(A) \). Then

\[
Z \subseteq D_{n-1} \setminus D_1. \tag{23}
\]

Indeed, from (15) and statement (3) of Lemma 7.5, it follows that the \( K_i \)-orbits outside \( D_{n-1} \) are the basic sets of \( A \). Besides, the orbits \( \{e\} \) and \( \{c_1\} \) are also basic sets, because \( A \geq \text{Cyc}(K_i, D) \). Finally, the orbit \( \{s, c_1\} \) belongs to \( S(A) \) by the second part of statement (1) of Lemma 7.5.

From (23) and the first part of statement (1) of Lemma 7.5, it follows that the set \( Z \) is regular. So it is an orbit of an automorphism group of \( C \). This implies that \( Z \) has cardinality 1, 2, or 4. The latter case is impossible, because otherwise \( Z = Z' \).

We claim that the first case is also impossible. Indeed, otherwise \( Z = \{z\} \) for some \( z \in D_{n-1} \setminus D_1 \). Then \( zX \) is a highest basic set of \( A \). However, \( (zX)_0 = \{zx, zxx^{-1}\} \). Therefore, \( \varepsilon(zx)^{-1} = zxx^{-1} \), and hence \( z = z^{-1} \). Thus, \( z \in D_1 \). Contradiction.

To complete the proof of Lemma 7.4, let \( |Z| = 2 \). Without loss of generality, we can assume that the order of an element in \( Z \) is minimal possible. Clearly, \( |Z'| = 4 \), and hence

\[
Z' = \{z^\pm 1, c_1z^\pm 1\},
\]

where either \( z = x^2 \), or \( z = sx^m \) with \( m \in \{3, \ldots, n - 3\} \) (see Table 2). Choose \( z \in Z \) so that

\[
Z = \{z, c_1z\} \quad \text{or} \quad Z = \{z, z^{-1}\},
\]
where \(e' \in \{e, c_1\}\). In the first case, the singleton \(Z^2 = \{z^2\}\) is a basic set of \(A\). By the above argument, this implies that \(z^2 \in D_1\). Thus, \(z \in D_2\). Contradiction. In the second case, \(A\) contains the element
\[
(sz + sz^{-1})(z + e'z^{-1}) = sz^2 + se'z^{-2} + s + se'.
\]
Since \(s \notin A\), this implies that \(e' = c_1\). Therefore, \(\{sz^2, se'z^{-2}\}\) cannot be a basic set of \(A\), and hence \(m \neq 3\). But then, the minimality of \(|z|\) implies that \(\{sz^2, se'z^{-2}, s, e'\} \in S(A)\) that is impossible, because \(s + sc_1 \in A\).

**Lemma 7.6.** Let \(|X_0| = 1\) and \(X_1 \neq \emptyset\). Then \(A = \text{Cyc}(K_i, D)\) with \(i \in \{8, 9, 10, 11\}\).

**Proof.** In this case \(X = \{x, ys\}\), where \(\langle y \rangle = C\). It follows that \(X \) generates \(D\). Moreover, \(n \geq 3\), because \(c_1 \notin \text{rad}(X)\). Therefore, there are two orthogonals in the \(S\)-ring \(A\): one of them is in \((X^{-1}X) \cap C, s\), and another one is in \((X^{-1}X) \cap C\).

Thus, \(A\) is quasi-thin by Lemma 5.4 and hence schurian by Lemma 5.6. The latter implies also that the stabilizer \(K\) of the point \(e\) in the group \(\text{Aut}(A)\), has a faithful regular orbit. Therefore, the index of \(D\) in \(\text{Aut}(A)\) is equal to 2. But then \(D \subseteq \text{Aut}(A)\), and hence \(K \subseteq \text{Aut}(D)\). Consequently, \(A = \text{Cyc}(K, D)\) and the group \(K\) is generated by an involution \(\sigma \in \text{Aut}(D)\). This involution interchanges \(x\) and \(ys\). Therefore, the automorphism \(\sigma\) is uniquely determined. We leave the reader to verify that \(\sigma\) is one of automorphisms that are listed in the rows 8, 9, 10, 11 of Table 1.

---

**8. **\(S\)-**rings over \(D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}\): automorphism groups in regular case**

In this section we find the automorphism group of a regular \(S\)-ring over \(D\) with trivial radical. For this purpose, we need the following concept introduced in [14]: a permutation group is called 2-isolated if no other group is 2-equivalent to it. The following statement is the main result of this section; it shows, in particular, that a regular \(S\)-ring over \(D\) with trivial radical is normal.

**Theorem 8.1.** Let \(A\) be a regular \(S\)-ring over the group \(D\). Suppose that \(\text{rad}(A) = e\). Then for any \(A\)-group \(L\) of order at most 2, the group \(\text{Aut}(A_D/L)\) is 2-isolated. In particular, if \(A = \text{Cyc}(K, D)\) for some \(K \subseteq \text{Aut}(D)\), then \(\text{Aut}(A) = DK\).

The proof will be given in the end of the section. The following statement provides a sufficient condition for a permutation group to be 2-isolated.

**Lemma 8.2.** Let \(A\) be an \(S\)-ring and \(G = \text{Aut}(A)\). Suppose that the point stabilizer of \(G\) has a faithful regular orbit. Then the group \(G\) is 2-isolated.

**Proof.** It was proved in [14] Theorem 3.5 that \(G\) is 2-isolated whenever it is 2-closed and a two-point stabilizer of \(G\) is trivial. However, the latter exactly means that a point stabilizer of \(G\) has a faithful regular orbit.

To apply Lemma 8.2 we need the following auxiliary statement giving a sufficient condition providing the existence of a faithful regular orbit of a point stabilizer in the automorphism group of an \(S\)-ring.

**Lemma 8.3.** Let \(A\) be an \(S\)-ring over an abelian group \(H\). Suppose that a set \(X \in S(A)\) satisfies the following conditions:

1. \(\langle \text{tr}(X) \rangle = H\),
(2) \( e^Z_X = 1 \) for each \( Z \in S(A)_{tr(X)} \) and some \( Y \in S(A) \),
(3) \( e_X^Y = 1 \) for each \( Y \in S(A)_{XX^{-1}} \).

Then \( X \) contains a faithful regular orbit of the group \( \text{Aut}(A)_e \).

**Proof.** Denote by \( \mathcal{X} \) the Cayley scheme over \( H \) associated with the S-ring \( A \). Then the relation \( r = R_H(tr(X)) \) is a union of basic relations of \( \mathcal{X} \). Clearly, \( r \) is symmetric, and connected (condition (1)). Moreover, conditions (2) and (3) imply that the coherent configuration \( (\mathcal{X})_{er} \) is semiregular. Thus, by [24, Theorem 3.3] given \( x \in X \), the two-element set \( \{e, x\} \) is a base of the scheme \( \mathcal{X} \), and hence of the group \( \text{Aut}(\mathcal{X}) \). This implies that \( \{x\} \) is a base of the group \( K = \text{Aut}(\mathcal{X})_e \). Thus, \( x^K \subseteq X \) is a faithful regular orbit of \( K \).

**Proof of Theorem 8.1.** From Theorem 7.1, it follows that \( A = \text{Cyc}(K, D) \), where \( K = K_i \) is one of the groups listed in Table 1, \( 1 \leq i \leq 11 \). Therefore, taking into account that the groups \( DK \) and \( \text{Aut}(A) \) are 2-equivalent, we conclude that the second part of the theorem statement immediately follows from the first one. To prove the latter, without loss of generality, we assume that \( i \geq 2 \) and \( n \geq 4 \).

Let \( L \leq D \) be an \( A \)-group. In what follows, we set \( H = D/L \) and \( \pi = \pi_L \). To prove that the group \( \text{Aut}(A_H)_e \) is 2-isolated, it suffices to verify that its point stabilizer has a faithful regular orbit (Lemma 8.2). The remaining part of the proof is divided into three cases.

**Case 1:** \( L = \langle \varepsilon s \rangle \), where \( \varepsilon \in \{e, c_1\} \). Here, \( H \) is a cyclic group and the S-ring \( A_H = \text{Cyc}(\pi(K), H) \) is cyclotomic. Moreover, \( i \in \{2, 3, 8, 9\} \) by statement (3) of Corollary 7.2. Therefore, the order of the group \( \pi(K) \leq \text{Aut}(H) \) is at most 2. By the implication (3) \( \Rightarrow \) (2) of [5, Theorem 6.1], this implies that the group \( \text{Aut}(A_H)_e \) has a faithful regular orbit. Thus, the group \( \text{Aut}(A_H)_e \) is 2-isolated by Lemma 8.2.

