Quasigroups and Related Systems **18** (2010), 105 – 112

Galina B. Belyavskaya's 70th birthday

On April 19, 2010 Galina Borisovna Belyavskaya turned 70. Presently she is a leading researcher in the Institute of Mathematics and Computer Science of the Academy of Sciences of the Republic of Moldova. She has made a significant contribution to the development of binary and n-ary quasigroup theory and published about 70 research works in mathematical journals.

For more than 20 years Galina was the Scientific secretary of the Specialized Council for conferring scientific degree at the Institute of Mathematics of the Academy of Sciences of Moldova.

G. Belyavskaya was born in Ust'-Kamenogorsk, the capital of the East-Kazakhstan Region of former USSR (now Oskemen in Kazakhstan). Her parents, born in Altai Region (Siberia) were engineers. Her father worked as a trees rafter on Siberian rivers. Both were Russian. The father's mother had re-married after her first husband died. G. Belyavskaya's father took polish sounding surname after her stepfather. Galina stayed with this surname. In the middle fifties the family moved to Gomel (Belarus) and then to Kishinev where her father became a teacher.

After her father she also inherited the love to play chess. In her youth she played chess and became a junior chess champion of Moldova.

In 1957 she began study at the Faculty of Physics and Mathematics of the Kishinev State University which she graduated with honors in 1962. In the same year she joined the newly established Institute of Mathematics of the Academy of Sciences of the Republic of Moldova, that was then a branch of the Academy of Sciences of the USSR. She still works there today.

Initially she worked in the computer laboratory and develop new programming languages, algorithms and software. Her paper [1] is from that period. In this paper one simple criterium for classifications of partially symmetric boolean functions is presented.

Since 1967, Belyavskaya begins cooperation with V. D. Belousov. Her first papers devoted to quasigroups are connected with the problem of a prolongation (extension) of quasigroups, i.e., a construction of a quasigroup on $(n+1)$-th order from a quasigroup of n-th order, and with the problem of a contraction (compression), i.e., a construction of a quasigroups of n-th order from quasigroups of $(n+1)$-th order. Necessary and sufficient conditions under which two contraction of a given quasigroup are isotopic are found in [2] and [3]. A new method of a prolongation is presented in [5]. Necessary and sufficient condition of isotopy of such two prolongations of a given quasigroup are found too. The problem of construction and decomposition of quasigroups was investigated in many of her papers (cf. [12], [27] and [33]).

Next she studied the systems of binary operations containing two projections, all quasigroup operations defined on a fixed set Q and satisfying the generalized Stein's identity ([7], [8] and [13]). Properties of such systems are described by means of balanced incomplete block design. A method for constructing such systems is presented in [7]. Later she generalized those results to the systems of n-ary quasigroup operations (see [49] and [61]).

Many papers of G. B. Belyavskaya are connected with the problem of ortogonality of binary and n-ary quasigroups. She start with a characterization of r-orthogonal quasigroups, i.e., quasigroups $Q(\cdot)$, $Q(\circ)$ for which the set $\{(x\cdot y, x\circ y) : x, y \in Q\}$ contains exactly r different ordered pairs. In [16] it is proved that for any $n \geqslant 4$ there exist $(n+k)$-orthogonal quasigroups for any k with $2 \leqslant k \leqslant [n/2]$. Necessary and sufficient conditions for a finite quasigroup to have an r-orthogonal quasigroup are found in [17]. Abelian groups of order $n > 2$, $n \neq 4$, have no $(n^2-2)-$, $(n^3-3)-$ or (n^2-5)-orthogonal quasigroups. Groups of prime order n have no $(n+2)-$, $(n+3)-$, $(n+4)-$ or $(n+5)$-orthogonal quasigroups. A method of construction of (n^2-2)-orthogonal quasigroups of even order n, where $n \neq 1 (\mathrm{mod}\, 3)$, by means of extensions of abelian groups is given in [21]. The set of possible values of r for which there exist pairs of r-orthogonal quasigroups of order n is described in [23], [25] and [37]. The class of self-orthogonal n-ary groupoids is characterized in [31]; pairwise orthogonality of n-ary operations in [53].

A new and more general version of orthogonality for n-ary operations is presented in [53] and [57]. It is connected with hypercubes which are a generalization of Latin squares to higher dimensions.

A series of her papers is devoted to admissible quasigroups $Q(\cdot)$, i.e., quasigroups with m elements containing a sequence of m elements from different rows and columns of the multiplication table of $Q(\cdot)$. If this sequence has exactly t distinct elements, then we say that a quasigroup $Q(\cdot)$ is *t-admissible*. The main results of Belyavskaya on such quasigroups are contained in [15], [18] and [24]. For example, all numbers t such that a cyclic group G is t-admissible are determined in [15]. For an arbitrary finite group similar result is obtained in [24]. Admissible n-ary quasigroups are studied in [19], [20] and [22].

In the early seventies of last century Belyavskaya investigated semisymmetric Stein quasigroups, for which she proved that a semisymmetric Stein quasigroup is invariant under parastrophy [9]. In this paper she also shows that a semisymmetric Stein quasigroup is isotopic to a group if and only if it is distributive.

In the late eighties Belyavskaya's scientific interest has been focused on the study of algebraic problems of quasigroups. In that time she introduced several new concepts and has received many important results. To the most important concepts should be included the concept of *chain isotopic quasigroups* [4], the concept of the *centre* and the new concept of *nuclei* that have led to many significant results (cf. [29], [30], [34], [36], [40], [41]). *Commutators* and *associators* of quasigroups introduced and described by her (cf. [44], [45], [46] and [47]) are useful during investigations of quasigroups.

A large cycle of her works is devoted to *T-quasigroups* and quasigroups which are *linear* or *alinear over groups* (cf. [38], [39], [42] and [43]). The characterization of T-quasigroups, linear and alinear quasigroups with the help of identities is one of the most important results in the theory of quasigroups which are linear over groups.

The last papers of G. Belyavskaya are connected with universal-algebraic problems of the theory of quasigroups and with application of binary and n-ary quasigroups in coding theory. In [65] she suggest a general method of the construction of secret-sharing schemes based on orthogonal systems of partial (in particular, everywhere determined) k-ary operations which generalizes some known methods of the construction of such schemes by finite fields and point out the orthogonal systems of k-ary operations respective of these known schemes.

Galina Belyavskaya was a supervisor of five PhD thesis (S. Murathudjaev, A. Lumpov, P. Syrbu, L. Ursu, A. Tabarov). Many scientists from Moldova and other countries were trained under her supervision. She was the scientific adviser of graduate students from the Kishinev State University.

Since 1971 G. B. Belyavskaya was the assistant of V. D. Belousov in the sector of the theory of quasigroups. After his death she has headed the research team of the theory of quasigroups at the Institute of Mathematics of the Academy of Sciences of Moldova.

She is an Advisory Editor of the international journal *Quasigroups and Related Systems*, and also a member of the Editorial Board of the *Bulletinul Academiei de Ştiinţe a Republicii Moldova, Matematica*.

G. B. Belyavskaya is kind, sympathetic, delicate, trustworthy, very disciplined, honest and modest woman. She is a good wife, mother, grandmother and great grandmother. Recently she has became interested in esoteric and she published two books on this topic.

Dear Galina Borisovna: The authors of this note heartily congratulate you on your 70th birthday and wish you continuing success in your scientific and pedagogical work, strong health, and many long years of life. Thank you for all that you have done for us.

Wieslaw A. Dudek
Victor Shcherbacov

Below we present the full list of publications of Galina B. Belyavskaya. English translations of Russian titles as given in *Mathematical Reviews* and *Zentralblatt für Mathematik* may be somewhat different from those used in this list.

List of publications of Galina B. Belyavskaya

1. *Accounting of partial symmetry of Boolean functions in the synthesis of logical shemes*, (with Yu. N. Pecherskij), (Russian), Teor. Diskret. Avtomatov, Akad. Nauk Latv. SSR (1967), 51 – 54.

2. *Contraction of quasigroups, I*, (Russian), Izv. Akad. Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **1** (1970), 6 – 12.

3. *Contraction of quasigroups, II*, (Russian), Izv. Akad. Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **3** (1970), 3 – 17.

4. *Chain-isotopic quasigroups*, (Russian), Mat. Issled. **5** (1970), 13 – 27.

5. *On generalized prolongation of quasigroups*, (Russian), Mat. Issled. **5**(1970), 28 – 48.

6. *Algorithms for the solution of certain problems in the theory of quasigroups*, (Russian), in "Voprosy teorii kvazigrupp i lup", Kishinev 1970, 20 – 30.

7. *S-systems of an arbitrary index, I*, (with A. M. Cheban), (Russian), Mat. Issled. **7** (1972), 27 – 43.

8. *S-systems of an arbitrary index, II*, (with A. M. Cheban), (Russian), Mat. Issled. **7** (1972), no. 2, 3 – 13.

9. *On semisymmetric Stein's quasigroups*, (with A. M. Cheban), (Russian), Mat. Issled. **7** (1972), no. 3, 231 – 237.

10. *Isotopy of A-quasigroups*, (with M. D. Kitoroage), (Russian), Mat. Issled. **8** (1973), no. 1, 3 – 19.

11. *On a representation of composition of n-ary operations by trees*, (with A. M. Cheban), (Russian), in "Issled. teorii kvazigrupp i lup", Kishynev 1973, 52 – 58.

12. *Wreath product of quasigroups by means of pairwise balanced block designs*, (Russian), in "Kombinatornyi analiz", Moscov MGU, 1974, 49 – 53.

13. *S-systems of quasigroups*, (Russian), Mat. Issled. **9** (1974), no. 2, 10 – 18.

14. *Interdependence of certain closure conditions in k-nets*, (with V. D. Belousov), (Russian), Izv. Akad Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **2** (1974), 44 – 51.

15. *On admissibility of quasigroups*, (with A. F. Russu), (Russian), Mat. Issled. **10** (1975), no. 1(35), 45 – 57.

16. r*-orthogonal quasigroups, I*, (Russian), Mat. Issled. **39** (1976), 32 – 39.

17. r*-orthogonal quasigroups, II*, (Russian), Mat. Issled. **43** (1977), 39 – 49.

18. *On partially admissible quasigroups*, (with A. F. Russu), (Russian), Mat. Issled. **43** (1977), 50 – 58.

19. *Admissible* n*-ary quasigroups, I*, (with S. Murathudjaev), (Russian), Izv. Akad. Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **2** (1977), 14 – 21.

20. *About admissibility of* n*-ary quasigroups*, (with S. Murathudjaev), Proc. Colloq. Math. Soc. J. Bolyai 18, Keszthely, Hungary, 1976, vol.1 "Combinatorics", North-Holland 1978, 101 – 119.

21. *Construction of* $(n-2)$*-orthogonal quasigroups of even order* n*, where* $n-1 \neq 0 (\bmod 3)$, (Russian), Mat. Issled. **51** (1979), 23 – 26.

22. *Admissible* n*-ary quasigroups, II*, (with S. Murathudjaev), (Russian), Mat. Issled. **51** (1979), 27 – 39.

23. *On the spectrum of partial orthogonality of quasigroups of lower orders*, (Russian), Mat. Issled. **66** (1982), 7 – 14.

24. *Spectrum of partial admissibility of finite quasigroups (Latin squares)*, (Russian), Mat. Zamietki **32** (1982), 777 – 788 (translation in Math. Notes **32** (1983), 874 – 880).

25. *On partially orthogonal quasigroups and systems of quasigroups*, (Russian), Mat. Issled. **71** (1983), 25 – 33.

26. *Cross product of two systems of quasigroups and its use in constructing partially orthogonal quasigroups*, with A. D. Lumpov), (Russian), Mat. Issled. **83** (1985), 26 – 38.

27. *Direct decompositions of quasigroups*, (Russian), Mat. Issled. **95** (1987), 23 – 38.

28. *Completion of a group and the construction of orthogonal quasigroups of order* $3t+i,\ i=0,1,2,\ t \neq 2,6,$ *with orthogonal subquasigroups of order* t, (with A. V. Nazarok), (Russian), Mat. Issled. **95** (1987), 39 – 52.

29. *The nuclei and center of a quasigroups*, (Russian), Mat. Issled. **102** (1988), 37 – 52.

30. T*-quasigroups and the center of a quasigroup*, (Russian), Mat. Issled. **111** (1989), 24 – 43.

31. *On one class of self-orthogonal* n*-groupoids*, (with P. N. Syrbu), (Russian), Izv. Akad. Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **2** (1989), 25 – 30.

32. *Latin squares, quasigroups and their applications*, (with V. D. Belousov), (Russian), Ştiinţa, Kishinev, 1989, ISBN: 5-376-00074-5.

33. *Complete direct decompositions of quasigroups with an idempotent*, (Russian), Mat. Issled. **113** (1990), 21 – 36.

34. *On the concept of a center in a quasigroup*, (Russian), Mat. Issled. **120** (1991), 8 – 17.

35. *On one equivalence in quasigroups*, (with A. D. Lumpov), (Russian), Mat. Issled. **120** (1991), 18 – 29.

36. *The nuclei and center of linear quasigroups*, (with A. Th. Tabarov), (Russian), Izv. Akad. Nauk Moldav. SRSR, ser. Fiz.-Tehn. Mat. Nauk **3** (1991), 37 – 42.

37. *r-orthogonal Latin squares*, Annals Discr. Math. **46** (1991), 169 – 202.

38. *Characterization of linear and alinear quasigroups*, (with A. Th. Tabarov), (Russian), Diskr. Mat. **4** (1992), 142 – 147.

39. *Autotopies determining isotopies and autotomorphism of T-quasigroups*, (with A. Th. Tabarov), (Russian), in "Algebraic methods in geometry", Univ. Druzhby Narodov, Moskva, 1992, 77 – 82.

40. *Centre and multiplication groups of quasigroups*, Bul. Acad. Ştiinţe Repub. Mold., Mat. **2(8)** (1992), 81 – 89.

41. *On concept of centre in quasigroups*, Demonstratio Math. **26** (1993), 75–84.

42. *Abelian qusigroups are T-quasigroups*, Quasigroups and Related Systems **1** (1994), 1 – 7.

43. *One-sided T-quasigroups and irreducible balanced identities*, Quasigroups and Related Systems **1** (1994), 8 – 21.

44. *Associators, commutators and linearity of a quasigroups*, Discrete Math. Appl. **5** (1995), 577 – 586.

45. *Theory of quasigroups: nuclei, center and commutator*, (Russian), Bul. Acad. Ştiinţe Repub. Mold., Mat. **2(21)** (1996), 47 – 71.

46. *Associants and the commutant of a quasigroup*, (Russian), Fundam. Prikl. Mat. **3** (1997), 715 – 737.

47. *On commutators of quasigroup congruences*, Bul. Acad. Ştiinţe Rep. Mold., Mat. **2(27)** (1998), 91 – 101.

48. *Centrally isotopic quasigroups*, Quasigroups and Related Systems **5** (1998), 1 – 12.

49. *Quasigroup power sets and cyclic S-systems*, Quasigroups and Related Systems **9** (2002), 1 – 17.

50. *Check character systems over quasigroups and loops*, (with V. I. Izbash and V. A. Shcherbacov), Quasigroups and Related Systems **10** (2003), 1 – 28.

51. *On check character systems over quasigroups and loops*, Algebra Discrete Math. **2** (2003), 1 – 13.

52. *On check character systems over groups*, (with A. Diordiev), Bul. Acad. Ştiinţe Repub. Mold., Mat. **3(46)** (2004), 17 – 24.

53. *Pairwise orthogonality of n-ary operations*, Bul. Acad. Ştiinţe Repub. Mold., Mat. **3(49)** (2005), 5 – 18.

54. *On some quasi-identities in finite quasigroups*, (with A. Diordiev), Bul. Acad. Ştiinţe Repub. Mold., Mat. **3(49)** (2005), 19 – 32.

55. *Check character systems using quasigroups, I*, (with V. I. Izbash and G. L. Mullen), Designs, Codes Cryptography **37** (1995), 215 – 227.

56. *Check character systems using quasigroups, II*, (with V. I. Izbash and G. L. Mullen), Designs, Codes Cryptography **37** (1995), 405 – 419.

57. *Orthogonal hypercubes and n-ary operations*, Quasigroups and Related Systems **13** (2005), 73 – 86.

58. *Strongly orthogonal and uniformly orthogonal many-place operations*, (with G. L. Mullen), Algebra Discrete Math. **1** (2006), 1 – 17.

59. *Power sets of n-ary quasigroups*, Bul. Acad. Ştiinţe Republ. Moldova, Mat. **1(53)** (2007), 37 – 45.

60. *Identities with permutations associated with quasigroups isotopic to groups*, Bul. Acad. Ştiinţe Republ. Moldova, Mat. **2(53)** (2007), 19 – 24.

61. *S-systems of n-ary quasigroups*, Quasigroups and Related Systems **15** (2007), 251 – 260.

62. *On groupoids with the identity defining commutative Moufang loops*, (with A.Tabarov), (Russian), Fund. Prik. Mat. **14** (2008), 33 – 39.

63. *Conjugate-orthogonality and complete multiplication groups of quasigroups*, (with A.Diordiev), Bul. Acad. Ştiinţe Republ. Moldova, Mat. **1(59)** (2008), 22 – 30.

64. *Identities with permutations leading to the linearity of quasigroups*, Discrete Math. Appl. **19** (2009), 173 – 190.

65. *Secret-sharing schemes and orthogonal systems of k-ary operations*, Quasigroups and Related Systems **17** (2009), 161 – 176.

66. *Check character systems and totally conjugate orthogonal T-quasigroups*, Quasigroups and Related Systems **18** (2010), 7 – 16.

67. *Polynomial k-ary operations, matrices, and k-mappings*, J. Gen. Lie Theory Appl. **4** Article ID 100301.

Quasigroups and Related Systems **18** (2010), 113 – 126

Interval-valued $(\in, \in \vee q_{\widetilde{m}})-$ fuzzy subquasigroups

Muhammad Akram and Wieslaw A. Dudek

Abstract. In this paper we introduce the notion of interval-valued $(\in, \in \vee q_{\widetilde{m}})-$ fuzzy subquasigroups and present some of their properties. We characterize interval-valued $(\in, \in \vee q_{\widetilde{m}})-$ fuzzy subquasigroups by their level subsets. The implication-based such new fuzzy subquasigroups are also established.

1. Introduction

The notion of interval-valued fuzzy sets was first introduced by Zadeh [21] as an extension of fuzzy sets in which the values of the membership degrees are intervals of numbers instead of the numbers. Thus, interval-valued fuzzy sets provide a more adequate description of uncertainty than the traditional fuzzy sets. It is therefore important to use interval-valued fuzzy sets in applications, such as fuzzy control. One of the computationally most intensive part of fuzzy control is defuzzification. Since interval-valued fuzzy sets are widely studied and used, we describe briefly the work of Gorzalczany on approximate reasoning [10, 11], Roy and Biswas on medical diagnosis [16] and Turksen on multivalued logic [17].

Murali [12] proposed a definition of a fuzzy point belonging to a fuzzy subset under a natural equivalence on a fuzzy set. The idea of quasi-coincidence of a fuzzy point with a fuzzy set, which is mentioned in [13] played a vital role to generate some different types of fuzzy subgroups. A new type of fuzzy subgroups, $(\in, \in \vee q)$-fuzzy subgroups, was introduced in earlier paper Bhakat and Das [5] by using the combined notions of *belongines* and *quasi-coincidence* of fuzzy point and fuzzy set. In fact, $(\in, \in \vee q)$-fuzzy subgroup is an important and useful generalization of Rosenfeld's fuzzy subgroup. On the other hand, Akram and Dudek applied this concept to subquasigroup in [2] and studied some of its properties. Further, it was discussed by same authors in [3]. In this paper we introduce the notion of

2010 Mathematics Subject Classification: 20N15, 94D05
Keywords: Interval-valued $(\in, \in \vee q_{\widetilde{m}})-$ fuzzy subquasigroup, implication-based fuzzy subquasigroup.

interval-valued $(\in, \in \vee q_m)-$ fuzzy subquasigroups and present some of their properties. We characterize interval-valued $(\in, \in \vee q_m)-$ fuzzy subquasigroups by their level subsets. The implication-based such fuzzy subquasigroups are also established. Some recent results obtained by Akram-Dudek [3] are extended and strengthened.

2. Preliminaries

A groupoid $(G, \cdot)$ is called a *quasigroup* if for any a , $b \in G$ each of the equations $a \cdot x = b$, $x \cdot a = b$ has a unique solution in G. A quasigroup may be also defined as an algebra $(G, \cdot, \backslash, /)$ with three binary operations $\cdot$, $\backslash$, $/$ satisfying the following identities:

$$(x \cdot y)/y = x, \qquad x \backslash (x \cdot y) = y,$$

$$(x/y) \cdot y = x, \qquad x \cdot (x \backslash y) = y.$$

Such defined quasigroup is called an *equasigroup*.

A nonempty subset S of a quasigroup $\mathcal{G} = (G, \cdot, \backslash, /)$ is called a *subquasigroup* if it is closed with respect to these three operations.

In this paper $\mathcal{G}$ always denotes an equasigroup $(G, \cdot, \backslash, /)$; G always denotes a nonempty set.

Definition 2.1. An interval number D is an interval $[a^-, a^+]$ with $0 \leqslant a^- \leqslant a^+ \leqslant 1$. Denote the set of all interval numbers by $D[0,1]$. Then the interval $[a, a]$ can be simply identified with the number $a \in [0,1]$. For any two given interval numbers $D_1 = [a_1^-, b_1^+]$ and $D_2 = [a_2^-, b_2^+] \in D[0,1]$, we define

$$\mathrm{rmin}\{D_1, D_2\} = \mathrm{rmin}\{[a_1^-, b_1^+], [a_2^-, b_2^+]\} = [\min\{a_1^-, a_2^-\}, \min\{b_1^+, b_2^+\}],$$

$$\mathrm{rmax}\{D_1, D_2\} = \mathrm{rmax}\{[a_1^-, b_1^+], [a_2^-, b_2^+]\} = [\max\{a_1^-, a_2^-\}, \max\{b_1^+, b_2^+\}],$$

and take

- $D_1 \leqslant D_2 \Longleftrightarrow a_1^- \leqslant a_2^-$ and $b_1^+ \leqslant b_2^+$,
- $D_1 = D_2 \Longleftrightarrow a_1^- = a_2^-$ and $b_1^+ = b_2^+$,
- $D_1 < D_2 \Longleftrightarrow D_1 \leqslant D_2$ and $D_1 \neq D_2$,
- $kD = k[a_1^-, b_1^+] = [ka_1^-, kb_1^+]$, where $0 \leqslant k \leqslant 1$.

Then, $(D[0,1], \leqslant, \vee, \wedge)$ forms a complete lattice under set inclusion with $[0,0]$ acts as its least element and $[1,1]$ acts as its greatest element. For interval numbers $D_1 = [a_1^-, b_1^+]$, $D_2 = [a_2^-, b_2^+] \in D[0,1]$ we define

- $D_1 + D_2 = [a_1^- + a_2^- - a_1^- a_2^-, b_1^+ + b_2^+ - b_1^+ b_2^+]$.

Definition 2.2. Let G be a given set. Then, the interval-valued fuzzy set (briefly, IF set) A in G is defined by

$$A = \{(x, [\mu_A^-(x), \mu_A^+(x)]) : x \in G\}$$

where $\mu_A^-(x)$ and $\mu_A^+(x)$ are fuzzy sets of G such that $\mu_A^-(x) \leqslant \mu_A^+(x)$ for all $x \in G$. Let $\widetilde{\mu}_A(x) = [\mu_A^-(x), \mu_A^+(x)]$. Then

$$A = \{(x, \widetilde{\mu}_A(x)) : x \in G\},$$

where $\widetilde{\mu}_A : G \to D[0,1]$.

Definition 2.3. An interval-valued fuzzy set $\widetilde{\mu}$ in a quasigroups $\mathcal{G}$ is called an *interval-valued fuzzy subquasigroup* of $\mathcal{G}$ if the following condition is satisfied:

$$\widetilde{\mu}(x * y) \geq \text{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} \quad \forall\ x,\ y\ \in G.$$

Definition 2.4. An *interval-valued fuzzy empty set* $\widetilde{0}$ and *interval-valued fuzzy whole set* $\widetilde{1}$ in a set G are defined by $\widetilde{0}(x) = [0,0]$ and $\widetilde{1}(x) = [1,1]$, for all $x \in G$. We write $\widetilde{t} = [t_1, t_2]$ and $\widetilde{s} = [s_1, s_2]$ in the interval $D[0,1]$.

Based on Bhakat and Das [4], we can extend the concept of quasi-coincidence of fuzzy point within a fuzzy set to the concept of quasi-coincidence of a fuzzy interval value with an interval valued fuzzy set as follows:

Definition 2.5. An interval valued fuzzy set $\widetilde{\mu}$ of a quasigroup $\mathcal{G}$ of the form

$$\widetilde{\mu}(y) = \begin{cases} \widetilde{t} \in (\widetilde{0}, \widetilde{1}], & \text{if } y = x \\ \widetilde{0}, & \text{if } y \neq x \end{cases}$$

is called *fuzzy interval value with support* x and interval value $\widetilde{t}$ and is denoted by $x_{\widetilde{t}}$. A fuzzy interval value $x_{\widetilde{t}}$ is said to be belong to an interval valued fuzzy set $\widetilde{\mu}$ written as $x_{\widetilde{t}} \in \widetilde{\mu}$ if $\widetilde{\mu}(x) \geqslant \widetilde{t}$. A fuzzy interval value $x_{\widetilde{t}}$ is said to be quasi-coincident with an interval valued fuzzy set $\widetilde{\mu}$ written as $x_{\widetilde{t}} q \widetilde{\mu}$ if $\widetilde{\mu}(x) + \widetilde{t} > \widetilde{1}$.

Let m be an element of $[0,1)$ and let $\widetilde{m}$ be an element of $D[0,1)$ unless otherwise specified. By $x_{\widetilde{t}}q_{\widetilde{m}}\widetilde{\mu}$, we mean $\widetilde{\mu}(x)+\widetilde{t}+\widetilde{m}>\widetilde{1},\ \ \widetilde{t}\in D(0,\frac{1-m}{2}]$. For brevity, we write the following notions:

- $x_{\widetilde{t}}\in\widetilde{\mu}$ or $x_{\widetilde{t}}q_{\widetilde{m}}\widetilde{\mu}$ will be denoted by $x_{\widetilde{t}}\in\!\vee q_{\widetilde{m}}\widetilde{\mu}$.
- $x_{\widetilde{t}}\in\widetilde{\mu}$ and $x_{\widetilde{t}}q_{\widetilde{m}}\widetilde{\mu}$ will be denoted by "$x_{\widetilde{t}}\in\!\wedge q_{\widetilde{m}}\widetilde{\mu}$."
- The symbol $\overline{\in\wedge q_{\widetilde{m}}}$ means neither $\in$ nor $q_{\widetilde{m}}$ hold.

3. Interval-valued $(\in,\in\vee q_m)-$fuzzy subquasigroups

Definition 3.1. An interval-valued fuzzy set $\widetilde{\mu}$ in G is called an interval-valued $(\in,\in\!\vee q_{\widetilde{m}})$-*fuzzy subquasigroup* of $\mathcal{G}$, if

$$x_{\widetilde{t}_1},y_{\widetilde{t}_2}\in\widetilde{\mu}\Longrightarrow(x*y)_{\mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\}}\in\vee q_{\widetilde{m}}\widetilde{\mu}$$

for all $x,y\in G$, $\widetilde{t}_1,\widetilde{t}_2\in D(0,1]$ and $*\in\{\cdot,\backslash,/\}$.

Note that an interval-valued $(\in,\in\!\vee q_{\widetilde{m}})$-*fuzzy subquasigroup* with $m=0$ is called *an interval-valued* $(\in,\in\!\vee q)$-*fuzzy subquasigroup*.

Example 3.2. Let $G=\{0,a,b,c\}$ be a quasigroup with the following multiplication table:

$\cdot$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

(i) Consider an interval-valued fuzzy set

$$\widetilde{\mu}(x)=\begin{cases}[0.65,0.7], & \text{if } x=0,\\ [0.75,0.8] & \text{if } x=a,\\ [0.35,0.4] & \text{if } x=b,\\ [0.35,0.4] & \text{if } x=c.\end{cases}$$

If $m=0.15$, then $U(\widetilde{\mu};\widetilde{t})=G$ for all $\widetilde{t}\in D(0,0.4]$. Hence $\widetilde{\mu}$ is an interval-valued $(\in,\in\vee q_{[0.15,0.15]})$-fuzzy subquasigroup of $\mathcal{G}$.

(ii) Now consider an interval-valued fuzzy set

$$\widetilde{\mu}(x) = \begin{cases} [0.42, 0.45] & \text{if } \ x = 0, \\ [0.40, 0.41] & \text{if } \ x = a, \\ [0.40, 0.41] & \text{if } \ x = c, \\ [0.47, 0.49] & \text{if } \ x = b. \end{cases}$$

In this case for $m = 0.04$ we have

$$U(\widetilde{\mu}; t) = \begin{cases} G & \text{if } \ t \in D(0, 0.4], \\ \{0, b\} & \text{if } \ t \in D(0.4, 0.45], \\ \{b\} & \text{if } \ t \in D(0.45, 0.48]. \end{cases}$$

Since $\{b\}$ is not a subquasigroup of $\mathcal{G}$, so $U(\widetilde{\mu}; t)$ is not a subquasigroup for $t \in D(0.45, 0.48]$. Hence $\widetilde{\mu}$ is not an interval-valued $(\in, \in \vee q_{[0.04,0.04]})$-fuzzy subquasigroup of a quasigroup $\mathcal{G}$. $\square$

We now formulate a technical characterization.

Theorem 3.3. *An interval-valued fuzzy set $\widetilde{\mu}$ in $\mathcal{G}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$ if and only if*

$$\widetilde{\mu}(x * y) \geqslant \operatorname{rmin}\Big\{\widetilde{\mu}(x), \widetilde{\mu}(y), \Big[\frac{1-m}{2}, \frac{1-m}{2}\Big]\Big\} \tag{1}$$

holds for all x, $y \in G$.

Proof. Let $\widetilde{\mu}$ be an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. Assume that (1) is not valid. Then there exist x', $y' \in G$ such that

$$\widetilde{\mu}(x' * y') < \operatorname{rmin}\Big\{\widetilde{\mu}(x'), \widetilde{\mu}(y'), \Big[\frac{1-m}{2}, \frac{1-m}{2}\Big]\Big\}.$$

If $\operatorname{rmin}(\widetilde{\mu}(x'), \widetilde{\mu}(y')) < [\frac{1-m}{2}, \frac{1-m}{2}]$, then $\widetilde{\mu}(x' * y') < \operatorname{rmin}(\widetilde{\mu}(x'), \widetilde{\mu}(y'))$. Thus

$$\widetilde{\mu}(x' * y') < \widetilde{t} \leqslant \operatorname{rmin}\{\widetilde{\mu}(x'), \widetilde{\mu}(y')\} \qquad \text{for some } \widetilde{t} \in D(0, 1].$$

It follows that $x'_{\widetilde{t}} \in \widetilde{\mu}$ and $y'_{\widetilde{t}} \in \widetilde{\mu}$, but $(x' * y')_{\widetilde{t}} \overline{\in} \widetilde{\mu}$, a contradiction. Moreover, $\widetilde{\mu}(x' * y') + \widetilde{t} < 2\widetilde{t} < [1-m, 1-m]$, and so $(x' * y')_{\widetilde{t}} \overline{q_{\widetilde{m}}} \widetilde{\mu}$. Hence, consequently $(x' * y')_{\widetilde{t}} \overline{\in \vee q_{\widetilde{m}}} \widetilde{\mu}$, a contradiction.

On the other hand, if $\mathrm{rmin}\{\widetilde{\mu}(x'),\widetilde{\mu}(y')\} \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$, then $\widetilde{\mu}(x') \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$, $\widetilde{\mu}(y') \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$ and $\widetilde{\mu}(x' * y') < [\frac{1-m}{2},\frac{1-m}{2}]$.

Thus $x'_{[\frac{1-m}{2},\frac{1-m}{2}]} \in \widetilde{\mu}$ and $y'_{[\frac{1-m}{2},\frac{1-m}{2}]} \in \widetilde{\mu}$, but $(x' * y')_{[\frac{1-m}{2},\frac{1-m}{2}]} \overline{\in} \widetilde{\mu}$. Also

$$\widetilde{\mu}(x'*y') + \left[\frac{1-m}{2},\frac{1-m}{2}\right] < \left[\frac{1-m}{2},\frac{1-m}{2}\right] + \left[\frac{1-m}{2},\frac{1-m}{2}\right] = [1-m,1-m],$$

i.e., $(x' * y')_{[\frac{1-m}{2},\frac{1-m}{2}]} \overline{q}_{\widetilde{m}} \widetilde{\mu}$. Hence $(x' * y')_{[\frac{1-m}{2},\frac{1-m}{2}]} \overline{\in \vee q_{\widetilde{m}}} \widetilde{\mu}$, a contradiction. So (1) is valid.

Conversely, assume that $\widetilde{\mu}$ satisfies (1). Let $x, y \in G$ and $\widetilde{t}_1, \widetilde{t}_2 \in D(0,1]$ be such that $x_{\widetilde{t}_1} \widetilde{\mu}$ and $y_{\widetilde{t}_2} \in \widetilde{\mu}$. Then

$$\widetilde{\mu}(x*y) \geqslant \mathrm{rmin}\Big\{\widetilde{\mu}(x),\widetilde{\mu}(y),\left[\frac{1-m}{2},\frac{1-m}{2}\right]\Big\} \geqslant \mathrm{rmin}\Big\{\widetilde{t}_1,\widetilde{t}_2,\left[\frac{1-m}{2},\frac{1-m}{2}\right]\Big\}.$$

Assume that $\widetilde{t}_1 \leqslant [\frac{1-m}{2},\frac{1-m}{2}]$ or $\widetilde{t}_2 \leqslant [\frac{1-m}{2},\frac{1-m}{2}]$. Then $\widetilde{\mu}(x * y) \geqslant \mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\}$, which implies that $(x * y)_{\mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\}} \in \widetilde{\mu}$. Now suppose that $\widetilde{t}_1 > [\frac{1-m}{2},\frac{1-m}{2}]$ and $\widetilde{t}_2 > [\frac{1-m}{2},\frac{1-m}{2}]$. Then $\widetilde{\mu}(x * y) \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$, and thus

$$\widetilde{\mu}(x*y) + \mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\} > \left[\frac{1-m}{2},\frac{1-m}{2}\right] + \left[\frac{1-m}{2},\frac{1-m}{2}\right] = [1-m,1-m],$$

i.e., $(x * y)_{\mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\}} q_{\widetilde{m}} \widetilde{\mu}$. Hence $(x * y)_{\mathrm{rmin}\{\widetilde{t}_1,\widetilde{t}_2\}} \in \vee q_{\widetilde{m}} \widetilde{\mu}$, and consequently, $\widetilde{\mu}$ is an interval-valued $(\in, \in\!\vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. □

The following Corollary follows when $m = 0$.

Corollary 3.4. *An interval-valued fuzzy set $\widetilde{\mu}$ in $\mathcal{G}$ is an interval-valued $(\in, \in \vee q)$-fuzzy subquasigroup of $\mathcal{G}$ if and only if*

$$\widetilde{\mu}(x * y) \geqslant \mathrm{rmin}\Big\{\widetilde{\mu}(x),\widetilde{\mu}(y)\Big\}$$

holds for all x, $y \in G$. □

Theorem 3.5. *An interval-valued fuzzy set $\widetilde{\mu}$ of G is an interval-valued $(\in, \in\!\vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$ if and only if each nonempty level set $U(\widetilde{\mu};\widetilde{t})$, $\widetilde{t} \in D(0,\frac{1-m}{2}]$, is a subquasigroup of $\mathcal{G}$.*

Proof. Assume that $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. Let $\widetilde{t} \in D(0, \frac{1-m}{2}]$ and $x, y \in U(\widetilde{\mu}; \widetilde{t})$. Then $\widetilde{\mu}(x) \geqslant \widetilde{t}$ and $\widetilde{\mu}(y) \geqslant \widetilde{t}$. It follows from Condition (1) that

$$\widetilde{\mu}(x*y) \geqslant \text{rmin}\Big\{\widetilde{\mu}(x), \widetilde{\mu}(y), \Big[\frac{1-m}{2}, \frac{1-m}{2}\Big]\Big\} \geqslant \text{rmin}\Big\{\widetilde{t}, \Big[\frac{1-m}{2}, \frac{1-m}{2}\Big]\Big\} = \widetilde{t},$$

so that $x * y \in U(\widetilde{\mu}; \widetilde{t})$. Hence $U(\widetilde{\mu}; \widetilde{t})$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$.

Conversely, suppose that the nonempty set $U(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$ for all $\widetilde{t} \in D(0, \frac{1-m}{2}]$. If the condition(1) is not true, then there exists a, $b \in G$ such that $\widetilde{\mu}(a * b) < \text{rmin}\{\widetilde{\mu}(a), \widetilde{\mu}(b), [\frac{1-m}{2}, \frac{1-m}{2}]\}$. Hence we can take $\widetilde{t} \in D(0, 1]$ such that $\widetilde{\mu}(a * b) < \widetilde{t}_1 < \text{rmin}\{\widetilde{\mu}(a), \widetilde{\mu}(b), [\frac{1-m}{2}, \frac{1-m}{2}]\}$. Then $\widetilde{t} \in D(0, \frac{1-m}{2}]$ and $a, b \in U(\widetilde{\mu}; \widetilde{t})$. Since $U(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$, it follows that $a*b \in U(\widetilde{\mu}; \widetilde{t})$, so $\widetilde{\mu}(a*b) \geqslant \widetilde{t}$. This is a contradiction. Therefore the condition (1) is valid, and so $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. □

We induce the following Corollary by putting $m = 0$.

Corollary 3.6. *An interval-valued fuzzy set $\widetilde{\mu}$ of G is an interval-valued $(\in, \in \vee q)$-fuzzy subquasigroup of $\mathcal{G}$ if and only if each nonempty level set $U(\widetilde{\mu}; \widetilde{t})$, $\widetilde{t} \in D(0, 1]$, is a subquasigroup of $\mathcal{G}$.* □

Theorem 3.7. *Let $\widetilde{\mu}$ be an interval-valued fuzzy set of a quasigroup $\mathcal{G}$. Then the nonempty level set $U(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$ for all $\widetilde{t} \in D(\frac{1-m}{2}, 1]$ if and only if*

$$\text{rmax}\Big\{\widetilde{\mu}(x * y), \Big[\frac{1-m}{2}, \frac{1-m}{2}\Big]\Big\} \geqslant \text{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$$

for all $x, y \in G$.

Proof. Suppose that $U(\widetilde{\mu}; \widetilde{t}) \neq \emptyset$ is a subquasigroup of $\mathcal{G}$. Assume that $\text{rmax}\{\widetilde{\mu}(x * y), [\frac{1-m}{2}, \frac{1-m}{2}]\} < \text{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} = \widetilde{t}$ for some x, $y \in G$, then $\widetilde{t} \in D(\frac{1-m}{2}, 1]$, $\widetilde{\mu}(x*y) < \widetilde{t}$, $x \in U(\widetilde{\mu}; \widetilde{t})$ and $y \in U(\widetilde{\mu}; \widetilde{t})$. Since x, $y \in U(\widetilde{\mu}; \widetilde{t})$, $U(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$, so $x * y \in U(\widetilde{\mu}; \widetilde{t})$, a contradiction.

The proof of the second part of Theorem is straightforward. □

The following Corollary follows when $m = 0$.

Corollary 3.8. *Let $\widetilde{\mu}$ be an interval-valued fuzzy set of a quasigroup $\mathcal{G}$. Then for every $\widetilde{t} \in D(0.5, 1]$ each nonempty level set $U(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$ if and only if*

$$\operatorname{rmax}\Big\{\widetilde{\mu}(x * y)\Big\} \geqslant \operatorname{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}$$

for all $x, y \in G$. □

Theorem 3.9. *For any finite strictly increasing chain of subquasigroups of $\mathcal{G}$ there exists an interval-valued$(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup $\widetilde{\mu}$ of $\mathcal{G}$ whose level subquasigroups are precisely the members of the chain with $\widetilde{\mu}_{[\frac{1-m}{2}, \frac{1-m}{2}]} = G_0 \subset G_1 \subset \ldots \subset G_n = G$.*

Proof. Let $\{\widetilde{t}_i \,|\, \widetilde{t}_i \in D(0, \frac{1-m}{2}], i = 1, \ldots, n\}$ be such that $[\frac{1-m}{2}, \frac{1-m}{2}] > \widetilde{t}_1 > \widetilde{t}_2 > \widetilde{t}_3 > \ldots > \widetilde{t}_n$. Consider the interval-valued fuzzy set $\widetilde{\mu}$ defined by

$$\widetilde{\mu}(x) = \begin{cases} [\frac{1-m}{2}, \frac{1-m}{2}] & \text{if } \ x \in G_0, \\ \widetilde{t}_k & \text{if } \ x \in G_k \setminus G_{k-1}, \ k = 1, \ldots, n \end{cases}$$

Let $x, y \in G$ be such that $x \in G_i \setminus G_{i-1}$ and $y \in G_j \setminus G_{j-1}$, where $1 \leqslant i, j \leqslant n$. We consider the following cases:
Case I: when $i \geqslant j$, then $x \in G_i$, $y \in G_i$, so $x * y \in G_i$. Thus

$$\widetilde{\mu}(x * y) \geqslant \widetilde{t}_i = \operatorname{rmin}\{\widetilde{t}_i, \widetilde{t}_j\} = \operatorname{rmin}\Big\{\widetilde{\mu}(x), \widetilde{\mu}(y), \left[\frac{1-m}{2}, \frac{1-m}{2}\right]\Big\}.$$

Case II: when $i < j$, then $x \in G_j$, $y \in G_j$, so $x * y \in G_j$. Thus

$$\widetilde{\mu}(x * y) \geqslant t_j = \operatorname{rmin}\{t_i, t_j\} = \operatorname{rmin}\Big\{\widetilde{\mu}(x), \widetilde{\mu}(y), \left[\frac{1-m}{2}, \frac{1-m}{2}\right]\Big\}.$$

Hence $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. □

The following Corollary follows when $m = 0$.

Corollary 3.10. *For any finite strictly increasing chain of subquasigroups of $\mathcal{G}$ there exists an interval-valued $(\in, \in \vee q)$-fuzzy subquasigroup $\widetilde{\mu}$ of $\mathcal{G}$ whose level subquasigroups are precisely the members of the chain with $\widetilde{\mu}_{[0.5,0.5]} = G_0 \subset G_1 \subset \ldots \subset G_n = G$.* □

Definition 3.11. For an interval-valued fuzzy set $\widetilde{\mu}$ in $\mathcal{G}$ and $\widetilde{t} \in D(0, 1]$, we define four sets:

(a) $Q(\widetilde{\mu};\widetilde{t}) = \{x \in G \mid x_{\widetilde{t}}q\widetilde{\mu}\}$,

(b) $Q^m(\widetilde{\mu};\widetilde{t}) = \{x \in G \mid x_{\widetilde{t}}q_{\widetilde{m}}\,\widetilde{\mu}\}$,

(c) $[\widetilde{\mu}]_{\widetilde{t}} = \{x \in G \mid x_{\widetilde{t}} \in \vee q\,\widetilde{\mu}\}$,

(d) $[\widetilde{\mu}]_t^m = \{x \in G \mid x_{\widetilde{t}} \in \vee q_{\widetilde{m}}\,\mu\}$.

It is clear that $[\widetilde{\mu}]_{\widetilde{t}}^m = U(\widetilde{\mu};\widetilde{t}) \cup Q^m(\widetilde{\mu};\widetilde{t})$.

Example 3.12. Let $G = \{0, a, b, c\}$ be a quasigroup which is given in Example 3.2. Consider interval-valued fuzzy sets

$$\widetilde{\mu}(x) = \begin{cases} [0.65,\ 0.67] & \text{if } x = 0, \\ [0.54,\ 0.56] & \text{if } x = a, \\ [0.45,\ 0.47] & \text{if } x = b, \\ [0.39,\ 0.41] & \text{if } x = c, \end{cases} \qquad \widetilde{\nu}(x) = \begin{cases} [0.58,\ 0.60] & \text{if } x = 0, \\ [0.03,\ 0.05] & \text{if } x = a, \\ [0.48,\ 0.50] & \text{if } x = b, \\ [0.04,\ 0.06] & \text{if } x = c. \end{cases}$$

(1) When $m = 0.6$, then $U(\widetilde{\mu};\widetilde{t}) = G$ and $Q(\widetilde{\mu};\widetilde{t}) = G$ for all $t \in D(0, 0.2]$. Thus $[\widetilde{\mu}]_{\widetilde{t}} = G$ for all $\widetilde{t} \in D(0, 0.2]$. Hence $[\widetilde{\mu}]_{\widetilde{t}}$ is an interval-valued $(\in, \in \vee q_{[0.6,0.6]})$-fuzzy subquasigroup of $\mathcal{G}$.

