ISSN: 2499-1287
Vol. 23 (2026)

Advances in Group Theory and Applications

an open access journal



AGTA

ISSN: 2499-1287
Vol. 23 (2026)

Advances in Group Theory and Applications

an open access journal



AGTA

CONTENTS

B. Amberg 1
Hermann Heineken (1936 – 2026)

C. Tsang 3
Finite almost simple groups whose holomorph contains a solvable regular subgroup

K.A. Al-Sharo – T. Foguel 13
Finite groups in which every subgroup of order divisible by p is normal

A. Galt – V. Gubarev 27
Rota–Baxter operators on dihedral and alternating groups

M.S. Malekan 63
About nilpotent profinite groups largely satisfying a word equation

S.I. Lendzenkova 73
On finite groups factorized by weakly $\mathbb{X}$-subnormal subgroups

M.L. Lewis – S.M. Tefft 85
The period of Ducci cycles on $\mathbb{Z}_{2^l}$ for tuples of length 2^k

C. Lassueur – J. Murray 117
The self-dual indecomposable modules in blocks with cyclic defect groups

F. Berlai 167
Bounded conciseness in the space of marked groups

S.H. Alavi – A. Daneshkham – H.P. Mosaed 183
On quantitative structure of symplectic groups of dimension four

Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 1–2 ISSN: 2499-1287
DOI: 10.32037/agta-2026-000

Hermann Heineken (1936 – 2026)

Bernhard Amberg



Professor Dr. Hermann Heineken, from the Julius–Maximilians–Universität of Würzburg passed away on April 4, 2026, at the age of 90. With his passing, the international mathematical community and the field of group theory in particular loses a distinguished scholar and an inspiring academic teacher.

Born in Hamburg on March 5, 1936, Hermann Heineken studied Mathematics and Physics at the universities in Hamburg, Marburg and Frankfurt from 1954 to 1959. He completed his studies with the state examination of higher education in Frankfurt and subsequently became an assistant to Reinhold Baer at the University of Frankfurt.

Already in the early stages of his career, he impressed by finding elegant and in some instances unexpectedly simple solutions to problems considered highly challenging by his mentor, Professor Reinhold Baer. Heineken's thesis addressed significant problems in group theory leading to his first scientific publications. Heineken became a true specialist in sophisticated commutator calculations and the study of Engel elements.

As an assistant in Frankfurt, Heineken was a vital member of the "Baer group", where he mentored and motivated many young students in their research.

Heineken earned his doctorate in 1961 with a thesis titled "Engel elements of length three"and completed his habilitation in 1966 with

a thesis on "Groups whose commutator structures satisfy certain closure properties". During this period he also served as a visiting professor at the University of Cambridge (England) and the University of Notre Dame (USA).

After working as a lecturer at the University of Erlangen, he accepted a professorship at the University of Würzburg in 1973, where he remained a central figure in the department for decades.

His academic work focused on algebra, specifically group theory. As a renowned expert in both finite and infinite groups, he published about 130 scientific papers on various problems especially for soluble and generalized soluble groups. A notable highlight of his career was the construction of the first infinite metabelian p-group with trivial center (a joint work with Ismael Mohamed in 1968). In recognition of their importance, these groups are now known as Heineken–Mohamed groups. Throughout his career, he supervised 26 Ph.D. theses.

Through extensive international collaborations spanning England, Italy, Spain, Russia, Ukraine, and the United States, he earned global respect. He regularly attended mathematical conferences and frequently invited distinguished colleagues to Würzburg to foster intellectual exchange. Known for his friendliness and genuine interest in the work of others, he collaborated with approximately 45 coauthors.

Beyond research Professor Heineken was deeply committed to academic life. He organized colloquia and encouraged regional collaboration through regular meetings between algebraists in Erlangen, Freiburg, München and Würzburg, most notably the biannual series "Groups and topological groups". He also took an active role in university governance, serving twice as dean of his faculty and as a member of the university senate.

Colleagues, students, and friends will always remember Hermann Heineken as a dedicated mathematician, a thoughtful mentor, and a bridge-builder within the international scientific community. His legacy will endure through his contributions to algebra and the many scholars he influenced.

Bernhard Amberg



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 3–12 ISSN: 2499-1287
DOI: 10.32037/agta-2026-001

Finite Almost Simple Groups whose Holomorph Contains a Solvable Regular Subgroup

Cindy (Sin Yi) Tsang

(*Received Jan. 17, 2024; Accepted Mar. 21, 2024 — Comm. by A. Ballester–Bolinches*)

Abstract

In our previous paper, we gave a complete list of the finite non-abelian simple groups whose holomorph contains a solvable regular subgroup. In this paper, we refine our previous work by considering all finite almost simple groups. In particular, our theorem yields a complete characterization of the finite almost simple groups which occur as the type of a Hopf–Galois structure on a solvable extension, or equivalently, the additive group of a skew brace having a solvable multiplicative group.

Mathematics Subject Classification (2020): 20B35, 20D05, 20D40

Keywords: holomorph; regular subgroup; almost simple group; group factorization; skew brace; Hopf–Galois structure

1 Introduction

Let G and N be two finite groups of the same order. We shall say that the pair (G, N) is *realizable* if the holomorph of N contains a regular subgroup that is isomorphic to G. Recall that the *holomorph of* N is defined to be

$$\mathrm{Hol}(N) = \rho(N) \rtimes \mathrm{Aut}(N) = \lambda(N) \rtimes \mathrm{Aut}(N)$$

as a subgroup of the symmetric group of N, where λ and ρ are the left and right regular representations of N. By [2, 5] and [6], respectively, it is known that (G, N) is realizable if and only if there exists

a Hopf–Galois structure of type N on a Galois G-extension of fields, or equivalently, a skew brace with additive group N and multiplicative group isomorphic to G. This is exactly our motivation of studying realizability (see [4] and [7] for more details).

For the pair (G, N) to be realizable, it is conjectured that if G is insolvable then N is also insolvable (see [3, 9] for some progress on this). On the other hand, the converse is known to be false — there exist realizable pairs (G, N) for which G is solvable but N is insolvable. It seems to be a natural problem to try and determine the insolvable groups N that can occur in such a pair. In [8, Theorems 1.2 and 1.3], we proved the following.

Theorem 1 *Let N be any finite almost simple group. If (G, N) is realizable for some solvable group G, then the socle of N is isomorphic to*

(1) $\mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(4)$, $\mathrm{PSL}_3(8)$, $\mathrm{PSU}_3(8)$, $\mathrm{PSU}_4(2)$, M_{11}; *or*

(2) $\mathrm{PSL}_2(q)$ *with $q \neq 2, 3$ a prime power.*

The converse is also true when N is a finite non-abelian simple group.

The purpose of this paper is to study the converse of Theorem 1 for an arbitrary finite almost simple group N that is not necessarily simple. It turns out that the proposition below (see [8, Corollary 2.2 and Proposition 2.7]) is enough to do the job apart from the case in which $N = \mathrm{PSU}_3(8)$. This case has already been dealt with in [8] and so may be ignored. In the following, $\mathrm{Inn}(N)$ denotes the inner automorphism group of N.

Proposition 2 *Let N be any finite group.*

(a) *If (G, N) is realizable for a solvable group G, then there exists a subgroup*

$$\mathrm{Inn}(N) \leqslant P \leqslant \mathrm{Aut}(N)$$

such that $P = AB$ is factorized by some solvable subgroups A, B that satisfy the equality $A \cdot \mathrm{Inn}(N) = B \cdot \mathrm{Inn}(N)$.

(b) *If N has trivial center and there exists a subgroup*

$$\mathrm{Inn}(N) \leqslant P \leqslant \mathrm{Aut}(N)$$

such that $P = AB$ is factorized by some solvable subgroups A, B that satisfy $A \cap B = 1$, $A \cdot \mathrm{Inn}(N) = B \cdot \mathrm{Inn}(N)$, and A splits over the intersection $A \cap \mathrm{Inn}(N)$, then (G, N) is realizable for some solvable group G.

The converse of Theorem 1 does not hold in general, but we have a very nice criterion and here is our main result.

Theorem 3 *Let* N *be a finite almost simple group whose socle* $\mathrm{Soc}(N)$ *is isomorphic to one of the non-abelian simple groups in Theorem 1. There is a solvable group* G *such that* (G, N) *is realizable if and only if one of the following conditions holds:*

(1) $\mathrm{Soc}(N) \simeq \mathrm{PSL}_2(q)$ *with* $q \neq 2, 3$ *a prime power;*

(2) $\mathrm{Soc}(N) \simeq \mathrm{PSL}_3(3)$, $\mathrm{PSL}_3(8)$, $\mathrm{PSU}_4(2)$, M_{11}*;*

(3) $\mathrm{Soc}(N) \simeq \mathrm{PSL}_3(4)$ *with* $[N : \mathrm{Soc}(N)] \neq 2, 4$*;*

(4) $\mathrm{Soc}(N) \simeq \mathrm{PSL}_3(4)$ *with* $[N : \mathrm{Soc}(N)] = 2$ *and* $N \trianglelefteq \mathrm{Aut}(\mathrm{Soc}(N))$*;*

(5) $\mathrm{Soc}(N) \simeq \mathrm{PSU}_3(8)$ *with* $[N : \mathrm{Soc}(N)] \neq 2, 6$*;*

(6) $\mathrm{Soc}(N) \simeq \mathrm{PSU}_3(8)$ *with* $[N : \mathrm{Soc}(N)] = 6$ *and* $N \trianglelefteq \mathrm{Aut}(\mathrm{Soc}(N))$.

Remark 4 Our result yields a complete classification of the finite almost simple groups that can occur as the type of a Hopf–Galois structure on a solvable extension, or equivalently, the additive group of a skew brace having a solvable multiplicative group.

By definition, an almost simple group N corresponds to a subgroup of the outer automorphism group of its socle $\mathrm{Soc}(N)$. Let us note that

$$\mathrm{Out}(\mathrm{PSL}_3(3)) \simeq \mathrm{C}_2,\ \ \mathrm{Out}(\mathrm{PSL}_3(4)) \simeq \mathrm{D}_{12},\ \ \mathrm{Out}(\mathrm{PSL}_3(8)) \simeq \mathrm{C}_6,$$

$$\mathrm{Out}(\mathrm{PSU}_3(8)) \simeq \mathrm{C}_3 \times \mathrm{S}_3,\ \ \mathrm{Out}(\mathrm{PSU}_4(2)) \simeq \mathrm{C}_2,\ \ \mathrm{Out}(\mathrm{M}_{11}) \simeq \mathrm{C}_1.$$

Moreover, for a prime power $q = p^f$ with $q \neq 2, 3$, we have

$$\mathrm{Out}(\mathrm{PSL}_2(q)) \simeq \mathrm{C}_{\gcd(2, q-1)} \times \mathrm{C}_f.$$

Here, as usual C_n is the cyclic group of order n, D_{2n} is the dihedral group of order $2n$, and S_n is the symmetric group on n letters (see for example [10]).

Therefore, the converse of Theorem 1 holds with only five exceptions of N, as follows. Here, only the isomorphism class of N matters, so it suffices to consider the subgroups of $\mathrm{Out}(\mathrm{Soc}(N))$ up to conjugacy.

- The subgroups $\mathrm{PSL}_3(4) \leqslant N \leqslant \mathrm{Aut}(\mathrm{PSL}_3(4))$ corresponding to

$$\langle s \rangle, \ \langle rs \rangle, \ \langle r^3, s \rangle.$$

  Note that $\langle r^3 \rangle$ is also a subgroup of D_{12} of order 2, but this is normal and so falls under case (4) of Theorem 3. Here r and s are the usual generators of D_{12} with $r^6 = s^2 = 1$ and $srs = r^{-1}$.

- The subgroups $\mathrm{PSU}_3(8) \leqslant N \leqslant \mathrm{Aut}(\mathrm{PSU}_3(8))$ corresponding to

$$\{1\} \times \langle (1\,2) \rangle \text{ and } C_3 \times \langle (1\,2) \rangle.$$

  Note that $\{1\} \times S_3$ is also a subgroup of $C_3 \times S_3$ of order 6, but this is normal and so falls under case (6) of Theorem 3.

We now move on and use Proposition 2 to prove Theorem 3. We use the help of Magma [1] except for the infinite family $\mathrm{PSL}_2(q)$ with $q \neq 2, 3$.

2 Proof of cases (2) to (6)

We ran the following code in Magma [1].

```
T:=(the non-abelian simple group in question);
AutT:=PermutationGroup(AutomorphismGroup(T));
InnT:=Socle(AutT);
NN:=[N`subgroup:N in Subgroups(AutT)|InnT subset N`subgroup];
//A list of the finite almost simple groups N with socle T
//up to conjugacy class in Aut(T).
for N in NN do
  AutN:=Normalizer(AutT,N);
  //We identify Aut(N) with the normalizer of N in Aut(T)
  //and in particular Inn(N) with N.
  PP:=[P`subgroup:P in Subgroups(AutN)|N subset P`subgroup];
  //A list of the subgroups P between Inn(N) and Aut(N)
  //up to conjugacy class in Aut(N).
  PPa:=[]; PPb:=[];
  //A list to contain the P that satisfies the conditions
  //in Proposition 2(a) and 2(b), respectively.
  for P in PP do
    SolSub:=[S`subgroup:S in SolvableSubgroups(P)];
    if exists{<A,B>:A,B in SolSub|
```

```
        #P eq #A*#B/#(A meet B) and
        sub<P|A,N> eq sub<P|B,N>} then
      Append(~PPa,P);
    end if;
    if exists{<A,B>:A,B in SolSub|
        #(A meet B) eq 1 and
        #P eq #A*#B and
        sub<P|A,N> eq sub<P|B,N> and
        HasComplement(A,A meet N)} then
      Append(~PPb,P);
    end if;
  end for;
  if IsEmpty(PPa) then
    conclusion:="false";
    //Proposition 2(a): If PPa is empty then (G,N) is not
    //realizable for any solvable group G.
    //Thus the converse of Theorem 1 is "false" for N.
  elif not IsEmpty(PPb) then
    conclusion:="true";
    //Proposition 2(b): If PPb is non-empty then (G,N) is
    //realizable for some solvable group G.
    //Thus the converse of Theorem 1 is "true" for N.
  else
    conclusion:="inconclusive";
    //Proposition 2 is not sufficient to determine if the
    //converse of Theorem 1 holds for N.
  end if;
  if IsNormal(AutT,N) then
    normalORnot:="normal";
  else
    normalORnot:="not normal";
  end if;
  <#N/#InnT,normalORnot,conclusion>;
end for;
```

For $T = PSL_3(3)$, $PSL_3(8)$, $PSU_4(2)$, M_{11}, the output of `conclusion` is all `true` and this yields case (2) of Theorem 3.

For $T = PSL_3(4)$ and $[N : Soc(N)] \neq 2, 4$, the output of `conclusion` is all `true` and this yields case (3) of Theorem 3.

For $T = PSL_3(4)$ and $[N : Soc(N)] = 2, 4$, the output is as follows:

```
<2, "normal", "true">
<2, "not normal", "false">
<2, "not normal", "false">
```

```
<4, "not normal", "false">
```

We then deduce case (4) of Theorem 3.

For $T = PSU_3(8)$ and $[N : Soc(N)] \neq 1, 2, 6$, the output of `conclusion` is all `true` and this yields case (5) of Theorem 3 except when $N \simeq PSU_3(8)$, which is already covered by Theorem 1. Let us remark that the output of `conclusion` is `inconclusive` in this case and [8] dealt with it using a slightly different method.

For $T = PSU_3(8)$ and $[N : Soc(N)] = 2, 6$, the output is as follows:

```
<2, "not normal", "false">
<6, "normal", "true">
<6, "not normal", "false">
```

We then deduce case (6) of Theorem 3.

3 Proof of case (1)

Let $q = p^f$ be a prime power with $q \neq 2, 3$ and let

$$PSL_2(q) \leqslant N \leqslant Aut(PSL_2(q)).$$

Since $Out(PSL_2(q))$ is abelian, N is normal in $Aut(PSL_2(q))$, so we may identify $Aut(N)$ with $Aut(PSL_2(q))$, and in particular $Inn(N)$ with N. By Proposition 2 (b), it is then enough to show that there is a subgroup

$$N \leqslant P \leqslant Aut(PSL_2(q))$$

for which there exist solvable subgroups A, B of P satisfying

$$P = AB,\ A \cap B = 1,\ AN = BN,\ \text{and } A \text{ splits over } A \cap N. \tag{3.1}$$

Note that the last two conditions are trivial when P is taken to be N, since then $AN = N = BN$ and A obviously splits over $A \cap N = A$.

We may regard $PSL_2(q)$ as a normal subgroup of $PGL_2(q)$ via the natural embedding, and in particular $PGL_2(q)$ as a subgroup of $Aut(PSL_2(q))$ acting on $PSL_2(q)$ via conjugation. It is well-known that

$$Aut(PSL_2(q)) = PGL_2(q) \rtimes F, \tag{3.2}$$

where $F \simeq C_f$ is the subgroup consisting of the automorphisms induced by the field automorphisms of $\mathbb{F}_{p^f}$ over $\mathbb{F}_p$. By the proof of [8, Theorem 1.3], we know that there are solvable subgroups C, D of $\mathrm{PGL}_2(q)$ such that

$$\mathrm{PGL}_2(q) = CD, \;\; C \cap D = 1, \;\; C \cdot \mathrm{PSL}_2(q) = D \cdot \mathrm{PSL}_2(q).$$

Explicitly, we may take $C = \widetilde{C}/Z$ and $D = \widetilde{D}/Z$, where

$$\widetilde{C} = \left\{ \begin{bmatrix} x & -dy \\ y & x - cy \end{bmatrix} : x, y \in \mathbb{F}_q, \, (x, y) \neq (0, 0) \right\}$$

and

$$\widetilde{D} = \left\{ \begin{bmatrix} u & v \\ 0 & w \end{bmatrix} : u, w \in \mathbb{F}_q^\times, \, v \in \mathbb{F}_q \right\}.$$

Here Z denotes the center of $\mathrm{GL}_2(q)$ and $X^2 + cX + d$ is the minimal polynomial over $\mathbb{F}_q$ of some generator of $\mathbb{F}_{q^2}^\times$. Observe that

$$\theta \cdot \begin{bmatrix} x & y \\ z & w \end{bmatrix} Z \cdot \theta^{-1} = \begin{bmatrix} \theta(x) & \theta(y) \\ \theta(z) & \theta(w) \end{bmatrix} Z$$

in the group (3.2) for all $\theta \in F$ and $\left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right] \in \mathrm{GL}_2(q)$. It in particular implies that D is normalized by F. Thus, we have that $DE = D \rtimes E$ is a subgroup of $\mathrm{Aut}(\mathrm{PSL}_2(q))$ for any subgroup E of F. In what follows, let us take E to be the projection of N onto F along $\mathrm{PGL}_2(q)$, and let

$$P = \mathrm{PGL}_2(q) \rtimes E.$$

Clearly P contains N. For the choices of A, B, we separate into cases.

First suppose that $q \equiv 0 \pmod 4$. Then $\mathrm{PGL}_2(q) = \mathrm{PSL}_2(q)$ and so

$$N = \mathrm{PGL}_2(q) \rtimes E = P.$$

Take $(A, B) = (C, D \rtimes E)$. That A, B are solvable, $P = AB$, and $A \cap B = 1$ are all clear. The last two conditions in (3.1) are trivial since $P = N$.

Next suppose that $q \equiv 1, 3 \pmod 4$. It was shown in [8, Section 4] that

$$\begin{cases} C \text{ splits over } C \cap \mathrm{PSL}_2(q) & \text{when } q \equiv 1 \pmod 4, \\ D \text{ splits over } D \cap \mathrm{PSL}_2(q) & \text{when } q \equiv 3 \pmod 4. \end{cases} \tag{3.3}$$

Here we shall take

$$(A, B) = \begin{cases} (C, D \rtimes E) & \text{when } q \equiv 1 \pmod 4, \\ (D \rtimes E, C) & \text{when } q \equiv 3 \pmod 4. \end{cases}$$

That A, B are solvable, $P = AB$, and $A \cap B = 1$ are all obvious. Since

$$C \cdot \mathrm{PSL}_2(q) = D \cdot \mathrm{PSL}_2(q) \text{ and } \mathrm{PSL}_2(q) \leqslant N,$$

we clearly have $CN = DN$. Note that $\mathrm{PGL}_2(q) = \mathrm{PSL}_2(q)D$ holds because D contains an element lying outside of $\mathrm{PSL}_2(q)$, for example

$$\begin{bmatrix} u & 0 \\ 0 & 1 \end{bmatrix} Z, \text{ where } u \in \mathbb{F}_q^\times \setminus (\mathbb{F}_q^\times)^2.$$

By definition, elements of E may be represented as $\pi\eta$ for $\pi \in \mathrm{PGL}_2(q)$ and $\eta \in N$. Since N contains $\mathrm{PSL}_2(q)$, we then deduce that E lies in

$$\mathrm{PGL}_2(q)N = \mathrm{PSL}_2(q)DN = DN.$$

Thus, we have $(D \rtimes E)N = DN = CN$ and this yields $AN = BN$. Finally, we check that A indeed splits over $A \cap N$.

- $q \equiv 1 \pmod 4$: Here $A = C$. Since $A \leqslant \mathrm{PGL}_2(q)$, we have

  $$A \cap N = \begin{cases} A \cap \mathrm{PSL}_2(q) & \text{if } N \cap \mathrm{PGL}_2(q) = \mathrm{PSL}_2(q), \\ A & \text{if } N \cap \mathrm{PGL}_2(q) = \mathrm{PGL}_2(q). \end{cases}$$

  In the former case A splits over $A \cap N$ by (3.3), and in the latter case A certainly splits over $A \cap N = A$.

- $q \equiv 3 \pmod 4$: Here $A = D \rtimes E$. Since $q = p^f$, the exponent f must be odd in this case, and so

  $$\mathrm{Out}(\mathrm{PSL}_2(q)) \simeq C_2 \times C_f \simeq C_{2f}$$

  is cyclic. We then see that there are only two possibilities for N, namely

  $$N = \mathrm{PSL}_2(q) \rtimes E \text{ or } N = \mathrm{PGL}_2(q) \rtimes E.$$

  In the latter case $N = P$ and A certainly splits over $A \cap N = A$.

In the former case, we observe that

$$A \cap N = (D \rtimes E) \cap (\mathrm{PSL}_2(q) \rtimes E) = (D \cap \mathrm{PSL}_2(q)) \rtimes E$$

and in particular

$$[A : A \cap N] = [D : D \cap \mathrm{PSL}_2(q)].$$

Here, instead of applying (3.3) directly, we shall need to use its proof given in [8, Section 4]. It was shown by noting that

$$[D : D \cap \mathrm{PSL}_2(q)] = 2, \ \ |D \cap \mathrm{PSL}_2(q)| = \frac{q(q-1)}{2}$$

and by using the Schur–Zassenhaus theorem. But then we have

$$[A : A \cap N] = 2, \ \ |A \cap N| = \frac{q(q-1)}{2} \cdot |E|.$$

Since $|E|$, being a divisor of f, is odd in this case, we can similarly use the Schur–Zassenhaus theorem to deduce that A splits over $A \cap N$.

In both cases, we have shown that A splits over $A \cap N$ for our choice of A.

We have thus verified the existence of P satisfying (3.1) in all cases. This proves case (1) of Theorem 3.

REFERENCES

[1] W. Bosma – J. Cannon – C. Playoust: "The Magma algebra system I: The user language", *J. Symbolic Comput.* 24 (1997), 235–265.

[2] N.P. Byott: "Uniqueness of Hopf Galois structure for separable field extensions", *Comm. Algebra* 24 (1996), 3217–3228, 3705.

[3] N.P. Byott: "On insoluble transitive subgroups in the holomorph of a finite soluble group", *J. Algebra* 638 (2024), 1–31.

[4] L.N. Childs: "Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory", *American Mathematical Society*, Providence, RI (2000).

[5] C. Greither – B. Pareigis: "Hopf Galois theory for separable field extensions", *J. Algebra* 106 (1987), 239–258.

[6] L. Guarnieri – L. Vendramin: "Skew braces and the Yang–Baxter equation", *Math. Comp.* 86 (2017), 2519–2534.

[7] A. Smoktunowicz – L. Vendramin: "On skew braces (with an appendix by N. Byott and L. Vendramin)", *J. Comb. Algebra* 2 (2018), 47–86.

[8] C. Tsang: "Non-abelian simple groups which occur as the type of a Hopf–Galois structure on a solvable extension", *Bull. London Math. Soc.* 55 (2023), 2324–2340.

[9] C. Tsang – C. Qin: "On the solvability of regular subgroups in the holomorph of a finite solvable group", *Int. J. Algebra Comput.* 30 (2020), 253–265.

[10] R.A. Wilson: "The Finite Simple Groups", *Springer*, London (2009).

Cindy (Sin Yi) Tsang
Department of Mathematics
Ochanomizu University
2-1-1 Otsuka, Bunkyo-ku
Tokyo (Japan)
e-mail: tsang.sin.yi@ocha.ac.jp



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 13–25 ISSN: 2499-1287
DOI: 10.32037/agta-2026-002

Finite Groups in which every Subgroup of Order Divisible by p is Normal

Khaled A. Al-Sharo — Tuval Foguel

(*Received Mar. 27, 2024; Accepted June 24, 2024 — Communicated by Martyn R. Dixon*)

Abstract

The article introduces two generalizations of Dedekind groups known as ${}_{pd}$Ddk-groups and ${}_{pd}$qHm-groups. In ${}_{pd}$Ddk-groups, subgroups with sizes that are multiples of a given prime p are normal, while in ${}_{pd}$qHm-groups, these subgroups are permutable. It is initially established that these groups belong to either p'-groups or supersolvable groups. It then proceeds to classify ${}_{pd}$Ddk-groups and ${}_{pd}$qHm-groups. The article concludes with a discussion of minimal non-${}_{pd}$Ddk-groups.

Mathematics Subject Classification (2020): 20D10, 20D15

Keywords: supersolvable group; nilpotent group; Dedekind group; quasi-Hamiltonian group; T-group; PT-group

1 Introduction

In this paper, our focus is solely on groups of finite order. Groups in which every subgroup is normal are termed Dedekind groups, and the non-abelian ones are referred to as Hamiltonian groups. The complete characterization of Dedekind groups and Hamiltonian groups was accomplished by R. Dedekind, E. Wendt, and R. Baer (see [1] and [4]).

Recall that two subgroups H and K are said to *permute* in G if

$$HK = KH.$$

A subgroup H is called permutable in G if H permutes with every subgroup of G. Besides, K. Iwasawa generalized the concept of Hamiltonian groups by looking at quasi-Hamiltonian groups, i.e. groups in which every subgroup is permutable and he classified all such finite groups in [8, Theorem 4].

Subsequent to this, numerous papers have delved into generalizations of this result. Two noteworthy contributions include the work of O.Y. Schmidt, who, in [12] and [13], was the first to study finite groups by imposing restrictions on their non-normal subgroups. He specifically examined the structure of finite groups where the non-normal subgroups either form a conjugacy class or constitute the union of two conjugacy classes.

E. Crestani [3] achieved a classification for all finite groups whose non-permutable subgroups have the same order and those that have a single conjugacy class of non-permutable subgroups.

In this article, we investigate two new extensions of Dedekind groups, referred to as ${}_{pd}$Ddk-groups and ${}_{pd}$qHm-groups. If p is a fixed prime number, in ${}_{pd}$Ddk-groups we specify that every subgroup whose order is divisible by p must be normal. Furthermore, in ${}_{pd}$qHm-groups, such subgroups are merely required to be permutable. At the beginning, it is established that these groups fall into either p'-groups or supersolvable groups. The article concludes with a classification of ${}_{pd}$Ddk-groups and ${}_{pd}$qHm-groups.

Before proceeding further, it is necessary to introduce some notation. Let n be a natural number; we denote by $\pi(n)$ the set of prime divisors of n. For a group G, we define $\pi(G) = \pi(|G|)$. Additionally, we say that a group G is a p'-group if $p \notin \pi(G)$.

Definition 1 Given a prime p, we call a subgroup H of a group G a pd-*subgroup* if $p \in \pi(H)$.

Definition 2 A group G is called ${}_{pd}$Ddk-*group* for p a prime if every pd-subgroup of G is normal in G.

Definition 3 A group G is called ${}_{pd}$qHm-*group* for p a prime if every pd-subgroup of G is permutable in G.

Remark 4 Every ${}_{pd}$Ddk-group is clearly a ${}_{pd}$qHm-group.

Remark 5 Every Dedekind group is clearly a ${}_{pd}$Ddk-group, and every quasi-Hamiltonian group is clearly a ${}_{pd}$qHm-group.

Remark 6 Every p′-group is a $_{pd}$Ddk-group and a $_{pd}$qHm-group. We will say that G is trivial $_{pd}$Ddk-group or trivial $_{pd}$qHm-group for such a group.

Example 7 For any prime p, p′-groups and Dedekind groups are examples of $_{pd}$Ddk-groups. Moreover, p′-groups, abelian group and quasi-Hamiltonian groups are examples of $_{pd}$qHm-groups.

Remark 8 A p-group need not be $_{pd}$Ddk-group or $_{pd}$qHm-group. Indeed, the dihedral group of order 8 is an example of 2-group that is not $_{2d}$Ddk-group.

The goal of this paper is to offer a classification of $_{pd}$Ddk-groups and $_{pd}$qHm-groups.

2 Auxiliary results

To initiate our exploration, we lay the groundwork by establishing foundational facts concerning $_{pd}$Ddk-groups and $_{pd}$qHm-groups.

Lemma 9 *If* G *is a* $_{pd}$*Ddk-group* (*respectively a* $_{pd}$*qHm-group*), *then* G *satisfies the following properties*:

(i) *every subgroup of* G *is* $_{pd}$*Ddk-group* (*respectively* $_{pd}$*qHm-group*). *In particular, the class of* $_{pd}$*Ddk-groups* (*respectively* $_{pd}$*qHm-groups*) *is closed for subgroups;*

(ii) *every factor group of* G *is* $_{pd}$*Ddk-group* (*respectively* $_{pd}$*qHm-group*). *In particular, the class of* $_{pd}$*Ddk-groups* (*respectively* $_{pd}$*qHm-groups*) *is closed for homomorphic images.*

Proof — (i) Let H be a subgroup of a $_{pd}$Ddk-group G and H_1 be a pd-subgroup in H. Then H_1 is pd-subgroup in G. Because G is $_{pd}$Ddk-group, H_1 must be normal in G. Therefore, H_1 is normal in H and hence H itself is a $_{pd}$Ddk-group.

(ii) Let N be a normal subgroup of a $_{pd}$Ddk-group G and let H be a pd-subgroup in G/N. Then, by the correspondence theorem, there exists a pd-subgroup H^* in G such that $H = H^*/N$. Since, by assumption, G is $_{pd}$Ddk-group, H^* must be normal in G. Therefore, H is normal in G and hence G/N itself is $_{pd}$Ddk-group.

The proof for $_{pd}$qHm-groups is basically identical to the proof above with replacing $_{pd}$Ddk-group by $_{pd}$qHm-group and normal subgroup by permutable subgroup. □

The direct product of two $_{pd}$Ddk-groups or $_{pd}$qHm-groups may not always result in a $_{pd}$Ddk-group or $_{pd}$qHm-group, as shown in the following example.

Example 10 Consider the group

$$G = \langle x, y : x^9 = y^3 = e, x^y = x^5 \rangle,$$

isomorphic to the semidirect product of a cyclic group of order 9 and a cyclic group of order 3. With an order of 27, G is a $_{2d}$Ddk-group. Moreover, the cyclic group $H = Z_2$ of order 2 is also a $_{2d}$Ddk-group. Now, by forming the group $D = G \times H$, the subgroup

$$S = \langle y \rangle \times H$$

emerges as a 2d-subgroup of D, yet it fails to be permutable within D.

3 Nontrivial $_{pd}$Ddk and $_{pd}$qHm-groups

In this section, we present results that establish significant properties of $_{pd}$Ddk-groups and $_{pd}$qHm-groups. This includes proving that nontrivial $_{pd}$Ddk-groups and $_{pd}$qHm-groups are supersolvable.

Theorem 11 *If* G *is a nontrivial* $_{pd}$*qHm-group, then* G *is supersolvable.*

Proof — Assume that G is a nontrivial $_{pd}$qHm-group, and let M be maximal subgroup of G.

Case 1: If $p \in \pi(M)$, then M is a permutable group and since it is also maximal by [11, 13.2.1], M is a normal subgroup that is also maximal, thus has prime index.

Case 2: If $p \notin \pi(M)$. Let $x \in G$ of order p and $N = \langle x \rangle$, since G is a nontrivial $_{pd}$Ddk-group N is permutable in G. Therefore M is a proper subgroup of $MN = G$ and thus the index of M in G is p.

So, based on both cases, any maximal subgroup M of G has prime index and hence, by Huppert's theorem [7], G is supersolvable. □

Corollary 12 *If* G *is nontrivial* ${}_{pd}$*Ddk-group, then* G *is supersolvable.*

Proof — Every ${}_{pd}$Ddk-group is a ${}_{pd}$qHm-group. □

Lemma 13 *If* $|G| = pq$ *where* p *and* q *are primes and* $p \geqslant q$*, then* G *is a* ${}_{pd}$*Ddk-group.*

Proof — If $p = q$, then G is abelian. Thus we may suppose $p > q$ in which case the Sylow p-subgroup of G is normal in G and the only other pd-subgroup is G itself. Hence, the result follows. □

Remark 14 The Dicyclic group of order 12 given by the presentation

$$\mathrm{Dic}_{12} = \left\langle a, x \mid a^6 = x^4 = 1,\ xax = a^{-1} \right\rangle$$

is a nontrivial non-Dedekind ${}_{pd}$Ddk-groups which is not of order pq.

Theorem 15 *If* G *is a nontrivial* ${}_{pd}$*Ddk-group with* $p = \min(\pi(G))$*, then* G *is a Dedekind group.*

Proof — Assume that G is a nontrivial ${}_{pd}$Ddk-group with

$$p = \min(\pi(G)),$$

and let H be a p'-subgroup of G, and $x \in G$ an element of order p. Let $K = \langle x \rangle H$. Note that $\langle x \rangle$ is normal in K and H having index

$$p = \min(\pi(K))$$

in K so is also normal by [10]. Therefore

$$K \simeq \langle x \rangle \times H$$

and H is characteristic in K, thus normal in G. Hence G is a Dedekind group. □

Remark 16 Note that, by Remark 8, not all supersolvable groups are ${}_{pd}$Ddk-groups. Also by Theorem 15 we see that, if $p \neq 2$ is a prime, then a nonabelian p-group is never a ${}_{pd}$Ddk-groups and note that such a group is nilpotent and thus supersolvable.

Theorem 17 *If* G *is a nontrivial* ${}_{pd}$*qHm-group with* $p = \min(\pi(G))$*, then* G *is a quasi-Hamiltonian group.*

Proof — Assume that G is a nonabelian nontrivial ${}_{pd}$qHm-group with $p = \min(\pi(G))$, and let H be a p'-subgroup of G. Now let J be a subgroup of G we will look at two cases.

Case 1: If $p \in \pi(J)$, then J is a permutable subgroup and $JH = HJ$.

Case 2: If $p \notin \pi(J)$, let $x \in G$ of order p and let $K = \langle x \rangle H$. Note that K is a subgroup since $\langle x \rangle$ is a permutable subgroup. Also note that since $\langle x \rangle$ is a permutable Sylow subgroup of K it is normal in K and H having index

$$p = \min(\pi(K))$$

in K is also normal by [10]. Therefore $K \simeq \langle x \rangle \times H$ and H is characteristic in K. Since $p \mid |K|$, K is permutable in G. Thus KJ is a subgroup of G. Using the same argument as above we see that

$$KJ = \langle x \rangle \times HJ.$$

Therefore HJ is a subgroup of G. So H is permutable in G. Hence G is a quasi-Hamiltonian group. □

4 Classification

In this section, we classify ${}_{pd}$Ddk-groups and ${}_{pd}$qHm-groups.

Corollary 18 *If* G *is a* ${}_{2d}$*qHm-group, then* G *is a Dedekind group or a* $2'$*-group.*

Proof — For a nontrivial ${}_{2d}$Ddk-group G, we observe that

$$2 = \min(\pi(G)),$$

and therefore, by Theorem 15, G is a Dedekind group. □

Corollary 19 *If* G *is a* ${}_{2d}$*Ddk-group, then* G *is a quasi-Hamiltonian group or a* $2'$*-group.*

Proof — Assume that G is a nontrivial ${}_{2d}$qHm-group and note that $2 = \min(\pi(G))$. Therefore, by Theorem 17, G is an abelian or a quasi-Hamiltonian group. □

Corollary 20 *If* G *is a* ${}_{2d}$*qHm-group, then* G *a solvable group.*

If G is a $2'$-group, then, by the Feit–Thompson Theorem [5], it is a solvable ${}_{2d}$qHm-group. Moreover, if $2 \in \pi(G)$, then G is solvable from Corollary 19.

Theorem 21 *Let* G *be a group. Then* G *is a* ${}_{pd}$*Ddk-group for* p *an odd prime if and only if* G *is isomorphic to one of the following groups*:

(1) *a* p'*-group,*

(2) *a Dedekind group,*

(3) $P \rtimes Q$ *where* P *is a cyclic subgroup of order* p *and* Q *is a* p'*-Dedekind group and* Q *acts as a group of nontrivial power automorphisms on* P*.*

Proof — Let G be a nontrivial ${}_{pd}$Ddk-group with p an odd prime. It is worth noting that the Sylow p-subgroup P of G is normal. We note that P is Dedekind, hence abelian. Since G is solvable, according to Theorem 11, we can deduce from the Schur–Zassenhaus Theorem (see [11, 9.1.2]) that G can be expressed as the semidirect product

$$G = P \rtimes Q,$$

where Q is a Hall p'-complement of P. Additionally, observe that all complements of P in G are conjugate. Also note that since $Q \simeq G/P$ it must be a Dedekind group. Lets look at two cases.

Case 1: If P is not cyclic, then there exist elements x and y in P of order p, and $\langle x\rangle \cap \langle y\rangle = \{1\}$. Let H be a subgroup of G. We can assume that H is a p'-group, as otherwise, it is normal by definition. Furthermore, by definition, $\langle x\rangle H$ and $\langle y\rangle H$ are both normal in G. Consequently, $H = \langle x\rangle H \cap \langle y\rangle H$ is normal in G. Thus, G is a Dedekind group.

Case 2: If $P = \langle x\rangle$ is cyclic, then G can be represented as

$$G = P \rtimes Q,$$

where Q is a p'-Dedekind group. It is important to note that Q acts as power automorphisms on P since P is cyclic. Now assume

$$|P| = p^n > p,$$

and let $z \in P$ be an element of order p^2 and $r \in Q$ an element of prime order that acts nontrivially on x. Note that r will also act nontrivially

on z. Note that class of r in $P\langle r\rangle$ is

$$Cl_{P\langle r\rangle}(r) = \{r, xr, \dots, x^{p^n-1}r\} \subset Cl_G(r)$$

which is not a subset of $H = \langle z^p\rangle\langle r\rangle$. Thus $\langle r\rangle$ is not normal, a contradiction.

Now assume that

$$G = P \rtimes Q$$

where $P = \langle x\rangle$ is a cyclic subgroup of order p and Q is a p'-Dedekind group and Q acts as a nontrivial power automorphisms on P. Let

$$P \neq H \leqslant G$$

with $p \in \pi(H)$, since P is the unique subgroup of order p, $P \leqslant H$ and H/P is a subgroup of G/P which is Dedekind, thus H/P is normal in G/P. Therefore H is normal in G. □

Remark 22 A T-group, as defined, is a group where the property of normality is transitive. In 1957, W. Gaschütz provided a description of soluble T-groups, see [6]. These groups, denoted by G, have a nilpotent residual that is an abelian Hall subgroup L of odd order, satisfying the conditions that G/L is Dedekind and G normalizes every subgroup of L. Note also that, Gaschütz's results, along with Corollary 19 and Theorem 21, lead to the conclusion in Corollary 23.

Corollary 23 *If* G *is a nontrivial* $_{pd}$*Ddk-group, then* G *is a* T*-group.*

Remark 24 A PT-group, by definition, is a group where the property of permutability is transitive. In 1964, G. Zacher provided a description of soluble PT-groups, see [2] and [15]. These groups, denoted by G, have a nilpotent residual that is an abelian Hall subgroup L of odd order, satisfying the conditions that G/L is abelian or a quasi-Hamiltonian and G normalizes every subgroup of L.

Lemma 25 *Let* G *be a group. If* G *is a nontrivial, nonabelian and non-quasi-Hamiltonian* $_{pd}$*qHm-group with* p *an odd prime, then*

$$G = P \rtimes Q$$

where P *is an abelian* p*-group and* Q *is an abelian or a quasi-Hamiltonian* p'*-group which acts as a nontrivial power automorphisms on* P*. In particular* G *is a metanilpotent supersovable group.*

Proof — Consider a nontrivial, nonabelian, and nonquasi-Hamiltonian $_{pd}$qHm-group G, where p is an odd prime. Hence, the Sylow p-subgroup P of G is normal because it is a permutable Sylow subgroup. Since G is solvable according to Theorem 11, we can deduce from the Schur–Zassenhaus Theorem (see [11, 9.1.2]) that G can be expressed as the semidirect product

$$G = P \rtimes Q,$$

where Q is a Hall p'-complement of P. Additionally, observe that all complements of P in G are conjugate.

Besides, note that P is a $_{pd}$qHm-group, making it a quasi-Hamiltonian p-group. Moreover, it is important to observe that by correspondence theorem, Q is also a quasi-Hamiltonian or an abelian p'-group. Consequently, G is metanilpotent, and by Theorem 11, it is also supersolvable. Now, let $x \in P$ and H a complement of P in G. Note that $\langle x \rangle$ is a permutable subgroup and

$$\big(|\langle x \rangle|, |H|\big) = 1,$$

thus, by [11],

$$H \leqslant N_G\big(\langle x \rangle\big).$$

Therefore Q acts as a nontrivial power automorphisms on P.

Note that, by [8] and [14], if P is not abelian, then

$$P = \langle x, A \rangle$$

where A is an abelian p-group $\langle x \rangle$ is a cyclic p-group and

$$a^x = a^{1+p^r},$$

for any $a \in A$. Thus the normal subgroups of P are P and all the subgroups of A. Now, since Q acts as power automorphisms on P, all the normal subgroups of P are normal in G. Thus, by [2, Lemma 1], it follows that G is a PT-group Therefore, by [15], P is abelian. □

Corollary 26 *If* G *is a nontrivial* $_{pd}$*qHm-group, then* G *is a* PT*-group.*

Proof — Zacher's results [2] and [15], along with Corollary 18 and Lemma 25 prove the claim. □

Theorem 27 *Let* G *be a group. Then* G *is a* ${}_{pd}qHm$*-group, for* p *an odd prime, if and only if* G *is isomorphic to one of the following groups*:

(1) *a* p'*-group,*

(2) *a quasi-Hamiltonian group,*

(3) $P \rtimes Q$ *where* P *is a cyclic* p*-group of order* p *and* Q *is an abelian or a quasi-Hamiltonian* p'*-group which acts as a nontrivial power automorphisms on* P*.*

Proof — Consider a nontrivial, nonabelian, and nonquasi-Hamiltonian ${}_{pd}$qHm-group G, where p is an odd prime. By Lemma 25,

$$G = P \rtimes Q$$

where P is an abelian p-group and Q is an abelian or a quasi-Hamiltonian p'-group which acts as a nontrivial group of power automorphisms on P.

Assume that P is not cyclic, then there exist elements x and y in P of order p, and $\langle x\rangle \cap \langle y\rangle = \{1\}$. Let H be a subgroup of G. We can assume that H is a p'-group, as otherwise, it is permutable by definition. Furthermore, by definition, $\langle x\rangle H$ and $\langle y\rangle H$ are both permutable in G. Let

$$K = \langle x\rangle\langle y\rangle H.$$

Since $\langle x\rangle H$ and $\langle y\rangle H$ are maximal permutable subgroups of K they are normal in K. Consequently,

$$H = \langle x\rangle H \cap \langle y\rangle H$$

is normal in K. Thus, since G is a PT-group, H is permutable in G and G is quasi-Hamiltonian.

Now assume that $P = \langle x\rangle$ is cyclic, $|P| = p^n > p$, and let $z \in P$ be an element of order p^{n-1} and $r \in Q$ an element of prime order that acts nontrivially on x. Note that r will also act nontrivially on z. The subgroup

$$H = \langle z\rangle\langle r\rangle$$

is permutable in G, thus it is permutable and maximal in $P\langle r\rangle$, i.e. it is normal in $P\langle r\rangle$.

Note that class of r is

$$Cl_{P\langle r\rangle}(r) = \left\{r, xr, \ldots, x^{p^n-1}r\right\}$$

is not a subset of $H = \langle z \rangle \langle r \rangle$, thus it is not normal, a contradiction.

Now assume that $G = P \rtimes Q$, where $P = \langle x \rangle$ is a cyclic subgroup of order p and Q is a quasi-Hamiltonian p'-group which acts as a nontrivial power automorphisms on P. Let

$$P \neq H \leqslant G$$

with $p \in \pi(H)$. Since P is the unique subgroup of order p, $P \leqslant H$. Moreover, H/P is a subgroup of G/P which is a quasi-Hamiltonian, thus H/P is permutable in G/P. Therefore H is permutable in G. □

Remark 28 Observe that, while it is true that every ${}_{pd}$Ddk-group is a ${}_{pd}$qHm-group (every T-group is a PT-group), the converse is not necessarily true. For example, any quasi-Hamiltonian p-group, for an odd prime p, is a ${}_{pd}$qHm-group and a PT-group, but it is not a ${}_{pd}$Ddk-group or a T-group.

It is also important to note that one can find PT-groups with a non-cyclic Hall subgroup of odd order divisible by a prime p. Such a group will not be a ${}_{pd}$qHm-group according to Theorem 27. Additionally, consider the Suzuki group $Sz(q)$, which has order

$$q^2(q-1)(q^2+1)$$

and is not divisible by 3. Therefore, it is a ${}_{3d}$qHm but not a PT-group.

5 Minimal non ${}_{pd}$Dedekind-groups

In this section, we introduce the critical $\mathfrak{X}$-groups where $\mathfrak{X}$ is the class of all finite ${}_{pd}$Ddk-groups. In particular, we prove that a critical ${}_{2d}$Ddk-groups must be solvable. Let us initially recall the following definitions.

Definition 29 Given a class of groups $\mathfrak{X}$, a group G is called a *minimal non* $\mathfrak{X}$-group, or an $\mathfrak{X}$-*critical* group, if G is not in $\mathfrak{X}$ but all its proper subgroups are in $\mathfrak{X}$.

Definition 30 A group G is called a *minimal non* ${}_{pd}$*Ddk*-group, if G is not ${}_{pd}$Ddk-group but all its proper subgroups are ${}_{pd}$Ddk-groups.

Example 31 The alternating group A_5 is an example of minimal non ${}_{5d}$Ddk-group, since the 5d-subgroups have orders 5 and 10, and they are ${}_{5d}$Ddk-groups. Note that A_5 is simple.

Example 32 The alternating group A_4 is an example of minimal non $_{2d}$Ddk-group. Note that A_4 is solvable.

Theorem 33 *If* G *is a minimal non* $_{2d}$*Ddk-group, then* G *must be a solvable group.*

Proof — Note that a minimal non $_{2d}$Ddk-group must have even order. Let G be a minimal non $_{2d}$Ddk-group. If G has a non trivial normal subgroup N, then N is solvable by Corollary 20 and G/N is either minimal non $_{2d}$Ddk-group or a $_{2d}$Ddk-group.

Suppose, for the sake of contradiction, that there exists a nonsolvable minimal non-$_{2d}$Ddk-group G. From the previous discussion, we can assume that G is simple. Therefore, by Corollary 18, the normalizer of its Sylow 2-subgroup must be a Dedekind group, which contradicts the result in [9]. □

Acknowledgments

The authors would like to express their gratitude to the referee for their valuable comments, which played a crucial role in guiding the classification presented in this paper.

REFERENCES

[1] R. Baer: "Situation der Untergruppen und Struktur der Gruppe", *Sitz.-Ber. Heidelberg. Akad. Wiss.* 2 (1933), 12–17.

[2] J. Beidleman – B. Brewster – D.J.S. Robinson: "Criteria for permutability to be transitive in finite group", *J. Algebra* 222 (1999), 400–412.

[3] E. Crestani: "A generalization of quasi-Hamiltonian groups", *Boll. Unione Mat. Ital. Sez. B Artic. Ric. Mat.* 10 (2007), 829–842.

[4] R. Dedekind: "Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind", *Math. Ann.* 48 (1897), 548–561.

[5] W. Feit – J.G. Thompson: "Solvability of groups of odd order", *Pacific J. Math.* 13 (1963), 775–1029.

[6] W. Gaschütz: "Gruppen, in denen das Normalteilersein transitiv ist", *J. Reine Angew. Math.* 198 (1957), 87–92.

[7] B. Huppert: "Normalteiler und maximale Untergruppen endlicher Gruppen", *Math. Z.* 60 (1954), 409–434.

[8] K. Iwasawa: "On the structure of infinite M-groups", *Jap. J. Math.* 18 (1943), 709–728.

[9] A.S. Kondraťev: "Normalizers of Sylow 2-subgroups in finite simple groups", *Mat. Zametki* 78 (2005), 368–376.

[10] T.Y. Lam: "On subgroups of prime index", *Am. Math. Mon.* 111 (2004), 256–258.

[11] D.J.S. Robinson: "A Course in the Theory of Groups", *Springer*, New York 80 (1995).

[12] O.Y. Schmidt: "Groups which have one class of not invariant subgroups", *Mat. Sb.* 33 (1926), 161–172.

[13] O.Y. Schmidt: "Groups with two classes of non-normal subgroups", *Proceeding of the Group Theory Seminar* (1938), 7–26.

[14] R. Schmidt: "Subgroup Lattices of Groups", *De Gruyter*, Berlin (1994).

[15] G. Zacher: "I gruppi risolubili finiti in cui i sottogruppi di composizione coincidono con i sottogruppi quasi-normali", *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.* 8 (1964), 150–154.

Khaled A. Al-Sharo
Department of Mathematics
Al al-Bayt University
25113 Mafraq (Jordan)
e-mail: sharo_kh@yahoo.com

Tuval Foguel (*corresponding author*)
Department of Mathematics and Computer Science
Adelphi University
One South Avenue
11010 Garden City, NY (USA)
e-mail: tfoguel@adelphi.edu



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 27–62 ISSN: 2499-1287
DOI: 10.32037/agta-2026-003

Rota–Baxter Operators on Dihedral and Alternating Groups

Alexey Galt — Vsevolod Gubarev

(*Received Apr. 27, 2024; Accepted Oct. 14, 2024 — Communicated by E. Jespers*)

Abstract

Rota–Baxter operators on algebras, which appeared in 1960, have connections with different versions of the Yang–Baxter equation, pre- and postalgebras, double Poisson algebras, etc. In 2020, the notion of Rota–Baxter operator on a group was defined by L. Guo, H. Lang, Yu. Sheng.

In 2023, V. Bardakov and the second author showed that all Rota–Baxter operators on simple sporadic groups are splitting, i.e. they are defined via exact factorizations. In this work, we clarify for which n there exist non-splitting Rota–Baxter operators on the alternating group A_n. For the corresponding n, we describe all non-splitting Rota–Baxter operators on A_n. Besides, we describe Rota–Baxter operators on dihedral groups D_{2n} providing the general construction which lies behind all non-splitting Rota–Baxter operators on A_n and D_{2n}.

Mathematics Subject Classification (2020): 20D06

Keywords: Rota–Baxter operator; Rota–Baxter group; dihedral group; alternating group

1 Introduction

In 1960 [3], G. Baxter introduced the notion of Rota–Baxter operator on an algebra A as a linear operator R satisfying the relation

$$R(x)R(y) = R(R(x)y + xR(y) + \lambda xy), \tag{1.1}$$

where $x, y \in A$ and the scalar λ from the ground field F is fixed, and it is called a weight of R.

The identity (1.1) for $\lambda = 0$ may be considered as a generalization of integration by parts formula. When $\lambda \neq 0$, the canonical example is a projection of the whole algebra A on its subalgebra A_1 provided a decomposition $A = A_1 \oplus A_2$ of A into a direct vector-space sum of its subalgebras A_1, A_2.

After more than 60 years of the study, a lot of connections and applications of Rota–Baxter operators were found: with different versions of the Yang–Baxter equation [1], [6], [31], pre- and postalgebras [1], [2], [21], double Poisson algebras [17], [18], [28], etc.