**Case 2:** \( e \leq L \leq \langle c_1 \rangle \) and \( |K| = 2 \). Here, \( i \notin \{1, 6, 7\} \) and each basic set of \( A \) is of cardinality at most 2. Since \( A \) is commutative, the latter is also true for the basic sets of \( A_H \). Therefore, this S-ring is quasi-thin. So by the second part of Lemma 8.3 it suffices to prove that \( A_H \) has at least two orthogonals. To do this let \( X \) be a basic set of \( A \) that contains a generator of \( C \). Since the S-ring \( A \) is cyclotomic, \( \pi(X^{(2)}) \) and \( \pi(X^{(4)}) \) are basic sets of \( A_H \). Moreover, they are distinct, because \( n \geq 4 \). Finally, they are orthogonals, because \( \pi(X^{(2)}) \leq \pi(X) \pi(X^{-1}) \) and \( \pi(X)^{(4)} \leq \pi(X^{(2)}) \pi(X^{-2}) \).

**Case 3:** \( e \leq L \leq \langle c_1 \rangle \) and \( |K| = 4 \). Here \( i = 6 \) or 7. It suffices to verify that the hypothesis of Lemma 8.3 is satisfied for a highest basic set \( X \) of the S-ring \( A_H \). To do this we first observe that the sets \( X_0 \) and \( X_1 \) are not empty. Therefore, \( \text{tr}(X) = D \setminus D_{n-1} \), and condition (1) is, obviously, satisfied.

To verify conditions (2) and (3), suppose first that \( L = e \). Then for \( x \in X_0 \), we have

\[
X = \{x, ex^{-1}, sce_2x, sc_2^{-1}ex^{-1}\},
\]

where \( \varepsilon \in \{e, c_1\} \). Since \( n \geq 4 \), the elements \( xy^{-1} \) with \( y \in X \) belong to distinct \( K \)-orbits of cardinalities 1, 2, 2 and 4. A straightforward check shows that if \( Y \) is one of these orbits, then

\[
|Y|c_{XX^{-1}}^Y = 4.
\]
Therefore, $4 = |Y|c_{X}^{c_{X}Y^{-1}} = |X|c_{Y}^{c_{X}Y^{-1}}$, and condition (3) is satisfied, because $|X| = 4$. Let now $Z \in S(\mathcal{A})_{tr(X)}$. Then

$$Z = \{xy, \varepsilon(xy)^{-1}, sc_2xy, sc_2^{-1}\varepsilon(xy)^{-1}\}$$

for some $y \in C_{n-1}$. Let $Y$ be the set $\{y^{\pm 1}, cyz, \{y^{\pm 1}\}, \{y\}$ depending on whether $y$ belongs to $C_{n-1} \setminus C_{n-2}$, $C_{n-2} \setminus C_1$, or $C_1$, respectively. Then $Y$ is a basic set of $\mathcal{A}$. Moreover, a straightforward computation shows that in any case, $c_{XY}^{XZ} = 1$. Since $c_{XY}^{XZ} = c_{XY}^{X^{-1}Z^{-1}} = c_{XY}^{X^{-1}}$, condition (2) is also satisfied.

Let now $L = \langle c_1 \rangle$. To simplify notations, we identify the group $H = D/L$ with $D_{n-1}$, write $\mathcal{A}$ instead of $\mathcal{A}_H$ and use the notation $x$ and $s$ for the $\pi$-images of $x$ and $sc_1$, respectively. Thus, $\mathcal{A}$ is a cyclotomic S-ring over $D_{n-1}$ and

$$X = \{x, x^{-1}, sx, sx^{-1}\}$$

is a highest basic set of $\mathcal{A}$. It follows that $C_{n-2}$ is an $\mathcal{A}$-group and any basic set inside $C_{n-2}$ is of the form $\{z^{\pm 1}\}$ for a suitable $z \in C_{n-2}$. Since $sC_{n-2}$ is an $\mathcal{A}$-set, the elements $xy^{-1}$ with $y \in X$ belong to distinct basic sets of $\mathcal{A}$. Therefore, the set $X^{-1}$ consists of basic sets $Y$ for which $c_{XY}^{X^{-1}} = 1$. Thus, condition (3) is satisfied. Let now $Z \in S(\mathcal{A})_{tr(X)}$. Then

$$Z = \{xy, (xy)^{-1}, sxy, s(xy)^{-1}\}$$

for some $y \in C_{n-2}$. Taking $Y$ to be the basic set $\{y^{\pm 1}\}$, we find that $c_{XY}^{XZ} = 1$. Thus, condition (2) is also satisfied, and we are done.

9. S-rings over $D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n}$: non-trivial radical case

In Theorems 6.1 and 6.2, we completely described the structure of an S-ring over $D$ that has trivial radical. In this section, we study the remaining S-rings.

**Theorem 9.1.** Let $\mathcal{A}$ be an S-ring over a group $D$. Suppose that $\text{rad}(\mathcal{A}) \neq e$. Then $\mathcal{A}$ is a proper generalized $S$-wreath product, where the section $S = U/L$ is such that

$$(24) \hspace{1cm} A_S = ZS \quad \text{or} \quad |S| = 4 \quad \text{or} \quad \text{rad}(A_U) = e \quad \text{and} \quad |L| = 2.$$

**Proof.** Denote by $U$ the subgroup of $D$ that is generated by all $X \in S(\mathcal{A})$ such that $\text{rad}(X) = e$.

**Lemma 9.2.** $U$ is an $\mathcal{A}$-group and $\text{rad}(A_U) = e$.

**Proof.** The first statement is clear. To prove the second one, without loss of generality, we can assume that $U = D$. Then there exists a highest set $X \in S(\mathcal{A})$ such that $\text{rad}(X) = e$. Suppose first that $X$ is not regular. Then $X \cap E \neq \emptyset$ by Theorem 6.2. Therefore, $X$ is one of basic sets $X_{c_1}$, $X_s$, or $X_{sc_1}$ from Theorem 6.1. Since $\text{rad}(X) = e$, we have $X = X_{c_1}$, and $X = X_{s}$ in statements (2) and (3) of this theorem, respectively. Moreover, since $X$ is highest, $D = \langle X \rangle$ in statements (1), (2), (3). Therefore, in these three cases $\text{rk}(A) = 2$, and hence $\text{rad}(A) = e$. In the remaining case (statement (4) of Theorem 6.1), we have $D = H$, and hence $\mathcal{A} = A_U \otimes A_s$. Since each of the factors is of rank 2, this implies that again $\text{rad}(A) = e$. From now on, we can assume that any highest basic set of $\mathcal{A}$ with trivial radical, is regular (Corollary 6.4). Moreover, if $X$ is one of them and both $X_0$ and $X_1$ are

---

6In our case, the S-ring $A_H$ does not depend on the choice of $i \in \{5, 6\}$.
not empty, then all highest basic sets are pairwise rationally conjugate and, hence \( \text{rad}(A) = \text{rad}(X) = e \). Thus, we can also assume that \( \langle X \rangle \) is a cyclic group \( C \) of order at least 4 that has index 2 in \( D \).

Since \( \text{rad}(\mathcal{A}_C) = \text{rad}(X) = e \), the circulant S-ring \( \mathcal{A}_C \) is cyclotomic (see Subsection 5.1). Together with \( |C| \geq 4 \), this shows that \( c_1 \in A \). We claim that any \( Y \in S(A) \) such that \( \text{rad}(Y) = e \) and \( D = \langle X, Y \rangle \), is regular. Indeed, otherwise by Theorem 6.2 we have \( Y = X_h \), where \( h \) is a non-identity element of the group \( E \). However, \( h \neq c_1 \): otherwise \( Y = \{c_1\} \) by above, and \( \langle X, Y \rangle = C \), in contrast to the assumption. Since \( X_{c_1} = \{c_1\} \) and \( \text{rad}(Y) = e \), only statement (4) of Theorem 5.1 can hold. But then, \( Y \) is a singleton in \( E \), and hence it is regular. Contradiction.

To complete the proof, let \( Y \) be a regular basic set with trivial radical. We can assume that \( Y \subseteq D \setminus C \), for otherwise \( D = C \) and \( \text{rad}(A) = \text{rad}(X) = e \). If \( Y \) is not highest, then any basic set \( Z \subseteq XY \) is highest, and \( \langle X, Z \rangle = D \). Moreover, \( \text{rad}(Z) = e \) by Lemma 4.3. Thus, we can also assume that \( Y \) is highest. Then any highest basic set of \( A \) is rationally conjugate to either \( X \) or \( Y \). Thus, \( \text{rad}(A) = e \), as required.

By the theorem hypothesis and Lemma 6.2, we have \( U \neq D \). We observe also that by Theorem 2.2 the group \( U \) contains every minimal \( A \)-group.