(2) When $m = 0.8$, then $U(\widetilde{\nu};\widetilde{t}) = G$ and $Q(\widetilde{\nu};\widetilde{t}) = \{0, b\}$ for all $\widetilde{t} \in D(0, 0.1]$. Thus $[\widetilde{\nu}]_{\widetilde{t}} = G$ for all $\widetilde{t} \in D(0, 0.1]$. Hence $[\widetilde{\nu}]_{\widetilde{t}}$ is an interval-valued $(\in, \in \vee q_{[0.8,0.8]})$-fuzzy subquasigroup of $\mathcal{G}$. □

We formulate a nice characterization.

Theorem 3.13. *An interval-valued fuzzy set $\widetilde{\mu}$ of $\mathcal{G}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$ if and only if for every $\widetilde{t} \in D(\frac{1-m}{2}, 1]$ each nonempty level $Q^m(\widetilde{\mu};\widetilde{t})$ is a subquasigroup of $\mathcal{G}$.*

Proof. Assume that $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$ and let $\widetilde{t} \in D(\frac{1-m}{2}, 1]$ be such that $Q^m(\widetilde{\mu};\widetilde{t}) \neq \emptyset$. Let $x, y \in Q^m(\widetilde{\mu};\widetilde{t})$. Then $x_{\widetilde{t}}q_{\widetilde{m}}\widetilde{\mu}$ and $y_{\widetilde{t}}q_{\widetilde{m}}\widetilde{\mu}$, i.e., $\widetilde{\mu}(x) + \widetilde{t} + \widetilde{m} > \widetilde{1}$ and $\widetilde{\mu}(y) + \widetilde{t} + \widetilde{m} > \widetilde{1}$. Using Theorem 3.3, we have

$$\widetilde{\mu}(x * y) \geqslant \text{rmin}\left\{\widetilde{\mu}(x), \widetilde{\mu}(y), \left[\frac{1-m}{2}, \frac{1-m}{2}\right]\right\}$$

$$\widetilde{\mu}(x * y) \geqslant \text{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} \quad \text{if } \text{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} \geqslant \left[\frac{1-m}{2}, \frac{1-m}{2}\right],$$

$$\widetilde{\mu}(x*y) \geqslant \left[\frac{1-m}{2}, \frac{1-m}{2}\right] \quad \text{if } \mathrm{rmin}\,\{\widetilde{\mu}(x), \widetilde{\mu}(y)\} < \left[\frac{1-m}{2}, \frac{1-m}{2}\right]$$

that is, $(x*y)_{\widetilde{t}}\, q_{\widetilde{m}}\, \widetilde{\mu}$. So $x*y \in Q^m(\widetilde{\mu}; \widetilde{t})$. Hence $Q^m(\widetilde{\mu}; \widetilde{t})$ is a subquasigroup of $\mathcal{G}$.

The proof of the sufficiency part is straightforward and is hence omitted. This completes the proof. □

Open problem. Prove or disprove that the following characterization is true.

An interval-valued fuzzy set $\widetilde{\mu}$ of $\mathcal{G}$ is an interval-valued $(\in, \in \vee q_m)$-fuzzy subquasigroup of $\mathcal{G}$ if and only if for every $\widetilde{t} \in D(\frac{1-m}{2}, 1]$ each nonempty level $[\widetilde{\mu}]^m_{\widetilde{t}}$ is an subquasigroup of $\mathcal{G}$.

4. Implication-based new fuzzy subquasigroups

Fuzzy logic is an extension of set theoretic multivalued logic in which the truth values are linguistic variables or terms of the linguistic variable truth. Some operators, for example $\vee$; $\wedge$; $\neg$; $\rightarrow$ in fuzzy logic are also defined by using truth tables and the extension principle can be applied to derive definitions of the operators. In fuzzy logic, the truth value of fuzzy proposition p is denoted by $[p]$. For a universe of discourse U, we display the fuzzy logical and corresponding set-theoretical notations used in this paper.

1. $[x \in p] = p(x)$,
2. $[p \wedge q] = \min\{[p], [q]\}$,
3. $[p \rightarrow q] = \min\{1, 1 - [p] + [q]\}$,
4. $[\forall x p(x)] = \inf_{x \in U}\{p(x)\}$,
5. $\models p$ if and only if $[p] = 1$ for all valuations.

The truth valuation rules given in (4) are those in the Lukasiewicz system of continuous-valued logic. Of course, various implication operators have been defined. We show only a selection of them in the following:

A. Gaines-Rescher implication operator (I_{GR}):

$$I_{GR}(x, y) := \begin{cases} 1 & \text{if } \ x \leqslant y, \\ 0 & \text{otherwise} \ . \end{cases}$$

B. Gödel implication operator (I_G):

$$I_G(x,y) := \begin{cases} 1 & \text{if } x \leqslant y, \\ y & \text{otherwise} . \end{cases}$$

C. The contraposition of Gödel implication operator $(\overline{I}_G)$:

$$\overline{I}_G(x,y) := \begin{cases} 1 & \text{if } x \leqslant y, \\ 1-x & \text{otherwise} . \end{cases}$$

Ying [19] introduced the concept of fuzzifying topology. We can extend this concept to a quasigroup, and we define an interval-valued fuzzfying subquasigroup as follows:

Definition 4.1. An interval-valued fuzzy set $\widetilde{\mu}$ in G is called an *interval-valued fuzzifying subquasigroup* of $\mathcal{G}$ if

$$\models \min\{[x \in \widetilde{\mu}], [y \in \widetilde{\mu}]\} \to [x * y \in \widetilde{u}]$$

for any x, $y \in G$.

Obviously, Definition 4.1 is equivalent to the Definition 2.3. Hence an interval-valued fuzzifying subquasigroup is a fuzzy subquasigroup. Ying [18] introduced the concept of t-topology, i.e., $\models_t p$ if and only if $[p] \geqslant t$ for all valuations. We give the definition of $\widetilde{t}$-implication-based subquasigroup.

Definition 4.2. Let $\widetilde{\mu}$ be an interval-valued fuzzy set of G and $\widetilde{t} \in D(0,1]$. Then $\widetilde{\mu}$ is called a *$\widetilde{t}$-implication-based subquasigroup* of $\mathcal{G}$ if for any $x, y \in G$ $\models_{\widetilde{t}} \min\{[x \in \widetilde{\mu}], [y \in \widetilde{\mu}]\} \to [x * y \in \widetilde{\mu}]$.

The following proposition is obvious.

Proposition 4.3. *Let I be an implication operator. An interval-valued fuzzy set $\widetilde{\mu}$ of $\mathcal{G}$ is a $\widetilde{t}$-implication based interval-valued fuzzy subquasigroup of $\mathcal{G}$ if and only if* $I(\mathrm{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y)\}, \widetilde{\mu}(x * y)) \geqslant \widetilde{t}$ *for all x, $y \in G$.* $\square$

We now formulate characterizations of implication-based interval-valued fuzzy subquasigroups.

Theorem 4.4. *Let $\widetilde{\mu}$ be an interval-valued fuzzy set in G. If $I = I_G$, then $\widetilde{\mu}$ is a $[\frac{1-m}{2}, \frac{1-m}{2}]$-implication- based interval-valued fuzzy subquasigroup of $\mathcal{G}$ if and only if $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$.*

Proof. Suppose that $\widetilde{\mu}$ is a $[\frac{1-m}{2},\frac{1-m}{2}]$-implication based subquasigroup of $\mathcal{G}$. Then

(i) $I_G(\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\},\widetilde{\mu}(x*y)) \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$ for all $x, y \in G$.

(i) implies that
$\widetilde{\mu}(x*y) \geqslant \mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\}$ or $\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\} \geqslant \widetilde{\mu}(x*y) \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$.
It follows that

$$\widetilde{\mu}(x*y) \geqslant \min\left\{\widetilde{\mu}(x),\widetilde{\mu}(y),\left[\frac{1-m}{2},\frac{1-m}{2}\right]\right\}.$$

From Theorem 3.3, it follows that $\widetilde{\mu}$ is an interval-valued $(\in,\in\vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$.

Conversely, suppose that $\widetilde{\mu}$ is an interval-valued $(\in,\in\vee q_{\widetilde{m}})$-fuzzy subquasigroup of $\mathcal{G}$. From Theorem 3.3, if $\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y),[\frac{1-m}{2},\frac{1-m}{2}]\} = \mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\}$, then

$$I_G(\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y),\widetilde{\mu}(x*y)\} = \widetilde{1} \geqslant \left[\frac{1-m}{2},\frac{1-m}{2}\right].$$

Otherwise, $I_G(\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y),\widetilde{\mu}(x*y)\} \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$. Hence $\widetilde{\mu}$ is a $[\frac{1-m}{2},\frac{1-m}{2}]$–implication based subquasigroup of $\mathcal{G}$. □

Theorem 4.5. *Let $\widetilde{\mu}$ be an interval-valued fuzzy set in G. If $I=\overline{I}_G$, then $\widetilde{\mu}$ is a $[\frac{1-m}{2},\frac{1-m}{2}]$-implication-based interval-valued fuzzy subquasigroup of $\mathcal{G}$ if and only if $\widetilde{\mu}$ satisfies the following assertion for all $x, y \in G$:*

(ii) $\mathrm{rmax}\{\widetilde{\mu}(x),[\frac{1-m}{2},\frac{1-m}{2}]\} \geqslant \mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y),\widetilde{1}\}$.

Proof. Suppose that $\widetilde{\mu}$ is a $\left[\frac{1-m}{2},\frac{1-m}{2}\right]$–implication based interval-valued fuzzy subquasigroup of $\mathcal{G}$. Then

(iii) $\overline{I}_G(\min\{\widetilde{\mu}(x*y),\widetilde{\mu}(x),\widetilde{\mu}(y)\}) \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$ for all $x,y \in G$.

From (iii), it follows that $\overline{I}_G(\mathrm{rmin}\{\widetilde{\mu}(x*y),\widetilde{\mu}(x),\widetilde{\mu}(y)\}) = \widetilde{1}$, that is, $\widetilde{\mu}(x*y) \geqslant \mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\}$ or $\widetilde{1}-\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\} \geqslant [\frac{1-m}{2},\frac{1-m}{2}]$, i.e., $\mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y)\} \leqslant [\frac{1-m}{2},\frac{1-m}{2}]$.
Thus

$$\mathrm{rmax}\left\{\widetilde{\mu}(x*y),\left[\frac{1-m}{2},\frac{1-m}{2}\right]\right\} \geqslant \mathrm{rmin}\{\widetilde{\mu}(x),\widetilde{\mu}(y),\widetilde{1}\}.$$

Hence $\widetilde{\mu}$ satisfies (ii).

The proof of converse part is obvious. □

Theorem 4.6. *Let $\widetilde{\mu}$ be an interval-valued fuzzy set in G. If $I = I_{GR}$, then $\widetilde{\mu}$ is a $[0.5, 0.5]$-implication- based interval-valued fuzzy subquasigroup of $\mathcal{G}$ if and only if $\widetilde{\mu}$ is an interval-valued fuzzy subquasigroup of $\mathcal{G}$.*

Proof. Obvious. □

Corollary 4.7. *Let $I = I_G$. Then $\widetilde{\mu}$ is a $[0.5, 0.5]$–implication-based interval-valued fuzzy subquasigroup of a quasigroup $\mathcal{G}$ if and only if $\widetilde{\mu}$ is an interval-valued $(\in, \in \vee q_{\widetilde{m}})$- fuzzy subquasigroup of $\mathcal{G}$.* □

Corollary 4.8. *Let $I = \overline{I}_G$. Then $\widetilde{\mu}$ is a $[0.5, 0.5]$–implication-based interval-valued fuzzy subquasigroup of a quasigroup $\mathcal{G}$ if and only if $\widetilde{\mu}$ satisfies the following conditions:*

$$\operatorname{rmax}\{\widetilde{\mu}(x * y), [0.5, 0.5]\} \geqslant \operatorname{rmin}\{\widetilde{\mu}(x), \widetilde{\mu}(y), \widetilde{1}\}$$

for all $x, y \in G$. □

References

[1] **M. Akram**, *Fuzzy subquasigroups with respect to a s-norm*, Bul. Acad. Sci. Republ. Moldova, ser. Mathematica **2** (2008), 3 – 13.

[2] **M. Akram and W. A. Dudek**, *Generalized fuzzy subquasigroups*, Quasigroups and Related Systems **16** (2008), 133 – 146.

[3] **M. Akram and W. A. Dudek**, *New fuzzy subquasigroups*, Quasigroups and Related Systems **17** (2009), 107 – 118.

[4] **S. K. Bhakat and P. Das**, *On the definition of a fuzzy subgroups*, Fuzzy Sets and Systems **51**(1992) 235-241.

[5] **S. K. Bhakat and P. Das**, $(\in, \in \vee q)$-fuzzy subgroup, Fuzzy Sets and Systems **80** (1996), 359 – 368.

[6] **P. Das**, *Fuzzy groups and level subgroups*, J. Math. Anal. Appl. **85** (1981), 264 – 269.

[7] **W. A. Dudek**, *Fuzzy subquasigroups*, Quasigroups and Related Systems **5** (1998), 81 – 98.

[8] **W. A. Dudek**, *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[9] **W. A. Dudek and Y. B. Jun**, *Fuzzy subquasigroups over a t-norm*, Quasigroups and Related Systems **6** (1999), 87 – 98.

[10] **M. B. Gorzalczany**, *A method of inference in approximate reasoning based on interval-valued fuzzy sets*, Fuzzy Sets and Systems **21** (1987), 1 – 17.

[11] **M. B. Gorzalczany**, *An Interval-valued fuzzy inference method some basic properties*, Fuzzy Sets and Systems **31** (1989), 243 – 251.

[12] **V. Murali**, *Fuzzy points of equivalent fuzzy subsets.* Information Sciences **158** (2004), 277 – 288.

[13] **P. M. Pu and Y. M. Liu**, *Fuzzy topology,I. Neighborhood structure of a fuzzy point and Moore-Smith convergence*, J. Math. Anal. Appl. **76** (1980), 571 – 599.

[14] **I. G. Rosenberg**, *Two properties of fuzzy subquasigroups of a quasigroup*, Fuzzy Sets and Systems **110** (2000), 447 – 450.

[15] **A. Rosenfeld**, *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[16] **M. K. Roy and R. Biswas**, *l-v fuzzy relations and Sanchez's approach for medical diagnosis*, Fuzzy Sets and Systems **47** (1992), 35 – 38.

[17] **I. B. Turksen**, *Interval valued fuzzy sets based on normal forms*, Fuzzy Sets and Systems **20** (1986), 191 – 210.

[18] **M. S. Ying**, *On standard models of fuzzy modal logics*, Fuzzy Sets and Systems **26** (1988), 357 – 363.

[19] **M. S. Ying**, *A new approach for fuzzy topology (I)*, Fuzzy Sets and Systems **39** (1991), 303 – 321.

[20] **L. A. Zadeh**, *Fuzzy sets*, Information Control. **8** (1965), 338 – 353.

[21] **L. A. Zadeh**, *The concept of a linguistic and int application to approximate reasoning I,* Information Science **8** (1975), 199 – 249.

Received March 30, 2010

M.Akram
Punjab University College of Information Technology, University of the Punjab, Old Campus, P. O. Box 54000, Lahore, Pakistan.
E-mail: m.akram@pucit.edu.pk

W.A.Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology, Wyb. Wyspiańskiego 27, 50-370 Wroclaw, Poland.
E-mail: wieslaw.dudek@pwr.wroc.pl

Quasigroups and Related Systems **18** (2010), 127 – 136

Once more about Brualdi's conjecture

Ivan Deriyenko

Abstract. A new algorithm for finding quasi-complete or complete mappings for Latin squares is presented. This algorithm is a modification of the previous algorithm by this author from 1988.

1. Introduction

In 1988 the author published the paper [3], where he proved the Brualdi's conjecture. In 2005 P. J. Cameron and I. M. Wanless disproved in [1] the author's proof and gave a counter-example. The author agrees with them that his proof presented in [3] is not complete. However, the author does not agree with the counter-example given in [1]. Problems seem to have appeared because the paper was written in Russian, the algorithm was described by the author in a complicated form and it was translated to English without the author's consultancy and not quite correctly (as well as the author's surname which should be Deriyenko, not Derienko). In the present paper the author again describes the algorithm in a simpler form, reveals the groundlessness of the counter-example given in the paper [1]. The way the algorithm works is presented on a concrete example.

The author does not claim that this algorithm gives the final confirmation of the Brualdi's conjecture, but believes that his algorithm gives significant progress in solution to this problem.

2. Preliminaries

$Q(\cdot)$ always denotes a quasigroup, Q – a finite set $\{1, 2, 3, \ldots, n\}$, φ, ψ – permutations of Q, S_Q – the set of all permutations of Q. The composi-

2010 Mathematics Subject Classification: 05B15, 20N05
Keywords: quasigroup, complete mapping, quasicomplete mapping, algorithm, Brualdi's conjecture.

tion of permutations is defined as $\varphi\psi(x) = \varphi(\psi(x))$. Permutations will be written as a composition of cycles; cycles will be separated by dots, e.g.

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 4 & 6 \end{pmatrix} = (132.45.6.)$$

Any permutation φ of Q defines on a quasigroup $Q(\cdot)$ a mapping

$$\overline{\varphi}(x) = x \cdot \varphi(x).$$

By the *range* $rg(\varphi)$ *of a permutation* $\varphi \in S_X$ we mean the number of elements of the set $\overline{\varphi}(X) = \{\overline{\varphi}(x) : x \in X \subseteq Q\}$.

If $|\overline{\varphi}(X)| = |X|$, then we say that φ is a *complete mapping* on the set X. In this case $\overline{\varphi}$ is one-to-one. If $|\overline{\varphi}(X)| < |X|$, then we say that φ is *incomplete* on the set X. In particular, when $|\overline{\varphi}(X)| = |X| - 1$ we say that φ is a *quasicomplete mapping.*

The Brualdi's conjecture (see for example [2])
Every finite quasigroup has a complete or quasicomplete mapping.

In other words, for every finite quasigroup $Q(\cdot)$ there is a permutation φ such that

$$|\overline{\varphi}(Q)| \geqslant |Q| - 1.$$

Some results on the Brualdi's conjecture are known. For example:

- *All groups of odd order have a complete mapping* (see [2]).
- *All symmetric groups* S_n $(n > 3)$ *have a complete mapping* (see [2]).
- *A finite group order* n *which has a cyclic Sylow* 2*-subgroup does not possess a complete mapping* (see [2]).
- *If a quasigroup of order* $4k + 2$ *has a subquasigroup of order* $2k + 1$, *then its multiplication table is without complete mappings* (see [5]).

Some known approximations of the range $t = rg(\varphi)$ of a permutation φ of a quasigroup of order n.

a) $t \geqslant [n - O(\log_2 n)]$, (Sade, 1963, [6])

b) $t \geqslant \left[\frac{2n+1}{3}\right]$ for $n > 7$, (Koksma, 1969, [4])

c) $t \geqslant [n - \sqrt{n}]$, (Woolbrighte, 1978, [9])

d) $t \geqslant \left[n - 5,5(\ln n)^2\right]$. (Shor, 1982, [7])

3. D-algorithm

In this section we describe the algorithm which gives the possibility to find a quasicomplete or complete mapping for a given finite quasigroup. But first we prove some auxiliary results.

Let $Q(\cdot)$ be a quasigroup, $X \subseteq Q$, φ some fixed permutation of Q. By the *block* $B_k = \{X, \varphi\}$ of a quasigroup $Q(\cdot)$, where $k = |X|$, we mean the subtable

$$B_k = X \times \varphi(X)$$

contained in the multiplication table of $Q(\cdot)$. The set X is called a *basis* of the block B_k. Note that the same block can be determined by two different permutations φ and ψ. This situation takes place when $\varphi(X) = \psi(X)$. The block $B_k = \{X, \varphi\}$ is called *complete* if

$$|X| = |\overline{\varphi}(X)|.$$

In this case, $\overline{\varphi}$ is one-to-one. If $|\overline{\varphi}(X)| < |X|$, then the block B_k is called *incomplete*. An incomplete block B_k is called *quasicomplete*, if

$$|\overline{\varphi}(X)| = |X| - 1,$$

and a *lopped block*, if

$$|\overline{\varphi}(X)| = |X| - 2. \tag{1}$$

In such block there exists at least one element $z^* \in \overline{\varphi}(X)$, called a *star-element*, such that

$$|\overline{\varphi}^{\,-1}(z^*)| > 1.$$

The following fact is obvious.

Lemma 3.1. *A lopped block has one or two star-elements.* □

Let Z^* be the set of all star-elements of a lopped block $B = \{X, \varphi\}$ and $\overline{\varphi}^{\,-1}(Z^*) = S$. If a lopped block B has one star-element z^*, then, obviously

$$S = \overline{\varphi}^{\,-1}(z^*) = \{s_1, s_2, s_3\}.$$

If it has two star-elements z_1^* and z_2^*, then we have

$$S' = \overline{\varphi}^{\,-1}(z_1^*) = \{s_1, s_2\}, \qquad S'' = \overline{\varphi}^{\,-1}(z_2^*) = \{s_3, s_4\},$$

$$S' \cup S'' = S, \qquad S' \cap S'' = \emptyset.$$

So, $|S| = r$, where $r \in \{3, 4\}$.

A transposition $\alpha = (s_i, s_j)$ such that $s_i, s_j \in S$ if $|S| = 3$ and $s_i \in S'$, $s_j \in S''$, if $|S| = 4$, is called a *star-transposition.* In the case $|S| = 3$ we have three possibilities to build α, in the case $|S| = 4$ we have four possibilities.

Lemma 3.2. *For a lopped block $B = \{X, \varphi\}$ the following inequality is true:*

$$rg(\varphi\alpha) \geqslant rg(\varphi)$$

Proof. Indeed, since $\varphi\alpha(x) = \varphi(x)$ for $x \in X \setminus S$, we have $\overline{\varphi\alpha}(x) = \overline{\varphi}(x)$ for all $x \in X \setminus S$. Hence $|\overline{\varphi\alpha}(X \setminus S)| = |\overline{\varphi}(X \setminus S)|$. For $s_i, s_j \in S$ elements $\overline{\varphi\alpha}(s_i)$ and $\overline{\varphi\alpha}(s_j)$ may not be in $\overline{\varphi}(X)$. So, $|\overline{\varphi\alpha}(X)| \geqslant |\overline{\varphi}(X)|$. □

Now, let us describe our D-algorithm which gives the possibility to find a quasicomplete or complete mapping.

D-ALGORITHM

Let $Q(\cdot)$ be a fixed quasigroup of order $n \geqslant 3$, $B_k = \{X, \varphi_0\}$ its arbitrary lopped block, $|X| = k$.

STEP 1.

(a) Determine the set S_0 according to $\overline{\varphi}_0$.
Let $S_0 = \{s_{01}, s_{02}, ..., s_{0r}\}$, where $r \in \{3, 4\}$.

(b) Determine all star-transpositions $\alpha_1^{(t)} = (s_{0i}, s_{0j})$, $1 \leqslant t \leqslant r$.

(c) Calculate all r permutations $\varphi_1^{(t)} = \varphi_0\alpha_1^{(t)}$.

(d) If $rg(\varphi_1^{(q)}) > rg(\varphi_0)$ for some $\varphi_1^{(q)}$, $1 \leqslant q \leqslant r$, then the goal has been achieved. If not, i.e.,

$$rg(\varphi_1^{(t)}) = rg(\varphi_0) \tag{2}$$

holds for all $1 \leqslant t \leqslant r$, then we can take one of the star-transpositions, say $\alpha_1 = \alpha_1^{(t_0)}$, calculated in ($b$), put $\varphi_1 = \varphi_0\alpha_1$ and we state in the same block $B_k = \{X, \varphi_1\}$ (with the same set X and $\varphi_1(X) = \varphi_0(X)$), which in view of (2), also will be a lopped block.

STEP $j + 1$.

First we start with $j = 1$.

(a) Determine the set S_j according to $\overline{\varphi}_j$, where φ_j was calculated in the previous step.

(b) Determine all star-transpositions $\alpha_{j+1}^{(t)}$.
One of the transpositions $\alpha_{j+1}^{(t)}$ will coincide with the transposition

$\alpha_j^{(t_0)}$ used in the previous step. Suppose that it is $\alpha_{j+1}^{(r)}$. We exclude it from further consideration because it returns us back to φ_j. So, in the future we will consider only permutations of the form

$$\varphi_{j+1}^{(t)} = \varphi_j \alpha_{j+1}^{(t)},$$

where $t = 1, 2, \ldots, r-1,\ \ r = |S_j|$.

(c) If $rg(\varphi_{j+1}^{(t)}) > rg(\varphi_j)$ for some $\varphi_{j+1}^{(t)}$, then the goal has been achieved. If not, i.e.,

$$rg(\varphi_{j+1}^{(t)}) = rg(\varphi_j) \tag{3}$$

for all $1 \leqslant t \leqslant r-1$, then we can take one of the star-transpositions, say $\alpha_{j+1} = \alpha_{j+1}^{(t_0)}$, calculated in (b), put $\varphi_{j+1} = \varphi_j \alpha_{j+1}$ and we state in the same block $B_k = \{X, \varphi_{j+1}\}$ (with the same set X such that $\varphi_{j+1}(X) = \varphi_j(X)$), which in view of (3), also will be a lopped block.

Next we go back to the beginning of the STEP $j+1$ replacing j by $j+1$, i.e., we go back to (a) taking φ_{j+1} instead of φ_j and so on, until we find a permutation $\varphi_m = \varphi_0 \alpha_1 \alpha_2 \ldots \alpha_m$ such that

$$rg(\varphi_m) > rg(\varphi_{m-1}). \tag{4}$$

Now, we can go to the block of higher order.

Inequality (4) admits of two possibilities:

$$rg(\varphi_m) - rg(\varphi_{m-1}) = 2,$$
$$rg(\varphi_m) - rg(\varphi_{m-1}) = 1.$$

In the first case we can add to the set $X = \{x_1, \ldots, x_k\}$ two new elements $x_{k+1}, x_{k+2} \in Q \setminus X$. In this way we obtain the set

$$X_1 = X \cup \{x_{k+1}, x_{k+2}\}.$$

In the second case we add only one element.

This set together with φ_m gives a new lopped block $B' = \{X_1, \varphi_m\}$. We mark it as $B_k = \{X, \varphi_0\}$ and repeat the above algorithm for this block starting from the STEP 1.

After several repetitions, the algorithm stops. The goal will be achieved.

4. Comments

This D-algorithm is not identical with our old algorithm described in [3]. These algorithms have common principles, but they are significantly different. In our old algorithm, each step, starting from the second is uniquely determined. Only in the first step, we have several possibilities to select the initial transposition α_1. In our D-algorithm on each step we have two or three possibilities to select the star-transposition α_j.

In [1] is given the counter-example to the work of our old algorithm. This counter-example shows that our old algorithm can cause a return to the beginning of the procedure. The author agrees with this counter-example, but he do not think that it is a "fatal error" (see [8]) because in each return to the beginning, we can choose a new value of α_1 and repeat the whole procedure. Then we get different results. This algorithm can be repeated in such a way six or eight times.

Our new D-algorithm gives even more possibilities. In this algorithm, in every step the transposition α_j can be chosen in two or three ways. This algorithm can be returned to the start many times and after that we can many times change the way of it works.

The author tested this algorithm on many examples and in each case he received a positive solution. He received a positive solution also in the case of quasigroups of large orders.

The author understands that it is not a complete proof of the Brualdi's conjecture, but if we can show that this D-algorithm gives the possibility to "look" $(k-2)^2+1$ cells from among k^2 cells of a block B_k, then it will be the proof of the Brualdi's conjecture or at least proof that our this algorithm always leads to the goal.

5. Counter-example

The counter-example to our old algorithm was given in [1]. This counter-example is built on "the partial Latin square of order 15". We complete this Latin square and present it below. Elements calculated in [1] are marked here.

$$
\left|\begin{array}{ccccccccccccccc}
\boxed{10} & 1 & 3 & 9 & 6 & 7 & 14 & 2 & 15 & 5 & 8 & 11 & 12 & 4 & 13 \\
1 & \boxed{15} & 2 & \boxed{14} & 3 & \boxed{12} & 7 & 4 & 6 & 9 & 10 & 8 & 11 & 13 & 5 \\
2 & \boxed{13} & \boxed{14} & 4 & 7 & 6 & 5 & 10 & 1 & 11 & 15 & 3 & 8 & 9 & 3 \\
3 & 4 & 1 & \boxed{13} & \boxed{14} & \boxed{15} & 6 & 5 & 8 & 2 & 9 & 12 & 7 & 10 & 11 \\
4 & 6 & \boxed{11} & 1 & \boxed{12} & 8 & \boxed{15} & 7 & 13 & 10 & 5 & 9 & 2 & 14 & 3 \\
5 & 3 & \boxed{12} & \boxed{15} & 4 & \boxed{11} & \boxed{13} & 6 & 9 & 1 & 2 & 14 & 10 & 8 & 7 \\
6 & 5 & 4 & 7 & 9 & 3 & \boxed{2} & \boxed{11} & 10 & 8 & 1 & 13 & 14 & 12 & 15 \\
8 & \boxed{11} & \boxed{13} & \boxed{10} & \boxed{15} & \boxed{14} & \boxed{12} & \boxed{1} & \boxed{4} & \boxed{6} & \boxed{7} & \boxed{2} & \boxed{5} & \boxed{3} & 9 \\
7 & 9 & 8 & 5 & 1 & 4 & 10 & \boxed{3} & \boxed{2} & 12 & 14 & 15 & 13 & 11 & 6 \\
9 & 10 & 15 & 11 & 2 & 1 & 8 & 13 & \boxed{5} & \boxed{3} & 12 & \boxed{7} & \boxed{4} & 6 & 14 \\
11 & 14 & 6 & 12 & 5 & 2 & 1 & 9 & \boxed{7} & 13 & \boxed{4} & 10 & \boxed{3} & 15 & 8 \\
12 & 8 & 9 & 2 & 13 & 10 & 3 & 14 & 11 & \boxed{7} & \boxed{6} & \boxed{5} & 15 & 1 & 4 \\
13 & 7 & 10 & 3 & 8 & 9 & 4 & 12 & 14 & 15 & 11 & 1 & \boxed{6} & \boxed{5} & 2 \\
14 & 2 & 5 & 8 & 11 & 13 & 9 & 15 & 12 & \boxed{4} & 3 & \boxed{6} & 1 & \boxed{7} & 10 \\
15 & 12 & 7 & 6 & 10 & 5 & 11 & 8 & 3 & 14 & 13 & 4 & 9 & 2 & \boxed{1}
\end{array}\right|
$$

Let us analyze the work of the algorithm using this counter-example.

STEP 1.

We start with the identity permutation $\varphi_0 = \varepsilon$. In this case

$$
\overline{\varphi}_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2^* & 1^* & 2^* & 3 & 4 & 5 & 6 & 7 & 1^* \end{pmatrix},
$$

$Z_0^* = \{1^*, 2^*\}$, $\overline{\varphi}_0^{-1}(1^*) = \{8, 15\} = S_0'$, $\overline{\varphi}_0^{-1}(2^*) = \{7, 9\} = S_0''$. Thus $rg(\varphi_0) = 13$.

Since $S = S' \cup S'' = \{7, 8, 9, 15\}$, we can choose x_0 in four ways. For each selected x_0 we have two possibilities to build a star-transposition α. Hence, we have eight ways to do the first step.

We we select $x_0 = 8$. This element will be fixed for this block in whole our procedure. In the next block another element will be selected and fixed.

For $x_0 = 8$ we have two star-transpositions:

$$\alpha_1^{(1)} = (8, 15) \quad \text{and} \quad \alpha_1^{(2)} = (8, 9).$$

Let us choose the second transposition $\alpha_1 = (8, 9)$. Then

$$\varphi_1 = \varphi_0 \alpha_1 = \varepsilon \alpha_1 = (8, 9).$$

Step 2.

Now we have

$$\overline{\varphi}_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 4^* & 3^* & 3^* & 4^* & 5 & 6 & 7 & 1 \end{pmatrix},$$

$Z_1^* = \{3^*, 4^*\}$, $\overline{\varphi}_1^{-1}(3^*) = \{9, 10\} = S_1'$, $\overline{\varphi}_1^{-1}(4^*) = \{8, 1\} = S_1''$ which means that $rg(\varphi_1) = 13$.

Since $x_0 = 8 \in S_1''$, the second element of a star-transposition α_2 should be in S_1'. From the fact that $\alpha_2 \neq \alpha_1$, we obtain

$$\alpha_2 = (8, 10).$$

Hence $\varphi_2 = \varphi_1\alpha_2 = (8,9)(8,10) = (8\ 10\ 9.)$.

Step 3.

$$\overline{\varphi}_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 6^* & 3 & 5^* & 4 & 5^* & 6^* & 7 & 1 \end{pmatrix},$$

$Z_2^* = \{5^*, 6^*\}$, $\overline{\varphi}_2^{-1}(5^*) = \{10, 12\} = S_2'$, $\overline{\varphi}_2^{-1}(6^*) = \{8, 13\} = S_2''$. Thus $rg(\varphi_2) = 13$.

Then $\alpha_3 = (8, 12)$ and $\varphi_3 = \varphi_2\alpha_3 = (8\ 12\ 10\ 9.)$.

Step 4.

$$\overline{\varphi}_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2^* & 2^* & 3 & 5 & 4 & 7^* & 6 & 7^* & 1 \end{pmatrix},$$

$Z_3^* = \{2^*, 7^*\}$, $\overline{\varphi}_3^{-1}(2^*) = \{7, 8\} = S_3'$, $\overline{\varphi}_3^{-1}(7^*) = \{12, 14\} = S_3''$. Hence $rg(\varphi_3) = 13$.

Then $\alpha_4 = (8, 14)$ and $\varphi_4 = \varphi_3\alpha_4 = (8\ 14\ 12\ 10\ 9.)$ and so on.

Continuing this procedure we obtain $\varphi_{48} = \varphi_0$, which means that we return to the start. After that we have seven possibilities to choose α_1. Now we again take $\alpha_1 = (8, 9)$, but in this case we select $x_0 = 9$ as a fixed element.

New step 1.

$\varphi_1 = \varphi_0\alpha_1 = \varepsilon\alpha_1 = (8, 9)$,

$$\overline{\varphi}_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14 & 13 & 12 & 11 & 2 & 4^* & 3^* & 3^* & 4^* & 5 & 6 & 7 & 1 \end{pmatrix},$$

$Z_1^* = \{3^*, 4^*\}$, $\overline{\varphi}_1^{-1}(3^*) = \{9, 10\} = S_1'$, $\overline{\varphi}_1^{-1}(4^*) = \{8, 11\} = S_1''$. Thus $rg(\varphi_1) = 13$.

Then $\alpha_2 = (9, 11)$ and $\varphi_2 = \varphi_1\alpha_2 = (8\ 9\ 11.)$.

New step 2.

$$\overline{\varphi}_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 10 & 15 & 14^* & 13 & 12 & 11 & 2 & 4 & 14^* & 3 & 9 & 5 & 6 & 7 & 1 \end{pmatrix},$$

$rg(\varphi_2) = 14$.

The goal has been achieved. $\overline{\varphi}_2$ is a quasicomplete mapping.

Remark 5.1. Note that in our old algorithm every step, beginning from the second one, was uniquely determined. In our new algorithm at each stage we have two or three possibilities to perform the next step. Number of possibilities depends on the number of elements of the set S.

Acknowledgments. The author highly values attention paid by Ian Wanless and Peter Cameron to the paper [3] and appreciates the efforts to study this paper written in Russian. The author looks forward to further fruitful cooperation.

Special thanks are due to Wieslaw A. Dudek for helping us writing the final version of the D-algorithm.

Added after publication (February 24, 2011). The citation [6] on page 128 is incorrect. The approximation $t \geqslant [n - O(\log_2 n)]$ was obtained by P. Hatami and P. W. Shor in the article *A lower bound for the length of a partial transversal in Latin square*, J. Comb. Theory, Ser. A, **115** (2008), 1103 – 1113.

References

[1] **P. J. Cameron and I. M. Wanless**, *Covering radius for sets of permutations*, Discrete Math. **293** (2005), 91 – 109.

[2] **J. Dénes and A. D. Keedwell**, *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[3] **I. I. Deriyenko**, *On the Brualdi hypothesis*, (Russian), Mat. Issled. **102** (1988), 53 – 65.

[4] **K. K. Koksma**, *A lower bound for the order of a partial transversal in a Latin square*, J. Comb. Theory **7** (1969), 94 – 95.

[5] **H. B. Mann**, *The construction of orthogonal Latin squares*, Ann. Math. Stat. **13** (1942), 418 – 423.

[6] **A. Sade**, *Isotopies d'un groupoide avec son conjont*, Rend. Circ. Mat. Palermo, II Ser. **12** (1963), 357 – 381.

[7] **P. W. Shor**, *A lower bound for the length of a partial transversal in a Latin square*, J. Comb. Theory, Ser A **33** (1982), 1 – 8.

[8] **I. M. Wanless**, *Transversals in Latin squares*, Quasigroups and Related Systems **15** (2007), 169 – 190.

[9] **D. E. Woolbright**, *An $n \times n$ Latin square has a transversal with at least $n - \sqrt{n}$ distinct symbols*, J. Comb. Theory **24** (1978), 235 – 237.

Received November 30, 2010

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

Quasigroups and Related Systems **18** (2010), 137 – 142

Intersection graphs of normal subgroups of groups

Sayyed Heidar Jafari and *Nader Jafari Rad*

Abstract. We give characterizations of groups whose intersection graphs of normal subgroups are connected, complete, forests, or bipartite.

1. Introduction

Let $F = \{S_i : i \in I\}$ be an arbitrary family of sets. The *intersection graph* $G(F)$ of F is the graph whose vertices are S_i, $i \in I$ and in which the vertices S_i and S_j $(i, j \in I)$ are adjacent if and only if $S_i \neq S_j$ and $S_i \cap S_j \neq \emptyset$. It is known that every simple graph is an intersection graph, ([4]).

It is interesting to study the intersection graphs $G(F)$ when the members of F have an algebraic structure. Bosak [1] in 1964 studied graphs of semigroups. Then Csákány and Pollák [2] in 1969 studied the graphs of subgroups of a finite group. Zelinka [6] in 1975 continued the work on intersection graphs of nontrivial subgroups of finite abelian groups.

Recall that a subgroup H of a group G is *normal* if $g^{-1}Hg = H$ for every $g \in G$.

In this paper, we consider the intersection graph of normal subgroups of a group. For a group G, the *intersection graph of normal subgroups of* G, denoted by $\Gamma(G)$, is the graph whose vertices are in a one-to-one correspondence with proper nontrivial normal subgroups of G and two distinct vertices are adjacent if and only if the corresponding normal subgroups of G have a nontrivial (nonzero) intersection. Clearly $\Gamma(G)$ does not exist if and only if G is simple. Note that the intersection graph of a simple group G is not defined, since a graph can not have an empty vertex set.

The graph theory and group theory notation terminology follow from [5] and [3], respectively.

Throughout the paper, to simplify, for a normal subgroup N in a group

2010 Mathematics Subject Classification: 20A05, 20D15, 20E07, 05C75
Keywords: Normal subgroup, simple, nilpotent, decomposable, intersection graph, connected graph, complete graph, bipartite graph.

G we use "the vertex N" instead of "the vertex in $\Gamma(G)$ corresponded to N". Also we use 0 as the trivial subgroup.

2. Connected and complete graphs

In this section we characterize all groups whose intersection graphs are connected or complete. We first some graph theory and group theory definitions. A graph G is *complete* if there is an edge between every pair of the vertices. We denote the complete graph on n vertices by K_n. A *path* of length n in a graph G is an ordered list of distinct vertices $v_0, v_1, \ldots, v_n$ such that v_i is adjacent to v_{i+1} for $i = 1, 2, \ldots, n-1$. We denote by $v_0 - v_1 - \ldots - v_n$ to such a path. A (u, v)-path is a path with endpoints u and v. For vertices x and y of G, let $d(x, y)$ be the length (the number of edges) of a shortest path from x to y ($d(x, x) = 0$, and $d(x, y) = \infty$ if there is no path between x and y). A graph G is *connected* if it has a (u, v)-path for each pair $u, v \in V(G)$.

Recall that a *chain* $0 = G_0 \subset G_1 \subset \ldots \subset G_n = G$ of subgroup of a group G is a *composition seriers* if $G_i \trianglelefteq G_{i+1}$ and $\frac{G_{i+1}}{G_i}$ is simple for $i = 0, 1, \ldots, n$. The *length* of the chain is n. If G has a composition series, then any two compositione series of G have the same length, denoted by $lc(G)$.

Lemma 2.1. *Let $G = A_1 \times A_2$. If $N_i \trianglelefteq A_i$ for $i = 1, 2$, then $N_1 \times N_2 \trianglelefteq G$.*

The *complement* $\overline{G}$ of G is the graph with vertex set $V(\overline{G}) = V(G)$, and $E(\overline{G}) = \{uv : uv \notin E(G)\}$. The complement of a complete graph is the *null graph*.

Lemma 2.2. *Let $G = N_1 \times N_2$, where N_1, N_2 are simple. Then $\Gamma(G)$ is null.*

Proof. Since N_1 and N_2 are simple, then $lc(G) = 2$. Then any normal nontrivial proper subgroup of G is both maximal and minimal. This completes the proof. $\square$

Recall that a group G is a *direct sum* of two normal subgroups N_1 and N_2 if $N_1 \cap N_2 = 0$ and $N_1 N_2 = G$, where $N_1 N_2 = \{xy : x \in N_1, y \in N_2\}$.

Theorem 2.3. *Let G be a group. Then $\Gamma(G)$ is disconnected if and only if $G = N_1 \oplus N_2$, where N_1 and N_2 are simple normal subgroups of G.*

Proof. Let $\Gamma(G)$ be disconnected. Then $\Gamma(G)$ has at least two components. Let N_1 and N_2 be two normal subgroups of G and the corresponding vertices included in two different components of $\Gamma(G)$. Thus, $N_1 \cap N_2 = 0$. Since $N_1 \cup N_2 \subseteq N_1N_2$, we obtain $N_1N_2 = G$. We conclude that $G = N_1 \oplus N_2$. Now we show that N_1 and N_2 are simple. If N_1 is not simple, then N_1 has a proper nontrivial subgroup N. Then by Lemma 2.1, $N \trianglelefteq G$. Now NN_2 is adjacent to both N_1 and N_2, a contradiction. Thus N_1 is simple. Similarly, N_2 is simple.

The converse follows from Lemma 2.2. □

The *center* $Z(G)$ of a group G is the set of all elements x which $xy = yx$ for every $y \in G$. A chain $G_0 = 0 \subseteq G_2 \subseteq \ldots \subseteq G_t = G$ is a *central series* of G if $\frac{G_i}{G_{i-1}} \subseteq Z(\frac{G}{G_{i-1}})$ for $i = 1, 2, \ldots, t$. A group G is *nilpotent* if G has a *central series*.

Corollary 2.4. *If G is nilpotent, then $\Gamma(G)$ is disconnected if and only if $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$, where p, q are two non necessarily distinct primes.*

Proof. Notice that any nilpotent simple group is in the form $\mathbb{Z}_p$, where p is a prime. □

The next theorem provides a characterization for all groups whose intersection graphs are complete.

Note that a group G satisfies the minimal condition on normal subgroups if any non-empty subset of normal subgroups of G contains a minimal element.

Theorem 2.5. *Let G be a non-simple group that satisfies the minimal condition on normal subgroups. Then $\Gamma(G)$ is complete if and only if G has a unique minimal normal subgroup.*

Proof. Let G be a non-simple group and G satisfies the minimal condition on normal subgroups. Let $\Gamma(G)$ be complete. Then G has at least one minimal normal subgroup. Let N be a minimal normal subgroup of G. If N_1 is a minimal normal subgroup different from N, then $N \cap N_1 = 0$, since $0 \leq N \cap N_1 \subsetneqq N$ and $N \cap N_1 \trianglelefteq G$. This implies N_1 and N are not adjacent in $\Gamma(G)$. This is a contradiction, since $\Gamma(G)$ is complete. We deduce that N is the unique minimal normal subgroup of G.

