Quasigroups and Related Systems **18** (2010), 1 − 6

Finite GS–quasigroups

Yahya Amad and M. Aslam Malik

Abstract. This paper is concerned with the determination of the set of possible orders of finite GS-quasigroups. Also some examples of finite GS-quasigroups are given.

1. Introduction

The following definition of GS-quasigroups was given by V.Volenec in [4] and [1].

Definition 1.1. A quasigroup $(Q,\cdot)$ is said to be *GS-quasigroup* (*golden section quasigroup*) if the equalities

$$\begin{aligned} aa &= a, \\ a(ab\cdot c)\cdot c &= b, \\ a\cdot(a\cdot bc)c &= b \end{aligned}$$

hold for all its elements.

The study of GS-quasigroups in [4] is motivated by:

Example 1.2. Let $\mathbb{C}$ be set of complex numbers and $*$ an operation on set $\mathbb{C}$ defined by:

$$a * b = \frac{1-\sqrt{5}}{2}a + \frac{1+\sqrt{5}}{2}b.$$

Let us regard complex numbers as points of the Euclidean plane, then the point b divides the pair a and $a * b$ in the ratio of golden section, which justifies the term of GS-quasigroups.

Here, we'll give some examples of finite GS-quasaigroups, and determine: $for\ which\ positive\ integer\ n\ there\ exists\ a\ GS-quasigroup\ of\ order\ n$?

We require the following elementary results, whose proofs are simple.

2000 Mathematics Subject Classification:
Keywords: golden section, square free, finite quasigroup.

Lemma 1.3. *Let* $(G_1, \cdot_1), (G_2, \cdot_2), \ldots, (G_n, \cdot_n)$ *be* $GS-quasigroups$*, and* $\circ$ *be the operation defined on* $G = G_1 \times G_2 \times \ldots \times G_n$ *by:*

$$(x_1, x_2, \ldots, x_n) \circ (y_1, y_2, \ldots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \ldots, x_n \cdot_n y_n).$$

Then $(G, \circ)$ *is a* $GS-quasigroup.$

Therefore, if GS-quasigroups of orders $k_1, k_2, \ldots, k_n$ exist, then a GS-quasigroup of order $k_1 k_2 \cdots k_n$ exists.

The following characterization of GS-quasigroups was given in [4].

Theorem 1.4. *A* $GS-quasigroup$ *on the set* Q *exists if and only if on the same set exists a commutative group* $(Q, +)$ *with an automorphism* φ *satisfying the identity*

$$(\varphi \circ \varphi)(x) - \varphi(x) - x = 0. \tag{1}$$

Then

$$a \cdot b = a + \varphi(b - a). \tag{2}$$

2. Commutative GS-quasigroups

By using Theorem 1.4 to study commutative GS-quasigroups we want to find all commutative groups $(Q, +)$ with an automorphism φ satisfying (1) and with the additional condition that the operation $\cdot$ defined by (2) is commutative. The commutativity of $\cdot$ implies

$$a + \varphi(b - a) = b + \varphi(a - b).$$

Thus

$$\varphi(b - a) - \varphi(a - b) = b - a,$$

and consequently

$$\varphi(x) + \varphi(x) = x \tag{3}$$

for all $x \in Q$.

From (1) it follows $\varphi(\varphi(x)) + \varphi(\varphi(x)) = \varphi(x) + \varphi(x) + x + x$, which by (3) gives $\varphi(x) = x + x + x$. Substituting this to (3) we get,

$$x + x + x + x + x + x = x.$$

Therefore, $x + x + x + x + x = 0$ for all $x \in Q$, i.e., each element of the group $(Q, +)$ is of order 5 or 1. The only finite groups which satisfy that condition are $(\mathbb{Z}_5)^n$, and the group of order 1.

On the other hand, if $x + x + x + x + x = 0$, for all $x \in Q$, then $\varphi(x) = x + x + x = -x - x$, i.e. $\varphi(x) = 3x = -2x$ is an automorphism satisfying (1) and the operation defined by (2) is commutative.

Thus we have proved:

Theorem 2.1. *The only non-trivial finite commutative $GS-$quasigroups are the quasigroups obtained in the technique described in Theorem* 1.4 *from the group* $(\mathbb{Z}_5)^n$, *for some* $n \in \mathbb{N}$.

From each group $(\mathbb{Z}_5)^n$ we obtain unique GS-quasigroup of order 5^n.

Example 2.2. From the group $(\mathbb{Z}_5)^2$ and the automorphism $\varphi(x) = 3x = -2x$ we obtain the GS-quasigroup of order 25:

$\cdot_{25}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
0	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12
1	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10
2	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13
3	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11
4	2	0	3	1	4	17	15	18	16	19	7	5	8	21	9	22	20	23	21	24	12	10	13	11	14
5	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2
6	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0
7	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3
8	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1
9	17	15	18	16	19	7	5	8	6	9	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4
10	5	8	6	9	7	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17
11	8	6	9	7	5	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15
12	6	9	7	5	8	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18
13	9	7	5	8	6	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16
14	7	5	8	6	9	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19
15	20	23	21	24	22	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7
16	23	21	24	22	20	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5
17	21	24	22	20	23	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8
18	24	22	20	23	21	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6
19	22	20	23	21	24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19	7	5	8	6	9
20	10	13	11	14	12	0	3	1	4	2	15	18	16	19	17	5	8	6	9	7	20	23	21	24	22
21	13	11	14	12	10	3	1	4	2	0	18	16	19	17	15	8	6	9	7	5	23	21	24	22	20
22	11	14	12	10	13	1	4	2	0	3	16	19	17	15	18	6	9	7	5	8	21	24	22	20	23
23	14	12	10	13	11	4	2	0	3	1	19	17	15	18	16	9	7	5	8	6	24	22	20	23	21
24	12	10	13	11	14	2	0	3	1	4	17	15	18	16	19	7	5	8	6	9	22	20	23	21	24

2. Cyclic groups

The automorphism $\varphi(x) = mx$ (m is relatively prime to n) of the group $\mathbb{Z}_n$ satisfies (1) if and only if $m^2 - m - 1 \equiv 0(\operatorname{mod} n)$.

Now by using Quadratic Reciprocity Law we want to find for which $n \in \mathbb{N}$ the quadratic congruence has solution m (in that case m and n are relatively prime).

Since $m^2 - m - 1$ is odd, n cannot be even. Therefore, it seems appropriate to begin by considering the congruence

$$m^2 - m - 1 \equiv 0(\operatorname{mod} p),$$

where p is an odd prime and $gcd(1, p) = 1$. The assumption that p is an odd prime implies that $gcd(4, p) = 1$. Thus, the quadratic congruence is equivalent to

$$4(m^2 - m - 1) \equiv 0(\operatorname{mod} p).$$

Now, completing the square we obtain

$$4(m^2 - m - 1) = (2m - 1)^2 - 5$$

The last quadratic congruence may be expressed as

$$(2m - 1)^2 \equiv 5(\operatorname{mod} p).$$

Now, putting $y = 2m - 1$ in last congruence, we get

$$y^2 \equiv 5(modp)$$

Thus, 5 is quadratic residue of p if and only if $p = \pm 1(\operatorname{mod} 5)$. So, that the solutions are all primes of the form $p = 5l \pm 1$, $l \in \mathbb{Z}$. Factors of $m^2 - m - 1$ are all primes of the form $p = 5l \pm 1$.

This proves the following:

Theorem 2.1. *The cyclic group $\mathbb{Z}_n$ has an automorphism that satisfies* (1) *if and only if its order n is a product of primes from the set* $\{5l \pm 1\}$*, where $l \in \mathbb{Z}$, i.e., if and only if n is an odd integer with any prime factor is congruent to* ± 1 *modulo* 5.

Example 2.2. The group $\mathbb{Z}_{11}$ has two such automorphisms: $\varphi(x) = 4x$ and $\varphi(x) = 8x$. So, we obtain two GS-quasigroups of order 11.

One induced by $\varphi(x) = 4x$:

$\cdot_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	4	8	1	5	9	2	6	10	3	7
1	8	1	5	9	2	6	10	3	7	0	4
2	5	9	2	6	10	3	7	0	4	8	1
3	2	6	10	3	7	0	4	8	1	5	9
4	10	3	7	0	4	8	1	5	9	2	6
5	7	0	4	8	1	5	9	2	6	10	3
6	4	8	1	5	9	2	6	10	3	7	0
7	1	5	9	2	6	10	3	7	0	4	8
8	9	2	6	10	3	7	0	4	8	1	5
9	6	10	3	7	0	4	8	1	5	9	2
10	3	7	0	4	8	1	5	9	5	6	10

and one induced by $\varphi(x) = 8x$:

$\cdot_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	8	5	2	10	7	4	1	9	6	3
1	4	1	9	6	3	0	8	5	2	10	7
2	8	5	2	10	7	4	1	9	6	3	0
3	1	9	6	3	0	8	5	2	10	7	4
4	5	2	10	7	4	1	9	6	3	0	8
5	9	6	3	0	8	5	2	10	7	4	1
6	2	10	7	4	1	9	6	3	0	8	5
7	6	3	0	8	5	2	10	7	4	1	9
8	10	7	4	1	9	6	3	0	8	5	2
9	3	0	8	5	2	10	7	4	1	9	6
10	7	4	1	9	6	3	0	8	5	2	10

Remark 2.3. Let p be an odd prime and suppose $k \geqslant 1$. If $(a, p) = 1$, then $x^2 \equiv a (\bmod p^k)$ has either no solutions or exactly two solutions, according as $x^2 \equiv a (\bmod p)$ is or not solvable.

Corollary 2.4. *The cyclic group $\mathbb{Z}_{p^k}$ has an automorphism satisfying* (1) *if and only if p is a prime from the set $\{5l \pm 1 : l \in \mathbb{Z}\}$, i.e., if and only if $p \equiv \pm 1 (\bmod 5)$.*

3. Conclusions

The following theorem is simple but crucial.

Theorem 3.1. *Let G be a commutative group of order $m_1 m_2$, where m_1 and m_2 are relatively prime positive integers, with an automorphism φ satisfying* (1)*. Then there exist groups G_1 and G_2 such that $G = G_1 \times G_2$, $|G_1| = m_1$, $|G_2| = m_1$ with automorphisms satisfying* (1).

Example 3.2. The group $\mathbb{Z}_{55} = \mathbb{Z}_5 \times \mathbb{Z}_{11}$ has two automorphisms $\varphi(x) = 8x$ and $\varphi(x) = 48x$ satisfying (1). $\mathbb{Z}_5$ and $\mathbb{Z}_{11}$ have automorphisms $\varphi(x) = 3x$ and $\varphi(x) = 4x$, $\varphi(x) = 8x$ satisfying (1), respectively.

So, for GS-quasigroups of orders 5^k and p^k, where p is a prime of the form $5l \pm 1$ there is no any GS-quasigroup of order p^k such that $p \neq 5l \pm 1$.

Thus the final result:

Theorem 3.3. *Let $n = \prod_{i=1}^{n} l_i$ be square free number. Then a $GS-$quasigroup of order n exists if and only if each prime factor of n is congruent to ± 1 modulo 5, i.e., if and only if $l_i \equiv \pm 1 (\bmod 5)$ for all $1 \leqslant i \leqslant n$.*

Acknowledgment. The authors wishes to thank Lyudmyla Turowska professor and Torbjörn Lundh associate professor at the Department of Mathematics of Chalmers University of Technology and Göteborg University for very valuable suggestions. Special thanks for Dr. Shahid S. Siddiqi and Dr. Muhammad Sharif.

References

[1] **Z. Kolar-Begović and V. Volenec**, *DGS-trapezoids in GS-quasigroups*, Math. Commun. **8** (2003), 215 – 218.

[2] **Z. Kolar-Begović and V. Volenec**, *Affine regular dodecahedron in GS-quasigroups*, Quasigroups and Related Systems **13** (2005), 229 – 236.

[3] **Z. Kolar-Begović and V. Volenec**, *GS-deltoids in GS-quasigroups*, Math. Commun. **10** (2005), 117 – 122.

[4] **V. Volenec**, *GS-quasigroups*, Čas. pěst. mat. **115** (1990), 307 – 318.

[5] **V. Volenec and Z. Kolar**, *GS-trapezoids in GS-quasigroups*, Math. Commun. **7** (2002), 143 – 158.

[6] **V. Volenec and Z. Kolar-Begović**, *Affine-regular pentagons in GS-quasigroups*, Quasigroups and Related System **12** (2004), 103 – 112.

[7] **V. Volenec and Z. Kolar-Begović**, *Affine regular decagons in GS-quasigroups*, Comment. Math. Univ. Carolin. **49** (2008), 383 – 395.

Received July 27, 2009

Y.Amad:
Department of Mathematical Sciences, Chalmers University of Technology and University of Gothenburg, SE-41296, Gothenburg, Sweden, E-mail: yahyamajeed2001@hotmail.com
M.A.Malik:
Department of Mathematics, University of the Punjab, Quaid-e-Azam Campus, Lahore-54590, Pakistan, E-mail: malikpu@yahoo.com

Quasigroups and Related Systems **18** (2010), 7 – 16

Check character systems and totally conjugate orthogonal T-quasigroups

Galina B. Belyavskaya

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. We continue investigations of check character systems with one check character over quasigroups under check equations without a permutation. These systems always detect all single errors (i.e., errors in only one component of a code word) and can detect some other errors occuring during transmission of data. For construction of such systems we use totally conjugate orthogonal T-quasigroups. These quasigroups are isotopic to abelian groups and have six mutually orthogonal conjugate quasigroups. We prove that a check character system over any totally conjugate orthogonal T-quasigroup is able to detect all transpositions and twin errors and establish additional properties of a totally conjugate orthogonal T-quasigroup by which such system can detect all jump transpositions and all jump twin errors. Some models of totally conjugate orthogonal T-quasigroups which satisfy all of the required properties for detection of each of the considered types of errors and an information with respect to the spectrum of such quasigroups are given.

1. Introduction

In this article we deal with error detecting systems (codes) with a single control symbol. Such systems have specific applications and are used for the detection of certain types of errors. More exactly, we study check character (or digit) systems with one check character.

A check character system (CCS) with one check character is an error detecting code over an alphabet A which arises by appending a check digit a_n to every word $a_1a_2...a_{n-1} \in A^{n-1} : A^{n-1} \to A^n, a_1a_2...a_{n-1} \to a_1a_2...a_{n-1}a_n$.

2000 Mathematics Subject Classification: 94B60, 20N05
Keywords: check character system, T-quasigroup, conjugate orthogonal quasigroup, orthomorphism.

The purpose of using such a system is to detect transmission errors (which can arise once in a code word), in particular, made by human operators during typing of data. These errors can be distinct types: single errors (that is errors in only one component of a code word), (adjacent) transpositions, i.e., errors of the form $\dots ab \dots \longrightarrow \dots ba \dots$, jump transpositions $(\dots abc \dots \to \dots cba \dots)$, twin errors $(\dots aa \dots \to \dots bb \dots)$, jump twin errors $(\dots aca \dots \to \dots bcb \dots)$ and so on can be made by human operators. Single errors and transpositions are the most prevalent ones.

The examples of check character systems used in practice are the following:

- the European Article Number (EAN) Code,
- the Universal Product Code (UPC),
- the International Standard Book Number (ISNB) Code,
- the system of the serial numbers of German banknotes,
- different bar-codes used in the service of transportation, automation of various processes and so on.

The work of I. Verhoeff [13] is the first significant publication relating to these systems. In this work decimal codes known in the 1970s are presented. A. Ecker and G. Poch in [8] have given a survey of check character systems and their analysis from a mathematical point of view. In particular, the group-theoretical background of the known methods was explained and new codes were presented that stem from the theory of quasigroups. Studies of check character systems were continued by R.-H. Schulz in [12]. He established necessary and sufficient conditions for a quasigroup with control formula (3) (see below) to detect transpositions and jump transpositions not only in information digits but, in addition, in the control digit of a code word $a_1a_2...a_n$. The complete survey of check character systems using quasigroups one can find in [3] due to G.B. Belyavskaya, V.I. Izbash, and V.A. Shcherbacov.

The control digit of a system based on a quasigroup (system over a quasigroup) is calculated by distinct check formulas (check equations) using quasigroup operations.

Choosing $Q(\cdot)$ as a finite set endowed with a binary algebraic structure (a groupoid) we can take one of the following general check (coding) formulas for calculation of the control symbol a_n:

$$a_n = (\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3) \dots) \cdot \delta_{n-1} a_{n-1} \tag{1}$$

$$(\dots((\delta_1 a_1 \cdot \delta_2 a_2) \cdot \delta_3 a_3) \dots) \cdot \delta_n a_n = c \tag{2}$$

for fixed permutations δ_i of Q, $i = 1, 2, \ldots, n$ and a fixed element c of Q.

It is easy to see that a CCS with check formula (1) or (2) detects all single errors if and only if $Q(\cdot)$ is a quasigroup. The other errors will be detected if and only if this quasigroup has specific properties.

Often a permutation δ_i in (1), (2) is chosen such that $\delta_i = \delta^{i-1}$, $i = 1, \ldots, n$, for a fixed permutation δ of Q. In this case we obtain the following check formulas respectively:

$$a_n = (\ldots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3) \ldots) \cdot \delta^{n-2} a_{n-1}, \tag{3}$$

$$(\ldots((a_1 \cdot \delta a_2) \cdot \delta^2 a_3) \ldots) \cdot \delta^{n-1} a_n = c. \tag{4}$$

In [4] CCSs over quasigroups with the check equation (3) or (4) are studied. In the article [5], which is a continue of [4], CCSs over T-quasigroups are considered, some properties of a T-quasigroup so that the CCS over it is able to detect transpositions, jump transpositions, twin errors and jump twin errors are established. Besides, some models of T-quasigroups, which satisfy all of the required properties for detection of errors of each of the considered types are given.

It is known that if a CCS over a quasigroup detects some of five considered types of errors, then this quasigroup has orthogonal mate (see, for example, [4, Corollary 1 and Corollary 5], [2, Proposition 3]).

On the other hand, in the article [6] the quasigroups, all six conjugates of which are distinct and pairwise orthogonal, are studied. Such quasigroups were called totally conjugate orthogonal quasigroups (shortly, *totCO*-quasigroups). Necessary and sufficient conditions that a T-quasigroup be a *totCO*-quasigroup (a *totCO*-T-quasigroup) are established.

In this article we continue to research check character systems with one check character over quasigroups under the check equation (3) or (4) when $\delta = \varepsilon$, $n > 4$. For constructing of such systems we use totally conjugate orthogonal T-quasigroups. These quasigroups generalize medial quasigroups and have six mutually orthogonal conjugate quasigroups.

We prove that a CCS over any totally conjugate orthogonal T-quasigroup is able to detect, besides single errors, all transpositions and all twin errors and establish additional properties of a totally conjugate orthogonal T-quasigroup such that a system over it can detect all jump transpositions and all jump twin errors. Some models of totally conjugate orthogonal T-quasigroups which satisfy all of the required properties to detect each of the considered types of errors and an information with respect to the spectrum of such quasigroups are given.

2. Check character systems over T-quasigroups

In this section we remind some necessary notions and results of [4,5] with respect to the check character systems using T-quasigroups.

A *quasigroup* is an ordered pair (Q, A) (or $(Q, \cdot)$) where Q is a set and A (or $\cdot$) is a binary operation defined on Q such that each of the equations $A(a, y) = b$ and $A(x, a) = b$ is uniquely solvable for any pair of elements a, b in Q. It is known that the multiplication table of a finite quasigroup defines a Latin square [7].

A quasigroup $Q(\cdot)$ is called a *T-quasigroup* if there exist an abelian group $Q(+)$, with automorphisms φ and ψ, and an element $c{\in}Q$ such that

$$x \cdot y = \varphi x + \psi y + c$$

for all $x, y \in Q$. Such quasigroups were considered by T. Kepka and P. Nemec in [10]. They are special cases of quasigroups, which are isotopic to abelian groups and generalize the well-known class of *medial quasigroups* when, in addition, the automorphisms φ and ψ commute, that is $\varphi\psi = \psi\varphi$. Note that below maps in a composition act from the right to the left.

A permutation α of a group $Q(+)$ is called an *orthomorphism* (respectively a *complete mapping*) if $x - \alpha x = \beta x$ $(x + \alpha x = \beta x)$ where β is a permutation of Q and $-x = Ix$ is the inverse element for x in the group $Q(+)$ [9]. It is easy to see (cf. [9]) that an automorphism α of a finite group $Q(+)$ is an orthomorphism if and only if α is a regular automorphism, that is the identity 0 of the group $Q(+)$ is the only element of Q fixed by α : $\alpha x \neq x$ if $x \neq 0$. If α is an orthomorphism, then $I\alpha$ is a complete mapping of $Q(+)$. A *complete mapping* of a quasigroup $Q(\cdot)$ is a bijective mapping $x \to \theta x$ of Q onto Q such that the mapping $x \to \eta x$ defined by $\eta x = x \cdot \theta x$ is again a bijective mapping of Q onto Q.

Denote by $OrtQ(+)$ the set of all orthomorphisms of a group $Q(+)$. In [5] the following theorems with respect to check character systems over T-quasigroups were proved (Theorem 1, Theorem 2 and Theorem 4 of [5] respectively) which we shall use.

Theorem 1. **[5]** *A check character system using a finite T-quasigroup $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ and check formula* (3) *with $n > 4$ is able to detect*

1. *single errors;*
2. *transpositions if and only if $\psi\delta\varphi^{-1}$, $\psi\delta\psi^{-1}\varphi^{-1}$, $I\psi\delta^{n-2} \in OrtQ(+)$;*
3. *jump transpositions if and only if $\psi\delta^2\varphi^{-2}$, $\psi\delta^2\psi^{-1}\varphi^{-2}$, $I\varphi\psi\delta^{n-3}$ are in $OrtQ(+)$;*

4. *twin errors if and only if* $i\psi\delta\varphi^{-1}$, $I\psi\delta\psi^{-1}\varphi^{-1}$, $\psi\delta^{n-2} \in OrtQ(+)$;
5. *jump twin errors if and only if* $I\psi\delta^2\varphi^{-2}$, $I\psi\delta^2\psi^{-1}\varphi^{-2}$, $\varphi\psi\delta^{n-3}$ *are in* $OrtQ(+)$. □

Theorem 2. **[5]** *In Theorem* 1 *let* $\delta = \varepsilon$. *Then a check character system detects*

1. *single errors;*
2. *transpositions if and only if the automorphisms* $\varphi\psi^{-1}$, φ, $I\psi$ *are regular;*
3. *jump transpositions if and only if the automorphisms* $\varphi^2\psi^{-1}$, φ^2, $I\varphi\psi$ *are regular;*
4. *twin errors if and only if the automorphisms* $I\varphi\psi^{-1}$, $I\varphi$, ψ *are regular;*
5. *jump twin errors if and only if the automorphisms* $I\varphi^2\psi^{-1}$, $I\varphi^2$, $\varphi\psi$ *are regular.* □

Theorem 3. **[5]** *A check character system using a finite* T*-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formula* (4) *with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions if and only if the automorphisms* φ *and* $\varphi\psi^{-1}$ *are regular;*
3. *jump transpositions if and only if the automorphisms* φ^2 *and* $\varphi^2\psi^{-1}$ *are regular;*
4. *twin errors if and only if the automorphisms* $I\varphi$, $I\varphi\psi^{-1}$ *are regular;*
5. *jump twin errors if and only if the automorphisms* $I\varphi^2$ *and* $I\varphi^2\psi^{-1}$ *are regular.* □

3. Totally conjugate orthogonal T-quasigroups

In this section we shall give some necessary notions and results of [6] with respect to the totally conjugate orthogonal T-quasigroups.

With any quasigroup (Q, A) the system Σ of six (not necessarily distinct) *conjugates* (*parastrophes*) is connected:

$$\Sigma = \left\{A, A^{-1}, {}^{-1}A, {}^{-1}\left(A^{-1}\right), ({}^{-1}A)^{-1}, A^*\right\},$$

where $A(x, y) = z \Leftrightarrow A^{-1}(x, z) = y \Leftrightarrow {}^{-1}A(z, y) = x \Leftrightarrow A^*(y, x) = z$.

It is known [11] that the number of distinct conjugates in Σ can be 1,2,3 or 6. Using suitable Belousov's designation of conjugates of a quasigroup (Q, A) of [1] we have the following system Σ of conjugates:

$$\Sigma = \left\{A,\ {}^{r}\!A,\ {}^{l}\!A,\ {}^{lr}\!A,\ {}^{rl}\!A,\ {}^{s}\!A\right\},$$

where ${}^{1}\!A = A$, ${}^{r}\!A = A^{-1}$, ${}^{l}\!A = {}^{-1}\!A$, ${}^{lr}\!A = {}^{-1}(A^{-1})$, ${}^{rl}\!A = ({}^{-1}\!A)^{-1}, {}^{s}\!A = A^{*}$. Note that $\left({}^{-1}(A^{-1})\right)^{-1} = {}^{rlr}\!A = {}^{-1}\left(({}^{-1}\!A)^{-1}\right) = {}^{lrl}\!A = {}^{s}\!A$ and ${}^{rr}\!A = {}^{ll}\!A = A$, ${}^{\sigma\tau}\!A = {}^{\sigma}({}^{\tau}\!A)$.

Two quasigroups (Q, A) and (Q, B) are *orthogonal* if the system of equations $\{A(x, y) = a,\ B(x, y) = b\}$ is uniquely solvable for all $a, b \in Q$.

A set $\Sigma = \{A_1, A_2, ..., A_n\}$ of quasigroups, defined on the same set, is orthogonal if any two quasigroups of it are orthogonal.

Quasigroups which are *orthogonal* to some their conjugates or two conjugates of which are orthogonal (known as *conjugate orthogonal or parastrophic-orthogonal quasigroups*) have encouraged great interest.

In [6] the quasigroups (Q, A) all conjugates of which are pairwise orthogonal and the spectrum of such quasigroups were considered. For these quasigroups the set of all conjugates $\Sigma = \left\{A,\ {}^{r}\!A,\ {}^{l}\!A,\ {}^{lr}\!A,\ {}^{rl}\!A,\ {}^{s}\!A\right\}$ is orthogonal.

Definition 1. **[6]** A quasigroup (Q, A) is called *totally conjugate orthogonal* (shortly, a *totCO-quasigroup*) if all its conjugates are pairwise orthogonal.

It is clear that a *totCO*-quasigroup is invariant with respect to the transformation of conjugation (that is if a quasigroup (Q, A) is a *totCO*-quasigroup then the quasigroup $(Q, {}^{\sigma}\!A)$ is also a *totCO*-quasigroup for any conjugate ${}^{\sigma}\!A$) and that all conjugates of a *totCO*-quasigroup are distinct.

Let φ and ψ be automorphisms of an abelian group $(Q, +)$ and $(\varphi + \psi)x = \varphi x + \psi x$ for any $x \in Q$, then $\varphi + \psi$ is an endomorphism of group $(Q, +)$. It is known that all endomorphisms of an abelian group form an associative ring with a unity under the operations of addition and multiplication.

Theorem 4. **[6]** *Let (Q, A) be a finite or infinite T-quasigroup of the form $A(x, y) = \varphi x + \psi y$. Then two its conjugates are orthogonal if and only if the maps corresponding to these conjugates:*

$(1 \perp l \ \mathit{or}\ s \perp lr) \to \varphi + \varepsilon,\quad (r \perp rl) \to \varphi + \varepsilon \ \mathit{and}\ \varphi - \varepsilon,$

$(1 \perp r \ \mathit{or}\ s \perp rl) \to \psi + \varepsilon,\quad (l \perp lr) \to \psi + \varepsilon \ \mathit{and}\ \psi - \varepsilon,$

$(1 \perp lr \ \mathit{or}\ s \perp l) \to \varphi + \psi^2,\quad (1 \perp rl \ \mathit{or}\ s \perp r) \to \varphi^2 + \psi,$

$(r \perp lr$ *or* $rl \perp l) \rightarrow \varphi - \psi$, $\quad (1 \perp s) \rightarrow \varphi - \psi$ *and* $\varphi + \psi$,
$(l \perp r$ *or* $lr \perp rl) \rightarrow \psi\varphi - \varepsilon$ *are permutations.* □

As it was noted in [6], for a T-quasigroup of the form $A(x,y) = \varphi x + \psi y + c$ with $c \neq 0$ the conditions of Theorem 4 are the same and do not depend on the element c. So if a T-quasigroup (Q,A): $A(x,y) = \varphi x + \psi y$ is a $totCO$-quasigroup, then the T-quasigroup (Q,B): $B(x,y) = \varphi x + \psi y + c$ is also a $totCO$-quasigroup for any $c \in Q$.

Theorem 5. [6] *A T-quasigroup (Q,A): $A(x,y) = \varphi x + \psi y + c$ is a $totCO$-quasigroup if and only if all maps $\varphi + \varepsilon$, $\varphi - \varepsilon$, $\psi + \varepsilon$, $\psi - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi - \psi$, $\varphi + \psi$, $\psi\varphi - \varepsilon$ are permutations.* □

The conditions of Theorem 5 we can write otherwise:

Theorem 5a. *A T-quasigroup (a medial quasigroup) (Q,A): $A(x,y) = \varphi x + \psi y + c$ is a $totCO$-quasigroup if and only if all maps $\varphi^2 - \varepsilon$, $\psi^2 - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi - \psi$, $\varphi + \psi$, $\psi\varphi - \varepsilon$ (all maps $\varphi^2 - \varepsilon$, $\psi^2 - \varepsilon$, $\varphi^2 + \psi$, $\psi^2 + \varphi$, $\varphi^2 - \psi^2$, $\psi\varphi - \varepsilon$ respectively) are permutations.*

Proof. Indeed, $(\varphi + \varepsilon)(\varphi - \varepsilon) = \varphi^2 - \varepsilon$, $(\psi + \varepsilon)(\psi - \varepsilon) = \psi^2 - \varepsilon$, and in the case of a medial quasigroup $(\varphi - \psi)(\varphi + \psi) = \varphi^2 - \psi^2$. □

Note that an operation A of the form $A(x,y) = (ax + by + c) \pmod n$, $n \geqslant 2$, is a quasigroup if and only if the numbers a, b modulo n are relatively prime to n. In this case $\varphi = L_a$, $\psi = L_b$, where $L_a x = ax \pmod n$, $x \in Q = \{0, 1, 2, ..., n-1\}$, are permutations (automorphisms of the additive group modulo n) and the quasigroup $Q(A)$ is a T-quasigroup (moreover, a medial quasigroup).

In [6] the following statement (Corollary 2 of [6]) is proved:

Corollary 1. [6] *A medial quasigroup (Q,A): $A(x,y) = (ax+by) \pmod n$ is a $totCO$-quasigroup if and only if all elements $a+1, a-1, b+1, b-1, a^2+b, b^2+a, a-b, a+b, ab-1$ modulo n are relatively prime to n.* □

This corollary can be rewrite otherwise:

Corollary 1a. *A medial quasigroup (Q,A): $A(x,y) = (ax + by) \pmod n$ is a $totCO$-quasigroup if and only if all elements $a^2 - 1, b^2 - 1, a^2 + b, b^2 + a, a^2 - b^2, ab - 1$ modulo n are relatively prime to n.* □

The following theorem (Theorem 3 of [6]) gives an information with respect to the spectrum of $totCO$-quasigroups.

Theorem 6. [6] *For any integer $n \geqslant 11$ which is relatively prime to $2, 3, 5$ and 7 there exists a $totCO$-quasigroup of order n.* □

4. Totally conjugate orthogonal T-quasigroups

Now we shall prove that a CCS over a *totCO-T*-quasigroup with check formulas (3) or (4) is able to detect some errors.

Theorem 7. *A check character system using a finite totCO-T-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formulae (3) with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions;*
3. *jump transpositions if and only if the mappings* $\psi - \varphi^2$ *and* $\varepsilon + \varphi\psi$ *are permutations;*
4. *twin errors;*
5. *jump twin errors if and only if the mapping* $\varepsilon + \varphi^2$, $\varphi\psi - \varepsilon$ *are permutations.*

Proof. From Theorem 5 it follows that all conditions for transpositions of Theorem 2 are fulled if we take into account that the automorphism $\varphi\psi^{-1}$ is regular if and only if the mapping $\varepsilon - \varphi\psi^{-1}$ (the same $\psi - \varphi$ or $\varphi - \psi$) is a permutation and the automorphism φ ($I\psi$) is regular if and if $\varepsilon - \varphi$ (respectively $\varepsilon + \psi$) is a permutation.

By Theorem 2 a CCS detects jump transpositions if and only if the automorphisms $\varphi^2\psi^{-1}$, φ^2, $I\varphi\psi$ are regular that is when the mappings $\varepsilon - \varphi^2\psi^{-1}$ (the same $\psi - \varphi^2$), $\varepsilon - \varphi^2$ and $\varepsilon + \varphi\psi$ are permutations. But by Theorem 5a in a *totCO-T*-quasigroup the mapping $\varepsilon - \varphi^2$ is a permutation.

According to Theorem 2 a CCS detects twin errors if and only if the automorphisms $I\varphi\psi^{-1}$, $I\varphi$, ψ are regular, that is the mappings $\varepsilon + \varphi\psi^{-1}$ (the same $\psi + \varphi$), $\varepsilon + \varphi$ and $\varepsilon - \psi$ are permutations. This is by Theorem 5.