Recently, in 2020 (published in 2021), the analogous notion of Rota–Baxter operator (of weight ± 1) on groups was suggested by L. Guo, H. Lang, and Yu. Sheng [22]. Since this pioneer article appeared, a dozen papers have been published, and the direction of Rota–Baxter groups is rapidly developing. On the one hand, the correspondence between Rota–Baxter operators on Lie groups and Rota–Baxter operators on Lie algebras is studied, see [22] and [24]. On the other hand, the definition of Rota–Baxter operator on groups was extended on Clifford semigroups [11], Hopf algebras [16], and others. There is a deep connection [5] between Rota–Baxter operators on groups and so called skew left braces [20], which, in turn, serve as a source of set-theoretical solutions to the quantum Yang–Baxter equation. The cohomology theory for Rota–Baxter (Lie) groups was presented in [14] and [24].

Given a group G, one has always trivial RB-operators

$$B_e \colon g \to e \quad \text{and} \quad B_{-1} \colon g \to g^{-1}.$$

The analog of the projection operator mentioned above for algebras is the following: Given an exact factorization $G = HL$, the map

$$B \colon hl \to l^{-1}$$

is a Rota–Baxter operator on G. We will call it a *splitting RB-operator*. The criterion, when a given RB-operator is a splitting one, was stated in [4]. It actually says that R is a splitting RB-operator on a group G if and only if $\mathrm{Im}(B\widetilde{B}) = 1$, where

$$\widetilde{B}\colon G \to G,\ \widetilde{B}(g) = g^{-1}B(g^{-1})$$

is another RB-operator on G defined with the help of B. Different constructions of non-splitting Rota–Baxter operators on groups were suggested therein. However, it occurs that there are no non-splitting RB-operators on all simple sporadic groups, see [4].

In the current work, we continue the mentioned in [4] direction of description of RB-operators on all finite simple groups; here we deal with alternating groups A_n. The main result is the complete classification of (non-splitting) Rota–Baxter operators on A_n. For any RB-operator B on a group G, one has a factorization

$$G = \mathrm{Im}(B) \cdot \mathrm{Im}(\widetilde{B}).$$

Thus, we may apply the known description of factorizations of finite simple groups [27]. Furthermore, we use sharply 2-transitive groups and involve the Zassenhaus theorems on them (see [23], Theorems XII.9.7 and XII.9.8). As a consequence, we show in Theorem 7.1 that there are non-splitting RB-operators R on A_n if and only if $n \in \{q^m,\ q^m + 1\}$, where:

(i) q is a prime-power.

(ii) Each prime divisor of m divides $q - 1$.

(iii) $q \equiv 3 \pmod 4$ and $m \equiv 2 \pmod 4$.

When n is so, we clarify the general construction, which lies behind R (see Lemma 5.1). Note that there is an infinite number of pairs q, m satisfying (i)–(iii).

We prove that if G is a finite group, B is an RB-operator on

it, $R = \mathrm{Im}(B\widetilde{B})$ is an abelian subgroup of G, and

$$G = H \cdot L = \mathrm{Ker}(B) \cdot \mathrm{Im}(B),$$

then $B(hl) = C(l)$ for an RB-operator C on L. Moreover, $\mathrm{Im}(\widetilde{C})$ normalizes H and C is a homomorphism from L onto its abelian subgroup isomorphic to R. We apply this result not only for alternating groups but also for dihedral ones. We show that for any non-splitting RB-operator B on A_n, we have $\mathrm{Im}(B\widetilde{B}) \simeq \mathbb{Z}_2$. Regarding to dihedral groups D_{2n}, we prove that there are no non-splitting RB-operators on D_{2n}, when n is odd. When n is even, we show that for any non-splitting RB-operator B on D_{2n}, we have either $\mathrm{Im}(B\widetilde{B}) \simeq \mathbb{Z}_2$ or $\mathrm{Im}(B\widetilde{B}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let us highlight that we suggest a new kind of equivalence on a set of Rota–Baxter operators. In [4], it was noted that given a Rota–Baxter group (G, B) and $\varphi \in \mathrm{Aut}(G)$, one has again an RB-operator $B^{(\varphi)}$ on G, which acts by the formula

$$B^{(\varphi)}(g) = \varphi^{-1} B \varphi(g).$$

Therefore, it is natural to classify Rota–Baxter operators on a group G up to such action of $\mathrm{Aut}(G)$. We present an equivalence obtained under the action of a subgroup of $\mathrm{Aut}(G \times G)$ isomorphic to

$$(\mathrm{Aut}(G) \times \mathrm{Inn}(G)) \rtimes \mathbb{Z}_2.$$

As far as we know, there is no analogous action for Rota–Baxter operators on algebras. We prove that such equivalence preserves main properties of Rota–Baxter operators, e.g. the property of splitting one. Moreover, the mentioned above construction of an RB-operator G such that $\mathrm{Im}(B\widetilde{B})$ is abelian, is preserved too. So, we find all non-splitting Rota–Baxter operators on A_n up to the equivalence.

The work is organized as follows. Firstly, we provide the required preliminaries about Rota–Baxter groups in Section 2 and about sharply doubly transitive groups in Section 3, re-

spectively. In Section 4, we define the new equivalence of RB-operators (see Proposition 4.2). In Section 5, we derive the construction of a Rota–Baxter operator B such that $R = \mathrm{Im}(B\widetilde{B})$ is abelian and $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$ (see Lemma 5.1).

In Section 6, we describe Rota–Baxter operators on dihedral groups (see Theorem 6.1). In Section 7, we classify, up to equivalence, Rota–Baxter operators on alternating groups A_n (see Theorem 7.1). In particular, for small n, we use a computer algebra system GAP [15] to compute RB-operators on A_n. We use the reformulation of a Rota–Baxter operator B in terms of its graph in $G \times G$ [24] (see Proposition 4.1) and write a program with a starting point based on the program from [30].

2 Preliminaries

Let G be a group. A map $B\colon G \to G$ is called a *Rota–Baxter operator of weight* 1 if

$$B(g)B(h) = B(gB(g)hB(g)^{-1}) \tag{2.1}$$

holds, for all $g, h \in G$ (see [22]).

Note that a notion of Rota–Baxter operator on an abelian G coincides with homomorphism.

Proposition 2.1 (see [22]) *Let* (G, B) *be a Rota–Baxter group. Then the following hold*:

(a) $\mathrm{Im}(B)$ *and* $\mathrm{Ker}(B)$ *are subgroups of* G.

(b) $B(e) = e$.

(c) $B(g)^{-1} = B(B(g)^{-1}g^{-1}B(g))$ *for every* $g \in G$.

(d) $B(h) = B(gh)$ *for all* $h \in G$ *and* $g \in \mathrm{Ker}(B)$.

Proposition 2.2 (see [22]) *Let* (G, B) *be a Rota–Baxter group. Then the following hold*:

(a) *The map* $\widetilde{B}$ *defined as* $\widetilde{B}(g) = g^{-1}B(g^{-1})$ *is a Rota–Baxter operator on* G.

(b) *If* $\varphi \in \mathrm{Aut}(G)$, *then* $B^{(\varphi)} = \varphi^{-1}B\varphi$ *is a Rota–Baxter operator on* G.

Proposition 2.3 (see [22]) *Let* $(G, \cdot, B)$ *be a Rota–Baxter group. Then the following hold*:

(a) *The pair* $(G, \circ)$ *with the product*

$$g \circ h = gB(g)hB(g)^{-1}, \quad g, h \in G, \tag{2.2}$$

is a group.

(b) *The operator* B *is a Rota–Baxter operator on the group* $(G, \circ)$.

(c) *The map* $B\colon (G, \circ) \to (G, \cdot)$ *is a homomorphism of Rota–Baxter groups.*

Hereinafter, we will denote the group $(G, \circ)$ as $G^{(\circ)}$.

Proposition 2.4 (see [22]) *If* (G, B) *is an RB-group, then the following hold*:

(a) $\mathrm{Ker}(B)$ *and* $\mathrm{Ker}(\widetilde{B})$ *are normal in* $G^{(\circ)}$.

(b) $\mathrm{Ker}(B) \trianglelefteq \mathrm{Im}(\widetilde{B})$ *and* $\mathrm{Ker}(\widetilde{B}) \trianglelefteq \mathrm{Im}(B)$ *in* G.

(c) *We have the isomorphism of the quotient groups*

$$\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B) \simeq \mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B}). \tag{2.3}$$

(d) *We have the factorization*

$$G = \mathrm{Im}(\widetilde{B})\mathrm{Im}(B). \tag{2.4}$$

From now on, denote by B_+ the map on the group G defined as follows,

$$B_+(g) = gB(g).$$

Proposition 2.5 (see [4, Lemma 5 (c)]) *If* (G, B) *is a Rota–Baxter group, then*

$$BB_+ = B_+B.$$

Remark 2.6 Because of Proposition 2.5, one may note

$$\mathrm{Im}(B\widetilde{B}) = \mathrm{Im}(\widetilde{B}B).$$

Indeed,

$$(B\widetilde{B})(g) = (BB_+)\big(g^{-1}\big) = (B_+B)\big(g^{-1}\big) = \widetilde{B}\big(\big(B(g^{-1})^{-1}\big).$$

However, the equality $B\widetilde{B} = \widetilde{B}B$ is not true, see Example 6.5 below.

Given an integer n, denote by $a^{\circ(n)}$ the nth power of a under the product $\circ$.

Proposition 2.7 (see [4, Proposition 14]) *If* (G, B) *is a Rota–Baxter group, we have the equality*

$$a^{\circ(k)} = (B_+(a))^k(B(a))^{-k},$$

for all $a \in G$ *and* $k \in \mathbb{Z}$.

Let us deduce an easy but important equality.

Lemma 2.8 *Let* (G, B) *be an RB-group. Then*

$$\mathrm{Im}(B\widetilde{B}) = \mathrm{Im}(\widetilde{B}B) = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B}).$$

Proof — The first equality follows from Remark 2.6 and it implies the inclusion $\mathrm{Im}(B\widetilde{B}) \subseteq \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})$. Now, suppose that $x \in \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})$, i.e., $x = B(g) = hB(h)$ for some $g, h \in G$. By Proposition 2.1 (c), we have

$$h = B(g)B(h)^{-1} = B(g)B(B(h)^{-1}h^{-1}B(h)) = B(z),$$

for $z = g \circ B(h)^{-1}h^{-1}B(h)$. Since $\mathrm{Im}(B)$ is a subgroup, we obtain that $h^{-1} \in \mathrm{Im}(B)$. Hence, $x = \widetilde{B}(h^{-1}) \in \mathrm{Im}(\widetilde{B}B)$. □

Example 2.9 (see [22, Lemma 2.6]) Let G be a group. Given an exact factorization $G = HL$, a map $B\colon G \to G$ defined as follows,

$$B(hl) = l^{-1}$$

is a Rota–Baxter operator on G.

We call such RB-operator on G a *splitting Rota–Baxter operator*.

Proposition 2.10 (see [4, Proposition 16]) *Let G be a group. Then, an RB-operator on G, $B\colon G \to G$, is a splitting Rota–Baxter operator on G if and only if* $\mathrm{Im}(\widetilde{B}B)=1$.

Proposition 2.11 (see [4, Proposition 20]) *Given a semidirect product $G = H \rtimes L$, let C be a Rota–Baxter operator on L. Then the map $B\colon G \to G$ defined by the formula*

$$B(hl) = C(l),$$

where $h \in H$ and $l \in L$, is a Rota–Baxter operator.

Corollary 2.12 *Given an exact factorization $G = HL$, let C be a Rota–Baxter operator on L. If $\mathrm{Im}(\widetilde{C}) \leqslant L$ normalizes H, then the map $B\colon G \to G$ defined by the formula*

$$B(hl) = C(l),$$

where $h \in H$ and $l \in L$, is a Rota–Baxter operator.

Proof — Let $h, h' \in H$ and $l, l' \in L$. Then

$$\begin{aligned} B\big(hlB(hl)h'l'(Bhl)^{-1}\big) &= B\big(hlC(l)h'l'C(l)^{-1}\big) \\ = B\big(hh''lC(l)l'C(l)^{-1}\big) &= C\big(lC(l)l'C(l)^{-1}\big) \\ = C(l)C(l') &= B(hl)B(h'l'), \end{aligned}$$

where $h'' = h'^{(lC(l))^{-1}} = h^{\widetilde{C}(l^{-1})^{-1}} \in H$. □

Proposition 2.13 (see [4, Proposition 21]) *Let G be a group and H an abelian subgroup of G. Then any homomorphism $B\colon G \to H$ is a Rota–Baxter operator.*

Lemma 2.14 *Let* B *be an RB-operator on a finite group* G *and let* $c \in Z(G)$. *Then the following hold*:

(a) *If* B *is invertible and* $B(x) = c$, *then* x *commutes with* $\mathrm{Im}(\widetilde{B})$.

(b) *We have that* $|B(c)|$ *divides* $|c|$.

Proof — (a) Since B is an isomorphism from $G^{(\circ)}$ onto G, we get $x \in Z(G^{(\circ)})$, i.e. $x \circ g = g \circ x$, for every $g \in G$. Hence,

$$xB(x)gB(x)^{-1} = xg = gB(g)xB(g)^{-1}.$$

Thus,

$$x = B_+(g)x(B_+(g))^{-1} = x^{(B_+(g))^{-1}}.$$

We apply that $\mathrm{Im}(\widetilde{B}) = \mathrm{Im}(B_+)$.

(b) Let $|c| = k$. By (2.1), we have

$$B(z)(B(c))^k = B(z)B(c) \cdot (B(c))^{k-1} = B(zc)(B(c))^{k-1}$$

$$= \ldots = B(zc^k) = B(z).$$

Hence, $(B(c))^k = e$. □

3 Sharply 2-transitive groups

In this section, we provide necessary information about sharply 2-transitive groups. The structure of a sharply 2-transitive group is described in the following theorems.

Theorem 3.1 (see [23, Theorem XII.9.7]) *Suppose that* q *is a prime-power and* m *is a natural number with the following properties*:

(1) *Each prime divisor of* m *divides* $q - 1$.

(2) *If* 4 *divides* m, *then* 4 *divides* $q - 1$.

Let $GF(q^m)^* = \langle w \rangle$ *and suppose that* $(m, t) = 1$. *Let* a, b *be the following elements of the group of semilinear mappings on* $GF(q^m)$*:*

$$xa = w^m x, \quad xb = w^t x^q. \tag{3.1}$$

Then $N = \langle a, b \rangle$ *is a regular permutation group on* $GF(q^m)^*$ *and* $\langle a \rangle$ *is an irreducible normal subgroup of* N. *If* F *is the group of all translations on* $GF(q^m)$, N *normalizes* F *and* $L(m, q, t) = FN$ *is a sharply doubly transitive permutation group of degree* q^m.

Note that the groups $L(m, q, t)$ are isomorphic for fixed m, q and different admissible t.

Theorem 3.2 (see [23, Theorem XII.9.8]) *Let* L *be a sharply doubly transitive permutation group. Then* L *is a Frobenius group with elementary abelian Frobenius kernel* F. *To within similarity,* L *permutes* $GF(p^r)$, *and* F *is the group of translations on* $GF(p^r)$. *If* p^r *is distinct from* $5^2, 7^2, 11^2, 23^2, 29^2$, *and* 59^2, L *is permutation isomorphic to one of the groups* $L(m, q, t)$ *defined in* Theorem 3.1.

We want to find the conditions when L is contained in the alternating group and L has a subgroup of index 2.

In the remarks after [34, Theorem A], the authors say that the sharply 2-transitive group consists of even permutations only if $p = 2$, or r is even and p is odd. Note that this condition is necessary but not sufficient. For example, if $n = 13^2$, then the symmetric group S_{169} has two sharply 2-transitive groups L_1 and L_2, where

$$L_1 \simeq (\mathbb{Z}_{13} \times \mathbb{Z}_{13}) : \mathbb{Z}_{168} \quad \text{and} \quad L_2 \simeq (\mathbb{Z}_{13} \times \mathbb{Z}_{13}) : (\mathbb{Z}_{21} : \mathbb{Z}_8)$$

It is clear that the generator of $\mathbb{Z}_{168}$ in L_1 and the generator of $\mathbb{Z}_8$ in L_2 are odd permutations, and so they do not belong to A_{169}.

Corollary 3.3 *Let* $L = FN$ *be a sharply doubly transitive permutation group of degree* $n = q^m$. *If* $L \leqslant A_n$ *and* L *has a subgroup of index* 2, *then one and only one of the following holds*:

(1) $q \equiv 3 \pmod 4$ *and* $L = L(m, q, t)$ *is defined in* Theorem 3.1. *Moreover,* L *has two non-isomorphic subgroups of index* 2*, except* $L = L(2, 3, 1)$ *which has only one non-isomorphic subgroup of index* 2*.*

(2) $n = 7^2$ *and* $N \simeq 2^-S_4 \simeq SL_2(3).2$*. Moreover,* L *has one non-isomorphic subgroup of index* 2*.*

(3) $n = 23^2$ *and* $N \simeq 2^-S_4 \times \mathbb{Z}_{11} \simeq SL_2(3).2 \times \mathbb{Z}_{11}$*. Moreover,* L *has one non-isomorphic subgroup of index* 2*.*

Proof — At first, consider the general case $L = L(m, q, t) = FN$. The Frobenius group of even degree does not have subgroups of index 2, and therefore q must be odd. Since q is odd, we have $F \leqslant A_n$, where $n = q^m$. It follows from the proof of Theorem 3.1 that

$$q^m - 1 = m(q-1)l$$

for some integer l, and the order of a is equal to $(q-1)l$. Moreover,

$$b^{-1}ab = a^q \quad \text{and} \quad b^m = a^{tl}.$$

Therefore, a is the product of m cycles of length $(q-1)l$. Thus, we have that $a \in A_n$ if and only if m is even.

It follows from the equality (3.1) that $m \,||b|$. Therefore,

$$|b| = \frac{m|a|}{(|a|, tl)} = \frac{m|a|}{l(q-1,t)} = \frac{q^m - 1}{l(q-1,t)} = \frac{n-1}{l(q-1,t)}.$$

Put $s = l(q-1,t)$. The element b is the product of s cycles of length $(n-1)/s$. Thus, $b \in A_n$ if and only if s is even. Since $(m,t) = 1$ and m must be even, we have t is odd. Therefore, s is even if and only if l is even.

Therefore, $N \leqslant A_n$ if and only if m and $l = (q^m - 1)/m(q-1)$ are even. It follows from [33, Lemma 1.7 (iii)] that l is even if and only if $q \equiv 3 \pmod 4$. Since $q \equiv 3 \pmod 4$, the property (2) of Theorem 3.1 is equivalent to $m \equiv 2 \pmod 4$.

Now $L = FN \leqslant A_n$ and N has the following presentation:

$$N = \left\langle a, b \mid a^{(q-1)l} = b^{(q-1)m} = 1, a^{tl} = b^m, b^{-1}ab = a^q \right\rangle.$$

The group N has three normal subgroups of index two:

$$S_1 = \left\langle a, b^2 \right\rangle, \quad S_2 = \left\langle a^2, b \right\rangle, \quad \text{and} \quad S_3 = \left\langle a^2, ab \right\rangle.$$

If $q^m = 3^2$, then $N = Q_8$ has three normal subgroups of index 2, isomorphic to $\mathbb{Z}_4$. If $q^m > 9$, then the group S_1 is not isomorphic to S_2 or S_3, however, $S_2 \simeq S_3$. Hence, L has two non-isomorphic subgroups FS_1 and FS_2 of index 2.

Now consider the exceptional cases when p^r is one of integers $5^2, 7^2, 11^2, 23^2, 29^2$, or 59^2. According to [19, Theorem 2.4] the group $L = FN$ is a Frobenius group, where F is the elementary abelian group of order p^2 and N is one of the following groups:

(i) $p = 5$ and $N \simeq SL_2(3)$.

(ii) $p = 7$ and $N \simeq 2^-S_4 \simeq SL_2(3).2$.

(iii) $p = 11$ and $N \simeq SL_2(3) \times \mathbb{Z}_5$.

(iv) $p = 11$ and $N \simeq SL_2(5)$.

(v) $p = 23$ and $N \simeq 2^-S_4 \times \mathbb{Z}_{11} \simeq SL_2(3).2 \times \mathbb{Z}_{11}$.

(vi) $p = 29$ and $N \simeq SL_2(5) \times \mathbb{Z}_7$.

(vii) $p = 59$ and $N \simeq SL_2(5) \times \mathbb{Z}_{29}$.

Note that the groups $SL_2(3)$ and $SL_2(5)$ have no subgroups of index 2. Thus, the only possibilities are (ii) and (v), wher N has one subgroup of index 2. □

4 Equivalence of Rota–Baxter operators

Proposition 4.1 (see [24]) *Let* B *be a map defined on a finite group* G *and construct* $H_B = \{(B(g), gB(g)) \mid g \in G\} \subset G \times G$.

Then the following hold:

(a) *If* B *is an RB-operator on* G*, then* H_B *is a subgroup of* $G \times G$.

(b) *If* H *is a subgroup of* $G \times G$*, then there exists an RB-operator* B *on* G *such that* $H = H_B$ *if and only if* $|H| = |G|$ *and*

$$\{ba^{-1} \mid (a, b) \in H\} = G.$$

Note that $\{ba^{-1} \mid (a, b) \in H\} = G$ is equivalent to the condition

$$H \cap \{(g, g) \mid g \in G\} = \{e\}.$$

Given an element x of a group G, the automorphism $g \mapsto g^x$ is denoted by α_x. Let us consider the following subgroup of $\mathrm{Aut}(G \times G)$:

$$\begin{aligned} Q(G) = &\{(\varphi, \varphi\,\alpha_x) \mid \varphi \in \mathrm{Aut}(G),\, x \in G\} \\ &\cup \{\tau((\varphi, \varphi\,\alpha_x)) \mid \varphi \in \mathrm{Aut}(G),\, x \in G\}, \end{aligned}$$

where $\tau((\varphi, \varphi\,\alpha_x))\colon (g, h) \to (\varphi\,\alpha_x(h), \varphi(g))$.

Proposition 4.2 *Let* B *be an RB-operator on a finite group* G*. For every* $\Phi \in Q(G)$*, there exists an RB-operator* B' *on* G *such that* $\Phi(H_B) = H_{B'}$.

Proof — It is clear that $|\Phi(H_B)| = |G|$, it remains to check that $\{ba^{-1} \mid (a, b) \in \Phi(H_B)\} = G$. Let us prove the statement for $\Phi = (\varphi, \varphi\,\alpha_x)$, the proof for $\Phi = \tau((\varphi, \varphi\,\alpha_x))$ is analogous. Thus, we have to find for every $g \in G$ such $(a, b) \in H_B$ that

$$\varphi(\alpha_x(b))\varphi(a)^{-1} = g.$$

Equivalently, we search for $(a, b) \in H_B$ such that $bxa^{-1} = h$, where $h = x\varphi^{-1}(g)$ may be any element from G. We may find $(a_0, b_0) \in H_B$ such that $b_0 a_0^{-1} = x$. Hence, we need to get a pair $(a, b) \in H_B$ satisfying the equality

$$bxa^{-1} = bb_0 a_0^{-1} a^{-1} = bb_0 (aa_0)^{-1} = h,$$

and it is possible, since $h = \widetilde{b}\widetilde{a}^{-1}$ for some $(\widetilde{a}, \widetilde{b}) \in H_B$. Thus, we obtain that $(a, b) = (\widetilde{a}, \widetilde{b})(a_0, b_0)^{-1} \in H_B$. □

Let us call a pair of RB-operators B, B' on a group G *equivalent*, if $\Phi(H_B) = H_{B'}$ for some $\Phi \in Q(G)$. Let us interpret Proposition 2.2 in terms of equivalent RB-operators. If $\Phi = \tau((id, id))$, we have $B' = \widetilde{B}$. If $\Phi = (\varphi, \varphi)$, then $B' = B^{(\varphi)}$.

Lemma 4.3 *Let G be a finite group and B, B' be a pair of equivalent RB-operators on G. Then the following hold*:

(a) $G^{(\circ)}(B) \simeq G^{(\circ)}(B')$.

(b) B *is trivial if and only if* B' *is trivial.*

(c) *Up to action of* $B \to \widetilde{B}$, *we have*

$$\mathrm{Im}(B) \simeq \mathrm{Im}(B') \quad \textit{and} \quad \mathrm{Im}(\widetilde{B}) \simeq \mathrm{Im}(\widetilde{B'}).$$

(d) $\mathrm{Im}(B\widetilde{B}) \simeq \mathrm{Im}(B'\widetilde{B'})$.

(e) B *is splitting if and only if* B' *is splitting.*

(f) *If* $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$, *then up to the action of* $B \to \widetilde{B}$, *one has*

$$G = \mathrm{Ker}(B') \cdot \mathrm{Im}(B').$$

Proof — (a) Define $\kappa\colon G \to H_B, g \mapsto (B(g), gB(g))$. Note that κ is bijective and $\kappa(g \circ h) \to \kappa(g)\kappa(h)$, thus, $G^{(\circ)}(B) \simeq H_B$, hence $G^{(\circ)}(B) \simeq H_B \simeq H_{B'} \simeq G^{(\circ)}(B')$.

(b), (c) They are trivial.

(d) Let us consider $\Phi = (\varphi, \alpha_x\varphi) \in Q(G)$, $\varphi \in \mathrm{Aut}(G)$, and $x \in G$. Note that $\mathrm{Im}(\widetilde{B^{(\varphi)}B^{(\varphi)}}) \simeq \mathrm{Im}(B\widetilde{B})$. Thus, it remains to study the case when B' comes from B with the help of $\Phi = (id, \alpha_x)$. Then $\mathrm{Im}(\widetilde{B}'B') = \alpha_x(\mathrm{Im}(\widetilde{B}B))$, i.e. the required subgroups are isomorphic.

(e) It follows from (d) and Proposition 2.10.

(f) It follows from the fact that $G = H \cdot L$ is an exact factorization if and only if $G = H \cdot \alpha_x(L)$ is an exact factorization, for any $x \in G$. □

Remark 4.4 Let us show that one may not generalize Proposition 4.2 on the whole $\mathrm{Aut}(G \times G)$. For this, take $G = A_4$ and identify $A_4 \times A_4$ with the corresponding subgroup in S_8. Then the map B defined on $A_4 = V \rtimes L$ by Proposition 2.11 for

$$V = \langle (12)(34), (13)(24) \rangle, \quad L = \langle (234) \rangle$$

and $B_{|_L} = \mathrm{id}$ is a Rota–Baxter operator. We have

$$H_B = \langle (234)(687), (13)(24), (12)(34) \rangle.$$

Let us consider $\psi = \mathrm{conj}_{(23)} \in \mathrm{Aut}(S_8)$, which induces the automorphism of $G \times G$. Then

$$\psi(H_B) = \langle (243)(687), (13)(24), (12)(34) \rangle$$

and now, $\psi(H_B)$ has a non-trivial intersection with the diagonal subgroup of $G \times G$. Thus, the condition (b) from Proposition 4.1 does not hold. Note that ψ has the form (φ, id) for the outer automorphism φ of A_4.

5 Properties of some explicit construction

Lemma 5.1 *Let* B *be an RB-operator on a finite group* G *such that*

(i) $R = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})$ *is abelian.*

(ii) $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$.

Then $\widetilde{B}_{|_{\mathrm{Im}(B)}}$ *is a homomorphism onto the abelian subgroup* R *of* $\mathrm{Im}(B)$, *and* B *is defined on* G *by the formula*

$$B(hl) = B_{|_{\mathrm{Im}(B)}}(l),$$

where $h \in \mathrm{Ker}(B)$ *and* $l \in \mathrm{Im}(B)$.

Proof — Due to Condition (ii), for any $g \in G$, we have a decomposition $g = kB(s)$, where $k \in \mathrm{Ker}(B)$ and $s \in G$. By Proposition 2.1 (d), $B(g) = B^2(s)$, which implies $\mathrm{Ker}(B) = \mathrm{Ker}(B^2)$.

By Proposition 2.4, $\mathrm{Ker}(\widetilde{B}) \trianglelefteq \mathrm{Im}(B)$, so we may consider the groups $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$, $\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B)$, and $B, \widetilde{B}$ are RB-operators on it. Moreover, $\widetilde{B}$ is a homomorphism from $(\mathrm{Im}(B))^{(\circ_{\widetilde{B}})}$ into

$$R = \mathrm{Im}(B\widetilde{B}) = \mathrm{Im}(\widetilde{B}B),$$

as well as B is a homomorphism from $(\mathrm{Im}(\widetilde{B}))^{(\circ_B)}$ into R. Here we define $\circ_B$ and $\circ_{\widetilde{B}}$ by (3). Since $\mathrm{Ker}(\widetilde{B}) = \mathrm{Ker}(\widetilde{B}) \cap \mathrm{Im}(B)$, the isomorphism theorem implies $\mathrm{Im}(B)^{(\circ_{\widetilde{B}})}/\mathrm{Ker}(\widetilde{B})^{\circ_{\widetilde{B}}} \simeq R$.

Let φ be a canonical homomorphism from $\mathrm{Im}(\widetilde{B})$ onto $\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B)$. We have the following sequence of homomorphisms:

$$\mathrm{Im}(B)^{(\circ_{\widetilde{B}})} \xrightarrow{\widetilde{B}} \mathrm{Im}(\widetilde{B}) \xrightarrow{\varphi} \mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B),$$

and define $B' = \widetilde{B} \circ \varphi$ as the composition of them. Let $B(h)$ be an element of $\mathrm{Ker}(B')$. Then

$$B'(B(h)) = \mathrm{Ker}\, B \cdot \widetilde{B}B(h) = \mathrm{Ker}\, B.$$

Since $\mathrm{Ker}(B) = \mathrm{Ker}(B^2)$ and $\mathrm{Im}(B\widetilde{B}) = \mathrm{Im}(\widetilde{B}B)$, we have that $B(h)$ belongs to $\mathrm{Ker}(\widetilde{B})$. Thus, $\mathrm{Ker}(\widetilde{B}) = \mathrm{Ker}(B')$ and by the isomorphism theorem

$$\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B) \simeq \mathrm{Im}(B)^{(\circ_{\widetilde{B}})}/\mathrm{Ker}(\widetilde{B})^{(\circ_{\widetilde{B}})} \simeq R.$$

Hence, $\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B)$ is abelian and $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$ is abelian too due to (2.3). Since $\widetilde{B}$ is an RB-operator on the abelian group $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$, we derive that $\widetilde{B}$ is an endomorphism of $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$.

Choose an independent set $r_1, \ldots, r_n$ of generators of an abelian group R and find $t_i \in \mathrm{Im}(B)$ such that $\widetilde{B}(t_i) = r_i$, $i = 1, \ldots, n$. Since $\widetilde{B}$ is a endomorphism of $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$, $\widetilde{B}(t_it_j) = k_{ij}r_ir_j$

for some $k_{ij} \in \mathrm{Ker}(\widetilde{B})$. By (2.1), we write down

$$r_i r_j = \widetilde{B}(t_i)\widetilde{B}(t_j) = \widetilde{B}(t_i r_i t_j r_i^{-1}).$$

Since $\widetilde{B}$ is well-defined on the abelian group $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$ and $\mathrm{Ker}(\widetilde{B})t_i t_j = \mathrm{Ker}(\widetilde{B})t_i r_i t_j r_i^{-1}$, we obtain $k_{ij} = e$ and $\widetilde{B}(t_i t_j) = r_i r_j$. Similarly, we show that $\widetilde{B}(t_i t_j t_k) = r_i r_j r_k$ and so on. Thus, $\widetilde{B}$ is a homomorphism from $\mathrm{Im}(B)$ to R. □

Now, we provide the conditions under which we may apply Lemma 5.1. Let B be an RB-operator on a finite group G. If $\mathrm{Ker}(B) = \mathrm{Im}(\widetilde{B})$, then B is a splitting RB-operator by Proposition 2.10. Consider the case

$$\mathrm{Ker}(\widetilde{B}) < \mathrm{Im}(B) \quad \text{and} \quad \mathrm{Ker}(B) < \mathrm{Im}(\widetilde{B}).$$

Denote $H = \mathrm{Im}(B)$, $L = \mathrm{Im}(\widetilde{B})$, and $R = H \cap L$. Then

$$\begin{aligned} |G| = |\mathrm{Im}(\widetilde{B})\mathrm{Im}(B)| &= \frac{|\mathrm{Im}(B)| \cdot |\mathrm{Im}(\widetilde{B})|}{|R|} \\ &= |\,\mathrm{Ker}(B)| \cdot |\mathrm{Im}(B)| = |\,\mathrm{Ker}(\widetilde{B})| \cdot |\mathrm{Im}(\widetilde{B})|, \end{aligned} \tag{5.1}$$

and

$$|R| = |\mathrm{Im}(B) : \mathrm{Ker}(\widetilde{B})| = |\mathrm{Im}(\widetilde{B}) : \mathrm{Ker}(B)| > 1.$$

Lemma 5.2 *Let B be a non-splitting RB-operator on a finite group G and*

$$R = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B}).$$

Then the following hold:

(a) $R \nleqslant \mathrm{Ker}(B)$ *or* $R \nleqslant \mathrm{Ker}(\widetilde{B})$.

(b) *if* $R \cdot \mathrm{Ker}(B) = \mathrm{Im}(\widetilde{B})$, *then* $G = \mathrm{Im}(B) \cdot \mathrm{Ker}(B)$ *is an exact factorization.*

Proof — (a) Observe that if $R \leqslant \mathrm{Ker}(B)$ and $R \leqslant \mathrm{Ker}(\widetilde{B})$, then $R \leqslant \mathrm{Ker}(B) \cap \mathrm{Ker}(\widetilde{B}) = 1$, a contradiction.

(b) Since $R \leqslant \mathrm{Im}(B)$, we have

$$G = \mathrm{Im}(B) \cdot \mathrm{Im}(\widetilde{B}) = \mathrm{Im}(B) \cdot R \cdot \mathrm{Ker}(B) = \mathrm{Im}(B) \cdot \mathrm{Ker}(B),$$

where the last factorization is exact. □

Corollary 5.3 *Let* B *be a non-splitting RB-operator on a finite group* G, $R = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})$ *and* $|R|$ *is prime. Then, up to the action* $B \to \widetilde{B}$, B *is defined on* G *by* Lemma 5.1.

Proof — By Lemma 5.2 (a), we may suppose that $R \nleqslant \mathrm{Ker}(B)$. Then $|R \cap \mathrm{Ker}(B)| = 1$ and thus, $R \cdot \mathrm{Ker}(B) = \mathrm{Im}(\widetilde{B})$. By (b) in Lemma 5.2, we get $G = \mathrm{Im}(B) \cdot \mathrm{Ker}(B)$. Therefore, all conditions of Lemma 5.1 are satisfied. □

Remark 5.4 Let us observe that Corollary 5.3 has a simple form, when $|R| = 2$ and $R \nleqslant \mathrm{Ker}(B)$. Indeed, we have the exact factorization $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$. Choose $t \in \mathrm{Im}(B) \setminus \mathrm{Ker}(\widetilde{B})$ and denote $r = \widetilde{B}(t)$. Hence, each $x \in G$ has the form $x = kl$, where $k \in \mathrm{Ker}(B)$ and $l \in \mathrm{Im}(B)$. Since $|\mathrm{Im}(B) : \mathrm{Ker}(\widetilde{B})| = 2$, we get $l = t^{\delta}y$, for some $y \in \mathrm{Ker}(\widetilde{B})$ and $\delta \in \{0, 1\}$. Therefore, B acts on G as follows:

$$B(x) = B(kl) = B(l) = l^{-1}\widetilde{B}(l^{-1}) = l^{-1}\widetilde{B}(y^{-1}t^{\delta}) = l^{-1}r^{\delta}. \quad (5.2)$$

6 Rota–Baxter operators on dihedral groups

Below, we define the dihedral group D_{2n} as follows,

$$D_{2n} = \langle r, s \mid r^n = s^2 = e,\ r^s = r^{-1} \rangle.$$

Theorem 6.1 *The following statements hold*:

(a) *There are no non-splitting RB-operators on* D_{2n}, *where* n *is odd.*

(b) *Let* n *be even. Then all non-splitting RB-operators* B *on* D_{2n} *come from an exact factorization* $D_{2n} = HL$, *where* $H = \mathrm{Ker}(B)$

and $L = \mathrm{Im}(B)$, *up to the action* $B \to \widetilde{B}$. *Moreover,* $\widetilde{B}_{|_L}$ *is a homomorphism onto* $\mathbb{Z}_2$ *or* $\mathbb{Z}_2^2$. *Hence,* B *on* D_{2n} *is defined by* Corollary 2.12.

Proof — (a) We want to show that $r^m s \in \mathrm{Ker}(B\widetilde{B})$, for all m such that $0 \leqslant m < n$. It would imply that $\mathrm{Ker}(B\widetilde{B})$ contains at least $n+1$ elements; since $\mathrm{Ker}(B\widetilde{B})$ is a subgroup, we prove that $B\widetilde{B}(g) = e$, for all $g \in G$. By Proposition 2.10, B is splitting. One of $B(r^m s), \widetilde{B}(r^m s)$ lies in $\langle r \rangle$, say $B(r^m s) = r^k$, for some k. Therefore

$$r^{2k} = B(r^m s)B(r^m s) = B(r^m s r^k r^m s r^{-k}) = B(r^{-2k}),$$

and $r^{2k} \in \mathrm{Ker}(\widetilde{B})$. Since n is odd, we get that $r^k \in \mathrm{Ker}(\widetilde{B})$, and we are done.

(b) Let n be even. For $n = 2$, one may check the statement directly. Let $n > 2$. Define $R = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})$. When $|R| = 2$, the statement follows from Remark 5.4. Hence, we may suppose that $|R| > 2$.

Assume that $\mathrm{Im}(B) = \langle r^{d_1} \rangle$ and $\mathrm{Im}(\widetilde{B}) = \langle r^{d_2}, s \rangle$, where $d_1 \mid n$ and $d_2 \mid n$. Since $\mathrm{Ker}(B) \trianglelefteq \mathrm{Im}(\widetilde{B}) \simeq D_{2n/d_2}$, we have

$$\mathrm{Ker}(B) = \langle r^{d_2 d_3} \rangle,$$

for some d_3. Thus, $\mathrm{Im}(\widetilde{B})/\mathrm{Ker}(B)$ is dihedral and noncyclic, whereas $\mathrm{Im}(B)/\mathrm{Ker}(\widetilde{B})$ is cyclic, a contradiction to (2.3).

It remains to study the situation when both $\mathrm{Im}(B)$ and $\mathrm{Im}(\widetilde{B})$ are dihedral groups.

Case 1. $|\mathrm{Im}(B)|, |\mathrm{Im}(\widetilde{B})| < |G|$.

Denote $H = \mathrm{Im}(B)$ and $L = \mathrm{Im}(\widetilde{B})$. Applying Lemma 2.8 and induction, we have

$$|\mathrm{Im}(B^2\widetilde{B})| = |\mathrm{Im}(B|_H) \cap \mathrm{Im}(\widetilde{B}|_H)| = 2^a, \ |\mathrm{Im}(B\widetilde{B}^2)|$$

$$= |\mathrm{Im}(B|_L) \cap \mathrm{Im}(\widetilde{B}|_L)| = 2^b,$$

for $a, b \in \{0, 1, 2\}$. By Lemma 2.8 and by (2.4), we have

$$R = \mathrm{Im}(B\widetilde{B}) = B(R) \cdot \widetilde{B}(R) = \mathrm{Im}(B^2\widetilde{B}) \cdot \mathrm{Im}(B\widetilde{B}^2).$$

Hence, similarly to (5.1), we deduce that $|R| = 2^c$, for $0 \leqslant c \leqslant 4$.

Case 1A. Suppose that R contains some reflection, so, up to the action of $\mathrm{Aut}(D_{2n})$, we may assume that $\mathrm{Im}(B) = \langle r^{d_1}, s\rangle$ and $\mathrm{Im}(\widetilde{B}) = \langle r^{d_2}, s\rangle$, where $d_1 \mid n$ and $d_2 \mid n$.

According to (2.4), we have $(d_1, d_2) = 1$ and so, $n = d_1 d_2 d_3$, for suitable d_3. Since

$$|R| \cdot |G| = |\mathrm{Im}(B)| \cdot |\mathrm{Im}(\widetilde{B})| = \frac{2n}{d_1} \cdot \frac{2n}{d_2} = 2d_3 \cdot 2n,$$

we derive that $|R| = 2d_3$. Hence, $\mathrm{Ker}(\widetilde{B})$ is a normal subgroup of index $2d_3$ in $\mathrm{Im}(B)$, i.e. $\mathrm{Ker}(\widetilde{B}) = \langle r^{d_1 d_3}\rangle$. Analogously, we obtain that $\mathrm{Ker}(B) = \langle r^{d_2 d_3}\rangle$.

Since we suppose that $|R| > 2$, it remains to study only the case $|R| = 2^c$, for $2 \leqslant c \leqslant 4$. Hence, $d_3 = 2^{c-1} > 1$. Thus, we obtain that $(d_1, d_3) = 1$ or $(d_2, d_3) = 1$. It means that we have an exact factorization, say, $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$. Such factorization implies that $\mathrm{Im}(B^2) = \mathrm{Im}(B)$. By induction,

$$|R| = |(\widetilde{B}B)(G)| = |(\widetilde{B}B^2)(G)| = |(\widetilde{B}B)(H)| = |(B\widetilde{B})(H)| \leqslant 4,$$

and we have exactly the case $R \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Hence, the statement follows from Lemma 5.1.

Case 1B. Now, consider the case, where R does not contain any reflection. Denote $\mathrm{Im}(B) = \langle r^{d_1}, s\rangle$ and $\mathrm{Im}(\widetilde{B}) = \langle r^{d_2}, r^k s\rangle$, where $d_1 \mid n$, $d_2 \mid n$, and $d_2 \nmid k$. Again, by (2.4), we have either $(d_1, d_2) = 1$ or $(d_1, d_2) = 2$. In the first case,

$$R = \mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B}) = 1,$$

a contradiction. In the second one, we get $R = \{e, r^{n/2}\}$, a contradiction with the assumption $|R| > 2$.

Case 2. Only one of $|\mathrm{Im}(B)|$ and $|\mathrm{Im}(\widetilde{B})|$ is equal to $|G|$.

Suppose that $\mathrm{Im}(B) = G$. Choose $a \in G$ such that $B(a) = r$. Denote $x = a^{\circ(n/2)}$, then $B(x) = r^{n/2}$. By Proposition 2.7, we may rewrite x as

$$x = \big(B_+(a)\big)^{n/2}\big(B(a)\big)^{-n/2} = (ar)^{n/2}r^{n/2}.$$

Hence, we have either $a = r^m s$, with $0 \leqslant m < n$, or $a = r^m$, with $1 \leqslant m < n$. Assume that $a = r^m s$ and $n/2$ is odd. Then we have $x = r^{n/2+m-1}s$. By Lemma 2.14, x is centralized by $\mathrm{Im}(\widetilde{B})$. Hence,

$$\mathrm{Im}(\widetilde{B}) \leqslant C_{D_{2n}}(x) = \big\{e, r^{m-1}s, r^{n/2}, r^{n/2+m-1}s\big\} \simeq \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Moreover, we have the exact factorization $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$, thus, we may again apply Lemma 5.1.

If $a = r^m s$ and $n/2$ is even or $a = r^m$, we get that $x = r^{n/2}$. Define $K = \langle r^{n/2}\rangle$, the normal subgroup of order 2 in D_{2n}. Since $B(r^{n/2}) = r^{n/2}$, we may consider induced RB-operators B and $\widetilde{B}$ on G/K. Note that $\widetilde{B}(r^{n/2}) = e$. By induction, $\mathrm{Im}(\widetilde{B}|_{G/K})$ is a subgroup of $\mathbb{Z}_2 \times \mathbb{Z}_2$. If $r^{n/2} \notin \mathrm{Im}(\widetilde{B})$, then

$$\mathrm{Im}(\widetilde{B}) \leqslant \mathbb{Z}_2 \times \mathbb{Z}_2,$$

and the statement holds by Lemma 5.1 due to the exact factorization $G = \mathrm{Ker}(B) \cdot \mathrm{Im}(B)$. If $r^{n/2} \in \mathrm{Im}(\widetilde{B})$, then

$$\mathrm{Im}(\widetilde{B}) \leqslant \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

(since $r^{n/2}$ is central, we get an additional factor $\mathbb{Z}_2$). The case $\mathrm{Im}(\widetilde{B}) \simeq \mathbb{Z}_2^3$ is impossible, because $\mathbb{Z}_2^3$ may not be a subgroup of any dihedral group. Hence, we again apply Lemma 5.1.

Case 3. $|\mathrm{Im}(B)| = |\mathrm{Im}(\widetilde{B})| = |G|$.

Recall that the map B_+, defined as $B_+(g) = gB(g)$, is a homomorphism from $G^{(\circ)}$ in G. Since $|\mathrm{Im}(\widetilde{B})| = |\mathrm{Im}(B_+)| = |G|$,

we have $\mathrm{Ker}(B_+) = e$ and B_+ is an isomorphism. Therefore, the map $\varphi = B^{-1}B_+$ is an automorphism of $G^{(\circ)} \simeq D_{2n}$. It is trivial to check that φ is fixed-point free. Since $n \geqslant 3$, the center of D_{2n} is preserved by every automorphism. Hence, D_{2n} does not admit fixed-point free automorphisms, and we arrive at a contradiction. □

In [14], the correspondence between extensions of RB-groups and the second cohomology group was studied. As examples, the authors considered RB-operators on S_3 and D_8.

Corollary 6.2 *All RB-operators on* $S_3 \simeq D_6$ *are splitting.*

The next example appeared in [32, Example 1.13] in the context of skew left braces, we reformulate it in terms of RB-operators.

Example 6.3 Define a map $B\colon S_3 \to S_3$ as follows,

$$B\colon (ij) \to (23), \quad B\colon (123)^k \to e, \quad i \neq j,\ 1 \leqslant i, j, k \leqslant 3.$$

Then B is a Rota–Baxter operator on S_3. By Corollary 6.2, we know that B is splitting, indeed,

$$S_3 = \langle (123) \rangle \cdot \langle (23) \rangle = \mathrm{Ker}(B) \cdot \mathrm{Ker}(\widetilde{B}).$$

Thus, $S_3^{(\circ)} \simeq \mathbb{Z}_6$.

Example 6.4 In [32, Example 1.18], we have a Rota–Baxter operator B on D_8 defined as follows,

$$B(r^k) = e, \quad B(r^k s) = r, \quad 0 \leqslant k < 4.$$

Note that $\widetilde{B}$ is invertible and $D_8^{(\circ)} \simeq Q_8$.

The next example shows that $\widetilde{B}B \neq B\widetilde{B}$ in general.

Example 6.5 Let us consider the exact factorization $D_{16} = HL$ for $H = \{e, s\}$, $L = \{e, r^2, r^4, r^6, rs, r^3s, r^5s, r^7s\}$. We define B

on D_{16} in such a manner that $H = \mathrm{Ker}(\widetilde{B})$, $\mathrm{Ker}(B) = \langle r^4, rs\rangle$, and

$$B(r^2) = B(r^6) = B(r^3s) = B(r^7s) = r^4.$$

Hence, B is a homomorphism from L onto $\langle r^4\rangle \simeq \mathbb{Z}_2$. In addition, $\mathrm{Im}(B)|_L$ normalizes $\mathrm{Ker}(\widetilde{B})$. Thus, we get an RB-operator on D_{16}. Note that

$$\begin{aligned}(B\widetilde{B})(r) &= B(\widetilde{B}(r)) = B(\widetilde{B}(sr)) = B(\widetilde{B}(r^7s))\\ &= B(r^7sB(r^7s)) = B(r^3s) = r^4,\end{aligned}$$

and

$$\begin{aligned}(\widetilde{B}B)(r) &= \widetilde{B}(B(r)) = \widetilde{B}(r^7\widetilde{B}(r^7)) = \widetilde{B}(r^7\widetilde{B}(sr^7))\\ &= \widetilde{B}(r^7\widetilde{B}(rs)) = \widetilde{B}(r^7\cdot rs) = \widetilde{B}(s) = e.\end{aligned}$$

The following example shows that the center of a group may not be preserved by an RB-operator.

Example 6.6 Define B on D_{2n} in such a way that

$$\widetilde{B}(r^{2k}) = e,\ \widetilde{B}(r^{2k+1}) = r^{n/2}s,\ \widetilde{B}(r^{2k}s) = r^{n/2},\ \widetilde{B}(r^{2k+1}s) = s,$$

with $0\leqslant k < n/2$. Then $\widetilde{B}$ is a homomorphism from D_{2n} onto the group $\mathbb{Z}_2\times\mathbb{Z}_2$ and B is a Rota–Baxter operator on D_{2n} due to the trivial factorization $D_{2n} = \mathrm{Ker}(B)\cdot\mathrm{Im}(B) = 1\cdot D_{2n}$. If $4\nmid n$, we have $B(r^{n/2}) = r^{n/2}\widetilde{B}(r^{n/2}) = s$.

Example 6.7 Consider the exact factorization

$$G = D_{60} = HL = \langle r^{10}\rangle\cdot\langle r^3, s\rangle.$$

We define an RB-operator on $L\simeq D_{20}$ as in Example 6.6. Further, we extend such B on the whole G, putting $\mathrm{Ker}(B) = H$. Surely, the group H is normalized by $\mathrm{Im}(\widetilde{B})$, since H is normal in G.

Remark 6.8 The descendent group $D_{2n}^{(\circ)}$ for odd prime n is discussed in [7, Corollary 6.5].

Recall that a generalized quaternion group Q_{4n} of order $4n$ is defined as follows:

$$Q_{4n} = \langle r, s \mid r^{2n} = e,\ s^2 = r^n,\ r^s = r^{-1} \rangle.$$

Corollary 6.9 *Let* B *be a non-splitting RB-operator on* Q_{4n}*, where* n *is odd. Then* B *is defined by* Remark 5.4.

Proof — It is known that $Z(Q_{4n}) = \{e, r^n\}$. Since r^n is a unique element of order 2 in Q_{4n}, we conclude, by Lemma 2.14, that the normal subgroup $K = \langle r^n \rangle$ is B-invariant: either $B(r^n) = r^n$ or $B(r^n) = e$. Therefore, B is an RB-operator on $Q_{4n}/K \simeq D_{2n}$. By Theorem 6.1 (a), we know that all RB-operators on D_{2n} are splitting. Hence, $|\mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B})| \leqslant 2$. Since B is non-splitting, we have $|R| = 2$. □

Let us show that the case $\mathrm{Im}(B) \cap \mathrm{Im}(\widetilde{B}) \simeq \mathbb{Z}_2$ is realizable on Q_{4n}.

Example 6.10 Consider the exact factorization

$$Q_{60} = \langle r^{10} \rangle \cdot \langle r^3, s \rangle = H \cdot L$$

and define $B\colon Q_{60} \to Q_{60}$ as follows, $\mathrm{Ker}(B) = H$ and $\widetilde{B}\colon L \to L$ acts by the formula

$$\widetilde{B}(r^{3k}s^i) = \begin{cases} r^{15}, & i = 1, \\ e, & i = 0. \end{cases}$$

It is an RB-operator on Q_{60}, since $\widetilde{B}$ is an endomorphism of L and $\mathrm{Im}(\widetilde{B}|_L)$ normalizes H.

Remark 6.11 *In [8], all braces with dihedral or generalized quaternion multiplicative group were described.*

7 Rota–Baxter operators on alternating groups

This section is devoted to the study of Rota–Baxter operators on simple groups A_n, $n \geqslant 5$. For completeness, let us deal with A_n for small n. Since $A_3 \simeq \mathbb{Z}_3$ is abelian, an RB-operator on it is nothing more than a homomorphism.

Computations show that, up to equivalence, we have the following non-trivial RB-operators on A_4:

(B1) Splitting one coming from the exact factorization $A_4 = HL$, where

$$H = \langle (234) \rangle \simeq \mathbb{Z}_3 \quad \text{and} \quad L = V_4$$

is the Klein four-group.

(B2) Non-splitting one coming from the exact factorization of the type $A_4 = HL$, where

$$H = \{e\} \quad \text{and} \quad L = A_4,$$

and an RB-operator C on L is a natural homomorphism from $L = \mathbb{Z}_3 \rtimes V_4$ onto $\mathbb{Z}_3$. Therefore, $\mathrm{Im}(B\widetilde{B}) \simeq \mathbb{Z}_3$ and Lemma 5.1 is again valid.

The fact that $A_4^{(\circ)}$ is isomorphic either to A_4 (for trivial RB-operators) or to $\mathbb{Z}_6 \times \mathbb{Z}_2$ may be derived from [13].

The study of splitting Rota–Baxter operators is the same as the study of exact factorizations, which are described in [34]. Therefore, we will focus on non-splitting RB-operators on A_n.

Below, we will apply the following conditions on the numbers m, q:

(i) q is a prime-power.

(ii) Each prime divisor of m divides $q - 1$.