Conversely, suppose that G has a unique minimal normal subgroup say N. Let K and L be two nontrivial normal subgroups of G. Since G satisfies the minimal condition on normal subgroups, K and L each contain a minimal normal subgroup. By assumption $N \subseteq K \cap L$, and so $K \cap L \neq 0$. Thus the vertices K and L are adjacent in $\Gamma(G)$. This means that $\Gamma(G)$ is complete. $\square$

Corollary 2.6. *For $n > 1$, $\Gamma(\mathbb{Z}_{p^n})$ is K_{n-1}.* $\square$

Example 2.7. The intersection graph of the generalized quaternion group Q_n, (of order $4n$) is complete. Note that Q_n has a unique minimal normal subgroup of order 2.

Example 2.8. For any prime p, the intersection graph of $\mathbb{Z}_{p^\infty} = \{\frac{m}{n} + \mathbb{Z} : m, n \in \mathbb{Z}, n = p^t \text{ for some } t \in \mathbb{N} \cup \{0\}\}$ is an infinite complete graph. To see this notice that all proper nontrivial normal subgroups of $\mathbb{Z}_{p^\infty}$ are in the form $\langle \frac{1}{p^i} + \mathbb{Z} \rangle$, where $i \geqslant 1$. However, the only minimal normal subgroup of $\mathbb{Z}_{p^\infty}$ is $\langle \frac{1}{p} + \mathbb{Z} \rangle$.

Corollary 2.9. *For a finite nilpotent group G, $\Gamma(G)$ is complete if and only if G is a p-group and $Z(G)$ is cyclic.*

Proof. Note that any subgroup of $Z(G)$ of prime order is a minimal normal subgroup of G, and a prime p is a prime factor of $|G|$ if and only if p is a prime factor of $Z(G)$. $\square$

Example 2.10. If n is a power of 2, then the intersection graph of the dihedral group D_n is complete. Notice that D_n is a 2-group and the center of this group is of order 2.

3. Forests and bipartite graphs

In this section we characterize all groups whose intersection graphs are forests or bipartite. We recall that a graph G is called *bipartite* if its vertex set can be partitioned into two independent subsets X and Y such that every edge of G has one endpoint in X and other endpoint in Y. We denote by C_n the *cycle* with vertex set $\{v_0, v_1, \ldots, v_n\}$ and edge set $\{v_i v_{i+1} : i = 1, 2, \ldots, n-1\} \cup \{v_1 v_n\}$.

Lemma 3.1. *Let $G = N_1 \times N_2$, where N_1, N_2 are normal subgroups of G. Then $\Gamma(G)$ has a cycle C_3 if and only if N_1 or N_2 is not simple.*

Proof. ($\Longrightarrow$) follows by Lemma 2.2.
($\Longleftarrow$) Assume that N_1 is not simple. Let N be a nontrivial proper normal subgroup of N_1. Then $N \times N_2 - N \times 0 - N_1 \times 0 - N \times N_2$ is a cycle on three vertices. $\square$

Lemma 3.2. *If G is an indecomposable group of length 2, then $\Gamma(G)$ is K_1.*

Proof. Since $lc(G) = 2$, G has at least one proper nontrivial normal subgroup. By assumption any proper nontrivial normal subgroup of G is both minimal and maximal. We show that G has exactly one proper nontrivial normal subgroup. Suppose to the contrary that N_1, N_2 are two distinct proper nontrivial normal subgroups of G. Then $N_1 \cap N_2 = 0$, and $G \cong N_1 N_2$, a contradiction. $\square$

A group G is indecomposable if it is not isomorphic to direct product of two nontrivial groups.

Lemma 3.3. *Let G be an indecomposable group with $lc(G) = 3$. If G has a unique maximal normal subgroup, then $\Gamma(G)$ is a forest.*

Proof. By assumption any normal subgroup of G is either minimal or maximal. Let N be the unique maximal normal subgroup of G. If there are two distinct normal subgroups K_1, K_2 of G different from N, then K_1 and K_2 are minimal, and so $K_1 \cap K_2 = 0$. This completes the proof. $\square$

We are now ready to characterize all groups whose intersection graphs are forest.

Theorem 3.4. *The intersection graph of a group G is a forest if and only if one of the following holds:*

- (i) $lc(G) = 2$,
- (ii) $lc(G) = 3$, *and G is an indecomposable group with a unique maximal normal subgroup,*
- (iii) $G \cong M_1 \times M_2$, *where M_1, M_2 are simple groups.*

Proof. ($\Leftarrow$) follows from Lemmas 3.3, 3.2, and 3.1.
($\Rightarrow$): Let $\Gamma(G)$ be a forest. We first show that G is a direct product of at most two groups. Let $G = M_1 \times M_2 \times \ldots \times M_k$, where M_i is a group for $i = 1, 2, \ldots, k$. If $k \geqslant 3$, then $H = M_2 \times M_3 \times \ldots \times M_k$ has at least one normal proper nontrivial subgroup $M_2 \times 0 \times \ldots \times 0$, and by Lemma 3.1 $\Gamma(G)$ contains a cycle. This contradiction implies that $k \leqslant 2$. If $k = 2$,

then Lemma 3.1 implies (iii). Thus we may assume that $k = 1$. So G is indecomposable.

We show that $lc(G) \leqslant 3$. Suppose the contrary that $lc(G) \geqslant 4$. There are three proper nontrivial normal subgroups N_1, N_2, N_3 such that $N_1 \subset N_2 \subset N_3$. Then N_1, N_2 and N_3 form a cycle, a contradiction. So $lc(G) \leqslant 3$. If $lc(G) = 2$, then (i) holds. So we suppose that $lc(G) = 3$. We prove that G has a unique normal maximal subgroup. Since $lc(G) < \infty$, G has a maximal normal subgroup N. If N_1 is another maximal normal subgroup of G, then $NN_1 = G$. Since G is indecomposable, $N \cap N_1 \neq 0$. Then $N - N \cap N_1 - N_1 - N$ forms a cycle in $\Gamma(G)$. This contradiction implies that N is the unique maximal normal subgroup of G. $\square$

Next we characterize all groups whose intersection graphs are bipartite. In view of the proof of Theorem 3.4 any produced cycle has three vertices. Also it is known that a graph G is bipartite if and only if any cycle of G has even number of vertices. These lead to the following.

Corollary 3.5. *The intersection graph $\Gamma(G)$ of a group G is bipartite if and only if $\Gamma(G)$ is a forest.*

References

[1] **J. Bosak**, *The graphs of semigroups*, in: Theory of graphs and applications, Academic Press, New York, 1964, 119 – 125.

[2] **B. Csákány and G. Pollák**, *The graph of subgroups of a finite group*, Czechoslovak Math. J. **19** (1969), 241 – 247.

[3] **W. R. Scott**, *Group theory*, Prentice-Hall, 1964.

[4] **E. Szpilrajn-Marczewski**, *Sur deux propriétés des classes d'ensembles*, Fund. Math. **33** (1945), 303 – 307.

[5] **D. B. West**, *Introduction to graph theory*, Prentice-Hall of India Pvt. Ltd, 2003.

[6] **B. Zelinka**, *Intersection graphs of finite abelian groups*, Czechoslovak Math. J. **25** (1975), 171 – 174.

Received May 18, 2010

Department of Mathematics, Shahrood University of Technology Shahrood, Iran
E-mails: shjafari55@gmail.com (S.H.Jafari), n.jafarirad@shahroodut.ac.ir (N.J.Rad)

Quasigroups and Related Systems **18** (2010), 143 – 148

Decompositions of an Abel-Grassmann's groupoid

Madad Khan

Abstract. In this paper we have decomposed AG-groupoids. We have proved that if S is an AG*-groupoid, then S/ρ is isomorphic to S/σ, for $n, m \geqslant 2$, where ρ and σ are congruence relations. Further it has shown that S/η is a separative semilattice homomorphic image of an AG-groupoid S with left identity, where η is a congruence relation.

1. Introduction

An *Abel-Grassmann's groupoid* [5], abbreviated as an *AG-groupoid*, is a groupoid S whose elements satisfy the invertive law:

$$(ab)c = (cb)a, \qquad \text{for all } a, b, c \in S. \tag{1}$$

It is also called a *left almost semigroup* [3, 4]. In [1], the same structure is called a *left invertive groupoid*. It is a useful non-associative algebraic structure, midway between a groupoid and a commutative semigroup, with wide applications in the theory of flocks.

An AG-groupoid S is *medial* [3], that is,

$$(ab)(cd) = (ac)(bd), \qquad \text{for all } a, b, c, d, \in S. \tag{2}$$

If an AG-groupoid satisfies the following property, then it is called an *AG^*-groupoid* [5].

$$(ab)c = b(ca), \qquad \text{for all } a, b, c \in S. \tag{3}$$

Then also

$$(ab)c = b(ac), \qquad \text{for all } a, b, c \in S. \tag{4}$$

It is easy to see that the conditions (3) and (4) are equivalent. In an AG*-groupoid S holds all permutation identities of a next type [6],

2010 Mathematics Subject Classification: 20M10, 20N99

Keywords: AG-groupoid, left invertive law, medial law, congruence.

$$(x_1x_2)(x_3x_4) = (x_{\pi(1)}x_{\pi(2)})(x_{\pi(3)}x_{\pi(4)}), \tag{5}$$

where $\{\pi(1), \pi(2), \pi(3), \pi(4)\}$ means any permutation of the set $\{1, 2, 3, 4\}$. It means that if $S = S^2$, then S becomes a commutative semigroup. Many characteristics of a non-associative AG*-groupoid are similar to a commutative semigroup.

As a consequence of (5), we would have $(x_1x_2x_3)^m = (x_{p(1)}x_{p(2)}x_{p(3)})^m$, where $\{p(1), p(2), p(3)\}$ means any permutation of the set $\{1, 2, 3\}$ and $m \geqslant 2$. The result can be generalized for finite numbers of elements of S.

2. The smallest separative congruences

In an AG*-groupoid S, $(ab)c = b(ac)$ holds for all $a, b, c \in S$. This leads us to $(aa)a = a(aa)$ which implies that $a^2a = aa^2$. Hence it is easy to note that $a^{n+1}a = aa^{n+1}$, $a^ma^n = a^{m+n}$, $(a^m)^n = a^{mn}$, $(ab)^n = a^nb^n$, for all a, b and positive integers m and n.

We define a relation ρ on an AG-groupoid S as follows: $a\rho b$ if and only if there exists a positive integer n such that $ab^n = b^{n+1}$ and $ba^n = a^{n+1}$.

We define a relation σ on an AG-groupoid S as follows: $a\sigma b$ if and only if there exists a positive integer n such that $a^nb = a^{n+1}$ and $b^na = b^{n+1}$.

A relation ρ on an AG-groupoid S is called separative if $ab\rho a^2$ and $ab\rho b^2$ imply that $a\rho b$.

The following lemma has been proved in [6].

Lemma 1. *Let $\acute{\sigma}$ be a separative congruence on an AG*-groupoid S, then for all a, $b \in S$ it follows that $ab\acute{\sigma}ba$.*

In the following two lemmas we have proved that the relations ρ and σ are commutative without using separativity.

Lemma 2. *If S is an AG*-groupoid, then $ab\rho ba$ for all a, b in S.*

Proof. By using (5) and (2), we have, $(ab)(ba)^m = (ab)(b^ma^m) = (ab)(a^mb^m)$ $= (aa^m)(bb^m) = (bb^m)(aa^m) = b^{m+1}a^{m+1} = (ba)^{m+1}$. Similarly $(ba)(ab)^m =$ $(ab)^{m+1}$. Hence $ab\rho ba$. □

Lemma 3. *If S is an AG*-groupoid, then $ab\sigma ba$ for all a, b in S.*

Proof. By using (5), we have, $(ba)^n(ab) = (b^na^n)(ab) = (b^nb)(a^na) =$ $b^{n+1}a^{n+1} = (ba)^{n+1}$. Similarly $(ab)^n(ba) = (ab)^{n+1}$. Hence $ab\sigma ba$. □

The proofs of the following theorems are available in [6] and [5].

Theorem 1. *S/ρ is a maximal separative commutative image of an AG^*-groupoid S.*

Theorem 2. *S/σ is a maximal separative commutative image of an AG^*-groupoid S.*

Lemma 4. *ρ is equivalent to σ for $m, n \geqslant 2$, on an AG^*-groupoid S.*

Proof. Let $a\rho b$, then there exists a positive integer n such that $ab^n = b^{n+1}$ and $ba^n = a^{n+1}$. Now multiply b on both sides of $ab^n = b^{n+1}$, then using (1), we get $b^{n+1}b = (ab^n)b = b^{n+1}a$.

Similarly $ba^n = a^{n+1}$ implies that $a^{n+1}b = a^{n+2}$. Hence $a\sigma b$.

Conversely, assume that $a\sigma b$, then there exists a positive integer m such that $b^m a = b^{m+1}$ and $a^m b = a^{m+1}$. Assume that $m \geqslant 2$. Now multiply b on both sides of $b^m a = b^{m+1}$, then, using (3) and (5), we get

$$bb^{m+1} = b(b^m a) = (ab)b^m = (ab)(b^{m-1}b) = (ba)(b^{m-1}b) = a(b^m b) = ab^{m+1}.$$

Similarly $a^m b = a^{m+1}$ implies that $ba^{m+1} = a^{m+2}$. Hence $a\rho b$. □

Theorem 3. *If S is an AG^*-groupoid, then S/ρ is isomorphic to S/σ, for $m, n \geqslant 2$.*

Proof. It follows from Lemma 4. □

Remark 1. *S/ρ is not isomorphic to S/σ for $n = m = 1$.*

If S is an AG-groupoid then $(ab)c = a(bc)$, is not generally true for all $a, b, c \in S$, that is $(Sx)S \neq S(xS)$, for some x in S.

The relations γ and δ be defined in S as follows:

$a\gamma b$ if and only if there exists a positive integer n such that $b^n \in S(aS)$ and $a^n \in S(bS)$ for all a and b in S

$a\delta b$ if and only if there exists a positive integer m such that $b^m \in (Sa)S$ and $a^m \in (Sb)S$ for all a and b in S.

Lemma 5. *δ is equivalent to γ on an AG^*-groupoid S.*

Proof. Let $a^n \in S(bS)$, then using (3) and (1), we get

$$\begin{aligned} a^{n+2} &\in (S(bS))a^2 = ((bS)S)a^2 = (a((bS)S))a = (a(S^2b))a \\ &= ((S^2a)b)a \subseteq (Sb)S. \end{aligned}$$

Similarly $b^n \in S(aS)$ implies that $b^{n+2} \in (Sa)S$.

Conversely, assume that $a^n \in (Sb)S$, using (1) and (5), we get,

$$a^{n+1} \in ((Sb)S)a = (aS)(Sb) = (aS)(bS) \subseteq S(bS).$$

Similarly $b^n \in (Sa)S$ implies that $b^{n+1} \in S(aS)$. □

3. The semilattice decomposition

In an AG-groupoid S with left identity we have,

$$a(bc) = b(ac), \quad \text{for all } a, b, c \in S. \tag{6}$$

The following law holds for an AG-groupoid with left identity,

$$(ab)(cd) = (dc)(ba), \quad \text{for all } a, b, c, d \in S. \tag{7}$$

Also it is easy to see that if an AG-groupoid S contains left identity e, then $SS = S$ and $Se = S = eS$.

In [2] the power of elements in an AG-groupoid has been defined as follows: $a^m = (...(((aa)a)a)...)a$, ($m$-times).

Here we begin with an example of an AG-groupoid.

Example 1. Let $S = \{1, 2, 3, 4\}$ and the binary operation "$\cdot$" be defined on S as follows:

$\cdot$	1	2	3	4
1	3	4	1	2
2	2	3	4	1
3	1	2	3	4
4	4	1	2	3

Then clearly $(S, \cdot)$ is an AG-groupoid with left identity 3. □

From now, by S, we shall mean an AG-groupoid with left identity e.

The following Lemma 6 and Theorems $4 - 8$ are available in [2].

Lemma 6. *If $a \in S$, then for every positive integer m,*

(*i*) $a^m = a^{m-1}a = a^{m-3}a^3 = a^{m-5}a^5 = a^{m-7}a^7 = ...,$
(*ii*) $a^m = a^2a^{m-2} = a^4a^{m-4} = a^6a^{m-6} = ...$

Theorem 4. *If $a \in S$, then $a^m a^{2n-1} = a^{m+2n-1}$, for all positive integers m and n.*

Theorem 5. *If $a \in S$, then $a^{2n}a^m = a^{2n+m}$, for all positive integers m and n.*

Theorem 6. *If $a \in S$, then $a^{2n} = a^{2n}e$, for every positive integer n.*

Theorem 7. *If $a \in S$, then $(a^m)^n = a^{mn}$, for all positive integers m and n.*

Theorem 8. *If each $a \in S$, then $(ab)^n = a^n b^n$, for every positive integer n.*

Define a relation η on S as follows: $x\eta y$ if and only if there exists n such that $(xa)^n \in (ya)S$ and $(ya)^n \in (xa)S$.

Lemma 7. *If $a, b \in S$, then $a^2b^2 = b^2a^2$.*

Theorem 9. *η is a semilattice congruence on S.*

Proof. It is reflexive and symmetric. For transitivity let us suppose that $x\eta y$ and $y\eta z$, then there exist positive integers m, n such that $(xa)^n \in (ya)S$, $(ya)^n \in (xa)S$ and $(ya)^m \in (za)S$, $(za)^m \in (ya)S$. More specifically, there exist t_1, $t_2 \in S$, such that $(xa)^n = (ya)t_1$ and $(za)^m = (ya)t_2$. Now using Theorems 7, 8, (1) and (6), we have,

$$\begin{aligned}(xa)^{2mn} &= ((xa)^n)^{2m} = ((ya)t_1)^{2m} = ((ya)^m)^2 t_1^{2m} \in ((za)S)^2S, \quad \text{but}\\ ((za)S)^2S &= ((za)S)(za)S))S = (S((za)S))((za)S)\\ &= (za)(S((za)S))S) = (za)S.\end{aligned}$$

Therefore $(xa)^{2mn} \in (za)S$. Similarly $(za)^{2mn} \in (xa)S$. Hence η is transitive.

To show compatibility, let $x\eta y$ then there exists a positive integer m such that $(xa)^m \in (ya)S$ and $(ya)^m \in (xa)S$. Hence there exists t_3 and t_4 such that $(xa)^m = (ya)t_3$ and $(ya)^m = (xa)t_4$. Now using Theorem 8, Lemma 7, (2), (7) and (6), we get

$$\begin{aligned}((xz)a)^{2m} &= ((xz)^2a^2)^m = ((xz)^2(a^2e))^m = ((xa)^2z^2)^m = ((xa)z)^2)^m\\ &= ((xa)z)^m)^2 = ((xa)^m z^m)^2 = (((ya)t_3)z^m)^2 = ((ya)^2z^{2m})t_3^2\\ &= ((yz^m)^2a^2)t_3^2 = (\left(y^2\left(z^{2m-1}z\right)\right)a^2)t_3^2 = ((\left(yz^{2m-1}\right)(yz)\right)a^2)t_3^2\\ &= ((\left(yz^{2m-1}\right)a)((yz)\,a))t_3^2 = t_3^2(((yz)a)((yz^{2m-1})a))\\ &= ((yz)a)\left(t_3^2((yz^{2m-1})a)\right) \in ((yz)\,a)\,S.\end{aligned}$$

Similarly we can show that $((yz)a)^{2m} \in ((xz)\,a)\,S$. Therefore $(xz)\eta(yz)$. Similarly we can show that η is left compatable. Hence η is a congruence relation.

Next we shall show that η is a band congruence, by using Theorem 8, Lemma 7 and (1), we have $(xa)^2 = x^2a^2 = a^2x^2 = (aa)\,x^2 = \left(x^2a\right)a \in \left(x^2a\right)S$. Also using (6), (1), (2) and (7) we get $\left(x^2a\right)^2 = \left(x^2a\right)\left(x^2a\right) = x^2(\left(x^2a\right)a) = x^2(a^2x^2) = x^2((ax)(ax)) = x^2((xa)(xa)) = (xa)(x^2(xa)) \in (xa)S$. Therefore $x\eta x^2$, that is, $x_\eta^2 = x_\eta$. Hence S/η is idempotent. Now let $x\eta y$ which implies that $x\eta x^2\eta xy$, therefore $x\eta xy$.

Let $x\eta y$ and using Lemma 7, we have

$$((xy)\,a)^2 = ((yx)\,a)^2 = ((yx)\,a)\,((yx)\,a) \in ((yx)\,a)\,S.$$

Similarly $((yx)\,a)^2 \in ((xy)a)\,S$. Therefore $xy\eta yx$, that is, $x_\eta y_\eta = y_\eta x_\eta$. Hence S/η is a commutative AG-groupoid and so is commutative semigroup of idempotents. □

Theorem 10. *η is separative on S.*

Proof. Let $x^2\eta xy$ and $xy\eta y^2$. Then we have $x^2\eta y^2$, but, $x^2\eta x$ and $y^2\eta y$. So, $x\eta x^2\eta y^2\eta y$. Therefore, $x\eta y$. Hence η is separative. □

Theorem 11. *S/η is a separative semilattice homomorphic image of S.*

Proof. It follows from Theorems 9 and 10. □

Remark 2. *If every congruence on S is left zero, i.e., $ax\tau a$, then S/η is a maximal separative semilattice homomorphic image of S.*

References

[1] **P. Holgate**, *Groupoids satisfying a simple invertive law*, The Math. Stud. **61** (1992), 101 – 106.

[2] **S. Kamran**, *Conditions for LA-semigroups to resemble associative structures*, Ph.D. Thesis, Quaid-i-Azam University, Islamabad, 1993.

[3] **M. A. Kazim and M. Naseeruddin**, *On almost semigroups*, The Alig. Bull. Math. **2** (1972), 1 – 7.

[4] **Q. Mushtaq and Q. Iqbal**, *Decomposition of a locally associative LA-semigroup*, Semigroup Forum **41** (1990), 154 – 164.

[5] **Q. Mushtaq and M. Khan**, *Decomposition of AG^*-groupoids*, Quasigroups and Related Systems **15** (2007), 303 – 308.

[6] **N. Stevanović and P. V. Protić**, *Some decompositions on Abel-Grassmann's groupoids*, PU. M. A. **8** (1997), 355 – 366.

Received January 05, 2010

Department of Mathematics, COMSATS Institute of Information Technology, Abbottabad, Pakistan.
E-mail: madadmath@yahoo.com

Quasigroups and Related Systems **18** (2010), 149 − 163

Identity sieves for quasigroups

Smile Markovski, Vesna Dimitrova and Simona Samardjiska

Abstract. In this paper we consider the set $\mathcal{Q}_n$ of all finite quasigroups of a given order n, where n is a positive integer. Using left and right translations, as well as suitably chosen quasigroup terms t, we define sets of identities that are satisfied in the class $\mathcal{Q}_n$. The set $\mathcal{Q}_n$ can be represented as a union of isomorphism classes $\mathbb{C}_i$, $\mathcal{Q}_n = \cup_{i=1}^{h}\mathbb{C}_i$, and we use sets of identities as sieves for classifying the isomorphism classes. In such a way we make a presentation of the set of all isomorphism classes of $\mathcal{Q}_n$ in the form of a disjoint union $\{\mathbb{C}_1, \dots, \mathbb{C}_p\} = \cup_{i=1}^{s}\mathcal{Q}^{(i)}$, where $\mathcal{Q}^{(i)}$ are unions of isomorphism classes. We show that these classifications can be used for obtaining quasigroups with special qualities, that can be applied for designing several kinds of cryptographic primitives (PRNG, hash functions, stream and block ciphers,...), or for defining error detecting and error correcting codes.

Also, by using suitably chosen identities, we show the fractal structure of some quasigroups in $\mathcal{Q}_4$.

1. Introduction

A groupoid $(G,\cdot)$ is a pair of a nonempty set G and a binary operation $\cdot : G^2 \to G$. Given a groupoid $(G,\cdot)$ and an element $a \in G$, the translations L_a and R_a, called left translation and right translation, are defined by $L_a(x) = ax$ and $R_a(x) = xa$, for each $x \in G$. A groupoid $(G,\cdot)$ is said to be a quasigroup if and only if L_a and R_a are permutations on G for each $a \in G$.

Note that each set of translations

$$S = \{L_{a_1}, \dots, L_{a_m}, R_{b_1}, \dots, R_{b_k}\},\ m \geqslant 0,\ k \geqslant 0,$$

on a groupoid $(G,\cdot)$ generates a semigroup $<S>$.

We have the following result.

Theorem 1.1. *Let $(G,\cdot)$ be a finite quasigroup, and let $S = \{L_{a_1}, \dots, L_{a_n}, R_{a_1}, \dots, R_{a_n}\}$, where $G = \{a_1, \dots, a_n\}$. Then for each $T \in <S>$ there is a smallest integer $r = r(T)$ such that $T^r = 1_G$.*

2010 Mathematics Subject Classification: 20N05
Keywords: quasigroup, identity, isomorphism class, identity sieve, fractal quasigroup.

Proof. Since L_a and R_a are permutations on G, $< S >$ is a group of permutations on G, so $r(T)$ is the order of the permutation T. □

If T is a permutation of a set $G = \{a_1, \dots, a_n\}$, then for each element $b \in G$ there is a number $r_b \leqslant n$ such that $T^{r_b}(b) = b$. (Namely, the set $\{b, T(b), T^2(b), \dots\}$ is a subset of G.) Then, for the number

$$r_T = LCM(r_{a_1}, r_{a_2}, \dots, r_{a_n}) \leqslant LCM(1, 2, \dots, n)$$

we have $T^{r_T}(x) = x$ for each $x \in G$. Hence, $T^{r_T} = 1_G$, and $r(T)$ is a factor of r_T. So, we have the next theorem:

Theorem 1.2. *The order $r(T)$ of each $T \in <S>$, where S is a set of left and right translations of a finite quasigroup G, is a factor of the number $LCM(1, 2, \dots, |G|)$.*

We need as well to introduce the notion of a term.

A groupoid term, where f denotes a binary functional symbol and X denotes a nonempty set of variables, is defined inductively as follows:

1) x is a term for each $x \in X$;

2) if $t_1, \dots, t_n$ are terms, then the expression $f(t_1, \dots, t_n)$ is a term.

Given a term t and different variables $x_1, \dots, x_k \in X$, by $t(x_1, \dots, x_k)$ we denote that only the variables $x_1, \dots, x_k$ may appear in the term t; hence, some variable x_j may not appear in t. In the sequel we consider special types of terms $t(x_1, \dots, x_k)$, where a variable x_i appears exactly once, and we denote it by $t(\bar{x}_i, x_i)$, where $\bar{x}_i$ denotes a fixed tuple of all other variables occurring in t. For example, the term $t(x, y, z, u, v, w) = (y(x((yz)u)))(zy)$ can be denoted as $t = t(\bar{x}, x)$ or $t = t(\bar{u}, u)$. There are several choices for $\bar{x}$ ($\bar{x} = (y, z, u)$, or $\bar{x} = (u, z, y)$, or $\bar{x} = (y, u, z)$, $\dots$) as well as for $\bar{u}$, and for our purposes it does not matter which one is chosen.

Let $(G, \cdot)$ be a given groupoid. Each term $t = t(x_1, \dots, x_k)$ defines an s-ary function t^G on the set G, where s is the number of all different variables that occur in t. Denote by $y_1, \dots, y_s \in X$ all different variables in t, in some ordering. (Depending on the ordering, different functions t^G can be defined.) The definition of t^G follows the inductive definition of a term. For each variable x we have that x^G is the identity mapping. If $t = t_1 t_2$, where t_1 contains the different variables $y_{i_1}, \dots, y_{i_p}$ and t_2 contains the different variables $y_{j_1}, \dots, y_{j_q}$, then for all $a_i \in G$ we define $t^G(a_1, \dots, a_s) = t_1^G(a_{i_1}, \dots, a_{i_p}) \cdot t_2^G(a_{j_1}, \dots, a_{j_q})$.

Given a term $t(y_1, \dots, y_s)$, where y_i are different variables that occur in t, and given an l-tuple $(a_{i_1}, \dots, a_{i_l}) \in G^l$, we can define an $(s-l)$-ary function $t^G_{a_{i_1}, \dots, a_{i_l}}$ on G by $t^G_{a_{i_1}, \dots, a_{i_l}}(a_1, \dots, a_{i_1 - 1}, a_{i_1 + 1}, \dots, a_{i_l - 1}, a_{i_l + 1}, \dots, a_s) =$

$t^G(a_1, \dots, a_s)$. We say that $t^G_{a_{i_1},\dots,a_{i_l}}$ is the l-th projection of t defined by the l-tuple $(a_{i_1}, \dots, a_{i_l}) \in G^l$.

By using the notation $t(\bar{x}, x)$ of a term t with s different variables, where x occurs exactly once in t, we denote by $t^G_{\bar{a}}$ the $(s-1)$-th projection of t, obtained by the $(s-1)$-tuple $\bar{a} \in G^{s-1}$. So, $t^G_{\bar{a}}$ is the mapping on G defined by $t^G_{\bar{a}}(x) = t^G(\bar{a}, x)$.

In the case of quasigroups, we have that $t^G_{\bar{a}} \in < S >$, where $G = \{a_1, \dots, a_n\}$ and $S = \{L_{a_1}, \dots, L_{a_n},\ R_{a_1}, \dots, R_{a_n}\}$. For example, when $t = (y(x((yz)u)))(zy) = t(\bar{x}, x)$, $\bar{x} = (u, y, z)$ and $\bar{a} = (b, c, d)$, we have $t^G_{\bar{a}} = R_{dc} L_c R_{(cd)b}$. Therefore, Theorem 1.1 and Theorem 1.2 hold for these mappings too.

Given two terms t_1 and t_2, the expression $t_1 \approx t_2$ is called an identity. An identity $t_1(x_1, \dots, x_k) \approx t_2(x_1, \dots, x_k)$ is said to be satisfied in a groupoid G if for every $a_i \in G$ we have $t^G_1(a_1, \dots, a_k) = t^G_2(a_1, \dots, a_k)$. An identity is satisfied in a class of groupoids $\mathcal{C}$ if it is satisfied in every groupoid of $\mathcal{C}$. (Note that t^G_1 and t^G_2 are not considered as k-ary functions on G, since some of the variables $x_1, \dots, x_k$ may not appear neither in t_1 nor in t_2.)

Further on, if there is no confusion, instead of t^G we will write simply t.

2. Sieve construction

In this Section we consider finite quasigroups only.

Lately, quasigroups have been intensively studied for use in cryptography and coding theory. The notion of a shapeless quasigroup was defined in [5] as a kind of quasigroup suitable for building cryptographic primitives. According to this definition, a shapeless quasigroup Q should not satisfy any identity of the form $x(x(\dots(xy)\dots)) = y$ or $(\dots((yx)x)\dots)x = y$, where x occurs $n < 2|Q|$ times. In general, quasigroups may satisfy different types of laws in the form of identities. Here, we make a wider characterization regarding a special form of identities that refines the notion of a shapeless quasigroup.

Let t be a term of the form $t = t(\bar{y}, y)$ such that $\bar{y} = (x_1, \dots, x_k)$, $k \geqslant 1$ (and $y \neq x_i$ for each $i = 1, \dots, k$). A t-sieve is said to be the set $Sieve(t)$ of identities defined recursively as follows:

$$Sieve(t) = \{t^{(1)} = t(\bar{y}, y),\ t^{(2)} = t(\bar{y}, t^{(1)}),\ t^{(3)} = t(\bar{y}, t^{(2)}), \dots\}.$$

Note that $t^{(2)} = t(\bar{y}, t(\bar{y}, y))$, $t^{(3)} = t(\bar{y}, t(\bar{y}, t(\bar{y}, y))), \dots$.

Theorem 2.1. *For each term $t = t(\bar{y}, y)$ and for each finite quasigroup Q, there is a smallest number $r(t, Q)$ such that $t^{(r(t,Q))} \approx y$ is an identity in Q.*

Proof. Let $t = t(\bar{y}, y)$, $\bar{y} = (x_1, \ldots, x_k)$ and $\bar{a} = (a_1, \ldots, a_k) \in Q^k$. Then, by Theorem 1.1, there is a smallest number $r(t_{\bar{a}})$ such that $t_{\bar{a}}^{r(t_{\bar{a}})}(y) = y$ for each $y \in Q$. Note that $t_{\bar{a}}^{r(t_{\bar{a}})} = t_{\bar{a}}^{(r(t_{\bar{a}}))}$, since $t_{\bar{a}}^{(p)}(y) = t(\bar{a}, t(\bar{a}, \ldots, t(\bar{a}, y))) = t_{\bar{a}}^{p}(y)$. It follows that for the number $r(t, Q) = LCM\{r(t_{\bar{a}})|\ \bar{a} \in Q^k\}$ we have $t_{\bar{a}}^{(r(t,Q))}(y) = y$ for every $\bar{a} \in Q^k$ and for each $y \in Q$. This means that $t^{(r(t,Q))} \approx y$ is an identity in Q. □

The number $r(t, Q)$ is called a rang of t in Q.

Let $\mathcal{Q}_n$ denote the set of all quasigroups of order n. We have the following.

Theorem 2.2. *For each term $t = t(\bar{y}, y)$ there is a number $r(t, n)$, such that $t^{(r(t,n))} \approx y$ is an identity in the set $\mathcal{Q}_n$.*

Proof. By Theorem 2.1 we have that for each $Q \in \mathcal{Q}_n$ there is a number $r(t, Q)$ such that $t^{(r(t,Q))} \approx y$ is an identity in Q. Let $r(t, n) = LCM\{r(t, Q)|\ Q \in \mathcal{Q}_n\}$. Then $t^{(r(t,n))} \approx y$ is an identity in Q for each $Q \in \mathcal{Q}_n$, i.e., it is an identity in $\mathcal{Q}_n$ as well. □

The number $r(t, n)$ is called a rang of t in $\mathcal{Q}_n$. It follows, by the definition of $r(t, n)$, that it is the smallest number such that $t^{(r(t,n))}(\bar{y}, y) \approx y$ is an identity in $\mathcal{Q}_n$. The upper bound of $r(t, n)$ is $LCM(2, 3, \ldots, n)$. When considering $Sieve(t)$ on $\mathcal{Q}_n$ in order to produce identities of the type $t^{(r(t,n))} \approx y$, it is enough to take its restriction, i.e., its finite subset

$$Sieve(t, n) = \{t^{(i)}|\ \ i|LCM(2, 3, \ldots, n)\}.$$

Using $Sieve(t, n)$, where $t = t(\bar{y}, y)$, we sieve the quasigroups from $\mathcal{Q}_n$ via the isomorphism classes of $\mathcal{Q}_n$. The sieving algorithm $SA(t, n)$ is the following.

1. Input: the set $\mathcal{Q}_n$.
2. Represent the set $\mathcal{Q}_n$ as (disjoint) union of its isomorphism classes, $\mathcal{Q}_n = \mathbb{C}_1 \cup \mathbb{C}_2 \cup \cdots \cup \mathbb{C}_h$.
3. For $j = 1, 2, \ldots, h$, take a representative quasigroup $Q_j \in \mathbb{C}_j$.

4. For each $i|LCM(2,3,\dots,n)$ form families of isomorphism classes $\mathcal{Q}^{(i)}$ as follows. $\mathbb{C}_j \in \mathcal{Q}^{(i)}$ if i is the smallest integer such that the identity $t^{(i)} \approx y$ is satisfied in Q_j.

5. Output: representation of the isomorphism classes of $\mathcal{Q}_n$ as a disjoint union of families of isomorphism classes,
$$\{\mathbb{C}_1,\dots,\mathbb{C}_h\} = \bigcup\{\mathcal{Q}^{(i)} |\ \ i|LCM(2,3,\dots,n)\}.$$

The definition of $\mathcal{Q}^{(i)}$ does not depend on Q_j, since if an identity is satisfied in Q_j, then it is satisfied in each quasigroup $Q \in \mathbb{C}_j$ too.

Note that the families $\mathcal{Q}^{(i)} = \mathcal{Q}^{(i)}(t)$ depend on the chosen term t. For different terms $t_1, t_2, t_3, \dots$, we can obtain different families $\mathcal{Q}^{(i)}(t_j), j = 1,2,3,\dots$. Then by using the intersection $\bigcap\{\mathcal{Q}^{(i)}(t_j)|\ j = 1,2,\dots\}$, we can classify the isomorphism classes in several different ways. By this classification we can separate isomorphism classes of quasigroups of given order n suitable for different purposes. The Section 3 contains such classifications for the set $\mathcal{Q}_4$ of quasigroups of order 4.

3. Classifications of quasigroups of order 4

In this section we consider the set $\mathcal{Q}_4$ of all binary quasigroups of order 4, consisting of 576 quasigroups. We order the set $\mathcal{Q}_4$ by lexicographic ordering, using the presentation of the multiplicative table of a quasigroup as a concatenation of the strings of its rows. The set $\mathcal{Q}_4$ can be represented as a union of 35 isomorphism classes $\mathbb{C}_j$, and we take the quasigroups with lexicographic numbers 1, 2, 3, 4, 6, 10, 14, 25, 26, 27, 28, 29, 30, 33, 34, 35, 37, 38, 39, 40, 73, 74, 77, 80, 83, 92, 149, 150, 155, 157, 158, 159, 160, 196, 213 as representatives for the classes $\mathbb{C}_1, \mathbb{C}_2, \dots, \mathbb{C}_{35}$, respectively.

We have $LCM(2,3,4) = 12$, and there are 6 factors of 12: 1, 2, 3, 4, 6 and 12. Thus, $Sieve(t,4) = \{t^{(i)}|\ \ i = 1,2,3,4,6,12\}$. Using the algorithm $SA(t,4)$, for different choices of the terms t, we can obtain different classifications of the isomorphism classes. Table 1 and Table 2 present special type of sieves constructed from all terms $t = t(\bar{y}, y)$ such that $\bar{y} = (x)$, and with $m \le 3$ appearances of the variable x in t. So, for $m = 1$ we have two terms xy, yx, for $m = 2$ we have 6 terms $x(xy), (yx)x, (xy)x, x(yx), (xx)y, y(xx)$, and so on. Altogether, there are 24 terms of this type. Instead of $\mathbb{C}_j$, the isomorphism classes in Table 1 (and in all other tables in this section) are denoted simply by j.

How can we read Tables 1 and 2? For $m = 3$, let us consider the term $t = x(x(xy))$ in Table 2. In column 1 we have 6 isomorphism classes: $\mathbb{C}_{23}, \mathbb{C}_{24}, \mathbb{C}_{25}$, $\mathbb{C}_{26}, \mathbb{C}_{34}, \mathbb{C}_{35}$. This means that the identity $t^{(1)} \approx y$, i.e., $x(x(xy)) \approx y$, is satisfied in all of these classes. We note that these classes also satisfy the identities $t^{(i)} \approx y$ for all other values of i, but $i = 1$ is the smallest value of i such that $t^{(i)} \approx y$ is an identity in these classes. Next, the identity $t^{(2)} \approx y$, i.e., $x(x(x(x(x(xy))))) \approx y$, is satisfied in the classes $\mathbb{C}_1, \mathbb{C}_4, \mathbb{C}_7, \mathbb{C}_8, \mathbb{C}_{11}, \mathbb{C}_{16}, \mathbb{C}_{29}$, and $i = 2$ is the smallest value of i such that $t^{(i)} \approx y$ is an identity in these classes. In all of the other classes the identity $t^{(i)} \approx y$ is satisfied for $i = 4$ (and also for $i = 12$), so they are given in column 4. Note that the rang of the term $t = x(x(xy))$ in $\mathcal{Q}_4$ is $r(t, 4) = 4$, the same rang has the term $((yx)x)x$, and the rang of the other terms in Tables 1 and 2 is 12, except of the terms $x(xy)$ and $(yx)x$, that have rang 6.

m	$t \setminus i$	1	2	3	4	6	12
6*1	xy		1,4,7,8,11,16,29	23,24,25,26,34,35	2,3,5,6,9,10,17,20,30,33		12,13,14,15,18,19,21,22,27,28,31,32
	yx		1,3,9,11,14,23,28	7,20,25,26,30,35	2,4,8,10,12,17,21,24,33,34		5,6,13,15,16,18,19,22,27,29,31,32
10*2	$x(xy)$	1,4,7,8,11,16,29	2,3,5,6,9,10,17,20,30,33	23,24,25,26,34,35		12,13,14,15,18,19,21,22,27,28,31,32	
	$(xy)x$	1,11,26	2,3,4,8,9,10,35	7,17,23,25,33	15,20,22,24,30,34	13,14,16,19,27,28,29	5,6,12,18,21,31,32
	$x(yx)$	1,11,26	2,3,4,8,9,10,35	7,17,23,25,33	15,20,22,24,30,34	13,14,16,19,27,28,29	5,6,12,18,21,31,32
	$(yx)x$	1,3,9,11,14,23,28	2,4,8,10,12,17,21,24,33,34	7,20,25,26,30,35		5,6,13,15,16,18,19,22,27,29,31,32	
	$(xx)y$	1,3	2,4,7,8,9,10,11,15,16,20,29	22,23,24,25,26,34,35	5,6,17,30,33	13,14,19,28	12,18,21,27,31,32
	$y(xx)$	1,8	2,3,4,9,10,11,14,22,23,24,28	7,15,20,25,26,30,35	12,17,21,33,34	13,16,19,29	5,6,18,27,31,32

Table 1: Application of $SA(t, 4)$ on $\mathcal{Q}_4$ by using terms $t = t(\bar{y}, y)$ with $\bar{y} = (x)$, for $m = 1$ and $m = 2$.

We analyze the obtained results in Tables 1 and 2. For that aim, we look at the frequency of appearance of an isomorphism class in different

m	$t \setminus i$	1	2	3	4	6	12
31*3	$x(x(xy))$	23,24,25,26, 34,35	1,4,7,8, 11,16,29		2,3,5,6,9,10, 12,13,14,15, 17,18,19,20, 21,22,27,28, 30,31,32,33		
	$(x(xy))x$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$x((xy)x)$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$((xy)x)x$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$x(x(yx))$	25	1,3,9,11, 17,24,34	7,20,23,26, 30,35	2,4,8,10, 13,27,33	5,12,14,15, 18,19,22	6,16,21,28, 29,31,32
	$(x(yx))x$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$x((yx)x)$	25	1,4,8,11, 17,20,30	7,23,24,26, 34,35	2,3,9,10, 13,27,33	5,12,15,16, 18,19,22	6,14,21,28, 29,31,32
	$((yx)x)x$	7,20,25,26, 30,35	1,3,9,11, 14,23,28		2,4,5,6,8,10, 12,13,15,16, 17,18,19,21, 22,24,27,29, 31,32,33,34		
	$x((xx)y)$	17	1,4,7,9,10, 20,30,33	23,24,25,26, 34,35	2,3,5,6,8, 11,15,16,18, 27,29,32	12,13,19,31	14,21,22,28
	$((xx)y)x$	26,35	1,3,8,10, 15,20,30	7,17,23,25, 33	2,4,9,11,19, 24,27,31,34	5,6,12,13, 14,18,32	16,21,22,28, 29
	$x(y(xx))$	26,35	1,3,8,10, 22,24,34	7,17,23,25, 33	2,4,9,11,19, 20,27,30,32	5,12,13,16, 18,21,31	6,14,15,28, 29
	$(y(xx))x$	17	1,4,9,10, 23,24,33,34	7,20,25,26, 30,35	2,3,8,11,12, 14,18,21,22, 27,28,31	5,13,19,32	6,15,16,29
	$(x(xx))y$		1,4,5,6,7,8, 11,16,17,20, 29,30,33	23,24,25,26, 34,35	2,3,9,10,18, 31	12,13,14,19, 21,27,32	15,22,28
	$y(x(xx))$	23	1,3,9,11,12, 14,17,24,28,34	7,20,25,26, 30,35	2,4,8,10,21, 33	5,13,18,19, 27,31	6,15,16,22, 29,32
	$((xx)x)y$	7	1,4,5,8,11, 16,17,20,29,30	23,24,25,26, 34,35	2,3,6,9,10, 33	12,13,18,19, 27,32	14,15,21,22, 28,31
	$y((xx)x)$		1,3,9,11,12, 14,17,21,23, 24,28,33,34	7,20,25,26, 30,35	2,4,8,10, 18,32	5,6,13,16, 19,27,31	15,22,29

Table 2: Application of $SA(t,4)$ on $\mathcal{Q}_4$ by using terms $t = t(\bar{y}, y)$ with $\bar{y} = (x)$, for $m = 3$.

columns. For example, the class $\mathbb{C}_1$ appears only in columns 1 and 2. It means that the identity $t^{(2)} \approx y$ is satisfied for each term t from Tables 1 and 2. Consequently, the quasigroups of the class $\mathbb{C}_1$ should not be used for cryptographic purposes, since they allow to be attacked by applying very simple identities. Nevertheless, they are suitable for defining some error detecting codes ([1]). On the other hand, the classes $\mathbb{C}_{31}$ and $\mathbb{C}_{32}$ appear 13 times in column 12, 6 times in column 6 and 5 times in column 4. We conclude that the quasigroups of the classes $\mathbb{C}_{31}$ and $\mathbb{C}_{32}$ are suitable for cryptographic purposes. They have better cryptographic properties regarding t, because it would be more unlikely and more difficult to reach an expression that can be replaced by a simpler one. They belong also to the class of shapeless quasigroups. Even more, for any term of the form $t = t(\bar{y}, y)$ from Tables 1 and 2, they satisfy the identity $t^{(i)} \approx y$ only when $mi \geqslant 12$. One can find some identities of type $t = t(\bar{y}, y)$, where x appears at least 5 times in t, such that the inequality $mi \geqslant 12$ is not satisfied. Nevertheless, the inequality $mi \geqslant 8$ was satisfied in all terms $t = t(\bar{y}, y)$, where $\bar{y} = (x)$, we have checked.

