Quasigroups and Related Systems **31** (2023), 165 – 174

https://doi.org/10.56415/qrs.v31.12

The Ramsey number $R_4(3)$ is not solvable by group partition means

Chimere Stanley Anabanti

Abstract. The *Ramsey number* $R_n(3)$ is the smallest positive integer such that colouring the edges of a complete graph on $R_n(3)$ vertices in n colours forces the appearance of a monochromatic triangle. A lower bound on $R_n(3)$ is obtainable by partitioning the non-identity elements of a finite group into disjoint union of n symmetric product-free sets. Exact values of $R_n(3)$ are known for $n \leqslant 3$. The best known lower bound that $R_4(3) \geqslant 51$ was given by Chung. In 2006, Kramer gave a proof of over 100 pages that $R_4(3) \leqslant 62$. He then conjectured that $R_4(3) = 62$. We say that the Ramsey number $R_n(3)$ is *solvable by group partition means* if there is a finite group G such that $|G|+1 = R_n(3)$ and $G\setminus\{1\}$ can be partitioned as a union of n symmetric product-free sets. For $n \leqslant 3$, the Ramsey number $R_n(3)$ is solvable by group partition means. Some authors believe that $R_4(3)$ not be solvable by a group partition approach. We prove this here. We also show that any finite group G whose size is divisible by 3 cannot enjoy $G\setminus\{1\}$ written as a disjoint union of its symmetric product-free sets. We conclude with a conjecture that $R_5(3) \geqslant 257$.

1. Introduction

Let G be a finite group, and S a non-empty subset of G. Then S is said to be *product-free* if $S \cap SS = \varnothing$. A *maximal product-free set* in G is a maximal by cardinality product-free set in G. Let $\lambda(G)$ denote the cardinality of a maximal product-free set in G. Suppose T is any product-free set in a finite group G. For $x_1 \in T$, define $x_1T := \{x_1x_2 | x_2 \in T\}$. As $|x_1T| = |T|$ and $T \cup x_1T \subseteq G$, we have that $2|T| \leqslant |G|$; so $|T| \leqslant \frac{|G|}{2}$. This shows that $\lambda(G) \leqslant \frac{|G|}{2}$; i.e., the size of a product-free set in a finite group G is at most half the size of G.

The value of $\lambda(G)$ is well-known when G is a finite abelian group, following the works of Diananda and Yap [9], as well as Green and Ruzsa [14]. On

2010 Mathematics Subject Classification: 20D60, 20P05, 05E15, 11B13.
Keywords: Ramsey numbers, product-free sets, groups, partition.

the other hand, the problem of determination of structures and sizes of maximal product-free sets in non-abelian groups is still open, although there has been great progress by many authors, including Kedlaya [17, 18] and Gowers [13]. An interested reader may also see [22, 23, 24, 12, 7, 6, 5, 1, 2, 4, 3] for works on maximal by inclusion product-free sets.

The *Ramsey number* $R_n(3)$ is the smallest positive integer such that colouring the edges of a complete graph on $R_n(3)$ vertices in n colours forces the appearance of a monochromatic triangle. Exact values of $R_n(3)$ are known for $n \leqslant 3$; for instance see [16]. The best known lower bound that $R_4(3) \geqslant 51$ was given by Chung [8] in 1973. Kramer [20], in 2006, after giving a proof of over 100 pages that $R_4(3) \leqslant 62$, conjectured that $R_4(3) = 62$. See also [10, 19].

A symmetric product-free set is a product-free set S such that $S = S^{-1}$. For a finite group G, it is known that if G^* (where $G^* = G \setminus \{1\}$) can be partitioned into disjoint union of m symmetric product-free sets (SPFS for short), then $R_m(3) \geqslant |G| + 1$. Examples by various authors show that the group partition approach gives a sharp lower bound that coincides with the exact value of $R_m(3)$ for $m \leqslant 3$. The main result of this paper is essentially folklore. Here, we show that the group partition approach cannot be used to improve the known lower bound of $R_4(3)$ to r for $52 \leqslant r \leqslant 62$; in particular, we demonstrate that $R_4(3)$ is not solvable by a group partition means. For the rest of this section, we give the following result.

Theorem 1.1. (Idea from [16, Theorem 1.1] and [24, pp. 247–248]) *If G is a finite group such that G^* can be partitioned into disjoint union of m symmetric product-free sets (where $m \geqslant 2$), then $R_m(3) \geqslant |G| + 1$.*

Proof. Suppose $G^* = S_1 \sqcup \cdots \sqcup S_m$ is a disjoint union of m symmetric product-free sets. We assign to the set S_i colour C_i for each $i \in \{1, \ldots, m\}$. Let $K_{|G|}$ be the complete graph on $|G|$ vertices: $v_1, v_2, \ldots, v_{|G|}$. [Note that the vertices of $K_{|G|}$ are the elements of G.] We m-colour $K_{|G|}$ as follows: colour the edge v_iv_j (from v_i to v_j) with colour C_k if $v_iv_j^{-1} \in S_k$. Since S_k is symmetric (i.e., $S_k = S_k^{-1}$), this induces a well-defined edge-colouring of the graph. Let v_a, v_b and v_c be any three vertices of $K_{|G|}$ and consider the triangle on these vertices. Suppose two of its edges say v_av_b and v_bv_c are coloured C_k. This means that $v_av_b^{-1}, v_bv_c^{-1} \in S_k$. Since S_k is product-free, we have that $(v_av_b^{-1})(v_bv_c^{-1}) = v_av_c^{-1} \notin S_k$. So v_av_c must be coloured C_l for $l \neq k$, and no monochromatic triangle is formed. Therefore $R_m(3) > |G|$. □

2. Main results

2.1 A group theoretic motivation

In 1955, Greenwood and Gleason [15] proved that

$$R_{n+1}(3) \leqslant (n+1)(R_n(3)-1)+2$$

for $n \geqslant 1$. This result of Greenwood and Gleason tells us that $R_2(3) \leqslant 6$ and $R_3(3) \leqslant 17$. Note that if $R_m(3) \leqslant k$, then Theorem 1.1 implies that for any group G with $|G| \geqslant k$, it is impossible to partition G^* into m symmetric product-free sets. Hence, if G^* is symmetric and product-free, then $|G| \leqslant 2$ (and clearly the only example is C_2), if G^* has a partition into two symmetric product-free sets, then $|G| \leqslant 5$, and if G^* has a partition into three symmetric product-free sets, then $|G| \leqslant 16$. It is then quick to check by hand that the only examples of groups G for which G^* has a partition into two symmetric product-free sets are $C_4, C_2 \times C_2$ and C_5.

We used GAP [11] to observe that there are only four groups G of order 16 such that G^* has a partition into three symmetric product-free sets. The groups are C_2^4, $C_4 \times C_4$, $(C_4 \times C_2) \rtimes C_2$ and $C_2 \times D_8$, with GAP IDs as $[16,14]$, $[16,2]$, $[16,3]$ and $[16,11]$ respectively. Each of them when combined with the result of Greenwood and Gleason tells us that $R_3(3) = 17$. The results for the two abelian cases (C_2^4 and $C_4 \times C_4$) are known in the literature; for instance, see [24].

G	An example of a partition of G^* into disjoint union of 3 symmetric product-free sets
$C_2^4 = \langle x_1, x_2, x_3, x_4 \mid x_i x_j = x_j x_i,\ x_i^2 = 1 \text{ for } 1 \leqslant i, j \leqslant 4 \rangle$	$\{x_1, x_2, x_3, x_4, x_1x_2x_3x_4\} \cup$ $\{x_1x_2, x_1x_3, x_2x_4, x_1x_2x_3, x_1x_2x_4\} \cup$ $\{x_1x_4, x_2x_3, x_3x_4, x_1x_3x_4, x_2x_3x_4\}$
$C_4 \times C_4 = \langle x, y \mid x^4 = 1 = y^4,\ xy = yx \rangle$	$\{x, x^3, y, y^3, x^2y^2\} \cup$ $\{x^2, xy, x^3y^3, x^2y, x^2y^3\} \cup$ $\{xy^3, x^3y, y^2, xy^2, x^3y^2\}$
$(C_4 \times C_2) \rtimes C_2 = \langle x, y \mid x^4 = 1 = y^2,\ (xyx)^2 = 1 = (yx^{-1})^4,\ (yxyx^{-1})^2 = 1 \rangle$	$\{y, x, x^3, (xy)^2, x^3yx\} \cup$ $\{yx, x^2, x^2y, x^3y, xyx\} \cup$ $\{x^2yx, xy, yxy, x(xy)^2, x^2(xy)^2\}$
$C_2 \times D_8 = \langle x, y, z \mid x^2 = 1,\ y^2 = 1, z^2 = 1,\ (zx)^2 = 1,\ (zy)^2 = 1,\ (yx)^4 = 1 \rangle$	$\{x, y, xz, (xy)^2, xyxz\} \cup$ $\{xy, z, yx, xyx, yz\} \cup$ $\{xyz, yxy, yxz, yxyz, (xy)^2z\}$

We now end this section with some GAP [11] programs that can be used to get the table above and investigate more groups.

Program A. This checks whether a set T is product-free

```
PFTest:=function(T) local x,y; for x in T do for y in T do
if x*y in T then return 1; fi; od; od; return 0; end;
```

Program B. This gives a partition of G^* into k product-free sets if such partition exists

```
PGk:=function(G,k) local LL, AA, g, P, p, PPk, PPkA, PPP;
LL:=List(G);; AA:=[];; for g in LL do if Order(g)>1 then Add(AA,g);
fi; od; AA:=Set(AA);; PPk:=PartitionsSet(AA,k);; PPkA:=[];;
for P in PPk do for p in P do if PFTest(p)=1 then Add(PPkA,P); fi;
od; od; PPkA:=Set(PPkA);; PPP:=Difference(PPk,PPkA);;
if Size(PPP)>0 then return PPP[1]; else return []; fi; end;
```

Program C. All groups G of order n such that G^* has a partition into k product-free sets

```
GGnk:=function(n,k) local M, MM, G, GG;
MM:=[];; GG:=AllSmallGroups(n);
for G in GG do M:=PGk(G,k); if Size(M)>0 then Add(MM,[IdGroup(G),M]);
fi; od; return MM; end;
```

2.2 $R_4(3)$ is not solvable by a group partition means

Recall that $51 \leqslant R_4(3) \leqslant 62$. We say a finite group G is *m-partitioned* if the non-identity elements of G can be partitioned into disjoint union of m symmetric product-free sets. A natural question is whether Chung's lower bound for $R_4(3)$ can be improved to r for $52 \leqslant r \leqslant 62$. We shall use an algorithmic approach to show that the group partition approach cannot be used to improve Chung's lower bound to r for $52 \leqslant r \leqslant 62$. We begin with Lemma 2.1 below.

Lemma 2.1. *If G is a finite group such that G^* has a partition into m symmetric product-free sets (where $m \geqslant 2$), then $|G|$ is not divisible by 3.*

Proof. Let G be a finite group such that $G^* = \bigcup_{i=1}^{m} S_i$, where $m \geqslant 2$ and each S_i is a symmetric product-free set in G. Suppose for contradiction that $|G|$ is divisible by 3. Then G has an element of order 3; say x. Without loss of generality, let $x \in S_1$. As S_1 is symmetric, $x^{-1} \in S_1$. But $x^{-1} = x^2$, a contradiction; as S_1 is product-free. Therefore $|G|$ is not divisible by 3. □

We used GAP [11] to observe that there are 56 groups whose sizes are from 51 up to 61; in particular, there are 1, 5, 1, 15, 2, 13, 2, 2, 1, 13 and 1 group(s) of orders 51, 52, 53, 54, 55, 56, 57, 58, 59, 60 and 61 respectively. In the light of Lemma 2.1, we discard 31 groups from the list, and only work with 25 groups; those whose order is one of $52, 53, 55, 56, 58, 59$ and 61.

Lemma 2.1 tells us that the group partition approach into symmetric product-free sets cannot be used to check whether $R_4(3)$ is 52. The next result (Theorem 2.2) shows that the group partition approach into SPFS cannot be used to prove the conjecture of Kramer that $R_4(3) = 62$.

Theorem 2.2. *The group of order* 61 *cannot be* 4*-partitioned.*

Proof. Suppose we 4-colour the edges of K_{61}. Choose any vertex v_0 of K_{61}. Suppose we edge join v_0 with each of the vertices $v_1, v_2, \ldots, v_m$ respectively. Consider the complete graph K_m on those m vertices. If we colour any edge in K_m with the first colour, then we force the appearance of a triangle in the first colour. So we only colour edges of K_m with any of the remaining three colours. As $R_3(3) = 17$, in order not to have a monochromatic triangle in K_m, we have that $m \leqslant 16$. This argument shows that the largest size of any symmetric product-free set involved in any 4-partition of C_{61} is 16.

The only possibilities of such partition is using SPFS of sizes 16, 16, 16 and 12 or SPFS of sizes 16, 16, 14 and 14. Hence, we only need to work with SPFS of sizes 12, 14 and 16 in our programs for such partition. Using Program E below, we see that there are 27060, 13680 and 3975 symmetric product-free sets of sizes 12, 14 and 16 respectively in C_{61}. We then use Program F below to check for either four SPFS of sizes 16, 16, 16 and 12 whose size of their union is 60 or those of sizes 16, 16, 14 and 14 whose size of their union is 60, and found none. Therefore C_{61} cannot be 4-partitioned. □

Remark 2.3. The same reasoning used for the group of order 61 in the proof of Theorem 2.2 above shows that the maximum size of any of the symmetric product-free sets in a 4-partition of any of the groups we consider here is 16. We shall use this repeatedly in our computations.

Algorithm D. This gives all SPFS of respective sizes (up to 16) in a finite group G

1. For $x \in G$, if $o(x) > 2$, then select only one element from the pair $\{x, x^{-1}\}$. Let A be a collection of all the selected elements. (In this case, $|A| = \frac{|G|-1-|InvG|}{2}$, where $InvG$ is the set of all involutions in G.)

2. Form all subsets of A whose sizes are from 1 up to 8. Test for product-freeness of each subset of A of respective sizes, and make sets T_i consisting of product-free sets of size i for each $i \in \{1, \ldots, 8\}$.

3. Create a non-empty set U_i for each $i \in \{1, \ldots, 8\}$. For each set M in each T_i, if the union of M and M^{-1} is product-free, then add the union to U_i. Repeat

this for each $i \in \{1, \ldots, 8\}$. Let spf be the collection of all the U_i's; i.e., $spf := [U_1, U_2, \ldots, U_8]$, where each U_i consists of all symmetric product-free sets of size $2i$; not containing an involution.

4. Let $InvG$ be the set of all involutions in G. Take subsets of sizes 1 up to 16 of $InvG$. Test for product-freeness. Let $Ispf$ be the set of all such product-free sets of respective sizes. Let $sprf$ be an empty set. Check whether the union of any set in spf and $Ispf$ is product-free. Add all such union which are product-free of size less than 17 to $sprf$. Also, add all members of spf and $Ispf$ to $sprf$. Then $sprf$ is the set of all SPFS of respective sizes up to 16 in G when $|G|$ is even.

Remark 2.4.
1. We apply only steps 1, 2 and 3 if $|G|$ is odd, and all the steps 1, 2, 3 and 4 if $|G|$ is even.

2. The motivation for treating the sets of involutions separately is to reduce computational time; since we know that $\binom{|G|-1}{16} > \binom{\frac{|G|}{2}+3}{16}$, where $\frac{|G|}{2} + 3$ is the maximum number of involutions in the groups involved.

3. We used Algorithm above (instead of program) because the actual program spreads up to 3 pages of the manuscript. An interested reader can request a copy of the GAP program used. We call the function in Algorithm D, SPFS. It takes only one input which is a finite group of our choice.

Program E. This gives the number of SPFS of various sizes (up to 16) in G

```
SizeSPFS:=function(G) local S,A,i,a; S:=SPFS(G); A:=[];
for i in S do a:=Size(i); if a>0 then Add(A,[Size(i[1]),a]);
fi; od; return A; end;
```

An example of Program E above is given below.

```
gap> SizeSPFS(CyclicGroup(61));
[ [ 2, 30 ], [ 4, 405 ], [ 6, 3000 ], [ 8, 12285 ], [ 10, 26166 ],
[ 12, 27060 ], [ 14, 13680 ], [ 16, 3975 ]]
```

Program F. It decides if G^* can be partitioned into SPFS of sizes a, b, c and d

```
IsPartG:=function(G,a,b,c,d)
local S,Sa,Sb,Sc,Sd,i,j,k,l;
S:=SPFS(G); Sa:=S[a]; Sb:=S[b]; Sc:=S[c]; Sd:=S[d];
for i in Sa do for j in Sb do for k in Sc do for l in Sd do
if Size(Set(Union(i,j,k,l)))=Size(G)-1 then Print([i,j,k,l]); fi;
od; od; od; od; end;
```

The next in the sequel is to have an understanding of the number of iterations we will perform to check all the groups of orders among $52, 53, 55, 56, 58$ and 59.

Program G1. This tells us the iterations to perform for each group G of even order n

```
ExpMathEven:=function(n)
local A, i,j,k,l,B;
A:=[2..16];; B:=[];;
for i in A do for j in A do for k in A do for l in A do
if i<=j and j<=k and k<=l and i+j+k+l=n-1 then Add(B,[i,j,k,l]); fi;
od; od; od; od; return B; end;
```

Program G2. This tells us the iterations to perform for each group G of odd order n

```
ExpMathOdd:=function(n)
local A, i,j,k,l,B,C;
A:=[2..16];; C:=[];; B:=[];;
for i in A do if IsEvenInt(i) then Add(C,i); fi; od;
for i in C do for j in C do for k in C do for l in C do
if i<=j and j<=k and k<=l and i+j+k+l=n-1 then Add(B,[i,j,k,l]); fi;
od; od; od; od; return B; end;
```

We now give some examples of Programs G1 and G2. |small

```
gap> [Size(ExpMathOdd(53)), ExpMathOdd(53)];
[ 9, [ [ 4, 16, 16, 16 ], [ 6, 14, 16, 16 ], [ 8, 12, 16, 16 ],
[ 8, 14, 14, 16 ], [ 10, 10, 16, 16 ], [ 10, 12, 14, 16 ],
[ 10, 14, 14, 14 ], [ 12, 12, 12, 16 ], [ 12, 12, 14, 14 ] ] ]
gap> [Size(ExpMathEven(58)), ExpMathEven(58)];
[ 11, [ [ 9, 16, 16, 16 ], [ 10, 15, 16, 16 ], [ 11, 14, 16, 16 ],
[ 11, 15, 15, 16 ], [ 12, 13, 16, 16 ], [ 12, 14, 15, 16 ],
[ 12, 15, 15, 15 ], [ 13, 13, 15, 16 ], [ 13, 14, 14, 16 ],
[ 13, 14, 15, 15 ], [ 14, 14, 14, 15 ] ] ]
```

The example above tells us that there are 9 (respectively 11) ways of choosing $[a, b, c, d]$ to be used in Program F, as well as what the possibilities are when $|G| = 53$ (respectively $|G| = 58$).

We now check the total possibilities across all groups of order n, where $n \in \{52, 53, 55, 56, 58, 59\}$.

```
A:=[52, 53, 55, 56, 58, 59];; B:=[];; for n in A do
if IsEvenInt(n) then Add(B,NrSmallGroups(n)*Size(ExpMathEven(n)));
else Add(B,NrSmallGroups(n)*Size(ExpMathOdd(n))); fi; od;
gap> B;
```

```
[ 195, 9, 12, 234, 22, 3 ]
gap> Sum(B);
475
```

We have checked all the 475 trials, and did not find such partition of any of the groups. By Lemma 2.1 and Theorem 2.2 therefore, no group of order from 51 up to 61 can be 4-partitioned.

2.3 Concluding remarks

In this paper, we have shown that, while $R_1(3)$, $R_2(3)$ and $R_3(3)$ are solvable by group partition means, the folklore that $R_4(3)$ is not solvable by group partition means is indeed true. It will be interesting to know which Ramsey numbers $R_k(3)$ are solvable by group partition means for $k \geqslant 5$. An interested reader may see [21, pp. 42–43] for bounds on $R_k(3)$ for some $k \geqslant 5$. It is known that $162 \leqslant R_5(3) \leqslant 307$, $538 \leqslant R_6(3) \leqslant 1838$ and $1682 \leqslant R_7(3) \leqslant 12861$. We anticipate that $R_5(3)$ is solvable by group partition means. We are motivated by our computer searches to conjecture that $R_5(3) \geqslant 257$, and that the lower bound can be obtained by partitioning the non-identity elements of a non-cyclic group of order 256 into a disjoint union of five SPFS.

Acknowledgment. The author is grateful to the anonymous reviewers for their useful comments.

References

[1] **C.S. Anabanti**, *On filled soluble groups*, Commun. Algebra, **46** (2018), 4914 – 4917.

[2] **C.S. Anabanti**, *Three questions of Bertram on locally maximal sum-free sets*, Applicable Algebra in Engineering, Communication and Computing, **30** (2019), 127–134.

[3] **C.S. Anabanti**, *On the three questions of Bertram on locally maximal sum-free sets*, Quaestiones Math., **44** (2021), 301 – 305.

[4] **C.S. Anabanti**, *Groups containing locally maximal product-free sets of size* 4, Algebra Discrete Math., **31** (2021), no.2, 167 – 194.

[5] **C.S. Anabanti, G. Erskine and S.B. Hart**, *Groups whose locally maximal product-free sets are complete*, Australasian J. Combin., **71**(2018), 544 – 563.

[6] **C.S. Anabanti and S.B. Hart**, *Groups containing small locally maximal product-free sets*, Intern. J. Combinatorics,, vol. 2016, Article ID 8939182 (2016), 5pp.

[7] **C.S. Anabanti and S.B. Hart**, *On a conjecture of Street and Whitehead on locally maximal product-free sets*, Australasian J. Combin., **63** (2015), 385 – 398.

[8] **F.R.K. Chung**, *On the Ramsey numbers* $N(3,3,\ldots,3)$, Disc. Math., **5** (1973), 317 – 321.

[9] **P.H. Diananda and H.P. Yap**, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad., **1** (1969), 1 – 5.

[10] **S. Fettes, R. Kramer and S. Radziszowski**, *An upper bound of* 62 *on the classical Ramsey number* $R(3,3,3,3)$, Ars Combin., **72** (2004), 41 – 63.

[11] **The GAP Group**, *GAP – Groups, Algorithms, and Programming*, Version 4.12.1, 2022. (http://www.gap-system.org)

[12] **M. Giudici and S. Hart**, *Small maximal sum-free sets*, The Electronic J. Combin., **16** (2009), 17 pp.

[13] **W.T. Gowers**, *Quasirandom groups*, Combinatorics, Probability and Computing, **17** (2008), 363 – 387.

[14] **B. Green and I.Z. Ruzsa**, *Sum-free sets in abelian groups*, Israel J. Math., **147** (2005), 157 – 188.

[15] **R.E. Greenwood and A.M. Gleason**, *Combinatorial relations and chromatic graphs*, Canadian J. Math., **7** (1955), 1 – 7.

[16] **R. Hill and R.W. Irving**, *On group paritions associated with lower bounds for symmetric Ramsey numbers*, European J. Combin., **3** (1982), 35 – 50.

[17] **K.S. Kedlaya**, *Large product-free subsets of finite groups*, J. Combin. Theory, Series A, **77** (1997), 339 – 343.

[18] **K.S. Kedlaya**, *Product-free subsets of groups*, Amer. Math. Monthly, **105** (1998), 900 – 906.

[19] **R.L. Kramer**, *The classical Ramsey number* $R(3,3,3,3;2)$ *is no greater than* 62, manuscript, Iowa State University (1994).

[20] **R.L. Kramer**, *The classical Ramsey number* $R(3,3,3,3)$ *is no greater than* 62, https://www.researchgate.net/publication/270703142, preprint (2006), 1 – 108.

[21] **S.P. Radziszowski**, *Small Ramsey numbers*, The Electronic J. Combin., (2021), DS1.16, 116 pages.

[22] **A.P. Street and E.G. Whitehead Jr.**, *Group Ramsey Theory*, J. Combin. Theory, Series A **17** (1974), 219 – 226.

[23] **A.P. Street and E.G. Whitehead Jr.**, *Sum-free sets, difference sets and cyclotomy*, Combinatorial Math., Lecture Notes in Math., **403**(1974), 109–124.

[24] **W.D. Wallis, A.P. Street and J. Seberry Wallis**, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Math. **292** (1972).

