ISSN 1592-7415 **eISSN 2282-8214**

Volume n. 34 – 2018

RATIO MATHEMATICA

Journal of Mathematics, Statistics, and Applications

Publisher
A.P.A.V.
Accademia Piceno – Aprutina dei Velati in Teramo
www.eiris.it – www.apav.it
apavsegreteria@gmail.com

RATIO MATHEMATICA

Journal of Mathematics, Statistics, and Applications

ISSN 1592-7415 - eISSN 2282-8214

Ratio Mathematica is an **International, double peer-reviewed, open access journal, published every six months** (June-December).

The main topics of interest for Ratio Mathematica are:

Foundations of Mathematics: Epistemology of Mathematics, Critique of the Foundations of Mathematics, Elementary Mathematics from a higher point of view, Elementary Theory of Numbers, Foundations of Mathematics of Uncertain; Criticism of the Foundations of Computer Science.

Applications of Mathematics: Applications to Engineering and Economics, Applications for Management and Business Administration, Decision making in conditions of uncertainty, Theory of Games, Fuzzy Logic and Applications, Probability, Statistics and Applications.

New theories and applications: Algebraic hyperstructures and Applications, Discrete Mathematics and Applications, Fuzzy structures.

New theories and practices for dissemination and communication of mathematics: Communication of History and Foundations, Communication of Discrete Mathematics, Communication of Probability and Statistics, Communication with Media.

Note on Peer-Review
All manuscripts are subjected to a double-blind review process. The reviewers are selected from the editorial board, but they also can be external subjects. The journal's policies are described at: http://eiris.it/ojs/index.php/ratiomathematica/about/submissions#authorGuidelines

Publisher: **APAV** - Accademia Piceno-Aprutina dei Velati in Teramo
Tax Code 92036140678, **Vat Id. Number** 02184450688
Registered Office Address: via del Concilio, 24 - 65121 Pescara
Operational Office: via Chiarini, 191 - 65126 Pescara

EDITORIAL BOARD OF RATIO MATHEMATICA

Ratio Mathematica
Vol. 34, 2018, pp. 5–13

ISSN: 1592-7415
eISSN: 2282-8214

Sums of Generalized Harmonic Series with Periodically Repeated Numerators (a, b) and (a, a, b, b)

Radovan Potůček*

Received: 01-15-2018. **Accepted**: 05-04-2018. **Published**: 30-06-2018.

doi:10.23755/rm.v34i0.405

Abstract

This paper deals with certain generalization of the alternating harmonic series – the generalized convergent harmonic series with periodically repeated numerators (a, b) and (a, a, b, b). Firstly, we find out the value of the numerators b of the first series, for which the series converges, and determine the formula for the sum $s(a)$ of this series. Then we determine the value of the numerators b of the second series, for which this series converges, and derive the formula for the sum $s(a, a)$ of this second series. Finally, we verify these analytically obtained results and compute the sums of these series by using the computer algebra system Maple 16 and its basic programming language.

Keywords: harmonic series, alternating harmonic series, sequence of partial sums, computer algebra system Maple.
2010 AMS subject classifications: 40A05, 65B10.

*Department of Mathematics and Physics, Faculty of Military Technology, University of Defence in Brno, Brno, Czech Republic; Radovan.Potucek@unob.cz

1 Introduction

Let us recall the basic terms, concepts and notions. For any sequence $\{a_k\}$ of numbers the associated *series* is defined as the sum $\sum_{k=1}^{\infty} a_k = a_1 + a_2 + a_3 + \cdots$.

The *sequence of partial sums* $\{s_n\}$ associated to a series $\sum_{k=1}^{\infty} a_k$ is defined for each n as the sum of the sequence $\{a_k\}$ from a_1 to a_n, i.e. $s_n = a_1 + a_2 + \cdots + a_n$.

The series $\sum_{k=1}^{\infty} a_k$ *converges* to a limit s if and only if the sequence of partial sums $\{s_n\}$ converges to s, i.e. $\lim_{n\to\infty} s_n = s$. We say that the series $\sum_{k=1}^{\infty} a_k$ has a *sum* s and write $\sum_{k=1}^{\infty} a_k = s$.

The *harmonic series* is the sum of reciprocals of all natural numbers (except zero), so this is the series

$$\sum_{k=1}^{\infty} \frac{1}{k} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} + \cdots .$$

The divergence of this series can be easily proved e.g. by using the integral test or the comparison test of convergence.

In this paper we will deal with the series of the form

$$\sum_{k=1}^{\infty} \left(\frac{a}{2k-1} + \frac{b}{2k} \right) \quad \text{and} \quad \sum_{k=1}^{\infty} \left(\frac{a}{4k-3} + \frac{a}{4k-2} + \frac{b}{4k-1} + \frac{b}{4k} \right),$$

where a, b are such numbers that these series converge.

If we know, these two types of infinite series has not yet been studied in the literature. The author has previously in the papers [1], [2], and [3] dealt with the series of the form

$$\sum_{k=1}^{\infty} \left(\frac{1}{2k-1} + \frac{a}{2k} \right), \quad \sum_{k=1}^{\infty} \left(\frac{1}{3k-2} + \frac{1}{3k-1} + \frac{a}{3k} \right),$$

$$\sum_{k=1}^{\infty} \left(\frac{1}{3k-2} + \frac{a}{3k-1} + \frac{b}{3k} \right), \text{ and } \sum_{k=1}^{\infty} \left(\frac{1}{4k-3} + \frac{a}{4k-2} + \frac{b}{4k-1} + \frac{c}{4k} \right),$$

so that this contribution is a free follow-up to these three papers. Let us note that in the previous issues of Ratio Mathematica, for example, papers [4] and [5] also deal with the topic infinite series and their convergence.

2 The sum of generalized harmonic series with periodically repeated numerators (a, b)

We deal with the numerical series of the form

$$\sum_{k=1}^{\infty}\left(\frac{a}{2k-1}+\frac{b}{2k}\right)=\frac{a}{1}+\frac{b}{2}+\frac{a}{3}+\frac{b}{4}+\frac{a}{5}+\frac{b}{6}+\cdots, \tag{1}$$

where $a, b \in \mathbb{R}$ are appropriate constants for which the series (1) converges. This series we shall call *generalized harmonic series with periodically repeated numerators* (a, b). We determine the value of the numerators b, for which the series (1) converges, and the sum $s(a)$ of this series.

The power series corresponding to the series (1) has evidently the form

$$\sum_{k=1}^{\infty}\left(\frac{ax^{2k-1}}{2k-1}+\frac{bx^{2k}}{2k}\right)=\frac{ax}{1}+\frac{bx^2}{2}+\frac{ax^3}{3}+\frac{bx^4}{4}+\frac{ax^5}{5}+\frac{bx^6}{6}+\cdots. \tag{2}$$

We denote its sum by $s(x)$. The series (2) is for $x \in (-1, 1)$ absolutely convergent, so we can rearrange it and rewrite it in the form

$$s(x)=a\sum_{k=1}^{\infty}\frac{x^{2k-1}}{2k-1}+b\sum_{k=1}^{\infty}\frac{x^{2k}}{2k}. \tag{3}$$

If we differentiate the series (3) term-by-term, where $x \in (-1, 1)$, we get

$$s'(x)=a\sum_{k=1}^{\infty}x^{2k-2}+b\sum_{k=1}^{\infty}x^{2k-1}. \tag{4}$$

After reindexing and fine arrangement the series (4) for $x \in (-1, 1)$ we obtain

$$s'(x)=a\sum_{k=0}^{\infty}x^{2k}+bx\sum_{k=0}^{\infty}x^{2k},$$

that is

$$s'(x)=(a+bx)\sum_{k=0}^{\infty}\left(x^2\right)^k. \tag{5}$$

When we summate the convergent geometric series on the right-hand side of (5) with the first term 1 and the ratio x^2, where $\left|x^2\right|<1$, i.e. for $x \in (-1, 1)$, we get

$$s'(x)=\frac{a+bx}{1-x^2}\,.$$

We convert this fraction using the CAS Maple 16 to partial fractions and get

$$s'(x) = \frac{a-b}{2(x+1)} - \frac{a+b}{2(x-1)} = \frac{a-b}{2(1+x)} + \frac{a+b}{2(1-x)}\,,$$

where $x \in (-1,1)$. The sum $s(x)$ of the series (2) we obtain by integration in the form

$$s(x) = \int\left(\frac{a-b}{2(1+x)} + \frac{a+b}{2(1-x)}\right)\mathrm{d}x = \frac{a-b}{2}\ln(1+x) - \frac{a+b}{2}\ln(1-x) + C.$$

From the condition $s(0) = 0$ we obtain $C = 0$, hence

$$s(x) = \frac{a-b}{2}\ln(1+x) - \frac{a+b}{2}\ln(1-x)\,. \tag{6}$$

Now, we will deal with the convergence of the series (2) in the right point $x = 1$. After substitution $x = 1$ to the power series (2) – it can be done by the extended version of Abel's theorem (see [6], p. 23) – we get the numerical series (1). By the integral test we can prove that the series (1) converges if and only if $b + a = 0$. After simplification the equation (6), where $b = -a$, we have

$$s(x) = \frac{a+a}{2}\ln(1+x) = a\ln(1+x)\,.$$

For $x = 1$ and after re-mark $s(1)$ as $s(a)$, we obtain a very simple formula

$$s(a) = a\ln 2\,, \tag{7}$$

which is consistent with the well-known fact that the sum of the *alternating harmonic series* $\displaystyle\sum_{k=1}^{\infty}\frac{(-1)^{k+1}}{k} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \cdots$ is equal to $\ln 2$.

3 The sum of generalized harmonic series with periodically repeated numerators (a, a, b, b)

Now, we deal with the numerical series of the form

$$\sum_{k=1}^{\infty}\left(\frac{a}{4k-3} + \frac{a}{4k-2} + \frac{b}{4k-1} + \frac{b}{4k}\right) = \frac{a}{1} + \frac{a}{2} + \frac{b}{3} + \frac{b}{4} + \cdots\,, \tag{8}$$

where $a, b \in \mathbb{R}$ are appropriate constants for which the series (8) converges. This series we shall call *generalized harmonic series with periodically repeated numerators* (a, a, b, b). We determine the value of the numerators b, for which the series (8) converges, and the sum $s(a, a)$ of this series.

The power series corresponding to the series (8) has evidently the form

$$\sum_{k=1}^{\infty}\left(\frac{ax^{4k-3}}{4k-3}+\frac{ax^{4k-2}}{4k-2}+\frac{bx^{4k-1}}{4k-1}+\frac{bx^{4k}}{4k}\right)=\frac{ax}{1}+\frac{ax^2}{2}+\frac{bx^3}{3}+\frac{bx^4}{4}+\cdots. \quad (9)$$

We denote its sum by $s(x)$. The series (9) is for $x\in(-1,1)$ absolutely convergent, so we can rearrange it and rewrite it in the form

$$s(x)=a\sum_{k=1}^{\infty}\frac{x^{4k-3}}{4k-3}+a\sum_{k=1}^{\infty}\frac{x^{4k-2}}{4k-2}+b\sum_{k=1}^{\infty}\frac{x^{4k-1}}{4k-1}+b\sum_{k=1}^{\infty}\frac{x^{4k}}{4k}. \quad (10)$$

If we differentiate the series (10) term-by-term, where $x\in(-1,1)$, we get

$$s'(x)=a\sum_{k=1}^{\infty}x^{4k-4}+a\sum_{k=1}^{\infty}x^{4k-3}+b\sum_{k=1}^{\infty}x^{4k-2}+b\sum_{k=1}^{\infty}x^{4k-1}. \quad (11)$$

After reindexing and fine arrangement the series (11) for $x\in(-1,1)$ we obtain

$$s'(x)=a\sum_{k=0}^{\infty}x^{4k}+ax\sum_{k=0}^{\infty}x^{4k}+bx^2\sum_{k=0}^{\infty}x^{4k}+bx^3\sum_{k=0}^{\infty}x^{4k},$$

that is

$$s'(x)=(a+ax+bx^2+bx^3)\sum_{k=0}^{\infty}\left(x^4\right)^k. \quad (12)$$

After summation the convergent geometric series on the right-hand side of (12) with the first term 1 and the ratio x^4, where $\left|x^4\right|<1$, i.e. for $x\in(-1,1)$, we get

$$s'(x)=\frac{a+ax+bx^2+bx^3}{1-x^4}=\frac{(a+bx^2)(1+x)}{(1+x^2)(1-x)(1+x)}=\frac{a+bx^2}{(1+x^2)(1-x)}.$$

We convert this fraction using the CAS Maple 16 to partial fractions and get

$$s'(x)=\frac{a+b}{2(1-x)}+\frac{a-b+ax-bx}{2(1+x^2)},$$

where $x\in(-1,1)$. The sum $s(x)$ of the series (9) we obtain by integration:

$$s(x)=\int\left(\frac{a+b}{2(1-x)}+\frac{a-b}{2(1+x^2)}+\frac{(a-b)x}{2(1+x^2)}\right)\mathrm{d}x\ =$$

$$=-\frac{a+b}{2}\ln(1-x)+\frac{a-b}{2}\arctan x+\frac{a-b}{4}\ln(1+x^2)+C.$$

From the condition $s(0) = 0$ we obtain $C = 0$, hence

$$s(x) = -\frac{a+b}{2}\ln(1-x) + \frac{a-b}{2}\arctan x + \frac{a-b}{4}\ln(1+x^2). \qquad (13)$$

Now, we will deal with the convergence of the series (9) in the right point $x = 1$. After substitution $x = 1$ to the power series (9) we get the numerical series (8). By the integral test we can prove that the series (8) converges if and only if $a + b = 0$. After simplification the equation (13), where $b = -a$, we have

$$s(x) = a\arctan x + \frac{a}{2}\ln(1+x^2) = \frac{a}{2}\big[2\arctan x + \ln(1+x^2)\big].$$

For $x = 1$ and after re-mark $s(1)$ as $s(a, a)$, we obtain a simple formula

$$s(a, a) = \frac{a}{4}(\pi + 2\ln 2)\,. \qquad (14)$$

4 Numerical verification

We have solved the problem to determine the sums $s(a)$ and (a, a) above of the convergent numerical series (1) and (8) for several values of a (and for $b = -a$) by using the basic programming language of the computer algebra system Maple 16. They were used two following very simple procedures `sumab` and `sumaabb`:

```
sumab=proc(t,a)
   local r,k,s; s:=0; r:=0;
   for k from 1 to t do
       r:=a*(1/(2*k-1) - 1/(2*k)); s:=s+r;
   end do;
   print("s(",a,")=",evalf[9](s),
       "f=",evalf[9](a*ln(2)));
end proc:
sumaabb:=proc(t,a)
   local r,k,s; s:=0; r:=0;
   for k from 1 to t do
       r:=a*(1/(4*k-3) + 1/(4*k-2) - 1/(4*k-1) - 1/(4*k));
       s:=s+r;
   end do;
   print("s(",a,a,")=",evalf[9](s),
       "f=",evalf[9](a*(Pi+2*ln(2))/4);
end proc:
```

For evaluation the sums $s(10^6, a)$ and $s(10^6, a, a)$ and the corresponding values $s(a)$ and $s(a, a)$ defined by the formulas (7) and (14) it was used this for-loop statement:

```
for a from 1 to 10 do
sumab(1000000,a); sumaabb(1000000,a);
end do;
```

The approximative values of the sums $s(10^6, a)$, $s(a)$, $s(10^6, a, a)$, and $s(a, a)$ rounded to seven decimals obtained by these procedures are written into the following Table 1. Let us note that the computation of 20 values $s(a)$ and $s(a, a)$ took almost 51 hours 26 minutes. The relative quantification accuracies $r(a) = \dfrac{|s(10^6, a) - s(a)|}{s(10^6, a)}$ of the sum $s(a, 10^6)$ and $r(a, a) = \dfrac{|s(10^6, a, a) - s(a, a)|}{s(10^6, a, a)}$ of the sum $s(a, a, 10^6)$ are stated in the fourth and eighth columns of Table 1. These relative quantification accuracies are approximately between $4 \cdot 10^{-7}$ and $2 \cdot 10^{-7}$.

a	$s(10^6, a)$	$s(a)$	$r(a)$	a	$s(10^6, a, a)$	$s(a, a)$	$r(a, a)$
1	0.6931469	0.6931472	$4{\cdot}10^{-7}$	1	1.1319715	1.1319718	$3{\cdot}10^{-7}$
2	1.3862939	1.3862944	$4{\cdot}10^{-7}$	2	2.2639430	2.2639435	$2{\cdot}10^{-7}$
3	2.0794408	2.0794415	$3{\cdot}10^{-7}$	3	3.3959145	3.3959153	$2{\cdot}10^{-7}$
4	2.7725877	2.7725887	$4{\cdot}10^{-7}$	4	4.5278860	4.5278870	$2{\cdot}10^{-7}$
5	3.4657347	3.4657359	$3{\cdot}10^{-7}$	5	5.6598575	5.6598588	$2{\cdot}10^{-7}$
6	4.1588816	4.1588831	$4{\cdot}10^{-7}$	6	6.7918290	6.7918305	$2{\cdot}10^{-7}$
7	4.8520285	4.8520303	$4{\cdot}10^{-7}$	7	7.9238005	7.9268023	$2{\cdot}10^{-7}$
8	5.5451754	5.5451774	$4{\cdot}10^{-7}$	8	9.0557720	9.0557740	$2{\cdot}10^{-7}$
9	6.2383224	6.2383246	$4{\cdot}10^{-7}$	9	10.1877435	10.1877458	$2{\cdot}10^{-7}$
10	6.9314693	6.9314718	$4{\cdot}10^{-7}$	10	11.3197150	11.3197175	$2{\cdot}10^{-7}$

Table 1: The approximate values of the sums of the generalized harmonic series with periodically repeating numerators $(a, -a)$ and $(a, a, -a, -a)$ for $a = 1, 2, \ldots, 10$

5 Conclusions

In this paper we dealt with the generalized harmonic series with periodically repeated numerators (a, b) and (a, a, b, b), i.e. with the series

$$\sum_{k=1}^{\infty} \left(\frac{a}{2k-1} + \frac{b}{2k} \right) = \frac{a}{1} + \frac{b}{2} + \frac{a}{3} + \frac{b}{4} + \frac{a}{5} + \frac{b}{6} + \cdots$$

with the sum $s(a)$ and with series

$$\sum_{k=1}^{\infty}\left(\frac{a}{4k-3}+\frac{a}{4k-2}+\frac{b}{4k-1}+\frac{b}{4k}\right)=\frac{a}{1}+\frac{a}{2}+\frac{b}{3}+\frac{b}{4}+\cdots$$

with the sum $s(a,a)$, where $a,b\in\mathbb{R}$.

We derived that the only value of the numerators $b\in\mathbb{R}$, for which these series converge, are $b=-a$, and we also derived that the sums of these series are determined by the formulas

$$s(a)=a\ln 2$$

and

$$s(a,a)=\frac{a}{4}(\pi+2\ln 2)\,.$$

So, for example, the series $\displaystyle\sum_{k=1}^{\infty}\left(\frac{5}{2k-1}-\frac{5}{2k}\right)=\frac{5}{2}\sum_{k=1}^{\infty}\frac{1}{(2k-1)k}$ has the sum $s(5)\doteq 3.4657$ and the series $\displaystyle\sum_{k=1}^{\infty}\left(\frac{5}{4k-3}+\frac{5}{4k-2}-\frac{5}{4k-1}-\frac{5}{4k}\right)=\frac{5}{4}\sum_{k=1}^{\infty}\frac{32k^2-24k+3}{(4k-3)(2k-1)(4k-1)k}$ has the sum $s(5,5)\doteq 5.6599$.

Finally, we verified these two main results by computing some sums by using the CAS Maple 16 and its basic programming language. These generalized harmonic series so belong to special types of convergent infinite series, such as geometric and telescoping series, which sum can be found analytically and also presented by means of a simple numerical expression. From the derived formulas for $s(a)$ and $s(a,a)$ above it follows that

$$a=\frac{s(a)}{\ln 2}\qquad\text{and}\qquad a=\frac{4s(a,a)}{\pi+2\ln 2}\,.$$

These relations allow calculate the value of the numerators a for a given sum $s(a)$ or $s(a,a)$, as illustrates the following Table 2:

$s(a)$	a	$s(a,a)$	a
1	1.4427	1	0.8834
$\ln 0.5\doteq -0.6391$	-1	$(-\pi-2\ln 2)/4\doteq -1.1320$	-1
$\ln 2\doteq 0.6391$	1	$(\pi+2\ln 2)/4\doteq 1.1320$	1

Table 2: The approximate values of the numerators a for some sums $s(a)$ and $s(a,a)$

6 Acknowledgements

The work presented in this paper has been supported by the project "Rozvoj oblastí základního a aplikovaného výzkumu dlouhodobě rozvíjených na katedrách teoretického a aplikovaného základu FVT (K215, K217)" **VÝZKUMFVT** (DZRO K-217).

References

[1] R. Potůček, *Sums of Generalized Alternating Harmonic Series with Periodically Repeated Numerators* $(1, a)$ *and* $(1, 1, a)$. In: Mathematics, Information Technologies and Applied Sciences 2014 post-conference proceedings of selected papers extended versions. University of Defence, Brno, (2014), 83-88. ISBN 978-8-7231-978-7.

[2] R. Potůček, *Sum of generalized alternating harmonic series with three periodically repeated numerators*. Mathematics in Education, Research and Applications, Vol. 1, no. 2, (2015), 42-48. ISSN 2453-6881.

[3] R. Potůček, *Sum of generalized alternating harmonic series with four periodically repeated numerators*. In: Proceedings of the 14th Conference on Applied Mathematics APLIMAT 2015. Slovak University of Technology in Bratislava, Publishing House of STU, Slovak Republic, (2015), 638-643. ISBN 978-80-227-4314-3.

[4] A. Fedullo, *Kalman filters and ARMA models*. In: Ratio Mathematica, Vol. 14 (2003), 41-46. ISSN 1592-7415. Available at: http://eiris.it/ojs/index.php/ratiomathematica/article/view/11. Accessed July 8, 2017.

[5] F. Bubeník and P. Mayer, *A Recursive Variant of Schwarz Type Domain Decomposition Methods*. In: Ratio Mathematica, Vol. 30 (2016), 35-43. ISSN 1592-7415. Available at: http://eiris.it/ojs/index.php/ratiomathematica/article/view/4. Accessed July 8, 2017.

[6] M. Hušek and P. Pyrih, *Matematická analýza*. Matematicko-fyzikální fakulta, Univerzita Karlova v Praze, (2000), 36 pp. Available at: http://matematika.cuni.cz/dl/analyza/25-raf/lekce25-raf-pmax.pdf. Accessed July 8, 2017.

Ratio Mathematica **ISSN**: 1592-7415
Vol. 34, 2018, pp. 15-33 **eISSN**: 2282-8214

On Rough Sets and Hyperlattices

Ali Akbar Estaji*, Fereshteh Bayati†

Received: 08-10-2017. **Accepted**: 28-01-2018. **Published**: 30-06-2018

doi:10.23755/rm.v34i0.350

Abstract

In this paper, we introduce the concepts of upper and lower rough hyper fuzzy ideals (filters) in a hyperlattice and their basic properties are discussed. Let θ be a hyper congruence relation on L. We show that if μ is a fuzzy subset of L, then $\overline{\theta}(< \mu >) = \overline{\theta}(< \overline{\theta}(\mu) >)$ and $\overline{\theta}(\mu^*) = \overline{\theta}((\overline{\theta}(\mu))^*)$, where $< \mu >$ is the least hyper fuzzy ideal of L containing μ and

$$\mu^*(x) = sup\{\alpha \in [0,1] : x \in I(\mu_\alpha)\}$$

for all $x \in L$. Next, we prove that if μ is a hyper fuzzy ideal of L, then μ is an upper rough fuzzy ideal. Also, if θ is a $\wedge-$complete on L and μ is a hyper fuzzy prime ideal of L such that $\overline{\theta}(\mu)$ is a proper fuzzy subset of L, then μ is an upper rough fuzzy prime ideal. Furthermore, let θ be a $\vee$-complete congruence relation on L. If μ is a hyper fuzzy ideal, then μ is a lower rough fuzzy ideal and if μ is a hyper fuzzy prime ideal such that $\underline{\theta}(\mu)$ is a proper fuzzy subset of L, then μ is a lower rough fuzzy prime ideal.

Keywords: rough set, upper and lower approximations, hyperlattice, hyper fuzzy prime ideal, hyper fuzzy prime filter.
2010 AMS subject classifications: 03G10, 03E72, 46H10, 06D50, 08A72.

*Faculty of Mathematics and Computer Sciences, Hakim Sabzevari University, Sabzevar, Iran. aaestaji@hsu.ac.ir

†Faculty of Mathematics and Computer Sciences, Hakim Sabzevari University, Sabzevar, Iran.fereshte.bayati@yahoo.com

1 Introduction

In this paper, we are using three basic notions: hyperlattice, rough set and fuzzy subset. Hyperstructure theory was born in 1934 when Marty [14] defined hypergroups as a generalization of groups. Extending lattices (also called hyperlattices) have been recently studied by a number of authors, in particular, Koguep, Nkuimi and Lele [12], Feng and Zou [8], Guo and Xin [9], Rahnamai-Barghi [19], etc.

Rough set theory was introduced by Pawlak in 1982 [17]. Many authors have studied the general properties of generalized rough sets [1, 4, 5].

The concept of fuzzy subsets was first introduced by Zadeh [22] in 1965 and then the fuzzy subsets have been used in the reconsideration of classical mathematics. The relationships between fuzzy subsets and algebraic hyperstructures had been already considered by many researchers (for example [2, 21]). Also, there have been many papers studying the connections and differences of fuzzy subset theory and rough set theory [3, 15, 18]. In recent years, many efforts have been made to compare and combine the three theories [6, 7].

This paper is structured as follows. After the introduction, in Section 2, we recall some basic notions and results on hyperlattices, rough sets and fuzzy subsets. In Section 3, the notions of hyper congruence relation on a hyperlattice are introduced. Next, some important properties of θ-upper approximations of a fuzzy subset will be studied. Also by an example, we show that Theorem 2.15 in [12] is incorrect (see Example 3.20) and a corrected version is considered, Proposition 3.21. Finally, in Section 4, θ-lower approximations of a fuzzy subset on a hyperlattice will be studied.

2 Preliminaries of hyperlattices, rough sets and fuzzy subsets

In the remainder of the paper we use some notation and results from the theory of hyperlattices, rough sets and fuzzy subsets. We present a few basic definitions here.

Let L be a set partially ordered by the binary relation $\leq$. The poset $(L, \leq)$ is a *meet-semilattice* if for all elements x and y of L, the greatest lower bound or the meet of the set $\{x, y\}$, denoted by $x \wedge y$, exists. For x and y in a meet-semilattice L, $x \leq y \Leftrightarrow x = x \wedge y$.