**Lemma 9.3.** Suppose that there is a unique minimal \( A \)-group, or \( c_1 \in \text{rad}(X) \) for all \( X \in S(A)_{D \setminus U} \). Then the statement of Theorem 7.1 holds.

**Proof.** Let \( L \) be a unique minimal \( A \)-group. Then the definition of \( U \) implies that \( A \) is a proper generalized S-wreath product, where \( S = U/L \). If, in addition, \( |L| \leq 2 \), then the third statement in (24) follows from Lemma 9.2 and we are done. Let now \( |L| > 2 \). Then \( \langle c_1 \rangle \) is not an \( A \)-group. By statement (1) of Corollary 7.2, this implies that the S-ring \( \mathcal{A}_U \) is not regular. So, by the first part of Theorem 6.1 it is rational. Now, by the second part of this theorem, the uniqueness of \( L \) implies that \( U = L \). Thus, \( |S| = 1 \) and the first statement in (24) holds.

To complete the proof, suppose that there are at least two minimal \( A \)-groups. Then, obviously, one of them, say \( H \), contains \( c_1 \). Therefore, \( c_1 \in H \leq U \). On the other hand, by the lemma hypothesis, \( c_1 \in \text{rad}(X) \) for all \( X \in S(A)_{D \setminus U} \). Thus, \( A \) is a proper generalized S-wreath product, where \( S = U/H \). Without loss of generality, we can assume that \( |H| > 2 \). If the S-ring \( \mathcal{A}_U \) is rational, then from the second part of Theorem 6.1 it follows that there is another minimal \( A \)-group \( L \) of order 2 and such that

\[ \mathcal{A}_U = \mathcal{A}_H \otimes \mathcal{A}_L. \]

Thus, \( |S| = |L| = 2 \), and the first statement in (24) holds. In the remaining case, \( \mathcal{A}_U \) is a regular S-ring by the first part of Theorem 6.1. By statement (1) of Corollary 7.2, this implies that \( H = \langle c_1 \rangle \). Thus, \( |H| = 2 \), and the third statement in (24) holds.

Denote by \( V \) the union of all sets \( X \in S(A) \) such that \( \text{rad}(X) = e \) or \( c_1 \in \text{rad}(X) \). Then, obviously, \( U \subseteq V \) and \( V \) is an \( A \)-set. By Lemma 6.3 we can assume that \( V \neq D \), and that \( U \) contains two distinct minimal \( A \)-groups. It is easily seen that in this case \( E \subseteq V \).

**Lemma 9.4.** In the above assumptions let \( X \in S(A)_{D \setminus V} \). Then

(1) \( \text{rad}(X) = \langle s \rangle \) or \( \langle sc_1 \rangle \),
(2) \( X \) is a regular set such that both \( X_0 \) and \( X_1 \) are not empty.

**Proof.** Since \( X \not\subseteq U \), we have \( \text{rad}(X) \neq e \). Besides, \( c_1 \not\subseteq \text{rad}(X) \) by the definition of \( V \). Thus, statement (1) holds, because \( \langle s \rangle \) and \( \langle sc_1 \rangle \) are the only subgroups of \( D \) that do not contain \( c_1 \). To prove statement (2), set

\[
L = \text{rad}(X) \quad \text{and} \quad \pi = \pi_{D/L}.
\]

Then \( \pi(X) = e \). However, \( D/L \) is a cyclic 2-group by statement (1). Therefore, \( \pi(X) \) is the basic set of a circulant \( S \)-ring \( \mathcal{A}_{D/L} \). From the description of basic sets of such an \( S \)-ring given in Subsection 4.1, it follows that \( \pi(X) \) is regular or is of the form

\[
\pi(X) = \pi(H)^\#
\]

for some \( A \)-group \( H \geq D_1 \) such that \( |H/L| \geq 4 \). In the latter case, \( X = H \setminus L \), and hence \( L \) is a unique minimal \( A \)-group in contrast to our assumption on \( U \). Thus, the set \( \pi(X) \) is regular. This implies that the set \( X \) is also regular. Finally, the fact that \( X_0 \) and \( X_1 \) are not empty, immediately follows from statement (1).

By statement (2) of Lemma 9.4, the union of \( \text{tr}(X) \), where \( X \) runs over the set \( S(\mathcal{A})_{D \setminus V} \), is of the form \( D \setminus D_k \) for some \( k \geq 1 \). However, the set \( V \) coincides with the complement to this union. Thus, \( V = D_k \) is an \( A \)-group. A similar argument shows that \( D_m \) is an \( A \)-group for all \( m \geq k \).

**Lemma 9.5.** Let \( m = \max\{2, k\} \). Then the group \( L := \text{rad}(X) \) does not depend on the choice of \( X \in S(\mathcal{A})_{D \setminus D_m} \).

**Proof.** Suppose on the contrary that there exist basic sets \( X \) and \( Y \) outside \( D_m \) such that \( \langle Y \rangle \subsetneq \langle X \rangle \) and \( \text{rad}(X) \neq \text{rad}(Y) \). Then by statement (1) of Lemma 9.4, without loss of generality, we can assume that

\[
\text{rad}(X) = \langle s \rangle \quad \text{and} \quad \text{rad}(Y) = \langle sc_1 \rangle.
\]

By statement (2) of that lemma, \( X_0 \) is a regular non-empty set. Therefore, it is an orbit of a subgroup of \( \text{Aut}(C) \). Moreover, from the first equality in (25), it follows that \( \text{rad}(X_0) = e \). Let now \( \pi : D \to D/\langle s \rangle \) be the quotient epimorphism. Then \( \pi(X) = X_0 \) is a basic set of a circulant \( S \)-ring \( \mathcal{A}' = \pi(\mathcal{A}) \). It follows that \( \mathcal{A}'(X_0) \) is a cyclotomic \( S \)-ring with trivial radical. Moreover, \( Y' = \pi(Y) \) is a basic set of this \( S \)-ring and \( |Y'| \geq 2^m + 1 \geq 8 \). Therefore, by Lemma 9.2, applied for \( \mathcal{A} = \mathcal{A}'(X_0) \) and \( S = \langle Y' \rangle \), we obtain that

\[
\text{rad}(\mathcal{A}'(Y')) = e.
\]

This implies that \( \text{rad}(Y') = e \). On the other hand, by the second equality in (25), we have \( \text{rad}(Y') = \langle c_1 \langle c_1 \neq e \). Contradiction.

By Lemma 9.5, the \( S \)-ring \( A \) is the generalized \( S \)-wreath product, where \( S = D_2/L \) if \( k = 1 \), and \( S = V/L \) if \( k \geq 2 \). The only case when this generalized product is not proper, is \( D = D_2 \) and \( k = 1 \). However, in this case \( A \) is, obviously, a proper \( E/L \)-wreath product and \( |E/L| = 2 \). Thus, if \( k \leq 2 \), then the first or the second statement in (24) holds, and we are done. To complete the proof of Theorem 9.1 it suffices to verify that the third statement in (24) holds whenever \( k \geq 3 \). But this immediately follows from the lemma below.

**Lemma 9.6.** If \( k \geq 3 \), then \( \text{rad}(\mathcal{A}_V) = e \). In particular, \( V = U \).
Proof. The second statement follows from the first one and statement (1) of Lemma 9.4. To prove that \( \text{rad}(A_V) = e \), let \( X \) be a highest basic set of the S-ring \( A_V \). Since \( V \neq D \), there exists a set \( Y \in \mathcal{S}(A)_{D \setminus V} \) such that \( X \subseteq Y^2 \).

By Lemma 9.4, we have \( Y \subseteq \text{Aut}(A) \). Let \( \Delta \) be the orbit \( \text{Aut}(A) \) of \( A \) such that \( \text{rad}(\Delta) = e \). However, \( Y_0 = \{ y \} \) or \( Y_0 = \{ y, \varepsilon y^{-1} \} \), where \( \varepsilon \in \{ e, c_1 \} \) (statement (1) of Lemma 6.1). Therefore,

\[
Y^2 = LY_0^2 = L \times \begin{cases} \{ y^2 \}, & \text{if } Y_0 = \{ y \}, \\ \{ \varepsilon, y^{\pm 2} \}, & \text{if } Y_0 = \{ y, \varepsilon y^{-1} \}. \end{cases}
\]

On the other hand, since \( X \subseteq V \), the definition of \( V \) implies that \( \text{rad}(X) = e \) or \( c_1 \in \text{rad}(X) \). In the former case, \( \text{rad}(A_V) = e \), and we are done. Suppose that \( c_1 X = X \). Then the set \( Y^2 \) contains \( \langle c_1 \rangle \)-coset \( \{ x, c_1 x \} \) for all \( x \in X \). By (26), this implies that \( \{ x, c_1 x \} \subseteq \{ \varepsilon, y^{\pm 2} \} \).

which is impossible, because \( |x| = 2^k \geq 8 \).