Received February 23, 2023
E-mails: chimere.anabanti@up.ac.za, chimere.anabanti@unn.edu.ng

Quasigroups and Related Systems **31** (2023), 175 – 184

https://doi.org/10.56415/qrs.v31.13

A note on comaximal graph and maximal topology on multiplication le-modules

Sachin Ballal, Sadashiv Puranik and Vilas Kharat

Abstract. In this article, the co-maximal graph $\Gamma(M)$ on le-modules M has been introduced and studied. The graph $\Gamma(M)$ consists of vertices as elements of ${}_RM$ and two distinct elements n, m of $\Gamma(M)$ are adjacent if and only if $Rn + Rm = e$. We have established a connection between the co-maximal graph and the maximal topology on $Max(M)$ in the case of multiplication le-modules. Also, the Beck's conjecture is settled for $\Gamma(M)$ which does not contain an infinite clique.

1. Introduction

An algebraic structure known as a le-module was introduced and explored by A.K. Bhuniya and M. Kumbhakar [3, 4, 5]. They were inspired to study abstract submodule theory, in particular le-module by the study of abstract ideal theory, particularly multiplicative lattices and lattice modules.

Sharma and Bhatwadekar [10] introduced a graph on elements of commutative ring R with unity by taking vertices as elements of R with two distinct vertices x and y are adjacent if and only if the addition of ideals generated by x and y is the whole ring R. They have shown that a commutative ring R is finite if and only if the graph associated with it is finitely colorable. Also, it is proved that the chromatic number of the graph is the sum of the number of maximal ideals and the number of units of R.

H.R. Maimani and others [6] studied a subgraph of a graph introduced in [10]. They studied the connectedness and diameter of the subgraph.

K. Samai [9] studied a subgraph $\Gamma_2(R)$ of $\Gamma(R)$ introduced in [10] with non-unit elements of R as a vertex set and obtained ring, graph as well

2010 Mathematics Subject Classification: 06E10, 06E99, 06F99,06B23, 06F25

Keywords: Prime submodule element, radical element, Zariski topology, complete lattices, le-modules

This research work is an outcome of the project supported by the Institute of Eminence (UoH-I0E-RC5-22-021), University of Hyderabad.

as the topological properties. Also, investigated the diameter, girth, cycles and dominating sets of a subgraph $\Gamma_2(R)$.

In [8], Puranik and others studied an associated graph $\Gamma(M)$ of a le-module ${}_RM$ with all non-zero proper submodule elements of M as vertices. Any two distinct vertices n and m are adjacent if and only if their sum is equal to e, the largest element of ${}_RM$. Also, the Beck's conjecture for $\Gamma(M)$ is established for coatomic le-modules.

In Section 1 we have recalled the definition of le-module and many concepts from le-modules as well as graph theory. In Section 2, we have settled Beck's conjecture for $\Gamma(M)$ which does not contain an infinite clique. Characterized the subgraph $\Gamma_3(M)$ to be complete bipartite if the number of maximal elements is exactly 2 and shown that it is n-partite if the number of maximal elements of M is exactly n. Also, prove that the subgraph $\Gamma_3(M)$ of $\Gamma(M)$ is connected with diameter is at most 3. In Section 3, we have proven that the existence of disjoint closed sets in the maximal spectrum ensures the existence of adjacent elements in the co-maximal graph and vice-versa. Also, it is shown that if the maximal spectrum of multiplication le-modules is Hausdorff, then the diameter of the subgraphs $\Gamma_2(M)$ and $\Gamma_3(M)$ are at least 3.

Definition 1.1. An *le-semigroup* $(M, +, \leqslant, e)$ is a commutative monoid with the zero element 0_M and is a complete lattice with the greatest element e, that satisfies $m + (\vee_{i\in I} m_i) = \vee_{i\in I}(m + m_i)$. Then M is called an *le-module* over a commutative ring R with unity 1_R if there is a mapping $: R \times M \to M$ satisfying:

1. $r(m_1 + m_2) = rm_1 + rm_2$
2. $(r_1 + r_2)m \leqslant r_1m + r_2m$
3. $(r_1r_2)m = r_1(r_2m)$
4. $1_Rm = m$; $0_Rm = r0_M = 0_M$
5. $r(\vee_{i\in I} m_i) = \vee_{i\in I}(rm_i)$ holds for all $r, r_i \in R$, $m, m_i \in M$ and $i \in I$ (I is an indexed set).

An element $n \in M$ is said to be a *submodule element* if $n+n, rn \leqslant n$ for all $r \in R$. The set of all submodule elements of M is denoted by $Sub(M)$.

Observe that if $n, m \in Sub(M)$ then $n + m \in Sub(M)$, $rn \in Sub(M)$, $n \wedge m \in Sub(M)$ and $n + n = n$. Let M be an le-module, $n \in M$ and

I be an ideal in R. Then $In = \vee\{\sum_{i=0}^{k} r_i n : k \in \mathbb{N}; r_i \in I\}$. If for each $n \in Sub(M)$, $n = Ie$ for some ideal I of R, then the le-module M is known as a *multiplication le-module*. An element $m \in Sub(M)$ is said to be *maximal* if $m < n$ for some $n \in Sub(M)$ implies $n = e$. The set of all maximal elements of M is denoted by $Max(M)$. If $l \in Sub(M)$ and $n \in M$, then $(l : n) = \{r \in R : rn \leqslant l\}$ is an ideal in R. If $t \in Sub(M)$ then $Ann(t) = \{r \in R : rt = 0\}$. Note that $Ann(t)$ is an ideal in R. We define radical of an le-module M as $Rad(M) = \wedge_{m \in Max(M)} m$.

A *graph* G is the pair $(V(G); E(G))$, where $V(G)$ is the vertex set and $E(G)$ is the edge set. The *degree* of a vertex n is denoted by $deg(n)$ and is equal to the number of edges incident on n. In G, the *distance* between two distinct vertices n and m, denoted by $d(n; m)$ is the length of the shortest path between n and m. The *diameter* of a graph G is given by $diam(G) = sup\{d(n; m)|n, m \in V(G)\}$. Graph G is called *connected*, if there is a path between any two vertices of G. The length of the shortest cycle in G is called the *girth* of G. A graph is called *complete* if each pair of vertices in G is adjacent. A *complete* $r - partite$ graph is one in which each vertex is joined to every other vertex not in the same subset. A *clique* of a graph is its maximal complete subgraph and the number of vertices in the largest clique of a graph G, denoted by $\omega(G)$, is called the *clique number of* G. The minimum n for which a graph G is n-colorable is called the *chromatic number* of G, and is denoted by $\chi(G)$.

Proposition 1.2. (cf. [5]) *Let M be an le-module and I be an ideal of R. Then $In \in Sub(M)$ for all $n \in M$ and Rn is the smallest element of $Sub(M)$ covering n i.e. if $l \in Sub(M)$ and $n \leqslant l$, then $n \leqslant Rn \leqslant l$.*

In particular, $Rn = n$ for all $n \in Sub(M)$.

Proposition 1.3. *Let M be a multiplication le-module. If $m \in Max(M)$ and $n_1, n_2, \ldots, n_m \in Sub(M)$ such that $(\wedge_\lambda n_\lambda) \leqslant m$, then there exist some λ such that $n_\lambda \leqslant m$.*

2. Comaximal graph of multiplication le-modules

Let M be an le-module and let $\Gamma(M)$ consist of vertices as elements of M and two distinct elements n, m of $\Gamma(M)$ are adjacent if and only if $Rn + Rm = e$. We denote $U(M) = \{n \in M | Rn = e\}$.

The following theorem shows that the Beck's conjecture is true for $\Gamma(M)$ which does not contain infinite clique.

Theorem 2.4. *Let M be an le-module. If $\Gamma(M)$ does not contain infinite clique, then $\chi(\Gamma(M)) = \omega(\Gamma(M)) = t + s$, where $t = |U(M)|$ and $s = |Max(M)|$.*

Proof. Note that $|U(M)|$ and $|Max(M)|$ are finite, otherwise $\Gamma(M)$ contains infinite clique. Suppose that $U(M) = \{n_1, n_2, \ldots, n_t\}$ and $Max(M) = \{m_1, m_2, \ldots, m_s\}$. Then $C = U(M) \cup Max(M)$ is a clique in $\Gamma(M)$. Then $\chi(\Gamma(M)) \geq t + s$. Let $V_1 = \{m \in M | m \leqslant m_1\}$ and for $i = 1, 2, \ldots, s; V_i = \{m \in M | m \leqslant m_i$ but $m \not\leqslant m_j$ for $j = 1, 2, \ldots, i-1\}$. Then $M = U(M) \cup V_1 \cup V_2 \cup \ldots \cup V_s$ is a disjoint union of sets. Define $f : M \to \{1, 2, \ldots, t+s\}$ as $f(n_i) = i$ where $n_i \in U(M)$ and $f(v_j) = t + j$ where $v_j \in V_j$ for $j = 1, 2, \ldots, s$. If $k_1, k_2 \in M$ with $k_1 \neq k_2$ and $Rk_1 + Rk_2 = e$ implies $f(k_1) \neq f(k_2)$. Thus the map f gives colouring implies $\chi(\Gamma(M)) = t + s$. □

In [10] Sharma and Bhatwadekar have shown that, every ring without infinite clique is finite. But the following example illustrates that even an infinite le-module can have a finite clique.

Example 2.5. Let $M = \{a_i | i \in \mathbb{N}\} \cup \{b_i | i \in \mathbb{N}\} \cup \{0, e\}$ is a le-module over $\mathbb{Z}_2$ with $+$ as $a_i + a_j = a_1, b_i + b_j = b_1$ and $a_i + b_j = e$ and scalar multiplication is $0x = 0$ and $1x = x$ for all $x \in M$. By Proposition 1.2, each a_i is adjacent to each b_j, because $Ra_i + Rb_j = a_1 + b_1 = e$.

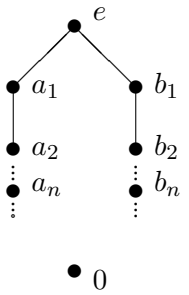

Figure 1 : Lattice of M.

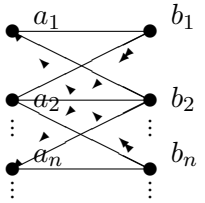

Figure 2 : $\Gamma(M)$ – Comaximal graph of M.

Here $Sub(M) = \{a_1, b_1\}$ and we have only 2 vertices clique because a_i is not adjacent to a_j and b_i is not adjacent to b_j for any $i, j \in \mathbb{N}$.

We consider subgraph $\Gamma_2(M)$ with the vertex set $\{n \in M | n \notin U(M)\}$.

Theorem 2.6. *The graph with the vertex set $U(M)$ is complete. Moreover, $m \leqslant Rad(M)$ if and only if $deg_{\Gamma_2}(m) = 0$, where $deg_{\Gamma_2}(m)$ is a degree of M in a subgraph $\Gamma_2(M)$.*

Proof. 1. Let $m_1, m_2 \in U(M)$. Then $Rm_1 = e$ and $Rm_2 = e$. Consequently, $Rm_1 + Rm_2 = e$ and hence every pair of elements of $U(M)$ are adjacent.

2. Let $m \leqslant Rad(M)$, which implies $m \leqslant m_i$ for all $m_i \in Max(M)$. If $deg_{\Gamma_2}(m) \neq 0$, then there exists $n \in \Gamma_2(M)$ such that $Rn + Rm = e$. Now, there exists $m_j \in Max(M)$ such that $n \leqslant m_j$. Therefore by Proposition 1.2, we have $Rn + Rm \leqslant Rm_j + Rm_j = m_j + m_j = m_j \neq e$, a contradiction. Hence $deg_{\Gamma_2}(m) = 0$.

Conversely, suppose that $deg_{\Gamma_2}(m) = 0$. If $m \nleqslant Rad(M)$, then there exists $m_j \in Max(M)$ such that $m \nleqslant m_j$. Thus $Rm + m_j = Rm + Rm_j = e$, a contradiction to $deg_{\Gamma_2}(m) = 0$. □

We consider subgraph $\Gamma_3(M)$ with the vertex set

$$\{n \in M | n \notin U(M) \text{ and } n \nleqslant Rad(M)\}.$$

Theorem 2.7. *Let M be an le-module. Then $\Gamma_3(M)$ is a complete bipartite if and only if $|Max(M)| = 2$.*

Proof. Let $Max(M) = \{m_1, m_2\}$. Then the vertex set of $\Gamma_3(M) = V_1 \cup V_2$, where

$$V_1 = \{m | m \leqslant m_1 \text{ and } m \nleqslant m_2\} \text{ and } V_2 = \{m | m \leqslant m_2 \text{ and } m \nleqslant m_1\}.$$

Now for $n_1 \in V_1$ and $n_2 \in V_2$ we have $Rn_1 \nleqslant m_2$ and $Rn_2 \nleqslant m_1$. Hence $Rn_i \leqslant Rn_1 + Rn_2 \nleqslant m_i$ for $i = 1, 2$. But $Rn_1 + Rn_2 \in Sub(M)$ and which implies $Rn_1 + Rn_2 = e$. Therefore $\Gamma_3(M)$ is a complete bipartite.

Conversely, suppose that $\Gamma_3(M)$ is a complete bipartite with V_1 and V_2 are two parts. Let $m_1 = \vee\{v_{i_1} | v_{i_1} \in V_1\}$ and $m_2 = \vee\{v_{i_2} | v_{i_2} \in V_2\}$. We first prove that $m_1 \in V_1$. Otherwise, we have following two cases: Let $v_{i_1}, v_{j_1} \in V_1$.

1. If $v_{i_1} \vee v_{j_1} \in U(M)$, then $R(v_{i_1} \vee v_{j_1}) = e$. Now $v_{i_1} \vee v_{j_1} \leqslant v_{i_1} + v_{j_1}$ implies $R(v_{i_1} \vee v_{j_1}) \leqslant R(v_{i_1} + v_{j_1}) = R(v_{i_1}) + R(v_{j_1})$. Therefore $R(v_{i_1} \vee v_{j_1}) = e$ implies $R(v_{i_1}) + R(v_{j_1}) = e$, a contradiction.

2. If $v_{i_1} \vee v_{j_1} \in V_2$, then $R(v_{i_1}) + R(v_{i_1} \vee v_{j_1}) = e$. Now $v_{i_1} \vee v_{j_1} \leqslant v_{i_1} + v_{j_1}$ implies $R(v_{i_1} \vee v_{j_1}) \leqslant R(v_{i_1} + v_{j_1}) = R(v_{i_1}) + R(v_{j_1})$. Therefore $R(v_{i_1}) + R(v_{i_1} \vee v_{j_1}) = e$ implies $R(v_{i_1}) + R(v_{i_1}) + R(v_{j_1}) = e$. Therefore, $R(v_{i_1}) + R(v_{j_1}) = e$, a contradiction.

Hence $m_1 \in V_1$ and similarly we have $m_2 \in V_2$. Since $m_1 \in V_1$, we have $Rm_1 \neq e$ and also $Rm_1 + Rv_{i_1} = Rm_1 \neq e$ implies $Rm_1 \notin V_2$. Similarly we have $Rm_2 \notin V_1$. If $n \in Max(M)$ then $n \leqslant m_1$ or $n \leqslant m_2$. Otherwise $Rn + Rm_1 = e$ and $Rn + Rm_2 = e$, which is a contradiction to $\Gamma_3(M)$ is a complete bipartite. □

Proposition 2.8. *Let M be an le-module and $n > 1$.*

1. *If $|Max(M)| = n < \infty$, then $\Gamma_3(M)$ is an n-partite.*
2. *If $\Gamma_3(M)$ is an n-partite, then $|Max(M)| \leqslant n$ and if $\Gamma_3(M)$ is not an $(n-1)$-partite, then $|Max(M)| = n$.*

Proof. 1. Let $Max(M) = \{m_1, m_2, \ldots, m_n\}$. Take $V_1 = \{m \in \Gamma_3(M) | m \leqslant m_1\}$ and $V_i = \{m \in \Gamma_3(M) | m \leqslant m_i$ and $m \nleqslant m_j$ for $j = 1, 2, \ldots, i-1\}$ for $i = 2, 3, \ldots, n$. If $m_{i_1}, m_{i_2} \in V_i$, then $Rm_{i_1} + Rm_{i_2} \leqslant Rm_i + Rm_i = m_i + m_i = m_i < e$. Thus m_{i_1} and m_{i_2} are not adjacent. Similarly no two elements of V_1 are adjacent. Therefore, $\Gamma_3(M)$ is n-partite.

2. Suppose that $\Gamma_3(M)$ is $n-$*partite* graph. Let $V_1, V_2, \ldots, V_n$ be the n parts of vertices of $\Gamma_3(M)$. Suppose that $|Max(M)| > n$. Let $\{m_1, m_2, \ldots, m_{n+1}\} \subseteq Max(M)$. Let $t_i \leqslant m_i$ but $t_i \nleqslant m_j$ for $i \neq j$. Note that $Rt_i + Rt_j \geqslant t_i, t_j$. If $Rt_i + Rt_j \neq e$ then $Rt_i + Rt_j \leqslant m_k$ for some $m_k \in Max(M)$. Therefore $t_i, t_j \leqslant m_k$, a contradiction. Hence $Rt_i + Rt_j = e$. Therefore $\{t_1, t_2, \ldots, t_{n+1}\}$ is a clique in $\Gamma_3(M)$. As we have $V_1, V_2, \ldots V_n$ are n parts of vertices of $\Gamma_3(M)$ and $\{t_1, t_2, \ldots, t_{n+1}\}$ is a clique in $\Gamma_3(M)$, by the Pigeonhole principle two $t_i \in V_i$ for some i, a contradiction. Therefore $|Max(M)| \leqslant n$.

Now, if $\Gamma_3(M)$ is not $(n-1)$-partite and if $|Max(M)| = s < n$, then by part (1), $\Gamma_3(M)$ is s-partite, a contradiction. Hence $|Max(M)| = n$. □

Theorem 2.9. *Let M be a multiplication le-module and $|Max(M)| \geqslant 2$. If $\Gamma_3(M)$ is a complete n-partite, then $n = 2$.*

Proof. Suppose that $\Gamma_3(M)$ is a complete n-partite. For $m_1, m_2 \in Max(M)$, let $V_1 = \{m \in \Gamma_3(M) | m \leqslant m_1$ and $m \nleqslant m_2\}$ and $V_2 = \{m \in \Gamma_3(M) | m \leqslant m_2$ and $m \nleqslant m_1\}$. Observe that the elements of V_i are not adjacent for $i = 1, 2$ and every element of V_1 is adjacent to each element of V_2. Since $\Gamma_3(M)$ is a complete n-partite graph implies V_1 and V_2 are two parts of $\Gamma_3(M)$. Now, we claim that $Rad(M) = m_1 \wedge m_2$. Suppose that $Rad(M) < m \leqslant m_1 \wedge m_2$ for some $m \in M$. This implies m is not adjacent to any element of V_1 and of V_2. This is contradiction to $\Gamma_3(M)$ is complete n-partite. Therefore $Rad(M) = m_1 \wedge m_2$ and for any $m_3 \in Max(M)$, we have $m_1 \wedge m_2 \wedge m_3 = m_1 \wedge m_2$. Which implies $m_1 \wedge m_2 \leqslant m_3$. Then by Propostion 1.3, we have $m_1 \leqslant m_3$ or $m_2 \leqslant m_3$. As $m_1, m_2, m_3 \in Max(M)$, implies $m_1 = m_3$ or $m_2 = m_3$ and therefore $|Max(M)| = 2$. Hence by Theorem 2.7, $\Gamma_3(M)$ is a complete bipartite. □

Theorem 2.10. *If M is a multiplication le-module, then $\Gamma_3(M)$ is connected and $diam(\Gamma_3(M)) \leqslant 3$.*

Proof. Let $n, l \in \Gamma_3(M)$. Then we consider the following two cases:

1. Suppose that $n \wedge l \nleqslant Rad(M)$. Then $n \wedge l \nleqslant m$ for some $m \in Max(M)$. Hence, $R(n \wedge l) + Rm = e$ and which implies $Rn + Rm = e$ and $Rl + Rm = e$. Therefore $n - m - l$ is a path and so $d(n, m) \leqslant 2$.

2. Suppose that $n \wedge l \leqslant Rad(M)$. Let $S_n = \{m \in Max(M) | n \leqslant m\}$ and $S_l = \{m \in Max(M) | l \leqslant m\}$ implies $Max(M) = S_n \cup S_l$. Because if there exist $m_0 \in Max(M)$ such that $m_0 \notin S_m$ and $m_0 \notin S_n$, then $n \wedge l \leqslant m_0$ implies $Rn \wedge Rl \leqslant m_0$. Suppose n is adjacent to t in $\Gamma_2(M)$. Then $t \nleqslant Rad(M)$. If $n \leqslant m_1$, then $t \nleqslant m_1$ and so $t \leqslant m_2$ for some $m_2 \in S_l - S_n$. If $Rt \wedge Rl \leqslant Rad(M)$ then by Proposition 1.3, $Rt \leqslant Rad(M)$ or $Rl \leqslant Rad(M)$. But $l \nleqslant m$ for some $m \in S_n$ implies $Rl \nleqslant m$ for some $m \in S_n$ and therefore$Rl \nleqslant Rad(M)$. Similarly $Rt \nleqslant Rad(M)$. Hence $Rt \wedge Rl \nleqslant Rad(M)$. Therefore by Case(i), there exists a path between Rt and Rl and $d(Rt, Rl) \leqslant 2$. Suppose $Rt - m - Rl$ is a path for some $m \in M$ and hence $n - Rt - m - l$ is a path between n and l. Consequently, $d(n, l) \leqslant 3$. □

3. Maximal spectrum and comaximal graph

In [5], Kumbhakar and Bhuniya, studied the Zariski topology on le-modules. They have defined $V(n) = \{p \in Spec(M) | n \leqslant p\}$ and $V^*(n) = \{p \in Spec(M) | (p : e) \subseteq (n : e)\}$ for $n \in Sub(M)$. If M is a multiplication le-module, then $\{V(n) | n \in Sub(M)\}$ forms the Zarisky topology of closed sets on the prime spectrum $Spec(M)$.

Throughout this section, M denotes a multiplication le-module unless otherwise stated.

Here, we consider $Max(M) = \{m \in Sub(M) | m \text{ is maximal element}\}$ as a subset of $Spec(M) = \{p \in Sub(M) | p \text{ is prime element}\}$ with the subspace topology.

Thus, if $M(t) = \{m \in Max(M) | t \leqslant m\}$, then $T = \{M(t) | t \in Sub(M)\}$ forms a basis of closed subsets on $Max(M)$.

Lemma 3.11. *Let M be a multiplication le-module. If A and B are disjoint closed subsets of $Max(M)$, then there exist $t_1, t_2 \in Sub(M)$ such that $A = M(t_1), B = M(t_2)$ and $Rt_1 + Rt_2 = e$. Also if A is closed and open set, then there exist $t_1, t_2 \in Sub(M)$ such that $Rt_1 + Rt_2 = e$ and $t_1 \wedge t_2 \leqslant Rad(M)$.*

Proof. If A and B are closed sets implies there exist $t_1, t_2 \in Sub(M)$ such that $A = M(t_1), B = M(t_2)$. We have $t_1 \leqslant Rt_1, t_2 \leqslant Rt_2$ and therefore $t_1 \leqslant Rt_1 + Rt_2$ and $t_2 \leqslant Rt_1 + Rt_2$. If $Rt_1 + Rt_2 \neq e$, then such that $Rt_1 + Rt_2 \leqslant m$ for some $m \in Max(M)$. But $t_1, t_2 \leqslant Rt_1 + Rt_2 \leqslant m$ and this implies $m \in M(t_1) \cap M(t_2) = A \cap B$, a contradiction. Consequently $Rt_1 + Rt_2 = e$.

Now, if A is both closed and open, then A and A^c are closed sets. Therefore by above argument there exist $t_1, t_2 \in Sub(M)$ such that $A = M(t_1), A^c = M(t_2)$ and $Rt_1 + Rt_2 = e$. Now we have $t_1 \leqslant m_1$ for all $m_1 \in A$ and $t_2 \leqslant m_2$ for all $m_2 \in A^c$. This implies $t_1 \wedge t_2 \leqslant m_1$ for all $m_1 \in A$ and $t_1 \wedge t_2 \leqslant m_2$ for all $m_2 \in A^c$. Therefore $t_1 \wedge t_2 \leqslant m$ for all $m \in Max(M)$. This implies $t_1 \wedge t_2 \leqslant Rad(M)$. □

Remark 3.12. The existence of disjoint closed subsets in the maximal spectrum gives the existence of adjacent elements in the comaximal graph.