Replacing greatest lower bound with least upper bound results in the dual concept of a *join-semilattice*. The least upper bound of $\{x, y\}$ is called the join of x and y and is denoted by $x \vee y$. A poset L is a *lattice* if and only if it is both a meet- and a join-semilattice.

In this paper, we use the following notion of a hyperlattice.

Let L be a non-empty meet-semilattice and $\vee : L \times L \to \mathcal{P}(L)^*$ be a hyperoperation, where $\mathcal{P}(L)$ is the power set of L and $\mathcal{P}(L)^* = \mathcal{P}(L) \setminus \{\emptyset\}$. Then $(L, \wedge, \vee)$ is a *hyperlattice* [19], if for all $a, b, c \in L$:

1. $a \in a \vee a$ and $a = a \wedge a$.
2. $a \vee b = b \vee a$ and $a \wedge b = b \wedge a$.
3. $(a \vee b) \vee c = a \vee (b \vee c)$ and $(a \wedge b) \wedge c = a \wedge (b \wedge c)$.
4. $a \in [a \wedge (a \vee b)] \cap [a \vee (a \wedge b)]$.
5. $a \in a \vee b \Leftrightarrow a \wedge b = b$.

Where for all non-empty subsets A and B of L, $A \wedge B = \{a \wedge b | a \in A, b \in B\}$, $A \vee B = \bigcup \{a \vee b | a \in A, b \in B\}$.

Throughout this paper, L is a hyperlattice with the least element 0 and the greatest element 1. For $X \subseteq L$ and $x \in L$ we write:

1. $\downarrow X = \{y \in L : y \leq x \text{ for some } x \in X\}$.
2. $\uparrow X = \{y \in L : y \geq x \text{ for some } x \in X\}$.
3. $\downarrow x = \downarrow \{x\}$.
4. $\uparrow x = \uparrow \{x\}$.

A pair (L, θ), where θ is an equivalence relation on L, is called an *approximation space* [17] and for $a \in L$, the equivalence class (or coset) of a modulo θ is the set $[a]_\theta = \{x \in L | (a, x) \in \theta\}$ and also for $A \subseteq L$, we put $[A]_\theta = \bigcup_{a \in A} [a]_\theta$.

For an approximation space (L, θ), by an *upper rough approximation* in (L, θ) we mean a mapping $\overline{Apr} : \mathcal{P}(L) \to \mathcal{P}(L)$ which is defined for every $X \in \mathcal{P}(L)$ by

$$\overline{Apr}(X) = \{a \in L : [a]_\theta \cap X \neq \emptyset\}.$$

Also, by a *lower rough approximation* in (L, θ) we mean a mapping $\underline{Apr} : \mathcal{P}(L) \to \mathcal{P}(L)$ defined for every $X \in \mathcal{P}(L)$ by

$$\underline{Apr}(X) = \{a \in L : [a]_\theta \subseteq X\}.$$

Then $Apr(X) = (\underline{Apr}(X), \overline{Apr}(X))$ is called a *rough subset* in (L, θ) if $\underline{Apr}(X) \neq \overline{Apr}(X)$. The following proposition is well known and easily seen.

Proposition 2.1. *Let (L, θ) be an approximation space. For every subsets $X, Y \subseteq L$, we have*

1. $\underline{Apr}(X) \subseteq X \subseteq \overline{Apr}(X)$.
2. *If $X \subseteq Y$, then $\underline{Apr}(X) \subseteq \underline{Apr}(Y)$ and $\overline{Apr}(X) \subseteq \overline{Apr}(Y)$.*
3. $\overline{Apr}(X \cup Y) = \overline{Apr}(X) \cup \overline{Apr}(Y)$ *and* $\overline{Apr}(X \cap Y) \subseteq \overline{Apr}(X) \cap \overline{Apr}(Y)$.
4. $\underline{Apr}(X \cap Y) = \underline{Apr}(X) \cap \underline{Apr}(Y)$ *and* $\underline{Apr}(X \cup Y) \supseteq \underline{Apr}(X) \cup \underline{Apr}(Y)$.
5. $\underline{Apr}\left(\underline{Apr}(X)\right) = \underline{Apr}(X)$ *and* $\overline{Apr}\left(\overline{Apr}(X)\right) = \overline{Apr}(X)$.

Proof. See [13]. □

Proposition 2.2. [12] *Let $(L, \vee, \wedge)$ be a hyperlattice.Then, for each pair $(a, b) \in L \times L$ there exist $a_1, b_1 \in a \vee b$, such that $a \leq a_1$ and $b \leq b_1$.*

Definition 2.3. [19] A nonempty subset J of L is called an *ideal* of L if for all $x, y \in L$

1. $x, y \in J$ implies $x \vee y \subseteq J$.
2. If $x \in J$, then $\downarrow x \subseteq J$.

Definition 2.4. [19] A nonempty subset F of L is called a *filter* of L if for all $x, y \in L$

1. $x, y \in F$ implies $x \wedge y \in F$.
2. If $x \in F$ and $x \leq y$, then $y \in F$.

Given a hyperlattice L and a set $X \subseteq L$, let $\mathrm{I}(X)$ denote the least ideal containing X, called the *ideal generated* by X.

A *fuzzy subset* of X is any function from X into $[0, 1]$. Let $\mathcal{F}(L)$ be the set of all fuzzy subsets of L. For $\mu, \lambda \in F(X)$, we say $\mu \subseteq \lambda$ if and only if $\mu(x) \leq \lambda(x)$ for all $x \in X$.

Definition 2.5. [12] Let μ be a fuzzy subset of L. Then

1. μ is a *hyper fuzzy ideal* of L if, for all $x, y \in L$,
   (a) $\bigwedge_{a \in x \vee y} \mu(a) \geq \mu(x) \wedge \mu(y)$.
   (b) $x \leq y \Rightarrow \mu(x) \geq \mu(y)$.

2. μ is a *hyper fuzzy filter* of L if, for all $x, y \in L$,

   (a) $\mu(x \wedge y) \geq \mu(x) \wedge \mu(y)$.

   (b) $x \leq y \Rightarrow \mu(x) \leq \mu(y)$.

Definition 2.6. [12] Let μ be a proper hyper fuzzy ideal of L.

1. μ is called a *hyper fuzzy prime ideal*, if $\mu(x \wedge y) \leq \mu(x) \vee \mu(y)$, for all $x, y \in L$.

2. μ is called a *hyper fuzzy prime filter*, if $\bigwedge_{a \in x \vee y} \mu(a) \leq \mu(x) \vee \mu(y)$, for all $x, y \in L$.

Definition 2.7. [6] Let θ be an equivalence relation on L and μ a fuzzy subset of L. Then we define the fuzzy subsets $\overline{\theta}(\mu)$ and $\underline{\theta}(\mu)$ as follows:

$$\overline{\theta}(\mu)(x) = \bigvee_{a \in [x]_\theta} \mu(a) \text{ and } \underline{\theta}(\mu)(x) = \bigwedge_{a \in [x]_\theta} \mu(a).$$

The fuzzy subsets $\overline{\theta}(\mu)$ and $\underline{\theta}(\mu)$ are, respectively, called the *θ-upper* and *θ-lower approximation* of the fuzzy subset μ. Then $\theta(\mu) = (\underline{\theta}(\mu), \overline{\theta}(\mu))$ is called a *rough fuzzy subset* with respect to μ if $\underline{\theta}(\mu) \neq \overline{\theta}(\mu)$.

Proposition 2.8. [6] *Let θ be an equivalence relation on L and $\mu, \lambda \in \mathcal{F}(L)$. Then*

1. $\underline{\theta}(\mu) \leq \mu \leq \overline{\theta}(\mu)$.

2. *If $\mu \subseteq \lambda$, then $\overline{\theta}(\mu) \leq \overline{\theta}(\lambda)$ and $\underline{\theta}(\mu) \leq \underline{\theta}(\lambda)$.*

3. $\overline{\theta}\,\overline{\theta}(\mu) = \overline{\theta}(\mu)$ *and* $\underline{\theta}\,\underline{\theta}(\mu) = \underline{\theta}(\mu)$.

4. $\underline{\theta}(\mu)(x) = \underline{\theta}(\mu)(a)$ *and* $\overline{\theta}(\mu)(x) = \overline{\theta}(\mu)(a)$, *for all $x \in L$ and $a \in [x]_\theta$.*

5. $\underline{\theta}\overline{\theta}(\mu) = \overline{\theta}(\mu)$ *and* $\overline{\theta}\underline{\theta}(\mu) = \underline{\theta}(\mu)$.

The proofs of the following propositions are straightforward.

Proposition 2.9. *Let θ be an equivalence relation on set A. Then the following statements hold:*

1. *For each $X \in \mathcal{P}(A)$,*

$$\overline{Apr}(X) = \bigcap \left\{ Y \in \mathcal{P}(A) : X \subseteq \underline{Apr}(Y) \right\} = \textit{Min} \left\{ Y \in \mathcal{P}(A) : X \subseteq \underline{Apr}(Y) \right\}.$$

2. *For each* $X \in \mathcal{P}(A)$,

$$\underline{Apr}(X) = \bigcup \left\{ Y \in \mathcal{P}(L) : \overline{Apr}(Y) \subseteq X \right\} = Max \left\{ Y \in \mathcal{P}(L) : \overline{Apr}(Y) \subseteq X \right\}.$$

Proposition 2.10. *Let* θ *be an equivalence relation on set* A*. Then the following statements hold:*

1. *For each* $\mu \in \mathcal{F}(A)$,

$$\overline{\theta}(\mu) = \bigwedge \{ \lambda \in \mathcal{F}(A) : \underline{\theta}(\lambda) \geq \mu \} = Min \{ \lambda \in \mathcal{F}(A) : \underline{\theta}(\lambda) \geq \mu \}.$$

2. *For each* $\mu \in \mathcal{F}(A)$,

$$\underline{\theta}(\mu) = \bigvee \left\{ \lambda \in \mathcal{F}(L) : \overline{\theta}(\lambda) \leq \mu \right\} = Max \left\{ \lambda \in \mathcal{F}(L) : \overline{\theta}(\lambda) \leq \mu \right\}.$$

3 Upper approximations of a fuzzy subset

In this section we give some important properties of $\overline{\theta}$ with many examples, starting with the following definition.

Definition 3.1. [16, 20] Let θ be an equivalence relation on a hyperlattice L. Then θ is called a *hyper congruence relation* if $(a, b) \in \theta$ implies that $(a \vee x) \times (b \vee x) \subseteq \theta$ and $(a \wedge x, b \wedge x) \in \theta$ for all $x \in L$.

It is clear that if L is a hyperlattice L and $\theta = L \times L$, then θ is a hyper congruence relation. Also, in Example 3.9, we'll provide a non-trivial example.

Lemma 3.2. *Let* θ *be a hyper congruence relation on* L*. Then, for every* $a, b, c, d \in L$*,*

1. *If* $(a, b) \in \theta$ *and* $(c, d) \in \theta$*, then* $(a \wedge c, b \wedge d) \in \theta$ *and* $(a \vee c) \times (b \vee d) \subseteq \theta$*.*
2. $[a]_\theta \vee [b]_\theta \subseteq [a \vee b]_\theta$*.*
3. $[a]_\theta \wedge [b]_\theta \subseteq [a \wedge b]_\theta$*.*

Proof. Evident. □

Proposition 3.3. *Let* θ *be an equivalence relation on* L *and* $X \subseteq L$*. If* $\mu \in \mathcal{F}(L)$ *is a hyper fuzzy ideal of* L*, then*

1. $\mu(\downarrow X) \subseteq \uparrow \mu(X)$.

2. $\mu(\uparrow X) \subseteq \downarrow \mu(X)$.
3. $\mu(\overline{Apr}(\downarrow X)) \subseteq \uparrow \mu(\overline{Apr}(X))$.
4. $\mu(\overline{Apr}(\uparrow X)) \subseteq \downarrow \mu(\overline{Apr}(X))$.
5. $\overline{\theta}(\mu)(\overline{Apr}(\downarrow X)) \subseteq \uparrow \overline{\theta}(\mu)(X)$.

Proof. (1) Let $a \in \downarrow X$. Then there exists $x \in X$ such that $a \leq x$. Since μ is a hyper fuzzy ideal, we conclude that $\mu(x) \leq \mu(a)$ which implies that $\mu(a) \in \uparrow \mu(X)$ and the proof is now complete.

(2) The proof is similar to the proof of (1).

(3) For each $X \subseteq L$, since $\downarrow \overline{Apr}(X) = \overline{Apr}(\downarrow X) = \downarrow \overline{Apr}(\downarrow X)$, we can then conclude from (1) that $\mu(\overline{Apr}(\downarrow X)) \subseteq \uparrow \mu(\overline{Apr}(X))$.

(4) For each $X \subseteq L$, we have $\uparrow \overline{Apr}(X) = \overline{Apr}(\uparrow X) = \uparrow \overline{Apr}(\uparrow X)$. By (2), $\mu(\overline{Apr}(\uparrow X)) \subseteq \downarrow \mu(\overline{Apr}(X))$.

(5) Since $\overline{\theta}(\mu)(\overline{Apr}(\downarrow X)) = \overline{\theta}(\mu)(\downarrow X)$, we can then conclude from (1) that $\overline{\theta}(\mu)(\overline{Apr}(\downarrow X)) \subseteq \uparrow \overline{\theta}(\mu)(X)$. □

Proposition 3.4. *Let θ be a hyper congruence relation on L and $x, y \in L$. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy ideal of L, then*

$$\bigvee_{a \in [x]_\theta, b \in [y]_\theta} \bigvee \mu(a \vee b) \leq \bigvee \overline{\theta}(\mu)(x \vee y).$$

Proof. By Lemma 3.2,

$$\begin{aligned} \bigvee_{a \in [x]_\theta, b \in [y]_\theta} \bigvee \mu(a \vee b) &\leq \bigvee_{z \in [x \vee y]_\theta} \mu(z) \\ &= \bigvee_{z \in \bigcup_{a \in x \vee y} [a]_\theta} \mu(z) \\ &= \bigvee_{a \in x \vee y} \bigvee_{z \in [a]_\theta} \mu(z) \\ &= \bigvee_{a \in x \vee y} \overline{\theta}(\mu)(a) \\ &= \bigvee \overline{\theta}(\mu)(x \vee y). \end{aligned}$$

□

Lemma 3.5. *Let θ be a hyper congruence relation on L and $x, y \in L$. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy filter of L, then $\overline{\theta}(\mu)(x \wedge y) = \bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b)$.*

Proof. By Lemma 3.2, $\bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) \leq \bigvee_{z \in [x \wedge y]_\theta} \mu(z) = \overline{\theta}(\mu)(x \wedge y)$. Now, assume that $z \in [x \wedge y]_\theta$. By Lemma 3.2, $(x \vee z) \times \{x\} \subseteq (x \vee z) \times (x \vee (x \wedge y)) \subseteq \theta$ and $(y \vee z) \times \{y\} \subseteq (y \vee z) \times (y \vee (x \wedge y)) \subseteq \theta$. Also, by Proposition 2.2, there exist $z_x \in x \vee z$ and $z_y \in y \vee z$ such that $z \leq z_x$ and $z \leq z_y$. Since $z \leq z_x \wedge z_y$ and μ is a hyper fuzzy filter of L, we conclude that $\mu(z) \leq \mu(z_x \wedge z_y)$. Therefore, $\overline{\theta}(\mu)(x \wedge y) = \bigvee_{z \in [x \wedge y]_\theta} \mu(z) \leq \bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b)$ and the proof is now complete. □

Definition 3.6. Let θ be an equivalence relation on L and $\mu \in \mathcal{F}(L)$. Then, μ is called an *upper rough fuzzy* (*prime*) *filter* if $\overline{\theta}(\mu)$ is a hyper fuzzy (prime) filter of L.

Proposition 3.7. *Let θ be a hyper congruence relation on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy filter, then μ is an upper rough fuzzy filter.*

Proof. Let $x, y \in L$ and $x \leq y$. If $z \in [x]_\theta$, then $(z, x) \in \theta$ and $(z \vee y) \times (x \vee y) \subseteq \theta$. Since $y \in x \vee y$, we conclude that $(z \vee y) \times \{y\} \subseteq \theta$. Also, by Proposition 2.2, there exists $z_1 \in z \vee y$ such that $z \leq z_1$, and so $\mu(z) \leq \mu(z_1) \leq \bigvee \mu(z \vee y)$. Therefore,

$$\begin{aligned} \overline{\theta}(\mu)(x) &= \textstyle\bigvee_{z \in [x]_\theta} \mu(z) \\ &\leq \textstyle\bigvee_{z \in [x]_\theta} \bigvee \mu(z \vee y) \\ &\leq \textstyle\bigvee_{t \in [y]_\theta} \mu(t) \\ &= \overline{\theta}(\mu)(y). \end{aligned}$$

Now, If $x, y \in L$, then

$$\begin{aligned} \overline{\theta}(\mu)(x \wedge y) &= \textstyle\bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) && \text{by Lemma 3.5} \\ &\geq \textstyle\bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a) \wedge \mu(b) && \mu \text{ is a hyper fuzzy filter} \\ &= \textstyle\bigvee_{a \in [x]_\theta} \mu(a) \wedge \bigvee_{b \in [y]_\theta} \mu(b) \\ &= \overline{\theta}(\mu)(x) \wedge \overline{\theta}(\mu)(y). \end{aligned}$$

Hence $\overline{\theta}(\mu)$ is a hyper fuzzy filter. □

Example 3.8. Let $L = \{0, a, b, c, d, 1\}$ and define $\wedge$ and $\vee$ by the following Cayley tables:

$\wedge$	0	a	b	c	d	1
0	0	0	0	0	0	0
a	0	a	a	a	a	a
b	0	a	b	a	b	b
c	0	a	a	c	c	c
d	0	a	b	c	d	d
1	0	a	b	c	d	1

$\vee$	0	a	b	c	d	1
0	$\{0\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{1\}$
a	$\{a\}$	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{1\}$
b	$\{b\}$	$\{b\}$	$\{b\}$	$\{d\}$	$\{d\}$	$\{1\}$
c	$\{c\}$	$\{c\}$	$\{d\}$	$\{c\}$	$\{d\}$	$\{1\}$
d	$\{d\}$	$\{d\}$	$\{d\}$	$\{d\}$	$\{d\}$	$\{1\}$
1	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$	$\{d, 1\}$

It is easy to see that the operations $\wedge$ and $\vee$ on L are well-defined and L is a hyperlattice. Let θ be an equivalence relation on the lattice L with the following equivalence classes: $[0]_\theta = \{0, a, b\}$; $[d]_\theta = \{d\}$; $[c]_\theta = \{c\}$; $[1]_\theta = \{1\}$. It is clear that θ is not a hyper congruence relation on the lattice L. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.1 & 0.2 & 0.7 & 0.2 & 0.7 & 0.9 \end{pmatrix},$$

then μ is a hyper fuzzy filter and

$$\overline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.7 & 0.7 & 0.7 & 0.2 & 0.7 & 0.9 \end{pmatrix}.$$

Since $0 \leq c$ and $\overline{\theta}(\mu)(0) = 0.7 \not\leq 0.2 = \overline{\theta}(\mu)(c)$, we conclude that $\overline{\theta}(\mu)$ is not a hyper fuzzy filter.

Example 3.9. Let the hyperlattice L be as in example 3.8. Let θ be an equivalence relation on the lattice L with the following equivalence classes: $[0]_\theta = \{0\}$ and $[1]_\theta = \{a, b, c, d, 1\}$. It is clear that θ is a hyper congruence relation on the lattice L.

Lemma 3.10. *Let θ be a hyper congruence relation on L and $x, y \in L$.Then*

1. *If $a \in [x]_\theta$ and $b \in [y]_\theta$, then $[\alpha]_\theta = [\beta]_\theta$ for every $\alpha \in [x \vee y]_\theta$ and $\beta \in [a \vee b]_\theta$.*

2. *If μ is a fuzzy subset of L, then $\bigvee_{a\in[x]_\theta, b\in[y]_\theta} \bigwedge_{z\in a\vee b} \mu(z) \leq \bigwedge_{z\in x\vee y} \overline{\theta}(\mu)(z)$.*

Proof. (1) Let $\alpha \in [x \vee y]_\theta$ and $\beta \in [a \vee b]_\theta$. Then, by Lemma 3.2, $(\alpha, \beta) \in (a \vee b) \times (x \vee y) \subseteq \theta$, it follows that $[\alpha]_\theta = [\beta]_\theta$.

(2) By statement (1), we have $\mu(z) \leq \bigvee_{d\in[z]_\theta} \mu(d) = \bigvee_{d\in[z']_\theta} \mu(d)$ for every $z \in a \vee b$ and $z' \in x \vee y$. Hence $\mu(z) \leq \bigwedge_{z'\in x\vee y} \bigvee_{d\in[z']_\theta} \mu(d)$ for every $z \in a \vee b$. Therefore $\bigwedge_{z\in a\vee b} \mu(z) \leq \bigwedge_{z'\in x\vee y} \bigvee_{d\in[z']_\theta} \mu(d)$, which follows that $\bigvee_{a\in[x]_\theta, b\in[y]_\theta} \bigwedge_{z\in a\vee b} \mu(z) \leq \bigwedge_{z\in x\vee y} \overline{\theta}(\mu)(z)$. □

Lemma 3.11. *Let θ be a hyper congruence relation on L and $x, y \in L$. If μ is a hyper fuzzy ideal of L and $x \leq y$, then $\overline{\theta}(\mu)(x) = \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b)$.*

Proof. It is clear that $\{a \wedge b : a \in [x]_\theta, b \in [y]_\theta\} \subseteq [x]_\theta$. Therefore,

$$\bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b) \leq \bigvee_{a\in[x]_\theta} \mu(a).$$

Now, we suppose that $a \in [x]_\theta$. Then $a \wedge y \in [x]_\theta$ and since μ is a hyper fuzzy ideal of L, we conclude that $\mu(a) \leq \mu(a \wedge y)$. Therefore

$$\begin{aligned} \overline{\theta}(\mu)(x) &= \bigvee_{a\in[x]_\theta} \mu(a) \\ &\leq \bigvee_{a\in[x]_\theta} \mu(a \wedge y) \\ &\leq \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b). \end{aligned}$$

Hence $\overline{\theta}(\mu)(x) = \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b)$. □

Definition 3.12. Let θ be an equivalence relation on L and $\mu \in \mathcal{F}(L)$. Then, μ is called an *upper rough fuzzy* (*prime*) *ideal* if $\overline{\theta}(\mu)$ is a hyper fuzzy (prime) ideal of L.

Proposition 3.13. *Let θ be a hyper congruence relation on L. If μ is a hyper fuzzy ideal of L, then μ is an upper rough fuzzy ideal.*

Proof. Let $x, y \in L$. Then

$$\begin{array}{rcll} \overline{\theta}(\mu)(x) \wedge \overline{\theta}(\mu)(y) & = & \bigvee_{a\in[x]_\theta} \mu(a) \wedge \bigvee_{b\in[y]_\theta} \mu(b) & \\ & = & \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a) \wedge \mu(b) & \\ & \leq & \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \bigwedge_{z\in a\vee b} \mu(z) & \mu \text{ is a hyper fuzzy ideal of } L \\ & \leq & \bigwedge_{z\in x\vee y} \overline{\theta}(\mu)(z) & \text{by Lemma 3.10.} \end{array}$$

Now, we suppose that $x, y \in L$ and $x \leq y$. Hence

$$\begin{array}{rcll} \overline{\theta}(\mu)(x) & = & \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b) & \text{by Lemma 3.11} \\ & \geq & \bigvee_{a\in[x]_\theta, b\in[y]_\theta} \mu(b) & \mu \text{ is a hyper fuzzy ideal of } L \\ & = & \overline{\theta}(\mu)(y). & \end{array}$$

□

Example 3.14. Let the hyperlattice L and the equivalence relation θ on L be as in example 3.8. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.3 & 0.3 & 0.2 & 0.3 & 0.2 & 0.1 \end{pmatrix},$$

then μ is a hyper fuzzy ideal and

$$\overline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.3 & 0.3 & 0.3 & 0.3 & 0.2 & 0.1 \end{pmatrix}.$$

Since $\bigwedge_{x\in b\vee c} \overline{\theta}(\mu)(x) = 0.2 \ngeq 0.3 = \overline{\theta}(\mu)(b) \wedge \overline{\theta}(\mu)(c)$, we conclude that $\overline{\theta}(\mu)$ is not a hyper fuzzy ideal.

Definition 3.15. Let θ be a hyper congruence relation on L. Then θ is called $\vee$-*complete* if $[a \vee b]_\theta = [a]_\theta \vee [b]_\theta$ for all $a, b \in L$. Likewise, θ is called $\wedge-$*complete* if $[a \wedge b]_\theta = [a]_\theta \wedge [b]_\theta$ for all $a, b \in L$. A hyper congruence relation on L which is both $\vee$-complete and $\wedge-$complete is called *complete*.

Proposition 3.16. *Let θ be a $\wedge-$complete on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy prime ideal of L such that $\overline{\theta}(\mu)$ is a proper fuzzy subset of L, then μ is an upper rough fuzzy prime ideal.*

Proof. If $x, y \in L$, then

$$\begin{array}{lll} \overline{\theta}(\mu)(x \wedge y) & = & \bigvee_{a \in [x \wedge y]_\theta} \mu(a) \\ & = & \bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) \qquad \theta \text{ is } \wedge\text{−complete} \\ & \leq & \bigvee_{a \in [x]_\theta, b \in [y]_\theta} \mu(a) \vee \mu(b) \qquad \mu \text{ is a hyper fuzzy prime ideal} \\ & = & \bigvee_{a \in [x]_\theta} \mu(a) \vee \bigvee_{b \in [y]_\theta} \mu(b) \\ & = & \overline{\theta}(\mu)(x) \vee \overline{\theta}(\mu)(y). \end{array}$$

Now, by Proposition 3.13, the proof is complete. □

Example 3.17. Let the lattice L be as in example 3.8. Let θ be a hyper congruence relation on the lattice L with the following equivalence classes: $[0]_\theta = \{0, a\}$; $[b]_\theta = \{b\}$; $[c]_\theta = \{c\}$; $[1]_\theta = \{1, d\}$. Since

$$[b \wedge c]_\theta = [a]_\theta = \{0, a\} \neq \{a\} = [b]_\theta \wedge [c]_\theta$$

we conclude that θ is not $\wedge-$ complete. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.9 & 0.8 & 0.8 & 0.7 & 0.7 & 0.2 \end{pmatrix},$$

then μ is a hyper fuzzy prime ideal and

$$\overline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.9 & 0.9 & 0.8 & 0.7 & 0.7 & 0.7 \end{pmatrix}.$$

Also, the ideal $\overline{\theta}(\mu)$ is not hyper fuzzy prime, because

$$\overline{\theta}(\mu)(b \wedge c) = 0.9 \nleqq 0.8 = \overline{\theta}(\mu)(b) \vee \overline{\theta}(\mu)(c).$$

Definition 3.18. Let μ be a fuzzy subset of L. The least hyper fuzzy ideal of L containing μ is called a hyper fuzzy ideal of L *induced* by μ and is denoted by $< \mu >$.