10. S-rings over \( D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n} \): Schurian

In this section, based on the results obtained in Sections 6–9, we prove the following main theorem.

**Theorem 10.1.** For any integer \( n \geq 1 \), every S-ring over the group \( D = \mathbb{Z}_2 \times \mathbb{Z}_{2^n} \) is schurian. In particular, \( D \) is a Schur group.

Proof. The induction on \( n \). An exhaustive computer search of all S-rings over small groups shows that \( D \) is a Schur group for \( n \leq 4 \). Let \( n \geq 5 \). We have to verify that any S-ring \( A \) over \( D \) is schurian. However, if \( \text{rad}(A) = e \), then this is true by Theorems 6.1 and 7.1. For the rest of the proof, we need the following result from [9], giving a sufficient condition for a generalized wreath product of S-rings to be schurian.

**Theorem 10.2.** [9, Corollary 5.7] Let \( A \) be an S-ring over an abelian group \( D \). Suppose that \( A \) is the generalized S-wreath product of schurian S-rings \( A_{D/L} \) and \( A_U \), where \( S = U/L \). Then \( A \) is schurian if and only if there exist two groups \( \Delta_0 \geq (D/L)_{\text{right}} \) and \( \Delta_1 \geq U_{\text{right}} \), such that

\[
\Delta_0 \cong 2 \text{ Aut}(A_{D/L}) \text{ and } \Delta_1 \cong 2 \text{ Aut}(A_U) \text{ and } (\Delta_0)^{U/L} = (\Delta_1)^{U/L}.
\]

**Corollary 10.3.** Under the hypothesis of Theorem 10.2, the S-ring \( A \) is schurian whenever the group \( \text{Aut}(A_S) \) is 2-isolated.

Proof. Set \( \Delta_0 = \text{Aut}(A_{D/L}) \) and \( \Delta_1 = \text{Aut}(A_U) \). Then the first two equalities in (27) hold, because the S-rings \( A_{D/L} \) and \( A_U \) are schurian. Since the group \( \text{Aut}(A_S) \) is 2-isolated, we have \( (\Delta_0)^S = \text{Aut}(A_S) = (\Delta_1)^S \), which proves the third equality in (27). Thus, \( A \) is schurian by Theorem 10.2.

Let us turn to the proof of Theorem 10.1. Now, we can assume that \( \text{rad}(A) \neq e \). Then by Theorem 9.1, the S-ring \( A \) is a proper generalized S-wreath product, where the section \( S = U/L \) is such that formula (24) holds. Besides, by induction, the S-rings \( A_{D/L} \) and \( A_U \) are schurian. Suppose that \( A_S = ZS \), or \( |S| = 4 \), or \( |L| = 2 \) and \( A_U \) is a regular S-ring with trivial radical. Then the group \( \text{Aut}(A_S) \)
is 2-isolated: this is obvious in the first two cases and follows from Theorem 8.1 (applied for $\mathcal{A} = \mathcal{A}_L$) in the third one. Thus, $\mathcal{A}$ is schurian by Corollary 10.3.

To complete the proof, we can assume that $|S| = 2^m$, where $m \geq 3$, and that $\mathcal{A}_L$ is a non-regular $S$-ring with trivial radical. Then $\mathcal{A}_L = \mathcal{A}_H \otimes \mathcal{A}_L$, where $|H| \geq 4$ and $\text{rk}(\mathcal{A}_H) = 2$ (Theorem 4.6). Therefore,

$$\text{Aut}(\mathcal{A}_L)^S = (\text{Sym}(H) \times \text{Sym}(L))^{U/L} = \text{Sym}(S).$$

On the other hand, $L = \langle s \rangle$ or $L = \langle sc_1 \rangle$, because $c_1 \in H$. Therefore, the $S$-ring $\mathcal{A}_{D/L}$ is circulant. Besides, $S$ is an $\mathcal{A}_{D/L}$-section of composite order. By [9, Theorem 4.6], this implies that

$$\text{Aut}(\mathcal{A}_{D/L})^S = \text{Sym}(S).$$

By (28) and (29), relations (27) are true for the groups $\Delta : = \text{Aut}(\mathcal{A}_{D/L})$ and $\Delta_1 : = \text{Aut}(\mathcal{A}_L)$. Thus, the $S$-ring $\mathcal{A}$ is schurian by Theorem 10.2.

11. A non-schurian $S$-ring over $M_{2^n}$

The main result of this section is the following theorem in the proof of which we construct a non-schurian $S$-ring over the group $M_{2^n}$ defined in (11).

**Theorem 11.1.** For any $n \geq 4$, the group $M_{2^n}$ is not Schur.

**Proof.** The group $M_{16}$ is not Schur [23, Lemma 3.1]. Suppose that $n \geq 5$. Denote by $e$ the identity of the group $G = M_{2^n}$, and by $H$ the normal subgroup of $G$ that is generated by the elements $c = a^{2^{n-3}}$ and $b$. Then $H \simeq Z_4 \times Z_2$ and

$$H = Z_0 \cup Z_1 \cup Z_2,$$

where the sets $Z_0 = \{e\}$, $Z_1 = \{c^2\}$, and $Z_2 = H \setminus \langle c^2 \rangle$ are mutually disjoint. Next, let us fix two other decompositions of $H$ into a disjoint union of subsets:

$$H = B \cup B_3 \cup B_2 \cup Bc \cup B^2c \cup B'c \cup B'^2c,$$

where $B$ and $B'$ are the groups of order 2 generated by the involutions $b$ and $b' := c^2b$. Then a straightforward computation shows that

$$Ha \cup Ha^{-1} = X_1a \cup X_2a^{-1} \cup Y_1a \cup Y_2a^{-1},$$

in particular, the sets $Z_3$ and $Z_4$ are disjoint. Moreover, $Z_3c^2 = Z_4$, because $Y_1 = X_1c^2$ and $Y_2 = X_2c^2$. Finally, there are exactly $m' = 2^{n-3} - 3$ cosets of $H$ in $G$, other than $H$, $Ha$, and $Ha^{-1}$. Let us combine them in pairs as follows

$$Z_{i+3} : = Ha_i \cup Ha^{-1}, \ i = 2, 3, \ldots, m,$$

where $m = (m' - 1)/2 + 1$ and $Z_{m+1} = Ha^{2^{n-2}}$. Then the sets $Z_0, Z_1, \ldots, Z_{r-1}$ with $r = m + 5$ form a partition of the group $G$; denote it by $S$. The submodule of $ZG$ spanned by the elements $Z_i, \ i = 0, \ldots, r - 1$, is denoted by $\mathcal{A}$.

**Lemma 11.2.** The module $\mathcal{A}$ is an $S$-ring over $G$. Moreover, $S(\mathcal{A}) = S$. 

Proof. From the above definitions, it follows that \( Z_i^{-1} = Z_i \) for all \( i \). Thus, it suffices to verify that given \( i \) and \( j \), the product \( Z_i Z_j \) is a linear combination of \( Z_k, k = 0, \ldots, r - 1 \). However, it is easily seen that

\[
Ha_i Ha_j = Ha_j Ha_i = Ha_i + j = a_i + j H
\]

for all \( i, j, k \). Therefore, the required statement holds whenever \( i, j \not\in \{3, 4\} \). To complete the proof, assume that \( i = 3 \) (the case \( i = 4 \) is considered analogously).

Then a straightforward check shows that

\[
\begin{align*}
Z_3 Z_1 &= Z_4, \\
Z_3 Z_2 &= Z_4, \\
Z_3 Z_{r-1} &= 4Z_{r-2}, \\
Z_3 Z_3 &= 8Z_1 + 2Z_5 + 4Z_2, \\
Z_3 Z_4 &= 8Z_1 + 2Z_5 + 4Z_2, \\
Z_3 Z_5 &= 4Z_3 + 4Z_4 + 4Z_6, \\
Z_3 Z_i &= 4Z_{i-1} + 4Z_{i+1}, \quad i = 6, \ldots, r - 2.
\end{align*}
\]

Since \( Z_3 \) commutes with \( Z_j \) for all \( j \), we are done.

By Lemma 11.2, the statement of Theorem 11.1 immediately follows from the lemma below.

Lemma 11.3. The S-ring \( A \) is not schurian.