At last, by Theorem 2 a CCS detects jump twin errors if and only if the automorphisms $I\varphi^2\psi^{-1}$, $I\varphi^2$, $\varphi\psi$ are regular. It means that the maps $\varepsilon + \varphi^2\psi^{-1}$ (the same $\psi + \varphi^2$), $\varepsilon + \varphi^2$ and $\varepsilon - \varphi\psi$ are permutations. By Theorem 5 the mapping $\psi + \varphi^2$ is a permutation. □

Corollary 2. *If in Theorem* 7 *a totCO-quasigroup* $Q(\cdot)$ *is medial, then in item* 5 *the condition* $\varphi\psi - \varepsilon$ *can be eliminated.*

Proof. Indeed, in any medial quasigroup $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ the automorphisms φ and ψ commute, so the mapping $\varphi\psi - \varepsilon = \psi\varphi - \varepsilon$ is a permutation in a *totCO-T*-quasigroup. □

Theorem 8. *A check character system using a finite totCO-T-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formula* (4) *with* $\delta = \varepsilon$, $n > 4$, *detects*

1. *single errors;*
2. *transpositions;*
3. *jump transpositions if and only if the mapping* $\psi - \varphi^2$ *is a permutation;*
4. *twin errors;*
5. *jump twin errors if and only if the mapping* $\varepsilon + \varphi^2$ *is a permutation.*

Proof. Follows from the proof of Theorem 7, if we take into account that for jump transpositions and jump twin errors in Theorem 3 there are less conditions than in Theorem 2. □

As a consequence of Theorems 7, 8 and Corollary 2 we obtain

Theorem 9. *A check character system using a finite medial totCO-quasigroup* $Q(\cdot) : x \cdot y = \varphi x + \psi y + c$ *and check formula* (3) (resp.(4)) *with* $\delta = \varepsilon$, $n > 4$, *detects single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the mappings* $\psi - \varphi^2$, $\varepsilon + \varphi\psi$ *and* $\varepsilon + \varphi^2$ ($\psi - \varphi^2$ *and* $\varepsilon + \varphi^2$ *respectively) are permutations.*

Corollary 3. *A check character system using a medial totCO-quasigroup* $Q(\cdot) : x \cdot y = (ax + by + c) \pmod n$ *and check formula* (3) (resp.(4)) *with* $\delta = \varepsilon$, $n > 4$, *detects single errors, transpositions, jump transpositions, twin errors and jump twin errors if and only if the mappings* $a^2 - b$, $1 + ab$ *and* $1 + a^2$ ($a^2 - b$ *and* $1 + a^2$ *respectively) modulo* n *are relatively prime to* n.

Proof. Indeed, in this case the maps

$$\begin{aligned} \varphi^2 - \psi &: (\varphi^2 - \psi)x = (L_a^2 - L_b)x = (a^2 - b)x \pmod n, \\ \varepsilon + \varphi\psi &: (\varepsilon + \varphi\psi)x = (\varepsilon + L_a L_b)x = (1 + ab)x \pmod n, \\ \varepsilon + \varphi^2 &: (\varepsilon + \varphi^2)x = (\varepsilon + L_a^2)x = (1 + a^2)x \pmod n \end{aligned}$$

are permutations if and only if the corresponding elements modulo n are relatively prime to n. Note that in this case the elements a, b are also relatively prime to n, since $(Q, \cdot)$ is a quasigroup. □

Theorem 10. *For any integer* $n \geqslant 11$ *which is relatively prime to* 2, 3, 5 *and* 7 *there exists a medial totCO-quasigroup of order* n *such that the check character system over this quasigroup with the check formulas* (3) *or* (4), $\delta = \varepsilon$, $n > 4$, *detects all single errors, transpositions, jump transpositions, twin errors and jump twin errors.*

Proof. Let $\overline{a}$ be the element a modulo n and (m, n) be the greatest common divisor of m and n. Consider the medial quasigroup $(Q, \cdot)$: $x \cdot y = 3x + 5y$

(mod n) where $(3, n) = 1$ and $(5, n) = 1$, $Q = \{0, 1, 2, ..., n-1\}$. In this case $a = 3, b = 5$. According to Proposition 1 of [6] this quasigroup is a $totCO$-quasigroup for any n relatively prime to 2,3,5 and 7.

Check the conditions of Corollary 3 for this quasigroup: $(a^2 - b)x = (9-5)x = 4x$, $(1+ab)x = 16x$, $(1+a^2)x = (1+9)x = 10x$ modulo n, $x \in Q$. Since $n \geqslant 11$ then the maps $4x, 10x$ modulo n are permutations if n is relatively prime to 2 and 5. Let n be relatively prime to 2,3,5 and 7, then $n \neq 16$ and $n < 16$ only for $n = 11, 13$. These orders are prime numbers, so $(\overline{16}, n) = 1$ for every of these numbers. If $n > 16$, then $\overline{16} = 16$ and $(16, n) = 1$ since n is relatively prime to 2. Thus, the quasigroup $A(x, y) = 3x+5y \pmod n$ is the needed $totCO$-quasigroup for any n which is relatively prime to 2,3,5 and 7. □

References

[1] **V.D. Belousov**, *Parastrophic-orthogonal quasigroups*, Quasigroups and Related Systems **13** (2005), 25 – 72.

[2] **G. Belyavskaya, A. Diordiev**, *On quasi-identities in finite quasigroups*, Bul. Acad. Sci. Republ. Moldova, Matematica **3(49)**, (2005), 19 – 32.

[3] **G.B. Belyavskaya, V.I. Izbash, and G.L. Mullen**, *Check character systems using quasigroups, I*, Designs, Codes and Cryptography **37** (2005), 215 – 227.

[4] **G.B. Belyavskaya, V.I. Izbash, and G.L. Mullen**, *Check character systems using quasigroups, II*, Designs, Codes and Cryptography **37** (2005), 405 – 419.

[5] **G.B. Belyavskaya, V.I. Izbash, and V.A. Shcherbacov**, *Check character systems over quasigroups and loops*, Quasigroups Related Systems **10** (2003), 1 – 28.

[6] **G.B. Belyavskaya, T.V. Popovich**, *Totally conjugate orthogonal quasigroups and complete graphs*, (to appear).

[7] **J. Dénes and A. D. Keedwell**, *Latin Squares and Their Applications*, Academic Press New York; Akademiai Kiado, Budapest, 1974.

[8] **A. Ecker and G. Poch**, *Check character systems,* Computing **37** (1986), 277–301.

[9] **D. M. Johnson, A. L. Dulmage, and N. S. Mendelsohn**, *Orthomorphisms of groups and orthogonal Latin squares I*, Canad. J. Math. **13** (1961), 356 – 372.

[10] **T. Kepka and P. Nemec**, *T-quasigroups*, Acta Univ. Carolinae Math. Phys. **12** (1971), Part I, No.1, 39 – 49, Part II, No.2, 31 – 39.

[11] **C. C. Lindner and D. Steedly**, *On the number of conjugates of a quasigroup*, Algebra Univ. **5** (1975), 191 – 196.

[12] **R.-H. Schulz**, *A note on check character systems using Latin squares*, Discrete Math. **97** (1991), 371 – 375.

[13] **J. Verhoeff**, *Error Detecting Decimal Codes,* Vol. 29, Math. Centre Tracts. Math. Centrum Amsterdam, 1969.

Received April 9, 2010

Institute of Mathematics and Computer Science, Academy of Sciences, Academiei str. 5, MD-2028, Chisinau, Moldova, E-mail: gbel1@rambler.ru

Quasigroups and Related Systems **18** (2010), 17 – 24

Configurations of conjugate permutations

Ivan I. Deriyenko

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. We describe some configurations of conjugate permutations which may be used as a mathematical model of some genetical processes and crystal growth.

1. Introduction

Let $Q = \{1, 2, 3, \ldots, n\}$ be a finite set. The set of all permutations of Q will be denoted by $\mathbb{S}_n$. The multiplication (composition) of permutations φ and ψ of Q is defined as $\varphi\psi(x) = \varphi(\psi(x))$. Permutations will be written in the form of cycles and cycles will be separated by points, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (123.45.6.)$$

By a *type* of a permutation $\varphi \in \mathbb{S}_n$ we mean the sequence

$$C(\varphi) = \{l_1, l_2, \ldots, l_n\},$$

where l_i denotes the number of cycles of the length i. Obviously,

$$\sum_{i=1}^{n} i \cdot l_i = n\,.$$

For example, for $\varphi = (132.45.6.)$ we have $C(\varphi) = \{1, 1, 1, 0, 0, 0\}$; for $\psi = (123456.)$ we obtain $C(\psi) = \{0, 0, 0, 0, 0, 1\}$.

As is well-known, two permutations $\varphi, \psi \in \mathbb{S}_n$ are *conjugate* if there exists a permutation $\rho \in \mathbb{S}_n$ such that

$$\rho\varphi\rho^{-1} = \psi. \tag{1}$$

2000 Mathematics Subject Classification: 05B15; 20N05
Keywords: permutation, conjugate permutation, stem-permutation, symmetric group, flock, telomere, configuration.

Theorem 1. (Theorem 5.1.3 in [1]) *Two permutations are conjugated if and only if they have the same type.* □

In this short note we find all solutions of (1), i.e., for a given φ and ψ we find all permutations ρ satisfying this equation, and describe some graphs connected with these solutions.

2. Solutions of the equation (1)

Let's consider the equation (1). If $\varphi = \psi = \varepsilon$, then as ρ we can take any permutation from $\mathbb{S}_n$. So, in this case (1) has $n!$ solutions.

If permutations φ and ψ are cyclic, then without loss of generality, we can assume that

$$\varphi = (1\,\varphi(1)\,\varphi^2(1)\,\varphi^3(1)\,\ldots\,\varphi^{n-1}(1).),$$
$$\psi = (1\,\psi(1)\,\psi^2(1)\,\psi^3(1)\,\ldots\,\psi^{n-1}(1).),$$

where $\varphi^0(1) = \varphi^n(1) = 1$ and $\psi^0(1) = \psi^n(1) = 1$. In this case for ρ_0 defined by

$$\rho_0(\varphi^i(1)) = \psi^i(1) = x_i, \quad i = 0, 1, \ldots, n-1, \tag{2}$$

we have

$$\rho_0\varphi\rho_0^{-1}(x_i) = \rho_0\varphi\rho_0^{-1}(\psi^i(1)) = \rho_0\varphi^{i+1}(1) = \psi^{i+1}(1) = \psi(\psi^i(1)) = \psi(x_i),$$

which shows that ρ_0 satisfies (1). Moreover, as is not difficult to see, each permutation of the form

$$\rho = \rho_0\varphi^i, \quad i = 0, 1, \ldots, n-1 \tag{3}$$

also satisfies this equation. There are no other solutions. So, in this case we have n different solutions.

In the general case when φ and ψ are decomposed into cycles of the length $k_1, k_2, \ldots, k_r$, i.e.,

$$\varphi = (a_{11}\,a_{12}\ldots a_{1k_1})\ldots(a_{r1}\ldots a_{rk_r}),$$
$$\psi = (b_{11}\,b_{12}\ldots b_{1k_1})\ldots(b_{r1}\ldots b_{rk_r}),$$

the solution ρ, according to [1], has the form

$$\beta = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1k_1} & \ldots & a_{r1} & \ldots & a_{rk_r} \\ b_{11} & b_{12} & \ldots & b_{1k_1} & \ldots & b_{r1} & \ldots & b_{rk_r} \end{pmatrix}, \tag{4}$$

where the first row contains all elements of φ, the second – elements of ψ written in the same order as in decompositions of φ and ψ into cycles. Replacing in φ the cycle $(a_{11}\, a_{12} \ldots a_{1k_1})$ by $(a_{12}\, a_{13} \ldots a_{1k_1}\, a_{11})$ we save the permutation φ but we obtain a new ρ. Similar to arbitrary cycles of φ and ψ. In this way we obtain all ρ satisfying (1).

Let's observe that the cycle $(a_{11}\, a_{12} \ldots a_{1k_1})$ gives k_1 possibilities for the construction ρ. From m cycles of the length k we can construct $m!\, k^m$ various ρ. So, in the case $C(\varphi) = C(\psi) = \{l_1, l_2, \ldots, l_n\}$ we can construct

$$N_\varphi = l_1! \cdot l_2! \cdot 2^{l_2} \cdot l_3! \cdot 3^{l_3} \cdot \ldots \cdot l_n! \cdot n^{l_n}$$

various ρ.

3. Configurations of conjugate permutations

As is well-known, any permutation φ of the set Q of order n can be decomposed into $r \leqslant n$ cycles of the length $k_1, k_2, \ldots, k_r$ with $k_1 + k_2 + \ldots + k_r = n$. We denote this fact by

$$Z = Z(\varphi) = [k_1, k_2, \ldots, k_r]$$

and assume that $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_r$. $Z(\varphi)$ is called the *cyclic type* of φ. The set of all permutations of the set Q with the same cyclic type Z_i is denoted by F_i and is called a *flock*. Permutations belonging to the same flock are conjugate (Theorem 1). The number of flocks $F_i \subset \mathbb{S}_n$ is equal to the number of possible decompositions of n into a sum of natural numbers.

In each flock we select one permutation σ and call it a *stem-permutation*. For simplicity we can assume that elements of this permutation are written in the natural order.

Example 1. Let's consider the set $Q = \{1, 2, 3, 4, 5\}$. The number 5 has seven decompositions into a sum of natural numbers, so the set of all permutations of Q has seven flocks. Below we present these flocks and their stem-permutations.

$Z_1 : 5 = 5$	$\sigma = (12345.)$
$Z_2 : 5 = 1 + 4$	$\sigma = (1.2345.)$
$Z_3 : 5 = 2 + 3$	$\sigma = (12.345.)$
$Z_4 : 5 = 1 + 2 + 2$	$\sigma = (1.23.45.)$
$Z_5 : 5 = 1 + 1 + 3$	$\sigma = (1.2.345.)$
$Z_6 : 5 = 1 + 1 + 1 + 2$	$\sigma = (1.2.3.45.)$
$Z_7 : 5 = 1 + 1 + 1 + 1 = 1$	$\sigma = (1.2.3.4.5.) = \varepsilon$.

□

Let's consider an arbitrary flock $F_i \subset \mathbb{S}_n$ and its stem-permutation σ. For an arbitrary permutation $\varphi_0 \in F_i$ we define the sequence of permutations $\varphi_0, \varphi_1, \varphi_2, \dots$ by putting

$$\varphi_{k+1} = \varphi_k \sigma \varphi_k^{-1}. \tag{5}$$

Obviously all φ_k are in F_i. The set F_i is finite, so $\varphi_p = \varphi_s$ for some p and s.

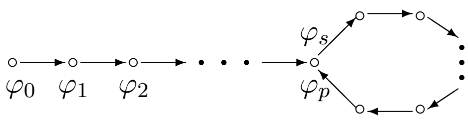


Fig. 1. The graph connected with the sequence (5).

The sequence $\varphi_1, \varphi_2, \varphi_3, \dots$ can be initiated by various φ_0 because for fixed φ_1 and σ the equation $\varphi_1 = \varphi\sigma\varphi^{-1}$ has many solutions.

Let's denote by Φ_k the set of all possible solutions of the equation (5), where φ_{k+1} and σ are fixed. Let

$$\overline{\Phi}_k = \{\varphi \in \Phi_k \,:\, Z(\varphi) = Z(\sigma)\}.$$

In the case when $\overline{\Phi}_k$ has only one element the permutation φ_{k+1} is called *simple*. If $\overline{\Phi}_k$ is the empty set, then φ_{k+1} is called a *telomere* and is denoted by $\hat{\varphi}_{k+1}$. In the corresponding oriented graph a telomere is a vertex which is not preceded by another vertex.

The following theorem is obvious.

Theorem 2. *Let σ be a stem-permutation of a flock F_i. If $\varphi \in F_i$ is a telomere, then also $\psi = \sigma\varphi\sigma^{-1}$ is a telomere.* □

Two permutations $\varphi, \psi \in F_i \subset \mathbb{S}_n$ have the same *configuration* K if $\varphi_p = \psi_q$ for some natural p and q, where

$$\varphi_p = \varphi_{p-1}\sigma\varphi_{p-1}^{-1}\,,\ \dots\,,\ \varphi_1 = \varphi\sigma\varphi^{-1},$$

$$\psi_q = \psi_{q-1}\sigma\psi_{q-1}^{-1}\,,\ \dots\,,\ \psi_1 = \psi\sigma\psi^{-1}$$

and σ is a stem-permutation from F_i.

4. A simple algorithm for determining configurations

1. In a given flock F_i we select a stem-permutation σ and one permutation $\varphi_0 \neq \sigma$. Using these two permutations and (5) we construct the sequence

$\varphi_0, \varphi_1, \ldots, \varphi_l$, where $\varphi_l \neq \varphi_s$ for all $0 \leqslant s < l$ and $\varphi_{l+1} = \varphi_t$ for some $0 \leqslant t < l$. In this way we obtain the graph

$$\varphi_0 \to \varphi_1 \to \varphi_2 \to \cdots \to \varphi_j \to \cdots \to \varphi_l$$

2. For each φ_j from the above sequence, from all solutions of the equation

$$\rho\sigma\rho^{-1} = \varphi_j$$

we select these solutions $\rho \neq \varphi_{j-1}$ which are in F_i and attach them to the previous solutions as immediately preceding φ_j. In this way we obtain the configuration $K = \{\varphi_0, \varphi_1, \ldots, \varphi_l, \rho_1, \rho_2, \ldots\}$ and the graph

$$\begin{tikzcd}
 & & & & \rho_1 \arrow[dr] & \rho_2 \arrow[d] & & \\
\varphi_0 \arrow[r] & \varphi_1 \arrow[r] & \varphi_2 \arrow[r] & \cdots \arrow[rr] & & \varphi_j \arrow[r] & \cdots \arrow[r] & \varphi_l
\end{tikzcd}$$

Next, for all new ρ_k attached to K we solve the equation $\rho\sigma\rho^{-1} = \rho_k$ and attach to K these solutions $\rho' \neq \rho_k$ which are in F_i. For this new ρ' we solve the equation $\rho\sigma\rho^{-1} = \rho'$ and so on. Since F_i is finite after some steps we obtain a telomere which completes this procedure.

5. Examples

Now we give some examples. We will consider the set $Q = \{1, 2, 3, 4, 5, 6\}$ and its permutations. For simplicity we consider the flock F_1 containing all cyclic permutations of Q and select $\sigma = (123456.)$ as a stem-permutation of F_1.

Example 2. If we choose $\varphi_0 = (125634.)$, then, according to (5), we obtain

$$\begin{aligned}
\varphi_1 &= \varphi_0\sigma\varphi_0^{-1} = (163254.),\\
\varphi_2 &= \varphi_1\sigma\varphi_1^{-1} = (143625.),\\
\varphi_3 &= \varphi_2\sigma\varphi_2^{-1} = (163254.) = \varphi_1\,.
\end{aligned}$$

Thus, the first step of our algorithm gives the configuration $K = \{\varphi_0, \varphi_1, \varphi_2\}$.

Now, for each $\varphi_i \in K$ we solve the equation $\rho\sigma\rho^{-1} = \varphi_i$ and add to K all solutions belonging to F_1.

The equation $\rho\sigma\rho^{-1} = \varphi_0$ is satisfied by the permutation $\rho_0 = (1.2.34.56.)$. So, according to (3), other solutions of this equation have the form

$$\begin{aligned}
\varphi_{01} &= \rho_0\sigma \ = (1.2.34.56.)(123456.) \ = (125436.),\\
\varphi_{02} &= \rho_0\sigma^2 = (1.2.34.56.)(135.246.) = (15.26.3.4.),\\
\varphi_{03} &= \rho_0\sigma^3 = (1.2.34.56.)(14.25.36.) = (165234.),\\
\varphi_{04} &= \rho_0\sigma^4 = (1.2.34.56.)(153.264.) = (13.24.5.6.),\\
\varphi_{05} &= \rho_0\sigma^5 = (1.2.34.56.)(165432.) \ = (145632.).
\end{aligned}$$

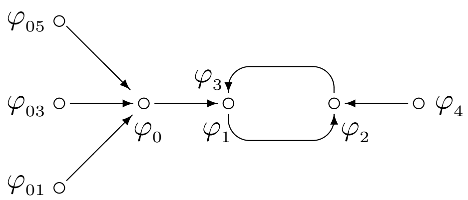
From these solutions only $\varphi_{01}, \varphi_{03}, \varphi_{05}$ are in F_1. We attach these solutions to K as the immediately preceding φ_0.

Next, we consider the equation $\rho\sigma\rho^{-1} = \varphi_1$. This equation has only one solution belonging to F_1. Since this solution coincides with ρ, we do not obtain permutations which should be added to K.

The equation $\rho\sigma\rho^{-1} = \varphi_2$ has only one solution $\rho = (145236.) \neq \varphi_1$ belonging to F_1. We denote it by φ_4 and add to K as the solution immediately preceding φ_2. At this instant we have the configuration (uncomplete)

$$K = \{\varphi_0, \varphi_1, \varphi_2, \varphi_{01}, \varphi_{03}, \varphi_{05}, \varphi_4\}$$

and the graph



Further we will work with the permutations φ_{01}, φ_{03}, φ_{05}, φ_4. Equations $\rho\sigma\rho^{-1} = \varphi_{0i}$, $i = 1, 3, 5$, do not have solutions belonging to F_i. So, φ_{01}, φ_{03}, φ_{05} are telomeres. We denote them by $\hat{\varphi}_{01}$, $\hat{\varphi}_{03}$, $\hat{\varphi}_{05}$.

The equation $\rho\sigma\rho^{-1} = \varphi_4$ has three solutions belonging to F_1. Namely,

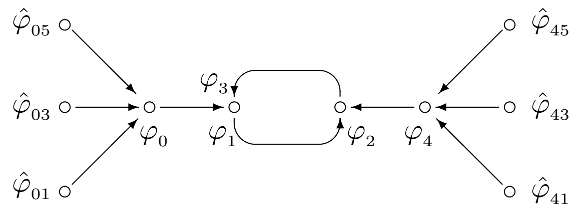
$$\begin{aligned}
\varphi_{41} &= \rho'\sigma \ = (1.6.24.35.)(123456.) \ = (143256.),\\
\varphi_{43} &= \rho'\sigma^3 = (1.6.24.35.)(14.25.36.) = (123654.),\\
\varphi_{45} &= \rho'\sigma^5 = (1.6.24.35.)(165432.) \ = (163452.).
\end{aligned}$$

Since equations $\rho\sigma\rho^{-1} = \varphi_{4j}$, $j = 1, 3, 5$, do not have solutions belonging to F_1, φ_{41}, φ_{43}, φ_{45} are telomeres.

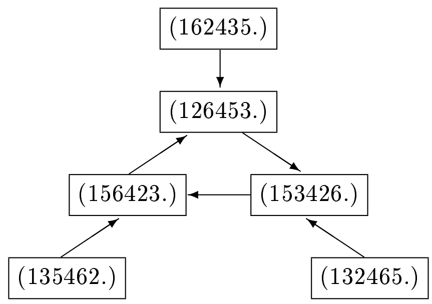
Summarizing the above we obtain the configuration

$$K = \{\varphi_0, \varphi_1, \varphi_2, \hat{\varphi}_{01}, \hat{\varphi}_{03}, \hat{\varphi}_{05}, \varphi_4, \hat{\varphi}_{41}, \hat{\varphi}_{43}, \hat{\varphi}_{45}\}$$

and the graph



Example 3. Using the same flock F_1 and the same σ but selecting another φ_0 we can obtain another configuration. For example by selecting $\varphi_0 = (162435.)$ we obtain the configuration K_2 presented by the following graph:



Remark. The flock F_1 has six configurations:

- K_1 and K_2 are described in the above examples,
- K_3 induced by $\varphi_0 = (125643.)$ contains 18 permutations,
- K_4 induced by $\varphi_0 = (135624.)$ contains 42 permutations,
- K_5 induced by $\varphi_0 = (136245.)$ contains 42 permutations,
- K_6 has only two permutations: σ and σ^{-1}.

Flocks K_4 and K_5 are isomorphic as graphs.

The set $\mathbb{S}_6$ is divided into 11 flocks.

The author does'nt know a general method that would allow to determine the number of configurations in each flock. Neither does he know how to quickly find a telomere using stem-permutations. It is also unknown how to check if two telomeres belong to the same configuration.

6. Conclusions

The results shown were inspired by some research in genetics. Some terminology (stem-permutation, telomere) was also drawn from genetics. The author thinks that the described method of configuration can be effectively used in chemistry in researching growth of crystals.

References

[1] **M. Hall**, *The theory of groups*, Macmillan, 1959.

Received May 8, 2010

Department of Higher Mathematics and Informatics, Kremenchuk State Polytechnic University, 20 Pervomayskaya str, 39600 Kremenchuk, Ukraine
E-mail: ivan.deriyenko@gmail.com

Quasigroups and Related Systems **18** (2010), 25 − 42

Free topological acts over a topological monoid

Behnam Khosravi

Abstract. First we present the free topological S-acts on sets, on topological spaces, and as well as on S-acts. Then, we give more concrete description of these free objects in some cases.

1. Introduction

The action of topological semigroups and their representations have a very wide usage in different branches of Mathematics like geometry, analysis, Lie groups or dynamical systems, and they are studied by many authors, see for example [4, 7, 20, 23, 24]. Furthermore, some notions are in fact topological S-acts with some extra properties, e.g., in analysis, S-flow is a compact topological S-act (see [5, 19]), or the representation of a discrete group G is in fact a topological G-act (see [2, 13, 17]). Also in geometry, flow is a smooth topological S-act, where S is $(\mathbb{R}, +)$ with its usual topology (see [7]). These kinds of topological S-acts are studied more and there are some works about their universal structures (for example see [15]). We note that, a space which a topological semigroup acts on it, sometimes has different names in different branches of Mathematics, e.g. in some text, it is called G-space where G is a topological group (e.g. see [12]), while in some others, it is called topological S-act (see for example [22]). In this note we use the latter terminology since we use theorems and terminology of [18]. Because of the importance of the universal structures and specially free structures, in this paper we study the notion of freeness which is a fruitful subject in the study of different categories (see for example [3, 8, 9, 16]). We present the free topological S-acts on sets, on topological spaces, and as well as on S-acts.

Let $(S, \cdot, \tau_S)$ be a topological monoid. In this note, we want to study different free topological S-acts. Note that since there are three forgetful functors from the category of topological S-acts to the category of topological spaces,

2000 Mathematics Subject Classification: 20M30, 54H10, 22A30, 08B20
Keywords: S-act, free topological S-act, topological semigroup

the category of S-acts and the category of sets, we can define free topological S-acts on a topological space, on an S-act and on a set. In Section 2, we briefly study topological S-acts, semitopological S-acts and compare them. In Section 3, first, we introduce the free topological S-acts on a topological space, then we describe the topology of free topological S-acts more concretely and study some of its properties, like its behavior with separation axioms. Also we give a coarser and finer topology than the topology of the free topological S-act on a topological space (X, τ_X) according to the topology of topological space (X, τ_X) and the topology of the topological monoid $(S, \cdot, \tau_S)$. Finally in Section 3, we introduce the free topological S-acts on a set. In Section 4, we study the free topological S-act on an S-act and present it. Then by using the notion of free topological S-acts on S-acts, we present some method for studying universal objects in the category of topological S-acts, using the known universal structures in the category of S-acts. To illustrate this method, we apply it to characterize projective topological S-acts by using the characterization of projective S-acts.

Now we briefly recall some definitions about S-acts needed in the sequel. For more information see [11, 18].

Recall that, for a semigroup S, a set A is a left *S-act* (or *S-set*) if there is, so called, an *action* $\mu : S \times A \to A$ such that, denoting $\mu(s, a) := sa$, $(st)a = s(ta)$ and, if S is a monoid with 1, $1a = a$. Right S-acts are defined similarly. An S-act A is called *cyclic*, if there exists an $a \in A$ such that $A = Sa$.

Each semigroup S can be considered as an S-act with the action given by its multiplication.

The definitions of a *subact* A of B, written as $A \leq B$, and a *homomorphism* between S-acts are clear. In fact S-homomorphisms, or S-maps, are action-preserving maps: $f : A \to B$ with $f(sa) = sf(a)$, for $s \in S$, $a \in A$. We denote the category of S-acts with S-maps, by **S-Act**.

A topological space (X, τ_X) has *Alexandroff topology*, if the intersection of an arbitrary family of open sets in (X, τ_X) is open. An space with an Alexandroff topology is called an *Alexandroff space*.

The algebraic structure of the free topological S-act on a topological space can be characterized concretely, however, like free topological groups, the topology of free topological S-acts can not be described as concretely as its algebraic structure.

2. Topological S-acts

In this section, we briefly state the notions we need about topological S-acts. First recall the following

Definition 2.1. Let S be a semigroup and a topological space with topology τ_S. S with this topology is called a *topological semigroup* if multiplication $(s,t) \mapsto st : S \times S \to S$ is (jointly) continuous ([5, 10, 14]). We use Kelley's notation in [14], and denote a topological semigroup by $(S, \cdot, \tau_S)$

Despite the above convention, for simplicity, we denote a topological $(S, \cdot, \tau_S)$-act by topological S-act.

Definition 2.2. For a topological semigroup $(S, \cdot, \tau_S)$, a (left) topological *S-act* or a topological *S-act* is a left S-act A with a topology τ_A such that the action $S \times A \to A$ is (jointly) continuous. Similar to topological semigroup, we denote a topological S-act by (A, τ_A). We denote the category of all topological S-acts with continuous S-maps by **S-Top**.

Definition 2.3. We say that a topological semigroup $(S, \cdot, \tau_S)$ has a *left ideal topology*, if each of its open sets, including the empty one, is a left ideal (sub S-act) of S. Also, a topological S-act (A, τ_A) is said to have a *subact topology* if all of its open sets, including the empty one, are subacts of A.

We use the above definition of a left ideal topology which is more general than the definition in [22].

Definition 2.4. By weak topology on a set Z, with respect to a family of functions on Z, we mean the coarsest topology on Z which makes those functions continuous. In other words, given a set Z and an indexed family $(Y_i)_{i \in I}$ of topological spaces with functions $f_i : Z \to Y_i$, the weak topology on Z is generated by the sets of the form $f_i^{-1}(U)$, where U is an open set in Y_i.

NOTATION. For any two arbitrary topological spaces (X_1, τ_{X_1}) and (X_2, τ_{X_2}), by $\tau_{X_1 \times X_2}$ we mean the product topology on $X_1 \times X_2$. For any set Z, we denote Z with discrete topology by (Z, τ_{dis}). For any S-act A, by $|A|$ we mean the underlying set of A.

Remark 2.5. Recall that for a semigroup S and an S-act A, the functions λ_s and ρ_a are defined for any $s \in S$ and $a \in A$ as follows

$$\lambda_s : A \to A, \quad y \mapsto sy \qquad \text{and} \qquad \rho_a : S \to A, \quad t \mapsto ta.$$

In the special case $A = S$, we use the notation $\lambda_s^{(S)} : S \to S$, to prevent misunderstanding.

Now if S has a topology τ_S for which its multiplication $S \times S \to S$ is (separately) continuous, that is, $\lambda_s^{(S)}$ and ρ_s are continuous for all $s \in S$, then S with topology τ_S is called a *semitopological semigroup*.

Similarly, one can define a *semitopological S-act* by taking $\lambda_s : A \to A$ and $\rho_a : S \to A$ to be continuous for each $s \in S$ and $a \in A$.

Clearly any topological S-act is a semitopological S-act, because every jointly continuous function is separately continuous. But, as the following example shows, for a topological semigroup $(S, \cdot, \tau_S)$, a semitopological S-act need not be a topological S-act. Note that clearly if S with a topology τ_S is a semitopological semigroup which is not a topological semigroup, then S with τ_S is a semitopological S-act which is not a topological S-act. However the following example shows that for a topological semigroup S, the joint continuity of the action of S-acts is independent from the joint continuity of the multiplication of S.

Example 2.6. Suppose that $S = [0,1]$ and τ_S is the usual topology on $[0,1]$ which is inherited from $\mathbb{R}$ by subspace topology. Define for each s and t in S, $s \cdot t = 0$. It is obvious that $(S, \cdot, \tau_S)$ is a topological semigroup. Again, consider $[0,1]$ with topology which is inherited from $\mathbb{R}$. For any $s, t \in S$, define the action of S on $[0,1]$ by

$$\mu(s,t) = \sum_{n=1}^{\infty} (\frac{1}{2})^n f_n(s,t),$$

where

$$\mathrm{f_n(s,t)} = \begin{cases} 0 & \text{if } s \leqslant s_n \text{ or } t \leqslant t_n \\ \frac{|(\mathbf{s}-\mathbf{s_n})(\mathbf{t}-\mathbf{t_n})|}{(\mathbf{s}-\mathbf{s_n})^2+(\mathbf{t}-\mathbf{t_n})^2} & \text{otherwise} \end{cases}$$

and $\{(s_n, t_n) | n = 1, 2, \ldots\}$ is any (non-void) subset of the product $[\frac{1}{2}, 1] \times [\frac{1}{2}, 1]$. If we take $T = [0, \frac{1}{2}]$, then by an straightforward checking, we can see that μ has the following properties:

1. $\mu((T \times [0,1]) \cup (S \times T)) = \{0\}$,
2. $\mu(S, [0,1]) \subseteq T = [0, \frac{1}{2}]$.

(For more details about the properties of the function μ, see [23, Example 5.14.]) So we have for all s, s' and t in S

$$\mu(st, s') = \mu(0, s') \in \mu(T \times [0,1]) = \{0\},$$

$$\mu(s, \mu(t, s')) \in \mu(S \times T) = \{0\}.$$

Therefore, $[0,1]$ is an S-act with the action μ. Again, by direct checking, one can see that μ, the action of $(S, \cdot, \tau_S)$ on $[0,1]$, is not continuous but all the functions $\lambda_s(-) = \mu(s,-)$ and $\rho_a(-) = \mu(-,a)$, for each s and a in S, are continuous. Hence $[0,1]$ is not a topological S-act but it is a semitopological S-act.