Proposition 3.13. *Let $n_1, n_2, n_3 \in \Gamma_3(M)$ be distinct elements and let $D(t) = Max(M)/M(t)$. Then*

(1) *n_1 is adjacent to n_2 and n_3 if and only if $M(Rn_1) \subseteq D(Rn_2 \wedge Rn_3)$.*

(2) *$d(n_1, n_2) = 1$ if and only if $M(Rn_1) \cap M(Rn_2) = \emptyset$.*

(3) *$d(n_1, n_2) = 2$ if and only if $M(Rn_1) \cap M(Rn_2) \neq \emptyset$ and $Rn_1 \wedge Rn_2 \nleqslant Rad(M)$.*

(4) *$d(n_1, n_2) = 3$ if and only if $M(Rn_1) \cap M(Rn_2) \neq \emptyset$ and $Rn_1 \wedge Rn_2 \leqslant Rad(M)$.*

Proof. (1). Suppose that $M(Rn_1) \subseteq D(Rn_2 \wedge Rn_3)$. This implies $Rn_1 + (Rn_2 \wedge Rn_3) = e$. Therefore, $Rn_1 + Rn_2 = e$ and $Rn_1 + Rn_3 = e$. Thus n_1 is adjacent to both n_2 and n_3.

Conversely, suppose that n_1 is adjacent to both n_2 and n_3. Therefore $Rn_1 + Rn_2 = e$ and $Rn_1 + Rn_3 = e$, which implies $M(Rn_1) \cap M(Rn_2) = \emptyset$ and $M(Rn_1) \cap M(Rn_3) = \emptyset$. On contrary, if there exist $m \in M(Rn_1)$ and $m \notin D(Rn_2 \wedge Rn_3)$, then $Rn_2 \wedge Rn_3 \leqslant m$, and by Proposition 1.3, we have $Rn_2 \leqslant m$ or $Rn_3 \leqslant m$. Hence we have $m \in M(Rn_2)$ or $m \in M(Rn_3)$ and consequently $m \notin M(Rn_1)$, a contradiction.

(2). $d(n_1, n_2) = 1$ if and only if $Rn_1 + Rn_2 = e$ if and only if $M(Rn_1) \cap M(Rn_2) = \emptyset$.

(3). Suppose that,$d(n_1, n_2) = 2$. Which implies $Rn_1 + Rt = e$ and $Rn_2 + Rt = e$ for some $t \in M$. Note that t is adjacent to both n_1 and n_2 and hence

by (i) above we have $M(Rt) \subseteq D(Rn_1 \wedge Rn_2)$. Thus $m \in M(Rt)$ implies $m \notin M(Rn_1 \wedge Rn_2)$. Hence $Rn_1 \wedge Rn_2 \nleqslant Rad(M)$. Conversely, suppose that $M(Rn_1) \cap M(Rn_2) \neq \emptyset$ and $Rn_1 \wedge Rn_2 \nleqslant Rad(M)$. Thus there exists $m \in Max(M)$ such that $Rn_1 \wedge Rn_2 \nleqslant m$ implies $Rn_1 + m = Rn_1 + Rm = e$ and $Rn_2 + m = Rn_2 + Rm = e$. Therefore $n_1 - m - n_2$ is a shortest path and which implies $d(n_1, n_2) = 2$.

(4) Follows from (2), (3) and Theorem 2.10. □

Theorem 3.14. *Let M be a multiplication le-module with $Max(M)$ is Hausdorff. Then $diam(\Gamma_3(M)) = min\{|Max(M)|, 3\}$. If $|Max(M)| = 2$, then $gr(\Gamma_3(M)) = 4$ or ∞ otherwise $gr(\Gamma_3(M)) = 3$.*

Proof. First we prove that $|Max(M)| \geqslant 3$ if and only if $diam(\Gamma_3(M)) = 3$. Suppose that $|Max(M)| \geqslant 3$ and m_1, m_2, m_3 are distinct maximal elements in M. Since $Max(M)$ is Hausdorff, there are $t_i \in Sub(M)$ such that $m_i \in D(t_i)$ and $D(t_i) \cap D(t_j) = \emptyset$ for $i \neq j$. Thus $D(t_i) \subseteq M(t_j)$ for $i \neq j$. Now $D(t_i) \cup M(t_i) = Max(M)$ implies $M(t_i) \cup M(t_j) = Max(M)$. Hence $t_i \wedge t_j \leqslant m$ for all $m \in Max(M)$ implies $t_i \wedge t_j \leqslant Rad(M)$. Now $m_3 \in M(t_1) \cap M(t_2)$ implies $M(t_1) \cap M(t_2) \neq \emptyset$. Therefore by the Proposition 3.13, $d(t_1, t_2) = 3$ implies $diam(\Gamma_3(M)) = 3$.

Conversely, suppose that $diam(\Gamma_3(M)) = 3$. On contrary if $|Max(M)| < 3$, then either $|Max(M)| = 1$ or 2. The case $|Max(M)| = 1$ is not possible, because then $\Gamma_3(M)$ will contain only one vertex, a contradiction to $diam(\Gamma_3(M)) = 3$. Now suppose that $Max(M) = \{m_1, m_2\}$ and for vertices n_1, n_2 we have $d(n_1, n_2) = 3$. Hence there are vertices t_1, t_2 such that $n_1 - t_1 - t_2 - n_2$ is a shortest path between n_1 and n_2. If $n_1 \leqslant m_1$ then $t_1 \leqslant m_2$ implies $t_2 \leqslant m_1$ and hence $n_2 \leqslant m_2$. This gives a contradiction, because n_1 and n_2 are not adjacent. Similarly $n_2 \leqslant m_2$ is not possible. Therefore $|Max(M)| \geqslant 3$.

Now let $|Max(M)| = 2$. Then $Max(M) = \{m_1, m_2\}$ and $Max(M)$ is Hausdorff implies there exist $t_1, t_2 \in Sub(M)$ with $M(t_1) = \{m_1\}$ and $M(t_2) = \{m_2\}$. Therefore, we have $t_1 + t_2 = Rt_1 + Rt_2 = m_1 + m_2 = e$ and we have shortest cycle of length 4 namely $t_1 - t_2 - m_1 - m_2 - t_1$. If $t_1, t_2, t_3 \in \Gamma_3(M)$, then by the Pigeonhole Principle at least two of them $\leqslant m_1$ or m_2. Therefore there is no triangle in $\Gamma_3(M)$. If $|M_{m_1}| = 2$ or $|M_{m_2}| = 2$ then $t \leqslant m_1$ implies $t = 0$ or $t = m_1$ for $|M_{m_1}| = 2$. Hence in this case we have no cycle implies $gr(\Gamma_3(M)) = \infty$. □

Corollary 3.15. *Let M be a multiplication le-module with $Max(M)$ is*

Hausdorff. Then $diam(\Gamma_2(M)) = min\{|Max(M)|, 3\}$. *If* $|Max(M)| = 2$, *then* $gr(\Gamma_2(M)) = 4$ *or* ∞ *otherwise* $gr(\Gamma_2(M)) = 3$.

References

[1] **S. Ballal and V. Kharat**, *Zariski topology on lattice modules*, Asian-Euro. J. Math., **8** (2015), no. 4, 1550066 (10 pages).

[2] **S. Ballal and V. Kharat**, *On minimal spectrum of multiplication lattice modules*, Math. Bohemica, **144** (2019), 85 – 97.

[3] **A.K. Bhuniya and M. Kumbhakar**, *On irrducible pseudo-prime spectrum of topological le-modules*, Quasigroups and Related Systems, **26** (2018),, 251 – 262.

[4] **A.K. Bhuniya and M. Kumbhakar**, *Uniqueness of primary decompositions in Laskerian le-modules*, Acta Math. Hungar., **158** (2019), 202 – 215.

[5] **A.K. Bhuniya and M. Kumbhakar**, *On the prime spectrum of an le-module*, J. Algebra Appl., **20** (2021), paper no. 2150220.

[6] **H.M. Maimani, M. Salimi and A. Sattari** *Comaximal graph of commutative rings*, J. Algebra, **319** (2008), 1801 – 1808.

[7] **J.R. Munkres**, Topology, Second Ed. , Prentice Hall, New Jersey, (1999).

[8] **S. Puranik, S. Ballal and V. Kharat**, *Associated graphs of le-modules*, International J. Next-Generation Computing, **12** (2021), 280 – 291.

[9] **K. Samei**, *On the comaximal graph of a commutative ring*, Canad. Math. Bull., **57** (2014), 413 – 423.

[10] **P.K. Sharma and S.M. Bhatwadekar** *A note on graphical representation of rings*, J. Algebra, **176** (1995), 124 – 127.

Received April 19, 2023

S. Ballal
School of Mathematics and Statistics, University of Hyderabad, Hyderabad-500 046, India
E-mail: sachinballal@uohyd.ac.in

S. Puranik, V. Kharat
Department of Mathematics, Savitribai Phule Pune University, Pune-411 007, India
E-mail: srpuranik28@gmail.com, laddoo1@yahoo.com

Quasigroups and Related Systems **31** (2023), 185 – 200

https://doi.org/10.56415/qrs.v31.14

On the nonexistence of certain associative subloops in the loop of invertible elements of the split alternative Cayley-Dickson algebra

Evgenii L. Bashkirov

Abstract. Let $O(k)$ be the octonion Cayley–Dickson algebra over a commutative associative ring k with 1. Let $G(k)$ be the Moufang loop of invertible elements of $O(k)$. Let $\mathcal{H}$ be a class of groups such that a group G is a member of $\mathcal{H}$ if and only if G satisfies the following three conditions: (a) G is not class-2 nilpotent. (b) G has a proper class-2 nilpotent subgroup. (c) G is not isomorphic to any subgroup of the group $GL_2(F)$ for any field F. The theorem proved in the paper states that if k is an integral domain with $1+1 \neq 0$, then $G(k)$ does not contain any subloop isomorphic to a group of class $\mathcal{H}$, while if k is an integral domain such that $1+1=0$, then $G(k)$ contains no subloop isomorphic to a class-2 nilpotent group at all.

Let $G(k)$ denote the loop of invertible elements in the split alternative Cayley-Dickson algebra over a field k. If the characteristic of k is not 2, then $G(k)$ has a subloop isomorphic to the group $UT_3(k)$ of all 3×3 upper unitriangular matrices over k ([1]). A natural question arises then, namely, whether $G(k)$ contains a subloop isomorphic to a group which is, in a sense, more larger than $UT_3(k)$. The present paper answers this question, actually, in the negative using as a working tool a class of groups that contain a class-2 nilpotent group as a proper subgroup. More precisely,

Definition. A group G belongs to the class $\mathcal{H}$ if and only if G satisfies the following three conditions:

(a) G is not class-2 nilpotent.

2010 Mathematics Subject Classification: 20N05, 17D05, 20F18
Keywords: Moufang loops, Alternative algebras, Nilponent groups

(b) G has a proper class-2 nilpotent subgroup.

(c) G is not isomorphic to any subgroup of the group $GL_2(F)$ for every field F.

The main purpose of the paper is to prove the following theorem which demonstrates, in particular, a distinction between the case involving fields of characteristic not 2 and that in which fields of characteristic 2 appear.

Theorem 1. *Let k be an associative and commutative integral domain with 1, $O(k)$ the alternative split Cayley-Dickson algebra over k and $G(k)$ a Moufang loop of invertible elements in $O(k)$.*

(i) If $1+1 \neq 0$, then the loop $G(k)$ does not contain any subloop isomorphic to a group of class $\mathcal{H}$.

(ii) If $1+1=0$, then the loop $G(k)$ contains no subloop isomorphic to a class-2 nilpotent subgroup.

Before exposing proof of the theorem a notational system will be established.

Let k be a commutative associative ring with 1. Then k^* is the multiplicative group of all invertible elements of k.

If $a \in k$ and $S, T \subseteq k$, then $aS = \{as \mid s \in S\}$ and $S + T = \{s + t \mid s \in S, t \in T\}$.

Let n be an integer, $n \geqslant 2$. Then $M_n(k)$ is the associative ring of $n \times n$ matrices with entries in k. As usual, $GL_n(k)$ denotes the group $M_n(k)^*$, the general linear group of degree n over k.

If 1_n is the identity matrix of degree n and $a \in k$, then $t_{ij}(a)$ denotes the matrix $1_n + ae_{ij}$, where e_{ij} is the $n \times n$ matrix which has 1 in its (i, j) position and zeros elsewhere. If $S \subseteq k$, then $t_{ij}(S) = \{t_{ij}(a) \mid a \in S\}$.

k^3 is the standard free k-module formed by column vectors of length 3 with components in k. The elements

$$\begin{bmatrix}1\\0\\0\end{bmatrix}, \quad \begin{bmatrix}0\\1\\0\end{bmatrix}, \quad \begin{bmatrix}0\\0\\1\end{bmatrix}$$

of k^3 are denoted by e_1, e_2, e_3, respectively. The zero element of k^3 is designated as $\mathbf{0}$.

If $\alpha, \beta \in k^3$, then $\alpha \cdot \beta$ and $\alpha \times \beta$ denote the usual dot product and cross product, respectively.

$O(k)$ is the set of all symbols of the form $\left(\begin{smallmatrix} a & \alpha \\ \beta & b \end{smallmatrix}\right)$ with $a, b \in k, \alpha, \beta \in k^3$. In $O(k)$, equality, addition and multiplication by elements of k are defined componentwise, whereas the operation of multiplication is given by

$$\begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix} = \begin{pmatrix} ac + \alpha \cdot \delta & a\gamma + \alpha d - \beta \times \delta \\ \beta c + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{pmatrix},$$
$$a, b, c, d \in k, \quad \alpha, \beta, \gamma, \delta \in k^3.$$

Under the operations just defined $O(k)$ is an alternative nonassociative k-algebra termed the split Cayley-Dickson algebra (or the octonion one). Elements of $O(k)$ are called octonions.

To avoid a proliferation of symbols, it is convenient to adopt the following convention. The symbol 1_2 is used to denote the identity of the algebra $O(k)$,

$$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix},$$

as well as the identity 2×2 matrix. Also the symbol 0_2 is used to designate two things: the zero octonion

$$\begin{pmatrix} 0 & \mathbf{0} \\ \mathbf{0} & 0 \end{pmatrix}$$

and the zero 2×2 matrix. The convention should lead to no ambiguity if one attends closely to the context in which the notation is employed.

The trace $\mathrm{tr}(x)$ and the norm $n(x)$ of the octonion

$$x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \in O(k)$$

are defined to be $a + b$ and $ab - \alpha \cdot \beta$, respectively.

$G(k)$ is the (Moufang) loop of octonions of $O(k)$ whose norms lie in k^*. The norm n determines the bilinear form $(x, y) = n(x+y) - n(x) - n(y)$ on the k-module $O(k)$. Throughout the article, all metric concepts mentioned are related to the bilinear form (x, y) determined by the norm mapping $n\colon O(k) \to k$. In particular, if $Y \subseteq O(k)$, then the orthogonal complement $Y^\perp$ is defined to be the set $\{x \in O(k) \mid (x, y) = 0 \text{ for all } y \in Y\}$.

The algebra $O(k)$ admits an involution $^-\colon O(k) \to O(k)$ given by

$$\bar{x} = \begin{pmatrix} b & -\alpha \\ -\beta & a \end{pmatrix}, \text{ whenever } x = \begin{pmatrix} a & \alpha \\ \beta & b \end{pmatrix} \qquad a, b \in k, \quad \alpha, \beta \in k^3.$$

Borrowing the notation from the theory of algebraic groups, the automorphism group of the algebra $O(k)$ is denoted by $G_2(k)$.

Let $UT(k)$ and $ZUT(k)$ be the subloops of $G(k)$ defined by

$$UT(k) = \left\{ \begin{pmatrix} 1 & a_2e_1 \\ a_3e_2 + a_4e_3 & 1 \end{pmatrix} \;\middle|\; a_i \in k \right\},$$
$$ZUT(k) = \left\{ \begin{pmatrix} a_1 & a_2e_1 \\ a_3e_2 + a_4e_3 & a_1 \end{pmatrix} \;\middle|\; a_1 \in k^*, a_2, a_3, a_4 \in k \right\},$$

and let $N_0(k)$ and $N(k)$ be the subgroups of $GL_3(k)$ such that

$$N_0(k) = \left\{ \begin{pmatrix} r & 2a & b \\ 0 & r & c \\ 0 & 0 & r \end{pmatrix} \;\middle|\; r \in k^*, a, b, c \in k \right\},$$
$$N(k) = \left\{ \begin{pmatrix} 1 & 2a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; a, b, c \in k \right\}.$$

A direct calculation shows that the restriction of multiplication in $O(k)$ to $ZUT(k)$ is associative, and since $UT(k) \subseteq ZUT(k)$, this is true also for $UT(k)$. Moreover, the mapping $\eta\colon ZUT(k) \to N_0(k)$ defined by

$$\begin{pmatrix} a_1 & a_2e_1 \\ a_3e_2 + a_4e_3 & a_1 \end{pmatrix} \mapsto \begin{pmatrix} a_1 & 2a_3 & a_3a_4a_1^{-1} - a_2 \\ 0 & a_1 & a_4 \\ 0 & 0 & a_1 \end{pmatrix},$$

satisfies for all $x, y \in ZUT(k)$ the condition $(xy)^\eta = x^\eta y^\eta$, where the multiplication on the right-hand side is performed in the group $GL_3(k)$. This means that η is a group homomorphism from $ZUT(k)$ onto $N_0(k)$. The kernel of η is isomorphic to the subgroup $k[2]$ of the additive group of k formed by all $a \in k$ with $2a = 0$. Thus $N_0(k)$ is isomorphic to the quotient $ZUT(k)/k[2]$ and the restriction of η to $UT(k)$ determines an isomorphism of $UT(k)/k[2]$ onto $N(k)$. If $2 \in k^*$, then $k[2] = 0, 2k = k$, and hence $ZUT(k)$ is isomorphic to the direct product $k^* \times UT_3(k)$ of the groups k^* and $UT_3(k)$, whereas $UT(k) \cong UT_3(k)$.

If X is a group and $x, x_1 \in X$, then $x_1^x = x^{-1}x_1x$, ${}^xx_1 = xx_1x^{-1}$, $[x_1, x] = x_1^{-1}x_1^x$. If $R \subseteq X$, then ${}^xR = \{\, {}^xr \mid r \in R\}$.

If X is a loop and M is a subset of X, then $\langle M \rangle$ denotes the subloop of X generated by M.

A series of auxiliary results must be established before giving a direct proof of Theorem 1. The first of these is concerned with the following situation related to general alternative algebras.

Let k be a field of characteristic $\neq 2$ and L an alternative k-algebra with 1. Choose $a_1, a_2, a \in k$ and suppose that L contains elements y_1, y_2 such that

$$y_1^2 = a_1, \quad y_2^2 = a_2, \quad y_1y_2 + y_2y_1 = a. \tag{1}$$

It is straightforward to check that the subspace $A = k + ky_1 + ky_2 + ky_1y_2$ of the k-vector space L is a subalgebra of L which is denoted as

$$\left(\frac{a_1, a_2, a}{k}, y_1, y_2\right). \tag{2}$$

A description of noncommutative algebras (2) is a constituent of the proof of Theorem 1. Certainly, some parts of this description can be extracted from the usual classification of quaternion algebras exposed, for example, in [2], pp. 13–20. However, the full list of subalgebras (2) can not be given within the framework of [2] (mainly, due to the fact that the case $a_1a_2 = a = 0$ is excluded in [2]). Therefore, it is desirable to have, at least as a sketch, an argument leading to a full description of subalgebras (2). This is done in Lemma 1 below. The proof of that lemma requires, in turn, the following notations in which some algebras of 2×2 matrices appear.

If x_0, x_1, x_2 are indeterminates and $b, c \in k$ are such that the quadratic form $x_0^2 - x_1^2b - x_2^2c$ does not represent zero in k, then

$$D(b, c, k) = \left\{ \begin{pmatrix} r_0 + r_1\sqrt{b} & r_2 + r_3\sqrt{b} \\ c(r_2 - r_3\sqrt{b}) & r_0 - r_1\sqrt{b} \end{pmatrix} \;\middle|\; r_i \in k \right\}.$$

In other words, $D(b, c, k)$ is the quaternion division algebra $\left(\frac{b,c}{k}\right)$ realized by matrices of degree 2 over the field $k(\sqrt{b})$.

If $b \in k$ is not a square in the field k, then

$$T_0(k(\sqrt{b})) = \left\{ \begin{pmatrix} r_0 + r_1\sqrt{b} & r_2 + r_3\sqrt{b} \\ 0 & r_0 - r_1\sqrt{b} \end{pmatrix} \;\middle|\; r_i \in k \right\}.$$

Finally, $T(k)$ denotes the k-algebra of 2×2 upper triangular matrices over k:

$$T(k) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in k \right\}.$$

Now the above mentioned description runs as follows.

Lemma 1. *Let k be a field of characteristic not 2, L an alternative algebra over k with 1, and $a_1, a_2, a \in k$. Suppose that L contains elements y_1, y_2 satisfying (1) and let A be the subalgebra of L defined by (2). Suppose that A is noncommutative. Then one of the following holds:*

(*i*) $A \cong M_2(k)$.

(*ii*) $A \cong D(b, c, k)$, *where the quadratic form* $x_0^2 - x_1^2 b - x_2^2 c$ *in* x_0, x_1, x_2 *does not represent 0 in* k.

(*iii*) $A \cong T_0(k(\sqrt{b}))$, *where b is not a square in k.*

(*iv*) $A \cong T(k)$.

(*v*) $\dim_k A = 4$ *and* $A \cong \left(\frac{1,0,0}{k}, z_1, z_2\right)$ *for some* $z_1, z_2 \in L$.

(*vi*) $A \cong \left(\frac{0,0,0}{k}, z_1, z_2\right)$ *for some* $z_1, z_2 \in L$.

Proof. PART ONE. Consider first the case $a = 0$. There are the following three possibilities for a_1:

(a) a_1 is not a square in k,

(b) a_1 is a nonzero square in k,

(c) $a_1 = 0$.

The corresponding possibilities exist for a_2 and exchanging, if necessary, y_1 and y_2, one obtains the following six possibilities for the ordered pair (a_1, a_2):

(1) Both a_1, a_2 are not squares in k.

(2) a_1 is not a square in k, a_2 is a nonzero square in k.

(3) a_1 is not a square in k, $a_2 = 0$.

(4) Both a_1, a_2 are nonzero squares in k.

(5) a_1 is a nonzero square in k, $a_2 = 0$.

(6) $a_1 = a_2 = 0$.

These cases are considered separately.

(1) Here $\dim_k A = 4$ and A is a quaternion algebra in the sense of [2], p. 14. So A is either a division algebra and $A \cong D(a_1, a_2, k)$ or $A \cong M_2(k)$.
(2) Again A is a quaternion algebra, and since a_2 is a square in k^*, $A \cong M_2(k)$.
(3) In this case, $\dim_k A = 4$ and $A \cong T_0(k(\sqrt{a_1}))$.
(4) Here again A is a quaternion algebra, A being isomorphic to $M_2(k)$.
(5) In this case, the following two possibilities arise for the dimension of A over k: this dimension is equal either to 3 or to 4. If $\dim_k A = 3$, then $A \cong T(k)$. If $\dim_k A = 4$, then setting $z_1 = y_1 b_1^{-1}$, where $a_1 = b_1^2, b_1 \in k$, and $z_2 = y_2$, one obtains $A \cong \left(\frac{1,0,0}{k}, z_1, z_2\right)$.
(6) Here A corresponds to the algebra listed in (vi).

PART TWO. Now consider the case $a \neq 0$. If, under this assumption, $a_1 = a_2 = 0$, then $\dim_k A = 4$ and the correspondence $y_1 \mapsto \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right), y_2 \mapsto \left(\begin{smallmatrix} 0 & 0 \\ a & 0 \end{smallmatrix}\right)$ determines an isomorphism of A upon $M_2(k)$. If $(a_1, a_2) \neq (0, 0)$, then exchanging, if necessary, y_1 and y_2, one may suppose that $a_1 \neq 0$ and

$$A = \left(\frac{a_1, a_1(-1 + 4a_1a_2a^{-2}), 0}{k}, y_1, y_1 - 2a_1a^{-1}y_2\right).$$

In particular, if $a_2 = 0$, then $A \cong M_2(k)$. If both a_1, a_2 are nonzero, then A is as in $(i) - (v)$ by part one of the proof. The lemma is proved. □

The next lemma adjusts Suprunenko's results on class-2 nilpotent linear groups over algebraically closed fields (see, [5], pp.210, 211) to the situation of fields which are not necessarily algebraically closed. For the needs of Theorem 1 proof, the case of linear groups of degree 2 is considered only.