The discussion above can help improve the definition of a shapeless quasigroup. Now, we define that a shapeless quasigroup should not satisfy any identity of the form $t^{(i)} \approx y$, for any term $t = t(\bar{y}, y)$, where $\bar{y} = (x)$, for $mi < 2n$. By this new definition, we have that only the quasigroups of the classes $\mathbb{C}_{13}, \mathbb{C}_{18}, \mathbb{C}_{19}, \mathbb{C}_{27}, \mathbb{C}_{31}$ and $\mathbb{C}_{32}$ can be considered as shapeless.

In Tables 1 and 2 we considered only special types of terms, in order to get more complete picture of the distribution of the isomorphism classes in the families $\mathcal{Q}^{(i)}$. Still, sieves of general type $Sieve(t)$, where $t = t(\bar{y}, y)$ such that $\bar{y} = (x_1, \dots, x_s),\ s \geqslant 1$, can be considered as well. For that aim we investigate the left and the right translations, which define the quasigroups. From the properties of these translations, we can derive general conclusions about the structure of the quasigroups, and how they can be sieved. This gives a different classification of the classes of isomorphism.

As we said earlier, in a quasigroup Q, for an arbitrary term $t = t(\bar{y}, y)$, and each $\bar{a} \in Q^{s-1}$, the mapping $t_{\bar{a}}^{Q} \in < S >$, where $Q = \{a_1, \dots, a_n\}$ and $S = \{L_{a_1}, \dots, L_{a_n},\ R_{a_1}, \dots, R_{a_n}\}$. Even more, each translation (being a permutation) can be represented as a composition of disjoint cycles. Hence, the permutation $t_{\bar{a}}^{Q}$ can be given by cycles and the order of $t_{\bar{a}}^{Q}$ depends on the lengths of these cycles. On the other hand, by Theorem 2.1, $r(t, Q) = LCM\{r(t_{\bar{a}}^{Q}) |\ \bar{a} \in Q^{s-1}\}$, so $r(t, Q)$ depends on $L_{a_1}, \dots, L_{a_n},\ R_{a_1}, \dots, R_{a_n}$, i.e., on the properties of their cycles.

Example 3.1. Consider the quasigroup $(Q, \cdot)$ that is a representative of the isomorphism class $\mathbb{C}_2$, given by its multiplicative table

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	2	1
4	4	3	1	2

Let $t = (xy)z = t(\bar{y}, y)$, where $\bar{y} = (x, z)$. Then, for $\bar{a} = (a, b) \in Q^2$, we have $t_{\bar{a}}^Q = L_a R_b$. Q is commutative with unit 1, so $L_1 = R_1 = (1)(2)(3)(4)$, $L_2 = R_2 = (12)(34)$, $L_3 = R_3 = (1324)$ and $L_4 = R_4 = (1423)$.

Now, $L_1R_1 = (1)(2)(3)(4)$, $L_1R_2 = L_2R_1 = (12)(34)$, $L_1R_3 = L_3R_1 = (1324)$, $L_1R_4 = L_4R_1 = (1423)$, $L_2R_2 = (1)(2)(3)(4)$, $L_2R_3 = L_3R_2 = (1423)$, $L_2R_4 = L_4R_2 = (1324)$, $L_2R_4 = L_4R_2 = (1324)$, $L_3R_3 = (12)(34)$, $L_3R_4 = L_4R_3 = (1)(2)(3)(4)$, $L_4R_4 = (12)(34)$.

Since we have cycles of lengths 1, 2 and 4, $r(t, Q) = LCM(1, 2, 4) = 4$.

This example shows how we can calculate $r(t, Q)$ for given t and Q. But, of course, there are an infinite number of terms, so such approach is not always suitable. Especially, if we are considering the properties of quasigroups used in some kind of quasigroup transformations in a cryptographic primitive. Still, the nature of the left and the right quasigroup translations can show how the mapping $t_{\bar{a}}^Q$ behaves for any t or Q. For cryptographic purposes, a quasigroup Q needs bigger $r(t, Q)$ for any t.

Denote by $r_{max} = max\{r(t, Q)|\ t \text{ is a term}\}$, which in fact is the maximal i for any $Sieve(t, 4)$ that sieves the quasigroup Q. Analyzing the cycles of the translations $L_1, R_1, \ldots, L_4, R_4$ from Example 3.1 we can conclude that any composition of these translations, produces only permutations with cycles of lengths 1, 2 and 4. Hence, we have that $r_{max} = 4$ for all quasigroups in the class $\mathbb{C}_2$.

r_{max}	Isomorphism class
2	1
3	7,23,25,26,35
4	2,3,4,8,9,10,11,17,20,24,30,33,34
12	5,6,12,13,14,15,16,18,19,21,22,27,28,29,31,32

Table 3: Classification of $\mathcal{Q}_4$ by $Sieve(t, 4)$, for any term t.

Table 3 gives the values r_{max} for all isomorphism classes in $\mathcal{Q}_4$. The analysis that led to this classification is rather cumbersome and not especially neat. That is why, here we give only a few examples that prove the correctness of Table 3.

Example 3.2. Consider the quasigroup with lexicographic order 1, that is a representative of the isomorphism class $\mathbb{C}_1$, and is given by its multiplication table

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

This quasigroup is commutative with unit 1, so $L_1 = R_1 = (1)(2)(3)(4)$, $L_2 = R_2 = (12)(34)$, $L_3 = R_3 = (13)(24)$ and $L_4 = R_4 = (14)(23)$.

Let t be an arbitrary term. Then the mapping $t^Q_{\bar{a}}$, $\bar{a} \in Q^{s-1}$ is some finite composition of the translations $L_1 = R_1, \dots, L_4 = R_4$. When composing any two of these translations, we have only the following three possibilities: $(ij)(kl) \cdot (ij)(kl) = (i)(j)(k)(l)$, $(ij)(kl) \cdot (ik)(jl) = (il)(kj)$ and $(ij)(kl) \cdot (i)(j)(k)(l) = (ij)(kl)$ (or $(i)(j)(k)(l) \cdot (ij)(kl) = (ij)(kl)$), i.e., again we get permutations of the same type. Hence, an arbitrary composition produces only permutations with cycles of lengths 1 and 2, which implies that $r_{max} = 2$ for all quasigroups in the class $\mathbb{C}_1$.

Example 3.3. Consider the quasigroups with lexicographic orders 92 and 213, that are representatives of the isomorphism classes $\mathbb{C}_{26}$ and $\mathbb{C}_{35}$ respectively. The quasigroups from these two different isomorphic classes have identical properties regarding the translations that define them. Namely, the left translations of the quasigroup 92 (given in Subsection 4.2) are $(1)(234)$, $(2)(143), (3)(124), (4)(132)$, which on the other hand are the right translations of the quasigroup 213. Again, the right translations of the quasigroup 92, $(1)(243), (2)(134), (3)(142)$, $(4)(123)$, are the left translations of the quasigroup 213.

Similarly, as in the previous example, it is crucial to discover all of the different cases of composing an arbitrary number of the translations that define these quasigroups. We make several observations.

When composing any two left, or any two right translations, we have these two possibilities: $(i)(jkl) \cdot (i)(jkl) = (i)(jlk)$ or $(i)(jkl) \cdot (j)(ilk) = (l)(ijk)$, i.e., again we have permutations of the same type and of order 3.

When composing a left and a right translation (in any order) we have $(i)(jkl) \cdot (i)(jlk) = (i)(j)(l)(k)$ or $(i)(jkl) \cdot (j)(ikl) = (il)(jk)$, i.e., we get a new permutation of order at most 2. Now, this new type of permutation can be composed with any of the quasigroup translations yielding $(i)(jkl) \cdot (il)(jk) = (ijl)(k)$, $(i)(jlk) \cdot (il)(jk) = (ikl)(j)$, and $(il)(jk) \cdot (i)(jkl) = (ilk)(j)$, $(il)(jk) \cdot (i)(jlk) = (ilj)(k)$, or two such permutations can be composed to give $(il)(jk) \cdot (il)(jk) = (i)(l)(j)(k)$ or $(ij)(lk) \cdot (il)(jk) = (ik)(lj)$.

Hence, an arbitrary composition produces only permutations with cycles of lengths 1 and 2, or only permutations with cycles of lengths 1 and 3. This means that $r_{max} = 3$ for the quasigroups in the classes $\mathbb{C}_{26}$ and $\mathbb{C}_{35}$.

Example 3.4. The quasigroup with lexicographic order 158, that is a representative of the isomorphism class $\mathbb{C}_{31}$, has the following multiplication table

$\cdot$	1	2	3	4
1	2	1	3	4
2	3	4	2	1
3	1	3	4	2
4	4	2	1	3

The left translations of this quasigroup are (12)(34), (1324), (1)(234), (143)(2), while the right ones are (123)(4), (1)(3)(24), (134)(2), (1432). Since these permutations have cycles of length 12, this immediately implies that $r_{max} = 12$.

We combine Tables 1, 2 and 3 to obtain Table 4, where the values r'_{max} come only from terms t from Tables 1 and 2, i.e., $r'_{max} = max\{r(t, Q)|\ t$ is a term from Tables 1 and 2$\}$. The families of isomorphism classes in Table 4 are separated by semi-columns. So, '1;' denotes the family $\{\mathbb{C}_1\}$, '7,23,35;' denotes the family $\{\mathbb{C}_7, \mathbb{C}_{23}, \mathbb{C}_{35}\}$, and so on. The family '3,4,8,9,11;' appears in the columns $i = 1$, $i = 2$ and $i = 4$. It means that for any term t from Tables 1 and 2, only identities of the form $t^{(i)} \approx y$ are satisfied (for the corresponding value of i). Note that $r'_{max} = r_{max} = 4$.

Tables 4 gives another information about the applications of quasigroups. Generally, the quasigroups from the classes in the row $r'_{max} = 12$ and columns $i = 4$, $i = 6$ and $i = 12$ should be used for building cryptographic primitives, while those in the rows $r'_{max} = 2, 3$ and columns $i = 1, 2, 3$ should be used for designing codes. As we have noted before, the family '13,18,19,27,31,32;' contains the best quasigroups for cryptographic purposes. Nevertheless, some other classes can be used quite as well. They are denoted by italic letters in the table (6, 21, 28 and 29). Namely, the "italic" classes have the properties that in at least half of the terms t from Tables 1 and 2, the identity $t^{(i)} \approx y$ is satisfied only for $i = 12$.

$r'_{max} \setminus i$	1	2	3	4	6	12
2	1;	1;				
3	7,23,35; 25,26;	7,23,35;	7,23,35; 25,26;			
4	3,4,8,9,11; 17,20,24,30,34;	2,10; 3,4,8,9,11; 33; 17,20,24,30,34;	33; 17,20,24,30,34;	2,10; 3,4,8,9,11; 33; 17,20,24,30,34;		
12	14,16, *28,29*;	15,22; 14,16, *28,29*; 5,12, *6,21*;	15,22;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;	15,22; 14,16, *28,29*; 5,12, *6,21*; 13,18,19,27, *31,32*;

Table 4: Classification of isomorphism classes by r'_{max}.

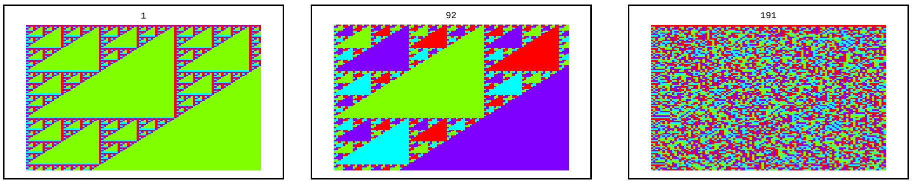
4. Proving the fractal structure of quasigroup transformations

There are several papers [6, 7], where quasigroup e- and d-transformations are considered. In [4] a method for graphical presentation of sequences obtained by quasigroup transformations is proposed. Using this method (without mathematical proof) the quasigroups are classified in two disjoint classes: the class of fractal quasigroups and the class of non-fractal quasigroups. Initiated by the identities sieves, here we give a proof that the quasigroups of order 4 with lexicographic numbers 1 and 92 are fractal (see Figure 1, where the patterns obtained from quasigroups with lexicographic numbers 1, 92 and 191 are given; 1 and 92 are fractal, 191 is non-fractal). In the same way it can be shown that all fractal quasigroups as classified in [4] have really a fractal structure too. The proofs given here use suitably chosen identities, satisfied in the quasigroup in question.

We consider here only e-transformations, defined on a quasigroup $(Q, *)$ as follows. Let $Q^+ = \{a_1 a_2 \dots a_n | a_i \in Q,\ n \geqslant 2\}$ denote the set of all finite sequences with elements of Q and let us take a fixed element $l \in Q$, called a leader. The e-transformation $e_l : Q^+ \to Q^+$ is defined by:

$$e_l(a_1a_2\dots a_n) = (b_1b_2\dots b_n) \Longleftrightarrow \begin{cases} b_1 &= l * a_1, \\ b_{i+1} &= b_i * a_{i+1}, \ \ 1 \leqslant i \leqslant n-1 \end{cases}$$

The method of producing images of quasigroup processed sequences is defined as follows. Take a sequence $aaa\dots a,\ a \in Q$, and put one under the other the sequences $e_l(aaa\dots a), e_l^2(aaa\dots a), \dots, e_l^k(aaa\dots a)$. For graphical presentation, like the one in Figure 1, we take different colors for different elements of Q.



a) b) c)

Figure 1: Images of e-transformations of the quasigroups 1, 92 and 191

4.1 The case of the quasigroup with lexicographic number 1

The quasigroup with lexicographic number 1 is given in Example 3.2. It can be checked that the following identities are satisfied by this quasigroup:

$$I_1: \quad xy \approx yx,\ (yx)x \approx y,\ y(yx) \approx x,\ (yx)^2y \approx y,\ x^2x^2 \approx x^2.$$

Let the starting sequence be $xxxxxxxxx\dots$ and let the leader be $l = y$, where x, y are variables. If we apply the e-transformation e_y consecutively on each produced sequence, then, using the identities I_1, we obtain the sequences shown on the table below,where the fractal structure appears clearly.

	x	x	x	x	x	x	x	x	x	x	$\dots$
y	yx	y	yx	y	yx	y	yx	y	yx	y	$\dots$
y	x	yx	$(yx)^2$	y	x	yx	$(yx)^2$	y	x	yx	$\dots$
y	yx	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$\dots$
y	x	x	x	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	x	x	$\dots$
y	yx	y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	yx	y	$\dots$
y	x	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	x	yx	$\dots$
y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	$(yx)^2$	y	yx	$(yx)^2$	$\dots$
y	x	x	x	x	x	x	x	yx	$(yx)^2$	$(yx)^2$	$\dots$
y	yx	y	yx	y	yx	y	yx	$(yx)^2$	$(yx)^2$	$(yx)^2$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

4.2 The case of the quasigroup with lexicographic number 92

The quasigroup with lexicographic number 92 is given by its multiplicative table:

$\cdot$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

In this quasigroup the following identities are satisfied:

$$I_{92}: \quad \begin{array}{l} xx \approx x,\ ((yx)x)x \approx y,\ y(yx) \approx (yx)x,\ ((yx)x)y \approx yx, \\ (yx)((yx)x) \approx y,\ y(y(yx)) \approx x,\ x((yx)x) \approx yx,\ (yx)y \approx x, \\ (yx)x \approx xy,\ ((yx)x)(yx) \approx x,\ x(yx) \approx y. \end{array}$$

We use the same starting sequence and leader as in the case of the quasigroup 1, and the resulting e-transformations are presented in the table below,where again a fractal structure appears.

	x	x	x	x	x	x	x	x	x	x	$\dots$
y	yx	$(yx)x$	y	yx	$(yx)x$	y	yx	$(yx)x$	y	yx	$\dots$
y	$(yx)x$	$(yx)x$	yx	yx	y	y	$(yx)x$	$(yx)x$	yx	yx	$\dots$
y	x	yx	yx	yx	x	$(yx)x$	$(yx)x$	$(yx)x$	x	y	$\dots$
y	yx	yx	yx	yx	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	y	y	$\dots$
y	$(yx)x$	x	y	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	yx	x	$\dots$
y	x	x	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	x	x	$\dots$
y	yx	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	y	yx	$\dots$
y	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	$(yx)x$	yx	yx	$\dots$
y	x	yx	y	x	yx	y	x	yx	yx	yx	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

The proofs for other fractal quasigroups are similar, and they may be quite complicated. But, if we try to write the sequences obtained by e-transformation for non-fractal quasigroups, we get very complicated terms, and it is almost impossible to obtain suitable identities.

Since if an identity is satisfied in a quasigroup Q, it is satisfied in all quasigroups isomorphic to Q, we conclude that all of the quasigroups of the isomorphism classes $\mathcal{C}_1$ and $\mathcal{C}_{26}$ are fractal.

References

[1] **V. Bakeva, N. Ilievska**, *A probabilistic model of error-detecting codes based on quaisgroups*, Quasigroups and Related Systems **17** (2009, 151 – 164.

[2] **V. D. Belousov**, *Osnovi teorii kvazigrupp i lupp*, (Russian), Nauka, Moskva, 1967.

[3] **J. Dénes, A. D. Keedwell**, *Latin squares and their applications*, Akademiai Kiado, Budapest, 1974.

[4] **V. Dimitrova, S. Markovski**, *Classification of quasigroups by image patterns*, Proc. of the Fifth International Conference for Informatics and Information Technology, 2007, Bitola, Macedonia, 152 – 160.

[5] **D. Gligoroski, S. Markovski, Lj. Kocarev**, *Edon-$\mathcal{R}$, an Infinite Family of Cryptographic Hash Functions*, The Second NIST Cryptographic Hash Workshop, UCSB, Santa Barbara, CA, 2006, 275 – 285.

[6] **S. Markovski**, *Quasigroup string processing and applications in cryptography*, Proc. of the 1st MII 2003 Conference, Thessaloniki, 2003, 278 – 290.

[7] **S. Markovski, D. Gligoroski, V. Bakeva**, *Quasigroup string processing: Part 1*, Contributions, Sec. Math. Tech. Sci., MANU, **XXI** (1999), 13 – 28.

[8] **V. Shcherbacov**, *Quasigroups in cryptology*, Computer Sci. J. Moldova **17** (2009), 193 – 228.

[9] **J. D. H. Smith**, *An introduction to quasigroups and their representations*, Academic Press, Inc., 1974.

Received August 30, 2010

S.Markovski and V.Dimitrova
Ss Cyril and Methodius University, Faculty of Sciences, Institute of Informatics, P.O. Box 162, 1000 Skopje, Republic of Macedonia,
E-mail: {smile,vesnap}@ii.edu.mk

S.Samardjiska
Department of Telematics, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology, O.S.Brag-stads plass 2B, N-7491 Trondheim, Norway,
E-mail: simona.samardziska@gmail.com

Quasigroups and Related Systems **18** (2010), 165 – 176

Non-commutative finite groups as primitive of public key cryptosystems

Dmitriy N. Moldovyan

Abstract. A new computationally difficult problem define over non-commutative finite groups is proposed as cryptographic primitive. Finite non-commutative rings of the four-dimension vectors over the ground field are defined with the vector multiplication operations of different types. Non-commutative multiplicative groups of the rings are applied to design public key cryptoschemes based on the proposed difficult problem.

1. Introduction

The most widely used in the public key cryptography difficult problems, factorization and finding discrete logarithm, can be solved in polynomial time on a quantum computer [5]. Quantum computing develops towards practical implementations therefore cryptographers look for some new hard problems that have exponential complexity while using both the ordinary computers and the quantum ones [1, 2]. Such new difficult problems have been defined over braid groups representing a particular type of infinite non-commutative groups. Using the braid groups as cryptographic primitive a number of new public key cryptosystems have been developed [3, 6].

Present paper introduces a new hard problem defined over finite non-commutative groups and public key cryptoschemes constructed using the proposed hard problem. It is also presented a theorem disclosing the local structure of the non-commutative group, which is exploited in the proposed hard problem. Then concrete type of the non-commutative finite groups is constructed over finite four-dimension vector space.

2010 Mathematics Subject Classification: 11G20, 11T71
Keywords: difficult problem, automorphism, non-commutative group, finite group, public key distribution, public encryption, commutative encryption.
The work was supported by the Russian Foundation for Basic Research grant # 08-07-00096-a.

2. New problem and its cryptographic applications

Suppose for some given finite non-commutative group Γ containing element Q possessing high prime order q there exists a method for easy selection of the elements from sufficiently large commutative subgroup $\Gamma_{comm} \in \Gamma$. One can select as private key a random element $W \in \Gamma_{comm}$ such that $W \circ Q \neq Q \circ W$ and a random number $x < q$ and then compute the public key $Y = W \circ Q^x \circ W^{-1}$ (note that it is easy to show that for arbitrary value x the inequality $W \circ Q^x \neq Q^x \circ W$ holds). Finding pair (W, x), while given Γ, Γ_{comm}, Q, and Y, is a computationally difficult problem that is suitable to design new public key cryptosystems. The problem suits also for designing commutative encryption algorithms.

The public key agreement protocols can be constructed as follows. Suppose two users have intension to generate a common secret key using a public channel. The first user generates his private key (W_1, x_1), computes his public key $Y_1 = W_1 \circ Q^{x_1} \circ W_1^{-1}$, and sends Y_1 to the second user. The last generates his private key (W_2, x_2), computes his public key $Y_2 = W_2 \circ Q^{x_2} \circ W_2^{-1}$, and sends Y_2 to the first user. Then the first user computes the value

$$\begin{aligned} K_{12} = W_1 \circ (Y_2)^{x_1} \circ W_1^{-1} &= W_1 \circ \left(W_2 \circ Q^{x_2} \circ W_2^{-1}\right)^{x_1} \circ W_1^{-1} \\ &= W_1 \circ W_2 \circ Q^{x_2 x_1} \circ W_2^{-1} \circ W_1^{-1}. \end{aligned}$$

The second user computes the value

$$\begin{aligned} K_{21} = W_2 \circ (Y_1)^{x_2} \circ W_2^{-1} &= W_2 \circ \left(W_1 \circ Q^{x_1} \circ W_1^{-1}\right)^{x_2} \circ W_2^{-1} \\ &= W_1 \circ W_1 \circ Q^{x_1 x_2} \circ W_1^{-1} \circ W_2^{-1}. \end{aligned}$$

The elements W_1 and W_2 belong to the commutative subgroup Γ_{comm}, therefore $K_{21} = K_{12} = K$, i.e. each of the users has generated the same secret K that can be used, for example, to encrypt confidential messages send through the public channel.

Suppose a public-key reference book is issued. Any person can send to some user a confidential message M using user's public key $Y = W \circ Q^x \circ W^{-1}$, where W and x are elements of user's private key. For this aim the following public key encryption scheme can be used, in which it is supposed using some encryption algorithm F_K controlled with secret key K representing an element of the group Γ.

1. Sender generates a random element $U \in \Gamma_{comm}$ and a random number u, then computes the elements $R = U \circ Q^u \circ U^{-1}$ and $K = U \circ Y^u \circ U^{-1} = U \circ \left(W \circ Q^x \circ W^{-1}\right)^u \circ U^{-1} = U \circ W \circ Q^{xu} \circ W^{-1} \circ U^{-1}$.

2. Using the element K as encryption key and encryption algorithm E_K sender encrypts the message M into the cryptogramm $C = F_K(M)$. Then he sends the cryptogram C and element R to the user.

3. Using the element R the user computes the encryption key K as follows $K = W \circ R^x \circ W^{-1} = W \circ \left(U \circ Q^u \circ U^{-1}\right)^x \circ W^{-1} = W \circ U \circ Q^{ux} \circ U^{-1} \circ W^{-1}$. Then the user decrypts the cryptogram C as follows $M = F_K^{-1}(C)$, where F_K^{-1} is the decryption algorithm corresponding to the encryption algorithm F_K.

The proposed hard problem represents some combining the exponentiation procedure with the procedure defining group mapping that is an automorphism. These two procedures are commutative therefore their combination can be used to define the following commutative-encryption algorithm.

1. Represent the message as element M of the group Γ.

2. Encrypt the message with the first encryption key (W_1, e_1), where $W_1 \in \Gamma_{comm}$, e_1 is a number invertible modulo m, and m is the least common multiple of all element orders in the group Γ, as follows $C_1 = W_1 \circ M^{e_1} \circ W_1^{-1}$.

3. Encrypt the cryptogram C_1 with the second encryption key (W_2, e_2), where $W_2 \in \Gamma_{comm}$, e_2 is a number invertible modulo m, as follows

$$C_{12} = W_2 \circ C_1^{e_2} \circ W_2^{-1} = W_2 \circ W_1 \circ M^{e_1 e_2} \circ W_1^{-1} \circ W_2^{-1}.$$

It is easy to show the encrypting the message M with the second key (W_2, e_2) and then with the first key (W_1, e_1) produces the cryptogram $C_{21} = C_{12}$, i.e. the last encryption procedure is commutative.

3. On choosing elements

In the cryptoschemes described in previous section the first element of the private key should be selected from some commutative group. A suitable way to define such selection is the following one. Generate an element $G \in \Gamma$ having sufficiently large prime order g and define selection of the element W as selection of the random number $1 < w < g$ and computing $W = G^w$. Using this mechanism the private key is selected as two random numbers w and x and the public key is the element $Y = G^w \circ Q^x \circ G^{-w}$. One can easy show that for arbitrary values w and x the inequality $G^w \circ Q^x \neq Q^x \circ W^w$ holds.

For security estimations it represents interest haw many different elements are generated from two given elements G and Q having prime orders

g and q, respectively. The following theorem gives a positive answer to this question.

Theorem 1. *Suppose elements G and Q of some non-commutative finite group Γ have the prime orders g and q, correspondingly, and satisfy the following expressions $G \circ Q \neq Q \circ G$ and $K \circ Q \neq Q \circ K$, where $K = G \circ Q \circ G^{-1}$. Then all of elements $K_{ij} = G^j \circ Q^i \circ G^{-j}$, where $i = 1, 2, \ldots, q-1$ and $j = 1, 2, \ldots, g$, are pairwise different.*

Proof. It is evident that for some fixed value j the elements $K_{ij} = G^j \circ Q^i \circ G^{-j}$, where $i = 1, 2, \ldots, q$, compose a cyclic subgroup of the order q. Condition $K \circ Q \neq Q \circ K$ means that element K is not included in the subgroup Γ_Q generated by different powers of Q. Suppose that for some values i, $i' \neq i$, j, and $j' \neq j$ elements K_{ij} and $K_{i'j'}$ are equal, i.e. $G^j \circ Q^i \circ G^{-j} = G^{j'} \circ Q^{i'} \circ G^{-j'}$. Multiplying the both parts of the last equation at the right by element G^j and at the left by element G^{-j} one gets $Q^i = G^{j'-j} \circ Q^{i'} \circ G^{-(j'-j)}$. The subgroup Γ_Q has the prime order, therefore its arbitrary element different from the unity element is generator of Γ_Q, i.e. for $i' \leq q-1$ the element $P = Q^{i'}$ generates subgroup Γ_Q. Taking this fact into account one can write

$$\begin{aligned}\left(Q^i\right)^z = \left(G^{j'-j} \circ Q^{i'} \circ G^{-(j'-j)}\right)^z &= G^{j'-j} \circ Q^{i'z} \circ G^{-(j'-j)} \\ &= G^{j'-j} \circ P^z \circ G^{-(j'-j)} \in \Gamma_Q.\end{aligned}$$

The last formula shows that mapping $\varphi_{G^{j'-j}}\left(P^z\right) = G^{j'-j} \circ P^z \circ G^{-(j'-j)}$ maps each element of Γ_Q on some element of Γ_Q. The mapping $\varphi_{G^{j'-j}}\left(\Gamma_Q\right)$ is bijection, since for $z = 1, 2, \ldots, q$ the set of elements $\left(Q^i\right)^z$ composes the subgroup Γ_Q. Thus, the mapping $\varphi_{G^{j'-j}}\left(\Gamma_Q\right)$ is a bijection of the subgroup Γ_Q onto itself.

Since order of the element G is prime, there exists some number $u = (j'-j)^{-1} \bmod g$ for which the following expressions hold $G = \left(G^{j'-j}\right)^u$ and

$$\varphi_G\left(\Gamma_Q\right) = \varphi_{\left(G^{j'-j}\right)^u}\left(\Gamma_Q\right) = \underbrace{\varphi_{G^{j'-j}}\left(\varphi_{G^{j'-j}}\left(\ldots \varphi_{G^{j'-j}}\left(\Gamma_Q\right)\ldots\right)\right)}_{u \text{ bijective mappings}},$$

where the mapping is represented as superposition of u mappings $\varphi_{G^{j'-j}}\left(\Gamma_Q\right)$. The superposition is also a bijection of the subgroup Γ_Q onto itself, since the mapping $\varphi_{G^{j'-j}}\left(\Gamma_Q\right)$ is the bijection Γ_Q onto Γ_Q. Therefore the following expression holds $K = G \circ Q \circ G^{-1} = \varphi_G(Q) \in \Gamma_Q$ and $K \circ Q = Q \circ K$.

The last formula conradicts to the condition $K \circ Q \neq Q \circ K$ of the theorem. This contradiction proves Theorem 1. $\square$

According to Theorem 1 there exist $(q-1)g$ different elements $Z_{ij} \neq E$, where E is unity element of Γ. Together with the unity element E they compose g cyclic subgroups of the order q and each of elements $Z_{ij} \neq E$ belongs only to one of such subgroups.

4. Finite rings of four-dimension vectors

Different finite rings of m-dimension vectors over the ground field $GF(p)$, where p is a prime, can be defined using technique proposed in [4]. The non-commutative rings of four-dimension vectors are defined as follows. Suppose $\mathbf{e}$, $\mathbf{i}$, $\mathbf{j}$, $\mathbf{k}$ be some formal basis vectors and $a, b, c, d \in GF(p)$, where $p \geqslant 3$, are coordinates. The vectors are denoted as $a\mathbf{e}+b\mathbf{i}+c\mathbf{i}+d\mathbf{k}$ or as (a, b, c, d). The terms $\tau\mathbf{v}$, where $\tau \in GF(p^d)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$, are called components of the vector.

The addition of two vectors (a, b, c, d) and (x, y, z, v) is defined addition of the coordinates corresponding to the same basis vector accordingly to the following formula

$$(a, b, c, d) + (x, y, z, v) = (a + x, b + y, c + z, d + v).$$

The multiplication of two vectors $a\mathbf{e} + b\mathbf{i} + c\mathbf{j} + z\mathbf{w}$ and $x\mathbf{e} + y\mathbf{i} + z\mathbf{j} + v\mathbf{k}$ is defined as multiplication of each component of the first vector with each component of the second vector in correspondence with the following formula

$$(a\mathbf{e}+b\mathbf{i}+c\mathbf{j}+z\mathbf{w})\circ(x\mathbf{e}+y\mathbf{i}+z\mathbf{j}+v\mathbf{k}) = ax\mathbf{e}\circ\mathbf{e}+bx\mathbf{i}\circ\mathbf{e}+cx\mathbf{j}\circ\mathbf{e}+dx\mathbf{k}\circ\mathbf{e}+$$
$$+az\mathbf{e}\circ\mathbf{j} + bz\mathbf{i}\circ\mathbf{j} + cz\mathbf{j}\circ\mathbf{j} + dz\mathbf{k}\circ\mathbf{j}+ av\mathbf{e}\circ\mathbf{k} + bv\mathbf{i}\circ\mathbf{k} + cv\mathbf{j}\circ\mathbf{k} + dv\mathbf{k}\circ\mathbf{k},$$

where $\circ$ denotes the vector multiplication operation. In the final expression each product of two basis vectors is to be replaced by some basis vector or by a vector containing only one non-zero coordinate in accordance with the basis-vector multiplication table (BVMT) defining associative and non-commutative multiplication. There are possible different types of the BVMTs, but in this paper there is used the BVMT of some particular type shown in Table 1, where $\mu \neq 0$. For arbitrary combination of the values $\mu \in GF(p)$ and $\tau \in GF(p)$ Table 1 defines formation of the non-commutative finite ring of four-dimension vectors.

Table 1: The basis-vector multiplication table

$\circ$	$\overrightarrow{e}$	$\overrightarrow{\imath}$	$\overrightarrow{\jmath}$	$\overrightarrow{k}$
$\overrightarrow{e}$	$\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$
$\overrightarrow{\imath}$	$\mu\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$	$\mathbf{k}$	$-\tau\mathbf{j}$
$\overrightarrow{\jmath}$	$\mu\mathbf{j}$	$-\mathbf{k}$	$-\mu^{-1}\mathbf{e}$	$\mathbf{i}$
$\overrightarrow{k}$	$\mu\mathbf{k}$	$\tau\mathbf{j}$	$-\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$

In the defined ring the vector $(\mu^{-1}, 0, 0, 0)$ plays the role of the unity element. For implementing the cryptoschemes described in Section 2 it represents interest the multiplicative group Γ of the constructed non-commutative ring. To generate the elements Q and G of sufficiently large orders it is required computing the group order Ω that is equal to the number of invertible vectors. If some vector $A = (a, b, c, d)$ is invertible, then there exists its inverses $A^{-1} = (x, y, z, v)$ for which the following formula holds $A \circ A^{-1} = E = (\mu^{-1}, 0, 0, 0)$. This vector equation defines the following system of four linear equations with four unknowns x, y, z, and v:

$$\left\{ \begin{array}{rcl} \mu ax - \mu^{-1}\tau by - \mu^{-1}cz - \mu^{-1}\tau dv & = & \mu^{-1} \\ \mu bx + \mu ay - dz + cv & = & 0 \\ \mu cx + \mu az - \tau bv + \tau dy & = & 0 \\ \mu dx - cy + bz + \mu av & = & 0. \end{array} \right.$$

If this system of equations has solution, then the vector (a, b, c, d) is invertible, otherwise it is not invertible. The main determinant of the system is the following one

$$\Delta(A) = \begin{vmatrix} \mu a & -\mu^{-1}\tau b & -\mu^{-1}c & -\mu^{-1}\tau d \\ \mu b & \mu a & -d & c \\ \mu c & \tau d & \mu a & -\tau b \\ \mu d & -c & b & \mu a \end{vmatrix}$$

Computation of the determinant gives

$$\Delta(A) = \left(\mu^2 a^2 + \tau b^2 + c^2 + \tau d^2\right)^2.$$

Counting the number of different solutions of the congruence $\Delta(A) \equiv 0 \bmod p$ one can define the number N of non-invertible vectors and then define the group order $\Omega = p^4 - N$. The indicated congruence has the same solutions as the congruence

$$\mu^2 a^2 + \tau b^2 + c^2 + \tau d^2 \equiv 0 \bmod p. \qquad (1)$$

Statement 1. *For prime $p = 4k+1$, where $k \geqslant 1$, $\mu \neq 0$, and $\tau \neq 0$, the order of the non-commutative group of the four-dimension vectors is equal to $\Omega = p(p-1)(p^2-1)$.*

Proof. For primes $p = 4k+1$ the number -1 is a quadratic residue, since $(-1)^{(p-1)/2} = (-1)^{2k} \equiv 1 \bmod p$. Therefore there exists number λ such that $\lambda^2 \equiv -1 \bmod p$ and congruence (1) can be represented as follows

$$\begin{aligned} (\mu a)^2 - (\lambda c)^2 &\equiv \tau\left((\lambda b)^2 - d^2\right) \bmod p, \\ (\mu a - \lambda c)(\mu a + \lambda c) &\equiv \tau\left((\lambda b)^2 - d^2\right) \bmod p, \\ \alpha\beta &\equiv \tau\left((\lambda b)^2 - d^2\right) \bmod p, \end{aligned}$$

where $\alpha \equiv \mu a - \lambda c \bmod p$ and $\beta \equiv \mu a + \lambda c \bmod p$. It is easy to see that for each pair of numbers (α, β) satisfying the last congruence correspond unique pair of numbers (a, c) satisfying congruence (1). Therefore the number of solutions of congruence (1) can be computed as number of solutions of the last equation. Two cases can be considered. The first case correspond to condition $(\lambda b)^2 - d^2 \not\equiv 0 \bmod p$ and there exist $(p-1)^2$ of different pairs (b, d) satisfying this condition. For each of such pairs (b, d) for all $(p-1)$ values $\alpha \not\equiv 0 \bmod p$ there exists exactly one value β such that the last congruence holds. Thus, the first case gives $N_1 = (p-1)^3$ different solutions of congruence (1).

The second case correspond to condition $(\lambda b)^2 - d^2 \equiv 0 \bmod p$ which is satisfied with $2p-1$ different pairs (b, d). The left part of the last congruence is equal to zero modulo p in the following subcases i) $\alpha \not\equiv 0 \bmod p$ and $\beta \equiv 0 \bmod p$ ($p-1$ different variants), ii) $\alpha \equiv 0 \bmod p$ and $\beta \not\equiv 0 \bmod p$ ($p-1$ different variants), and iii) $\alpha \equiv 0 \bmod p$ and $\beta \equiv 0 \bmod p$ (one variant). Thus, the subcases gives $2p-1$ different variants of the pairs (a, c), therefore the second case gives $N_2 = (2p-1)^2$ different solutions of congruence (1). In total we have $N = N_1 + N_2 = (p-1)^3 + (2p-1)^2 = p^3 + p^2 - p$ solutions. The value N is equal to the number of non-invertible vectors and defines the group order $\Omega = p^4 - N = p^4 - p^3 - p^2 + p = p(p-1)(p^2-1)$. □

Statement 2. *Suppose prime $p = 4k+3$, where $k \geqslant 1$, $\mu \neq 0$, $\tau \neq 0$, and the value τ is a quadratic non-residue modulo p. Then the order of the non-commutative group of four-dimension vectors is equal to $\Omega = p(p-1)(p^2-1)$.*

Proof. For primes $p = 4k+3$ the number -1 is a quadratic non-residue, since $(-1)^{(p-1)/2} = (-1)^{2k+1} \equiv -1 \bmod p$. Since the value τ is quadratic non-residue the following formulas hold $\tau^{(p-1)/2} \equiv -1 \bmod p$ and $(-\tau)^{(p-1)/2} \equiv 1 \bmod p$. The last formula shows that there exists number λ such that $\lambda^2 \equiv -\tau \bmod p$ and congruence (1) can be represented as follows

$$\begin{aligned} (\mu a)^2 - (\lambda b)^2 &\equiv (\lambda d)^2 - c^2 \bmod p, \\ (\mu a - \lambda b)(\mu a + \lambda b) &\equiv (\lambda d)^2 - c^2 \bmod p, \\ \gamma\delta &\equiv (\lambda d)^2 - d^2 \bmod p, \end{aligned}$$

where $\gamma \equiv \mu a - \lambda b \bmod p$ and $\delta \equiv \mu a + \lambda b \bmod p$. Then, counting different solutions of the last equation is analogous to counting solutions in the proof of Statement 1. This gives $N = p^3 + p^2 - p$ different solutions of congruence (1) and the group order $\Omega = p(p-1)(p^2-1)$. □

5. Computational experiments and illustrations

Numerous computational experiments have shown that in the case $p = 4k + 3$, where $k \geqslant 1$, $\mu \neq 0$, $\tau \neq 0$, when the value τ is a quadratic residue modulo p, the group order also equals to $\Omega = p(p-1)(p^2-1)$. However the formal proof of the last fact have not been found. The experiments have also shown that for given modulus p the structure of the non-commutative group of four-dimension vectors is the same for all non-zero values of the structural coefficients μ and τ. Here under structure of the group it is supposed a table showing the number of different vectors having the same order ω for all possible values ω. In the case of the commutative finite groups of four-dimension vectors the group structure changes with changing values of structural coefficients. The experiments have been performed using different other variants (than Table 1) of the BVMTs defining non-commutative groups of four-dimension vectors and in all cases the same structure and the same group order have been get, for all non-zero values of the structural coefficients.

Defining a group of four-dimension vectors with Table 1 and parameters $\mu = 1$, $\tau = 1$, and $p = 234770281182692326489897$ (it is a 82-bit number) one can easily generate the vectors Q and G having the prime orders $q = g = 117385140591346163244949$ (it is a 81-bit number) and then generate vector $K = G \circ Q \circ G^{-1}$:

$$\begin{aligned} Q = (&197721689364623475468796, 104620049500285101666611, \\ &91340663452028702293061, 190338950319800446198610); \end{aligned}$$

$$
\begin{aligned}
G = (&4409060537627489852 8561, 3353925177096835790 5908,\\
&6284941899395431619 9414, 1219310761289994770 30014);\\
G^{-1} = (&4409060537627489852 8561, 2012310294117239685 83989,\\
&1719208621887380102 90483, 1128392050536928494 59883);\\
K = (&1977216893646234754 68796, 1273242940387157270 80605,\\
&2058373894328657110 27118, 1694028311025209058 89980).
\end{aligned}
$$

The vectors satisfy the conditions $G \circ Q \neq G \circ Q$ and $K \circ Q \neq Q \circ K$ (see Theorem 1), therefore they can be used to implement the cryptoschemes presented in Sections 2 and 3. It is easy to generate many other different pairs of the vectors Q and G possessing 81-bit prime orders q and g and satisfying the condition of Theorem 1. The least common multiple of all element orders in the constructed group is

$$
\begin{aligned}
m = &1293985352618831314433621283538939645931 6\\
&9206096475895902974719696473 76.
\end{aligned}
$$

The exponent e of the encryption key for commutative encryption algorithm can be selected as $e = 7364758519536461719117$. Then the exponent of the decryption key is computed using formula $d = e^{-1} \bmod p$:

$$
\begin{aligned}
d = &8969427630416482351904498868955232431090386202\\
&1889673810644036709266 61.
\end{aligned}
$$

Accordingly to the algorithm for computing the private key from the public one, which is described in the next section, the 80-bit security of the proposed cryptoschemes is provided in the case of 80-bit primes q and g. In this case the difficulty of the computation of the public key from the private one does not exceed 5800 multiplications modulo 80-bit prime. In the corresponding cryptoschemes of the public encryption and of the public key agreement, which are based on elliptic curves, the difficulty of computing the public key from the private one is equal to about 2400 multiplications modulo 160 prime. Taking into account that difficulty of the modulo multiplication is proportional to squared length of the modulus one can estimate that the proposed cryptoschemes are about 1.6 times faster than analogous schemes implemented using elliptic curves. Besides, performance of the proposed cryptoschems can be significantly enhanced defining computation of the secrete element W as a sum of small powers of G, for example, $W = \sum_{s=1}^{6} \rho_s G^{t_s}$, where $\rho_s \in GF(p)$, $t_s \leqslant 15$, $s = 1, 2, \ldots, 6$.

6. Algorithm for computing the private key

Using the known parameters Q and G having the orders q and $g = q$ the following algorithm finds the private key (w, x) from the public one $Y = G^w \circ Q^x \circ G^{-w}$.