Now we recall the definition of different free topological S-acts in the following definition. Since these definitions are very similar, we state them together.

Definition 2.7. A topological S-act (F, τ_F) with one-one S-map $\nu : B \to F$, (the embedding $\nu : (X, \tau_X) \to (F, \tau_F)$), (one-one function $\nu : Z \to F$) is the *free topological S-act over the S-act B* (*over the topological space X*) (*over the set Z*), if for every topological S-act (A, τ_A) and an S-map $f : B \to A$, (a continuous function $f : (X, \tau_X) \to (A, \tau_A)$), (a function $f : Z \to A$), there exists a unique continuous S-map $\widetilde{f} : (F, \tau_F) \to (A, \tau_A)$ such that $\widetilde{f} \circ \nu = f$ (for the general definition of the free objects in an arbitrary category, see [1, 6]).

The free topological space over a set Z is the set Z together with the discrete topology. The free S-act, for a monoid S, on a set Z is defined as follow. Consider the set $S \times Z$ with the action defined by $t(s,z) = (ts, z)$ for any $t, s \in S$ and $z \in Z$, and define $\nu : Z \to S \times Z$ as follows $\nu(z) = (1, z)$. It is a known fact that $S \times Z$ with this action is an S-act. From now on, for any set Z, by $F(Z)$ we mean this S-act which is defined on $S \times Z$. Furthermore, it is a known fact that $F(Z)$ is the free S-act over the set Z (it means that for any S-act A and a function $f : Z \to A$, there exists a unique S-map $\widetilde{f} : F(Z) \to A$ such that $\widetilde{f} \circ \nu = f$ (for more details see, [11, 18])).

3. Free topological S-act on a topological space

In this section, we present the free topological S-act over a topological space and then describe it more concretely in some special instances, e.g, when τ_S is Alexandroff. First note the following remark.

Remark 3.1. Let $\{(A, \tau_i)\}_{i \in I}$ be a family of topological S-acts. Let τ_A be the topology generated by the subbasis $\cup_{i \in I} \tau_i$ on A. Then we show that (A, τ_A) is a topological S-act. Let $s \in S$, $a \in A$, and $U \in \tau_A$ such that $sa \in U$ and $U \in \tau_A$. As we have in section 2.18 of [21], we can and will suppose that U is an element of the subbasis $\cup_{i \in I} \tau_i$. So there is some $i \in I$ such that $U \in \tau_i$.

Since (A, τ_i) is a topological S-act, there exist open sets $W \in \tau_i$ and $V \in \tau_S$ which contain a and s, respectively such that $V \cdot W \subseteq U$. Since $\tau_i \subseteq \tau_A$, (A, τ_A) is a topological S-act.

Proposition 3.2. *For any topological monoid $(S, \cdot, \tau_S)$, the free topological S-act on a topological space (X, τ_X) is $F(X)$ with the topology τ_X^* which is generated by the union of all topologies τ_i on $|F(X)| = S \times X$ which makes $F(X)$ to a topological S-act and furthermore $\nu : (X, \tau_X) \longrightarrow (S \times X, \tau_i)$ is a topological embedding.*

Proof. Let (X, τ_X) be a topological space. We first show that if τ_X^* is the topology generated by the union of all topologies τ_i on $|F(X)| = S \times X$ where $(F(X), \tau_i)$ satisfies the following conditions

(a) the map $\nu : X \to (F(X), \tau_i)$ defined by $\nu(x) = (1, x)$ is a topological embedding.

(b) $(F(X), \tau_i)$ is a topological S-act.

Then $(F(X), \tau_X^*)$ satisfies conditions (a) and (b).

Define

$$\Gamma_{(X,\tau_X)} := \{\tau | \tau \text{ is a topology on } |F(X)| = S \times X \text{ satisfying (a) and (b)}\}.$$

We show that τ_X^* belongs to $\Gamma_{(X,\tau_X)}$ and $(F(X), \tau_X^*)$ is the desired free topological S-act. (One can easily check that $\tau_{S \times X} \in \Gamma_{(X,\tau_X)}$ and so $\Gamma_{(X,\tau_X)} \neq \emptyset$.)

Since τ_X^* is finer than each $\tau_i \in \Gamma_{(X,\tau_X)}$, so ν^{-1} is continuous and since τ_X^* is generated by all $\tau_i \in \Gamma_{(X,\tau_X)}$, so ν is continuous, therefore τ_X^* satisfies condition (a). By Remark 3.1, τ_X^* satisfies condition (b), too. Thus, $\tau_X^* \in \Gamma_{(X,\tau_X)}$. Therefore $(F(X), \tau_X^*)$ is a topological S-act.

Finally, to prove that $(F(X), \tau_X^*)$ is actually the free topological S-act on X, let $g : (X, \tau_X) \to (A, \tau_A)$ be a continuous function into a topological S-act (A, τ_A). We claim that the function $\tilde{g} : F(X) \to A$, defined by $\tilde{g}((s, x)) := sg(x)$, is the unique continuous S-map with $\tilde{g}\nu = g$. Clearly, $\tilde{g}$ is an S-map. Since $\tau_{S \times X} \subseteq \tau_X^*$, $(id_S, g) : (S \times X, \tau_X^*) \to (S \times A, \tau_{S \times A})$ is continuous and since the action $S \times A \to A$ is also continuous, $\tilde{g}$ is continuous.

For the uniqueness of $\tilde{g}$, let $\tilde{g} \circ \nu = h \circ \nu$. Therefore $h((1, x)) = \tilde{g}((1, x))$, and so $\tilde{g} = h$. Hence, the S-act $F(X)$ with τ_X^* is the free topological S-act on the topological space (X, τ_X). □

Before we begin to describe the topology τ_X^* more concretely, we need some definitions and results which are presented in the following

Remark 3.3. Suppose that we are given a topological space (X, τ_X) and a topological monoid $(S, \cdot, \tau_S)$. We define $\tau(S, X)$ as follows: $O \in \tau(S, X)$ if there exist open sets $Y \in \tau_X$ and $T \in \tau_S$ such that $\pi_1(O) = T$ and $\pi_2(O) = Y$ and for any $(s, x) \in O$, there exist an open set $V(O, x) \in \tau_S$ and an open set $W(O, s) \in \tau_X$ which contain s and x, respectively such that

$$\pi_1(O \cap (S \times \{x\})) = V(O, x) \text{ and } \pi_2(O \cap (\{s\} \times X)) = W(O, s).$$

One can obviously see that

$$V(O, x) = \{s \in S | (s, x) \in O\} \text{ and } W(O, s) = \{x \in X | (s, x) \in O\}. \qquad \text{(I)}$$

(where π_1 and π_2 are the usual projections of O onto its first and second factors, respectively). Note that for each $O \in \tau(S, X)$ and the corresponding open sets $\{V(O, x)\}_{x \in Y} \subseteq \tau_S$ and $\{W(O, s)\}_{s \in T} \subseteq \tau_X$ which are obtained by the definition of $\tau(S, X)$, we have

$$O = \bigcup_{x \in Y} (V(O, x) \times \{x\}) \text{ and } O = \bigcup_{s \in T} (\{s\} \times W(O, s)). \qquad \text{(II)}$$

Therefore if we define for an open set $Y \in \tau_X$ and an open set $T \in \tau_S$,

$$\begin{aligned} \tau_1(T, Y) := \quad & \{O \subseteq T \times Y | \forall (s, x) \in O, \exists V(O, x) \in \tau_S : s \in V(O, x) \text{ and} \\ & \pi_1(O \cap (S \times \{x\})) = V(O, x)\} \\ \tau_2(T, Y) := \quad & \{O \subseteq T \times Y | \forall (s, x) \in O, \exists W(O, s) \in \tau_X : x \in W(O, s) \text{ and} \\ & \pi_2(O \cap (\{s\} \times X)) = W(O, s)\} \end{aligned}$$

and

$$\tau_1(S, X) := \bigcup_{T \in \tau_S,\ Y \in \tau_X} \tau_1(T, Y) \quad \text{and} \quad \tau_2(S, X) := \bigcup_{T \in \tau_S,\ Y \in \tau_X} \tau_2(T, Y),$$

then by the definition of $\tau(S, X)$, one can easily see that

$$\tau(S, X) = \tau_1(S, X) \cap \tau_2(S, X).$$

By an easy check, one can see that $\tau_1(S, X)$ and $\tau_2(S, X)$ are two topologies on $|F(X)| = S \times X$ (Note that each element of $\tau_1(S, X)$ satisfies the right side of Relation (II) and each element of $\tau_2(S, X)$ satisfies the left side of Relation (II)), so $\tau(S, X)$ is a topology on $F(X)$, too. (Since the intersection of any two topologies on a space is a topology on it.)

Lemma 3.4. *Let $(S, \cdot, \tau_S)$ be a topological semigroup and (X, τ_X) be a topological space. Then $(F(X), \tau(S, X))$ is a semitopological S-act.*

Proof. We prove that for any $s \in S$ and $(t, x) \in F(X)$, the functions $\lambda_s : F(X) \to F(X)$ and $\rho_{(t,x)} : S \to F(X)$ are continuous. First, we show that the function λ_s is continuous. Suppose that we are given $U \in \tau(S, X)$. We show that $\lambda_s^{-1}(U)$ is an open set in $F(X)$. By the definition of $\tau(S, X)$ there exist open sets $T \in \tau_S$ and $Y \in \tau_X$ such that $U \subseteq T \times Y$ and for any $t' \in T$ and $x' \in Y$ such that $(t', x') \in U$, there exist open sets $V(U, x')$ and $W(U, t')$ which contain t' and x', respectively, such that

$$\pi_1(U \cap (S \times \{x'\})) = V(U, x') \text{ and } \pi_2(U \cap (\{t'\} \times X)) = W(U, t').$$

Note that since $(S, \cdot, \tau_S)$ is a topological monoid, the function $\lambda_s^{(S)} : S \to S$ is continuous. Now by the definition of the action of $F(X)$, we have

$$\lambda_s^{-1}(U) = \bigcup_{y \in Y} [(\lambda_s^{(S)})^{-1}(V(U, y)) \times \{y\}].$$

To prove $\lambda_s^{-1}(U)$ is in $\tau(S, X)$, we show that it is equal to an open set which belongs to $\tau(S, X)$. Define $V_1 := (\lambda_s^{(S)})^{-1}(T)$ and $U' := \cup_{t' \in V_1}(\{t'\} \times W(U, st'))$ where $W(U, st')$ is the open set which is found for the element $(st', y) \in U$ for some $y \in X$, by the assumption $U \in \tau(S, X)$. (Note that since we have $\pi_2(U \cap (\{st'\} \times X)) = W(U, st')$, $W(U, st')$ does not depend on the choice of $y \in X$.) We show that $\lambda_s^{-1}(U)$ equals U', and U' belongs to $\tau_1(S, X)$, since it is easy to see that $U' \in \tau_2(V_1, Y) \subseteq \tau_2(S, X)$. (Note that $U \in \tau_2(S, X)$ and recall Relation (I).) By the definition of the action of $F(X)$, we have obviously $\lambda_s(U') \subseteq U$. Suppose that $(t_1, y) \in \lambda_s^{-1}(U)$ for some $t_1 \in S$ and $y \in X$, so we have $(st_1, y) \in U$. Therefore we have $\{st_1\} \times W(U, st_1) \subseteq U$ which by the definition of the action $F(X)$, implies that $(t_1, y) \in \{t_1\} \times W(U, st_1)$. But $\{t_1\} \times W(U, st_1)$ is a subset of U', hence $(t_1, y) \in U'$. Therefore $U' = \lambda_s^{-1}(U)$ which implies that $\lambda_s^{-1}(U) \in \tau(S, X)$.

Now, we show the continuity of $\rho_{(t,x)}$. Consider U like the above and suppose that we are given $s' \in S$ such that $s' \in \rho_{(t,x)}^{-1}(U)$. Again note that since $(S, \cdot, \tau_S)$ is a topological monoid, the function $\rho_t : S \to S$ is continuous. Since $U \in \tau(S, X)$, there exists open set $V(U, x)$ in τ_S which contains $s't$ and $V(U, x) \times \{x\} \subseteq U$. Therefore $s' \in \rho_t^{-1}(V(U, x)) \in \tau_S$. We have $\rho_{(t,x)}(s') \in \rho_{(t,x)}(\rho_t^{-1}(V(U, x))) \subseteq V(U, x) \times \{x\} \subseteq U$. So $\rho_t^{-1}(V(U, x)) \subseteq \rho_{(t,x)}^{-1}(U)$. Hence $\rho_{(t,x)}^{-1}(U) \in \tau_S$. □

The following result shows a characterization of $\tau(S, X)$.

Proposition 3.5. *Let (X, τ_X) be a topological space and $(S, \cdot, \tau_S)$ be a topological monoid. Then $\tau(S, X)$ is the finest topology on $F(X)$ such that $F(X)$ is a semitopological S-act and $\nu : (X, \tau_X) \to (F(X), \tau(S, X)), x \rightsquigarrow (1, x)$, is continuous.*

Proof. By the above proposition and the definition of $\tau(S, X)$, $\tau(S, X)$ has the above properties. Let τ be a topology on $|F(X)| = S \times X$ with the above properties. First note that if $s(1, x) = (s, x) \in U$ and $U \in \tau$, then by the continuity of $\rho_{(1,x)}$, λ_s and ν we can conclude that

$$s \in \rho^{-1}_{(1,x)}(U) \text{ and } x \in \nu^{-1}(\lambda^{-1}_s(U)),$$

where $\rho^{-1}_{(1,x)}(U) \in \tau_S$ and $\nu^{-1}(\lambda^{-1}_s(U)) \in \tau_X$. Furthermore we have obviously

$$\pi_1(U \cap (S \times \{x\})) = \rho^{-1}_{(1,x)}(U) \in \tau_S$$

and also

$$\pi_2(U \cap (\{s\} \times X)) = \nu^{-1}(\lambda^{-1}_s(U)) \in \tau_X$$

Hence, $U \in \tau(S, X) = \tau_1(S, X) \cap \tau_2(S, X)$. Therefore $\tau \subseteq \tau(S, X)$ □

By the above proposition, we can explain the topology τ^*_X in another way and we can present a coarser and finer topology than it, according to the topologies τ_S and τ_X (note that any topological S-act is a semitopological S-act and note that τ^*_X satisfies condition (b) in the proof of Proposition 3.2).

Corollary 3.6. *Let $(S, \cdot, \tau_S)$ be a topological monoid and (X, τ_X) be a topological space. Then, $\tau_{S\times X} \subseteq \tau^*_X \subseteq \tau(S, X)$ and τ^*_X is the finest topology which is coarser than $\tau(S, X)$ and it makes $F(X)$ a topological S-act.* □

Proposition 3.7. *For any Alexandroff topological monoid $(S, \cdot, \tau_S)$ and any topological space (X, τ_X), the topology τ^*_X is the product topology on $|F(X)| = S \times X$. In fact we have $\tau^*_X = \tau_{S\times X} = \tau(S, X)$.*

Proof. We first show that, in this case, τ^*_X equals to $\tau(S, X)$ and then we show that $\tau(S, X)$ equals to the product topology $\tau_{S\times X}$. Note that by Corollary 3.6, we have $\tau^*_X \subseteq \tau(S, X)$. On the other hand, since $\tau(S, X)$ obviously satisfies condition (a) by Relation (I) in Remark 3.3, to complete our proof, it is enough to prove that $(F(X), \tau(S, X))$ is a topological S-act. Suppose $t(s, x) = (ts, x) \in U$ and $U \in \tau(S, X)$. Hence there exists open set $W(U,ts) \in \tau_X$ with $x \in W(U,ts)$ such that $\{ts\} \times W(U,ts) \subseteq U$. But for any $y \in W(U,ts)$, since again $U \in \tau(S,X)$, there exists open set $V(U,y) \in \tau_S$ such that $V(U,y) \times \{y\} \subseteq U$ and $ts \in V(U,y)$. Now define $V := \cap_{y \in V(U,y)} V(U,y) \in \tau_S$, because τ_S is Alexandroff, V contains ts and we have:

$$V \times W(U,ts) \subseteq \bigcup_{y \in W(U,ts)} (V(U,y) \times \{y\}) \subseteq U. \quad (*)$$

Now since $(S, \cdot, \tau_S)$ is a topological monoid, there exist open sets V_s and V_t which contain s and t, respectively and satisfy the relation $V_t \cdot V_s \subseteq V$. By Corollary 3.6, if we define $W := V_s \times W(U,ts)$, then $W \in \tau_{S \times X} \subseteq \tau(S,X)$ which contains (s,x) such that

$$t(s,x) \in V_t \cdot W = (V_t \cdot V_s) \times W(U,ts) \subseteq V \times W(U,ts) \subseteq U.$$

So $(F(X), \tau(S,X))$ is a topological S-act. Now suppose that $U \in \tau(S,X)$. If U is a non-empty open subset of $|F(X)| = S \times X$, then consider an arbitrary element (t,x) in U. We have clearly $t(1,x) \in U$, so by the above discussion, there exists an open set $V \in \tau_S$ which contains t such that $(t,x) = t(1,x) \in V \times W(U,t) \subseteq U$. (Recall Relation (*) with $s = 1$.) Since $V \times W(U,t)$ belongs to the product topology on $|F(X)| = S \times X$, $\tau_{S \times X}$ is finer than $\tau(S,X)$. Therefore by Corollary 3.6 we have $\tau_X^* = \tau(S,X) = \tau_{S \times X}$. $\square$

Proposition 3.8. *Suppose that $(S, \cdot, \tau_S)$ is a topological monoid. For each Alexandroff topological space (X, τ_X), the topology τ_X^* is the product topology on $S \times X$ and more precisely $\tau_X^* = \tau_{S \times X} = \tau(S,X)$.*

Proof. τ_X^* satisfies conditions (a) and (b) in Proposition 3.2 so $\tau_{S \times X} \subseteq \tau(S,X)$. Suppose that we are given $(ts,x) \in U$ for some $t,s \in S$, $x \in X$ and an open set $U \in \tau(S,X)$. Since $U \in \tau(S,X)$, we can choose for $(ts,x) \in U$, the open set $V(U,x)$ such that $V(U,x) \times \{x\} \subseteq U$ and $ts \in V(U,x)$. Choose for any $s' \in V(U,x)$, an open set $W(U,s')$ such that $\{s'\} \times W(U,s') \subseteq U$ and $x \in W(U,s')$. Define $W := \cap_{s' \in V(U,x)} W(U,s')$. Now, by a similar argument as in the proof of Proposition 3.7, we can get the result. $\square$

Since every discrete topological space is Alexandroff, as an immediate consequence of the above proposition and Proposition 3.5, we have

Proposition 3.9. (Free topological S-act on a set) *Let $(S, \cdot, \tau_S)$ be a topological monoid and Z be a set. Then the free topological S-act on the set Z is $F(Z)$ with the topology $\tau_{S \times Z}$ where τ_Z in the definition of $\tau_{S \times Z}$ is the discrete topology.*

Now we discuss the properties of the free topological S-act on a topological space which satisfies some of the separation axiom, (for more details about the separation axioms, see [21].)

Proposition 3.10. *Let $(S, \cdot, \tau_S)$ be a topological monoid with left ideal topology. Suppose that (X, τ_X) satisfies one of the separation axioms T_i for $i = 0, 1, 2, 3, 3\frac{1}{2}$. Then, the free topological S-act on (X, τ_X) satisfies that separation axiom if and only if $S = \{1\}$.*

Proof. For the non-trivial part, let (X, τ_X) be a T_i space for some i. Then, by assumption, the free topological S-act on (X, τ_X) is a T_i space. Note that if a topological S-act (A, τ_A) which has subact topology, satisfies T_i, then for any $a \in A$, $Sa = \{a\}$. For, if there exist $s \in S$ and $a \in A$ such that $sa \neq a$, then any open set in the subact topology τ_A containing a, also contains sa. Thus, we have $S(s, x) = \{(s, x)\}$ for each $(s, x) \in F(X)$. In particular, $S(1, x) = \{(1, x)\}$. Therefore $S = S1 = \{1\}$. $\square$

Although Proposition 3.10 shows that for any non-trivial topological monoid $(S, \cdot, \tau_S)$ with left ideal topology, the free topological S-act on a T_i space does not satisfy any of the separation axioms T_i, but the following proposition shows that if $(S, \cdot, \tau_S)$ itself satisfies any T_i, $i = 0, 1, 2$ then the free topological S-act on a topological space which satisfies that T_i, satisfies that separation axiom, too.

First, note that if (X_1, τ_{X_1}) and (X_2, τ_{X_2}) are two topological spaces which satisfy T_i for some $i = 0, 1, 2$, then their product space satisfies that T_i, too (for more details, see [10] or [21]).

Proposition 3.11. *Let $(S, \cdot, \tau_S)$ be a topological monoid which satisfies T_i for some $0 \leq i < 3$. Then, the free topological S-act on a topological space which satisfies that T_i, satisfies that separation axiom, too.*

Proof. suppose that the topological space (X, τ_X) satisfies T_i. Clearly $S \times X$ with product topology also satisfies T_i, too and since for any topological space (X, τ_X), we have $\tau_{S \times X} \subseteq \tau_X^*$, then $(F(X), \tau_X^*)$ satisfies T_i. $\square$

Remark 3.12. About the preservation of $T_{3\frac{1}{2}}$, first, we prove that if we define $\Gamma'_{(X,\tau_X)}$ as follows,

$$\{\tau | \tau \text{ is a completely regular topology on } |F(X)| \text{ satisfing (a) and (b)}\}$$

and let τ'_X be defined to be the generated topology by $\cup_{\tau_i \in \Gamma_{(X,\tau_X)}} \tau_i$, then $(F(X), \tau'_X)$ is a completely regular topological S-act. Then we give a condition such that the completely regularity is preserved. For our assertion, we just need to show the completely regularity of $(F(X), \tau'_X)$, since it is straightforward to see that τ'_X satisfies conditions (a) and (b). For this purpose, we show that the generated topology by a family of topologies $(\tau_i)_{i\in I}$ on a set C such that each τ_i is completely regular for any $i \in I$, is a completely regular topology on C. Let $(\tau_i)_{i\in I}$ be a family of completely regular topologies on a set C. Let τ be the generated topology by $\cup_{i\in I}\tau_i$. Let K be a closed set in C with the topology τ and $c \in C \setminus K$. Since $O = C \setminus K$ belongs to τ, there exists a family of open sets $\{O_j\}_{j\in J} \subseteq \cup_{i\in I}\tau_i$ such that O is equal to a union of their finite intersections of O_i's. Therefore we can assume that there exists $O_1 \cap \ldots \cap O_n$ such that $K = C \setminus O \subseteq C \setminus (O_1 \cap \ldots \cap O_n)$ and $c \in O_1 \cap \ldots \cap O_n$. Since for any i, O_i is open in τ_{n_i} and since τ_{n_i} is completely regular, for closed set $C \setminus O_i$ and c, there exists a continuous real valued function $f_i : C \to \mathbb{R}$ such that $f_i(C \setminus O_i) = 1$ and $f_i(c) = 0$. Since τ is the generated topology by τ_i, all the functions f_i are continuous real valued function from C with the topology τ to $\mathbb{R}$ such that $f_i(C \setminus O_i) = 1$ and $f_i(c) = 0$. Let f be defined by $f(x) := max\{f_1(x), \ldots, f_n(x)\}$, for any $x \in C$. Therefore τ is completely regular, since f is a continuous function from C with topology τ to $\mathbb{R}$ such that f is continuous and $f(K) = 1$ and $f(c) = 0$. Therefore, since τ'_X is the generated topology by $\cup_{\tau_i \in \Gamma'_{(X,\tau_X)}}\tau_i$, and since for each $\tau_i \in \Gamma'_{(X,\tau_X)}$, τ_i is completely regular, τ'_X is completely regular. Hence $(F(X), \tau'_X)$ is a completely regular topological S-act.

Now if for a topological semigroup $(S, \cdot, \tau_S)$ and a topological space (X, τ_X), we have $\tau'_X = \tau^*_X$ or more specially, if $\Gamma'_{(X,\tau_X)} = \Gamma_{(X,\tau_X)}$, then the separation axiom $T_{3\frac{1}{2}}$ is preserved. For an example of a topological semigroup $(S, \cdot, \tau_S)$ and a topological space (X, τ_X) with this property, let $(S, \cdot, \tau_{dis})$ be a topological monoid. Then for any completely regular space (X, τ_X), clearly, by Proposition 3.7, $\tau^*_X = \tau_{S\times X} = \tau'_X$. Therefore for a topological semigroup which has discrete topology, the separation axiom $T_{3\frac{1}{2}}$ is preserved.

4. The free topological S-act on an S-act

The category **S-Act** is a very well-known category and its universal structures are studied comprehensively by many authors. In this section we want to present a very useful and effective tool which enables us to study **S-Top** by using the studies in **S-Act**. First, in this section, we present the free topological S-act on an S-act, then to illustrate the application of this result, we characterize the projective topological S-acts. In fact, we show that the projective topological S-acts are exactly the free topological S-acts on projective S-acts.

Now we discuss the free topological S-act on an S-act. One might naturally expect that an S-act A with discrete topology to be the free topological S-act on A, but, as Proposition 4.1 shows, A with this topology may not be a topological S-act and if it happens to be so, then it is indeed the free topological S-act on A.

Since by the definition of topological S-acts, the proof of the following result is straightforward, we state it without proof.

Proposition 4.1. *An S-act A with the discrete topology is a topological S-act if and only if for any $a \in A$ and $s \in S$, $(sa : a) := \{t \in S | ta = sa\} \in \tau_S$.* $\square$

Proposition 4.2. *If $(S, \cdot, \tau_S)$ is a topological semigroup with a right identity, then the following statements are equivalent*

(1) *All the S-acts with discrete topology are topological S-acts.*

(2) *τ_S is the discrete topology.*

(3) *If we define* G *from category* **S-Act** *to category* **S-Top** *as follows, $A \mapsto (A, \tau_{dis})$, then* G *is the free functor.*

Proof. Since (1) and (3) are equivalent, for the non-trivial part of the proof, by Proposition 4.1, we just need to show (1) $\Rightarrow$(2). Since S with the discrete topology is a topological S-act, if e is the right identity of S, then the function $id_S = \rho_e : (S, \tau_S) \to (S, \tau_{dis})$ is continuous and hence $\tau_S = \tau_{dis}$. $\square$

Now, we discuss about the free topological S-act on an S-act in general.

Proposition 4.3. *For any topological semigroup $(S, \cdot, \tau_S)$, the free topological S-act on an S-act A is defined as follows*

$$(A, \tau_{*A}), \qquad (A \in \mathbf{S-Act})$$

in which τ_{*A} is the topology generated on A by the union of all τ_i on A, where (A, τ_i) is a topological S-act.

Proof. Let A be an arbitrary S-act and define

$$\Sigma_A := \{\tau | \ (A, \tau) \text{ is a topological } S\text{-act}\}.$$

(Note that every S-act is a topological S-act with trivial topology, so Σ_A is not empty.)

Similar to the proof of Proposition 3.2, we can show that τ_{*A} which is the topology generated by the union of all τ_i where $\tau_i \in \Sigma_A$, makes A a topological S-act.

To prove that (A, τ_{*A}) with $id_A : A \to (A, \tau_{*A})$ is the free topological S-act on A, let $f : A \to (B, \tau_B)$ be an S-map into a topological S-act (B, τ_B). Then, the same function $f : (A, \tau_{*A}) \to (B, \tau_B)$ is claimed to be a continuous S-map.

Let $\tau_f := \{f^{-1}(U)\}_{U \in \tau_B}$. To prove the claim, first we show that (A, τ_f) is a topological S-act. Let $U \in \tau_B$, $sa \in f^{-1}(U)$ for some $a \in A$ and $s \in S$. Since $f(sa) = sf(a) \in U$ and (B, τ_B) is a topological S-act, there exists $V_s \in \tau_S$ and $W_{f(a)} \in \tau_B$ such that $s \in V_s$ and $f(a) \in W_{f(a)}$ and

$$sf(a) \in V_s \cdot W_{f(a)} \subseteq U.$$

Thus, $sa \in V_s \cdot f^{-1}(W_{f(a)}) \subseteq f^{-1}(U)$, and so (A, τ_f) is a topological S-act.

Now, since $\{f^{-1}(U)\}_{U \in \tau_B}$ belongs to Σ_A, by the definition of τ_{*A}, we have

$$\tau_f = \{f^{-1}(U)\}_{U \in \tau_B} \subseteq \tau_{*A}.$$

So $f : (A, \tau_{*A}) \to (B, \tau_B)$ is continuous.

The rest of the proof is trivial. $\square$

Now using the concept of weak topology and the above proposition and its proof, we can explain τ_{*A} in these ways.

Proposition 4.4.

(i) *τ_{*A} is the weak topology which is induced on $|A|$ with respect to the family of S-homomorphisms $id : A \to (A, \tau_i)$ where (A, τ_i) is a topological S-act.*

(ii) *τ_{*A} is the weak topology on $|A|$ with respect to the family of all S-homomorphisms from A to other topological S-acts.* $\square$

Note that, for a topological space (X, τ_X) and any topological monoid $(S, \cdot, \tau_S)$, since $(F(X), \tau_X^*)$ is a topological S-act, it is obvious that τ_X^* on $|F(X)| = S \times X$ is coarser than $\tau_{*F(X)}$. (See the definitions of $\Gamma_{(X,\tau_X)}$ and $\Sigma_{F(X)}$ in the proof of Propositions 3.2 and 4.3.)

But, the following example shows that τ_X^* can be a proper subset of $\tau_{*F(X)}$.

Example 4.5. Let $(S, \cdot, \tau_{dis})$ be a topological monoid and let (X, τ_X) be a non-discrete topological space. Then $\tau_X^* \subsetneq \tau_{*F(X)}$. Because, by Proposition 4.2, $\tau_{*F(X)}$ is discrete. On the contrary, suppose that $\tau_{*F(X)}$ equals to τ_X^*. Since ν is an embedding, and since $\{1\} \times X$ with the subspace topology is the discrete topology (because $\tau_{*F(X)}$ is discrete), (X, τ_X) is a discrete space, which is impossible. So we have the result.

For all universal objects in category **S-Top**, we can use the free topological S-acts on S-acts to change any given diagrams in **S-Act** to a given diagram in **S-Top**. Therefore, we can study the algebraic structure of universal structures by using the known universal objects in **S-Act**. To illustrate this method, we apply it in the next proposition to characterize the projective topological S-acts.

Proposition 4.6. *Let $(S, \cdot, \tau_S)$ be a topological monoid. Then the projective topological S-acts are the free topological S-acts on the S-acts $\sqcup_{i \in I} Se_i$, where e_i's are idempotents in S, I is a set and $\sqcup_{i \in I} Se_i$ denote the coproduct of Se_i's.*

Proof. Let (P, τ_P) be a projective S-act. First, we show that (P, τ_P) is the free topological S-act on S-act P. For this purpose, we show that topology τ_P is the finest topology which makes P a topological S-act. Let (P, τ) be a topological S-act. We show that τ is coarser than τ_P. Consider the generated topology by the union of τ and τ_P, and denote it by τ'. Consider the identity maps $id_P : (P, \tau_P) \to (P, \tau_P)$ and $id_P : (P, \tau') \to (P, \tau_P)$. Since (P, τ_P) is a projective topological S-act, the identity map $id_P : (P, \tau_P) \to (P, \tau')$ is continuous. Therefore τ' is coarser than τ_P and therefore $\tau \subseteq \tau_P$. Now, to complete the proof, we show that P is a projective S-act and then we use [18, Theorem 1.5.10], to characterize the algebraic structure of (P, τ_P). Suppose that $f : A \to B$ be a surjective S-map, where A and B are S-acts and let $g : P \to B$ be an S-map. Since the epimorphisms in category **S-Act** are exactly onto S-maps (see [18]), it is straightforward to see that $f : (A, \tau_{*A}) \to (B, \tau_{*B})$ is an epimorphism in **S-Top** and $g : (P, \tau_P) \to (B, \tau_{*B})$ is continuous (note that if C is an S-act, (D, τ_D) is a topological S-act and $h : C \to (D, \tau_D)$ is an S-map, then $\tau_1 = \{V \subseteq C | V = f^{-1}(U)$, where U is an open set in $(D, \tau_D)\}$ is a topology on C such that (C, τ_1) is a topological S-act). Since (P, τ_P) is a projective topological S-act, there exists a continuous S-map $h : (P, \tau_P) \to (A, \tau_{*A})$ such that $f \circ h = g$. Since h is an S-map, P is a projective S-act. Therefore by [18, Theorem 1.5.10], there exists a family $\{e_i\}_{i \in I}$ of idempotents in S such that P is algebraically isomorphic to $\sqcup_{i \in I} Se_i$, where $\sqcup$ denotes the coproduct of Se_i's in **S-Act**. Therefore, P is the projective S-act which is a coproduct of cyclic S-acts in **S-Act** and (P, τ_P) is the free topological S-act on S-act P. □

Finally in this paper we show that the free topological S-act on the set

For a non-empty family of S-acts, like $\{A_i\}_{i \in I}$, the coproduct of A_i's in **S-Act** is the disjoint union of A_i's with its natural action (see [18]).

Z is the free topological S-act on the S-act $F(Z)$. (So if we define the free topological S-act on a set Z in this way, then the result will be the same.)