Lemma 2. *Let k be a field of characteristic $\neq 2$ and X a class-2 nilpotent subgroup of $GL_2(k)$. Then*

$$X = B1_2 \cup Bx_1 \cup Bx_2 \cup Bx_1x_2,$$

where $B \leqslant k^*$ with $-1 \in B$, and $x_1, x_2 \in GL_2(k)$ are such that $x_1^2, x_2^2 \in B1_2$ and $x_2x_1 = -x_1x_2$.

Proof. Let Ω be an algebraic closure of k. For every field F, the group $GL_2(F)$ does not possess any reducible class-2 nilpotent subgroup. Therefore X, being a class-2 nilpotent subgroup of $GL_2(\Omega)$, is an irreducible

subgroup of $GL_2(\Omega)$. If M is a maximal irreducible class-2 nilpotent subgroup of $GL_2(\Omega)$ with $M \geqslant X$, then according to Theorem 7 [5], pp. 210, 211, M is conjugate by an element $q \in GL_2(\Omega)$ to the group Γ formed by all elements $\lambda a_1^{\alpha_1} a_2^{\alpha_2}$, where $\lambda \in \Omega^*, \alpha_1, \alpha_2$ integers, and

$$a_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

In other words, $\Gamma = \Omega_0 \cup \Omega_1 \cup \Omega_2 \cup \Omega_3$, where $\Omega_0 = \Omega^* 1_2$, $\Omega_i = \Omega^* a_i$ $(i = 1, 2)$, $\Omega_3 = \Omega^* a_1 a_2$. Choose not permutable $x_1, x_2 \in X$ and let $q_i = x_i^q (i = 1, 2)$. Then neither q_1 nor q_2 can lie in Ω_0 and also q_1, q_2 can not belong to one and the same set Ω_i with $i \in \{1, 2, 3\}$. Interchanging, if necessary, x_1 and x_2 and replacing (again if necessary) the ordered pair x_1, x_2 either by that of $x_1, x_1 x_2$ or by $x_1 x_2, x_1$, one may assume that $q_1 \in \Omega_1, q_2 \in \Omega_2$. So

$$q_1 = \begin{pmatrix} \omega_1 & 0 \\ 0 & -\omega_1 \end{pmatrix}, \quad q_2 = \begin{pmatrix} 0 & \omega_2 \\ \omega_2 & 0 \end{pmatrix}$$

for some $\omega_1, \omega_2 \in \Omega$. Denote X^q by C. Put then

$$B_0 = \{b \in \Omega^* \mid b1_2 \in C\}, \quad B_1 = \{b \in \Omega^* \mid bq_1 \in C\},$$
$$B_2 = \{b \in \Omega^* \mid bq_2 \in C\}, \quad B_3 = \{b \in \Omega^* \mid bq_1 q_2 \in C\},$$

and let U be the union $B_0 1_2 \cup B_1 q_1 \cup B_2 q_2 \cup B_3 q_1 q_2$. Clearly $U \subseteq C$. The definition of B_0 implies that $B_0 \leqslant \Omega^*$. Squaring q_1, q_2 and $q_1 q_2$, one gets that ω_1^2, ω_2^2 and -1 are in B_0. Observe also that all B_i contain 1. Therefore, since $B_0 B_i \subseteq B_i (i = 1, 2, 3)$, $B_0 \subseteq B_i$. On the other hand, $B_i B_i \subseteq B_0$ and again the relation $1 \in B_i$ shows that $B_i \subseteq B_0$ giving then $B_i = B_0 (i = 1, 2, 3)$. Denoting the common value of B_i by B, one has

$$U = B1_2 \cup Bq_1 \cup Bq_2 \cup Bq_1 q_2.$$

Now let h be an element of C. Writing

$$h = \begin{pmatrix} x & y \\ z & t \end{pmatrix}, \quad x, y, z, t \in \Omega,$$

and denoting $[q_1, h] = q_1^{-1} h^{-1} q_1 h$ by q_3, one has

$$q_3 = (\det h)^{-1} \begin{pmatrix} tx + yz & 2ty \\ 2xz & tx + yz \end{pmatrix}.$$

Since q_3 commutes with q_1 which is diagonal but not scalar, q_3 must be diagonal itself. It follows that $ty = xz = 0$ because char $k \neq 2$. If $x \neq 0$, then

$$h = \begin{pmatrix} x & 0 \\ 0 & t \end{pmatrix}.$$

Since $[q_2, h]$ commutes with q_2, one obtains $t = \pm x$. If $t = x$, then $h = x1_2$, and $h \in B1_2 \subseteq U$. If $t = -x$, then $hq_1 = x\omega_1 1_2 \in C$, so $x\omega_1 = b_0 \in B$. Thus $h = q_1 b_0 \omega_1^{-2} \in q_1 B \subseteq U$. Next let $x = 0$ and so

$$h = \begin{pmatrix} 0 & y \\ z & 0 \end{pmatrix}.$$

Since C contains the diagonal matrix

$$hq_2 = \begin{pmatrix} y\omega_2 & 0 \\ 0 & z\omega_2 \end{pmatrix},$$

$z = \pm y$. If $z = y$, then $hq_2 = y\omega_2 1_2$ and hence $y = z = b_1\omega_2^{-1}$ with $b_1 \in B$. This shows $h = q_2 b_1 \omega_2^{-2} \in q_2 B \subseteq U$. If $z = -y$, then $hq_2q_1 = y\omega_2\omega_1 1_2$, whence $y = b_2\omega_1^{-1}\omega_2^{-1}$ with $b_2 \in B$ and $h = q_1q_2b_2\omega_1^{-2}\omega_2^{-2} \in q_1q_2B \subseteq U$. Thus $h \in U$ in any case and consequently $C = U$. It follows that $X = B1_2 \cup Bx_1 \cup Bx_2 \cup Bx_1x_2$. But $X \leqslant GL_2(k)$, so $B \leqslant k^*$. Also $x_i^2 = ({}^{q}q_i)^2 = {}^{q}(q_i^2) = \omega_i^2 1_2$, that is, $x_i^2 \in B1_2 (i = 1, 2)$. Finally, $x_1x_2 + x_2x_1 = q(q_1q_2 + q_2q_1)q^{-1} = 0_2$ which completes the proof of the lemma. □

The following assertion has a technical character and is used in the subsequent description of subloops of $G(k)$ that are isomorphic to class-2 nilpotent groups.

Lemma 3. *Let*

$$x_1 = \begin{pmatrix} r & \mathbf{0} \\ \mathbf{0} & s \end{pmatrix}, \quad x_2 = \begin{pmatrix} u & \rho \\ \pi & v \end{pmatrix}$$

be elements of $G(k)$ such that $\rho \cdot \pi = 0$ with both ρ and π nonzero. If x_1 and x_2 are not permutable, then $[x_1, x_2]$ does not commute with x_1.

Proof. A straightforward calculation gives

$$[x_1, x_2] = \begin{pmatrix} 1 & e\rho \\ f\pi & 1 \end{pmatrix}$$

with $e = u^{-1}(1 - sr^{-1}), f = v^{-1}(1 - rs^{-1})$. If this commutes with x_1, then $es\rho = er\rho$ and $fr\pi = fs\pi$. Since ρ and π are both nonzero, $es = er, fr = fs$. But either $e \neq 0$ or $f \neq 0$ for $[x_1, x_2] \neq 1_2$. Therefore, $r = s$, hence x_1 commutes with x_2 which is impossible. □

Now the description of subloops of $G(k)$ that are isomorphic to class-2 nilpotent groups can be given for fields k of characteristic $\neq 2$.

Lemma 4. *Let k be a field of characteristic $\neq 2$ and $X \leqslant G(k)$. Suppose that X is isomorphic to a class-2 nilpotent group. Then one of the following holds:*

(*i*) *X is isomorphic to a subgroup of $GL_2(k_1)$ where either $k_1 = k$ or k_1 is a quadratic field extension of k.*

(*ii*) *There is $\psi \in G_2(k)$ such that $X^\psi \leqslant ZUT(k)$.*

Proof. Choose not permutable $x_1, x_2 \in X$. Since $x_i \in O(k)$, $x_i^2 = x_i t_i + n_i 1_2$ for some $t_i \in k$ and $n_i \in k^*$. As char $k \neq 2$, one can put $y_i = x_i - 2^{-1}t_i 1_2$, $a_i = 4^{-1}t_i^2 + n_i$ so that $y_i^2 = a_i 1_2$. This implies $\bar{y}_i = -y_i$ and $y_1y_2 + y_2y_1 = a1_2$ with $a \in k$. Let $A = k1_2 + ky_1 + ky_2 + ky_1y_2$. By Lemma 1, one of Possibilities $(i) - (vi)$ listed in that lemma can arise for A.

Suppose first that Possibility (iv) arises. Then there is a ring isomorphism $\chi_0 \colon (A, +, \cdot) \to (T(k), +, \cdot)$. Considering A and $T(k)$ as semigroups (under corresponding multiplications), one obtains a semigroup isomorphism $\tilde{\chi}_0 \colon (A, \cdot) \to (T(k), \cdot)$. Restricting $\tilde{\chi}_0$ on A^*, the set of invertible elements of A, one has a group homomorphism χ of $(A^*, \cdot)$ into the group of all 2×2 invertible upper triangular matrices over k. Due to the equation $x_i = y_i + 2^{-1}t_i 1_2$ and since $k1_2 \subseteq A$, both x_1 and x_2 are in A. Hence $\langle x_1, x_2 \rangle^\chi$ is a reducible class-2 nilpotent subgroup of $GL_2(k)$ which is false. Thus Possibility (iv) is in fact impossible. A similar argument shows that Possibility (iii) from Lemma 1 also can not arise.

Now suppose that Possibility (v) from Lemma 1 takes place for A. Assume first that $a \neq 0$. Then if (v) takes place, one may suppose without loss of generality that $a_1 = b_1^2, b_1 \in k^*$ and $(y_1 - 2a_1a^{-1}y_2)^2 = 0_2$. So replacing X by X^φ with a suitable $\varphi \in G_2(k)$, one may suppose that

$$y_1 = \begin{pmatrix} b_1 & \mathbf{0} \\ \mathbf{0} & -b_1 \end{pmatrix}.$$

Putting then

$$y_1 - 2a_1a^{-1}y_2 = \begin{pmatrix} c & \gamma \\ \delta & d \end{pmatrix}, \quad c, d \in k, \quad \gamma, \delta \in k^3,$$

one has $c = d = 0$ in view of the equation $y_1(y_1 - 2a_1a^{-1}y_2) + (y_1 - 2a_1a^{-1}y_2)y_1 = 0_2$. The condition $(y_1 - 2a_1a^{-1}y_2)^2 = 0_2$ gives $\gamma \cdot \delta = 0$, where γ and δ are both nonzero because $\dim_k A = 4$. It follows that

$$y_2 = \left[y_1 - (y_1 - 2a_1a^{-1}y_2)\right] \frac{a}{2a_1} = \begin{pmatrix} \frac{a}{2b_1} & -\gamma\frac{a}{2b_1^2} \\ -\delta\frac{a}{2b_1^2} & -\frac{a}{2b_1} \end{pmatrix}.$$

Therefore,

$$x_1 = y_1 + \frac{t_1}{2}1_2 = \begin{pmatrix} r & \mathbf{0} \\ \mathbf{0} & s \end{pmatrix},$$

where $r = b_1 + 2^{-1}t_1, s = -b_1 + 2^{-1}t_1$, and

$$x_2 = y_2 + \frac{t_2}{2}1_2 = \begin{pmatrix} u & \rho \\ \pi & v \end{pmatrix},$$

for some $u, v \in k$ and $\rho = -2^{-1}\gamma a b_1^{-2}, \pi = -2^{-1}\delta a b_1^{-2}$. Now observe that both γ and δ are nonzero because $\dim_k A = 4$. So $\rho \neq 0, \pi \neq 0$ and applying Lemma 3 one obtains a contradiction. A similar argument leads to a contradiction when $a = 0$, so Possibility (v) is impossible at all.

Suppose Case (ii) takes place. This means that A is isomorphic to a quaternion division k-algebra $(\frac{b,c}{k})$. In particular, the subalgebra A contains 1_2, and the restriction of the bilinear form $(,)$ to A is nondegenerate. Thus the subspace $A^{\perp}$ is nondegenerate too and hence it contains v with $n(v) \neq 0$ so that $O(k) = A \oplus vA$. Now let x be an arbitrary element of X. Then $x = a + vb$ with $a, b \in A$ and $(xx_1)x_2 = x(x_1x_2)$. But $(xx_1)x_2 = ax_1x_2 + v(x_2x_1b)$ and $x(x_1x_2) = ax_1x_2 + v(x_1x_2b)$ (see, [3], p. 26), whence it follows that $v(x_2x_1b) = v(x_1x_2b)$, and since v is invertible, $x_2x_1b = x_1x_2b$. Note that x_1 and x_2 are not permutable elements of the class-2 nilpotent group $\langle x_1, x_2\rangle$. According to Lemma 2, x_1 and x_2 must anticommute. So $-x_1x_2b = x_1x_2b$, and since x_1x_2 is invertible and char $k \neq 2$, one gets $b = 0$, hence $x \in A$. Thus $X \subseteq A$, that is, X is isomorphic to a subgroup of $GL_2(k(\sqrt{b}))$. In a similar fashion, one can show that X is isomorphic to a subgroup of $GL_2(k)$ if Case (i) of Lemma 1 takes place.

It remains to consider the situation when A is as in Possibility (vi) of Lemma 1. Using the terminology of [1], this can be expressed by saying

that y_1 and y_2 form a half extra-special pair. According to Lemma 5.3 [1], there is $\psi \in G_2(k)$ such that

$$x_1^\psi = \begin{pmatrix} r_1 & \mathbf{0} \\ e_2 & r_1 \end{pmatrix}, \quad x_2^\psi = \begin{pmatrix} r_2 & \mathbf{0} \\ e_3 & r_2 \end{pmatrix}, \quad r_i = \frac{t_i}{2}.$$

Now let

$$x^\psi = \begin{pmatrix} f & \gamma \\ \delta & d \end{pmatrix}, \quad f, d \in k, \quad \gamma, \delta \in k^3$$

be an element of X^ψ. Then $(x_1^\psi x_2^\psi)x^\psi = x_1^\psi(x_2^\psi x^\psi)$ which leads to the equality

$$\begin{pmatrix} r_1r_2f - e_1 \cdot \delta & r_1r_2\gamma - e_1d - (e_2r_2 + e_3r_1) \times \delta \\ (e_2r_2 + e_3r_1)f + \delta r_1r_2 - e_1 \times \gamma & * \end{pmatrix} = \begin{pmatrix} r_1r_2f & r_1(r_2\gamma - e_3 \times \delta) - e_2 \times (e_3f + \delta r_2) \\ e_2r_2f + r_1(e_3f + \delta r_2) & * \end{pmatrix}. \tag{3}$$

Comparing the corresponding entries in the position (11) shows that $e_1 \cdot \delta = 0$. This means exactly that $\delta \in e_2k + e_3k$. Further, comparing the vectors in the position (12) leads to the equality $d = f$. Finally, comparing vectors in the position (21) yields $e_1 \times \gamma = \mathbf{0}$ which means that $\gamma \in ke_1$. Collecting all this information, one concludes $x^\psi \in ZUT(k)$ which completes the proof of the lemma. □

After all these preparations, Part (i) of Theorem 1 can be proved. This will be done as the demonstration of the following proposition.

Proposition 1. *Let k be an associative and commutative integral domain with 1. If $1+1 \neq 0$, then the loop $G(k)$ does not have any subloop isomorphic to a group of class $\mathcal{H}$.*

Proof. The ring k can be considered as a subring of a field which, due to the condition $1 + 1 \neq 0$, must have characteristic $\neq 2$. So from the very beginning one can assume that k is a field and char $k \neq 2$. Suppose that $G(k)$ has a subloop G isomorphic to a group of class $\mathcal{H}$. By Item (b) in Definition, G contains a proper subloop X isomorphic to a class-2 nilpotent subgroup. By Lemma 4, X is either isomorphic to a subgroup of the group $GL_2(k_1)$, where k_1 is a field extension of k with $[k_1 : k] \leqslant 2$ or there is $\psi \in G_2(k)$ such that $X^\psi \leqslant ZUT(k)$.

Suppose that X is isomorphic to a subgroup of $GL_2(k_1)$. Consider the k_1-algebra $O(k_1) = O(k) \otimes_k k_1$. One has $X \leqslant G \leqslant G(k) \leqslant G(k_1)$, and

following the line of Lemma 4 proof, namely, those places of the proof which address Possibilities (i) and (ii) of Lemma 1, it is readily seen that X is a subset of the subalgebra A' of $O(k_1)$ such that A' is isomorphic to $M_2(k_1)$. So there is $\varphi \in G_2(k_1)$ with $X^\varphi \leqslant G_{[1]}(k_1)$, where

$$G_{[1]}(k_1) = \left\{ \begin{pmatrix} a & be_1 \\ ce_1 & d \end{pmatrix} \;\middle|\; a, b, c, d \in k_1, ad - bc \neq 0 \right\}$$

([4], p. 17, Corollary 1.7). Using again the proof of Lemma 4, one can deduce that $G \leqslant G_{[1]}(k_1)$, that is, that G is isomorphic to a subgroup of $GL_2(k_1)$. But this contradicts Item (c) in Definition. Hence $X^\psi \leqslant ZUT(k)$ for some $\psi \in G_2(k)$, and the argument employing equation (3) shows that $G^\psi \leqslant ZUT(k)$. Therefore, G is isomorphic to a class-2 nilpotent group which contradicts Item (a) in Definition. This final contradiction proves the proposition completely. □

Now an example that illustrates the result just proved will be given.

Example 1. Let $\mathbb{Q}$ be the field of all rational numbers, and B the subset of $\mathbb{Q}$ consisted of all numbers $\pm 11^n, n \in \mathbb{Z}$. Let θ be a root of the polynomial $\lambda^2 + 11 \in \mathbb{Q}[\lambda]$. Clearly B is a subgroup of $\mathbb{Q}(\theta)^*$. Let

$$h_1 = \begin{pmatrix} \theta & 0 \\ 0 & -\theta \end{pmatrix}, \quad h_2 = \begin{pmatrix} 0 & \theta \\ \theta & 0 \end{pmatrix}.$$

Then $H = B1_2 \cup Bh_1 \cup Bh_2 \cup Bh_1h_2$ is a class-2 nilpotent subgroup of $GL_2(\mathbb{Q}(\theta))$. Though H is not isomorphic to any subgroup of $GL_2(\mathbb{Q})$, H can be realized as a subloop of $G(\mathbb{Q})$. Indeed, if

$$x_1 = \begin{pmatrix} 1 & e_1 + 3e_2 + 2e_3 \\ e_1 - 3e_2 - 2e_3 & -1 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix},$$

and $X = \langle x_1, x_2 \rangle$, then the correspondence $x_1 \mapsto h_1, x_2 \mapsto (-11)^{-1}h_1h_2$ and $b \mapsto b$ for every $b \in B$, determines an isomorphism of X onto H. The subalgebra $A_0 = \mathbb{Q}1_2 + \mathbb{Q}x_1 + \mathbb{Q}x_2 + \mathbb{Q}x_1x_2$ of $O(\mathbb{Q})$ is isomorphic to the quaternion division algebra $\left(\frac{-11,-1}{\mathbb{Q}}\right)$ and is of the type $\left(\frac{-11,-1,0}{\mathbb{Q}}, x_1, x_2\right)$. One has $A_0 \otimes_{\mathbb{Q}} \mathbb{Q}(\theta) \cong M_2(\mathbb{Q}(\theta))$. By [4], Corollary 1.7 on p. 17, there is an automorphism φ of the algebra $O(\mathbb{Q}(\theta)) \cong O(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}(\theta)$ such that $X^\varphi \leqslant G_{[1]}(\mathbb{Q}(\theta))$.

The following situation can serve as an application of Proposition 1.

Let R be an associative and commutative ring with 1 and let $EAff_{2+1}(R)$ denote the subgroup of $GL_3(R)$ generated by the set $t_{12}(R) \cup t_{21}(R) \cup t_{13}(1)$. It is claimed that $EAff_{2+1}(R)$ is a group of class $\mathcal{H}$.

The center of $EAff_{2+1}(R)$ is trivial. Therefore, Item (a) of Definition is satisfied. Since $UT_3(R) \leqslant EAff_{2+1}(R)$, Item (b) in Definition also holds. Now suppose that there exists a field F such that $EAff_{2+1}(R)$ is isomorphic to subgroup H of $GL_2(F)$. Then $GL_2(F)$ must have a subgroup H_0 isomorphic to $UT_3(R)$. In particular, H_0 is class-2 nilpotent. If Ω is an algebraic closure of F, then H_0, being a class-2 nilpotent subgroup of $GL_2(\Omega)$, is an irreducible subgroup of $GL_2(\Omega)$. Therefore, by Corollary 2 [5], p. 209, char $\Omega \neq 2$, hence char $F \neq 2$ too. By Lemma 2, H_0 contains the matrix -1_2 which commutes with all elements of $GL_2(F)$, in particular, with all elements of H. Since char $F \neq 2$, $-1_2 \neq 1_2$ which means that the center of H is nontrivial. This contradiction shows that Item (c) in Definition holds, and consequently $EAff_{2+1}(R) \in \mathcal{H}$. Now Proposition 1 shows that the following assertion is valid.

Corollary 1. *Let k and R be associative and commutative rings with identities, the identity of k being designated by 1. Suppose that k is an integral domain and that $1+1 \neq 0$. Then the loop $G(k)$ does not contain any subloop isomorphic to the group $EAff_{2+1}(R)$.*

Note that it is this corollary that has been the initial point for writing the present paper.

The proof of Part (*ii*) of Theorem 1 is given as the proof of the following proposition.

Proposition 2. *Let k be an associative and commutative integral domain with 1. Suppose that $1 + 1 = 0$. Then $G(k)$ contains no subloop isomorphic to a class-2 nilpotent group.*

Proof. One may assume that k is a field of characteristic 2. Suppose that $G(k)$ has a subloop G which is isomorphic to a class-2 nilpotent group. Then G contains not permutable elements g_1, g_2 such that both of them commutes with their group commutator $[g_1, g_2]$ or, which is equivalent, with $\bar{g}_1\bar{g}_2g_1g_2$. Note that to satisfy the latter condition each g_i can be replaced by any of its scalar multiples. So if $\mathrm{tr}(g_i) \neq 0$, one may assume that $\mathrm{tr}(g_i) = 1$. Thus interchanging, if necessary, g_1 and g_2, there are three cases to consider each to be handled separately.

(i) $\mathrm{tr}(g_1) = \mathrm{tr}(g_2) = 1$.

(ii) $\mathrm{tr}(g_1) = 1, \mathrm{tr}(g_2) = 0$.

(iii) $\mathrm{tr}(g_1) = \mathrm{tr}(g_2) = 0$.

Case (i). Here $g_i^2 = g_i + r_i 1_2$ for some $r_i \in k^*$ and $\bar{g}_i = 1_2 + g_i (i = 1, 2)$. Therefore,

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r_1 g_2 + g_2 g_1 g_2 + g_1 g_2 g_1 g_2. \tag{4}$$

Denoting by r the trace of the product $g_1 g_2$, one obtains

$$g_2 g_1 = (r+1)1_2 + g_1 + g_2 + g_1 g_2.$$

So

$$g_2 g_1 g_2 = r g_2 + r_2 g_1 + r_2 1_2, \tag{5}$$

hence

$$g_1 g_2 g_1 g_2 = r g_1 g_2 + r_1 r_2 1_2. \tag{6}$$

Substituting (5) and (6) into (4), one gets

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r_1 g_2 + r g_2 + r_2 g_1 + r_2 1_2 + r g_1 g_2 + r_1 r_2 1_2.$$

Since g_2 commutes with $\bar{g}_1 \bar{g}_2 g_1 g_2$,

$$g_2 g_1 (r_2 1_2 + r g_2) = g_1 (r_2 1_2 + r g_2) g_2 = g_1 g_2 (r_2 1_2 + r g_2).$$

This shows that if $r_2 1_2 + r g_2$ were invertible, then g_2 would commute with g_1 which is impossible. Thus $n(r_2 1_2 + r g_2) = 0$ whence it follows that $r^2 + r + r_2 = 0$. Observe further that the roles of g_1 and g_2 are completely symmetric which implies that $r^2 + r + r_1 = 0$, and so $r_1 = r_2 = r^2 + r$. It follows that if $h_i = g_i + r 1_2 (i = 1, 2)$, then h_i is an idempotent of $O(k)$. Therefore, if $h_3 = (r+1)1_2 + h_1 + h_2$, then $h_3 \in (k1_2 + kh_1)^{\perp}$ and the subalgebra $A = k1_2 + kh_1 + h_3(k1_2 + kh_1)$ of $O(k)$ is isomorphic to the associative algebra $M_2(k)$ (see, [6], pp. 43–45). Since $g_1, g_2 \in A$, the subloop $\langle g_1, g_2 \rangle$ of G is isomorphic to a class-2 nilpotent subgroup of $GL_2(k)$. According to [5], Corollary 2, p. 209, this is false. So Case (i) is impossible.