(iii) $q \equiv 3 \pmod 4$ and $m \equiv 2 \pmod 4$.

Theorem 7.1 *The following statements hold*:

(1) *A non-splitting Rota–Baxter operator on a simple alternating group* A_n *exists if and only if* $n \in \{q^m,\ q^m+1\}$ *and* m, q *satisfy the conditions* (i)–(iii).

(2) *If a non-splitting Rota–Baxter operator on* A_n *exists, then there are* s *non-equivalent non-splitting Rota–Baxter operators on* A_n, *where*:

(a) $s = 3$ *for* $n \in \{7^2,\ 23^2\}$.

(b) $s = 2$ *for* $n = q^m$, $n \notin \{3^2,\ 7^2,\ 23^2\}$.

(c) $s = 1$ *for* $n \in \{3^2,\ q^m+1\}$.

Proof — Let B be a non-splitting RB-operator on $G = A_n$. According to Proposition 2.4, we have

$$G = \mathrm{Im}(B)\cdot\mathrm{Im}(\widetilde{B}) = H\cdot L,\ \mathrm{Ker}(\widetilde{B}) \trianglelefteq \mathrm{Im}(B),\ \text{and}\ \mathrm{Ker}(B) \trianglelefteq \mathrm{Im}(\widetilde{B}).$$

If $\mathrm{Ker}(B) = 1$ then B is a splitting RB-operator [4, Theorem 50]. If $\mathrm{Ker}(B) = \mathrm{Im}(\widetilde{B})$ then B is also a splitting RB-operator by Proposition 2.10. The same is true for $\mathrm{Ker}(\widetilde{B})$. Therefore, we consider only the following case:

$$1 < \mathrm{Ker}(\widetilde{B}) < \mathrm{Im}(B) \qquad \text{and} \qquad 1 < \mathrm{Ker}(B) < \mathrm{Im}(\widetilde{B}).$$

Define $R = H \cap L$. By Lemma 5.2 (a) it follows that either

$$R \not\leqslant \mathrm{Ker}(B) \qquad \text{or} \qquad R \not\leqslant \mathrm{Ker}(\widetilde{B}).$$

Since $\mathrm{Ker}(\widetilde{B}) > 1$ and $\mathrm{Ker}(B) > 1$, we obtain that $G = HL$, where H and L are proper subgroups of G. Then, according to [27, Theorem D], L is k-homogeneous ($1 \leqslant k \leqslant 5$), and

$$A_{n-k} \trianglelefteq H \leqslant (S_{n-k} \times S_k) \cap A_n.$$

We consider all the possibilities for k. In order to avoid non-simple groups A_n, we assume that $n \geqslant 10$. The cases $5 \leqslant n \leqslant 9$

can be checked manually using the information from [12] or with the help of GAP.

$k = 1$. In this case, $H = A_{n-1}$ is a simple group and it follows from the proof of [4, Theorem 53] that B must be splitting.

$k = 5$. By [25, Theorem 1], there is no 5-homogeneous but not 5-transitive finite group. Therefore, L is 5-transitive, and, by [9, Theorem 5.3], L must be one of the Mathieu groups M_{12} or M_{24}. Mathieu groups are simple, and we do not have a non-splitting RB-operator.

$k = 4$. Observe that the Mathieu groups M_{11} and M_{23} are the only finite 4-transitive groups, which are not 5-transitive and so have not been considered. Since these two groups are simple, we need to consider 4-homogeneous but not 4-transitive groups. By [25, Theorem 1], we have $L \in \{PSL_2(8), P\Gamma L_2(8), P\Gamma L_2(32)\}$.

Since $n \geqslant 10$, we need to consider only the case $L = P\Gamma L_2(32)$. By [25], we have that $L = P\Gamma L_2(32)$ acts sharply 3-transitively on $\Omega = \{1, 2, \ldots, 33\}$. Since the only proper normal subgroup of L is $PSL_2(32)$, we have

$$\mathrm{Ker}(B) = PSL_2(32) \qquad \text{and} \qquad |P\Gamma L_2(32) : PSL_2(32)| = 5.$$

Then,

$$R \simeq \mathbb{Z}_5 \qquad \text{and} \qquad R \cdot \mathrm{Ker}(B) = \mathrm{Im}(\widetilde{B}),$$

since $(|R|, |\mathrm{Ker}(B)|) = 1$. Therefore,

$$G = \mathrm{Im}(B) \cdot \mathrm{Ker}(B) = H \cdot PSL_2(32)$$

is the exact factorization. Since $PSL_2(32)$ acts sharply 3-transitively on Ω, we get that $H = A_{30}$, see [34, Theorem A(I)]. Thus, H is simple, and we do not have a non-splitting RB-operator.

$k = 2$. In this case, $A_{n-2} \trianglelefteq H \leqslant (S_{n-2} \times S_2) \cap A_n$. Since H is not simple, we have

$$\mathrm{Im}(B) = H = (S_{n-2} \times S_2) \cap A_n \simeq S_{n-2}.$$

The only proper normal subgroup of S_{n-2} is A_{n-2}. Therefore

$$\mathrm{Ker}(\widetilde{B}) = A_{n-2} \qquad \text{and} \qquad |R| = |S_{n-2} : A_{n-2}| = 2.$$

(a) Assume that $R \not\leqslant \mathrm{Ker}(B)$. By Lemma 5.2 (b) we have the exact factorization

$$G = \mathrm{Im}(B)\,\mathrm{Ker}(B) = S_{n-2} \cdot K.$$

According to [34, Theorem A(II)], we have that $K = ASL(1, q)$, where $q \equiv 3 \pmod 4$. Since

$$\mathrm{Ker}(B) \trianglelefteq \mathrm{Im}(\widetilde{B}) \qquad \text{and} \qquad |\mathrm{Im}(\widetilde{B}) : \mathrm{Ker}(B)| = |R| = 2,$$

it follows that $\mathrm{Im}(\widetilde{B}) = AGL(1, q)$. However, $AGL(1, q)$ contains odd permutations; a contradiction.

(b) Assume that $R \not\leqslant \mathrm{Ker}(\widetilde{B})$. By Lemma 5.2 (b) we have the exact factorization

$$G = \mathrm{Im}(\widetilde{B})\,\mathrm{Ker}(\widetilde{B}) = L \cdot A_{n-2}.$$

According to [34, Theorem A(I)], L is a sharply 2-transitive group. Since $|\mathrm{Im}(\widetilde{B}) : \mathrm{Ker}(B)| = 2$, L must contain a normal subgroup of index 2 and we may apply Corollary 3.3.

At first, consider the case (1) of Corollary 3.3, where

$$L = L(m, q, t) = FN.$$

Then we have the following conditions:

(1) Each prime divisor of m divides $q - 1$.

(2) If 4 divides m, then 4 divides $q - 1$.

(3) $q \equiv 3 \pmod 4$.

Since $q \equiv 3 \pmod 4$, then condition (2) is equivalent to the condition $m \equiv 2 \pmod 4$ and we have the conditions (i)–(iii) of the theorem. By Corollary 3.3(1), $L = FN$ has two non-isomorphic normal subgroups FS_1 and FS_2.

Thus, we apply Remark 5.4 and get two non-equivalent RB-operators on G (see Examples 7.2 and 7.3 below).

The cases (2) and (3) of Corollary 3.3 provide two other sharply 2-transitive groups $L = FN$ of degree $n = 7^2$ and $n = 23^2$, respectively. Each of these groups has only one normal subgroup of index 2, and again by Remark 5.4 we get one RB-operator in each case. Note that, if $n = 7^2$, we have two non-isomorphic sharply 2-transitive groups

$$L_1 = L(m, q, t) = L(2, 7, 1) \quad \text{and} \quad L_2 = FN$$

with $N \simeq SL_2(3).2$. As it was mentioned above, L_1 provides two non-equivalent RB-operators on G and L_2 provides the third one. Since $L = \mathrm{Im}(\widetilde{B})$ and $L_1 \not\simeq L_2$, we have three non-equivalent RB-operators on $G = A_{7^2}$. Similarly, we get three non-equivalent RB-operators on $G = A_{23^2}$.

k = 3. In this case, we have that $A_{n-3} \trianglelefteq H \leqslant (S_{n-3} \times S_3) \cap A_n$ and L is 3-homogeneous. Since H is not simple, we have

$$H \in \big\{(S_{n-3} \times S_3) \cap A_n,\ (S_{n-3} \times S_2) \cap A_n,\ A_{n-3} \times A_3\big\}.$$

(a) At first, consider the case $H = (S_{n-3} \times S_2) \cap A_n \simeq S_{n-3}$. The only proper normal subgroup of H is A_{n-3}. Therefore

$$\mathrm{Ker}(\widetilde{B}) = A_{n-3},\ |R| = |H : \mathrm{Ker}(\widetilde{B})| = 2,$$

and

$$|\mathrm{Im}(\widetilde{B})| = |L| = \frac{|G| \cdot |R|}{|H|} = \frac{(n!/2) \cdot 2}{(n-3)!} = n(n-1)(n-2).$$

Then L is a sharply 3-transitive group. Such groups have degree $q + 1 = p^r + 1$, for some prime p. It follows that, if $p = 2$, by [23, Theorem 2.1], $L \simeq PSL_2(q)$ is simple, which is not the case.

Let p be an odd prime. By [23, Theorem 2.6], we have either $L = PGL_2(q)$, or r is even and $L = M(p^r) \simeq PSL_2(q).2$. In

both cases, $\mathrm{PSL}_2(q)$ is a subgroup of index 2 in L. Since $\mathrm{PGL}_2(q)$ contains an element g of order $q+1$, we have $g \notin \mathrm{A}_{q+1} = \mathrm{A}_n$ and $\mathrm{L} \neq \mathrm{PGL}_2(q)$.

The group $\mathrm{L} = \mathrm{M}(p^r)$ acts on the projective line

$$\Omega = \mathrm{GF}(p^r) \cup \{\infty\}$$

(see [23, Example 1.3]). The stabilizer L_∞ is a sharply 2-transitive Frobenius group of odd degree q. This case was considered above, and we have the conditions (i)–(iii) on the numbers m and q.

Note that, under these conditions, we have the exact factorization $\mathrm{G} = \mathrm{A}_{n-3} \cdot \mathrm{L}$, where $\mathrm{Ker}(\widetilde{\mathrm{B}}) = \mathrm{A}_{n-3} \trianglelefteq \mathrm{H} = (\mathrm{S}_{n-3} \times \mathrm{S}_2) \cap \mathrm{A}_n$ and $\mathrm{Ker}(\mathrm{B}) = \mathrm{PSL}_2(q) \trianglelefteq \mathrm{L} = \mathrm{M}(q^m)$. Now we can apply Remark 5.4 to get one RB-operator in each case.

(b) $\mathrm{H} = (\mathrm{S}_{n-3} \times \mathrm{S}_3) \cap \mathrm{A}_n \simeq (\mathrm{A}_{n-3} \times \mathrm{A}_3) : \mathbb{Z}_2$. We have

$$|\mathrm{R}| = \frac{|\mathrm{H}| \cdot |\mathrm{L}|}{|\mathrm{G}|} = \frac{(n-3)! \cdot 3 \cdot |\mathrm{L}|}{(n!/2)} = 3 \cdot \frac{2|\mathrm{L}|}{(n-2)(n-1)n}.$$

If L is 3-transitive, then $n(n-1)(n-2)$ divides L. If L is not 3-transitive, then $|\mathrm{L}|$ is divisible by $\mathrm{L} = A\Gamma\mathrm{L}_1(32)$ or

$$|\mathrm{PSL}_2(q)| = (q-1)q(q+1)/2 = (n-2)(n-1)n/2$$

(see [25, Theorem 1 (ii), (iii)]). Since $|A\Gamma\mathrm{L}_1(32)| = 32 \cdot 31 \cdot 5$, we have $|\mathrm{R}| = 30/33$ and this case is impossible. In two other cases, we obtain that 3 divides $|\mathrm{R}| = |\mathrm{Im}(\mathrm{B}) : \mathrm{Ker}(\widetilde{\mathrm{B}})|$.

On the other hand, $\mathrm{Im}(\mathrm{B}) = \mathrm{H} = (\mathrm{A}_{n-3} \times \mathrm{A}_3) : \mathbb{Z}_2$ has only three proper normal subgroups: $\mathrm{A}_{n-3} \times \mathrm{A}_3$, A_{n-3}, and A_3.

Since $|\mathrm{H} : (\mathrm{A}_{n-3} \times \mathrm{A}_3)| = 2$, the case $\mathrm{Ker}(\widetilde{\mathrm{B}}) = \mathrm{A}_{n-3} \times \mathrm{A}_3$ is impossible.

If $\mathrm{Ker}(\widetilde{\mathrm{B}}) = \mathrm{A}_3$ then $|\mathrm{R}| = |\mathrm{Im}(\mathrm{B})|/3 = (n-3)!$, a contradiction with $\mathrm{R} \leqslant \mathrm{L}$.

Assume that $\mathrm{Ker}(\widetilde{\mathrm{B}}) = \mathrm{A}_{n-3}$. Then $\mathrm{R}| = |\mathrm{Im}(\mathrm{B}) : \mathrm{Ker}(\widetilde{\mathrm{B}})| = 6$

and

$$|L| = \frac{|G| \cdot |R|}{|H|} = \frac{(n!/2) \cdot 6}{((n-3)!/2) \cdot 6} = n(n-1)(n-2).$$

Then L is a sharply 3-transitive group. According to case (a) we have $L \simeq PSL_2(q).2$. Therefore, L has proper normal subgroups only of index 2. It is a contradiction with

$$|R| = |\mathrm{Im}(\widetilde{B}) : \mathrm{Ker}(B)| = |L : \mathrm{Ker}(B)| = 6,$$

(c) $H = A_{n-3} \times A_3$. The only proper normal subgroups of H are A_{n-3} and A_3. If $\mathrm{Ker}(\widetilde{B}) = A_3$ then

$$|R| = \frac{|H|}{|A_3|} = \frac{(n-3)!}{2},$$

a contradiction with $R \leqslant L$.

Therefore, $\mathrm{Ker}(\widetilde{B}) = A_{n-3}$ and $|R| = |H : \mathrm{Ker}(\widetilde{B})| = 3$. We have

$$|\mathrm{Im}(\widetilde{B})| = |L| = \frac{|G| \cdot |R|}{|H|} = \frac{(n!/2) \cdot 3}{((n-3)!/2) \cdot 3} = n(n-1)(n-2).$$

Thus, L is a sharply 3-transitive group. According to case (a) we have $L \simeq PSL_2(q).2$. Therefore, L has proper normal subgroups only of index 2. It is a contradiction with

$$|R| = |\mathrm{Im}(\widetilde{B}) : \mathrm{Ker}(B)| = |L : \mathrm{Ker}(B)| = 3,$$

which completes the proof. □

Example 7.2 We start with an exact factorization

$$A_9 = \mathrm{Ker}(B) \cdot \mathrm{Im}(B) = A_7 \cdot L,$$

where $A_7 = \langle (1234567), (123) \rangle$ and

$$L = \langle (1456)(2789), (1683)(2579) \rangle \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) : Q_8.$$

Then

$$H = \mathrm{Im}(\widetilde{B}) = (S_7 \times S_2) \cap A_9 = \langle A_7, r \rangle,$$

where $r = (17)(25)(34)(89)$. Note that $R = H \cap L = \langle r \rangle$. The group L has three isomorphic subgroups of index 2, and we choose one of them,

$$\mathrm{Ker}(\widetilde{B}) = S = \langle (167)(238)(459), (1683)(2579) \rangle \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) : \mathbb{Z}_4.$$

Then the RB-operator B on A_9 is defined by Remark 5.4. Namely, each $x \in A_9$ has the form

$$x = kl = kt^{\delta}y,$$

where $k \in \mathrm{Ker}(B)$, $y \in \mathrm{Ker}(\widetilde{B})$, and $\delta \in \{0, 1\}$. The operator B acts as follows:

$$B(x) = B(kt^{\delta}y) = l^{-1}r^{\delta}.$$

The following example provides an infinite series of non-splitting Rota–Baxter operators on A_n.

Example 7.3 Let $m = 2$, $q = p$ be a prime, and $p \equiv 3 \pmod 4$. There is an infinite number of such primes p and the conditions (i)–(iii) of Theorem 7.1 hold. For every such p we get a Rota–Baxter operator on A_{p^2} as in Example 7.2.

We start with an exact factorization

$$A_n = \mathrm{Ker}(B) \cdot \mathrm{Im}(B) = A_{n-2} \cdot L,$$

where L is a sharply 2-transitive group. Then

$$H = \mathrm{Im}(\widetilde{B}) = (S_{n-2} \times S_2) \cap A_n = \langle A_{n-2}, r \rangle,$$

where $r \in R = H \cap L$. The group L has two non-isomorphic subgroups of index 2 and we choose one of them as $\mathrm{Ker}(\widetilde{B})$. Denote $S = \mathrm{Ker}(\widetilde{B})$.

Observe that each $x \in A_n$ has the form $x = kl = kt^{\delta}y$, where $k \in \mathrm{Ker}(B)$, $y \in \mathrm{Ker}(\widetilde{B})$, and $\delta \in \{0, 1\}$. The operator B

again acts by the formula (5.2). Let us clarify the structure of the descendent group $A_n^{(\circ)}$ (2.2). We have

$$A_n^{(\circ)} = A_{n-2} \rtimes L = (A_{n-2} \times S^{op}).2,$$

where for all $h \in A_{n-2}$, $l \in L$ one computes

$$l \circ h = lB(l)hB(l)^{-1} = r^{\delta} h r^{\delta} l = h^{r^{\delta}} l = h^{r^{\delta}} \circ l;$$

the product $\circ$ on A_{n-2} coincides with $\cdot$; the product $\circ$ on the set S is antiisomorphic to $\cdot$, i.e. $s \circ s' = s's$.

The authors can make the GAP code used in this study available upon request.

Acknowledgements

The authors are grateful to Andrey Mamontov for the helpful discussions and to the anonymous referee for the useful remarks. The study was supported by a grant from the Russian Science Foundation n.23-71-10005 (see `https://rscf.ru/project/23-71-10005/`).

REFERENCES

[1] M. Aguiar: "Pre-Poisson algebras", *Lett. Math. Phys.* 54 (2000), 263–277.

[2] C. Bai – O. Bellier – L. Guo – X. Ni: "Splitting of operations, Manin products, and Rota–Baxter operators", *Int. Math. Res. Not. IMRN* 3 (2013), 485–524.

[3] G. Baxter: "An analytic problem whose solution follows from a simple algebraic identity", *Pacific J. Math.* 10 (1960), 731–742.

[4] V.G. Bardakov – V. Gubarev: "Rota–Baxter operators on groups", *Proc. Indian Acad. Sci.* 133 (2023), Paper No. 4, 29pp.

[5] V.G. Bardakov – V. Gubarev: "Rota-Baxter groups, skew left braces, and the Yang–Baxter equation", *J. Algebra* 596 (2022), 328–351.

[6] A.A. Belavin – V.G. Drinfel'd: "Solutions of the classical Yang–Baxter equation for simple Lie algebras", *Functional Anal. Appl.* 16 (1982), 159–180.

[7] N.P. Byott: "Hopf–Galois structures on Galois field extensions of degree pq", *J. Pure Appl. Algebra* 188 (2004), 45–57.

[8] N.P. Byott – F. Ferri: "On the number of quaternion and dihedral braces and Hopf–Galois structures", *J. Algebra* 665 (2025), 72–102.

[9] P.J. Cameron: "Finite permutation groups and finite simple groups", *Bull. Lond. Math. Soc.* 13 (1981), 1–22.

[10] P.J. Cameron: "Permutation Groups", *Cambridge University Press*, Cambridge (1999).

[11] F. Catino – M. Mazzotta – P. Stefanelli: "Rota–Baxter operators on Clifford semigroups and the Yang–Baxter equation", *J. Algebra* 622 (2023), 587–613.

[12] J.H. Conway – R.T. Curtis – S.P. Norton – R.A. Parker – R.A. Wilson: "ATLAS of Finite Groups", *Oxford University Press*, Eynsham (1985).

[13] T. Crespo – D. Gil-Muñoz – A. Rio – M. Vela: "Inducing braces and Hopf Galois structures", *J. Pure Appl. Algebra* 227 (2023), 16pp.

[14] A. Das – N. Rathee: "Extensions and automorphisms of Rota–Baxter groups", *J. Algebra* 636 (2023), 626–665.

[15] The GAP Group: "GAP – Groups, Algorithms, and Programming", v4.13.1 (2024).

[16] M.E. Goncharov: "Rota–Baxter operators on cocommutative Hopf algebras", *J. Algebra* 582 (2021), 39–56.

[17] M.E. Goncharov – V. Gubarev: "Double Lie algebras of nonzero weight", *Adv. Math.* 409 (2022), 30pp.

[18] M.E. Goncharov – P.S. Kolesnikov: "Simple finite-dimensional double algebras", *J. Algebra* 500 (2018), 425–438.

[19] T. Grundhöfer – C. Hering: "Finite nearfields classified, again", *J. Group Theory* 20 (2017), 829–839.

[20] L. Guarnieri – L. Vendramin: "Skew braces and the Yang–Baxter equation", *Math. Comp.* 86 (2017), 2519–2534.

[21] L. Guo: "An Introduction to Rota–Baxter Algebra", *Higher Education Press*, Beijing 4 (2012).

[22] L. Guo – H. Lang – Y. Sheng: "Integration and geometrization of Rota–Baxter Lie algebras", *Adv. Math.* 387 (2021), 34pp.

[23] B. Huppert – N. Blackburn: "Finite Groups III", *Springer*, Berlin (1982).

[24] J. Jiang – Y. Sheng – C. Zhu: "Lie theory and cohomology of relative Rota–Baxter operators", *J. Lond. Math. Soc.* 109 (2024), 34pp.

[25] W. Kantor: "k-Homogeneous groups", *Math. Z.* 124 (1972), 261–265.

[26] P. Kleidman – M. Liebeck: "The Subgroup Structure of the Finite Classical Groups", *Cambridge University Press*, Cambridge (1990).

[27] M.W. Liebeck – C.E. Praeger – J. Saxl: "The maximal factorizations of the finite simple groups and their automorphism groups", *Mem. Am. Math. Soc.* 86 (1990), 155pp.

[28] A. Odesskii – V. Rubtsov – V. Sokolov: "Double Poisson brackets on free associative algebras", *Contemp. Math.* 592 (2013), 225–239.

[29] D.S. Passman – W.A. Benjamin: "Permutation Groups", *Dover*, Mineola, NY (2012).

[30] N. Rathee – M. Singh: "Relative Rota–Baxter groups and skew left braces", *Forum Math.* 37 (2025), 919–935.

[31] M.A. Semenov-Tyan-Shanskii: "What a classical r-matrix is?", *Functional Anal. Appl.* 17 (1983), 259–272.

[32] A. Smoktunowicz – L. Vendramin: "On skew braces (with an appendix by N. Byott and L. Vendramin)", *J. Comb. Algebra* 2 (2018), 47–86.

[33] A.V. Vasil'ev: "On finite groups isospectral to simple classical groups", *J. Algebra* 423 (2015), 318–374.

[34] J. Wiegold – A. Williamson: "The factorisation of the alternating and symmetric groups", *Math. Z.* 175 (1980), 171–179.

Alexey Galt
Novosibirsk State University
Pirogova str. 1, 630090, Novosibirsk (Russia)
Sobolev Institute of Mathematics
Acad. Koptyug ave. 4, 630090, Novosibirsk (Russia)
e-mail: galt84@gmail.com

Vsevolod Gubarev (*corresponding author*)
Novosibirsk State University
Pirogova str. 1, 630090, Novosibirsk (Russia)
Sobolev Institute of Mathematics
Acad. Koptyug ave. 4, 630090, Novosibirsk (Russia)
e-mail: wsewolod89@gmail.com



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 63–71 ISSN: 2499-1287
DOI: 10.32037/agta-2026-004

About Nilpotent Profinite Groups Largely Satisfying a Word Equation

Meisam Soleimani Malekan

(*Received March 8, 2024; Accepted May 28, 2024 — Communicated by Pavel Shumyatsky*)

Abstract

We show that in a nilpotent profinite group, the set of answers of a word equation has nonempty interior, provided that this set has a positive Haar measure. This fact shows that the conjecture proposed by Lévai and Pyber is true for nilpotent profinite groups.

Mathematics Subject Classification (2020): 20E18, 20P05
Keywords: compact group; profinite group; large subset

1 Introduction

The following conjecture was proposed by Lévai and Pyber in [7].

Conjecture 1.1 *The solutions of equation* $x^n = 1$ *in a profinite group* G *has positive Haar measure if and only if it's interior is nonempty.*

This conjecture is Problem 14.53 in [8]. In that problem, it is pointed out that it would be interesting to see whether similar

results hold for profinite groups in which the set of solutions of some word equation has positive measure.

In [1], the authors have shown that the correctness of this conjecture results in the existence of the universal upper bound on the index of generalized Hughes–Thompson subgroup of finite groups whenever it is non-trivial. It is known that the latter is widely open even for all primes $n = p > 5$. Recall that, for any finite group G and any positive integer n, the generalized Hughes–Thompson subgroup is defined as the subgroup

$$\langle x \in G : x^n \neq 1 \rangle$$

of G (see Chapter 7 of [6]).

So far, we know that Conjecture 1.1 holds for $n = 2$ and $n = 3$ (see [7] and [1]); in these two cases, first it is shown that the profinite group G is virtually nilpotent and then the correctness of the conjecture is proven for nilpotent groups. In this article, we show that if a nilpotent profinite group that satisfies a word equation on a set of positive Haar measure, then this set should have nonempty interior (see Theorem 3.1). We also show that if G is a compact group satisfies the equation $x^n = 1$ on a set of positive Haar measure, then $Z(G)$ and G/G' are of finite exponent, where $Z(G)$ and G' stands for the center and commutator subgroup of G, respectively.

2 Preliminaries

Let us begin by introducing the following notion of largeness, which was introduced in [4].

Definition 2.1 A subset X of a group G is called k-*large*, for a positive integer k, if the intersection of any k left translates of X is non-empty.

We also require the following definition.

Definition 2.2 Let m and n be positive integers. Then for all $\mathbf{x} = (x_1, \ldots, x_m)$ in G^m and $\Sigma = (\sigma_1, \ldots, \sigma_n)$ in $\mathrm{Aut}(G)^n$, we define $y := x^{\Sigma} \in G^{mn}$ by

$$y_{(i-1)n+j} = x_i^{\sigma_j}, \quad 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n.$$

Let $w : G^{mn} \to G$ be a word map on G. We call the following map, a *twisted word map*:

$$G^m \to G,\ x \mapsto w\big(x^{\Sigma}\big)$$

The following theorem differs from [5, Theorem 6.5] only by a minor modification.

Theorem 2.3 *Let G be a nilpotent group of class at most k and*

$$w : G^r \times G^s \to G,$$

with $r > 0$, a twisted word map on G. If the set

$$\big\{x \in G^r : w(x, g) = c\big\}$$

is 2^k-large, for constants $g \in G^s$ and $c \in G$, then it should be whole of G^r.

With the notations in the above theorem, we write "G satisfies 2^k-largely an equation $w(x, g) = c$" instead of the expression "the set $\{x \in G^r : w(x, g) = c\}$ is 2^k-large".

Remark 2.4 If it is added in [5, Definition 6.1.] that for a supercommutator v and an automorphism ϕ of the group G, v^{ϕ} is also a supercommuter with the same variable set as v, and also the hypothesis of subgroup H being normal in [5, Lemma 6.3.] is replaced by "being characteristic", the proofs in section 6 of [5] will still be correct, and therefore, in the key Theorem 6.5., we can replace "word map" with "twisted word map", as we did in Theorem 2.3.

3 Nilpotent compact groups largely satisfying a word equation

In the following, we denote the normalized Haar measure of a compact group G by m_G, and we drop the index G, if there is no ambiguity. Also, we assume all automorphisms used to define twisted word maps to be continuous.

In this section, we prove the main result of the article which states that Conjecture 1.1 holds for nilpotent profinite groups.

Theorem 3.1 *Let G be a nilpotent profinite group. Assume that G satisfies a word equation $w = 1$ on a set of positive Haar measure, i.e.*

$$m_{G^d}\big(\{g \in G^d : w(g) = 1\}\big) > 0.$$

Then $\{g \in G^d : w(g) = 1\}$ has nonempty interior.

We start with the following simple result.

Lemma 3.2 *Let G be a compact group and $A \subseteq G$ be a measurable subset. If $m(A) > 1 - \frac{1}{n}$, then A is n-large.*

Proof — By [1, Lemma 2.1] we have $m\big(\bigcap_{k=1}^{n} g_k A\big) > 0$, so, in particular, $\bigcap_{k=1}^{n} g_k A$ is nonempty. □

By the above lemma and Theorem 2.3 we obtain the following result.

Theorem 3.3 *Let G be a nilpotent compact group and $w : G^d \to G$ a twisted word map. Then*

$$m_{G^d}\big(\{g \in G^d : w(g) = c\}\big) \in \left[0, \frac{2^k - 1}{2^k}\right] \cup \{1\},$$

where k is the nilpotency class of G.

Remark 3.4 For large values of k, the gap obtained in the above corollary becomes very small. The author does not know if it can be improved or not, and has no idea about it; but this

gap, even if very small, plays an essential role in proving the main theorem of the paper.

Now we are in a position to prove Theorem 3.1.

Proof of Theorem 3.1 — Let G be a k-step nilpotent group. Put

$$\mathfrak{A} := \{g \in G^d : w(g) = 1\}.$$

By [1, Lemma 2.4], there exists $t := (t_1, \dots, t_d) \in \mathfrak{A}$ and open normal subgroup N of G^d, such that

$$m_N\big(N \cap t^{-1}\mathfrak{A}\big) > 1 - 2^{-k}.$$

But,

$$N \cap t^{-1}\mathfrak{A} = \big\{x \in N : w(tx) = 1\big\},$$

and one can easily see, using the elementary equations

$$(tx)^n = t^n \prod_{j=1}^{n} x^{t^{n-j}}, \quad ts = st[t, s]$$

that the map

$$N^d \to N,\ x \mapsto w(tx)$$

is a twisted word map on N. Now, Theorem 3.3 implies that

$$w(tx) = 1,$$

for all $x \in N$, whence

$$N \cap t^{-1}\mathfrak{A} = N$$

and the proof is complete. □

In the two following propositions, we give some results about the nilpotent quotients and closed nilpotent normal subgroups of a compact group satisfying largely in a word.

Proposition 3.5 *Let* G *be a compact group and* w *be a word on* G.

Assume that

$$m_{G^d}\big(\{g \in G^d : w(g) = c\}\big) > 1 - 2^{-d}.$$

Then w is an equation on all compact quotients of G which are nilpotent of class at most k.

Proof — Let H be an k-step nilpotent group and $\psi : G \to H$ be a quotient map. By [2, Lemma 2.3.], we obtain

$$m_{H^d}\big(\{h \in H^d : w(h) = \psi(c)\}\big) \geqslant m_{G^d}\big(\{g \in G^k : w(g) = c\}\big).$$

Therefore, the result is obtained by Theorem 3.3. □

Proposition 3.6 *Let G be a compact group and w be a word on G. Assume that*

$$m_{G^d}\big(\{g \in G^d : w(g) = 1\}\big) > 1 - 2^{-k},$$

and N is a closed k-step nilpotent normal subgroup of G. Then a coset of N satisfies the word equation $w = 1$.

Proof — Put $\mathfrak{A} := \{g \in G^d : w(g) = 1\}$. By [3, Theorem 2.49], we obtain

$$m_{G^d}(\mathfrak{A}) = \int_{\frac{G^d}{N^d}} m_{N^d}\big(N^d \cap g^{-1}\mathfrak{A}\big)\, d\overline{g},$$

where $d\overline{g}$ is the integration with respect to m_{G^d/N^d}. This equation reveals the existence of $t := (t_1, \ldots, t_k) \in \mathfrak{A}$ such that

$$m_{N^d}\Big(N^d \cap t^{-1}\mathfrak{A}\Big) > 1 - 2^{-k}.$$

But,

$$N^d \cap t^{-1}\mathfrak{A} = \big\{x \in N^d : w(tx) = 1\big\},$$

and, as we have seen in the proof of Theorem 3.1, the map

$$N^d \to N,\ x \mapsto w(tx)$$

is a twisted word map on N, therefore, the result is obtained from Theorem 3.3. □

As a result of the above propositions, we have: As a consequence of the above propositions, we have the following result.

Corollary 3.7 *Let G be a compact group, w be a word on G and*

$$m_{G^d}\big(\{g \in G^d : w(g) = 1\}\big) > \frac{1}{2}.$$

Then w is an equation on $G/\overline{G'}$ and $Z(G)$, where $\overline{G'}$ is the closure of G' in G.

Proof — Only note that $w(tx) = 1$ and $w(t) = 1$ implies $w(x) = 1$ provided $x \in Z(G)^d$. □

Let us conclude the paper with the following result.

Theorem 3.8 *Let G be a compact group such that the solutions set of $x^n = 1$ has positive Haar Measure α. Then $G/\overline{G'}$ and $Z(G)$ are of finite exponents at most $n\lfloor\frac{1}{\alpha}\rfloor!$.*

Proof — Put

$$\mathfrak{A} := \{x \in G : w(x) = x^n = 1\}.$$

For $t \in Z(G)$, $w(t\mathfrak{A}) = t^n$, so the subgroup $\{t^n : t \in Z(G)\}$ should be finite of size at most $\lfloor\frac{1}{\alpha}\rfloor$, because $w^{-1}(\{t^n\})$, $t \in Z(G)$ is of Haar measure at least α.

In a similar manner, $\{t^n\overline{G'} : t \in G\}$ should be a finite subgroup of $G/\overline{G'}$ of size at most $\lfloor\frac{1}{\alpha}\rfloor$. □

Acknowledgement

This research was in part supported by a grant from the Institute for Research in Fundamental Sciences (IPM) (No. 1404420112). I am grateful to Sean Eberhard for reading the article carefully

and for the suggestions that led to a great improvement of the article, especially Definition 2.2 is one of Sean's suggestions.

REFERENCES

[1] A. Abdollahi – M.S. Malekan: "Profinite groups with many elements of bounded order", *Adv. Group Theory Appl.* 13 (2022), 71–81.

[2] A. Abdollahi – M.S. Malekan: "Nilpotent probability of compact groups", *J. Algebra* 631 (2023), 136–147.

[3] G.B. Folland: "A Course in Abstract Harmonic Analysis", *CRC Press*, Boca Raton, FL (1995).

[4] J. Khaled – F.O. Wagner: "Largeur et nilpotence", *Comm. Algebra* 28 (2000), 2869–2885.

[5] J. Khaled – F.O. Wagner: "Largeness and equational probability in groups", *Ann. Math. Blaise Pascal* 27 (2020), 1–17.

[6] E.I. Khukhro: "Nilpotent Groups and Their Automorphisms", *de Gruyter*, Berlin (1993).

[7] L. Lévai – L. Pyber: "Profinite groups with many commuting pairs or involutions", *Arch. Math.* (*Basel*), 75 (2000), 1–7.

[8] V.D. Mazurov – E.I. Khukhro: "The Kourovka Notebook: Unsolved Problems in Group Theory", 19th edition, *Russian Academy of Sciences*, Novosibirsk (2019).

Meisam Soleimani Malekan

Department of Mathematics, Faculty of Science
Shahid Rajaee Teacher Training University
16785-136, Tehran (Iran)

School of Mathematics
Institute for Research in Fundamental Sciences (IPM)
P.O. Box 19395-5746, Tehran (Iran)

e-mail: m.soleimani@sru.ac.ir;
msmalekan@gmail.com



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 73–83 ISSN: 2499-1287
DOI: 10.32037/agta-2026-005

On Finite Groups Factorized by Weakly $\mathbb{X}$-Subnormal Subgroups

S.I. Lendzenkova

(*Received May 29, 2024; Accepted Aug. 1, 2024 — Communicated by Alexander Skiba*)

Abstract

Let $\mathbb{X}$ be a nonempty set of natural numbers. A subgroup A of a finite group G is said to be $\mathbb{X}$-*subnormal* in G if there is a chain of subgroups

$$A = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_{n-1} \leqslant A_n = G,$$

where $|A_i : A_{i-1}| \in \mathbb{X}$, for all i. Besides, A is *weakly* $\mathbb{X}$-*subnormal* in G if $A = \langle U_1, U_2 \rangle$, where U_1 is subnormal and U_2 is $\mathbb{X}$-subnormal subgroups of G.

We establish the properties of weakly $\mathbb{X}$-subnormal subgroups and extend the known results on finite factorizable groups with $\mathbb{X}$-subnormal factors to finite factorizable groups with weakly $\mathbb{X}$-subnormal factors. In particular, we establish solvability and r-solvability of a finite group $G = AB$ with weakly $\mathbb{X}$-subnormal solvable or r-solvable subgroups A and B for some $\mathbb{X}$.

Mathematics Subject Classification (2020): 20D10, 20D20, 20E26

Keywords: finite group; r-solvable group; $\mathbb{X}$-subnormal subgroup; weakly $\mathbb{X}$-subnormal subgroup

1 Introduction

All groups in this paper are finite. We use the standard notation and terminology of [8]. In particular, $\mathbb{P}$ is the set of all primes.

Further in the text, $\mathbb{X}$ is a nonempty set of natural numbers closed with respect to divisors, i.e. $\mathbb{X}$ has the following property: If $x \in \mathbb{X}$

and a natural number y divides x, then $y \in \mathbb{X}$. Note that $1 \in \mathbb{X}$, and $\mathbb{P}^\infty := \{1\} \cup \mathbb{P}$ is one of such sets.

Recall that a subgroup A of a group G is said to be *semipermutable* [1] or *seminormal* in G if there exists a subgroup B in G such that $G = AB$ and A permutes with all subgroups U of B (that is, $AU = UA$). Besides, A is *weakly subnormal* in G (see [2]) if

$$A = \langle U_1, U_2 \rangle,$$

where U_1 is subnormal and U_2 is semipermutable subgroups of G. Moreover, A is $\mathbb{X}$-*subnormal* in G [12] (denoted by $\mathbb{X}$-sn G) if there is a chain of subgroups

$$A = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_{n-1} \leqslant A_n = G,$$

where $|A_i : A_{i-1}| \in \mathbb{X}$, for all i.

In this paper, we discuss some applications of the following generalization of $\mathbb{X}$-subnormality.

Definition 1.1 A subgroup A of a group G is *weakly* $\mathbb{X}$-*subnormal* in G if $A = \langle U_1, U_2 \rangle$, where U_1 is subnormal and U_2 is $\mathbb{X}$-subnormal subgroups of G.

It is clear that a $\mathbb{X}$-subnormal subgroup is weakly $\mathbb{X}$-subnormal in the group. In the alternating group of degree 6, the identity subgroup is subnormal, but not $\mathbb{X}$-subnormal for $\mathbb{X} = \mathbb{P}^\infty$. In addition, in a solvable group, each weakly subnormal subgroup is weakly $\mathbb{P}^\infty$-subnormal, see Lemma 3.5.

Groups factorized by weakly subnormal subgroups were studied in [2] and [11]. In particular, in [2, Theorem 1.4], supersolvability of a group $G = AB$ with the nilpotent derived subgroup and supersolvable weakly subnormal factors A and B is established. A metanilpotent group $G = AB$ with weakly subnormal multipliers of mutually simple indices is also supersolvable [11, Corollary 4.2]. Moreover, V.N. Tyutyanov and V.N. Knyagina studied groups factorized by r-solvable $\mathbb{X}$-subnormal subgroups (see [12]).

In this paper, we establish the properties of $\mathbb{X}$-subnormal and weakly $\mathbb{X}$-subnormal subgroups that allow us to extend many well-known results on groups with sets of $\mathbb{X}$-subnormal subgroups to groups with weakly $\mathbb{X}$-subnormal subgroups. In particular, we show solvability and r-solvability of a finite group $G = AB$ with weakly $\mathbb{X}$-subnormal solvable and, respectively, r-solvable subgroups A and B, for

some sets $\mathbb{X}$. So, for example, a group $G = AB$ is solvable if A and B are weakly $\mathbb{L}$-subnormal solvable subgroups, where $\mathbb{L}$ is the set that consists of all odd primes and numbers 2 and 4.

2 Auxiliary results

We use $\pi(G)$ to denote the set of all primes dividing the order of a group G, and $\mathbb{N}$ the set of all natural numbers. Let us denote by $O_\pi(G)$ the largest normal π-subgroup of G for $\pi \subseteq \pi(G)$. We write

$$X \leqslant Y, \qquad X < Y, \qquad X \lhd Y, \qquad X \lhd\lhd Y$$

if X is a subgroup, a proper subgroup, a normal subgroup, a subnormal subgroup of a group Y, respectively. Moreover, $|X|$ is the order of a group X and $|X : Y|$ is the index of $Y \leqslant X$. In addition, we use the following notation for a group X and its subgroup Y:

- Y_X is the largest normal subgroup of X contained in Y;
- Y_{sX} is the largest subnormal subgroup of X contained in Y.

Definition 2.1 Let G be a group and fix a prime $r \in \pi(G)$. If G contains a normal Sylow r-subgroup, then G is said to be r-*closed*. Moreover, G is called r-*solvable* if it has a normal series such that factors are either r-groups, or r'-groups.

Definition 2.2 A group G of order $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$, with $p_i \in \mathbb{P}$ and $p_1 > p_2 > \dots > p_n$, $\alpha_i \in \mathbb{N}$, $i = 1, \dots, n$, has a *Sylow tower of supersolvable type* if G has a normal subgroup of the order $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_i^{\alpha_i}$, for each $i = 1, 2, \dots, n$.

Lemma 2.3 (see [10], Lemma 1.2) *Let M be a maximal subgroup of a group G, then $M_G = M_{sG}$.*

Lemma 2.4 (see [8],[7]) *Let N be a normal subgroup of a group G and H is subnormal in G. Then the following assertions hold*:

(1) $HN/N \lhd\lhd G/N$ *and* $H \leqslant O_{\pi(H)}(G)$;

(2) *If H is solvable, then H^G is solvable.*

3 Properties of $\mathbb{X}$-subnormal and weakly $\mathbb{X}$-subnormal subgroups

Lemma 3.1 *Let* $T \leqslant U \leqslant G$, *let* U **X**-*sn* G *and let* $N \lhd G$. *The following statements hold*:

(1) *If* T $\mathbb{X}$-*sn* U, *then* T $\mathbb{X}$-*sn* G;

(2) $(U \cap N)$ $\mathbb{X}$-*sn* N *and* UN/N $\mathbb{X}$-*sn* G/N;

(3) UN $\mathbb{X}$-*sn* G;

(4) U $\mathbb{X}$-*sn* UN.

Proof — Statements (1)–(3) are proved in [5, Lemma 1].

(4) Since U is $\mathbb{X}$-subnormal in G, then there exists a chain of subgroups

$$U = U_0 < U_1 < \ldots < U_{n-1} < G$$

such that $|U_i : U_{i-1}| \in \mathbb{X}$, for each i. Let $U_{n-1} \leqslant U^\star < G$, $U^\star$ is a maximal subgroup in G. Moreover,

$$|G : U_{n-1}| = |G : U^\star||U^\star : U_{n-1}|.$$

Since $|G : U_{n-1}| \in \mathbb{X}$ and $\mathbb{X}$ are closed with respect to the divisors, then

$$|G : U^\star| \in \mathbb{X} \quad \text{and} \quad |U^\star : U_{n-1}| \in \mathbb{X}.$$

Therefore, $U^\star$ is a maximal subgroup in G in which U is $\mathbb{X}$-subnormal and $|G : U^\star| \in \mathbb{X}$. Let us use induction on the group order. We can assume that UN is a proper subgroup of G. If $UN \leqslant U^\star$, then by induction, U is $\mathbb{X}$-subnormal in UN. Let UN not be contained in $U^\star$. Then N is not contained in $U^\star$, $G = U^\star N$ and

$$|G : U^\star| = |N : (N \cap U^\star)| \in \mathbb{X}.$$

By Dedekind's identity, $U \leqslant UN \cap U^\star = U(N \cap U^\star) \leqslant UN$. Since

$$|UN : U(N \cap U^\star)| = \frac{|U||N||U \cap N \cap U^\star|}{|U \cap N||U||N \cap U^\star|} = |N : (N \cap U^\star)| \in \mathbb{X},$$

then $|UN : U(N \cap U^\star)| \in \mathbb{X}$. Applying inductions to the group $U^\star$ in which $N \cap U^\star$ is normal and U is $\mathbb{X}$-subnormal, we conclude that U is $\mathbb{X}$-subnormal in $U(N \cap U^\star)$. The subgroup U is $\mathbb{X}$-subnormal in UN by (1). □

Definition 3.2 (see [3]) A subgroup A of a group G is $K\mathbb{X}$-*subnormal* if there is a chain of subgroups

$$A = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_{n-1} \leqslant A_n = G$$

such that, for each $i > 0$, either A_{i-1} is normal in A_i or

$$|A_i : A_{i-1}| \in \mathbb{X}.$$

Lemma 3.3 *Let G be a solvable group and $\pi(G) \subseteq \mathbb{X}$. Then every $K\mathbb{X}$-subnormal subgroup of G is $\mathbb{X}$-subnormal in G.*

Proof — Let $\pi(G) \subseteq \mathbb{X}$ and let U be $K\mathbb{X}$-subnormal subgroup of a solvable group G. Then there is a chain of subgroups such that either U_{i-1} is normal in U_i, or $|U_i : U_{i-1}| \in \mathbb{X}$, for each i. Note that, if $|U_i : U_{i-1}| \in \mathbb{X}$, for each i, then U is $\mathbb{X}$-subnormal in G. Suppose that for some i, U_{i-1} is normal in U_i. Since U_i is solvable, then its composition series

$$U_{i-1} = V_0 < V_1 < \ldots < V_{m-1} < V_m = U_i$$

has indices $|V_j : V_{j-1}| \in \pi(G) \subseteq \mathbb{X}$, for each j. Repeating this compaction for every pair $U_{i-1} \lhd U_i$, we get the chain of subgroups in which all indices belong to $\mathbb{X}$. Therefore, U is $\mathbb{X}$-subnormal in G. □

Lemma 3.4 (1) *Every weakly $\mathbb{X}$-subnormal subgroup of a group G is a $K\mathbb{X}$-subnormal subgroup of G.*

(2) *If G is a solvable group and $\pi(G) \subseteq \mathbb{X}$, then each weakly $\mathbb{X}$-subnormal subgroup of G is an $\mathbb{X}$-subnormal subgroup of G.*

Proof — (1) Use induction on the group order. Let $U = \langle U_1, U_2 \rangle$ be a weakly $\mathbb{X}$-subnormal subgroup of G and M is a maximal subgroup of G containing U. Here U_1 is subnormal in G, and U_2 is $\mathbb{X}$-subnormal in G. According to Lemma 2.3, $M_{sG} = M_G$, therefore

$$U_1 \leqslant M_G,\ U = \langle U_1, U_2 \rangle \leqslant M_G U_2 \leqslant M < G.$$

Since U_2 is $\mathbb{X}$-subnormal in G, then U_2M_G is $\mathbb{X}$-subnormal in G, according to Lemma 3.1 (3). By Lemma 3.1 (4), U_2 is $\mathbb{X}$-subnormal in U_2M_G. Therefore, U is weakly $\mathbb{X}$-subnormal in U_2M_G. By induction, U is $K\mathbb{X}$-subnormal in U_2M_G. So, we obtain U $K\mathbb{X}$-sn U_2M_G and U_2M_G $\mathbb{X}$-sn G, it follows that U is $K\mathbb{X}$-subnormal in G.

(2) Applying (1) and Lemma 3.3, we obtain the claim. □

Lemma 3.5 *If H is a seminormal subgroup of a solvable group G, then H is $\mathbb{P}^\infty$-subnormal in G.*

Proof — By the definition of a seminormal subgroup, there exists a subgroup K, such that $G = HK$ and HL is a proper subgroup of G, for each $L < K$. Since K is solvable, its composition series has prime indices

$$1 = K_0 \leqslant K_1 \leqslant \ldots \leqslant K_{n-1} \leqslant K_n = K,$$

$$K_i \lhd K_{i+1}, \quad |K_{i+1} : K_i| \in \mathbb{P}, \ \ \forall\, i.$$

Since H is seminormal in G, then $HK_i = K_iH$ is a subgroup, for any i, and there is a chain of subgroups

$$1 = HK_0 \leqslant HK_1 \leqslant HK_2 \leqslant \ldots \leqslant HK_{n-1} \leqslant HK_n = H = G,$$

such that

$$|HK_{i+1} : HK_i| = \frac{|H||K_{i+1}|}{|H \cap K_{i+1}|} : \frac{|H||K_i|}{|H \cap K_i|} = \frac{|K_{i+1} : K_i|}{|H \cap K_{i+1} : H \cap K_i|} \in \{1\} \cup \mathbb{P}.$$

We conclude that H is $\mathbb{P}^\infty$-subnormal in G. □

4 On the product of weakly $\mathbb{X}$-subnormal subgroups

Fix a natural number t and a prime number r. Let

$$\mathbb{P}_r^t = \left\{p^i \mid p \in \mathbb{P}\backslash\{r\},\ i \in \{0\} \cup \mathbb{N}\right\} \cup \left\{r^j \mid j \in \{0\} \cup \mathbb{N},\ j \leqslant t\right\}.$$

For $r = t = 2$, we get the set $\mathbb{P}_2^2$, which consists of numbers 1, 2, 4 and all natural powers of odd primes. Let

$$\mathbb{P}^t = \{p^k \mid p \in \mathbb{P},\ k \in \{0, 1, \ldots, t\}\}.$$

For $t = 2$, we get the set $\mathbb{P}^2 = \{p^k \mid p \in \mathbb{P},\ k \in \{0, 1, 2\}\}$. The set

$$\mathbb{L} = \{2, 4\} \cup \{2n - 1 \mid n \in \mathbb{N}\}$$

consists of all odd primes and numbers 2 and 4.
Since the sets $\mathbb{P}_r^t$, $\mathbb{P}_2^2$, $\mathbb{P}^t$, $\mathbb{P}^2$, $\mathbb{L}$ and $\mathbb{P}^\infty$ are closed with respect to divisors, then Lemmas 3.1, 3.3 and 3.4 are valid for each of these sets.

Lemma 4.1 *In a solvable group* G*, a subgroup* H *is* $\mathbb{L}$*-subnormal in* G *if and only if* H *is* $\mathbb{P}_2^2$*-subnormal in* G*.*

Proof — Let H be an $\mathbb{L}$-subnormal subgroup of a solvable group G. Then there is a chain of subgroups

$$H = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_{n-1} \leqslant H_n = G$$

such that $|H_i : H_{i-1}| \in \mathbb{L}$. Let $H_{i-1} \leqslant K \leqslant H_i$, K is a maximal subgroup of H_i. Moreover,

$$|H_i : H_{i-1}| = |H_i : K||K : H_{i-1}| \in \mathbb{L}.$$

Since the set $\mathbb{L}$ is closed with respect to divisors, then $|H_i : K| \in \mathbb{L}$. In view of G is solvable, we have

$$|H_i : K| \in \mathbb{P}^\infty.$$

Therefore, $|H_i : K| \in \mathbb{P}_2^2$. Conducting the same reasoning with each pair of subgroups $H_{i-1} < H_i$, we obtain a maximal subgroup chain with indices from $\mathbb{P}_2^2$. It follows that H is $\mathbb{P}_2^2$-subnormal in G.

The converse is true due to the fact that $\mathbb{P}_2^2 \subseteq \mathbb{L}$. □

Let us observe that factorized groups with $\mathbb{X}$-subnormal factors were studied in [3],[4],[6],[9] and [12]. The obtained properties of weakly $\mathbb{X}$-subnormal subgroups allow to extend a lot of the results of these papers to factorizable groups with weakly $\mathbb{X}$-subnormal factors.

Theorem 4.2 *If* A *and* B *are weakly* $\mathbb{L}$*-subnormal solvable subgroups of a group* $G = AB$*, then* G *is solvable.*

Proof — Let $A = \langle A_1, A_2 \rangle$, $B = \langle B_1, B_2 \rangle$, where A_1, B_1 are subnormal subgroups of G, and A_2, B_2 are $\mathbb{L}$-subnormal in G. Since A_1 is subnormal in G, then A_1^G is solvable by Lemma 2.4. Similarly, B_1^G is solvable. Let $N = A_1^G B_1^G$. Then N is a solvable normal subgroup of G. The quotient group

$$G/N = (AN/N)(BN/N) = (A_2N/N)(B_2N/N),$$

where A_2N/N and B_2N/N are $\mathbb{L}$-subnormal subgroups of G/N according to Lemma 3.1 (2). By [4, Theorem 2], we obtain that G/N is solvable, and G is solvable. □

Note that Theorem 4.2 can also be proved in view of Lemma 3.4 (1) and [3, Theorem 4.2].