Proposition 4.7. *let $(S, \cdot, \tau_S)$ be a topological monoid. The free topological S-act on the set Z equals to the free topological S-act on the S-act $F(Z)$.*

Proof. Since a discrete topological space (Z, τ_{dis}) is Alexandroff, by Proposition 3.8 we have $\tau_Z^* = \tau_{S\times Z}$. We show that the topology τ_* on $F(Z)$ equals to τ_Z^*. For this purpose, we show that $\Sigma_{F(Z)} = \Gamma_{(Z,\tau_{dis})}$. Since obviously, $\tau_Z^* \in \Sigma_{F(Z)}$, it is enough to show that $\tau_{*F(Z)}$ belongs to $\Gamma_{(Z,\tau_{dis})}$. Clearly, $\tau_{*F(Z)}$ on $F(Z)$ satisfies condition (a). Since $\tau_{S\times Z} = \tau_Z^* \subseteq \tau_{*F(Z)}$ and Z is a discrete space, then $\{U \cap (\{1\} \times Z) | U \in \tau_{*F(Z)}\}$ is the discrete topology on $\{1\} \times Z$. Since $\nu : Z \to \{1\} \times Z$ is a one to one, onto function from a discrete topological space to another discrete topological space, it is an embedding. Therefore $\tau_{*F(Z)}$ satisfies conditions (a) and (b) in Proposition 3.2 and hence $\tau_{*F(Z)} \in \Gamma_{(Z,\tau_{dis})}$. □

In fact, the proof of the above proposition shows that:

Corollary 4.8. *Let $(S, \cdot, \tau_S)$ be a topological monoid. Then for each set Z, we have $\tau_{*F(Z)}$ is the product topology $\tau_{S\times Z}$ on $S \times Z$, where τ_Z in the definition of $\tau_{S\times Z}$ is the discrete topology on Z.* □

5. Acknowledgement

The author is highly grateful to the referees for very valuable suggestions and corrections which improve the paper essentially. The author gratefully acknowledges the financial support from Shahid Beheshti University, given to him by his supervisor, Professor Ebrahimi, and wants to express his thanks to Professor Ebrahimi for his kindness and helps and his advisor, Professor Mahmoudi. Also he is grateful to Professor Gutik, for his helpful communications.

References

[1] **J. Adamek, H. Herlich and G. Strecker**, *Abstract and concrete categories*, John Wiley & Sons, Inc., New York, 1990.

[2] **A. Aldroubi, D. Larson, W. Tang and E. Weber**, *Geometric aspects of frame representation of Abelian groups*, Trans. Am. Math. Soc. **356** (2004), $4767 - 4786$.

[3] **T. O. Banakh, I. Yo. Guran and O. V. Gutik**, *Free topological inverse semigroups*, Mat. Stud. (Lvov) **15** (2001), 23 – 43.

[4] **J. F. Berglund and K. H. Hofmann**, *Compact semitopological semigroups and weakly almost periodic functions*, Lecture Notes in Math. 42, Springer-Verlag, Berlin-New York, 1967.

[5] **J. F. Berglund, H. D. Junghenn and P. Milnes**, *Analysis on semigroups. Function spaces, compactifications, representations* Canadian Math. Soc. Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York, 1989.

[6] **T. S. Blyth**, *Categories*, John Wiley & Sons, Inc., New York, 1986.

[7] **G. B. Bredon**, *Topology and Geometry*, Springer-Verlag, New York, 1993.

[8] **S. Bulman-Fleming and M. Mahmoudi**, *The category of S-posets*, Semigroup Forum **71** (2005), 443 – 461.

[9] **D. Dikranjan and M. Tkačenko**, *Weakly complete free topological groups*, Topology Appl. **112** (2001), 259 – 287.

[10] **J. Dugundji**, *Topology*, Reprinting of the 1966 original. Allyn and Bacon, Inc., Boston, Mass.-London-Sydney, 1978.

[11] **M. M. Ebrahimi and M. Mahmoudi**, *The category of M-sets*, Ital. J. Pure Appl. Math. **9** (2001), 123 – 132.

[12] **G. B. Folland**, *A course in abstract harmonic analysis*, Studies Adv. Math., CRC Press, Boca Raton, FL, 1995.

[13] **D. Han and D. R. Larson**, *Frames, bases and group representations*, Mem. Am. Math. Soc. **147** (2000), 697.

[14] **J. L. Kelley**, *General topology*, Reprint of the 1955 edition. Graduate Texts in Mathematics, No. 27. Springer-Verlag, New York-Berlin, 1975.

[15] **H. B. Keynes**, *A note on universal flows*, Amer. Math. Monthly **76** (1969), 276 – 277.

[16] **B. Khosravi**, *The category of semitopological S-acts*, World Appl. Sci. J. **7** (2009), 7 – 13.

[17] **A. Khosravi and B. Khosravi**, *Frames and bases in tensor products of Hilbert spaces and Hilbert C^*-modules*, Proc. Indian Acad. Sci. Math. Sci. **117** (2007), 1 – 12.

[18] **M. Kilp, U. Knauer and A. Mikhalev**, *Monoids, acts and categories*, Walter de Gruyter, Berlin, New York, 2000.

[19] **J. Lawson and A. Lisan**, *Flows, congruences, and factorizations*, Topology Appl. **58** (1994), 35 – 46.

[20] **J. M. Lee**, *Introduction to smooth manifolds*, Springer-Verlag, New York, 2003.

[21] **J. R. Munkres**, *Topology*, Prentice-Hall, New Jersey, 2000.

[22] **P. Normak**, *Topological S-acts: preliminaries and problems*, Transformation semigroups (Colchester, 1993), $60-69$, Univ. Essex, Colchester.

[23] **W. Ruppert**, *Compact semitopological semigroups: an intrinsic theory*, Lecture Notes in Math. Springer-Verlag, Berlin, 1984.

[24] **G. I. Zhitomirski**, *Topologically complete representations of inverse semigroups*, Semigroup Forum **66** (2003), $121-130$.

Received July 16, 2009
Revised February 28, 2010

Department of Mathematics, Shahid Beheshti University, Tehran, Iran
E-email: behnam_kho@yahoo.com

Quasigroups and Related Systems **18** (2010), 43 – 58

Transversals in loops. 1. Elementary properties

Eugene Kuznetsov

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. A new notion of a transversal in a loop to its subloop is introduced and studied. This notion generalized a well-known notion of a transversal in a group to its subgroup and can be correctly defined only in the case, when some specific condition (condition A) for a loop and its subloop is fulfilled. Elementary properties of the transversals in a loop to its subloop are investigated and proved. With the help of the notion of transversal in a loop to its subloop a new notion of permutational representation of a loop by left (right) cosets to its subloop is introduced and studied.

1. Introduction

In group theory, in group representation theory and in quasigroup theory the following notion is well-known – the notion of a left (right) transversal in a group to its subgroup [1, 5, 6, 10].

Definition 1.1. Let G be a group and H be a subgroup in G. A complete system $T = \{t_i\}_{i \in E}$ of representatives of the left (right) cosets of H in G $(e = t_1 \in H)$ is called a *left* (*right*) *transversal in* G *to* H.

In the present work a variant of natural generalization of the notion of transversal at the class of loops is proposed and studied. As the elements of a left (right) transversal in a group to its subgroup are the representatives of every left (right) coset to the subgroup, then a notion of a left (right) transversal in a loop to its subloop can be correctly defined only in a case when this loop admits a left (right) coset decomposition by its subloop (see [11] and the Condition A below).

2000 Mathematics Subject Classification: 20N05
Keywords: quasigroup, loop, transversal, coset, representation.

In the part 2 of this article we start studying a class of loops which admits a left (right) coset decomposition by its subloop (admits the left (right) condition A). Elementary properties of those loops are proved. One of these properties (for finite loops) is an analogue of Lagrange theorem for groups.

In the part 3 of this article at the investigated class of loops we introduce the notion of left (right) transversals to its subloops. Some elementary properties of the transversals are investigated and proved.

In the part 4 of this article at this class of loops we introduce and study a notion of a permutational representation of loop by the left (right) cosets to its subloop. Elementary properties of this new notion are proved. Also we will prove an equivalence of this notion and a notion of permutation loop from [3].

Further we shall use the following notations:

$\langle L, \cdot, e\rangle$ is an initial loop with the unit e;

$\langle R, \cdot, e\rangle$ is its proper subloop;

E is a set of indexes ($1 \in E$) of the left (right) cosets R_i in L to R (assume $R_1 = R$).

2. Preliminaries

Definition 2.1. The system $\langle E, \cdot\rangle$ is called [2] a *right* (*left*) *quasigroup* if for arbitrary $a, b \in E$ the equation $x \cdot a = b$ ($a \cdot y = b$) has a unique solution in E. If $\langle E, \cdot\rangle$ is both a right and left quasigroup, then it is called a *quasigroup*. If in a right (left) quasigroup $\langle E, \cdot\rangle$ there exists an element $e \in E$ such that

$$x \cdot e = e \cdot x = x$$

for every $x \in E$, then $\langle E, \cdot\rangle$ is called a *right* (*left*) *loop* (the element e is called a *unit* or an *identity element*). If $\langle E, \cdot\rangle$ is both a right and left loop, then it is called a *loop*.

Definition 2.2. Let $\langle L, \cdot\rangle$ be a loop and $\langle R, \cdot\rangle$ be its proper subloop. Then a *left coset* of R is a set of the form

$$xR = \{xr \mid r \in R\},$$

and a *right coset* has the form

$$Rx = \{rx \mid r \in R\}.$$

The cosets in a loop to its subloop do not necessarily form a partition of the loop. This leads us to the following definition.

Definition 2.3. A loop L has a *left* (*right*) *coset decomposition by its proper subloop* R, if the left (right) cosets form a partition of the loop L, is equal for some set of indexes E

1. $\bigcup_{i \in E} (a_i R) = L$;
2. for every $i, j \in E$, $i \neq j \quad (a_i R) \cap (a_j R) = \varnothing$.

In order to define correctly a notion of a left (right) transversal in a loop to its proper subloop, it is necessary that the following condition be fulfilled.

Definition 2.4 (see [9]). (*Left Condition A*) Let R be a subloop of a loop L. For all $a, b \in L$ there exists $c \in L$ such that

$$a(bR) = cR. \tag{1}$$

The *right condition A* is defined analogously.

In [11] the following theorem was proved.

Lemma 2.5. *The following conditions are equivalent:*

1. *A loop L has a left cosets decomposition by its proper subloop R.*
2. *The following condition takes place (it can be named the weak left condition A): for every $a \in L$*

$$(aR)R = aR. \tag{2}$$

Proof. See in [11], Theorem I.2.12. □

Below we shall prove all statements only for a case of the left cosets (if the *left condition A* take place); in a case of the right cosets all proofs are similar.

Lemma 2.6. *Let the left condition A in a loop L to its subloop R be satisfied. Then*

$$(a \cdot R) \cdot R = a \cdot R \tag{3}$$

for all $a \in L$.

Proof. By the left condition A for all $a, b \in L$ there exists an element $c = c(a,b) \in L$ such that $a \cdot (b \cdot R) = c \cdot R$. In the loop L always it is possible to find an element $d = d(a,b)$ such that $c = a \cdot d$. Then

$$a \cdot (b \cdot R) = (a \cdot d) \cdot R. \tag{4}$$

So, for some $r_1 \in R$ we have $a \cdot (b \cdot r_1) = (a \cdot d) \cdot e = a \cdot d$. Thus, $b \cdot r_1 = d$, i.e., $d \in b \cdot R$. Therefore, $b \in R$ implies $d \in R$. Hence, for $b \in R$ from (4) it follows $a \cdot R = (a \cdot R) \cdot R$. The Lemma is proved. □

Lemma 2.7. *The following conditions are equivalent:*

1. *The left condition A is fulfilled in the loop L to its subloop R.*
2. *For every* $a, b \in L$

$$a \cdot (b \cdot R) = (a \cdot b) \cdot R. \tag{5}$$

Proof. $1 \Rightarrow 2$. Let the left condition A holds. Then for all $a, b \in L$ and all $r \in R$ there exist $c = c(a,b) \in L$ and $r_1 \in R$ such that $a \cdot (b \cdot r) = c \cdot r_1$. If $r = e$, then $a \cdot b = c \cdot r_1' \in c \cdot R$. Hence, according to Lemma 2.6,

$$(a \cdot b) \cdot R = (c \cdot R) \cdot R = c \cdot R,$$

which proves 2.

$2 \Rightarrow 1$. It is evident. □

Let us define (see [12]) for all $a, b \in L$ the *left inner mapping*

$$l_{a,b}(x) = (a \cdot b) \setminus (a \cdot (b \cdot x)), \qquad x \in L, \tag{6}$$

where "$\setminus$" is a left division in the loop $\langle L, \cdot, e\rangle$, and the *right inner mapping*

$$r_{a,b}(x) = ((x \cdot b) \cdot a) / (b \cdot a), \qquad x \in L, \tag{7}$$

where "/" is a right division in the loop $\langle L, \cdot, e\rangle$.

Lemma 2.8. *Let the left condition A in a loop L to its subloop R be satisfied. Then* $l_{a,b}(R) = R$ *for all* $a, b \in L$.

Proof. The proof is an evident corollary of Lemma 2.7. □

Lemma 2.9. *Let the right condition A in a loop L to its subloop R be satisfied. Then* $r_{a,b}(R) = R$ *for all* $a, b \in L$.

Proof. The proof is similar to the proof of a Lemma 2.8. □

Remark 2.10. It is known (see [12]) that the mappings $l_{a,b}$ generate the *left inner mappings group* $LI\left(\langle L, \cdot, e\rangle\right)$ of a loop L, and the mapings $r_{a,b}$ generate the *right inner mappings group* $RI\left(\langle L, \cdot, e\rangle\right)$ of a loop L. Therefore, if the left (right) condition A in a loop L to its subloop R is fulfilled, then the investigated class of loops satisfies a condition of an invariance of a subloop R relating to an action of the group $LI\left(\langle L, \cdot, e\rangle\right)$ (group $RI\left(\langle L, \cdot, e\rangle\right)$, respectively). So we can say that the subloop R is a *left* (*right*) *invariant subloop* of the loop L.

Remark 2.11. The condition (5) is called in [4] a *strong left coset decomposition of the loop L by its proper subloop R.*

Lemma 2.12. *Let the left condition A for a loop L and its subloop R is fulfilled. Then the following conditions hold:*

1. *Left cosets R_i form a left coset decomposition of the loop L;*
2. *If a loop L is finite, then the "Lagrange property" takes place: an order of the subloop R divides an order of the loop L.*

Proof. (see also [11]) 1. Let $R_i = aR$, $R_j = bR$. Assume that these cosets have a common element $c \in L$, i.e.,

$$c \in R_i \cap R_j = (aR) \cap (bR).$$

Then $c = a \cdot r_1 = b \cdot r_2$ for some $r_1, r_2 \in R$. So, $(a \cdot r_1) \cdot r = (b \cdot r_2) \cdot r$ for every $r \in R$. Let us show there exists an element $r_0 \in R$ such that

$$(a \cdot r_1) \cdot r_0 = a.$$

Indeed, if the left condition A for the loop L and its subloop R is fulfilled, then a subloop R is a left invariant subloop in the loop L. Hence $\forall a, b \in L$: $l_{a,b}\left(R\right) = R$. Let us take $r_0 = l_{a,r_1}\left(r_1 \backslash e\right)$. Then

$$r_0 = (a \cdot r_1) \backslash (a \cdot (r_1 \cdot (r_1 \backslash e))) = (a \cdot r_1) \backslash (a \cdot e) = (a \cdot r_1) \backslash a,$$

i.e., $(a \cdot r_1) \cdot r_0 = a$. So, by Lemma 2.6, we obtain

$$a = (a \cdot r_1) \cdot r_0 = (b \cdot r_2) \cdot r_0 = b \cdot r_2' \in b \cdot R.$$

Thus $a \cdot R = (b \cdot R) \cdot R = b \cdot R$. So, if $a \cdot R \neq b \cdot R$, then $(a \cdot R) \cap (b \cdot R) = \varnothing$.

Since $c \in (c \cdot R)$, for any element $c \in L$, we have $\bigcup\limits_{c \in L} (c \cdot R) = L$. So, left cosets R_i form a left coset decomposition of the loop L.

2. Let L be finite. Let us show that the number of elements in any left coset R_i is equal to the number of elements in R. Because L is a loop then

$$r_1 \neq r_2 \quad \Leftrightarrow \quad a \cdot r_1 \neq a \cdot r_2 \quad \forall r_1, r_2 \in R.$$

So, the left translation $L_a(r) = a \cdot r$ is an injection. Since L is finite, then the translation L_a is a surjection, i.e., it is a bijection. So, R and $a \cdot R$ have the same order for any $a \in R$.

Then, by 1, we have $L = \bigcup\limits_{c \in L} (c \cdot R)$, and consequently

$$|L| = \sum_{c_i \in L} |c_i \cdot R| = m \cdot |R|.$$

The Lemma is completely proved. □

Now we give two examples of loops and its proper subloops, where the left condition A is fulfilled.

Example 2.13. A loop L and its normal subloop R.

It is well known (see [2]), that if a subloop R is normal in a loop L, then an action of the left and right inner permutations $l_{a,b}$ and $r_{a,b}$ is an invariant relation $\forall a, b \in L$. Therefore both left and right conditions A are fulfilled in this case.

Example 2.14. A loop of pairs $L = \langle E \times E \backslash \{\Delta\}, *, \langle 0, 1 \rangle \rangle$ of an arbitrary DK-ternar $\langle E, (x, t, y), 0, 1 \rangle$ and its subloop $R = \{\langle 0, x \rangle \,| x \in E \backslash \{0\}\}$.

As it is known (see [7]), in a loop of pairs $L = \langle E \times E \backslash \{\Delta\}, *, \langle 0, 1 \rangle \rangle$ the operation "$*$" is defined through the ternary operation (x, t, y) of the DK-ternar $\langle E, (x, t, y), 0, 1 \rangle$ by the following way:

$$\langle x, y \rangle * \langle u, v \rangle \stackrel{def}{=} \langle (x, u, y), (x, v, y) \rangle.$$

The elements $\langle 0, x \rangle$ (where $x \in E \backslash \{0\}$) form a subloop R with the operation "$*$". Then for $a = \langle x, y \rangle \in L$, $b = \langle u, v \rangle \in L$ and $r = \langle 0, z \rangle \in R$ we have:

$$\begin{aligned} a * (b * r) &= \langle x, y \rangle * (\langle u, v \rangle * \langle 0, z \rangle) = \langle x, y \rangle * \langle u, (u, z, v) \rangle \\ &= \langle (x, u, y), (x, (u, z, v), y) \rangle = \langle \alpha_{x,y}(u), \alpha_{x,y} \alpha_{u,v}(z) \rangle. \end{aligned}$$

On the other hand, for $r_1 = \langle 0, z_1 \rangle$, we have:

$$\begin{aligned}(a * b) * r_1 &= (\langle x, y\rangle * \langle u, v\rangle) * \langle 0, z_1\rangle = \langle (x,u,y), (x,v,y)\rangle * \langle 0, z_1\rangle \\ &= \langle (x,u,y), ((x,u,y), z_1, (x,v,y))\rangle \\ &= \left\langle \alpha_{x,y}(u), \alpha_{\alpha_{x,y}(u),\alpha_{x,y}(v)}(z_1)\right\rangle .\end{aligned}$$

If elements $x, y, u, v \in E$ are given, then for every $z \in E\backslash\{0\}$ there exists $z_1 \in E\backslash\{0\}$ such that

$$\alpha_{x,y}\alpha_{u,v}(z) = \alpha_{\alpha_{x,y}(u),\alpha_{x,y}(v)}(z_1),$$

namely,

$$z_1 = \alpha^{-1}_{\alpha_{x,y}(u),\alpha_{x,y}(v)}\alpha_{x,y}\alpha_{u,v}(z).$$

Thus $a * (b * R) = (a * b) * R$. Hence the left condition A is fulfilled.

3. A transversal in a loop to its subloop.

Definition 3.1 (see [9]). Let $\langle R, \cdot, e\rangle$ be a subloop of the loop $\langle L, \cdot, e\rangle$ and let the left (right) condition A be satisfied. If $\{R_x\}_{x\in E}$ is the set of all left (right) cosets on L determined by R, then the set $T = \{t_x\}_{x\in E} \subset L$ is called the *left* (*right*) *transversal* in L if for every $x \in E$ there exists a unique element $t_x \in T$ such that $t_x \in R_x$. If $T = \{t_x\}_{x\in E}$ is both left and right transversal in L simultaneously, then it is called the *two-sided transversal.*

Remark 3.2. Analogously as in groups we assume that $t_1 = e$. If this assumption is not fulfilled then we have the so-called *non-reducible left* (*right*) *transversals.*

On E we define the following *transversal operations*:

$$x \overset{(T)}{\cdot} y = z \overset{def}{\Leftrightarrow} t_x \cdot t_y = t_z \cdot r, \tag{8}$$

where $t_x, t_y, t_z \in T$ are left transversals L to R and $r \in R$,

$$x \overset{(T)}{\circ} y = z \quad \overset{def}{\Leftrightarrow} \quad t_x \cdot t_y = r \cdot t_z, \tag{9}$$

where $t_x, t_y, t_z \in T$ are right transversals L to R.

Also we can define the operation on the set of left transversal by putting

$$t_x \overset{(T)}{\cdot} t_y = t_z \quad \overset{def}{\Leftrightarrow} \quad t_x \cdot t_y = t_z \cdot r \tag{10}$$

for $t_x, t_y, t_z \in T$ and $r \in R$. Similarly for the right transversal.

Lemma 3.3. *$\langle E, \overset{(T)}{\cdot}, 1\rangle$ is isomorphic to $\langle T, \overset{(T)}{\cdot}, t_1\rangle$.*

Proof. The proof follows easily from (8) and (10). The isomorphism has the form $\varphi : E \to T$, $\varphi(x) = t_x$. $\square$

Lemma 3.4. *$\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a left loop with the two-sided unit 1.*

Proof. Since $t_1 = e \in R$, for ever $x \in E$ we have

$$x \overset{(T)}{\cdot} 1 = u \Leftrightarrow t_x \cdot e = t_u \cdot r \Leftrightarrow t_x = t_u \cdot r_1 \Leftrightarrow t_x \in t_u \cdot R \Leftrightarrow u = x.$$

Hence $x \overset{(T)}{\cdot} 1 = x$. On the other sided

$$1 \overset{(T)}{\cdot} x = v \Leftrightarrow e \cdot t_x = t_v \cdot r \Leftrightarrow t_x = t_v \cdot r_1 \Leftrightarrow t_x \in t_v \cdot R \Leftrightarrow v = x.$$

Thus $1 \overset{(T)}{\cdot} x = x$. So, $1 \in E$ is a two-sided unit in $\langle E, \overset{(T)}{\cdot}, 1\rangle$.

Let $a \overset{(T)}{\cdot} x = b$ for some $a, b \in E$. Then $t_a \cdot t_x = t_b \cdot r$. Hence

$$t_x = t_a \backslash (t_b \cdot r) = t_c \cdot r' \quad \text{for some } c \in E \;\Leftrightarrow\; x = c.$$

So, there exists an element $c \in E$ such that $a \overset{(T)}{\cdot} c = b$. This means that the equation $a \overset{(T)}{\cdot} x = b$ has a solution. If this solution is not uniquely determined, then $a \overset{(T)}{\cdot} x_1 = b = a \overset{(T)}{\cdot} x_2$ for some $x_1, x_2 \in E$, $x_1 \neq x_2$. Then

$$\begin{cases} t_a \cdot t_{x_1} = t_b \cdot r_1, \\ t_a \cdot t_{x_2} = t_b \cdot r_2. \end{cases}$$

Hence, by Lemmas 2.6 and 2.7 we obtain

$$t_a \cdot (t_{x_1} R) = (t_a \cdot t_{x_1}) \cdot R = (t_b \cdot r_1) \cdot R = t_b R,$$
$$t_a \cdot (t_{x_2} R) = (t_a \cdot t_{x_2}) \cdot R = (t_b \cdot r_2) \cdot R = t_b R.$$

So, for every $r' \in R$ there exists $r'' \in R$ such that

$$t_a \cdot \left(t_{x_1} \cdot r'\right) = t_b \cdot r^* = t_a \cdot \left(t_{x_2} \cdot r''\right).$$

This implies $t_{x_1} \cdot r' = t_{x_2} \cdot r''$, and consequently $x_1 = x_2$, which is a contradiction. So, $\langle E, \overset{(T)}{\cdot}, 1\rangle$ is a left loop. $\square$

In the same way we can prove

Lemma 3.5. *$\langle E, \overset{(T)}{\circ}, 1\rangle$ is a right loop with the two-sided unit 1.* $\square$

If $\langle E, \overset{(T)}{\cdot}, 1\rangle$ (resp. $\langle E, \overset{(T)}{\circ}, 1\rangle$) is a loop, then the transversal T is called a *left* (*right*) *loop transversal* in L to R.

4. Representation of loops by cosets

Let $\langle R, \cdot, e\rangle$ be a subloop of the loop $\langle L, \cdot, e\rangle$ and let the left condition A be satisfied in $\langle L, \cdot, e\rangle$. Using the left transversal L to R we define the *left action* of L on E as the map $f : L \times E \to E$, $(g, x) \to y = \hat{g}(x)$ such that

$$\hat{g}(x) = y \overset{def}{\Leftrightarrow} g \cdot (t_x \cdot R) = t_y \cdot R. \tag{11}$$

Lemma 4.1. *$\hat{g}$ is a permutation on E.*

Proof. Let g be an arbitrary element of L. Then for every $y \in E$, every $r' \in R$ and some $x \in E$ we have

$$g \backslash \left(t_y \cdot r'\right) = g' \in t_x \cdot R.$$

So, $g \cdot (t_x \cdot R) = t_y \cdot R$, i.e., $\hat{g}(x) = y$. Hence $\hat{g}$ is a surjective map.

Now, if $\hat{g}(x_1) = y = \hat{g}(x_2)$ for some $x_1, x_2 \in E$, then, according to (11), we have:

$$g \cdot (t_{x_1} \cdot R) = g \cdot (t_{x_2} \cdot R).$$

Hence, for every $r_1 \in R$ there exists $r_2 \in R$ such that

$$g \cdot (t_{x_1} \cdot r_1) = g \cdot (t_{x_2} \cdot r_2).$$

Thus, $t_{x_1} \cdot r_1 = t_{x_2} \cdot r_2$, which implies $t_{x_1} \cdot R = t_{x_2} \cdot R$, and consequently $x_1 = x_2$. Therefore $\hat{g}$ is a permutation on E. $\square$

In this way we obtain a permutation representation of a loop $\langle L, \cdot, e\rangle$ by $\varphi : L \to \hat{L} \subset S_E$, where $\varphi : g \to \hat{g}$. The multiplication of permutations from $\hat{L}$ is defined by

$$\hat{g}_1 * \hat{g}_2 = \hat{g}_3 \quad \overset{def}{\Leftrightarrow} \quad g_1 \cdot g_2 = g_3 \quad \text{in a loop } \langle L, \cdot, e\rangle.$$

Since $\varphi(g_1) * \varphi(g_2) = \hat{g}_1 * \hat{g}_2 = \hat{g}_3 = \widehat{g_1 \cdot g_2} = \varphi(g_1 \cdot g_2)$, φ is a homomorphism from $\langle L, \cdot, e\rangle$ to $\left\langle \hat{L}, *, id\right\rangle$.

Lemma 4.2. *The kernel of the homomorphism φ is a subloop R^* of a loop L such that $R^* \subseteq R$ and*

$$R^* = \bigcap_{u \in L} R_u^{-1} L_u(R).$$

Proof. The kernel of this homomorphism is the set

$$R^* = \{g \in L |\, \hat{g}(x) = x \ \ \forall\, x \in E\}.$$

By Lemmas 2.6 and 2.7 for every $x \in E$ we have

$$\hat{g}(x) = x \ \Leftrightarrow \ g \cdot (t_x \cdot R) = t_x \cdot R \ \ \Leftrightarrow \ g \cdot ((t_x \cdot r) \cdot R) = (t_x \cdot r) \cdot R.$$

Thus

$$\hat{g}(x) = x \;\forall x \in E \ \Leftrightarrow \ g \cdot (u \cdot R) = u \cdot R \;\forall u \in L \ \Leftrightarrow \ (g \cdot u) \cdot R = u \cdot R \;\forall u \in L.$$

The last is equivalent to the fact that $g \in (u \cdot R)/u \;\forall u \in L$, i.e., $g \in R_u^{-1} L_u(R) \;\forall u \in L$. Hence $R^* = \bigcap\limits_{u \in L} R_u^{-1} L_u(R)$.

For $u = e$ we have $g \in R$. Thus $R^* \subseteq R$. □

Obviously, R^* is a normal subloop of L and has the form

$$R^* = \{r \in R \,|\, L_u^{-1} R_u(r) \in R \ \ \forall u \in L\}.$$

Further R^* will be denoted as $Core_L(R)$ and will be called the *core* of R in L.

Lemma 4.3. *The following statements are true:*

1) $Core_L(R)$ *is a maximal subloop among the all normal subloops of L contained in R.*
2) *Let* $L' = L/Core_{L(R)}$. *If* $T = \{t_x\}_{x \in E}$ *is a left transversal in L to R and* $\psi : L \to L'$ *is a natural homomorphism, then:*
   a) *The set* $T' = \{\psi(t_x) | x \in E\}$ *is a left transversal in* L' *to* $R' = \psi(R) = R/Core_L(R)$;
   b) $\langle E, \overset{(T')}{\cdot}, 1\rangle \equiv \langle E, \overset{(T)}{\cdot}, 1\rangle$.
3) $Core_{L'}(R') = \{e\}$.

Proof. 1) Let N be any normal subloop of L contained in R. Since N is normal, it is invariant by any middle inner permutation of the loop L, i.e., $L_u^{-1} R_u(N) = N$ for all $u \in L$. Then $R_u^{-1} L_u(N) = N$ for every $u \in L$.

Since $N \subseteq R$, for all $u \in L$ we have $N = R_u^{-1} L_u(N) \subseteq R_u^{-1} L_u(R)$, and consequently

$$N = \bigcap_{u \in L} N = \bigcap_{u \in L} R_u^{-1} L_u(N) \subseteq R_u^{-1} L_u(R) = R^*.$$

2) Let $T = \{t_x\}_{x\in E}$ be a left transversal in L to R and

$$\psi :\ L \to L' = L \backslash Core_{L(R)}$$

be a natural homomorphism. Let us denote:

$$R' = \psi(R), \quad t'_x = \psi(t_x) \quad \forall x \in E.$$

a) Let us show that $T' = \{\psi(t_x) | x \in E\}$ is a left transversal in a loop L' to its subloop R'. Firstly, because $a\cdot(b\cdot R) = (a\cdot b)\cdot R$ for all $a, b \in L$, then $\psi(a\cdot(b\cdot R)) = \psi((a\cdot b)\cdot R)$, i.e., $\psi(a)\cdot(\psi(b)\cdot\psi(R)) = (\psi(a)\cdot\psi(b))\cdot\psi(R)$. Thus $a'\cdot(b'\cdot R') = (a'\cdot b')\cdot R'$ for all $a', b' \in L'$, which shows that the left condition A is fulfilled for a loop L' and its subloop R'.

Secondly, for every $g' \in L'$ there exists $g \in L$ such that $g' = \psi(g)$. Since for any $g \in L$ we have a representation $g = t_u \cdot r$, $t_u \in T$, $r \in R$, we obtain

$$g' = \psi(g) = \psi(t_u \cdot r) = \psi(t_u) * \psi(r) = t'_u * r',$$

where $t'_u \in T'$, $r' \in R'$. This means that each $g' \in L'$ may be represented in the form $g' = t'_u \cdot r'$, where $t'_u \in T'$, $r' \in R'$.

Finally, let $t'_y = t'_x * r'_1$ for some $x, y \in E$ and $r'_1 \in R'$. Then, for $r'_1 = \psi(r_1)$ we have $\psi(t_y) = \psi(t_x) * \psi(r_1) = \psi(t_x \cdot r_1)$. From this we obtain $t_y \cdot Core_L(R) = (t_x \cdot r_1)\cdot Core_L(R)$.

Since $R^* = Core_L(R) \subseteq R$, then $t_y \cdot r_1^* = (t_x \cdot r_1)\cdot r_2^*$, where r_1^*, r_2^* are in $R^* \subseteq R$. Thus

$$t_y \cdot R = (t_y \cdot r_1^*)\cdot R = ((t_x \cdot r_1)\cdot r_2^*)\cdot R = (t_x \cdot r_1)\cdot R = t_x \cdot R.$$

So $x = y$, since T is a left transversal in L to R. Therefore T' is a left transversal in L' on R'.

b) We have

$$\begin{gathered} x \overset{(T)}{\cdot} y = z \ \Leftrightarrow\ t_x \cdot t_y = t_z \cdot r \text{ (where } t_x, t_y, t_z \in T,\ r \in R) \ \Leftrightarrow \\ \psi(t_x \cdot t_y) = \psi(t_z \cdot r) \ \Leftrightarrow\ \psi(t_x) * \psi(t_y) = \psi(t_z) * \psi(r) \ \Leftrightarrow \\ t'_x \cdot t'_y = t'_z \cdot r' \text{ (where } t'_x, t'_y, t'_z \in T',\ r' \in R') \ \Leftrightarrow\ x \overset{(T')}{\cdot} y = z. \end{gathered}$$

Thus $x \overset{(T)}{\cdot} y = z = x \overset{(T')}{\cdot} y$. So, $\langle E, \overset{(T)}{\circ}, 1\rangle$ and $\langle E, \overset{(T')}{\circ}, 1\rangle$ are isomorphic.