By Remark 2.6 in [12], if μ is a fuzzy subset of L, then there exits $< \mu >$.

Definition 3.19. For every $\mu \in \mathcal{F}(L)$, we define

$$\mu^*(x) = sup\{\alpha \in [0, 1] : x \in I(\mu_\alpha)\}$$

for all $x \in L$.

With the following example, we prove that Theorem 2.15 in [12] is incorrect.

Example 3.20. Let the hyperlattice L be as in example 3.8. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.5 & 0.8 & 0.4 & 0.5 & 0.7 & 0.6 \end{pmatrix},$$

then $\mu \in \mathcal{F}(L)$ and

$$\mu^* = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 1 & 0.8 & 0.7 & 0.7 & 0.7 & 0.6 \end{pmatrix}.$$

If

$$\nu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.9 & 0.8 & 0.7 & 0.7 & 0.7 & 0.6 \end{pmatrix},$$

then ν is the hyper fuzzy ideal of L, $\mu \leq \nu$ and $\mu^* \not\leq \nu$. Therefore, μ^* is not the hyper fuzzy ideal induced by μ. Hence, Theorem 2.15 in [12] is incorrect.

Also, if $\lambda_n = 0.7 - \frac{1}{n}$, for every $n \in \mathbb{N}$, then $b \in \bigcap_{n\in\mathbb{N}} I(\mu_{\lambda_n}) = \downarrow d$, but $b \notin \mu_{\lambda_n}$ for every $n \geq 10$. Hence the last paragraph of the proof of Theorem 2.15 in [12] is incorrect.

Now we give the correct version of Theorem 2.15 in [12].

Proposition 3.21. *Let μ be a fuzzy subset of L. Then the fuzzy subset μ^* of L is the hyper fuzzy ideal of L and*

1. $\mu \leq \mu^*$.

2. $\mu^* = \bigwedge\{\lambda \in \mathcal{FI}(L) | \mu \leq \lambda \text{ and } \lambda(0) = 1\}$.

Proof. For $\lambda \in Im(\mu^*)$, let $\lambda_n = \lambda - \frac{1}{n}$, for $n \in \mathbb{N}$, and let $x \in \mu^*_\lambda$. Then $\mu^*(x) \geq \lambda$, which implies that $\mu^*(x) > \lambda_n$. Hence there exists $\beta \in \{\alpha \in [0,1] | x \in \mathrm{I}(\mu_\alpha)\}$ such that $\beta > \lambda_n$. Thus $\mu_\beta \subseteq \mu_{\lambda_n}$ and so $x \in \mathrm{I}(\mu_\beta) \subseteq \mathrm{I}(\mu_{\lambda_n})$ for all $n \in \mathbb{N}$. Therefore, $x \in \bigcap_{n\in\mathbb{N}} \mathrm{I}(\mu_{\lambda_n})$. Conversely, if $x \in \bigcap_{n\in\mathbb{N}} \mathrm{I}(\mu_{\lambda_n})$, $\lambda_n \in \{\alpha \in [0,1] : x \in \mathrm{I}(\mu_\alpha)\}$, for $n \in \mathbb{N}$. Therefore, $\lambda_n = \lambda - \frac{1}{n} \leq \bigvee\{\alpha \in [0,1] : x \in \mathrm{I}(\mu_\alpha)\} = \mu^*(x)$. Hence $\mu^*(x) \geq \lambda$, so that $x \in \mu^*_\lambda$. Then we have $\mu^*_\lambda = \bigcap_{n\in\mathbb{N}} \mathrm{I}(\mu_{\lambda_n})$ which is an ideal of L.

For $x \in L$, let $\beta \in \{\alpha \in [0,1] : x \in \mu_\alpha\}$. Then $x \in \mu_\beta$, and so $x \in \mathrm{I}(\mu_\beta)$. Thus $\beta \in \{\alpha \in [0,1] : x \in \mathrm{I}(\mu_\alpha)\}$, which implies that $\mu(x) = \bigvee\{\alpha \in [0,1] : x \in \mu_\alpha\} \leq \bigvee\{\alpha \in [0,1] : x \in \mathrm{I}(\mu_\alpha)\} = \mu^*(x)$. Therefore, $\mu \leq \mu^*$ (see [11, 12]).

Now, let ν be a hyper fuzzy ideal of L containing μ such that $\nu(0) = 1$. Then for every $\alpha \in [0,1]$, since $\nu_\alpha \neq \emptyset$, we conclude that $I(\mu_\alpha) \leq I(\nu_\alpha) = \nu_\alpha$. Hence

$$\mu^*(x) = \bigvee\{\alpha \in [0,1] : x \in I(\mu_\alpha)\} \leq \bigvee\{\alpha \in [0,1] : x \in \nu_\alpha\} = \nu(x)$$

for every $x \in L$. Also, for every $\alpha \in [0,1]$, $0 \in \mathrm{I}(\mu_\alpha)$ and we infer that $\mu^*(0) = \bigvee\{\alpha \in [0,1] : 0 \in \mathrm{I}(\mu_\alpha)\} = 1$. Therefore, $\mu^* \in \{\lambda \in \mathcal{FI}(L) | \mu \leq \lambda \; and \; \lambda(0) = 1\}$. Finally, we have

$$\mu^* = \bigwedge\{\lambda \in \mathcal{FI}(L) | \mu \leq \lambda \; and \; \lambda(0) = 1\}.$$

□

Proposition 3.22. *Let θ be a hyper congruence relation on L and $\mu \in \mathcal{F}(L)$. Then $\overline{\theta}(< \mu >) = \overline{\theta}(< \overline{\theta}(\mu) >)$ and $\overline{\theta}(\mu^*) = \overline{\theta}((\overline{\theta}(\mu))^*)$.*

Proof. Since $\mu \leq < \mu > \leq \mu^*$, we conclude from Proposition 2.8 that

$$\overline{\theta}(\mu) \leq \overline{\theta}(< \mu >) \leq \overline{\theta}(\mu^*).$$

It is clear that $\overline{\theta}(\mu^*)(0) = 1$ and by Propositions 3.13 and 3.21, we have

$$< \overline{\theta}(\mu) > \leq \overline{\theta}(< \mu >) \text{ and } (\overline{\theta}(\mu))^* \leq \overline{\theta}(\mu^*).$$

Again, by Proposition 2.8,

$$\overline{\theta}(< \overline{\theta}(\mu) >) \leq \overline{\theta}(< \mu >) \text{ and } \overline{\theta}((\overline{\theta}(\mu))^*) \leq \overline{\theta}(\mu^*).$$

Since $\mu \leq \overline{\theta}(\mu)$, we conclude that

$$< \mu > \leq < \overline{\theta}(\mu) > \text{ and } \mu^* \leq (\overline{\theta}(\mu))^*$$

and by Proposition 2.8,

$$\overline{\theta}(< \mu >) \leq \overline{\theta}(< \overline{\theta}(\mu) >) \text{ and } \overline{\theta}(\mu^*) \leq \overline{\theta}((\overline{\theta}(\mu))^*).$$

Finally, we have

$$\overline{\theta}(< \mu >) = \overline{\theta}(< \overline{\theta}(\mu) >) \text{ and } \overline{\theta}(\mu^*) = \overline{\theta}((\overline{\theta}(\mu))^*).$$

□

By the following example, we prove that the condition for an equivalence relation on L does not imply $\overline{\theta}((\overline{\theta}(\mu))^*) = \overline{\theta}(\mu^*)$.

Example 3.23. Let the hyperlattice L and the equivalence relation θ on L be as in example 3.8. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.5 & 0.8 & 0.4 & 0.7 & 0.5 & 0.6 \end{pmatrix},$$

then

$$\overline{\theta}(\mu^*) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 1 & 1 & 1 & 0.7 & 0.6 & 0.6 \end{pmatrix},$$

and

$$\overline{\theta}((\overline{\theta}(\mu))^*) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 1 & 1 & 1 & 0.7 & 0.7 & 0.6 \end{pmatrix}.$$

Hence $\overline{\theta}(\mu^*) \neq \overline{\theta}((\overline{\theta}(\mu))^*)$. Therefore, in general $\overline{\theta}(\mu^*) = \overline{\theta}((\overline{\theta}(\mu))^*)$ doesn't hold.

4 Lower approximations of a fuzzy subset

In this section we give some important properties of $\underline{\theta}$ with many examples.

Lemma 4.1. *Let θ be a hyper congruence relation on L and $x, y \in L$. If μ is a hyper fuzzy filter of L and $x \leq y$, then $\underline{\theta}(\mu)(x) = \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b)$.*

Proof. Since $x \leq y$, we can then conclude from Lemma 3.2 that $\{\mu(a \wedge b) : a \in [x]_\theta, b \in [y]_\theta\} \subseteq \{\mu(z) : z \in [x]_\theta\}$. Hence $\underline{\theta}(\mu)(x) \leq \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b)$. Also, since μ is a hyper fuzzy filter of L, we conclude that $\mu(a \wedge b) \leq \mu(a)$ for every $a \in [x]_\theta$ and $b \in [y]_\theta$, which follows that $\underline{\theta}(\mu)(x) \geq \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b)$ and the proof is now complete. □

Definition 4.2. Let θ be an equivalence relation on L and $\mu \in \mathcal{F}(L)$. Then, μ is called a *lower rough fuzzy* (*prime*) *ideal* if $\underline{\theta}(\mu)$ is a hyper fuzzy (prime) ideal of L.

Proposition 4.3. *Let θ be a $\vee$-complete congruence relation on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy ideal, then μ is a lower rough fuzzy ideal.*

Proof. Let $x, y \in L$. Since $\bigwedge_{t\in x\vee y} \mu(t) \in \{\bigwedge_{t\in a\vee b} \mu(t) : a \in [x]_\theta, b \in [y]_\theta\}$, we conclude that

$$\begin{array}{rcll} \underline{\theta}(\mu)(x) \wedge \underline{\theta}(\mu)(y) & = & \bigwedge_{a\in[x]_\theta} \mu(a) \wedge \bigwedge_{b\in[y]_\theta} \mu(b) & \\ & = & \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a) \wedge \mu(b) & \\ & \leq & \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \bigwedge_{t\in a\vee b} \mu(t) & \mu \text{ is a hyper fuzzy ideal} \\ & = & \bigwedge_{t\in[x]_\theta\vee[y]_\theta} \mu(t) & \\ & = & \bigwedge_{t\in[x\vee y]_\theta} \mu(t) & \theta \text{ is } \vee\text{-complete} \\ & = & \bigwedge_{z\in x\vee y} \bigwedge_{t\in[z]_\theta} \mu(t) & \\ & = & \bigwedge_{z\in x\vee y} \underline{\theta}(\mu)(z). & \end{array}$$

Let $x, y \in L$ and $x \leq y$. Hence

$$\begin{array}{rcll} \underline{\theta}(\mu)(x) & = & \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a \wedge b) & \text{by Lemma 4.1} \\ & \geq & \bigwedge_{b\in[y]_\theta} \mu(b) & \mu \text{ is a hyper fuzzy ideal} \\ & = & \underline{\theta}(\mu)(y). & \end{array}$$

□

Example 4.4. Let the hyperlattice L and the hyper congruence relation θ on L be as in example 3.17. Let

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 1 & 0.8 & 0.6 & 0.4 & 0.4 & 0 \end{pmatrix}.$$

It is clear that μ is a hyper fuzzy ideal on L and

$$\underline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.8 & 0.8 & 0.6 & 0.4 & 0 & 0 \end{pmatrix}.$$

It is easy to see that θ is not $\vee$ - complete, because

$$[b \vee c]_\theta = \{1.d\} \neq \{d\} = [b]_\theta \vee [c]_\theta.$$

Also, since

$$\underline{\theta}(\mu)(b) \wedge \underline{\theta}(\mu)(c) = 0.4 \not\leq 0 = \bigwedge_{d \in b \vee c} \underline{\theta}(\mu)(d)$$

we conclude that $\underline{\theta}(\mu)$ is not a hyper fuzzy ideal.

Definition 4.5. Let θ be an equivalence relation on L and $\mu \in \mathcal{F}(L)$. Then, μ is called a *lower rough fuzzy* (*prime*) *filter* if $\underline{\theta}(\mu)$ is a hyper fuzzy (prime) filter of L.

Proposition 4.6. *Let θ be a $\wedge-$complete congruence relation on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy filter, then μ is a lower rough fuzzy filter.*

Proof. Let $x, y \in L$.

$$\begin{array}{rcll} \underline{\theta}(\mu)(x \wedge y) & = & \bigwedge_{a \in [x \wedge y]_\theta} \mu(a) & \\ & = & \bigwedge_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) & \theta \text{ is } \wedge-\text{complete} \\ & \geq & \bigwedge_{a \in [x]_\theta, b \in [y]_\theta} \mu(a) \wedge \mu(b) & \mu \text{ is a hyper fuzzy filter} \\ & = & \bigwedge_{a \in [x]_\theta} \mu(a) \wedge \bigwedge_{b \in [y]_\theta} \mu(b) & \\ & = & \underline{\theta}(\mu)(x) \wedge \underline{\theta}(\mu)(y). & \end{array}$$

Let $x, y \in L$ and $x \leq y$. Hence

$$\begin{array}{rcll} \underline{\theta}(\mu)(x) & = & \bigwedge_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) & \text{by Lemma 4.1} \\ & \leq & \bigwedge_{b \in [y]_\theta} \mu(b) & \mu \text{ is a hyper fuzzy filter} \\ & = & \underline{\theta}(\mu)(y). & \end{array}$$

□

Example 4.7. Let the hyperlattice L and the hyper congruence relation θ on L be as in example 3.17. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.1 & 0.6 & 0.6 & 0.7 & 0.7 & 0.9 \end{pmatrix},$$

then μ is a hyper fuzzy filter and

$$\underline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.1 & 0.1 & 0.6 & 0.7 & 0.7 & 0.7 \end{pmatrix}.$$

Since

$$[b \wedge c]_\theta = \{0, a\} \neq \{a\} = [b]_\theta \wedge [c]_\theta,$$

we conclude that θ is not $\wedge-$ complete. Also $\underline{\theta}(\nu)$ is not a hyper fuzzy filter, because

$$\underline{\theta}(\nu)(b \wedge c) = \underline{\theta}(\nu)(a) = 0.1 \not\geq 0.6 = \underline{\theta}(\nu)(b) \wedge \underline{\theta}(\nu)(c).$$

Proposition 4.8. *Let θ be a $\vee$-complete on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy prime ideal such that $\underline{\theta}(\mu)$ is a proper fuzzy subset of L, then μ is a lower rough fuzzy prime ideal.*

Proof. Let $x, y \in L$.

$$\begin{array}{rcll} \underline{\theta}(\mu)(x \wedge y) & = & \bigwedge_{z \in [x \wedge y]_\theta} \mu(z) & \\ & \leq & \bigwedge_{a \in [x]_\theta, b \in [y]_\theta} \mu(a \wedge b) & \text{by Lemma 3.2} \\ & \leq & \bigwedge_{a \in [x]_\theta, b \in [y]_\theta} \mu(a) \vee \mu(b) & \mu \text{ is a hyper fuzzy prime ideal} \\ & = & \bigwedge_{a \in [x]_\theta} \mu(a) \vee \bigwedge_{b \in [y]_\theta} \mu(b) & \\ & = & \underline{\theta}(\mu)(x) \vee \underline{\theta}(\mu)(y). & \end{array}$$

By Proposition 4.3, the proof is now complete. □

Example 4.9. Let the lattice L and the hyper congruence relation θ on L be as in example 3.17. If

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.9 & 0.8 & 0.8 & 0.7 & 0.7 & 0.2 \end{pmatrix},$$

then μ is a hyper fuzzy prime ideal and

$$\underline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.8 & 0.8 & 0.8 & 0.7 & 0.2 & 0.2 \end{pmatrix}.$$

Since

$$[b \vee c]_\theta = \{1.d\} \neq \{d\} = [b]_\theta \vee [c]_\theta,$$

we conclude that θ is not $\vee$ - complete. Also $\underline{\theta}(\mu)$ is not hyper fuzzy ideal, because

$$\underline{\theta}(\mu)(b) \wedge \underline{\theta}(\mu)(c) = 0.7 \not\leq 0.2 = \bigwedge_{d \in (b \vee c)} \underline{\theta}(\mu)(d).$$

Proposition 4.10. *Let θ be a complete congruence relation on L. If $\mu \in \mathcal{F}(L)$ is a hyper fuzzy prime filter such that $\underline{\theta}(\mu)$ is a proper fuzzy subset of L, then μ is a lower rough fuzzy prime filter.*

Proof. Let $x, y \in L$.

$$\begin{array}{rcll} \underline{\theta}(\mu)(x) \vee \underline{\theta}(\mu)(y) & = & \bigwedge_{a\in[x]_\theta} \mu(a) \vee \bigwedge_{b\in[y]_\theta} \mu(b) & \\ & = & \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \mu(a) \vee \mu(b) & \\ & \geq & \bigwedge_{a\in[x]_\theta, b\in[y]_\theta} \bigwedge_{t\in a\vee b} \mu(t) & \mu \text{ is a hyper fuzzy prime filter} \\ & = & \bigwedge_{z\in x\vee y} \bigwedge_{t\in[z]_\theta} \mu(t) & \theta \text{ is } \vee\text{-complete} \\ & = & \bigwedge_{z\in x\vee y} \underline{\theta}(\mu)(z). & \end{array}$$

By Proposition 4.6, the proof is now complete. □

Example 4.11. Let the hyperlattice L and the hyper congruence relation θ on L be as in example 3.17. It is clear that

$$\mu = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.1 & 0.3 & 0.7 & 0.3 & 0.7 & 0.9 \end{pmatrix}$$

is a hyper fuzzy prime filter and

$$\underline{\theta}(\mu) = \begin{pmatrix} 0 & a & b & c & d & 1 \\ 0.1 & 0.1 & 0.7 & 0.3 & 0.7 & 0.7 \end{pmatrix}.$$

Since

$$\underline{\theta}(\mu)(b) \wedge \underline{\theta}(\mu)(c) = 0.3 \not\leq 0.1 = \underline{\theta}(\mu)(b \wedge c),$$

we conclude that $\underline{\theta}(\mu)$ is not a hyper fuzzy ideal. Also, as we have seen in Example 4.4, θ is not $\vee$ - complete.

5 Conclusion

Rough set, fuzzy set and hyperlattice are different aspects of set theory. Combining the three theories, one gets the rough concept fuzzy hyperlattice of a given context. We introduced the concepts of upper and lower rough hyper fuzzy ideals (filters) in a hyperlattice and its basic properties have been discussed. Also, we discussed the relations between hyper fuzzy (prime) ideal and hyper fuzzy (prime) filter with their upper and lower approximations, respectively. In addition, by an example we show that Theorem 2.15 in [12] is incorrect (see Example 3.20) and a corrected version is considered, Proposition 3.21.

Acknowledgement

We express our gratitude to Professor M. Mehdi Ebrahimi.

References

[1] S. M. Anvariyeh, S. Mirvakili and B. Davvaz, *Pawlaks approximations in $\Gamma-$semihypergroups*, Computers & Mathematics with Applications, Volume **60**, Issue 1, July 2010, 45-53.

[2] M. Asghari-Larimi, *Hyperstructures with fuzzy subgroup and Fuzzy Ideal*, International Mathematical Forum, **5**, 2010, no. 10, 467-476.

[3] K. Chakrabarty, R. Biswas and S. Nanda, *Fuzziness in rough sets*, Fuzzy Sets Syst. 110 (**2**) (2000) 247-251.

[4] B. Davvaz, *Approximations in hyperrings*, Journal of Multiple-Valued Logic and Soft Computing **15** (2009) 471-488.

[5] C. Degang, Z. Wenxiu, D. Yeung and E. C. C. Tsang, *Rough approximations on a complete completely distributive lattice with applications to generalized rough sets*, Information Sciences **176** (2006) 1829-1848.

[6] A. A. Estaji, S. Khodaii and S. Bahrami, *On rough set and fuzzy sublattice*, Information Sciences, Volume **181**, Issue 18, 15 September 2011, 3981-3994.

[7] A. A. Estaji, M. R. Hooshmandasl and B. Davvaz, *Rough set theory applied to lattice theory*, Information Sciences, Volume **200**, 1 October 2012, 108-122.

[8] Y. Feng and L. Zou, *On Product of Fuzzy Subhyperlattice and Interval-Valued Fuzzy Subhyperlattice*, Discrete Mathematics, Algorithms and Applications Vol. **2**, No. 2 (2010) 239-246.

[9] X. Z. Guo and X.L. Xin, *On hyperlattice*, Pure and Applied Mathematics **20** (1) (2004) 40-43.

[10] O. Kazancı, S. Yamak and B. Davvaz, *The lower and upper approximations in a quotient hypermodule with respect to fuzzy sets*, Information Sciences **178** (2008) 2349-2359.

[11] B. B. N. Koguep, C. Nkuimi and C. Lele, *On fuzzy prime ideal of lattice*, Samsa Journal of Pure and Applied Mathematics, **3** (2008) 1-11.

[12] B. B. N. Koguep, C. Nkuimi and C. Lele, *On Fuzzy Ideals of Hyperlattice*, International Journal of Algebra, Vol. **2**, 2008, no. 15, 739-750.

[13] M. Kondo, On the structure of generalized rough sets, Information Sciences 176 (2006) 589-600.

[14] F. Marty, *Sur une generalization de la notion de group*, 8th Congress Math. Scandenaves, Stockholm, (1934), 45-49.

[15] J. N. Mordeson, *Rough set theory applied to (fuzzy) ideal theory*, Fuzzy Sets Syst. **121** (2) (2001) 315-324.

[16] A. D. Lokhande and Aryani Gangadhara, Congruences in hypersemilattices, International Mathematical Forum, Vol. 7, 2012, no. 55, 2735 - 2742.

[17] Z. Pawlak, *Rough sets*, International Journal of Computer and Information Sciences **11** (1982) 341-356.

[18] A. M. Radzikowska and E. E. Kerre, *A comparative study of fuzzy rough sets*, Fuzzy Sets Syst. **126** (6) (2002) 137-156.

[19] A. Rahnamai-Barghi, *The prime ideal theorem for distributive hyperlattices*, Ital. Journal of Pure and Applied Math., vol. **10**, 2001 , 75-78.

[20] M. Sambasiva Rao, Multipliers of Hypersemilattices, International Journal of Mathematics and Soft Computing Vol.3, No.1 (2013), 29 - 35.

[21] S. Yamak, O. Kazancı, and B. Davvaz, *Soft hyperstructure*, Computers & Mathematics with Applications, Volume **62**, Issue 2, July 2011, Pages 797-803.

[22] L. A. Zadeh, *Fuzzy sets*, Inform. and Control, **8** (1965) 338-353.

Ratio Mathematica
Vol.34, 2018, pp. 35-47

ISSN: 1592-7415
eISSN: 2282-8214

On a Geometric Representation of Probability Laws and of a Coherent Prevision-Function According to Subjectivistic Conception of Probability

Pierpaolo Angelini*, Angela De Sanctis†

Received: 22-03-2018. **Accepted**: 30-05-2018. **Published**: 30-06-2018

doi:10.23755/rm.v34i0.401

Abstract

We distinguish the two extreme aspects of the logic of certainty by identifying their corresponding structures into a linear space. We extend probability laws $\mathbf{P}$ formally admissible in terms of coherence to random quantities. We give a geometric representation of these laws $\mathbf{P}$ and of a coherent prevision-function $\mathbf{P}$ which we previously defined. This work is the foundation of our next and extensive study concerning the formulation of a geometric, well-organized and original theory of random quantities.

Keywords: metric; collinearity; vector subspace; convex set; linear dependence

2010 AMS subject classifications: 51A05; 60A02; 60B02.

*MIUR, Roma, Italia. pierpaolo.angelini@istruzione.it

†DEA, Univerity "G. D'Annunzio" of Chieti-Pescara, Pescara, Italia angela.desanctis@unich.it

1 Introduction

An event E is conceptually a mental separation between subjective sensations: it is actually a proposition or statement such that, by betting on it, we can establish in an unmistakable fashion whether it is true or false, that is to say, whether it has occurred or not and so whether the bet has been won or lost ([9], [15]). For any individual who does not certainly know the true value of a quantity X, which is random in a non-redundant usage for him, there are two or more than two possible values for X. The set of these values is denoted by $I(X)$. In any case, only one is the true value of each random quantity and the meaning that you have to give to random is the one of unknown by the individual of whom you consider his state of uncertainty or ignorance. Thus, random does not mean undetermined but it means established in an unequivocal fashion, so a supposed bet based upon it would unmistakably be decided at the appropriate time. When one wonders if infinite events of a set are all true or which is the true event among an infinite number of events, one can never verify if such statements are true or false. These statements are infinite in number, so they do not coincide with any mental separation between subjective sensations: they are conceptually meaningless. Hence, we can understand the reason for which it is not a logical restriction to define a random quantity as a finite partition of incompatible and exhaustive events, so one and only one of the possible values for X belonging to the set $I(X) = \{x_1, \ldots, x_n\}$ is necessarily true. A random quantity is dealt with by the logic of certainty as well as by the logic of probable ([8]). We recognize two different and extreme aspects concerning the logic of certainty. At first we distinguish a more or less extensive class of alternatives which appear objectively possible to us in the current state of our information: when a given individual outlines the domain of uncertainty he does not use his subjective opinions on what he does not know because the possible values of X depend only on what he objectively knows or not. Afterwards we definitively observe which is the true alternative to be verified among the ones logically possible. The probability is an additional notion, so it comes into play after constituting the range of possibility and before knowing which is the true alternative to be verified: the logic of probable will fill in this range in a coherent way by considering a probabilistic mass distributed upon it. An individual correctly makes a prevision of a random quantity when he leaves the objective domain of the logically possible in order to distribute his subjective sensations of probability among all the possible alternatives and in the way which will appear most appropriate to him ([7], [12], [13]). Given an evaluation of probability p_i, $i = 1, \ldots, n$, a prevision of X turns out to be $\mathbf{P}(X) = x_1p_1 + \ldots + x_np_n$, where we have $0 \leq p_i \leq 1, i = 1, \ldots, n$, and $\sum_{i=1}^{n} p_i = 1$: it is rendered as a function of the probabilities of the possible values for X and it is admissible in terms of coherence because it is a barycenter of these values. It is usually called the

mathematical expectation of X or its mean value ([14]). It is certainly possible to extend this result by using more advanced mathematical tools such as Stieltjes integrals. Nevertheless, such an extension adds nothing from conceptual and operational point of view and for this reason we will not consider it. Conversely, the possible values of any possible event are only two: 0 and 1. Therefore, each event is a specific random quantity. The same symbol $\mathbf{P}$ denotes both prevision of a random quantity and probability of an event ([10]).