1. For all values $j = 1, 2, \ldots, q$ compute vectors $T(j) = G^j \circ Y \circ G^{-j}$ (difficulty of this step is $2q$ vector multiplications).
2. Order the table computed at the step 1 accordingly to the values $T(j)$ (difficulty of this step is $q \log_2 q$ comparison operations).
3. Set counter $i = 1$ and initial value of the vector $V = (\mu^{-1}, 0, 0, 0)$.
4. Compute the vector $V \leftarrow V \circ Q$.
5. Check if the value V is equal to some of the vectors $T(j)$ in the ordered table. If there is some vector $T(j') = V$, then deliver the private key $(w, x) = (j', i)$ and STOP. Otherwise go to step 6.
6. If $i \neq q$, then increment counter $i \leftarrow i + 1$ and go to step 4. Otherwise STOP and output the message INCORRECT CONDITION. (Difficulty of steps 5 and 6 does not exceed q vector multiplication operations and $q \log_2 q$ comparison operations.)

Overall the time complexity of this algorithm is about $3q$ vector multiplication operations and $2q \log_2 q$ comparison operations, i.e. the time complexity is $O(q)$ operations, where $O(\cdot)$ is the order notation. The algorithm requires storage for q vectors and for the same number of $|p|$-bit numbers, i.e. the space complexity is $O(q)$.

This algorithm shows that the 80-bit security of the proposed cryptosystems can be provided selecting 80-bit primes q and g. Such prime orders of the vectors Q and G can be get using 81-bit primes p.

Is seems that element G having composite order can be used in the cryptoschemes described above and this will give higher security, while using the given fixed modulus p. However this item represents interest for independent research.

7. Conclusions

Results of this paper shows that finite non-commutative groups represent interest for designing fast public key agreement schemes, public encryption algorithms, and commutative encryption algorithms. Such cryptoschemes are fast and the hard problem they are based on is expected to have exponential difficulty using both the ordinary computers and the quantum ones.

Theorem 1 is useful for justification of the selection elements Q and G while defining parameters of the cryptoschemes. The proposed non-commutative finite group of the four-dimension vectors seems to be appropriate for practical implementation of the proposed schemes. We have proved the formulas for computing the order of such groups in majority of cases. Unfortunately for a quarter of cases the formal proof have not been found and this item remains open for future consideration. However the proved cases covers the practical demands while implementing the proposed cryptoscheme in the case of using the constructed non-commutative groups of four-dimension vectors.

It is easy to show that there exists multiplicative homomorphism of the proposed groups of four-dimension vectors into the finite field over which the vector space is defined. Therefore in the case of using the constructed finite non-commutative group in the proposed cryptoschemes one should take into account the existing homomorphism. To prevent attacks using this homomorphism the large prime orders g and q of the elements G and Q should satisfy conditions $g|p+1$ and $q|p+1$ (i.e., $g \not| p-1$ and $q \not| p-1$, since $g > 2$ and $q > 2$).

References

[1] **I. Anshel, M. Anshel and D. Goldfeld**, *An algebraic method for public key cryptography*, Math. Research Letters **6** (1999), 287 – 291.

[2] **K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang and C. Park**, *New public-key cryptosystems using Braid groups*, Advances in Cryptology – CRYPTO 2000, Lecture Notes Computer Sci. **1880** (2000), 166 – 183.

[3] **E. Lee and J. H. Park**, *Cryptanalysis of the public key encryption based on Braid groups*, Advances in Cryptology – EUROCRYPT 2003, Lecture Notes Computer Sci. **2656** (2003), 477 – 489.

[4] **N. A. Moldovyan and P. A. Moldovyanu**, *New primitives for digital signature algorithms: vector finite fields*, Quasigroups and Related Systems **18** (2010), 11 – 20.

[5] **P. W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing **26** (1997), 1484–1509.

[6] **G. K. Verma**, *A proxy blind signature scheme over Braid groups*, Int. J. Network Security **9** (2009), 214 – 217.

Received January 18, 2010

St. Petersburg Institute for Informatics and Automation
Russian Academy of Sciences
14 Liniya, 39
St. Petersburg 199178
Russia
E-mail: mdn.spectr@mail.ru

Quasigroups and Related Systems **18** (2010), 177 – 186

Cryptoschemes over hidden conjugacy search problem and attacks using homomorphisms

Dmitriy N. Moldovyan and *Nikolay A. Moldovyan*

Abstract. There are considered attacks on cryptoschemes based on the recently proposed hard problem called hidden conjugacy search problem (HCSP), defined over finite non-commutative groups. It is shown that using homomorphisms of the non-commutative finite group into finite fields $GF(p^s)$, $s \geqslant 1$, in some cases the HCSP can be reduced to two independent problems: discrete logarithm and conjugacy search problem. Two methods for preventing such attacks are proposed. In the first method there are used elements of the order p. The second method uses non-invertible elements and relates to defining the HCSP over the finite non-commutative ring.

1. Introduction

Since the factorization and finding discrete logarithm problems (DLP) can be solved in polynomial time on a quantum computer [6] new hard problems attracts attention of the researchers in the cryptology area. One of such problems called conjugacy search problem (CSP) [1, 2] is defined over finite non-commutative groups as follows. Suppose Γ is a finite non-commutative group, $G, Y \in \Gamma$, $X \in \Gamma_c$, where Γ_c is a commutative subgroup of Γ, and $Y = XGX^{-1}$. Given G and Y find $X \in \Gamma_c$. Recently [4] a novel hard problem that can be called the hidden conjugacy search problem (HCSP) has been applied to design the key agreement protocol, commutative encryption algorithm, and public-key encryption algorithm. The HCSP is defined as follows. Given G and Y recover integer x and element $X \in \Gamma_c$ such that $Y = XG^xX^{-1}$. If the value x is known, the HCSP is reduced to CSP. If the element X is known, the HCSP is reduced to DLP.

2010 AMS Subject Classification: 94A60, 16Z05, 14G50, 11T71, 16S50
Keywords: difficult problem, finite group, homomorphism, non-commutative group, non-commutative ring, public-key cryptoscheme

Present paper introduces two attacks on the HCSP-based cryptoschemes that are implemented using finite non-commutative groups Γ of the m-dimensional vectors and matrices $m \times m$ defined over the finite ground field $GF(p)$. It is described a general homomorphism of the finite commutative and non-commutative groups of vectors into $GF(p)$. The first attack uses the homomorphism of the Γ into $GF(p)$ to reduce the HCSP to two independent problems, DLP and CSP. The second attack uses the hypothetic homomorphisms $\psi^{(s)}$ of the Γ into $GF(p^s)$, where $s \leqslant m$ to reduce the HCSP to two independent problems, DLP and CSP. Methods for preventing this attack are proposed. To prevent the both attacks there are two approaches. The first approach uses the element G possessing the order equal to p. The second approach uses the non-invertible element G of the finite ring $\mathbf{R}$ containing the group Γ. In the first case $\forall s \in \{1, \ldots, m\}$ the homomorphism $\psi^{(s)}: \ \Gamma \to GF(p^s)$ maps the element Y into the unity element of $GF(p^s)$ for all $s \leqslant m$. In the second case $\forall s \in \{1, \ldots, m\}$ the homomorphism $\psi^{(s)}: \ \mathbf{R} \to GF(p^s)$ maps the element Y into zero of $GF(p^s)$.

2. Homomorphisms of the finite groups and rings

Finite rings $\mathbf{R}$ of m-dimensional vectors are defined over the ground field $GF(p)$, where p is a prime. Suppose $\mathbf{e}$, $\mathbf{i}$, ..., $\mathbf{w}$ be some m basis vectors and $a, b, \ldots, z \in GF(p)$ are coordinates. Then the vectors are denoted as $a\mathbf{e} + b\mathbf{i} + \cdots + z\mathbf{w}$ or as $(a, b, \ldots, z)$. The terms like $\tau\mathbf{v}$, where $\tau \in GF(p)$ and $\mathbf{v} \in \{\mathbf{e}, \mathbf{i}, \ldots, \mathbf{w}\}$, are called *components* of the vector. The addition of two vectors is defined in the natural way, the multiplication by the formula

$$
\begin{gathered}
(a\mathbf{e}+b\mathbf{i}+\cdots+z\mathbf{w})\circ(a'\mathbf{e}+b'\mathbf{i}+\cdots+z'\mathbf{w}) = aa'\mathbf{e}\circ\mathbf{e}+ba'\mathbf{i}\circ\mathbf{e}+\cdots+za'\mathbf{w}\circ\mathbf{e}+ \\
+ab'\mathbf{e}\circ\mathbf{i} + bb'\mathbf{i}\circ\mathbf{i} + \cdots + cb'\mathbf{z}\circ\mathbf{i} + \ldots \\
\cdots + az'\mathbf{e}\circ\mathbf{w} + bz'\mathbf{i}\circ\mathbf{w} + \cdots + zz'\mathbf{w}\circ\mathbf{w},
\end{gathered}
$$

where in the last expression each product of two basis vectors should be replaced by some basis vector $\mathbf{v}$ or by a vector $\tau\mathbf{v}$ in accordance with some given table called the *basis-vector multiplication table* (BVMT) such that operation $\circ$ is associative. There are possible different types of the BVMTs defining commutative [3] and non-commutative rings $\mathbf{R}$ [4]. In general case there exists the homomorphism $\mathbf{R} \to GF(p^s)$. Indeed, suppose the vector A is invertible, then the vector equation

$$A \circ X = V \tag{1}$$

with unknown X has unique solution for arbitrary vector V: $X = A^{-1} \circ V$. Equation (1) can be rewritten as a system of m linear equations over $GF(p)$ with m unknowns that are coordinates of the vector X. Let Δ_A be the main determinant of the system of equation relating to formula (1). The determinant Δ_A is completely defined by coordinates of the vector A.

Theorem 1. *The determinant Δ_A defines the multiplicative homomorphism $\psi(A) = \Delta_A$ of the ring $\mathbf{R}$ into the field $GF(p)$.*

Proof. If A is not invertible, then $\Delta_A = 0$, i.e., all non-invertible vectors are mapped into zero of $GF(p)$. Let us consider the vector equation (1) with invertible vector A and arbitrary vector V. For all vectors $V \in \{V\}$, where $\{V\}$ denotes the considered vector space, equation (1) has unique solution, therefore $\Delta_A \neq 0$ and multiplication of the vector A by all vectors V of the considered vector space $\{V\}$ defines a linear transformation T_A of $\{V\}$. The matrix M_A of coefficients of the system of linear equations corresponding to the vector equation (1) can be put into correspondence to T_A. Another invertible vector B defines the transformation T_B corresponding to analogous matrix M_B. The vector multiplication operation in $\mathbf{R}$ is associative, therefore we have

$$(A \circ B) \circ V = A \circ (B \circ V). \tag{2}$$

The left part of (2) represents the linear transformation $T_{A \circ B}$ corresponding to the matrix $M_{A \circ B}$. The right part of (2) is the superposition $T_B * T_A$ of linear transformations T_B and T_A, therefore we have

$$T_{A \circ B} = T_B * T_A \Rightarrow M_{A \circ B} = M_A M_B \Rightarrow \Delta(A \circ B) = \Delta_A \Delta_B.$$

The last expression means that the mapping $\psi : A \to \Delta_A$ is the multiplicative homomorphism of the multiplicative group Γ of the ring $\mathbf{R}$ into the field $GF(p)$. Since for arbitrary non-invertible vectors A and B we have $\Delta_A = 0$ and $\Delta_B = 0$, the last fact means that $\psi : A \to \Delta_A$ is the multiplicative homomorphism of $\mathbf{R}$ into $GF(p)$. Theorem 1 is proved. $\square$

In a particular case when the ring $\mathbf{R}$ is a vector finite field $GF(p^m)$ [5] the homomorphism defined by Theorem 1 is the same mapping as norm homomorphism defined for the extension finite fields. Below it is also used the following well known fact. If $\mathbf{R}$ is a finite ring of matrices M defined over $GF(p)$, then mapping ψ' such that $\forall M : \ \psi'(M) \to \Delta_M$, where Δ_M is the determinant of the matrix M, represents the multiplicative homomorphism $\psi' : \ \mathbf{R} \to GF(p)$.

3. The fist attack

Using the homomorphism ψ in the case of the group of vectors (or ψ' in the case of group of matrices) described in Section 2 the following attack on cryptoschemes based on the HCSP [4] is possible. The homomorphism ψ maps the equation over the non-commutative group Γ used for computing the public key $Y = XG^x X^{-1}$, where X and x are the secret key, into the following equation over the field $GF(p)$

$$\psi(Y) = \psi(X)\,(\psi(G))^x\,(\psi(X))^{-1} = (\psi(G))^x \,. \tag{3}$$

There are possible the following three cases.

1. The order of the value $\psi(G) \in GF(p)$ is equal to the order of the element $G \in \Gamma$. In this case the secret value x can be found solving the DLP in $GF(p)$. Then the secret element X can be found solving the CSP. Thus, in this case the HCSP is reduced to two independent well known hard problems and the attack can be considered as successful one.

2. The order of the value $\psi(G) \in GF(p)$ is less than the order of the element $G \in \Gamma$. In this case the partial information about the secret value x can be found solving the DLP in $GF(p)$, i.e., solving the equation $\psi(Y) = (\psi(G))^{x'}$ one can found the value $x' \equiv x \bmod \omega_{\psi(G)}$, where $\omega_{\psi(G)}$ is the order of the value $\psi(G) \in GF(p)$. The last means that the difficulty of the HCSP is reduced.

3. The homomorphism ψ maps the element G to the unity element of the field $GF(p)$ and equation (3) degenerates into trivial equation $1 = 1^x$, from which no information about the secret value can be obtained. In this case the considered attack is not efficient to reduce the HCSP.

Thus, in the design of the cryptoschemes based on the HCSP it should be used the element G such that $\psi(G) = 1$ and the order $\omega_{\psi(G)}$ is a sufficiently large prime [4]. Selection of such element G depends on the order of the concrete group used for constructing a cryptoscheme based on the HCSP. The following theorem is very useful to select the suitable element G.

Theorem 2. *If the element G has the order ω_G such that $\gcd(\omega_G, p-1) = 1$, then $\psi(G) = 1$.*

Proof. Suppose E is the unity element of the group Γ and $\psi(G) \neq 1$. Then $\psi\left(G^{\omega_G}\right) = \psi(E) = 1$ and $\psi\left(G^{\omega_G}\right) = (\psi(G))^{\omega_G}$ imply $(\psi(G))^{\omega_G} = 1$. Thus $\gcd(\omega_G, p-1) \neq 1$, which contradicts to the assumption. □

We use Theorem 2 for a selection of the element G in the finite non-commutative group Γ of four-dimensional vectors with multiplication defined by BVMT presented in Table 1.

$\circ$	$\overrightarrow{e}$	$\overrightarrow{\imath}$	$\overrightarrow{j}$	$\overrightarrow{k}$
$\overrightarrow{e}$	$\mu\mathbf{e}$	$\mu\mathbf{i}$	$\mu\mathbf{j}$	$\mu\mathbf{k}$
$\overrightarrow{\imath}$	$\mu\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$	$\mathbf{k}$	$-\tau\mathbf{j}$
$\overrightarrow{j}$	$\mu\mathbf{j}$	$-\mathbf{k}$	$-\mu^{-1}\mathbf{e}$	$\mathbf{i}$
$\overrightarrow{k}$	$\mu\mathbf{k}$	$\tau\mathbf{j}$	$-\mathbf{i}$	$-\mu^{-1}\tau\mathbf{e}$

Table 1. The basis-vector multiplication table ($m = 4$) [4].

The order of this group is $\Omega = p(p-1)^2(p+1)$ (cf. [4]). In this case it is possible to generate a 90-bit prime $p = 2q - 1$ such that q is a prime. Then we can generate the vector G having sufficiently large prime order $\omega_G = q$ satisfying the condition $\gcd(\omega_G, p-1) = 1$ (cf. [4]). In the case of groups Γ corresponding to matrices $m \times m$ and m-dimensional vectors the choice of G satisfying Theorem 2 is relatively simple. Such choice prevents the attacks using the considered homomorphism. However there are potentially possible some other ways for reducing the HCSP to independent DLP and CSP, which use multiplicative homomorphisms $\psi^{(s)}: \Gamma \to GF(p^s)$, where $s \leqslant m$.

4. The second attack

Taking into account possibility to define the HCSP over different variants of the finite non-commutative groups it is reasonable to consider some attack on the HCSP-based cryptoschemes, in which some other potentially possible multiplicative homomorphisms can be exploited. Such attacks are also oriented to reducing the HCSP to two independent hard problems each of which is significantly less difficult than HCSP. In the second type of attacks there is assumed existence of some hypothetic multiplicative homomorphisms $\psi^{(s)}: \Gamma \to GF(p^s)$, where the cases $s \leqslant m$ provide sufficient generality for finite groups of vectors and matrices over the field $GF(p)$. Indeed, in the case of matrices the order group is described by the formula

$$\Omega_{m\times m} = \prod_{i=0}^{m-1} p^i \left(p^{m-i} - 1\right). \tag{4}$$

Since order of the multiplicative group of $GF(p^s)$ is equal to $p^s - 1$, the values $s = 1, 2, \ldots, m$ cover all cases that can be used in the second attack.

Like in the case of the first attack described in Section 3 one can formulate the following statement.

Theorem 3. *If the element G has the order ω_G such that* $\gcd(\omega_G, r) = 1$, *where* $r = \prod_{i=1}^{m} (p^m - 1)$, *then* $\forall s \leqslant m$ *the following formula holds* $\psi^s(G) = 1$.

Proof. The proof is analogous to the proof of Theorem 2. □

It is remarkable that order of the non-commutative group Γ in the case of matrices and in many cases of vectors contains the divisor p. This fact provides the first method to provide security of the HCSR-based cryptoschemes against attacks of the second type. The method consists in using element G having the order $\omega_G = p$. Then, accordingly to Theorem 3 for all $s \leqslant m$ the following mappings hold: $\psi^{(s)}(G) = 1$ and $\psi^{(s)}(Y) = 1$, therefore the considered hypothetic homomorphisms become inefficient to reduce the difficulty of the HCSP.

The number of elements possessing the order equal to p is comparatively small and some special properties of the groups Γ are to be exploited to find the elements of such order. In the case of finite non-commutative group of four-dimensional vectors with the group operation defind with Table 1 different elements having order p can be computed (and applied as element G) using the following statement.

Statement 1. *Suppose Γ is the finite group of four-dimensional vectors over the field $GF(p)$ and the group operation is defined with Table 1. Then the vectors (μ^{-1}, b, c, d) have order equal to p, if the coordinates $b, c,$ and d satisfy condition*

$$\tau b^2 + c^2 + \tau d^2 \equiv 0 \bmod p. \tag{5}$$

Proof. Squaring the vector (μ^{-1}, b, c, d) gives

$$(\mu^{-1}\mathbf{e} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})^2 = \left(\mu^{-1} - \mu^{-1}(\tau b^2 + c^2 + \tau d^2)\right)\mathbf{e} + 2b\mathbf{i} + 2c\mathbf{j} + 2d\mathbf{k}.$$

Taking into account condition (5) we get $(\mu^{-1}, b, c, d)^2 = (\mu^{-1}, 2b, 2c, 2d)$. Suppose for integer $k > 1$ the following formular holds

$$(\mu^{-1}, b, c, d)^k = (\mu^{-1}, kb, kc, kd). \tag{6}$$

Then

$$\begin{aligned} &(\mu^{-1}, b, c, d)^{k+1} = (\mu^{-1}, b, c, d)^k \circ (\mu^{-1}, b, c, d) \\ &= (\mu^{-1}, kb, kc, kd) \circ (\mu^{-1}, b, c, d) = \left(\mu^{-1}, (k+1)b, (k+1)c, (k+1)d\right). \end{aligned}$$

Therefore formula (6) holds for all $k > 1$. If $k = p$, then $(\mu^{-1}, b, c, d)^p = (\mu^{-1}, pb, pc, pd) = E$, where $E = (\mu^{-1}, 0, 0, 0)$ is the unity element of Γ. If $k < p$, then $(\mu^{-1}, b, c, d)^k \neq E$. Therefore the value p is the order of the vector (μ^{-1}, b, c, d). Statement 1 is proved. □

Another method preventing attacks of the second type consists in using non-invertible elements N of the finite ring $\mathbf{R}$ containing the group Γ, where as G is used some non-invertible element N such that the set $\{N, N^2, \ldots, N^i, \ldots\}$ contains sufficiently large number of different elements $N^i \in \mathbf{R}$. Actually it is considered the variant of the HCSP defined over the finite non-commutative ring and it is supposed the HCSP-based cryptosystems exploit the public key Y computed as $Y = XN^xX^{-1}$. Applying the homomorphisms $\psi^{(s)}$ to the last equation gives $\psi^{(s)}(Y) = 0$, since $\psi^{(N)} = 0$. Thus, this method is also efficient to prevent attacks of the second type.

Existence of the elements N suitable for defining the HCSP over finite non-commutative rings and designing the public key cryptosystems is demonstrated in the case of the 2×2 matrices by the following statement.

Statement 2. *For the 2×2 matrix $N_{2\times 2}$ defined over the ground field $GF(p)$ for all positive integers $i \geqslant 2$ the following formula holds*

$$N_{2\times 2}^i = \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^i = \begin{pmatrix} \lambda^{i-1}a & \lambda^{i-1}b \\ \lambda^{i-1}c & \lambda^{i-1}(\lambda - a) \end{pmatrix}, \tag{7}$$

where $a = \lambda/2 \pm \sqrt{(\lambda/2)^2 - bc}$.

Proof. It is easy to show that $\begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^2 = \begin{pmatrix} \lambda a & \lambda b \\ \lambda c & \lambda(\lambda - a) \end{pmatrix}$.
If (7) holds for some $i \geqslant 2$, then for $i+1$ we have

$$\begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^{i+1} = \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}^i \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix}$$
$$= \begin{pmatrix} \lambda^{i-1}a & \lambda^{i-1}b \\ \lambda^{i-1}c & \lambda^{i-1}(\lambda - a) \end{pmatrix} \begin{pmatrix} a & b \\ c & \lambda - a \end{pmatrix} = \begin{pmatrix} \lambda^i a & \lambda^i b \\ \lambda^i c & \lambda^i(\lambda - a) \end{pmatrix},$$

which completes the proof. □

Suppose the order of $\lambda \in GF(p)$ is ω_λ. Then powers of the matrix $N_{2\times 2}$ generate ω_λ different non-invertible matrices. Selecting a prime p such that $p = 2q + 1$, where q is a prime, and λ having the order $\omega_\lambda = q$ one can define different variants of the matrix $N_{2\times 2}$ suitable for application in the method for preventing attacks of the second type.

Using the ring $\mathbf{R}_{2\times2} \supset \Gamma$ of the 2×2 matrices and the matrix $N_{2\times2}$ defined over the ground field with characteristic $p > 2^{80}$ one can define the key agreement scheme as follows. Some uses A and B computes their public keys $Y_A = X_A N_{2\times2}^{x_A} X_A^{-1}$ and $Y_B = X_B N_{2\times2}^{x_B} X_B^{-1}$, where (X_A, x_A) is the private key of the user A and (X_B, x_B) is the private key of the user B. Then the first and second users compute the values K_{AB} and K_{BA}, correspondingly, as follows

$$K_{AB} = X_A Y_B^{x_A} X_A^{-1} = X_A \left(X_B N_{2\times2}^{x_B} X_B^{-1} \right)^{x_A} X_A^{-1} = X_A X_B N_{2\times2}^{x_B x_A} X_B^{-1} X_A^{-1}.$$

$$K_{BA} = X_B Y_A^{x_B} X_B^{-1} = X_B \left(X_A N_{2\times2}^{x_A} X_A^{-1} \right)^{x_B} X_B^{-1} = X_B X_A N_{2\times2}^{x_A x_B} X_A^{-1} X_B^{-1}.$$

In this scheme it is assumed that X_A and X_B are selected from some specified commutative subgroup $\Gamma_c \subset \Gamma \subset \mathbf{R}_{2\times2}$, therefore $K_{21} = K_{12} = K$, i.e., each of the users computes the same secret value K. Security of the described cryptoscheme is defined by difficulty of the HCSP over $\mathbf{R}_{2\times2}$, which cannot be reduced with attacks of the second type (note that the second type attacks cover the case of the fist attack described in Section 3).

5. Discussion and conclusion

Consideration of the multiplicative homomorphisms of the non-commutative finite rings $\mathbf{R} \supset \Gamma$ (or groups Γ) is an important item of the investigation of the difficulty of the HCSP defined over $\mathbf{R}$ (or over Γ), which relates to security estimation of the HCSP-based cryptoschemes. Using the matrices and vectors defined over the field $GF(p)$ for implementing the HCSP-based cryptoschemes is very attractive. In the case of matrices M the multiplicative homomorphism $\psi' : M \to \Delta_M$ is well known. A general multiplicative homomorphism ψ of the vector finite rings into $GF(p)$ have been described. If the ring of m-dimensional vectors represents the field $GF(p)$ [5] the homomorphism ψ coincide with the norm homomorphism, more detailed consideration of this fact is out of the scope of this paper though. In Section 3 the mentioned homomorphisms have been used in the first attack proposed against the HCSP-based cryptoschemes. To prevent this attack the condition for selecting parameters of the HCSP have been proposed.

The considered attacks of the second type relates to using hypothetic homomorphisms $\psi^{(s)} : \mathbf{R} \to GF(p^s)$, where $s \leqslant m$. These attacks are more powerful and cover the case of the first attack. While designing concrete cryptoschemes their parameters are selected depending on the order Ω of the multiplicative group Γ of the ring $\mathbf{R}$. In the case of matrices the formula describing the order Ω is known. However using the $m \times m$ matrices is limited by sufficiently small values m, since the size $|Y|$ of the public key Y increases approximately as $m^2|p|$, where $|p|$ denotes the size of p, and to provide the security of the HCSP-based cryptoschemes the order Ω should contain the prime divisor q having the size $|q| \geqslant 80$ bits. The value of q is limited by p^{m-1}, therefore $|q|(m-1)|p|$ and $|Y| \approx m^2(m-1)^{-1}|q|$ (the last holds for prime m; for composite m the increase of $|Y|$ is more significant).

In the case of the m-dimensional vectors the parameters of the ring $\mathbf{R}$ can be selected so that the secure size of the public key is approximately equal to $4|q| \approx 320$ bits for small $(m = 4)$ and large $(m = 8, 16, 32)$ values of m. Table 2 presents the comparison of the size of public key in the case of diferent dimensions of the matrices and vectors. Practical interest to use the large values m is connected with the fact that in the case of vectors the computational difficulty of the multiplication operation decreases significantly with increasing value of m. However construction of the non-commutative finite vector groups for large values of m relates to less investigated problem. Table 3 presents an example of the BVMT for the case $m = 8$. If structural coefficient $\tau \in GF(p)$ is such that equation $x^2 = \tau$ has no solution in $GF(p)$, then the order of the group Γ of eight-dimensional vectors, which is defined with this BVMT, contains divisor $p^2 + 1$. It is easy to generate values p such that $q = \left(p^2 + 1\right)/2$ is prime (for example, for $p = 307970789149$ and $\tau = 2$ we have $q = 47423003484528908072101$). Investigation of different variants of the vector groups Γ for $m = 6, 8, 12, 16, 20, 28, 32$ relates to a separate problem.

Elements of Γ	dimension	$\lvert p\rvert$, bits	$\lvert Y\rvert$, bits
matrices	2×2	80	320
matrices	3×3	40	360
matrices	4×4	40	640
matrices	5×5	20	500
matrices	6×6	20	720
matrices	7×7	14	686
vectors	4	80	320
vectors	8	40	320
vectors	16	21	336
vectors	32	11	352

Table 2. A rough estimation of the public-key size of the HCSP-based cryptoschemes possessing the 80-bit security.

$\circ$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$
$\mathbf{e}$	$\mathbf{e}$	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{k}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$
$\mathbf{i}$	$\mathbf{i}$	$-\mathbf{e}$	$\mathbf{k}$	$-\mathbf{j}$	$\mathbf{v}$	$-\mathbf{u}$	$\mathbf{x}$	$-\mathbf{w}$
$\mathbf{j}$	$\mathbf{j}$	$-\mathbf{k}$	$-\mathbf{e}$	$\mathbf{i}$	$\mathbf{w}$	$-\mathbf{x}$	$-\mathbf{u}$	$\mathbf{v}$
$\mathbf{k}$	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{i}$	$-\mathbf{e}$	$\mathbf{x}$	$\mathbf{w}$	$-\mathbf{v}$	$-\mathbf{u}$
$\mathbf{u}$	$\mathbf{u}$	$\mathbf{v}$	$\mathbf{w}$	$\mathbf{x}$	$\tau\mathbf{e}$	$\tau\mathbf{i}$	$\tau\mathbf{j}$	$\tau\mathbf{k}$
$\mathbf{v}$	$\mathbf{v}$	$-\mathbf{u}$	$\mathbf{x}$	$-\mathbf{w}$	$\tau\mathbf{i}$	$-\tau\mathbf{e}$	$\tau\mathbf{k}$	$-\tau\mathbf{j}$
$\mathbf{w}$	$\mathbf{w}$	$-\mathbf{x}$	$-\mathbf{u}$	$\mathbf{v}$	$\tau\mathbf{j}$	$-\tau\mathbf{k}$	$-\tau\mathbf{e}$	$\tau\mathbf{i}$
$\mathbf{x}$	$\mathbf{x}$	$\mathbf{w}$	$-\mathbf{v}$	$-\mathbf{u}$	$\tau\mathbf{k}$	$\tau\mathbf{j}$	$-\tau\mathbf{i}$	$-\tau\mathbf{e}$

Table 3. The basis-vector multiplication table for case $m = 8$.

References

[1] **D. Grigoriev, V. Shpilrain**, *Authentication from matrix conjugation*, Groups-Complexity-Cryptology **1** (2009), 199 – 205.

[2] **Ko Kihyoung, Lee Sangjin, Cha Jaechoon, Choi Dooho**, *Cryptosystems based on non-commutativity*, Patent Application # WO2001KR01283. Publication # WO03013052 (A1), February 13, 2003.

[3] **N. A. Moldovyan**, *Fast signatures based on non-cyclic finite groups*, Quasigroups and Related Systems **18** (2010), 83 – 94.

[4] **D. N. Moldovyan**, *Non-commutative finite groups as primitive of public-key cryptoschemes*, Quasigroups and Related Systems **18** (2010), 165 – 176.

[5] **N. A. Moldovyan, P. A. Moldovyanu**, *New primitives for digital signature algorithms: vector finite fields*, Quasigroups and Related Systems **17** (2009), 271 – 282.

[6] **P.W. Shor**, *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*, SIAM J. Computing. **26** (1997), 1484 – 1509.

Received January 18, 2010

St. Petersburg Institute for Informatics and Automation
Russian Academy of Sciences
14 Liniya, 39
St. Petersburg 199178
Russia
E-mails: nmold@mail.ru

Quasigroups and Related Systems **18** (2010), 187 – 194

Para-associative groupoids

Dumitru I. Pushkashu

Abstract. We study properties of left (right) division (cancellative) groupoids with associative-like identities: $x \cdot yz = zx \cdot y$ and $x \cdot zy = xy \cdot z$.

1. Introduction

A quasigroup can be defined as an algebra $(Q, \cdot)$ with one binary operation in which some equations are uniquely solvable or as an algebra $(Q, \cdot, \backslash, /)$ with three binary operations satisfying some identities. The first definition is motivated by Latin squares, the second – by universal algebras. In the case of quasigroups various connections between these three operations are well described.

In this note we describe connections between these three operations in para-associative division groupoids, i.e., left (right) division groupoids satisfying some identities similar to the associativity.

By the proving of many results given in this paper we have used Prover9-Mace4 prepared by W. McCune [7].

2. Basic facts and definitions

By a *binary groupoid* $(Q, \cdot)$ we mean a non-empty set Q together with a binary operation denoted by juxtaposition. Dots will be only used to avoid repetition of brackets. For example, the formula $((xy)(zy))(xz) = (xz)z$ will be written in the abbreviated form as $(xy \cdot zy) \cdot xz = xz \cdot z$. In this notion the associative law has the form

$$x \cdot yz = xy \cdot z. \tag{1}$$

2010 Mathematics Subject Classification: 20N02, 20N05
Keywords: groupoid, right division groupoid, left division groupoid, right cancellative groupoid, left cancellative groupoid, quasigroup, abelian group.

If we permute the arguments in each side of (1) we can obtain 16 new equations. Hosszú observed (see [5]) that all these equations can be reduced to one of the following four cases: (1),

$$x \cdot yz = z \cdot yx, \tag{2}$$

$$x \cdot yz = y \cdot xz, \tag{3}$$

$$x \cdot yz = zx \cdot y. \tag{4}$$

Unfortunately Hosszú gives only two examples of such reductions.

Example 2.1. The equation $yz \cdot x = yx \cdot z$ is equivalent to $x * (z * y) = z * (x * y)$, where $t * s = st$. □

Example 2.2. If in the identity

$$x \cdot zy = xy \cdot z \tag{5}$$

(called by Hosszú – *Tarki's associative law*) we put $z = x$ and replace xy by t, we obtain $xt = tx$. Hence, in groupoids $(Q, \cdot)$ in which each element $t \in Q$ can be written in the form xy, $x, y \in Q$, (5) implies each of the equations (1) – (4). □

M. A. Kazim and M. Naseeruddin considered in [6] the following laws:

$$xy \cdot z = zy \cdot x \tag{6}$$

$$x \cdot yz = z \cdot yx. \tag{7}$$

Groupoids satisfying (6) are called *left almost semigroups* (*LA-semigroups*), groupoids satisfying (7) are called *right almost semigroups* (*RA-semigroups*).

All these identities are strongly connected with para-associative rings. Namely, a non-associative ring R is *para-associative* of type (i, j, k) (cf. [2] or [4]) or an(i, j, k)-*associative ring*, if $x_1x_2 \cdot x_3 = x_i \cdot x_jx_k$ is valid for all $x_1, x_2, x_3 \in R$, where (i, j, k) is a fixed permutation of the set $\{1, 2, 3\}$.

As usual, the map $L_a : Q \to Q$, $L_ax = ax$ for all $x \in Q$, is a *left translation*, the map $R_a : Q \to Q$, $R_ax = xa$, is a *right translation*.

A groupoid $(Q, \cdot)$ is a *left cancellation groupoid*, if $ax = ay$ implies $x = y$ for all $a, x, y \in Q$, i.e., if L_a is an injective map for every $a \in Q$. Similarly, $(Q, \cdot)$ is a *right cancellation groupoid*, if $xa = ya$ implies $x = y$ for all $a, x, y \in G$, i.e., if R_a is an injective map for every $a \in Q$. A *cancellation groupoid* is a groupoid which is both a left and right cancellation groupoid.

By a *left division groupoid* (shortly: *ld-groupoid*) we mean a groupoid in which all left translations L_x are surjective. A *right division groupoid* (shortly: *rd-groupoid*) is a groupoid in which all right translations R_x are surjective. If all L_x and all R_x are surjective, then we say that such groupoid is a *division groupoid*.

Example 2.3. Let $(\mathbb{Z}, +, \cdot)$ be the ring of integers. Consider on $\mathbb{Z}$ two operations: $x \circ y = x + 3y$ and $x * y = [x/2] + 3y$. It is possible to check that $(\mathbb{Z}, \circ)$ is a left cancellation groupoid, $(\mathbb{Z}, *)$ is a left cancellation right division groupoid. $\square$

Definition 2.4. A groupoid $(Q, \circ)$ is called a *right quasigroup* (a *left quasigroup*) if, for all $a, b \in Q$, there exists a unique solution $x \in Q$ of the equation $x \circ a = b$ (respectively: $a \circ x = b$), i.e., if all right (left) translations of $(Q, \circ)$ are bijective maps of Q.

A groupoid which is a left and right quasigroup is called a *quasigroup*. A quasigroup with the identity is called a *loop*.

T. Evans [3] proved that a quasigroup $(Q, \cdot)$ can be considered as an equationally defined algebra. Namely, he proved

Theorem 2.5. *A groupoid $(Q, \cdot)$ is a quasigroup if and only if $(Q, \cdot, \backslash, /)$ is an algebra with three binary operations $\cdot$, $\backslash$ and $/$ satisfying the following four identities:*

$$x \cdot (x \backslash y) = y, \tag{8}$$

$$(y/x) \cdot x = y, \tag{9}$$

$$x \backslash (x \cdot y) = y, \tag{10}$$

$$(y \cdot x)/x = y. \tag{11}$$

Another characterization of quasigroups was given by G. Birkhoff in [1].

Theorem 2.6. *A groupoid $(Q, \cdot)$ is a quasigroup if and only if $(Q, \cdot, \backslash, /)$ is an algebra with three binary operations $\cdot$, $\backslash$ and $/$ satisfying the identities* $(8) - (11)$ *and*

$$(x/y) \backslash x = y, \tag{12}$$

$$y/(x \backslash y) = x. \tag{13}$$

In the case of groupoids connections between these three operations are described in [8] and [9]. Namely, the following theorem is true.

Theorem 2.7. *Let $(Q, \cdot)$ be an arbitrary groupoid. Then*

1. *$(Q, \cdot)$ is a left division groupoid if and only if there exists a left cancellation groupoid $(Q, \backslash)$ such that an algebra $(Q, \cdot, \backslash)$ satisfies* (8),
2. *$(Q, \cdot)$ is a right division groupoid if and only if there exists a right cancellation groupoid $(Q, /)$ such that an algebra $(Q, \cdot, /)$ satisfies* (9),
3. *$(Q, \cdot)$ is a left cancellation groupoid if and only if there exists a left division groupoid $(Q, \backslash)$ such that an algebra $(Q, \cdot, \backslash)$ satisfies* (10),
4. *$(Q, \cdot)$ is a right cancellation groupoid if and only if there exists a right division groupoid $(Q, /)$ such that an algebra $(Q, \cdot, /)$ satisfies* (11).

3. Cyclic associative law

In this section we study various groupoids satisfying the cyclic associative law (4).

Theorem 3.1. *A right division groupoid $(Q, \cdot, /)$ satisfying* (4) *is an associative and commutative division groupoid.*

Proof. By Theorem 2.7 such groupoid satisfies (9). Hence

$$yz \cdot (x/y) \overset{(4)}{=} z \cdot (x/y)y \overset{(9)}{=} zx.$$

Using just proved identity, we obtain

$$xy \cdot z \overset{(4)}{=} y \cdot zx = y \cdot (yz \cdot (x/y)) \overset{(4)}{=} (x/y)y \cdot yz \overset{(9)}{=} x \cdot yz,$$

which proves the associativity. Moreover, for all $x, y \in Q$ we have

$$xy \overset{(9)}{=} x \cdot (y/z)z \overset{(4)}{=} zx \cdot (y/z) \overset{(1)}{=} z \cdot x(y/z) \overset{(4)}{=} (y/z)z \cdot x \overset{(9)}{=} yx.$$

So, $(Q, \cdot)$ is associative and commutative division groupoid. □

Corollary 3.2. *A right cancellation rd-groupoid $(Q, \cdot, /)$ satisfying* (4) *is a commutative group with respect to the operation $\cdot$ and satisfies the identities* $(2) - (4)$.

Proof. By the previous theorem such groupoid is a commutative division groupoid. Since it also is a cancellation groupoid, it is a commutative group. Obviously it satisfies $(2) - (4)$. □

Theorem 3.3. *A left cancellation rd-groupoid* $(Q,\cdot,\backslash,/)$ *satisfying* (4) *is a commutative group with respect to the operation* $\cdot$ *and satisfies the identities* (2) – (4).

Proof. By Theorem 2.7 such groupoid satisfies (9) and (10). Hence

$$xy \overset{(9)}{=} (x/x)x \cdot y \overset{(4)}{=} x \cdot y(x/x).$$

from this we obtain $x\backslash(xy) = y(x/x)$, which, in view of (9), gives

$$y = y(x/x). \tag{14}$$

So, for all $x, y \in Q$, we have

$$y\backslash y = x/x \tag{15}$$

Thus

$$y \overset{(9)}{=} (y/y)y \overset{(15)}{=} (x\backslash x)y \overset{(15)}{=} (x/x)y.$$

This, together with (14), shows that $e = x/x = x\backslash x$ is the identity of $(Q,\cdot)$.

Since

$$xy = xy \cdot e \overset{(4)}{=} y \cdot ex = yx.$$

$(Q,\cdot)$ is a commutative loop. Hence $xy \cdot z = yx \cdot z = x \cdot zy = x \cdot yz$, which means that it is a commutative group. Obviously it satisfies (2) – (4). □

Theorem 3.4. *A left division groupoid* $(Q,\cdot,\backslash)$ *satisfying* (4) *is a commutative division groupoid.*

Proof. By Theorem 2.7, such groupoid satisfies (8). Hence

$$zx \overset{(8)}{=} y(y\backslash z) \cdot x \overset{(4)}{=} (y\backslash z) \cdot xy.$$

Using just proved identity, we obtain

$$x \cdot yz \overset{(4)}{=} zx \cdot y = ((y\backslash z) \cdot xy) \cdot y \overset{(4)}{=} xy \cdot y(y\backslash z) \overset{(8)}{=} xy \cdot z,$$

which proves the associativity. Moreover, for all $x, y \in Q$ we have

$$xy \overset{(8)}{=} z(z\backslash x) \cdot y \overset{(4)}{=} (z\backslash x) \cdot yz \overset{(1)}{=} (z\backslash x)y \cdot z \overset{(4)}{=} y \cdot z(z\backslash x) \overset{(8)}{=} yx.$$

So, $(Q,\cdot)$ is associative and commutative division groupoid. □

Corollary 3.5. *A left cancellation ld-groupoid* $(Q, \cdot, \backslash)$ *satisfying* (4) *is a commutative group with respect to the operation* $\cdot$ *and satisfies the identities* (2) – (4).

Proof. By the previous theorem such groupoid is a commutative division groupoid. Since it also is a cancellation groupoid, it is a commutative group. Obviously it satisfies the identities (2) – (4). □

Theorem 3.6. *A right cancellation ld-groupoid* $(Q, \cdot, \backslash, /)$ *satisfying* (4) *is a commutative group with respect to the operation* $\cdot$ *and satisfies the identities* (2) – (4).

Proof. The proof is very similar to the proof of Theorem 3.3. □

4. Groupods in which x·zy = xy·z

Lemma 4.1. *A left division groupoid* $(Q, \cdot, \backslash)$ *satisfying* (5) *is commutative and associative.*

Proof. By Theorem 2.7 such groupoid satisfies (8). Hence

$$xy \stackrel{(8)}{=} y(y\backslash x) \cdot y \stackrel{(5)}{=} y \cdot y(y\backslash x) \stackrel{(8)}{=} yx$$

for all $x, y \in Q$. The associativity is obvious. □

Theorem 4.2. *A left cancellation ld-groupoid* $(Q, \cdot, \backslash)$ *satisfying* (5) *is a commutative group with the identity* $e = x\backslash x$ *and satisfies* (2) – (4).

Proof. Indeed, $xy \stackrel{(8)}{=} x(x\backslash x) \cdot y \stackrel{(5)}{=} x \cdot y(x\backslash x)$, which implies $y = y(x\backslash x)$. □

Corollary 4.3. *In a right cancellation ld-groupoid* $(Q, \cdot, \backslash, /)$ *satisfying* (5) *we have* $x\backslash y = y/x$ *for all* $x, y \in Q$.

Proof. By Lemma 4.1 such groupoid is commutative. Hence $y = xz = zx$ implies $x\backslash y = y/x$. □

Theorem 4.4. *A right cancellation ld-groupoid* $(Q, \cdot, \backslash, /)$ *satisfying* (5) *is a commutative group with respect to the operation* $\cdot$ *and satisfies the identities* (2) – (4).

Proof. By Lemma 4.1 such groupoid is associative and commutative. Hence it also is left cancellative. Theorem 4.2 completes the proof. □

Lemma 4.5. *A left cancellation groupoid* $(Q,\cdot,\backslash)$ *satisfying* (5) *is associative and commutative.*

Proof. In fact, using (5), we obtain

$$u(xy\cdot z)=uz\cdot xy=(uz\cdot y)x=(u\cdot yz)x=u(x\cdot yz).$$

This, by the left cancellativity, implies the associativity. Therefore,

$$x\cdot yz=xy\cdot z\overset{(5)}{=}x\cdot zy,$$

which shows that $(Q,\cdot)$ is also commutative. □

Theorem 4.6. *A left cancellation rd-groupoid* $(Q,\cdot,\backslash)$ *satisfying* (5) *is a commutative group with respect to the operation* $\cdot$ *and satisfies the identities* (2) – (4).