3) Let $Core_{L'}(R') = M_0 \neq \{e\}$. Since M_0 is a normal subloop of L', the preimage

$$M_1 = \psi^{-1}(M_0) = \{g \in L \,|\, \psi(g) \in M_0\}$$

is a subloop in L. Further,

$$\begin{array}{rcl} e & \in & M_0 \quad \Rightarrow \quad Core_L(R) = Ker\,\psi = \psi^{-1}(e) \subset \psi^{-1}(M_0) = M_1, \\ M_0 & \subseteq & R' \quad \Rightarrow \quad M_1 = \psi^{-1}(M_0) \subseteq \psi^{-1}(R') = R. \end{array}$$

Since a homomorphism ψ transforms any inner permutation from L to an inner permutation from L', then M_1 should be a normal subloop in L. So, $M_1 \subset R$ and $Core_L(R) \subset M_1$. This contradicts to the previous condition of this Lemma. □

Remark 4.4. According to the above lemma, the study of left transversals in loops may be reduced to the case, when $Core_L(H) = \{e\}$. In this case $\langle E, *, id\rangle \equiv \hat{L} \cong L = \langle E, \cdot, e\rangle$.

In the case when $\langle R, \cdot, e\rangle$ is as subloop of $\langle L, \cdot, e\rangle$ and the right condition A is satisfied we obtain analogical results. Namely, if $T = \{t_x\}_{x\in E}$ is a right transversal in L to R, then $f : L \times E \to E$, $f : (g, x) \to y = \breve{g}\,(x)$ defined by

$$\breve{g}\,(x) = y \overset{def}{\Leftrightarrow} (R \cdot t_x) \cdot g = R \cdot t_y.$$

is a right action of L on E. Consequently, the following lemmas are true.

Lemma 4.5. *$\breve{g}$ is a permutation on E.* □

So, $\varphi' : L \to \breve{L} \subset S_E$, $\varphi' :\ g \to \breve{g}$ is another permutation representation of a loop L.

Lemma 4.6. *The kernel $R^{\circledast}$ of the homomorphism φ' is a subloop L such that $R^{\circledast} \subseteq R$ and $R^{\circledast} = \bigcap\limits_{u\in L} L_u^{-1}R_u(R)$.* □

Lemma 4.7. *The following statements are true:*

1) *$R^{\circledast}$ is a maximal subloop among the all normal subloops of the loop L contained in R.*
2) *Let $L'' = L/R^{\circledast}$. If $T = \{t_x\}_{x\in E}$ is a right transversal in L to R and $\psi : L \to L''$ is a natural homomorphism, then:*
   a) $T'' = \{\psi(t_x) | x \in E\}$ is a right transversal in L'' to $R'' = \psi(R) = R/R^{\circledast}$;
   b) $\langle E, \overset{(T'')}{\cdot}, 1\rangle \equiv \langle E, \overset{(T)}{\cdot}, 1\rangle$.
3) $\bigcap\limits_{u\in L''} L_u^{-1}R_u(R'') = \{e\}$. □

Remark 4.8. According to the last Lemma a research of right transversals in loops may be reduced to a case when $\bigcap\limits_{u\in L''} L_u^{-1}R_u(R'') = \{e\}$. In this case

$$\langle \breve{L}, *, id\rangle \equiv \hat{L} \cong L = \langle L, \cdot, e\rangle \,.$$

Lemma 4.9. *If $T = \{t_x\}_{x\in E}$ is a two-sided transversal in a loop L to its subloop R and two-sided conditions A is satisfied, then*

$$R^{\circledast} = \bigcap_{u\in L} L_u^{-1}R_u(R) = R^* = \bigcap_{u\in L} R_u^{-1}L_u(R) = Core_L(R).$$

Proof. It is a consequence of Lemmas 4.3 and 4.7. □

Definition 4.10. [3] A loop $\langle L, \cdot, e\rangle$ is called a *permutation loop* on a set E, if there exists a map $f : L\times E \to E$, $f\,(g, x) = \hat{g}\,(x)$ satisfying the following conditions:

(1) $\hat{e}\,(x) = x$ for all $x \in E$, where e is a unit of the loop L,

(2) if $b \in N\,(\langle L, \cdot, e\rangle)$, where N is a kernel of L, then

$$(\widehat{a\cdot b})\,(x) = \hat{a}(\hat{b}(x))$$

for every $a \in L$ and $x \in E$,

(3) there exists an element $x_0 \in E$ such that

$$R_{x_0} \stackrel{def}{=} \{g \in L |\, \hat{g}\,(x_0) = x_0\}$$

is a subloop of L and the following conditions are fulfilled:

(a) $(\widehat{b\cdot a})(x_0) = \hat{b}(\hat{a}(x_0))$ for $b \in R_{x_0}$ and $a \in L$,

(b) $(\widehat{g_2\cdot g_1})(x_0) \neq \hat{g}_2(x_0)$ for $g_1, g_2 \in L$ and $\hat{g}_1(x_0) \neq x_0$,

(c) $(\widehat{g_2\cdot g_1})(x_0) \neq \hat{g}_1(x_0)$ for $g_2 \notin R_{\hat{g}_1(x_0)}$.

Let us show that a permutational representation $\hat{L}$ defined by (11) satisfies all conditions of Definition 4.10.

Lemma 4.11. *Let the left condition A for a loop $\langle L, \cdot, e\rangle$ to its subloop $\langle R, \cdot, e\rangle$ be satisfied. If a permutation representation $\left\langle \hat{L}, \cdot, \hat{e}\right\rangle$ of the loop L is defined by* (11)*, then $\left\langle \hat{L}, \cdot, \hat{e}\right\rangle$ is a loop of permutations in the sense of Definition* 4.10.

Proof. If a representation is defined by (11), then

$$\hat{e}\,(x) = u \;\Leftrightarrow\; e \cdot (t_x \cdot R) = t_u \cdot R \;\Leftrightarrow\; t_x \cdot R = t_u \cdot R \;\Leftrightarrow\; u = x,$$

which shows that in this case $\hat{e}\,(x) = x$ for all $x \in E$. This verifies the first condition of Definition 4.10.

Now, if $b \in N\,(\langle L, \cdot, e\rangle)$, then for $u, v \in L$ we have $(b \cdot u) \cdot v = b \cdot (u \cdot v)$. Thus $(u \cdot v) \cdot b = u \cdot (v \cdot b)$, and consequently $(u \cdot b) \cdot v = u \cdot (b \cdot v)$. This means that for every $a \in L$ and every $x \in E$ we have $\widehat{(a \cdot b)}\,(x) = y$. Therefore $(a \cdot b) \cdot (t_x \cdot R) = t_y \cdot R$, which means that $(a \cdot b) \cdot t_x = t_y \cdot r'$ for some $r' \in R$. But $a \cdot (b \cdot t_x) = t_y \cdot r'$, $\;b \cdot t_x = t_z \cdot r''$ and $a \cdot (t_z \cdot r'') = t_y \cdot r'$ imply $\hat{b}(x) = z$ and $\hat{a}(z) = y$. Hence $\hat{a}(\hat{b}(x)) = y$. Consequently $\widehat{(a \cdot b)}\,(x) = \hat{a}(\hat{b}(x))$. This verifies the second condition of Definition 4.10.

Now we prove that the third condition of Definition 4.10 is satisfied for $x_0 = 1$. First we prove that for all g_1, $g_2 \in L$ we have

$$(\widehat{g_1 \cdot g_2})(1) = \hat{g}_1(\hat{g}_2(1)). \tag{12}$$

Indeed, by Lemma 2.7, $(\widehat{g_1 \cdot g_2})(1) = u$, i.e., $(g_1 \cdot g_2)(e \cdot R) = t_u \cdot R$. Thus $(g_1 \cdot g_2) \cdot R = t_u \cdot R$. But $g_1 \cdot (g_2 \cdot R) = t_u \cdot R$, $\;g_2 \cdot R = t_z \cdot R$ and $g_1 \cdot (t_z \cdot R) = t_u \cdot R$ imply $\hat{g}_2(1) = z$ and $\hat{g}_1(z) = u$. Hence $\hat{g}_1(\hat{g}_2(1)) = u$. This completes the proof of (12). From (12) the condition (a) follows automatically.

Further, let g_1, $g_2 \in L$ and $\hat{g}_1(1) = u_0 \neq 1$. Then by (12) we have

$$(\widehat{g_2 \cdot g_1})(1) = \hat{g}_2 \cdot (\hat{g}_1(1)) = \hat{g}_2(u_0) \neq \hat{g}_2(1),$$

since $\hat{g}_2$ is a permutation. This proves (b).

Finally, let

$$g_2 \notin R_{\hat{g}_1(1)} = \{g \in L |\, \hat{g}(\hat{g}_1(1)) = \hat{g}_1(1)\}\,.$$

Then, by (12), we obtain $(\widehat{g_2 \cdot g_1})(1) = \hat{g}_2 \cdot (\hat{g}_1(1)) \neq \hat{g}_1(1)$, since $g_2 \notin R_{\hat{g}_1(1)}$. This proves (c). □

Lemma 4.12. *For an arbitrary left transversal $T = \{t_x\}_{x \in E}$ in a loop $L = \langle L, \cdot, e\rangle$ to its subloop $R = \langle R, \cdot, e\rangle$ the following statements are true:*

1) $\hat{r}(1) = 1$ *for all* $r \in R$,

2) $\hat{t}_x(y) = x \overset{(T)}{\cdot} y$, $\quad \hat{t}_x^{-1}(y) = x \backslash y$ *for all* $x, y \in E$,
where $\hat{t}_x^{-1}$ *is an inverse permutation to a permutation* $\hat{t}_x$ *in* S_E*, and* "$\backslash$" *is a left division in a left loop* $\langle E, \overset{(T)}{\cdot}, 1\rangle$*. Moreover,*

$$\hat{t}_x(1) = x, \quad \hat{t}_1(x) = x, \quad \hat{t}_x^{-1}(1) = x \backslash 1, \quad \hat{t}_x^{-1}(x) = 1.$$

Proof. 1) Let $\hat{r}(1) = u$. Then $r \cdot (e \cdot R) = t_u \cdot R$, i.e., $R = t_u \cdot R$. Thus $t_u = e = t_1$. Consequently, $u = 1$. This proves $\hat{r}(1) = 1$.

2) Let $\hat{t}_x(y) = u$. Then $t_x \cdot (t_y \cdot R) = t_u \cdot R$, and consequently

$$t_u \cdot R = (t_x \cdot t_y) \cdot R = (t_{x \cdot y} \cdot r') \cdot R = t_{x \cdot y} \cdot R.$$

Thus $u = x \cdot y$ and $\hat{t}_x(y) = x \cdot y$.

Further,

$$\hat{t}_x^{-1}(y) = z \;\Leftrightarrow\; y = \hat{t}_x(z) = x \cdot z \;\Leftrightarrow\; z = x \backslash y,$$

so, $\hat{t}_x^{-1}(y) = x \backslash y$. The rest follows from just proved identities. □

Lemma 4.13. *The following conditions are equivalent:*

1) $T = \{t_x\}_{x \in E}$ *is a left loop transversal in a loop* L *to its subloop* R*;*
2) $\hat{T} = \{\hat{t}_x\}_{x \in E}$ *is a sharply transitive set of permutations in* S_E*.*

Proof. The proof is based on the following sequence of the equivalent statements:

- $T = \{t_x\}_{x \in E}$ is a left loop transversal in a loop L to its subloop R,
- $\langle E, \overset{(T)}{\cdot}, 1 \rangle$ is a loop with the unit 1,
- $x \overset{(T)}{\cdot} a = b$ has a unique solution in E for every $a, b \in E$,
- $\hat{t}_x(a) = b$ has a unique solution in E for every $a, b \in E$,
- $\hat{T} = \{\hat{t}_x\}_{x \in E}$ is a sharply transitive set of permutations in S_E. □

The proof of the following two lemmas about is analogous to the proof of Lemmas 4.12 and 4.13.

Lemma 4.14. *For an arbitrary right transversal* $T = \{t_x\}_{x \in E}$ *in a loop* $L = \langle L, \cdot, e \rangle$ *to its subloop* $R = \langle R, \cdot, e \rangle$ *the following statements are true:*

1) $\check{r}(1) = 1$ *for all* $r \in R$*,*
2) $\check{t}_x(y) = y \overset{(T)}{\circ} x, \quad \check{t}_x^{-1}(y) = x/y$ *for all* $x, y \in E$*,*
where $\check{t}_x^{-1}$ *is an inverse permutation to a permutation* $\check{t}_x$ *in* S_E*, and* *"/" is a right division in a right loop* $\langle E, \overset{(T)}{\circ}, 1 \rangle$*. Moreover,*

$$\check{t}_x(1) = x, \quad \check{t}_1(x) = x, \quad \check{t}_x^{-1}(1) = x/1, \quad \check{t}_x^{-1}(x) = 1.$$

Lemma 4.15. *The following conditions are equivalent:*

1) $T = \{t_x\}_{x \in E}$ *is a right loop transversal in a loop* L *to its subloop* R*;*
2) $\check{T} = \{\check{t}_x\}_{x \in E}$ *is a sharply transitive set of permutations in* S_E*.*

References

[1] **P. Baer**, **Nets and groups**. Trans. Amer. Math. Soc. **46** (1939), 110 – 141.

[2] **V. D. Belousov**, *Foundations of quasigroup and loop theory*, (Russian), Moscow, "Nauka", 1967.

[3] **F. Bonetti, G. Lunardon and K. Strambach**, *Cappi di permutazioni.* Rend. Math., **12**(1979), No. 3-4, 383 – 395.

[4] **T. Foguel and L. C. Kappe**, *On loops covered by subloops*, Expositiones Math. **23** (2005), 255 – 270.

[5] **K. W. Johnson**, *S-rings over loops, right mapping groups and transversals in permutation groups*, Math. Proc. Camb. Phil. Soc. **89** (1981), 433 – 443.

[6] **E. A. Kuznetsov**, *Transversals in groups.* 1. *Elementary properties*, Quasigroups and Related Systems **1** (1994), 22 – 42.

[7] **E. A. Kuznetsov**, *About some algebraic systems related with projective planes*, Quasigroups and Related Systems **2** (1995), 6 – 33.

[8] **E. A. Kuznetsov**, *Transversals in groups. Semidirect product of a transversal operation and subgroup*, Quasigroups and Related Systems **8** (2001), 37 – 44.

[9] **E. A. Kuznetsov**, *Transversals in loops*, Abstracts of International Conference "Loops-03", Prague, August 10-17, 2003, 18 – 20.

[10] **M. Niemenmaa and T. Kepka**, *On multiplication groups of loops*, J. Algebra **135** (1990), 112 – 122.

[11] **H. Pflugfelder**, *Quasigroups and loops: Introduction.* Sigma Series in Pure Math., 7, Helderman Verlag, New York, 1972.

[12] **L. V. Sabinin and O. T. Mikheev**, *Quasigroups and differential geometry*, in "Quasigroups and loops: theory and applications, Helderman-Verlag, Berlin 1990, 357 – 430.

Received May 13, 2010

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str.
Chishinau, MD-2028
Moldova
E-mail: kuznet1964@mail.ru

Quasigroups and Related Systems **18** (2010), 59 – 82

Polynomial functions on the units of $\mathbb{Z}_{2^n}$

Smile Markovski, Zoran Šunić and Danilo Gligoroski

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. Polynomial functions on the group of units Q_n of the ring $\mathbb{Z}_{2^n}$ are considered. A finite set of reduced polynomials $\mathcal{RP}_n$ in $\mathbb{Z}[x]$ that induces the polynomial functions on Q_n is determined. Each polynomial function on Q_n is induced by a unique reduced polynomial - the reduction being made using a suitable ideal in $\mathbb{Z}[x]$. The set of reduced polynomials forms a multiplicative 2-group. The obtained results are used to efficiently construct families of exponential cardinality of, so called, huge k-ary quasigroups, which are useful in the design of various types of cryptographic primitives. Along the way we provide a new (and simpler) proof of a result of Rivest characterizing the permutational polynomials on $\mathbb{Z}_{2^n}$.

1. Introduction

The need for new kinds of computational methods and devices is growing as a result of the possibility of their application in the new developing fields in mathematics and computer science, in particular cryptography and coding theory. Finite fields and integer quotient rings are traditionally used for such computational needs. The integer quotient rings are somewhat disadvantaged due to the fact that their nonzero multiplicative structure does not form a group (except when they happen to be fields). The structure of the ring of polynomials over rings, and especially over integer quotient rings, has been under investigation for almost a century. Let us mention here chronologically some of the authors: Kempner (1921) [9], Nöbauer (1965) [13], Keller and Olson (1968) [7], Mullen and Stevens (1984) [12],

2000 Mathematics Subject Classification: 13F20, 20N05, 20D99
Keywords: group, ring, polynomial, polynomial function, quasigroup.
The visit of the first and the third author to the "Special semester on Gröbner bases – Gröbner Bases in Cryptography, Coding Theory, and Algebraic Combinatorics", April 30 - May 06, 2006 in Linz, Austria, organized by RISC and RICAM, was very helpful and stimulated some of the ideas that are presented in this paper.
The second author was partially supported by NSF grant DMS-0805932.

Rivest (2001) [15], Bandini (2002) [1], Zhang (2004) [18]. We emphasize that the paper of Rivest [15] is closest to our work and his results can be inferred from ours (see Section 5).

We consider its group of units Q_n in $\mathbb{Z}_{2^n}$ and define a finite set $\mathcal{RP}_n$ of reduced polynomials over $\mathbb{Z}$ that induce the set $\mathcal{PF}_n$ of all polynomial functions that keep Q_n invariant. The set $\mathcal{RP}_n$ is a finite 2-group under polynomial multiplication modulo functional equivalence. Exactly half of the reduced polynomials induce permutations on Q_n.

The reduced polynomials are obtained by using an ideal I_n in $\mathbb{Z}[x]$ such that every polynomial in I_n induces the 0 constant function on Q_n and two polynomials are functionally equivalent over Q_n if and only if they are equivalent with respect to the ideal I_n.

By using our reduction algorithms we are able to give efficient answers to several problems. We show that there are efficient algorithms (polynomial complexity with respect to the input parameters) for the following problems:

(i) given a polynomial inducing a polynomial function on Q_n, determine the reduced polynomial inducing the same polynomial function,

(ii) given a polynomial inducing a permutation on Q_n, determine the reduced polynomial inducing the inverse permutation.

(iii) given a polynomial inducing a polynomial function on Q_n, determine the reduced polynomial for the multiplicative inverse.

In the last part of the paper we use the obtained results to construct families of quasigroups of large cardinality. We define the concept of huge quasigroups as quasigroups of large order that can be handled effectively, in the sense that the multiplication in the quasigroup, as well as in its adjoint operations, can be effectively realized (polynomial complexity with respect of $\log n$, where n is the order of the quasigroup). The need for permutations and quasigroups of large (huge) orders such as 2^{16}, 2^{32}, 2^{64}, 2^{128}, that can be easily handled is associated with the development of the modern massively produced 32-bit and 64-bit processors. Strong links between modern cryptography and quasigroups (equivalently, Latin squares) have been observed by Shannon [17] more than 50 years ago. Subsequently, the cryptographic potential of quasigroups in the design of different types of cryptographic primitives has been addressed in numerous works. Authentication schemas have been proposed by Dènes and Keedwell (1992) [5], secret sharing schemes by Cooper, Donovan and Seberry (1994) [4], a version of popular DES block cipher by using Latin squares by Carter, Dawson, and Nielsen (1995) [3], different proposals for use in the design of cryptographic hash functions by several authors [16], a hardware stream cipher by Gligoroski, Markovski, Kocarev and Gusev (2005) [6]. One application of the quasigroups as defined here can be found in the paper [11], where a new public key cryptsystem is defined.

We want to emphasize that the results in this work concerning effective constructions of large quasigroups, besides in cryptography, can also be of interest in other areas (such as coding theory, design theory, ...).

1.1. Organization of the content

Well known background on the structure of the group Q_n and on Hensel lifting (useful to extract inverses in Q_n) is presented in Section 2. Full description of the polynomials in $\mathbb{Z}[x]$ that induce transformations on Q_n (and the finite set of reduced polynmials that represent them) is provided in Section 3, while the polynomials in $\mathbb{Z}[x]$ that induce permutations on Q_n are characterized in Section 4. Section 5 is a brief interlude in which we use our results to present a new proof or a result of Rivest [15] providing a characterization of polynomials in $\mathbb{Z}[x]$ that induce permutations on $\mathbb{Z}_{2^n}$. The group of reduced polynomials under multiplication is briefly considered in Section 6. Section 7 provides polynomial algorithms that handle construction of reduced polynomials related to interpolation, functional inversion, and multiplicative inversion. Finally, applications to effective constructions of large k-ary quasigroups are provided in Section 8.

2. The group $(Q_n, \cdot)$

The integer quotient ring $(\mathbb{Z}_k, +, \cdot)$, where k is a positive integer, is a well known mathematical structure, where the addition and multiplication are interpreted modulo k. This ring is associative and commutative ring with a unit element 1. Here we are concerned solely with the case $k = 2^n$. The set $Q_n = \{1, 3, \ldots, 2^n - 1\}$ is a subgroup of the multiplicative semigroup $(\mathbb{Z}_{2^n}, \cdot)$. Indeed, Q_n is precisely the group of units of $\mathbb{Z}_{2^n}$. Note that if $n = 1$, then Q_n is trivial, and if $n = 2$, $Q_2 = \mathbb{Z}_2 = \langle -1 \rangle$. The structure of the abelian group Q_n, for $n \geqslant 3$, is given by the following result.

Proposition 1. *Let $n \geqslant 3$. Then $(Q_n, \cdot) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. Moreover, Q_n is generated by -1 and 5, the order of -1 is 2, and the order of 5 is 2^{n-2}.*

Proof. The subset $F_n \subseteq Q_n$ of numbers of the form $4k+1$ forms a subgroup of index 2 in Q_n. Since $5 \in F_n$, we have $5^{2^{n-2}} = 1$ in Q_n. On the other hand,

$$5^{2^{n-3}} = (4+1)^{2^{n-3}} = \sum_{i=0}^{2^{n-3}} \binom{2^{n-3}}{i} 2^{2i}.$$

The highest power of 2 dividing $i!$ is $\lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \cdots < i/2 + i/4 + \cdots = i$. Thus each of the terms $\binom{2^{n-3}}{i} 2^{2i}$ is divisible by $2^{n-3+2i-(i-1)} = 2^{n-2+i}$ and we have

$$5^{2^{n-3}} \equiv 1 + 2^{n-3} \cdot 2^2 \equiv 2^{n-1} + 1 \pmod{2^n}. \tag{1}$$

Therefore $5^{2^{n-3}} \neq 1$ in Q_n, the order of 5 is 2^{n-2}, and F_n is a cyclic group generated by 5.

The order of -1 is clearly 2. Since -1 is not in F_n (it has the form $4k+3$) we have that $Q_n = \langle -1 \rangle \times \langle 5 \rangle = \mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$. □

Corollary 1. *Let $n \geqslant 3$. The multiplicative order of every $a \in Q_n$ divides 2^{n-2}.* □

Given a large value of n and $a \in Q_n$, can we effectively find the inverse a^{-1}? Note that if we express a as $a = (-1)^i \cdot 5^j$, for some $i \in \{0,1\}$, $j \in \{0, 1, \ldots, 2^{n-2}-1\}$, then its inverse in Q_n is given by

$$a^{-1} = (-1)^i \cdot 5^{2^{n-2}-j}.$$

However, this requires representing a in the form $a = (-1)^i \cdot 5^j$, for some $i \in \{0,1\}$. It is fairly easy to decide if $i = 0$ or $i = 1$. Indeed, $i = 0$ when a is of the form $4k+1$ and $i = 1$ otherwise. However, to determine j we need to solve a discrete logarithm problem of the type $5^x = a \pmod{2^n}$. This apparent difficulty can be sidestepped by calculating the inverse by applying Hensel lifting [14] (also known as Newton-Hensel lifting [8]).

The basic idea is to use binary representation of the integers modulo 2^n. Given $r \in \mathbb{Z}_{2^n}$, its binary representation is $r_{n-1}r_{n-2}\ldots r_1r_0$, where $r_j \in \{0,1\}$ is the $(j+1)-$th bit of r. In the same way, the binary representation of a variable x is given by $x_{n-1}x_{n-2}\ldots x_1x_0$, where x_j are bit variables. Now, let r be a root of the polynomial $P(x)$. Then $P(x) = (x-r)S(x)$ for some polynomial $S(x)$. The equality $P(x) = (x-r)S(x)$ in the ring $\mathbb{Z}_{2^k}$, where $k < n$, is given by

$$P(x_{k-1}\ldots x_1x_0) = (x_{k-1}\ldots x_1x_0 - r_{k-1}\ldots r_1r_0)S(x_{k-1}\ldots x_1x_0).$$

The last equality shows that if we want to find the k least significant bits of a root r of $P(x)$, we need to consider the equation $P(x) = 0$ in the ring $\mathbb{Z}_{2^k}$.

One variant of the Hensel lifting algorithm for finding a root of $P(x)$ is the following:

STEP 1: *Determine a bit* r_0 *such that* $P(r_0) = 0$ *in* $\mathbb{Z}_2$.

This can be accomplished simply by checking if $P(0) = 0$ or $P(1) = 0$ (or both!) in $\mathbb{Z}_2$.

Let the bits $r_0, \ldots, r_{k-1}$ be already chosen in STEP 1 – STEP k.

STEP $k+1$: *Determine a bit* r_k *such that* $P(r_k r_{k-1} \ldots r_0) = 0$ *in* $\mathbb{Z}_{2^{k+1}}$.

Since the bits $r_0, \ldots, r_{k-1}$ are known, this can be accomplished by checking if $P(0r_{k-1} \ldots r_0) = 0$ or $P(1r_{k-1} \ldots r_0) = 0$ (or both) in $\mathbb{Z}_{2^{k+1}}$.

The algorithm stops after STEP n.

In order to find all roots of a polynomial one has to follow all the branching points of the algorithm (whenever both 0 and 1 are good choices one has to follow both choices, and whenever neither 0 nor 1 are good choices one discards that particular branch of the search).

Given $a \in Q$, the root of the polynomial $ax - 1$ is the inverse of a. In this case, the above algorithm has polynomial complexity in n, since there is only one root and the above algorithm will produce the unique correct bit of a^{-1} at each step (there is no branching).

3. Polynomial functions on Q_n

Every polynomial $P(x)$ from the polynomial ring $\mathbb{Z}[x]$ induces a polynomial function $p : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ by the evaluation map (taken modulo 2^n). We are interested here in polynomial functions on Q_n, i.e., polynomial functions $p : Q_n \to Q_n$ induced by polynomials $P(x)$ in $\mathbb{Z}[x]$ such that $p(Q_n) \subseteq Q_n$. Denote by $\mathcal{P}_n$ the set of polynomials in $\mathbb{Z}[x]$ that induce polynomial function on Q_n and denote by $\mathcal{PF}_n$ the set of corresponding polynomial functions on Q_n. We implicitly assume that $n \geqslant 2$ (as was already mentioned, Q_1 is trivial).

We first determine precisely the polynomials over $\mathbb{Z}$ that induce polynomial functions on Q_n, i.e., we determine $\mathcal{P}_n$.

Proposition 2. *Let* $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ *be a polynomial in* $\mathbb{Z}[x]$. *Then* $P(x)$ *is in* $\mathcal{P}_n$ *(i.e.,* $P(x)$ *induces a polynomial function on* Q_n*) if and only if the sum of the coefficients* $a_0 + a_1 + \cdots + a_d$ *is odd, which, in turn, is equivalent to the condition that* $p(1)$ *is odd.*

Proof. For every odd number a, all the powers a^i, $i = 0, \ldots, d$ are also odd. Thus the parity of $p(a) = a_0 + a_1 a + \cdots + a_d a^d$ is equal to the parity of $a_0 + \cdots + a_d$. □

The finite set $\mathcal{PF}_n$ of polynomial functions on Q_n is induced by the infinite set of polynomials in $\mathcal{P}_n$. We will determine a finite set of polynomials, that induce all polynomial functions in $\mathcal{PF}_n$. In order to define this set, we need some preliminary definitions.

For an integer i, define $t_i = \lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \lfloor i/8 \rfloor + \ldots$, i.e., t_i is the largest integer ℓ such that 2^ℓ divides $i!$. Let d_n be the largest integer i such that $n - i - t_i$ is positive.

Definition 1. A polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ in $\mathcal{P}_n$ is called *reduced* if

(i) the degree of $P(x)$ is no higher than d_n,

(ii) $0 \leqslant a_i \leqslant 2^{n-i-t_i} - 1$, for $i = 0, \ldots, d_n$.

Denote the set of reduced polynomials in $\mathcal{P}_n$ by $\mathcal{RP}_n$.

Proposition 3. *The number of reduced polynomials in $\mathcal{RP}_n$ is*

$$|\mathcal{RP}_n| = 2^{(2n-d_n)(d_n+1)/2-1-\sum_{i=0}^{d_n} t_i}.$$

Proof. The number of polynomial of degree at most d_n with restrictions on the coefficients given by (ii) is

$$2^{\sum_{i=0}^{d_n} n-i-t_i} = 2^{n(d_n+1)-d_n(d_n+1)/2-\sum_{i=0}^{d_n} t_i}.$$

Exactly half of such polynomials also satisfies the condition required by Proposition 2 on the parity of the sum of the coefficients. Indeed, we can match up any polynomial $P(x) = a_0 + a_1 x + \cdots + a_d x^d$ in that satisfies the conditions (i) and (ii) with the polynomial $P(x) + 1$ if a_0 is even and with $P(x) - 1$ if a_0 is odd. In both cases, the obtained polynomial also satisfies the conditions (i) and (ii). In such a matching exactly one polynomial in each pair has odd sum of coefficients. □

Two polynomials $P(x)$ and $T(x)$ in $\mathcal{P}_n$ are said to be *functionally equivalent* over Q_n if they induce the same polynomial function on Q_n. In that case we write $P(x) \approx T(x)$. Clearly, $\approx$ is an equivalence relation on $\mathcal{P}_n$.

The polynomials $P(x)$ and $T(x)$ are functionally equivalent over Q_n if and only if the difference $P(x) - T(x)$ induces the constant 0 function on Q_n. With this in mind, we define now a finite set of polynomials over $\mathbb{Z}$ that induce the 0 constant function on Q_n.

Definition 2. For $i = 0, \ldots, d_n$, define the polynomial

$$P_{n,i}(x) = 2^{n-i-t_i}(x+1)(x+3)\ldots(x+2i-1)$$

of degree i. When $i = 0$ the understanding is that $P_{n,0} = 2^n$. Define also the polynomial

$$P_{n,d_n+1}(x) = (x+1)(x+3)\ldots(x+2d_n+1)$$

of degree $d_n + 1$.

Denote the ideal generated by $P_{n,i}(x)$, $i = 0, \ldots, d_n + 1$, in $\mathbb{Z}[x]$ by I_n. Thus

$$I_n = \left\{ \sum_{i=0}^{d_n+1} S_i(x)P_{n,i}(x) \mid S_i(x) \in \mathbb{Z}[x],\ i = 0, \ldots, d_n + 1 \right\}.$$

Proposition 4. *Every polynomial in I_n induces the 0 constant function on Q_n.*

Proof. What we need to prove is that, for every $x \in Q_n$

$$p_{n,i}(x) \equiv 0 \pmod{2^n}.$$

This is clear since, for any $x \in Q_n$ the product $(x+1)(x+3)\ldots(x+2i-1)$ is a product of i consecutive even numbers and it is therefore divisible by $2^i i!$, implying that it is divisible by 2^{i+t_i}. For $i = 0, \ldots, d_n$ we then have that $p_{n,i}(x)$ is divisible by $2^{n-i-t_i} \cdot 2^{i+t_i} = 2^n$. For $i = d_n + 1$, we have that $n \leqslant i + t_i$, and therefore 2^n divides $p_{n,i}(x)$ in this case as well. □

We state now the two main results of this section.

Theorem 1. *Two polynomials $P(x)$ and $T(x)$ in $\mathcal{P}_n$ are functionally equivalent over Q_n if and only if $P(x) - T(x)$ is a member of I_n.*

Theorem 2. *Every polynomial function in $\mathcal{PF}_n$ is induced by a unique reduced polynomial in $\mathcal{RP}_n$.*

We will prove the Theorem 1 and Theorem 2 through a series of lemmas and propositions. Along the way we provide some additional information (for instance Proposition 6 establishes a linear upper bound on the degree of a reduced polynomial). While some other approaches are certainly possible, we chose to follow a simple constructive route, since we are interested in algorithmic/complexity issues (see Section 7).

Proof of Theorem 1, *sufficiency.* If $P(x) - T(x)$ is in I_n then, by Proposition 4, $P(x) - T(x)$ induces the constant 0 function on Q_n, implying that $P(x)$ and $Q(x)$ are functionally equivalent over Q_n. □

Proposition 5. *Every polynomial function in $\mathcal{PF}_n$ is induced by a reduced polynomial in $\mathcal{RP}_n$. Moreover, for every polynomial $P(x)$ in $\mathbb{Z}[x]$ there exists a polynomial $S_P(x)$ in I_n such that $P(x) - S_P(x)$ is reduced and functionally equivalent to $P(x)$ over Q_n.*

Proof. Let $p(x)$ be a polynomial function in $\mathcal{PF}_n$ induced by the polynomial $P(x)$.