2 Space of alternatives as a linear space

When we consider one random quantity X, each possible value of it, for a given individual at a certain instant, is a real number in the space $\mathcal{S}$ of alternatives coinciding with a line on which an origin, a unit of length and an orientation are chosen. Every point of this line is assumed to correspond to a real number and every real number to a point: the real line is a vector space over the field $\mathbb{R}$ of real numbers, that is to say, over itself, of dimension 1. When we consider two random quantities, X_1 and X_2, a Cartesian coordinate plane is the space $\mathcal{S}$ of alternatives: possible pairs (x_1, x_2) are the Cartesian coordinates of a possible point of this plane. Every point of a Cartesian coordinate plane is assumed to correspond to an ordered pair of real numbers and vice versa: $\mathbb{R}^2$ is a vector space over the field $\mathbb{R}$ of real numbers of dimension 2 and it is called the two-dimensional real space. When we consider three random quantities, X_1, X_2 and X_3, the three-dimensional real space $\mathbb{R}^3$ corresponds to the set $\mathcal{S}$ of alternatives and possible triples (x_1, x_2, x_3) are the Cartesian coordinates of a possible point of this linear space. There is a bijection between the points of the vector space $\mathbb{R}^3$ over the field $\mathbb{R}$ of real numbers and the ordered triples of real numbers. More generally, in the case of n random quantities, where n is an integer > 3, one can think of the Cartesian coordinates of the n-dimensional real space $\mathbb{R}^n$. There is a bijection between the points of the vector space $\mathbb{R}^n$ over the field $\mathbb{R}$ and the ordered n-tuples of real numbers. It is always essential that different pairs of real numbers are made to correspond to distinct points or different triples of real numbers are made to correspond to different points or, more generally, distinct n-tuples of real numbers are made to correspond to dissimilar points ([11]). Those alternatives which appear possible to us are elements of the set $\mathcal{Q}$ and they are embedded in the space $\mathcal{S}$ of alternatives. Such a space is conceptually a set of points whose subset $\mathcal{Q}$ consists of those possible points non-themselves subdivisible for the purposes of the problem under consideration. Sometimes, the set $\mathcal{Q}$ coincides with $\mathcal{S}$. There is a very meaningful point among the points of $\mathcal{Q}$: it represents the true alternative, that is to say, the one which will turn out to be verified "a posteriori". It is a random point "a priori" and it expresses everything there is to

be said.

3 Two different aspects of the logic of certainty into a linear space

We study the two aspects of the logic of certainty into a linear space coinciding with the n-dimensional real space $\mathbb{R}^n$ where we consider n random quantities $X_1, \ldots, X_n$. Therefore, we have n orthogonal axes to each other: a same Cartesian coordinate system is chosen on every axis. Thus, the real space $\mathbb{R}^n$ has a Euclidean structure and it is evidently our space $\mathcal{S}$ of alternatives. Into the logic of certainty exist certain and impossible and possible as alternatives with respect to the temporary knowledge of each individual: each random quantity justifies itself "a priori" because every finite partition of incompatible and exhaustive events referring to it shows the possible ways in which a certain reality may be expressed. A multiplicity of possible values for every random quantity is only a formal construction that precedes the empirical observation by means of which a single value among the ones of the set $\mathcal{Q}$ is realized. The set $\mathcal{Q}$ of every random quantity is a subset of a vector subspace of dimension 1 into the n-dimensional real space $\mathbb{R}^n$. In general, given X, we have $\mathcal{Q} = I(X) = \{x_1, \ldots, x_n\}$. It is absolutely the same thing if every possible value of each random quantity is viewed as a particular n-tuple of real numbers or as a single real number. Every possible value for a random quantity definitively becomes 0 or 1 when we make an empirical observation referring to it: into the logic of certainty also exist true and false as final answers ([2], [3]). Logical operations are applicable to idempotent numbers 0 and 1. If A and B are events, the negation of A is $\bar{A} = 1 - A$ and such an event is true if A is false, while if A is true it is false; the negation of B is similarly $\bar{B} = 1 - B$. The logical product of A and B is $A \wedge B = AB$ and such an event is true if A is true and B is true, otherwise it is false; the logical sum of A and B is $(A \vee B) = \left(\overline{\bar{A} \wedge \bar{B}}\right) = 1 - (1 - A)(1 - B)$, from which it follows that such an event is true if at least one of events is true, where we have $A \vee B = A + B$ when A and B are incompatible events because it is impossible for them both to occur. Concerning the logical product and the logical sum, we have evidently the same thing when we consider more than two events. An algebraic structure $(L, \wedge, \vee)$, where the logical product $\wedge$ and the logical sum $\vee$ are two binary operations on the set L whose elements are 0 and 1, is a Boolean algebra because commutative laws, associative laws, absorption laws, idempotent laws and distributive laws hold for 0 and 1 of L. It admits both an identity element with respect to the logical product and an identity element with respect to the logical sum, so we have

$$(x \wedge 1) = x, (x \vee 0) = x,$$

for all x of L. It admits that every x of L has a unique complement $\bar{x}$, so we have

$$(x \wedge \bar{x}) = 0, (x \vee \bar{x}) = 1.$$

We can extend the logical operations into the field of real numbers when we make the following definitions: $x \wedge y = min(x, y)$, $x \vee y = max(x, y)$, $\bar{x} = 1 - x$. Therefore, it is not true that the logical operations are applicable only to idempotent numbers 0 and 1 because they are also applicable to all real numbers. On the other hand, it is not true that the arithmetic operations are applicable only to natural, rational, real, complex numbers or integers because they are also applicable to idempotent numbers 0 and 1 identifying events. For instance, the arithmetic sum of many events coincides with the random number of successes given by $Y = E_1 + \ldots + E_n$. Therefore, we observe that the set $\mathcal{Q}$ of every random quantity considered into a linear space becomes a Boolean algebra whose two idempotent numbers are on every axis of $\mathbb{R}^n$. These two numbers are elements of a subset of a vector subspace of dimension 1 into the n-dimensional real space $\mathbb{R}^n$ over the field $\mathbb{R}$ of real numbers. That being so, it is evident that to postulate that the field over which the probability is defined be a σ-algebra is not natural. Hence, what we will later say is conceptually and mathematically well-founded.

4 Probability laws P formally admissible in terms of coherence

The probability $\mathbf{P}$ of an event E, in opinion of a given individual, is operationally a price in terms of gain and a bet is the real or conceptual experiment to be made oneself in order to obtain its measurement ([4]). If $p = \mathbf{P}(E)$ is a coherent assessment expressed by this individual, then such a bet is fair because it is acceptable in both senses indifferently. Therefore, he considers as fair an exchange, for any S positive or negative, between a certain sum pS and the right to a sum S dependent on the occurrence of E ([5]). From notion of fairness it follows that the two possible values of the random quantity $G' = (\lambda - p)S$, where λ is a random quantity whose possible values are 0 and 1, do not have the same sign. Given S, if these values of G' are only positive or negative, then we have an incoherent assessment and the bet on the event under consideration is not fair. If E is a certain event, then we have $p = 1$ in a coherent fashion. If E is an impossible event, then we have $p = 0$ in a coherent fashion. If E is a possible event because it is not either certain or impossible, then we have $0 \leq p \leq 1$ in a coherent fashion. Even the probability $\mathbf{P}$ of the trievent $E = E''|E'$ is a price in terms of gain. It is the price to be paid for a bet that can be won or lost or annulled if E' does not occur. Nevertheless, we will not consider the notion of conditional

probability from now on, because it is not essential to this context. Given n events $E_1, \ldots, E_n$ of the set $\mathcal{E}$ of events, a certain individual assigns to them, respectively, the probabilities $p_1 = \mathbf{P}(E_1), \ldots, p_n = \mathbf{P}(E_n)$ in a coherent way. Thus, by betting on $E_1, \ldots, E_n$, this individual considers as fair an exchange, for any $S_1, \ldots, S_n$ positive or negative, between a certain sum $p_1 S_1 + \ldots + p_n S_n$ and the right to a sum $E_1 S_1 + \ldots + E_n S_n$ dependent on the occurrence of $E_1, \ldots, E_n$, where we have $E_i = 1$ or $E_i = 0$, $i = 1, \ldots, n$, whether E_i occurs or not. Evidently, if $p_1 = \mathbf{P}(E_1), \ldots, p_n = \mathbf{P}(E_n)$ are not coherent assessments, then the possible values of the random quantity $G = (\lambda_1 - p_1)S_1 + \ldots + (\lambda_n - p_n)S_n$ are all positive or negative. Probability laws $\mathbf{P}$ formally admissible in terms of coherence allow to extend in a logical or coherent way the probabilities of the events of $\mathcal{E}$ which are already evaluated in a subjective way. These laws allow to determine which is the most general set of events whose probabilities are uniquely determined, in accordance with theorems of probability calculus, because one knows the probability of each event of $\mathcal{E}$. Moreover, probability laws $\mathbf{P}$ allow to determine which is the most general set of events for which their probabilities lie between two numbers, which are not 0 and 1, after evaluating the probability of each event of $\mathcal{E}$ in a subjective way, while for the remaining events can be said nothing in addition to the banal observation that their probabilities are included between 0 and 1. If $\mathcal{E}$ is a finite set of incompatible and exhaustive events $E_1, \ldots, E_n$, then $\mathbf{P}$ is a probability law formally admissible in terms of coherence with regard to events of $\mathcal{E}$ if and only if the theorem of total probability is valid, so we have $\mathbf{P}(E_1) + \ldots + \mathbf{P}(E_n) = 1$. Probability laws $\mathbf{P}$ formally admissible are evidently ∞^n and a given individual may subjectively choose one of these laws depending on the circumstances. Given A, its probability $\mathbf{P}(A)$ is uniquely determined when A is a logical sum of two or more than two incompatible events of $\mathcal{E}$: A is linearly dependent on these events. Otherwise, we can only say that $\mathbf{P}(A)$ is greater than or equal to the sum of the probabilities of the events E_i which imply A and less than or equal to the sum of the probabilities of the events E_i which are compatible with A. If $\mathcal{E}$ is a finite set of events $E_1, \ldots, E_n$ whatsoever, then the 2^n constituents $C_1, \ldots, C_s$ form a finite set of incompatible and exhaustive events for which it is certain that one and only one of them occurs. These constituents are elementary or atomic events and they are obtained by the logical product $E_1 \wedge \ldots \wedge E_n$: each time we substitute in an orderly way one event E_i, $i = 1, \ldots, n$, or more than one event with its negation $\bar{E}_i$ or their negations, we obtain one constituent of the set of constituents generated by $E_1, \ldots, E_n$. It is possible that some constituent is impossible, so the number of possible constituents is $s \leq 2^n$. The most general probability law assigns to the possible constituents $C_1, \ldots, C_s$ the probabilities $q_1, \ldots, q_s$ which sum to 1, while the probability of an impossible constituent is always 0. Conversely, every probability law which is valid for the events of $\mathcal{E}$ can be extended to the constituents $C_1, \ldots, C_s$, so the

probabilities $p_1 = \mathbf{P}(E_1), \ldots, p_n = \mathbf{P}(E_n)$ are admissible if and only if the non-negative numbers $q_1, \ldots, q_s$ satisfy a system of $n + 1$ linear equations in the s variables $q_1, \ldots, q_s$ expressed by

$$\begin{cases} \sum_i^{(1)} q_i = p_1 \\ \vdots \\ \sum_i^{(n)} q_i = p_n \\ \sum_{i=1}^{s} q_i = 1. \end{cases}$$

The notation $\sum_i^{(h)} q_i$ represents the sum concerning those indices i for which C_i is an event implying E_h. If A is a logical sum of some constituent, then we have $x = \sum_i^{(A)} q_i$ and we can say that the probability of A is uniquely determined because $x = \sum_i^{(A)} q_i$ is linearly dependent on the $n + 1$ linear equations of the system under consideration. If A is not a logical sum of constituents, then A' is the greatest logical sum of the ones which are contained in A and A'' is the lowest logical sum of the ones which contain A, so we have $x' \leq x \leq x''$, where x' is the lowest admissible probability of A', while x'' is the greatest admissible probability of A''. If $\mathcal{E}$ is an infinite set of events, then $\mathbf{P}$ is a probability law formally admissible with regard to events of $\mathcal{E}$ if and only if $\mathbf{P}$ is a probability law formally admissible with regard to any finite subset of $\mathcal{E}$. Therefore, given A, its probability $\mathbf{P}(A)$ is uniquely determined or bounded from above and below or absolutely undetermined because we have $0 \leq \mathbf{P}(A) \leq 1$. Now we extend probability laws $\mathbf{P}$ formally admissible in terms of coherence to random quantities we defined in the beginning. The set $\mathcal{X}$ can be a finite set of n random quantities $X_1, \ldots, X_n$ or it can be an infinite set of random quantities. In general, given X, $I(X) = \{x_1, \ldots, x_n\}$ is the set of its possible values. Thus, after assigning to every possible value x_i of X its subjective and corresponding probability p_i, with $\sum_{i=1}^{n} p_i = 1$, we have $infI(X) \leq \mathbf{P}(X) \leq supI(X)$ in accordance with convexity property of $\mathbf{P}$. Given $Z = X_1 + \ldots + X_n$ which is a linear combination of n random quantities $X_1, \ldots, X_n$ of $\mathcal{X}$, $I(Z) = \{z_1, \ldots, z_n\}$ is the set of its possible values. Therefore, its coherent prevision must satisfy convexity property of $\mathbf{P}$, so we have $infI(Z) \leq \mathbf{P}(Z) \leq supI(Z)$, where it turns out to be $\mathbf{P}(Z)$ = $\mathbf{P}(X_1) + \ldots + \mathbf{P}(X_n)$ in accordance with linearity property of $\mathbf{P}$. Linearity property can clearly be of interest to any linear combination of n random quantities. We may also consider less than n random quantities. The possibility of certain consequences whose unacceptability appears recognizable to everyone is excluded when convexity property of $\mathbf{P}$ and its linearity property are valid. They are the foundation of the whole theory of probability because they are necessary and sufficient conditions for coherence: decisions under conditions of uncertainty lead to a certain loss when linearity and convexity of $\mathbf{P}$ are broken ([1]). The

probabilities of every possible value of a given random quantity belonging to a finite or infinite set of random quantities sum to 1 in a coherent way according to probability laws $\mathbf{P}$ formally admissible in terms of coherence with regard to these possible values.

5 A coherent prevision-function P

From mathematical point of view, $\mathbf{P}$ is a function. We define it by taking into account its objective coherence. The domain of $\mathbf{P}$ is the arbitrary set $\mathcal{X} = \{X_1, \ldots, X_n\}$ consisting of a finite number of random quantities: for each of them, the set of possible values is $I(X_i) = \{x_{i1}, \ldots, x_{in}\}$, with $x_{i1} < \ldots < x_{in}$, $i = 1, \ldots, n$. Moreover, we suppose $x_{i1} \neq x_{j1}$ and $x_{in} \neq x_{jn}$, with $i \neq j$, $i, j = 1, \ldots, n$. The codomain of $\mathbf{P}$ is the set $\mathcal{Y}$ consisting of as many intervals as random quantities are found into the set $\mathcal{X}$ of $\mathbf{P}$, with $infI(X_i) \leq \mathbf{P}(X_i) \leq supI(X_i)$ for every interval referring to the random quantity X_i, $i = 1, \ldots, n$. Therefore, both $\mathcal{X}$ and $\mathcal{Y}$ are sets whose elements are themselves sets. The coherent function $\mathbf{P}$ is called prevision-function and it is a bijective function because each element of $\mathcal{X}$, $X_i \in \mathcal{X}$, is paired with exactly one element of $\mathcal{Y}$, for which it turns out to be $infI(X_i) \leq \mathbf{P}(X_i) \leq supI(X_i)$, and each element of $\mathcal{Y}$ is paired with exactly one element of $\mathcal{X}$. There are no unpaired elements, with $\mathbf{P}(X_i)$ which is a prevision of X_i on the basis of the state of information of a certain individual at a given instant. Given the set $I(X) = \{x_1, \ldots, x_n\}$, with $x_1 < \ldots < x_n$, the image of X under $\mathbf{P}$ is $\mathbf{P}(X) = x_1p_1 + \ldots + x_np_n$, with $0 \leq p_i \leq 1, i = 1, \ldots, n$, and $\sum_{i=1}^{n} p_i = 1$: such an image coincides with all weighted arithmetic means calculated in a coherent fashion when p_i varies while x_i is constant. All coherent previsions of X satisfy the inequality $infI(X) \leq \mathbf{P}(X) \leq supI(X)$. The image of the entire domain $\mathcal{X}$ of $\mathbf{P}$ is the image of $\mathbf{P}$ and it coincides with the entire codomain $\mathcal{Y}$. If $\mathcal{X}$ is an infinite set of random quantities, we can always consider a restriction of the prevision-function $\mathbf{P}$ which is a new function obtained by choosing a smaller and finite domain. Therefore, the above observations remain unchanged because such a new function coincides with $\mathbf{P}$ whose domain is a finite set of random quantities. In the case in which the domain of $\mathbf{P}$ is the arbitrary set $\mathcal{E} = \{E_1, \ldots, E_n\}$ consisting of a finite number of possible events, its codomain is the set $\mathcal{Y}$ consisting of as many intervals as events are found into the set $\mathcal{E}$ of $\mathbf{P}$, with $infE_i \leq \mathbf{P}(E_i) \leq supE_i$, $i = 1, \ldots, n$, for each of such intervals. Nevertheless, since we have $infE_i = 0$ and $supE_i = 1$, $i = 1, \ldots, n$, it turns out to be $0 \leq \mathbf{P}(E_i) \leq 1$ for every interval of $\mathcal{Y}$. The coherent function $\mathbf{P}$ is called probability-function and it is a bijective function because each element of $\mathcal{E}$, $E_i \in \mathcal{E}$, is paired with exactly one element of $\mathcal{Y}$, for which it turns out to be $0 \leq \mathbf{P}(E_i) \leq 1$, and each element of $\mathcal{Y}$ is paired with exactly one element of $\mathcal{E}$.

There are no unpaired elements, with $\mathbf{P}(E_i)$ which is an evaluation of probability of E_i. The image of E_i under $\mathbf{P}$ is an interval. If $\mathcal{E}$ is an infinite set of events, we can always consider a restriction of the probability-function $\mathbf{P}$ as above. We admit that $\mathbf{P}$ can be evaluated by anybody for every event E or random quantity X. Thus, it is not true that it would make sense to speak of probability only when all events under consideration are repeatable, as well as it is not true that it would make sense to speak of prevision only when all random quantities under consideration belong to a measurable set $\mathcal{I}$. We cannot pretend that $\mathbf{P}$ is actually imagined as determined, by any individual, for all events or random quantities which could be considered in the abstract. We must recognize if $\mathbf{P}$ includes or not any incoherence. If so the individual, when made aware of such an incoherence, should eliminate it. Thus, the subjective evaluation is objectively coherent and can be extended to any larger set of events or random quantities. It is necessary to interrogate a given individual in order to force him to reveal his evaluation of elements of the codomain $\mathcal{Y}$ of $\mathbf{P}$, $\mathbf{P}(X_i)$ or $\mathbf{P}(E_i)$, $i = 1, \ldots, n$: both prevision of a random quantity and probability of an event always express what an individual chooses in his given state of ignorance, so it is wrong to imagine a greater degree of ignorance which would justify the refusal to answer. If a prevision-function is not understood as an expression of the opinion of a certain individual, we can interrogate many individuals in order to study their common opinion which is denoted by $\mathbf{P}$. Therefore, $\mathbf{P}$ will exist in the ambit of those random quantities X for which all evaluations $\mathbf{P}_i(X)$, $i = 1, \ldots, n$, coincide. Such evaluations will define $\mathbf{P}(X)$ in this way. Evidently, $\mathbf{P}$ will not exist elsewhere, for other random quantities X for which the subjective evaluations $\mathbf{P}_i(X)$ do not coincide. The above observations remain valid when a given individual confines himself to evaluations which conform to more restrictive criteria coinciding with classical definition of probability and with the statistical one ([6], [16]).

6 Geometric representation of $\mathbf{P}$

Given the set $\mathcal{X} = \{X_1, \ldots, X_n\}$ or the set $\mathcal{E} = \{E_1, \ldots, E_n\}$, the possible values of each random quantity or random event can geometrically be represented on n lines for which a Cartesian coordinate system has been chosen. Such lines belong to the vector space $\mathbb{R}^n$ over the field $\mathbb{R}$ of real numbers. $\mathbb{R}^n$ has a Euclidean structure characterized by a metric. Hence, the standard basis of $\mathbb{R}^n$ is given by $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$, where we have $\mathbf{e}_1 = (1, \ldots, 0)$, …, $\mathbf{e}_n = (0, \ldots, 1)$, and it consists of orthogonal vectors to each other having a Euclidean norm equal to 1. The point of $\mathbb{R}^n$ where n lines meet is the origin of $\mathbb{R}^n$ given by $(0, \ldots, 0)$. We have an one-to-one correspondence between the points of $\mathbb{R}^n$ and the n-tuples of real numbers. We consider n coordinate subspaces of dimension 1 in the vector space $\mathbb{R}^n$. In fact,

when we project every point of $\mathbb{R}^n$ referring to $(X_1, X_2, \ldots, X_n)$ and expressed by $(x_1, x_2, \ldots, x_n)$ onto the coordinate axis x_1, it becomes $(x_1, \ldots, 0)$. When we project the same point onto the coordinate axis x_2, it becomes $(0, x_2, \ldots, 0)$ and so on. After projecting all the possible points of X_1 onto the coordinate axis x_1, ..., all the possible points of X_n onto the coordinate axis x_n, every point onto the coordinate axis x_1, coinciding with a particular n-tuple of real numbers of $\mathbb{R}^n$, can be viewed as a real number of $\mathbb{R}$, ..., every point onto the coordinate axis x_n, coinciding with a particular n-tuple of real numbers of $\mathbb{R}^n$, can be viewed as a real number of $\mathbb{R}$. It is finally clear that n projected points onto the coordinate axis x_1 can be viewed as n real numbers of an one-dimensional vector space, ..., n projected points onto the coordinate axis x_n can be viewed as n real numbers of an one-dimensional vector space. The possible points of E_i projected onto the coordinate axis $x_i, i = 1, \ldots, n$, are evidently only two. For instance, if n = 3, we have the points $(1, 0, 0)$ and $(0, 0, 0)$ onto the coordinate axis x_1 referring to E_1 which can respectively be viewed as 1 and 0, ..., the points $(0, 0, 1)$ and $(0, 0, 0)$ onto the coordinate axis x_3 referring to E_3 which can respectively be viewed as 1 and 0. Nevertheless, we have always three real lines, so we do not get confused. In any case, it is conceptually the same thing if we make use only of particular n-tuples of real numbers of $\mathbb{R}^n$ without seeing them as real numbers of $\mathbb{R}$. The codomain of $\mathbf{P}$ is the set $\mathcal{Y}$ consisting of n intervals which coincide with n line segments belonging to n different real lines. These line segments could become increasingly larger by virtue of linearity of $\mathbf{P}$ extended to any finite number of random quantities considered on a same line. Indeed, we observe that all weights or probabilistic masses, which are non-negative and sum to 1, remain unchanged with respect to starting point characterized by only one random quantity. Nevertheless, they are paired with real numbers whose absolute values are evidently greater. Such numbers can be interpreted as the possible values of one random quantity considered on a same line. It is evident that the set of all coherent previsions of every random quantity X_i as well as the set of all coherent probabilities of every random event E_i, $i = 1, \ldots, n$, is a subset of a vector subspace of dimension 1. Such a subset is however a convex set while the set of the possible values for every random quantity considered into $\mathbb{R}^n$ is not a convex set. The same thing goes when we consider the set of the possible values for every random event represented into $\mathbb{R}^n$. We already saw that it is always possible to consider a finite number of events or random quantities in order to study probability laws $\mathbf{P}$ formally admissible in terms of coherence. As a first step we refer to events. Given n events $E_1, \ldots, E_n$ of $\mathcal{E}$, we represent them by means of n axes of $\mathbb{R}^n$. Nevertheless, instead of concentrating our attention on n axes of $\mathbb{R}^n$ as above, we consider only one of them which we choose in an arbitrary fashion. Such an axis is an one-dimensional vector subspace of $\mathbb{R}^n$. It is generated by a vector of the standard basis of $\mathbb{R}^n$. Every point of $\mathbb{R}^n$ on a same line

is obtained multiplying by a real number the vector of the standard basis of $\mathbb{R}^n$ which we have arbitrarily chosen. Therefore, we can always multiply by any real number a same n-tuple of real numbers in order to obtain points of $\mathbb{R}^n$ which are said to be collinear. Now the real number or coefficient of the linear combination under consideration, characterized by only one scalar, represents the probability of an event A into our geometric scheme of representation. Given $\mathbf{P}(E_1)$, ..., $\mathbf{P}(E_n)$, we know that $\mathbf{P}(A)$ can be uniquely determined or bounded from above and below or absolutely undetermined depending on the circumstances. If it is uniquely determined, then we have a precise point of $\mathbb{R}^n$ on the axis under consideration. If it is bounded from above and below, then we have two points of $\mathbb{R}^n$ on this axis and an admissible probability is found between them. If it is absolutely undetermined, then we have a larger interval on this axis which is included between the lowest admissible probability of any event and the greatest admissible one. In particular, given $\mathbf{P}(E_1) = p_1$, ..., $\mathbf{P}(E_n) = p_n$, after choosing the vector $\mathbf{e}_n$ of the standard basis of $\mathbb{R}^n$, by means of the linear combination given by $[(\lambda_1 - p_1)S_1 + \ldots + (\lambda_n - p_n)S_n]\mathbf{e}_n$, with $S_i \neq 0$, $i = 1, \ldots, n$, we can obtain the possible values of the random quantity $G = (\lambda_1 - p_1)S_1 + \ldots + (\lambda_n - p_n)S_n$ referring to n bets concerning n events as special n-tuples of $\mathbb{R}^n$. The same thing goes if we choose another vector of the standard basis of $\mathbb{R}^n$. Thus, we even represent n bets concerning n events into a linear space. By examining n random quantities $X_1, \ldots, X_n$ of $\mathcal{X}$, we similarly represent them by means of n axes of $\mathbb{R}^n$. Nevertheless, by considering another random quantity Z which is again bounded from above and below, instead of concentrating our attention on n axes of $\mathbb{R}^n$, we consider only one of them which we choose in an arbitrary way. After individuating two points of $\mathbb{R}^n$ on this axis which are respectively the lowest possible value of the random quantity under consideration and the greatest possible one, $\mathbf{P}(Z)$ can be viewed as a point of $\mathbb{R}^n$ coherently included between the two points of $\mathbb{R}^n$ already individuated. Probability laws $\mathbf{P}$ formally admissible in terms of coherence are those laws for which the probabilities of the possible values of the random quantity under consideration sum to 1.