Case (ii). Here $\bar{g}_1 = 1_2 + g_1, \bar{g}_2 = g_2, g_1^2 = g_1 + r_1 1_2, g_2^2 = r_2 1_2, r_1, r_2 \in k^*$. Following the line of the consideration in the previous case, one obtains

$$\bar{g}_1 \bar{g}_2 g_1 g_2 = r g_2 + g_1 r_2 + r_2 1_2 + r g_1 g_2 + r_1 r_2 1_2,$$

where r is the trace of g_1g_2. Since g_2 commutes with $\bar{g}_1\bar{g}_2g_1g_2$, $g_2(g_1r_2 + rg_1g_2) = (g_1r_2 + rg_1g_2)g_2$, whence $r_2 = r^2$, and in particular $r \neq 0$. This, together with the fact that g_1 and $\bar{g}_1\bar{g}_2g_1g_2$ commute, implies $g_1(g_2+g_1g_2) = (g_2+g_1g_2)g_1$ which can be written as $(1_2+g_1)g_1g_2 = (1_2+g_1)g_2g_1$. It follows that $n(1_2 + g_1) = 0$, or $(1_2 + g_1)(1_2 + g_1 + 1_2) = (1_2 + g_1)g_1 = 0_2$. But $g_1 \in G(k)$, and so $g_1 = 1_2$ which is false. So Case (ii) is impossible.

Case (iii). Here $g_i^2 = r_i1_2$ with $r_i \in k^*$ and $\bar{g}_i = g_i (i = 1, 2)$. The condition that g_1 commutes with $\bar{g}_1\bar{g}_2g_1g_2 = g_1g_2g_1g_2$ leads to the equation

$$r_1g_2g_1g_2 = g_1g_2g_1g_2g_1. \tag{7}$$

Denoting the trace of g_1g_2 by r, one has $g_2g_1g_2 = rg_2 + g_1r_2, g_1g_2g_1g_2g_1 = r^2g_1+rr_1g_2+r_1r_2g_1$. Then (7) becomes $r_1(rg_2+g_1r_2) = r^2g_1+rr_1g_2+r_1r_2g_1$, whence $r^2g_1 = 0_2$ which is false. Case (iii) is impossible. This completes the proof of the proposition. □

Corollary 2. *Let k and R be associative commutative rings with identity elements. Suppose that 1 is the identity of k and that $1 + 1 = 0$. Suppose also that k is an integral domain. Then the loop $G(k)$ does not contain any subloop isomorphic to the group $UT_3(R)$.*

References

[1] **E.L. Bashkirov**, *On subloops of the loop of invertible elements of the split Cayley-Dickson algebra over a field that contain a subloop of transvections*, Commun. Algebra, **50** (2022), no. 4, 2083–2108.

[2] **R.S. Pierce**, *Associative algebras.* Graduate Texts in Mathematics, **88**, Springer Verlag, New York, Berlin (1988).

[3] **R. D. Shafer**, *An introduction to nonassociative algebras*, Academic Press, New York (1966).

[4] **T.A. Springer, F.D. Veldkamp**, *Octonions, Jordan algebras and exceptional groups*, Springer Verlag, Berlin, Heidelberg, New York (2000).

[5] **D.A. Suprunenko**, *Matrix groups*, Transl. Math. Monogr., **45**, Amer. Math. Soc., Providence, Rhode Island (1976).

[6] **K.A. Zhevlakov, A. M.Slin'ko, I.P. Shestakov, A.I. Shirshov**, *Rings that are nearly associative*, Academic Press, New York (1982).

Received March 21, 2023

Kalinina str 25, ap. 24
Minsk 220012
Belarus
E-mail: zh.bash@mail.ru

Quasigroups and Related Systems **31** (2023), 201 – 206

https://doi.org/10.56415/qrs.v31.15

On topological Menger n-groupoids

Hamza Boujouf

Abstract. We present the necessary and sufficient conditions for the existence of left-invariant measure on a topological Menger n-groupoid.

1. Introduction

The terminology and notations used in this article are are typical for this theory (see for example [3]). A nonempty set X with an n-ary operation f is an *n-semigroup* if this operation is associative, i.e.

$$f(f(x_1^n), x_{n+1}^{2n-1}) = f(x_1^j, f(x_{j+1}^{j+n}), x_{j+n+1}^{2n-1})$$

holds for all $j = 1, 2, \ldots, n-1$ and $x_1^{2n-1} \in X$.

If the operation f is superassociative, i.e. if

$$f(f(x_1^n), y_1^{n-1}) = f(x_1, f(x_2, y_1^{n-1}), \ldots, f(x_n, y_1^{n-1}))$$

holds for all $x_1^n, y_1^{n-1} \in X$, the (X, f) is called a Menger n-groupoid.

We start with some examples of Menger n-groupoids.

1. The set $\mathbb{R}$ of real number with the 4-ary operation f defined by $f(x_1^4) = x_1 + x_2 - x_3 + x_4$.
2. The set $(R, +, \cdot)$ with the operation $f(x_1^3) = x_1(x_2 + x_3)$.
3. The group $\mathbb{Z}_n$ with the operation $f(x_1^n) = x_1 + x_2 + \ldots + x_n (\mathrm{mod}\, n)$.
4. The set $\mathbb{R}$ of real number with the operation $f(x_1^n) = \frac{x_1 + x_2 + \ldots + x_n}{n}$.

2010 Mathematics Subject Classification: 20N15, 28C10, 22A30

Keywords: Menger n-groupoid, n-semigroup, topological n-group, invariant measure.

More examples can be found in [3].

Recall that an element e of a Menger n-groupoid (X, f) is called *spacial* if $f(x, {}^{n-1}e) = f(e, {}^{n-1}x) = x$ holds for all $x \in X$. A Menger n-groupoid is *cancellative* if all its translations $t_k(x) = f(a_1^{k-1}, x, a_{k+1}^n)$ are injective. A Menger n-groupoid in which all translations t_1 (respetively, t_n) are injective is called *left* (respectively, *right*) *cancellative*. A Menger n-groupoid (X, f) is called *i-solvable*, if the equation $f(a_1^{k-1}, x, a_k^{n-1}) = b$ is uniquely solvable for $k = 1$ and $k = i + 1$. A nonempty subset $I \subset X$ is called a *k-ideal* of (X, f), if $x_k \in I$ implies $f(x_1^{k-1}, x_k, x_{k+1}^n) \in I$, for all $x_1^{k-1}, x_{k+1}^n \in X$. If I is a k-ideal for each $1 \leqslant k \leqslant n$, then it is valled an *ideal*.

In the topological Menger n-groupoid (X, f, τ) the collection of all compact subsets of X is denoted by $\mathcal{K}(X)$, and the smallest σ-ring containing $\mathcal{K}(X)$ is denote by $\mathcal{B}(X)$; the elements of $\mathcal{B}(X)$ are called Borel sets. A measure μ on $\mathcal{B}(X)$ such that $\mu(C) < +\infty$ for any $C \in \mathcal{K}(X)$ and such that any $a \in X$ has an neighborhood U with

$$\mu_*(U) = \sup\{\mu(C) \,|\, \mathcal{K}(C) \ni C \subset U\} < +\infty$$

is called a *Borel measure*. If for any $B \in \mathcal{B}(X)$, $\mu(B) = \mu_*(B)$ the Borel measure is called *inner regular*. The set $\{f(x_1^{i-1}, k, x_{i+1}^{n-1}) \,|\, k \in K\}$, where $K \subset X$, $x_1^n \in X$, will be denoted by $[x_1^{i-1}, K, x_{i+1}^n]$. A Borel measure μ is said to be *left-invariant* on (X, f, τ) if $\mu(B) = \mu([a_1^{n-1}, B])$ for any $a_1^{n-1} \in X$ and $B \in \mathcal{B}(X)$. Note that $[a_1^{k-1}, C, a_{k+1}^n] \in \mathcal{K}(X)$ for any $C \in \mathcal{K}(X)$ and $a_1^n \in X$.

2.Results

Let (X, f) be a Menger n-groupoid with a topology τ and let $g = f_{(2)}$, i.e. $g(x_1^n, y_2^n) = f(f(x_1^n), y_2^n$. In [1] is an example of a Menger n-groupoid with a topology τ in which the operation g is continuous but the operation f is not continuous.

Theorem 2.1. *Let (X, f) be a right cancellative Menger n-groupoid endowed with a topology τ such that for any $a \in X$ the translation $t(x) = f(x, {}^{n-1}a)$ is open in τ. Then the operation $g = f_{(2)}$ is continuous in τ if and only if the operation f is continuous in τ.*

Proof. Let $a_1^n \in X$. Let W be an open neighborhood of the point $f(a_1^n)$. Then, from the assumption, the set $[W, {}^{n-1}a]$ is an open neighborhood of

$f(f(a_1^n), {}^{n-1}a)$. If the operation $g = f_{(2)}$ is continuous in τ, then there exists the open neighborhoods U_i of a_i, $i = 1, \ldots, n$, and an open neighborhood U of a such that $f(f(x_1^n), y_1^{n-1}) \in [W, {}^{n-1}a]$, where $x_i \in U_i$, $i = 1, \ldots, n$, $y_j \in U$, $j = 1, \ldots, n-1$, in particular $f(f(x_1^n), {}^{n-1}a) \in [W, {}^{n-1}a]$. As (X, f) is right cancellative, so $f(x_1^n) \in W$, which gives the continuity of f in τ.

The converse is obvious. □

If (X, f) is a Menger n-groupoid, then X with the operation $x \cdot y = f(x, {}^{n-1}y)$ is a semigroup called a *diagonal semigroup* of (X, f) (see for example [2]). The neutral element e of $(X, \cdot)$, if it exists, is called a *special element* of (X, f). From Theorem 2.6 in [3] it follows that if an associative Menger n-groupoid with a special element has an element $a \in X$ such that $f({}^{n-1}x, a) = x$ for all $x \in X$, then this Menger n-groupoid is derived from its diagonal semigroup, i.e. $f(x_1^n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n$. Moreover, if (X, f) is a left or right cancellative, then $(X, \cdot)$ is commutative.

Theorem 2.2. *Let (X, f, τ) be an associative, right or left cancellative, topological Menger n-groupoid with a special element in which for every $a, b \in X$ the equation $f(a, {}^{n-1}x) = b$ has a solution, $x \in X$. Then (X, f) contains an ideal with open translations.*

Proof. Let $\Gamma = \{V \mid V \subset X, V \in \tau\}$, $I = \bigcup_{V \in \Gamma} V$. Then $I \subset X$ and $I \in \tau$ and, by Theorem 2.6. in [3], (X, f) is derived from its diagonal semigroup $(X, \cdot)$ which is commutative. From the fact that for every $a, b \in X$ the equation $f(a, {}^{n-1}x) = b$ has a solution, it follows that $(X, \cdot)$ is a commutative group. Thus, if for $x_1^n \in X$ and $x \in I$ we have $f(x_1^{k-1}, x, x_{k+1}^{n-1}) \in [x_1 \cdot \ldots \cdot x_{k-1} \cdot I \cdot x_{k+1} \cdot \ldots \cdot x_n] \subset X$, then $f(x_1^{k-1}, I, x_{k+1}^{n-1}) = [x_1^{k-1}, I, x_{k+1}^n] \in \tau$. Let $U \in \tau$ and $U \subset f(x_1^{k-1}, I, x_{k+1}^n)$. Since $\lambda(x) = f(x_1^{k-1}, x, x_{k+1}^{n-1})$ is a continuous translation of X, the set $W = x_{k-1}^{-1} \cdot \ldots \cdot x_1^{-1} \cdot U \cdot x_n^{-1} \cdot \ldots \cdot x_{k+1}^{-1} = \lambda^{-1}(U)$ is open in (X, τ) and $W \subset I$. So, W is open in (X, τ). As the set $x_1 \cdot \ldots \cdot x_{k-1} \cdot W \cdot x_{k+1} \cdot \ldots \cdot x_{n-1} = U$ is open in (X, τ), $f(x_1^{k-1}, I, x_{k+1}^{n-1}) \subset I$. Hence$I$ is an ideal of (X, f).

Finally, if $V \subset I$, $V \in \tau$, then for all translations λ from X to X, we have $X \supset \lambda(V) = [x_1^{k-1} V x_{k+1}^n] = x_1 \cdot \ldots \cdot x_{k-1} \cdot V \cdot x_{k+1} \cdot \ldots \cdot x_{n-1} \in \tau$, i.e. the translation is open in (X, τ). □

Theorem 2.3. *Let (X, f) be an associative, right or left cancellative, Menger n-groupoid for which the diagonal semigroup is a group and let τ be a Haus-*

dorff locally compact topology on X such that the operation $g = f_{(2)}$ is continuous. Then the following conditons are equivalen:

(*A*) *(X, f, τ) has an open locally compact ideal with open translations;*

(*B*) *on (X, f, τ) there exists nonzero left-invariant measure μ such that for all $x_1^{n-1} \in X$ there exists a compact set K, such that $\mu([K, x_1^{n-1}]) > 0$;*

(*C*) *the operation f is continuous in τ, the diagonal semigroup $(X, \cdot)$ becomes a topological group, and $(X, \diamond)$, where $x \diamond y = f(x, a_1^{n-2}, y)$ with fixed $a_1^{n-2} \in X$, is a topological group.*

Proof. $(B) \Rightarrow (C)$. According to Theorem 2.6 from [3] (X, f) is derived from its diagonal semigroup $(X, \cdot)$, which is a group. Thus, for $a_1^{n-2} \in X$, the operation $x \diamond y = f(x, a_1^{n-2}, y) = x \cdot a_1 \cdots a_{n-2} y = xay$, where $a = a_1 \cdots a_{n-2}$ is calculated in the group $(X, \cdot)$, is associative. Then a^{-1} is the neutral element of $(X, \diamond)$ and $a^{-1}x^{-1}a^{-1}$ is the inverse of x. So $(X, \diamond)$ is a group. Since the operation $g = f_{(2)}$ is continuous in τ, then by Theorem 2.1, the operation f is continuous in τ, and consequently the binary operations $(\cdot)$ and $(\diamond)$ also are continuous in τ. This implies the continuity of the left and right translations $x \mapsto x \cdot b$, $x \mapsto b \cdot x$. Therefore the operation $(x, y) \mapsto x \cdot b \cdot y$ is continuous as well. Finally, we have $x^{-1} = a \cdot (a^{-1} \cdot x^{-1} \cdot a^{-1}) \cdot a$, so the inversion $x \mapsto x^{-1}$ is continuous in $(X, \cdot, \tau)$. Consequently, the diagonal semigroup $(X, \cdot, \tau)$ is a topological group.

If μ is a nonzero left-invariant measure on (X, f, τ), then μ is left-invariant on topological semigroup $(X, \diamond, \tau)$. Thus for $x \in X$, there exists a compact subset $K \subset X$ such that $\mu(K \diamond x) = \mu(f(K, a_1^{n-2}, x)) = \mu([K, a_1^{n-2}x]) > 0$. Hence, by [5], $(X, \diamond, \tau)$ is a topological group.

$(C) \Rightarrow (A)$. The operation f is continuous in τ, so, by Theorem 2.2, (X, f, τ) has an open locally compact ideal with open translations.

$(A) \Rightarrow (B)$. Let (X, f) has an open locally compact ideal I with open translations, and let $a \in I$, $x \in X$. Then $x \cdot \underbrace{a \cdots a}_{n-1} = f(x, {}^{n-1}a) \in I$. Therefore (I, f, τ) is a topological n-semigroup, $(X, \cdot, \tau)$ is a locally compact topological semigroup, and $(X, \diamond, \tau)$ is a locally compact group. Then, by Theorem 1 in [5], there exists nonzero regular left invariant measure μ such that $\mu(C) > 0$ for all $C \in \mathcal{K}(X)$, and $\mu([Cx]) > 0$ for all $x \in X$.

As for any compact subset $K \subset X$ we have $K \subset [a^{n-1}K] \subset I$ then $[a^{n-1}K]$ is a compact subset of (X, τ). By this we have that all Borelian subset of (X, f, τ) is a Borelian subset of $(X, \cdot, \tau)$. Let μ be a left Haar

measure (cf.[4]) on the topological semigroup $(X, \cdot, \tau)$, then $\mu(K) > 0$ implies $\mu([Kx_1^{n-1}]) > 0$ for all $x_1^{n-1} \in X$. This proves (B). □

Analogously as Theorem 2.2 above, using Corollary 3.3. in [3] one can prove the following result.

Theorem 2.4. *Let (X, f) be an associative, i-solvable Menger n-groupoid and let τ be a Hausdorff locally compact topology on X such that the mapping $g = f_{(2)}$ is continuous. Then the following conditions are equivalent.*

- (A) *(X, f, τ) has an open locally compact ideal with open translations;*
- (B) *on (X, f, τ) there exists nonzero left-invariant measure μ such that for all $x_1^{n-1} \in X$ there exists a compact set K such that $\mu([K, x_1^{n-1}]) > 0$;*
- (C) *the operation f is continuous in τ; the diagonal semigroup $(X, \cdot)$ becomes a topological group; and $(X, \diamond)$ is a topological group, where the binary operation $(\diamond)$ is defined as follows : $x \diamond y = f(x, a_1^{n-2}, y)$.*

Remark 2.5. Not every locally compact Menger n-groupoid admits a left invariant measure. For example, the set $X = \{a, b\}$ with the n-ary operation $f(x_1^n) = x_1$ is an idempotent Menger n-groupoid and $aX = \{a\}$, $bX = \{b\}$. Therefore, no measure on X can have $\mu(X) = \mu(aX) = \mu(bX)$.

Theorem 2.6. *Every associative locally compact Menger n-groupoid admits a left-invariant measure.*

Proof. Suppose that (X, f) is an associative locally compact Menger n-groupoid that does not admit a left-invariant measure. Let $c = \mu([0, 1])$. Then, for any $k \in \mathbf{N}$, we have $c^k = \mu([0, 1])^k = \mu([0, 1]^k) \leqslant \mu(X)$. Since X is locally compact, it contains a closed subset homeomorphic to $[0, 1]^k$ for every $k \in N$. Therefore, we have $c^k \leqslant \mu(X)$ for every $k \in \mathbf{N}$. Now, consider the sequence $(c^k)_{k \geqslant N}$. Since c is a probability measure, we have $0 \leqslant c^k \leqslant c$ for every $k \in N$. Therefore, the sequence $(c^k)_{k \geqslant 1}$ is decreasing and bounded by 0, so it converges to some limit $p \in [0, c]$. Since X is locally compact, it contains a closed subset homeomorphic to $[0, 1]$, so $p = \mu([0, 1]) = c$. Therefore, we have $c^k \leqslant c$ for every $k \in \mathbf{N}$, which implies that $c = 0$ or $c = 1$. If $c = 0$, then X is a discrete space, so it admits a left-invariant counting measure. If $c = 1$, then X is a compact space, so it admits a left-invariant Haar measure. Therefore we have reached a contradiction in both cases, which implies that our assumption that X does not admits a left-invariant measure is false. Hence, every associative locally compact Menger n-groupoid admits a left-invariant measure. □

References

[1] **H. Boujouf**, *On the embedding Menger n-groupoids in n-ary topological groups*, J. Sebha Univ., Pure and Appl. Sci. **12** (2013), no. 2, 108 – 113.

[2] **W.A. Dudek and V.S. Trokhimenko**, *Algebra of multiplace functions*, Walter de Gruyter GmbH Co. KG, Berlin/Boston, (2012).

[3] **W.A. Dudek**, *On goup-like Menger n-groupoids*, Radovi Matematicki **2** (1986), 81 – 98.

[4] **P.R. Halmos**, *Measure theory*, (Russian), Moscow, (1953).

[5] **V.V. Mukhin**, *Measures and the imbedding of topological semigroup in locally compact groups*, (Russian), Izv. AN BSSR, **2917** (1985), 1 – 23.

Received April 15, 2023

Ecole Supérieur des Sciences de L'ingénierie Commerciale
132, Avenue des FAR
50000 Meknes
Morocco
E-mail: hamzaan14@gmail.com

Quasigroups and Related Systems **31** (2023), 207 – 220

https://doi.org/10.56415/qrs.v31.16

Quasigroups generated by shift registers and Feistel networks

Sucheta Chakrabarti, Alexei V. Galatenko, Valentin A. Nosov, Anton E. Pankratiev and Sharwan K. Tiwari

Abstract. Formula-based specification of large quasigroups with the use of complete mappings over Abelian groups is investigated. Complete mappings specified by generalized feedback registers and generalized Feistel networks are considered. In both cases criteria for the mapping completeness are established. A procedure for uniform sampling of quasigroups induced by complete mappings under study is suggested. The classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families of functions are shown to be disjoint.

1. Introduction

Finite quasigroups are a promising platform for the implementation of various cryptographic primitives [9, 18]. In particular, quasigroup-based algorithms regularly take part in NIST contest, e.g., hash functions NaSHA [10] and EDON-R′ [8] participated in SHA-3 contest, and GAGE and InGAGE suite [7] was a candidate for Lightweight Cryptography Standard.

Of special interest is the apparatus of binary networks proposed by Cherednik [2, 3]. The networks are parameterized by either a quasigroup operation or a left (or right) quasigroup operation. It turned out to be possible to construct networks such that the transform implemented for any sufficiently large domain size is transitive or even multiply transitive.

NaSHA hash function uses quasigroups of the order 2^{64}; tabular specification of such a large quasigroup is impossible due to memory limitations. A possible way around is to switch to some sort of a formula-based specification. The solution used in NaSHA is based on a recursive application

2010 Mathematics Subject Classification: 20N05, 05B15

Keywords: quasigroup, orthomorphism, feedback shift register, Feistel network

of extended Feistel networks introduced by Markovski and Mileva in [11]. The idea behind extended Feistel networks is the connection between complete mappings of Abelian groups and quasigroups noticed by Sade [17]: if σ is a complete mapping of an Abelian group $G = (Q, +)$, i.e., both $\sigma(x)$ and $\sigma(x) - x$ are bijective, then $(Q, \sigma(x - y) + y)$ is a quasigroup. Later Markovski and Mileva proposed other generalizations of Feistel networks and established sufficient conditions for completeness of the corresponding mappings [12, 13].

In our paper we consider generalized feedback shift registers (GFSR) over Abelian groups, a model that, on the one hand, is a straightforward extension of classic feedback registers, and, on the other hand, covers the major part of generalizations proposed by Markovski and Mileva. We prove a completeness criterion for the mapping specified by generalized feedback shift registers and use this criterion to obtain the cardinality of the set of quasigroups generated by GFSRs. We also describe a procedure for uniform sampling of quasigroups generated by GFSRs. If a quasigroup is used as a key of a cryptographic transform, then the cardinality of the set generated determines the strength against brute force attacks; a set of a high cardinality can also be viewed as an approximation of Cherednik's model. Random objects often possess a number of beneficial properties (in particular, random quasigroups are polynomially complete, i.e. simple and non-affine [1], and even not isotopic to quasigroups that are polynomially incomplete [5]), so selection of a quasigroup at random may be a good idea. Properties of "random" quasigroups generated by generalized feedback registers are the subject of future research.

The generalized Feistel network is another generalization of extended Feistel networks from [11]. In this case, we increase the number of non-linear feedback loops. Similarly to the case of GFSR, we establish a completeness criterion, evaluate the cardinality of the set of quasigroups generated and provide a procedure for uniform sampling.

Proper families of functions over Abelian groups and permutation construction applied to proper families over Abelian groups are another way to specify big families of large quasigroups in a memory-efficient way [14, 15]. Interestingly, this method is "orthogonal" to generalized feedback shift registers and generalized Feistel networks in a sense that the classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families of functions turn out to be disjoint.