If the degree d of $P(x)$ is higher than d_n we may replace $P(x)$ by $P(x) - a_d x^{d-d_n-1} P_{n,d_n+1}$, where a_d is the coefficient of x^d in $P(x)$. The polynomial $P(x) - a_d x^{d-d_n-1} P_{n,d_n+1}$ has degree smaller than d and is functionally equivalent to $P(x)$. We may continue this until we obtain a polynomial that is functionally equivalent to $P(x)$ and has degree no higher than d_n.

We assume now that $P(x)$ has degree no higher than d_n. If $P(x)$ is reduced we are done. Otherwise, let i be the highest degree of a coefficient a_i of x^i that does not satisfy the requirement $0 \leqslant a_i \leqslant 2^{n-i-t_i} - 1$. If q is the quotient obtained by dividing a_i by 2^{n-i-t_i} then $P(x) \approx P(x) - qP_{n,i}$, and the coefficient at degree i in $P(x) - qP_{n,i}$ is in the correct range $0, \ldots, 2^{n-i-t_i} - 1$.

We repeat this procedure with the next highest degree that has a coefficient out of range until we reach a reduced polynomial that is functionally equivalent to $P(x)$. □

Example 1. Let $n = 5$. We have $0 + t_0 = 0$, $1 + t_1 = 1$, $2 + t_2 = 3$, $3 + t_3 = 4$ and $4 + t_4 = 7$. Therefore $d_5 = 3$, and every reduced polynomial has the form

$$R(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3,$$

where $0 \leqslant a_0 \leqslant 31$, $0 \leqslant a_1 \leqslant 15$, $0 \leqslant a_2 \leqslant 3$ and $0 \leqslant a_3 \leqslant 1$. The polynomials $P_{5,i}(x)$, $i = 0, 1, 2, 3, 4$ are given by

$$P_{5,0}(x) = 2^5 = 32,$$
$$P_{5,1}(x) = 2^4(x+1) = 16 + 16x,$$
$$P_{5,2}(x) = 2^2(x+1)(x+3) = 12 + 16x + 4x^2,$$
$$P_{5,3}(x) = 2(x+1)(x+3)(x+5) = 30 + 14x + 18x^2 + 2x^3,$$
$$P_{5,4}(x) = (x+1)(x+3)(x+5)(x+7) = 9 + 16x + 22x^2 + 16x^3 + x^4.$$

Then, for the polynomial $P(x) = 3x^5 + 1$, we have

$$\begin{aligned} P(x) &= 1 + 3x^5 \approx (1 + 3x^5) - 3xP_{5,4}(x) \approx 1 + 5x + 16x^2 + 30x^3 + 16x^4 \\ &\approx (1 + 5x + 16x^2 + 30x^3 + 16x^4) - 16P_{5,4}(x) \\ &\approx 17 + 5x + 16x^2 + 30x^3 \approx (17 + 5x + 16x^2 + 30x^3) - 15P_{5,3}(x) \\ &\approx 15 + 19x + 2x^2 \approx (15 + 19x + 2x^2) - P_{5,1}(x) \\ &\approx 31 + 3x + 2x^2. \end{aligned}$$

The calculations are done modulo 32 all the time. This is equivalent to using $P_{5,0} = 32$ to make reductions. □

Proposition 6. *Every polynomial function in $\mathcal{PF}_n$ is induced by a polynomial of degree smaller than $(n + 1 + \lfloor \log_2 n \rfloor)/2$.*

Proof. We need to prove that $d_n < (n + 1 + \lfloor \log_2 n \rfloor)/2$.

First note that $i - 1 - \lfloor \log_2 i \rfloor \leqslant t_i$. Indeed $t_i = \lfloor i/2 \rfloor + \lfloor i/4 \rfloor + \dots$. Only the first $\lfloor \log_2 i \rfloor$ terms of the series are possibly positive. Thus $t_i = \sum_{k=1}^{\lfloor \log_2 i \rfloor} \lfloor i/2^k \rfloor > \sum_{k=1}^{\lfloor \log_2 i \rfloor} (i/2^k - 1) = i\left(1 - \frac{1}{2^{\lfloor \log_2 i \rfloor}}\right) - \lfloor \log_2 i \rfloor > i\left(1 - \frac{1}{2^{\log_2 i - 1}}\right) - \lfloor \log_2 i \rfloor = i - 2 - \lfloor \log_2 i \rfloor$.

Assume that $n \geqslant i \geqslant \frac{n+1+\lfloor \log_2 n \rfloor}{2}$. Then

$$i + t_i \geqslant 2i - 1 - \lfloor \log_2 i \rfloor \geq 2\frac{n + 1 + \lfloor \log_2 n \rfloor}{2} - 1 - \lfloor \log_2 n \rfloor = n.$$

Since d_n is the largest integer i such that $n - i - t_i$ is positive, we must have $d_n < \frac{n+1+\lfloor \log_2 n \rfloor}{2}$. □

Lemma 1. *Let M_m be the $(m+1) \times (m+1)$ Vandermonde matrix*

$$M_m = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 3 & 3^2 & \dots & 3^m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (2m+1) & (2m+1)^2 & \dots & (2m+1)^m \end{bmatrix},$$

in which the rows and columns are indexed by $0, \dots, m$. The matrix M_m is row equivalent over $\mathbb{Z}$ to a matrix of the form

$$R_m = \begin{bmatrix} 1 & * & \dots & * \\ 0 & 2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 2^m m! \end{bmatrix},$$

where the $*$*'s represent integers (whose values are irrelevant for our purposes), and the only type of row reduction used is the one in which an integer multiple of a row is added to another row.*

Proof. We will prove, by induction on m, that

(i) every vector $r_{i,m} = (1, 2i+1, \dots, (2i+1)^m)$, $i \geqslant m+1$, is a linear combination of the rows $0, \dots, m$ in M_m,

(ii) the matrix R_m can be obtained by row reduction of the indicated type from M_m.

(iii) assuming $r_{i,m} = \alpha_0 r_{0,m} + \cdots + \alpha_m r_{m,m}$ in (i),

$$r_{i,m+1} - (\alpha_0 r_{0,m+1} + \cdots + \alpha_m r_{m,m+1}) = (0, 0, \dots, 0, s_i),$$

where $s_{m+1} = 2^{m+1}(m+1)!$ and s_i is divisible by $2^{m+1}(m+1)!$ if $i \geqslant m+2$.

The claims (i),(ii),(iii) are clear for $m = 0$ and assume they are valid for some $m \geqslant 0$. We proceed to the inductive step.

(i) Consider the vector $r_{i,m+1} = (1, 2i+1, \dots, (2i+1)^{m+1})$, $i \geqslant m+2$. From the inductive assumption (iii),

$$r_{i,m+1} - (\alpha_0 r_{0,m+1} + \cdots + \alpha_m r_{m,m+1}) = (0, 0, \dots, 0, s_i)$$

and

$$r_{m+1,m+1} - (\alpha'_0 r_{0,m+1} + \cdots + \alpha'_m r_{m,m+1}) = (0, 0, \dots, 0, 2^{m+1}(m+1)!).$$

Since $2^{m+1}(m+1)!$ divides s_i we see that $r_{i,m+1}$ can be indeed written as a linear combination of the rows $0, \dots, m+1$ in M_{m+1}.

(ii) Since, from inductive assumption (iii),

$$r_{m+1,m+1} - (\alpha'_0 r_{0,m+1} + \cdots + \alpha'_{m,m} r_{m,m+1}) = (0, 0, \dots, 0, 2^{m+1}(m+1)!).$$

we see that M_{m+1} is row equivalent to a matrix R'_{m+1} in which the bottom row is $(0, 0, \dots, 0, 2^{m+1}(m+1)!)$ and the upper left block of size $(m+1) \times (m+1)$ is M_m. The inductive assumption (ii) shows that R'_{m+1} is row equivalent to R_{m+1}.

(iii) Consider the matrix $M_{m+2}(i)$ obtained from M_{m+1} by extending it by the column vector $(1, 3^{m+2}, \dots, (2m+3)^{m+2})$ on the right and then by the row vector $r_{i,m+2}$, $i \geqslant m+2$, at the bottom. The new matrix is the $(m+3) \times (m+3)$ Vandermonde matrix corresponding to the values $1, 3, 5, \dots, 2m+3$ and $2i+1$. From parts (i) and (ii) of the inductive step that we just proved, we know that $M_{m+2}(i)$ is row equivalent to a matrix $R_{m+2}(i)$ in which the bottom row is $(0, 0, \dots, s_i)$, for some integer s_i, and the upper left block of size $(m+2)\times(m+2)$ is R_{m+1}. The determinant of the Vandermonde matrix $M_{m+2}(i)$ is equal to

$$\begin{aligned}\det(M_{m+2}(i)) =&(3-1)\cdot(5-3)(5-1)\cdot\ldots\cdot((2m+3)-(2m+1))\ldots\\ &\ldots((2m+3)-1)\cdot((2i+1)-(2m+3))\ldots((2i+1)-1)\\ =&\det(M_{m+1})\cdot((2i+1)-(2m+3))\ldots((2i+1)-1).\end{aligned}$$

On the other hand, the row equivalence of $M_{m+2}(i)$ and $R_{m+2}(i)$ shows that

$$\det(M_{m+2}(i)) = \det(R_{m+2}(i)) = \det(R_{m+1})\cdot s_i = \det(M_{m+1})\cdot s_i.$$

Since $\det(M_{m+1}) \neq 0$ we obtain that

$$s_i = ((2i+1)-(2m+3))\ldots((2i+1)-1).$$

In case $i = m+2$, $s_{m+2} = 2\cdot 4\cdot\cdots\cdot(2(m+2)) = 2^{m+2}(m+2)!$.

If $i \geqslant m+3$, then s_i is a product of $m+2$ consecutive even numbers and is therefore divisible by $2^{m+2}(m+2)!$. The inductive claim (iii) now easily follows. $\square$

Proof of Theorem 2, *uniqueness.* Let p be a polynomial function in $\mathcal{PF}_n$. All reduced polynomials inducing p are given by

$$P(x) = a_0 + a_1x + \cdots + a_dx^d,$$

where $d = d_n$, and the coefficients $a_0,\ldots,a_d$ satisfy the linear system

$$M_d(a_0,a_1,\ldots,a_d)^T = (p(1),p(3),\ldots,p(2d+1))^T,$$

where $(.)^T$ stands for transposition. By Lemma 1, this system is equivalent in $\mathbb{Z}_{2^n}$ to the upper triangular system

$$R_d(a_0,a_1,\ldots,a_d)^T = (b_0,b_1,\ldots,b_d)^T,$$

where b_i are some elements in $\mathbb{Z}_{2^n}$. Since odd numbers are units in $\mathbb{Z}_{2^n}$ this system is equivalent to a triangular system

$$R'_d(a_0,a_1,\ldots,a_d)^T = (b'_0,b'_1,\ldots,b'_d),$$

where

$$R'_d = \begin{bmatrix} 2^{0+t_0} & * & \ldots & * \\ 0 & 2^{1+t_1} & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 2^{d+t_d} \end{bmatrix}. \tag{2}$$

The last equation of this system now reads $2^{d+t_d}a_d = b'_d$. Since $0 \leqslant a_d \leqslant 2^{n-d-t_d} - 1$ this equation can only have one solution in $\mathbb{Z}_{2^n}$. We can substitute this solution in the second to last equation to obtain an equation $2^{d-1+t_{d-1}}a_{d-1} = b''_{d-1}$, which will also have a unique solution in $\mathbb{Z}_{2^n}$ since $0 \leqslant a_{d-1} \leqslant 2^{n-d-1-t_{d-1}} - 1$.

Continuing with the backward substitution in the triangular system with matrix R'_d we obtain a unique solution for all the coefficients $a_d, a_{d-1}, \dots, a_0$ of $P(x)$. $\square$

Proposition 7. *The number of polynomial functions in $\mathcal{PF}_n$ is equal to the number of reduced polynomials in $\mathcal{RP}_n$.*

Example 2. Let $n = 4$. In this case $d = d_4 = 2$. Let p be a polynomial function in $\mathcal{PF}_4$ for which $p(1) = 9$, $p(3) = 5$ and $p(5) = 9$. We are trying to determine the unique reduced polynomial $P(x) = a_0 + a_1x + a_2x^2$ in $\mathcal{RP}_4$ that induces p. Note that the coefficients must satisfy the range conditions $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$. The known values of p give the system

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 1 & 3 & 9 & | & 5 \\ 1 & 5 & 9 & | & 9 \end{bmatrix},$$

which is row equivalent to

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 0 & 2 & 8 & | & 12 \\ 0 & 0 & 8 & | & 8 \end{bmatrix}.$$

The last equation $8a_2 = 8$, together with the condition $0 \leqslant a_2 \leqslant 1$, gives $a_2 = 1$. The second equation $2a_1 + 8a_2 = 12$, together with the conditions $a_2 = 1$ and $0 \leqslant a_1 \leqslant 7$, gives $a_1 = 2$. Finally, the first equation $a_0 + a_1 + a_2 = 9$, together with the conditions $a_2 = 1$, $a_1 = 2$ and $0 \leqslant a_0 \leqslant 15$, gives $a_0 = 6$. Thus the unique reduced polynomial inducing p is $P(x) = 6 + 2x + x^2$. $\square$

Example 3. It is clear that one can uniquely determine the reduced polynomial $R(x)$ that is functionally equivalent to $P(x)$ from the value of p at any $d_n + 1$ consecutive values of x.

On the other hand, not any $d_n + 1$ values are sufficient. Indeed, let $n = 4$ and p be a polynomial function in $\mathcal{PF}_4$ for which $p(1) = 9$, $p(5) = 9$ and $p(9) = 9$. We are trying to determine a reduced polynomial $R(x) =$

$a_0 + a_1x + a_2x^2$ in $\mathcal{RP}_4$ that induces p. The known values of p give the system

$$\begin{bmatrix} 1 & 1 & 1 & | & 9 \\ 1 & 5 & 9 & | & 9 \\ 1 & 9 & 1 & | & 9 \end{bmatrix},$$

which, together with the range conditions $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$, gives the following 4 solutions: $R(x) = 9$, $R(x) = 6 + 2x + x^2$, $R(x) = 5 + 4x$, $R(x) = 2 + 6x + x^2$. Note than one of these is the solution obtained in Example 2. □

Proof of Theorem 1, necessity. Let $P(x)$ and $T(x)$ be two functionally equivalent polynomials. By Proposition 5, there exists polynomials $S_P(x)$ and $S_T(x)$ in I_n such that $P(x) - S_P(x)$ and $T(x) - S_T(x)$ are reduced polynomials which are functionally equivalent to $P(x)$ and $T(x)$. Theorem 2 then shows that $P(x) - S_P(x) = T(x) - S_T(x)$, implying that $P(x) - T(x) = S_P(x) - S_T(x) \in I_n$. □

Proposition 8. *The set of polynomials in $\mathbb{Z}_{2^n}[x]$ that induce the 0 constant function on Q_n is precisely the ideal I_n.*

Proof. We already know from Proposition 4 that the polynomials in I_n induce the constant 0 function on Q_n. Conversely, let $P(x)$ induce the constant 0 function on Q_n. By Proposition 5 there exists a polynomial $S_P(x)$ in I_n such that $P(x) - S_P(x)$ is reduced and functionally equivalent to $P(x)$. Since the zero polynomial is reduced, we must have $P(x) - S_P(x) = 0$, by Theorem 2. Therefore $P(x) = S_P(x) \in I_n$. □

4. Permutational polynomial functions on Q_n

Some polynomial function on Q_n are permutations on Q_n. Denote the set of such (permutational) polynomial functions by $\mathcal{PPF}_n$ and the set of polynomials over $\mathbb{Z}$ inducing such functions by $\mathcal{PP}_n$.

Proposition 9. *Let $P(x) = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial in $\mathcal{P}_n$. Then $P(x)$ is in $\mathcal{PP}_n$ (i.e. $P(x)$ induces a permutational polynomial function on Q_n) if and only if the sum of the odd indexed coefficients $a_1 + a_3 + a_5 + \cdots$ is an odd number.*

Proof. Let $a, b \in Q_n$. We have

$p(a) - p(b) = a_1(a - b) + a_2(a^2 - b^2) + \cdots + a_d(a^d - b^d) =$

$$= (a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d),$$

where $A_1 = 1$ and $A_i = a^{i-1} + a^{i-2}b + \cdots + ab^{i-2} + b^{i-1}$, for $i \geqslant 2$. The number A_i is even if and only if i is even. Consequently, $a_1A_1 + a_2A_2 + \cdots + a_dA_d$ is odd if and only if $a_1 + a_3 + a_5 + \cdots$ is odd number.

If $a_1 + a_3 + a_5 + \cdots$ is even then $(a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d) \equiv 0 \pmod{2^n}$, for $a = 2^{n-1}+1$, $b = 1$. Thus, for this choice of a and b, we have $p(a) = p(b)$ and, therefore, p is not a permutation on Q_n.

If $a_1 + a_3 + a_5 + \cdots$ is odd then $(a-b)(a_1A_1 + a_2A_2 + \cdots + a_dA_d) \equiv 0 \pmod{2^n}$ if and only if $a - b \equiv 0 \pmod{2^n}$, i.e., $a = b$ in Q_n. Thus p is a permutation in this case. □

Since we have a bijective correspondence between reduced polynomials and polynomial functions, it is clear that we also have a bijective correspondence between the reduced polynomials in $\mathcal{RP}_n$ with odd sum of odd indexed coefficients and the permutational polynomial functions in $\mathcal{PPF}_n$.

Proposition 10. *The number of permutational polynomial functions in $\mathcal{PPF}_n$ is equal to*

$$|\mathcal{PPF}_n| = 2^{(2n-d_n)(d_n+1)/2-2-\sum_{i=0}^{d_n} t_i}$$

Example 4. Reduced polynomials in $\mathcal{RP}_n$ of degree at most 3 that induce permutational polynomial functions in $\mathcal{PPF}_n$ have the form $a_0 + a_1x + a_2x^2 + a_3x^3$, where $a_1 + a_3$ is odd, $a_0 + a_2$ is even, $0 \leqslant a_0 \leqslant 2^n - 1$, $0 \leqslant a_1 \leqslant 2^{n-1} - 1$, $0 \leqslant a_2 \leqslant 2^{n-3} - 1$, and $0 \leqslant a_3 \leqslant 2^{n-4} - 1$. □

Proposition 11. *The inverse of a permutational polynomial function $p \in \mathcal{PPF}_n$ is also a polynomial function.*

Proof. If $p \in \mathcal{PF}_n$ is a permutation on Q_n, then $p \in \sigma(Q_n)$, where $\sigma(Q_n)$ denotes the full permutation group of Q_n. Let r be the order of p in $\sigma(Q_n)$. Then $p^{-1} = p^{r-1}$ and therefore, if p is induced by the polynomial $P(x)$, then p^{-1} is induced by the polynomial $\underbrace{P(P(\dots P(}_{r-1}x)))$. □

Example 5. A linear permutational polynomial function p has a linear permutational polynomial function as its inverse. Indeed, if p is induced by $b + ax$, then a must be odd, a^{-1} exists in $\mathbb{Z}_{2^n}$ and p^{-1} is induced by the polynomial $-a^{-1}b + a^{-1}x$. □

We can use the permutational polynomial functions on Q_n to define permutations on $\mathbb{Z}_{2^n}$ (this will be useful in our last section). Denote by Q'_n the set $\mathbb{Z}_{2^n} \setminus Q_n$ (consisting of 0 and all zero divisors in $\mathbb{Z}_{2^n}$). We can easily conjugate the action of a polynomial function on Q_n to an action on Q'_n. Namely, given a polynomial function $h : Q_n \to Q_n$, define $h' : Q'_n \to Q'_n$ by $h'(x) = h(x+1) - 1$.

Given a permutation $p \in \mathcal{PF}_n$, we can define a permutation $\hat{p}$ on $\mathbb{Z}_{2^n}$ by

$$\hat{p}(x) = \begin{cases} p(x), & x \in Q_n \\ p'(x), & x \in Q'_n \end{cases}. \tag{3}$$

More generally, given permutations $p, h \in \mathcal{PF}_n$, a permutation $f_{p,h}$ on $\mathbb{Z}_{2^n}$ can be defined by

$$f_{p,h} = \begin{cases} p(x), & x \in Q_n \\ h'(x), & x \in Q'_n \end{cases}. \tag{4}$$

5. On a result of Rivest

The main result of Rivest in [15] provides a criterion for a polynomial over $\mathbb{Z}$ to induce a permutation on $\mathbb{Z}_{2^n}$. We infer now this result from our results. Note that our proof only relies on Proposition 2 and Proposition 9, both of which have short and rather elementary proofs.

Theorem 3 (Rivest [15]). *A polynomial $P(x) = a_0 + a_1x + \cdots + a_dx^d$ of degree $d \geqslant 1$ over $\mathbb{Z}$ induces a permutation on $\mathbb{Z}_{2^n}$ if and only if the following conditions are satisfied:*

(a) *the sum $a_2 + a_4 + a_6 + \ldots$ is even,*
(b) *the sum $a_3 + a_5 + a_7 + \ldots$ is even,*
(c) *a_1 is odd.*

Proof. If $P(x)$ is a polynomial that permutes $\mathbb{Z}_{2^n}$ then all elements in $Q'_n = \mathbb{Z}_{2^n} \setminus Q_n$ are mapped to elements of Q'_n or all of them are mapped to elements in Q_n depending on the parity of a_0. Let us first characterize those polynomials over $\mathbb{Z}$ that permute both Q_n and Q'_n. They are precisely the polynomials for which

(i) a_0 is even,
(ii) the sum of all coefficients $a_0 + a_1 + \cdots + a_d$ is odd,
(iii) the sum of the odd index coefficients $a_1 + a_3 + \ldots$ is odd,

(iv) the sum of the odd index coefficients in $P(x+1)-1$ is odd.

The first condition ensures that Q'_n is invariant, the second that Q_n is invariant (Proposition 2), the third that $P(x)$ induces a permutation on Q_n (Proposition 9) and the last that $P(x)$ induces a permutation on Q'_n (by conjugating the action from Q'_n to Q_n we can again use Proposition 9). Let $S(x)=P(x+1)-1$. The sum of odd index coefficients of $S(x)$ is odd exactly when $(S(1)-S(-1))/2$ is odd. But $(S(1)-S(-1))/2=(P(2)-P(0))/2=a_1+2a_2+2^2a_3+\cdots+2^{d-1}a_d$, and therefore this condition is equivalent to a_1 being odd. Therefore the conditions (i)-(iv) are equivalent to

(i') a_0 is even,

(ii') the sum $a_2+a_4+a_6+\dots$ is even,

(iii') the sum $a_3+a_5+a_7+\dots$ is even,

(iv') a_1 is odd.

Thus, in order to characterize all polynomials that induce a permutation on $\mathbb{Z}_{2^n}$ we just need to drop the condition that a_0 is even (which allows Q_n and Q'_n to be mapped to each other, when a_0 is odd). $\square$

In fact, we may establish a precise connection between the (permutational) polynomial functions on Q_n and those on $\mathbb{Z}_{2^n}$.

Proposition 12. *Let $n \geqslant 2$. For every pair of polynomials functions $p,h \in \mathcal{PF}_n$, there exists a polynomial function g on $\mathbb{Z}_{2^n}$, such that*

$$g(x)=f_{p,h}(x),$$

for x in $\mathbb{Z}_{2^n}$.

Proof. Consider the polynomial

$$V_0(x)=\begin{cases} x^{2^{n-2}}, & n \geqslant 4 \\ x^4, & n=3, \\ x^2, & n=2. \end{cases}$$

We claim that, for the associated polynomial function $v_0(x)$ on $\mathbb{Z}_{2^n}$,

$$v_0(x)=\begin{cases} 1, & x \in Q_n, \\ 0, & x \in Q'_n. \end{cases}$$

The claim can be easily verified directly for $n=2,3$. Assume $n \geqslant 4$. From Proposition 1, it follows that $v_0(x)=1$, for $x \in Q_n$. On the other hand, $2^{n-2} \geqslant n$, for $n \geqslant 4$, which then implies that $v_0(x)=x^{2^{n-2}}=0$, for $x \in Q'_n$.

Let $V_1(x) = 1 - V_0(x)$. For the associated polynomial function $v_1(x)$ we clearly have

$$v_1(x) = \begin{cases} 0, & x \in Q_n, \\ 1, & x \in Q'_n. \end{cases}$$

Therefore, if $P(x)$ and $H(x)$ are polynomial representing the polynomial functions $p(x)$ and $h(x)$ then the polynomial

$$G(x) = P(x)V_1(x) + H'(x)V_0(x),$$

where $H'(x) = H(x+1) - 1$, induces the function $f_{p,h}$, showing that this function is a polynomial function on $\mathbb{Z}_{2^n}$. □

Corollary 2. *Let $n \geqslant 2$. The number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is*

$$2^{(2n-d_n)(d_n+1)-3-2\sum_{i=0}^{d_n} t_i}, \tag{5}$$

where t_i is the largest integer ℓ such that 2^ℓ divides $i!$, and d_n is the largest integer i such that $n - i - t_i$ is positive.

Proof. Note that the correspondence that associates to each pair of permutational polynomial functions (p, h) on Q_n the element $f_{p,h}$ in the set of permutational polynomial functions on $\mathbb{Z}_{2^n}$ that keep both Q_n and Q'_n invariant is a bijection. Thus, the number of such permutational polynomial functions on $\mathbb{Z}_{2^n}$ is $|\mathcal{PPF}_n|^2$. The number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is twice larger than this number since we need to take into account the polynomial functions that permute Q_n and Q'_n. Thus, the total number is

$$2|\mathcal{PPF}_n|^2 = 2^{(2n-d_n)(d_n+1)-3-2\sum_{i=0}^{d_n} t_i}.$$ □

It is interesting to compare the last corollary to earlier results counting permutational polynomial functions on $\mathbb{Z}_{2^n}$. For instance, the following formula is proved in [7]. For $n \geqslant 2$, the number of permutational polynomial functions on $\mathbb{Z}_{2^n}$ is equal to

$$2^{3+\sum_{j=3}^{n} \beta_j}, \tag{6}$$

where β_j is the smallest integer s such that 2^j divides $s!$. Combining this with our result yields the identity

$$2\sum_{i=0}^{d_n} t_i + \sum_{j=3}^{n} \beta_j = (2n - d_n)(d_n + 1) - 6,$$

for $n \geqslant 2$. We note that the number of permutational polynomials given by our formula (5) in Corollary 2 seems easier to evaluate than by using (6), since the summation goes to a smaller bound (d_n rather than n) and the summands are easier to compute.

6. Multiplication operation on reduced polynomials

Here we consider the multiplication operation on the set $\mathcal{RP}_n$ of reduced polynomials.

We recall that $\mathcal{RP}_n$ is the set of representatives of the congruences classes of $\mathcal{P}_n$ modulo the functional equivalence relation $\approx$. In that sense, given $P(x), S(x) \in \mathcal{RP}_n$, we denote by $P(x) \cdot S(x)$ the corresponding reduced polynomial inducing the same polynomial function as the product $P(x)S(x)$ of the polynomials $P(x)$ and $S(x)$. The set $\mathcal{P}_n$ forms a monoid under polynomial multiplication. Indeed, if the sum of the coefficient of both $P(x)$ and $S(x)$ is odd, then $p(1)$ and $s(1)$ are odd and therefore so is p(1)s(1), implying that the sum of the coefficients of $P(x)S(x)$ is also odd.

Theorem 4. *The equivalence $\approx$ is a congruence on $\mathcal{P}_n$. The factor $(\mathcal{RP}_n, \cdot)$ $= \mathcal{P}_n/\approx$ is a finite 2-group.*

Proof. Let $P_i(x) \approx S_i(x)$, for $i = 1, 2$, $T_P(x) = P_1(x)P_2(x)$, and $T_S(x) = S_1(x)S_2(x)$. Then $t_P(x) = p_1(x)p_2(x) = s_1(x)s_2(x) = t_S(x)$. Thus we have $P_1(x)P_2(x) \approx S_1(x)S_2(x)$ and $\approx$ is a congruence on $\mathcal{P}$.

For every $a \in Q_n$, we have $a^{2^{n-2}} = 1$ in Q_n. Therefore, for any polynomial $P(x)$ in $\mathcal{P}_n$, the polynomial $P(x)^{2^{n-2}}$ is functionally equivalent to 1. Thus each reduced polynomial has a multiplicative inverse. □

In order to avoid confusion we denote inverses of polynomial functions under composition by $(.)^{-1}$, and the inverse of a reduced polynomial $P(x)$ under multiplication by $\frac{1}{P(x)}$.

The subset $\mathcal{PRP}_n$ of $\mathcal{RP}_n$ consisting of reduced polynomials that induce permutations on Q_n is not closed under multiplication. Indeed, $P(x) = 2+x$ induces a permutation on Q_n, while $P(x)^2 = 4 + 4x + x^2$ does not.

Proposition 13. *The set of reduced permutational polynomials $\mathcal{PRP}_n$ is closed under multiplicative inversion, i.e., $P(x) \in \mathcal{PRP}_n$ implies $\frac{1}{P(x)} \in$ $\mathcal{PRP}_n$.*

Proof. This directly follows from the fact that different elements in Q_n have different multiplicative inverses. □

Example 6. We have $\frac{1}{2+x} = 2 + x$ in $\mathcal{RP}_3$, $\frac{1}{4+3x} = 3 + 3x + x^2$ in $\mathcal{RP}_4$, and $\frac{1}{31+2x+2x^2+x^3+x^4} = 4 + 7x + 2x^2$ in $\mathcal{RP}_5$. $\square$

We note that finding the inverse polynomial by using the equality $\frac{1}{P(x)} = P(x)^{2^{n-2}-1}$ is not effective. We provide an effective method in the next section.

7. Algorithmic aspects

We briefly address the complexity issues related to interpolation of polynomial functions, inversion of permutational polynomial functions and multiplicative inversion of polynomials.

Theorem 5. *There exists an algorithm of polynomial complexity in n that, given the values $p(1), p(3), \ldots, p(2d_n+1)$ of a polynomial function p in $\mathcal{PF}_n$, produces the unique reduced polynomial $R(x)$ that induces p.*

Proof. Note that d_n has a linear upper bound in n by Proposition 6. Running the row reduction on the $(d_n+1) \times (d_n+1)$ linear system as suggested in the uniqueness part of the proof of Theorem 2 takes polynomially many steps in terms of n. $\square$

Theorem 6. *There exists an algorithm of polynomial complexity in $n+m$ that, given a polynomial $P(x) \in \mathcal{P}_n$ of degree m (with coefficients reduced modulo 2^n, i.e., coefficients in the range between 0 and $2^n - 1$ inclusive), produces the unique reduced polynomial $R(x)$ that is functionally equivalent to $P(x)$.*

Proof. By Theorem 5 it is sufficient to calculate $p(1), p(3), \ldots, p(2d_n + 1)$ in polynomially many steps in terms of $n + m$. This is possible since the degree of $P(x)$ is m and the calculations are done modulo 2^n.

Another approach would be to use the reduction algorithm suggested in the proof of Proposition 5 and implemented in Example 1. $\square$

Theorem 7. *There exists an algorithm of polynomial complexity in $n+m$ that, given a polynomial $P(x)$ in $\mathcal{PP}_n$ of degree m (with coefficients reduced modulo 2^n), produces the unique reduced polynomial inducing the inverse polynomial function p^{-1}.*

Proof. First calculate $p(1), p(3), \ldots, p(2d_n + 1)$. Set up a system of linear equations to determine the coefficients of the reduced polynomial $R(x) = a_0 + a_1x + \cdots + a_dx^d$ that is functionally equivalent to p^{-1}, where $d = d_n$. The system has the form

$$\begin{bmatrix} 1 & p(1) & p(1)^2 & \ldots & p(1)^d \\ 1 & p(3) & p(3)^2 & \ldots & p(3)^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p(2d+1) & p(2d+1)^2 & \ldots & p(2d+1)^d \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ \vdots \\ 2d+1 \end{bmatrix}.$$

We apply row reduction to this system. The crucial observation is that since, for every $a, b \in Q_n$,

$$P(a) - P(b) = (a - b)k_{a,b},$$

where $k_{a,b}$ is an odd number (see the proof of Proposition 9) and odd numbers are units in $\mathbb{Z}_{2^n}$ the row reduction will eventually lead to a system in which the matrix of the system has the form (2). This system has unique solution that can be found by back substitution. □

Example 7. Let $n = 4$ and $P(x) = 5 + x + x^2$. The polynomial $P(x)$ induces a permutation p on Q_4. We will find the unique reduced polynomial $R(x) = a_0 + a_1x + a_2x^2$, with $0 \leqslant a_0 \leqslant 15$, $0 \leqslant a_1 \leqslant 7$, and $0 \leqslant a_2 \leqslant 1$, that induces the inverse permutation p^{-1} on Q_n.