7 Conclusions

We distinguished the two extreme aspects of the logic of certainty by identifying their corresponding structures into a linear space. We extended probability laws $\mathbf{P}$ formally admissible in terms of coherence to random quantities. We proposed a geometric representation of these laws and of a coherent prevision-function $\mathbf{P}$ which we previously defined. We connected the convex set of all coherent previsions of a random quantity as well as the convex set of all coherent probabilities of an event with a specific algebraic structure: such a structure is an

one-dimensional vector subspace over the field $\mathbb{R}$ of real numbers because events of any finite set of events can be viewed as special points of a vector space of dimension n over the field $\mathbb{R}$ of real numbers. It is exactly the linear space of random quantities having a Euclidean structure characterized by a metric coinciding with the dot product in a natural way. Overall, we pointed out that linearity is the most meaningful concept concerning probability calculus whose laws gain a more extensive rigour by means of the geometric scheme of representation we showed. On the other hand, it is possible to extend linearity concept in order to formulate a geometric, well-organized and original theory of random quantities: we will make this into our next works.

References

[1] G. Coletti and R. Scozzafava, *Probabilistic logic in a coherent setting*, Kluwer Academic Publishers, Dordrecht/Boston/London, 2002.

[2] B. de Finetti, *Teoria delle probabilità: sintesi introduttiva con appendice critica, voll. I e II*, Einaudi, Torino, 1970.

[3] B. de Finetti, *Probability, Induction and Statistics (The art of guessing)*, J. Wiley & Sons, London-New York-Sydney-Toronto, 1972.

[4] B. de Finetti, *La probabilità: guardarsi dalle contraffazioni!*, Scientia, 111 (1976), 255–281.

[5] B. de Finetti, *The role of "Dutch Books" and of "proper scoring rules"*, The British Journal of Psychology of Sciences, 32 (1981), 55–56.

[6] B. de Finetti, *Probability: the different views and terminologies in a critical analysis*, Logic, Methodology and Philosophy of Science, VI (Hannover, 1979) (1982), 391–394.

[7] I. J. Good, *Subjective probability as the measure of a non-measureable set*, Logic, Methodology and Philosophy of Science, Proc. 1960 Internat. Congr. (1962), 319–329.

[8] H. Jeffreys, *Theory of probability, 3rd edn.*, Clarendon Press, Oxford, 1961.

[9] B. O. Koopman, *The axioms and algebra of intuitive probability*, Annals of Mathematics 41, (1940), 269–292.

[10] H. E. Kyburg jr. and H. E. Smokler, *Studies in subjective probability*, J. Wiley & Sons, New York, London, Sydney, 1964.

[11] G. Pompilj, *Teoria affine delle variabili casuali*, L'industria, 2 (1956), 143–163.

[12] F. P. Ramsey, *The foundations of mathematics and other logical essays. Edited by R. B. Braithwaite with a preface by G. E. Moore*, Littlefield, Adams & Co, Paterson, N. J., 1960.

[13] L. J. Savage, *The foundations of statistics*, J. Wiley & Sons, New York, 1954.

[14] B. de Finetti, *La prévision: ses lois logiques, ses sources subjectives*, Ann. Inst. H. Poincaré 7, 1, (1937), 1–68.

[15] B. de Finetti, *Sulla proseguibilità di processi aleatori scambiabili*, Rend. Ist. Mat. Univ. Trieste 1, (1969), 53–67.

[16] B. de Finetti, *Probability and statistics in relation to induction, from various points of view*, Induction and statistics, CIME Summer Schools, Springer, Heidelberg 18, (2011), 1–122.

Ratio Mathematica **ISSN**: 1592-7415
Vol. 34, 2018, pp. 49-65 **eISSN**: 2282-8214

A New Provably Secure Cryptosystem Using Dedekind Domain Direct Product Approach

Amir Hassani Karbasi[1]

Received: 27-02-2018. **Accepted**: 01-06-2018. **Published**: 30-06-2018

doi: 10.23755/rm.v34i0.404

Abstract

We would like to prevent, detect, and protect communication and information systems' attacks, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service by providing cryptographic techniques. If we prove that an encryption algorithm is based on mathematical NP-hard problems, we can prove its security. In this paper, we present a new NTRU-Like public-key cryptosystem with security provably based on the worst-case hardness of the approximate lattice problems (NP-hard problems) in some structured lattices (ideal lattices) in order to attain the applicable objectives of preserving the confidentiality of communication and information system resources (includes hardware, software, firmware, information/data, and telecommunications). Our proposed scheme is an improvement of ETRU cryptosystem. ETRU is an NTRU-Like public-key cryptosystem based on the Eisenstein integers

[1] Department of Mathematics, University of Guilan, Rasht, Iran. karbasi@phd.guilan.ac.ir

where is a primitive cube root of unity. ETRU has heuristic security and it has no proof of security. We show that our cryptosystem has security stronger than that of ETRU, over Cartesian product of Dedekind domains and extended cyclotomic polynomials. We prove the security for our main algorithm from the R-SIS and R-LWE problems as NP-hard problems.
Keywords: Lattice-based cryptography; Ideal lattices; ETRU; Provable security; Dedekind domain.
2010 subject classification: 94A60; 11T71; 14G50; 68P25.

1. Introduction

Public-key cryptography has many exciting applications for web browsers, e-mail programs, cell phones, bank cards, RFID tags, smart cards, government communications, banking systems, and so on. The users to communicate over non-secure channels without any prior communication can use public-key cryptography. The idea of public-key cryptography was first proposed by Diffie and Hellman in 1976 [1]. Lattice-based cryptography as a field of public-key cryptography has attracted considerable interest and it has been categorized into post-quantum cryptography [6]. Lattice-based cryptography enjoys efficient implementations, very strong security proofs based on worst-case hardness, as well as great simplicity. Our focus here will be mainly on the theoretical aspects of lattice-based cryptography.

The NTRU cryptosystem which is a famous lattice-based crypto scheme devised by Hoffstein, Pipher and Silverman, was first presented at the Crypto'96 rump session [2]. Although its structure relies on arithmetic over the quotient polynomial ring $\mathbf{Z}_q[x]/<x^N-1>$ for N prime and q a small integer, it was quickly shown that breaking it could be reflected as a problem over Euclidean lattices [3]. At the ANTS'98 conference, the NTRU authors presented an improved variant including a thorough assessment of its practical security against lattice attacks [4]. The NTRU cryptosystem standard number and version is IEEE P1363.1 [5]. The NTRU encryption (NTRUEncrypt) system is also often considered as the most practical post-quantum public-key crypto scheme [6] and this scheme uses the properties of structured lattices to achieve high efficiency but its security remains heuristic and it was an important open challenge to provide a provably secure scheme with comparable efficiency. For example, an 8-dimensional lattice in 2D view is shown in Figure 1.

By rising number of attacks and practical variants of NTRU, provable security in lattice-based cryptography is developed. The first provably secure lattice-based cryptosystem and its variant of GapSVP in arbitrary lattices were presented by Ajtai and Dwork [8, 9]. Ajtai's average-case problem is now reflected to as the Small Integer Solution problem (SIS). Another major

achievement in this field was the introduction in 2005 of the Learning with Errors problem (LWE) by Regev [13]. Micciancio [10] presented an alternative based on the worst-case hardness of the restriction of Poly(n)-SVP to cyclic lattices and succeeded in restricting SIS to structured matrices while preserving a worst-case to average-case reduction, which correspond to ideals in polynomial ring $\mathbf{Z}[x]/<x^n-1>$. Subsequently, Lyubashevsky and Micciancio [11] and independently Peikert and Rosen [12] showed how to modify Micciancio's function to construct an efficient and provably secure collision resistant hash function. So, they introduced the more general class of ideal lattices, which correspond to ideals in polynomial rings $\mathbf{Z}_q[x]/<\Phi>$ with a Φ that is irreducible cyclotomic polynomial, also is sparse (e.g., $\Phi = x^n + 1$ for n a power of 2). Their system relies on the hardness of the restriction of Poly(n)-SVP to ideal lattices (called Poly(n)-Ideal-SVP). The average-case collision-finding problem is a natural computational problem called Ideal-SIS, which has been reflected to be as hard as the worst-case instances of Ideal-SVP. In 2011, Stehlé and Steinfeld [14] proposed a structured variant of the NTRU, which they proved as hard as CPA security from the hardness of a variant of R-SIS and R-LWE (Ring Learning with Errors problem). R-LWE has great efficiency and provides more natural and flexible cryptographic constructions. The current paper was motivated by [14], in which the integers were replaced with the ring of Cartesian product of Eisenstein integers.

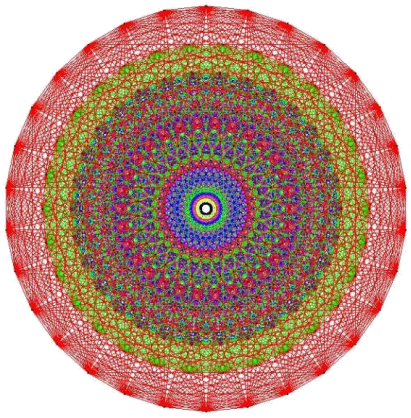

Figure 1. An 8-dimensional lattice in 2D view.

The ETRU is obtained from the NTRU by replacing $\mathbf{Z}$ with the ring of Eisenstein integers [7]. It is faster and has smaller size of keys for the same or better level of security than that of NTRU. Both division algorithm for Eisenstein integers and the choice of lattice embedding are integral, thus significantly improving their efficiency over the complex-valued versions

proposed in [15]. Note that the ETRU security is based on both SVP and then CVP so its security remains heuristic. The other author's lattice-based schemes are [20 – 28] which are suitable for application to WSNs and IoT [29-31].

In this paper, our proposed cryptosystem based on extended ideal lattices over $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ (for $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ with $n+1$ a prime) exploits the properties of the ETRU structured lattice to achieve high efficiency and it has IND-CPA security based on ideal lattices with established hardness of R-SIS and R-LWE problems. We prove that our modification of ETRU is provably secure, assuming the quantum hardness of standard worst-case problems over extended ideal lattices.

The rest of this paper is structured as follows: In section 2, we shortly review the ETRU system and explain the security related to the computational problems. In section 3, we study ideal lattices, R-SIS and R-LWE problems. In section 4, we suggest a key generation algorithm, where the generated public key follows a distribution for which Ideal-SVP reduces to R-LWE. In section 5, we make our modified ETRU cryptosystem as secure as worst-case problems over ideal lattices. Finally, the paper concludes in section 6.

2. ETRU Cryptosystem

2.1. Parameters Creation

We denote by ζ_3 a complex cube root of unity, that is $\zeta_3^3 = 1$ where $\zeta_3 = 1/2(-1+\sqrt{3}i)$ since $\zeta_3^3 - 1 = (\zeta_3 - 1)(\zeta_3^2 + \zeta_3 + 1) = 0$, we have $\zeta_3^2 + \zeta_3 + 1 = 0$ and hence $\zeta_3^2 = -1 - \zeta_3$. The ring of Eisenstein integers, denoted $\mathbf{Z}[\zeta_3]$, is the set of complex numbers of the form $\alpha = a + b\zeta_3$ with $a, b \in \mathbf{Z}$. For $\alpha = a + b\zeta_3$ we will define $d(\alpha) = \alpha\overline{\alpha} = a^2 + b^2 - ab$ which is the square of the usual analytic complex norm $|\alpha|$. Note that $d(\alpha)$ is a positive integer for $\alpha \neq 0$ since $d(\alpha)$ is the square of a norm and $a, b \in \mathbf{Z}$. For any complex numbers α, β we have that $|\alpha\beta| = |\alpha| . |\beta|$ hence it follows that $d(\alpha\beta) = d(\alpha).d(\beta)$. The Eisenstein integers $\mathbf{Z}[\zeta_3]$ form a lattice in X generated by the basis $B = \{1, \zeta_3\}$. Note that the two basis vectors 1 and ζ_3, represented by the vectors (1, 0) and $(-1/2, \sqrt{3}/2)$ in P^2, have 120 degrees with equal length. Let β be an Eisenstein integer. We define the ideal $L(\beta) = \{a\beta + b\beta\zeta_3 \mid a, b \in \mathbf{Z}\}$. Therefore $L(\beta)$ is a lattice generated by the basis $\{\beta, \beta\zeta_3\}$. According to [7], we deduce that the Eisenstein integers are an Euclidean domain that the units and Eisenstein primes exist. For each matrix *B* with entries that are Eisenstein integers we will set < *B* > to be the *2n* by *2n* matrix. We choose an prime *n* and set $R = \mathbf{Z}[\zeta_3, x]/ < x^n - 1 >$, we also choose *p*

and q in $\mathbf{z}[\zeta_3]$ relatively prime, with $|q|$ much larger than $|p|$. Since each ETRU coefficient is a pair of integers, an element of ETRU at degree n is comparable with an element of NTRU of degree $n' = 2n$.

2.2. Key Generation

Private key consists of two randomly chosen polynomials f, g in R. We define the inverses $Fq = f^{-1}$ in Rq and $Fp = f^{-1}$ in Rp. Hence public key is generated by $h = Fq * g$. The public key h is a polynomial with n coefficients which are reduced modulo q. Each coefficient consists of two integers which by Theorem 3 in [7] can be stored as binary strings of length $\lceil \log_2(4|q|/3) \rceil$, hence the size of the ETRU public key is $K = 2n\lceil \log_2(4|q|/3) \rceil$. An NTRU public key, corresponding to polynomials with $n' = 2n$ coefficients reduced modulo an integer q', has size $K' = n'\lceil \log_2(q') \rceil$. Therefore to maintain the same key size as NTRU with $n' = 2n$ and $q' = 2k$, we should choose $|q| \leq (3/4)q'$ so that $\lceil \log_2(4|q|/3) \rceil \leq \lceil \log_2(q') \rceil$.

2.3. Encryption

Each encryption requires the user to compute $e = \phi * ph + m \bmod q$ where m is a plaintext and ϕ is a ephemeral key. In total one counts $n'^2 + n' \sim 4n^2 + 2n$ operations for NTRU encryption at $n' \sim 2n$ in contrast to only $3n^2 + 27n$ operations for ETRU encryption.

2.4. Decryption

Each decryption requires the user to compute both $a = f * e \bmod q$ and $m = F_p * a \bmod p$. For decryption, we have $2n'^2 + 2n' \sim 8n^2 + 4n$ operations for NTRU and only $6n^2 + 29n$ operations for ETRU.

2.5. Decryption Failure and Security

In [7] is shown that in fact $|q| \sim (3/8)q'$ is an optimal choice in view of security against decryption failure and lattice attacks. Based on this choice the public key size for ETRU will be smaller than that of the NTRU public key.

3. Ideal Lattices and Their Hard Problems

Our results are restricted to the sequence of rings $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ with $\Phi = < (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + \ldots + (1,1,1,1)x + (1,1,1,1) >$ where n+1 is a prime

that Φ is irreducible cyclotomic polynomial. We can refer to [19] for irreducibility of cyclotomic polynomials F_n in $\mathbf{Z}[z_3][x]$ where n is prime in $\mathbf{Z}[z_3]$ The R-LWE problem is known to be hard when Φ is cyclotomic [16]. The security analysis for our proposed scheme allows encrypting and decrypting $\Omega(n)$ plaintext bits for $\tilde{O}(n)$ bit operations, while achieving security against $2^{g(n)}$ -time attacks, for any $g(n)$ that is $\Omega(\log n)$ and $o(n)$, assuming the worst-case hardness of $poly(n)$-Ideal-SVP against $2^{O(g(n))}$-time quantum algorithms for each element component-wise in complex pair-wise system because note that each polynomial in R has its coefficients of the form $((a_i, b_i z_3), (c_i, d_i z_3))(a_i, b_i \zeta_3)$ where $a_i, b_i, c_i, d_i \in \mathbf{Z}$, so in this paper, all operations execute for a_i's, b_i's, c_i's and d_i's separately, that is, $X \cong P^2$ component-wise. The latter assumption is believed to be valid for any $g(n)=o(n)$. Also we can define £ and ³ as poset orders.

3.1. Notation

Similar to [14] we denote by $\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}(x_1, x_2, x_3, x_4)$ (respectively $\upsilon_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$) the standard n-dimensional Gaussian function (respectively distribution) with center (0,0,0,0) and variance $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. We denote by $Exp(\mu)$ the exponential distribution on P^{4n} with mean μ and by $U(E)$ the uniform distribution over a finite set E. If D_1 and D_2 are two distributions on discrete oracle E, their statistical distance is $\Delta(D_1; D_2) = 1/2\sum_{x\in E} | D_1(x_1, x_2, x_3, x_4) - D_2(x_1, x_2, x_3, x_4) |$. We write $z \leftarrow D$ when the random variable z is chosen from the distribution D. The integer n is called the *lattice dimension*. Note that in our proposed scheme with pairwise components and coefficients in vectors, the dimension increases four times without increasing n. The *minimum* $\lambda_1(L)$ (respectively $\lambda_1^{\infty}(L)$) is the Euclidean (respectively infinity) norm of any shortest vector of $L \setminus (0,0,0,0)$.

The *dual* of lattice L is the lattice $\hat{L} = \{(c_1, c_2, c_3, c_4) \in R^{4n} : \forall i, <(c_1, c_2, c_3, c_4), (b_{i1}, b_{i2}, b_{i3}, b_{i4})> \in \mathbf{Z}^4\}$ where the b_{ij}'s are a *basis* of L. For a lattice L, $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) > (0, 0, 0, 0)$ and $(c_1,c_2,c_3,c_4) \in P^{4n}$, we define the *lattice Gaussian distribution* of support L, deviation $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ and center (c_1,c_2,c_3,c_4) by

$D_{L,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1, b_2, b_3, b_4) = \rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1, b_2, b_3, b_4) / \rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(L)$, for any $(b_1, b_2, b_3, b_4) \in L$.

We extend the definition of $D_{L,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}$ to any $M \subseteq L$ (not necessarily a sub-lattice), by setting

$D_{M,(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1,b_2,b_3,b_4) = (\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(b_1,b_2,b_3,b_4)) / (\rho_{(\sigma_1,\sigma_2,\sigma_3,\sigma_4),(c_1,c_2,c_3,c_4)}(M))$ and for

$(\delta_1,\delta_2,\delta_3,\delta_4) > (0,0,0,0)$, we denote the *smoothing parameter* $\eta_{(\delta_1,\delta_2,\delta_3,\delta_4)}(L)$ as the smallest $(\sigma_1,\sigma_2,\sigma_3,\sigma_4) > (0,0,0,0)$ such that

$\rho_{(1,1,1,1)/(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}(\hat{L} \setminus (0,0,0,0)) \le (\delta_1,\delta_2,\delta_3,\delta_4)$.

It quantifies how large $(\sigma_1,\sigma_2,\sigma_3,\sigma_4)$ needs to be for $D_{L,(\sigma_1,\sigma_2,\sigma 3,\sigma_4),(c_1,c_2,c_3,c_4)}$ to behave like a continuous Gaussian. We will typically consider $\delta_i = 2^{-n}$.

3.2. Definition

Let *n*+1 be a prime and $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ which is irreducible over $\mathrm{Q}[z_3]' \ \mathrm{Q}[z_3]$ also let $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$. An (integral) ideal *I* of *R* is a subset of *R* closed under addition and multiplication by arbitrary elements of *R*. By mapping polynomials to the vectors of their coefficients, we see that an ideal $I \neq (0,0,0,0)$ corresponds to a full-rank sub-lattice of Z^{4n}. Thus we can view *I* as both a lattice and an ideal. An *ideal lattice* for Φ is a sub-lattice of $(Z*Z)^{2n}$ that corresponds to a non-zero ideal $I \subseteq R$. The *algebraic norm N*(*I*) is equal to det *I*, where *I* is regarded as a lattice. In the following, an ideal lattice will implicitly refer to a Φ -ideal lattice.

By restricting SVP (respectively γ -SVP) to instances that are ideal lattices, we obtain Ideal-SVP (respectively γ -ideal-SVP). The latter is implicitly parameterized by the polynomial $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$. No algorithm is known to perform non-negligibly better for γ -ideal-SVP than for γ -SVP [14].

3.3. Properties of The Ring of Cartesian Product

For $(v_1,v_2,v_3,v_4) \in R$ we define by ||(v_1, v_2, v_3, v_4)|| its Euclidean norm. We denote the multiplicative *expansion factor* by

$\gamma_{\times}(R) = \max_{u_i,v_i \in R}(\| (u_1,u_2,u_3,u_4) \times (v_1,v_2,v_3,v_4) \|) / (\| (u_1,u_2,u_3,u_4) \| . \| (v_1,v_2,v_3,v_4) \|)$.

Since Φ is the *n+1*-th cyclotomic polynomial, the ring *R* is exactly the maximal order of the cyclotomic field $K := \frac{(\mathrm{Q}[z_3]' \ \mathrm{Q}[z_3])[x]}{\mathrm{F}} @ \mathrm{Q}[z,z']$. We denote by $(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4})_{i \le n}$ the complex embeddings. We can choose $(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4}) : K \to K(\zeta_1^{2i+1},\zeta_2^{2i+1},\zeta_3^{2i+1},\zeta_4^{2i+1})$ for $i \le n$.

Lemma 3.1. *The norm of* α *as an element in* $\Theta(\zeta_3)$ *is* $a^2 + b^2$ *- ab. This is also* $|\alpha|^2$, *where* α *is denoted as an element of* **X**.

Proof. The minimal polynomial of ζ_3 over Θ is the cyclotomic polynomial $\Phi_3 = x^2 + x + 1$. Thus, there exist exactly two monomorphisms (isomorphisms in this case) from Θ to X fixing Θ and permuting the roots of Φ_3. Since Φ_3 has two roots ζ_3 and ζ_3^2, the embeddings are $\sigma_1(a+b\zeta_3) = a+b\zeta_3$ and $\sigma_2(a+b\zeta_3) = a+b\zeta_3^2$, where $a, b \in \Theta$. By definition, the algebraic norm of $\alpha = a+b\zeta_3$ is

$$N(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha)$$
$$= (a+b\zeta_3)(a+b\zeta_3^2)$$

Note that $\zeta_3^2 = \overline{\zeta}_3$ and $\zeta_3 + \overline{\zeta}_3 = -1$. So we have

$$N(\alpha) = (a+b\zeta_3)(a+b\overline{\zeta}_3)$$
$$= a^2 + b^2 + ab(\zeta_3 + \overline{\zeta}_3)$$
$$= a^2 + b^2 - ab$$

Now we show that $d(\alpha) = N(\alpha) = |\alpha|^2$.

$$|\alpha|^2 = |a+b\zeta_3|^2$$
$$= |a+b(\frac{-1+\sqrt{3}i}{2})|$$
$$= |a-\frac{b}{2}+\frac{b\sqrt{3}i}{2}|^2$$
$$= \left(a-\frac{b}{2}\right)^2 + \left(\frac{b\sqrt{3}}{2}\right)^2$$
$$= a^2 + b^2 - ab$$

□

In rest of the paper, all of computations are done component-wise for each complex element as an integer. We define T_2-norm by $T_2(\alpha_1,\alpha_2,\alpha_3,\alpha_4)^2 = (\sum_{i\le n}|\sigma_{i1}(\alpha_1)|^2, \sum_{i\le n}|\sigma_{i2}(\alpha_2)|^2, \sum_{i\le n}|\sigma_{i3}(\alpha_3)|^2, \sum_{i\le n}|\sigma_{i4}(\alpha_4)|^2)$. We also use the fact that for any $(\alpha_1,\alpha_2,\alpha_3,\alpha_4) \in R$, we have $|N(\alpha_1,\alpha_2,\alpha_3,\alpha_4)|$ = det $< (\alpha_1,\alpha_2,\alpha_3,\alpha_4) >$, where $<(\alpha_1,\alpha_2,\alpha_3,\alpha_4)>$ is the ideal of R generated by $(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$. Let (q_1, q_2, q_3, q_4) be a prime element such that Φ has n distinct linear factors modulo (q_1, q_2, q_3, q_4), that is,
$\Phi = (\prod_{i\le n}((x_1,x_2,x_3,x_4) - (\zeta_1^i, \zeta_2^i, \zeta_3^i, \zeta_4^i)) \bmod (q_1,q_2,q_3,q_4)$ where ζ_i's are primitive $n+1$-th root of unity modulo (q_1, q_2, q_3, q_4) component-wise. Also we know that $R_{(q_1,q_2,q_3,q_4)} = R/(q_1R)' R/(q_2R)' R/(q_3R)' R/(q_4R)$.

3.4. Adaptation of Ideal Lattice Problems

Definition 3.1. *The ring small integer solution problem with parameters* $(q_1, q_2, q_3, q_4), m, (b_1, b_2, b_3, b_4), \mathrm{F}$ *is: Given m polynomials* $(a_{11}, a_{21}, a_{31}, a_{41}), ..., (a_{m1}, a_{m1}, a_{m1}, a_{m1})$ *chosen uniformly and independently in* $R_{(q_1,q_2,q_3,q_4)}$, *find* (t_1, t_2, t_3, t_4) *in assumed R-module such that* $\| (t_1, t_2, t_3, t_4) \| £ (b_1, b_2, b_3, b_4)$.

In [14] is shown that R-SIS and R-LWE are dual. For $(s_1, s_2, s_3, s_4) \in R_{(q_1,q_2,q_3,q_4)}$ and $(\psi_1, \psi_2, \psi_3, \psi_4)$ some distributions in $R_{(q_1,q_2,q_3,q_4)}$, we have $A_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ as the distribution obtained by sampling the pair $((a_1, a_2, a_3, a_4), (a_1, a_2, a_3, a_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4))$ with $((a_1, a_2, a_3, a_4), (e_1, e_2, e_3, e_4)) \leftarrow U(R_{(q_1,q_2,q_3,q_4)}) \times (\psi_1, \psi_2, \psi_3, \psi_4)$. The Ring Learning With Errors problem (R-LWE) was introduced by Lyubashevsky *et al.*[16] and shown hard for specific error distributions ψ. The error distributions $(\psi_1, \psi_2, \psi_3, \psi_4)$ that we use are an adaptation of those introduced in [16].