The rest of the paper is organized as follows. Section 2 contains basic definitions. Section 3 is devoted to generalized feedback registers. Section 4 covers generalized Feiltel networks. Section 5 is the conclusion.

2. Main definitions

A *finite quasigroup* is a pair (Q, f), where Q is a finite set and f is a binary operation on Q invertible in each variable, i.e. for any $a, b \in Q$ the equations $f(x, a) = b$ and $f(a, y) = b$ are uniquely solvable. All objects considered in our paper are finite, so for the sake of brevity the word "finite" will be omitted.

Obviously (Q, f) is a quasigroup if and only if the Cayley table of f is a *Latin square*, i.e., the elements comprising any row or column are distinct.

Let $(Q, +)$ be a finite Abelian group, σ be a bijective mapping (i.e., a permutation) on Q. The mapping σ is *complete* with respect to the group $(Q, +)$ if the mapping σ' specified by the rule $\sigma'(x) = \sigma(x) - x$ is also bijective. In this case the mapping σ' is called the *ortomorphism* associated with σ.

Complete mappings can be used to specify quasigroups. Namely, in [17] it is shown that if σ is complete with respect to an Abelian group $(Q, +)$ and

$$f(x, y) = \sigma(x - y) + y, \tag{1}$$

then (Q, f) is a quasigroup. It can be easily shown that the assertion also holds for

$$f(x, y) = \sigma(x + y) - y. \tag{2}$$

Indeed, the equation

$$f(a, y) = \sigma(a + y) - y = b$$

has a unique solution $y = (\sigma')^{-1}(b - a) - a$, and the equation

$$f(x, a) = \sigma(x + a) - a = b$$

has a unique solution $x = \sigma^{-1}(b+a)-a$. If $(Q, +)$ is an elementary Abelian 2-group (i.e., isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$), then $\sigma(x - y) + y = \sigma(x + y) - y = \sigma(x + y) + y$.

Assume that $|Q| = k^n$ for some $k, n \in \mathbb{N}$, $k \geqslant 2$. Then the elements $q_0, q_1, \ldots, q_{k^n-1}$ of Q can be naturally represented by n-tuples corresponding to the k-ary notation of the element indices. For example, q_0 is represented by the n-tuple $(0, \ldots 0)$ and q_{k^n-1} is represented by the n-tuple

$(k-1,\dots,k-1)$. Denote the set $\{0,1,\dots,k-1\}$ by E_k. Denote the set of all t-ary functions on E_k by P_k^t. Without loss of generality one can assume that $Q = E_k^n$ and write the equality $z = f(x,y)$ in the form

$$\begin{aligned} z_1 &= f_1(x_1,\dots,x_n,y_1,\dots,y_n)\\ z_2 &= f_2(x_1,\dots,x_n,y_1,\dots,y_n)\\ &\vdots\\ z_n &= f_n(x_1,\dots,x_n,y_1,\dots,y_n), \end{aligned} \tag{3}$$

where $f_i \in P_k^{2n}$. The relations (3) are referred to as a multivariate representation of the operation f.

Assume that $k \in \mathbb{N}$, $k \geqslant 2$, $G = (E_k, +)$ is an Abelian group, 0 is the neutral element of G, $n \in \mathbb{N}$, $n \geqslant 2$, $\mathcal{G} = G^n$. We will use the same notation for operations on G and $\mathcal{G}$; the domain of the operation will be clear from the context.

A multivariate mapping $\sigma = (f_1(x_1,\dots,x_n),\dots,f_n(x_1,\dots,x_n)) \colon E_k^n \to E_k^n$ specified by the relations

$$\begin{aligned} f_1 &= x_2\\ f_2 &= x_3\\ &\vdots\\ f_{n-1} &= x_n\\ f_n &= x_1 + g(x_2,\dots,x_n), \end{aligned} \tag{4}$$

where g is some function from E_k^{n-1} to E_k, is referred to as a *feedback shift register*. Obviously the mapping σ is a permutation on E_k^n. In Section 3 we will establish a criterion for $\sigma(x)$ being a complete mapping.

A *Feistel network* is defined for the case $n = 2$ by the multivariate mapping $(f_1 = x_2, f_2 = x_1 + g(x_2))$, where g is a mapping on E_k. On the one hand, it is a special case of a feedback shift register; on the other hand, it is well known that a Feistel network is a complete mapping if and only if g is a bijection.

In [11, 12, 13] the authors analyzed a number of generalizations of Feistel networks. A Parametrized Feistel Network (PFN) is defined for $n = 2$ and is specified by the relations $f_1 = x_2 + c_1$, $f_2 = x_1 + c_2 + g(x_2)$, where $g \in P_k^1$, $c_1, c_2 \in E_k$. If g is a bijection, then the mapping specified by PFN is complete [12, Theorem 3.3]. Other generalizations are defined for arbitrary n. A type-1 Parameterized Extended Feistel Network (PEFN) is specified by the relations $f_1 = x_2 + g(x_1) + c_1$, $f_2 = x_3 + c_2$, $f_3 = x_4 + c_3$,

$\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + c_n$, where $g \in P_k^1$, $c_1, \ldots, c_n \in E_k$. A consistent renumbering of functions and variables makes these relations take the form $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + g(x_n) + c_n$. Similarly to the case of PFN, if g is a bijection, then the mapping is complete [12, Theorem 3.4]. A Parameterized Generalized Feistel Non Linear Feedback Shift Register (PGF-NLFSR) is specified by the relations $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_2 + x_3 + \ldots + x_n + c_n + g(x_1)$ with $g \in P_k^1$ and $c_1, \ldots, c_n \in E_k$. If the group G is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, n is even and g is a bijection, then the mapping specified by PGF-NLFSR is complete [12, Theorem 3.5]. Finally, a type-4 Parameterized Extended Feistel Network (PEFN) is defined by the relations $f_1 = x_2 + c_1$, $f_2 = x_3 + c_2$, $\ldots$, $f_{n-1} = x_n + c_{n-1}$, $f_n = x_1 + c_n + g(x_2 + x_3 \ldots + x_n)$, where $c_1, \ldots, c_n$ are some constants from E_k, $g \in P_k^1$. Similarly to the case of PGF-NLFSR, if the group G is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, n is even and g is a bijection, then the mapping is complete [13, Theorem 5].

Similarly to the constructions from [11, 12, 13] we generalize the definition of a feedback shift register by adding linear summands to the relations (4). A multivariate mapping

$$\sigma = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \colon E_k^n \to E_k^n$$

specified by the relations

$$\begin{aligned} f_1 &= x_2 + c_1 \\ f_2 &= x_3 + c_2 \\ &\vdots \\ f_{n-1} &= x_n + c_{n-1} \\ f_n &= x_1 + g(x_2, \ldots, x_n) + c_n, \end{aligned} \tag{5}$$

where g is some function from E_k^{n-1} to E_k, $c_1, \ldots, c_n \in E_k$, is referred to as a *generalized feedback shift register*. Identically to the case of "regular" feedback shift registers, the mapping σ is obviously a permutation on E_k^n. Note that PFN, type-1 PEFN (after renumbering) and type-4 PEFN are generalized feedback shift registers.

Consider another way of generalization of a Feistel network. A *generalized Feistel network* is defined for the case $n = 2$ by the relations

$$\begin{aligned} f_1 &= s(x_2) \\ f_2 &= x_1 + p(x_2), \end{aligned} \tag{6}$$

where s, p are some functions from E_k to E_k. In Section 4 we will establish a criterion of mapping completeness for the case of generalized Feistel

networks.

Proper families of functions over Abelian groups is another way of a formula-based specification of large families of quasigroups. A family $(g_1, \ldots, g_n)$, $g_i \in P_k^n$, $i = 1, \ldots, n$, is *proper*, if for any $\alpha, \alpha' \in E_k^n$, $\alpha = (a_1, \ldots, a_n)$, $\alpha' = (a'_1, \ldots, a'_n)$, $\alpha \neq \alpha'$, there exists an index i, $1 \leqslant i \leqslant n$, such that $a_i \neq a'_i$ and $g_i(\alpha) = g_i(\alpha')$.

Suppose that $f \in P_k^n$ is some function, $1 \leqslant i \leqslant n$. The variable x_i is said to be *dummy* (or *inessential*) for the function f, if for any $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in E_k$ the function

$$f'(x) = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$$

is a constant. In other words, the function f does not depend on the value of the ith variable. Obviously if a family $(g_1, \ldots, g_n)$ is proper, then for $i = 1, \ldots, n$ the variable x_i is dummy for g_i.

Let

$$f_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = x_i + y_i + g_i(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)), \quad (7)$$

where $p_1, \ldots, p_n$ are arbitrary functions from P_k^2. If the family $(g_1, \ldots, g_n)$ is proper, then $(f_1, \ldots, f_n)$ is a multivariate representation of a quasigroup operation [14, Theorem 1]. Thus a single proper family generates $\left(k^{k^2}\right)^n$ quasigroups, though some of these quasigroups may coincide. It is known [6, Theorem 8] that all quasigroups specified by proper families over Abelian groups contain a unique subquasigroup of the order 1 (i.e., a "fixed point" α such that $f(\alpha, \alpha) = \alpha$). A possible way to overcome this problem is to use the permutation construction proposed by Piven [15]. The construction consists in applying permutations $\beta, \gamma, \delta \in S_n$ to the indices of the variables x, y and functions in the representation (7), respectively, so that the relations (7) take the form

$$f_{\delta(i)} = x_{\beta(i)} + y_{\gamma(i)} + g_i(p_1(x_{\beta(1)}, y_{\gamma(1)}), \ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})). \quad (8)$$

If the family $(g_1, \ldots, g_n)$ is proper, then the relations (8) define a quasigroup operation for any choice of the internal functions $p_1, \ldots, p_n$ and permutations β, γ, δ [15, Theorem 2]. On the one hand, the permutations can be stored using $O(n \log_2 n)$ bytes which is negligible in comparison with the quasigroup order k^n. On the other hand, utilizing permutation construction allows one to increase the cardinality of the set of quasigroups generated and to improve some of important properties, e.g., to get rid of subquasigroups

or affinity. Without loss of generality one can assume that δ is the identical permutation, since applying a non-trivial δ can be reduced to applying additional permutations β and γ and possibly changing the proper family [16, Theorem 1]. The assertions obtained by Piven are formally established for the case $k = 2$, $G = (E_2, \oplus)$, but the proofs do hold for the general case.

We will show that the set of quasigroups specified by permutation construction applied to proper families of functions does not intersect with the set of quasigroups specified by generalized feedback shift registers and generalized Feistel networks.

3. Quasigroups generated by feedback shift registers

Theorem 3.1. *A generalized feedback shift register is a complete mapping if and only if any non-trivial shift changes the value of the function g, i.e., for any tuple $(a_2, \ldots, a_n) \in E_k^{n-1}$ and any $a \in E_k$, $a \neq 0$, it holds that $g(a_2, \ldots, a_n) \neq g(a_2 + a, \ldots, a_n + a)$.*

Proof. Assume that a function g does not satisfy the hypothesis, i.e., there exist a tuple $(a_2, \ldots, a_n) \in E_k^{n-1}$ and a constant $a \neq 0$ such that $g(a_2, \ldots, a_n) = g(a_2 + a, \ldots, a_n + a)$. Show that in this case the mapping $\sigma(x) - x$ is not injective. Arbitrarily select the value of the variable x_1 and denote the selected value by a_1. Consider the tuples $\alpha = (a_1, \ldots, a_n)$ and $\alpha' = (a_1 + a, \ldots, a_n + a)$. If $1 \leqslant i \leqslant n - 1$, then the ith component of $\sigma(\alpha) - \alpha$ and $\sigma(\alpha') - \alpha'$ equals $a_{i+1} + c_i - a_i$. The nth component of $\sigma(\alpha) - \alpha$ equals $a_1 + g(a_2, \ldots, a_n) + c_n - a_n$. The nth component of $\sigma(\alpha') - \alpha'$ equals $a_1 + a + g(a_2 + a, \ldots, a_n + a) + c_n - a_n - a = a_1 + g(a_2, \ldots, a_n) + c_n - a_n + c_n$, thus injectivity is violated.

Conversely, assume that a function g satisfies the hypothesis. Assume that bijectivity of the mapping $\sigma(x) - x$ is violated. Since the set E_k^n is finite, it means that the mapping $\sigma(x) - x$ is not injective. Assume that $\alpha = (a_1, \ldots, a_n)$ and $\alpha' = (a'_1, \ldots, a'_n)$ are distinct tuples such that $\sigma(\alpha) - \alpha = \sigma(\alpha') - \alpha'$. Thus it holds that

$$\begin{aligned}
&a_2 + c_1 - a_1 = a'_2 + c_1 - a'_1 \\
&a_3 + c_2 - a_2 = a'_3 + c_2 - a'_2 \\
&\vdots \\
&a_n + c_{n-1} - a_{n-1} = a'_n + c_{n-1} - a'_{n-1} \\
&a_1 + g(a_2, \ldots, a_n) + c_n - a_n = a'_1 + g(a'_2, \ldots, a'_n) + c_n - a'_n.
\end{aligned} \tag{9}$$

Note that if $a_1 = a'_1$, then the first equality of the system (9) implies that $a_2 = a'_2$, the second equality implies that $a_3 = a'_3$, and so on. Hence the tuples are equal, which contradicts the assumption. Thus, $a_1 = a'_1 + a$ for some $a \in E_k$, $a \neq 0$. The first $n-1$ equalities of the system (9) yield the equalities $a_i = a'_i + a$, $i = 2, \ldots, n$. Substitute these relations into the nth equality of (9):

$$a_1 + g(a_2, \ldots, a_n) + c_n - a_n = a'_1 + a + g(a'_2 + a, \ldots, a'_n + a) + c_n - a'_n - a =$$
$$a'_1 + g(a'_2 + a, \ldots, a'_n + a) + c_n - a'_n = a'_1 + g(a'_2, \ldots, a'_n) + c_n - a'_n.$$

As a result, we obtain the equality $g(a'_2 + a, \ldots, a'_n + a) = g(a'_2, \ldots, a'_n)$ which contradicts the assumption. □

Corollary 3.2. *A feedback shift register is a complete mapping if and only if any non-trivial shift changes the value of the function g, i.e., for any tuple $(a_2, \ldots, a_n) \in E_k^{n-1}$ and any $a \in E_k$, $a \neq 0$, it holds that $g(a_2, \ldots, a_n) \neq g(a_2 + a, \ldots, a_n + a)$.*

Theorem 3.1 can be directly applied to the cases of PFN, type-1 PEFN (after renumbering) and type-4 PEFN. In the first two cases the function g is unary, so the condition on g in Theorem 3.1 is equivalent to bijectivity.

Corollary 3.3. *A mapping specified by PFN or by type-1 PEFN after renumbering is complete if and only if the function g is a bijection.*

Corollary 3.3 shows that sufficient completeness conditions established in [12] are actually necessary and sufficient.

If type-4 PEFN is rewritten as a generalized feedback shift register, then the function g takes the form $h(x_2 + \ldots + x_n)$, where h is a unary function. If h is not a bijection, i.e., some value $b \in E_k$ does not belong to the image of h, by Dirichlet box principle for any $(n-1)$-tuple $(a_2, \ldots, a_n)$ the set $\{h(a_2 + a + \ldots + a_n + a) \mid a \in E_k\}$ contains equal elements. Now assume that h is a bijection. Then the hypothesis of Theorem 3.1 holds if the equality $x_2 + x_3 + \ldots + x_n = (x_2 + a) + (x_3 + a) + \ldots + (x_n + a)$ is satisfied only for $a = 0$, or, equivalently, the equation

$$\underbrace{a + a + \ldots + a}_{n-1} = 0 \tag{10}$$

has a unique solution $a = 0$. By Lagrange's theorem there are no non-zero solutions if and only if $n-1$ and k are coprime. In paricular, if G

is isomorphic to $\mathbb{Z}_2^m$ for some $m \in \mathbb{N}$, then the equation (10) has a unique solution $a = 0$ if and only if $n-1$ is odd and thus n is even. Thus the following assertion holds.

Corollary 3.4. *A mapping specified by type-4 PEFN is complete if and only if the function g is a bijection and $(n-1)$ and k are coprime.*

Corollary 3.4 extends sufficient conditions obtained in [13] for the case of elementary Abelian 2-groups to necessary and sufficient conditions for arbitrary Abelian groups.

PGF-NLFSR can be considered in a similar way after another model generalization (i.e., replacing x_1 in the last line of (5) with $s(x_1)$, $s \in P_k^1$; if s is not a bijection, then, by the cardinality argument, σ is also non-bijective, otherwise Theorem 3.1 and Corollary 3.4 hold for the generalized construction).

Generalized feedback shift registers that satisfy the hypothesis of Theorem 3.1 specify quasigroup operations of the form

$$\begin{aligned} z_1 &= x_2 \pm y_2 + c_1 \mp y_1 \\ z_2 &= x_3 \pm y_3 + c_2 \mp y_2 \\ &\vdots \\ z_{n-1} &= x_n \pm y_n + c_{n-1} \mp y_{n-1} \\ z_n &= x_1 \pm y_1 + g(x_2 \pm y_2, \ldots, x_n \pm y_n) + c_n \mp y_n. \end{aligned} \tag{11}$$

It can be easily seen that changing the value of c_n can be compensated by shifting the value of the function g, thus without loss of generality one can assume that $c_n = 0$.

Remark 3.5. If $k = 2$, then the requirement imposed by Theorem 3.1 is equivalent to self-duality of the function g. Thus the construction (11) generates $2^{n-1} \cdot 2^{2^{n-2}}$ distinct quasigroup operations of the order 2^n.

If $k > 2$, then the requirement imposed on the function g can be written out in the following form. The set of input tuples is split into the union of equivalence classes with respect to shifts ($(a_2, \ldots, a_n) \sim (a_2', \ldots, a_n')$ if there exists a constant $a \in E_k$ such that $a_i = a_i' + a$, $i = 2, \ldots, n$). Obviously the cardinality of any class equals k, so the number of classes is the number of $(n-1)$-tuples divided by k, i.e., k^{n-2}. Different inputs from the same class give different outputs, so inside a class the function g is a permutation. For any class one can select the permutation arbitrarily ($k!$ options), thus the number of distinct quasigroups generated is $k^{n-1} \cdot (k!)^{k^{n-2}}$.

The considerations presented above lead to the following procedure that allows uniform sampling of quasigroups generated by generalized feedback shift registers. In the Boolean case ($k = 2$) one just has to perform uniform independent selection of the values of the function g on all tuples with $x_2 = 0$ and to extend the function by self-duality. If $k \geqslant 3$, then it is sufficient to select independent uniformly distributed permutations (e.g., with the help of well-known Fisher–Yates shuffle, see [4, p. 26–27]) for all equivalence classes. Constants $c_1, \ldots, c_{n-1}$ are selected independently and uniformly from the set E_k. Obviously, in both cases all results are equiprobable.

Now show that quasigroups specified by the relations (11) can not be generated by proper families over the group G or by permutation construction applied to proper families over the group G. The first assertion follows from the fact that the first variable is dummy for the first function of a proper family, thus the identity

$$x_2 \pm y_2 + c_1 \mp y_1 = x_1 + y_1 + g_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n))$$

can not be satisfied for any proper family, since the left-hand side does not contain x_1, but the right-hand side does.

Prove the following assertion required to consider the case of permutation construction.

Lemma 3.6. *Let $(g_1, \ldots, g_n)$ be a proper family, $p_1, \ldots, p_n \in P_k^2$ be arbitrary functions and*

$$h_i(x_1, \ldots, x_n, y_1, \ldots, y_n) = g_i(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)),\ i = 1, \ldots, n.$$

Then for any distinct $2n$-tuples $\alpha = (a_1, \ldots, a_n, b_1, \ldots, b_n)$ and $\alpha' = (a'_1, \ldots, a'_n, b'_1, \ldots, b'_n)$ from E_k^{2n} there exists an index j, $1 \leqslant j \leqslant n$, such that $(a_j, b_j) \neq (a'_j, b'_j)$, but $h_j(\alpha) = h_j(\alpha')$.

Proof. There are two possible cases. If $p_1(a_1, b_1) = p_1(a'_1, b'_1), \ldots, p_n(a_n, b_n) = p_n(a'_n, b'_n)$, then the assertion is trivial, since for any j such that $(a_j, b_j) \neq (a'_j, b'_j)$ it obviously holds that $h_j(\alpha) = h_j(\alpha')$.

Now, if $(p_1(a_1, b_1), \ldots, p_n(a_n, b_n))$ and $(p_1(a'_1, b'_1), \ldots, p_n(a'_n, b'_n))$ are distinct, then by definition of properness there exists an index j such that $p_j(a_j, b_j) \neq p_j(a'_j, b'_j)$ (and thus $(a_j, b_j) \neq (a'_j, b'_j)$) and $g_j(p_1(a_1, b_1), \ldots, p_n(a_n, b_n)) = g_j(p_1(a'_1, b'_1), \ldots, p_n(a'_n, b'_n))$. □

Theorem 3.7. *The classes of quasigroups generated by generalized feedback shift registers using relation (1) or (2) and by permutation construction applied to proper families over the group G are disjoint.*

Proof. We will conduct the proof for the case of the relation (1). The case of the relation (2) can be considered in a similar way. Assume that there exists a generalized feedback shift register that satisfies the hypothesis of Theorem 3.1, a proper family $(g_1, \ldots, g_n)$, functions $p_1, \ldots, p_n \in P_k^2$ and permutations β and γ (as it was noticed, without loss of generality one may assume that the permutation δ is identical) such that the corresponding quasigroup operations coincide, i.e. it holds that

$$x_{i+1} - y_{i+1} + c_i + y_i = x_{\beta(i)} + y_{\gamma(i)} + g_i(p_1(x_{\beta(1)}, y_{\gamma(1)}), \ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})) \tag{12}$$

for $i = 1, \ldots, n-1$ and

$$x_1 - y_1 + g(x_2 - y_2, \ldots, x_n - y_n) + y_n = \\ = x_{\beta(n)} + y_{\gamma(n)} + g_n(p_1(x_{\beta(1)}, y_{\gamma(1)}), \ldots, p_n(x_{\beta(n)}, y_{\gamma(n)})). \tag{13}$$

Since the ith variable is dummy for g_i, the identities (12) yield the equalities $\beta(i) = i + 1$, $\gamma(i) = i$, $i = 1, \ldots, n-1$. Since β and γ are permutations, $\beta(n) = 1$, $\gamma(n) = n$. Cancel equal terms on the left-hand and on the right-hand side of the identities (12), (13) and impose inverse permutations on variable indices to obtain the relations

$$\begin{aligned} &g_1(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_2 + c_1 \\ &g_2(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_3 + c_2 \\ &\vdots \\ &g_{n-1}(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_n + c_{n-1} \\ &g_n(p_1(x_1, y_1), \ldots, p_n(x_n, y_n)) = -y_1 + g(x_1 - y_2, \ldots, x_{n-1} - y_n). \end{aligned}$$

Substitute the values $x_1 = \ldots = x_n = y_1 = \ldots = y_n = 0$ and $x_1 = \ldots = x_n = y_1 = \ldots = y_n = 1$ in these relations. Note that the inputs of the function g for these substitutions coincide, and the subtracted values y_i are different. Thus there is no index j such that the values of g_j coincide for the substitutions considered, which contradicts Lemma 3.6. Thus the family $(g_1, \ldots, g_n)$ is not proper. □

4. Quasigroups and generalized Feistel networks

Theorem 4.8. *A generalized Feistel network specifies a complete mapping if and only if the mappings $s(x)$ and $s(x) + p(x) + x$ are bijective.*

Proof. First note that the relations (6) specify a permutation on E_k^2 if and only if s is a bijection. Indeed, if s is not bijective, then the cardinality

of the image of a generalized Feistel network is less than the cardinality of the preimage. Conversely, if s is a bijection, then obviously the inverse of the transform (6) is the mapping $(f_1 = x_2 - p\left(s^{-1}(x_1)\right), f_2 = s^{-1}(x_1))$. Further in the course of the proof we assume that s is a bijection.

Assume that $s(x) + p(x) - x$ is a bijection. Suppose that there exist pairs (x_1, x_2) and (y_1, y_2) such that

$$\begin{aligned} s(x_2) - x_1 &= s(y_2) - y_1 \\ x_1 + p(x_2) - x_2 &= y_1 + p(y_2) - y_2 \end{aligned} \tag{14}$$

Sum these equalities up to obtain the relation

$$s(x_2) + p(x_2) - x_2 = s(y_2) + p(y_2) - y_2,$$

thus by the assumption $x_2 = y_2$ and so $s(x_2) = s(y_2)$. The latter equality and the first equality of (14) directly imply the relation $x_1 = y_1$. Hence the mapping is complete.