We calculate $p(1) = 7$, $p(3) = 1$ and $p(5) = 3$. We then perform row reduction (over $\mathbb{Z}_{16}$) on the system

$$\left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 3 & 9 & 5 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 10 & 0 & 2 \\ 0 & 12 & 8 & 4 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 2 & 0 & 10 \\ 0 & 4 & 8 & 12 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 7 & 1 & 1 \\ 0 & 2 & 0 & 10 \\ 0 & 0 & 8 & 8 \end{array}\right],$$

where the third matrix is obtained from the second by re-scaling the second row by $13 = 5^{-1}$ and the third row by $11 = 3^{-1}$. The last system is triangular and has unique solution $a_2 = 1$ $a_1 = 5$ and $a_0 = 13$. Thus $R(x) = 13 + 5x + x^2$ induces the inverse polynomial function p^{-1}. □

Theorem 8. *There exists an algorithm of polynomial complexity in* $n + m$ *that, given a polynomial* $P(x) \in \mathcal{P}_n$ *of degree* m *(with coefficients reduced modulo* 2^n*), produces the multiplicative inverse* $\frac{1}{P(x)}$ *in reduced form.*

Proof. To calculate the reduced polynomial $S(x) = \frac{1}{P(x)}$ it suffices to calculate $p(x)$ for $x = 1, 3, \ldots, 2d_n + 1$, then calculate the multiplicative inverses $s(x) = \frac{1}{p(x)}$, for $x = 1, 3, \ldots, 2d_n + 1$, and finally use Theorem 5 to find the coefficients of $S(x)$. □

8. Huge quasigroups defined by polynomial functions

A k-groupoid ($k \geqslant 2$) is an algebra (Q, f) on a nonempty set Q as its universe and with one k-ary operation $f : Q^k \to Q$.

Definition 3. A k-groupoid (Q, f) is said to be a *k-quasigroup* if any k out of any $k+1$ elements $a_1, a_2, \ldots, a_{k+1} \in Q$ satisfying the equality

$$f(a_1, a_2, \ldots, a_k) = a_{k+1}$$

uniquely determine the remaining one.

A k-groupoid is said to be a *cancellative* k-groupoid if it satisfies the cancellation law

$$f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k) = f(a_1, \ldots, a_{i-1}, y, a_{i+1}, \ldots, a_k) \Rightarrow x = y,$$

for each $i = 1, \ldots, k$ and all $x, y, a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_k$ in Q.

For $k = 2$ we obtain the standard notion of a quasigroup.

The definition of a k-quasigroup immediately implies the following. Let (Q, f) be a finite k-quasigroup and let the map $\varphi : Q \to Q$ be defined by $\varphi(x) = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_k)$, for some fixed $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots$ $\ldots, a_k$ in Q. Then φ is a permutation on Q.

Here we consider only finite k-quasigroups (Q, f), i.e., Q is a finite set, and in this case we have the following property ([10]).

Proposition 14. *The following statements are equivalent for a finite k-groupoid (Q, f):*

(a) (Q, f) *is a k-quasigroup,*

(b) (Q, f) *is a cancellative k-groupoid.* □

Given a k-quasigroup (Q, f) we can define k new k-ary operations f_i, $i = 1, 2, \ldots, k$, by

$$f_i(a_1, \ldots, a_k) = b \iff f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k) = a_i.$$

These operations are called adjoint operations of f. Then (Q, f_i) are k-quasigroups as well ([2]).

Definition 4. A *huge* k-quasigroup is said to be a k-quasigroup (Q, f) such that all of the operations $f, f_1, f_2, \ldots, f_k$ can be computed with complexity $\mathcal{O}((\log |Q|)^\alpha)$ for some constant α.

The problem of effective constructions of quasigroups of any order can be solved, for example, by using P. Hall's algorithm for choosing different representatives for a family of sets. The algorithm is of complexity $\mathcal{O}(n^3)$, where n is the order of the quasigroup, and is not applicable for, let say, $n = 2^{16}$. We will show here how the permutational polynomial functions from $\mathcal{PF}_n$ can be used in order to construct families of huge quasigroups on the sets Q_n and $\mathbb{Z}_{2^n}$.

Theorem 9. *Let $p_1, p_2, \ldots, p_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on Q_n by*

$$f(a_1, a_2, \ldots, a_k) = p_1(a_1)p_2(a_2)\cdots p_k(a_k) \pmod{2^n}. \tag{7}$$

Then the k-groupoid (Q_n, f) is a huge quasigroup.

Proof. Let $r = 2^n$. The permutations in $\mathcal{PPF}_n$ are defined by polynomials $P(x)$ of degree smaller than $(\log_2 r + 1 + \lfloor \log_2(\log_2 r)\rfloor)/2$ (by Proposition 6). Then the evaluation of $P(x)$ modulo 2^n can be computed in polynomial complexity with respect to $\log_2 r$. Consequently, the function f defined by (7) can be computed in polynomial complexity with respect to $\log_2 r$.

Consider now the adjoint operations f_i of f. We have, for any $a_1, a_2, \ldots$ $\ldots, a_k, b \in Q_n$:

$$\begin{aligned}
&f_i(a_1, a_2, \ldots, a_k) = b \iff \\
&\quad\iff f(a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k) = a_i \\
&\quad\iff p_1(a_1)\cdots p_{i-1}(a_{i-1})p_i(b)p_{i+1}a_{i+1}\cdots p_k(a_k) = a_i \\
&\quad\iff p_i(b) = (p_{i-1}(a_{i-1}))^{-1}\cdots(p_1(a_1))^{-1}a_i(p_k a_k)^{-1}\cdots(p_{i+1}(a_{i+1}))^{-1} \\
&\quad\iff b = p_i^{-1}((p_{i-1}(a_{i-1}))^{-1}\cdots(p_1(a_1))^{-1}a_i(p_k a_k)^{-1}\cdots(p_{i+1}(a_{i+1}))^{-1})
\end{aligned}$$

By using the Hensel lifting technique the inverse elements $(p_j(a_j))^{-1}$ can be computed in polynomial complexity with respect to $\log_2 r$ (see Section 2), and the same is true for the inverse permutation p_i^{-1} by Theorem 7. □

Theorem 10. *Let $p_1, p_2, \ldots, p_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on $\mathbb{Z}_{2^n}$ by*

$$f(a_1, a_2, \ldots, a_k) = \hat{p_1}(a_1) + \hat{p_2}(a_2) + \cdots + \hat{p_k}(a_k) \pmod{2^n}, \tag{8}$$

where $\hat{p_i}$ are defined by (3). Then the k-groupoid (Q_n, f) is a huge quasigroup.

Proof. The proof is similar to the proof of Theorem 9. We only need to note that the inverse permutation

$$\hat{p_i}^{-1} = \begin{cases} p_i^{-1}(a), & a \in Q_n \\ p_i^{-1}(a+1) - 1, & a \in Q'_n \end{cases}$$

can be computed in polynomially complexity with respect to $\log_2 r$. □

Theorem 11. *Let $p_1, \ldots, p_k$ and $h_1, \ldots, h_k$ be permutations in $\mathcal{PPF}_n$. Define a k-ary operation f on $\mathbb{Z}_{2^n}$ by*

$$f(a_1, a_2, \ldots, a_k) = f_{p_1,h_1}(a_1) + f_{p_2,h_2}(a_2) + \cdots + f_{p_k,h_k}(a_k) \pmod{2^n},$$

where f_{p_i,h_i} are defined by (4). *Then the k-groupoid (Q_n, f) is a huge quasigroup.* □

We note that Rivest [15] gives a simple necessary and sufficient condition for a bivariate polynomial $P(x, y)$ modulo 2^n to represent a quasigroup on $\mathbb{Z}_{2^n}$, namely $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$ should be univariate permutational polynomials on $\mathbb{Z}_{2^n}$. This result is based on his main result in [15] (see Theorem 3 in Section 5).

References

[1] **A. Bandini**, *Functions $f : \mathbb{Z}_{/p^n\mathbb{Z}} \to \mathbb{Z}_{/p^n\mathbb{Z}}$ induced by polynomials of $\mathbb{Z}[X]$*, Annali di Matem. **181** (2002), 95 – 104.

[2] **V. D. Belousov**, *n-ary quasigroups*, (Russian), Stiinca, Kishiniev, 1972.

[3] **G. Carter, E. Dawson and L. Nielsen**, *A latin square version of DES*, In Proc. Workshop of Selected Areas in Cryptography, Ottawa, Canada, 1995.

[4] **J. Cooper, D. Donovan and J. Seberry**, *Secret sharing schemes arising from Latin Squares*, Bull. Inst. Combin. Appl. **4** (1994), 33 – 43.

[5] **J. Dènes and A. D. Keedwell**, *A new authentication scheme based on latin squares*, Discrete Math., **106-107** (1992), 157 – 161.

[6] **D. Gligoroski, S. Markovski, L. Kocarev, and M. Gusev**, *Edon80 Hardware Synchronous stream cipher*, SKEW 2005 - Symmetric Key Encryption Workshop, Aarhus Denmark, 2005.

[7] **G. Keller and F. R. Olson**, *Counting polynomial functions (mod p^n)*, Duke Math. J. **35** (1968), 835 – 838.

[8] **E. Kaltofen**, *Sparse Hensel Lifting*, EUROCAL'85, European Conf. Comput. Algebra Proc. **2** (1985), $4-17$.

[9] **A. J. Kempner**, *Polynomials and their residue systems*, Amer. Mat. Soc. Trans. **22** (1921), $240-288$.

[10] **S. Markovski, V. Dimitrova and A. Mileva**, *A new method for computing the number of n-quasigroups*, Bul. Acad. Sti. Republ. Moldova, Matematica **3(52)** (2006), $1-84$.

[11] **S. Markovski, S. Samardziska, D. Gligoroski, S. J. Knapskog**, *Multivariate trapdoor functions based on multivariate left quasigroups and left polynomial quasigroups*, Proc. 2nd Inter. Conf. Symbolic Computation and Cryptography SCC 2010, London (in print).

[12] **G. Mullen and H. Stevens**, *Polynomial functions* $\pmod m$, Acta Math. Hung. **44** (1984), $237-241$.

[13] **W. Nöbauer**, *Über permutations polynome und permutation function für primzahl potenzen*, Monatsh. Math. **69** (1965), $230-238$.

[14] **O. Perron**, *Obituary: Kurt Hensel*, Jber. Bayer. Akad. Wiss, München (1948), $234-236$.

[15] **R. L. Rivest**, *Permutation polynomials modulo* 2^w, Finite Fields and Their Appl. **7** (2001), $287-292$.

[16] **C. P. Schnorr and S. Vaudenay**, *Black Box Cryptanalysis of hash networks based on multipermutations*, In Advances of Cryptology - EUROCRYPT'94, Springer, Berlin 1995.

[17] **C. E. Shannon**, *Communication theory of secrecy systems*, Bell Sys. Tech. J. **28** (1949), $657-715$.

[18] **Q. Zhang**, *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Numb. Theory **105** (2004), $192-202$.

Received December 09, 2009

S. Markovski

Ss Cyril and Methodius University, Faculty of Sciences, Institute of Informatics, P.O. Box 162, 1000 Skopje, Republic of Macedonia, E-mail: smile@ii.edu.mk

Z. Šunić

Department of Mathematics, Texas A&M University, College Station, TX 77843-3368, USA E-mail: sunic@math.tamu.edu

D. Gligoroski

Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology, O.S.Brag-stads plass 2B, N-7491 Trondheim, Norway, E-mail: danilog@item.ntnu.no

Quasigroups and Related Systems **18** (2010), 83 − 94

Fast signatures based on non-cyclic finite groups

Nikolay A. Moldovyan

Devoted to the memory of Valentin D. Belousov (1925-1988)

Abstract. Finite rings of the m-dimension vectors over the ground field are defined with the vector multiplication operations of different types. Non-cyclic multiplicative groups of the rings in particular cases possess structure described in terms of the multi-dimension cyclicity. The vector finite groups relating to such cases are applied to design fast digital signature algorithms.

1. Introduction

The cyclic finite groups of different types are widely used as primitives of the digital signature (DS) algorithms [7, 9]. A group is called cyclic, if there exists a group element G (called generator) such that all elements of the group can be generated as different powers of G. Usually in the DS schemes based on difficulty of the discrete logarithm problem (DLP) the public key is computed as a group element $Y = G^x$, where G is the $\omega(G)$ order group element, and x is the secret key ($x < \omega(G)$). Security of the DS scheme is provided by the necessary requirement that the value ω contains a large prime factor q such that $q \geqslant 2^{160}$ [2] and by some other requirements depending on type of the used group, the first requirement being a common one for all cyclic groups used as primitive of the DS algorithms. The upper security boundary is limited by the difficulty of the DLP. There are known the general-purpose methods for solving the DLP, which work in any type cyclic group [2]. Such methods have exponential complexity $W = O(\sqrt{q})$ group operations, where $O(\cdot)$ is the order notation, and q is the largest prime divisor of the group order. If $q \geqslant 2^{160}$, then solving the DLP with the general-purpose methods are computationally infeasible. For

2000 Mathematics Subject Classification: 11G20, 11T71
Keywords: digital signatures, non-cyclic groups, vector finite groups
Supported by the Russian Foundation for Basic Research grant # 08-07-00096-a.

some finite groups there are known specialized methods having subexponential difficulty. Such groups are also used in some DS schemes, however they do not provide sufficiently high performance of the signature generation and verification procedures.

At present finite groups of the elliptic curve (EC) points represent the most efficient primitive of the DS algorithms. In the DS schemes there are used properly defined ECs for which the most efficient methods for solving the DLP are the general-purpose ones. Therefore it is sufficient to use the EC defined over finite fields (FFs) having the order size 160 to 320 bits [1]. Due to sufficiently small size of the FF order the DS algorithms based on ECs [3] provide the high performance.

Unfortunately the performance of the EC-based DS algorithms is limited by the inversion operation in the underlying FF, which is included in the procedure implementing the operation of adding the EC points. To overcome this limitation the finite groups of vectors over the ground FFs have been proposed as primitives of the DS algorithms [5]. For detailed justification of this proposal it is required to consider the structure of the vector finite groups (VFGs) that in general case are not cyclic. Only in some particular cases the multiplicative VFGs have cyclic structure. Such cases relates to formation of the vector finite fields (VFFs) [4] that have been proposed to define ECs providing higher performance of the EC-based DS algorithms. Essentially higher performance is expected from the DS based on non-cyclic VFGs.

Present paper presents the results on investigation of the structure of the non-cyclic VFGs and describes peculiarities of designing the DS algorithm based on computations in the VFGs. Section 2 provides description of the finite rings of the m-dimension vectors and defines a class of the vector multiplication operations. Section 3 provides general description of the structure of the vector finite rings in terms of the multi-dimension cyclicity (MDC). The proposed formulas describing the group structure have been confirmed by computational experiments. Section 4 explains the features of designing the DS algorithms based on VFGs possessing the MDC and presents new DS schemes and a rough performance comparison with the well known DS algorithms. Section 5 concludes the paper.

2. Finite rings of the m-dimension vectors

Finite rings of m-dimension vectors are defined over the ground field $GF(p)$, where p is a prime. Suppose $\mathbf{e}$, $\mathbf{i}$, $\ldots$, $\mathbf{w}$ be some m formal basis vectors and $a, b, z \in GF(p)$, where $p \geqslant 3$, are coordinates. The set of vectors

$$a\mathbf{e} + b\mathbf{i} + \cdots + z\mathbf{w}$$

is a finite m-dimension vector space. A vector can be also represented as a set of its coordinates $(a, b, \ldots, z)$. The terms $\tau\mathbf{v}$, where $\tau \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{w}\}$, are called components of the vector. The addition and multiplication operations over the vectors are defined as follows. The addition of two vectors $(a, b, \ldots, z)$ and $(a', b', \ldots, z')$ is defined via addition of the coordinates corresponding to the same basis vector accordingly to the following formula

$$(a, b, \ldots, z) + (a', b', \ldots, z') = (a + a', b + b', \ldots, z + z').$$

The multiplication of two vectors $a\mathbf{e}+b\mathbf{i}+\cdots+z\mathbf{w}$ and $a'\mathbf{e}+b'\mathbf{i}+\cdots+z'\mathbf{w}$ is defined as pair-wise multiplication of all components of the vectors in correspondence with the following formula

$$\begin{aligned}(a\mathbf{e}+b\mathbf{i}+\cdots+z\mathbf{w})\circ(a'\mathbf{e}+b'\mathbf{i}+\cdots+z'\mathbf{w}) = aa'\mathbf{e}\circ\mathbf{e}+ba'\mathbf{i}\circ\mathbf{e}+\cdots+za'\mathbf{w}\circ\mathbf{e}+\\ +ab'\mathbf{e}\circ\mathbf{i}+bb'\mathbf{i}\circ\mathbf{i}+\cdots+cb'\mathbf{w}\circ\mathbf{i}+\ldots\\ \cdots+az'\mathbf{e}\circ\mathbf{w}+bz'\mathbf{i}\circ\mathbf{w}+\cdots+zz'\mathbf{w}\circ\mathbf{w},\end{aligned}$$

where $\circ$ denotes the vector multiplication operation. In the final expression each product of two basis vectors is to be replaced by some basis vector $\mathbf{v}$ or by a vector $\tau\mathbf{v}$ ($\tau \in GF(p)$) in accordance with some given table called basis-vector multiplication table (BVMT). There are possible different types of the BVMTs, but in this paper there is used the BVMT of some general type proposed in [6] (see Table 1). For arbitrary values m and τ Table 1 defines the vector multiplication that is a commutative and associative operation. Different values τ define different types of the vector multiplication operation that defines the structure of the multiplicative group of the vector finite ring (VFR).

$\circ$	$\vec{e}$	$\vec{\imath}$	$\vec{j}$	$\vec{k}$	$\vec{u}$	$\ldots$	$\vec{w}$
$\vec{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\ldots$	$\mathbf{w}$
$\vec{\imath}$	$\mathbf{i}$	$\epsilon\mathbf{j}$	$\epsilon\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$
$\vec{j}$	$\mathbf{j}$	$\epsilon\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$
$\vec{k}$	$\mathbf{k}$	$\epsilon\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$
$\vec{u}$	$\mathbf{u}$	$\epsilon\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$
$\ldots$	$\ldots$	$\epsilon\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$
$\vec{w}$	$\mathbf{w}$	$\epsilon\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\ldots$

Table 1. The basis-vector multiplication table of the general type [6].

3. Cyclicity of the multiplicative group of VFR

The fixed vector addition operation is used in the VFR described in Section 2. On the contrary, for the given values m and p different types of the multiplication operation are specified with different values of the "expansion" coefficient τ. In this section the structure of the multiplicative group is considered. There are possible a variety of different structures of the VFGs depending on selection of the value τ. The simplest example is provided by the example of the VFFs that are formed in the cases $m|p-1$, while usingle values τ such that the equation $x^m = \tau$ has no solution in the field $GF(p)$. In such cases the VFGs have the cyclic structure and the VFG order is equal to $\Omega = p^m - 1$. Majority of other cases (for some values m there are possible specific conditions of the VFFs formation) the VFGs possess non-cyclic structure. The known example are VFGs formed in the case $m|p-1$, while using value τ such that the equation $x^m = \tau$ has a solution in the field $GF(p)$. In the last case for $m = 2$ and $m = 3$ the order of the VFGs is expressed by the following formula derived theoretically [6] $\Omega = (p-1)^m$. However the last formula does not explain the VFG structure. In the case of non-cyclic VFGs the computational experiments appear to be required to reveal the structure. The computational experiments have shown that the last formula is correct for all values m and the structure of such non-cyclic groups can be described in terms of MDC. The experiment have also shown in all cases the multiplicative VFGs possess structure described in terms of the MDC, except the case of the VFFs while the VFGs possess one-dimension cyclicity.

3.1. Multi-dimension cyclicity of the VFG structure

Let us consider a hypothetic group Γ_μ of the order $\Omega(\Gamma_\mu) = q^\mu$, where q is a prime, in which there exist μ elements $G_1, G_2, \ldots, G_\mu$ possessing the same order q, such that any group element $G \in \Gamma_\mu$ can be represented as product $\prod_{i=1}^{\mu} G_i^{s_i}$ for some set of powers $(s_1, s_2, \ldots, s_\mu)$ and none of these elements, for example, G_j can be expressed as product $\prod_{i=1;i\neq j}^{\mu} G_i^{s_i}$.

Non-cyclic groups produced by the generator system in which all generators have the same order value are called in this paper groups possessing the structure with multi-dimension cyclicity (MDC). The value μ is called dimension of the MDC of the group structure. The term MDC is used to describe the VFG structures since it corresponds well to the fact that the elements of the considered groups are vectors, besides the term reflects the fact that in all cases the multiplicative groups of the VFRs can be described from a single position. Indeed, the cyclic structure of the multiplicative groups of the VFFs can be considered as a particular case of MDC, i.e., as one-dimension cyclicity.

Since the element order divides the group order, the minimum order of elements

G_i is value $\omega(G_i) = q$. It is easy to show that the basis $\{G_1, G_2, \dots, G_\mu\}$ generates $\omega(G_1)\omega(G_2)\dots\omega(G_\mu) \geqslant q^\mu$ different elements of the group Γ_μ. It is evident that $\Omega(\Gamma_\mu) \geqslant \omega(G_1)\omega(G_2)\dots\omega(G_\mu)$. The number of different elements in the group Γ_μ is equal to $\Omega(\Gamma_\mu) = q^\mu$, therefore the last inequality holds, only if all elements of the basis have the minimum possible order q. The last means that all elements of the group, except the unity element, have the same order q.

Suppose the group Γ_μ contains $N_{\Omega'=q}$ different cyclic subgroups. Each of such subgroups contains $q-1$ non-unity elements, therefore $N_{\Omega'=q}(q-1) = q^\mu - 1$ and

$$N_{\Omega'=q} = \frac{q^\mu - 1}{q - 1}. \tag{1}$$

There exist few real examples of such groups. Among vector finite groups we have the example relating to selection of the parameters $m = 2$, $p = 3$, and $\tau = 1$ that define the fourth order group containing three elements (0,1), (2,0), and (0,2) of the second order and the unity elements (1,0). Other example are provided by some subgroups in the groups considered below. It is a typical case that VFGs contains subgroups like Γ_μ. (Among the VFRs defined over the finite polynomial fields $GF(p^d)$, where $d \geqslant 2$, we have some more examples of the VFGs possessing the MDC structure and containing only elements having the same prime order.)

Note that in some group of the order q^d, where q is a prime, the dimension μ of the MDC satisfies the condition $\mu \leqslant d$. Let us consider a hypothetic group $\Gamma_{t\mu}$ of the order $\Omega = q^d$, where $d = t\mu$. Suppose the group $\Gamma_{t\mu}$ contains μ independent elements of the order $\omega = q^t$, composing a basis $\{G_1, G_2, \dots, G_\mu\}$, then we have the following facts.

1. The group $\Gamma_{t\mu}$ contains μ exponentially independent elements of the order $\omega = q^j$ for each of the values $j = 1, 2, \dots t$.

2. For all values $j = 1, 2, \dots t$ the group Γ_t contains $N_{\omega=q^j}$ elements G of the order $\omega(G) = q^j$, which is equal to the value

$$N_{\omega=q^j} = q^{\mu(j-1)}(q^\mu - 1). \tag{2}$$

3. For each of the values $j = 1, 2, \dots t$ the group Γ_t contains $N_{\Omega'=q^j}$ different cyclic subgroups of the order $\Omega' = q^j$, which is equal to the value

$$N_{\Omega'=q^j} = q^{(\mu-1)(j-1)} \frac{q^\mu - 1}{q - 1}. \tag{3}$$

The VFGs provide sufficient number of real examples of groups of the $\Gamma_{t\mu}$ type, which relates to the cases $m = 2, 4, \dots 2^d$ $(d = 1, 2, 3 \dots)$ and primes p having the structure $p = 2^k + 1$ $(k = 4, 8, 16)$. Table 2 presents experimental results.

$m=2;\ p=257;\ \tau=169$		$m=4;\ p=257;\ \tau=81$		$m=8;\ p=17;\ \tau=1$	
ω	N_ω	ω	N_ω	ω	N_ω
2	3	2	15	2	255
4	12	4	240	4	65280
8	48	8	3840	8	16711680
16	192	16	61440	16	4278190080
32	768	32	983040	-	-
64	3072	64	15728640	-	-
128	12288	128	251658240	-	-
256	49152	256	4026531840	-	-

Table 2. Some particular variants of the vector finite groups of order $(p-1)^m$.

3.2. Vector groups having multi-dimension cyclicity structure

Let us consider a hypothetic group Γ of the order $\Omega = \left(\prod_{i=1}^{z} q_i^{t_i}\right)^{\mu}$, where q_i is a prime for all $i \in \{1,2,\ldots z\}$. Suppose for all $i = 1,2,\ldots z$ the group Γ contains μ exponentially independent elements of the order $\omega = q_i^{t_i}$, which compose the basis $\{G_1^{(i)}, G_2^{(i)}, \ldots, G_\mu^{(i)}\}$. Such assumption leads to the following facts.

1. The group Γ contains μ exponentially independent elements of the order $\omega = \prod_{i=1}^{z} q_i^{t_i}$, that generate all of the group elements.

2. The group Γ contains μ exponentially independent elements of the order $\omega = D$, where D is a divisor of the group order.

3. For each divisor D of the group order such that $D = q_i^{t_i'}$, where $i \in \{1,2,\ldots z\}$ and $0 \leqslant t_i' \leqslant t_i$, the group Γ contains the number of elements $N_{\omega=q_i^{t_i'}}$ of the order D, which is equal to

$$N_{\omega=q_i^{t_i'}} = q_i^{\mu(t_i'-1)}(q_i^{\mu}-1). \tag{4}$$

4. For each divisor D of the group order such that $D = \prod_{i=1}^{z'} q_i^{t_i'}$, where $i = 1,2,\ldots z$ and $1 \leqslant t_i' \leqslant t_i$, the group Γ contains the number of elements $N_{\omega=D}$ of the order D, which is equal to

$$N_{\omega=D} = \prod_{i=1}^{z'} q_i^{\mu(t_i'-1)}(q_i^{\mu}-1). \tag{5}$$

5. For each divisor $D|\Omega$ of the group order such that $D = \prod_{i=1}^{z'} q_i^{t_i'}$, where $i = 1,2,\ldots z$ and $1 \leqslant t_i' \leqslant t_i$, the group Γ contains the number $N_{\Omega'=D}$ of cyclic subgroups of the order $\Omega' = D$, which equals to

$$N_{\Omega'=D} = \prod_{i=1}^{z'} q_i^{(\mu-1)(t_i'-1)} \frac{q_i^{\mu}-1}{q_i-1}. \tag{6}$$

Among different types of the multiplicative groups of VFRs the VFGs possessing the MDC structure are more attractive as primitive of the DS algorithms, some other particular types of the non-cyclic VFGs also represent interest for public key cryptography though. In the VFGs possessing the MDC for each prime divisor q_i of the group order Ω there exist subgroups of the orders $\Omega' = \left(q_i^{t'_i}\right)^{\mu}$, where $t'_i = 1, 2, \ldots t_i$, which possess the MDC structure with the same dimension value μ. In particular for some large prime q there exists the q^{μ}-order subgroup all elements of which have the same order q, except the unity element. Such subgroups play important role in the DS algorithms proposed below. Examples confirming the facts and formulas presented above are given in the next section.

4. Experimental confirmation

For values $m = 2$ and $m = 3$ in the case $m|p-1$ it has been theoretically derived [6] the following formula

$$\Omega = (p-1)^m. \tag{7}$$

In all our experiments relating to the case $p > m$ and $m|p-1$ the group order is described with formula (7), if the coefficient τ is the mth power of some element $x \in GF(p)$. To determine the real structure of the VFGs we have computed the order of all elements in the VFGs involved in experiments (multiplying the group elements G many times, the order $\omega(G)$ has been calculated). Experimental results are presented in Table 3. The results are completely described by formulas (4) and (5).

$m = 10;\ p = 11;\ \tau = 1$		$m = 7;\ p = 29;\ \tau = 28$		$m = 6;\ p = 19;\ \tau = 1$	
ω	N_ω	ω	N_ω	ω	N_ω
2	1023	2	127	2	63
5	9765624	4	16256	3	728
10	9990233352	7	823542	6	45864
-	-	14	104589834	9	530712
-	-	28	13387498752	18	33434856

Table 3. Structure of the VFGs possessing the order $\Omega = (p-1)^{\mu}$, where $\mu = m$ (N_ω is the number of the group elements having the order ω).

Thus, performing many different computational experiments in all cases, when τ can be represented as the mth degree of some element of the ground field $GF(p)$ and $m|p-1$, we have get the vector group structure that is described in terms of the MDC with $\mu = m$. The experiments have also revealed different other conditions under which there are formed the VFG possessing the MDC structure described by formula (5). From the results for the case $m|p-1$ the following formula for the VFG order have been derived

$$\Omega = (p^{\nu} - 1)^{\mu}, \tag{8}$$

where μ is the dimension of MDC, $\mu|m$, $\nu = m/\mu$, which describes the VFG structure when the parameter τ is such that the equation $\tau = x^{\mu}$ has solutions in $GF(p)$, and the equation $\tau = x^{\mu\delta}$ has no solutions in $GF(p)$ for each divisor $\delta|\nu$, $\delta > 1$. Examples of the VFGs relating to such cases are presented in Table 4. In the next section formula (8) is used to define the VFGs suitable to implementation of the DS algorithms. In Table 4 the formulas describing the group order Ω for cases $m \leqslant 8$ have been obtained from experiments on finding the order ω for each group element, like experiments used to obtain results of Table 3. For cases $m > 8$ the formulas have been preliminary composed and then experimentally proved.

The cases $\mu = 1$ relates to VFRs that are extension FFs $GF(p)$, when the VFGs are cyclic. Such VFFs are very attractive for application in EC-based DS algorithms [4] due to sufficiently fast multiplication operation and possibility of the efficient parallelization of the vector multiplication. In this paper only non-cyclic VFGs ($\mu \geqslant 2$) are discussed as primitives of the DS algorithms.

$m,\ p,\ \tau$	Ω	μ	$m,\ p,\ \tau$	Ω	μ
10, 11, 4	$(p^5-1)^{\mu}$	2	24, 1201, 729	$(p-1)^{\mu}$	24
10, 11, 10	$(p^2-1)^{\mu}$	5	24, 1201, 49	$(p^2-1)^{\mu}$	12
9, 13, 1	$(p^3-1)^{\mu}$	3	24, 1201, 16	$(p^3-1)^{\mu}$	8
9, 19, 1	$(p-1)^{\mu}$	9	24, 1201, 19	$(p^4-1)^{\mu}$	6
8, 17, 4	$(p^2-1)^{\mu}$	4	24, 1201, 61	$(p^6-1)^{\mu}$	4
8, 5, 4	$(p^4-1)^{\mu}$	2	24, 1201, 23	$(p^8-1)^{\mu}$	3
6, 19, 8	$(p^2-1)^{\mu}$	3	24, 1201, 289	$(p^{12}-1)^{\mu}$	2
6, 19, 16	$(p^3-1)^{\mu}$	2	24, 1201, 101	$(p^{24}-1)^{\mu}$	1
42, 421, 67	$(p-1)^{\mu}$	42	42, 421, 29	$(p^2-1)^{\mu}$	21
42, 421, 277	$(p^3-1)^{\mu}$	14	42, 421, 73	$(p^6-1)^{\mu}$	7
42, 421, 7	$(p^7-1)^{\mu}$	6	42, 421, 19	$(p^{14}-1)^{\mu}$	3
42, 421, 79	$(p^{21}-1)^{\mu}$	2	42, 421, 2	$(p^{42}-1)^{\mu}$	1

Table 4. Analytic description of the experimental results on investigation of the VFG structure (cases $\mu \leqslant m$).

5. Designing the DS algorithms based on the VFGs

In the standard case of the DS algorithm design based on cyclic groups the group order Ω should contain a large prime divisor $q|\Omega$ such that $g \geqslant 2^{160}$ [2, 7]. However taking into account the MDC of the VFG structure it can be shown that for VFGs the standard cryptographic requirement is essentially excessive. If the prime divisor q of the VFG order relates to the MDC subgroup of the order q^{μ}, then the general security requirement can be specified as $q \geqslant 2^{160/\mu}$, where μ is the dimension of the cyclicity of the group structure. However to make use of this essential correction some changes in the design of the DS algorithms should be introduced.

First, the public key is to be generated as μ vectors $Y_1, Y_2, ..., Y_\mu$ in accordance with the following formula

$$Y_i = G_1^{x_{1i}} \circ G_2^{x_{2i}} \cdots \circ G_\mu^{x_{\mu i}} = \prod_{j=1}^{\mu} G_j^{x_{ji}},$$

where $\omega(G_i) = q \ \forall i \in \{1, 2, \ldots, \mu\}$, $G_1, G_2, \ldots G_\mu$ is the generator system of the subgroup having the order q^μ, and the set $\{x_{ji}\}$ is the secret key $(i, j \in \{1, 2, \ldots, \mu\})$. Computation of the secret key defines a problem of finding multi-dimension logarithm at the basis $G_1, G_2, \ldots G_\mu$. This problem can be solved using some modifications of the general-purpose methods for finding discrete logarithms in cyclic groups [2]. The difficulty of such modified methods is $O(\sqrt{q^\mu})$ exponentiation operations in the used VFG, therefore the minimum security (corresponding to difficulty of breaking the DS algorithm, which is equal to 2^{80} exponentiation operations) can be provided with the condition $|p| \approx |q| \geqslant 160/\mu$ bits.

Second, the DS scheme should be modified in accordance with the modified public key. All parts of the public key $(Y_1, Y_2, \ldots, Y_\mu)$ should be used in the DS verification procedure. The following DS schemes takes into account the mentioned modifications.

Generation of the DS corresponding to the message M is performed as follows:

1. Select μ random values $k_1, k_2, \ldots, k_\mu$ such that for all $i = 1, 2, \ldots, \mu$ it holds $k_i < q$.

2. Calculate vector $R = (r_1, r_2, \ldots, r_m) = G_1^{k_1} \circ G_2^{k_2} \cdots \circ G_\mu^{k_\mu}$.

3. Using some specified hash function F_h (different examples see in [2]) calculate the hash value h from the message to which the vector R is concatenated: $h = F_h(M \| r_1 \| r_2 \| \ldots \| r_m)$.