Proof. By Lemma 4.5 such groupoid is commutative. Hence it is a left division groupoid, too. Theorem 4.2 completes the proof. □

Theorem 4.7. *A right division groupoid* $(Q,\cdot,/)$ *satisfying* (5) *is associative and satisfies the identity* $x(y/y)=x$.

Proof. By Theorem 2.7 it satisfies (9). Hence

$$y\overset{(9)}{=}(x/y)y\overset{(9)}{=}(x/y)\cdot(y/y)y\overset{(5)}{=}(x/y)y\cdot(y/y)\overset{(9)}{=}x(y/y).$$

Let $e=y/y$. Then $xe=x$ for every $x\in Q$ and

$$xy\cdot z=(xy\cdot z)e\overset{(5)}{=}xy\cdot ez\overset{(5)}{=}x(ez\cdot y)\overset{(5)}{=}x(e\cdot yz)\overset{(5)}{=}(x\cdot yz)e=x\cdot yz,$$

which completes the proof. □

Note that a right cancellation rd-groupoid satisfying (5) may not be a group. A non-empty set Q with the multiplication defined by $xy=x$ is a simple example of a non-commutative right cancellation rd-groupoid without two-sided identity.

Acknowledgment: The author thanks to V. A. Shcherbacov for their useful comments and suggestions.

References

[1] **G. Birkhoff**, *Lattice Theory*, AMS Colloquium Publ., Providence, 1967.

[2] **I. M. Dudek**, *On ternary semigroups connected with para-associative rings*, Ricerche di Mat. **35** (1986), 191 – 203.

[3] **T. Evans**, *On multiplicative systems defined by generators and relations*, Math. Proc. Camb. Phil. Soc. **47** (1951), 637 – 649.

[4] **B. Gleichgewicht**, *Para-associative rings and algebras*, (Russian), Acta Univ. Wratislaviensis **58** (1967), 21 – 35.

[5] **M. Hosszú**, *Some functional equations related with the associative law*, Publ. Math. Debrecen **3** (1954), 205 – 214.

[6] **M. A. Kazim and M. Naseeruddin**, *On almost-semigroups*, The Alig Bull. Math. **2** (1972), 1 – 7.

[7] **W. McCune**, *Prover9 and Mace4*, University of New Mexico, 2005-2010. www.cs.unm.edu/∼mccune/prover9/

[8] **V. A. Shcherbacov**, *On definitions of groupoids closely connected with quasigroups*, Bul. Acad. Stiinte Repub. Mold., Mat. **2** (2007), 43 – 54.

[9] **V. A. Shcherbacov, A. Kh. Tabarov and D. I. Pushkashu**, *On congruences of groupoids closely connected with quasigroups*, Fundam. Prikl. Mat. **14** (2008), 237 – 251.

Received July 22, 2010
Revised November 26, 2010

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str.
Chişinău MD−2028
Moldova
E-mail: dpuscasu@math.md

Quasigroups and Related Systems **18** (2010), 195 − 212

Hemirings characterized by the properties of their fuzzy ideals with thresholds

Muhammad Shabir and *Tahir Mahmood*

Abstract. We define fuzzy h-subhemiring, fuzzy h-ideals and fuzzy generalized h-bi-ideals with thresholds, and characterize h-hemiregular and h-intra-hemiregular hemirings by the properties of their fuzzy h-ideals, fuzzy h-bi-ideals and fuzzy h-quasi-ideals with thresholds.

1. Introduction

Semirings are algebraic structures with two binary operations, introduced by Vandiver [23]. In more recent times semirings have been deeply studied, especially in relation with applications [10]. Semirings have also been used for studying optimization, graph theory, theory of discrete event, dynamical systems, matrices, determinants, generalized fuzzy computation, theory of automata, formal language theory, coding theory, analysis of computer programmes [9, 24]. Hemirings, which are semirings with commutative addition and zero element, appears in a natural manner, in some applications to the theory of automata, the theory of formal languages and in computer sciences [10, 19]

Ideals of hemirings and semirings play a central role in the structure theory and are useful for many purposes. However, in general, they do not coincide with the usual ring ideals. Many results in rings apparantly have no analogues in hemirings using only ideals. In [11] Henriksen defined a more restricted class of ideals in semirings, called k-ideals, with the property that if the semiring R is the ring, then a complex in R is a k-ideal if and only if it is a ring ideal. Another more restricted, but very important, class of ideals in hemirings, called now h-ideals, has been given and investigated by

2010 Mathematics Subject Classification: 16Y99, 16D25, 08A72
Keywords: hemiring, fuzzy h-ideal, h-hemiregular.
The first author is thankful to Quaid-i-Azam University for providing University Research Fund (DFNS/10-49) for this work.

Izuka [12] and La Torre [16].

The theory of fuzzy sets was first developed by Zadeh [26] in 1965, and has been applied to many branches in Mathematics. The fuzzification of algebraic structures was initiated by Rosenfeld [22] and he introduced the notion of fuzzy subgroups. In [3] J. Ahsan initiated the study of fuzzy semirings(See also [2]), fuzzy k-ideals in semirings are studied in [8], and fuzzy h-ideals are studied in [13, 17, 27]. The fuzzy algebraic structures play an important role in mathematics with wide applications in many other branches such as theoretical physics, computer sciences, control engineering, information sciences, coding theory and topological spaces [1, 10, 24].

The notions of "belongingness" and "quasicoincidence" of fuzzy points and fuzzy sets proposed and discussed in [20, 21]. Many authors used these concepts to generalize some concepts of algebra, for example [4, 5, 6, 14]. In [7, 18] (α, β)-fuzzy ideals of hemirings are defined.

In this paper we define fuzzy h-subhemiring, fuzzy h-ideal and fuzzy generalized h-bi-ideals with thresholds, and characterize h-hemiregular and h-intra-hemiregular hemiring by the properties of their fuzzy h-ideals, fuzzy h-bi-ideals, fuzzy generalized h-bi-ideals, fuzzy h-quasi-ideals with thresholds.

2. Preliminaries

A *semiring* is a set $R \neq \emptyset$ together with two binary operations addition and multiplication such that $(R, +)$ and $(R, \cdot)$ are semigroups and both algebraic structures are connected by the distributive laws:

$$a\,(b+c) = ab + ac \qquad \text{and} \qquad (a+b)\,c = ac + bc$$

for all $a, b, c \in R$.

An element $0 \in R$ is called a *zero* of the semiring $(R, +, \cdot)$ if $0x = x0 = 0$ and $0 + x = x + 0 = x$ for all $x \in R$. An additively commutative semiring with zero is called a *hemiring*. An element 1 of a hemiring R is called the *identity* of R if $1x = x1 = x$ for all $x \in R$. A hemiring with commutative multiplication is called a *commutative hemiring*. A non-empty subset A of a hemiring R is called a *subhemiring* of R if it contains zero and is closed with respect to the addition and multiplication of R. A non-empty subset I of a hemiring R is called a *left* (*right*) *ideal* of R if I is closed under addition and $RI \subseteq I$ ($IR \subseteq I$). A non-empty subset I of a hemiring R is called an *ideal* of R if it is both a left ideal and a right ideal of R. A non-empty subset

Q of a hemiring R is called a *quasi-ideal* of R if Q is closed under addition and $RQ \cap QR \subseteq Q$. A subhemiring B of a hemiring R is called a *bi-ideal* of R if $BSB \subseteq B$. Every one sided ideal of a hemiring R is a quasi-ideal and every quasi-ideal is a bi-ideal but the converse is not true.

A left (right) ideal I of a hemiring R is called a *left* (*right*) *h-ideal* if for all $x, z \in R$ and for any $a, b \in I$ from $x + a + z = b + z$ it follows $x \in I$. A bi-ideal B of a hemiring R is called an *h-bi-ideal* of R if for all $x, z \in R$ and $a, b \in B$ from $x + a + z = b + z$ it follows $x \in B$ [25].

The *h-closure* $\overline{A}$ of a non-empty subset A of a hemiring R is defined as

$$\overline{A} = \{x \in R \mid x + a + z = b + z \text{ for some } a, b \in A, z \in R\}.$$

A quasi-ideal Q of a hemiring R is called an *h-quasi-ideal* of R if $\overline{RQ} \cap \overline{QR} \subseteq Q$ and $x + a + z = b + z$ implies $x \in Q$, for all $x, z \in R$ and $a, b \in Q$ [25]. Every left (right) h-ideal of a hemiring R is an h-quasi-ideal of R and every h-quasi-ideal is an h-bi-ideal of R. However, the converse is not true in general.

A fuzzy subset f of a universe X is a function from X into the unit closed interval $[0, 1]$, that is $f : X \to [0, 1]$. A fuzzy subset f in a universe X of the form

$$f(y) = \begin{cases} t \in (0,1] & \text{if } y = x \\ 0 & \text{if } y \neq x \end{cases}$$

is said to be a *fuzzy point* with support x and value t and is denoted by x_t. For a fuzzy point x_t and a fuzzy set f in a set X, Pu and Liu [21] gave meaning to the symbol $x_t \alpha f$, where $\alpha \in \{\in, q, \in \vee q, \in \wedge q\}$. A fuzzy point x_t is said to belong to (resp. quasi-coincident with) a fuzzy set f written $x_t \in f$ (resp. $x_t q f$) if $f(x) \geqslant t$ (resp. $f(x) + t > 1$), and in this case, $x_t \in \vee q f$ (resp. $x_t \in \wedge q f$) means that $x_t \in f$ or $x_t q f$ (resp. $x_t \in f$ and $x_t q f$). To say that $x_t \overline{\alpha} f$ means that $x_t \alpha f$ does not hold. Let f be a fuzzy subset of R and $t \in (0, 1]$ then the set $U(f; t) = \{x \in R : f(x) \geqslant t\}$ is called the *level subset* of R. For any two fuzzy subsets f and g of X, $f \leqslant g$ means that, for all $x \in X$, $f(x) \leqslant g(x)$. The symbols $f \wedge g$, and $f \vee g$ will mean the following fuzzy subsets of X

$$(f \wedge g)(x) = \min\{f(x), g(x)\}, \qquad (f \vee g)(x) = \max\{f(x), g(x)\}$$

for all $x \in X$. More generally, if $\{f_i : i \in \Lambda\}$ is a family of fuzzy subsets of X, then $\wedge_{i \in \Lambda} f_i$ and $\vee_{i \in \Lambda} f_i$ are defined by

$$(\bigwedge_{i \in \Lambda} f_i)(x) = \min_{i \in \Lambda}\{f_i(x)\}, \qquad (\bigvee_{i \in \Lambda} f_i)(x) = \max_{i \in \Lambda}\{f_i(x)\}$$

and are called the *intersection* and the *union* of the family $\{f_i : i \in \Lambda\}$ of fuzzy subsets of X, respectively.

Definition 2.1. Let f and g be two fuzzy subsets in a hemiring R. The *h-intrinsic product* of f and g is defined by

$$(f \odot g)(x) = \sup\left\{ \bigwedge_{i=1}^{m} \big(f(a_i) \wedge g(b_i)\big) \wedge \bigwedge_{j=1}^{n} \big(f(a_j') \wedge g(b_j')\big) \right\}$$

if $x \in R$ can be expressed as $x+\Sigma_{i=1}^{m} a_i b_i + z = \Sigma_{j=1}^{n} a_j' b_j' + z$, and 0 otherwise.

Proposition 2.2. [25] *Let R be a hemiring and f, g, h, k be any fuzzy subsets of R. If $f \leqslant g$ and $h \leqslant k$, then $f \odot h \leqslant g \odot k$.* □

Lemma 2.3. [25] *Let R be a hemiring and $A, B \subseteq R$. Then we have*
(i) $A \subseteq B \Leftrightarrow \chi_A \leqslant \chi_B$,
(ii) $\chi_A \wedge \chi_B = \chi_{A \cap B}$,
(iii) $\chi_A \odot \chi_B = \chi_{\overline{AB}}$. □

Definition 2.4. A fuzzy subset f in a hemiring R is called a *fuzzy h-sub-hemiring* of R if for all $x, y, z, a, b \in R$ we have
(i) $f(x+y) \geqslant \min\{f(x), f(y)\}$,
(ii) $f(xy) \geqslant \min\{f(x), f(y)\}$,
(iii) $x+a+z = b+z \Rightarrow f(x) \geqslant \min\{f(a), f(b)\}$.

Definition 2.5. A fuzzy subset f in a hemiring R is called a *fuzzy left (right) h-ideal* of R if for all $x, y, z, a, b \in R$ we have
(i) $f(x+y) \geqslant \min\{f(x), f(y)\}$,
(ii) $f(xy) \geqslant f(y) \quad (f(xy) \geqslant f(x))$,
(iii) $x+a+z = b+z \Rightarrow f(x) \geqslant \min\{f(a), f(b)\}$.

A fuzzy subset f of R is called a *fuzzy h-ideal* of R if it is both a fuzzy left and a fuzzy right h-ideal of R.

Definition 2.6. [25] A fuzzy subset f in a hemiring R is called a *fuzzy h-bi-ideal* of R if for all $x, y, z, a, b \in R$ we have
(i) $f(x+y) \geqslant \min\{f(x), f(y)\}$,
(ii) $f(xy) \geqslant \min\{f(x), f(y)\}$,
(iii) $f(xyz) \geqslant \min\{f(x), f(z)\}$,
(iv) $x+a+z = b+z \Rightarrow f(x) \geqslant \min\{f(a), f(b)\}$.

Definition 2.7. [25] A fuzzy subset f in a hemiring R is called a *fuzzy h-quasi-ideal* of R if for all $x, y, z, a, b \in R$ we have

(i) $f(x+y) \geqslant \min\{f(x), f(y)\}$,

(ii) $(f \odot \mathcal{R}) \wedge (\mathcal{R} \odot f) \leqslant f$,

(iii) $x + a + z = b + z \Rightarrow f(x) \geqslant \min\{f(a), f(b)\}$,

where $\mathcal{R}$ is the fuzzy subset of R mapping every element of R on 1.

Note that if f is a fuzzy left h-ideal (right h-ideal, h-bi-ideal, h-quasi-ideal), then $f(0) \geqslant f(x)$ for all $x \in R$.

Definition 2.8. [25] A hemiring R is said to be *h-hemiregular* if for each $x \in R$, there exist $a, b, z \in R$ such that $x + xax + z = xbx + z$.

Lemma 2.9. [25] *A hemiring R is h-hemiregular if and only if for any right h-ideal I and any left h-ideal L of R we have $\overline{IL} = I \cap L$.* □

Definition 2.10. [25] A hemiring R is said to be *h-intra-hemiregular* if for each $x \in R$, there exist $a_i, a_i', b_j, b_j', z \in R$ such that $x + \sum_{i=1}^{m} a_i x^2 a_i' + z = \sum_{j=i}^{n} b_j x^2 b_j' + z$.

Lemma 2.11. [25] *A hemiring R is h-intra-hemiregular if and only if for any right h-ideal I and any left h-ideal L of R we have $I \cap L \subseteq \overline{LI}$.* □

Lemma 2.12. [25] *The following conditions are equivalent.*

(i) *R is both h-hemiregular and h-intra-hemiregular hemiring,*

(ii) *$B = \overline{B^2}$ for every h-bi-ideal B of R,*

(iii) *$Q = \overline{Q^2}$ for every h-quasi-ideal Q of R.* □

3. Fuzzy ideals with thresholds (α, β)

In this section we will discuss fuzzy h-subhemiring, fuzzy h-ideals, fuzzy h-bi-ideals, fuzzy generalized h-bi-ideals and fuzzy h-quasi-ideals with thresholds (α, β) of a hemiring R.

Definition 3.1. Let $\alpha, \beta \in (0, 1]$ and $\alpha < \beta$. Then a fuzzy subset f of a hemiring R is called a *fuzzy h-subhemiring with thresholds* (α, β) of R if it satisfies

(1) $\max\{f(x+y), \alpha\} \geqslant \min\{f(x), f(y), \beta\}$,

(2) $\max\{f(xy), \alpha\} \geqslant \min\{f(x), f(y), \beta\}$,

(3) $x + a + z = b + z \Rightarrow \max\{f(x), \alpha\} \geqslant \min\{f(a), f(b), \beta\}$

for all $x, y, z, a, b \in R$.

Definition 3.2. Let $\alpha, \beta \in (0,1]$ and $\alpha < \beta$. Then a fuzzy subset f of a hemiring R is called a *fuzzy left* (resp. *right*) *h-ideal with thresholds* (α, β) of R if it satisfies $(1), (3)$ and

(4) $\max\{f(xy), \alpha\} \geqslant \min\{f(y), \beta\}$

(resp. $\max\{f(xy), \alpha\} \geqslant \min\{f(x), \beta\}$)

for all $x, y \in R$.

A fuzzy subset f of a hemiring R is called a *fuzzy h-ideal with thresholds* (α, β) of R if it is both fuzzy left and fuzzy right h-ideal with thresholds (α, β) of R.

Definition 3.3. [18] Let $\alpha, \beta \in (0,1]$ and $\alpha < \beta$. Then a fuzzy subset f of a hemiring R is called a *fuzzy h-bi-ideal with thresholds* (α, β) of R if it satisfies $(1), (2), (3)$ and

(5) $\max\{f(xzy), \alpha\} \geqslant \min\{f(x), f(y), \beta\}$

for all $x, y, z, \in R$.

Definition 3.4. Let $\alpha, \beta \in (0,1]$ and $\alpha < \beta$. Then a fuzzy subset f of a hemiring R is called a *fuzzy generalized h-bi-ideal with thresholds* (α, β) of R if it satisfies (3) and (5).

Definition 3.5. [18] Let $\alpha, \beta \in (0,1]$ and $\alpha < \beta$. Then a fuzzy subset f of a hemiring R is called fuzzy h-quasi-ideal with thresholds (α, β) of R if it satisfies (1), (3) and

(6) $\max\{f(x), \alpha\} \geqslant \min\{(f \odot \mathcal{R})(x), (\mathcal{R} \odot f)(x), \beta\}$

for all $x \in R$, where $\mathcal{R}$ is the fuzzy subset of R mapping every element of R into 1.

As a simple consequence of the Transfer Principle for fuzzy sets proved in [15] we obtain

Theorem 3.6. *A fuzzy subset f of a hemiring R is a fuzzy h-subhemiring with thresholds (α, β) of R if and only if $U(f;t) \neq \emptyset$ is h-subhemiring of R for all $t \in (\alpha, \beta)$.* □

Theorem 3.7. *A fuzzy subset f of a hemiring R is a fuzzy left h-ideal (right h-ideal, h-ideal, generalized h-bi-ideal, h-bi-ideal, h-quasi-ideal) with thresholds (α, β) of R if and only if $U(f;t) \neq \emptyset$ is a left h-ideal (right h-ideal, h-ideal, generalized h-bi-ideal, h-bi-ideal, h-quasi-ideal) of R for all $t \in (\alpha, \beta)$.* □

Theorem 3.8. *A non-empty subset A of a hemiring R is h-ideal (h-bi-ideal, generalized h-bi-ideal, h-quasi-ideal) of R if and only if the characteristic function χ_A is fuzzy h-ideal (h-bi-ideal, generalized h-bi-ideal, h-quasi-ideal) of R with thresholds (α, β) of R for all $\alpha, \beta \in (0, 1]$ and $\alpha < \beta$.* □

Theorem 3.9. *Let f be a fuzzy h-bi-ideal with thresholds (α, β) of R , then $f \wedge \beta$ is fuzzy h-bi-ideal with thresholds (α, β) of R.*

Proof. Let $a, b, x, y, z \in R$. Then $(f \wedge \beta)(x) = f(x) \wedge \beta$ for all $x \in R$ and

$$\begin{aligned}\max\{(f \wedge \beta)(x+y), \alpha\} &= \max\{f(x+y) \wedge \beta, \alpha\} \\ &= \min\{\max\{f(x+y), \alpha\}, \beta\} \geqslant \min\{f(x), f(y), \beta\} \\ &= \min\{(f \wedge \beta)(x), (f \wedge \beta)(y), \beta\}.\end{aligned}$$

Similarly we can show that

$$\max\{(f \wedge \beta)(xy), \alpha\} \geqslant \min\{(f \wedge \beta)(x), (f \wedge \beta)(y), \beta\} \quad \text{and}$$
$$\max\{(f \wedge \beta)(xzy), \alpha\} \geqslant \min\{(f \wedge \beta)(x), (f \wedge \beta)(y), \beta\}.$$

Now let $x + a + z = b + z$, then

$$\begin{aligned}\max\{(f \wedge \beta)(x), \alpha\} &= \max\{f(x) \wedge \beta, \alpha\} = \min\{\max(f(x), \alpha), \beta\} \\ &\geqslant \min\{f(a), f(b), \beta\} = \min\{(f \wedge \beta)(a), (f \wedge \beta)(b), \beta\}\end{aligned}$$

This shows that $f \wedge \beta$ is a fuzzy h-bi-ideal with thresholds (α, β) of R. □

Similarly we can show:

Theorem 3.10. *Let f be a fuzzy h-bi-ideal (h-subhemiring, generalized h-bi-ideal, h-ideal, h-quasi-ideal) with thresholds (α, β) of R, then $f \wedge \beta$ is a fuzzy h-bi-ideal (h-subhemiring, generalized h-bi-ideal, h-ideal, h-quasi-ideal) with thresholds (α, β) of R.* □

Definition 3.11. Let f, g be fuzzy subsets of a hemiring R. Then for all $\in R$ we define

$$(f \wedge_\alpha^\beta g)(x) = \{(f \wedge g)(x) \wedge \beta\} \vee \alpha,$$
$$(f \vee_\alpha^\beta g)(x) = \{(f \vee g)(x) \wedge \beta\} \vee \alpha,$$
$$(f \odot_\alpha^\beta g)(x) = \{(f \odot g)(x) \wedge \beta\} \vee \alpha,$$
$$(f +_\alpha^\beta g)(x) = (\sup\{f(a_1) \wedge f(a_2) \wedge g(b_1) \wedge g(b_2)\} \wedge \beta) \vee \alpha$$

for all possible expressions of x in the form $x + (a_1 + b_1) + z = (a_2 + b_2) + z$.

Lemma 3.12. *Let A, B be subsets of R, then*

$$(\chi_A +_\alpha^\beta \chi_B)(x) = (\chi_{\overline{A+B}}(x) \wedge \beta) \vee \alpha.$$

Proof. Let A, B be subsets of a hemiring R and $x \in R$. If $x \in \overline{A+B}$ then there exist $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $x+(a_1+b_1)+z = (a_2+b_2)+z$ for some $z \in R$. Thus

$$\begin{aligned}(\chi_A +_\alpha^\beta \chi_B)(x) &= (\sup\{\chi_A(a_1') \wedge \chi_A(a_2') \wedge \chi_B(b_1') \wedge \chi_B(b_2')\} \wedge \beta) \vee \alpha \\ &= (1 \wedge \beta) \vee \alpha = (\chi_{\overline{A+B}}(x) \wedge \beta) \vee \alpha.\end{aligned}$$

If $x \notin \overline{A+B}$ then there do not exist $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $x + (a_1 + b_1) + z = (a_2 + b_2) + z$ for some $z \in R$. Thus $(\chi_A +_\alpha^\beta \chi_B)(x) = (0 \wedge \beta) \vee \alpha = (\chi_{\overline{A+B}}(x) \wedge \beta) \vee \alpha$. Hence $(\chi_A +_\alpha^\beta \chi_B)(x) = (\chi_{\overline{A+B}}(x) \wedge \beta) \vee \alpha$. □

Lemma 3.13. *A fuzzy subset f of a hemiring R satisfies* (1) *and* (3) *if and only if it satisfies*

(7) $f +_\alpha^\beta f \leqslant (f \wedge \beta) \vee \alpha$.

Proof. Let f satisfies (1), (3) and $x + (a_1 + b_1) + z = (a_2 + b_2) + z$ for some $a_1, a_2, b_1, b_2, z \in R$. Then

$$\begin{aligned}(f +_\alpha^\beta f)(x) &= (\sup\{f(a_1) \wedge f(a_2) \wedge f(b_1) \wedge f(b_2)\} \wedge \beta) \vee \alpha \\ &= (\sup\{(f(a_1) \wedge f(b_1) \wedge \beta) \wedge (f(a_2) \wedge f(b_2) \wedge \beta)\} \wedge \beta) \vee \alpha \\ &\leqslant (\sup\{(f(a_1 + b_1) \vee \alpha) \wedge (f(a_2 + b_2) \vee \alpha)\} \wedge \beta) \vee \alpha \\ &= (\sup\{\{f(a_1 + b_1) \wedge f(a_2 + b_2)\} \vee \alpha\} \wedge \beta) \vee \alpha \\ &= (\sup\{f(a_1 + b_1) \wedge f(a_2 + b_2) \wedge \beta\} \vee \alpha) \vee \alpha \\ &= (\sup\{f(a_1 + b_1) \wedge f(a_2 + b_2) \wedge \beta\} \wedge \beta) \vee \alpha \\ &\leqslant ((f(x) \vee \alpha) \wedge \beta) \vee \alpha \\ &= (f(x) \wedge \beta) \vee \alpha.\end{aligned}$$

Thus $f +_\alpha^\beta f \leqslant (f \wedge \beta) \vee \alpha$.

Conversely, assume that $(f +_\alpha^\beta f)(x) \leqslant (f \wedge \beta)(x) \vee \alpha$. Then for each $x, z \in R$ we have $0 + x + x + z = x + x + z$. Hence

$$\begin{aligned}f(0) \vee \alpha \geqslant (f \wedge \beta)(0) \vee \alpha &\geqslant (f +_\alpha^\beta f)(0) \\ &= (\sup\{f(a_1) \wedge f(a_2) \wedge f(b_1) \wedge f(b_2)\} \wedge \beta) \vee \alpha \\ &\geqslant \sup\{f(a_1) \wedge f(a_2) \wedge f(b_1) \wedge f(b_2)\} \wedge \beta \geqslant f(x) \wedge \beta.\end{aligned}$$

This means that for all $x \in R$ we have

$$f(0) \vee \alpha \geqslant f(x) \wedge \beta. \qquad (*)$$

Let $x, y \in R$. Then for all $a_1, a_2, b_1, b_2, z \in R$ such that $(x + y) + (a_1 + b_1) + z = (a_2 + b_2) + z$, we have

$$\begin{aligned}\max\{f(x + y), \alpha\} \geqslant \max\{(f \wedge \beta)(x + y), \alpha\} &\geqslant (f +_\alpha^\beta f)(x + y) \\ &= (\sup\{f(a_1) \wedge f(a_2) \wedge f(b_1) \wedge f(b_2)\} \wedge \beta) \vee \alpha \\ &\geqslant (\{f(0) \wedge f(x) \wedge f(0) \wedge f(y)\} \wedge \beta) \vee \alpha,\end{aligned}$$

because $(x + y) + (0 + 0) + 0 = (x + y) + 0$.

From the above using($*$) we get $\max\{f(x+y),\alpha\} \geqslant \min\{f(x),f(y),\beta\}$, which proves (1).

Now let $a,b,x,z \in R$ be such that $x+a+z=b+z$. Then for all possible $a_1,a_2,b_1,b_2,z \in R$ satisfying the identity $x+(a_1+b_1)+z=(a_2+b_2)+z$ we have

$$\begin{aligned}\max\{f(x),\alpha\} \geqslant \max\{(f\wedge\beta)(x),\alpha\} &\geqslant (f +_\alpha^\beta f)(x)\\ &= (\sup\{f(a_1)\wedge f(a_2)\wedge f(b_1)\wedge f(b_2)\}\wedge\beta)\vee\alpha\\ &\geqslant f(a)\wedge f(b)\wedge\beta \qquad \text{because } x+a+z=b+z\\ &= \min\{f(a),f(b),\beta\}.\end{aligned}$$

Thus f satisfies (3). □

Theorem 3.14. *A fuzzy subset f of a hemiring R is a fuzzy left* (*resp. right*) *h-ideal with thresholds* (α,β) *of R if and only if it satisfies* (7) *and*

(8) $\mathcal{R}\odot_\alpha^\beta f \leqslant (f\wedge\beta)\vee\alpha$ (*resp.* $f\odot_\alpha^\beta \mathcal{R} \leqslant (f\wedge\beta)\vee\alpha$).

Proof. Suppose f is a fuzzy left h-ideal with thresholds (α,β) of a hemiring R, then by Lemma 3.13, f satisfies (7). Now we show that f satisfies (8). Let $x\in R$. If $(\mathcal{R}\odot_\alpha^\beta f)(x)=0$, then $\mathcal{R}\odot_\alpha^\beta f \leqslant (f\wedge\beta)\vee\alpha$. Otherwise, there exist elements $a_i,b_i,c_j,d_j,z\in R$ such that $x+\sum_{i=1}^m a_ib_i+z=\sum_{j=1}^n c_jd_j+z$. Thus

$$\begin{aligned}(\mathcal{R}\odot_\alpha^\beta f)(x) &= \Big(\sup\Big\{\bigwedge_{i=1}^m\Big(\mathcal{R}(a_i)\wedge f(b_i)\Big)\wedge\bigwedge_{j=1}^n\Big(\mathcal{R}(a_j')\wedge f(b_j')\Big)\Big\}\wedge\beta\Big)\vee\alpha\\ &= \Big(\sup\Big\{\bigwedge_{i=1}^m f(b_i)\wedge\bigwedge_{j=1}^n f(b_j')\Big\}\wedge\beta\Big)\vee\alpha\\ &= \Big(\sup\Big\{\Big(\bigwedge_{i=1}^m f(b_i)\wedge\beta\Big)\wedge\Big(\bigwedge_{j=1}^n f(b_j')\wedge\beta\Big)\Big\}\wedge\beta\Big)\vee\alpha\\ &\leqslant \Big(\sup\Big\{\bigwedge_{i=1}^m\Big(f(a_ib_i)\vee\alpha\Big)\wedge\bigwedge_{j=1}^n\Big(f(a_j'b_j')\vee\alpha\Big)\Big\}\wedge\beta\Big)\vee\alpha\\ &= \Big(\sup\Big\{\Big(\bigwedge_{i=1}^m f(a_ib_i)\wedge\beta\Big)\wedge\Big(\bigwedge_{j=1}^n f(a_j'b_j')\wedge\beta\Big)\Big\}\wedge\beta\Big)\vee\alpha\\ &\leqslant \Big(\sup\Big\{\Big(f\big(\textstyle\sum_{i=1}^m a_ib_i\big)\vee\alpha\Big)\wedge\Big(f\big(\textstyle\sum_{j=1}^n a_j'b_j'\big)\vee\alpha\Big)\Big\}\wedge\beta\Big)\vee\alpha\\ &\leqslant (f(x)\wedge\beta)\vee\alpha.\end{aligned}$$

This implies that $\mathcal{R}\odot_\alpha^\beta f \leqslant (f\wedge\beta)\vee\alpha$.

Conversely, assume that f satisfies (7) and (8). Then, by Lemma 3.13, it satisfies (1) and (3). To show that f satisfies (4) let $x,y\in R$ and $a_i,b_i,c_j,d_j,z\in R$ be such that $xy+\sum_{i=1}^m a_ib_i+z=\sum_{j=1}^n c_jd_j+z$. Then we have

$$f(xy)\vee\alpha \geqslant (f(xy)\wedge\beta)\vee\alpha \geqslant (\mathcal{R}\odot_\alpha^\beta f)(xy)$$

$$= \left(\sup \left\{ \bigwedge_{i=1}^{m} \left(\mathcal{R}(a_i) \wedge f(b_i) \right) \wedge \bigwedge_{j=1}^{n} \left(\mathcal{R}(c_j) \wedge f(d_j) \right) \right\} \wedge \beta \right) \vee \alpha$$
$$= \left(\sup \left\{ \bigwedge_{i=1}^{m} f(b_i) \wedge \bigwedge_{j=1}^{n} f(d_j) \right\} \wedge \beta \right) \vee \alpha$$
$$\geqslant (f(y) \wedge \beta) \vee \alpha \geqslant f(y) \wedge \beta$$

because $xy + 0y + z = xy + z$.

This shows that f satisfies (4). So f is a fuzzy left h-ideal with thresholds (α, β) of R.

For fuzzy right h-ideals the proof is similar. □

Theorem 3.15. *A fuzzy subset f of a hemiring R is a fuzzy h-quasi-ideal with thresholds (α, β) of R if and only if f satisfies (6) and (7).*

Proof. Proof is straightforward because by Lemma 3.13, (1) and (3) are equivalent to (7). □

Theorem 3.16. *Every fuzzy left h-ideal with thresholds (α, β) of a hemiring R is a fuzzy h-quasi-ideal with thresholds (α, β) of R.*

Proof. Proof is straightforward because (8) implies (6). □

Theorem 3.17. *Every fuzzy h-quasi-ideal with thresholds (α, β) of R is a fuzzy h-bi-ideal with thresholds (α, β) of R.* □

Lemma 3.18. *If f and g are fuzzy right and left h-ideals with thresholds (α, β) of R respectively, then $f \odot_\alpha^\beta g \leqslant f \wedge_\alpha^\beta g$.*

Proof. Let $x \in R$. If $(f \odot_\alpha^\beta g)(x) = \alpha$, then $f \odot_\alpha^\beta g \leqslant f \wedge_\alpha^\beta g$. Otherwise, there exist elements $a_i, b_i, c_j, d_j, z \in R$ such that $x + \sum_{i=1}^{m} a_i b_i + z = \sum_{j=1}^{n} c_j d_j + z$. Then for all such expressions we have

$$(f \odot_\alpha^\beta g)(x) = \left(\sup \left\{ \bigwedge_{i=1}^{m} \left(f(a_i) \wedge g(b_i) \right) \wedge \bigwedge_{j=1}^{n} \left(f(a_j') \wedge g(b_j') \right) \right\} \wedge \beta \right) \vee \alpha$$
$$= \left(\sup \left\{ \begin{array}{l} \bigwedge_{i=1}^{m} \left\{ \left(f(a_i) \wedge \beta \right) \wedge \left(g(b_i) \wedge \beta \right) \right\} \wedge \\ \bigwedge_{j=1}^{n} \left\{ \left(f(a_j') \wedge \beta \right) \wedge \left(g(b_j') \wedge \beta \right) \right\} \end{array} \right\} \wedge \beta \right) \vee \alpha$$
$$\leqslant \left(\sup \left\{ \begin{array}{l} \bigwedge_{i=1}^{m} \left\{ \left(f(a_i b_i) \vee \alpha \right) \wedge \left(g(a_i b_i) \vee \alpha \right) \right\} \wedge \\ \bigwedge_{j=1}^{n} \left\{ \left(f(a_j' b_j') \vee \alpha \right) \wedge \left(g(a_j' b_j') \vee \alpha \right) \right\} \end{array} \right\} \wedge \beta \right) \vee \alpha$$

$$= \left(\sup \left\{ \begin{array}{l} \bigwedge\limits_{i=1}^{m} \left\{ \Big(f\left(a_i b_i\right) \wedge \beta \Big) \wedge \Big(g\left(a_i b_i\right) \wedge \beta \Big) \right\} \wedge \\ \bigwedge\limits_{j=1}^{n} \left\{ \Big(f(a'_j b'_j) \wedge \beta \Big) \wedge \Big(g(a'_j b'_j) \wedge \beta \Big) \right\} \end{array} \right\} \wedge \beta \right) \vee \alpha$$

$$\leqslant \left(\sup \left\{ \max \left\{ \begin{array}{l} f(\sum_{i=1}^{m} a_i b_i), g(\sum_{i=1}^{m} a_i b_i), \\ f(\sum_{j=1}^{n} a'_j b'_j), g(\sum_{j=1}^{n} a'_j b'_j), \alpha \end{array} \right\} \right\} \wedge \beta \right) \vee \alpha$$

$$\leqslant (f \wedge_\alpha^\beta g)(x),$$

because $\min\{f(x), f(y), \beta\} \leqslant \{f(x+y, \alpha)\}$. □

4. h-hemiregular hemirings

In this section we characterize h-hemiregular hemirings by the properties of their h-ideals, h-quasi-ideals and h-bi-ideals with thresholds (α, β).

Theorem 4.1. *For a hemiring R the following conditions are equivalent:*

(i) *R is h-hemiregular,*

(ii) *$f \wedge_\alpha^\beta g = f \odot_\alpha^\beta g$ for every fuzzy right and left h-ideals f and g with thresholds (α, β) of R, respectively.*

Proof. $(i) \Rightarrow (ii)$ Let $x \in R$, then there exists $a, a', z \in R$ such that $x + xax + z = xa'x + z$. Now for all $x, a_i, b_i, c_j, d_j, z \in R$ such that $x + \sum_{i=1}^{m} a_i b_i + z = \sum_{j=1}^{n} c_j d_j + z$, we have

$$(f \odot_\alpha^\beta g)(x) = \Big(\sup \Big\{ \bigwedge_{i=1}^{m} \Big(f\left(a_i\right) \wedge g\left(b_i\right) \Big) \wedge \bigwedge_{j=1}^{n} \Big(f(a'_j) \wedge g(b'_j) \Big) \Big\} \wedge \beta \Big) \vee \alpha$$

$$\geqslant (f(xa) \wedge f(xa') \wedge g(x) \wedge \beta) \vee \alpha \geqslant (f(x) \wedge g(x) \wedge \beta) \vee \alpha = (f \wedge_\alpha^\beta g)(x)$$

because $x + xax + z = xa'x + z$.

Thus $(f \odot_\alpha^\beta g)(x) \geqslant (f \wedge_\alpha^\beta g)(x)$. But by Lemma 3.18, $(f \odot_\alpha^\beta g)(x) \leqslant (f \wedge_\alpha^\beta g)(x)$, hence $f \wedge_\alpha^\beta g = f \odot_\alpha^\beta g$.

$(ii) \Rightarrow (i)$ Let A and B be right and left h-ideals of R,respectively. Then by Theorem 3.8, χ_A is fuzzy right and χ_B is fuzzy left h-ideal with thresholds (α, β) of R. By hypothesis $\chi_A \odot_\alpha^\beta \chi_B = \chi_A \wedge_\alpha^\beta \chi_B$ implies $(\chi_{\overline{AB}} \wedge \beta) \vee \alpha = (\chi_{A \cap B} \wedge \beta) \vee \alpha$. Hence $A \cap B = \overline{AB}$. So, R is h-hemiregular. □

Lemma 4.2. [25] *Let R be a hemiring. Then the following conditions are equivalent:*

(i) *R is h-hemiregular,*

(ii) *$B = \overline{BRB}$ for every h-bi-ideal B of R,*

(iii) *$Q = \overline{QRQ}$ for every h-quasi-ideal Q of R.* □

Theorem 4.3. *For a hemiring R, the following conditions are equivalent:*

(i) *R is h-hemiregular,*

(ii) $(f \wedge \beta) \vee \alpha \leqslant (f \odot_{\alpha}^{\beta} \mathcal{R} \odot_{\alpha}^{\beta} f)$ *for every fuzzy h-bi-ideal f with thresholds (α, β) of R,*

(iii) $(f \wedge \beta) \vee \alpha \leqslant (f \odot_{\alpha}^{\beta} \mathcal{R} \odot_{\alpha}^{\beta} f)$ *for every fuzzy h-quasi-ideal f with thresholds (α, β) of R.*

Proof. $(i) \Rightarrow (ii)$ Let $x \in R$, then there exists $a, a', z \in R$ such that $x + xax + z = xa'x + z$. Now for all $x, a_i, b_i, c_j, d_j, z \in R$ such that $x + \sum_{i=1}^{m} a_i b_i + z = \sum_{j=1}^{n} c_j d_j + z$, we have

$$(f \odot_{\alpha}^{\beta} \mathcal{R} \odot_{\alpha}^{\beta} f)(x) =$$

$$= \left(\sup \left\{ \begin{array}{c} \bigwedge_{i=1}^{m} \left\{ (f \odot_{\alpha}^{\beta} \mathcal{R})(a_i) \wedge f(b_i) \right\} \wedge \\ \bigwedge_{j=1}^{n} \left\{ (f \odot_{\alpha}^{\beta} \mathcal{R})(a'_j) \wedge f(b'_j) \right\} \end{array} \right\} \wedge \beta \right) \vee \alpha$$

$$\geqslant \left(\left\{ (f \odot_{\alpha}^{\beta} \mathcal{R})(xa) \wedge (f \odot_{\alpha}^{\beta} \mathcal{R})(xa') \wedge f(x) \right\} \wedge \beta \right) \vee \alpha$$

$$= \left(\left\{ \begin{array}{c} \bigwedge_{i=1}^{m} \left(\left(\sup \left\{ \bigwedge_{i=1}^{m} f(a_i) \wedge \bigwedge_{j=1}^{n} f(a'_j) \right\} \wedge \beta \right) \vee \alpha \right) \wedge \\ \bigwedge_{j=1}^{n} \left(\left(\sup \left\{ \bigwedge_{i=1}^{m} f(a_i) \wedge \bigwedge_{j=1}^{n} f(a'_j) \right\} \wedge \beta \right) \vee \alpha \right) \wedge f(x) \end{array} \right\} \wedge \beta \right) \vee \alpha$$

$$\geqslant \left(\left\{ \begin{array}{c} \{(\min\{f(xax), f(xa'x)\} \wedge \beta) \vee \alpha\} \wedge \\ \{(\min\{f(xax), f(xa'x)\} \wedge \beta) \vee \alpha\} \end{array} \right\} \wedge \beta \right\} \vee \alpha \geqslant (f(x) \wedge \beta) \vee \alpha$$

since $xa + xaxa + za = xa'xa + za$ and $xa' + xaxa' + za' = xa'xa' + za'$.

$(ii) \Rightarrow (iii)$ This is straightforward.

$(iii) \Rightarrow (i)$ Let Q be any h-quasi ideal of R, then by Theorem 3.8, χ_Q is h-quasi-ideal with thresholds (α, β) o R.

Now by the given condition $(\chi_Q \wedge \beta) \vee \alpha \leqslant (\chi_Q \odot_{\alpha}^{\beta} \mathcal{R} \odot_{\alpha}^{\beta} \chi_Q) = \chi_{\overline{QRQ}}$ implies $Q \subseteq \overline{QRQ}$. Also $\overline{QRQ} \subseteq \overline{RQ} \cap \overline{QR} = Q$. Thus$Q = \overline{QRQ}$. Therefore, by Lemma 4.2, R is h-hemiregular. □

Theorem 4.4. *For a hemiring R, the following conditions are equivalent:*

(i) *R is h-hemiregular,*

(ii) $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g \odot_{\alpha}^{\beta} f$ *for every fuzzy h-bi-ideal f and fuzzy h-ideal g with thresholds (α, β) of R,*

(iii) $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g \odot_{\alpha}^{\beta} f$ *for every fuzzy h-quasi-ideal f and fuzzy h-ideal g with thresholds (α, β) of R.*

Proof. $(i) \Rightarrow (ii)$ Let f be any fuzzy h-bi-ideal and g any fuzzy h-ideal with thresholds (α, β) of R. Since R is h-hemiregular, so for any $a \in R$

there exist $x_1, x_2, z \in R$ such that $a + ax_1a + z = ax_2a + z$. Now for all $a, a_i, b_i, c_j, d_j, z \in R$ such that $a + \sum_{i=1}^{m} a_ib_i + z = \sum_{j=1}^{n} c_jd_j + z$, we have

$$\left(f \odot_\alpha^\beta g \odot_\alpha^\beta f\right)(a) = \left[\sup\left\{\begin{array}{c}\bigwedge\limits_{i=1}^{m}\left(\left(f \odot_\alpha^\beta g\right)(a_i) \wedge f(b_i)\right) \wedge \\ \bigwedge\limits_{j=1}^{n}\left(\left(f \odot_\alpha^\beta g\right)(a'_j) \wedge f(b'_j)\right)\end{array}\right\} \wedge \beta\right] \vee \alpha$$

$$\geqslant \left(\{(f \odot_\alpha^\beta g)(ax_1) \wedge f(a) \wedge (f \odot_\alpha^\beta g)(ax_2)\} \wedge \beta\right) \vee \alpha$$

because $a + ax_1a + z = ax_2a + z$

$$= \left(\left[\begin{array}{l}\left\{\left[\sup\left\{\begin{array}{c}\bigwedge\limits_{i=1}^{m}\left(f(c_i) \wedge g(d_i)\right) \wedge \\ \bigwedge\limits_{j=1}^{n}\left(f(c'_j) \wedge g(d'_j)\right)\end{array}\right\} \wedge \beta\right] \vee \alpha\right\} \wedge f(a) \\ \left\{\left[\sup\left\{\begin{array}{c}\bigwedge\limits_{i=1}^{m}\left(f(p_i) \wedge g(q_i)\right) \wedge \\ \bigwedge\limits_{j=1}^{n}\left(f(p'_j) \wedge g(q'_j)\right)\end{array}\right\} \wedge \beta\right] \vee \alpha\right\}\end{array}\right] \wedge \beta\right) \vee \alpha$$

for all possible expressions $ax_1 + \Sigma_{i=1}^{m} c_id_j + z = \Sigma_{j=1}^{n} c'_jd'_j + z$ and $ax_2 + \Sigma_{i=1}^{m} pq_i + z = \Sigma_{j=1}^{n} p'_jq'_j + z$

$$\geqslant \{f(a) \wedge g(x_1ax_1) \wedge g(x_1ax_2) \wedge g(x_2ax_1) \wedge g(x_2ax_2) \wedge \beta\} \vee \alpha$$

$$\geqslant \{f(a) \wedge g(a) \wedge \beta\} \vee \alpha = (f \wedge_\alpha^\beta g)(a)$$

because $ax_1 + ax_1ax_1 + zx_1 = ax_2ax_1 + zx_1$ and $ax_2 + ax_1ax_2 + zx_2 = ax_2ax_2 + zx_2$.