Conversely, assume that there exist $x_2 \neq y_2$ such that $s(x_2) + p(x_2) - x_2 = s(y_2) + p(y_2) - y_2$. Let $x_1 = s(x_2)$, $y_1 = s(y_2)$ and note that the pairs (x_1, x_2) and (y_1, y_2) satisfy the relations (14). Thus, the mapping is not complete. □

By Theorem 4.8 the number of quasigroups specified by generalized Feistel networks via the relation (1) or (2) equals $(k!)^2$. Indeed, $s(x)$ and $s'(x) = s(x) + p(x) - x$ can be set equal to arbitrary permutations on E_k, and the function p can be easily recovered from s and s'. Uniform and independent selection of the permutations allows one to perform uniform sampling on the set of quasigroups generated.

Generalized Feistel networks specify quasigroup operations

$$\begin{aligned} f_1 &= s(x_2 \mp y_2) \pm y_1 \\ f_2 &= x_1 \mp y_1 + p(x_2 \mp y_2) \pm y_2 \end{aligned}$$

It can be easily shown that these operations can not be generated by proper families over the group G or by permutation construction applied to proper families over G. Indeed, any transformation of the functions f_1, f_2 to the form $x_i + y_j + g(p(x_{i'}, y_{j'}))$ is such that the third summand is not constant. On the other hand, all proper families of the size 2 must contain a constant function [6, Assertion 1].

5. Conclusion

We considered complete mappings specified by generalized feedback registers and generalized Feistel networks. In both cases, criteria for the mapping completeness have been established. A procedure for uniform sampling of quasigroups induced by complete mappings under study has been suggested. The classes of quasigroups generated by generalized feedback shift registers or generalized Feistel networks and by the permutation construction applied to proper families over the group G are shown to be disjoint.

6. Acknowledgments.

The research has been supported by the Interdisciplinary Scientific and Educational School of Moscow University "Brain, Cognitive Systems, Artificial Intelligence".

The authors thank the reviewer for correcting inaccuracies and useful remarks that contributed to the improvement of the presentation of the material.

The authors started this research in the framework of the Indo-Russian joint project "Quasigroup based cryptography: security, analysis and development of crypto-primitives and algorithms (QGSEC)" headed by V. A. Artamonov.

References

[1] **P.J. Cameron**, *Almost all quasigroups have rank* 2, Discrete Math. **106–107** (1992), 111 – 115.

[2] **I.V. Cherednik**, *Using binary operations to construct a transitive set of block transformations*, Discrete Math. Appl. **30** (2020), no. 6, 375 – 389.

[3] **I.V. Cherednik**, *On the use of binary operations for the construction of a multiply transitive class of block transformations*, Discrete Math. Appl. **31** (2021), no. 2, 91 – 111.

[4] **R.A. Fisher, F. Yates**, *Statistical tables for biological, agricultural and medical research*, London: Oliver & Boyd, 1948.

[5] **A.V. Galatenko, V.V. Galatenko, A.E. Pankratiev**, *Strong polynomial completeness of almost all quasigroups*, Math. Notes **111** (2022), no. 1, 7 – 12.

[6] **A.V. Galatenko, V.A. Nosov, A.E. Pankratiev**, *Latin squares over quasigroups*, Lobachevskii J. Math. **41** (2020), no. 2, 194 – 203.

[7] **D. Gligoroski, H. Mihajloska, D. Otte, M. El-Hadedy**, *GAGE and InGAGE*, http://gageingage.org/upload/GAGEandInGAGEv1.03.pdf

[8] **D. Gligoroski, R.S. Ødegård, M. Mihova, S.J. Knapskog, A. Drapal, V. Klíma, J. Amundse, M. El-Hadedy**, *Cryptographic hash function EDON-R′*, Proceedings of the 1st International Workshop on Security and Communication Networks, IWSCN (2009), 1 – 9.

[9] **M. M. Glukhov**, *Some applications of quasigroups in cryptography*, Prikl. Diskr. Mat. (2008), no. 2(2), 28 – 32.

[10] **S. Markovski, A. Mileva**, *NaSHA — family of cryptographic hash functions*, The First SHA-3 Candidate Conference, Leuven, 2009.

[11] **S. Markovski, A. Mileva**, *Generating huge quasigroups from small nonlinear bijections via extended Feistel function*, Quasigroups Related Systems **17** (2009), 91 – 106.

[12] **A. Mileva, S. Markovski**, *Shapeless quasigroups derived by Feistel orthomorphisms*, Glasnik Matematicki **47** (2012), no. 2, 333 – 349.

[13] **A. Mileva, S. Markovski**, *Quasigroup representation of some Feistel and Generalized Feistel ciphers*, Advances in Intelligent Systems and Computing — ICT Innovations 2012, **207**, Springer (2013), 161 – 171.

[14] **V.A. Nosov, A.E. Pankratiev**, *Latin squares over Abelian groups*, J. Math. Sci. **149** (2008), no. 3, 1230 – 1234.

[15] **N.A. Piven**, *Investigation of quasigroups generated by proper families of Boolean functions of order 2*, Intell. Syst. Theory Appl. **22** (2018), no. 1, 21 – 35.

[16] **N.A. Piven**, *Some properties of the permutation construction for parametric quasigroup specification*, Intell. Syst. Theory Appl. **23** (2019), no. 2, 71 – 78.

[17] **A. Sade**, *Quasigroups automorphes par le groupe cyclique*, Canadian J. Math. **9** (1957), 321 – 335.

[18] **V. A. Shcherbacov**, *Quasigroups in cryptology*, Comput. Sci. J. Mold. **17** (2009), no. 2(50), 193 – 228.

Received February 07, 2023

S. Chakrabarti*, S.K Tiwari
Scientific Analysis Group, DRDO, Delhi, India (* Former)
* Visiting Scientist (Honorary), Indian Statistical Institute, Kolkata, India
E-mail: suchetadrdo@hotmail.com, shrawant@gmail.com

A.V. Galatenko, V.A. Nosov, A.E. Pankratiev
Faculty of Mechanics and Mathematics, Lomonosov Moscow State University
Main Building, GSP-1, 1 Leninskiye Gory, Moscow, Russia
E-mail: agalat@msu.ru, vnosov40@mail.ru, apankrat@intsys.msu.ru

Quasigroups and Related Systems **31** (2023), 221 – 232

https://doi.org/10.56415/qrs.v31.17

Endomorphisms of precyclic n-groups

Sonia Dog and Nikolay A. Shchuchkin

Abstract. We characterize the sets of homomorphisms, endomorphisms and automorphisms of n-ary groups with cyclic retracts.

1. Introduction

Polyadic groups, called also n-ary groups or n-groups, are a generalization of groups. Therefore, n-group theory is closely related to group theory. It is known that for every n-group (G, f) there exists a group $(G, *)$ and its automorphism φ such that $f(x_1, \dots, x_n) = x_1 * \varphi(x_2) * \dots * \varphi^{n-1}(x_n) * b$, $\varphi^{n-1}(x) * b = b * x$ and $\varphi(b) = b$ for some element $b \in G$ (see for example [2]). Then we write $(G, f) = \mathrm{der}_{\varphi,b}(G, *)$. If in the n-group operation f we fix all inner elements, we get the operation $\diamond$ that depends only on two outer elements. The algebra $(G, \diamond)$ obtained in this way is a group called the *retract* of (G, f). All retracts of an n-group $(G, f) = \mathrm{der}_{\varphi,a}(G, *)$ are isomorphic to the group $(G, *)$ (see [3]). Therefore, we can assume that $x \diamond y = f(x, a, \dots, a, y)$. We then write $(G, \diamond) = \mathrm{ret}_a(G, f)$. Moreover, for each $a \in G$, the mapping $\varphi(x) = f(\overline{a}, x, a, \dots, a)$ is an automorphism of the group $(G, \diamond)$ and $(G, f) = \mathrm{der}_{\varphi,b}(\mathrm{ret}_a(G, f))$ for $b = f(\overline{a}, \dots, \overline{a})$, where $\overline{a}$ is such that $f(a, \dots, a, \overline{a}) = a$ (see [3]). An n-group with an abelian retract is called *semiabelian*. In [5] it is shown that an n-group is semiabelian if and only if it is medial (entropic). In this case φ^{n-1} is the identity mapping.

An n-group with a cyclic retract is called *precyclic* (in Russian terminology – *semicyclic*). An infinite precyclic n-group is isomorphic to the n-group $(\mathbb{Z}, f_l) = \mathrm{der}_{1,l}(\mathbb{Z}, +)$, $0 \leqslant l \leqslant \frac{n-1}{2}$, or to the n-group $(\mathbb{Z}, f_{(-1)}) = \mathrm{der}_{-1,0}(\mathbb{Z}, +)$ (for odd n only) [6]. The first is type $(\infty, 1, l)$, the second type $(\infty, -1, 0)$. A finite precyclic n-group of order m is isomorphic to the n-group $\mathrm{der}_{1,l}(\mathbb{Z}_m, +)$ with $l | gcd(m, n-1)$ or to the n-group $\mathrm{der}_{k,l}(\mathbb{Z}_m, +)$,

2010 Mathematics Subject Classification: 20N15.

Keywords: Semiabelian n-group, precyclic n-group, endomorphism, automorphism, $(n, 2)$-semiring.

where $k > 1$, $gcd(k, m) = 1$, $k^{n-1} = 1(\mathrm{mod}\, m)$, $kl = l(\mathrm{mod}\, m)$ and $l|gcd(m, S_k)$, $S_k = 1 + k + k^2 + \ldots + k^{n-2} = \frac{k^{n-1}-1}{k-1}$. We say (cf. [6]) that the first is type $(m, 1, l)$, the second is type (m, k, l).

First we will show that the set of all homomorphisms from a precyclic n-group into a semiabelian n-group forms an n-group. Next we characterize $(n, 2)$-semirings of endomorphisms of precyclic n-groups. Some of our results were inspired by theorems proved in [7] and [8]. We give them in a more general, more useful version. We also provide new, simpler and shorter proofs.

For simplicity, the sequence $x_i, x_{i+1}, \ldots, x_j$ will be written as x_i^j; the sequence $x, x, \ldots, x$ (k times) as $\overset{(k)}{x}$. We also assume that $n > 2$.

2. Homomorphisms of precyclic n-groups

Using the mediality it is not difficult to see that the set $\mathrm{Hom}(G, G')$ of all homomorphisms of an n-group (G, f) into a semiabelian n-group (G', f') forms a semiabelian n-group with respect the n-ary operation F defined by

$$F(h_1, h_2, \ldots, h_n)(x) = f'(h_1(x), h_2(x), \ldots, h_n(x)),$$

where the homomorphism skew to h is defined by $\overline{h}(x) = \overline{h(x)}$.

Note that if an n-group (G', f') has no dempotents, the set $\mathrm{Hom}(G, G')$ may be empty. This is the case, for example, with the 5-groups $(\mathbb{Z}_6, f)$ and $(\mathbb{Z}_4, f')$ 1-derived from the additive groups $\mathbb{Z}_6$ an $\mathbb{Z}_4$, respectively. Indeed, for any homomorphism $h : (\mathbb{Z}_6, f) \to (\mathbb{Z}_4, f')$ there will be $h(0) = c$, $h(1) = hf(0, 0, 0, 0, 0) = f'(h(0), h(0), h(0), h(0), h(0)) = c + 1$, $h(2) = hf(1, 0, 0, 0, 0) = h(1) + 4c + 1 = c + 2$. So, $h(k) = c + k(\mathrm{mod}\, 4)$. But then $h(1) = hf(1, 4, 0, 0, 0) = h(1) + h(4) + 3c + 1 = c + 2(\mathrm{mod}\, 4)$ which is impossible.

Let's start with lemmas that will be needed later. The first lemma is obvious, the second is a modification of Theorem 3 from [4]

Lemma 2.1. *Consider the diagram*

$$\begin{array}{ccc} (G, f) & \xrightarrow{\psi} & (H, f_1) \\ \downarrow{\scriptstyle \lambda_G} & & \downarrow{\scriptstyle \lambda_H} \\ (G', f') & \xrightarrow{\psi'} & (H', f_1') \end{array}$$

where ψ and ψ' are isomorphism of the corresponding n-groups. If λ_G, λ_H are homomorphisms of n-groups, and n-groups (G', f'), (H', f') are semiabelian, then $\mathrm{Hom}(G, G')$ *and* $\mathrm{Hom}(H, H')$ *form isomorphic n-groups. This isomorphism acts according to the rule $\Phi(\alpha) = \psi'\alpha\psi^{-1}$.*

The converse is not true. This is the case, for example, when G' has only one element.

Lemma 2.2. *A mapping h from an n-group* $\mathrm{der}_{\varphi,a}(G, *)$ *into a semiabelian n-group* $\mathrm{der}_{\psi,d}(G', \cdot)$ *is an n-group homomorphism if and only if there exists an element $c \in G'$ and a group homomorphism $\beta : (G, *) \to (G', \cdot)$ such that $\beta\varphi = \psi\beta$, $h = R_c\beta$ and $\beta(a) = D(c) \cdot d$, where $R_c(x) = x \cdot c$ for all $x \in G'$ and $D(c) = c \cdot \psi(c) \cdot \psi^2(c) \cdot \ldots \cdot \psi^{n-2}(c)$.*

Proof. Let $(G, f) = \mathrm{der}_{\varphi,a}(G, *)$ and $(G', f') = \mathrm{der}_{\psi,d}(G', \cdot)$ be two n-groups and let (G', f') be semiabelian.

If there exists a group homomorphism $\beta : (G, *) \to (G', \cdot)$ such that $\beta\varphi = \psi\beta$ and $\beta(a) = D(c) \cdot d$ for some fixed $c \in G'$, then for $h(x) = \beta(x) \cdot c$ we have

$$\begin{aligned}
h(f(x_1^n)) &= \beta(f(x_1^n)) \cdot c = \beta(x_1 * \varphi(x_2) * \ldots * \varphi^{n-1}(x_n) * a) \cdot c \\
&= \beta(x_1) \cdot \beta\varphi(x_2) \cdot \ldots \cdot \beta\varphi^{n-1}(x_n) \cdot \beta(a) \cdot c \\
&= \beta(x_1) \cdot \psi\beta(x_2) \cdot \ldots \cdot \psi^{n-1}\beta(x_n) \cdot D(c) \cdot d \cdot c \\
&= \beta(x_1) \cdot \psi\beta(x_2) \cdot \ldots \cdot \psi^{n-1}\beta(x_n) \cdot c \cdot \psi(c) \cdot \ldots \cdot \psi^{n-2}(c) \cdot d \cdot c \\
&= (\beta(x_1) \cdot c) \cdot \psi(\beta(x_2) \cdot c) \cdot \ldots \cdot \psi^{n-1}(\beta(x_n) \cdot c) \cdot d \\
&= h(x_1) \cdot \psi h(x_2) \cdot \ldots \cdot \psi^{n-1}h(x_n) \cdot d \\
&= f'(h(x_1), h(x_2), \ldots, h(x_n)).
\end{aligned}$$

Hence $h : G \to G'$ is an n-group homomorphism.

Conversely, let $h : (G, f) \to (G', f')$ be an n-group homomorphism and $(G, \circ) = \mathrm{ret}_a(G, f)$, $(G', \diamond) = \mathrm{ret}_b(G', f')$. Then $\beta : (G, \circ) \to (G', \diamond)$ defined by $\beta'(x) = f'(h(x), \overset{(n-2)}{h(a)}, \overline{a})$ is a homomorphism. Since $\overline{a}$ and $\overline{b}$ are neutral elements of these groups, $\beta'(\overline{a}) = \overline{b}$.

Let $\overline{a} = h(g)$ for some $g \in G$. Then
$\beta'(x) = f'(h(x), \overset{(n-2)}{h(a)}, \overline{a}) = f'(h(x), \overset{(n-2)}{h(a)}, h(g)) = h(f(x, \overset{(n-2)}{a}, g)) = h(x \circ g)$.

Thus $h(\overline{a}) = h(g^{-1} \circ g) = h(g^{-1})$.

Now, denoting $h(g^{-1})$ by c', we obtain

$$h(x) = h(x \circ g^{-1} \circ g) = \beta'(x \circ g^{-1}) = \beta'(x) \diamond \beta'(g^{-1}) = \beta'(x) \diamond c'.$$

All retracts of an n-group $\mathrm{der}_{\varphi,b}(G,\star)$ are isomorphic to $(G,\star)$ (cf. [3]), so $(G,\circ)$ and $(G,*)$, also $(G',\diamond)$ and $(G',\cdot)$, are isomorphic. Thus, a group homomorphism β' corresponds to some homomorphism $\beta : (G,*) \to (G,\cdot)$. Hence $h(x) = \beta(x) \cdot c$, i.e. $h = R_c\beta$ for some $c \in G'$.

Since $h : (G,f) \to (G',f')$ is a homomorphism of n-groups,

$$h(f(x_1^n)) = f'(h(x_1), h(x_2), \ldots, h(x_n))$$

implies

$$\beta(f(x_1^n)) \cdot c = f'(\beta(x_1) \cdot c, \beta(x_2) \cdot c, \ldots, \beta(x_n) \cdot c).$$

Consequently,

$$\beta(x_1) \cdot \beta\varphi(x_2) \cdot \beta\varphi^2(x_3) \cdot \ldots \cdot \beta\varphi^{n-1}(x_n) \cdot \beta(a) \cdot c$$
$$= (\beta(x_1) \cdot c) \cdot \psi(\beta(x_2) \cdot c) \cdot \psi^2(\beta(x_3) \cdot c) \cdot \ldots \cdot \psi^{n-1}(\beta(x_n) \cdot c) \cdot d.$$

From this, putting $x_i = \overline{a}$ for all $i = 1, 2, \ldots, n$, we obtain

$$\beta(a) \cdot c = c \cdot \psi(c) \cdot \psi^2(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot b = D(c) \cdot \psi^{n-1}(c) \cdot d = D(c) \cdot d \cdot c,$$

which shows that $\beta(a) = D(c) \cdot d$.

Putting in the previous identity $x_2 = x$ and $x_i = \overline{a}$ for other x_i we get

$$\begin{aligned} \beta\varphi(x) \cdot \beta(a) \cdot c &= c \cdot \psi\beta(x) \cdot \psi(c) \cdot \psi^2(c) \cdot \ldots \cdot \varphi^{n-1}(c) \cdot d \\ &= \psi\beta(x) \cdot D(c) \cdot d \cdot c = \psi\beta(x) \cdot \beta(a) \cdot c. \end{aligned}$$

Thus $\beta\varphi = \psi\beta$, which completes the proof. □

As a consequence of the above lemma we obtain

Corollary 2.3. *A mapping h from an n-group $\mathrm{der}_{\varphi,a}(G,*)$ into a semiabelian n-group $\mathrm{der}_{\psi,d}(G',\cdot)$ is an n-group homomorphism if and only if there exists an element $c \in G'$ such that $\beta = h \cdot c^{-1}$ is a group homomorphism from $(G,*)$ into $(G',\cdot)$, $\beta\varphi = \psi\beta$ and $\beta(a) = D(c) \cdot d$.*

Let $(G,f) = \mathrm{der}_{\varphi,a}(G,*)$ and $(G',f') = \mathrm{der}_{\psi,d}(G',\cdot)$. If (G',f') is a semiabelian n-group, then each homomorphism $h_i \in \mathrm{Hom}(G,G')$ has the form $h_i = R_{c_i}\beta_i$, where β_i and c_i are as in the above lemma. Consequently,

$$\begin{aligned}F(h_1^n)(x) &= f'(h_1(x), h_2(x), \dots, h_{n-1}(x), h_n(x))\\ &= f'(\beta_1(x)\cdot c_1, \beta_2(x)\cdot c_2, \dots, \beta_{n-1}(x)\cdot c_{n-1}, \beta_n(x)\cdot c_n)\\ &= (\beta_1(x)\cdot c_1)\cdot \psi(\beta_2(x)\cdot c_2)\cdot \ldots \cdot \psi^{n-2}(\beta_{n-1}(x)\cdot c_{n-1})\cdot(\beta_n(x_n)\cdot c_n)\cdot d\\ &= \beta_1(x)\cdot\psi\beta_2(x)\cdot\ldots\cdot\psi^{n-2}\beta_{n-1}(x)\cdot\beta_n(x)\cdot c_1\cdot\psi(c_2)\cdot\ldots\cdot\psi^{n-2}(c_{n-1})\cdot c_n\cdot d\\ &= \beta_1(x)\cdot\psi\beta_2(x)\cdot\ldots\cdot\psi^{n-2}\beta_{n-1}(x)\cdot\beta_n(x)\cdot f'(c_1^n) = \beta(x)\cdot f'(c_1^n),\end{aligned}$$

where $\beta = \beta_1\cdot\psi\beta_2\cdot\ldots\cdot\psi^{n-2}\beta_{n-1}\cdot\beta_n = \beta_1\cdot\beta_2\varphi\cdot\ldots\cdot\beta_{n-1}\varphi^{n-2}\cdot\beta_n$ is a homomorphism from $(G,*)$ to $(G',\cdot)$. Thus,

$$F(h_1^n) = R_u\beta, \quad \text{where} \quad u = f'(c_1^n), \quad \beta = \beta_1\cdot\beta_2\varphi\cdot\ldots\cdot\beta_{n-1}\varphi^{n-2}\cdot\beta_n. \quad (1)$$

Let (G',f') be a semiabelian n-group. Then $(G',\cdot) = \mathrm{ret}_a(G',f')$ is an abelian group (for any $a\in G'$) and $(G',f') = \mathrm{der}_{\psi,d}(G',\cdot)$ for $d = f'(\overset{(n)}{\overline{a}})$ and $\psi(x) = f'(\overline{a}, x, \overset{(n-2)}{a})$. Moreover, $D(x) = x\cdot\psi(x)\cdot\psi^2(x)\cdot\ldots\cdot\psi^{n-2}(x)$ is an endomorphism of $(G',\cdot)$ such that $\psi(d\cdot D(x)) = d\cdot D(x) = f'(\overset{(n-1)}{x}, \overline{a})$ for every $x\in G'$.

We will use these facts to describe the set of homomorphisms of precyclic n-groups. We'll start with precyclic n-groups of type $(\infty,1,l)$.

First, for $(G',f') = \mathrm{der}_{\psi,d}(G',\cdot)$ and an arbitrary natural l we define the set

$$G'_{(l,d)} = \{(z,c)\,|\,\psi(z) = z,\ z^l = d\cdot D(c)\} \subseteq G'\times G'.$$

Using the mediality of (G',f') and the above facts, we can see that $G'_{(l,d)}$ with the operation

$$g'((z_1,c_1),(z_2,c_2),\dots,(z_n,c_n)) = (z_1\cdot z_2\cdot\ldots\cdot z_n, f'(c_1^n)) \quad (2)$$

is a semiabelian n-group.

Theorem 2.4. *If the set of all homomorphisms from a precyclic n-group (G,f) of type $(\infty,1,l)$ into a semiabelian n-group $(G',f') = \mathrm{der}_{\psi,d}(G',\cdot)$ is nonempty, then it forms an n-group isomorphic to the n-group $(G'_{(l,d)}, g')$.*

Proof. Any precyclic n-group of type $(\infty,1,l)$ is isomorphic to the n-group $(\mathbb{Z},f_l) = \mathrm{der}_{1,l}(\mathbb{Z},+)$. Let h be a homomorphism from $(\mathbb{Z},f_l)$ into a semiabelian n-group $(G',f') = \mathrm{der}_{\psi,d}(G',\cdot)$. Then, according to Lemma 2.2, $h = R_c\beta$ for some homomorphism β from $(\mathbb{Z},+)$ to $(G',\cdot)$, $\beta(x) = \psi(\beta(x))$ and $\beta(l) = d\cdot D(c)$ for some $c\in G'$. Any homomorphism β of a cyclic

group is determined by the value of β on the generator of this group. So, if $\beta(1) = z$, then $z = \beta(1) = \psi\beta(1) = \psi(z)$ and $z^l = \beta(l) = d \cdot D(c)$. Hence, any homomorphism $h : (\mathbb{Z}, f_l) \to (G', f')$ determines one pair $(z, c) \in G'_{(l,d)}$.