Definition 3.2. $(R - LWE^{\Phi}_{(q_1,q_2,q_3,q_4),(\alpha_1,\alpha_2,\alpha_3,\alpha_4)})$*: Let* $(\psi_1, \psi_2, \psi_3, \psi_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ *and* $(s_1, s_2, s_3, s_4) \leftarrow U(R_{(q_1,q_2,q_3,q_4)})$ *where* $\overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ *is a family of distributions. Given access to an oracle O that produces samples in* $R_{(q_1,q_2,q_3,q_4)} \times R_{(q_1,q_2,q_3,q_4)}$ *, distinguish whether O outputs samples from* $A_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ *or from* $U(R_{(q_1,q_2,q_3,q_4)} \times R_{(q_1,q_2,q_3,q_4)})$. *The distinguishing advantage should be* $1/poly(n)$ $(resp.\ 2^{-o(n)})$ *over the randomness of the input, the randomness of the samples and the internal randomness of the algorithm, component-wise [14].*

Theorem 1 in [14] indicates that R-LWE is hard, assuming that the worst-case γ-Ideal-SVP cannot be efficiently solved using quantum computers, for small γ. It was recently improved by Lyubashevsky *et al.* [18] if the number of samples that can be chosen to the oracle *O* is bounded by a constant (which is the case in our application), then the result also holds with simpler errors than $(e_1, e_2, e_3, e_4) \leftarrow (\psi_1, \psi_2, \psi_3, \psi_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$, and with an even smaller Ideal-SVP approximation factor γ. This should allow to both simplify the proposed scheme and to strengthen its security guarantee.

3.5. Our Proposed Variants of R-LWE

For $(s_1, s_2, s_3, s_4) \in R_{(q_1,q_2,q_3,q_4)}$ and $(\psi_1, \psi_2, \psi_3, \psi_4)$ some distributions in $R_{(q_1,q_2,q_3,q_4)}$, we denote $A^{\times}_{(s_1,s_2,s_3,s_4),(\psi_1,\psi_2,\psi_3,\psi_4)}$ as the distribution obtained by sampling

the pair $((a_1,a_2,a_3,a_4),(a_1,a_2,a_3,a_4)(s_1,s_2,s_3,s_4)+(e_1,e_2,e_3,e_4))$ with $((a_1,a_2,a_3,a_4),(e_1,e_2,e_3,e_4)) \leftarrow U(R^{\times}_{(q_1,q_2,q_3,q_4)})\times(\psi_1,\psi_2,\psi_3,\psi_4)$, where $R^{\times}_{(q_1,q_2,q_3,q_4)}$ is the set of invertible elements of $R_{(q_1,q_2,q_3,q_4)}$. This variant is hard and called $R-LWE^{\times}_{++}$ as [14]. Furthermore, as explained in [18], the nonce (s_1,s_2,s_3,s_4) can also be sampled from the error distribution without incurring any security loss. We call this variant $R-LWE^{\times}_{HNF++}$. According to adaptation of lemmas 7, 8 and 9 as well as Theorem 2 in [14] the problems $R-LWE^{\times}_{++}$ and $R-LWE^{\times}_{HNF++}$ are dual to γ-Ideal-SVP and are defined some families of *R*-modules for *I*, an arbitrary ideal of $R_{(q_1,q_2,q_3,q_4)}$ as a lattice, also short vectors exist in ideal and statistical distance (regularity bound) is exactly appropriate and reliable.

4. The Proposed Key Generation Algorithm

We now use the results of the previous section on modular ideal lattice to derive a key generation algorithm for the ETRU for each component in vectors, where the generated public key follows a distribution for which Ideal-SVP reduces to R-LWE. Algorithm 1 is as follows.

Input: $n, q_1, q_2, q_3, q_4 \in \mathbf{Z}, p_1, p_2, p_3, p_4 \in R^{\times}_{(q_1,q_2,q_3,q_4)}, (\sigma_1,\sigma_2,\sigma_3,\sigma_4) \in \mathbf{R}$.

Output: A key pair $(sk, pk) \in R \times R^{\times}_{(q_1,q_2,q_3,q_4)}$.

Sample $(f_1, f_2, f_3, f_4)'$ from $D_{\mathbf{Z}^{4n},(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$; let $(f_1, f_2, f_3, f_4) = (p_1, p_2, p_3, p_4).(f_1, f_2, f_3, f_4)'+(1,1,1,1)$; if $((f_1, f_2, f_3, f_4) \mod (q_1, q_2, q_3, q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}$, resample. Sample (g_1, g_2, g_3, g_4) from $D_{\mathbf{Z}^{4n},(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}$; if $((g_1, g_2, g_3, g_4) \mod (q_1, q_2, q_3, q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}$, resample. Return secret key $sk = (f_1, f_2, f_3, f_4)$ and public key $pk = (h_1, h_2, h_3, h_4) = (p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4) / (f_1, f_2, f_3, f_4) \hat{I}\ R^{'}_{(q_1,q_2,q_3,q_4)}$.

The following Theorem ensures that for some appropriate choice of parameters, the key generation algorithm terminates in expected polynomial time.

Theorem 4.1[Adapted from 14]**.** *Let* $n \geq 8$ *and n+1 be a prime such that* $\Phi = <(1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1)>$ *splits into n linear factors modulo prime* $(q_1,q_2,q_3,q_4) \geq (5,5,5,5)$ *component-wise. Let*

$\sigma_i \geq \sqrt{n \ln(2n(1+1/\delta_i))/\pi}.q_i^{1/n}$, *or an arbitrary* $\delta_i \in (0,1/2)$. *Let* $(a_1, a_2, a_3, a_4) \in R$ *and* $(p_1, p_2, p_3, p_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$

Then

$\Pr_{(f_1,f_2,f_3,f_4)' \leftarrow D_{\mathbb{Z}^4,(\sigma_1,\sigma_2,\sigma_3,\sigma_4)}}[((p_1,p_2,p_3,p_4).(f_1,f_2,f_3,f_4)'+(a_1,a_2,a_3,a_4) \bmod (q_1,q_2,q_3,q_4)) \notin R^{\times}_{(q_1,q_2,q_3,q_4)}] \leq n((1,1,1,1)/(q_1,q_2,q_3,q_4)+$
$+2(\delta_1,\delta_2,\delta_3,\delta_4))$

component-wise.

The following Lemma ensures that the generated secret key is small.

Lemma 4.1[Adapted from 14]**.** *Let* $n \geq 8$ *and n+1 be a prime such that* $\Phi = <(1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1)>$ *splits into n linear factors modulo prime* $(q_1, q_2, q_3, q_4) \geq (8,8,8,8)n$. *Let* $\sigma_i \geq \sqrt{2n \ln(6n)/\pi}.q_i^{1/n}$. *The secret key polynomials* $(f_1, f_2, f_3, f_4), (g_1, g_2, g_3, g_4)$ *returned by the algorithm* 1 *satisfy, with probability* $\geq 1 - 2^{-n+3}$:
$\| (f_1, f_2, f_3, f_4) \| \leq (2,2,2,2)n \| (p_1, p_2, p_3, p_4) \| (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *and* $\| (g_1, g_2, g_3, g_4) \| \leq \sqrt{n}(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$.
If $\deg(p_1, p_2, p_3, p_4) \leq (1,1,1,1)$, then

$\| (f_1, f_2, f_3, f_4) \| \leq (4,4,4,4)\sqrt{n} \| (p_1, p_2, p_3, p_4) \| (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ *with probability* $\geq 1 - 2^{-n+3}$ *component-wise.*

Theorem 3 in [14] shows that the public key can be uniformly distributed in the whole ring and this satisfy cryptographic pseudo randomness for our Algorithm 1, which seems necessary for exploiting the established hardness of R-LWE (and R-SIS). Now we can construct the proposed cryptosystem over ideal lattices with high efficiency and provable security (CPA-secure).

5. The Proposed New Cryptosystem

Using our new results above, we describe our proposed cryptosystem for which we can provide a security proof under a worst-case hardness assumption.

5.1. Decryption Failure

The correctness condition for each pairwise coefficient in the proposed cryptosystem is as follows.

Lemma 5.1 [Adapted from 14]**.** *If* $\omega(n^{1.5} \log n)\alpha_i \deg((p_i)) \| (p_i) \|^2 \sigma_i < (1,1,1,1)$ *(resp.* $\omega(n^{0.5} \log n)\alpha_i \| (p_i) \|^2 \sigma_i < (1,1,1,1)$ *if* $\deg(p_i) \leq (1,1,1,1)$*)* *and* $\alpha_i q_i \geq n^{0.5}$, *then the decryption algorithm of the proposed cryptosystem recovers* (M_1, M_2, M_3, M_4) *with probability* $1 - n^{-\omega(1)}$ *over the choice of* s_i, e_i, f_i *and* g_i *component-wise.*

Proof. In the decryption algorithm, we have

$$(C_1, C_2, C_3, C_4)' = (p_1, p_2, p_3, p_4).((g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4)(f_1, f_2, f_3, f_4)) +$$
$$+ (f_1, f_2, f_3, f_4)(M_1, M_2, M_3, M_4) \bmod (q_1, q_2, q_3, q_4)$$

and let

$$(C_1, C_2, C_3, C_4)'' = (p_1, p_2, p_3, p_4).((g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4) + (e_1, e_2, e_3, e_4)(f_1, f_2, f_3, f_4)) +$$
$$+ (f_1, f_2, f_3, f_4)(M_1, M_2, M_3, M_4)$$

computed in R (not modulo (q_1, q_2, q_3, q_4)). If $\| (C_1, C_2, C_3, C_4)'' \|_\infty < (q_1, q_2, q_3, q_4)/2$ then we have $(C_1, C_2, C_3, C_4)' = (C_1, C_2, C_3, C_4)''$ in R and hence, since $(f_i) \equiv (1,1,1,1) \bmod (p_i), (C_i)' \bmod (p_i) = (C_i)'' \bmod (p_i) = (M_i) \bmod (p_i)$, i.e., the decryption algorithm succeeds. It thus suffices to give an upper bound on the probability that $\| (C_1, C_2, C_3, C_4)'' \|_\infty > (q_1, q_2, q_3, q_4)/2$. From Lemma 2, we know that with probability $\geq 1 - 2^{-n+3}$ both (f_1, f_2, f_3, f_4) and (g_1, g_2, g_3, g_4) have Euclidean norms $\leq 2n \| (p_i) \| \sigma_i$ $(resp.\ (4,4,4,4)\sqrt{n} \| (p_i) \| \sigma_i$ *if* $\deg(p_i) \leq (1,1,1,1))$ this implies that, $\| (p_i)(f_i) \|, \| (p_i)(g_i) \| \leq (2,2,2,2) n^{1.5} \| (p_i) \|^2 \sigma_i$ $(resp.\ (8,8,8,8)\sqrt{n} \| (p_i) \|^2 \sigma_i)$ with probability $\geq 1 - 2^{-n+3}$. From Lemma 6 in [14], both $(p_1, p_2, p_3, p_4)(f_1, f_2, f_3, f_4)(e_1, e_2, e_3, e_4)$ and $(p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4)(s_1, s_2, s_3, s_4)$ have infinity norm

$(resp. \leq (2,2,2,2)\alpha_i q_i n^{1.5} \omega(\log n). \| (p_i) \|^2 \sigma_i$ $(8,8,8,8)\alpha_i q_i \sqrt{n} \omega(\log n). \| (p_i) \|^2 \sigma_i$), with probability $1 - n^{-\omega(1)}$. Independently:

Proposed Encryption Scheme

Parameters Creation:

1. We use $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ with $n \geq 8$ and $n+1$ a prime, $R := (\mathbf{Z}[z_3]' \ \mathbf{Z}[z_3])[x]/ < \mathrm{F} >$ and $R_{(q_1,q_2,q_3,q_4)} = R/(q_1R) \times R/(q_2R) \times R/(q_3R) \times R/(q_4R)$ with $(q_1,q_2,q_3,q_4) \geq (5,5,5,5)$ prime such that $\Phi = \prod_{k=1}^{n} \phi_k$ in $R_{(q_1,q_2,q_3,q_4)}$ with distinct ϕ_k's component-wise.

Key Generation:

2. We use the algorithm 1 and return $sk = (f_1, f_2, f_3, f_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$ with $(f_1, f_2, f_3, f_4) \equiv (1,1,1,1) \bmod (p_1, p_2, p_3, p_4)$, and $pk = (h_1,h_2,h_3,h_4) = (p_1, p_2, p_3, p_4)(g_1, g_2, g_3, g_4) / (f_1, f_2, f_3, f_4) \hat{\mathrm{I}} \ R'_{(q_1,q_2,q_3,q_4)}$, component-wise.

Encryption:

3. Given message $(M_1,M_2,M_3,M_4) \in P$, set $(s_1, s_2, s_3, s_4), (e_1, e_2, e_3, e_4) \leftarrow \overline{\Upsilon}_{(\alpha_1,\alpha_2,\alpha_3,\alpha_4)}$ and return ciphertext $(C_1,C_2,C_3,C_4) = (h_1,h_2,h_3,h_4)(s_1,s_2,s_3,s_4) + (p_1,p_2,p_3,p_4)(e_1,e_2,e_3,e_4) + (M_1,M_2,M_3,M_4) \in R_{(q_1,q_2,q_3,q_4)}$

Decryption:

4. Given ciphertext (C_1,C_2,C_3,C_4) and secret key (f_1, f_2, f_3, f_4), compute $(C_1,C_2,C_3,C_4)' = (f_1, f_2, f_3, f_4).(C_1,C_2,C_3,C_4) \in R_{(q_1,q_2,q_3,q_4)}$ and return $(C_1,C_2,C_3,C_4)' \bmod (p_1, p_2, p_3, p_4)$.

$$\| (f_i)(M_i) \|_\infty \leq \| (f_i)(M_i) \| \leq \sqrt{n} \| (f_i) \| . \| (M_i) \| \leq (2,2,2,2).(\deg(p_i) + (1,1,1,1).n^2 \| (p_i) \|^2 \ \sigma_i$$

(resp. $(8,8,8,8)n \| (p_i) \|^2 \ \sigma_i$). Since $\alpha_i q_i \geq \sqrt{n}$, we conclude that $\| (C_i)'' \|_\infty \leq ((6,6,6,6) + (2,2,2,2)\deg(p_i)).\alpha_i q_i n^{1.5} \omega(\log n). \| (p_i) \|^2 \ \sigma_i$ (resp. $(24,24,24,24)\alpha_i q_i n^{0.5} \omega(\log n). \| (p_i) \|^2 \ \sigma_i$), with probability $1 - n^{-\omega(1)}$, component-wise.

□

5.2. Security

The security of the proposed cryptosystem follows by an elementary reduction from the decisional $R-LWE^{\times}_{HNF++}$, exploiting the uniformity of the public key in $R^{\times}_{(q_1,q_2,q_3,q_4)}$ (adaptation of Theorem 3 in [14]), and the invertibility of (p_1, p_2, p_3, p_4) in $R_{(q_1,q_2,q_3,q_4)}$.

Lemma 5.2 [adapted from 7]**.** *Suppose n+1 is a prime such that* $\Phi =< (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ *splits into n linear factors modulo prime* $q_i = \omega(1)$. *Let* $\sigma_i \geq (2,2,2,2)n\sqrt{\ln(8nq_i)}.q_i^{(1/2,1/2,1/2,1/2)+\varepsilon_i}$ *and* $(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4),(\delta_1,\delta_2,\delta_3,\delta_4) > (0,0,0,0), (p_1, p_2, p_3, p_4) \in R^{\times}_{(q_1,q_2,q_3,q_4)}$. *If there exists an IND-CPA attack against the proposed cryptosystem that runs in time T and has success probability* $(1/2,1/2,1/2,1/2)+\delta_i$ *with parameters* αi *and* q_i*, then there exists an algorithm solving* $R-LWE^{\times}_{HNF++}$ *that runs in time T' = T + O(n) and has success probability* $\delta_i' = \delta_i - q_i^{-\Omega(n)}$.

Proof. Let *A* denote the given IND-CPA attack algorithm. We construct an algorithm *B* against $R-LWE^{\times}_{HNF++}$ that runs as follows, given oracle *O* that samples from either $U(R^{\times}_{q_i} \times R_{q_i})$ or $A^{\times}_{s_i,\psi_i}$ for some previously chosen $s_i \leftarrow \psi_i$ and $\psi_i \leftarrow \bar{\Upsilon}_{\alpha_i}$. Algorithm *B* first calls *O* to get a sample $((h_i)', (C_i)')$ from $R^{\times}_{q_i} \times R_{q_i}$. Then, algorithm *B* runs *A* with public key $(h_i) = (p_i).(h_i)' \in R_{q_i}$. When *A* outputs challenge messages $(M_{0i}), (M_{1i}) \in P$, algorithm *B* picks $b \leftarrow U(\{0,1\})$, computes the challenge ciphertext $(C_i) = (p_i).(C_i)' + (M_{bi}) \in R_{q_i}$, and returns (C_i) to *A*. Eventually, when *A* outputs its guess *b'* for *b*, algorithm *B* outputs 1 if *b' = b* and 0 otherwise. The $(h_i)'$ used by *B* is uniformly random in $R^{\times}_{q_i}$ and therefore so is the public key (h_i) given to *A*, thanks to the invertibility of (p_i) modulo (q_i). Thus, by Theorem 3 in [14], the public key given to *A* is within statistical distance $q^{-\Omega(n)}$ of the public key distribution in the genuine attack, component-wise. Moreover, since $(C_i)' = (h_i).s_i + e_i$ with $s_i, e_i \leftarrow \psi_i$, the ciphertext (C_i) given to *A* has the right distribution as in the IND-CPA attack. Overall, if *O* outputs samples from $A^{\times}_{s_i,\psi_i}$ then *A* succeeds and *B* returns 1 with probability $\geq (1/2,1/2,1/2,1/2) + \delta_i - q_i^{-\Omega(n)}$. Now, if *O* outputs samples from $U(R^{\times}_{q_i} \times R_{q_i})$, then, since $p_i \in R^{\times}_{q_i}$, the value of $(p_i)(C_i)'$ and hence (C_i), is uniformly random in R_{qi} and independent of *b*. It follows that *B* outputs 1 with probability 1/2, component-wise. The claimed advantage of *B* follows. □

By combining lemmata 3 and 4 (with adaptation of Theorem 1 in [14]) we obtain main result.

6. Conclusions

In this paper, we provided a new cryptosystem that uses the properties of the ETRU cryptosystem and its structured lattice to achieve high efficiency by providing a provable security (CPA-secure) based on ideal lattices and a variant of R-LWE problem. Also we showed that each polynomial in $R = (\mathbf{Z}[\zeta_3] \times \mathbf{Z}[\zeta_3])[x] / < (1,1,1,1)x^n + (1,1,1,1)x^{n-1} + ... + (1,1,1,1)x + (1,1,1,1) >$ has its coefficients of the form $((a_i, b_i z_3), (c_i, d_i z_3))$ where $a_i, b_i, c_i, d_i \in \mathbf{Z}$, so we made both lemmata and theorems here for a_i's, b_i's, c_i's and d_i's separately, that is, we reflected $(C, C) @ (R^2, R^2)$. Hence, we could enhance the dimension of lattice 4-times without increasing *n*.

References

[1] W. Diffie and M.E. Hellman, "*New directions in cryptography*," In IEEE Trans. On Information Theory, (1976), 22, 644-654.

[2] J. Hoffstein, J. Pipher, and J.H. Silverman, "*NTRU: a new high speed public-key cryptosystem*," Preprint; presented at the rump session of Crypto (1996).

[3] D. Coppersmith and A. Shamir, "*Lattice attacks on NTRU*," In Fumy, W. (ed.) EUROCRYPT, LNCS, (1997), 1233, 52–61.

[4] J. Hoffstein, J. Pipher, and J.H. Silverman, "*NTRU: A ring-based public-key cryptosystem*," In Buhler, J.P. (ed.) ANTS, LNCS, (1998), 1423, 267–288.

[5] IEEE P1363. Standard specifications for public-key cryptography, http://grouper.ieee.org/groups/1363/

[6] R.A. Perlner and D.A. Cooper, "*Quantum resistant public-key cryptography: a survey*," In Proc. of IDtrust, ACM, New York, (2009), 85–93.

[7] K. Jarvis and M. Nevins, "*ETRU: NTRU over the Eisenstein Integers*," Designs, Codes and Cryptography, DOI: 10. 1007/s10623-013-9850-3, (2013).

[8] M. Ajtai and C. Dwork, "*A public-key cryptosystem with worst-case/average-case equivalence*," In Proceedings of STOC, ACM, (1997), 284-293.

[9] V. Lyubashevsky and D. Micciancio, "*On bounded distance decoding, unique shortest vectors, and the minimum distance problem*," In Proceedings of Crypto, (2009), 5677, 450-461.

[10] D. Micciancio, "*Generalized compact knapsacks, cyclic lattices, and efficient oneway functions*," Computational Complexity, (2007), 16, 4, 365-411.

[11] V. Lyubashevsky and D. Micciancio, "*Generalized compact knapsacks are collision resistant*," In Proceedings of ICALP, (2006), 4052, 144-155.

[12] C. Peikert and A. Rosen, "*Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices*," In Proceedings of TCC, (2006), 145-166.

[13] O. Regev, "*On lattices, learning with errors, random linear codes, and cryptography*," Journal of ACM, (2009), 56, 6.

[14] D. Stehle and R. Steinfeld, "*Making NTRU as Secure as Worst-Case Problems over Ideal Lattices*," In Eurocrypt, (2011), 6632, 27-47.

[15] M. Nevins, C. Karimianpour, and A. Miri, "*NTRU over rings beyond Z*," Des. Codes Cryptogr., (2010), 56, 1, 65–78.

[16] V. Lyubashevsky, C. Peikert, and O. Regev, "*On ideal lattices and learning with errors over rings*," In Gilbert, H. (ed.) EUROCRYPT, (2010), 6110, 1–23.

[17] C. Gentry, "*Fully homomorphic encryption using ideal lattices*," In Proc. of STOC, (2009), 169–178.

[18] V. Lyubashevsky, C. Peikert, and O. Regev, "*On ideal lattices and learning with errors over rings*," Draft version, dated 01/02/2011.

[19] P. Garrett, "*Abstract Algebra*," University of Minnesota, (2007), 211-217.

[20] R.E. Atani, S.E. Atani, and A.H. Karbasi, "*EEH: A GGH-Like Public Key Cryptosystem Over The Eisenstein Integers Using Polynomial Representation*," The ISC International Journal of Information Security (IseCure), (2015), 7, 2, 115-126.

[21] A.H. Karbasi and R.E. Atani, "*ILTRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices*," IACR Cryptology ePrint Archive, (2015), 549.

[22] A.H. Karbasi and R.E. Atani, "*PSTRU: A provably secure variant of NTRUEncrypt over extended ideal lattices*," The 2nd National Industrial Mathematics Conference, Tabriz, Iran, (2015).

[23] A.H. Karbasi and R.E. Atani, "*A Survey on Lattice-based Cryptography*," (in Persian), Biannual Journal for Cyberspace Security (Monadi AFTA), (2015), 3, 1, 3-14.

[24] A.H. Karbasi, M.A. Nia, and R.E. Atani, "*Designing of An Anonymous Communication System Using Lattice-based Cryptography*," (in Persian), Journal of Electronic and Cyber Defence, (2014), 2, 3, 13-22.

[25] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*A Provably Secure Variant of ETRU Based on Extended Ideal Lattices over Direct Product of Dedekind domains*," Submitted.

[26] A.H. Karbasi, R.E. Atani, and S.E. Atani, "*A New Ring-Based SPHF and PAKE Protocol On Ideal Lattices*," Submitted.

[27] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*PairTRU: Pairwise Non-commutative Extension of The NTRU Public key Cryptosystem*," International Journal of Information Security Science, (2018), 7, 1, 11-19.

[28] S.E. Atani, R.E. Atani, and A.H. Karbasi, "*NETRU: A Non-Commutative and Secure Variant of CTRU Cryptosystem*," The ISC international journal of information security (IseCure), (2018), 10, 1, 1-9.

[29] A.H. Karbasi and R.E. Atani, "*Application of dominating sets in wireless sensor networks*," Int. J. Security and its Application, (2013), 7, 4.

[30] A.H. Karbasi and R.E. Atani. "*Projective plane-based key pre-distribution by key copying and exchanging based on connected dominating set in distributed wireless sensor networks*," International Journal of Information and Communication Technology, (2016), 9, 4, 438-462.

[31] S. Tahouri, R.E. Atani, A.H. Karbasi, and Y. Deldjou, "*Application of connected dominating sets in wildfire detection based on wireless sensor networks*," International Journal of Information Technology, Communications and Convergence, (2015), 3, 2, 139-160.

Ratio Mathematica
Vol. 34, 2018, pp. 67–76

ISSN: 1592-7415
eISSN: 2282-8214

Algebraic Spaces and Set Decompositions.

Jan Chvalina[*], Bedřich Smetana[†]

Received: 13-06-2018. **Accepted**: 24-06-2018. **Published**: 30-06-2018

doi:10.23755/rm.v34i0.415

Abstract

The contribution is growing up from certain parts of scientific work by professor Borůvka in several ways. Main focus is on the decomposition theory, especially algebraized decompositions of groups. Professor Borůvka in his excellent and well-known book [3] has developped the decomposition (partition) theory, where the fundamental role belongs to so called generating decompositions. Furthermore, the contribution is also devoted to hypergroups, to algebraic spaces called also quasi-automata or automata without outputs. There is attempt to develop more fresh view point on this topic.

Keywords: algebraic space; decomposition; join space;
2010 AMS subject classifications: 20N20, 93A10, 20M35.

[*]Brno University of Technology, Brno, Czech Republic. chvalina@feec.vutbr.cz
[†]University of Defence, Brno, Czech Republic. bedrichsmetana@unob.cz

1 Introduction

The present contribution is growing up from certain parts of scientific work by professor Borůvka in several ways. First of all is the decomposition theory, especially algebraized decompositions of groups. Professor Borůvka in his excellent and well-known book [3] has developped the decomposition (partition) theory, in (and on) sets which is applied to decompositions on groupoids and groups where the fundamental role belongs to so called generating decompositions. It is to be noted that a decomposition $\overline{A}$ in a groupoid $(G,\cdot)$ is called *generating* if there exists, to any two-membered sequence of the elements $\bar{a},\bar{b}\in\overline{A}$ an element $\bar{c}\in\overline{A}$ such that $\bar{a}\bar{b}\subset\bar{c}$. With the decomposition $\overline{A}$ in a groupoid $(G,\cdot)$ there can be uniquely associate a groupoid denoted (in the mentioned book) by $\mathcal{U}$ and defined such a way that the carrier set of $\mathcal{U}$ is the decomposition $\overline{A}$ and the multiplication is defined by $\bar{a}\circ\bar{b}=\bar{c}$, where $\bar{a},\bar{b},\bar{c}\in\overline{A}$ are such elements (i. e. cosets) that $\bar{a}\cdot\bar{b}\subset\bar{c}$ in the groupoid $(G,\cdot)$. A special and important case of generating decompositions on a group $(G,\cdot)$ created by left on right cosets of an invariant (normal) subgroup $(H,\cdot)$ of $(G,\cdot)$ is the carrier of a factor-group G/H which is a factoroid created by cosets of the form $a\cdot H$ (or which is the same $H\cdot a$) for an invariant subgroup H of G. On the other hand if left or right decompositions generated by a subgroup H which is not invariant in a noncommutative group G are algebraized in a similar way as above, we get multivalued binary operations on these decompositions which determine a structure called a *multigroups* or a *hypergroup* by the latest terminology. This one has been done by Marty in 1934 and since the time these structures were investigated by many mathematicians in France, Italy, Greece, Roumania, USA, Canada , Czechoslovakia and elsewhere.