Proof. Suppose on the contrary that \( A \) is schurian. Then it is the S-ring associated with the group \( \Gamma = \text{Aut}(A) \). It follows that the basic set \( Z_2 \) is an orbit of the one-point stabilizer of \( \Gamma \). Since \( |Z_2| = 6 \), there exists an element \( \gamma \in \Gamma \) such that

\[
|\gamma Z_2| = 3.
\]

On the other hand, due to (31), the quotient S-ring \( A_{G/H} \) is isomorphic to the S-ring associated with the dihedral group of order \( 2^{n-2} \) in its natural permutation representation of degree \( 2^{n-3} \). Therefore, \( \text{Aut}(A_{G/H}) \) is a 2-group. It contains a subgroup \( \Gamma_{G/H} \), and hence the element \( \gamma^{G/H} \). So by (33), the permutation \( \gamma \) leaves each \( H \)-coset fixed (as a set). Therefore,

\[
\gamma^{H \cup Ha} \in \text{Aut}(C),
\]

where \( C \) is the bipartite graph with vertex set \( H \cup Ha \) and the edges \((h, hx)\) with \( x \in X_1 \). However, the graph \( C \) is isomorphic to the lexicographic product of the empty graph with 2 vertices and the undirected cycle of length 8. Therefore, \( \text{Aut}(C) \) is a 2-group. By (34), this implies that \( |H| \) is a power of 2. But this contradicts to (33), because \( Z_2 \subset H \).

12. S-rings over \( D = D_{2n}: \) divisible difference sets

12.1. Preliminaries. In the rest of the paper, we deal with S-rings over a dihedral 2-group \( D = D_{2n} \) of order \( 2n \). Interesting examples of such rings arise from difference sets. To construct them, let us recall some definitions from [27].

Let \( T \) be a \( k \)-subset of a group \( G \) of order \( mn \) such that every element outside a subgroup \( N \) of order \( n \) has exactly \( \lambda_2 \) representations as a quotient \( gh^{-1} \) with elements \( g, h \in G \), and elements in \( N \) different from the identity have exactly \( \lambda_1 \) such representations,

\[
T \cdot T^{-1} = k \cdot e + \lambda_1 N \setminus e + \lambda_2 G \setminus N.
\]
Then $T$ is called an $(m, n, k, \lambda_1, \lambda_2)$-divisible difference set in $G$ relative to $N$. If $\lambda_1 = 0$ (resp. $n = 1$), then we say that $T$ is a relative difference set or relative $(m, n, k, \lambda_2)$-difference set (resp. difference set). A difference set $T$ is trivial if it equals $G$, $\{x\}$ or $G \setminus \{x\}$, where $x \in G$.

**Theorem 12.1.** Let $C$ be a cyclic 2-group. Then

1. any difference set in $C$ is trivial,
2. there is no relative $(2^n, 2, 2^n, 2^n - 1)$-difference set in $C$.

**Proof.** Statement (1) follows from [2, Theorem II.3.17] and [3, Theorem 1.2]. Statement (2) follows from [27, Theorems 4.1.4,4.1.5].

12.2. Constructions. Let $D$ be a dihedral group of order $2n$, $C$ the cyclic subgroup of $D$ of order $n$ and $H$ a subgroup of $C$. Let $T$ be a non-empty subset of $C$ such that $|T \cap xH|$ does not depend on $x \in T$ (the intersection condition, cf. Lemma 12.1). Set

$$S := \{e, H \setminus e, C \setminus H, Ts, T's\},$$

where $T' = C \setminus T$. Clearly, $S$ is a partition of $D$ such that condition (S1) is satisfied. Since all the elements of $S$ are symmetric, condition (S2) is also satisfied. Set

$$A := A(T, C) = \text{Span}\{X : X \in S\}.$$  

**Theorem 12.2.** In the above notation, $A$ is an S-ring over $D$ with $S(A) = S$ if and only if $T$ is a divisible difference set in $C$ relative to $H$.

**Proof.** To prove the “only if” part, suppose that $A$ is an S-ring with $S(A) = S$. Then $Ts$ is a basic set of $A$ and $TsTs = TT^{-1}$ is a subset of $C$. Therefore,

$$T \cdot T^{-1} = T^2 = |T|e + \lambda_1 H \setminus e + \lambda_2 C \setminus H,$$

where $\lambda_1 = c^H_{TsTs}$ and $\lambda_2 = c^C_{TsTs}$. Thus, $T$ is a divisible difference set in $C$ relative to $H$.

To prove the “if” part, suppose that $T$ is a divisible difference set in $C$ relative to $H$. It suffices to verify that $A \cdot A \subseteq A$. To do this, denote by $A'$ the module spanned by $e, H, C$, and $D$. Then, obviously, $A' \cdot A' \subseteq A'$ and $A = \text{Span}\{A', \frac{1}{2}T\}$. Thus, we have to check that

$$sT^2 \in A \quad \text{and} \quad A' \cdot sT \subseteq A.$$ 

The first inclusion follows from (35), because $T$ is a divisible difference set. Routine calculations show that the second inclusion is equivalent to the inclusion $\frac{1}{2}T, H \in A$. However, this easily follows from the intersection condition.

We do not know any divisible difference set over a cyclic 2-group that satisfies the intersection condition. However, we can slightly modify the construction by taking the set $T$ to satisfy the intersection condition, but this time inside $C \setminus H$. Then using the same argument, one can construct an S-ring of rank 6 that coincides with $A$ on $C$ and has three basic sets outside $C$: $Ts, T's$, and $Hs$, where $T' = C \setminus (T \cup H)$.

The S-rings of this form do exist. It suffices to take a classical relative $(q + 1, 2, q, (q - 1)/2)$-difference set $T$ defined as follows (see [27, Theorem 2.2.13]). Take an affine line $L$ in a 2-dimensional linear space over finite field $\mathbb{F}_q$ that does not contain the origin. Then $L$ is a relative $(q + 1, q - 1, q, 1)$-difference set in the multiplicative group of $\mathbb{F}_q^\times$. Let $\pi$ be a quotient epimorphism from this group onto
such that $|\ker(\pi)| = m$ for some divisor $m$ of $q - 1$. Then $\pi(L)$ is a cyclic relative $(q + 1, (q - 1)/m, q, m)$-difference set in $C$. When $C$ is a 2-group, the number $q + 1$ is a 2-power, and so, $q$ is a Mersenne number. If, in addition, $m = (q - 1)/2$, then we come to the required set $T$.

**Corollary 12.3.** Let $A$ be an $S$-ring over a dihedral 2-group $D$. Suppose that $C$ is an $A$-group. Then

1. if $\text{rk}(AC) = 2$, then $A \cong AC \rtimes B$, where $* \in \{\wr, \cdot\}$ and $B = \mathbb{Z}/2\mathbb{Z}$,
2. if $\text{rk}(AC) = 3$ and $\text{rk}(A) = 5$, then $A = A(T, C)$, where $T$ is a divisible difference set in $C$.

**Proof.** To prove statement (1), suppose that $\text{rk}(AC) = 2$. Let $X$ be a basic set outside $C$. Then $X = T^s$ for some set $T \subseteq C$. From (37) with $H = e$, it follows that $T$ is a difference set in $C$. By statement (1) of Theorem 12.1, this implies that either $T = C$, or $T$ or $C \setminus T$ is a singleton. It is easily seen, that $A$ is isomorphic to $AC \rtimes B$ in the former case, and to $AC \otimes B$ in the other two.

To prove statement (2), suppose that $\text{rk}(AC) = 3$ and $\text{rk}(A) = 5$. Then $$A_C = \text{Span}\{e, H, C\}$$ for some $A$-group $H < C$. Besides, any $X \in S(A)_{D\setminus C}$ is of the form $X = T$s for some set $T \subseteq C$ satisfying the intersection condition (Lemma 2.1). Thus, $A = A(T, C)$. So, $T$ is a divisible difference set in $C$ by Theorem 12.2.

12.3. **Schurity.** The main goal of this subsection is to prove the following theorem showing that the first construction given in the previous subsection, produces mainly non-schurian $S$-rings.

**Theorem 12.4.** Let $T$ be a divisible difference set in a cyclic 2-group $C$ relative to a group $H \leq C$. Suppose that the intersection condition holds and $HT \neq T$. Then the $S$-ring $A(T, C)$ defined in (36) is not schurian.

We will deduce this theorem in the end of this subsection from a general statement on schurian $S$-rings over a dihedral 2-group. This statement shows that if $T$ is a divisible difference set in a cyclic 2-group relative to a subgroup $H$, and the $S$-ring of rank 6 associated with $T$, is schurian but not a proper generalized wreath product, then $H$ is of order 2.

**Theorem 12.5.** Let $A$ be a schurian $S$-ring over a dihedral 2-group $D$ and $H < C$ a minimal $A$-group. Suppose that $A$ is not a proper generalized wreath product. Then $|H| = 2$.