Corollary 4.3 *If A and B are $\mathbb{L}$-subnormal solvable subgroups of a group*

$$G = AB,$$

then A and B are $\mathbb{P}_2^2$-subnormal in G.

Proof — According to Theorem 4.2, G is solvable, and according to Lemma 4.1, A and B are $\mathbb{P}_2^2$-subnormal in G. □

In view of $\mathbb{P}^2 \subseteq \mathbb{P}_2^2 \subseteq \mathbb{L}$, and Theorem 4.2, we obtain the following results.

Corollary 4.4 *If A and B are weakly $\mathbb{P}_2^2$-subnormal solvable subgroups of a group $G = AB$, then G is solvable.*

Corollary 4.5 *If A and B are weakly $\mathbb{P}^2$-subnormal solvable subgroups of a group $G = AB$, then G is solvable.*

Example 4.6 The simple group $PSL(2,7) = S_4(C_7C_3)$ can be represented as the product of the solvable subgroups S_4 and C_7C_3, where S_4 is the symmetric group of degree 4, and C_7C_3 is a noncyclic group of order 21. The subgroup S_4 is weakly $\mathbb{P}^\infty$-subnormal in $PSL(2,7)$, and C_7C_3 is weakly $\mathbb{P}^3$-subnormal in $PSL(2,7)$. It follows that, in Corollaries 4.4 and 4.5, the assumptions of weakly $\mathbb{P}_2^2$-subnormality and weakly $\mathbb{P}^2$-subnormality of factors cannot be weakened to weakly $\mathbb{P}_2^3$- and weakly $\mathbb{P}^3$-subnormality, respectively.

Corollary 4.7 *Let r be the largest prime divisor of the order of a group G, let A and B be solvable r-closed weakly $\mathbb{P}^2$-subnormal subgroups of G, and let $G = AB$. If $r > 3$, then G is r-closed.*

Proof — According to Corollary 4.5, the group G is solvable, and A and B are $\mathbb{P}^2$-subnormal by Lemma 3.4 (2). By [4, Theorem 1 (2)], we obtain that G is r-closed. □

Example 4.8 In Corollary 4.7, the requirement $r > 3$ cannot be removed. For example, the symmetric group S_4 of degree 4 can be represented as the product of a weakly $\mathbb{P}^\infty$-subnormal subgroup of order 8 and a weakly $\mathbb{P}^2$-subnormal subgroup of order 3, but S_4 is not 3-closed.

Corollary 4.9 *If A and B are weakly $\mathbb{P}^2$-subnormal supersolvable subgroups of a group $G = AB$ and H is a Hall $\{2,3\}'$-subgroup of the group G, then H has a Sylow tower of supersolvable type and H is normal in G.*

Proof — By Corollary 4.5, G is solvable and, by Lemma 3.4 (2), A and B are $\mathbb{P}^2$-subnormal in G. By [4, Theorem 1 (3)], we obtain that H is normal in G and H has a Sylow tower of supersolvable type. □

Theorem 4.10 *Let A and B be weakly $\mathbb{X}$-subnormal subgroups of a group*

$$G = AB.$$

If A and B are r-solvable, then G is r-solvable in each of the following cases:

(1) $\mathbb{X} = \mathbb{P}_2^2$;

(2) $\mathbb{X} = \mathbb{P}^\infty$ *and* $r \in \pi(G)\backslash\{2,3,7\}$.

Proof — According to Lemma 3.4 (1), A and B are $K\mathbb{X}$-subnormal in G. Hence, if we assume (1), then G is r-solvable by [3, Theorem 2.2]. If we assume (2), then G is r-solvable by [3, Theorem 3.1]. □

Acknowledgements

The author is deeply grateful for the helpful suggestions and remarks of the referee. The author is supported by the Ministry of Education of the Republic Belarus (Grant no. 20211780 <Convergence-2025>).

REFERENCES

[1] W. Guo – K.P. Shum – A.N. Skiba: "X-semipermutable subgroups of finite groups", *J. Algebra* 315 (2007), 31–41.

[2] J. Huang – B. Hu – A.N. Skiba: "Finite groups with weakly subnormal and partially subnormal subgroups", *Sib. Math. J.* 62 (2021), 169–177.

[3] V.N. Kniahina – I.K. Chirik: "Finite factored groups with solvable $\mathbb{X}$-subnormal factors", *Probl. Fiz. Mat. Tekh.* 39 (2019), 76–80.

[4] V.N. Kniahina – V.S. Monakhov: "Finite factorizable groups with solvable $\mathbb{P}^2$-subnormal subgroups", *Sib. Math. J.* 54 (2013), 56–63.

[5] V.N. Kniahina – V.S. Monakhov: "Finite groups with given indices of 2-maximal subgroups", *J. Algebr. Appl.* 15 (2016), 1–5.

[6] V.N. Kniahina – V.S. Monakhov: "Finite groups with $\mathbb{P}$-subnormal Sylow subgroups", *Ukrainian Math. J.* 72 (2021), 1571–1578.

[7] J.C. Lennox – S.E. Stonehewer: "Subnormal Subgroups of Groups", *Clarendon*, Oxford (1987).

[8] V.S. Monakhov: "Introduction to the Theory of Finite Groups and their Classes", *Vyshejshaja Shkola*, Minsk (2006).

[9] V.S. Monakhov: "Finite factorizable groups with $\mathbb{P}$-subnormal v-supersolvable and sh-supersolvable factors", *Math. Notes* 111 (2022), 407–413.

[10] L.R. Nyhoff: "The influence on a finite group of the cofactors and subcofactors of its subgroups", *Trans. Amer. Math. Soc.* 154 (1971), 459–491.

[11] A.A. Trofimuk: "On finite groups factorizable by weakly subnormal subgroups", *Sib. Math. J.* 62 (2021), 1133–1139.

[12] V.N. Tyutianov – V.N. Kniahina: "Factorization of finite groups by r-solvable subgroups with given embeddings", *Ukrainian Math. J.* 66 (2014), 1431–1435.

Svetlana I. Lendzenkova
Department of Mathematics and Technologies of Programming
Francisk Skorina Gomel State University
Kirova Str. 119, 246019 Gomel (Belarus)
e-mail: slendenkova@mail.ru



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 85–116 ISSN: 2499-1287
DOI: 10.32037/agta-2026-006

The Period of Ducci Cycles on $\mathbb{Z}_{2^l}$ for Tuples of Length 2^k

Mark L. Lewis — Shannon M. Tefft

(*Received Aug. 20, 2024; Accepted Nov. 23, 2024 — Communicated by M.R. Dixon*)

Abstract

Let the Ducci function $D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ be defined as

$$D(x_1, x_2, \ldots, x_n) = (x_1 + x_2 \mod m, x_2 + x_3 \mod m, \ldots, x_n + x_1 \mod m)$$

and let the Ducci sequence of u be the sequence $\{D^\alpha(u)\}_{\alpha=0}^\infty$. In this paper, we will provide another proof that for $n = 2^k$ and $m = 2^l$, all Ducci sequences will end in $(0, 0, \ldots, 0)$ and additionally prove that this will happen in at most $2^{k-1}(l+1)$ iterations of D.

Mathematics Subject Classification (2020): 20D60, 11B83, 11B50

Keywords: Ducci sequence; modular arithmetic; length, period; n-number game

1 Introduction

Consider a function $D : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$, which we define as

$$D(x_1, x_2, \ldots, x_n) = (x_1 + x_2 \mod m, x_2 + x_3 \mod m, \ldots, x_n + x_1 \mod m).$$

Like [2, 10, 13], we call D the *Ducci function* and for a given tuple $u \in \mathbb{Z}_m^n$, we say that the *Ducci sequence of* u is the sequence $\{D^\alpha(u)\}_{\alpha=0}^\infty$.

Looking at an example, consider $(3,1,3) \in \mathbb{Z}_4^3$ and the first few terms in its Ducci sequence:

$$(3,1,3),\ (0,0,2),\ (0,2,2),\ (2,0,2),\ (2,2,0),\ (0,2,2).$$

One can see that if you continue the Ducci sequence, it cycles through the tuples

$$(0,2,2),\ (2,0,2),\ (2,2,0).$$

We say that these three tuples are the Ducci cycle of the Ducci sequence of $(3,1,3)$. More specifically, we say that the *Ducci cycle* of a tuple u is the set

$$\left\{v \mid \exists \alpha \in \mathbb{Z}^+ \cup \{0\}, \beta \in \mathbb{Z}^+ \ni v = D^{\alpha+\beta}(u) = D^{\alpha}(u)\right\},$$

a term [2, 7, 14] also uses. We define $\mathrm{Len}(u)$ to be the smallest α that can be found to satisfy the equation

$$v = D^{\alpha+\beta}(u) = D^{\alpha}(u)$$

from our definition for some $\beta \in \mathbb{Z}^+, v \in \mathbb{Z}_m^n$. We adopt the notations $\mathrm{Len}(u)$ and $\mathrm{Per}(u)$ from [2, Definition 1]. The notation $\mathrm{Per}(u)$ is also referred to as the *period* in the literature (see, for example, [3, 6, 10]).

Notice that $\mathrm{Per}(u)$ is also the number of distinct tuples in the Ducci cycle of u. If a tuple $v \in \mathbb{Z}_m^n$ is in the Ducci cycle of the Ducci sequence for some tuple u, we may simply say that v is in a Ducci cycle. Since $\mathbb{Z}_m^n$ is finite, every Ducci sequence enters a cycle.

Define

$$K(\mathbb{Z}_m^n) = \left\{u \in \mathbb{Z}_m^n \mid u \text{ is in some Ducci cycle}\right\},$$

which is given in [2, Definition 4]. The following theorem about $K(\mathbb{Z}_m^n)$ is stated in [2, p.6001] but we will provide a proof of it in Section 3.

Theorem 1.1 *The set $K(\mathbb{Z}_m^n)$ is a subgroup of $\mathbb{Z}_m^n$.*

If for a tuple u there exists a tuple v such that $D(v) = u$, we say that v is a *predecessor* of u. We believe [14, p.259] is the first time this term is used, then later by [2, 13].

It is not always the case that the Ducci sequence ends in a cycle containing more than one tuple. Notice that the Ducci cycle of $(0, 0, \ldots, 0)$ consists only of itself and that satisfies $\mathrm{Per}(u) = 1$. In addition to this, let us observe that $(0, 0, \ldots, 0)$ is the only tuple that satisfies the condition $D(u) = u$, which we believe is first noted in [6, Remark 5] and then again by [2]. This means that only $(0, 0, \ldots, 0)$ and tuples whose Ducci cycle are

$$\{(0, 0, \ldots, 0)\}$$

have a period of 1. We say that a Ducci sequence *vanishes* when its cycle is $\{(0, 0, \ldots, 0)\}$, a term first used by [6, p.117] and also by [2, 13].

A key Ducci sequence is the one corresponding to

$$(0, 0, \ldots, 0, 1) \in \mathbb{Z}_m^n.$$

We call the Ducci sequence of this tuple the *basic Ducci sequence* of $\mathbb{Z}_m^n$, following its first use in [10, p.302], and also in [2, 9, 13]. Following, in particular, [2, Definition 5] and [10, 13], we denote

$$L_m(n) = \mathrm{Len}(0, 0, \ldots, 0, 1) \quad \text{and} \quad P_m(n) = \mathrm{Per}(0, 0, \ldots, 0, 1).$$

These results are significant since, by [2, Lemma 1], for every $u \in \mathbb{Z}_m^n$, we have

$$L_m(n) \geqslant \mathrm{Len}(u) \qquad \text{and} \qquad \mathrm{Per}(u) | P_m(n).$$

The notation $P_m(n)$ for the maximal period of a Ducci sequence on $\mathbb{Z}_m^n$ is also used in [3, p.858].

In this paper, we focus on the case where $m = 2^l$ and $n = 2^k$ for integers $k, l \geqslant 1$. It is first proven [20, p.103, (I)] that all Duc-

ci sequences in $\mathbb{Z}_{2^l}^{2^k}$ vanish. Moreover, [9, Theorem 2.3] also provides a proof of this. However, we would like to establish a value for $L_m(n)$ in this case. Our main goal is to prove the following result.

Theorem 1.2 *Let $n = 2^k$, $m = 2^l$ for integers $l, k \geqslant 1$. Then*

$$P_m(n) = 1 \qquad \textit{and} \qquad L_m(n) = (l+1)2^{k-1}.$$

As part of the proof in [20], it is shown that

$$D^{l*2^k}(u) = (0, 0, \ldots, 0),$$

for every tuple $u \in \mathbb{Z}_{2^l}^{2^k}$; however, neither [20] nor [9] determine a value for $L_{2^l}(2^k)$.

It is worth noting that as a result of all Ducci sequences vanishing, we gain the following result.

Corollary 1.3 *The group $K(\mathbb{Z}_{2^l}^{2^k})$ is trivial.*

The research presented in this paper was conducted while the second author was a Ph.D. student at Kent State University under the supervision of the first author and will appear as part of the second author's dissertation.

2 Background

There are many different versions of the Ducci function. The first and most common Ducci function is

$$\overline{D} : (\mathbb{Z}^+ \cup \{0\})^n \to (\mathbb{Z}^+ \cup \{0\})^n$$

being defined as

$$\overline{D}(x_1, x_2, \ldots, x_n) = (|x_1 - x_2|, |x_2 - x_3|, \ldots, |x_n - x_1|),$$

with [10, 12, 13, 14] being a few examples, or similarly defined on $\mathbb{Z}^n$ like in [2].

Other sources, such as [5, 7, 18], define it on $\mathbb{R}^n$. Note that if $u \in \mathbb{Z}^n$, then $\overline{D}(u) \in (\mathbb{Z}^+ \cup \{0\})^n$. Therefore, for simplicity, we will refer to the Ducci case on $(\mathbb{Z}^+ \cup \{0\})^n$ or $\mathbb{Z}^n$ as the Ducci case on $\mathbb{Z}^n$.

For both Ducci on $\mathbb{Z}^n$ and Ducci on $\mathbb{R}^n$, it has been proven that all Ducci sequences enter a cycle. Some examples of sources that explain why this happens on $\mathbb{Z}^n$ are [6, 10, 13, 14] and [18] proves it for $\mathbb{R}^n$ in Theorem 2. For Ducci on $\mathbb{Z}^n$, when looking at the tuples in a Ducci cycle, all of the entries belong to $\{0, c\}$, for some $c \in \mathbb{Z}^+$, which is proved in [14, Lemma 3] and then again later by [16]. Because $\overline{D}(\lambda u) = \lambda \overline{D}(u)$ when $\lambda \in \mathbb{Z}$ and $u \in \mathbb{Z}^n$, this means that for this case, one only needs to worry about when Ducci is defined on $\mathbb{Z}_2$ when examining Ducci cycles and periods, something that [2, 10, 13, 14] all talk about. For the $\mathbb{R}^n$ case, [18] proves a similar result in Theorem 1: if the Ducci sequence reaches a limit point, then all of the entries in the tuple belong to $\{0, c\}$, for some $c \in \mathbb{R}$.

It has been proven that the Ducci sequence will eventually vanish for all tuples in $\mathbb{Z}^n$ if and only if if n is a power of 2. According to [4, 7], the paper [8] is the first to provide a proof of this with other papers, like [13, 14], also citing [8] for a proof of this fact. The first paper published that talks about Ducci sequences is also [8]. Unfortunately, we are unable to find a copy of [8]; a review of the paper can be found at [17]. Many different proofs for the fact that all Ducci sequences vanish have been made since [8], with [10, 12, 15, 16] being a few. As discussed in the introduction, this conclusion can be extended to $m = 2^l$ where $l \geqslant 1$. Our ultimate goal is to establish how long we can expect it to take for a sequence to reach $(0, 0, \ldots, 0)$.

For the Ducci case on $\mathbb{Z}_2^n$, there have been a few sources that look at the maximum value of the length of a Ducci sequence, $L_2(n)$, for a variety of values for n. The first source is [10, p.303], which shows that for odd n, $L_2(n) = 1$. The next

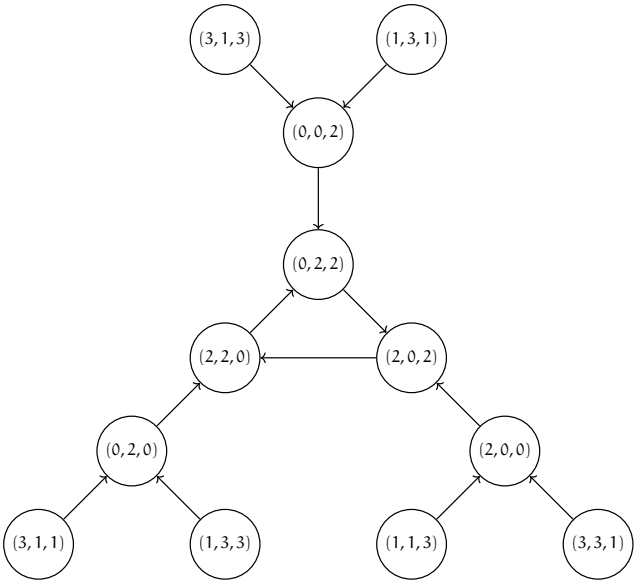


Figure 1: Transition graph for $\mathbb{Z}_4^3$

example is the specific case where

$$n = 2^{k_1} + 2^{k_2},$$

for $k_1 > k_2 \geqslant 0$, considered in [13, Theorem 6], where it is shown that $L_2(n) = 2^{k_2}$. As proved in [1, Theorem 4] the result extends to all even n, showing that if $n = 2^k n_1$ where n_1 is odd, then $L_2(n) = 2^k$. This supports the case where $l = 1$ for Theorem 1.2.

Returning to our Ducci case, [20] is the first paper to look at Ducci sequences on $\mathbb{Z}_m^n$, followed by [2, 3, 9].

We start by discussing more about our example of the Ducci cycle of $(3,1,3)$ to provide a better visualization of what Ducci sequences in $\mathbb{Z}_m^n$ look like. We can do this by creating a transition graph that maps all of the Ducci sequences of $\mathbb{Z}_4^3$ and direct our focus to the connected component containing $(3,1,3)$, which can be found in Figure 2.

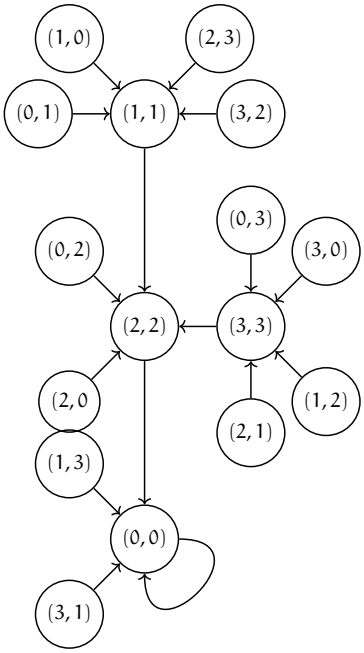


Figure 2: Transition graph for $\mathbb{Z}_4^2$

Using our earlier definitions, one can see

$$\text{Len}(3,1,3) = 2,\ \text{Len}(0,0,2) = 1, \quad \text{and} \quad \text{Len}(0,2,2) = 0.$$

Although $(1,3,1)$ is not in the Ducci sequence of $(3,1,3)$, we can see that the Ducci sequences of $(3,1,3)$ and $(1,3,1)$ have the same Ducci cycle, as well as every other tuple, in this connected component. In addition to this, all of these tuples have period 3.

Notice that $(0,0,2)$ has two predecessors, $(3,1,3)$ and $(1,3,1)$. But not all tuples have predecessors; both $(3,1,3)$ and $(1,3,1)$ are examples of this.

We also present the transition graph for $\mathbb{Z}_4^2$ to give an example where all Ducci sequences vanish in Figure 2. For this graph, all tuples in $\mathbb{Z}_4^2$ are part of the same component. Here, we can see that $L_2(4) = 3$, but not all tuples without predecessors have this length. For example, $(2,3)$ and $(1,3)$ both do not have

predecessors, but

$$\mathrm{Len}(2,3) = 3 \qquad \text{and} \qquad \mathrm{Len}(1,3) = 1.$$

Notice that all tuples in $\mathbb{Z}_4^2$ that have a predecessor have exactly four predecessors. This is not a coincidence, in fact, the following result holds.

Theorem 2.1 *Let n be even. If a tuple $u = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$ has a predecessor $(y_1, y_2, \ldots, y_n)$, then*

$$(y_1 + z, y_2 - z, \ldots, y_{n-1} + z, y_n - z)$$

is also a predecessor of u where $z \in \mathbb{Z}_m$. Moreover, if a tuple u has a predecessor, it has exactly m predecessors.

Proof — Let $x_i, y_i \in \mathbb{Z}_m$. Clearly, if $(y_1, y_2, \ldots, y_n)$ is a predecessor to $(x_1, x_2, \ldots, x_n)$, then so is $(y_1 + z, y_2 - z, \ldots, y_n - z)$ if $z \in \mathbb{Z}_m$. This gives us at least m predecessors to $(x_1, x_2, \ldots, x_n)$, each beginning with a different element in $\mathbb{Z}_m$.

We now confirm that these are all the predecessors of the tuple $(x_1, x_2, \ldots, x_n)$. If we consider two tuples that are predecessors to $(x_1, x_2, \ldots, x_n)$ that both begin with the same element, say $(y_1, y_2, \ldots, y_n)$ and $(y_1, y_2', \ldots, y_n')$, then we have the relations

$$y_1 + y_2 \equiv x_1 \mod m \qquad \text{and} \qquad y_1 + y_2' \equiv x_1 \mod m,$$

which gives us $y_2 = y_2'$. We can repeat this to see $y_i = y_i'$, for every $i, 1 \leqslant i \leqslant n$ and, as a result, $(x_1, x_2, \ldots, x_n)$ only has one unique predecessor beginning with y_1, so it has exactly m predecessors. □

Let us now draw our attention back to D specifically. Because

$$\begin{aligned} &D((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D(x_1 + x_1', x_2 + x_2', \ldots, x_n + x_n') \end{aligned}$$

$$= (x_1 + x_2 + x_1' + x_2', x_2 + x_3 + x_2' + x_3', \ldots, x_n + x_1 + x_n' + x_1')$$
$$= (x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1) + (x_1' + x_2', x_2' + x_3', \ldots, x_n' + x_1')$$
$$= D(x_1, x_2, \ldots, x_n) + D(x_1', x_2', \ldots, x_n'),$$

it is true that $D \in \mathrm{End}(\mathbb{Z}_m^n)$. Also, it remains true that

$$D(\lambda u) = \lambda D(u)$$

when $\lambda \in \mathbb{Z}_m$ and $u \in \mathbb{Z}_m^n$. Since this means $D^\alpha(\lambda u) = \lambda D^\alpha(u)$ for $\alpha \in \mathbb{Z}^+$, the Ducci sequence for λu is $\left\{\lambda D^\alpha(u)\right\}_{\alpha=0}^{\infty}$ and if $u \in K(\mathbb{Z}_m^n)$, then so is λu.

Define $H : \mathbb{Z}_m^n \to \mathbb{Z}_m^n$ as

$$H(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1).$$

We also have that $H \in \mathrm{End}(\mathbb{Z}_m^n)$ and $D = I + H$ where I is the identity endomorphism. This function was first introduced in [10, p.302] and is also used by [2, 13]. Note that

$$H(D(x_1, x_2, .., x_n)) = H(x_1 + x_2, x_2 + x_3, \ldots, x_n + x_1)$$
$$= (x_2 + x_3, x_3 + x_4, \ldots, x_n + x_1, x_2 + x_1)$$
$$= D(x_2, x_3, .., x_n, x_1) = D(H(x_1, x_2, \ldots, x_n)),$$

and therefore H, D commute. This means that if $\{D^\alpha(u)\}_{\alpha=0}^{\infty}$ is the Ducci sequence for $u \in \mathbb{Z}_m^n$, then $\{H^\beta(D^\alpha(u))\}_{\alpha=0}^{\infty}$ is the Ducci sequence for $H^\beta(u)$ when $0 \leqslant \beta \leqslant n-1$. Consequently, if $u \in K(\mathbb{Z}_m^n)$, then so is $H^\beta(u)$.

3 Findings on Ducci for n, m arbitrary

We can now prove Theorem 1.1 from Section 1. Note that this theorem is stated as a fact in [2], but a proof is provided here for completeness.

Proof of Theorem 1.1 — We start by showing that

$$\begin{aligned} &D^{\alpha}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D^{\alpha}(x_1, x_2, \ldots, x_n) + D^{\alpha}(x_1', x_2', \ldots, x_n') \end{aligned}$$

by induction for $\alpha \in \mathbb{Z}^+$. This is true for $\alpha = 1$ because D is an endomorphism.

Assume that it is true for $\alpha - 1$, then

$$\begin{aligned} &D^{\alpha}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D(D^{\alpha-1}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')). \end{aligned}$$

By induction, we have

$$D(D^{\alpha-1}(x_1, x_2, \ldots, x_n) + D^{\alpha-1}(x_1', x_2', \ldots, x_n'))$$

and

$$D(D^{\alpha-1}(x_1, x_2, \ldots, x_n)) + D(D^{\alpha-1}(x_1', x_2', \ldots, x_n')),$$

which is equal to

$$D^{\alpha}(x_1, x_2, \ldots, x_n) + D^{\alpha}(x_1', x_2', \ldots, x_n').$$

Now suppose $(x_1, x_2, \ldots, x_n), (x_1', x_2', \ldots, x_n') \in K(\mathbb{Z}_m^n)$. Consequently, if $d = P_m(n)$, then $D^d(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n)$ and $D^d(x_1', x_2', \ldots, x_n') = (x_1', x_2', \ldots, x_n')$. Therefore,

$$\begin{aligned} &D^{d}((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \\ &= D^{d}(x_1, x_2, \ldots, x_n) + D^{d}(x_1', x_2', \ldots, x_n'), \end{aligned}$$

which equals $(x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')$ and thus

$$((x_1, x_2, \ldots, x_n) + (x_1', x_2', \ldots, x_n')) \in K(\mathbb{Z}_m^n).$$

It follows then that $K(\mathbb{Z}_m^n) \leqslant \mathbb{Z}_m^n$. □

When examining a Ducci sequence, it is useful to determine the value of $D^r(u)$ for a given $u \in \mathbb{Z}_m^n$. To this end, define $a_{r,s}$, with $r, s \in \mathbb{Z}$, $r \geqslant 0$, and $1 \leqslant s \leqslant n$, so that

$$D^r(0,0,\ldots,0,1) = (a_{r,n}, a_{r,n-1}, \ldots, a_{r,1}).$$

Now, any tuple $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_m^n$ can be written as

$$(x_1, x_2, \ldots, x_n) = \sum_{s=1}^{n} x_s H^{-s}(0,0,..,0,1),$$

which gives

$$D^r(x_1, x_2, \ldots, x_n) = \sum_{s=1}^{n} x_s H^{-s}(a_{r,n}, a_{r,n-1}, \ldots, a_{r,1})$$

or

$$\sum_{s=1}^{n} x_s (a_{r,s}, a_{r,s-1}, \ldots, a_{r,s+1}).$$

Using this, we can now define $a_{r,s}$ as the coefficient on x_{s-i+1} in the ith coordinate of $D^r(x_1, x_2, \ldots, x_n)$, with

$$a_{0,s} = \begin{cases} 0 & \text{if } s \neq 1 \\ 1 & \text{if } s = 1 \end{cases}.$$

We now aim to prove a few more observations about $a_{r,s}$.

Theorem 3.1 *Let $r \geqslant 1$, $1 \leqslant s \leqslant n$. The the following are satisfied*:

(1) $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$.

(2) *For $r < n$,* $a_{r,s} = \binom{r}{s-1}$.

(3) $a_{r+t,s} = \sum_{i=1}^{n} a_{t,i} a_{r,s-i+1}$, *where $t \geqslant 1$.*

PROOF — (1) We first note that

$$D^{r-1}(0,0,\ldots,0,1) = (a_{r-1,n}, a_{r-1,n-1}, \ldots, a_{r-1,1}).$$

Hence, by the definition of D, the s-th entry of $D^r(0,0,\ldots,0,1)$ will be

$$a_{r-1,s} + a_{r-1,s-1}.$$

This, by definition, is also $a_{r,s}$ and (1) follows.

We proceed to prove statement (2) by induction on r, and statement (3) by induction on t.

(2) *Basis Step*: $r = 1$. This follows from (1) and

$$a_{0,s} = \begin{cases} 0 & \text{if } s \neq 1 \\ 1 & \text{if } s = 1 \end{cases}.$$

Inductive Step: Note that if $s - 1 > r$, we use the convention that

$$a_{r,s} = \binom{r}{s-1} = 0.$$

Assume $a_{r-1,s} = \binom{r-1}{s-1}$ when $r < n$. By (1), we have that for $1 < s \leqslant n$, $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$, which by induction is

$$\binom{r-1}{s-1} + \binom{r-1}{s-2} \qquad \text{or} \qquad \binom{r}{s-1}.$$

For $s = 1$, we have $a_{r,1} = a_{r-1,1} + a_{r-1,n}$. By induction, this is

$$\binom{r-1}{0} + \binom{r-1}{n-1}$$

which is 1 or $\binom{r}{0}$ as long as $r < n$.

(3) We prove this via induction on t.

Basis Steps: $t = 1, 2$. Calculating $a_{r,s}$ in terms of $a_{r-1,i}$ we obtain that $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$, which can be further expanded in terms of $a_{r-2,i}$ as $a_{r,s} = a_{r-2,s} + 2a_{r-2,s-1} + a_{r-2,s-2}$. This is

$$a_{2,1}a_{r-2,s} + a_{2,2}a_{r-2,s-1} + a_{2,3}a_{r-2,s-2}$$

and the basis case follows.

Inductive Step: Assume that for $t' < t$, $a_{r+t',s} = \sum_{i=1}^{n} a_{t',i}a_{r,s-i+1}$. Then calculating $a_{r+t,s}$, we have

$$a_{r+t,s} = \sum_{i=1}^{n} a_{t-1,i}a_{r+1,s-i+1}\,.$$

Breaking down $a_{r,s-i+1}$, this is

$$\sum_{i=1}^{n} a_{t-1,i}(a_{r,s-i+1} + a_{r,s-i})\,.$$

Distributing $a_{t-1,i}$ and breaking the sum up, this is

$$\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i+1} + \sum_{i=1}^{n} a_{t-1,i}a_{r,s-i}\,. \tag{3.1}$$

Note that, for the sum $\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i}$, from equation (3.1), we have

$$\sum_{i=1}^{n} a_{t-1,i}a_{r,s-i} = \sum_{i=2}^{n+1} a_{t-1,i-1}a_{r,s-i+1}\,.$$

As the s-coordinate of $a_{r,s}$ is reduced modulo n, it follows that

$$\sum_{i=1}^{n} a_{t-1,i-1}a_{r,s-i+1}\,.$$

Therefore, equation (3.1) is equal to

$$\sum_{i=1}^{n}(a_{t-1,i} + a_{t-1,i-1})a_{r,s-i+1} \qquad \text{or} \qquad \sum_{i=1}^{n} a_{t,i}a_{r,s-i+1}\,.$$

Therefore, equation (3) holds. □

We now prove some other useful facts about the $a_{r,s}$ coefficients that we will need later.

Corollary 3.2 *For all integers n and s with $1 \leqslant s \leqslant n$, the terms $a_{n,s}$ are given by*

$$a_{n,s} = \begin{cases} \binom{n}{s-1} & s \neq 1 \\ 2 & s = 1 \end{cases}$$

Proof — Let $s > 1$. Then $a_{n,s} = a_{n-1,s} + a_{n-1,s-1}$ gives us

$$a_{n,s} = \binom{n-1}{s-1} + \binom{n-1}{s-2} \qquad \text{or} \qquad \binom{n}{s-1},$$

by Theorem 3.1.

For $s = 1$, $a_{n,1} = a_{n-1,1} + a_{n-1,n}$ gives us

$$a_{n,1} = \binom{n-1}{0} + \binom{n-1}{n-1} \qquad \text{or} \qquad 2\,,$$

by Theorem 3.1. □

We have one last lemma about the $a_{r,s}$ that is true for all n, m.

Lemma 3.3 *For $r \geqslant 0$, $a_{r,s} = a_{r,r-s+2}$.*

Proof — We work by induction on r.

Basis Step: We take advantage of Theorem 3.1 to see that when $r < n$,

$$a_{r,s} = \binom{r}{s-1} = \binom{r}{r-s+1} = a_{r,r-s+2}.$$

Inductive Step: Suppose that the theorem is true for $r-1$. Then we have

$$a_{r-1,s} = a_{r-1,r-s+1} \qquad \text{and} \qquad a_{r-1,s-1} = a_{r-1,r-s+2}.$$

Since $a_{r,s} = a_{r-1,s} + a_{r-1,s-1}$,

$$a_{r,s} = a_{r-1,r-s+1} + a_{r-1,r-s+2},$$

which is equal to $a_{r,r-s+2}$. Therefore, the claim follows. □

4 All tuples vanish in $\mathbb{Z}_{2^l}^{2^k}$

Recall that it is our main goal to prove that for $m = 2^l, n = 2^k$, then $L_m(n) = (l+1)2^{k-1}$. In order to do this, we first aim to prove a number of lemmas, starting with a few lemmas that explore the value of certain binomial coefficients. We believe that Lemmas 4.1–4.3, and 4.5 are known but we are including the following proofs for the sake of completeness. Throughout these proofs, we rely on the well known fact that $\binom{2^j}{t}$ is even when $t \neq 0, 2^j$, a proof of which can be found in [11, Theorem 3].

Lemma 4.1 *For any integer* $j \geqslant 2$*, we have*

$$\binom{2^j}{2^{j-1}} \equiv 2 \mod 4.$$

Proof — By the Chu–Vandermonde identity (see [19]), we obtain

$$\binom{2^j}{2^{j-1}} = \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}^2 = \binom{2^{j-1}}{0}^2 + \binom{2^{j-1}}{2^{j-1}}^2 + \sum_{i=1}^{2^{j-1}-1} \binom{2^{j-1}}{i}^2,$$

which is congruent to 2 mod 4. □

For the other binomial coefficients $\binom{2^j}{t}$, we have the following result.

Lemma 4.2 *When* $t \neq 0, 2^{j-1}, 2^j$ *and* $j \geqslant 2$*, then*

$$\binom{2^j}{t} \equiv 0 \textit{ mod } 4.$$

Proof — First to address the cases when $t \in \{0, 2^{j-1}, 2^j\}$, we know

$$\binom{2^j}{0} = \binom{2^j}{2^j} = 1 \qquad \text{and} \qquad \binom{2^j}{2^{j-1}} \equiv 2 \mod 4.$$

We prove the rest of the lemma by induction on j.

Basis Step: $j = 2$.

$$\binom{4}{1} = \binom{4}{3} = 4.$$

Inductive Step: Assume that

$$\binom{2^{j-1}}{t} \equiv 0 \mod 4$$

when $t \neq 0, 2^{j-2}, 2^{j-1}$. We start with when $0 < t < 2^{j-2}$ and use

the Chu–Vandermonde Identity to see that

$$\begin{aligned}\binom{2^j}{t} &= \sum_{i=0}^{t} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i} \\ &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{t} + \binom{2^{j-1}}{t}\binom{2^{j-1}}{0} + \sum_{i=1}^{t-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which is congruent to 0 mod 4 by induction. Next, we consider $2^{j-2} < t < 2^{j-1}$. Then

$$\begin{aligned}\binom{2^j}{t} &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{t} + \binom{2^{j-1}}{t}\binom{2^{j-1}}{0} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}}{t-2^{j-2}} \\ &+ \binom{2^{j-1}}{t-2^{j-2}}\binom{2^{j-1}}{2^{j-2}} + \sum_{\substack{i=1 \\ i\neq 2^{j-2}, t-2^{j-2}}}^{t-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which by induction is congruent to 0 mod 4. Now if we consider $t = 2^{j-2}$, then

$$\begin{aligned}\binom{2^j}{2^{j-2}} &= \binom{2^{j-1}}{0}\binom{2^{j-1}}{2^{j-2}} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}}{0} \\ &+ \sum_{i=1}^{2^{j-2}-1} \binom{2^{j-1}}{i}\binom{2^{j-1}}{t-i},\end{aligned}$$

which is equivalent to 0 mod 4 by Lemma 4.1 and induction.

Now suppose that $2^{j-1} < t < 2^j$. Then $0 < 2^j - t < 2^{j-1}$, so

$$\binom{2^j}{t} = \binom{2^j}{2^j - t} \equiv 0 \bmod 4$$

and the lemma follows. □

We still need to know more about the value of $\binom{2^j}{2^{j-1}}$ so we prove the following result.

Lemma 4.3 *For* $j \geqslant 2$,

$$\binom{2^j}{2^{j-1}} \equiv 6 \text{ mod } 8.$$

Proof — *Basis Step*: $j = 2$. The claim holds for the base case, since

$$\binom{4}{2} = 6.$$

Inductive Step: Assume $\binom{2^{j-1}}{2^{j-2}} \equiv 6 \mod 8$. Therefore, by the Chu–Vandermonde Identity,

$$\begin{aligned}\binom{2^j}{2^{j-1}} &= \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}^2 \\ &= \binom{2^{j-1}}{0}^2 + \binom{2^{j-1}}{2^{j-1}}^2 + \binom{2^{j-1}}{2^{j-2}}^2 + \sum_{\substack{i=1 \\ i \neq 2^{j-2}}}^{2^{j-1}-1} \binom{2^{j-1}}{i}^2.\end{aligned}$$

Hence, by induction and Lemma 4.2, we obtain that

$$\binom{2^j}{2^{j-1}} \equiv 6 \mod 8.$$

Therefore, the claim follows. □

The next result is a consequence of Lucas's Theorem, which can be found, for example, in [11, Theorem 1].

Lemma 4.4 *For every integer* t *with* $0 \leqslant t \leqslant 2^j - 1$, *we have*

$$\binom{2^j - 1}{t}$$

is odd.

To be more specific about $\binom{2^j - 1}{2^{j-1}}$, we state the result below.

Lemma 4.5 *For $j \geqslant 2$, we have*

$$\binom{2^j - 1}{2^{j-1}} \equiv 3 \bmod 4.$$

Proof — We prove this via induction.

Basis Step: $j = 2$. The claim holds for the base case, since

$$\binom{3}{2} = 3.$$

Inductive Step: Assume that $\binom{2^{j-1}-1}{2^{j-2}} \equiv 3 \bmod 4$. Hence, by the Chu–Vandermonde Identity,

$$\binom{2^j - 1}{2^{j-1}} = \sum_{i=0}^{2^{j-1}} \binom{2^{j-1}}{i}\binom{2^{j-1}-1}{2^{j-1}-i}$$

or

$$\binom{2^{j-1}}{0}\binom{2^{j-1}-1}{2^{j-1}} + \binom{2^{j-1}}{2^{j-1}}\binom{2^{j-1}-1}{0} + \binom{2^{j-1}}{2^{j-2}}\binom{2^{j-1}-1}{2^{j-2}} + \sum_{\substack{i=1 \\ i \neq 2^{j-2}}}^{2^{j-1}-1} \binom{2^{j-1}}{i}\binom{2^{j-1}-1}{2^{j-1}-i}.$$

This is equivalent to $1 + (2 * 3) \bmod 4 \equiv 3 \bmod 4$. Therefore, the claim follows. □

We now direct our attention back to the $a_{r,s}$ coefficients and examine what happens at certain values of r. We first note that for $n = 2^k$, $a_{r,s+2^{k-1}} = a_{r,s-2^{k-1}}$.

Lemma 4.6 *Let $l \geqslant 1$ and $n = 2^k$. Then, for every $1 \leqslant s \leqslant 2^k$,*

$$a_{l2^{k-1},s} + a_{l2^{k-1},s-2^{k-1}} \equiv 0 \bmod 2^l.$$

Proof — We prove this by induction on l. To simplify the nota-

tion in the following proofs, we introduce functions to represent certain coefficients $a_{r,s}$. To this end, we define

$$f(\gamma, \delta) = a_{\gamma 2^{k-1}, \delta}.$$

It is worth noting that, by Lemma 3.3,

$$f(\gamma, \delta) = f(\gamma, \gamma * 2^{k-1} - \delta + 2).$$

Additionally, when $n = 2^k$, we have

$$f(\gamma, \delta + 2^{k-1}) = f(\gamma, \delta - 2^{k-1}).$$

In terms of f, we want to show

$$f(l, s) + f(l, s - 2^{k-1}) \equiv 0 \mod 2^l.$$

Basis Step: $l = 1$. It suffices to show

$$f(1, s) + f(1, s - 2^{k-1}) \equiv 0 \mod 2.$$

Then, for $s \neq 1, 2^{k-1} + 1$,

$$f(1, s) + f(1, s - 2^{k-1}) = \binom{2^{k-1}}{s-1} + \binom{2^{k-1}}{s - 2^{k-1} - 1} \equiv 0 \mod 2$$

since both of these binomial coefficients are even by Lemma 4.2. For $s = 1, 2^{k-1} + 1$,

$$f(1, 1) + f(1, 1 + 2^{k-1}) = \binom{2^{k-1}}{0} + \binom{2^{k-1}}{2^{k-1}} = 2$$

and the basis case follows.

Inductive Step: Assume

$$f(l - 1, s) + f(l - 1, s - 2^{k-1}) \equiv 0 \mod 2^{l-1}.$$

Then

$$
\begin{aligned}
&f(l,s)+f(l,s-2^{k-1})\\
&=\sum_{i=1}^{2^k}[f(l-1,i)f(1,s-i+1)+f(l-1,i)f(1,s-2^{k-1}-i+1)]
\end{aligned}
$$

by part (3) of Theorem 3.1. We now break this up into the following two sums:

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(l-1,i)f(1,s-i+1)+f(l-1,i)f(1,s-2^{k-1}-i+1)]\\
&+\sum_{i=2^{k-1}+1}^{2^k}[f(l-1,i)f(1,s-i+1)\\
&+f(l-1,i)f(1,s-2^{k-1}-i+1)].
\end{aligned}
$$

Changing the indices of the second sum to match the first, this is

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(l-1,i)f(1,s-i+1)\\
&+f(l-1,i)f(1,s-2^{k-1}-i+1)]\\
&\quad+\sum_{i=1}^{2^{k-1}}[f(l-1,i-2^{k-1})f(1,s-i+2^{k-1}+1)\\
&\quad+f(l-1,i-2^{k-1})f(1,s-i+1)],
\end{aligned}
$$

which can be factored into

$$
\begin{aligned}
&\sum_{i=1}^{2^{k-1}}[f(1,s-i+1)\\
&+f(1,s-i+2^{k-1}+1)][f(l-1,i)+f(l-1,i-2^{k-1})].
\end{aligned}
\tag{4.1}
$$

By induction, since

$$f(l-1,i)+f(l-1,i-2^{k-1}) \equiv 0 \mod 2^{l-1},$$

the addend in the sum from (4.1) is congruent to $0 \mod 2^l$ if both $f(1,s-i+1)$ and $f(1,s-i+2^{k-1}+1)$ are even. The only times this does not happen is when $i=s$ and $i=s+2^{k-1}$. In both cases, the addend in the sum of (4.1) is

$$[f(1,1)+f(1,2^{k-1}+1)][f(l-1,s)+f(l-1,s-2^{k-1})].$$

This is $2[f(l-1,s)+f(l-1,s-2^{k-1})]$, and, by induction, we obtain that $2[f(l-1,s)+f(l-1,s-2^{k-1})] \equiv 0 \mod 2^l$. Therefore, equation (4.1) is congruent to $0 \mod 2^l$ and the lemma follows. □

We have one last lemma to prove before Theorem 1.2. We are once more interested in a sum of two specific $a_{r,s}$ coefficients.

Lemma 4.7 *Let* $n=2^k$. *For* $l \geqslant 3$,

$$a_{(l-1)2^{k-1},l2^{k-2}+1}+a_{(l-1)2^{k-1},l2^{k-2}-2^{k-1}+1} \equiv 0 \mod 2^l.$$

Proof — Let us define

$$g(\gamma,\epsilon,\delta)=a_{\gamma 2^{k-1},\epsilon 2^{k-2}+\delta}.$$

In terms of g, we aim to show that

$$g(l-1,l,1)+g(l-1,l,2^{k-1}+1) \equiv 0 \mod 2^l.$$

Using Theorem 3.1, we obtain that

$$\begin{aligned} &g(l-1,l,1)+g(l-1,l,2^{k-1}+1)\\ &=\sum_{i=1}^{2^k}[f(1,i)g(l-2,l,2-i)+f(1,i)g(l-2,l,2^{k-1}+2-i)]. \end{aligned}$$

As in the proof of Lemma 4.6, we decompose the sum and adjust the indices to obtain

$$\sum_{i=1}^{2^{k-1}} [f(1,i)g(l-2,l,2-i) + f(1,i)g(l-2,l,2^{k-1}+2-i)]$$
$$+ \sum_{i=1}^{2^{k-1}} [f(1,i-2^{k-1})g(l-2,l,2^{k-1}+2-i)$$
$$+ f(1,i-2^{k-1})g(l-2,l,2-i)].$$

Factoring yields

$$\sum_{i=1}^{2^{k-1}} [f(1,i) + f(1,i-2^{k-1})][g(l-2,l,2-i) + g(l-2,l,2^{k-1}+2-i)]. \tag{4.2}$$

Note that by Lemma 4.6,

$$g(l-2,l,2-i) + g(l-2,l,2^{k-1}+2-i) \equiv 0 \mod 2^{l-2}.$$

Consequently, if $f(1,i) + f(1,i-2^{k-1}) \equiv 0 \mod 4$, then each term in the sum in (4.2) is congruent to $0 \mod 2^l$.

Observe that if

$$i \neq 1, 2^{k-2}+1, 2^{k-1}+1, 2^{k-1}+2^{k-2}+1,$$

then both $f(1,i)$ and $f(1,i-2^{k-1})$ are equivalent to $0 \mod 4$ by Lemma 4.2. Thus, reducing modulo 2^l, expression (4.2) becomes

$$\begin{aligned}
&[f(1,1) + f(1,2^{k-1}+1)][g(l-2,l,1) \\
&+ g(l-2,l,2^{k-1}+1)] \\
&+ [f(1,2^{k-1}+1) + f(1,1)][g(l-2,l,2^{k-1}+1) \\
&+ g(l-2,l,1)] + [g(1,1,1) \\
&+ g(1,1,2^{k-1}+1)][g(l-2,l-1,1)
\end{aligned} \tag{4.3}$$

$$+ g(l-2, l-1, 2^{k-1}+1)] + [g(1,1,2^{k-1}+1)$$
$$+ g(1,1,1)][g(l-2, l-1, 2^{k-1}+1) + g(l-2, l-1, 1)].$$

Notice that

$$f(1,1) + f(1, 2^{k-1}+1) = \binom{2^{k-1}}{0} + \binom{2^{k-1}}{2^{k-1}}$$

and

$$g(1,1,1) + g(1,1,2^{k-1}+1 = \binom{2^{k-1}}{2^{k-2}} + \binom{2^{k-1}}{2^{k-1}+2^{k-2}}.$$

Moreover, by Lemma 4.6,

$$g(l-2, l, 1) + g(l-2, l, 2^{k-1}+1) \equiv 0 \mod 2^{l-1}$$

and

$$g(l-2, l-1, 1) + g(l-2, l-1, 2^{k-1}+1) \equiv 0 \mod 2^{l-1}.$$

It follows that expression (4.3) is congruent to $0 \pmod{2^l}$, thereby completing the proof of the lemma. □

We are now equipped with all the tools required to prove the main theorem.

Proof of Theorem 1.2 — We note once again that, according to [20, (I), p.103] and [9, Theorem 2.3]), all tuples vanish in $\mathbb{Z}_{2^l}^{2^k}$, for all $l, k \in \mathbb{Z}^+$. We also provide a proof of this result. Indeed, to show that

$$L_{2^l}(2^k) = (l+1)2^{k-1},$$

we are going to prove that

$$D^{(l+1)2^{k-1}}(0,0,\ldots,0,1) = (0,0,\ldots,0),$$

which in turn implies that $P_{2^l}(2^k) = 1$ and that all tuples in $\mathbb{Z}_{2^l}^{2^k}$ vanish.

We prove this result by induction on l, with two base cases.

However, since several results used in the proof require the assumption $k \geqslant 2$, we first treat the case $k = 1$. That is, we show that $L_{2^l}(2) = l + 1$ and that $P_{2^l}(2) = 1$, for every $l > 0$.

Basis Step: $k = 1$. Notice that $D^{\alpha}(0,1) = (2^{\alpha-1}, 2^{\alpha-1})$. It follows that $D^{l+1}(0,1) = (0,0)$ and hence $P_{2^l}(2) = 1$. Moreover, since

$$D^{l}(0,1) = (2^{l-1}, 2^{l-1}) \not\equiv (0,0) \pmod{2^l},$$

we conclude that $L_{2^l}(2) = l + 1$.

For the rest of the proof, we assume $n = 2^k$, $k \geqslant 1$.

Basis Step: $l = 1$. We first prove $f(2,s) \equiv 0 \mod 2$, for all $1 \leqslant s \leqslant n$. Recall that $f(2,1) = 2$ and, for $1 < s \leqslant 2^k$,

$$f(2,s) = \binom{2^k}{s-1} \equiv 0 \mod 2$$

which gives us $P_2(2^k) = 1$. Note also that, for $r < 2^k$,

$$a_{r,1} = 1 \not\equiv 0 \mod 2.$$

Therefore, this is the first time we have that $a_{r,s} \equiv 0 \mod 2$, for all s, so $L_2(2^k) = 2^k$.

Basis Step: $l = 2$. It suffices to show that $L_4(2^k) = 3 * 2^{k-1}$ and $P_4(2^k) = 1$. We begin by showing that $f(3,s) \equiv 0 \mod 4$, for every s. We first observe that, by Theorem 3.1, we have

$$f(3,s) = \sum_{i=1}^{2^k} f(1,i) f(2, s-i+1).$$

We then separate the terms where $i = 1, 2^{k-1}+1$ to produce

$$\begin{aligned} &f(1,2^{k-1}+1) f(2, s-2^{k-1}) + f(1,1) f(2,s) \\ &+ \sum_{\substack{i=2 \\ i \neq 2^{k-1}+1}}^{2^k} f(1,i) f(2, s-i+1). \end{aligned} \tag{4.4}$$

We do this because $f(1,i) \equiv 0 \mod 2$ for $i \neq 1, 2^{k-1}+1$ and

$$f(2, s-i+1) \equiv 0 \mod 2$$

as shown in our first basis case. Hence, expression (4.4) is equivalent to

$$f(2, s-2^{k-1}) + f(2,s) \pmod 4, \tag{4.5}$$

which, by Lemma 4.6, is congruent to $0 \pmod 4$. Therefore we have that $P_4(2^k) = 1$ and $L_4(2^k) \leqslant 3 * 2^{k-1}$. We now need to show that there exists s such that $a_{3*2^{k-1}-1,s} \not\equiv 0 \mod 4$. To this end, define

$$h(\gamma, \delta) = a_{\gamma 2^{k-1}-1,\delta}.$$

Calculating $h(3,s)$ for general s using Theorem 3.1, we obtain

$$h(3,s) = \sum_{i=1}^{2^k} f(1,i)h(2, s-i+1).$$

We now separate the terms where i is $1, 2^{k-2}+1$ or $2^{k-1}+1$, which gives

$$\begin{aligned} &f(1,1)h(2,s) + f(1,2^{k-1}+1)h(2,s-2^{k-1}) \\ &+ g(1,1,1)h(2,s-2^{k-2}) + \sum_{i\in J} f(1,i)h(2,s-i+1) \end{aligned} \tag{4.6}$$

where

$$J = \left\{2 \leqslant i \leqslant 2^k \mid i \neq 2^{k-1}, 2^{k-2}+1\right\}.$$

We do this so the sum over J is congruent to $0 \mod 4$ by Lemma 4.2. If we also consider $s = 1$, then expression (4.6) is congruent to

$$\begin{aligned} &f(1,1)h(2,1) + f(1,2^{k-1}+1)h(2,2^{k-1}+1) \\ &+ g(1,1,1)h(2,2^k - 2^{k-2}+1) \mod 4, \end{aligned}$$

which is equivalent to $1 + h(2, 2^{k-1} + 1) + 2 \mod 4$ because

$$g(1, 1, 1) \equiv 2 \mod 4$$

and $h(2, 2^k - 2^{k-2} + 1)$ is odd. From Lemma 4.5, this is congruent to $2 \mod 4$ and $h(3, 1) \not\equiv 0 \mod 4$, so $L_4(2^k) = 3 * 2^{k-1}$.