4. Represent the value h as some concatenation of μ elements: $h = h_1 \| h_2 \| ... \| h_\mu$ and compute the second element of the DS as the set of μ values $\{s_1, s_2, \ldots s_\mu\}$:

$$s_j = t_j + \sum_{i=1}^{i=\mu} x_{ji} h_i \bmod q,$$

where $j = 1, 2, \ldots \mu$.

Verification of the DS corresponding to the message M is performed as follows:

1. Compute the vector $R' = Y_1^{-h_1} \circ Y_2^{-h_2} \cdots \circ Y_\mu^{-h_\mu} \circ G_1^{s_1} \circ G_2^{s_2} \cdots \circ G_m^{s_\mu}$.

2. Compute the value $h' = F_h(M \| r'_1 \| r'_2 \| \ldots \| r'_m)$.

3. Compare the values h' and h. If $h' = h$, then the DS is valid.

There are possible different variants of the values m and μ that provide fast generation and verification of the DS, the values $\mu = 2$ (for $m = 2, 6, 10, 14$ and 22) and $\mu = 3$ (for $m = 3, 9, 15$, and 21) are the most interesting for practical applications though. Values $\mu > 3$ lead to comparatively large size of the public key. The values m corresponding to $\mu = 2$ and $\mu = 3$, which are indicated in brackets, provides possibility to select the values p providing faster procedures for DS generation and verification.

Let us consider some particular variants of the DS scheme described above.

Example 1. $m = 6$, $p = 3112656501667$, and $\tau = 32295434991243198100935\,19$. These parameters define formation of the VFG having the order $\Omega = \left(p^5 - 1\right)^\mu$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 322954349912431981009351 9$. The subgroup of the order q^μ is generated by the following pair of the q-order vectors

$G_1 =$
$(2461700031734, 482034324490, 156834270570, 1324447431161, 2740416991343, 1220868764310),$
$G_2 =$
$(2538171306005, 283399862632, 192519072375, 891592729264, 760409728893, 2653262071023).$

Example 2. $m = 10$, $p = 14152871$, and $\tau = 9$. These parameters define formation of the VFG having the order $\Omega = \left(p^5 - 1\right)^\mu$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 80243196241149105837960045\,41$. The subgroup of the order q^μ is generated by the following pair of the q-order vectors

$G_1 =$
$(6283401, 4259768, 6598451, 3709261, 8444571, 82053, 6685050, 10303674, 9996976, 10471343),$
$G_2 =$
$(1523659, 5587678, 3962704, 8694664, 3478222, 2379965, 4305324, 860257, 4524271, 8938870).$

Example 3. $m = 14$, $p = 8093$, and $\tau = 9$. These parameters define formation of the VFG having the order $\Omega = \left(p^7 - 1\right)^\mu$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 40143281293465596069349$. The subgroup of the order q^μ is generated by the following pair of the q-order vectors

$$G_1 = (6324, 3153, 1575, 5913, 3701, 5665, 3268, 5171, 4816, 1661, 1926, 4203, 678, 4187),$$
$$G_2 = (5992, 4360, 4442, 2341, 6950, 2525, 921, 1565, 2120, 3592, 6668, 248, 399, 6214).$$

Example 4. $m = 2$, $p = 6917891042381689626702539$, and $\tau = 2^{32} = 4294967296$. These parameters define formation of the VFG having the order $\Omega = (p-1)^\mu$ and dimension of the cyclicity $\mu = 2$.

The largest prime divisor of Ω is $q = 3458945521190844813351269$. The subgroup of the order q^μ is generated by the following pair of the q-order vectors

$$G_1 = (3, 0), \quad G_2 = (1, 5).$$

Example 5. $m = 3$, $p = 275352871102525507$, and $\tau = 2^{24} = 16777216$. These parameters define formation of the VFG having the order $\Omega = (p-1)^\mu$ and dimension of the cyclicity $\mu = 3$. The largest prime divisor of Ω is $q = 45892145183754251$. The subgroup of the order q^μ is generated by the following three of the q-order vectors

$$G_1 = (21, 0, 0),$$
$$G_2 = (217941963753891151,\ 239089986535147009,\ 109899378481277797),$$
$$G_3 = (158846680700738144,\ 28761476487049241,\ 144620654759850124).$$

Example 6. $m = 4$, $p = 11780627332037$, and $\tau = 2^{24} = 16777216$. These parameters define formation of the VFG having the order $\Omega = (p-1)^\mu$ and dimension of the cyclicity $\mu = 2$. The largest prime divisor of Ω is $q = 2945156833009$. The subgroup of the order q^μ is generated by the following four of the q-order vectors

$G_1 = (17, 0, 0, 0)$,
$G_2 = (872502753155,\ 6114625095567,\ 4745624761713,\ 4690788873292)$,
$G_3 = (11269823703275,\ 5374465446130,\ 6550130852697,\ 7523825764505)$,
$G_4 = (9996654190922,\ 7883587942021,\ 9910063088313,\ 272051995111)$.

The computational difficulty of the DS generation and verification procedures is approximately equal to difficulty of three modulo exponentiation operations like $g^s \bmod n$, where $|s| = \mu|q|$ and $|n| = m|p|$. As it has been shown above in the case $m = \mu$ the characteristic of the field $GF(p)$ can be selected such that $|p| \approx |q| \geqslant 160/\mu$ bits. This provides high performance of the proposed algorithm. Comparison with the performance (in arbitrary unites) of some widely used DS algorithms is presented in Table 6, where the performance is estimated for the size of the DS parameters providing supposed security of 2^{80} group operations.

DS scheme	DL problem in ...	$\|p\|$, bits	Public key size, bits	DS size, bits	Rate, arb. un.
GOST 1994 [10]	$GF(p)$	1024	1024	1024	1
DSA [11]	$GF(p)$	1024	1024	320	3
Shnorr [8]	$GF(p)$	1024	1024	320	3
GOST 2001 [10]	EC	256	512	512	6
ECDSA [11]	EC	160	320	320	10
Proposed ($m = 6$; $\mu = 2$)	VFG	42	512	320	70
Proposed ($m = 10$; $\mu = 2$)	VFG	21	420	320	80
Proposed ($m = \mu = 2$)	VFG	82	328	320	100
Proposed ($m = \mu = 3$)	VFG	56	504	320	100
Proposed ($m = \mu = 4$)	VFG	43	688	320	100

Table 5. Rough performance comparison of different DS schemes based on difficulty of the DL problem (EC denotes elliptic curve defined over $GF(p)$).

6. Conclusion

Using specially introduced BVNTs to define the vector multiplication operation in the finite vector spaces over the finite ground fields leads to formation of the VFRs containing the multiplicative group possessing the MDC structure. The MDC is a common feature for such VFGs. The dimension of the structure cyclicity μ is equal to some divisor of the vector dimension m. Using different values of the expansion coefficient τ that is the flexible parameter of the used BVMT different values μ are assigned. The particular case of the VFFs formation corresponds to value $\mu = 1$.

The VFGs relating to cases $\mu = 2$ and $\mu = 3$ are very attractive as primitives for fast DS algorithms. It has been proposed a DS scheme in which some design features have been applied taking into account the MDC structure of the VFGs.

Several concrete VFGs suitable to application in the frame of the proposed DS scheme have been described. An algorithm for finding two-dimension algorithms has been described and used to estimate the security of the DS algorithms based on computations in FVGs possessing the structure with two-dimension cyclicity. Performance comparison with the known fast DS schemes shows the proposed ones provides significantly higher rate. Besides, the vector multiplication operation suite well to parallelization therefore the propose DS scheme is significantly more efficient in parallelized hardware implementation than other known DS algorithms, especially when the VFGs with sufficiently large value m are applied.

References

[1] **N. Koblitz**, *A course in number theory and cryptography*, Springer-Verlag. Berlin, 2003.

[2] **A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone**, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[3] **A. J. Menezes and S. A. Vanstone**, *Elliptic curve cryptosystems and their implementation*, J. Cryptology **6** (1993), 209 − 224.

[4] **N. A. Moldovyan**, *A method for generating and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008140403. October 14, 2008.

[5] **N. A. Moldovyan and D. N. Moldovyan**, *A method for computing and verifying electronic digital signature certifying an electronic document*, Russian patent application # 2008130759. July 24, 2008.

[6] **N. A. Moldovyan and P. A. Moldovyanu**, *New primitives for digital signature algorithms*, Quasigroups and Related Systems **17** (2009), 271 − 282.

[7] **J. Pieprzyk, Th. Hardjono and J. Seberry**, *Fundamentals of computer security*, Springer-Verlag. Berlin, 2003.

[8] **C. P. Schnorr**, *Efficient signature generation by smart cards*, J. Cryptology **4** (1991), 161 − 174.

[9] **N. Smart**, *Cryptography: an Introduction*, McGraw-Hill Publication, London, 2003.

[10] GOST R 34.10-94 (and GOST R 34.10-2001). Russian Federation Standard. Information Technology. Government Committee of the Russia for Standards.

[11] International Standard ISO/IEC 14888-3:2006(E).

Received January 26, 2009

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, 14 Linya str. 39, St. Petersburg 199178, Russia, E-mail: nmold@mail.ru

Quasigroups and Related Systems **18** (2010), 95 − 104

Topological LA-groups and LA-rings

Tariq Shah and Kamran Yousaf

Abstract. We introduce the notion of topological LA-groups and topological LA-rings which are some generalizations of topological groups and topological rings respectively. We extend some characterizations of topological groups and rings to topological LA-groups and topological LA-rings.

1. Introduction

Kazim and Naseerudin [4] have introduced the concept of *LA-semigroups*, i.e., groupoids whose elements satisfy the *left invertive law*: $(ab)c = (cb)a$. Such groupoids also are known as Abel-Grassmann's groupoids or AG-groupoids (see [2]). Many interesting results on LA-semigroups one can find in [5], [6] and [7]. Some authors studied also *left almost groups* (*LA-groups*), i.e., LA-semigroups in which for every $a \in G$ there exists $e \in G$ such that $ea = a$ and $a^{-1} \in G$ such that $a^{-1}a = e$. LA-rings are studied by T. Shah and I. Rehman (cf. [9]).

In this paper we introduced the notion of topological LA-groups and topological LA-rings. Furthermore we established some of properties regarding products, quotient and subgroups of a topological LA-group. In case of topological LA-ring we prove that the product of any family of topological LA-rings is again a topological LA-ring and an LA-subring of a topological LA-ring is again a topological LA-ring.

2. Preliminaries

A *topological group* is a group $(G, *)$ with a topology τ such that the group operations $G \times G \to G : (x, y) \to x * y$ and $G \to G : x \to x^{-1}$ are continuous

2000 Mathematics Subject Classification: 20M02, 22A05, 22A30
Keywords: LA-group, LA-ring, topological group, topological ring, topological LA-group, topological LA-ring.

or the map $G \times G \to G : (x, y) \to x * y^{-1}$ is continuous. For topological group one may consult [3] and [8].

Definition 2.1. A non empty set G is called a *topological LA-group* if

(a) $(G, *)$ is an LA-group,

(b) (G, τ) is a topological space,

(c) LA-group operation $* : G \times G \to G$ and the inversion function $i : G \to G$ defined by $i(x) = x^{-1}$ are continuous.

The condition (c) can be replaced by

$(c)'$ The mapping $(x, y) \to x * y^{-1}$ of $G \times G$ onto G is continuous.

Example 2.2. Let G be an LA-group. It is easy to verify that the condition (a) is true in the discrete (respectively indiscrete) topology on G. Consequently G is an LA-topological group. In this manner any LA-group may be considered as a topological LA-group in the discrete (respectively indiscrete) topology. □

The following theorem is a generalization of Proposition 3.2 from [3].

Theorem 2.3. *Let G be a topological LA-group. Then*

(1) *the right translation $r_a : x \to xa$ is homeomorphism,*

(2) *the left translation $l_a : x \to ax$ is homeomorphism and*

(3) *the inversion mapping $i : x \to x^{-1}$ is homeomorphism.*

Proof. (1) Let $x = y$. This implies $xa = ya$ which shows that $r_a(x) = r_a(y)$, which shows that r_a is well-defined.

Let $r_a(x) = r_a(y)$. This implies $xa = ya$. Since G is cancellative, so $x = y$, so r_a is one-to-one.

For each $x \in G$ there exist $xa^{-1} \in G$ such that $r_a(xa^{-1}) = (xa^{-1})a = (aa^{-1})x = ex = x$ implies that r_a is onto. Thus r_a is bijective.

Let U be any neighbourhood of $r_a(x) = xa$. Since G is a topological LA-group, so the mapping $* : G \times G \to G$ is continuous and for any neighbourhood U of $r_a(x) = xa$ there exists neighbourhoods V and W of x and a (respectively) such that $V * W \subseteq U$.

Now $r_a(V) = V * a \subseteq V * W$. So, $r_a(V) \subseteq V * W \subseteq U$. Thus $r_a(V) \subseteq U$. Since x is an arbitrary element of G, the mapping r_a is continuous.

Let U be any neighbourhood of $r_a^{-1}(x) = xa^{-1}$. Since G is a topological LA-group, the mapping $* : G \times G \to G$ is continuous. Hence for any neighbourhood U of $r_a^{-1}(x) = xa^{-1}$ there exists neighbourhoods V and W of x and a^{-1} respectively such that $V * W \subseteq U$.

Now as $r_a^{-1}(V) = V * a^{-1} \subseteq V * W$, we have $r_a^{-1}(V) \subseteq V * W \subseteq U$. Thus $r_a^{-1}(V) \subseteq U$. As x is an arbitrary element of G, the mapping r_a^{-1} is continuous. Hence r_a is a homeomorphism.

(2) The proof is analogous to (1).

(3) Let $i(x) = i(y)$. Then $x^{-1} = y^{-1}$. Now $e = yy^{-1} = yx^{-1}$, which implies $ex = (yx^{-1})x$ and therefore by left invertive law we have $x = (xx^{-1})y = ey = y$ and hence i is one-to-one.

For each $x \in G$ there exist $x^{-1} \in G$ such that $i(x^{-1}) = (x^{-1})^{-1} = x$, so i is onto.

Since G is a topological LA-group, i is continuous. Also $i^{-1}(x) = x^{-1}$ is continuous because i is one-to-one. □

Remark 2.4. The mappings $x \mapsto a(xa^{-1})$, $x \mapsto a^{-1}(xa)$, $x \mapsto (ax)a^{-1}$, $x \mapsto (a^{-1}x)a$ are homeomorphisms as composition of two homeomorphisms $x \mapsto xa(xa^{-1})$ and $x \mapsto ax(a^{-1}x)$.

Remark 2.5. In topological groups we obtain only one homeomorphism axa^{-1}, but in the case of topological LA-groups we obtain distinct homeomorphisms $a(xa^{-1})$, $a^{-1}(xa)$, $(ax)a^{-1}$ etc.

Corollary 2.6. *Let E be open and F be closed in a topological LA-group G and A be any subset of G. Then for $a \in G$*

(1) *aE, Ea, E^{-1} are open,*

(2) *aF, Fa, F^{-1} are closed and AE, EA are open.*

Proof. The mappings in Theorem2.3 are homeomorphisms, so (1) is obvious.

Since $AE = \cup_{a \in A} aE$, $EA = \cup_{a \in A} Ea$, and the union of open sets is open, therefore (2) is established. □

3. Topological LA-groups

In this section we define topological LA-groups and give some characterizations of such LA-groups.

3.1. Construction of a new topological LA-group from old

We can always construct a new topological LA-group from old ones. A product of topological LA-groups permits us the construction of a new topological LA-group from the given ones and also permits the reduction of the study of relatively complicated topological LA-groups to the investigation of their simple constituents.

The following theorem is a generalization of Proposition 3.12 from [3].

Theorem 3.1. *Let A be an index set. For each $\alpha \in A$, let G_α be a topological LA-group. Then $G = \prod\limits_{\alpha \in A} G_\alpha$ endow with product topology, is also a topological LA-group.*

Proof. To prove that G is a topological LA-group, we have to show that the onto mapping $* : G \times G \to G$; $(x, y) \mapsto xy^{-1}$ is continuous.

Let W be a neighbourhood of xy^{-1} in G, then there exists an open set U such that $xy^{-1} \in U \subseteq W$, where $U = \prod_{\alpha \in A} U_\alpha$ with U_α is an open neighbourhood of $x_\alpha y_\alpha^{-1}$ in G_α. Since $(x_\alpha, y_\alpha) \mapsto x_\alpha y_\alpha^{-1}$ is continuous for each $\alpha \in A$, so there exists neighbourhoods V_{α_i}, $V_{\alpha_i}'^{-1}$ of x_{α_i} and y_{α_i} respectively such that $V_{\alpha_i} V_{\alpha_i}'^{-1} \subseteq U_{\alpha_i}$for each $1 \leqslant i \leqslant n$. Now let $V = \prod\limits_{\alpha \in A} V_\alpha$ and $V' = \prod\limits_{\alpha \in A} V_\alpha'$, then V and V' are neighbourhoods of x and y respectively. This means $VV'^{-1} = \prod(V_{\alpha_i} V_{\alpha_i}'^{-1}) \subseteq \prod U_\alpha = U \subseteq W$. This proves the theorem. □

Now we give the following definition.

Definition 3.2. Let G be a topological LA-group and H be an LA-subgroup of G. Then H endow with relative topology, is a topological LA-group called *topological LA-subgroup* of G.

Theorem 3.3. *An LA-subgroup H of a topological LA-group G is a topological LA-subgroup.*

Proof. Let G be a topological LA-group and H be an LA-subgroup of G. Then H is endowed with relative topology induced from G. Since the mapping $(x, y) \mapsto xy^{-1}$ of $G \times G$ onto G is continuous, so its restriction from $H \times H$ onto H is also continuous. Let a, b be two elements of H and let $ab^{-1} = c$. Every neighbourhood W' of the element c in H can be obtained as the intersection with H of some neighbourhood W of c in G, i.e., $W' = H \cap W$. Since G is a topological LA-group, so there exists neighbourhoods U and V of a, b such that $UV^{-1} \subseteq W$. Now $U' = H \cap U$ and $V' = H \cap V$ are the relative neighbourhoods of a and b in H. Thus we have $U'V'^{-1} \subseteq W$ and also $U'V'^{-1} \subseteq H$. Hence $U'V'^{-1} \subseteq W'$ and H is a topological LA-subgroup. □

3.2. Topological factor LA-groups

Let G be a topological LA-group and H is an LA-subgroup of G. Then G/H denotes the set of all cosets Ha, $a \in G$. Let φ be a canonical mapping of G onto G/H. With the help of φ we can define a topology on G/H as follows: A subset A' of G/H is open if and only if $\varphi^{-1}(A')$ is an open subset of G. This topology in G/H is called the *quotient topology* and G/H, endowed with quotient topology, is called the *quotient space*.

The following theorem is a generalization of Proposition 3.8 from [3].

Theorem 3.4. *Let G be a topological LA-group and H be an LA-subgroup of G. Let G/H be the quotient space endowed with the quotient topology and φ be the canonical mapping of G onto G/H, then*

(1) *φ is homomorphism,*
(2) *φ is continuous,*
(3) *φ is open.*

Proof. (1) Let $x, y \in G$, then $\varphi(xy) = H(xy) = (HH)(xy) = (Hx)(Hy) = \varphi(x)\varphi(y)$.

(2) φ is continuous by the definition of quotient topology.

(3) Let U be open in G. We have to prove that $\varphi(U)$ is open in G/H. That is, $\varphi^{-1}(\varphi(U))$ is open in G. But $\varphi^{-1}(\varphi(U)) = \{g : g \in uH$ for some $u \in U\} = UH$, which is open. Hence φ is open. □

The following theorem is a generalization of Proposition 3.10(ii) from [3].

Theorem 3.5. *Let G be a topological LA-group and H be an LA-subgroup of G. Then G/H endowed with the quotient topology, is a topological LA-group.*

Proof. To prove that G/H is a topological LA-group we have to show that the mapping $* : (x', y') \to x'y'^{-1}$ of $G/H \times G/H$ onto G/H is continuous.

Let W be an open neighbourhood of $x'y'^{-1}$, where $x' = xH$ and $y' = yH$ and $x, y \in G$. Clearly $\varphi^{-1}(W)$ is open in G and $x'y'^{-1} \in \varphi^{-1}(W)$.

Since G is a topological LA-group, so there exists open sets U and V such that $x \in U$, $y^{-1} \in V^{-1}$ and $xy^{-1} \in UV^{-1} \subseteq \varphi^{-1}(W)$. Since by Theorem 3.4 φ is continuous and open homomorphism so $x'y'^{-1} \in \varphi(U)(\varphi(V))^{-1} \subset \varphi(\varphi^{-1}(W))$, which implies $x'y'^{-1} \in \varphi(U)(\varphi(V))^{-1} \subset W$.

As by theorem 3.4 φ is open, so $\varphi(U)$ and $\varphi((V))^{-1} = \varphi(V^{-1})$ are open because U and V are open. Thus G/H is a topological LA-group. □

Definition 3.6. A topological LA-group G is said to be *homogeneous* if for all x, $y \in G$, there exists a homeomorphism $f : G \to G$ such that $f(x) = y$.

The following theorem is a generalization of Proposition 3.14 from [3].

Theorem 3.7. *Let G be a topological LA group and H be a subgroup of G. Then the topological LA-group G/H is a homogeneous space.*

Proof. Let $x' = Hx$, $y' = Hy$ and $g \in G$ be such that $g = yx^{-1}$. Define the mapping $f_g : x' = Hx \mapsto H(gx)$ for all $x' \in G/H$.

Let $Hx = Hy$, then $g(Hx) = g(Hy)$ implies $H(gx) = H(gy)$ and hence $f_g(Hx) = f_g(Hy)$. Thus the mapping is well-defined.

Let $f_g(Hx) = f_g(Hy)$. Then $H(gx) = H(gy)$ and $g(Hx) = g(Hy)$. Hence $Hx = Hy$ and so f_g is one-to-one.

For each $x' = Hx \in G/H$ there exists $H\{(g^{-1}e)x\} \in G/H$ such that

$$\begin{aligned} f_g(H\{(g^{-1}e)x\}) &= H\{g((g^{-1}e)x)\} = H\{g((xe)g^{-1})\} \\ &= H\{(xe)gg^{-1}\} = H\{(xe)e\} = H\{(ee)x\} = Hx, \end{aligned}$$

which shows that f_g is onto.

Let U be any neighbourhood of $f_g(Hx) = H(gx)$. Since G/H is a topological LA-group, so the mapping $* : G/H \times G/H \to G/H$ is continuous and thus for any neighbourhood U of $f_g(x) = H(gx) = Hg * Hx$ there exists neighbourhoods V and W of Hg and Hx respectively such that $V * W \subseteq U$.

Now $f_g(V) = f_g(HS) = H(gS)$, so $f_g(V) = Hg * HS$ implies $f_g(V) \subseteq W * V \subseteq U$. As x is an arbitrary element of G, we see that f_g is continuous.

Now let U be any neighbourhood of $f_g^{-1}(Hx) = H(g^{-1}e)x = H(g^{-1}e) * Hx$. Since G/H is a topological LA-group, so for any neighbourhood U of $f_g^{-1}(Hx)$ there exists neighbourhoods V and W of $H(g^{-1}e)$ and Hx respectively such that $V * W \subseteq U$.

Now $f_g^{-1}(W) = f_g^{-1}(HS)$ so $f_g^{-1}(W) = H\{(g^{-1}e)S\}$ implies $f_g^{-1}(W) = H(g^{-1}e) * HS$ and this means $f_g^{-1}(W) \subseteq V * W \Rightarrow f_g^{-1}(W) \subseteq V * W \subseteq U$. Hence $f_g^{-1}(W) \subseteq U$ and therefore f_g^{-1} is continuous. Thus we concluded that f_g^{-1} is a homeomorphism.

Clearly

$f_g(x') = f_g(Hx) = H(gx) = H((yx^{-1})x) = H((xx^{-1})y) = Hy = y'$,

which shows that G/H is a homogeneous space. □

The following theorem is a generalization of Proposition 3.4 from [3].

Theorem 3.8. *For a topological LA-group G, the following statements are equivalent:*

(1) *G is a T_0-space,*

(2) *G is a T_1-space,*

(3) *G is a T_2-space,*

(4) *$\cap U = \{e\}$,where U is a fundamental system of neighbourhood of the identity e.*

Proof. (1) $\Rightarrow$ (2) Let $x, y \in G$, $x \neq y$. (1) implies that for at least one of x and y, there exists an open neighbourhood P of x such that $y \notin P$. Since $x \in P$, so $xx^{-1} \in Px^{-1}$, i.e., $e \in Px^{-1}$ and $Px^{-1} = V$ is an open neighbourhood of e.

Now $V \cap V^{-1} = Q$ is an open symmetric neighbourhood of e, so $e \in Q$, which implies $ey \in Qy$. Hence $y \in Qy$. Now $x \notin Qy$ because if $x \in Qy$ then $x^{-1} \in y^{-1}Q$ $(Q = Q^{-1})$ and $x^{-1} \in y^{-1}Q \subset y^{-1}V\ x^{-1} \subset y^{-1}(Px^{-1}) = P(y^{-1}x^{-1})$ but this implies that

$$e = x^{-1}x \in (P(y^{-1}x^{-1}))x = (y^{-1}x^{-1})(Px).$$

Thus, by medial law,

$$e \in (y^{-1}P)(x^{-1}x) = (y^{-1}P)e = (eP)y^{-1} = Py^{-1}.$$

Hence,

$$y = ey \in (Py^{-1})y = (yy^{-1})P = eP = P,$$

which is a contradiction.

(2) $\Rightarrow$ (3) Let $x, y \in G$, $x \neq y$. By (2) G is a T_1-space, so $\{x\}$ is a closed set and therefore $P = G \backslash \{x\}$ is an open neighbourhood of y, thus $y \in P$, which implies $y^{-1}y \in y^{-1}P$, this means $e \in y^{-1}P$ and hence $y^{-1}P$ is an open neighbourhood of e by Theorem 2.3.

Let V be an open neighbourhood of e such that $VV^{-1} \subset y^{-1}P$. Then Vy is an open neighbourhood of y. Let $Q = G \backslash \overline{Vy}$, an open set and $x \in Q$.

Otherwise $x \in \overline{Vy}$ and hence by the definition of closure $Vy \cap Vx \neq \emptyset$.

But this shows that $x \in (ye)(VV^{-1}) \subset (ye)(y^{-1}P)$, which implies that $x \in (yy^{-1})(eP) = eP$ and hence $x \in P$, a contradiction. Clearly $Q \cap Vy = \emptyset$ gives $y \in Vy$ and so $x \in Q$. This proves (3).

(3) $\Rightarrow$ (4) Let $x \in U$ for each U in $\{U\}$ and assume $x \neq e$. Then (3) shows that there exists a neighbourhood P of e such that $x \notin P$. But then there exists a U in $\{U\}$ such that $U \subset P$. We have a contradiction that $x \in U \subset P$ and $x \notin P$. Hence $x = e$ and (4) is satisfied.

(4) $\Rightarrow$ (1) Let $x \neq y$. Then $xy^{-1} \neq e$ and hence by (4) there exists a U in $\{U\}$ such that $xy^{-1} \notin U$. Thus Uy being a neighbourhood of y and $x \notin Uy$. This proves (1). $\square$

4. Topological LA-rings

The following definition of a topological ring is taken from [1].

Definition 4.1. A *topological ring* is a ring R with a topology τ such that the additive group of the ring R is topological group in topology τ and the one of the following equivalent conditions is satisfied:

(a) the maps $R \times R \to R : (x, y) \to xy$ is continuous, (multiplication condition (MC)),

(b) for any two elements $x, y \in R$ and arbitrary neighborhood U of the element xy there exist neighborhoods V and W of elements x and y respectively such that $VW \subset U$.

Definition 4.2. An LA-ring $(R, +, \cdot$ is called a *topological LA-ring* if

(a) $(R, +)$ is an LA-group,

(b) (R, τ) is a topological space,

(c) the algebraic operations defined in R are continuous in topological space R, i.e., the mappings $(a, b) \to a - b$ and $(a, b) \to a \cdot b$ of the topological space $R \times R$ to the topological space R are continuous. In greater detail: for arbitrary elements $a, b \in R$ and for arbitrary neighbourhoods W and W' of the elements $a - b$ and ab respectively, there exist neighbourhoods U and V of a and b such that $U - V \subset W$ and $UV \subset W'$.

Example 4.3. By the virtue of above definition the additive LA-group of any topological LA-ring is a topological LA-group. Conversely, if R is a topological LA-group, then R could be transformed into the LA-ring by the definition of zero multiplication on R, i.e., setting $a.b = 0$ for any $a, b \in R$. In doing so, the condition (MC) is fulfilled, and hence R is transformed into a topological LA-ring. In this manner every LA-group may be considered as a topological LA-ring with zero multiplication.

Theorem 4.4. *Let R be a topological LA-ring, then for each $r \in R$, the functions $\phi_r : x \to rx$ and $\psi_r : x \to xr$ are continuous from R to R.*

Proof. Let U be any neighbourhood of $\varphi_r(x) = xr$. Since R is a topological LA-ring so the mapping $* : R \times R \to R$ is continuous so for any neighbourhood U of $\varphi_r(x) = xr$ there exists neighbourhoods V and W of x and r respectively such that $V * W \subseteq U$

Now

$$\varphi_r(V) = V * r \subseteq V * W \subseteq U.$$

As x is an arbitrary element of R, so φ_r is continuous.

Similarly we can prove theorem for ψ_r. $\square$

Theorem 4.5. *Let A be an index set. For each $\alpha \in A$, let R_α be a topological LA-ring. Then $R = \prod\limits_{\alpha \in A} R_\alpha$ endow with the product topology, is also a topological LA-ring.*

Proof. As R is a LA-ring so $(R, +)$ is a topological group, so $* : (x, y) \to x - y$ is continuous. We have to check the continuity of : $(x, y) \to xy$ only.

Let W be a neighbourhood of xy in R, then there exists an open set U such that $xy \in U \subseteq W$, where $U = \prod_{\alpha \in A} U_\alpha$ and U_α is an open neighbourhood of $x_\alpha y_\alpha$ in R_α. Since $(x_\alpha, y_\alpha) \to x_\alpha y_\alpha$ is continuous for each $\alpha \in A$, so there exists neighbourhoods $V_{\alpha_i}, V'^{-1}_{\alpha_i}$of x_{α_i} and y_{α_i} respectively such that $V_{\alpha_i} V'^{-1}_{\alpha_i} \subseteq U_{\alpha_i}$ for each $i = 1, 2, \ldots, n$. Now let $V = \prod\limits_{\alpha \in A} V_\alpha$ and $V' = \prod\limits_{\alpha \in A} V'_\alpha$, then V and V' are neighbourhoods of x, y respectively. This implies $VV'^{-1} = \prod (V_{\alpha_i} V'^{-1}_{\alpha_i}) \subseteq \prod U_\alpha = U \subseteq W$. This proves the theorem. $\square$

We finish our work by the following

Theorem 4.6. *An LA-subring S of a topological LA-ring R is a topological LA-subring.*

Proof. Let R be a topological LA-ring and S be an algebraic LA-subring of R. Then S is endowed with relative topology induced from R. Since the mappings : $(x, y) \to x - y$ and $(x, y) \to xy$ of $R \times R$ are continuous so their restriction from $S \times S$ into S is also continuous.

Let a, b be two elements of S and let $ab^{-1} = c$. Every neighbourhood W' of the element c in H can be obtained as the intersection with S of some neighbourhood W of c in G. i.e., $W' = H \cap W$. Since R is a topological LA-ring so there exists neighbourhoods U and V of a, b such that $UV^{-1} \subseteq W$. Now $U' = S \cap U$ and $V' = S \cap V$ are the relative neighbourhoods of a and b in S. Thus we have $U'{V'}^{-1} \subseteq W$ and also $U'{V'}^{-1} \subseteq H$. Hence $U'{V'}^{-1} \subseteq W'$. Hence S is a topological LA-subring. $\square$

References

[1] **V. I. Arnautov, S. T. Glavatsky and A. V. Mikhalev**, *Introduction to the theory of topological rings and modules*, Marcel Dekker, New York, 1996.

[2] **P. Holgate**, *Groupoids satisfying a simple invertive law*, Math. Stud. **61** (1992), 101 – 106.

[3] **T. Hussain:**, *Introduction to topological groups*, W. B. Saunders Company, 1966.

[4] **M. A. Kazim and M. Naseerudin**, *On almost semigroups*, Alig. Bull. Math. **2** (1972), 1 – 7.

[5] **Q. Mushtaq and Q. Iqbal**, *Decomposition of a locally associative LA-semigroups*, Semigroup Forum **41** (1991), 155 – 64.

[6] **Q. Mushtaq and M. S. Kamran**, *On LA-semigroup with weak associative law*, Scientific Khyber. **1** (1989), 69 – 71.

[7] **Q. Mushtaq and S. M. Yusuf:**, *On LA-semigroups*, Alig. Bull. Math. **8** (1978), 65 – 70.

[8] **L. Pontrjagin**, *Topological groups*, Princeton University Press, 1946.

[9] **T. Shah and I. Rehman**, *On LA-rings of finitely nonzero functions*, Int. J. Contemp. Math. Sci. **5** (2010), 209 – 222.

Received April 14, 2010

Department of Mathematics
Quaid-i-Azam University
Islamabad
Pakistan
E-mail: stariqshah@gmail.com, kamranmaths@gmail.com