**Proof.** By the hypothesis, $S(A) = \text{Orb}(G_e, D)$ for some group $G \leq \text{Sym}(D)$ containing $D_{\text{right}}$. Since $H$ is an $A$-group, the partition $D/H$ of the group $D$ into the right $H$-cosets, forms an imprimitivity system for $G$. Denote by $N$ the stabilizer of this partition in $G$, $$N = \{g \in G : (Hx)^g = Hx \text{ for all } x \in D\}.$$ Since $H_{\text{right}} \leq N$, the group $N^x$ is transitive for each block $X \in D/H$. The following statement can also be deduced from [17, Lemma 2.1].

**Lemma 12.6.** For each block $X \in D/H$, the group $N^X$ is 2-transitive.
A is a unique minimal transitive. However, $N$ contains a non-trivial normal subgroup of $G^X$. Therefore, $N^X$ contains $K$, and hence is 2-transitive.

Let us define an equivalence relation $\sim$ on the $H$-cosets by setting $X \sim Y$ if and only if the actions of $N$ on $X$ and $Y$ have the same permutation character. Then by Lemma 12.6 and a remark in [3] p.2, the group $N_e$ acts transitively on each $X$ not equivalent to $H$. Denote by $U$ the class of $\sim$ that contains $H$. Then each orbit of $G_e$ outside $U$ is a union of $N$-orbits. Thus, $A$ is the generalized $U/H$-wreath product. By the theorem hypothesis, this implies that $U = D$. Therefore, all classes of the equivalence relation $\sim$ are singletons. So by Lemma 12.6 we have

$$|\text{Orb}(N, X \times Y)| = 2 \quad \text{for all } X, Y \in D/H.$$  

This yields us two symmetric block-designs between $X$ and $Y$ which are complementary to each other. Since $N$ contains a cyclic subgroup $H$ which acts regularly on $X$ and $Y$, these block-designs are circulant, and so correspond to cyclic difference sets. By statement (1) of Lemma 12.1, they are trivial. Thus, the group $N_x$ with $x \in X$, has two orbits on $Y$ of cardinalities 1 and $|Y| - 1$.

To complete the proof, suppose on the contrary that $|H| > 2$. Then, obviously, $|Y| > 2$. Therefore, the group $N_e$ fixes exactly one point in each $H$-coset $Y$. This implies that the set $F$ of all fixed points of $N_e$, is of cardinality $[D : H]$. On the other hand, by [17] Proposition 5.2, the set $F$ is a block of $G$. Therefore, $F$ is a subgroup of $D$. Moreover, since $F \cap H = e$, it is a complement for $H$ in $D$. Thus, $H = C$. Contradiction.

Proof of Theorem 12.4 Suppose on the contrary that the S-ring $A = A(T, C)$ is schurian. Then the hypothesis of Theorem 12.5 is satisfied, because $H$ is a minimal $A$-group and $HT \neq T$. Thus, $|H| = 2$. Denote by $x$ the element of order 2 in $H$. Then $x \in A$, and hence $x(Ts) = T's$. This implies that $|Ts| = |T's| = m$, where $m = |C|/2$, and that $x$ appears neither in $T_s^2$, nor in $Ts^2$. Therefore, $T$ has parameters $(m, 2, m, 0, m/2)$. It follows that $T$ is a relative $(m, 2, m, m/2)$-difference set in $C$. However, this contradicts part (2) of Theorem 12.1.

13. S-rings over $D = D_{2n+1}$: A unique minimal $A$-group not in $C$

In this section we deal with S-rings over a dihedral group $D = D_{2n+1}$ of order $2^{n+1}$ and keep the notation of Subsection 1.2. The main result here is given by the following statement.

Theorem 13.1. Let $A$ be an $S$-ring over the dihedral group $D$. Suppose that there is a unique minimal $A$-group $H$, and that $H \not\subseteq C$. Then $A$ is isomorphic to an $S$-ring over $\mathbb{Z}_2 \times \mathbb{Z}_{2^n}$.

Proof. The hypothesis on $H$ implies that every basic set $X$ outside $H$ is mixed, for otherwise $(X)$ contains a non-identity $A$-subgroup of $C$. Moreover, either $H = \langle s \rangle$ for some $s \in D \setminus C$, or $H$ is a dihedral group. Let us consider these two cases separately.
Case 1: $H = \langle s \rangle$ for some $s$. In this case, all basic sets except for $\{e\}$ and $\{s\}$ are mixed. By statement (1) of Lemma 13.2, this implies that $X_0^{-1} = X_0$ for all $X \in S(A)$. Besides, $xs \in S(A)$, because $s \in A$, and $(xs)_0 = X_1$ and $(xs)_1 = X_0$. Thus, $X_1^{-1} = X_1$ also for all $X$.

Denote by $\sigma$ the automorphism of $D$ that takes $(c, s)$ to $(c^{-1}, s)$, where $c$ is a generator of $C$. Then by the above paragraph, we have

$$X^\sigma = (X_0 \cup X_1)s^\sigma = X_0^{-1} \cup X_1^{-1} = X_0 \cup X_1s = X$$

for all $X \in S(A)$. Therefore, the semidirect product $D \rtimes \langle \sigma \rangle \leq \text{Sym}(D)$ is an automorphism group of $A$. The element $s\sigma$ of this group has order two and commutes with $c$. Therefore, the group $D' = \langle s\sigma, c \rangle$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2^\ast$. On the other hand, $D'$ is a regular subgroup in $\text{Sym}(D)$. Thus, the Cayley scheme over $D$ associated with $A$ is isomorphic to a Cayley scheme over $D'$. Consequently, $A$ is isomorphic to an S-ring over $\mathbb{Z}_2 \times \mathbb{Z}_2^\ast$.

Case 2: $H$ is dihedral. In this case all basic sets of $A$ other than $\{e\}$ are mixed. Moreover, the S-ring $A_H$ is primitive by the minimality of $H$. Therefore, $\text{rk}(A_H) = 2$ by Theorem 2.2. In particular, $\text{Aut}(A_H) = \text{Sym}(H)$. Below, we will prove that

$$(38) \quad H \leq \text{rad}(X) \text{ for all } X \in S(A)_{D \setminus H}.$$ 

Then the Cayley scheme associated with $A$ is isomorphic to the wreath product of the scheme associated with $A_H$ and a circulant scheme on the right $H$-cosets. Therefore, the group $\text{Aut}(A)$ contains a subgroup isomorphic to $\text{Sym}(H) \wr \mathbb{Z}_m$, where $m = [D : H]$. Since the latter group contains a regular subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2^\ast$, we are done.

To complete the proof, we will check statement (38) in two steps: first for rational S-rings, and then in general.

Lemma 13.2. Statement (38) holds whenever the S-ring $A$ is rational.

Proof. The rationality of $A$ implies that it is symmetric, and hence commutative. Toward a contradiction, suppose that $HX \neq X$ for some basic set $X$ contained in $D \setminus H$. Then the product $HX$ is a union of $m > 1$ basic sets $X, Y, \ldots$. Without loss of generality, we may assume that $|X| \leq |Y| \leq \cdots$.

Since $H$ is an $A$-group, it follows from Lemma 2.4 that the number $\lambda = |X \cap xH|$ does not depend on the choice of $x \in X$. Therefore, each $x$ appears $\lambda$ times in the product $HX$, i.e.

$$(39) \quad HX = \lambda(X + Y + \cdots).$$

By the minimality of $X$, this implies that $|H| |X| \geq \lambda m |X|$, and hence $|H| \geq \lambda m$. On the other hand, $(H \cap C)X_0 = X_0$ by the rationality of $X$. Therefore, the element $X$ appears in the product $HX$ at least $|H \cap C| = |H|/2$ times. Thus, $\lambda \geq |H|/2$, and

$$|H| \geq \lambda m \geq m|H|/2.$$

Due to $m > 1$, we have $m = 2$ and $\lambda = |H|/2$. Consequently, $H_0 = H_1 = H \cap C$, because the group $H$ is dihedral. Therefore,

$$HX = H_0(e + s)(X_0 + sX_1) = H_0X_0 + H_0sX_0 + H_0X_1 + H_0sX_1 = |H_0|X_0 + H_0X_1 + \cdots.$$
By (39), all coefficients in the last expression are equal to \( \lambda = |H_0| \). Therefore, the set \( H_0X_1 \cap X_0 \) must be empty. It follows that \( H_0X_1 = |H_0|H_0X_1 \). However, this means that \( H_0 \leq \text{rad}(X_1) \). Since also \( H_0 \leq \text{rad}(X_0) \), we conclude that \( H_0 \leq \text{rad}(X) \). But \( H_0 \neq e \), because \( H \) is dihedral. Thus, \( \text{rad}(X) \) is non-trivial, and so contains the minimal \( A \)-group \( H \). But then, \( HX = X \). Contradiction.