Inductive Step: Assume that

$$L_{2^{l-1}}(2^k) = l2^{k-1} \qquad \text{and} \qquad P_{2^{l-1}}(2^k) = 1.$$

This implies that $f(l, s) \equiv 0 \mod 2^{l-1}$, for every s. Calculating $f(l + 1, s)$ with Theorem 3.1, we have

$$f(l + 1, s) = \sum_{i=1}^{2^k} f(l, i) f(1, s - i + 1).$$

If we separate out the terms where $s - i + 1 = 1, 2^{k-1} + 1$, this becomes

$$\begin{aligned} &f(l, s) f(1, 1) + f(l, s - 2^{k-1}) f(1, 2^{k-1} + 1) \\ &+ \sum_{i \in J} f(l, i) f(1, s - i + 1) \end{aligned} \tag{4.7}$$

where

$$J = \left\{ 1 \leqslant i \leqslant 2^k \mid i \neq s, s - 2^{k-1} \right\}.$$

We do this so the sum over J is equivalent to $0 \mod 2^l$ by induction and because $f(1, s - i + 1)$ is even over J. Therefore, expression (4.7) is equivalent to

$$f(l, s) + f(l, s - 2^{k-1}) \mod 2^l,$$

which, by Lemma 4.6, is congruent to $0 \mod 2^l$. This gives us that

$$P_m(n) = 1 \qquad \text{and} \qquad L_m(n) \leqslant (l + 1) 2^{k-1}.$$

It remains to show that $L_m(n) > (l + 1) 2^{k-1} - 1$, which will

then establish the remainder of the theorem. Observe that, since $P_m(n) = 1$, it suffices to show the existence of s such that

$$h(l+1, s) \not\equiv 0 \mod 2^l.$$

We begin by decomposing $h(l+1, s)$ as follows:

$$h(l+1, s) = \sum_{i=1}^{2^k} f(l, i) h(1, s-i+1). \tag{4.8}$$

Since $a_{r,s} = a_{r,r-s+2}$, by Lemma 3.3, most $a_{r,s}$ coefficients have another coefficient that it is equal to. The case where this does not happen is when $s \equiv r - s + 2 \mod 2^k$. In our case, $h(l, i)$ is not equal to any other coefficient when

$$i = l2^{k-1} - i + 2 \qquad \text{and} \qquad i = l2^{k-1} - i + 2^k + 2.$$

Solving for i, this is when

$$i = l2^{k-2} + 1 \qquad \text{and} \qquad i = l2^{k-2} + 2^{k-1} + 1.$$

We separate these out from our sum so, using equation (4.8), we can view $h(l+1, s)$ as

$$\begin{aligned} &g(l, l, 1) h(1, s - l2^{k-2}) + g(l, l, 2^{k-1} + 1) h(1, s - l2^{k-2} - 2^{k-1}) \\ &+ \sum_{i \in M} [f(l, i) h(1, s - i + 1) + g(l, 2l, 2 - i) h(1, s - l2^{k-1} + i - 1) \end{aligned}$$

where M is defined to preserve equality. We now consider the case $s = l2^{k-2} + 1$, so $h(l+1, l2^{k-2} + 1)$ is

$$\begin{aligned} &g(l, l, 1) h(1, 1) + g(l, l, 2^{k-1} + 1) h(1, 2^{k-1} + 1) \\ &+ \sum_{i \in M} [f(l, i) h(1, l2^{k-2} + 2 - i) \\ &+ g(l, l, 2 - i) h(1, l2^{k-2} - l2^{k-1} + i)]. \end{aligned} \tag{4.9}$$

Examining each term of (4.9), we note that

$$g(l, l, 2^{k-1} + 1)\, h(1, 2^{k-1} + 1) = 0,$$

since $h(1, 2^{k-1} + 1) = 0$. For the sum in (4.9), this becomes

$$\sum_{i \in M} f(l, i)\left[h(1, l2^{k-2} + 2 - i) + h(1, l2^{k-2} - l2^{k-1} + i)\right],$$

because $f(l, i) = g(l, l, 2 - i)$. Since $h(1, s)$ is odd, for all s, by Lemma 4.4, we obtain that

$$h(1, l2^{k-2} - i + 2) + h(1, l2^{k-2} - l2^{k-1} + i)$$

is even. We know $f(l, i) \equiv 0 \mod 2^{l-1}$, therefore the whole sum is congruent to $0 \mod 2^l$. Hence, reducing expression (4.9) modulo 2^l, we conclude that

$$g(l + 1, l, 1) \equiv g(l, l, 1) \mod 2^l.$$

Thus, if we can show that $g(l, l, 1) \not\equiv 0 \mod 2^l$, then the statement will follow. Since we already know that

$$g(l, l, 1) \equiv 0 \mod 2^{l-1},$$

we are left to prove the following claim:

$$g(l, l, 1) \equiv 2^{l-1} \mod 2^l,$$

for $l \geqslant 2$. Let us prove this claim by induction on l.

Basis Step: $l = 2$. By Lemma 4.1, we have

$$g(2, 2, 1) \equiv 2 \mod 4,$$

hence the basis case follows.

Inductive Step: Assume that $g(l - 1, l - 1, 1) \equiv 2^{l-2} \mod 2^{l-1}$, then

$$g(l,l,1) = \sum_{i=1}^{2^k} f(l-1,i)g(1,l,2-i).$$

Let

$$J^* = \left\{1 \leqslant i \leqslant 2^k \mid i \neq (l-1)2^{k-2}+1, l2^{k-2}+1, l2^{k-2}-2^{k-1}+1\right\}$$

and separate all terms not in J^* to see this is

$$\begin{aligned} &g(l-1,l-1,1)g(1,1,1) + g(l-1,l,1)f(1,1) \\ &+ g(l-1,l,2^{k-1}+1)g(1,2,1) \\ &+ \sum_{i\in J^*} f(l-1,i)g(1,l,2-i) \end{aligned} \tag{4.10}$$

Once more, we separate this sum over J^* because it is congruent to $0 \mod 2^l$ because

$$f(l-1,i) \equiv 0 \mod 2^{l-2} \quad \text{and} \quad g(1,l,2-i) \equiv 0 \mod 4,$$

by Lemma 4.2. Looking at the remaining pieces from expression (4.10),

$$g(l-1,l-1,1)g(1,1,1) \equiv 2^{l-1} \mod 2^l$$

by induction and Lemma 4.1. Next, we have

$$\begin{aligned} &g(l-1,l,1)f(1,1) + g(l-1,l,2^{k-1}+1)g(1,2,1) \\ &= g(l-1,l,1) + g(l-1,l,2^{k-1}+1) \end{aligned}$$

which, by Lemma 4.7, is congruent to $0 \mod 2^l$. Thus, the claim follows.

Hence, $g(l+1,l,1) \equiv 2^{l-1} \mod 2^l$ and $L_m(n) > (l+1)2^{k-1}-1$. Therefore,

$$L_m(n) = (l+1)2^{k-1},$$

which concludes the proof. □

REFERENCES

[1] F. Breuer: "A note on a paper by Glaser and Schöffl", *Fibonacci Quart.* 36 (1998), 463–466.

[2] F. Breuer: "Ducci sequences over abelian groups", *Comm. Algebra* 27 (1999), 5999–6013.

[3] F. Breuer: "Ducci sequences and cyclotomic fields", *J. Difference Equ. Appl.* 16 (2010), 847–862.

[4] R. Brown – J.L. Merzel: "Limiting behavior in Ducci sequences", *Period. Math. Hungar.* 47 (2003), 45–50.

[5] R. Brown – J.L. Merzel: "The length of Ducci's four-number game", *Rocky Mountain J. Math.* 37 (2007), 45–65.

[6] M. Burmester – R. Forcade – E. Jacobs: "Circles of numbers", *Glasgow Math. J.* 19 (1978), 115–119.

[7] M. Chamberland: "Unbounded Ducci sequences", *J. Difference Equ. Appl.* 9 (2003), 887–895.

[8] C. Ciamberlini – A. Marengoni: "Su una interessante curiosità numerica", *Periodico Mat.* 17 (1937), 25–30.

[9] B. Dular: "Cycles of sums of integers", *Fibonacci Quart.* 58 (2020), 126–139.

[10] A. Ehrlich: "Periods in Ducci's n-number game of differences", *Fibonacci Quart.* 28 (1990), 302–305.

[11] N.J. Fine: "Binomial coefficients modulo a prime", *Amer. Math. Monthly* 54 (1947), 589–592.

[12] B. Freedman: "The four number game", *Scr. Math.* 14 (1948), 35–47.

[13] H. Glaser – G. Schöffl: "Ducci-sequences and Pascal's triangle", *Fibonacci Quart.* 33 (1995), 313–324.

[14] A.L. Furno: "Cycles of differences of integers", *J. Number Theory* 13 (1981), 255–261.

[15] R. Miller: "Mathematical notes: a game with n numbers", *Amer. Math. Monthly* 85 (1978), 183–185.

[16] F. Pompili: "Evolution of finite sequences of integers...", *Math. Gaz.* 80 (1996), 322–332.

[17] H. Rothe-Ille: ZbMath Review on the paper "Su una interessante curiosità numerica" by C. Ciamberlini and A. Marengoni.

[18] M. Misiurewicz – A. Schinzel: "On n numbers on a circle", *Hardy–Ramanujan J.* 11 (1988), 30–39.

[19] M.Z. Spivey: "The Art of Proving Binomial Identities", *Chapman*, New York (2019).

[20] F.B. Wong: "Ducci processes", *Fibonacci Quart.* 20 (1982), 97–105.

Mark L. Lewis
Department of Mathematical Sciences
Kent State University
1300 Lefton Esplanade
Kent, OH 44242 (USA)
e-mail: lewis@math.kent.edu

Shannon M. Tefft (*corresponding author*)
Department of Mathematical Sciences
Kent State University
1300 Lefton Esplanade
Kent, OH 44242 (USA)

Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803

e-mail: stefft@kent.edu



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 117–166 ISSN: 2499-1287
DOI: 10.32037/agta-2026-007

The Self-Dual Indecomposable Modules in Blocks with Cyclic Defect Groups

Caroline Lassueur — John Murray

(*Received Sep. 9, 2024; Accepted Dec. 9, 2024 — Communicated by N. Mazza*)

Abstract

Let p be an odd prime and let **B** be p-block of a finite group, such that **B** has cyclic defect groups. We describe the self-dual indecomposable **B**-modules and for each such module determine whether it is symplectic or orthogonal.

Mathematics Subject Classification (2020): 20C15, 20C20, 20D06

Keywords: Real block; block with cyclic defect groups; self-dual module; Auslander–Reiten quiver

1 Introduction

Let G be a finite group and let k be an algebraically closed field of prime characteristic p. The ordinary irreducible characters $\mathrm{Irr}(G)$ of G are partitioned into (p-)blocks, depending on their values on the p'-order elements of G. These blocks are in bijection with the blocks of the group algebra kG, that is, the minimal two-sided ideals of kG. Moreover, if M is an indecomposable kG-module, there is exactly one block of kG which does not annihilate M. We then say that M belongs to the corresponding block of G.

Let $\mathbf{B}$ be a block of G. The defect groups of $\mathbf{B}$ are a certain conjugation orbit of p-subgroups of G. For example, the block of G containing the trivial kG-module is called the principal block of G and its defect groups are the Sylow p-subgroups of G. At the other extreme, any block which contains a single irreducible character of G has a trivial defect group.

Suppose that $p \neq 2$, that $\mathbf{B}$ has a non-trivial cyclic defect group D and e irreducible modules. Then e is called the inertial index of $\mathbf{B}$, and it is known that $\mathbf{B}$ has a finite number, namely $e|D|$, of isomorphism classes of indecomposable modules.

The Brauer tree of $\mathbf{B}$ is a planar embedded graph $\sigma(\mathbf{B})$ which has e edges labelled by the irreducible $\mathbf{B}$-modules. Now, $\sigma(\mathbf{B})$ has $e+1$ vertices. One vertex is said to be *exceptional*, and it comes with a positive integer $m := (|D|-1)/e$, called its multiplicity (or the exceptional multiplicity of $\sigma(\mathbf{B})$). The exceptional vertex is associated with a family of m *exceptional characters* in $\mathrm{Irr}(\mathbf{B})$. The remaining e vertices are then said to be non-exceptional, and each of them corresponds to a single non-exceptional character in $\mathrm{Irr}(\mathbf{B})$. Thus $\mathrm{Irr}(\mathbf{B})$ contains $e+m$ characters. Notice that if $m = 1$, then any vertex may be designated as the exceptional vertex. Furthermore, it is known that the Morita equivalence class of $\mathbf{B}$ is determined by $\sigma(\mathbf{B})$ together with its exceptional vertex and exceptional multiplicity m. We make this more precise below.

The complex conjugates of the characters in $\mathbf{B}$ form another block $\mathbf{B}^\circ$ that is called the contragredient of $\mathbf{B}$. Furthermore, if M is an indecomposable $\mathbf{B}$-module, then the dual kG-module $M^* := \mathrm{Hom}_k(M,k)$ is an indecomposable $\mathbf{B}^\circ$-module. We say that $\mathbf{B}$ is a *real block* if it coincides with $\mathbf{B}^\circ$.

Now, suppose that $\mathbf{B}$ is a real block. In [6], J. Green showed that the real valued non-exceptional characters in $\mathbf{B}$, together with the exceptional characters in $\mathbf{B}$, correspond to a line segment in $\sigma(\mathbf{B})$, known as the *real stem* of $\sigma(\mathbf{B})$. The edges in the real stem correspond to the self-dual irreducible $\mathbf{B}$-modules. All

or none of the exceptional characters are real-valued. Moreover, the complex conjugate of an exceptional character is exceptional and duality acts as reflection in the real stem.

Let us note that, as p is an odd prime, each self-dual indecomposable kG-module M affords a non-degenerate G-equivariant quadratic form ($+$ type) or a non-degenerate G-equivariant symplectic form ($-$ type) (see [14, Proposition 2.1]). The type indicates whether the associated group representation $G \to GL(M)$ factors through an orthogonal subgroup $O(M)$ or a symplectic subgroup $Sp(M)$ of $GL(M)$, respectively.

Our aim in this article is two-fold. First, we want to provide a concrete classification of the self-dual indecomposable **B**-modules (up to isomorphism). Second, we want to determine their type. We will make use of Janusz' classification of all indecomposable **B**-modules in terms of certain walks on the Brauer tree called *paths* (see [11]). We then reduce the determination of the type of a self-dual module, to the determination of the type a certain self-dual indecomposable module of a local subgroup of G. This in turn can be computed using the character table of the subgroup.

We summarize our main results in the following two theorems. The statements will be made more precise in Theorem 4.2 and Theorem 4.4 in Section 4.

Theorem 1.1 *Let M be a non-projective indecomposable module belonging to* **B**. *Then M is self-dual if and only if one of the following conditions is satisfied*:

(1) *M is an irreducible module indexed by an edge on the real stem of $\sigma(\mathbf{B})$; or*

(2) *M is reducible and its Janusz path (in the sense of Notation A.1) is fixed under reflection in the real stem.*

We highlight a family of indecomposable **B**-modules, called *hooks* in [2, Section 2.3], and defined as quotients of the PIMs

of **B** as follows. If E is an irreducible **B**-module, then its projective cover $P(E)$ has

$$E = \operatorname{soc}(P(E)) = \operatorname{hd}(P(E)).$$

Moreover, there are uniserial (possibly zero) **B**-modules Q_a and Q_b such that

$$\operatorname{rad}(P(E))/\operatorname{soc}(P(E)) = Q_a \oplus Q_b.$$

We can visualize $P(E)$ using the following diagram:

$$P(E) = \boxed{\begin{array}{c} E \\ Q_a \oplus Q_b \\ E \end{array}}.$$

Then the two uniserial quotients of $P(E)$ of the form

$$H_a := \boxed{\begin{array}{c} E \\ Q_a \end{array}} \qquad \text{and} \qquad H_b := \boxed{\begin{array}{c} E \\ Q_b \end{array}}$$

are called *hooks*. When $Q_a = 0$ (respectively $Q_b = 0$), then we have that $H_a = E$ (respectively $H_b = E$) is irreducible. Clearly, **B** has exactly $2e$ isomorphism classes of hooks. We also note, that the hooks are precisely the modules occurring in Green's walk around the Brauer tree [6], and they form the boundary of the stable Auslander–Reiten quiver $\Gamma_s(\mathbf{B})$ of **B** (see Subsection 2.3 for this notion).

Regarding the type of the **B**-modules, we have the following result.

Theorem 1.2 *Up to isomorphism* **B** *has exactly* $|D| - 1$ *non-projective indecomposable self-dual modules. There are two self-dual hooks in* **B**.

(1) *Each self-dual indecomposable* **B***-module* M *has the same type as a self-dual hook* H*, with* H *determined by the position of* M *in the stable Auslander–Reiten quiver* $\Gamma_s(\mathbf{B})$.

(2) *The type of* H *coincides with the type of its Green correspon-*

dent $g(H)$ *in* $N_G(D)$. *Moreover the type of* $g(H)$ *can be computed from the character table of* $N_G(D)$.

The paper is structured as follows. In Section 2, we set up our notation and prove preliminary results that allow us to determine the number of all self-dual indecomposable modules in **B**. In Section 3, we investigate our main problem for the case of a uniserial block, where we explicitly describe the type of each self-dual module. In Section 4, we give a concrete classification of the self-dual indecomposable modules in **B** in terms of Janusz' classification of the indecomposable **B**-modules. Besides, we provide a procedure to determine the type of any such module. Finally, in Appendix 4, for completeness, we briefly recap Janusz' parametrization mentioned above.

2 Notation and preliminary results

We begin with a condensed summary of some standard notation for blocks with cyclic defect groups which will be used throughout this article. All results mentioned below without reference can be found in the foundational paper of E. Dade [3] or [1, Section 6.5].

2.1 General notation

Let G be a finite group and let k be an algebraically closed field of prime characteristic $p \neq 2$. Moreover, let **B** be a real p-block of G and let D be a defect group of **B**. We assume that D is cyclic of order $|D| = p^a$, with $a \geqslant 1$.

Let D_i be the unique subgroup of D which has order p^i, set $N_i := N_G(D_i)$ and let $\mathbf{B}_i$ be a p-block of N_i such that $\mathbf{B}_i^G = \mathbf{B}$, for each $i = 0, \ldots, a$. Let **b** be a block of $C_G(D)$ which has defect group D and which satisfies $\mathbf{b}^G = \mathbf{B}$. If E is the stabilizer of **b** in $N_G(D)$, then $e := [E : C_G(D)]$ gives the inertial index of **B**.

Consider the action of E on $\mathrm{Irr}(D)$. We choose a set Λ of representatives for the orbits of E on the non-trivial characters in $\mathrm{Irr}(D)$. Each such orbit has cardinality e. Hence,

$$|\Lambda| = \frac{|D|-1}{e}.$$

This number is the multiplicity m mentioned in the introduction.

Recall that $\mathbf{B}$ has e isomorphism classes of irreducible modules, with representatives $E_0, \dots, E_{e-1}$, and $e+m$ ordinary irreducible characters, of which e are non-exceptional and m are exceptional. So we use the notation

$$\mathrm{Irr}(\mathbf{B}) = \{\chi_1, \dots, \chi_e\} \cup \{\chi_\lambda \mid \lambda \in \Lambda\},$$

and set

$$\chi_\Lambda := \sum_{\lambda \in \Lambda} \chi_\lambda$$

as the sum of the exceptional characters.

Suppose now that $m = 1$. Then there is no canonical choice of exceptional character in $\mathbf{B}$. (One character can artificially be designated to be exceptional.) Moreover, E has a single orbit on the non-trivial characters in $\mathrm{Irr}(D)$. So $|D| = p$, and there are p characters in $\mathrm{Irr}(\mathbf{B})$. As p is odd, at least one irreducible character in $\mathbf{B}$ is real. So we can and do assume that χ_Λ is real valued in this case.

Recall that $\sigma(\mathbf{B})$ denotes the Brauer tree of $\mathbf{B}$. For convenience we identify $\sigma(\mathbf{B})$ with a connected subset of $\mathbb{C}$. The real irreducible characters are represented by vertices placed on $\mathbb{R}$, with the exceptional vertex placed at 0. So every self-dual irreducible $\mathbf{B}$-module is represented by an edge in $\mathbb{R}$. Moreover the complex conjugate of an irreducible character placed at $x+iy$ is placed at $x-iy$. In this way duality on $\sigma(\mathbf{B})$ extends to complex conjugation on $\mathbb{C}$. In our drawings we indicate the non-exceptional vertices with hollow nodes and the exceptional

vertex with a black node.

It is known that $\mathbf{B}$ has $e|D|$ isomorphism classes of indecomposable modules. We next outline two quite different ways of parametrizing the non-projective indecomposable $\mathbf{B}$-modules. In our discussion we may identify a module with its isomorphism class.

2.2 Janusz' parametrization of the indecomposable modules

First, it is convenient to split the isomorphism classes of indecomposable $\mathbf{B}$-modules into three families:

1. the e isomorphism classes of irreducible $\mathbf{B}$-modules that we denote by $E_0, \ldots, E_{e-1}$;
2. the e isomorphism classes of projective indecomposable modules $P(E_0), \ldots, P(E_{e-1})$, which are the projective covers of $E_0, \ldots, E_{e-1}$, respectively;
3. the $e(|D|-2)$ isomorphism classes of all the indecomposable $\mathbf{B}$-modules which are neither irreducible nor projective.

The Loewy structure of the projective indecomposable modules is well-known. We refer to [1, Section 4.18] for a detailed description. Then, G. Janusz [11] parametrized the $e(|D|-2)$ non-projective and non-irreducible indecomposable $\mathbf{B}$-modules using certain walks in the Brauer tree $\sigma(\mathbf{B})$, which he called *paths*. We refer the reader to Appendix 4, Notation A.1, for a more detailed description of this parametrization. In brief, each such indecomposable $\mathbf{B}$-module X can be described by three parameters:

(1) a *path* on $\sigma(\mathbf{B})$, which is a directed connected subgraph of Type I or Type II as defined in Notation A.1, and the edges of which form an ordered sequence $(S_1, \ldots, S_t)$ of irreducible $\mathbf{B}$-modules such that the odd-indexed modules are in the head of X and the even-indexed edges are in the socle of X, or conversely;

(2) a *direction* $(\varepsilon_1, \varepsilon_t)$, where, for $i \in \{1, t\}$ we set $\varepsilon_i =: 1$ if S_i is in the head of X and $\varepsilon_i =: -1$ if S_i is in the socle of X;

(3) a *multiplicity* μ, defined as follows. Set $\mu := 0$ if $m = 1$, and if $m > 1$, then μ corresponds to the number of times that an irreducible module adjacent to the exceptional vertex on the path occurs as a composition factor of X.

Observe in particular that a non-irreducible uniserial **B**-module M is described by a path of length 2 of the form

$$\overset{\chi_a}{\bullet} \xrightarrow{T} \overset{\chi_b}{\bullet} \xrightarrow{S} \overset{\chi_c}{\bullet}$$

where the vertices χ_a, χ_b, χ_c belong to $\{\chi_1, \dots, \chi_e\} \cup \{\chi_\Lambda\}$ and S and T are irreducible **B**-modules. If the direction is $\varepsilon = (1, -1)$, then $T = \mathrm{hd}(M)$ and $S = \mathrm{soc}(M)$.

The hooks of **B**, which we defined in the introduction, are either irreducible, or uniserial with composition length greater than 1, thus described by paths of length 2, as given above. Let us note that a precise description of all uniserial and all self-dual uniserial **B**-modules in terms of path, direction, multiplicity is given in Remark A.2 (d) and Lemma A.3.

In Section 4 we will describe all the self-dual indecomposable **B**-modules in terms of these three parameters.

2.3 The stable Auslander–Reiten quiver

Next, the Auslander–Reiten quiver $\Gamma_s(\mathbf{B})$ of **B** is a directed graph whose vertices index the isomorphism classes of the non-projective indecomposable **B**-modules. This graph has a particularly rich structure.

Recall that the *projective cover* of a kG-module M is a certain projective module $P(M)$, together with a short exact sequence of kG-modules

$$0 \to \Omega^1(M) \to P(M) \to M \to 0.$$

The kernel $\Omega^1(M)$ is called the *Heller translate* of M. Dualising the above short exact sequence gives another short exact sequence

$$0 \to M^* \to P(M)^* \to \Omega^1(M)^* \to 0.$$

Now, the *injective envelope of* M^* is a certain injective kG-module $I(M^*)$, together with a short exact sequence of kG-modules

$$0 \to M^* \to I(M^*) \to \Omega^{-1}(M^*) \to 0.$$

But $P(M)^* \simeq I(M^*)$. So

$$\Omega^1(M)^* \simeq \Omega^{-1}(M^*)\,, \tag{2.1}$$

whence

$$\Omega^2(M)^* \simeq \Omega^{-2}(M^*). \tag{2.2}$$

For a precise description of the Auslander–Reiten quiver $\Gamma_s(\mathbf{B})$, we refer the reader to [1, Section 6.5]. Summed up, in blocks with cyclic defect groups, it is well-known, that all modules are periodic of period $2e$. It follows that the quiver $\Gamma_s(\mathbf{B})$ is a finite tube of type $(\mathbb{Z}/e\mathbb{Z})A_{|D|-1}$, where the Auslander–Reiten translate is Ω^{-2}. This tube consists of $|D|-1 = em$ *levels* arranged consecutively from level 1 to level em, with each level consisting of e indecomposable modules arranged in a loop. More precisely, level ℓ can be described as

$$\{\Omega^{-2j}(M) \mid 0 \leqslant j \leqslant e-1\}$$

where M is an arbitrarily chosen module on the level, and for each $j = 0, \ldots, e-1$ the right successor of $\Omega^{-2j}(M)$ on the loop is $\Omega^{-2j-2}(M)$. For this reason the levels of $\Gamma_s(\mathbf{B})$ are usually called Ω^2-*orbits*.

Observe that the $2e$ modules which constitute the two ends of the tube $(\mathbb{Z}/e\mathbb{Z})A_{|D|-1}$ are the hooks of $\mathbf{B}$. Moreover, there exists an irreducible $\mathbf{B}$-module X which is a leaf of $\sigma(\mathbf{B})$ such

that level 1 is

$$\{\Omega^{-2j}(X) \mid 0 \leqslant j \leqslant e-1\}$$

and level em is

$$\{\Omega^{-2j+1}(X) \mid 0 \leqslant j \leqslant e-1\},$$

or conversely.

Let us show the following preliminary result.

Lemma 2.1 *If e is odd, then each level of $\Gamma_s(\mathbf{B})$ has 1 self-dual module, and if e is even, then each level of $\Gamma_s(\mathbf{B})$ has 0 or 2 self-dual modules.*

Proof — Let $\ell \in \{1, \dots, em\}$ and suppose that the ℓ-th level of $\Gamma_s(\mathbf{B})$ consists of the modules Y_i, for $i \in \mathbb{Z}$. Then, we have that $Y_{i+1} = \Omega^{-2}(Y_i)$ and $Y_i \simeq Y_j$ if and only if $i \equiv j \pmod{e}$.

If e is odd, then level ℓ contains at least one self-dual module. If e is even, we may assume that level ℓ contains a self-dual module. In both cases we choose notation so that Y_0 is self-dual. Then $Y_i = \Omega^{-2i}(Y_0)$ and isomorphism (2.2) gives $Y_i^* \simeq Y_{e-i}$, for all $i = 0, \dots, e-1$. The congruence $i \equiv e - i \pmod{e}$ has one solution $i = 0$ if e is odd, and the two solutions $i = 0, e/2$, if e is even. □

Corollary 2.2 *The block $\mathbf{B}$ has two isomorphism classes of self-dual hooks. In particular, we have that*:

(1) *If H is a self-dual hook, then the other self-dual hook is $\Omega^e(H)$.*

(2) *If e is odd, then H lies on one end Ω^2-orbit and $\Omega^e(H)$ lies on the other end Ω^2-orbit.*

(3) *If e is even, H and $\Omega^e(H)$ lie on the same end Ω^2-orbit of $\Gamma_s(\mathbf{B})$.*

Proof — To start with, we prove that $\mathbf{B}$ contains at least one self-dual hook. First, it follows from the definition that the dual of a hook of $\mathbf{B}$ is again a hook of $\mathbf{B}$. Now, if $\mathbf{B}$ contains a hook H_0 such that $H_0^* \not\simeq H_0$, then $e > 1$ and there is $1 < i < e$

such that $H_0^* \simeq \Omega^{-2i}(H_0)$. Indeed, as duality acts as reflection in the real stem, H_0 and its dual must lie on the same end Ω^2-orbit of $\Gamma_s(\mathbf{B})$. Then, the hook $\Omega^{-i}(H_0)$ is self-dual since

$$\Omega^{-i}(H_0)^* \simeq \Omega^i(H_0^*) \simeq \Omega^{i-2i}(H_0) = \Omega^i(H_0)$$

by isomorphism (2.1).

Next, it is clear that if H is a self-dual hook, then so is $\Omega^e(H)$ as

$$\Omega^e(H)^* \simeq \Omega^{-e}(H^*) \simeq \Omega^{-e}(H) \simeq \Omega^{-e+2e}(H) = \Omega^e(H)$$

again by isomorphism (2.1).

If e is odd, then we clearly have that H and $\Omega^e(H)$ lie in different end Ω^2-orbits. If e is even, then H and $\Omega^e(H)$ lie on the same end Ω^2-orbit of $\Gamma_s(\mathbf{B})$ and, by isomorphism (2.1), we obtain that $\Omega^{-2j+1}(H)$ cannot be self-dual, for any $0 \leqslant j \leqslant e-1$. Finally, Lemma 2.1 shows that H and $\Omega^e(H)$ account for all the self-dual hooks of $\mathbf{B}$. □

2.4 Socle and radical layers and duality

In order to determine the self-dual indecomposable modules we use the following well-known formulae for the socle and radical layers of the dual of a kG-module X (see, e.g., [13, Section 6.3]). For each non-negative integer n, we have

$$\operatorname{soc}^{n+1}(X^*)/\operatorname{soc}^n(X^*) \simeq \left(\operatorname{rad}^n(X)/\operatorname{rad}^{n+1}(X)\right)^*. \tag{2.3}$$

In particular, the socle and the head of X and X^* are related by

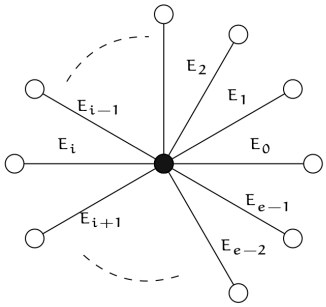
$$\operatorname{soc}(X^*) \simeq \operatorname{hd}(X)^* \qquad \text{and} \qquad \operatorname{hd}(X^*) \simeq \operatorname{soc}(X)^*. \tag{2.4}$$

3 Uniserial blocks

We retain the assumptions of Subsection 2.1. In particular, D_1 is the unique subgroup of D of order p and $\mathbf{B}_1$ is the Brauer

correspondent of $\mathbf{B}$ in $N_G(D_1)$. Now, D is also a defect group of $\mathbf{B}_1$ and the Brauer tree $\sigma(\mathbf{B}_1)$ is a star, with exceptional central vertex and e edges attached to this vertex. Moreover, we adopt the following additional notation:

- The edges (and irreducible $\mathbf{B}_1$-modules) are labelled in counter-clockwise order as $E_0, \dots, E_{e-1}$,.
- We extend notation by defining $E_z := E_{\bar{z}}$, where $\bar{z}$ is the residue of z modulo e, for all $z \in \mathbb{Z}$.



Each non-projective indecomposable module in $\mathbf{B}$ has a Green vertex D_i, for some $i = 1, \dots, a$. As $N_G(D_i) \leqslant N_G(D_1)$, Green correspondence establishes a bijection between the non-projective indecomposable $\mathbf{B}$-modules and the non-projective indecomposable $\mathbf{B}_1$-modules. It also induces a graph isomorphism $\Gamma_s(\mathbf{B}) \simeq \Gamma_s(\mathbf{B}_1)$. Moreover, we have the following result.

Lemma 3.1 *Green correspondence restricts to a type-preserving bijection between the self-dual indecomposable* $\mathbf{B}$*-modules and the self-dual indecomposable* $\mathbf{B}_1$*-modules.*

Proof — Let M be a self-dual indecomposable $\mathbf{B}$-indecomposable module which has vertex D_i, where $D_i \neq 1$. Then

$$M{\downarrow_{N_G(D_1)}} = N \oplus X,$$

where N is the Green correspondent of M with respect to D_i in $N_G(D_1)$. So N belongs to $\mathbf{B}_1$ and has vertex D_i and no in-

decomposable summand of X has vertex D_i. Taking duals, we get

$$M{\downarrow_{N_G(D_1)}} \simeq M^*{\downarrow_{N_G(D_1)}} = N^* \oplus X^*.$$

As N^* has vertex D_i, it follows that $N^* \simeq N$.

The types of M and N coincide, according to the main result in [5]. □

As $\sigma(\mathbf{B}_1)$ is a star, $\mathbf{B}_1$ is a uniserial algebra. This means that each indecomposable $\mathbf{B}_1$-module is uniserial, that is, has a unique composition series. One consequence of this is that we may assume that the modules on the ℓ-th level of the stable Auslander–Reiten quiver of $\mathbf{B}_1$ have composition length ℓ, for each $\ell = 1, \ldots, em$. (See, e.g., [1, Section 6.4].)

We use $[i, \ell]$ to denote the unique uniserial $\mathbf{B}_1$-module with ℓ composition factors $E_i, E_{i-1}, E_{i-2}, \ldots, E_{i-\ell+1}$, listed from socle to head. Notice that $[i, \ell]$ is a submodule of $[j, k]$ if and only if $i = j$ and $\ell \leqslant k$, while $[i, \ell]$ is a factor module of $[j, k]$ if and only if $i - \ell \equiv j - k \bmod e$ and $\ell \leqslant k$.

For each residue i modulo e, define i^* so that $E_i^* \simeq E_{i^*}$. It follows from [6] that

$$i^* = 0^* - i,$$

for all i. Moreover, we may choose notation so that

$$E_0^* \simeq E_0 \quad \text{or} \quad E_0^* \simeq E_{-1}.$$

In the first case, $i^* = -i$ and, in the second case, $i^* = -i - 1$.

Lemma 3.2 *The block $\mathbf{B}_1$ possesses $|D| - 1$ isomorphism classes of non-projective self-dual indecomposable modules. More precisely, $[i, \ell]$ is self-dual if and only if $\ell \equiv i - i^* + 1 \pmod{e}$.*

Proof — As $[i, \ell]$ has head $E_{i-\ell+1}$, (2.3) implies that $[i, \ell]^*$ has socle $E_{i-\ell+1}^*$. Moreover, $[i, \ell]^*$ has the same composition length, namely ℓ, as $[i, \ell]$. It follows that

$$[i, \ell]^* \simeq [(i - \ell + 1)^*, \ell].$$

This gives the congruence condition which determines if $[i, \ell]$ is self-dual.

For each of the e possible values of i, there will be m values of ℓ satisfying the stated congruence condition. This gives the total count of $em = |D| - 1$ non-projective self-dual indecomposable $\mathbf{B}_1$-modules. □

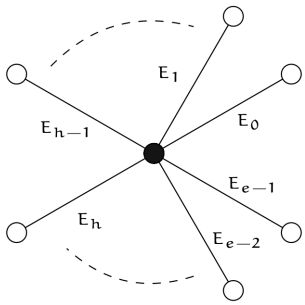
Corollary 3.3 *The block* $\mathbf{B}$ *has exactly* $|D| - 1$ *isomorphism classes of non-projective self-dual indecomposable modules.*

Proof — This follows from Lemmas 3.1 and 3.2. □

From [12], $\mathbf{B}$ (and thus also $\mathbf{B}_1$) has a real exceptional character if and only if $\mathbf{b}$ is real and e is even, or $\mathbf{b}$ is not real and e is odd. Also, all exceptional characters are real if any one of them is real. Finally, if e is even but $\mathbf{b}$ is not real (so $\mathbf{B}_1$ has no real exceptional characters), and the real stem of $\mathbf{B}_1$ contains two edges, then the Frobenius–Schur indicators of the two real (non-exceptional) irreducible characters in $\mathbf{B}_1$ are $+1$ and -1, in some order.

In what follows, we distinguish three cases, depending on the number of self-dual irreducible $\mathbf{B}_1$-modules.

Case 1: $\mathbf{B}_1$ *has no self-dual irreducible modules.*
In this case, we have that e is even and the real stem of $\sigma(\mathbf{B}_1)$ consists of the exceptional vertex. Set $h := e/2$ and assume that $0^* = -1$.



Then $i^* \equiv -1 - i \pmod{e}$, and in particular $h^* = h - 1$. Also,

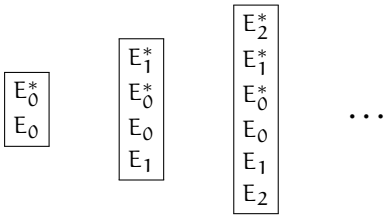
we have that $[i, \ell]$ is self-dual if and only if

$$\ell \equiv 2i + 2 \pmod{e},$$

by Lemma 3.2.

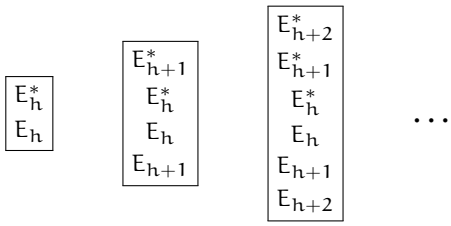
Proposition 3.4 *Non-projective self-dual indecomposable* $\mathbf{B}_1$*-modules can be divided into two families*:

(1) *The modules* $[i, 2i+2]$*, for* $i = 0, 1, \ldots, mh - 1$*:*



In particular, these modules have the same type as the hook module $[(mh)^*, me]$.

(2) *The modules* $[h+i, 2i+2]$*, for* $i = 0, 1, \ldots, mh - 1$:



In particular, these modules have the same type as the hook module $[(mh+h)^*, me]$.

Moreover, there is one self-dual module from each family in each even numbered level of $\Gamma_s(\mathbf{B}_1)$*, and none in each odd numbered level.*

Proof — Let us notice that

$$0^* \equiv -1 \qquad \text{and} \qquad h^* \equiv h - 1 \pmod{e}.$$

There are no self-dual projective indecomposable modules in this case, because such a module would be the projective cover of a self-dual irreducible module.

The projective cover of E_{0^*} has Jacobson radical $[0^*, me]$. This module is self-dual as

$$0 \equiv me \equiv 2 \times 0^* + 2 \pmod{e}.$$

Let B_0 be a non-degenerate G-invariant bilinear form on $[0^*, me]$. The submodule $[0^*, me - i]$ of $[0^*, me]$ has B_0-dual $[0^*, i]$. Therefore B_0 induces a non-degenerate G-invariant bilinear form (of the same type as B_0) on the factor module

$$[0^*, me - i]/[0^*, i] = [i^*, me - 2i].$$

When $i = mh - 1$, we get the shortest module $[mh, 2]$ in the family. These self-dual subquotients of $[0^*, me]$ give all modules in one of the families.

Similarly, the Jacobson radical $[h^*, me]$ of the projective cover of E_h^* is self-dual. Its subquotients give the modules

$$[(h + i)^*, me - 2i]$$

in the other family. When $i = mh - 1$, we get the shortest module

$$[(m + 1)h, 2]$$

in the family.

This accounts for all non-projective self-dual indecomposable modules in $\mathbf{B}_1$. The last statement is clear as the level of a module in $\Gamma_s(\mathbf{B}_1)$ is given by its composition length. □

Example 3.5 Consider the group $C_{15} : C_8$, where a generator of C_8 squares a generator of C_{15}. Note that this group has a real 5-block $\mathbf{B}$ of defect 1 which has no real irreducible characters. Besides, the Brauer tree is a star with

$$e = 2 = m.$$

If S is an irreducible $\mathbf{B}$-module, then the irreducible $\mathbf{B}$-modules are S and S^*. There is a self-dual indecomposable $\mathbf{B}$-module with composition series S/S^* and another with composition series S^*/S. One of these is of $+$ type and the other is of $-$ type.



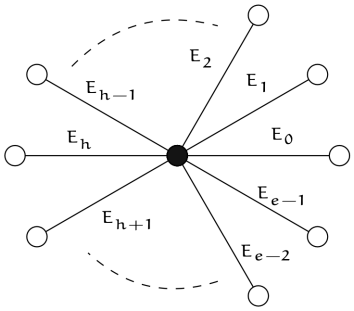
Example 3.6 Consider the group $C_5 : C_4$, where a generator of the C_4 inverts C_5. This group has a real 5-block $\mathbf{B}$ of defect 1 which has a pair of real exceptional characters but no real non-exceptional characters. The Brauer tree is a star such that

$$e = 2 = m.$$

Let S be an irreducible $\mathbf{B}$-module. Therefore, the other irreducible $\mathbf{B}$-module is S^*. The block has 4 self-dual indecomposable modules, all of $-$ type. It should be noted that both exceptional characters have Frobenius–Schur indicator -1.



Case 2: $\mathbf{B}_1$ *has two self-dual irreducible modules.*
In this case, e is even and again we set $h := e/2$. We may assume that E_0 and E_h are the self-dual irreducible $\mathbf{B}_1$-modules. So the real stem of $\sigma(\mathbf{B}_1)$ consists of the edges E_0 and E_h and their endpoints. Moreover, $E_i^* = E_{-i}$, for all $i = 0, \ldots, e-1$.



Proposition 3.7 *The non-projective self-dual indecomposable* $\mathbf{B}_1$ *modules are divided into two families*:

(1) *The modules* $[i, 2i+1]$, *for* $i = 0, 1, \ldots, mh-1$*:*

$$\boxed{E_0} \qquad \boxed{\begin{matrix} E_1^* \\ E_0 \\ E_1 \end{matrix}} \qquad \boxed{\begin{matrix} E_2^* \\ E_1^* \\ E_0 \\ E_1 \\ E_2 \end{matrix}} \qquad \cdots$$

These modules have the same type as that of E_0 *and of the projective cover of* E_{mh}.

(2) *The modules* $[h+i,\ 2i+1]$, *for* $i = 0, 1, \ldots, mh-1$:

$$\boxed{E_h} \qquad \boxed{\begin{matrix} E_{h+1}^* \\ E_h \\ E_{h+1} \end{matrix}} \qquad \boxed{\begin{matrix} E_{h+2}^* \\ E_{h+1}^* \\ E_h \\ E_{h+1} \\ E_{h+2} \end{matrix}} \qquad \cdots$$

These modules have the same type as that of E_h *and of the projective cover of* $E_{(m+1)h}$.

There is one self-dual module from each family in each odd numbered level of $\Gamma_s(\mathbf{B}_1)$*, and none in each even numbered level.*

PROOF — In this case, notice that $\mathbf{B}_1$ contains two non-isomorphic self-dual PIMs, namely the projective covers of E_0 and E_h. The self-dual subquotients of the projective cover of E_{mh} give all modules in the first family and the self-dual subquotients of the projective cover of $E_{(m+1)h}$ give all modules in the second family. This determines the type of the modules in each family, as in the proof of Proposition 3.4. We omit the details.

This accounts for all non-projective self-dual indecomposable modules in $\mathbf{B}_1$. The last statement is clear as the level of a module in $\Gamma_s(\mathbf{B}_1)$ is given by its composition length. □

Let us observe that the type of E_0 coincides with the Frobenius–Schur indicator of the real non-exceptional character which lifts the Brauer character of E_0. Likewise the type of E_h coincides with the Frobenius–Schur indicator of the other real non-exceptional character.

Corollary 3.8 *All self-dual indecomposable* $\mathbf{B}_1$*-modules have the same type, if* m *is odd.*

PROOF — The hypothesis implies that

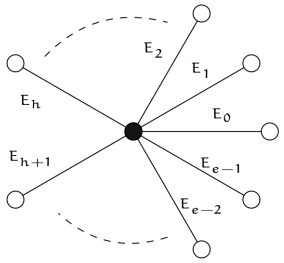
$$mh \equiv h \pmod{e}.$$

Hence, modules in the first family, including E_0, have the same type as the projective cover of E_h. However, let us note that Proposition 2.2 in [14] shows that E_h and its projective cover have the same type. Therefore, all self-dual indecomposable $\mathbf{B}_1$-modules have the same type as E_0. □

Example 3.9 Consider the group $C_{15} : C_4$, where a generator of the C_4 squares a generator of C_{15}. Observe that this group has a real 5-block $\mathbf{B}$ of defect 1 which has two exceptional characters, one with Frobenius–Schur indicator $+1$ and the other with Frobenius–Schur indicator -1. The two exceptional characters form a complex conjugate pair. The Brauer tree is a star with $e = 2 = m$. Then, $\mathbf{B}$ has two self-dual irreducible modules S and T, where S has $+$ type and T has $-$ type.



Case 3: $\mathbf{B}_1$ *has one self-dual irreducible module.*
In this case, e is odd and we may assume that E_0 is the unique self-dual irreducible $\mathbf{B}_1$-module. Also m is even, as $me = |D| - 1$ is even. The real stem of $\sigma(\mathbf{B}_1)$ consists of E_0 and its endpoints, and $E_i^* = E_{-i}$, for $i = 0, \dots, e-1$. We set $h := (e-1)/2$.



Proposition 3.10 *The class of all non-projective self-dual indecomposable* $\mathbf{B}_1$*-modules are divided into two families*:

(1) *The modules* $[i, 2i+1]$, *for* $i = 0, 1, \dots, me/2 - 1$*:*

$$\boxed{E_0} \qquad \boxed{\begin{matrix} E_1^* \\ E_0 \\ E_1 \end{matrix}} \qquad \boxed{\begin{matrix} E_2^* \\ E_1^* \\ E_0 \\ E_1 \\ E_2 \end{matrix}} \qquad \dots$$

These modules have the same type as the projective cover of E_0.

(2) *The modules* $[h+i, 2i+2]$, *for* $i = 0, \dots, me/2 - 1$:

$$\boxed{\begin{matrix} E_h^* \\ E_h \end{matrix}} \qquad \boxed{\begin{matrix} E_{h+1}^* \\ E_h^* \\ E_h \\ E_{h+1} \end{matrix}} \qquad \boxed{\begin{matrix} E_{h+2}^* \\ E_{h+1}^* \\ E_h^* \\ E_h \\ E_{h+1} \\ E_{h+2} \end{matrix}} \qquad \dots$$

In particular, these modules have the same type as the hook module

$$[h^*, me] \simeq \Omega^e(E_0).$$

There is one module in the first (*respectively second*) *family on each odd* (*respectively even*) *numbered level of* $\Gamma_s(\mathbf{B}_1)$.

Proof — There is exactly one self-dual PIM in $\mathbf{B}_1$, namely the projective cover of E_0. The self-dual proper subquotients of $P(E_0)$ have the same type and give all modules in the first family. The smallest of these modules is E_0.

Similarly, we have that the Jacobson radical $[h^*, me]$ of the projective cover of E_h^* is self-dual, as its head is E_h and its socle is E_h^*. The self-dual subquotients of $[h^*, me]$ have the same type and give all modules in the second family. The smallest of these modules is $[h, 2]$.

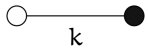
Furthermore, the isomorphism

$$[h^*, me] \simeq \Omega^e(E_0)$$

follows from Corollary 2.2.

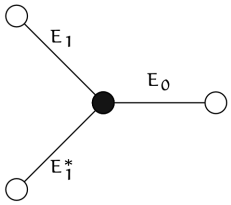
This accounts for all non-projective self-dual indecomposable modules in $\mathbf{B}_1$. The last statement is clear as the level of a module in $\Gamma_s(\mathbf{B}_1)$ is given by its composition length. □

Example 3.11 The cyclic group C_3 has a single 3-block of defect 1. The trivial character is non-exceptional and the two exceptional characters form a complex conjugate pair. The unique irreducible module (the trivial module) has $+$ type, and the unique 2-dimensional indecomposable module has $-$ type.



Example 3.12 Let $p = 7$ and let $\mathbf{B}$ be a self-dual 7-block with a cyclic defect group $D \simeq C_7$. Moreover, assume $e = 3$, and thus $m = 2$. The Brauer tree of the Brauer correspondent $\mathbf{B}_1$ of $\mathbf{B}$ in $N_G(D_1)$ is a star with three edges and exceptional vertex at

its centre and there is precisely one self-dual simple $\mathbf{B}_1$-module, say E_0:



Let us write E_1 and E_1^* for the remaining pair of dual irreducible modules, that is

$$E_1^* = E_2.$$

The $|D| - 1 = 6$ self-dual non-projective $\mathbf{B}_1$-modules can be described as follows.

1. In family (1), we have

$$[1^*, 5] = \begin{bmatrix} E_1 \\ E_1^* \\ E_0 \\ E_1 \\ E_1^* \end{bmatrix}, \quad [1, 3] = \begin{bmatrix} E_1^* \\ E_0 \\ E_1 \end{bmatrix} \quad \text{and} \quad [0, 1] = E_0\,.$$

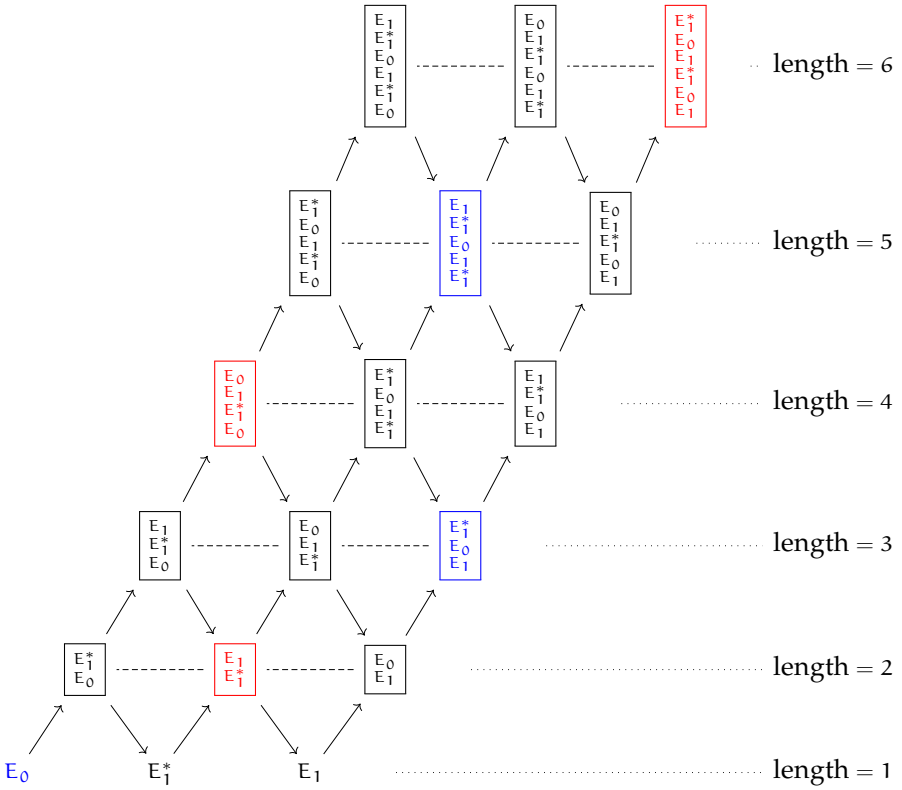
2. In family (2), we have

$$[1, 6] = \begin{bmatrix} E_1^* \\ E_0 \\ E_1 \\ E_1^* \\ E_0 \\ E_1 \end{bmatrix}, \quad [0, 4] = \begin{bmatrix} E_0 \\ E_1 \\ E_1^* \\ E_0 \end{bmatrix} \quad \text{and} \quad [1^*, 2] = \begin{bmatrix} E_1 \\ E_1^* \end{bmatrix}.$$

The stable Auslander–Reiten quiver $\Gamma_s(\mathbf{B}_1)$ is as follows. Observe that, formally, we should draw arrows from from the third diagonal to the first diagonal, which close the tube of shape

$$(\mathbb{Z}/3\mathbb{Z})A_6.$$

We omit them, however, for clarity, as these are easy to work out.



3.1 Case when the defect group is normal

In this section, we assume that a defect group D of **B** is normal in G. We can then use an inner-product calculation to determine the types of the self-dual indecomposable **B**-modules.

Let us recall that **b** is a block of $C_G(D)$ covered by **B**. Set $G_{\mathbf{b}}$ as its stabilizer in G. Then,

$$e = [G_{\mathbf{b}} : C_G(D)]$$

is the inertial index of **B**. Also the Brauer tree $\sigma(\mathbf{B})$ is a star with e edges, indexing the irreducible **B**-modules. The central

vertex is exceptional, and it has multiplicity

$$m = \frac{|D| - 1}{e}.$$

As the quotient group $G_{\mathbf{b}}/C_G(D)$ is cyclic of p'-order e, the unique irreducible $\mathbf{b}$-module has e non-isomorphic extensions to $G_{\mathbf{b}}$. Moreover, each extension induces irreducibly to G. These represent the e isomorphism classes of irreducible $\mathbf{B}$-modules.