2 Preliminaries

A hypergroup in the sense of Marty is a pair $(H,\cdot)$ where H is a non-empty set and $\cdot: H\times H\to\mathcal{P}'(H)$ (the system of all non-empty subsets off H) is an associative multioperation (called also a hyperoperation) satisfying the reproduction axiom: $a\cdot H=H=H\cdot a$ for any $a\in H$ [11, 12].

A commutative hypergroup $(H,\cdot)$ is called a *join hypergroup* or a *join space* if it satisfies the *exchange condition*: For any quadruple $a,b,c,d\in H$ such that $a/b\cap c/d\neq\emptyset$ (where $a/b=\{x\in H; a\in x\cdot b\}$ and similarly for c/d) we have

$$(a\cdot d)\cap(b\cdot c)\neq\emptyset.$$

In the last years investigations of hypergroups which are determined by binary relations (i.e. the binary hyperoperation $\cdot$ is derived by a certain standard way from a given relation on its carrier set) are of certain interests in investigations on this

field. The notion of a join space has been introduced by W. Prenowitz and used by him and afterwards together with J. Jantosciak to built again several branches of geometry. In the opinion of professor P. Corsini - which is one of present leading personalities in the hypergroup theory - the presentation and development of geometry in the context of join spaces is an important moment in the recent history of mathematics. There are also close connections of the, mentioned structure to ternary spaces, especially formed by sets endowed by ternary betweenness relations, here.

It is to be noted that any abelian group is a join space with single-valued operations. A simple example of a non-trivial join space or a join hypergmup can be constructed from arbitrary (non-extremal) decomposition of a set: Let $\overline{A}$ be a decomposition on a non-empty set A. For any pair of elements $x, y \in A$ let us define $x \cdot y = \bar{a} \cup \bar{b}$, where $\bar{a}, \bar{b} \in \overline{A}$ are blocks of the given decomposition such that $x \in \bar{a}, y \in \bar{b}$. Then it is easy to see that $(A, \cdot)$ is a join hypergroup (a join space) in which for a pair $x, y \in A$ the fraction x/y is either a block of A containing x or $x/y = A$ whenever x, y belong to the same block of A.

The algebraic theory of automata is widely elaborated classical discipline; the golden age or which can be designated from the beginning of sixties up to the end of tne last century. Nevertheless fundamental publications from the earlier time due to N. Wiener, J. von Neumann, S. Ginsburg, M. A. Arbib, V. M. Gluškov, R. E. Kálmán, M. O. Rabin, D. Scott, S. Greibach, K. B. Krohn, J. L. Rhodes, E. F. More and others, have massive influence on the development of the automata and artificial languages theory. In spite of studies devoted to finite automata also infinite automata and their generalizations have been of some interests (cf. Ferenc Gécseg, István Peák nad others). It is to be noted that various concepts of a product of automata (the basic of which has been introduced and studied by M. V. Gluškov in 1961 as an abstract model of electronic cirquits) are treated in a large collection of studies devoted to this topics. During the years of investigations of the mentioned thema, there occure various modifications; most of them can be generalized to the case of multiautomata or to actions of multistructures. Investigations of automata in connection with multistructures yield more new impulses. It is evident that infinite antomata without outputs called also quasi-automata are in fact discrete modifications or "algebraic skelets" of dynamical systems. Objects of investigations of the mentioned theories can be also considered as special general systems and they are close to the control theory.

The other connection of this contribution to the research of professor Borůvka consists in investigations of group and semigroup actions on sets which are substantial parts of the algebraic concept of an automaton, namely if we concentrate on changes of states rather than outputs which has been used by professor Borůvka in his two-parted paper [4]. Automata without outputs are termed also algebraic spaces (according to Dubreil, Dubreil - Jacobin and Borůvka). So, we can use

also this terminology. In accordance with [4] we define an *algebraic space with operators* as a triad $\boldsymbol{E} = (E, G, \alpha)$, where $E \neq \emptyset$ (a *state set* or a *phase set*), G is a monoid the identity e (in a special case G is supposed to be a group) called also an *input* or *phase monoid* and $\alpha : G \times E \to E$ is an action (called also a *transition function*) wich satisfies two conditions:

1. Identity condition $\alpha(e, x) = x$ for any $x \in E$,
2. Condition of mixed associativity $\alpha(b, (\alpha(a, x)) = \alpha(ab, x)$ for any $a, b \in G$, $x \in E$.

An algebraic space $\boldsymbol{E} = (E, G, \alpha)$ is said to be *homogenous* if G is acting on the set E transitively, i.e. for any pair of elements $x, y \in E$ there exists $a \in G$ such that $\alpha(a, x) = y$. Usually an algebraic space $\boldsymbol{E}$ is called homogenous if G is a group transitively acting on E, which we can called *strong homogeneous* or shortly *s-homogeneous.*

3 Algebraic spaces and hypergroups

We assign to every algebraic space $\boldsymbol{E} = (E, G, \alpha)$ a commutative hypergroup $\mathbf{H}(\boldsymbol{E}) = (E, \bullet)$ in this way: For any pair $x, y \in E$ we define

$$x \bullet y = \alpha(G, x) \cup \alpha(G, y),$$

where $\alpha(G, x) = \{\alpha(a, x); a \in G\}$ is the trajectory of the element x over the monoid G. Then the hypergroup $\mathbf{H}(\boldsymbol{E})$ is called a *state hypergroup* of the algebraic space $\boldsymbol{E}$. It is clear that on the state set of any algebraic space $\boldsymbol{E} = (E, G, \alpha)$ there are defined two totally additive closure operations:

$$\boldsymbol{S}_+, \boldsymbol{S}_- : \mathcal{P}(E) \to \mathcal{P}(E)$$

in this way: $\boldsymbol{S}_+(X) = \alpha(G, X)$, $\boldsymbol{S}_-(X) = \{x \in X; \alpha(a, x) \in X$ for some $a \in G\}$ if X is a non-empty subset of the set E and $\boldsymbol{S}_+(\emptyset) = \boldsymbol{S}_-(\emptyset) = \emptyset$ (caled a *source* and an *successor* closure operation, respectively).

The above defined transfer can be extended into functorial if we consider suitable morphism between hypergroups (where we use mostly homomorphisms and good homomorphisms).

By [18] a hypergroup H is said to be *cyclic* if for some $h \in H$ we have $H = \bigcup_{k \in \mathbf{N}} h^k$ and it is called single-power cyclic (more exactly *n-singIe-power cyclic*) if there exist $h \in H$, $n \in \mathbf{N}$ such that $H = h^n$. In this case the element his called *n-generating*. From the above definition of a state hypergroup we get:

Proposition 1. *An algebraic space **E** is homogeneous if and only if its state hypergroup* $\mathbf{H}(\boldsymbol{E})$ *is 2-single-power cyclic and each element* $x \in E$ *is a 2- generating element of this hypergroup.*□

The following theorem gives necessary and sufficient conditions under which the state hypergroup of an algebraic space is a join hypergroup:

Theorem 1. *Let* $(E, \bullet)$ *be a state hypergroup of an algebraic space* (E, G, α). *Then the following conditions are equivalent:*

1. $(E, \bullet)$ *is a join hypergroup.*

2. *For any pair* $(x, y) \in E \times E$ *such that* $x \bullet y \subseteq u^2$ *for a suitable element* $u \in E$, *there exists an element* $v \in E$ *with the property* $v^2 \subseteq x^2 \cap y^2$.

3. *For any pair* $(x, y) \in E \times E$ *such that there exists a pair* $(a, b) \in G \times G$ *and an element* $u \in E$ *with* $\alpha(a, u) = x$, $\alpha(b, u) = y$, *we have* $\alpha(c, x) = \alpha(d, y)$ *for some pair* $(c, d) \in G \times G$.

□

On the contrary to the case of algebraic structures with single-valued operations in the case of hypergroups there are possible various modifications of the concept of generating decomposition of the carrier set of a hypergroup. It depends on the various approaches to the congruence concept for hyperstructures. One of them is the following notion:

Definition. Let $(G, \cdot)$ be a hypergroupoid (i. e. $\cdot : G \times G \to \mathcal{P}(G)$ is an arbitrary mapping) Let $\overline{G}$ be such a decomposition on the set G that for any quadruple $a, b, c, d \in G$ with the property $a, c \in \bar{a}$, $b, d \in \bar{b}$ for some $a, b \in G$ we have $(a \cdot b \left[\overline{G}\right) = (c \cdot d \left[\overline{G}\right)$; here $X \left[\bar{G}\right.$ denotes the closure of the set X in the decomposition $\overline{G}$ ([3], 2. 3). Then the decomposition $\overline{G}$ is called *generating (on the hypergroupoid* $(G, \cdot)$) or *h-generating.*

Example 1. Let X be a nonempty set, $f : X \to X$ be a mapping. For $x, y \in X$ we put

$$x \cdot y = \{f^n(u); u \in \{x, y\}, n \in \mathbf{N}_0\},$$

where f^n is the *n*-th iteration of the mapping f. Then it is easy to verify that $(X, \cdot)$ is a commutative hypergroup in the above considered sense. Then the decomposition $\overline{X}_f$ corresponding to a KW-equivalence (Kuratowski -Whyburn - equivalence) $\mathbf{r}$ on X is defined by $x \,\mathbf{r}\, y$ iff $f^m(x) = f^n(x)$ for some pair $m, n \in \mathbf{N}_0$ (the set of all non-negative integers) Then the decomposition $\overline{X}_f$ is generating on the

hypergroup $(X, \cdot)$.

Example 2. By a deformation of one hypergroupoid $(G, \cdot)$ onto another one hypergroupoid $(H, \cdot)$ we mean a good (also called strong) homomorphism $f : (G, \cdot) \to (H, \cdot)$, i.e. for any pair $x, y \in G$ we have $f(x \cdot y) = f(x) \cdot f(y)$. Then the decomposition $\overline{G}$ of the hypergroupoid $(G, \cdot)$ corresponding to deformation f (i.e. elements $x, y \in G$ belong to some element $\bar{a} \in \overline{G}$ if an only if $f(x) = f(y)$) i.e. the decomposition corresponding to f is h-generating.

4 h-genenerating and Levine's decompositions

Now we define a hyperoperation on an h-genenerating decomposition $\overline{G}$ on a hypergroupoid $(G, \cdot)$. For arbitrary pair of elements $\bar{a}, \bar{b} \in \overline{G}$ we put

$$\bar{a} \cdot \bar{b} = (x.y)[\overline{G},$$

where $(x, y) \in \bar{a} \times \bar{b}$ is an arbitrary pair.
It is easy to prove that then $(G, \cdot)$ is a hypergroupoid and that the definition is correct (it is independent on the choice of elements x, y). The hypergroupoid $(\overline{G}, \cdot)$ is then called a *factor - hypergroupoid* on $(G, \cdot)$ or a *hyperfactoroid on* $(G, \cdot)$ or a *hyperfactoroid of* $(G, \cdot)$. Moreover we have:

Theorem 2. *Let $\overline{G}$ be an h-generating decomposition on a hypergroup $(G, \cdot)$. Then the hyperfactoroid $(\overline{G}, \cdot)$ of $(G, \cdot)$ is a hypergroup.* □

Now consider an algebraic space with operators $\boldsymbol{E} = (E, G, \alpha)$ with a monoid G of operators. On the system $\mathcal{P}(E)$ of all subsets of E, i.e. the power set of E, we define a decomposition in this way: Denote $\mathcal{S}(E) = \{K \in \mathcal{P}(E); S + K) = K\}$, i.e. $K \in \mathcal{S}(E)$ whenever $\alpha(G, K) = K$. Now suppose $\overline{\mathcal{P}(E)}$ is a decomposition of $\mathcal{P}(E)$ such that sets $X, Y, \in \mathcal{P}(E)$ belong to some element of $\overline{\mathcal{P}(E)}$ if for any set $M \in \mathcal{P}(E)$ such that $M = E \setminus K$(a complement) for some $K \in \mathcal{S}(E)$ we have $X \subseteq M$ if and only if $Y \subseteq M$. Then the decomposition $\overline{\mathcal{P}(E)}$ is called a *decomposition of the Levine's type* or a *Levine's decomposition* of the power set $\mathcal{P}(E)$.

Proposition 2. *Let $\boldsymbol{E} = (E, G, \alpha)$ be an algebraic space with operators, $\overline{\mathcal{P}(E)}$ be the Levine's decomposition of power set $\mathcal{P}(E)$. Then sets $X, Y \in \mathcal{P}(E)$ belong to the same element of $\overline{\mathcal{P}(E)}$ if and only if $x \in X$ implies $\alpha(G, x) \cap Y \neq \emptyset$ and $y \in Y$ implies $\alpha(G, y) \cap X \neq \emptyset$.*

Denote by $\mathcal{CS}(\boldsymbol{E}) = \{M; M \subseteq E, E \setminus M \in \mathcal{S}(\boldsymbol{E})\}$ and $\mathcal{U}_E(X) = \{M; X \subseteq M, M \in \mathcal{CS}(\mathbf{E})\}$ for any $X \in \mathcal{P}(E)$. Then we get:

Theorem 3. *Let $\boldsymbol{E} = (E, G, \alpha)$ be an algebraic space with operators. For any pair of sets $A, B \in \mathcal{P}(E)$ we define $A \bullet B = \mathcal{U}_E(A) \cup \mathcal{U}_E(B) \cup \{A, B\}$. Then $(\mathcal{P}(E), \bullet)$* is a *commutative extensive join hypergroup and the Levine's decomposition $\overline{\mathcal{P}(E)}$ is h-generating* on $(\mathcal{P}(E), \bullet)$.

Let $f : X \to Y$ be a mapping. We denote by $f_+ : \mathcal{P}(X) \to \mathcal{P}(Y)$ its lifing into power sets, i.e. we define $f_+(A) = f(A) = \{f(a); a \in A\}$ for any non-empty set $A \in \mathcal{P}(X)$ and $f_+(\emptyset) = \emptyset$ Then we have

Theorem 4. *Let $\boldsymbol{E}_i = (E_i, G_i, \alpha_i)$, $i = 1, 2$, be algebraic spaces with operators, $f : E_1 \to E_2$. be a mapping preserving $\mathcal{CS}$ - systems of spaces $\boldsymbol{E}_i$,* i.e. *$X \in \mathcal{CS}(\boldsymbol{E}_1)$ implies $f(X) \in \mathcal{CS}(\boldsymbol{E}_2)$. Then f_+ is a homomorphism of the hypergroup $(\mathcal{P}(\boldsymbol{E}_1), \bullet)$ into the hypergroup $(\mathcal{P}(\boldsymbol{E}_2), \bullet)$. If moreover the mapping f is surjective and reflects $\mathcal{CS}$- systems, ie. $Y \in \mathcal{CS}(\boldsymbol{E}_2)$ implies $f^-(Y) \in \mathcal{CS}(\boldsymbol{E}_1)$ (where $f^-(Y)$ is the preimage of the set Y) we have*

$$f_+ : (\mathcal{P}(\boldsymbol{E}_1), \bullet) \to (\mathcal{P}(\boldsymbol{E}_2), \bullet)$$

is a deformation, i. e. a good homomorphism of hypergroups and determines a homomorphism f_{++} of corresponding factor hypergroups

$$f_{++} = (\overline{\mathcal{P}(\boldsymbol{E}_1)}, \bullet) \to (\overline{\mathcal{P}(\boldsymbol{E}_2)}).$$

Remark. The closure operations $\mathcal{S}_+, \mathcal{S}_- : \mathcal{P}(E) \to \mathcal{P}(E)$ determine a quasidiscrete or Alexandroff discrete topologies on the state set E of the algebraic space **E**, thus some of the above constructions can be expressed in terms of the topological spaces theory with the use of their special morphisms. Language of the decomposition theory is in certain sense parallel to algebra of equivalence relations, however the first approach is useful in the context with coverings of spaces and with non-associative hyperstructures which are determined by the mentioned coverings of sets.

There are many papers devoted to hyperstructures - hypergroups and some of their generalizations in connection with automata and multiautomata. We mention at least papers [6,7,8,9,10] and [12, 13, 14, 15, 16, 17] from references of this contribution. The mentioned papers contain investigation of transposition hypergroups and application of these multistructures for the constructing of actions and multiactions in connection with some other mathematical concepts.

5 Conclusion

Considering the class of all quasiautomata (algebraic spaces) with pointed monoids as input alphabets (i.e. monoids with distinguished elements) we can construct multiautomata in such a way that input alphabets are centralizers of distinguished elements within the given monoids. Hyperoperations on mentioned alphabets are defined by products of elements using powers of distinguished elements. Then we obtain a class of multiautomata, where the mentioned construction - described exactly e. g. in paper [10], page 5 - is functorial, which means that it preserves homomorphisms; more precisely homomorphisms of quasiautomata (of algebraic spaces with input monoids) turn out into good homomorphisms of multiautomata. It is to be noted that multiautomata are serving as suitable tools for modelling of various processes concernig important mathematical objects and structures.

References

[1] Z. Bavel : *The source as a tool in automata* . Inform. Control 18 (1971), pp. 140 - 155.

[2] O. Borůvka : *ber Zerlegungen von Mengen. Mitteilungen.* Tschech Akad. Wiss. LIII, 23 (1943), 14 pp.

[3] O. Borůvka :*Foundations of the Theory of Groupoids and Groups.* VEB Deutscher Verlag der Wissenschaften, Berlin 1974.

[4] O. Borůvka :Algebraic spaces with operators and their realization by differential equations I, II (Czech). Text of the Seminar on Differential Equations. Brno 1988, 35 pp.

[5] J. Chvalina : *Functional Graphs, Quasi-ordered Sets and Commutative Hypergroups* (Czech). Masaryk University Brno 1995.

[6] J. Chvalina - L. Chvalinová : *State hypergroups of automata.* Acta Math. et Inform. Univ. Ostrav. 4, No. 1 (1996), pp. 105 - 119.

[7] J. Chvalina, Š. Křehlík and M. Novák: *Cartesian composition and the problem of generalizing the MAC condition to quasi- multiautomata.* Analele Stiintifice Ale Universitatii Ovidius Constanta, Seria Matematica, 2016, Vol. XXIV, No. 3, pp. 79-100.

[8] J. Chvalina - Š. Mayerová: *On certain proximities and preorderings on the transposition hypergroups of linear first-order partial differential operators.* Analele Stiintifice Ale Universitatii Ovidius Constanta, Seria Matematica, 2014, Vol. 2014, No. 22, pp. 85-103.

[9] J. Chvalina - Š. Mayerová: *General Omega-hyperstructures and certain applications of those*. Ratio Mathematica, 2013, Vol. 2012, No. 23, pp. 3-20.

[10] J. Chvalina, J. Moučka and R. Vémolová: *Functorial passage from quasi-automata to multiautomata.* In XXIV International Colloquium on the Acquisition Process Management, CD- ROM. Brno: UNOB Brno, 2006. pp. 1 - 8.

[11] P. Corsini : *Prolegomena of Hypergroup Theory.* Aviani Edittore, Tricesimo 1993.

[12] P. Corsini and V. Leoreanu: *Application of Hyperstructure Theory*, Dordrecht, Kluwer Academic Pub., 2003.

[13] Š. Hošková - J. Chvalina: *Discrete transformation hypergroups and transformation hypergroups with phase tolerance space*, DISCRETE MATHEMATICS, 2008, Vol. 2008, No. 308, pp. 4133-4143.

[14] Š. Hošková, J. Chvalina and P. Račková: *Transposition hypergroups of Fredholm integral operators and related hyperstructures I.* Journal of Basic Science, 2008, Vol. 4(2008), No. 1, pp. 43-54.

[15] Š. Hošková, J. Chvalina and P. Račková: *Transposition hypergroups of Fredholm integral operators and related hyperstructures II.* Journal of Basic Science, 2008, Vol. 4(2008), No. 1, pp. 55-60.

[16] N. Levine: *An equivalence relation in tapology.* Math. J. Okayama Univ. 15(1971-72), pp. 113 - 123.

[17] B. Mikolajczak (ed.) : *Algebraic and Structural Automota Theory.* Annals of Discretc Math. 44, North - Holland - Amsterdam, New York, Oxford, Tokyo 1991.

[18] T. Vougiouklis : *Cyclicity in a special class of hypergroups.* Acta Univ. Carol. Math Phys. 22, 1 (1981), pp. 3 - 6.

Ratio Mathematica
Vol. 34, 2018, pp. 77–83

ISSN: 1592-7415
eISSN: 2282-8214

Notes on the Solutions of the First Order Quasilinear Differential Equations

Alena Vagaská*, Dušan Mamrilla†

Received: 11-05-2018. **Accepted**: 24-06-2018. **Published**: 30-06-2018

doi:10.23755/rm.v34i0.414

Abstract

The system of the quasilinear differential first order equations with the antisymetric matrix and the same element $f(t, x(t))$ on the main diagonal have the property that $r'(t) = f(t, x(t))\, r(t)$, where $r(t) \geq 0$ is the polar function of the system. In special cases, when values $f(t, x(t))$ and $g(t, x(t))$ are only dependent on $r^2(t)$, $t \in J_0$ we can find the general solution of the system (1) explicitly.

Keywords: nonlinear; quasilinear; differential equation; differential system;
2010 AMS subject classifications: 34C10.

*Technical University of Košice, Faculty of Manufacturing Technologies, Prešov, Slovakia. alena.vagaska@tuke.sk

†Prešov, Slovakia. dusan.mamrilla@gmail.com

1 Introduction

Norkin, S. B. and Tchartorickij, J. A. [1] and Kurzweill, J. [2] investigated the oscillatory properties of the 1,2-nontrivial solutions $x(t)$ of systems of two first order linear differential equations applying polar coordinates. Mamrilla, D. and Norkin, S. B. [3] investigated the oscilatory properties of the 1,2,3-nontrivial solutions $x(t)$ of systems of three first order linear differential equations applying spherical coordinates.
Applying polar (spherical) coordinates, the boundedness and oscillatority of the 1,2 (1,2,3)-nontrivial solutions $x(t)$ of systems of two (three) first order quasi-linear differential equations have been investigated by Mamrilla, D. [4], [5], [6] and Mamrilla, D. and Seman, J. and Vagaská, A. [7], while special attention was paid to the study of the properties of the $x\left(t\right)$ solutions of the systems, the matrix of which has the same element $f\left(t,x\left(t\right)\right)$ on the main diagonal.

This paper gives some asymptotical and oscillatory properties of the solutions to the system of the nonlinear differential equations:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}' = \begin{pmatrix} f\left(t,x\left(t\right)\right) & 0 & g\left(t,x\left(t\right)\right) \\ 0 & f\left(t,x\left(t\right)\right) & 0 \\ -g\left(t,x\left(t\right)\right) & 0 & f\left(t,x\left(t\right)\right) \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \qquad (1)$$

where $t > 0$, $0 \neq f\left(t,x\left(t\right)\right)$, $0 \neq g\left(t,x\left(t\right)\right) \in C_0\left(D \equiv J \times R^3, R\right)$.

We assume that each solution

$$\begin{aligned} x\left(t\right) &= \left(x_1\left(t\right), x_2\left(t\right), x_3\left(t\right)\right), \qquad (2) \\ x_1\left(t_0\right) &= x_1^0, \\ x_2\left(t_0\right) &= x_2^0, \\ x_3\left(t_0\right) &= x_3^0,\ t_0 \in J \end{aligned}$$

exists on the interval J and we denote $h > t_0 > 0$ the right endpoint of the interval J and $J_0 = [t_0, h)$.

We shall denote

$$\begin{aligned} g_1\left(t,x\right) &= f\left(t,x\right)x_1 + g\left(t,x\right)x_3, \\ g_2\left(t,x\right) &= f\left(t,x\right)x_2, \qquad (3) \\ g_3\left(t,x\right) &= -g\left(t,x\right)x_1 + f\left(t,x\right)x_3. \end{aligned}$$

It is known that if $D_0 \subset D$ is open nonempty set and derivatives $(\partial g_i(t,x)/\partial x_j)$ are continuous functions on D_0 for every $i,j \in \{1,2,3\}$ then each point $(t_0, x_1^0, x_2^0, x_3^0) \in D_0$ is passed by one and only one integral curve $x \in D$ of the system (1) [3].

Definition 1.1. *The solution $x(t)$ to the system (1) is called $i-trivial$, $i \in \{1,2,3\}$ is fixed, if $x_i(t) = 0$ on the interval J_0. Otherwise $x(t)$ is $i-nontrivial$ solution. If for at least one $i \in \{1,2,3\}$ the solution to the system (1) is $i-nontrivial$, shortly so solution $x(t)$ is said to be $nontrivial$.*

It is obvious that system (1) has $1,2,3-trivial$ solution; $1,3-trivial$ and $2-nontrivial$ solution; $1,3-nontrivial$ and $2-trivial$ solution; $1,2,3-nontrivial$ solution.

Definition 1.2. *The solution $x(t)$ to the system (1) is called $i-positive$ ($i-negative$), $i \in \{1,2,3\}$ is fixed, if $x_i(t)$ is positive (negative) function on the interval J_0.*

Definition 1.3. *The solution $x(t)$ to the system (1) is called $i-nondecreasing$ ($i-nonincreasing$), $i \in \{1,2,3\}$ is fixed, if $x_i(t)$ is nondecreasing (nonincreasing) function on the interval J_0.*

It is obvious that if $f(t,x)x_2 \geq 0$ ($f(t,x)x_2 \leq 0$) for any point $(t,x) \in D$ then arbitrary solution $x(t)$, $t \in J_0$ to the system (1) is $2-nondecreasing$ ($2-nonincreasing$).

Definition 1.4. *The solution $x(t)$ to the system (1) is called $i-bounded$, $i \in \{1,2,3\}$ is fixed, if $x_i(t)$ is the bounded function on interval J_0. At other cases $x(t)$ is $i-unbounded$ one which is called $i-from\ above$ ($i-from\ below$) $unbounded$, $i \in \{1,2,3\}$ is fixed, if $x_i(t)$ is from above (from below) unbounded function on interval J_0.*

It is obvious that if for every continuous function y defined on interval J_0 :

a) $\sup\limits_y \left(\int_{t_0}^h |f(t,y)\,y_2|dt\right) < \infty$, then any solution $x(t)$, $t \in J_0$ to the system (1) is $2-bounded$,

b) $\sup\limits_y \left(\int_{t_0}^h f(t,y)\,y_2 dt\right) = -\infty \left(\inf\limits_y \left(\int_{t_0}^h f(t,y)\,y_2 dt\right) = \infty\right)$ then there exists a point $t^* \geq t_0$ and $2-negative$ ($2-positive$) solution $x(t)$, $t \in [t^*, h)$ to the system (1) such that it is $2-from\ below$ ($2-from\ above$) unbounded.