$(ii) \Rightarrow (iii)$ is straightforward.

$(iii) \Rightarrow (i)$ Let f be fuzzy h-quasi-ideal and $\mathcal{R}$ be fuzzy h-ideal with thresholds (α, β) *of* R. Then by hypothesis, $f \wedge_\alpha^\beta \mathcal{R} \leqslant f \odot_\alpha^\beta \mathcal{R} \odot_\alpha^\beta f$ implies $(f \wedge \beta) \vee \alpha \leqslant f \odot_\alpha^\beta \mathcal{R} \odot_\alpha^\beta f$. Then, by Theorem 4.3, R is h-hemiregular. □

Theorem 4.5. *For a hemiring R, the following conditions are equivalent:*

(i) *R is h-hemiregular,*

(ii) *$f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for every fuzzy h-bi-ideal f and fuzzy left h-ideal g with thresholds (α, β) of R,*

(iii) *$f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for every fuzzy h-quasi-ideal f and fuzzy left h-ideal g with thresholds (α, β) of R,*

(iv) *$f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for every fuzzy right h-ideal f and fuzzy h-bi-ideal g with thresholds (α, β) of R,*

(v) *$f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for every fuzzy right h-ideal f and fuzzy h-quasi-ideal g with thresholds (α, β) of R,*

(vi) $f \wedge_{\alpha}^{\beta} g \wedge_{\alpha}^{\beta} h \leqslant f \odot_{\alpha}^{\beta} g \odot_{\alpha}^{\beta} h$ *for every fuzzy right h-ideal f, fuzzy h-bi-ideal g and fuzzy left h-ideal h with thresholds (α, β) of R,*

(vii) $f \wedge_{\alpha}^{\beta} g \wedge_{\alpha}^{\beta} h \leqslant f \odot_{\alpha}^{\beta} g \odot_{\alpha}^{\beta} h$ *for every fuzzy right h-ideal f, fuzzy h-quasi-ideal g and fuzzy left h-ideal h with thresholds (α, β) of R.*

Proof. $(i) \Rightarrow (ii)$ Let f be any fuzzy h-bi-ideal and g any fuzzy left h-ideal with thresholds (α, β) of R. Since R is h-hemiregular, so for any $a \in R$ there exist $x_1, x_2, z \in R$ such that $a + ax_1a + z = ax_2a + z$. Now for all $a, a_i, b_i, c_j, d_j, z \in R$ such that $a + \sum_{i=1}^{m} a_ib_i + z = \sum_{j=1}^{n} c_jd_j + z$, we have

$$
\begin{aligned}
&(f \odot_{\alpha}^{\beta} g)(a) = \\
&= \Big(\sup \Big\{ \bigwedge_{i=1}^{m} \Big(f(a_i) \wedge g(b_i) \Big) \wedge \bigwedge_{j=1}^{n} \Big(f(a_j') \wedge g(b_j') \Big) \Big\} \wedge \beta \Big) \vee \alpha \\
&\geqslant (\{ f\,(a) \wedge g\,(x_1a) \wedge g\,(x_2a) \} \wedge \beta) \vee \alpha \quad \text{because } a+ax_1a+z = ax_2a+z \\
&\geqslant (\{ f\,(a) \wedge g\,(a) \} \wedge \beta) \vee \alpha = (f \wedge_{\alpha}^{\beta} g)(a).
\end{aligned}
$$

So, $f \odot_{\alpha}^{\beta} g \geqslant f \wedge_{\alpha}^{\beta} g$.

$(ii) \Rightarrow (iii)$ is straightforward.

$(iii) \Rightarrow (i)$ Let f be any fuzzy right h-ideal and g be any fuzzy left h-ideal with thresholds (α, β) of R. Since every fuzzy right h-ideal with thresholds (α, β) is fuzzy h-quasi-ideal with thresholds (α, β), so by (iii) we have $f \odot_{\alpha}^{\beta} g \geqslant f \wedge_{\alpha}^{\beta} g$. But by Lemma 3.18, $f \odot_{\alpha}^{\beta} g \leqslant f \wedge_{\alpha}^{\beta} g$. Hence $f \odot_{\alpha}^{\beta} g = f \wedge_{\alpha}^{\beta} g$ for every fuzzy right h-ideal f with thresholds (α, β) of R, and for every fuzzy left h-ideal g with thresholds (α, β) of R. Thus by Theorem 4.1, R is h-hemiregular.

Similarly we can show that $(i) \Leftrightarrow (iv) \Leftrightarrow (v)$.

$(i) \Rightarrow (vi)$ Let f be a fuzzy right h-ideal, g be a fuzzy h-bi-ideal and h be a fuzzy left h-ideal with thresholds (α, β) of R. Since R is h-hemiregular, so for any $a \in R$ there exist $x_1, x_2, z \in R$ such that $a + ax_1a + z = ax_2a + z$. Now for all $a, a_i, b_i, c_j, d_j, z \in R$ such that $a + \sum_{i=1}^{m} a_ib_i + z = \sum_{j=1}^{n} c_jd_j + z$, we have

$$
\begin{aligned}
&(f \odot_{\alpha}^{\beta} g \odot_{\alpha}^{\beta} h)(a) = \\
&= \Big(\sup \Big\{ \bigwedge_{i=1}^{m} \Big((f \odot_{\alpha}^{\beta} g)(a_i) \wedge h(b_i) \Big) \wedge \bigwedge_{j=1}^{n} \Big((f \odot_{\alpha}^{\beta} g)(a_j') \wedge h(b_j') \Big) \Big\} \wedge \beta \Big) \vee \alpha \\
&\geqslant (\{ (f \odot_{\alpha}^{\beta} g)(a) \wedge h(x_1a) \wedge h(x_2a) \} \wedge \beta) \vee \alpha \\
&\geqslant \Big(\Big\{ \Big(\sup \Big\{ \bigwedge_{i=1}^{m} \Big(f(a_i) \wedge g(b_i) \Big) \wedge \bigwedge_{j=1}^{n} \Big(f(a_j') \wedge g(b_j') \Big) \Big\} \wedge \beta \Big) \vee \alpha \Big\} \wedge h(x_1a) \wedge h(x_2a) \wedge \beta \Big) \vee \alpha \\
&\geqslant (f(ax_1) \wedge f(ax_2) \wedge g(a) \wedge h(x_1a) \wedge h(x_2a) \wedge \beta) \vee \alpha \\
&\geqslant (f(a) \wedge g(a) \wedge h(a) \wedge \beta) \vee \alpha = (f \wedge_{\alpha}^{\beta} g \wedge_{\alpha}^{\beta} h)(a).
\end{aligned}
$$

$(vi) \Rightarrow (vii)$ is straightforward.

$(vii) \Rightarrow (i)$ Let f be a fuzzy right h-ideal, and h be a fuzzy left h-ideal with thresholds (α, β) of R. Then

$$f \wedge_\alpha^\beta h = f \wedge_\alpha^\beta \mathcal{R} \wedge_\alpha^\beta h \leqslant f \odot_\alpha^\beta \mathcal{R} \odot_\alpha^\beta h \leqslant f \odot_\alpha^\beta h.$$

But $f \odot_\alpha^\beta h \leqslant f \wedge_\alpha^\beta h$ always. Hence $f \odot_\alpha^\beta h = f \wedge_\alpha^\beta h$ for every fuzzy right h-ideal f and for every fuzzy left h-ideal h with thresholds (α, β) of R. Thus by Theorem 4.1, R is h-hemiregular. □

5. h-intra-hemiregular hemirings

In this section we characterize h-intra-hemiregular hemirings and hemirings which are both h-hemiregular and h-intra-hemiregular in terms of their fuzzy ideals with thresholds (α, β).

Theorem 5.1. *A hemiring R is h-intra-hemiregular if and only if $f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for every fuzzy left h-ideal f and for every fuzzy right h-ideal g with thresholds (α, β) of R.*

Proof. Let R be an h-intra-hemiregular and f be a fuzzy left h-ideal and g a fuzzy right h-ideal with thresholds (α, β) of R. As R is h-intra-hemiregular so for every $x \in R$, there exist $a_i, a_i', b_j, b_j', z \in R$ such that $x + \sum_{i=1}^m a_i x^2 a_i' + z = \sum_{j=1}^n b_j x^2 b_j' + z$. Then

$$\begin{aligned}(f \odot_\alpha^\beta g)(x) &= \Big(\sup\Big\{\bigwedge_{i=1}^m f(a_i) \wedge \bigwedge_{i=1}^m g(b_i) \wedge \bigwedge_{j=1}^n f(a_j') \wedge \bigwedge_{j=1}^n g(b_j')\Big\} \wedge \beta\Big) \vee \alpha \\ &\geqslant \Big(f(a_i x) \wedge f(b_j x) \wedge g(x a_i') \wedge g(x b_j') \wedge \beta\Big) \vee \alpha,\end{aligned}$$

because $x + \sum_{i=1}^m (a_i x)(x a_i') + z = \sum_{j=1}^n (b_j x)(x b_j') + z$.

Conversely assume that A and B are left and right h-ideals of R, respectively. Then, by Theorem 3.8, the characteristic functions $\chi_A$and χ_B are respectively fuzzy left h-ideal and fuzzy right h-ideal with thresholds (α, β). Then by hypothesis $\chi_A \wedge_\alpha^\beta \chi_B \leqslant \chi_A \odot_\alpha^\beta \chi_B$ implies $(\chi_{A\cap B} \wedge \beta) \vee \alpha \leqslant (\chi_{\overline{AB}} \wedge \beta) \vee \alpha$. Hence $A \cap B \subseteq \overline{AB}$. Thus, by Lemma 2.11, R is h-intra-hemiregular. □

Theorem 5.2. *The following conditions are equivalent for a hemiring R:*

(i) *R is both h-hemiregular and h-intra-hemiregular,*

(ii) *$(f \wedge \beta) \vee \alpha = f \odot_\alpha^\beta f$ for every fuzzy h-bi-ideal f with thresholds (α, β) of R,*

(iii) *$(f \wedge \beta) \vee \alpha = f \odot_\alpha^\beta f$ for every fuzzy h-quasi-ideal f with thresholds (α, β) of R.*

Proof. $(i) \Rightarrow (ii)$ Let f be a fuzzy h-bi-ideal with thresholds (α, β) of R and $x \in R$. Since R is both h-hemiregular and h-intra-hemiregular, there exist elements $a_1, a_2, p_i, p_i', q_j, q_j', z \in R$ such that

$$x+\sum_{j=1}^{n}(xa_2q_jx)(xq_j'a_1x)+\sum_{j=1}^{n}(xa_1q_jx)(xq_j'a_2x)+\sum_{i=1}^{m}(xa_1p_ix)(xp_i'a_1x) +\sum_{i=1}^{m}(xa_2p_ix)(xp_i'a_2x)+z=\sum_{i=1}^{m}(xa_2p_ix)(xp_i'a_1x)+\sum_{i=1}^{m}(xa_1p_ix)(xp_i'a_2x) +\sum_{j=1}^{n}(xa_1q_jx)(xq_j'a_1x)+\sum_{j=1}^{n}(xa_2q_jx)(xq_j'a_2x)+z$$

(cf. Lemma 5.6 in [25]).

$$\begin{aligned} f\odot_\alpha^\beta f(x) &= \left(\sup\left\{\bigwedge_{i=1}^{m}\Big(f(a_i)\wedge f(b_i)\Big)\wedge\bigwedge_{j=1}^{n}\Big(f(a_j')\wedge f(b_j')\Big)\right\}\wedge\beta\right)\vee\alpha \\ &\geqslant \left(\begin{array}{l}\bigwedge_{j=1}^{n}\Big(f(xa_2q_jx)\wedge f(xq_j'a_1x)\wedge f(xa_1q_jx)\wedge f(xq_j'a_2x)\Big)\wedge \\ \bigwedge_{i=1}^{m}\Big(f(xa_1p_ix)\wedge f(xp_i'a_1x)\wedge f(xa_2p_ix)\wedge f(xp_i'a_2x)\Big)\wedge\beta\end{array}\right)\vee\alpha \\ &\geqslant (\{(f(x)\wedge\beta)\vee\alpha\}\wedge\beta)\vee\alpha = (f(x)\wedge\beta)\vee\alpha. \end{aligned}$$

This implies that $f \odot_\alpha^\beta f \geqslant (f\wedge\beta)\vee\alpha$

On the other hand, if $x + \Sigma_{i=1}^{m} a_ib_i + z = \Sigma_{j=1}^{n} a_j'b_j' + z$, we have

$$\begin{aligned} (f(x)\wedge\beta)\vee\alpha &= ((f(x)\wedge\beta)\vee\alpha)\vee\alpha = ((f(x)\vee\alpha)\wedge\beta)\vee\alpha \\ &\geqslant (f(\Sigma_{i=1}^{m}a_ib_i)\wedge f(\Sigma_{j=1}^{n}a_j'b_j')\wedge\beta)\vee\alpha \qquad \text{by (3)} \\ &\geqslant \Big(\bigwedge_{i=1}^{m} f(a_ib_i)\wedge\bigwedge_{j=1}^{n} f(a_j'b_j')\wedge\beta\Big)\vee\alpha \\ &\geqslant \Big(\bigwedge_{i=1}^{m}\Big(f(a_i)\wedge f(b_i)\Big)\wedge\bigwedge_{i=1}^{m}\Big(f(a_i)\wedge f(b_i)\Big)\wedge\beta\Big)\vee\alpha. \end{aligned}$$

Thus

$$\begin{aligned} (f\odot_\alpha^\beta f)(x) &= \left(\sup\left\{\bigwedge_{i=1}^{m}\Big(f(a_i)\wedge f(b_i)\Big)\wedge\bigwedge_{j=1}^{n}\Big(f(a_j')\wedge f(b_j')\Big)\right\}\wedge\beta\right)\vee\alpha \\ &\leqslant (f(x)\wedge\beta)\vee\alpha. \end{aligned}$$

Consequently $f \odot_\alpha^\beta f = (f\wedge\beta)\vee\alpha$.

$(ii) \Rightarrow (iii)$ Obvious.

$(iii) \Rightarrow (i)$ Let Q be an h-quasi-ideal of R. Then χ_Q is a fuzzy h-quasi-ideal with thresholds (α, β) of R. Thus by hypothesis

$$[\chi_Q\wedge\beta]\vee\alpha = \chi_Q\odot_\alpha^\beta\chi_Q = [\chi_Q\odot\chi_Q\wedge\beta]\vee\alpha = [\chi_{\overline{Q^2}}\wedge\beta]\vee\alpha.$$

Then it follows $Q = \overline{Q^2}$. Hence by Lemma 2.12, R is both h-hemiregular and h-intra-hemiregular. □

Theorem 5.3. *The following conditions are equivalent for a hemiring R:*

(i) *R is both h-hemiregular and h-intra-hemiregular,*

(ii) *$f \wedge_\alpha^\beta g \leqslant f \odot_\alpha^\beta g$ for all fuzzy h-bi-ideals f and g with thresholds (α, β) of R,* (*iii*) $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g$ *for every fuzzy h-bi-ideal f and every fuzzy h-quasi-ideals f with thresholds* (α, β) *of R,*

(*iv*) $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g$ *for every fuzzy h-quasi-ideal f and every fuzzy h-bi-ideals f with thresholds* (α, β) *of R,*

(*v*) $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g$ *for all fuzzy h-quasi-ideals f and g with thresholds* (α, β) *of R.*

Proof. $(i) \Rightarrow (ii)$ Analogously as in previous proof.

$(ii) \Rightarrow (iii) \Rightarrow (v)$ and $(ii) \Rightarrow (iv) \Rightarrow (v)$ are straightforward.

$(v) \Rightarrow (i)$ Let f be a fuzzy left h-ideal and g be a fuzzy right h-ideal with thresholds (α, β) of R. Then f and g are fuzzy h-bi-ideals with thresholds (α, β) of R. So by hypothesis $f \wedge_{\alpha}^{\beta} g \leqslant f \odot_{\alpha}^{\beta} g$ but $f \wedge_{\alpha}^{\beta} g \geqslant f \odot_{\alpha}^{\beta} g$ by Lemma 3.18. Thus $f \wedge_{\alpha}^{\beta} g = f \odot_{\alpha}^{\beta} g$. Hence by Theorem 4.1, R is h-hemiregular. On the other hand by hypothesis we also have $f \wedge_{\alpha}^{\beta} g \leqslant g \odot_{\alpha}^{\beta} f$. By Theorem 5.1, R is h-intra-hemiregular. □

References

[1] **A. W. Aho and J. D. Ullman**, *Introduction to automata theory, languages and computation*, Addison Wesley, Reading, MA, 1979.

[2] **J. Ahsan**, *Semirings characterized by their fuzzy ideals*, J. Fuzzy Math. **6** (1998), 181 – 192.

[3] **J. Ahsan, K. Saifullah and M. F. Khan**, *Fuzzy semirings*, Fuzzy Sets Syst. **60** (1993), 309 – 320.

[4] **S. K. Bhakat**, $(\in \vee q)$*-level subset*, Fuzzy Sets Syst. **103** (1999), 529 – 533.

[5] **S. K. Bhakat and P. Das**, *Fuzzy subrings and ideals redefined*, Fuzzy Sets Syst. **81** (1996), 383 – 393.

[6] **B. Davvaz**, $(\in, \in \vee q)$*-fuzzy subnearrings and ideals*, Soft Comput. **10** (2006), 206 – 211.

[7] **W. A. Dudek, M. Shabir and M. Irfan Ali**, (α, β)*-fuzzy ideals of hemirings*, Comput. Math. Appl. **58** (2009), 310 – 321.

[8] **S. Ghosh**, *Fuzzy k-ideals of semirings*, Fuzzy Sets Syst. **95** (1998), 103 – 108.

[9] **K. Glazek**, *A guide to litrature on semirings and their applications in mathematics and information sciences: with complete bibliography*, Kluwer Acad. Publ. Nederland, 2002.

[10] **J. S. Golan**, *Semirings and their applications*, Kluwer Acad. Publ. 1999.

[11] **M. Henriksen**, *Ideals in semirings with commutative addition*, Amer. Math. Soc. Notices **6** (1958), 321.

[12] **K. Iizuka**, *On Jacobson radical of a semiring*, Tohoku Math. J. **11** (1959), 409 – 421.

[13] **Y. B. Jun, M. A. Özürk and S. Z. Song**, *On fuzzy h-ideals in hemirings*, Inform. Sci. **162** (2004), 211 – 226.

[14] **Y. B. Jun and S. Z. Song**, *Generalized fuzzy interior ideals in semigroups*, Inform. Sci. **176** (2006), 3079 – 3093.

[15] **M. Kondo and W. A. dudek**: On the transfer principle in fuzzy theory, Mathware and Soft Computing **12** (2005), 41 – 55.

[16] **D. R. La Torre**, *On h-ideals and k-ideals in hemirings*, Publ. Math. (Debrecen) **12** (1965), 219 – 226.

[17] **X. Ma and J. Zhan**, *On fuzzy h-ideals of hemirings*, J. Syst. Sci. Complexity **20** (2007), 470 – 478.

[18] **X. Ma and J. Zhan**, *Generalized fuzzy h-bi-ideals and h-quasi-ideals of hemirings*, Inform. Sci. **179** (2009), 1249 – 1268.

[19] **J. N. Mordeson and D. S. Malik**, *Fuzzy automata and languages, theory and applications*, Computational Math. Series, Chapman and Hall/CRC, Boca Raton 2002.

[20] **V. Murali**, *Fuzzy points of equivalent fuzzy subsets*, Inform. Sci. **158** (2004), 277 – 288.

[21] **P. M Pu and Y. M. Liu**, *Fuzzy topology I, neighborhood structure of a fuzzy point and Moore-Smith convergence*, J. Math. Anal. Appl. **76** (1980), 571 – 599.

[22] **A. Rosenfeld**, *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[23] **H.S. Vandiver**, *Note on a simple type of algebra in which cancellation law of addition does not hold*, Bull. Amer. Math. Soc. **40** (1934), 914 – 920.

[24] **W. Wechler**, *The concept of fuzziness in automata and language theory*, Akademic verlog, Berlin, 1978.

[25] **Y. Yin and H. Li**, *The charatecrizations of h-hemiregular hemirings and h-intra-hemiregular hemirings*, Inform. Sci. **178** (2008), 3451 – 3464.

[26] **L. A. Zadeh**, *Fuzzy sets*, Information and Control **8** (1965), 338 – 353.

[27] **J. Zhan and W. A. Dudek**, *Fuzzy h-ideals of hemirings*, Inform. Sci. **177** (2007), 876 – 886.

Received April 6, 2010

M.Shabir
Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan
E-mail: mshabirbhatti@yahoo.co.uk

T.Mahmood
Department of Mathematics, International Islamic Univesity, Islamabad, Pakistan
E-mail: tahirbakhat@yahoo.com

Quasigroups and Related Systems **18** (2010), 213 − 228

ARO–quasigroups

Vladimir Volenec, Zdenka Kolar–Begović and Ružica Kolar–Šuper

Abstract. In this paper the concept of ARO–quasigroup is introduced and some identities which are valid in a general ARO–quasigroup are proved. The "geometric" concepts of the midpoint, parallelogram and affine regular octagon are introduced in a general ARO–quasigroup. The geometric interpretation of some proved identities and introduced concepts is given in the quasigroup $\mathbb{C}\left(1+\frac{\sqrt{2}}{2}\right)$.

1. Definition and examples

A quasigroup $(Q,\cdot)$ will be called *ARO–quasigroup* if it satisfies the following identities of *idempotency* and *mediality*

$$aa = a, \tag{1}$$

$$ab \cdot cd = ac \cdot bd \tag{2}$$

and besides that the identity

$$ab \cdot b = ba \cdot a. \tag{3}$$

Example 1. Let $(G,+)$ be a commutative group in which there exists the automorphism φ which satisfies the identity

$$(\varphi\circ\varphi)(a) + (\varphi\circ\varphi)(a) - \varphi(a) - \varphi(a) - \varphi(a) - \varphi(a) + a = 0,$$

which can be written in a simpler form

$$2(\varphi\circ\varphi)(a) - 4\varphi(a) + a = 0. \tag{4}$$

If the multiplication $\cdot$ on the set G is defined by the formula

$$ab = a + \varphi(b-a) \tag{5}$$

2010 Mathematics Subject Classification: 20N05
Key words and phrases: ARO–quasigroup, affine regular octagon, parallelogram.

we shall prove that $(G,\cdot)$ is ARO–quasigroup. For each $a,b\in G$ the equations $ax=b$ and $ya=b$, owing to (5), are equivalent to the equations

$$a+\varphi(x-a)=b,\qquad y+\varphi(a)-\varphi(y)=b. \tag{6}$$

The first equation has the unique solution $x=a+\varphi^{-1}(b-a)$, and out of the second equation it follows

$$\begin{aligned}2(\varphi\circ\varphi)(y)-2\varphi(y)&=2(\varphi\circ\varphi)(a)-2\varphi(b),\\ 2y-2\varphi(y)&=2b-2\varphi(a).\end{aligned}$$

The addition of two last equations gives

$$2(\varphi\circ\varphi)(y)-4\varphi(y)+2y=2(\varphi\circ\varphi)(a)-2\varphi(a)-2\varphi(b)+2b,$$

i.e., owing to (4) the solution must have the form

$$y=2\varphi(a)-a-2\varphi(b)+2b. \tag{7}$$

Really, it is a solution of (6) because from (7), according to (4), we get

$$\begin{aligned}y-\varphi(y)&=2\varphi(a)-a-2\varphi(b)+2b-\varphi(2\varphi(a)-a-2\varphi(b)+2b)\\ &=2(\varphi\circ\varphi)(b)-4\varphi(b)+2b-(2(\varphi\circ\varphi)(a)-3\varphi(a)+a)=b-\varphi(a).\end{aligned}$$

We have proved that $(G,\cdot)$ is a quasigroup. Its idempotency is obvious by (5). According to (5) we also get

$$\begin{aligned}ab\cdot cd&=ab+\varphi(cd-ab)=a+\varphi(b-a)+\varphi(c+\varphi(d-c)-a-\varphi(b-a))\\ &=a-2\varphi(a)+(\varphi\circ\varphi)(a)+\varphi(b)-(\varphi\circ\varphi)(b)+\varphi(c)-(\varphi\circ\varphi)(c)+(\varphi\circ\varphi)(d).\end{aligned}$$

The symmetry of the obtained expression by b and c proves the mediality (2). By (5) it follows

$$\begin{aligned}ab\cdot b&=ab+\varphi(b-ab)=a+\varphi(b-a)+\varphi(b-a-\varphi(b-a))\\ &=(\varphi\circ\varphi)(a)-2\varphi(a)+a+2\varphi(b)-(\varphi\circ\varphi)(b),\end{aligned}$$

and analogously

$$ba\cdot a=2\varphi(a)-(\varphi\circ\varphi)(a)+(\varphi\circ\varphi)(b)-2\varphi(b)+b,$$

whence owing to (4)

$$ab\cdot b-ba\cdot a=2(\varphi\circ\varphi)(a)-4\varphi(a)+a-(2(\varphi\circ\varphi)(b)-4\varphi(b)+b)=0,$$

i.e., the identity (3) is valid. □

Example 2. Let $(F,+,\cdot)$ be a field. If the equation

$$2q^2 - 4q + 1 = 0 \tag{8}$$

has the solution q in F and if the operation $*$ on F is defined by the formula

$$a * b = (1-q)a + qb. \tag{9}$$

then $\varphi(a) = qa$ obviously defines an automorphism of a commutative group $(F,+)$. As the equality (8) is valid it implies that the equality (4) holds for all $a \in F$. However, (9) can be also written in the form

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

and by Example 1, $(F,*)$ is ARO–quasigroup. □

Example 3. Let $(\mathbb{C},+,\cdot)$ be a field of complex numbers and $*$ binary operation on $\mathbb{C}$ defined by (9), where q is the solution of the equation (8), i.e., $q = 1 + \frac{\sqrt{2}}{2}$ or $q = 1 - \frac{\sqrt{2}}{2}$. According to Example 2 $(\mathbb{C},*)$ is ARO–quasigroup. For example, let $q = 1+\frac{\sqrt{2}}{2}$. The obtained quasigroup has a nice geometric interpretation, which justifies the studying ARO–quasigroups and defining the geometric concepts in them. Let us consider the set $\mathbb{C}$ as the set of the points in the Euclidean plane. For the different points a and b the equality (9) can be written as

$$\frac{a * b - a}{b - a} = q$$

which means that the points a, b, $a * b$ determine the quotient ratio q. The operation $*$ is presented in the Figure 1 where, instead of $a * b$, we shall shortly write ab, and in the sequel we will use this notation in all figures.

Figure 1.

The identity (3) is illustrated in the Figure 2.

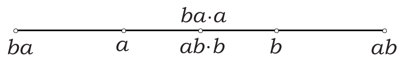


Figure 2.

□

2. The basic properties

The immediate consequences of the identities (1) and (2) are the identities of *elasticity*, *left* and *right distributivity*

$$ab \cdot a = a \cdot ba, \tag{10}$$

$$a \cdot bc = ab \cdot ac, \tag{11}$$

$$ab \cdot c = ac \cdot bc \tag{12}$$

Let us prove the following theorem.

Theorem 1. *In the ARO–quasigroup* $(Q, \cdot)$ *the following identities*

$$(ab \cdot b)a = (a \cdot ab)b, \tag{13}$$

$$(ab \cdot c)c = (c \cdot ba)a, \tag{14}$$

$$(ab \cdot b)b = (b \cdot ba)a, \tag{15}$$

$$(ab \cdot ba)c = (ac \cdot ca)b, \tag{16}$$

$$(ab \cdot ba)a = ab, \tag{17}$$

$$(ab \cdot ba)c \cdot c = cb \cdot a, \tag{18}$$

$$(ab \cdot ba)b \cdot b = ba, \tag{19}$$

$$(ab \cdot ba)b = ba \cdot ab, \tag{20}$$

$$(ab \cdot ba) \cdot ca = ac \cdot b \tag{21}$$

are valid.

Proof. Firstly we get

$$(ab \cdot b)a \overset{(12)}{=} (ab \cdot a) \cdot ba \overset{(10)}{=} (a \cdot ba) \cdot ba \overset{(2)}{=} ab \cdot (ba \cdot a) \overset{(3)}{=} ab \cdot (ab \cdot b) \overset{(12)}{=} (a \cdot ab)b,$$

$$(ab \cdot c)c \overset{(3)}{=} (c \cdot ab) \cdot ab \overset{(2)}{=} ca \cdot (ab \cdot b) \overset{(3)}{=} ca \cdot (ba \cdot a) \overset{(12)}{=} (c \cdot ba)a,$$

$$\begin{aligned}(ab\cdot ba)c &\overset{(12)}{=} (ab\cdot c)(ba\cdot c) \overset{(11)}{=} (ab\cdot c)(ba)\cdot(ab\cdot c)c \overset{(2)}{=} (ab\cdot b)(ca)\cdot(ab\cdot c)c\\ &\overset{(2)}{=} (ab\cdot b)(ab\cdot c)\cdot(ca\cdot c) \overset{(11)}{=} (ab\cdot bc)(ca\cdot c) \overset{(2)}{=} (ab\cdot ca)(bc\cdot c)\\ &\overset{(3)}{=} (ab\cdot ca)(cb\cdot b) \overset{(2)}{=} (ab\cdot cb)(ca\cdot b) \overset{(12)}{=} (ac\cdot b)(ca\cdot b) \overset{(12)}{=} (ac\cdot ca)b,\end{aligned}$$

so the identities (13), (14) and (16) hold. From (14) using $c = b$ the identity (15) follows, and using $c = a$ from (16) owing to (1) the identity (17) follows. Further we get

$$\begin{aligned}(ab\cdot ba)c\cdot c &\overset{(12)}{=} (ab\cdot c)c\cdot(ba\cdot c)c \overset{(3)}{=} (c\cdot ab)(ab)\cdot(ba\cdot c)c \overset{(2)}{=} (ca)(ab\cdot b)\cdot(ba\cdot c)c\\ &\overset{(3)}{=} (ca)(ba\cdot a)\cdot(ba\cdot c)c \overset{(12)}{=} (c\cdot ba)a\cdot(ba\cdot c)c \overset{(2)}{=} (c\cdot ba)(ba\cdot c)\cdot ac\\ &\overset{(16)}{=} (c\cdot ac)(ac\cdot c)\cdot ba \overset{(3)}{=} (c\cdot ac)(ca\cdot a)\cdot ba \overset{(10)}{=} (ca\cdot c)(ca\cdot a)\cdot ba\\ &\overset{(11)}{=} (ca\cdot ca)\cdot ba \overset{(1)}{=} ca\cdot ba \overset{(12)}{=} cb\cdot a,\end{aligned}$$

i.e., the equality (18) is valid, wherefrom with $c = b$ because of (1) it follows (19). Finally, we obtain

$$(ab\cdot ba)b \overset{(12)}{=} (ab\cdot b)(ba\cdot b) \overset{(3)}{=} (ba\cdot a)(ba\cdot b) \overset{(11)}{=} ba\cdot ab,$$

$$(ab{\cdot}ba){\cdot}ca \overset{(2)}{=} (ab{\cdot}c)(ba{\cdot}a) \overset{(3)}{=} (ab{\cdot}c)(ab{\cdot}b) \overset{(11)}{=} ab{\cdot}cb \overset{(12)}{=} ac{\cdot}b. \qquad \square$$

3. Midpoints and parallelograms

Let $(Q,\cdot)$ be ARO–quasigroup. The elements of the set Q will be called *points*. The geometric presentation in the Figure 2 leads to the following definition. For any two points a and b the point c, given by the equalities

$$c = a * b = ab\cdot b \overset{(3)}{=} ba\cdot a, \tag{22}$$

will be called the *midpoint* of the points a and b.

Theorem 2. *If the operation $*$ on the set Q is defined by the formula* (22), *then $(Q, *)$ is idempotent medial commutative quasigroup.*

Proof. The equations $a * x = b$ and $y * a = b$, which according to (22) can be written as $xa \cdot a = b$ and $ya \cdot a = b$, are uniquely solvable for x and y for each $a, b \in Q$. Commutativity and idempotency of the operation $*$ are obvious, and mediality follows by means of (2) like this:

$$\begin{aligned}(a * b) * (c * d) &= (ab \cdot b)(cd \cdot d) \cdot (cd \cdot d) = (ab \cdot cd)(bd) \cdot (cd \cdot d)\\ &= (ac \cdot bd)(cd) \cdot (bd \cdot d) = (ac \cdot c)(bd \cdot d) \cdot (bd \cdot d)\\ &= (a * c) * (b * d). \qquad \square\end{aligned}$$

We shall say that the points a, b, c, d are the *vertices of a parallelogram* and we shall write $Par(a, b, c, d)$ if $a * c = b * d$. If $a * c = b * d = o$, we shall say that the point o is the *center* of that parallelogram and write $Par_o(a, b, c, d)$.

Theorem 3. *(Q, Par) is a parallelogram space, i.e., the following properties are valid:*

$(P1)$ *For any points a, b, c there is the unique point d such that $Par(a, b, c, d)$.*

$(P2)$ *For any cyclic permutation (e, f, g, h) of (a, b, c, d) or of (d, c, b, a) from $Par(a, b, c, d)$ follows $Par(e, f, g, h)$.*

$(P3)$ *From $Par(a, b, c, d)$ and $Par(c, d, e, f)$ follows $Par(a, b, f, e)$.*

Proof. The statement $Par(a, b, c, d)$ is according to (22) equivalent to the equality $ac \cdot c = db \cdot b$, which is unique solvable by d, so the property (P1) is valid. The property (P2) is the consequence of the commutativity of the operation $*$. It remains to prove the property (P3). From $Par(a, b, c, d)$ and $Par(c, d, e, f)$ it follows $a * c = b * d$ and $c * e = d * f$. By means of the mediality and commutativity of the operation $*$ we get

$$\begin{aligned}(a * f) * (c * f) &= (a * c) * (f * f) = (b * d) * (f * f) = (b * f) * (d * f)\\ &= (b * f) * (c * e) = (b * f) * (e * c) = (b * e) * (f * c)\\ &= (b * e) * (c * f),\end{aligned}$$

wherefrom we get $a * f = b * e$, i.e., $Par(a, b, f, e)$. $\square$

4. Affine–regular octagon

Now we are going to introduce the concept of the affine regular octagon in a general ARO–quasigroup. Firstly, we will prove the theorem which will lead to the definition of the mentioned concept.

Theorem 4. *In a cyclical sequence from eight equalities* $a_i a_{i+1} = a_{i+3} a_{i+2}$ $(i = 1,2,3,4,\ 5,6,7,8)$, *where indexes are taken modulo* 8 *from the set* $\{1,2,3,4,\ 5,\ 6,7,8\}$, *each five adjacent equalities imply the remaining three equalities.*

Proof. It is sufficient to prove that the equalities

$$a_1 a_2 = a_4 a_3, \tag{23}$$

$$a_2 a_3 = a_5 a_4, \tag{24}$$

$$a_3 a_4 = a_6 a_5, \tag{25}$$

$$a_4 a_5 = a_7 a_6, \tag{26}$$

$$a_5 a_6 = a_8 a_7, \tag{27}$$

imply the equality

$$a_6 a_7 = a_1 a_8. \tag{28}$$

Firstly, let us prove that from the equality (23)–(25) the equality

$$a_1 a_3 = a_6 a_4, \tag{29}$$

follows, and in the same manner (by the substitution $i \to i+2$) from equalities (25) – (27) the equality

$$a_3 a_5 = a_8 a_6 \tag{30}$$

follows. Really, we get successively

$$\begin{aligned}
(a_1 a_3 \cdot a_5) a_4 &\overset{(12)}{=} (a_1 a_5 \cdot a_3 a_5) a_4 \overset{(12)}{=} (a_1 a_4 \cdot a_5 a_4)(a_3 a_4 \cdot a_5 a_4) \\
&\overset{(24)}{=} (a_1 a_4 \cdot a_2 a_3)(a_3 a_4 \cdot a_5 a_4) \overset{(2)}{=} (a_1 a_2 \cdot a_4 a_3)(a_3 a_4 \cdot a_5 a_4) \\
&\overset{(23)}{=} (a_4 a_3 \cdot a_4 a_3)(a_3 a_4 \cdot a_5 a_4) \overset{(1)}{=} a_4 a_3 \cdot (a_3 a_4 \cdot a_5 a_4) \\
&\overset{(2)}{=} (a_4 \cdot a_3 a_4)(a_3 \cdot a_5 a_4) \overset{(10)}{=} (a_4 a_3 \cdot a_4)(a_3 \cdot a_5 a_4) \\
&\overset{(2)}{=} (a_4 a_3 \cdot a_3)(a_4 \cdot a_5 a_4) \overset{(3)}{=} (a_3 a_4 \cdot a_4)(a_4 \cdot a_5 a_4) \\
&\overset{(10)}{=} (a_3 a_4 \cdot a_4)(a_4 a_5 \cdot a_4) \overset{(12)}{=} (a_3 a_4 \cdot a_4 a_5) a_4 \\
&\overset{(25)}{=} (a_6 a_5 \cdot a_4 a_5) a_4 \overset{(12)}{=} (a_6 a_4 \cdot a_5) a_4,
\end{aligned}$$

wherefrom the equality (29) follows. Now, we can also prove the equality (28), which follows from

$$a_1a_8 \cdot a_6 \overset{(12)}{=} a_1a_6 \cdot a_8a_6 \overset{(30)}{=} a_1a_6 \cdot a_3a_5 \overset{(2)}{=} a_1a_3 \cdot a_6a_5 \overset{(29)}{=} a_6a_4 \cdot a_6a_5$$
$$\overset{(11)}{=} a_6 \cdot a_4a_5 \overset{(26)}{=} a_6 \cdot a_7a_6 \overset{(10)}{=} a_6a_7 \cdot a_6. \qquad \square$$

We shall say that a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8 are the *vertices of an affine–regular octagon* and we shall write $\mathrm{ARO}(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ if any five adjacent, and then all eight, equalities from eight equalities $a_ia_{i+1} = a_{i+3}a_{i+2}$ $(i = 1, 2, 3, 4, 5, 6, 7, 8)$ are valid (Figure 3).

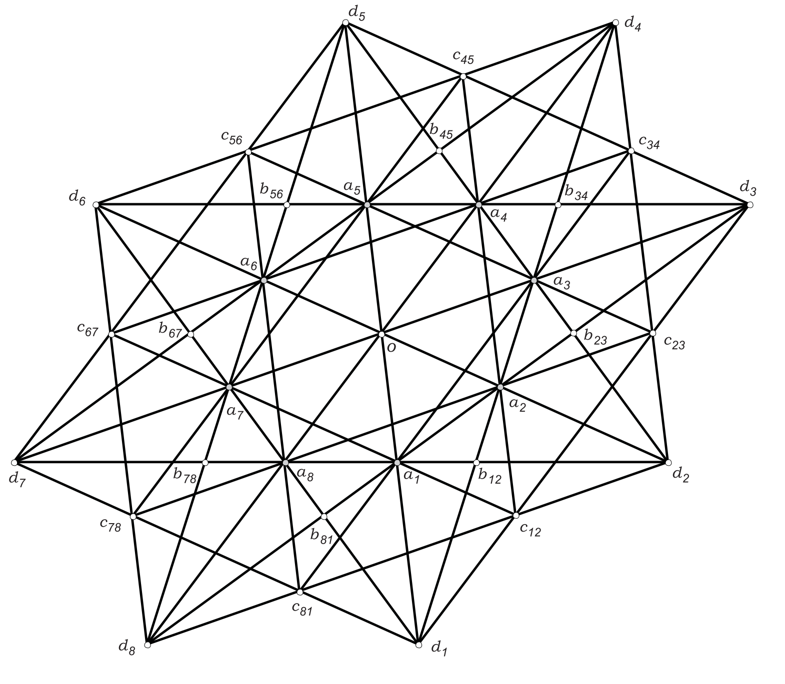


Figure 3.

Corollary 1. *If* $(i_1, i_2, i_3, i_4, i_5, i_6, i_7, i_8)$ *is any cyclic permutation of* $(1, 2, 3, 4, 5, 6, 7, 8)$ *or of* $(8, 7, 6, 5, 4, 3, 2, 1)$, *then* $ARO(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ *implies* $ARO(a_{i_1}, a_{i_2}, a_{i_3}, a_{i_4}, a_{i_5}, a_{i_6}, a_{i_7}, a_{i_8})$.

Corollary 2. *If the statement* $ARO(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ *holds, then for each* $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ *the statement* $a_ia_{i+2} = a_{i+5}a_{i+3}$ *also holds.*

Corollary 3. *Affine–regular octagon is uniquely determined by any three adjacent vertices.* □

Theorem 5. *If the statement $ARO(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ is valid, then for each $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ we have*

$$a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1} = a_{i+4}a_i, \quad a_{i+3}a_{i+2} \cdot a_{i+2}a_{i+3} = a_i a_{i+4}, \tag{31}$$

$$a_{i+4}a_i \cdot a_{i+1} = a_{i+1}a_{i+2} = a_{i+4}a_{i+3}, \quad a_i a_{i+4} \cdot a_{i+3} = a_{i+3}a_{i+2} = a_i a_{i+1}. \tag{32}$$

Proof. The proof of the second equality (31) follows from the proof of the first one (31) by the substitution of indexes $i \leftrightarrow i+4$, $i+1 \leftrightarrow i+3$. Because of Corollary 1 it is sufficient to prove, for example, the equality $a_2a_3 \cdot a_3a_2 = a_5a_1$. We get successively

$$\begin{aligned}(a_2a_3 \cdot a_3a_2)a_2 &\overset{(17)}{=} a_2a_3 \overset{(1)}{=} a_2a_3 \cdot a_2a_3 \overset{(24)}{=} a_5a_4 \cdot a_2a_3 \\ &\overset{(2)}{=} a_5a_2 \cdot a_4a_3 \overset{(23)}{=} a_5a_2 \cdot a_1a_2 \overset{(12)}{=} a_5a_1 \cdot a_2,\end{aligned}$$

so $a_2a_3 \cdot a_3a_2 = a_5a_1$ follows. The first equalities in (32) are obtained by multiplication the equalities (31) with a_{i+1} respectively a_{i+3} because of the identity (17), and other equalities are taken from the definition of the relation ARO. □

Theorem 6. *Let the statement $ARO(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ be valid. There is the point o such that for each $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ the equalities*

$$(a_{i+1}a_i \cdot a_ia_{i+1})\, a_{i+2} = o, \quad (a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1})\, a_i = o \tag{33}$$

are valid, where indexes are taken modulo 8.

Proof. By (16) the mutual equivalence of the equalities (33) hold.