To complete the proof of (38), take a basic set \( X \) outside \( H \). So by Lemma 13.2 we have

\[
Y_0 + sY_1 = \frac{1}{|H|} H \cdot Y = \frac{1}{|H|} (e + s) (H_0Y_0 + H_0Y_1).
\]

Therefore, \(|Y_0| = |Y_1|\). On the other hand, for every integer \( m \) coprime to \( |D| \), we have \(|(X(m))_0| = |X_0|\). By Lemma 13.5 this implies that \(|(X(m))_1| = |X_1|\). Thus,

\[
k|X_0| = |Y_0| = |Y_1| = k|X_1|,
\]

where \( k \) is the number of all distinct sets \( X(m) \)'s. It follows that \(|X_0| = |X_1|\) for each basic set \( X \) outside \( H \).

Denote by \( \rho \) the restriction to \( A \) of the one-dimensional representation of \( D \) that takes \( s \) and \( e \) to \(-1\) and \( 1\), respectively. Then \( \rho \) is an irreducible representation of \( A \) such that \( \rho(e) = 1 \) and \( \rho(H^\#) = -1 \). Moreover, for any basic set \( X \) outside \( H \), we obtain by above that \( \rho(X) = -|X_1| + |X_0| = 0 \). In particular, \( \rho(X^{-1}) = 0 \). Therefore,

\[
0 = \rho(X^{-1}) = \sum_{Y \in S(A)} c_{X^{-1}}^Y \rho(Y) = c_{X^{-1}}^e \rho(e) + c_{X^{-1}}^{H^\#} \rho(H^\#) = c_{X^{-1}}^e - c_{X^{-1}}^{H^\#}.
\]

It follows that \(|X| = c_{X^{-1}}^e = c_{X^{-1}}^{H^\#} \). Therefore, \( HX = X \) for all basis sets outside \( H \), and we are done.

14. Proof of Theorem 13.3

Let \( D \) be a dihedral 2-group and \( C \) its cyclic subgroup of index 2. Let \( A \) be an \( S \)-ring over the group \( D \). Suppose that \( r := \text{rk}(A) \) is at most 5. For \( r = 2 \), part (1) of Theorem 13.3 holds trivially. Let \( r \geq 3 \). Then from Theorem 2.2 it follows that the \( S \)-ring \( A \) is imprimitive; denote by \( H \) a minimal non-trivial \( A \)-group. Then \( \text{rk}(A_H) = 2 \). Now, if \( r = 3 \), then \( A \) is a proper wreath product by Corollary 3.3.

Thus, we can assume that \( r = 4 \) or \( r = 5 \).

Lemma 14.1. If there is a minimal \( A \)-group \( L \neq H \), then statement (2) holds.

Proof. By the minimality of the groups \( H \) and \( L \), we have \( H \cap L = e \). Therefore, at least one of them intersects \( C \) trivially. Moreover, if \( H \cap C = L \cap C = e \), then \( \langle HL \rangle \) is an \( A \)-group contained in \( C \), and we replace \( H \) by a minimal \( A \)-subgroup in \( \langle HL \rangle \). Thus, without loss of generality, we can assume that

\[
H \cap C \neq e \quad \text{and} \quad L \cap C = e.
\]

Then \( L = \langle s \rangle \) for some involution \( s \in D \setminus C \). Moreover, \( sHs = H \) by the minimality of \( H \). Thus, \( HL \) is an \( A \)-group and the set \( S(A_{HL}) \) contains 4 elements: \( \{e\}, H^\#, \{s\} \), and \( sH^\# \). Therefore,

\[
A_{HL} = A_H \cdot A_L.
\]

This implies the required statement for \( r = 4 \), and by Corollary 3.3 also for \( r = 5 \).
By Lemma 14.1 we can assume that $H$ is a unique minimal $A$-group. If it is not contained in $C$, then statement (1) holds by Theorem 15.1. Thus, from now, on we also assume that $H \subseteq C$. Denote by $F$ the union of all basic sets of $A$ that are not $C$-mixed. Clearly, $H \subseteq F$.

**Lemma 14.2.** $F$ is an $A$-group. Moreover, if $r = r(A_F) + 1$, then $A$ is a proper wreath product.

**Proof.** The second part of our statement follows from the first one and Corollary 3.3. To prove the first statement, denote by $U$ and $V$ the unions of all basic sets of $A$ contained in $C$ and $D \setminus C$, respectively. We have to prove that $U \cup V$ is a group. Since $U$ is, obviously, an $A$-group, without loss of generality, we may assume that $V$ is not empty. Then $V = U'$, where $s \in D \setminus C$ is such that $U \cap Us$ is a subgroup of $D$. It follows that

$$UU' \subseteq U' \quad \text{and} \quad U'U' \subseteq U.$$  

Since also $U' \subseteq UU'$, the first inclusion implies that $U' = UU'$. Therefore, $U'$ is a union of some $U$-cosets contained in $C$. Since the group $C$ is a cyclic 2-group, this together with the second inclusion implies $U' = U$. Thus, the set $U \cup V = U \cup Us$ is a group.

Suppose first that $F_0 = C$. Then from the definition of $F$, it follows that $C$ is an $A$-group. By Corollary 3.3, we can assume that $r_C = \text{rk}(A_C)$ is not equal to $r - 1$. Since, obviously, $r_C \geq 2$, we have

$$(r, r_C) = (4, 2), \ (5, 2) \text{ or } (5, 3).$$

In the former two cases, we are done by statement (1) of Corollary 3.3, whereas in the third one by statement (2). Thus, in what follows, we can assume that

$$F_0 < C \quad \text{and} \quad H = F \text{ or } r_F = 3,$$

where $r_F = \text{rk}(A_F)$. In particular, there are two or three basic sets outside $F$ (notice, that they are $C$-mixed).

**Lemma 14.3.** Let $X \in S(A)_{D \setminus F}$. Suppose that $X$ is rational or $[V : H] \geq 4$, where $V = (X_0)$. Then $H \leq \text{rad}(X)$.

**Proof.** It suffices to verify that $H \leq \text{rad}(X_0)$. Indeed, then the coefficient at $X$ in $H X$ is at least $|H|$. Since it can not be larger than $|H|$, we are done.

Suppose first that $X$ is rational. Then by statement (2) of Lemma 4.3 the set $X_0$ is rational. Since $X_0 \subseteq C \setminus H$, we conclude that $H \leq \text{rad}(X_0)$, as required.

Let now $[V : H] \geq 4$. Then $V \cong \mathbb{Z}_{2^k}$ for some $k \geq 2$. Since $r \leq 5$, there are at most two basic rationally conjugate to $X$. Therefore, the stabilizer of $X_0$ in the group $(\mathbb{Z}_{2^k})^*$, has index at most 2 in it. It follows that this stabilizer contains the subgroup of all elements $x \mapsto x^{1+4m}$, $x \in \mathbb{Z}_{2^k}$, with $m \in \mathbb{Z}_{2^k}$. By statement (2) of Lemma 4.3, this implies that $\text{rad}(X_0) \geq V^4 \geq H$.

From Lemma 14.3 it follows that if all basic sets outside $F$ are rational, then $A$ is a proper wreath product. Indeed, this is obvious when $H = F$. If $H \neq F$, this is also true, because then $F \setminus H$ is a basic set, the radical of which equals $H$.

Thus, we can assume that two of basic sets outside $F$, say $X$ and $Y$, are rationally conjugate, and the third one (if exists) is rational. The rest of the proof is divided into four cases below.
Case 1: \( F = H \) and \( r = 4 \). Using the computer package COCO, \[23\] we found exactly five and three \( S \)-rings of rank 4 over the groups \( D_8 \) and \( D_{16} \), respectively. In both cases, only two of them have a unique minimal \( A \)-group contained in \( C \) and they are proper wreath products. Thus, in what follows, we assume that \( |D| \geq 32 \).