Let $u \in D$ generate the unique order p subgroup of D. As $\langle u \rangle$ is normalized by G, we have that, for each $g \in G$, there is an integer $n(g)$, determined modulo p, such that $gug^{-1} = u^{n(g)}$. It is clear that $\lambda(g) := n(g)1_k$ defines a faithful linear k-character of $G/C_G(D)$.

Let S be an irreducible $\mathbf{B}$-module and identify λ with the corresponding 1-dimensional kG-module. By [6, Section 5], we then obtain that $S, \lambda S, \dots, \lambda^{e-1}S$ are representatives of the isomorphism classes of irreducible $\mathbf{B}$-modules. Besides, notice that these index the edges of $\sigma(\mathbf{B})$ in counter-clockwise order around 0. Thus $S \simeq \lambda^e S$ and the $|D|$ composition factors of the (uniserial) projective cover of S are $S, \lambda S, \dots, \lambda^{me}S \simeq S$, listed from top to bottom.

Let χ and μ be irreducible characters of G whose restrictions to the p-regular elements of G are the Brauer character of S and λ, respectively. Then $\chi, \mu\chi, \dots, \mu^{e-1}\chi$ are the non-exceptional irreducible characters in $\mathbf{B}$ and the restriction of $\mu^i\chi$ to the p-regular elements of G is the Brauer character of $\lambda^i S$, for all $i = 0, \dots, e-1$.

The statement of the following lemma is slightly more general than needed.

Lemma 3.13 *Let G be a finite group, S an irreducible kG-module, and $\lambda : G \to k^\times$ a linear representation such that $S^* \simeq \lambda S$. Suppose that μ and χ are ordinary characters of G lifting the Brauer characters*

of λ and S, respectively. Define

$$\epsilon_\mu(\chi) := \frac{1}{|G|}\sum_{g\in G}\mu(g)\chi(g^2). \tag{3.1}$$

Then $\epsilon_\mu(\chi) = \pm 1$, and there is a bilinear form $B : S \times S \to k$ such that

$$B(s_2, s_1) = \epsilon_\mu(\chi)B(s_1, s_2) \quad \textit{and} \quad B(gs_1, gs_2) = \lambda(g)B(s_1, s_2),$$

for all $g \in G$ and $s_1, s_2 \in S$. Moreover, B is uniquely determined by S and λ, up to a non-zero scalar.

Proof — Let $\alpha : G \to GL_n(k)$ be a matrix representation for the kG-module S. Now, the transpose inverse map $M \mapsto M^{-t}$, for $M \in GL_n(k)$, is an outer automorphism of $GL_n(k)$. Composing this with α, we obtain that $\alpha^* : G \to GL_n(k)$, defined by $\alpha^*(g) := \alpha(g)^{-t}$, for all $g \in G$. This is a matrix representation corresponding to the dual kG-module S^*.

As $\lambda S \simeq S^*$, there is $B \in GL_n(k)$, determined up to a non-zero scalar, such that

$$\alpha(g)^{-t} = \lambda(g)B\alpha(g)B^{-1}, \tag{3.2}$$

for all $g \in G$. Applying the transpose inverse to both sides, we get

$$\alpha(g) = \lambda(g)^{-1}\lambda(g)B^{-t}B\alpha(g)B^{-1}B^t = (B^{-t}B)\alpha(g)(B^{-t}B)^{-1}.$$

As α is irreducible, Schur's Lemma implies that $B^t = \zeta B$, for some $\zeta \in k$. Then, transposing both sides of this equation, we get $B = \zeta^2 B$. So $\zeta = \pm 1_k$. Clearly, B is symmetric if $\zeta = +1$, or alternating if $\zeta = -1$.

Now, (3.2) can be rewritten as

$$\alpha(g)^{-t}B\alpha(g)^{-1} = \lambda(g)B,$$

for all $g \in G$. So kB is a G-invariant subspace of $S^* \otimes_k S^*$ which

is isomorphic to the 1-dimensional kG-module λ.

As $\mathrm{char}(k) \neq 2$, there is a kG-isomorphism

$$S^* \otimes_k S^* \simeq \mathrm{Sym}(S) \oplus \mathrm{Alt}(S),$$

where $\mathrm{Sym}(S)$ is the space of symmetric bilinear forms on S and $\mathrm{Alt}(S)$ is the space of alternating bilinear forms on S. Now,

$$\overline{\chi}^2 = \overline{\chi}_s + \overline{\chi}_a,$$

where χ_s is the symmetric part of χ^2 and χ_a is the alternating part of χ^2. Besides, the restrictions of $\overline{\chi}_s$ and $\overline{\chi}_a$ to the p-regular elements of G give the Brauer characters of $\mathrm{Sym}(S)$ and $\mathrm{Alt}(S)$, respectively. Thus,

$$\zeta = \langle \mu, \overline{\chi}_s - \overline{\chi}_a \rangle = \frac{1}{|G|} \sum_{g \in G} \mu(g)\chi(g^2),$$

which completes the proof. □

Now, let us return to our block B with a cyclic normal defect group D, inertial index e, and irreducible module S. Also, we have that $S^* \simeq \lambda S$, where λ is the linear k-representation determined by the action of G on the elements of order p in D. Since λS is the counter-clockwise successor of S in $\sigma(\mathbf{B})$ there is a non-split short exact sequence of $\mathbf{B}$-modules

$$0 \to \lambda S \to M \to S \to 0,$$

where M is uniserial with composition length 2, socle λS and head S. Clearly, M is self-dual, as $\lambda S \simeq S^*$.

Theorem 3.14 *With the notation above, the self-dual indecomposable* $\mathbf{B}$*-module* $M = \begin{smallmatrix} S \\ \lambda S \end{smallmatrix}$ *has orthogonal type if* $\epsilon_\mu(\chi) = -1$*, or symplectic type if* $\epsilon_\mu(\chi) = +1$.

Proof — Let $\alpha : G \to \mathrm{GL}_n(k)$ be a matrix representation corresponding to S. Then corresponding to M, there is an indecom-

posable matrix representation $X : G \to GL_{2n}(k)$ which has block matrix form

$$X(g) = \begin{bmatrix} \lambda(g)\alpha(g) & \beta(g) \\ 0 & \alpha(g) \end{bmatrix},$$

for all $g \in G$. Here, $\beta(g)$ is an $n \times n$-matrix with entries in k, for each $g \in G$.

Now, D is a normal p-subgroup of G and S and λ are irreducible kG-modules. Let d be a generator of the group D. Then,

$$\alpha(d) = I \quad \text{and} \quad \lambda(d) = 1_k\,.$$

On the other hand, $D \not\leqslant \ker(M)$, as M is indecomposable. Therefore,

$$X(d) = \begin{bmatrix} I & \beta(d) \\ 0 & I \end{bmatrix},$$

where $\beta(d) \neq 0$.

Notice that

$$X(d^m) = \begin{bmatrix} I & m\beta(d) \\ 0 & I \end{bmatrix},$$

for all $m \in \mathbb{Z}$. In particular, $\langle d^p \rangle \leqslant \ker(M)$. Thus, recalling that $\lambda(g)$ is defined modulo p by the equation $gug^{-1} = u^{\lambda(g)}$,

$$X(g)X(d) = X(d)^{\lambda(g)}X(g),$$

for all $g \in G$. This equality implies in turn that

$$\lambda(g)\alpha(g)\beta(d) = \beta(d)\lambda(g)\alpha(g),$$

for all $g \in G$, As α is irreducible and $\lambda(g) \in k^\times$, Schur's Lemma gives $\beta(d) = \sigma I$, for some $\sigma \in k^\times$.

Now, $M^* \simeq M$ as kG-modules. Hence, there is a matrix E such that $X(g)^{-t}E = EX(g)$, for all $g \in G$. We may also assume

that $E^t = \epsilon E$, where $\epsilon = \pm 1$. Writing $E = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$, and set

$$\gamma(g) := -\frac{1}{\lambda(g)}\alpha(g)^{-1}\beta(g)\alpha(g)^{-1},$$

for all $g \in G$. Then, the equality

$$\begin{bmatrix} \frac{1}{\lambda(g)}\alpha(g)^{-t} & 0 \\ \gamma(g)^t & \alpha(g)^{-t} \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} \lambda(g)\alpha(g) & \beta(g) \\ 0 & \alpha(g) \end{bmatrix} \quad (3.3)$$

is satisfied. First consider the case $g = d$. Then,

$$\begin{bmatrix} I & 0 \\ -\sigma I & I \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} I & \sigma I \\ 0 & I \end{bmatrix}.$$

In particular, $B = \sigma A + B$ and $-\sigma B + D = \sigma C + D$. The first equation gives $A = 0$, and the second gives $C = -B$. Putting this back into (3.3), we get

$$\frac{1}{\lambda(g)}\alpha(g)^{-t}B = B\alpha(g),$$

for all $g \in G$. This rearranges to (3.2). It then follows from Lemma 3.13 that $B^t = \epsilon_\mu(\chi)B$, where χ and μ are ordinary characters of G which lift the Brauer characters of S and λ, respectively, and $\epsilon_\mu(\chi) = \langle \lambda, \chi^{(2)} \rangle$ is defined by (3.1). Finally, as $C = -B$, we have

$$\begin{bmatrix} 0 & \epsilon B \\ -\epsilon B & \epsilon D \end{bmatrix} = \epsilon E = E^t = \begin{bmatrix} 0 & -\epsilon_\mu(\chi)B \\ \epsilon_\mu(\chi)B & D^t \end{bmatrix}.$$

Hence, $\epsilon = -\epsilon_\mu(\chi)$ and $D^t = \epsilon D$. We conclude that M has orthogonal or symplectic type, as $\epsilon_\mu(\chi) = -1$ or $+1$, respectively. □

Example 3.15 Consider $G = \mathrm{SmallGroup}(120, 7)$, in GAP nota-

tion. This is isomorphic to $C_{15} : C_8$, where a generator of the C_8 squares a generator of the C_{15}. Then, G has a 5-block

$$\mathbf{B} = \{X_{11}, X_{12}, X_{15}, X_{16}\}$$

with cyclic defect group C_5 and $e = 2$. There are two irreducible **B**-modules, S and S^*, say. We assume that the Brauer character of S is the restriction of X_{11} to the 5-regular elements of G and the Brauer character of S^* is the restriction of X_{12} to the 5-regular elements of G. The characters $X_{16} = \overline{X}_{15}$ are exceptional. We may take $\lambda = X_3$ as the linear character. Then we find that

$$\langle X_3, X_{11}^{(2)} \rangle = +1 \qquad \text{and} \qquad \langle X_3, X_{12}^{(2)} \rangle = -1.$$

So one of the self-dual indecomposable modules S/S^* in **B** has symplectic type while the other S^*/S has orthogonal type.

We note that in a general example of this type with e even, we have a linear character λ and an irreducible character χ such that $\overline{\chi} = \lambda\chi$. Also $\lambda^e\chi = \chi$. Hence, we will have to compute $\langle \lambda, \chi^{(2)} \rangle$ and $\langle \lambda, \lambda^e\chi^{(2)} \rangle$. These inner-products can be different, in spite of the fact that $(\lambda^e\chi)^2 = \chi^2$.

Example 3.16 Consider $G = C_5 : C_4$, where a generator of the C_4 inverts a generator of the C_5. Then G has a 5-block with cyclic defect group C_5 and $e = 2$. Again, **B** has no self-dual irreducible modules. But, now, its two exceptional characters are real, with Frobenius–Schur indicator -1. So immediately all self-dual indecomposable **B**-modules have symplectic type.

We can also work out the type, using the technique of this note. Let S and S^* be the irreducible **B**-modules, with corresponding lifted ordinary characters χ and $\overline{\chi}$. Now, λ is a real linear character of G. We find that

$$\langle \lambda, \chi^{(2)} \rangle = \langle \lambda, \overline{\chi}^{(2)} \rangle = +1.$$

Hence, both self-dual indecomposable modules S/S^* and S^*/S have symplectic type.

4 Self-dual modules: the general case

We now turn to the description of the self-dual indecomposable modules and their type for the general case of a real p-block $\mathbf{B}$ which has a cyclic defect group D of order $p^a \geqslant p \geqslant 3$, inertial index e and exceptional multiplicity m.

If $e = 1$, then the self-dual modules and their type are described as in Section 3. Therefore, we may assume $e \geqslant 2$. Moreover, throughout this section, we adopt the following conventions. We denote by $\mathbf{B}_1$ the Brauer correspondent of $\mathbf{B}$, by f the Green correspondence from $\mathbf{B}$ to $\mathbf{B}_1$, and by g the Green correspondence from $\mathbf{B}_1$ to $\mathbf{B}$. The irreducible $\mathbf{B}$-modules are labelled $E_0, \ldots, E_{e-1}$. In this section, the irreducible $\mathbf{B}_1$-modules are labelled $E_0(\mathbf{B}_1), \ldots, E_{e-1}(\mathbf{B}_1)$ and correspond to the edges of $\sigma(\mathbf{B}_1)$ in counter-clockwise order around the central exceptional vertex as in Section 3.

Notation 4.1 There is no general pattern for the shape of the Brauer tree $\sigma(\mathbf{B})$. However, we can choose our notation so that the edges split into three families as follows:

(1) b edges $\{E_0, \ldots, E_{b-1}\}$ labelling the real stem with $0 \leqslant b \leqslant e$ (clearly b is such that $e - b$ is even);

(2) $(e-b)/2$ edges $\{E_b, \ldots, E_{b-1+(e-b)/2}\}$ lying above the real stem in the planar embedding of $\sigma(\mathbf{B})$;

(3) $(e-b)/2$ edges $\{E_b^*, \ldots, E_{b-1+(e-b)/2}^*\}$ lying below the real stem in the planar embedding of $\sigma(\mathbf{B})$.

Moreover, provided $m \geqslant 2$, we let κ denote the number edges of $\sigma(\mathbf{B})$ which are not on the real stem and whose shortest path

to the real stem connects them to a node which is distinct from the exceptional node. Then, $e - b - \kappa$ is the number of edges of $\sigma(\mathbf{B})$ which are not on the real stem and whose shortest path to the real stem connects them to the exceptional node.

Now, recall that there is a bijection between the irreducible modules and the PIMs of $\mathbf{B}$ given by the taking of projective covers. By this and formula (2.3), a PIM of $\mathbf{B}$ is self-dual if and only if it is the projective cover of a self-dual irreducible module. This means that the total number of isomorphism classes of self-dual indecomposable $\mathbf{B}$-modules somehow depends on the shape of the Brauer tree $\mathbf{B}$, and more precisely on the length of the real stem. However, the number of isomorphism classes of non-projective self-dual indecomposable $\mathbf{B}$-modules depends only on $|D|$, namely by Corollary 3.3 there are exactly $|D| - 1$ of them.

Let us note that, with this information, it is easy to produce a list of self-dual $\mathbf{B}$-modules and prove that they account for all the self-dual $\mathbf{B}$-modules using a counting argument. The precise classification is given by the following theorem and gives us Theorem 1.1 of the introduction.

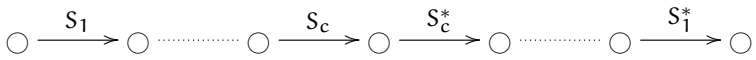
Theorem 4.2 *Let p be a prime number, $p \neq 2$, and $\mathbf{B}$ be a real p-block which has a non-trivial cyclic defect group D, inertial index $e \geqslant 2$, exceptional multiplicity m, and Brauer tree $\sigma(\mathbf{B})$. Then, up to isomorphism, the self-dual indecomposable $\mathbf{B}$-modules are as listed below.*

(a) *For $m \geqslant 1$, the b irreducible $\mathbf{B}$-modules labelling the edges of the real stem of $\sigma(\mathbf{B})$ are self-dual, where possibly $0 \leqslant b \leqslant e$.*

(b) *For $m \geqslant 1$, the b projective indecomposable $\mathbf{B}$-modules of $\mathbf{B}$ which are the projective covers of the b irreducible modules labelling the real stem of $\sigma(\mathbf{B})$ are self-dual.*

(c) *If $m = 1$, then there are precisely $e - b$ isomorphism classes of non-projective non-irreducible self-dual indecomposable $\mathbf{B}$-mod-*

ules, each parametrised by a path of shape



with direction $(1,-1)$*, multiplicity* $\mu = 0$*, and where, moreover, either*

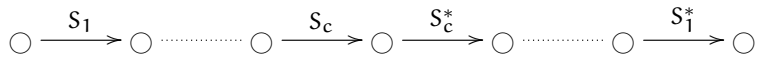
$$S_1, \dots, S_c \in \left\{E_b, \dots, E_{b-1+(e-b)/2}\right\}$$

or

$$S_1, \dots, S_c \in \left\{E_b^*, \dots, E_{b-1+(e-b)/2}^*\right\}.$$

(d) *If* $m \geqslant 2$*, then the pairwise distinct isomorphism classes of all non-projective non-irreducible indecomposable* **B***-modules parametrized by the following paths of even length are self-dual*:

(i) *the* κ *paths of shape*



with direction $(1,-1)$*, multiplicity* $\mu = 0$*, and where, moreover, either*

$$S_1, \dots, S_c \in \left\{E_b, \dots, E_{b-1+(e-b)/2}\right\}$$

or

$$S_1, \dots, S_c \in \left\{E_b^*, \dots, E_{b-1+(e-b)/2}^*\right\};$$

(ii) *the* $e - b - \kappa$ *paths of shape*



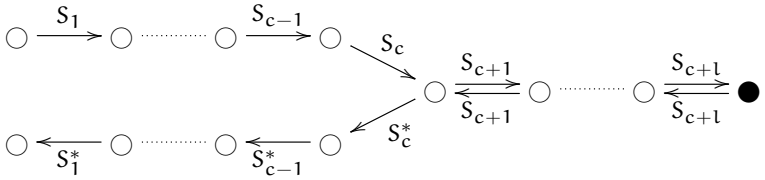
with direction $(1,-1)$*, multiplicity* μ *such that* $1 \leqslant \mu \leqslant m$*, and where, moreover, either*

$$S_1, \dots, S_c \in \left\{E_b, \dots, E_{b-1+(e-b)/2}\right\}$$

or

$$S_1, \dots, S_c \in \left\{E_b^*, \dots, E_{b-1+(e-b)/2}^*\right\};$$

(iii) *the* κ *paths of shape*



with direction $(1,-1)$, *multiplicity* $2 \leqslant \mu \leqslant m$, $l \geqslant 1$, *and where, moreover, either*

$$S_1, \dots, S_c \in \left\{E_b, \dots, E_{b-1+(e-b)/2}\right\}$$

or

$$S_1, \dots, S_c \in \left\{E_b^*, \dots, E_{b-1+(e-b)/2}^*\right\},$$

and $S_{c+1}, \dots, S_{c+l} \in \{E_0, \dots, E_{b-1}\}$;

(iv) *the* b *paths of shape*



with direction $(1,-1)$, *multiplicity* $2 \leqslant \mu \leqslant m$, *and*

$$S_1, \dots, S_c \in \{E_0, \dots, E_{b-1}\}.$$

Proof — Let us initially observe that assertions (a) and (b) are straightforward. We also notice that all the paths given in (c) and (d) give rise to pairwise non-isomorphic self-dual modules by the description of the composition factors of the associated modules in Notation A.1 and equation (2.3) for the socle layers of the dual module. Now, by Corollary 3.3, there are precisely $|D| - 1 = e$ isomorphism classes of non-projective indecomposable self-dual **B**-modules. Therefore, it only remains

to verify that the numbers of modules described in (a) and (c) if $m = 1$, respectively in (a) and (d) if $m \geqslant 2$, add up to $|D| - 1$.

First, assume that $m = 1$. If $b = e$, then there is nothing to do. Indeed, by (a), we have already $|D| - 1 = e$ pairwise non-isomorphic non-projective indecomposable $\mathbf{B}$-modules, namely the irreducible modules $E_0, \dots, E_{e-1}$. If $1 \leqslant b < e$, then there exists $e - b$ paths as given in (c), starting at each edge not on the real stem. Adding up these modules with the e irreducible modules from (a), we have already

$$(e - b) + b = e = |D| - 1$$

pairwise non-isomorphic self-dual indecomposable modules, proving the assertion (c).

Next, assume that $m \geqslant 2$. Hence, there are κ isomorphism classes of modules of type (i), $(e - b - \kappa)m$ of type (ii), $\kappa(m-1)$ of type (iii), $b(m-1)$ of type (iv). Thus, altogether (a) and (d) provide us with

$$b + \kappa + (e - b - \kappa)m + \kappa(m-1) + b(m-1) = em = |D| - 1$$

isomorphism classes of self-dual indecomposable $\mathbf{B}$-modules. Therefore, assertion (d) and the claim of the theorem follow. □

Now, we explain how to describe the type of the self-dual modules listed in the previous Theorem 4.2. It is clear that the type of a self-dual indecomposable $\mathbf{B}$-module is not an invariant of the Morita equivalence class of $\mathbf{B}$. In other words, the data encoded in the Brauer tree is not sufficient to determine the type. However, as in the uniserial case, we can always compare self-dual indecomposables with self-dual hooks of $\mathbf{B}$. In order to achieve this, we use concepts and results from [2] and [8]. First, it is necessary to define the side of the tube

$$\Gamma_s(\mathbf{B}) = (\mathbb{Z}/e\mathbb{Z})A_{|D|-1}$$

which we consider as *level* 1. This is unfortunately technical. We

explain, however, how it works in the next remark in details.

Remark 4.3

(1) The hooks of **B** are all liftable modules and the ordinary characters afforded by their lifts are easy to describe. More precisely, if E is an irreducible **B**-module labelling the edge

$$\cdots \underset{\chi_a}{\bigcirc} \overset{E}{\text{———}} \underset{\chi_b}{\bigcirc} \cdots$$

of $\sigma(\mathbf{B})$, then its projective cover $P(E)$ is

$$P(E) = \begin{array}{|c|}\hline E \\ Q_a \oplus Q_b \\ E \\ \hline \end{array}.$$

with $\operatorname{rad}(P(E))/\operatorname{soc}(P(E)) = Q_a \oplus Q_b$ for two uniserial (possibly zero) **B**-modules Q_a and Q_b. The hooks of **B** are defined to be the uniserial quotients

$$H_a := \begin{array}{|c|}\hline E \\ Q_a \\ \hline \end{array} \qquad \text{and} \qquad H_b := \begin{array}{|c|}\hline E \\ Q_b \\ \hline \end{array}.$$

The projective indecomposable character afforded by $P(E)$ is

$$\Phi_{S_j} = \chi_a + \chi_b,$$

and as $e > 1$, counting constituents, it easily follows from the decomposition matrix of **B** that any lift of H_a affords the character χ_a and any lift of H_b affords the character χ_b. We refer, for example, to [6] and [10] for proofs of these results.

(2) Let u be a generator of the subgroup D_1 of D of order p. Since projective characters vanish at p-elements, we have that $\chi_a(u) = -\chi_b(u)$. Moreover, these character values are integers. Hence, following [8, Section 4.2.], for $c \in \{a, b\}$ we say that the hook H_c is a *positive hook* if $\chi_c(u) > 0$, respectively a *negative hook* if $\chi_c(u) < 0$.

By [8, Corollary 4.3], we have that a hook of $\mathbf{B}$ is positive if its Green correspondent in $\mathbf{B}_1$ is irreducible, and it is negative if its Green correspondent in $\mathbf{B}_1$ has composition length $|D|-1$. In other words, one end Ω^2-orbit of $\Gamma_s(\mathbf{B})$ consists of the positive hooks and the other end Ω^2-orbit of $\Gamma_s(\mathbf{B})$ consists of the negative hooks.

(3) For $w \in \mathbb{Z}$, write $\overline{w} := w + e\mathbb{Z}$ for the residue class of w in $\mathbb{Z}/e\mathbb{Z}$. We say that an indecomposable $\mathbf{B}$-module Z is located at position $(\overline{v}, \ell)$ in $\Gamma_S(\mathbf{B}) \simeq (\mathbb{Z}/e\mathbb{Z})A_{|D|-1}$ if the Green correspondent $f(Z)$ of Z is the unique uniserial $\mathbf{B}_1$-module with composition length ℓ and socle $E_w(\mathbf{B}_1)$ with $0 \leqslant w \leqslant e-1$ and $\overline{w} = \overline{v}$ in $\mathbb{Z}/e\mathbb{Z}$.

(4) We have that each non-projective indecomposable $\mathbf{B}$-module M defines a uniquely determined positive hook H^+_M of $\mathbf{B}$ as follows. Assume we consider the positive hooks of $\mathbf{B}$ constitute level 1 of $\Gamma_s(\mathbf{B}) \simeq (\mathbb{Z}/e\mathbb{Z})A_{|D|-1}$ and M is located at position $(\overline{v}, \ell)$. Then, H^+_M is defined to be the module at position $(\overline{v}, 1)$. So, H^+_M lies at the end of a shortest path in $\Gamma_s(\mathbf{B})$ from M to the rim consisting of the positive hooks. Still following [8, Section 4.2.] we define the *positive distance* of M to the rim, written

$$d^+(M, H^+_M),$$

to be the length of the shortest path in $\Gamma_s(\mathbf{B})$ between M and H^+_M. Furthermore, we let $d^-(M, H^+_M)$ to be the length of the shortest path in $\Gamma_s(\mathbf{B})$ between M and $\Omega^1(H^+_M)$. We have that

$$d^+(M, H^+_M) + d^-(M, H^+_M) = |D| - 2.$$

(5) The main results of [2] provide us with closed formulae to compute the distances $d^+(M, H^+_M)$ and $d^-(M, H^+_M)$ from M to the rim of $\Gamma_s(\mathbf{B})$. These formulae are based on the description of the modules by their path, direction and mul-

tiplicity (if not irreducible). They are very technical and involve a large number of further parameters. We do not repeat them here, but refer the reader directly to Theorem 3.3 and Theorem 3.5 in [2].

Theorem 4.4 *Let* p *be an odd prime number. Let* $\mathbf{B}$ *be a real* p*-block which has a non-trivial cyclic defect group* D*, inertial index* $e \geqslant 2$*, exceptional multiplicity* m*, and Brauer tree* $\sigma(\mathbf{B})$*. Let* $\mathbf{B}_1$ *denote the Brauer correspondent of* $\mathbf{B}$ *in* $N_G(D_1)$*. Let* M *be a non-projective self-dual indecomposable* $\mathbf{B}$*-module and assume the hook* H^+_M *as well as* $d^+(M, H^+_M)$ *have been determined using* Theorems 3.3 *and* 3.5 *in* [2]*. Then the following assertions hold*:

(a) *Assume that* e *is even and* $\mathbf{B}_1$ *has two pairwise non-isomorphic self-dual irreducible modules. Then, there exists an integer* i*, with* $0 \leqslant i < (|D|-1)/2$*, such that*

$$d^+(M, H^+_M) =: 2i.$$

In addition, the type of M *is equal to the type of the self-dual hook* $\Omega^{-2i}(H^+_M)$*. If* m *is odd, then all self-dual indecomposable* $\mathbf{B}$*-modules have the same type.*

(b) *Assume that* e *is even and* $\mathbf{B}_1$ *has no self-dual irreducible modules. Then there exists an integer* i*, with* $0 \leqslant j < (|D|-1)/2$ *such that*

$$d^-(M, H^+_M) =: 2j$$

and, moreover, the type of M *is equal to the type of the self-dual hook* $\Omega^{2j+1}(H^+_M)$*.*

(c) *Assume that* e *is odd. If* $E_0(\mathbf{B}_1)$ *denotes the unique self-dual irreducible* $\mathbf{B}_1$*-module, then the following hold*:

(i) *if* $d^+(M, H^+_M)$ *is even, then the type of* M *is equal to the type of the self-dual hook* $g(E_0(\mathbf{B}_1))$*;*

(ii) *if* $d^+(M, H^+_M)$ *is odd, then the type of* M *is equal to the type of the self-dual hook* $\Omega^e(g(E_0(\mathbf{B}_1)))$*.*

Proof — By Lemma 3.1 Green correspondence between $\mathbf{B}$ and $\mathbf{B}_1$ preserves the type of the self-dual indecomposable modules. Thus, M and $f(M)$ have the same type, and so do H^+_M and $f(H^+_M)$. Moreover, in $\mathbf{B}_1$ we have

$$f(H^+_M) \simeq H^+_{f(M)} \simeq \mathrm{soc}(f(M))$$

and

$$d^+(M, H^+_M) = d^+\big(f(M), H^+_{f(M)}\big)$$

is the composition length of $f(M)$ minus one. In addition, the Green correspondence commutes with the Heller operator, so it suffices to prove the theorem for the Green correspondents in $\mathbf{B}_1$ of the modules involved.

(a) With the notation of Proposition 3.7, either

$$f(M) = [i, 2i+1]\,,$$

with $0 \leqslant i \leqslant mh-1$, or

$$f(M) = [h+i, 2i+1]\,,$$

with $0 \leqslant i \leqslant mh-1$. In both cases, the composition length is $2i+1$. Moreover, in the former case the type of $f(M)$ is the type of

$$E_0(\mathbf{B}_1) \simeq \Omega^{-2i}(\mathrm{soc}(f(M))) = \Omega^{-2i}(f(H^+_M))\,,$$

and in the latter case the type of $f(M)$ is the type of

$$E_h(\mathbf{B}_1) = \Omega^{-2i}(\mathrm{soc}(f(M))) \simeq \Omega^{-2i}(f(H^+_M))\,.$$

The second claim follows directly from Corollary 3.8.

(b) With the notation of Proposition 3.4, either

$$f(M) = [i, 2i+2]\,,$$

with $0 \leqslant i \leqslant mh-1$, or

$$f(M) = [h+i, 2i+2]\,,$$

with $0 \leqslant i \leqslant mh-1$. In both cases, the composition length is $2i+2$. So, $d^-(f(M), H_M^+) = 2j$, for $j := (|D|-3)/2-i$, and in the former case the type of $f(M)$ is the type of the self-dual hook

$$[((mh)^*, me)] \simeq \Omega^{2j+1}(\mathrm{soc}(f(M))) \simeq \Omega^{2j+1}(f(H_M^+))\,,$$

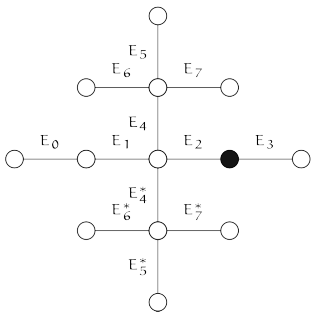
and in the latter case the type of $f(M)$ is the type of the self-dual hook

$$[((mh+h)^*, me)] \simeq \Omega^{2j}(\Omega(\mathrm{soc}(f(M)))) \simeq \Omega^{2j+1}(f(H_M^+))\,.$$

(c) Assertions (i) and (ii) are immediate from the above ones and Proposition 3.10. □

The following is an example a real block such that $e = 12$ and $m = 9$.

Example 4.5 Consider the principal 109-block $\mathbf{B}_0$ of the Ree group ${}^2F_4(q^2)$ with $q^2 = 2^{2u+1}$ for $u := 1$. Its planar embedded Brauer tree was determined in [7, Theorem 4.7]. A defect group D is cyclic of order 109, the inertial index is $e = 12$, the exceptional multiplicity is $m = (|D|-1)/e = 9$ and the Brauer tree $\sigma(\mathbf{B}_0)$ is of the following form:

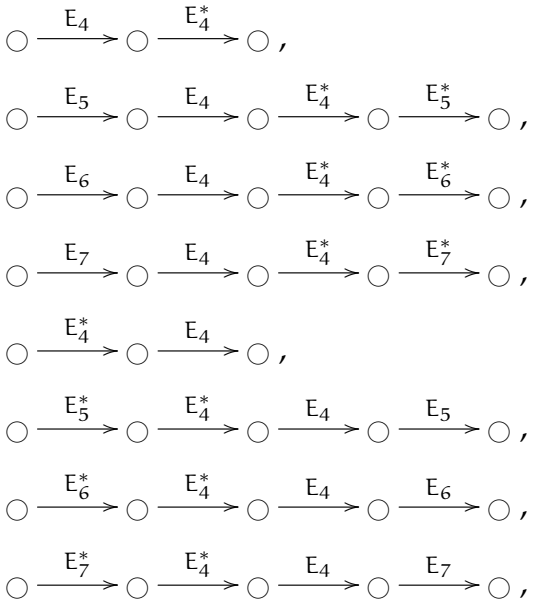


In particular, the real stem consists of 4 edges, which we label as $E_0, \dots, E_3$, i.e. $b = 4$. Note that E_0 is the trivial module.

By Corollary 3.3, there are $|D| - 1 = 108$ isomorphism classes of non-projective self-dual indecomposable $\mathbf{B}_0$-modules, which, by Theorem 4.2, are as given below:

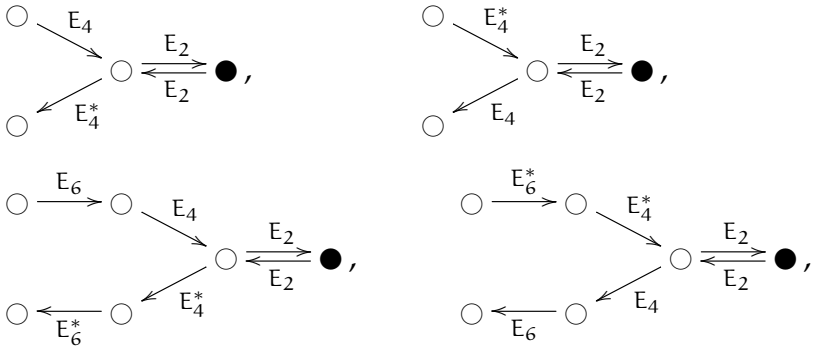
(i) the $b = 4$ simple modules E_0, E_1, E_2 and E_3;

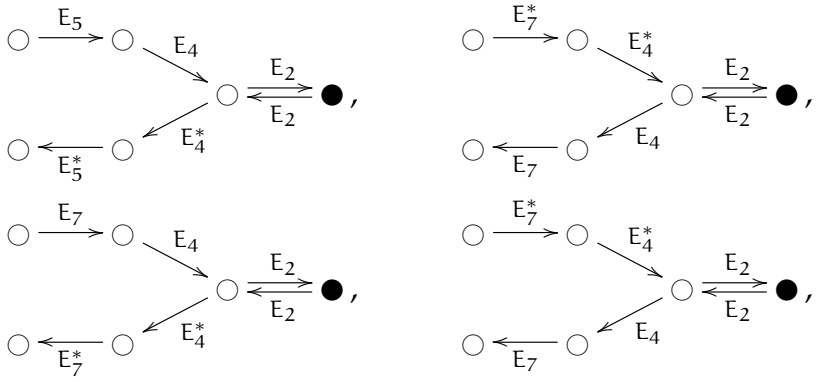
(ii) the modules given by the $\kappa = 8$ paths



all of which with direction $(1, -1)$ and multiplicity $\mu = 0$;

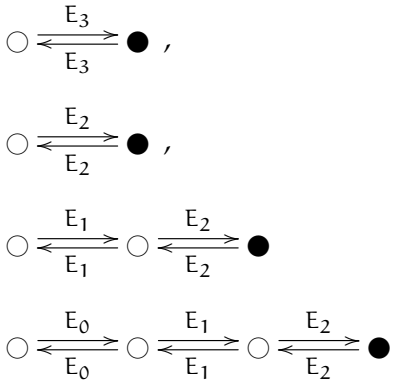
(iii) the modules given by the $\kappa = 8$ paths





with direction $(1,-1)$ and multiplicity $2 \leqslant \mu \leqslant 9$;

(iv) the modules given by the $b = 4$ paths

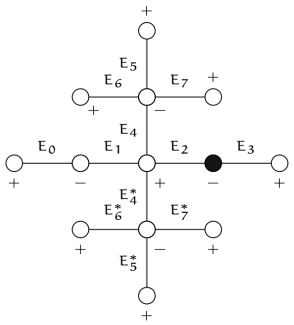


with direction $(1,-1)$ and multiplicity $2 \leqslant \mu \leqslant m = 9$.

We note that (i) yields 4 isomorphism classes of self-dual modules, (ii) yields 8 isomorphism classes of self-dual modules, (iii) yields 8×8 isomorphism classes of self-dual modules and (iv) yields 4×8 isomorphism classes of self-dual modules. Hence, adding up, we see that we have described the 108 required isomorphism classes of non-projective self-dual indecomposable $\mathbf{B}_0$-modules.

Next we describe the positive hooks, according to the definition we gave in Remark 4.3 (2). As the trivial character is the character afforded by the trivial module, it is positive on any

generator u of D_1, so we obtain positive and negative signs for the values $\chi(u)$ for $\chi \in \mathrm{Irr}(\mathbf{B}_0)$ as follows:



It follows, from Remark 4.3, that the positive hooks are the following 12 uniserial modules: E_0, E_5, E_5^*, E_6, E_6^*, E_7, E_7^*, E_3,

$$\bigcirc \xrightarrow{E_1} \bigcirc \xrightarrow{E_4} \bigcirc$$

with direction $(1,-1)$ and multiplicity $\mu = 0$,

$$\bigcirc \xrightarrow{E_4} \bigcirc \xrightarrow{E_2} \bigcirc$$

with direction $(1,-1)$ and multiplicity $\mu = 0$,

$$\bigcirc \xrightarrow{E_2} \bigcirc \xrightarrow{E_4^*} \bigcirc$$

with direction $(1,-1)$ and multiplicity $\mu = 0$, and

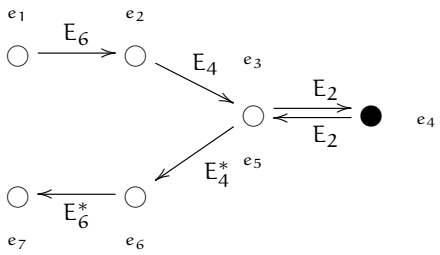
$$\bigcirc \xrightarrow{E_4^*} \bigcirc \xrightarrow{E_1} \bigcirc$$

with direction $(1,-1)$ and multiplicity $\mu = 0$.

Let us note that the Brauer correspondent of $\mathbf{B}_0$ is the principal block of $N_G(D_1)$. Hence, in this case, we actually know, from Theorem 4.4 (a), that all self-dual modules have the same type, namely the type of the trivial module.

However, we illustrate the procedure of Theorem 4.4 to deter-

mine the type of the module M given by the path



with direction $(1,-1)$ and multiplicity $\mu = 6$ assuming we do not know, a priori, that the type is the type of the trivial module. Notice that we have named the vertices e_1 to e_7, as the path is of length 6. We apply [2, Theorem 3.5] in order to obtain the position of M in $\Gamma_s(\mathbf{B}_0)$. More precisely, in order to use the formula of [2, Theorem 3.5] for $d^+(M, H_M^+)$, we need to determine a series of local parameters defined in [2]. These are:

$$\alpha = 1,\ s = 6, v_a = e_6 = v_1,\ v_z = e_1 = v_{n+1},$$

$$S_a = E_6^* = X_1,\ S_z = E_6 = X_n, X_{i_1} = E_6^*, X_{i_2} = E_4^*,$$

$$X_{i_3} = E_2,\ X_{i_4} = E_2,\ X_{i_5} = E_4,\ X_{i_6} = E_6,$$

$$n = 33,\ k_0 = 4,\ \eta = \mu - 2 = 6 - 2 = 4$$

and, in addition, the distance of M is calculated to the positive hook $H_M^+ = E_6$. This yields

$$d^+(M, H_M^+) = \frac{n-1}{2} + \eta \cdot e = \frac{33-1}{2} + 4 \cdot 12 = 16 + 48 = 64\,.$$

Hence, the integer i of Theorem 4.4 (a) is $i = 32$ and the type of M is the type of the self-dual hook

$$\Omega^{-64}(H_M^+) \simeq \Omega^{-4}(H_M^+) \simeq E_0 \simeq k$$

where the last-but-one isomorphism follows from the shape of the Brauer tree.

Acknowledgements

The idea for this paper arose during the conference on Representation Theory which took place at MFO Oberwolfach in April 2023. Much of the detail was then developed during a visit of the second author to the University of Kaiserslautern–Landau (RPTU Kaiserslautern–Landau) in July 2023. We would like to thank both institutions and the DFG/SFB-TRR 195 for their support.

Appendix A. Parametrisation of the indecomposable modules

In this appendix, we shortly recall how the indecomposable modules of a block $\mathbf{B}$ with a cyclic defect group $D \simeq C_{p^a}$ with $a \geqslant 1$ and inertial index e can be described using the data given by its planar embedded Brauer tree $\sigma(\mathbf{B})$ with exceptional multiplicity m. If not otherwise stated, we keep the notation introduced in Section 1 and Section 2. In particular, we let $\{E_0, ..., E_{e-1}\}$ denote the set of all pairwise non-isomorphic irreducible $\mathbf{B}$-modules. We refer the reader to [11], and also [10] for details.

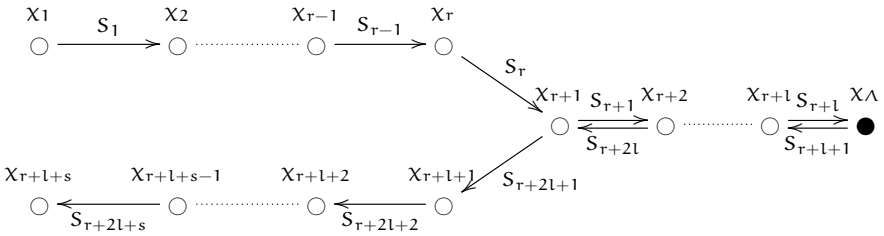
Notation A.1 Based on work of Bleher–Chinburg [2] and standard results of Janusz [11, Section 5], up to isomorphism, each non-projective non-irreducible indecomposable $\mathbf{B}$-module X can be encoded using the following three parameters.

(1) A *path* on $\sigma(\mathbf{B})$, which is, by definition, a directed connected subgraph of $\sigma(\mathbf{B})$ of one of the following two types:

(Type I)



with $t \geqslant 1$ and $S_1, \ldots, S_t \in \{E_0, \ldots, E_{e-1}\}$ are pairwise distinct and not adjacent to the exceptional vertex, or, if $m \geqslant 2$, (Type II)



where $l, r, s \geqslant 0$, $t := r + 2l + s \geqslant 2$, possibly $\chi_{r+1} = \chi_\Lambda$ (in which case $l := 0$), $S_1, \ldots, S_{r+l}, S, \ldots, S_t \in \{E_0, \ldots, E_{e-1}\}$ are pairwise distinct,

$$S_{r+l+i} \simeq S_{r+l-(i-1)},$$

for each $1 \leqslant i \leqslant l$ and S_{r+l}, is adjacent to the exceptional vertex.

Let us observe that, these paths may be seen as an ordered sequence $(S_1, \ldots, S_t)$ of edges of $\sigma(\mathbf{B})$, called *top-socle sequence* of X, and where S_i, S_{i+1} have a common vertex, for every $1 \leqslant i \leqslant t$, the odd-labelled edges are constituents of the head of X and the even-labelled edges are constituents of the socle of X, or conversely.

(2) A *direction* $\varepsilon = (\varepsilon_1, \varepsilon_t)$, where, for $i \in \{1, t\}$, we set $\varepsilon_i = 1$ if S_i is in the head of X and $\varepsilon_i = -1$ if S_i is in the socle of X.

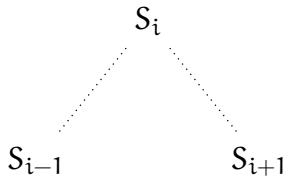
(3) A *multiplicity* μ. If $m = 1$, then $\mu := 0$. If $m > 1$, then μ corresponds to the number of times that an irreducible module S_j adjacent to the exceptional vertex occurs as a composition factor of X (which is independent of the choice of S_j).

The structure of an indecomposable $\mathbf{B}$-module X with top-socle sequence $(S_1, \ldots, S_t)$, direction ε and multiplicity μ can then be understood as follows. First, write

$$\Delta := \{1 \leqslant i \leqslant t \mid S_i \in \mathrm{hd}(X)\}.$$

Then, for each $i \in \Delta$, there is a submodule X_i of X with unique head composition factor S_i and with socle composition factors consisting of the edges of $\sigma(\mathbf{B})$ adjacent to S_i.

$X_i =$

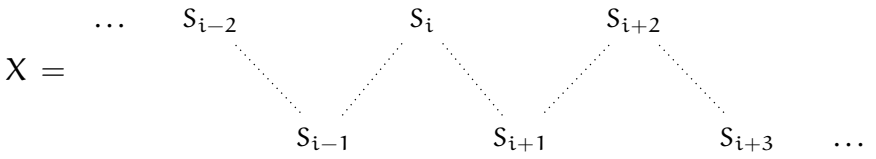


Let us note that if S_{i-1} and S_i have χ_i as common vertex and S_i and S_{i+1} have χ_{i+1} as common vertex, then the composition factors of the left leg of X_i, from bottom to top, correspond to the edges of $\sigma(\mathbf{B})$ adjacent to χ_i encountered on a clockwise walk around χ_i from S_{i-1} to S_i. The composition factors of the right leg of X_i, from top to bottom, correspond to the edges of $\sigma(\mathbf{B})$ adjacent to χ_{i+1} encountered on a counter-clockwise walk around χ_{i+1} from S_i to S_{i+1}. If the path starts with S_i, respectively ends with S_i, then X_i has no left leg, respectively no right leg. In other words, X_i is uniserial.

If the vertex between S_{i-1} and S_i, respectively between S_i and S_{i+1} is the exceptional vertex, then we walk around χ_i, respectively χ_{i+1}, several full circles in such a way that S_i occurs with multiplicity μ in the left, respectively right, leg of X_i. Finally, the indecomposable module X is obtained abstractly by amalgamating the modules isomorphic to X_i along their common socle constituents, i.e.

$$X = \sum_{i \in \Delta} X_i.$$

It can be visualised as follows:



Remark A.2

(a) When $m = 1$, even if one vertex is artificially designated to be exceptional, the above parametrization considers that there is no exceptional vertex. Thus, in this case, for simplicity we draw only paths of Type I.

(b) Warning: the set of indecomposable modules obtained by combining all possible paths, directions and multiplicities are not pairwise non-isomorphic. Even-length paths can give rise to doubles when the direction is switched. Such configurations are called *mirror images* in [2]. This is the reason why it is helpful to consider directions.

(c) In particular, when considering uniserial modules, we may always assume that the direction is $(1, -1)$. Uniserial modules with direction $(-1, 1)$ are then doubles of those with direction $(1, -1)$.

(d) A non-projective non-irreducible uniserial **B**-module can be encoded by five types of paths:

(U1) $\circ \xrightarrow{S_1} \circ \xrightarrow{S_2} \circ$ with direction $(1, -1)$ and multiplicity $\mu = 0$;

(U2) $\circ \xrightarrow{S_1} \circ \xrightarrow{S_2} \bullet$ with direction $(1, -1)$ and multiplicity $\mu = 1$;

(U3) $\bullet \xrightarrow{S_1} \circ \xrightarrow{S_2} \circ$ with direction $(1, -1)$ and multiplicity $\mu = 1$;

(U4) $\circ \xrightarrow{S_1} \bullet \xrightarrow{S_2} \circ$ with direction $(1,-1)$ and multiplicity μ such that $1 \leqslant \mu \leqslant m$; or

(U5) $\circ \underset{S_1}{\overset{S_1}{\rightleftarrows}} \bullet$ with direction $(1,-1)$ and multiplicity μ such that $2 \leqslant \mu \leqslant m$.

Here it is implicitly assumed $S_1, S_2 \in \{E_0, \dots, E_{e-1}\}$ and that paths of type (U1) can occur for an $m \geqslant 1$ arbitrary, whereas paths of types (U2), (U3), (U4), (U5) occur only when $m \geqslant 2$.

It is also easy to describe the self-dual uniserial modules using this notation.

Lemma A.3 *Let X be a non-projective and non-irreducible uniserial $\mathbf{B}$-module and assume $S_1 \in \{E_0, \dots, E_{e-1}\}$. Then, if X is self-dual, if $m \geqslant 1$, X is parametrized by the path*

$$\circ \xrightarrow{S_1} \circ \xrightarrow{S_1^*} \circ \tag{USD1}$$

with direction $(1,-1)$ and multiplicity $\mu = 0$. If $m \geqslant 2$, X is parametrized by the paths

$$\circ \xrightarrow{S_1} \bullet \xrightarrow{S_1^*} \circ \tag{USD2}$$

with direction $(1,-1)$ and multiplicity μ such that $1 \leqslant \mu \leqslant m$ or

$$\circ \underset{S_1}{\overset{S_1}{\rightleftarrows}} \bullet \tag{USD3}$$

with direction $(1,-1)$, multiplicity μ with $2 \leqslant \mu \leqslant m$ and $S_1 \simeq S_1^*$.

Proof — Initially, by Remark A.2 (c), we have that the non-irreducible uniserial $\mathbf{B}$-modules are given by paths of type (U1) to (U5). Now, if a uniserial module is self-dual, by (2.4), we obtain that $S_2 \simeq S_1^*$ for modules of type (U1), (U2), (U3) and (U4),

whereas $S_1 \simeq S_1^*$ for modules of type (U5). As the exceptional vertex is always on the real stem and duality induces a reflection with respect to the real stem, it follows, from the above, that modules of type (U2) and (U3) cannot be self-dual. The remaining modules of type (U1), (U4) and (U5) with direction and multiplicity as given in the claim are all self-dual by the description of their composition factors in Notation A.1 and equation (2.3) for the socle layers of the dual. □

REFERENCES

[1] D.J. Benson: "Representations and Cohomology I", *Cambridge University Press*, Cambridge (1991).

[2] F.M. Bleher – T. Chinburg: "Locations of modules for Brauer tree algebras", *J. Pure Appl. Algebra* 169 (2002), 109–135.

[3] E.C. Dade: "Blocks with cyclic defect groups", *Ann. of Math.* (2) 84 (1966), 20–48.

[4] W. Feit: "The Representation Theory of Finite Groups", *North-Holland*, Amsterdam 25 (1982).

[5] R. Gow – W. Willems: "A note on Green correspondence and forms", *Comm. Algebra* 23 (1995), 1239–1248.

[6] J.A. Green: "Walking around the Brauer Tree", *J. Austral. Math. Soc.* 17 (1974), 197–213.

[7] G. Hiss: "The Brauer trees of the Ree Groups", *Comm. Algebra* 19 (1991), 871–888.

[8] G. Hiss – C. Lassueur: "The classification of the trivial source modules in blocks with cyclic defect groups", *Algebr. Represent. Theory* 24 (2021), 673–698.

[9] G. Hiss – K. Lux: "Brauer Trees of Sporadic Groups", *The Clarendon Press, Oxford University Press*, New York (1989).

[10] G. Hiss – N. Naehrig: "The classification of the indecomposable liftable modules in blocks with cyclic defect groups", *Bull. Lond. Math. Soc.* 44 (2012), 974–980.

[11] G.T. Janusz: "Indecomposable modules for finite groups", *Ann. of Math.* (2) 89 (1969), 209–241.

[12] J.C. Murray: "Frobenius–Schur indicators of characters in blocks with cyclic defect", *J. Algebra* 533 (2019), 90–105.

[13] P. Webb: "A Course in Finite Group Representation Theory", *Cambridge University Press*, Cambridge (2016).

[14] W. Willems: "Duality and forms in representation theory", in Representation Theory of Finite Groups and Finite-Dimensional Algebras, *Birkhäuser*, Basel (1991).

Caroline Lassueur (*corresponding author*)
Fachbereich Mathematik
RPTU Kaiserslautern–Landau
67653 Kaiserslautern (Germany)

Institut für Algebra, Zahlentheorie und Diskrete Mathematik
Leibniz Universität Hannover
30167 Hannover (Germany)
e-mail: lassueur@mathematik.uni-kl.de;
lassueur@math.uni-hannover.de

John Murray
Department of Mathematics & Statistics
Maynooth University
Maynooth (Ireland)
e-mail: John.Murray@mu.ie



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 167–181 ISSN: 2499-1287
DOI: 10.32037/agta-2026-008

Bounded Conciseness in the Space of Marked Groups

Federico Berlai

(*Received Oct. 5, 2024; Accepted Feb. 8, 2025 — Communicated by P. Shumyatsky*)

Abstract

We prove that bounded conciseness is a closed property in the space of marked groups. As a consequence, we reformulate a conjecture of Fernández-Alcober and Shumyatsky [7] about conciseness in the class of residually finite groups.