Definition 1.5. *The solution $x(t)$ to the system (1) is called $i-oscillatory$, $i \in \{1,2,3\}$ is fixed, if $x_i(t)$ is the oscillatory function, i. e. if there exists the increasing sequence $\{t_n\}_{n=1}^{\infty}$ such that $t_n \in J_0$, $t_n \to h$ and $x_i(t_n).x_i(t_{n+1}) < 0$ for each $n \in N$. The solution $x(t)$ is called $i-nonoscillatory$ if there exists $h_1 < h$ such that $x_i(t)$ is not changing its sign on the interval $[h_1, h)$, resp. if it has maximally finite number of zero point on the interval $[t_0, h)$.*

2 Main results

Theorem 2.1. *The general solution to the system (1) is generated by the trinity of the functions:*

$$x_1(t) = \left(C_2 \cos\left(\int_{t_0}^{t} g(s, x(s))\, ds \right) - C_3 \sin\left(\int_{t_0}^{t} g(s, x(s))\, ds \right) \right) \times \exp\left(\int_{t_0}^{t} f(s, x(s))\, ds \right),$$

$$x_2(t) = C_1 \exp\left(\int_{t_0}^{t} f(s, x(s))\, ds \right),$$

$$x_3(t) = \left(-C_2 \sin\left(\int_{t_0}^{t} g(s, x(s))\, ds \right) - C_3 \cos\left(\int_{t_0}^{t} g(s, x(s))\, ds \right) \right) \times \exp\left(\int_{t_0}^{t} f(s, x(s))\, ds \right),$$

where $C_i\,(i = 1, 2, 3) \in R$ are arbitrary constants.

Proof. The characteristic quasipolynomial of the system (1) is

$$det\left(A(t, x(t)) - \lambda(t, x(t))\, E\right) = \\ = \left(f(t, x(t)) - \lambda(t, x(t))\right)^3 + g^2(t, x(t))\left(f(t, x(t)) - \lambda(t, x(t))\right) = 0$$

the solutions of which are the functions

$$\lambda_1(t, x(t)) = f(t, x(t)) \quad \text{and}$$

$$\lambda_{2,3}(t, x(t)) = f(t, x(t)) \pm i g(t, x(t)).$$

The fundamental system of the solutions to the system (1) is generated by the vector functions $X_1(t, x(t))$, $ReX_2^c(t, x(t))$, $ImX_2^c(t, x(t))$, where

$$X_1(t, x(t)) = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \exp\left(\int_{t_0}^{t} f(s, x(s))\, ds \right)$$

$$X_2^c(t, x(t)) = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + i \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \right) \exp\left(\int_{t_0}^{t} \left(f(s, x(s)) - i g(s, x(s))\right) ds \right),$$

e.g.,

$$X_2(t,x(t)) = \\ = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \cos\left(\int_{t_0}^{t} g(s,x(s))\,ds \right) + \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \sin\left(\int_{t_0}^{t} g(s,x(s))\,ds \right) \right) \\ \times \exp\left(\int_{t_0}^{t} f(s,x(s))\,ds \right),$$

$$X_3(t,x(t)) = \\ = \left(\begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix} \cos\left(\int_{t_0}^{t} g(s,x(s))\,ds \right) - \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \sin\left(\int_{t_0}^{t} g(s,x(s))\,ds \right) \right) \\ \times \exp\left(\int_{t_0}^{t} f(s,x(s))\,ds \right).$$

This proves the theorem.□

Corolary 2.1. *If we put $g(t,x(t)) = 1$ in Theorem (2.1), we obtain assertion of Theorem (2.1) in [7].*

Theorem 2.2. *Let for all continuous functions y defined on the interval J_0:*

a) $\sup_y \left(\int_{t_0}^{h} |f(s,y)|ds \right) < \infty$*, then each solution $x(t)$, $t \in J_0$ to the system (1) is $1,2,3-$bounded,*

b) $\sup_y \left(\int_{t_0}^{h} f(s,y)\,ds \right) = -\infty$*, then each solution $x(t)$, $t \in J_0$ to the system (1) is $1,2,3-$bounded and such that $x_1(t) \to 0$, $x_2(t) \to 0$, $x_3(t) \to 0$ for $t \to h$,*

c) $\inf_y \left(\int_{t_0}^{h} f(s,y)\,ds \right) = \infty$*, then each solution $x(t)$, $t \in J_0$ to the system (1) is such that it is $i-$unbounded at least for one $i \in \{1,2,3\}$.*

Proof. Theorem (2.1)implies that the general solution to the system (1) fulfils a condition $x_1^2(t) + x_2^2(t) + x_3^2(t) = (C_1^2 + C_2^2 + C_3^2) \exp\left(2\int_{t_0}^{t} f(s,x(s))\,ds \right)$, and this implies the assertion of the theorem. □

We assume that for each nontrivial solution $x(t)$, $t \in J_0$ to the system (1) there exists the trinity of the functions $r(t) > 0$, $u(t)$, $v(t) \in C_1(J_0,R)$ such that the coordinates $x_i(t)$, $t \in J_0$, $i = 1,2,3$ fulfil [7]:

$$\begin{aligned} x_1(t) &= r(t)\cos u(t), \\ x_2(t) &= r(t)\sin u(t)\cos v(t), \\ x_3(t) &= r(t)\sin u(t)\sin v(t), \\ r'(t) &= x_1'(t)\cos u(t) + x_2'(t)\sin u(t)\cos v(t) + \\ &+ x_3'(t)\sin u(t)\sin v(t), \\ r(t)u'(t) &= -x_1'(t)\sin u(t) + x_2'(t)\cos u(t)\cos v(t) + \\ &+ x_3'(t)\cos u(t)\sin v(t), \\ r(t)\sin u(t)v'(t) &= -x_2'(t)\sin v(t) + x_3'(t)\cos v(t). \end{aligned} \tag{4}$$

The function $r(t)$ is called the polar, $u(t)$ the first angle function and $v(t)$ the second angle function. From this after equivalent arrangement for nontrivial solutions to the system (1) we get:

$$\begin{aligned} r'(t) &= f(t, x(t))\, r(t), \\ u'(t) &= -g(t, x(t))\sin v(t), \\ \sin u(t)\, v'(t) &= -g(t, x(t))\cos u(t)\cos v(t). \end{aligned} \tag{5}$$

3 Conclusions

The paper deals with qualitative and quantitative properties of the solutions of special differential equations and systems of differential equations. Non-linear and quasi-linear equations are less researched in mathematical publications, so the goal of this paper was to investigate some asymptotical and oscillatory properties of non-trivial solutions of such differential equations and systems thus contributing to knowledge in this field of research. Special attention was focused on the study of the asymptotic and oscillatory properties of the $x(t)$ solutions of the systems, the matrix of which has the same element on the main diagonal. We have achieved new results due to the investigation of this subject by applying of polar or spherical coordinates.

4 Acknowledgements

The research work is supported by the project KEGA 026TUKE-4/2016. Title of the project: Implementation of Modern Information and Communication Technologies in Education of Natural Science and Technical Subjects at Technical Faculties.

References

[1] S. B. Norkin and J. A. Tchartorickij, *Investigation of oscillatory properties of a system of two linear differential equations by means of angle function, Differential equations and approximation theory*, MADI (1977), Moscow, pp. 19-32

[2] J. Kurzweill, *Ordinary differential equations*, SNTL, Praha, 1978

[3] D. Mamrilla, S. B. Norkin, *Investigation of oscillatory properties of linear third order differential equations systems by means of angle functions, Investigations of differential equations* , MADI 1986, Moscow, pp. 97-106

[4] D. Mamrilla *On boundedness and oscillatoricity of certain differential equations systems*, Fasciculi Mathematici 24 (1994), pp. 27-35, Poznan

[5] D. Mamrilla *The theory of angle functions and some properties of certain nonlinear differential systems*, Fasciculi Mathematici 24 (1994), pp. 55-65, Poznan

[6] D. Mamrilla *On the systems of first order quasi - linear differential equations*, Tribun EU Brno (2008)

[7] D. Mamrilla and J. Seman and A. Vagaská *On the solutions of the first order nonlinear differential equations*, Journal of the Applied Mathematics, Statistics and Informatics 1(JAMSI), 3(2007), pp. 63 - 70, Trnava

Ratio Mathematica
Vol.34, 2018, pp. 85–93

ISSN : 1592-7415
eISSN : 2282-8214

Some Kinds of Homomorphisms on Hypervector Spaces

Elham Zangiabadi*, Zohreh Nazari†

Received: 24-05-2018 . **Accepted**: 24-06-2018. **Published**: 30-06-2018

doi: 10.23755/rm.v34i0.416

Abstract

In this paper, we introduce the concepts of homomorphism of type 1 , 2 and 3 and good homomorphism . Then we investigate some properties of them.
Keywords : Hypervector space , Homomorphism , Homomorphism of type 1 , 2 and 3 , good homomorphism .
2010 AMS subject classifications : 20N20 , 22A30 .

1 Introduction and Preliminaries

The concept of hyperstructure was first introduced by Marty [13] in 1934 . He defined hypergroups and began to analysis their properties and applied them to groups and rational algebraic functions . Tallini introduced the notion of hypervector spaces [14] , [15] and studied basic properties of them . Homomorphisms of hypergroups are studied by several authers ([2] - [12]) . Since some kinds of homomorphisms on hypergroup were defined , we encourage to define them on hypervector spaces . In this paper , we introduce the concept of homomorphism of type 1 , 2 and 3. And give an example of a homomorphism that is not a homomorphism of type 1, 2 and 3. We show that if f be a homomorphism of type 1, 2 and 3, then f is a homomorphism and every homomorphism of type 2 or 3

*Department of Mathematics, Vali-e-asr University, Rafsangan, Iran. e.zangiabadi@vru.ac.ir
†Department of Mathematics, Vali-e-asr University, Rafsangan, Iran. z.nazari@vru.ac.ir

is a homomorphism of type 1. Also, we define a good homomorphism and obtain that every homomorphism of type 2 is a good homomorphism and every good homomorphism is a homomorphism. Finally, w e prove that every onto strong homomorphism is a good homomorphism.

Let us recall some definitions which are useful in our results .

Definition 1.1. *A hypervector space over a field K is a quadruplet $(V, +, \circ, K)$ such that $(V, +)$ is an abelian group and*

$$\circ : K \times V \to P_*(V)$$

is a mapping of $K \times V$ into the power set of V (deprived of the empty set) , such that

$$\begin{aligned}
(a+b) \circ x &\subseteq (a \circ x) + (b \circ x), \quad \forall a, b \in K, \ \forall x \in V, && (1)\\
a \circ (x+y) &\subseteq (a \circ x) + (a \circ y), \quad \forall a \in K, \ \forall x, y \in V, && (2)\\
a \circ (b \circ x) &= (ab) \circ x, \quad \forall a, b \in K, \ \forall\, x \in V, && (3)\\
x &\in 1 \circ x, \quad \forall x \in V, && (4)\\
a \circ (-x) &= -a \circ x, \quad \forall a \in K, \ \forall x \in V. && (5)
\end{aligned}$$

Definition 1.2. *Let $(V, +, \circ, K)$ be a hypervector space . Then $H \subseteq V$ is a subspace of V , if*

1) the zero vector , 0 , is in H ,

2) $U, V \in H$, then $U + V \in H$,

3) $U \in H, r \in K$, then $r \circ U \subseteq H$.

Definition 1.3. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces . A mapping*

$$f : V \to W$$

is called

1) a homomorphism , if $\forall r \in K, \ \forall x, y \in V$:

$$\begin{aligned}
f(x+y) &= f(x) \oplus f(y), && (6)\\
f(r \circ x) &\subseteq r * f(x). && (7)
\end{aligned}$$

2) a strong homomorphism, if $\forall r \in K, \ \forall x, y \in V$:

$$\begin{aligned}
f(x+y) &= f(x) \oplus f(y), && (8)\\
f(r \circ x) &= r * f(x). && (9)
\end{aligned}$$

2 The main results

In this paper, the ground field of a hypervector space V is presented with K, This field is usually considered by $\mathbb{R}$ or $\mathbb{C}$. Let $(V, +, \circ)$ and $(W, \oplus, *)$ be two hypervector spaces and $f : V \to W$ be a mapping. We employ for simplicity of notation $x_f = f^{-1}(f(x))$ and for a subset A of V, $A_f = f^{-1}(f(A)) = \bigcup\{x_f : x \in A\}$.

Lemma 2.1. *Let $r \in K$ and $x \in V$. Then the following statements are valid:*

i) $r \circ x \subseteq (r \circ x)_f$,

ii) $r \circ x \subseteq r \circ x_f$,

iii) $(r \circ x)_f \subseteq (r \circ x_f)_f$,

iv) $r \circ x_f \subseteq (r \circ x_f)_f$.

Definition 2.1. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces and $f : V \to W$ be a map such that $f(x + y) = f(x) \oplus f(y)$, for all $a, b \in V$. Then, for any $r \in K$ and $x, y \in V$, f is called a homomorphism of*

i) type 1, if $f^{-1}(r * f(x)) = (r \circ x_f)_f$,

ii) type 2, if $f^{-1}(r * f(x)) = (r \circ x)_f$,

iii) type 3, if $f^{-1}(r * f(x)) = (r \circ x_f)$.

Theorem 2.1. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces, A be a non-empty subset of V and $f : V \to W$ be a map such that $f(a + b) = f(a) \oplus f(b)$, for all $a, b \in V$. Then, f is a homomorphism of*

i) type 1 implies $f^{-1}(r * f(A)) = (r \circ A_f)_f$,

ii) type 2 implies $f^{-1}(r * f(A)) = (r \circ A)_f$,

iii) type 3 implies $f^{-1}(r * f(A)) = (r \circ A_f)$.

Proof. Each part is established by a straightforward set theoretic argument. □

Example 2.1. *Let $(W, +, \cdot, K)$ be a classical vector space, P be a proper subspace of W, $W_1 = (W, +, \cdot, K)$ and $W_2 = (W, \oplus, \circ, K)$ that $r \circ a = r \cdot a + P$ for $r \in K$ and $a \in W$. Then W_1 and W_2 are hypervector spaces.*
Let $f : W_1 \to W_2$ be the function defined by $f(x) = k \cdot x$, where $k \in K$. We show

that f is a homomorphism, but not a homomorphism of type 1, 2 and 3.

For every $r \in K$ and $x \in W_1$ we have

$$f(r \cdot x) = rk \cdot x \subsetneq rk \cdot x + P = r \circ f(x).$$

Thus f is a homomorphism. Since f is one to one, we obtain $x_f = x$, for $x \in W$. It followes that

$$(r \cdot x_f)_f = (r \cdot x)_f = (r \cdot x_f) = (r \cdot x).$$

On the other hand,

$$f^{-1}(r \circ f(x)) = f^{-1}(kr \cdot x + P) = \{t \in W_1 : f(t) \in kr \cdot x + P\}$$

$$= \{t \in W_1 : k \cdot t \in kr \cdot x + P\} = \{t \in W_1 : k \cdot t - kr \cdot x \in P\}.$$

Hence,

$$f^{-1}(r \circ f(x)) \neq r \cdot x.$$

Therefore, f is not a homomorphism of type 1, 2 and 3.

Theorem 2.2. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces and $f : V \to W$ be a homomorphism of type n, for n=1,2,3. Then f is a homomorphism map.*

Proof. If f be a homomorphism of type 1. Then by using Lemma 2.1, we have

$$f(r \circ x) \subseteq f(r \circ x_f) \subseteq f((r \circ x_f)_f) = f(f^{-1}(r * f(x)) \subseteq r * f(x).$$

Suppose f is a homomorphism of type 2. Then

$$f(r \circ x) \subseteq f((r \circ x)_f) = f(f^{-1}(r * f(x)) \subseteq r * f(x).$$

Similarly, if f is a homomorphism of type 3, then

$$f(r \circ x) \subseteq f(r \circ x_f) = f(f^{-1}(r * f(x))) \subseteq r * f(x).$$

□

Lemma 2.2. *Let f be a homomorphism. Then*

$$(r \circ x_f)_f \subseteq f^{-1}(r * f(x)).$$

Proof. Since f is a homomorphism, for all $r \in K$ and $x \in V$, we have

$$f(r \circ x_f) \subseteq r * f(x_f).$$

Since $r * f(x_f) = r * f(f^{-1}(f(x)) \subseteq r * f(x)$, hence, $f(r \circ x_f) \subseteq r * f(x)$. Therefore,

$$(r \circ x_f)_f \subseteq f^{-1}(r * f(x)).$$

□

Proposition 2.1. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces and $f : V \to W$ be a homomorphism of type 2 or 3. Then f is a homomorphism of type 1.*

Proof. Suppose that $r \in K$, $x \in V$ and $f : V \to W$ be a homomorphism of type 2, then by Lemma 2.2 we have

$$(r \circ x)_f \subseteq (r \circ x_f)_f \subseteq f^{-1}(r * f(x)) = (r \circ x)_f.$$

Similarly, if f is a homomorphism of type 3, then

$$r \circ x_f \subseteq (r \circ x_f)_f \subseteq f^{-1}(r * f(x)) = r \circ x_f.$$

□

Proposition 2.2. *Let $(V, +, \circ, K)$ and $(W, +\oplus, *, K)$ be two hypervector spaces and $f : V \to W$ be an onto mapping. Then, given $r \in K$ and $x \in V$, f is a homomorphism of*

i) type 1 if and only if $f(r \circ x_f) = r * f(x)$,

ii) type 2 if and only if $f(r \circ x) = r * f(x)$.

Proof. Since f is onto, we obtain

$$ff^{-1}(r * f(x)) = r * f(x).$$

Thus, (i) and (ii) are trivial. □

Corolary 2.1. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces, A and B be non-empty subsets of V and $f : V \to W$ be an onto mapping.Then, f is homomorphism of*

i) type 1 implies $f(r \circ A_f) = r * f(A)$,

ii) type 2 implies $f(r \circ A) = r * f(A)$.

Remark 2.1. *On onto homomorphisms between hypervector spaces, a homomorphism of type 2 is equivalent with a strong homomorphism.*

Theorem 2.3. *Let $(V_1, +_1, \circ_1, K)$, $(V_2, +_2, \circ_2, K)$ and $(V_3, +_3, \circ_3, K)$ be hypervector spaces. For $n = 1, 2, 3$, let f be a homomorphism of type n of V_1 onto V_2 and g be a homomorphism of type n of V_2 onto V_3. Then, gf is a homomorphism of type n of V_1 onto V_3.*

Proof. Let $x, y \in V$. We have $gf(x +_1 y) = g(f(x) +_2 f(y)) = gf(x) +_3 gf(y))$. One can easily seen that $x_{gf} = f^{-1}(f(x)_g)$.
Let $n = 1$. By above relation, we obtain

$$gf(r \circ x_{gf}) = gf(r \circ f^{-1}(f(x)_g)).$$

Since f is onto, there exists a subset A of V such that $f(A) = f^{-1}(f(x)_g)$. By Corollary 2.1, we obtain

$$gf(r \circ_1 f^{-1}(f(x)_g)) = g(r \circ_2 f(x)_g).$$

Then, by Proposition 2.2, we have

$$g(r \circ_2 f(x)_g) = r \circ_3 gf(x).$$

Let $n = 2$. Similar to the previous case, but simpler.
Let $n = 3$. Since g is of type 3,

$$(gf)^{-1}(r \circ_3 (gf)(x)) = f^{-1}g^{-1}r \circ_3 (gf)(x)) = f^{-1}(r * f(x)_g).$$

Since f is onto, the item (iii) of Theorem 2.1 implies

$$f^{-1}(r \circ_2 f(x)_g) = r \circ_1 f^{-1}(f(x)_g) = r \circ_1 x_{gf}.$$

□

Definition 2.2. *Let $a \in V$ and $r \in K$. We define*

$$a/r = \{x \in V \ : \ a \in r \circ x\}.$$

Proposition 2.3. *Let $(V_1, +, \circ, K)$ and $(V_2, \oplus, *, K)$ be two hypervector spaces. If $f : V_1 \to V_2$ be an onto mapping. Then we have*

1) *$f(a/r) = f(a)/r$, if f is a homomorphism of type 2.*

2) *$f(a)/r \subseteq f(a_f)/r$, if f is a homomorphism of type 3.*

Proof. 1) We know that an onto homomorphism of type 2 is a strong homomorphism. Suppose that $y \in f(a/r)$. Then, there exists $t \in a/r$ such that $f(t) = y$, so $a \in r \circ t$ and $f(a) \in r * f(t)$. It implies that $y = f(t) \in f(a)/r$. Therefore, $f(a/r) \subset f(a)/r$. Note that the inverse inclusion is always true. 2) If $y \in f(a)/r$, there is $t \in V_1$ such that $f(t) = y$. Since f is homomorphism of type 3, we have $a_f \in r \circ t_f$, which means that $t_f \in a_f/r$, therefore $y \in f(a_f)/r$. □

Definition 2.3. *Let $(V, +, \circ, K)$ and $(W, *, \oplus, K)$ be two hypervector spaces and $f : V \to W$ be a map such that $f(a + b) = f(a) \oplus f(b)$. Then f is called a good homomorphism if*

$$f(a/r) = f(a)/r,$$

for any $a,\ b \in V$ and $r \in K$.

Remark 2.2. *According to Proposition 2.3, if f is a homomorphism of type 2, then f is a good homomorphism.*

Theorem 2.4. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces. If $f : V \to W$ be a good homomorphism then, f is a homomorphism.*

Proof. Let $r \in K$ and $a \in V_1$. If $y \in f(r \circ a)$, then, there exists $t \in r \circ a$ such that $y = f(t)$. Hence, $f(a) \in f(t/r) = f(t)/r$. Abviously, $y = f(t) \in r * f(a)$. □

Theorem 2.5. *Let $(V_1, +_1, \circ_1, K)$, $(V_2, +_2, \circ_2, K)$, and $(V_3, +_3, \circ_3, K)$ be hypervector spaces. Let f be a good homomorphism of V_1 to V_2 and g be a good homomorphism of V_2 to V_3. Then, gf is a good homomorphism of V_1 to V_3.*

Proof. For every $r \in K$ and $a \in V_1$, we have

$$gf(a/r) = g(f(a)/r) = gf(a)/r.$$

□

Proposition 2.4. *Let V and W be two hypervector spaces over K and $f : V \to W$ be a good homomorphism. Then*

$$f(A/K) = f(A)/K,$$

where $A \subseteq V$ and $A/K = \bigcup\{a/r : a \in A, r \in K\}$.

Proof. Let $y \in f(A/K)$. There exist $r \in K$ and $a \in A$ such that $y \in f(a/r) = f(a)/r \subseteq f(A)/K$. Conversely, let $y \in f(A)/k$. Then, there exist $r \in k$ and $a \in V$ such that $y \in f(a)/r = f(a/r)$ and so $y \in f(A/K)$. □

Theorem 2.6. *Let $(V, +, \circ, K)$ and $(W, \oplus, *, K)$ be two hypervector spaces, f be onto strong homomorphism from V to W. Then f is a good homomorphism.*

Proof. Let $f(t) \in f(x/r)$. So $x \in r \circ t$. It followes that $f(t) \in f(x)/r$. Therefore $f(x/r) \subseteq f(x)/r$.
On the other hand, let $y \in f(x)/r$. Since f is an onto mapping, there exists a $t \in V$ such that $y = f(t)$. Hence, $f(x) \in r * f(t) = f(r \circ t)$. Thus $x \in r \circ t$ and then we have $t \in x/r$ and $y = f(t) \in f(x/r)$. Therefore $f(x)/r \subseteq f(x/r)$. This implies that $f(x/r) = f(x)/r$.

□

References

[1] R. Ameri, O. R. Dehghan, *On dimension of hypervector spaces*, Eur. J. Pure Appl. Math, 1 (2008), 32-50.

[2] P. Corsini, *Recent results in the theory of hypergroups*, Boll. Unione Mat. Ital. (9), 2 (1983), 133-138.

[3] P. Corsini, V. Leoreanu, *Applications of hyperstructure theory*, Kluwer Academic Publishers, Advances in Mathematics, 2003.

[4] B. Davvaz, *Isomorphism theorems of polygroups*, Bull. Malays. Math. Sci. Soc. (2), 33 (2010), 385-392.

[5] B. Davvaz, *Groups in polygroups*, Iran. J. Math. Sci. Inform., 1 (2006), 25-31.

[6] J. E. Eaton, *Theory of cogroups*,Duke Math. J., 6 (1940), 101-107.

[7] D. Freni, *Strongly transitive geometric spaces : Applications to hypergroups and semigroups theory*, Comm. Algebra, 32 (2004), 969-988.

[8] D. Freni, *A new characterization of the derived hypergroup via strongly regular equivalences*, Comm. Algebra, 30 (2002), 3977-3989.

[9] T. W. Hungerford, *Algebra, graduate texts in mathematics*, 73. Springer-Verlag, New York-Berlin, 1980.

[10] J. Jantosciak, *Homomorphisms, equivalences and reductions in hypergroups*, Riv. Mat., 9 (1991), 23-47.

[11] M. Koskas, *Groupoides, demi-hypergroupes et hypergroupes. (French)*, J. Math. Pures Appl. (9), 49 (1970), 155-192.

[12] M. Krasner, *A class of hyperrings and hyperfiels*, internat. J. Math. Math. Sci., 6 (1983), 307-311.

[13] F. Marty, *Sur nue generalization de la notion do group*, 8nd congress of the Scandinavic Mathematics, Stockholm, (1934), 45-49.

[14] M. S. Tallini, *Weak hypervector space and norms in such spaces, Algebraic Hyper Structurs and Applications*, Jast, Rumania, Hadronic Press, (1994), 199-206.

[15] M. S. Tallini, *Hypervector spaces*, Proceedings of the fourth international congress of algebraic hyperstructures and applications, Xanthi, Greece, (1990), 167-174.

Publisher:
Accademia Piceno – Aprutina dei Velati in Teramo (A.P.A.V.)

Periodicity:
every six months

Printed in 2018 in Pescara (Italy)

Autorizzation n. 9/90 of 10/07/1990 released by Tribunale di Pescara
ISSN: 1592-7415 (printed version)

Autorizzation n. 16 of 17/12/2013 released by Tribunale di Pescara
ISSN: 2282-8214 (online version)

Accademia Piceno - Aprutina dei Velati in Teramo
ACCADEMIA DI SCIENZE, LETTERE, ARTI E TECNOLOGIA

www.eiris.it – www.apav.it

Ratio Mathematica, 34, 2018

Contents

Published by Accademia Piceno - Aprutina dei Velati in Teramo (A.P.A.V.)