On the other side, for each pair $(z, c) \in G'_{(l,d)}$ there is only one homomorphism $\beta : (\mathbb{Z}, +) \to (G', \cdot)$ such that $\beta(1) = z$. Hence $\beta(k) = z^k$. Thus $\psi\beta(k) = \psi(z^k) = \psi(z)^k = z^k = \beta(k)$ for every $k \in \mathbb{Z}$. So, $\psi\beta = \beta$ and $\beta(l) = z^l = d \cdot D(c)$.

This shows that the pair (z, c) uniquely determines the homomorphism $h = R_c\beta$ with $\beta(1) = z$. So, there is one-to-one correspondence between elements of the set $\mathrm{Hom}(G, G')$ and elements of the set $G'_{(l,d)}$. Denote this correspondence by τ, i.e. $\tau(h_i) = (z_i, c_i)$ for $h_i = R_{c_i}\beta_i$ and $z_i = \beta_1(1)$. Then $\beta_i(k) = \beta_i(k1) = \beta_i(1)^k = z_i^k$.

Since $\beta(1) = (\beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_n)(1) = z_1 \cdot z_2 \cdot \ldots \cdot z_n$,

$$\begin{aligned}\tau(F(h_1^n)) &= (z_1 \cdot z_2 \cdot \ldots \cdot z_n, f'(c_1^n)) = g((z_1, c_1), (z_2, c_2), \ldots, (z_n, c_n)) \\ &= g(\tau(h_1), \tau(h_2), \ldots, \tau(h_n)).\end{aligned}$$

Hence τ is an isomorphism. □

Since $z^k = \beta(k) = e$ for $k \in \operatorname{Ker}\beta$, the first coordinate of each pair $(z, c) \in G'_{(l,d)}$ has finite order in the group $(G', \cdot)$.

All precyclic n-groups of type $(\infty, -1, 0)$ are idempotent and exist only for odd n. All such n-groups can be identified with the n-group $(\mathbb{Z}, f_{(-1)}) = \mathrm{der}_{-1,0}(\mathbb{Z}, +)$. The homomorphic image of the idempotent n-group is also the n-idempotent group. This means that the homomorphism from $(\mathbb{Z}, f_{(-1)})$ into the n-group (G', f') exists only if (G', f') has at least one idemotent. By Lemma 2.2, any such homomorphism has the form $h = R_c\beta$, where $\beta(0) = D(c) \cdot d$ and $\psi\beta(x) = \beta(x)^{-1}$ for $x \in \mathbb{Z}$. So, $D(c) = d^{-1}$ and $\psi(z) = z^{-1}$ for $z \in \beta(\mathbb{Z})$. Moreover, $h(0) = R_c\beta(0) = c$. Consequently, $c = h(0) = hf_{(-1)}(\overset{(n)}{0}) = f'(\overset{(n)}{h(0)}) = f'(\overset{(n)}{c})$. Thus as a consequence of Lemma 2.2 we obtain

Lemma 2.5. *A mapping h from an n-group $\mathrm{der}_{-1,0}(\mathbb{Z}, +)$ into a semiabelian n-group $\mathrm{der}_{\psi,d}(G', \cdot)$ is an n-group homomorphism if and only if there exists an idempotent $c \in G'$ and a group homomorphism $\beta : (\mathbb{Z}, +) \to (G', \cdot)$ such that $h = R_c\beta$, $D(c) = d^{-1}$ and $\beta(x)^{-1} = \psi\beta(x)$ for $x \in \mathbb{Z}$.*

The proofs of the following theorems is very similar to the proof of Theorem 2.4. So we skip them.

Theorem 2.6. *If the set of all homomorphisms from a precyclic n-group of type $(\infty, -1, 0)$ into a semiabelian n-group $(G', f') = \mathrm{der}_{\psi,d}(G', \cdot)$ is nonempty, then it forms an n-group isomorphic to the n-group (G''_d, g''), where*

$$G''_d = \{(z, c) \mid \psi(z) = z^{-1},\ D(c) = d^{-1}\} \subseteq G' \times G' \quad \textit{and}$$
$$g''((z_1, c_1), (z_2, c_2), \ldots, (z_n, c_n)) = (z_1 \cdot z_2^{-1} \cdot z_3 \cdot z_4^{-1} \cdot \ldots \cdot z_{n-1}^{-1} \cdot z_n, f'(c_1^n)).$$

Theorem 2.7. *If the set of all homomorphisms from a precyclic n-group of type (m, k, l) with $k \geqslant 1$, into a semiabelian n-group $(G', f') = \mathrm{der}_{\psi,d}(G', \cdot)$ is nonempty, then it forms an n-group isomorphic to the n-group $(G'_{(l,d)}, g')$.*

Example 2.8. Let us consider three 5-groups: $(G_1, f_1) = \mathrm{der}_{5,3}(\mathbb{Z}_6, +)$, $(G_2, f_1) = \mathrm{der}_{1,1}(\mathbb{Z}, +)$ and $(G', f') = \mathrm{der}_{1,1}(\mathbb{Z}_4, +)$. Then, as already mentioned, the set $\mathrm{Hom}(G_1, G')$ is empty. The set $\mathrm{Hom}(G_1, G')$ contains four homomorphisms. They are defined by $h_c(x) = r + c (\mathrm{mod}\, 4)$, where $x = 4t + r$, $0 \leqslant r < 4$ and $c = 0, 1, 2, 3$. $\mathrm{Hom}(G', G')$ also contains four homomorphisms, namely $h_c(x) = x + c (\mathrm{mod}\, 4)$, $c = 0, 1, 2, 3$.

3. Endomoprhisms of precyclic n-groups

Recall that an $(n, 2)$-*nearring* $(G, f, \cdot)$ is an n-group (G, f) with an associative multiplication such that

$$a \cdot f(x_1^n) = f(\{a \cdot x_i\}_1^n) \quad \text{and} \quad f(x_1^n) \cdot a = f(\{x_i \cdot a\}_1^n)$$

for all $a, x_1^n \in G$. An $(n, 2)$-nearring $(G, f, \cdot)$ with a semiabelian n-group (G, f) is called an $(n, 2)$-*semiring*; with an abelian n-group – an $(n, 2)$-*ring*.

In [5] it is noted that the set $\mathrm{End}(G, f)$ of all endomorphisms of a semiabelian n-group (G, f) forms an $(n, 2)$-semiring with respect to the n-ary operation F defined as for homomorphisms and an ordinary superposition of endomorphisms. The set of all endomorphisms of an abelian n-group forms an $(n, 2)$-ring with unity.

Based on the results of the previous section, we can characterize $(n, 2)$-semirings of endomorphisms of precyclic n-groups. For this we will use the following lemma which is a consequence of Lemma 2.2.

Lemma 3.1. *A mapping $h : \mathbb{Z} \to \mathbb{Z}$ is an endomorphism of an n-group $(\mathbb{Z}, f_l)$ of type $(\infty, 1, l)$ if and only if here exists an element $c \in \mathbb{Z}$ and an endomorphism β of $(\mathbb{Z}, +)$ such that $h = R_c\beta$ and $\beta(l) = (n-1)c + l$.*

Let $h = R_c\beta$ be an endomorphism of $(\mathbb{Z}, f_l)$. Then $h(0) = c$. Hence, if $\beta(1) = m$, then $\beta(l) = \beta(l1) = l\beta(1) = lm$. So, $lm = (n-1)c + l$, i.e. for fixed m, n and l there is only one c satisfying this equation. This means that each endomorphism of $(\mathbb{Z}, f_l)$ depends only on m and has the form $h_m(x) = xm + c_m$, where $c_m = h_m(0)$ and $ml = l(\mathrm{mod}\,(n-1))$. So, $\tau(h_m) = m$ is a bijection from the set $\mathrm{End}(\mathbb{Z}, f_l)$ onto the set

$$\mathbb{Z}_{(l,n)} = \{m \,|\, ml = l(\mathrm{mod}\,(n-1))\} \subseteq \mathbb{Z}.$$

This is an $(n, 2)$-semiring with respect to the operation

$$g'(m_1, m_2, \ldots, m_n) = m_1 + m_2 + \ldots + m_n$$

and an ordinary multiplication of numbers.

Since $lm = (n-1)c + l$ means that $c = \frac{l(m-1)}{n-1}$, we have

$$\begin{aligned}
&F(h_{m_1}, h_{m_2}, \ldots, h_{m_n})(z) = f_l(h_{m_1}(z), h_{m_2}(z), \ldots, h_{m_n}(z)) \\
&= (zm_1 + c_{m_1}) + (zm_2 + c_{m_2}) + \ldots + (zm_n + c_{m_n}) + l \\
&= z(m_1 + m_2 + \ldots + m_n) + f_l(c_{m_1}, c_{m_2}, \ldots, c_{m_n}) \\
&= z(m_1 + m_2 + \ldots + m_n) + \tfrac{l(m_1+m_2+\ldots+m_n-n)}{n-1} + l \\
&= z(m_1 + m_2 + \ldots + m_n) + \tfrac{l(m_1+m_2+\ldots+m_n-1)}{n-1} \\
&= z(m_1 + m_2 + \ldots + m_n) + c_{m_1+m_2+\ldots+m_n} = h_{m_1+m_2+\ldots+m_n}(z).
\end{aligned}$$

Hence $\tau(F(h_{m_1}, h_{m_2}, \ldots, h_{m_n})) = g'(\tau(h_{m_1}), \tau(h_{m_2}), \ldots, \tau(h_{m_n}))$.

Also $\tau(h_{m_1} \circ h_{m_2}) = \tau(h_{m_1}) \cdot \tau(h_{m_2})$.

So, τ is an isomorphism between $(\mathrm{End}(\mathbb{Z}, f_l), F, \circ)$ and $(\mathbb{Z}_{(l,n)}, g', \cdot)$.

Theorem 3.2. *The set of endomorphisms of a precyclic n-group of type $(\infty, 1, l)$ forms an $(n, 2)$-semiring isomorphic to $(\mathbb{Z}_{(l,n)}, g', \cdot)$.*

Endomorphisms of precyclic n-groups of type $(\infty, -1, 0)$ are characterized by

Lemma 3.3. *A mapping $h : \mathbb{Z} \to \mathbb{Z}$ is an endomorphism of a precyclic n-group of type $(\infty, -1, 0)$ if and only if $h(x) = mx + c$ for some $m, c \in \mathbb{Z}$.*

Using the same method as in the proof of Theorem 3.2 we obtain

Theorem 3.4. *The set of all endomorphisms of a precyclic n-group $(\mathbb{Z}, f_{(-1)})$ of type $(\infty, -1, 0)$ forms an $(n,2)$-semiring isomorphic to the $(n,2)$-semiring $(\mathbb{Z}\times\mathbb{Z}, g, *)$, where*

$$g((m_1,c_1),(m_2,c_2),\dots,(m_n,c_n)) = (f_{(-1)}(m_1^n), f_{(-1)}(c_1^n)) \quad \textit{and}$$
$$(m_1,c_1)*(m_2,c_2) = (m_1m_2, m_1c_2+c_1).$$

For endomorphisms of precyclic n-groups of type (m,k,l) we have

Theorem 3.5. *A mapping $h\colon \mathbb{Z}_m \to \mathbb{Z}_m$ is an endomorphism of an n-group $(\mathbb{Z}_m, f_{(k,l)})$ if and only if $h(x) = tx + c (\mathrm{mod}\, m)$ and $tl = S_kc + l (\mathrm{mod}\, m)$ for some $t, c \in \mathbb{Z}_m$. Such endomorphisms forms an $(n,2)$-semiring isomorphic to the $(n,2)$-semiring $(\mathbb{Z}_m^{(k,b)}, g, *)$, where*

$$\mathbb{Z}_m^{(k,l)} = \{(t,c) \mid t,c \in \mathbb{Z}_m,\ tl = S_kc + l (\mathrm{mod}\, m)\},$$
$$g((t_1,c_1),(t_2,c_2),\dots,(t_n,c_n)) = (f_{(k,0)}(t_1^n), f_{(k,l)}(c_1^n)) \quad \textit{and}$$
$$(t_1,c_1)*(t_2,c_2) = (t_1t_1, t_1c_2+c_1).$$

Proof. Each endomorphism of $(\mathbb{Z}_m, +)$ has the form $\beta(x) = tx (\mathrm{mod}\, m)$. Hence, by Lemma 2.2, $h\colon \mathbb{Z}_m \to \mathbb{Z}_m$ is an endomorphism of an n-group $(\mathbb{Z}_m, f_{(k,l)})$ if and only if $h(x) = \beta(x) + c = tx + c (\mathrm{mod}\, m)$ for some $c \in \mathbb{Z}_m$ such that $\beta(l) = D(c) + l$. But $D(c) = c + kc + k^2c + \ldots + k^{n-2}c = S_kc$. So, $\beta(l) = tl = S_kc + l (\mathrm{mod}\, m)$. In $\mathbb{Z}_m$ there is only one c satisfying this equation. Indeed, if $\beta(l) = D(c) + l$, then $\beta(x) + d = h(x) = \beta(x) + c$, whence $c = d (\mathrm{mod}\, m)$. Thus, $\tau(h) = (t,c)$ is a bijection between the set of all endomorphism of $(\mathbb{Z}_m, f_{(k,l)})$ and $\mathbb{Z}_m^{(k,l)}$.

Moreover, for all $h_1,\dots,h_n \in \mathrm{End}(\mathbb{Z}_m, f_{(k,l)})$ we have

$$\begin{aligned}
&F(h_1^n)(x) = f_{(k,l)}(h_1(x), h_2(x), \dots, h_n(x))\\
&= (t_1x+c_1)+k(t_1+c_1)+k^2(t_2x+c_2)+\ldots+k^{n-2}(t_{n-1}x+c_{n-1})+(t_nx+c_n)+l\\
&= (t_1 + kt_2 + \ldots + k^{n-2}t_{n-1} + t_n)x + (c_1 + kc_2 + \ldots + k^{n-2}c_{n-1} + c_n + l)\\
&= f_{(k,0)}(x) + f_{(k,l)}(c_1^n) = h_{f_{(k,0)}} + f_{(k,l)}.
\end{aligned}$$

Hence

$$\begin{aligned}
\tau(F(h_1^n)) &= (f_{(k,0)}, f_{(k,b)}) = g((t_1,c_1),(t_2,c_2),\dots,(t_n,c_n))\\
&= g(\tau(h_1), \tau(h_2), \dots, \tau(h_n)),
\end{aligned}$$

which shows that τ is an isomorphism. □

Observe that in the above proof for fixed k and l the element c is uniquely determined by t, so an endomorphism $h = R_c\beta$ of $(\mathbb{Z}_m, f_{(k,l)})$ is uniquely determined by the value of $t = \beta(1)$. Thus, the the set $\mathbb{Z}_m^{(k,l)}$ can be identified with the set $\mathbb{P}_m^{(k,l)} = \{t \in \mathbb{Z}_m \,|\, tb = S_k c + l (\mathrm{mod}\, m)\}$. Consequently, the $(n,2)$-semiring $(\mathbb{Z}_m^{(k,l)}, g, *)$ can be identified with the $(n,2)$-semiring $(\mathbb{P}_m^{(k.l)}, f_{(k,0)}, \cdot)$, where $\cdot$ is an ordinary multiplication modulo m.

4. Automoprhisms of precyclic n-groups

A binary composition (superposition) of automorphisms of a fixed n-group is an automorphism of this n-group. Thus for a given n-group (G, f) the set $\mathrm{Aut}(G, f)$ of all its automorphisms is a group contained in the semigroup $\mathrm{End}(G, f)$. Hence, as a consequence of the above results, we obtain

Proposition 4.1. *A mapping $h : G \to G$ is an automorphism of a semiabelian n-group $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$ if and only if there exists $c \in G$ and an automorphism β of $(G, \cdot)$ such that $\beta\varphi = \varphi\beta$, $h = R_c\beta$ and $\beta(a) = D(c) \cdot a$.*

Theorem 3.10 in [1] implies the following characterization:

Proposition 4.2. *A mapping $h : G \to G$ is an automorphism of a semiabelian n-group $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$ if and only if $h = R_c\beta$, where β is an automorphism of $(G, \cdot)$, $\beta(a) = a$ and $\varphi(c) = c = c^n$.*

Corollary 4.3. *Let $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$ be a precyclic n-group, $c \in G$ and $\beta \in \mathrm{Aut}(G, \cdot)$. Then $h = R_c\beta \in \mathrm{Aut}(G, f)$ if and only if $R_c \in \mathrm{Aut}(G, f)$ and $\beta \in \mathrm{Aut}(G, f)$.*

Proof. If $h = R_c\beta$ is an automorphism of $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$, then, by the above Propositions, $\beta\varphi = \varphi\beta$ and $\beta(a) = a$. Hence, as it is not difficult to see, β is an automorphism of (G, f). Consequently, also $R_c = h\beta^{-1}$ is an automorphism of (G, f). The converse statement is obvious. □

The above fact also follows from the results proven in [1].

Theorem 4.4. *If $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$ is a precyclic n-group, then*

$$\mathrm{Aut}(G, f) \cong \mathcal{R}_\varphi(G, f) \ltimes \mathrm{Aut}_a(G, \cdot),$$

where

$$\mathcal{R}_\varphi(G, f) = \{R_c \,|\, \varphi(c) = c = c^n\} \quad \text{and}$$
$$\mathrm{Aut}_a(G, \cdot) = \{\beta \in \mathrm{Aut}(G, \cdot) \,|\, \beta(a) = a\}.$$

Proof. $\mathcal{R}_\varphi(G,f)$ and $\mathrm{Aut}_a(G,\cdot)$ are subgroups of $\mathrm{Aut}(G,f)$ and $\mathrm{Aut}(G,\cdot)$, respectively. $(G,\cdot)$ is abelian, so $\mathcal{R}_\varphi(G,f)$ is a normal subgroup. Moreover, if $\psi \in \mathcal{R}_\varphi(G,f) \cap \mathrm{Aut}_a(G,\cdot)$, then $\varphi = R_c = \beta$. Thus, $R_c(a) = \beta(a) = a$, which gives $c = e$. Therefore, $\mathcal{R}_\varphi(G,f) \cap \mathrm{Aut}_a(G,\cdot) = \{\varepsilon\}$. Consequently, $\mathrm{Aut}(G,f) \cong \mathcal{R}_\varphi(G,f) \ltimes \mathrm{Aut}_a(G,\cdot)$. □

Theorem 4.5. *If a precyclic n-group $(G,f) = \mathrm{der}_{\varphi,a}(G,\cdot)$ has at least one idempotent, then*

$$\mathrm{Aut}(G,f) \cong \mathcal{R}_{E(G,f)} \ltimes \mathrm{Aut}(G,\cdot),$$

where $\mathcal{R}_{E(G,f)}$ is a group of right translations of $(G,\cdot)$ determined by idempotent elements.

Proof. Let $(G,f) = \mathrm{der}_{\varphi,a}(G,\cdot)$ be a precyclic n-group containing at least one idempotent. We will show first that (G,f) is isomorphic to $(G,g) = \mathrm{der}_\varphi(G,\cdot)$.

Let c be an idempotent of (G,f). Then

$$c = f(c,c,\dots,c) = c \cdot \varphi(c) \cdot \varphi^2(c) \cdot \ldots \cdot \varphi^{n-2}(c) \cdot c \cdot a. \tag{3}$$

Thus,

$$a \cdot c^{-1} = c^{-1} \cdot \varphi(c^{-1}) \cdot \varphi^2(c^{-1}) \cdot \ldots \cdot \varphi^{n-2}(c^{-1}) \cdot c^{-1}. \tag{4}$$

Hence

$$\begin{aligned}
&R_{c^{-1}} f(x_1^n) = x_1 \cdot \varphi(x_2) \cdot \varphi^2(x_3) \cdot \ldots \cdot \varphi^{n-2}(x_{n-1}) \cdot x_n \cdot a \cdot c^{-1} \\
&\overset{(4)}{=} x_1 \cdot c^{-1} \cdot \varphi(x_2) \cdot \varphi(c^{-1}) \cdot \varphi^2(x_3) \cdot \varphi^2(c^{-1}) \cdot \ldots \cdot \varphi^{n-2}(x_{n-1}) \cdot \varphi^{n-2}(c^{-1}) \cdot x_n \cdot c^{-1} \\
&= x_1 \cdot c^{-1} \cdot \varphi(x_2 \cdot c^{-1}) \cdot \varphi^2(x_3 \cdot c^{-1}) \cdot \ldots \cdot \varphi^{n-2}(x_{n-1} \cdot c^{-1}) \cdot x_n \cdot c^{-1} \\
&= R_{c^{-1}}(x_1) \cdot \varphi R_{c^{-1}}(x_2) \cdot \varphi^2 R_{c^{-1}} \cdot \ldots \cdot \varphi^{n-2} R_{c^{-1}}(x_{n-1}) \cdot R_{c^{-1}}(x_n) \\
&= g(R_{c^{-1}}(x_1), R_{c^{-1}}(x_2), \dots, R_{c^{-1}}(x_n)).
\end{aligned}$$

Therefore $R_{c^{-1}} : (G,f) \to (G,g)$ is a homomorphism. Since it is a bijection, $(G,f) \cong (G,g)$. Then also $\mathrm{Aut}(G,f) \cong \mathrm{Aut}(G,g)$ and $\mathcal{R}_{E(G,f)} \cong \mathcal{R}_{E(G,g)}$. So it is sufficient to prove our theorem for (G,g).

The neutral element of $(G,\cdot)$ is an idempotent of (G,g). Thus the set $\mathcal{R}_{E(G,g)}$ is nonempty and $R_b R_c = R_{c \cdot b}$ for all $R_c, R_b \in \mathcal{R}_{E(G,g)}$ because, by (3), $c \cdot b$ is an idempotent. Thus $\mathcal{R}_{E(G,g)}$ is a subgroup of $\mathrm{Aut}(G,g)$ such that $(R_b\beta)^{-1} \circ R_c \circ R_b\beta = R_{\beta^{-1}(c)}$ for $R_b\beta \in \mathrm{Aut}(G,g)$ and $R_c \in \mathcal{R}_{E_{(G,g)}}$. Since, $\beta^{-1}(c) = \beta^{-1}g(c,c,\dots,c) = g(\beta^{-1}(c), \beta^{-1}(c), \dots, \beta^{-1}(c))$, by Corollary

4.3, $\beta^{-1}(c)$ is an idempotent of (G, g). Consequently, $R_{\beta^{-1}(c)} \in \mathcal{R}_{E(G,g)}$, which shows that $\mathcal{R}_{E(G,g)}$ is a normal subgroup of $\mathrm{Aut}(G, g)$. Moreover, $\mathcal{R}_{E(G,g)} \cap \mathrm{Aut}(G, \cdot) = \{\varepsilon\}$. So, $\mathrm{Aut}(G, g) \cong \mathcal{R}_{E(G,g)} \ltimes \mathrm{Aut}(G, \cdot)$. □

Corollary 4.6. *If a precyclic n-group* $(G, f) = \mathrm{der}_{\varphi,a}(G, \cdot)$ *has only one idempotent, then*

$$\mathrm{Aut}(G, f) \cong \mathrm{Aut}(G, \cdot)$$

References

[1] **W.A. Dudek,** *Automorphisms of n-ary groups*, Results Math. **77** (2022), paper no. 46.

[2] **W.A. Dudek, K. Głazek,** *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

[3] **W.A. Dudek, J. Michalski,** *On a generalization of Hosszú theorem*, Demonstratio Math. **15** (1982), 783 – 805.

[4] **W.A. Dudek, J. Michalski,** *On retracts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

[5] **K. Głazek, B. Gleichgewicht,** *Abelian n-groups*, Coll. Math. Soc. J. Bolyai, 29. Universal Algebra, Esztergom (Hungary) 1977, 321 – 329.

[6] **N.A. Shchuchkin,** *Semicyclic n-ary groups,* (Russian), Izv. F. Skaryna Univ., Gomel, **3** (2009), 186 – 194.

[7] **N.A. Shchuchkin,** *Homomorphisms from infinite semilcyclic n-groups to a semiabelian n-group*, (Russian), Chebyshevskiĭ Sb. **22** (2021), 340 – 352.

[8] **N.A. Shchuchkin,** *Endomorphisms of semicyclic n-groups*, (Russian), Chebyshevskiĭ Sb. **22** (2021), 353 – 369.

Received August 24, 2023

S. Dog
22 Pervomayskaya str, 39600 Kremenchuk, Ukraine
Temporary address: WSB Merito University, Wroclaw, Poland
Email: soniadog2@gmail.com

N.A. Shchuchkin
Volgograd State Pedagogical University, Lenina prosp., 27, 400131 Volgograd, Russia
Email: nikolaj_shchuchkin@mail.ru