Mathematics Subject Classification (2020): 20F10

Keywords: conciseness; word value; residual finiteness; marked group

1 Introduction

Conciseness draws its roots in the work of Philip Hall in the 50s. Given a word $w \in F(x_1, \dots, x_n)$, one says that w is *concise in a group* G if, whenever the set of w-values

$$w\{G\} = \{w(g_1, \dots, g_n) \mid g_i \in G\}$$

is finite, then the subgroup G_w generated by these finitely many values is also finite. A word is said to be *concise in a class* $\mathcal{C}$ of groups if it is concise in all groups of the class $\mathcal{C}$, and it is said

to be *concise* if it is concise in the class of all groups. Already in the 1950s, Hall raised the question of whether all words are concise. Since then many positive results have been obtained, but there are now expamples of non-concise words [9]. The similar question — but now restricted to the family of residually finite groups — is still open: that is, is every word concise in the class of residually finite groups?

Analogously, a word w is said to be *boundedly concise* in a class of groups $\mathcal{C}$ if the following holds: there exists a function

$$\delta_{\mathcal{C},w}(m) = \delta(m) \colon \mathbb{N} \to \mathbb{N}$$

such that whenever $G \in \mathcal{C}$ and $w\{G\}$ is finite, then

$$|G_w| \leqslant \delta\big(|w\{G\}|\big)$$

(and in particular the group G_w is finite). By an ultraproduct argument [6], it is known that if a word is concise in the class of all groups, then it is boundedly concise.

In this article, after recalling known facts about the space of marked groups, we prove the following result.

Theorem 1.1 *Let $\mathcal{C}$ be a class of groups, $w \in F$ a word in a finitely generated free group, and suppose that the word w is boundedly concise in $\mathcal{C}$. Then the word w is boundedly concise in the class $\mathcal{L}$ of limits of groups in $\mathcal{C}$ in the space of marked groups.*

LEF groups generalise residually finite groups, and are defined as follow. A group is said to be *locally embeddable into finite groups* (abbreviated LEF) if for all finite subsets $F \subseteq G$ there exists a finite group Q and a map $\varphi \colon G \to Q$ such that $\varphi \restriction_F$ is injective and $\varphi(f_1 f_2) = \varphi(f_1)\varphi(f_2)$, for all $f_1, f_2 \in F$. If G is residually finite, this map φ is an actual homomorphism and Q is a finite quotient of G. LEF groups are precisely the limits of finite groups in the space of marked groups.

From Theorem 1.1 we deduce the following result.

Corollary 1.2 *Let $w \in F$ be a word. The following are equivalent*:

(1) *w is boundedly concise in the class of residually finite groups;*

(2) *w is boundedly concise in the class of LEF groups;*

(3) *w is concise in the class of LEF groups.*

It is conjectured [7] that a word is concise in the class of residually finite groups if and only if it is boundedly concise in the same class. Thus, with Corollary 1.2 we can restate the conjecture as "a word is concise in the class of residually finite groups if and only if it is concise in the class of LEF groups". Possibly, the latter reformulation can be of help in proving the conjecture.

2 Space of marked groups

In this section, for the interested reader, we briefly discuss the space of marked groups, and we collect the proofs of some basic results that will be used later.

A *marked group* is a pair (G, S), where G is a group and S is a sequence of elements that generate G. If $|S| = n$ is finite, then (G, S) is called an n-marked group.

If we have an n-marked group (G, S), then there is a surjective homomorphism $\pi = \pi_{(G,S)}$ from the free group on n free generators $x_1, \dots, x_n$ to the group G defined on the generators as $\pi(x_i) := s_i$. Two n-marked groups $(G, (s_1, \dots, s_n))$ and $(G', (s'_1, \dots, s'_n))$ are isomorphic if the bijection $\varphi(s_i) := s'_i$ extends to an isomorphism of groups $\varphi\colon G \to G'$. In particular, two marked groups with given generating sets of different size are never isomorphic as marked groups, although they might be isomorphic as abstract groups.

Let $\mathcal{G}_n$ denote the set of n-marked groups, up to isomorphism of marked groups. Then $\mathcal{G}_n$ corresponds bijectively to the set of normal subgroups of the free group F_n on n free generators $\{x_1, \dots, x_n\}$. It is a compact totally disconnected ultrametric space [3].

Let $(G,S),(G',S') \in \mathcal{G}_n$ and let N, N' be the normal subgroups of $F = F_n$ such that $F/N \simeq G$ and $F/N' \simeq G'$. Let $B_F(r)$ denote the ball of radius r in F centered at the identity element with respect to the generating set $\{x_1^{\pm 1},\dots,x_n^{\pm 1}\}$. The function

$$\begin{aligned}\nu(N,N') &:= \sup\{r \in \mathbb{N} \mid N \cap B_F(r) \\ &= N' \cap B_F(r)\} \in \mathbb{N} \cup \{+\infty\}\end{aligned} \tag{2.1}$$

defines on $\mathcal{G}_n$ the ultrametric

$$d\big((G,S),(G',S')\big) := 2^{-\nu(N,N')}. \tag{2.2}$$

An n-marked group (G,S) can be viewed as an $(n+1)$-marked group by adding the trivial element e_G to S. This defines an isometric embedding of $\mathcal{G}_n$ into $\mathcal{G}_{n+1}$. Therefore, the ultrametrics given in equation (2.2) extend to an ultrametric d on $\mathcal{G} := \bigcup_{n\in\mathbb{N}} \mathcal{G}_n$. This space is called the *space of finitely generated marked groups*.

Let (G,S) be a marked group. The *Cayley graph* of (G,S) is the directed graph

$$\Gamma := \mathrm{Cay}(G,S),$$

whose vertex set is $V\Gamma = G$, and such that there is a directed edge (g,gs) whenever $g \in G$ and $s \in S \setminus \{e_G\}$. Thus, this graph is locally finite. In general, $(gs,g) \notin E\Gamma$, unless s^{-1} too belongs to S (and not just s). There is also a natural labeling of the edges in $\mathrm{Cay}(G,S)$ by the set $S \setminus \{e_G\}$: any edge (g,gs) is labeled by the letter s.

Given a marked group $(G,S) \in \mathcal{G}_n$, we can always assume that S is symmetric set by considering $(G,\widetilde{S}) \in \mathcal{G}_{2n}$, where

$$\widetilde{S} = S \cup S^{-1}.$$

When this happens, the Cayley graph $\mathrm{Cay}(G,\widetilde{S})$ can be viewed as an *undirected* labeled graph, by replacing the edges (g,gs), labeled by s, and (gs,g), labeled by s^{-1}, with the undirected

edge $\{g, gs\}$ labeled by s. Nevertheless, we will not enforce this in what follows.

Let (G, S) be a marked group. One can naturally define a norm $|-|_S \colon G \to \mathbb{N}$ in the following way:

$$|g|_S := \min\left\{l \in \mathbb{N} \mid g = s_1 \cdot \ldots \cdot s_l,\ s_i \in S \cup S^{-1},\ \forall i = 1, \ldots, l\right\}.$$

The following fact is well known. We provide a proof to make the paper more self-contained and accessible. Note that the equivalence between the first and the third condition is discussed in [3, Section 2.2].

Proposition 2.1 *Let (G, S) and $\{(G_r, S_r)\}_{r\in\mathbb{N}}$ be n-marked groups, and let N and $\{N_r\}_{r\in\mathbb{N}}$ be normal subgroups of the free group F on n generators such that $F/N \simeq G$ and $F/N_r \simeq G_r$. The following are equivalent*:

(1) *the sequence $\{(G_r, S_r)\}_{r\in\mathbb{N}}$ converges to the point (G, S) in the space $(\mathcal{G}_n, d)$;*

(2) *for all $x \in N$ (for all $y \notin N$, respectively), there exists $\bar{r}$ such that $x \in N_r$ ($y \notin N_r$, respectively) for $r \geqslant \bar{r}$;*

(3) *for all $R \in \mathbb{N}$, there exists $\bar{r}$ such that the Cayley graphs*

$$\mathrm{Cay}(G, S) \qquad \textit{and} \qquad \mathrm{Cay}(G_r, S_r)$$

have balls of radius R isomorphic as labeled directed graphs, for all $r \geqslant \bar{r}$.

Proof — Before starting with the proof, we fix some notation. Let $F = F(X)$ be the free group on n generators $X = \{x_1, \ldots, x_n\}$. Let $\pi \colon F \to G$ be the surjective homomorfism defined by

$$\pi(x_i) := s_i,$$

for all $i = 1, \ldots, n$, where $S = (s_1, \ldots, s_n)$, and the analogous surjective homomorfisms $\pi_r \colon F \to G_r$ such that $\pi_r(x_i) := s_{r,i}$, for all $i = 1, \ldots, n$, for all $r \in \mathbb{N}$, where $S_r = (s_{r,1}, \ldots, s_{r,n})$. By

construction we have that $N = \ker(\pi)$ and that $N_r = \ker(\pi_r)$. Let

$$l_i := \min\{l \in \mathbb{N} \mid s_i = wN \text{ and } |w|_X = l\},$$

for all $s_i \in S = (s_1, \dots, s_n)$, that is, l_i is the length in F (with respect the word metric defined by the generating set X) of a minimal representative of the coset s_i. Set $L := \max\{l_1, \dots, l_n\}$.

We now prove three implications. To begin, suppose that the sequence $\{(G_r, S_r)\}_{r\in\mathbb{N}}$ converges to the point $(G, S) \in \mathcal{G}_n$. In particular, for all $\varepsilon > 0$ there exists $\delta \in \mathbb{N}$ for which

$$d\big((G, S), (G_m, S_m)\big) = 2^{-\nu(N, N_m)} < \varepsilon, \qquad \forall\, m \geqslant \delta,$$

or, taking logarithms, such that

$$\nu(N, N_m) > -\log_2(\varepsilon).$$

Let $x \in N$ ($y \notin N$, respectively) be fixed. Therefore, there exists a minimal natural number $r \in \mathbb{N}$ such that $x \in B_F(r)$ ($y \notin B_F(r)$, respectively). Then, we can choose ε_0 so that

$$-\log_2(\varepsilon_0) > r.$$

Thus, with this choice of ε_0 (and its corresponding δ_0), we have that $x \in N_m$, for all $m \geqslant \delta_0$ (respectively, $y \notin N_m$). We set $\bar{r} = \delta_0$.

Now, suppose that the second condition holds, and let $R \in \mathbb{N}$ be fixed. Let us consider the finite set

$$B := B_F(2LR) \subseteq F,$$

the ball of radius $2LR$ (with respect to the word metric defined by X) centered at the identity of F. We apply condition (2) to each of the finitely many elements in this ball and, after taking maximums, we obtain a natural number $\bar{r}$ such that, for all elements $x \in B$, we have that $x \in N$ if and only if $x \in N_r$, for all $r \geqslant \bar{r}$.

Let $B_G(R)$ be the ball of radius R centered at the identity in

the Cayley graph $\mathrm{Cay}(G, S)$ and let B_r be the ball of radius R centered at the identity in the Cayley graph $\mathrm{Cay}(G_r, S_r)$. Let us define the maps $\varphi_r \colon B_G(R) \to B_r$, for all $r \geqslant \bar{r}$, in the following way: if $g \in B_G(R)$ is a vertex, then $g = wN$, for some $w \in F$. Let w be such an element of minimal length (with the choice of constants we made, we have $w \in B_F(LR)$). Define $\varphi_r(g) := wN_r$.

First, let us check that φ is a well-defined map. If we assume that $wN = w_0N$, for all $w, w_0 \in B$ of minimal length, then $w^{-1}w_0 \in N$, and moreover $w^{-1}w_0 \in B_F(2LR)$. Thus, it must be that $w^{-1}w_0 \in N_r$, for all $r \geqslant \bar{r}$, and therefore $wN_r = w_0N_r$.

The map φ_r is clearly surjective and injective. We now check that it preserves edges. Suppose that two vertices two vertices $g, gs_i \in B_G(R)$ joined by a directed edge (labeled by s_i), for some $s_i \in S$, where $g = wN$ and $s_i = x_iN$, then $\varphi_r(g) = wN_r$ and

$$\varphi_r(gs_i) = \varphi_r(wx_iN) = (wx_i)N_r = wN_r \cdot x_iN_r = wN_r \cdot s_{r,i},$$

hence $(\varphi_r(g), \varphi_r(gs_i))$ is an edge in the Cayley graph $\mathrm{Cay}(G_r, S_r)$, labeled by $s_{r,i}$. The argument is completely symmetric, because $x \in B \cap N$ if and only if $x \in B \cap N_r$. Thus, φ_r is an isomorphism of labeled directed graphs, and condition (3) is met.

To conclude, suppose that the third condition holds, and fix $\varepsilon > 0$. Given $r \in \mathbb{N}$, we have that $d\big((G, S), (G_r, S_r)\big) < \varepsilon$ if and only if $\nu(N, N_r) > -\log_2(\varepsilon)$. Notice, if the balls $B_G(R)$ and B_r are isomorphic labeled graphs, then

$$\nu(N, N_r) \geqslant LR.$$

Thus, if we consider R such that $LR > -\log_2(\varepsilon)$, then for the associated $\bar{r}$ we have that

$$d\big((G, S), (G_r, S_r)\big) = 2^{-\nu(N, N_r)} < \varepsilon, \qquad \forall\, r \geqslant \bar{r},$$

and the proof is concluded. □

3 Conciseness and bounded conciseness

For the following definition we need to introduce some notation. Suppose that we are given a word w in finitely many variables, that is an element of a finitely generated free group, say $w \in F_r$. This word defines an evaluation map

$$w : G^r \longrightarrow G,\ (g_1, \dots, g_r) \longmapsto w(g_1, \dots, g_r).$$

We denote by $w\{G\}$ the set of images of w in the group G. Notice that this set may fail to be a subgroup: for instance, the set of commutators in a group G (that is when we consider the word $w = [x, y] \in F_2$) in general is not a subgroup of G. We denote by G_w the subgroup of G generated by the set $w\{G\}$.

Definition 3.1 Let $w \in F_r$ be a word. We say that the word is *concise* in a group G if the following holds: whenever $w\{G\}$ is finite, then the group G_w is also finite. Restricting this notion to a class of groups $\mathcal{C}$, one says that w is concise in $\mathcal{C}$ if the above statement is met for all groups in the class $\mathcal{C}$.

A word w is *boundedly concise* in a class of groups $\mathcal{C}$ if the following holds: there exists a function

$$\delta_{\mathcal{C},w}(m) = \delta(m) \colon \mathbb{N} \to \mathbb{N}$$

such that whenever $G \in \mathcal{C}$ and $w\{G\}$ is finite, then

$$|G_w| \leqslant \delta\big(|w\{G\}|\big)$$

(and in particular the group G_w is finite).

Given a property of groups $\mathcal{P}$, a group G is said to be locally $\mathcal{P}$ if all finitely generated subgroups of G satisfy property $\mathcal{P}$. For instance, a group is locally finite if all its finitely generated subgroups are finite, or it is locally residually finite if all its finitely generated subgroups are residually finite.

The following result is straightforward.

Lemma 3.2 *Let $\mathcal{C}$ be a class of groups, $w \in F_r$ be a word, and suppose that w is boundedly concise in $\mathcal{C}$. Then w is boundedly concise in the class of groups that are locally $\mathcal{C}$, maintaining the same function $\delta\colon \mathbb{N} \to \mathbb{N}$.*

Thus, given a word $w \in F_r$ and a class of groups $\mathcal{C}$ in which w is (boundedly) concise, in view of Lemma 3.2 we can always assume that the class $\mathcal{C}$ is closed with respect to taking groups that are locally in $\mathcal{C}$.

It is not clear if the class of groups on which a word is concise is closed under taking subgroups. Nevertheless, the next weaker lemma will be useful when considering non-finitely generated groups.

Lemma 3.3 *Let G be a group and $w \in F_r$ be a word such that $w\{G\}$ is a finite set. There exists a finitely generated subgroup $H \leqslant G$ such that w is concise in G if and only if w is concise in H.*

Proof — If $w\{G\}$ is a finite set, then there exists a finite subset F of G such that $w\{F\} = w\{G\}$. If we consider the finitely generated subgroup $H := \langle F \rangle$ of G, we see that

$$w\{H\} = w\{G\}.$$

Thus, the claim follows. □

Theorem 3.4 *Let $\mathcal{C}$ be a class of groups closed under subgroups, let $w \in F$ be a word in a finitely generated free group, and suppose that the word w is boundedly concise in $\mathcal{C}$. Then the word w is boundedly concise in the class $\mathcal{L}$ of limits of groups in $\mathcal{C}$ in the space of marked groups.*

Proof — We start by assuming that G is finitely generated, to then consider the general case. Let S be a finite generating set for G, and suppose that (G, S) is a limit of $\mathcal{C}$-groups, say limit of the sequence

$$\{(G_r, S_r)\}_{r\in\mathbb{N}} \subseteq \mathcal{G}.$$

If $w\{G\}$ is an infinite set, there is nothing to prove. Thus, suppose that $w\{G\} \subseteq G$ is finite, so that there exists $R \in \mathbb{N}$ such that

$$w\{G\} \subseteq B_{(G,S)}(R).$$

By Proposition 2.1, there exists $\bar{r} \in \mathbb{N}$ such that $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G_r,S_r)$, for all $r \geqslant \bar{r}$, have balls of radius R isomorphic as labeled graphs. In particular, $w\{G\}$ and $w\{G_r\}$ are identified under these isomorphisms, thus we have that $|w\{G\}| = |w\{G_r\}|$, for all $r \geqslant \bar{r}$.

As $G_r \in \mathcal{C}$ and $w\{G_r\}$ is a finite set, we have that $(G_r)_w$ is a finite group, because the word w is (boundedly) concise in $\mathcal{C}$ and $G_r \in \mathcal{C}$. Moreover, as the word w is boundedly concise in this class and the cardinality $|w\{G_r\}| = |w\{G\}|$ remains constant, for all $r \geqslant \bar{r}$, we obtain a uniform bound $\delta = \delta\big(|w\{G\}|\big) \in \mathbb{N}$ such that the cardinality of the finite groups $(G_r)_w$ is bounded by δ, for all $r \geqslant \bar{r}$.

Replacing R with a bigger constant, if needed, we can suppose without loss of generality that the balls of radius R in G_r contain the finite group $(G_r)_w$ (of cardinality at most δ, uniformly), for all sufficiently large indices r, say for all $r \geqslant \widetilde{r} \geqslant \bar{r}$. Thus, G_w must be a finite subgroup of G, of cardinality bounded by δ, because G and G_r have isomorphic balls of radius R, for all sufficiently large r.

If G is not finitely generated and $w\{G\}$ is a finite set (say, realised by a finite set $F \subseteq G$ of elements, that is $w\{G\} = w\{F\}$), then Lemma 3.3 and [3, Proposition 2.20] imply that the finitely generated subgroup $\langle F \rangle$ is a limit of (H_r, T_r), for sufficiently large indices, where $H_r \leqslant G_r$ are given by Lemma 3.3. As $\mathcal{C}$ is closed under taking subgroups, we deduce that $H_r \in \mathcal{C}$, for all r. In particular, $(H_r)_w$ is a finite subgroup of H_r, with uniform bound on the cardinality not depending on r, but just on $|w\{F\}|$, and we can apply what we proved in the previous part of the proof. Therefore, the claim follows. □

This point of view is general, and does not depend on a spe-

cific class. Applying the previous theorem to the class of (residually) finite groups, we extend all known results on bounded conciseness for those groups to LEF groups (that is, limit of finite groups in the space of marked groups).

Definition 3.5 A group G is *locally embeddable into finite groups* (for short, a LEF group) if for all $F \subseteq G$ finite subset there exists a finite group Q and a map $\varphi\colon G \to Q$ such that

(1) $\varphi \restriction_F$ is an injective map;

(2) $\varphi(gh) = \varphi(g)\varphi(h)$, for all $g, h \in F$.

The second condition of a LEF group guarantees that the map φ behaves like a homomorphism on the finite set F, whereas the first condition excludes non-meaningful ways to do that (for instance, by mapping all elements of F to the trivial element e_Q).

When the group G is residually finite, then we can construct *homomorphisms* onto finite quotients of G with these properties. It turns out that, for finitely *presented* LEF groups, that is always the case, that is finitely presented LEF groups are residually finite. This is not the case for finitely generated groups. For instance, the groups of permutations $S := \mathrm{Sym}_f(\mathbb{Z})$ with finite support of an infinite set is an infinite non-residually finite group because it contains the simple infinite group of even permutations with finite support. Let us consider the translation $t\colon \mathbb{Z} \to \mathbb{Z}$ defined by

$$t(n) := n + 1,$$

for all integer numbers n. Then, the group $S \rtimes \langle t \rangle$ is a finitely generated LEF group that is not residually finite (it is generated by t and the transposition $(0\ 1) \in S$).

Notice that a limit of residually finite groups is LEF. Indeed, if G is a limit of residually finite groups and F is a finite subset

of G, then there exists a radius R such that the finite subset

$$F \cdot F = \{fh \mid f, h \in F\}$$

is contained in the ball in G of radius R. This finite ball is eventually isomorphic as a labeled directed graph to the ball of radius R in a residually finite group G_r. Call ψ the restriction of this graph isomorphism to the vertex set and extend arbitrarily ψ to a map $G \to G_r$. As G_r is residually finite, we can find a homomorphism $\pi\colon G_r \to Q$ onto a finite group Q that is injective on the finite set $\psi(F \cdot F)$. Then

$$\pi \circ \psi\colon G \to Q$$

is a map that meets the conditions of Definition 3.5 for the set F, proving therefore that G is LEF.

As an application of Theorem 3.4 we obtain the following result.

Corollary 3.6 *Let $w \in F$ be a word. The following are equivalent*:

(1) *w is boundedly concise in the class of residually finite groups;*

(2) *w is boundedly concise in the class of LEF groups;*

(3) *w is concise in the class of LEF groups.*

Proof — The implication (1) $\Rightarrow$(2) is Theorem 3.4, whereas the implications (2) $\Rightarrow$ (1) and (2) $\Rightarrow$ (3) follow directly from the definitions. The remaining implication follows from the fact that an untraproduct of LEF groups is itself a LEF group (this is mentioned/proved in [12, Proposition 2.2], but compare also the appendix of [6]). □

4 Some examples

In this concluding section we collect some examples of groups that are far from being residually finite (thus, neither linear)

such that all words are concise in these groups.

We record the following lemma, whose proof can be adapted from [13, Proposition 1.1.3].

Lemma 4.1 *Let $w \in F_r$ be a word and suppose that w is concise in a class of groups $\mathcal{C}$. Then, it is concise in the class of finite-by-$\mathcal{C}$ groups.*

Lemma 4.1 is of interest because there exist several finitely presented finite-by-linear (central) extensions that are very far away from being residually finite. One such family is given by quotients of Deligne's group [4, 5, 11]. Deligne's group D is a central extension

$$\{e\} \to \mathbb{Z} \to D \to Sp_{2n}(\mathbb{Z}) \to \{e\},$$

where $Sp_{2n}(\mathbb{Z})$ is the group of symplectic matrices with integer coefficients, that is

$$Sp_{2n}(\mathbb{Z}) := \left\{ P \in \mathcal{M}_{2n}(\mathbb{Z}) \mid P^t \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} P = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \right\}.$$

Thus, in particular, $Sp_{2n}(\mathbb{Z})$ is a linear group. The group D is finitely presented because both $\mathbb{Z}$ and $Sp_{2n}(\mathbb{Z})$ are finitely presented. What is relevant to us is that Deligne [5] proved that D is not residually finite, because the intersection of all subgroups of finite index is a cyclic subgroup of order two. Moreover, it satisfies Kazhdan's property (T) (see [1, Example 1.7.13 (iii)]), and in particular any amenable quotient of D must be finite. Thus, D is not residually amenable, nor a limit of amenable groups in the space of marked groups (being finitely presented, these two notions coincide).

This, of course, is a central extension with *infinite* normal subgroup and linear quotient, and thus the hipoteses of Lemma 4.1 are not met. Nevertheless, we can consider the quotients $D/m\mathbb{Z}$ given by the central subgroups $m\mathbb{Z}$: these are central extensions

of the form

$$\{e\} \to \mathbb{Z}/m\mathbb{Z} \to D/m\mathbb{Z} \to \mathrm{Sp}_{2n}(\mathbb{Z}) \to \{e\},$$

thus finite-by-linear central extensions, and hence any word w is concise in these $D/m\mathbb{Z}$. Notice that these groups too are not residually finite, and they are isolated points in the space of marked groups [4, Section 5.8]. All words are concise in the class of linear groups [10]. Therefore, by Lemma 4.1, all words are concise in these (non-linear) examples.

Acknowledgements

The author is supported by the Spanish Government, grant number PID2020-117281GB-I00, partly by the European Regional Development Fund (ERDF), and the Basque Government, grant number IT1483-22. He is very thankful to Gustavo Fernández, Matteo Pintonello, Andoni Zozaya for insightful conversations on this topic, and to an anonymous referee for their comments that improved a lot the quality of exposition of this work.

REFERENCES

[1] B. Bekka – P. de la Harpe – A. Valette: "Kazhdan's Property (T)", *Cambridge University Press*, Cambridge (2008).

[2] C. Champetier: "L'espace des groupes de type fini", *Topology* 39 (2000), 657–680.

[3] C. Champetier – V. Guirardel: "Limit groups as limit of free groups", *Israel J. Math.* 146 (2005), 1–75.

[4] Y. de Cornulier – L. Guyot – W. Pitsch: "On the isolated points in the space of groups", *J. Algebra* 307 (2007), 254–277.

[5] P. Deligne: "Extensions centrales non résiduellement finies de groupes arithmétiques", *C.R. Acad. Sci. Paris Sér. A-B* 287 (1978), A203–A208.

[6] G.A. Fernández-Alcober – M. Morigi: "Outer commutator words are uniformly concise", *J. Lond. Math. Soc.* (2) 82 (2010), 581–595.

[7] G.A. Fernández-Alcober – P. Shumyatsky: "On bounded conciseness of words in residually finite groups", *J. Algebra* 500 (2018), 19–29.

[8] R.I. Grigorchuk: "Degrees of growth of finitely generated groups and the theory of invariant means", *Izv. Akad. Nauk SSSR Ser. Mat.* 48 (1984), 939–985.

[9] S.V. Ivanov: "Hall's conjecture on the finiteness of verbal subgroups", *Izv. Vyssh. Uchebn. Zaved. Mat.* 33 (1989), 59–70.

[10] Ju.I. Merzljakov: "Verbal and marginal subgroups of linear groups", *Dokl. Akad. Nauk SSSR* 177 (1967), 1008–1011.

[11] D.W. Morris: "A lattice with no torsion-free subgroups of finite index (after P. Deligne)" (2009); url:`https://people.uleth.ca/ dave.morris /talks/deligne-torsion.pdf`.

[12] A. Ould Houcine – F. Point: "Alternatives for pseudofinite groups", *J. Group Theory* 16 (2013), 461–495.

[13] D. Segal: "Words: Notes on Verbal Width in Groups", *Cambridge University Press*, Cambridge (2009).

Federico Berlai
Department of Mathematics
University of the Basque Country UPV/EHU
Barrio Sarriena s/n, 48940, Leioa (Spain)
e-mail: federico.berlai@ehu.eus



Advances in Group Theory and Applications
© 2026 AGTA - www.advgrouptheory.com/journal
23 (2026), pp. 183–213 ISSN: 2499-1287
DOI: 10.32037/agta-2026-009

On Quantitative Structure of Symplectic Groups of Dimension Four

S.H. Alavi — A. Daneshkham — H.P. Mosaed

(*Received Nov. 16, 2023; Accepted May. 16, 2025 — Communicated by M. Trombetti*)

Abstract

The main aim of this article is to study the quantitative structure of projective symplectic groups $PSp_4(q)$ with $q > 2$ even. Indeed, we prove that the groups $PSp_4(q)$ with $q > 2$ even are uniquely determined by their orders and the set of the number of elements of the same order. This result links to the well-known J.G. Thompson's problem (1987) for finite simple groups.

Mathematics Subject Classification (2020): 20E32, 20D06, 20D60

Keywords: Thompson's problem; projective symplectic group; element order

1 Introduction

For a finite group G and a positive integer n, let G_n consist of all elements x satisfying $x^n = 1$. The *type* of G is defined to be the function whose value at n is the order of G_n. This notion links to the notion of *same-order type* $\tau(G)$ of G, that is to say, *the set of the number of elements of the same order* in G. Indeed, it turns out that if two groups G and H are of the same type, then $\tau(G) = \tau(H)$ and $|G| = |H|$. However, finite groups with the same order and same-order type may not have the same type or even the same *spectrum*, the set of element orders. The smallest examples of such groups that we have found are

$$G := \mathbb{Z}_4 \times (\mathbb{Z}_7 : \mathbb{Z}_3) \qquad \text{and} \qquad H := \mathbb{Z}_3 \times (\mathbb{Z}_7 : \mathbb{Z}_4)$$

of order 84 in which $\tau(G) = \tau(H) = \{1, 2, 6, 12, 14, 28\}$, and G has an element of order 28 while H has no such an element. Moreover, G and H are not of the same type as $|G_3| = 15$ and $|H_3| = 3$.

The main objective of this paper is to investigate the structure of groups with the same-order type as finite simple groups. In this direction, Shao et al. [14] studied finite simple groups whose order is divisible by at most four primes. This problem has been studied for several families of simple groups including small Ree groups and Suzuki groups [1, 2]. In this paper, we study groups with the same order and the same-order type as $PSp_4(q)$ with q even.

Theorem 1.1 *Let* G *be a group such that* $\tau(G) = \tau(S)$ *and* $|G| = |S|$, *where* $S = PSp_4(q)$ *with* $q > 2$ *even. Then* G *is isomorphic to* S.

In 1987, J.G. Thompson [10, Problem 12.37] asked if a group with the same type as a solvable group is still solvable. One may ask this problem for non-solvable groups, in particular, finite simple groups. It is easy to see that two groups with the same type share the same order and and the same spectrum. Hence, the recognition of finite simple groups by their orders and spectra, which is known known in the literature as Shi's problem [10, Problem 12.39], gives a positive answer to Thompson's problem. It is worth noting that Vasil'ev, Grechkoseeva and Mazurov [15] finalized a complete solution to Shi's problem, and consequently Thompson's problem holds for finite simple groups. As noted above, two groups G and H with the same type have the same order and same-order type, and hence Theorem 1.1 also gives a positive answer to Thompson's problem for finite simple groups $PSp_4(q)$ with q even.

Corollary 1.2 *If* G *is a finite group of the same type as* $S := PSp_4(q)$ *with* $q > 2$ *even, then* G *is isomorphic to* S.

Our analysis in proving Theorem 1.1 depends on determining $\tau(S)$, where $S = PSp_4(q)$ with $q > 2$ even, see Proposition 3.3. Despite of the investigation of the groups which have been previously considered, we have generally no isolated vertex in the prime graph of a group G with the same number of elements of the same order as S.

1.1 Definitions and notation

In this section, we give some brief comments on the notation used in this paper. Throughout this article all groups are finite. Our group theoretic notation is standard, and it is consistent with the notation

in [3, 5, 8] with noting that we use Alt_n to denote the alternating group on n letters. In particular, we follow the notation below for the finite simple classical groups:

$\mathrm{PSL}_n(q)$, for $n \geqslant 2$ and $(n,q) \neq (2,2),(2,3)$,

$\mathrm{PSU}_n(q)$, for $n \geqslant 3$ and $(n,q) \neq (3,2)$,

$\mathrm{PSp}_{2m}(q)$, for $m \geqslant 2$ and $(m,q) \neq (2,2)$,

$\mathrm{P\Omega}_{2m+1}(q)$, for $m \geqslant 3$ and q odd,

$\mathrm{P\Omega}^{\pm}_{2m}(q)$, for $m \geqslant 4$.

In this manner, the only repetitions are:

$\mathrm{PSL}_2(4) \simeq \mathrm{PSL}_2(5) \simeq \mathrm{Alt}_5$, $\mathrm{PSL}_2(7) \simeq \mathrm{PSL}_3(2)$, $\mathrm{PSL}_2(9) \simeq \mathrm{Alt}_6$,

$\mathrm{PSL}_4(2) \simeq \mathrm{Alt}_8$ and $\mathrm{PSp}_4(3) \simeq \mathrm{PSU}_4(2)$.

We denote the set of Sylow p-subgroups of G by $\mathrm{Syl}_p(G)$. We also use $n_p(G)$ to denote the number of Sylow p-subgroups of G. For a positive integer n, the set of prime divisors of n is denoted by $\pi(n)$, and if G is a finite group, $\pi(G) := \pi(|G|)$, where $|G|$ is the order of G. Moreover, we denote the set of elements' orders of G by $\omega(G)$ known as *spectrum* of G. The *prime graph* $\Gamma(G)$ of a finite group G is a graph whose vertex set is $\pi(G)$, and two distinct vertices p and q are adjacent if and only if $pq \in \omega(G)$. Assume further that $\Gamma(G)$ has $t(G)$ connected components $\pi_i := \pi_i(G)$, for $i = 1, 2, \ldots, t(G)$. The positive integers n_i with $\pi(n_i) = \pi_i$ are called *order components* of G. Evidently, $|G| = n_1 \ldots n_{t(G)}$. We denote by $\mathrm{oc}(G)$ the set of all order components of G. In the case where G is of even order, we always assume that $2 \in \pi_1$, and π_1 is said to be the even component of G. In this way, π_i and n_i are called odd components and odd order components of G, respectively. Recall that $\tau(G)$ is the set of the number of elements in G with the same order. In other word, $\tau(G)$ consists of the numbers $m_i(G)$ of elements of order i in G, for $i \in \omega(G)$. Here, φ and ψ are the *Euler totient* function and the *Dedekind arithmetic* function, respectively. In the other word, for every positive integer n,

$$\varphi(n) = n \prod_{p \in \pi(n)} \left(1 - \frac{1}{p}\right) \qquad \text{and} \qquad \psi(n) = n \prod_{p \in \pi(n)} \left(1 + \frac{1}{p}\right).$$

We also use $\Phi_n(q)$ to denote the n-*th cyclotomic polynomial* of order n.

2 Preliminaries

In this section, we give some useful results which we frequently use in order to prove our results.

Lemma 2.1 (see [4], Theorem 1) *Let* G *be a Frobenius group of even order with kernel* K *and complement* H*. Then* $\pi(H)$ *and* $\pi(K)$ *are the only connected components of* $\Gamma(G)$*.*

A group G is called 2-Frobenius group if there exists a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that G/H and K are Frobenius groups with kernels K/H and H, respectively.

Lemma 2.2 (see [4], Theorem 2) *Let* G *be a 2-Frobenius group of even order. Then* $\Gamma(G)$ *has exactly two connected components. Moreover, there exists a normal series* $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ *such that*

(i) $\pi_1(G) = \pi(H) \cup \pi(G/K)$*, and* $\pi_2(G) = \pi(K/H)$*;*

(ii) G/K *and* K/H *are cyclic groups;*

(iii) $|G/K|$ *divides* $|Aut(K/H)|$*, and* $(|G/K|, |K/H|) = 1$*;*

(iv) H *is a nilpotent group and* G *is a solvable group.*

Lemma 2.3 (see [11, 17]) *Let* G *be a finite group with more than one prime graph component. Then one of the following statements holds*:

(i) G *is a Frobenius group;*

(ii) G *is a 2-Frobenius group;*

(iii) G *admits a normal series* $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ *such that* H *and* G/K *are* $\pi_1(G)$*-groups,* K/H *is a non-abelian simple group,* H *is a nilpotent group,* $|G/K|$ *divides* $|Out(K/H)|$*,* $t(K/H) \geqslant t(G)$*, and for every* $i \in \{2, \ldots, t(G)\}$*, there exists* $j \in \{2, \ldots, t(K/H)\}$ *such that*

$$\pi_i(G) = \pi_j(K/H).$$

Lemma 2.4 (see [13], p. 50) *All subgroups and all quotient groups of any cyclic group are cyclic. If* G *is a cyclic group of finite order* n*, then* G *has just one subgroup* H *of order* m *for each divisor* m *of* n*,* H *is cyclic and* G/H *is cyclic of order* n/m*.*

Lemma 2.5 (see [13], p. 35) *Let n be an integer, $n > 1$, and let the factorization of n as a product of primes be*

$$n = p_1^{m_1} p_2^{m_2} \dots p_r^{m_r},$$

where $r, m_1, \dots, m_r$ are positive integers and $p_1, \dots, p_r$ distinct primes. Then $\mathbb{Z}_n$ is decomposable if $r > 1$, and

$$\mathbb{Z}_n \simeq \mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \dots \times \mathbb{Z}_{q_r},$$

where $q_i = p_i^{m_i}$, for each $i = 1, \dots, r$. Moreover, for each prime p and positive integer m, $_{p^m}$ is indecomposable.

Lemma 2.6 (see [13], p. 198) *Let n be a positive integer, and let G be an abelian group. Also let*

$$G_n = \{x \in G \,:\, x^n = 1\} \qquad \text{and} \qquad G^n = \{x^n \,:\, x \in G\}.$$

Then the following statements hold:

(i) $G_n \leqslant G$, *and* $G/G_n \simeq G^n$;

(ii) *Suppose that G is finite, so that there are elements $x_1, \dots, x_r$ of G such that*

$$G = \langle x_1 \rangle \times \dots \times \langle x_r \rangle.$$

For each $i = 1, \dots, r$, let $n_i = o(x_i)$ and $k_i = n_i/(n_i, n)$. Then

$$G_n = \langle x_1^{k_1} \rangle \times \dots \times \langle x_r^{k_r} \rangle;$$

(iii) *If G is finite, then $G/G^n \simeq G_n$.*

Lemma 2.7 (see [9], Theorem 9.1.2) *Let G be a finite group, and let n be a positive integer dividing $|G|$. Then n divides $|G_n|$.*

The proof of the following result is straightforward by Lemma 2.7.

Lemma 2.8 *Let G be a finite group. Then, for every $i \in \omega(G)$,*

$$m_i(G) = k\varphi(i),$$

where k is the number of cyclic subgroups of order i in G, and i divides

$$\sum_{j|i} m_j(G).$$

Moreover, if $i > 2$, *then* $m_i(G)$ *is even.*

Lemma 2.9 (see [16], Theorem 3) *Let* G *be a finite group. Then the number of elements whose orders are multiples of* n *is either zero, or a multiple of the greatest divisor of* $|G|$ *that is prime to* n.

Lemma 2.10 (see [18], Lemma 2.6) *Let* G *be a finite group, and* $PSp_4(q)$ *be a projective symplectic group, where* $q > 3$. *If* $oc(G) = oc(PSp_4(q))$, *then* $G \simeq PSp_4(q)$.

Lemma 2.11 (see [6]) *Let* p *and* q *be primes such that* $p^m = q^n + 1$, *for some positive integers* m *and* n. *Then one of the following statements holds*:

(i) $(p, q, m, n) = (3, 2, 2, 3)$;

(ii) $p = 2^n + 1$ *is a Fermat prime with* n *a power of* 2;

(iii) $q = 2^m - 1$ *is a Mersenne prime with* m *prime.*

Lemma 2.12 *Let* q *be a power of* 2. *Then the following statements hold*:

(i) $2q^2 + 3$ *does not divide* $q^4(q^4 - 1)(q^2 - 1)$;

(ii) *If* $q^2 + 2$ *divides* $q^4(q^4 - 1)(q^2 - 1)$, *then* $q = 2, 4$;

(iii) *If* $2q^2 + 1$ *divides* $q^4(q^4 - 1)(q^2 - 1)$, *then* $q = 2$;

(iv) *If* $3q^2 + 2$ *divides* $q^4(q^4 - 1)(q^2 - 1)$, *then* $q = 4$;

(v) $q^4 - 9$ *does not divide* $q^4(q^4 - 1)(q^2 - 1)$.

Proof — We know that $2q^2 + 3$ is coprime to $q^4(q^2 + 1)$. If $2q^2 + 3$ would divide $q^4(q^4 - 1)(q^2 - 1)$, then $2q^2 + 3$ would divide $(q^2 - 1)^2$. Since $4(q^2 - 1)^2 = (2q^2 - 7)(2q^2 + 3) + 25$, it would follow that

$$2q^2 + 3 \mid 25,$$

and so $q^2 \leqslant 11$ which is true when $q = 2$ but in this case $2q^2 + 3 = 11$ does not divide 25. This follows part (i). To prove part (ii), since $q^2 + 2$ is coprime to $q^2 + 1$, if $q^2 + 2$ divides $q^4(q^4 - 1)(q^2 - 1)$, we conclude that $q^2 + 2$ has to divide $q^4(q^2 - 1)^2$. We know that

$$q^4(q^2 - 1)^2 = (q^6 - 4q^4 + 9q^2 - 18)(q^2 + 2) + 36.$$

Then $q^2 + 2$ divides 36, and this is true if and only if $q = 2, 4$, as desired. Parts (iii)–(v) can be proved in a same manner. □

3 Properties of projective symplectic groups

In this section, we state some useful facts about projective symplectic groups of dimension 4 and their element orders in order to obtain the number of the elements of the same order of $\mathrm{PSp}_4(q)$ with $q = 2^f > 2$ in Section 3.2 below.

3.1 Conjugacy classes

Let $\overline{\mathbb{F}}$ be the algebraic closure of the finite field $\mathbb{F}$ of size $q = p^f$. Let also

$$\mathbb{F}_i = \left\{x \in \overline{\mathbb{F}} \,:\, x^{q^i} = x\right\}$$

be the subfield of $\overline{\mathbb{F}}$ with q^i elements, and let $\mathbb{F}_1 := \mathbb{F}$. Let now κ be a fixed generator of the multiplicative group $\mathbb{F}_4^\times$, and set

$$\tau := \kappa^{q^2-1},\ \theta := \kappa^{q^2+1},\ \eta := \theta^{q-1} \quad \text{and} \quad \gamma := \theta^{q+1}.$$

Then $\mathbb{F}_2^\times = \langle\theta\rangle$ and $\mathbb{F}^\times = \langle\gamma\rangle$. For $t \in \mathbb{F}$ and $z_i \in \mathbb{F}_4^\times$, define

$$x_a(t) = \begin{bmatrix} 1 & t & & \\ & 1 & & \\ & & 1 & -t \\ & & & 1 \end{bmatrix}, \quad x_{a+b}(t) = \begin{bmatrix} 1 & & t & \\ & 1 & & t \\ & & 1 & \\ & & & 1 \end{bmatrix},$$

$$x_b(t) = \begin{bmatrix} 1 & & & \\ & 1 & t & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \quad x_{2a+b}(t) = \begin{bmatrix} 1 & & & t \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}, \tag{3.1}$$

$$\text{and} \quad h(z_1, z_2) = \begin{bmatrix} z_1 & & & \\ & z_2 & & \\ & & z_2^{-1} & \\ & & & z_1^{-1} \end{bmatrix}.$$

Let

$$\omega_\iota := x_\iota(1)' x_\iota(-1) x_\iota(1)$$

for $\iota \in \Delta^+ := \{a, b, a+b, 2a+b\}$, where $x_\iota(1)'$ is the transposed matrix of $x_\iota(1)$. In particular,

$$\omega_a = \begin{bmatrix} & 1 & & \\ -1 & & & \\ & & & -1 \\ & & 1 & \end{bmatrix} \quad \text{and} \quad \omega_b = \begin{bmatrix} 1 & & & \\ & & 1 & \\ & -1 & & \\ & & & 1 \end{bmatrix}. \tag{3.2}$$

Therefore, the 4-dimensional projective symplectic group $PSp_4(q)$ over $\mathbb{F}$ is generated by $x_\iota(t)$, $h(z_1, z_2)$, ω_a and ω_b defined as in (3.1) and (3.2). We use the following set of parameters for the conjugacy classes: for $i, j \in \mathbb{Z}$, "$\mathbb{Z} \pmod m$" means that i and j give the same class if $i \equiv j \pmod m$.

$$\begin{aligned}
T_0 &= \{i \in \mathbb{Z} \pmod{q-1}\},\\
T_1 &= \{i \in T_0 : i \not\equiv 0 \pmod{q-1}\},\\
T_2 &= \{i \in \mathbb{Z} \pmod{q+1} : i \not\equiv 0 \pmod{q+1}\},\\
S_0 &= \{(i,j) \in T_0 \times T_0 : i \not\equiv j \pmod{q-1}\},\\
S_1 &= \{(i,j) \in T_1 \times T_1 : i \not\equiv \pm j \pmod{q-1}\},\\
S_2 &= \{(i,j) \in T_2 \times T_2 : i \not\equiv \pm j \pmod{q+1}\},\\
R_1 &= \{i \in \mathbb{Z} \pmod{q^2-1} : i \not\equiv qi \pmod{q^2-1}\},\\
R_2 &= \{i \in \mathbb{Z} \pmod{q^2-1} : i \not\equiv \pm qi \pmod{q^2-1}\}, \text{ and}\\
R_3 &= \{i \in \mathbb{Z} \pmod{q^2+1} : i \not\equiv 0 \pmod{q^2+1}\}.
\end{aligned}$$

Remark 3.1 Let us notice that the detail information of the conjugacy classes of $PSp_4(2^f)$ are recorded in [7]. We summarise required information in Table 1. By [7, p. 92], we also note that:

(i) eight classes $B_t(\pm i, \pm j)$ and $B_t(\pm j, \pm i)$ are the same, for $t = 1, 4$;

(ii) four classes $B_t(\pm i)$, $B_t(\pm qi)$ are the same, for $t = 2, 5$;

(iii) four classes $B_t(\pm i, \pm j)$ are the same, for $t = 3$;

(iv) two classes $C_t(\pm i)$ are the same, for $1 \leqslant t \leqslant 4$;

(v) two classes $D_t(\pm i)$ are the same, for $1 \leqslant t \leqslant 4$.

Table 1: Conjugacy classes of $PSp_4(q)$ with $q = 2^f$

Name	Conditions	Representative	Order of Reps.	Number of class	Length of class
A_1		$h(1,1)$	1	1	1
A_2		$x_{2a+b}(1)$	2	1	(q^4-1)
A_{31}		$x_{a+b}(1)$	2	1	(q^4-1)
A_{32}		$x_{a+b}(1)x_{2a+b}(1)$	2	1	$(q^2-1)(q^4-1)$
A_{41}		$x_a(1)x_b(1)$	4	1	$\frac{q^2(q^2-1)(q^4-1)}{2}$
A_{42}	$\xi \in \mathbb{F}$	$x_a(1)x_b(1)x_{2a+b}(\xi)$	4	1	$\frac{q^2(q^2-1)(q^4-1)}{2}$
$B_1(i,j)$	$(i,j) \in S_1$	$h(\gamma^i, \gamma^j)$	$\frac{(q-1)}{(q-1,i,j)}$	$\frac{(q-2)(q-4)}{8}$	$q^4(q+1)^2(q^2+1)$
$B_2(i)$	$i \in R_2$	$h(\theta^i, \theta^{qi})$	$\frac{(q^2-1)}{(q^2-1,i)}$	$\frac{q(q-2)}{4}$	$q^4(q^4-1)$
$B_3(i,j)$	$(i,j) \in T_1 \times T_2$	$h(\gamma^i, \eta^j)$	$\frac{(q^2-1)}{(q-1,i)(q+1,j)}$	$\frac{q(q-2)}{4}$	$q^4(q^4-1)$
$B_4(i,j)$	$(i,j) \in S_2$	$h(\eta^i, \eta^j)$	$\frac{q+1}{(q+1,i,j)}$	$\frac{q(q-2)}{8}$	$q^4(q-1)^2(q^2+1)$
$B_5(i)$	$i \in R_3$	$h(\tau^i, \tau^{qi})$	$\frac{q^2+1}{(q^2+1,i)}$	$\frac{q^2}{4}$	$q^4(q^2-1)^2$
$C_1(i)$	$i \in T_1$	$h(1, \gamma^i)$	$\frac{q-1}{(q-1,i)}$	$\frac{(q-2)}{2}$	$q^3(q+1)(q^2+1)$
$C_2(i)$	$i \in T_1$	$h(\gamma^i, \gamma^{-i})$	$\frac{q-1}{(q-1,i)}$	$\frac{(q-2)}{2}$	$q^3(q+1)(q^2+1)$
$C_3(i)$	$i \in T_2$	$h(1, \eta^i)$	$\frac{q+1}{(q+1,i)}$	$\frac{q}{2}$	$q^3(q-1)(q^2+1)$
$C_4(i)$	$i \in T_2$	$h(\eta^i, \eta^{-i})$	$\frac{q+1}{(q+1,i)}$	$\frac{q}{2}$	$q^3(q-1)(q^2+1)$
$D_1(i)$	$i \in T_1$	$h(1, \gamma^i)x_{2a+b}(1)$	$\frac{2(q-1)}{(q-1,i)}$	$\frac{(q-2)}{2}$	$q^3(q+1)(q^4-1)$
$D_2(i)$	$i \in T_1$	$h(\gamma^i, \gamma^{-i})x_{a+b}(1)$	$\frac{2(q-1)}{(q-1,i)}$	$\frac{(q-2)}{2}$	$q^3(q+1)(q^4-1)$
$D_3(i)$	$i \in T_2$	$h(1, \eta^i)x_{2a+b}(1)$	$\frac{2(q+1)}{(q+1,i)}$	$\frac{q}{2}$	$q^3(q-1)(q^4-1)$
$D_4(i)$	$i \in T_2$	$h(\eta^i, \eta^{-i})x_{a+b}(1)$	$\frac{2(q+1)}{(q+1,i)}$	$\frac{q}{2}$	$q^3(q-1)(q^4-1)$

3.2 Elements of the same order

In this section, we determine the number of the elements of the same order of $PSp_4(q)$ with $q = 2^f > 2$ in Proposition 3.3 below.

Lemma 3.2 (see [12], Lemma 7) *Let* $S := PSp_4(q)$ *with* $q = 2^f > 2$. *If* n *is an element order of* S, *then* n *divides one of the five numbers*

$$4,\ 2(q-1),\ 2(q+1),\ q^2-1,\ q^2+1.$$

Proof — The representative of the conjugacy classes of the group S is listed as in the third column of Table 1. Note that each such representative is presented in the form of $x_\iota(t)$, $h(z_1, z_2)$ or their products, for some $t \in \mathbb{F}$, $z_i \in \mathbb{F}_4^\times$, and $\iota \in \Delta^+ := \{a, b, a+b, 2a+b\}$. The explicit definition of $x_\iota(t)$ and $h(z_1, z_2)$ are given in (3.1). It is then easy to find the order of each representative of the conjugacy classes of the group S as in the fourth column of Table 1, and hence the proof follows. □

Proposition 3.3 *Let* $S := PSp_4(q)$ *with* $q = 2^f > 2$. *Then the following statements holds*:

(i) $m_2(S) = (q^2+1)(q^4-1)$;

(ii) $m_4(S) = q^2(q^2-1)(q^4-1)$;

(iii) *if* $1 \neq r \mid q-1$,

$$m_r(S) = \varphi(r)q^3(q^2+1)(q+1)\left(1 - \frac{q(q+1)}{2} + \frac{q(q+1)}{8}\psi(r)\right);$$

(iv) *if* $1 \neq r \mid q+1$,

$$m_r(S) = \varphi(r)q^3(q^2+1)(q-1)\left(1 - \frac{q(q-1)}{2} + \frac{q(q-1)}{8}\psi(r)\right);$$

(v) *if* $1 \neq r \mid q-1$, $m_{2r}(S) = \varphi(r)q^3(q+1)(q^4-1)$;

(vi) *if* $1 \neq r \mid q+1$, $m_{2r}(S) = \varphi(r)q^3(q-1)(q^4-1)$;

(vii) *if* $1 \neq r \mid q-1$ *and* $1 \neq s \mid q+1$, $m_{rs}(S) = \frac{1}{2}\varphi(rs)q^4(q^4-1)$;

(viii) *if* $1 \neq r \mid q^2+1$, $m_r(S) = \frac{1}{4}\varphi(r)q^4(q^2-1)^2$.

Proof — For $r \in \omega(S)$, let $cl_r(S)$ be the set of the conjugacy classes of S containing all elements of order r. Then

$$m_r(S) = \sum_{c \in cl_r(S)} |c|.$$

In what follows, for each $r \in \omega(S)$, we obtain $cl_r(S)$, and then $m_r(S)$.

If $r = 2$, then

$$cl_2(S) = \{A_2, A_{31}, A_{32}\},$$

and so by Table 1, we have that

$$\begin{aligned} m_2(S) &= |A_2| + |A_{31}| + |A_{32}| = (q^4-1) + (q^4-1) + (q^2-1)(q^4-1) \\ &= (q^2+1)(q^4-1). \end{aligned}$$

Similarly,

$$\begin{aligned} m_4(S) &= |A_{41}| + |A_{42}| = q^2(q^2-1)(q^4-1)/2 + q^2(q^2-1)(q^4-1)/2 \\ &= q^2(q^2-1)(q^4-1). \end{aligned}$$

We now prove part (iii). Let $r \neq 1$ be a divisor of $q-1$. By Table 1, the elements of order r are in the classes $B_1(i,j)$, $C_1(i)$ and $C_2(i)$. Thus $\mathrm{cl}_r(S) = B_1 \cup C_1 \cup C_2$, where

$$\begin{aligned} B_1 &= \{B_1(i,j) : (i,j) \in S_1,\ |h(\gamma^i, \gamma^j)| = r\}, \\ C_1 &= \{C_1(i) : i \in T_1,\ |h(1, \gamma^i)| = r\}, \\ C_2 &= \{C_2(i) : i \in T_1,\ |h(\gamma^i, \gamma^{-i})| = r\}. \end{aligned}$$

We now determine $|B_1|$, $|C_1|$ and $|C_2|$.