In our case, the non-trivial basic sets of \( A \) are \( X \) and \( Y \) and \( Z = H^# \). It is easily seen that the hypothesis of Lemma \[4.5\] is satisfied. Since \( X \) and \( Y \) are rationally conjugate, there is an algebraic isomorphism of \( A \) that takes \( X \) to \( Y \), and \( Y \) to \( X \). Therefore,

\[
(40) \quad H X = a(X + Y),
\]

where \( a = |H|/2 \). Consequently, \( c^X_{ZX} = a - 1 \). On the other hand, since \( X \) and \( Z \) are symmetric, we have \( C^X_{XX} = |X|^a |C^X_{ZX} \). It follows that \( |Z| = 2a - 1 \) divides

\[
|X| c^X_{ZX} = \frac{(d - 2a)(a - 1)}{2},
\]

where \( d = |D| \). However, by Lemma \[14.3\] without loss of generality, we can assume that \( |C : H| = 2 \). Therefore, \( 2a = |H| = d/4 \). It follows that \( 2a - 1 \) divides \( 3a(a - 1) \). But \( a \) being a power of 2, must be coprime to \( 2a - 1 \). Consequently, \( 2a - 1 \) divides \( 3a - 3 \). Since this is possible only for \( a \leq 2 \), i.e. when \( d \leq 16 \), we are done.

Case 2: \( F = H \) and \( r = 5 \). Denote by \( Z \) the basic set in \( S(A)_{D \setminus H} \) other than \( X \) and \( Y \). It is easily seen that the hypothesis of Lemma \[4.5\] is satisfied. Since \( X \) and \( Y \) are rationally conjugate, there is an algebraic isomorphism of \( A \) that takes \( X \) to \( Y \), \( Y \) to \( X \) and leaves \( Z \) fixed. Therefore, the rational closure of \( A \) is of rank 4. So by Lemma \[14.3\] it is the wreath product \( A_H \wr B \), where \( B \) is isomorphic to the rational closure of \( A_{D/H} \). Therefore, \( \text{rk}(B) = 3 \), and hence there exists a non-trivial \( B \)-group. Denote by \( U \) its preimage in \( A \). Then, obviously, \( H \leq U < D \).

Since \( X \) and \( Y \) are rationally conjugate, we have \( X \cup Y \subseteq U \) or \( X \cup Y \subseteq D \setminus U \). However, \( \text{rk}(A) = r = 5 \). Therefore, \( Z = D \setminus U \) in the former case, and \( Z = U \setminus H \) in the latter one. In any case, \( H \leq \text{rad} \, Z \). By Lemma \[14.3\] this implies that if \( Z = U \setminus H \), then

\[
(41) \quad \text{rad}(X) = \text{rad}(Y) \geq H,
\]

and \( A \) is a proper wreath product. Let now, \( Z = D \setminus U \). Then \( \text{rk}(A_U) = 4 \), and \( A_U \) is the wreath product \( A_H \wr A_{U/H} \). Therefore, again \[41\] holds, and \( A \) is a proper wreath product.

Case 3: \( C \geq F > H \). In this case, \( F = H \cup Hs \). So by Lemma \[14.3\] the sets \( X_0 \) and \( Y_0 \) are orbits of an index 2 subgroup of \( \text{Aut}(C) \), unless \( A \) is a proper wreath product. This implies that the group \( \text{rad}(X_0) = \text{rad}(Y_0) \) has index 2 in \( H \). Therefore, equality \[41\] holds with \( a = |H|/2 \). Exactly as in Case 2, we conclude that \( 2a - 1 \) divides

\[
|X| c^X_{ZX} = \frac{(d - 4a)(a - 1)}{2},
\]

where \( Z = H^# \) and \( d = |D| = 4|H| = 8a \). Thus, \( 2a - 1 \) divides \( 2a(a - 1) \). Contradiction.
Case 4: $C \geq F > H$. In this case, $F = F_0 < C$ by the above assumption. Therefore, $X_0$ (and also $Y_0$) contains a generator of $C$. It follows that

$$\langle X_0 \rangle : H = [C : H] \geq [C : F][F : H] \geq 4.$$ 

By Lemma 14.3 this implies that (11) holds. Since also $F \setminus H$ is the basic set and $H = \text{rad}(F \setminus H)$, the group $H$ is contained in the radical of every basic set outside $H$. Thus, $A$ is a proper wreath product.

References

[1] R. A. Bailey, P. J. Cameron, Crested products of association schemes, J. London Math. Soc., 72 (2005), 2, 1-24.
[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, 2nd edition, Cambridge University Press, Cambridge, 1999.
[3] P. J. Cameron, On groups with several doubly-transitive permutation representations, Math. Z., 128 (1972), 1-14.
[4] J. A. Davis, K. Smith, A construction of difference sets in high exponent 2-groups using representation theory, Journal Algebraic Combin., 3 (1994), 137-151.
[5] S. Evdokimov, I. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, St. Petersburg Math. J., 14 (2003), no. 2, 189–221.
[6] S. Evdokimov, I. Ponomarenko, A new look at the Burnside-Schur theorem, Bulletin of the London Mathematical Society, 37 (2005), 535-546.
[7] S. Evdokimov, I. Ponomarenko, Permutation group approach to association schemes, European Journal Combin., 30 (2009), 6, 1456–1476.
[8] S. Evdokimov, I. Ponomarenko, Schur rings over a product of Galois rings, Beitr. Algebra Geom., 55 (2014), 1, 105–138.
[9] S. Evdokimov, I. Ponomarenko, Sphericity of S-rings over a cyclic group and generalized wreath product of permutation groups, Algebra and Analysis, 24 (2012), 3, 84–127.
[10] S. Evdokimov, I. Kovács, I. Ponomarenko, Characterization of cyclic Schur groups, Algebra and Analysis, 25 (2013), 5, 61–85.
[11] S. Evdokimov, I. Kovács, I. Ponomarenko, On sphericity of finite abelian groups, arXiv:1309.0989 [math.GR] (2013), 1–20 (accepted to Communication in Algebra).
[12] M. Hirasaka, M. Muzychuk, Association schemes generated by a non-symmetric relation of valency 2, Discrete Math., 244 (2002), 109–135.
[13] G. A. Jones, Cyclic regular subgroups of primitive permutation groups, Journal Group Theory, 5 (2002), 403–407.
[14] L. A. Kaluzhnin, M. Kh. Klin, Certain numerical invariants of permutation groups, Latv. Mat. Ezheg., 18 (1976), 81–99 (in Russian).
[15] M. Kh. Klin, The axiomatics of cellular rings, Investigations in the algebraic theory of combinatorial objects, 6–32, Vsesoyuz. Nauchno-Issled. Inst. Sistem. Issled., Moscow, 1985 (in Russian).
[16] R. Kochendörffer, Untersuchungen über eine Vermutung von W. Burnside, Schr. Math. Semin. u. Inst. Angew. Math. Univ. Berlin, 3 (1937), 155–180.
[17] I. Kovács, D. Marušič, M. Muzychuk, On dihedrants admitting arc-regular group actions, Journal Algebraic Combin., 35 (2011), 409–426.
[18] K. H. Leung, S. L. Ma, The structure of Schur rings over cyclic groups, Journal Pure Appl. Algebra, 66 (1990), 287–302.
[19] K. H. Leung, S. H. Man, On Schur Rings over Cyclic Groups, Israel J. Math., 106 (1998), 251–267.
[20] M. Muzychuk, $V$-rings of permutation groups that have invariant metric, Thesis, (1987) (in Russian).
[21] M. Muzychuk, I. Ponomarenko, Schur rings, European Journal Combin., 30 (2009), 6, 1526–1539.
[22] M. Muzychuk, I. Ponomarenko, On quasi-thin association schemes, Journal of Algebra, 351 (2012), 467–489.
[23] Ch. Pech, S. Reichard, M. Ziv-Av, The COCO share package for GAP, https://github.com/MatanZ/coco-ii.
[24] I. N. Ponomarenko, *Bases of Schurian antisymmetric coherent configurations and isomorphism test for Schurian tournaments*, J. Math. Sci. (N. Y.), 192 (2013), no. 3, 316-338.
[25] I. Ponomarenko, A. Vasil’ev, *On non-abelian Schur groups*, Journal of Algebra and Its Applications, 13 (2014), 8, 1450055-1–1450055-22.
[26] R. Pöschel, *Untersuchungen von S-ringen insbesondere im gruppenring von p-gruppen*, Math. Nachr., 60 (1974), 1–27.
[27] A. Pott, *Finite geometry and character theory*, Berlin: Springer-Verlag, 1995.
[28] I. Schur, *Zur Theorie der einfach transitiven Permutationss.), S.-B. Preus Akad. Wiss. Phys.-Math. Kl., (1933), 598–623.
[29] H. Wielandt, *Zur Theorie der einfach transitiven Permutationsgruppen. II*, Mathematische Zeitschrift, 52 (1949), 384–393.
[30] H. Wielandt, *Finite permutation groups*, Academic Press, New York - London, 1964.

Netanya Academic College, Netanya, Israel
E-mail address: muzy@netanya.ac.il

Steklov Institute of Mathematics at St. Petersburg, Russia
E-mail address: inp@pdmi.ras.ru