Let $\mathcal{B} = \{h(\gamma^i, \gamma^j) : (i,j) \in S_1\}$. Then

$$\begin{aligned} \mathcal{B} &= \{h(\gamma^i, \gamma^j) : (i,j) \in S_1\} \\ &= \{h(\gamma^i, \gamma^j) : 0 < i, j < q-1,\ i \not\equiv \pm j \pmod{q-1}\} \\ &= \{h(z_1, z_2) : z_1, z_2 \in \mathbb{F}^\times,\ z_1, z_2 \neq 1,\ z_1 \neq z_2 \text{ and } z_1 \neq z_2^{-1}\}. \end{aligned}$$

Then $\mathcal{B} = \mathcal{B}_0 \setminus (\mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3 \cup \mathcal{B}_4)$, where

$$\mathcal{B}_0 = \{h(z_1, z_2) : z_1, z_2 \in \mathbb{F}^\times\},\ \mathcal{B}_1 = \{h(1, z) : z \in \mathbb{F}^\times\},$$
$$\mathcal{B}_2 = \{h(z, 1) : z \in \mathbb{F}^\times\},\ \mathcal{B}_3 = \{h(z, z) : z \in \mathbb{F}^\times\},$$
$$\text{and} \qquad \mathcal{B}_4 = \{h(z, z^{-1}) : z \in \mathbb{F}^\times\}.$$

Note that

$$\mathcal{B}_0 \simeq \mathbb{Z}_{q-1} \times \mathbb{Z}_{q-1},\ \mathcal{B}_1 \simeq \mathcal{B}_2 \simeq \mathcal{B}_3 \simeq \mathcal{B}_4 \simeq \mathbb{Z}_{q-1},$$
$$\text{and} \qquad \mathcal{B}_i \bigcap \mathcal{B}_j = \{h(1,1)\},$$

for all $1 \leqslant i, j \leqslant 4$ with $i \neq j$. Lemmas 2.5 and 2.6 imply that the number of elements of $\mathcal{B}_0$ of order r is equal to $\varphi(r)\psi(r)$. Moreover, by Lemma 2.4, the number of elements of order r in $\mathcal{B}_i$ is equal to $\varphi(r)$, for all $i = 1, 2, 3, 4$. Therefore, the number $m_r(\mathcal{B})$ of elements of order r in $\mathcal{B}$ is equal to $\varphi(r)\psi(r) - 4\varphi(r)$. Note that, by Remark 3.1,

$$B_1(\pm i, \pm j) = B_1(\pm j, \pm i).$$

Then

$$|B_1| = \frac{1}{8} m_r(\mathcal{B}) = \frac{\varphi(r)}{8}\psi(r) - \frac{\varphi(r)}{2}.$$

We now obtain $|C_1|$. Let $s := (q-1)/r$. By Remark 3.1, note that

$$C_1(i) = C_1(-i),$$

for all $i \in T_1$. Then

$$\begin{aligned} 2|C_1| &= \left|\{i \in T_1 : |h(1, \gamma^i)| = r\}\right| \\ &= \left|\{i \in T_1 : \frac{q-1}{(q-1,i)} = r\}\right| \\ &= \left|\{i \in T_1 : 0 < i < q-1,\ (q-1,i) = s\}\right|. \end{aligned}$$

Observe that $(q-1,i) = s$ if and only if $((q-1)/s, i/s) = 1$, or equivalently, $(r, i/s) = 1$. Thus

$$2|C_1| = |\{i/s : 0 < i/s < r,\ (r, i/s) = 1\}| = \varphi(r).$$

Therefore, $|C_1| = \varphi(r)/2$. Similarly,

$$2|C_2| = |\{i \in T_1 : |h(\gamma^i, \gamma^{-i})| = r\}| = \varphi(r),$$

that is to say, $|C_2| = \varphi(r)/2$. Hence

$$\begin{aligned} m_r(S) &= \sum_{c \in cl_r(S)} |c| \\ &= \sum_{c \in B_1} |c| + \sum_{c \in C_1} |c| + \sum_{c \in C_2} |c| \\ &= |B_1(i,j)| \cdot |B_1| + |C_1(i')| \cdot |C_1| + |C_2(i')| \cdot |C_2| \\ &= q^4(q+1)^2(q^2+1) \cdot \left(\frac{\varphi(r)}{8}\psi(r) - \frac{\varphi(r)}{2}\right) \\ &\qquad + q^3(q+1)(q^2+1) \cdot \frac{\varphi(r)}{2} + q^3(q+1)(q^2+1) \cdot \frac{\varphi(r)}{2} \\ &= \varphi(r)q^3(q^2+1)(q+1)\left(1 - \frac{q(q+1)}{2} + \frac{q(q+1)}{8}\psi(r)\right). \end{aligned}$$

This proves part (iii). By the same argument as in part (iii), part (iv) follows.

In order to prove part (v), suppose that $r \neq 1$ is a divisor of $q-1$.

Then $\mathrm{cl}_{2r}(S) = D_1 \cup D_2$, where

$$D_1 = \{D_1(i) : i \in T_1, |h(1, \gamma^i)x_{2a+b}(1)| = 2r\},$$
$$D_2 = \{D_2(i) : i \in T_1, |h(\gamma^i, \gamma^{-i})x_{a+b}(1)| = 2r\}.$$

It follows from Remark 3.1 that $D_1(i) = D_1(-i)$, for all $i \in T_1$. Therefore, if $s := (q-1)/r$, then

$$\begin{aligned} 2|D_1| &= \big|\{i \in T_1 : |h(1, \gamma^i)x_{2a+b}(1)| = 2r\}\big| \\ &= \big|\{i \in T_1 : \frac{2(q-1)}{(q-1, i)} = 2r\}\big| \\ &= \big|\{i \in T_1 : \frac{q-1}{(q-1, i)} = r\}\big| \\ &= \big|\{i \in T_1 : 0 < i < q-1,\ (q-1, i) = s\}\big|. \end{aligned}$$

As noted above $(q-1, i) = s$ if and only if $(r, i/s) = 1$, and so

$$2|D_1| = |\{i/s : 0 < i/s < r,\ (r, i/s) = 1\}| = \varphi(r).$$

Hence, $|D_1| = \varphi(r)/2$. Similarly, $|D_2| = \varphi(r)/2$. Thus

$$\begin{aligned} m_{2r}(S) &= \sum_{c \in \mathrm{cl}_r(S)} |c| = \sum_{c \in D_1} |c| + \sum_{c \in D_2} |c| \\ &= q^3(q+1)(q^4-1)|D_1| + q^3(q+1)(q^4-1)|D_2| \\ &= q^3(q+1)(q^4-1)\frac{1}{2}\varphi(r) + q^3(q+1)(q^4-1)\frac{1}{2}\varphi(r). \end{aligned}$$

Hence

$$m_{2r}(S) = \varphi(r)q^3(q+1)(q^4-1),$$

and this proves part (v). To conclude the proof, let us notice that parts (vi), (vii) and (viii) follows in the same manner as part (v). □

Lemma 3.4 *Let* $S := \mathrm{PSp}_4(q)$ *with* $q = 2^f > 2$. *If* $r > 1$ *is a divisor of* $q^2 + 1$, *then the order of each Sylow 2-subgroup of* S *divides* $m_r(S)$, *and so* $4 \mid \varphi(r)$.

Proof — Let $r > 1$ be a divisor of $q^2 + 1$. Then by Lemma 3.2, we note that S has no element of order $2r$, and so the Sylow 2-subgroups

of S act fixed point freely (by conjugation) on the set of elements of order r in S. Thus the order of each Sylow 2-subgroup of S divides $m_r(S)$. By Proposition 3.3 (viii), $m_r(S) = \frac{1}{4}\varphi(r)q^4(q^2-1)^2$, and so $q^4 \mid \frac{1}{4}\varphi(r)q^4(q^2-1)^2$. This requires $4 \mid \varphi(r)$. □

4 Proof of the main result

This section is devoted to proving Theorem 1.1.

For a positive integer q, we define the sets $\mathcal{A}_1, \ldots, \mathcal{A}_9$ as below:

$$\mathcal{A}_1 = \{1\},\ \ \mathcal{A}_2 = \big\{(q^2+1)(q^4-1)\big\},\ \ \mathcal{A}_3 = \big\{q^2(q^2-1)(q^4-1)\big\},$$

$$\mathcal{A}_4 = \big\{\varphi(r)q^3(q^2+1)(q+1)\big(1-\tfrac{q(q+1)}{2}+\tfrac{q(q+1)}{8}\psi(r)\big) : 1 \neq r \mid q-1\big\},$$

$$\mathcal{A}_5 = \big\{\varphi(r)q^3(q^2+1)(q-1)\big(1-\tfrac{q(q-1)}{2}+\tfrac{q(q-1)}{8}\psi(r)\big) : 1 \neq r \mid q+1\big\},$$

$$\mathcal{A}_6 = \big\{\varphi(r)q^3(q+1)(q^4-1) : 1 \neq r \mid q-1\big\};$$

$$\mathcal{A}_7 = \big\{\varphi(r)q^3(q-1)(q^4-1) : 1 \neq r \mid q+1\big\};$$

$$\mathcal{A}_8 = \big\{\tfrac{1}{2}\varphi(rs)q^4(q^4-1) : 1 \neq r \mid q-1 \text{ and } 1 \neq s \mid q+1\big\};$$

$$\mathcal{A}_9 = \big\{\tfrac{1}{4}\varphi(r)q^4(q^2-1)^2 : 1 \neq r \mid q^2+1\big\}.$$

Proposition 4.1 *Let* $S := \mathrm{PSp}_4(q)$ *with*

$$q = 2^f > 2,$$

and let $\mathcal{A}_i$ *with* $i = 1, \ldots, 9$ *be as above. Suppose that* G *is a group such that* $\tau(G) = \tau(S)$ *and* $|G| = |S|$. *Then*

(i) $m_2(G) \in \mathcal{A}_2$;

(ii) $m_r(G) \in \mathcal{A}_9$ *if* $r > 1$ *is a prime divisor of* q^2+1;

(iii) $m_r(G) \in \mathcal{A}_4 \cup \mathcal{A}_5$ *if* $r > 1$ *is a prime divisor of* q^2-1.

Proof — Since $\tau(G) = \tau(S)$, it follows that $\tau(G)$ consists of the positive numbers recorded in parts (i)-(viii) of Proposition 3.3. Then we observe that 1 and $(q^2+1)(q^4-1)$ are the only odd numbers

of $\tau(G)$, and so Lemma 2.8 implies that $m_2(G) \in \mathcal{A}_2$. In order to prove part (ii), let us suppose that $r > 1$ is a prime divisor of q^2+1. By Lemma 2.8, we have that $(r, m_r(G)) = 1$, and so $m_r(G) \in \mathcal{A}_9$. Similarly, if $r > 1$ is a prime divisor of q^2-1, we apply Lemma 2.8 and conclude that $(r, m_r(G)) = 1$, and hence

$$m_r(G) \in \mathcal{A}_4 \cup \mathcal{A}_5,$$

as desired in part (iii). □

In what follows, for a positive integer i, let $\mathbf{f}(i)$ be the number of elements of order r in G such that r is a multiple of i. Since $m_r(G)$ is the number of elements of order r in G, we conclude that

$$\mathbf{f}(i) = \sum_{i|r} m_r(G).$$

Let also $\mathbf{f}_j(i)$ be the number of elements of order r in G such that r is a multiple of i and $m_r(G) \in \mathcal{A}_j$, for $j = 1, \ldots, 9$, that is to say,

$$\mathbf{f}_j(i) = \sum_{\substack{i|r \\ m_r(G)\in\mathcal{A}_j}} m_r(G).$$

For each possible r, the number $m_r(G)$ of elements of order r in G belongs to exactly one of $\mathcal{A}_j$ with $j = 1, \ldots, 9$, and so

$$\mathbf{f}(i) = \sum_{i|r} m_r(G) = \sum_{j=1}^{9} \sum_{\substack{i|r \\ m_r(G)\in\mathcal{A}_j}} m_r(G).$$

Therefore, $\mathbf{f}(i) = \sum_{j=1}^{9} \mathbf{f}_j(i)$. By Lemma 2.8, if $i \geqslant 3$, then

$$\mathbf{f}(i) = \sum_{j=3}^{9} \mathbf{f}_j(i).$$

Proposition 4.2 *Let $S := PSp_4(q)$ with $q = 2^f > 2$, and let G be a group such that $\tau(G) = \tau(S)$ and $|G| = |S|$. Then $\pi(q^2+1)$ and $\pi(2(q^2-1))$ are not in the same connected component of the prime graph $\Gamma(G)$ of G. In particular, $\Gamma(G)$ has at least two connected components.*

Proof — Suppose, conversely, that $\pi(q^2+1)$ and $\pi(2(q^2-1))$ are in the same connected component of $\Gamma(G)$. Since $\pi(G)$ is disjoint union of $\pi(q^2+1)$ and $\pi(2(q^2-1))$, it follows that there exist

$$p_1 \in \pi(q^2+1) \qquad \text{and} \qquad p_2 \in \pi(2(q^2-1))$$

such that $p_1p_2 \in \omega(G)$. Therefore, by Lemma 2.9, there exists positive integer r such that $\mathbf{f}(p_1) = r|G|/|P_1| \neq 0$, where $P_1 \in \mathrm{Syl}_{p_1}(G)$. Since the elements of $\mathcal{A}_9$ express in the form

$$\frac{1}{4}\varphi(i)q^4(q^2-1)^2$$

where $1 \neq i \mid q^2+1$, and by Lemma 3.4, we obtain that $4 \mid \varphi(i)$. Moreover, Proposition 4.1 implies that there is a positive integer r' such that $\mathbf{f}_9(p_1) = q^4(q^2-1)^2r'$. Thus

$$\mathbf{f}(p_1) - \mathbf{f}_9(p_1) = \sum_{k=3}^{8} \mathbf{f}_k(p_1).$$

If $\sum_{k=3}^{8} \mathbf{f}_k(p_1) \neq 0$, then q^2+1 divides

$$\sum_{k=3}^{8} \mathbf{f}_k(p_1) = q^4(q^2-1)^2[r(q^2+1)/|P_1| - r'],$$

and so $q^2+1 < r(q^2+1)/|P_1|$. This implies that $|G| < \mathbf{f}(p_1)$, which is impossible. Therefore,

$$\sum_{k=3}^{8} \mathbf{f}_k(p_1) = 0,$$

or equivalently, $\mathbf{f}(p_1) = \mathbf{f}_9(p_1)$. Thus, $m_{p_1p_2}(G) \in \mathcal{A}_9$, and hence

$$\mathbf{f}_9(p_2) = q^4(q^2-1)^2s \neq 0,$$

for some positive integer s.

Since p_2 is a prime divisor of $2(q^2-1)$ and q is a power of 2, it follows that $p_2 = 2$ or $p_2 \in \pi(q^2-1)$. We now discuss these two possible cases:

(1) Let $p_2 = 2$. Then Proposition 4.1 implies that $m_{p_2}(G) \in \mathcal{A}_2$, and so $\mathbf{f}(p_2) \neq 0$. By Lemma 2.9, there exists a positive integer t such that $\mathbf{f}(p_2) = (q^4-1)(q^2-1)t$. Thus

$$\mathbf{f}(p_2) = \sum_{k=2}^{8} \mathbf{f}_k(p_2) + \mathbf{f}_9(p_2).$$

Since $\sum_{k=2}^{8} \mathbf{f}_k(p_2) = (q^2+1)u$, for some positive integer u, we have that

$$(q^2+1)\big((q^2-1)^2t - u\big) = q^4(q^2-1)^2s.$$

Thus

$$q^4(q^2-1)^2 \mid (q^2-1)^2t - u.$$

Therefore,

$$|G| = q^4(q^2-1)^2(q^2+1) < (q^2+1)(q^2-1)^2t \leqslant \mathbf{f}(p_2),$$

and hence $|G| < \mathbf{f}(p_2)$, which is a contradiction.

(2) Let $p_2 \in \pi(q^2-1)$. Hence, by Proposition 4.1, $m_{p_2}(G) \in \mathcal{A}_4 \cup \mathcal{A}_5$. Then $\mathbf{f}_4(p_2) + \mathbf{f}_5(p_2) \neq 0$. It follows from Lemma 2.9 that

$$\mathbf{f}(p_2) = t|G|/|P_2| \neq 0,$$

for some positive integer t and Sylow p_2-subgroup P_2 of G. Thus

$$\mathbf{f}(p_2) = \sum_{k=3}^{8} \mathbf{f}_k(p_2) + \mathbf{f}_9(p_2).$$

Note that $\sum_{k=3}^{8} \mathbf{f}_k(p_2) = (q^2+1)u$, for some positive integer u. Then

$$(q^2+1)\big(\tfrac{q^4(q^2-1)^2}{|P_2|}t - u\big) = q^4(q^2-1)^2s,$$

for some positive integer s. Therefore, $(q^2+1) \mid s$, and hence

$$|G| = q^4(q^2-1)^2(q^2+1) \leqslant q^4(q^2-1)^2s = \mathbf{f}_9(p_2) < \mathbf{f}(p_2),$$

that is to say, $|G| < \mathbf{f}(p_2)$, which is a contradiction. □

Proposition 4.3 *Let* $S := PSp_4(q)$ *with* $q = 2^f > 2$. *If* G *is a group such that* $\tau(G) = \tau(S)$ *and* $|G| = |S|$, *then we have that* G *has a normal series* $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ *such that* H *and* G/K *are* $\pi_1(G)$*-groups,* K/H *is a non-abelian simple group,* H *is a nilpotent group,* $|G/K|$ *divides* $|Out(K/H)|$, *and* $t(K/H) \geqslant t(G)$. *Moreover, any odd component of* G *is also an odd component of* K/H.

Proof — By Lemma 2.3 and Proposition 4.2, it suffices to show G is neither a Frobenius group, nor a 2-Frobenius group. Let first G be a Frobenius group with kernel K and complement H. Then Lemma 2.1 implies that $\pi(H)$ and $\pi(K)$ are the connected components of $\Gamma(G)$. By Proposition 4.2, $\pi(q^2+1)$ and $\pi(2(q^2-1)$ must be the connected components of $\Gamma(G)$, and so

$$|H| = q^2 + 1 \qquad \text{and} \qquad |K| = q^4(q^2-1)^2,$$

or

$$|H| = q^4(q^2-1)^2 \qquad \text{and} \qquad |K| = q^2 + 1.$$

However, both cases cannot occur as $|H|$ does not divide $|K|-1$. Let now G be a 2-Frobenius group. Then by Lemma 2.2, there exists normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that G/H and K are Frobenius groups with kernels K/H and H, respectively. Moreover,

$$\pi_1(G) = \pi(H) \cup \pi(G/K) \qquad \text{and} \qquad \pi_2(G) = \pi(K/H).$$

Applying Proposition 4.2, we conclude that $|H|$ divides $q^4(q^2-1)^2$ and $|K/H| = q^2+1$. Since G/H is a Frobenius group with kernel K/H, it follows that $|G/K|$ divides $|K/H|-1$, and so $|G/K|$ divides q^2. Hence, we obtain that $q^2(q^2-1)^2$ is a divisor of $|H|$. This implies that the prime graph of $\Gamma(H)$ is complete because H is nilpotent, and so by Proposition 4.2, $\pi(q^2+1)$ and $\pi(2(q^2-1))$ are connected components of the graph $\Gamma(G)$. Thus $oc(G) = oc(S)$. We apply Lemma 2.10 and conclude that $G \simeq S$, and hence S is a 2-Frobenius group which is a contradiction. This completes the proof. □

4.1 Proof of Theorem 1.1

Let $S := PSp_4(q)$ be a projective symplectic simple group, with $q = 2^f$. If G is a group with $\tau(G) = \tau(S)$ and $|G| = |S|$, then Proposition 4.3

implies that G has a normal series $1 \trianglelefteq H \trianglelefteq K \trianglelefteq G$ such that H and G/K are π_1-groups, K/H is a non-abelian simple group, H is a nilpotent group, $|G/K|$ divides $|\mathrm{Out}(K/H)|$, and $t(K/H) \geqslant t(G)$. Moreover, any odd component of G is also an odd component of K/H. It also follows from Proposition 4.2 that q^2+1 is an odd order component of G.

Since $t(K/H) \geqslant t(G) \geqslant 2$, if K/H has two connected components, then G has exactly two connected components, and hence q^2+1 is the odd order component of K/H. If K/H has more than two connected components, then by Proposition 4.2, we know that q^2+1 is an odd order component of G, and so it is equal to an odd order component of K/H or a product of some of odd order components of K/H. Since K/H is a non-abelian simple group with $t(K/H) \geqslant t(G) \geqslant 2$, the group K/H is isomorphic to one of the simple groups listed in [11, 17]. For convenience, we record the odd order components of some non-abelian finite simple groups in Table 2.

Table 2: The odd order components of some non-abelian finite simple groups with at least two components.

Group	Conditions	Odd order components
Alt_n	$n = p, p+1, p+2$, p odd prime	$p, p-2$
$\mathrm{PSL}_p(q')$	p odd prime, $(p,q') \neq (3,2),(3,4)$	$(q'^p-1)/[(q'-1)(p,q'-1)]$
$\mathrm{PSL}_{p+1}(q')$	p odd prime, $q'-1 \mid p \pm 1$	$(q'^p-1)/(q'-1)$
$\mathrm{PSL}_3(2)$		$3,7$
$\mathrm{PSL}_3(4)$		$3^2,5,7$
$\mathrm{PSL}_2(q')$	q' even	$q'\pm 1$
$\mathrm{PSL}_2(q')$	$q' \equiv \pm 1 \pmod 4$	$q', (q'\mp 1)/2$
$\mathrm{PSU}_p(q')$	p odd prime	$(q'^p+1)/[(q'+1)(p,q'+1))]$
$\mathrm{PSU}_{p+1}(q')$	p odd prime, $q'+1 \mid p+1$, $(p,q') \neq (3,2),(5,2)$	$(q'^p+1)/(q'+1)$
$\mathrm{PSU}_4(2)$		5
$\mathrm{PSU}_6(2)$		7, 11
$\mathrm{PSp}_{2m}(q')$	$m = p$ prime, $q' = 2,3$	$(q'^p-1)/(2,q'-1)$
$\mathrm{PSp}_{2m}(q')$	$m = 2^t \geqslant 2$	$(q'^m+1)/(2,q'-1)$
$\mathrm{P}\Omega_{2m+1}(q')$	$m = 2^t \geqslant 4$	$(q'^m+1)/2$
$\mathrm{P}\Omega_{2m+1}(3)$	m odd prime	$(3^m-1)/2$
$\mathrm{P}\Omega^+_{2m}(q')$	$m \geqslant 5$ odd prime, $q' = 2,3,5$	$(q'^m-1)/(q'-1)$
$\mathrm{P}\Omega^+_{2m+2}(3)$	m odd prime	$(3^m-1)/2$
$\mathrm{P}\Omega^-_{2m}(q')$	$m = 2^t \geqslant 4$	$(q'^m+1)/(2,q'-1)$
$\mathrm{P}\Omega^-_{2m}(3)$	$2^t+1 \neq m \geqslant 5$ odd	$(3^m+1)/4$
$\mathrm{P}\Omega^-_{2m}(3)$	$5 \leqslant m = 2^t+1$ not prime	$(3^{m-1}+1)/2$
$\mathrm{P}\Omega^-_{2m}(3)$	$5 \leqslant m = 2^t+1$ odd prime	$(3^{m-1}+1)/2, (3^m+1)/4$
$\mathrm{P}\Omega^-_{2m+2}(2)$	$m \neq 2^t-1$ odd prime	2^m-1
$\mathrm{P}\Omega^-_{2m+2}(2)$	$m = 2^t-1$ odd prime	$2^{m-1}+1, 2^m+1.$
${}^2\mathrm{B}_2(q')$	$q' = 2^{2t+1} \geqslant 8$ even	$q'-1, q' \pm \sqrt{2q'}+1$
$\mathrm{F}_4(q')$		$q'^4+1, q'^4-q'^2+1$

In what follows, we discuss the possibilities for the factor group K/H

and the proof of Theorem 1.1 follows immediately from the following lemmas.

Lemma 4.4 *The group* K/H *cannot be isomorphic to an alternating group, the Tits group* ${}^2F_4(2)'$ *or a sporadic simple group.*

Proof — If K/H is isomorphic to Alt_n with $n \geqslant 7$, then by Table 2, we have that $n = p$, $p+1$ or $p+2$. As noted above, q^2+1 is an odd order component or a product of some odd order components of K/H. Thus q^2+1 is p, $p-2$ or $p(p-2)$. If $q^2+1 = p$ or $p-2$, then

$$q^2 - 3 = p - 4 \qquad \text{or} \qquad q^2 + 3 = p,$$

respectively. So $q^2 \mp 3$ divides $|G|$ and this contradicts Lemma 2.12(v). If $q^2+1 = p(p-2)$, then

$$(p-1-q)(p-1+q) = 2,$$

which is impossible. If $K/H \simeq \mathrm{Alt}_n$, where $n = 5, 6$, then $q^2+1 = 3, 5$ or 15 which leads to no suitable solution for q. Therefore, K/H cannot be isomorphic to an alternating group. Similarly, the case where K/H is the Tits group or a sporadic simple group can be ruled out. □

Lemma 4.5 *The group* K/H *cannot be isomorphic to a finite simple exceptional group.*

Proof — By Table 2, the group K/H is isomorphic to one of the simple groups ${}^2B_2(q')$ with

$$q' = 2^{2t+1} \geqslant 8$$

the groups ${}^3D_4(q')$, $G_2(q')$, ${}^2G_2(q')$ with

$$q' = 3^{2t+1} \geqslant 27,$$

the groups $F_4(q')$, ${}^2F_4(q')$ with

$$q' = 2^{2t+1} \geqslant 8,$$

and $E_6^{\pm}(q')$, $E_6^{-}(2)$, $E_7(2)$, $E_7(3)$ and $E_8(q')$. Recall that q^2+1 is an odd order component or a product of some order components of K/H.

We easily see that K/H cannot be isomorphic to ${}^2E_6(2)$, $E_7(2)$ or $E_7(3)$ as if q^2+1 has to be equal to one of the following numbers:

$$\begin{aligned} {}^2E_6(2): &\quad 13, 17, 19, 13\cdot 17, 13\cdot 19, 17\cdot 19, 13\cdot 17\cdot 19,\\ E_7(2): &\quad 73, 127, 73\cdot 127,\\ E_7(3): &\quad 757, 1093, 757\cdot 1093. \end{aligned}$$

Thus, the only case that can occur is the one in which $K/H \simeq {}^2E_6(2)$ when $q = 4$. However, in this case, $|{}^2E_6(2)|$ must divide $|PSp_4(4)|$, which is a contradiction.

Suppose that K/H is isomorphic to one of the groups listed in the first column of Table 3. Then q^2+1 is equal to one of the polynomials recorded in the third column of the same table. But such an equality contradicts the fact that q is a power of 2.

Suppose that K/H is isomorphic to a Suzuki group ${}^2B_2(q')$. Then the odd order components of K/H are

$$q'-1 \qquad \text{or} \qquad q' \pm \sqrt{2q'}+1$$

by Table 2. Therefore, q^2+1 is equal to

$$\begin{gathered} q'-1,\ q' \pm \sqrt{2q'}+1,\ {q'}^2+1,\ (q'-1)(q' \pm \sqrt{2q'}+1)\\ \text{or} \qquad (q'-1)({q'}^2+1). \end{gathered}$$

If $q^2+1 \neq {q'}^2+1$, then we conclude that q is not a power of 2, which is a contradiction. Thus $q^2+1 = {q'}^2+1$, and so $q = q'$. Clearly, every two vertices r and s of $\Gamma(K/H)$ with

$$r \in \pi(q' - \sqrt{2q'}+1) \qquad \text{and} \qquad s \in \pi(q' + \sqrt{2q'}+1)$$

are disconnect, and hence they are also disconnected in $\Gamma(G)$. Therefore the Sylow s-subgroup of G acts fixed point freely on $m_r(G)$. This implies that $q' + \sqrt{2q'}+1 \mid m_r(G)$. On the other hand, it follows from Lemma 4.1 that $m_r(G) \in \mathcal{A}_9$. Therefore, $q' + \sqrt{2q'}+1$ divides

$$\varphi(r)q^4(q^2-1)^2/4 = \varphi(r){q'}^4({q'}^2-1)^2/4$$

and hence $q' + \sqrt{2q'}+1$ divides $\varphi(r)$, where $r \in \pi(q' - \sqrt{2q'}+1)$, which is a contradiction.

Suppose that K/H is isomorphic to $F_4(q')$. Then by Table 2, the odd order components of K/H is

$$q'^4+1 \qquad \text{or} \qquad q'^4-q'^2+1,$$

and so q^2+1 is

$$q'^4+1,\ q'^4-q'^2+1 \qquad \text{or} \qquad q'^8-q'^6+2q'^4-q'^2+1.$$

If $q^2+1=q'^4-q'^2+1$ or $q'^8-q'^6+2q'^4-q'^2+1$, then

$$q^2=q'^4-q'^2 \qquad \text{or} \qquad q'^8-q'^6+2q'^4-q'^2,$$

which is a contradiction as q is a power 2. Thus $q^2+1=q'^4+1$, and so $q^{12}=q'^{24}$. Since q'^{24} divides $|K/H|$, so does $|G|$, and hence the 2-part of $|G|$ is at least q^{12}, which is a contradiction.

Suppose that K/H is isomorphic to $E_6^{\pm}(q')$ with $q'\equiv\pm1 \pmod 3$. Then $q^2+1=(q'^6\pm q'^3+1)/3$, and so $3q^2+2=q'^6\pm q'^3$. Note that $q'^6\pm q'^3$ divides $|K/H|$, so does $|G|$. Thus $3q^2+2$ divides $|G|$ which is impossible by Lemma 2.12. □

Table 3: Some polynomials in Lemma 4.5.

Group	Conditions	Polynomials
$G_2(q')$		$\Phi_3(q')$, $\Phi_6(q')$, $\Phi_3(q'^2)$
$E_6(q')=E_6^+(q')$	$q'\overset{3}{\equiv}0,-1$	$\Phi_9(q')$
$E_8(q')$		$\Phi_{15}(q')$, $\Phi_{20}(q')$, $\Phi_{24}(q')$, $\Phi_{30}(q')$, $\Phi_{15}(q')\Phi_{20}(q')$, $\Phi_{15}(q')\Phi_{24}(q')$, $\Phi_{15}(q')\Phi_{30}(q')$, $\Phi_{20}(q')\Phi_{24}(q')$, $\Phi_{20}(q')\Phi_{30}(q')$, $\Phi_{24}(q')\Phi_{30}(q')$, $\Phi_{15}(q')\Phi_{20}(q')\Phi_{24}(q')$, $\Phi_{15}(q')\Phi_{20}(q')\Phi_{30}(q')$, $\Phi_{15}(q')\Phi_{24}(q')\Phi_{30}(q')$, $\Phi_{20}(q')\Phi_{24}(q')\Phi_{30}(q')$, $\Phi_{15}(q')\Phi_{20}(q')\Phi_{24}(q')\Phi_{30}(q')$
${}^3D_4(q')$		$\Phi_{12}(q')$
${}^2G_2(q')$		$\Phi_6^+(q')$, $\Phi_6^-(q')$, $\Phi_6(q')$
${}^2F_4(q')$		$\Phi_{12}^+(q')$,$\Phi_{12}^-(q')$,$\Phi_{12}(q')$
${}^2E_6(q')=E_6^-(q')$	$q'\overset{3}{\equiv}0,1$	$\Phi_{18}(q')$

Note: $\Phi_6^{\pm}(q'):=q'\pm\sqrt{3q'}+1$ and $\Phi_{12}^{\pm}(q'):=q'^2\pm q'\sqrt{2q'}+q'\pm\sqrt{2q'}+1$.

Lemma 4.6 *If* K/H *is isomorphic to* $PSL_n(q')$ *with* $(n,q')\neq(2,2),(2,3)$, *then* $(n,q')=(2,q^2)$ *with* $q=2^f$, *and hence* $G\simeq S$.

Proof — By Table 2, we have to consider the following possibilities:

(1) $n \geqslant 5$ is prime. It follows from Table 2 that

$$q^2+1 = (q'^n-1)/[(q'-1)(n, q'-1)].$$

Suppose that q' is even. If $q' = 2$, then $q^2+1 = q'^n-1$, and so $2^{2f-1}+1 = 2^{n-1}$, which is a contradiction. Thus $q' > 2$, and hence

$$q'^n-1 = (q'-1)(n, q'-1)(q^2+1) > q^2+1.$$

Then $q'^{2n} > q^4$. Let us observe that the 2-part of $|K/H|$ is $q'^{\frac{n(n-1)}{2}}$ and the 2-part of G is q^4. Since $|K/H|$ divides $|G|$, we have that

$$n(n-1)/2 < 2n$$

which is valid only for $n < 5$, which is a contradiction. If q' is odd, then $2q^2 < q'^n-1$, and so $q'^{\frac{n(n-1)}{2}}$ divides $(q-1)^2$ or $(q+1)^2$ as $|K/H|$ is a divisor of G. Thus

$$2q^2 < q'^n-1 \leqslant q'^{\frac{n(n-1)}{2}} \leqslant (q+1)^2,$$

and so $2q^2 < (q+1)^2$. Therefore, $q < 3$, which is a contradiction.

(2) $n = p+1$, where p is an odd prime and $q'-1 \mid p \pm 1$. In this case,

$$q^2+1 = (q'^p-1)/(q'-1),$$

that is to say,

$$q^2 = q'^{p-1}+q'^{p-2}+\ldots+q' = q'(q'^{p-1}-1)/(q'-1).$$

Thus $p = 2$ and $q' = q^2$ which is a contradiction.

(3) $n = 3$. If $q' = 2, 4$, then by Table 2, q^2+1 is equal to one of

$$15,\ 21,\ 27,\ 35,\ 45,\ 63,\ 105,\ 135,\ 189,\ 315 \text{ and } 945$$

which leads to no possible solution for q. Therefore, $q' \neq 2, 4$, and hence $q^2+1 = (q'^2+q'+1)/(3, q'-1)$. Thus

$$q'(q'+1) = q^2 \qquad \text{or} \qquad 3q^2+2.$$

Since q is a power of 2, we deduce that $q'(q'+1) = 3q^2+2$. More-

over, $3q^2+2$ divides $|K/H|$, and so does $|G|$, and this contradicts Lemma 2.12.

(4) $n=2$ and q' is odd and $q' \equiv \pm 1 \pmod 4$. In this case, we must have

$$q^2+1 = q', \ (q' \mp 1)/2 \qquad \text{or} \qquad q'(q' \mp 1)/2.$$

If $q^2+1=q'$, then $q^2+2 = q'+1$ which is a divisor of $|K/H|$. This implies that q^2+2 divides $|G|$, and so by Lemma 2.12-(ii) and the fact that $q>2$, we conclude that $q=4$, and hence

$$q' = q^2+1 = 17.$$

It follows that $K/H \simeq PSL_2(17)$ and $S = PSp_4(4)$. Since $|G/K|$ divides $|Out(K/H)| = 2$, we deduce that $|H| = 2^a \cdot 5^2$, where $a = 3,4$. Since H is nilpotent, it follows that the Sylow 5-subgroup of H is normal in G, and so $m_5(H) = m_5(G)$. Therefore $m_5(G) = m_5(H)$ divides $|H|$, but $|H| \mid 400$, and this contradicts Proposition 4.1.

If $q^2+1 = (q' \mp 1)/2$, then

$$q' = 2q^2+3 \qquad \text{or} \qquad 2q^2+1.$$

Thus $2q^2+3$ or $2q^2+1$ is a divisor of $|G|$, which is impossible by Lemma 2.12 as $q \neq 2$. Similarly, if $q^2+1 = q'(q' \mp 1)/2$, then

$$2q^2 = (q' \pm 1)(q' \mp 2)$$

which is a contradiction because q is even and $q' \mp 2$ is odd.

(5) $n=2$ and q' is even. Then q^2+1 is equal to $q'-1, q'+1, q'^2-1$. We first observe that q^2+1 cannot be equal to $q'-1$ or q'^2-1 as if not $q^2+2 = q'$ or q'^2, respectively, which is impossible. Thus

$$q^2+1 = q'+1,$$

and hence $q^2 = q'$. Note that $\pi(q^2+1)$ is a connected component of $\Gamma(K/H)$. Then Proposition 4.2, $\pi(q^2+1)$ is a connected component of $\Gamma(G)$. We show that $\pi(2(q^2-1))$ is the other connected component of $\Gamma(G)$. If $|H|$ is coprime to q^2-1, then q^2-1 divides $|G/K|$ which is a divisor of

$$|Out(K/H)| = \log_2 q' = 2\log_2 q,$$

and so $q^2-1 \mid 2\log_2 q$, which is impossible. It follows that there is

a prime $p \in \pi(q^2-1)$ such that $p \mid |H|$. On the other hand, we have that $2 \in \pi(H)$. Since H is a nilpotent group, we have $2p \in \omega(H)$, and this implies that $2p \in \omega(G)$. Therefore, $\pi(2(q^2-1))$ is the other connected component of $\Gamma(G)$. This, together with the fact that $|G| = |S|$, implies that $oc(G) = oc(S)$, and hence by Lemma 2.10, we conclude that $G \simeq S$. □

Lemma 4.7 *The group* K/H *cannot be isomorphic to* $PSU_n(q')$.

Proof — According to Table 2, we have the following possibilities:
(1) $n = 4, 6$ and $q' = 2$. Then q^2+1 is equal to one of 5, 7, 11, and 77 which leads to no possible solution for q.
(2) $n = p+1$, or $n = p$ and $(q'+1, p) = 1$. Then

$$q^2+1 = (q'^p+1)/(q'+1)$$

and so

$$q^2 = q'^{p-1} - q'^{p-2} + \ldots - q',$$

which is a contradiction as q is a power 2.
(3) $n = p$ and $(q'+1, p) = p$. Then

$$q^2+1 = \frac{q'^p+1}{(q'+1)\cdot p}.$$

If q' is even, then we have that the 2-part $|K/H|_2 = q'^{\frac{p(p-1)}{2}}$ of K/H divides $|G|_2 = q^4$. It follows from $q^2+1 = \frac{q'^p+1}{(q'+1)\cdot p}$ that $q^4 < q'^{2p}$, and so

$$q'^{\frac{p(p-1)}{2}} \leqslant q^4 < q'^{2p}.$$

Then $\frac{p(p-1)}{2} < 2p$. This inequality is true only for $p = 3$ in which case we have that $3q^2 = (q'+1)(q'-2)$, which is impossible. Suppose now that q' is odd. Since $|K/H|$ is a divisor of $|G|$, it follows that $q'^{\frac{p(p-1)}{2}} \mid (q \pm 1)^2$. On the other hand, $q^2+1 = \frac{q'^p+1}{(q'+1)\cdot p}$ implies that $2q^2 < q'^p + 1$. If $p > 3$, then

$$2q^2 < q'^p + 1 \leqslant q'^{\frac{p(p-1)}{2}} < (q \pm 1)^2,$$

that is to say, $2q^2 < (q \pm 1)^2$ which implies that $q < 3$, which is a contradiction. If $p = 3$, then $q^2+1 = \frac{q'^3+1}{3(q'+1)}$, and so $3q^2+2$ divides $|G|$,

and so Lemma 2.12-(iv) implies that $q = 4$. Thus,

$$\frac{q'^3 + 1}{3(q' + 1)} = q^2 + 1 = 17,$$

and so $q'^2 - q' - 50 = 0$, which has no possible solution. □

Lemma 4.8 *If* K/H *is isomorphic to* $PSp_{2m}(q')$, *then* $(m, q') = (2, q)$ *with* $q = 2^f$, *and hence* $G \simeq S$.

Proof — By Table 2, we have the following possibilities:
(1) $m = p$ is prime, and $q' = 2, 3$. Then $q^2 + 1 = (q'^p - 1)/(2, q' - 1)$, and so $2q^2 = 3^p - 3$ or $q^2 + 2 = 2^p$, which is a contradiction because q is a power 2.
(2) $m = 2^t \geqslant 2$. Then

$$q^2 + 1 = (q'^m + 1)/(2, q' - 1).$$

If q' is odd, then $2q^2 + 1 = q'^m$, and hence, by Lemma 2.11, we have $m = 1$, which is a contradiction. Therefore, q' is even, and hence $q^2 + 1 = q'^m + 1$ which implies that $q^{2m} = q'^{m^2}$. Since $|K/H|$ divides $|G|$, we have that $q'^{m^2} \mid q^4$, and so $q^{2m} \mid q^4$. Thus $m = 2$, and hence $q = q'$. Therefore $K/H \simeq PSp_4(q)$, and since $|K/H| = |G|$, we conclude that $H = 1$, that is to say, $G = K \simeq PSp_4(q)$. □

Lemma 4.9 *The group* K/H *cannot be isomorphic to*

$$P\Omega_n(q') \qquad \textit{and} \qquad P\Omega_n^{\pm}(q').$$

Proof — Assume to the contrary that K/H is isomorphic to $P\Omega_n(q')$ or $P\Omega_n^{\pm}(q')$. We have one of the following possibilities by Table 2:
(1) K/H is isomorphic to $P\Omega_{2m+1}(q')$ with $m = 2^t$ for $t \geqslant 2$. Then

$$q^2 + 1 = (q'^m + 1)/2,$$

and so $2q^2 + 1 = q'^m$, which is impossible by Lemma 2.11.
(2) K/H is isomorphic to $P\Omega_{2m+1}(3)$ with m prime. Then

$$q^2 + 1 = (3^m - 1)/2$$

and so $2q^2 = 3^m - 3$ which is a contradiction because q is a power of 2.

(3) K/H is isomorphic to $P\Omega^+_{2m}(q')$, where $m \geqslant 5$ is an odd prime and $q' = 2, 3, 5$. Then

$$q^2 + 1 = (q'^m - 1)/(q' - 1).$$

Thus

$$q^2 = q'^{m-1} + q'^{m-2} + \ldots + 1,$$

which is a contradiction.

(4) K/H is isomorphic to $P\Omega^+_{2m+2}(q')$, where m is an odd prime and $q' = 3$. Then $q^2 + 1 = (3^m - 1)/2$. Thus $2q^2 = 3^m - 3$, which is a contradiction.

(5) K/H is isomorphic to $P\Omega^-_{2m}(q')$, where $m = 2^t \geqslant 4$. If q' is odd, then

$$q^2 + 1 = (q'^m + 1)/2$$

and so $2q^2 + 1 = q'^m$. Thus $2q^2 + 1$ divides $|K/H|$, and hence $2q^2 + 1$ divides $|G|$, which is a contradiction. If q' is even, then

$$q^2 + 1 = q'^m + 1,$$

and so $q^{2(m-1)} = q'^{m(m-1)}$. Since $|K/H|$ divides $|G|$, we deduce that $q^{2(m-1)} \mid q^4$. This implies that $m - 1 \mid 2$, and so $m = 2$ or 3 which contradicts the fact that $m = 2^t \geqslant 4$.

(6) K/H is isomorphic to $P\Omega^-_{2m}(3)$, where $2^t + 1 \neq m \geqslant 5$ is odd. Then $q^2 + 1 = (3^m + 1)/4$, and so $4q^2 = 3^m - 3$, which is a contradiction as q is a power 2.

(7) K/H is isomorphic to $P\Omega^-_{2m}(3)$, where $5 \leqslant m = 2^t + 1$ is not prime. Then

$$q^2 + 1 = (3^{m-1} + 1)/2$$

and so $2q^2 + 1 = 3^{m-1}$. By Lemma 2.11, $m = 3$, which is impossible as $m \geqslant 5$.

(8) K/H is isomorphic to $P\Omega^-_{2m}(3)$, where $5 \leqslant m = 2^t + 1$ is an odd prime. Then $q^2 + 1$ equals to

$$(3^{m-1} + 1)/2, \ (3^m + 1)/4 \qquad \text{or} \qquad (3^{m-1} + 1)(3^m + 1)/8.$$

If $q^2+1=(3^{m-1}+1)/2$, then

$$2q^2+1=3^{m-1},$$

and since $3^{m-1} \mid |K/H|$, it follows that $2q^2+1 \mid |G|$, and so by Lemma 2.12, we conclude that $q=2$, which is a contradiction. Now, if $q^2+1=(3^m+1)/4$, then

$$4q^2=3^m-3,$$

which is a contradiction because q is a power 2. If

$$q^2+1=\Big(\frac{3^{m-1}+1}{2}\Big)\Big(\frac{3^m+1}{4}\Big).$$

Since $3^{m(m-1)}$ divides $|K/H|$, it follows that $3^{m(m-1)} \mid |G|$, and so

$$3^{m(m-1)} \mid (q\pm 1)^2.$$

Then $3^{m(m-1)/2} \leqslant q+1$, and so

$$3^{m(m-1)/2} \leqslant q+1 < q^2+1 \leqslant \Big(\frac{3^{m-1}+1}{2}\Big)\Big(\frac{3^m+1}{4}\Big) \leqslant 3^{2m},$$

that is to say, $m(m-1)/2 \leqslant 2m$. This is true only if $m=5$ in which case

$$q^2+1=\Big(\frac{3^4+1}{2}\Big)\Big(\frac{3^5+1}{4}\Big)=2501,$$

and so $q=50$, which is a contradiction.

(9) K/H is isomorphic to $P\Omega^-_{2m+2}(2)$, where $m \neq 2^t-1$ prime. Then $q^2+1=2^m-1$, which is a contradiction as q is a power of 2.

(10) K/H is isomorphic to $P\Omega^-_{2m}(2)$, where $m=p+1$ with p odd prime. Then

$$q^2+1=2^p+1,\ 2^{p+1}+1 \qquad \text{or} \qquad (2^p+1)(2^{p+1}+1).$$

If $q^2+1=2^p+1$, then $p=2f$, which is a contradiction because p is odd prime. If $q^2+1=2^{p+1}+1$, then

$$2^{4f}=2^{2p+2}.$$

Since $|K/H|$ divides $|G|$ and the 2-part of $|G|$ is $q^4 = 2^{4f}$, we deduce that $2^{p(p+1)} \mid 2^{4f}$. This implies that $p \leqslant 2$, which is a contradiction. If $q^2 + 1 = (2^p + 1)(2^{p+1} + 1)$, then

$$q^2 = 2^{2p+1} + 2^p + 2^{p+1},$$

which is a contradiction because q is a power 2. □

Proof of Theorem 1.1 — The proof immediately follows from Proposition 4.3 and Lemmas 4.4-4.9. □

Proof of Corollary 1.2 — Since G and S are of the same type, it follows that $\tau(G) = \tau(S)$ and $|G| = |S|$, and hence the result immediately follows from Theorem 1.1. □

Acknowledgements

The authors would like to thank the anonymous referees for helpful comments and suggestions. They confirm that there are no known conflicts of interest associated with this publication. The authors have no competing interests to declare that are relevant to the content of this article and they confirm that availability of data and material is not applicable. The list of authors is in alphabetic order and all authors contributed equally to this manuscript.

REFERENCES

[1] S.H. Alavi – A. Daneshkhah – H. Parvizi Mosaed: "On quantitative structure of small Ree groups", *Comm. Algebra* 45 (2017), 4099–4108.

[2] S.H. Alavi – A. Daneshkhah – H. Parvizi Mosaed: "Finite groups of the same type as Suzuki groups", *Int. J. Group Theory* 8 (2019), 35–42.

[3] R.W. Carter: "Simple Groups of Lie Type", *Wiley*, London (1972).

[4] G. Chen: "On structure of Frobenius and 2-Frobenius group", *J. Southwest China Normal Univ.* 20 (1995), 485–487.

[5] J.H. Conway – R.T. Curtis – S.P. Norton – R.A. Parker – R.A. Wilson: "ATLAS of Finite Groups", *Oxford University Press*, Eynsham (1985).

[6] P. Crescenzo: "A Diophantine equation which arises in the theory of finite groups", *Adv. Math.* 17 (1975), 25–29.

[7] H. Enomoto: "The characters of the finite symplectic group $Sp(4, q)$, $q = 2^f$", *Osaka Math. J.* 9 (1972), 75–94.

[8] D. Gorenstein: "Finite Groups", *Chelsea*, New York (1980).

[9] M. Hall: "The Theory of Groups", *Macmillan*, New York (1959).

[10] E.I. Khukhro – V.D. Mazurov: "The Kourovka Notebook: Unsolved Problems in Group Theory" (2014); *ArXiv*:1401.0300.

[11] A.S. Kondrat′ev: "On prime graph components of finite simple groups", *Mat. Sb.* 180 (1989), 787–797.

[12] V.D. Mazurov – M.C. Su – C.P. Chao: "Recognition of the finite simple groups $L_3(2^m)$ and $U_3(2^m)$ from the orders of their elements", *Algebra Log.* 39 (2000), 567–585.

[13] J.S. Rose: "A Course on Group Theory", *Dover*, New York (1994).

[14] C. Shao – W. Shi – Q. Jiang: "Characterization of simple K_4-groups", *Front. Math. China* 3 (2008), 355–370.

[15] A.V. Vasil′ev – M.A. Grechkoseeva – V.D. Mazurov: "Characterization of finite simple groups by spectrum and order", *Algebra Logika* 48 (2009), 685–728.

[16] L. Weisner: "On the number of elements of a group which have a power in a given conjugate set", *Bull. Amer. Math. Soc.* 31 (1925), 492–496.

[17] J.S. Williams: "Prime graph components of finite groups", *J. Algebra* 69 (1981), 487–513.

[18] L. Zhang – W. Shi: "A new characterization of the group $S_4(q)$ using a graph of noncommutativity", *Sibirsk. Mat. Zh.* 50 (2009), 669–679.

Seyed Hassan Alavi (*corresponding author*)
Department of Mathematics
Faculty of Science
Bu-Ali Sina University
Hamedan, Iran
e-mail: alavi.s.hassan@basu.ac.ir

Ashraf Daneshkhah
Department of Mathematics
Faculty of Science
Bu-Ali Sina University
Hamedan, Iran
e-mail: adanesh@basu.ac.ir

Hosein Parvizi Mosaed
Alvand Institute of Higher Education
Hamedan, Iran
e-mail: h.parvizi.mosaed@alvand.ac.ir

Instructions for Authors

The submission of a paper to Advances in Group Theory and Applications, which will happen via the online submission system at www.advgrouptheory.com/journal, implies that it is not been previously published (in any language) and that it is not under evaluation for publication elsewhere; moreover, its submission must be approved by all coauthors (if any). If the paper is accepted for publication, the authors are assumed to have transferred the copyright to AGTA.
In the preparation of a paper for submission, the author should respect the following rules:

(a) the paper must be written in English

(b) the first page of the paper must contain the title (chosen in a concise but understandable way), the name and the family name of each author (with indication of the corresponding author), a short abstract describing the purpose of the research and (eventually) the main results, the 2010 Mathematics Subject Classification codes and the keywords

(c) references must be numbered consecutively (in arabic numbers) and alphabetically named by the first author's family name; the list of references cannot contain entries which are not cited in the text

(d) acknowledgments, financial supports and dedications must be put at the end of the text, before the list of references

(e) footnotes should not be used

(f) the affiliation and the complete address of each author (including e-mail) must be put at the end of the paper

After acceptance of a paper, the author(s) will be required to prepare their work using the LaTex style of the journal, that can be downloaded at

www.advgrouptheory.com/journal/AGTA_style.zip

together with an example of final compilation.

The journal *Advances in Group Theory and Applications* is a publication issued by the nonprofit association AGTA (advgrouptheory.com), with the aim of publishing high-quality research papers containing original and significant results in any topic of group theory and its applications. Papers are accepted after a rigorous peer-review process.

Advances in Group Theory and Applications is an open access journal, i.e. all accepted papers are freely available on the web site www.advgrouptheory.com/journal. There are no publication processing charges, since all costs associated with the publication and production are covered by the association AGTA.

AGTA wishes that the journal could be a reference point for all group theorists, and in particular for the young ones; to this aim the journal also contains a section of open problems.

Marco Trombetti **Editor in Chief**

Eli Aljadeff
Adolfo Ballester-Bolinches
Dikran Dikranjan
Montserrat Casals-Ruiz
Martyn R. Dixon
Eric Jespers
Lev Kazarin
Leonid A. Kurdachenko
Nadia Mazza
Vahagn Mikaelian
Pavel Shumyatsky
Alexander Skiba
Igor Subbotin
Frank O. Wagner

Paola Stefanelli **Managing Editor**