If $o = (a_2a_3 \cdot a_3a_2)a_1$, then $o = (a_2a_1 \cdot a_1a_2)a_3$. By Corollary 1 it is sufficient to prove the equality $o = (a_3a_4 \cdot a_4a_3)a_2$. We get

$$\begin{aligned}(a_3a_4 \cdot a_4a_3)a_2 &\overset{(23)}{=} (a_3a_4 \cdot a_1a_2)a_2 \overset{(12)}{=} (a_3a_4 \cdot a_2)(a_1a_2 \cdot a_2) \\ &\overset{(3)}{=} (a_3a_4 \cdot a_2)(a_2a_1 \cdot a_1) \overset{(2)}{=} (a_3a_4 \cdot a_2a_1) \cdot a_2a_1 \\ &\overset{(3)}{=} (a_2a_1 \cdot a_3a_4) \cdot a_3a_4 \overset{(2)}{=} (a_2a_1 \cdot a_3)(a_3a_4 \cdot a_4) \\ &\overset{(3)}{=} (a_2a_1 \cdot a_3)(a_4a_3 \cdot a_3) \overset{(2)}{=} (a_2a_1 \cdot a_4a_3)a_3 \\ &\overset{(23)}{=} (a_2a_1 \cdot a_1a_2)a_3 = o.\end{aligned}$$

□

The point o from Theorem 6 will be called the *center* of the affine–regular octagon $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ and it will be written in the form $\mathrm{ARO}_o(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$.

Theorem 7. *With hypotheses of Theorem* 6 *for each* $i \in \{1, 2, 3, 4, 5, 6, 7, 8\}$ *the equalities*

$$o = a_i * a_{i+4} = a_i a_{i+4} \cdot a_{i+4}, \tag{34}$$

$$a_{i+1}a_{i+2} \cdot a_i = o \cdot a_{i+1}a_i, \quad a_{i+1}a_i \cdot a_{i+2} = o \cdot a_{i+1}a_{i+2}, \tag{35}$$

$$oa_i = a_i a_{i+2} \cdot a_{i+1}, \quad oa_{i+2} = a_{i+2}a_i \cdot a_{i+1} \tag{36}$$

are valid.

Proof. We get

$$\begin{aligned} a_i * a_{i+4} &\overset{(22)}{=} a_{i+4}a_i \cdot a_i \overset{(31)}{=} (a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1})a_i \overset{(33)}{=} o, \\ a_{i+1}a_{i+2} \cdot a_i &\overset{(17)}{=} (a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1})a_{i+1} \cdot a_i \\ &\overset{(12)}{=} (a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1})a_i \cdot a_{i+1}a_i \overset{(33)}{=} o \cdot a_{i+1}a_i, \\ oa_i &\overset{(33)}{=} (a_{i+1}a_{i+2} \cdot a_{i+2}a_{i+1})a_i \cdot a_i \overset{(18)}{=} a_i a_{i+2} \cdot a_{i+1}. \end{aligned}$$ □

In the previous proof the equivalence of the equations (33) and (34) is proved, therefore the center of an affine–regular octagon can be also characterized by (34).

5. The determination of the affine–regular octagon

The statements of the unique determination of the affine regular octagon will be proved in this chapter.

Theorem 8. *Affine–regular octagon is uniquely determined by any three of its vertices.*

Proof. By Corollary 1 and 3 it is sufficient to prove only the following statements

(i) The vertices a_1, a_2, a_4 uniquely determine the vertex a_3. This statement is obvious from the equalities (23).

(ii) The vertices a_1, a_2, a_5 or a_1, a_3, a_5 uniquely determine the vertex a_3, respectively a_2. Indeed, let o is the point such that $o = a_5a_1 \cdot a_1$, and then a_3 respectively a_2 the point such that $oa_1 = a_1a_3 \cdot a_2$, and a_4 the point such that $a_1a_2 = a_4a_3$. It should be proved the equality $a_2a_3 = a_5a_4$. It is the consequence of the following consideration:

$$\begin{aligned}
(a_2a_3 \cdot a_2a_3)(a_4a_3) \cdot a_4a_3 &\overset{(1)}{=} (a_2a_3 \cdot a_4a_3) \cdot a_4a_3 \overset{(3)}{=} (a_4a_3 \cdot a_2a_3) \cdot a_2a_3 \\
&\overset{(2)}{=} (a_4a_3 \cdot a_2)(a_2a_3 \cdot a_3) \overset{(3)}{=} (a_4a_3 \cdot a_2)(a_3a_2 \cdot a_2) \\
&\overset{(12)}{=} (a_4a_3 \cdot a_3a_2)a_2 = (a_1a_2 \cdot a_3a_2)a_2 \overset{(12)}{=} (a_1a_3 \cdot a_2)a_2 \\
&= oa_1 \cdot a_2 = (a_5a_1 \cdot a_1)a_1 \cdot a_2 \\
&\overset{(12)}{=} (a_5a_2 \cdot a_1a_2)(a_1a_2) \cdot (a_1a_2) \\
&= (a_5a_2 \cdot a_4a_3)(a_4a_3) \cdot (a_4a_3) \\
&\overset{(2)}{=} (a_5a_4 \cdot a_2a_3)(a_4a_3) \cdot (a_4a_3).
\end{aligned}$$

(iii) The vertices a_1, a_3, a_6 uniquely determine the vertex a_2. Really, let a_4 be a point such that $a_1a_3 = a_6a_4$, then a_2 be a point such that $a_1a_2 = a_4a_3$, and a_5 the point such that $a_2a_3 = a_5a_4$. It should be proved the equality $a_3a_4 = a_6a_5$, which follows from this:

$$\begin{aligned}
(a_3a_4 \cdot a_4a_5)a_4 &\overset{(12)}{=} (a_3a_4 \cdot a_4)(a_4a_5 \cdot a_4) \overset{(10)}{=} (a_3a_4 \cdot a_4)(a_4 \cdot a_5a_4) \\
&\overset{(3)}{=} (a_4a_3 \cdot a_3)(a_4 \cdot a_5a_4) \overset{(2)}{=} (a_4a_3 \cdot a_4)(a_3 \cdot a_5a_4) \\
&\overset{(10)}{=} (a_4 \cdot a_3a_4)(a_3 \cdot a_5a_4) \overset{(2)}{=} a_4a_3 \cdot (a_3a_4 \cdot a_5a_4) \\
&\overset{(12)}{=} a_4a_3 \cdot (a_3a_5 \cdot a_4) \overset{(1)}{=} (a_4a_3 \cdot a_4a_3)(a_3a_5 \cdot a_4) \\
&= (a_1a_2 \cdot a_4a_3)(a_3a_5 \cdot a_4) \overset{(2)}{=} (a_1a_4 \cdot a_2a_3)(a_3a_5 \cdot a_4) \\
&= (a_1a_4 \cdot a_5a_4)(a_3a_5 \cdot a_4) \overset{(12)}{=} (a_1a_5 \cdot a_4)(a_3a_5 \cdot a_4) \\
&\overset{(12)}{=} (a_1a_5 \cdot a_3a_5)a_4 \overset{(12)}{=} (a_1a_3 \cdot a_5)a_4 \\
&= (a_6a_4 \cdot a_5)a_4 \overset{(12)}{=} (a_6a_5 \cdot a_4a_5)a_4.
\end{aligned}$$

□

If the statement $\mathrm{ARO}(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$ hold, then two vertices of the form a_i and a_{i+4} are said to be *opposite vertices* of the considered affine–regular octagon.

Theorem 9. *Affine–regular octagon is uniquely determined by its center and by any two of its vertices which are not opposite.*

Proof. (i) The center o and vertices a_1, a_2 respectively the vertices a_1, a_3 uniquely determine the remaining vertices. Let a_3 respectively a_2 be a point such that $oa_1 = a_1a_3 \cdot a_2$, then a_4 be a point such that $a_1a_2 = a_4a_3$, and a_5 be a point such that $o = a_5a_1 \cdot a_1$. It should be proved $a_2a_3 = a_5a_4$, and the proof is the same as the proof of the part (ii) of the proof Theorem 8.

(ii) The center o and the vertices a_2, a_5 uniquely determine the remaining vertices. Let a_1 be a point such that $o = a_1a_5 \cdot a_5$, and a_3 point such that $oa_1 = a_1a_3 \cdot a_2$, and a_4 point such that $a_1a_2 = a_4a_3$. Further the proof is the same as in a previous case. □

5. Some new associated affine–regular octagons

In this chapter we are going to consider some new octagons whose vertices can be obtained by means of the vertices of the initial octagon.

Equal products from the definition of the affine–regular octagon will be labelled like this

$$a_ia_{i+1} = b_{i+1,i+2} = a_{i+3}a_{i+2}, \tag{37}$$

where the indexes will be always taken mod 8 from the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$. On the base of the proof of Theorem 4 according to Corollary 1 it follows that there exists the point $c_{i+2,i+3}$ such that

$$a_ia_{i+2} = c_{i+2,i+3} = a_{i+5}a_{i+3}. \tag{38}$$

Besides that, let

$$d_i = a_{i+4}a_i. \tag{39}$$

With these labels the equalities (31) and (32) can be written in the form

$$b_{i+2,i+3}\, b_{i,i+1} = d_i, \quad b_{i,i+1}\, b_{i+2,i+3} = d_{i+3}, \tag{40}$$

$$d_i\, a_{i+1} = b_{i+2,i+3}, \quad d_{i+3}\, a_{i+2} = b_{i,i+1}, \tag{41}$$

where the indexes in the second equalities in (40) and (41) are reduced for 1. The equalities (31) can also be written in the form

$$d_i = a_{i+1}\, a_{i+2} \cdot a_{i+2}\, a_{i+1}, \quad d_{i+2} = a_{i+1}\, a_i \cdot a_i\, a_{i+1}, \tag{42}$$

and the equalities (33) can be written in this shortened form:

$$d_ia_i = o. \tag{43}$$

The equalities (35) and (36) can also be written as the equalities

$$b_{i+2,i+3}\, a_i = o\, b_{i-1,i}, \quad b_{i-1,i}\, a_{i+2} = o\, b_{i+2,i+3}, \tag{44}$$

$$o\, a_i = c_{i+2,i+3}\, a_{i+1}, \quad o\, a_{i+2} = c_{i-1,i}\, a_{i+1}. \tag{45}$$

Let us prove some more similar equalities. We get for example:

$$d_1 a_3 \overset{(42)}{=} (a_2 a_3 \cdot a_3 a_2) a_3 \overset{(20)}{=} a_3 a_2 \cdot a_2 a_3 \overset{(42)}{=} d_4,$$

and generally the equalities

$$d_i\, a_{i+2} = d_{i+3}, \quad d_i\, a_{i-2} = d_{i-3} \tag{46}$$

are valid. Due to the example

$$d_1 a_2 \overset{(42)}{=} (a_2 a_3 \cdot a_3 a_2) a_2 \overset{(17)}{=} a_2 a_3 \overset{(37)}{=} b_{34},$$

the general equalities

$$d_i\, a_{i+1} = b_{i+2,i+3}, \quad d_i\, a_{i-1} = b_{i-3,i-2} \tag{47}$$

hold. Let us prove for example

$$c_{12} c_{23} \overset{(38)}{=} a_4 a_2 \cdot a_5 a_3 \overset{(2)}{=} a_4 a_5 \cdot a_2 a_3 \overset{(37)}{=} a_4 a_5 \cdot a_5 a_4 \overset{(42)}{=} d_3$$

and generally,

$$c_{i,i+1}\, c_{i+1,i+2} = d_{i+2}, \quad c_{i+1,i+2}\, c_{i,i+1} = d_i. \tag{48}$$

On the base of the equalities (37) and (48) we get for example

$$b_{12} b_{23} \overset{(37)}{=} a_3 a_2 \cdot a_4 a_3 \overset{(2)}{=} a_3 a_4 \cdot a_2 a_3 \overset{(37)}{=} b_{45} b_{34},$$

$$c_{12} c_{23} \overset{(48)}{=} d_3 = c_{45} c_{34},$$

i.e., generally we have $b_{i,i+1} b_{i+1,i+2} = b_{i+3,i+4} b_{i+2,i+3}$ and $c_{i,i+1} c_{i+1,i+2} = c_{i+3,i+4} c_{i+2,i+3}$, which proves the statements

$$ARO(b_{12}, b_{23}, b_{34}, b_{45}, b_{56}, b_{67}, b_{78}, b_{81}), \tag{49}$$

$$ARO(c_{12}, c_{23}, c_{34}, c_{45}, c_{56}, c_{67}, c_{78}, c_{81}). \tag{50}$$

The proof of the statement

$$ARO(d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8) \tag{51}$$

is more complicated. We get for example

$$\begin{aligned} d_1d_2 &\overset{(46)}{=} d_4a_2 \cdot d_5a_3 \overset{(2)}{=} d_4d_5 \cdot a_2a_3 \overset{(37)}{=} d_4d_5 \cdot a_5a_4 \overset{(2)}{=} d_4a_5 \cdot d_5a_4 \overset{(47)}{=} b_{67}b_{23} \\ &\overset{(47)}{=} d_1a_8 \cdot d_8a_1 \overset{(2)}{=} d_1d_8 \cdot a_8a_1 \overset{(37)}{=} d_1d_8 \cdot a_3a_2 \overset{(2)}{=} d_1a_3 \cdot d_8a_2 \overset{(46)}{=} d_4d_3. \end{aligned}$$

All three affine–regular octagons (52)–(54) have the center o because we get for example

$$\begin{aligned} b_{12} * b_{56} &= b_{12}b_{56} \cdot b_{56} \overset{(37)}{=} (a_3a_2 \cdot a_7a_6) \cdot a_7a_6 \overset{(2)}{=} (a_3a_7 \cdot a_2a_6) \cdot a_7a_6 \\ &\overset{(2)}{=} (a_3a_7 \cdot a_7)(a_2a_6 \cdot a_6) = (a_3 * a_7)(a_2 * a_6) \overset{(34)}{=} o\,o \overset{(1)}{=} o, \end{aligned}$$

$$\begin{aligned} c_{12} * c_{56} &= c_{12}c_{56} \cdot c_{56} \overset{(38)}{=} (a_4a_2 \cdot a_8a_6) \cdot a_8a_6 \overset{(2)}{=} (a_4a_8 \cdot a_2a_6) \cdot a_8a_6 \\ &\overset{(2)}{=} (a_4a_8 \cdot a_8)(a_2a_6 \cdot a_6) = (a_4 * a_8)(a_2 * a_6) \overset{(34)}{=} o\,o \overset{(1)}{=} o, \end{aligned}$$

$$\begin{aligned} d_1 * d_5 &= d_1d_5 \cdot d_5 \overset{(42)}{=} (a_2a_3 \cdot a_3a_2)(a_6a_7 \cdot a_7a_6) \cdot (a_6a_7 \cdot a_7a_6) \\ &\overset{(2)}{=} (a_2a_3 \cdot a_6a_7)(a_3a_2 \cdot a_7a_6) \cdot (a_6a_7 \cdot a_7a_6) \\ &\overset{(2)}{=} (a_2a_6 \cdot a_3a_7)(a_3a_7 \cdot a_2a_6) \cdot (a_6a_7 \cdot a_7a_6) \\ &\overset{(2)}{=} (a_2a_6 \cdot a_3a_7)(a_6a_7) \cdot (a_3a_7 \cdot a_2a_6)(a_7a_6) \\ &\overset{(2)}{=} (a_2a_6 \cdot a_6)(a_3a_7 \cdot a_7) \cdot (a_3a_7 \cdot a_7)(a_2a_6 \cdot a_6) \\ &= (a_2 * a_6)(a_3 * a_7) \cdot (a_3 * a_7)(a_2 * a_6) \overset{(34)}{=} o\,o \cdot o\,o \overset{(1)}{=} o. \end{aligned}$$

A numerous parallelograms are related to the affine–regular octagon. So, for example we get the equalities

$$\begin{aligned} a_1 * a_2 &= a_2a_1 \cdot a_1 \overset{(21)}{=} (a_2a_1 \cdot a_1a_2) \cdot a_1a_2 \overset{(37)}{=} (a_2a_1 \cdot a_4a_3) \cdot a_4a_3 \\ &\overset{(2)}{=} (a_2a_1 \cdot a_4)(a_4a_3 \cdot a_3) \overset{(3)}{=} (a_2a_1 \cdot a_4)(a_3a_4 \cdot a_4) \overset{(12)}{=} (a_2a_1 \cdot a_3a_4)a_4 \\ &\overset{(2)}{=} (a_2a_3 \cdot a_1a_4)a_4 \overset{(37)}{=} (a_5a_4 \cdot a_1a_4)a_4 \overset{(12)}{=} (a_5a_1 \cdot a_4)a_4 \overset{(39)}{=} d_1a_4 \cdot a_4 \\ &= a_4 * d_1, \end{aligned}$$

$$\begin{aligned}a_1 * b_{34} &= a_1b_{34}\cdot b_{34} \overset{(37)}{=} (a_1\cdot a_2a_3)\cdot a_2a_3 \overset{(2)}{=} a_1a_2\cdot(a_2a_3\cdot a_3)\\ &\overset{(3)}{=} a_1a_2\cdot(a_3a_2\cdot a_2) \overset{(37)}{=} a_4a_3\cdot(a_3a_2\cdot a_2) \overset{(2)}{=} (a_4\cdot a_3a_2)\cdot a_3a_2\\ &\overset{(37)}{=} a_4b_{12}\cdot b_{12} = b_{12} * a_4,\end{aligned}$$

$$\begin{aligned}a_1 * d_1 &= a_1d_1\cdot d_1 \overset{(39)}{=} (a_1\cdot a_5a_1)\cdot a_5a_1 \overset{(10)}{=} (a_1a_5\cdot a_1)\cdot a_5a_1 \overset{(12)}{=} (a_1a_5\cdot a_5)a_1\\ &= (a_1 * a_5)a_1 \overset{(34)}{=} oa_1 \overset{(45)}{=} c_{34}a_2 \overset{(38)}{=} a_1a_3\cdot a_2 \overset{(12)}{=} a_1a_2\cdot a_3a_2\\ &\overset{(32)}{=} (a_1a_5\cdot a_4)(a_3a_7\cdot a_8) \overset{(2)}{=} (a_1a_5\cdot a_3a_7)\cdot a_4a_8 \overset{(2)}{=} (a_1a_3\cdot a_5a_7)\cdot a_4a_8\\ &\overset{(38)}{=} (a_6a_4\cdot a_2a_8)\cdot a_4a_8 \overset{(2)}{=} (a_6a_2\cdot a_4a_8)\cdot a_4a_8 \overset{(39)}{=} d_2d_8\cdot d_8 = d_2 * d_8,\end{aligned}$$

$$\begin{aligned}b_{12} * d_3 &= b_{12}d_3\cdot d_3 \overset{(37),(39)}{=} (a_3a_2\cdot a_7a_3)\cdot a_7a_3 \overset{(2)}{=} (a_3a_7\cdot a_2a_3)\cdot a_7a_3\\ &\overset{(2)}{=} (a_3a_7\cdot a_7)(a_2a_3\cdot a_3) \overset{(34),(3)}{=} o(a_3a_2\cdot a_2) \overset{(34)}{=} (a_2a_6\cdot a_6)(a_3a_2\cdot a_2)\\ &\overset{(2)}{=} (a_2a_6\cdot a_3a_2)\cdot a_6a_2 \overset{(2)}{=} (a_2a_3\cdot a_6a_2)\cdot a_6a_2 \overset{(37),(39)}{=} b_{34}d_2\cdot d_2 = d_2 * b_{34},\end{aligned}$$

$$\begin{aligned}o * c_{34} &= oc_{34}\cdot c_{34} \overset{(33),(38)}{=} ((a_2a_1\cdot a_1a_2)a_3\cdot a_1a_3)\cdot a_1a_3\\ &\overset{(12)}{=} ((a_2a_1\cdot a_1a_2)a_1\cdot a_1)a_3 \overset{(19)}{=} a_1a_2\cdot a_3 \overset{(37)}{=} a_4a_3\cdot a_3 = a_3 * a_4,\end{aligned}$$

and we get the statements $Par(a_1, a_4, a_2, d_1)$, $Par(a_1, b_{12}, b_{34}, a_4)$, $Par(a_1, d_2, d_1, d_8)$, $Par(b_{12}, d_2, d_3, b_{34})$, $Par(o, a_3, c_{34}, a_4)$ or more general statements

$$Par(a_i,\, a_{i+3},\, a_{i+1},\, d_i), \quad Par(a_i,\, a_{i-3},\, a_{i-1},\, d_i), \tag{52}$$

$$Par(a_i,\, b_{i,i+1},\, b_{i+2,i+3},\, a_{i+3}), \tag{53}$$

$$Par(a_i,\, d_{i+1},\, d_i,\, d_{i-1}), \tag{54}$$

$$Par(b_{i,i+1},\, d_{i+1},\, d_{i+2},\, b_{i+2,i+3}), \tag{55}$$

$$Par(o,\, a_i,\, c_{i,i+1},\, a_{i+1}). \tag{56}$$

We have proved:

Theorem 10. *Let the statement $ARO_o(a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8)$ holds. Then there are the points $b_{i,i+1}$, $c_{i,i+1}$, d_i such that the statements (37)−(48) and (52) − (56) hold, where the indexes are taken modulo 8 from the set $\{1,2,3,4,5,6,7,8\}$, and the statements $ARO_o(b_{12},b_{23},b_{34},b_{45},b_{56},b_{67},b_{78},b_{81})$, $ARO_o(c_{12},c_{23},c_{34},c_{45},c_{56},c_{67},c_{78},c_{81})$ and $ARO_o(d_1,d_2,d_3,d_4,d_5,d_6,d_7,d_8)$ are also valid.* □

All results from the Theorems 5, 6, 7 and 10 can be illustrated in the Figure 3.

References

[1] **W. A. Dudek**, *Quadratical quasigroups*, Quasigroups and Related Systems **4** (1997), 9 – 13.

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

[3] **Z. Kolar-Begović and V. Volenec**, *LGS-quasigroups*, Quasigroups and Related Systems **17** (2009), 77 – 99.

[4] **S. K. Stein**, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228 – 256.

[5] **V. Volenec**, *Geometry of medial quasigroups*, Rad Jugoslav. Akad. Znan. Umj. **421** (1986), 79 – 91.

[6] **V. Volenec**, *Geometry of IM-quasigroups*, Rad Jugoslav. Akad. Znan. Umj. **456** (1991), 139 – 146.

[7] **V. Volenec**, *Squares in quadratical quasigroups*, Quasigroups and Related Systems **7** (2000), 37 – 44.

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

Received November 06, 2010

V.Volenec
Department of Mathematics, University of Zagreb, Bijenička c. 30, 10 000 Zagreb, Croatia
E-mail: volenec@math.hr

Z.Kolar-Begović
Department of Mathematics, University of Osijek, Gajev trg 6, 31 000 Osijek, Croatia
E-mail: zkolar@mathos.hr

R.Kolar-Šuper
Faculty of Teacher Education, University of Osijek, Lorenza Jägera 9, 31 000 Osijek, Croatia
E-mail: rkolar@ufos.hr

Quasigroups and Related Systems **18** (2010), 229 – 240

Parallelograms in quadratical quasigroups

Vladimir Volenec and Ružica Kolar–Šuper

Abstract. The "geometric" concept of parallelogram is introduced and investigated in a general quadratical quasigroup and geometrical interpretation in the quadratical quasigroup $\mathbb{C}(\frac{1+i}{2})$ is given. Some statements about relationships between the parallelograms and some other "geometric" structures in a general quadratical quasigroup will be also considered.

A grupoid $(Q,\cdot)$ is said to be *quadratical* if the identity

$$ab \cdot a = ca \cdot bc \tag{1}$$

holds and the equation $ax = b$ has a unique solution $x \in Q$ for all $a, b \in Q$ i.e., $(Q,\cdot)$ is a right quasigroup. In [16] it is proved that $(Q,\cdot)$ is then a quasigroup. $(Q,\cdot)$ is satisfying the following identitites

$$aa = a, \tag{2}$$

$$ab \cdot cd = ac \cdot bd, \tag{3}$$

$$ab \cdot a = a \cdot ba, \tag{4}$$

$$ab \cdot a = ba \cdot b, \tag{5}$$

$$a \cdot bc = ab \cdot ac, \tag{6}$$

$$ab \cdot c = ac \cdot bc \tag{7}$$

and the equivalencies

$$ab = cd \Leftrightarrow bc = da, \tag{8}$$

$$ax = b \Leftrightarrow x = (b \cdot ba) \cdot (b \cdot ba)(ba \cdot a), \tag{9}$$

$$xa = b \Leftrightarrow x = (a \cdot ab)(ab \cdot b) \cdot (ab \cdot b). \tag{10}$$

2010 Mathematics Subject Classification: 20N05
Keywords: Quadratical quasigroup, parallelogram, square

Let $(\mathbb{C}, +, \cdot)$ be the field of complex numbers and $*$ the operation on $\mathbb{C}$ defined by

$$a * b = (1-q)a + qb \tag{11}$$

where $q = \frac{1+i}{2}$. It can be proved that $(\mathbb{C}, *)$ is a quadratical quasigroup. This quasigroup has a nice geometric interpretation which motivates the study of quadratical quasigroup. Let us regard the complex numbers as points of the Euclidean plane. For any point a we obviously have $a * a = a$, and for two different points a, b the equality (11) can be written in the form

$$\frac{a * b - a}{b - a} = \frac{q - 0}{1 - 0},$$

which means that the points $a, b, a * b$ are the vertices of a triangle directly similar to the triangle with the vertices $0, 1, q$ (Figure 1). We can say that $a * b$ is the centre of a square with two adjacent vertices a and b, which justifies the name "quadratical quasigroup". We shall denote this quasigroup by $\mathbb{C}(\frac{1+i}{2})$ because we have $a * b = \frac{1+i}{2}$ if $a = 0$ and $b = 1$.

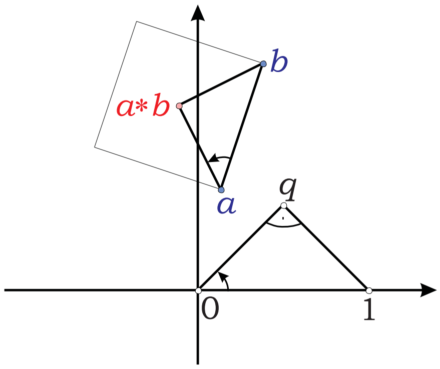


Figure 1.

The figures in the quasigroup $\mathbb{C}(\frac{1+i}{2})$ can be used as the illustrations of "geometric" relations in any quadratical quasigroup $(Q, \cdot)$. For example, the left side of the identity (1) is obviously the midpoint of the points a and b and this identity is illustrated in Figure 2 (here and in all other figures in the article we shall use the sign $\cdot$ instead of the sign $*$).

In the sequel let $(Q, \cdot)$ be any quadratical quasigroup. The elements of Q are said to be *points*.

If $\bullet$ is an operation in the set Q defined by

$$a \bullet b = a \cdot ba = ab \cdot a = ca \cdot bc, \tag{12}$$

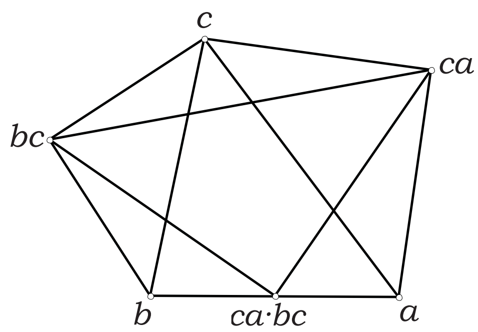


Figure 2.

then (cf. [16]) $(Q, \bullet)$ is an idempotent medial commutative quasigroup, i.e., the identities

$$a \bullet a = a, \tag{13}$$

$$(a \bullet b) \bullet (c \bullet d) = (a \bullet c) \bullet (b \bullet d), \tag{14}$$

$$a \bullet b = b \bullet a \tag{15}$$

hold. The point $a \bullet b$ is said to be a *midpoint* of the pair $\{a, b\}$ of points.

In [15] the notion of a parallelogram is defined in any medial quasigroup and because of mediality (3) we can apply this definition in our quadratical quasigroup $(Q, \cdot)$. According to [15, Cor.1] the points a, b, c, d are said to be the vertices of a *parallelogram* and we write $Par(a, b, c, d)$ if there are two points p and q such that $ap = bq$, $dp = cq$. In [15] it is proved that (Q, Par) is a *parallelogram space*, i.e., we have the properties:

(P1) For any $a, b, c \in Q$ there is an unique point d such that $Par(a, b, c, d)$ holds.

(P2) If (e, f, g, h) is any cyclical permutation of (a, b, c, d) or of (d, c, b, a), then $Par(a,\ b, c, d)$ implies $Par(e, f, g, h)$.

(P3) $Par(a, b, c, d)$, $Par(c, d, e, f) \Rightarrow Par(a, b, f, e)$.

But, the parallelogram can be defined directly, using the midpoints, as we have:

Theorem 1. $Par(a, b, c, d) \Leftrightarrow a \bullet c = b \bullet d$.

Proof. Let $ap = bq$. We must prove the equivalence of the equalities $dp = cq$ and $a \bullet c = b \bullet d$. We obtain successively

$$(a \bullet c)(pq \cdot p) \overset{(12)}{=} (ac \cdot a)(pq \cdot p) \overset{(3)}{=} (ac \cdot pq) \cdot ap \overset{(3)}{=} (ap \cdot cq) \cdot ap = (bq \cdot cq) \cdot bq,$$
$$(b \bullet d)(pq \cdot p) \overset{(12)}{=} (bd \cdot b)(pq \cdot p) \overset{(5)}{=} (bd \cdot b) \cdot (qp \cdot q) \overset{(3)}{=} (bd \cdot qp) \cdot bq \overset{(3)}{=} (bq \cdot dp) \cdot bq,$$

wherefrom it follows the mentioned equivalence. □

Corollary 1. $Par(a, c, b, c) \Leftrightarrow a \bullet b = c$.

If we use the equivalence $Par(a, b, c, d) \Leftrightarrow a \bullet c = b \bullet d$ as the definition for parallelograms, then the properties (P1)–(P3) can be proved simply by the properties of the quasigroup $(Q, \bullet)$. The properties (P1) and (P2) are obvious. For the proof of (P3) we must prove that $a \bullet c = b \bullet d$ and $c \bullet e = d \bullet f$ imply $a \bullet f = b \bullet e$. We obtain

$$\begin{aligned}(a \bullet f) \bullet (c \bullet d) &\overset{(14)}{=} (a \bullet c) \bullet (f \bullet d) \overset{(15)}{=} (a \bullet c) \bullet (d \bullet f) = (b \bullet d) \bullet (c \bullet e) \\ &\overset{(15)}{=} (b \bullet d) \bullet (e \bullet c) \overset{(14)}{=} (b \bullet e) \bullet (d \bullet c) \overset{(15)}{=} (b \bullet e) \bullet (c \bullet d)\end{aligned}$$

and therefore $a \bullet f = b \bullet e$.

Theorem 1 enables us to define the centre of a parallelogram. We say that (a, b, c, d) is a parallelogram with a *centre* o and we write $Par_o(a, b, c, d)$ if $a \bullet c = b \bullet d = o$.

The parallelogram can be defined explicitly in the quasigroup $(Q, \cdot)$ (Figure 3), without the auxiliary points, because of the following theorem.

Theorem 2. *The statement* $Par(a, b, c, d)$ *is equivalent with the equality*

$$d = [b(bc \cdot c) \cdot (bc \cdot c)c][a(a \cdot ab) \cdot (a \cdot ab)b] \tag{16}$$

Proof. According to (P1) it is sufficient only to prove that (16) implies $Par(a, b, c, d)$. Let

$$p = b(bc \cdot c) \cdot (bc \cdot c)c, \tag{17}$$

$$q = a(a \cdot ab) \cdot (a \cdot ab)b. \tag{18}$$

By (16) we have $d = pq$. According to (6) and (3) the equality (17) can be written in the form

$$p = (b \cdot bc)(bc) \cdot (bc \cdot c)c = (b \cdot bc)(bc \cdot c) \cdot (bc \cdot c)$$

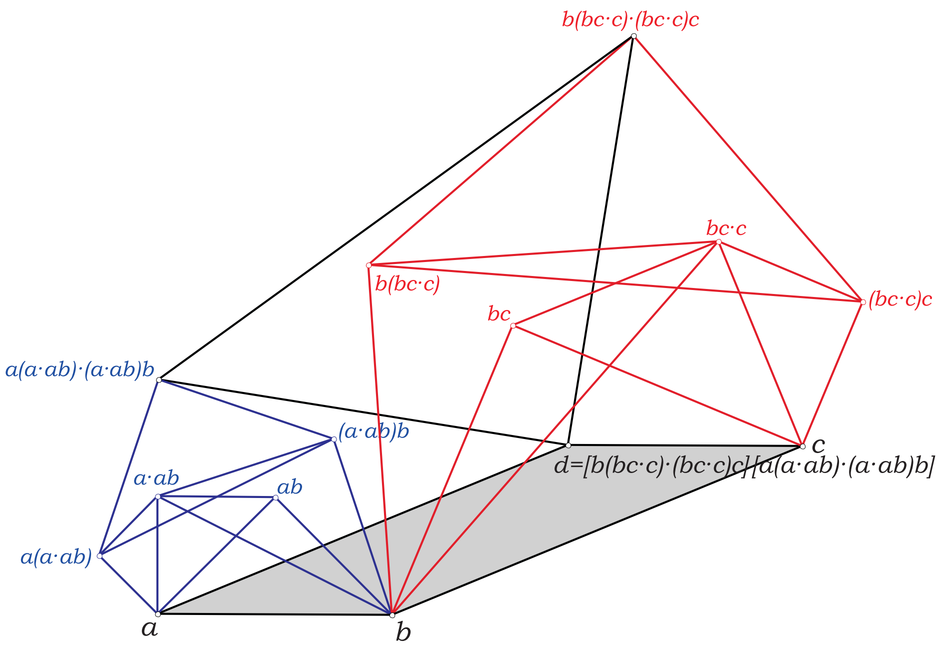


Figure 3.

equivalent with $pb = c$ because of (10). Owing to (7) and (3) the equality (18) can be written in the form

$$q = a(a \cdot ab) \cdot (ab)(ab \cdot b) = (a \cdot ab) \cdot (a \cdot ab)(ab \cdot b)$$

equivalent with $bq = a$ because of (9). This equality can be written as $aa = bq$ by (2). On the other hand we obtain

$$da = pq \cdot bq \overset{(7)}{=} pb \cdot q = cq.$$

The equalities $aa = bq$ and $da = cq$ prove the statement $Par(a, b, c, d)$. $\square$

Corollary 2. *$Par(a, b, c, d)$ holds if and only if there are two points p and q such that $pb = c$, $bq = a$, $pq = d$.*

Figure 4 shows how the equalities $pb = c$, $bq = a$, $pq = d$ imply $Par(a, b, c, d)$ in the quasigroup $\mathbb{C}(\frac{1+i}{2})$.

Using Theorem 1 let us prove some new properties of the relation Par in any idempotent medial commutative quasigroup $(Q, \bullet)$.

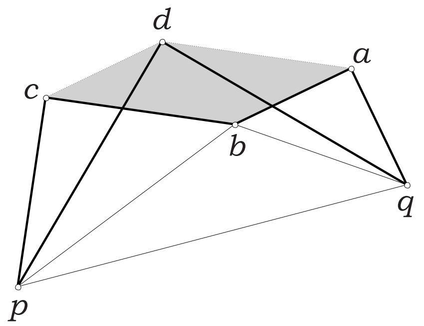


Figure 4.

Theorem 3. *Let* $Par_{o'}(a', b', c', d')$. *The statements* $Par_o(a, b, c, d)$ *and* $Par_{o \bullet o'}(a \bullet a', b \bullet b', c \bullet c', d \bullet d')$ *are equivalent.*

Proof. It is sufficient to prove the equivalence of the equalities $a \bullet c = o$ and $(a \bullet a') \bullet (c \bullet c') = o \bullet o'$ if we have the equality $a' \bullet c' = o'$. But, this is obvious because of

$$(a \bullet c) \bullet o' = (a \bullet c) \bullet (a' \bullet c') \overset{(14)}{=} (a \bullet a') \bullet (c \bullet c'). \quad \square$$

For any $p \in Q$ we have $Par_p(p, p, p, p)$ because of (13). Therefore, we obtain:

Corollary 3. $Par_o(a, b, c, d) \Rightarrow Par_{p \bullet o}(p \bullet a, p \bullet b, p \bullet c, p \bullet d)$.

$Par_o(a, b, c, d)$ implies $Par_o(b, c, d, a)$ and we obtain:

Corollary 4. $Par_o(a, b, c, d) \Rightarrow Par_o(a \bullet b, b \bullet c, c \bullet d, d \bullet a)$.

But, we have more generally:

Theorem 4. *For any points* a, b, c, d *the statement* $Par(a \bullet b, b \bullet c, c \bullet d, d \bullet a)$ *holds.*

Proof. We obtain

$$(a \bullet b) \bullet (c \bullet d) \overset{(15)}{=} (a \bullet b) \bullet (d \bullet c) \overset{(14)}{=} (a \bullet d) \bullet (b \bullet c) \overset{(15)}{=} (b \bullet c) \bullet (d \bullet a). \quad \square$$

Corollary 5. *It holds* $Par(a \bullet b, b \bullet c, c \bullet a, a)$ *for any points* a, b, c.

A concept of a square is defined in [17]. We say that (a, b, c, d) is a square with the centre o and we write $S_o(a, b, c, d)$ or simply $S(a, b, c, d)$ if $ab = bc = cd = da = o$. Then we have the equalities $ac = d$, $bd = a$, $ca = b$, $db = c$ too. Any two of these four equalities imply $S(a, b, c, d)$. In [17, Th. 2] it is proved that $S_o(a, b, c, d)$ implies $o = a \bullet c = b \bullet d$, i.e., we have:

Theorem 5. *$S_o(a,b,c,d) \Rightarrow Par_o(a,b,c,d)$, i.e., every square is a parallelogram with the same centre.*

The following theorem generalizes Theorem 5 in [17].

Theorem 6. *$Par_o(a,b,c,d) \Leftrightarrow S_o(ba,cb,dc,ad)$.*

Proof. We obtain

$$a \bullet c \overset{(12)}{=} ba \cdot cb$$

and the equalities $a \bullet c = o$ and $ba \cdot cb = o$ are equivalent. Analogously, we have

$$b \bullet d = o \Leftrightarrow cb \cdot dc = o,$$

$$c \bullet a = o \Leftrightarrow dc \cdot ad = o,$$

$$d \bullet b = o \Leftrightarrow ad \cdot ba = o.$$

□

In the quasigroup $\mathbb{C}(\frac{1+i}{2})$ Theorem 6 proves a well–known statement (cf. [13], [2], [3], [9], [7], [10], [12], [11]):

If we construct positively oriented squares on the sides of a given oriented quadrangle, then the centers of these squares form a negatively oriented square if and only if the given quadrangle is a parallelogram.

In [5] and [1, p. 241] a statement is proved, which is illustrated in Figure 5 in the quasigroup $\mathbb{C}(\frac{1+i}{2})$ and can be formulated as the following theorem.

Theorem 7. *If*

$$S_{a'}(b,c,a_1,a_2),\ S_{b'}(c,a,b_1,b_2),\ S_{c'}(a,b,c_1,c_2) \tag{19}$$

and if $\widehat{a}$, $\widehat{b}$, $\widehat{c}$ are points such that

$$Par(b_1,a,c_2,\widehat{a}),\ Par(c_1,b,a_2,\widehat{b}),\ Par(a_1,c,b_2,\widehat{c}) \tag{20}$$

then we have the equalities

$$\widehat{c}\,\widehat{b} = a, \qquad \widehat{a}\,\widehat{c} = b, \qquad \widehat{b}\,\widehat{a} = c, \tag{21}$$

$$\widehat{b} \bullet \widehat{c} = a', \qquad \widehat{c} \bullet \widehat{a} = b', \qquad \widehat{a} \bullet \widehat{b} = c', \tag{22}$$

$$a\widehat{c} = \widehat{b}a = a', \qquad b\widehat{a} = \widehat{c}b = b', \qquad c\widehat{b} = \widehat{a}c = c'.$$

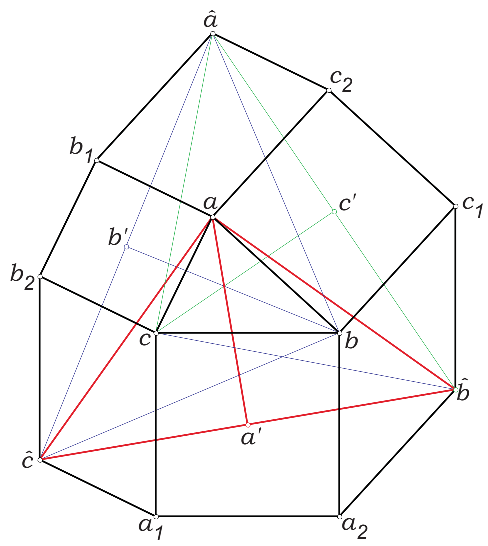


Figure 5.

Proof. Let $\widehat{a}$, $\widehat{b}$, $\widehat{c}$ be points such that $\widehat{a}c = c'$, $\widehat{b}a = a'$, $\widehat{c}b = b'$. According to (19) we have the equalities $b_1c = a$, $ca = b'$, $bc = a'$, $c_2a = c'$ (among others). The equalities $b_1c = a = aa$ and $\widehat{a}c = c' = c_2a$ prove the first statement (20) and analogously the other two statements (20) can be proved. According to (8) from $ca = b' = \widehat{c}b$ it follows $a\widehat{c} = bc$, i.e., $a\widehat{c} = a'$. Therefore we have $a\widehat{c} = \widehat{b}a$ and by (8) it follows $\widehat{c}\widehat{b} = aa$, i.e., the first equality (21). Finally, we obtain the first equality (22): $\widehat{b} \bullet \widehat{c} \overset{(15)}{=} \widehat{c} \bullet \widehat{b} \overset{(12)}{=} a\widehat{c} \cdot \widehat{b}a = a'a' \overset{(2)}{=} a'$. $\square$

A point o is said to be the *center of the square on the segment* (a, b) if $S_o(a, b, c, d)$ holds for some points c and d, i.e., if $ab = o$. A *rotation* for a (positively oriented) right angle about a point o is the mapping $a \mapsto b$ such that $ab = o$.

Theorem 8. *If a_1, a_2, a_3, a_4 are any points and b_{ij} is the center of the square on the segment (a_i, a_j) for any $i, j \in \{1, 2, 3, 4\}$ $(i \neq j)$, then we have the statements $Par(b_{12}, b_{32}, b_{34}, b_{14})$ and $Par(b_{21}, b_{23}, b_{43}, b_{41})$. The rotation for a right angle about the point $a_1 \bullet a_3$ maps $Par(b_{23}, b_{21}, b_{41}, b_{43})$ onto $Par(b_{12}, b_{32}, b_{34}, b_{14})$ and the rotation for a right angle about the point $a_2 \bullet a_4$ maps $Par(b_{12}, b_{32}, b_{34}, b_{14})$ onto $Par(b_{41}, b_{43}, b_{23}, b_{21})$ (Figure 6).*

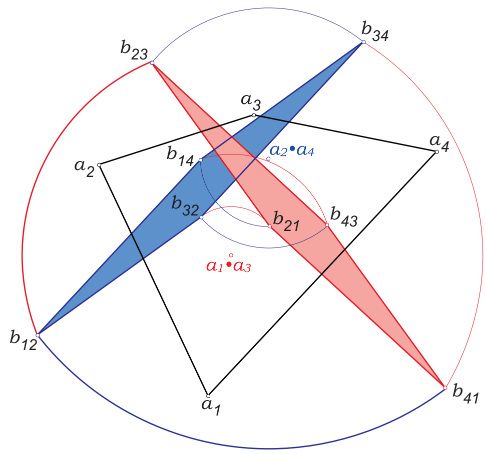


Figure 6.

Proof. According to [15, Th. 28] we have the statement $Par(a_1a_2,\ a_3a_2,\ a_3a_4, a_1a_4)$ and $Par(a_2a_1,\ a_2a_3, a_4a_3, a_4a_1)$ and for any $i, j \in \{1, 2, 3, 4\}$ $(i \neq j)$ we have the equality $a_ia_j = b_{ij}$. The rotation for a right angle about the point $a_1 \bullet a_3$ maps the points b_{23}, b_{21}, b_{41}, b_{43} onto the points b_{12}, b_{32}, b_{34}, b_{14} because of the equalities

$$b_{23}b_{12} = a_2a_3 \cdot a_1a_2 \overset{(12)}{=} a_3 \bullet a_1 \overset{(15)}{=} a_1 \bullet a_3 = a_2a_1 \cdot a_3a_2 = b_{21}b_{32},$$

$$b_{41}b_{34} = a_4a_1 \cdot a_3a_4 \overset{(12)}{=} a_1 \bullet a_3 \overset{(15)}{=} a_3 \bullet a_1 = a_4a_3 \cdot a_1a_4 = b_{43}b_{14}. \qquad \square$$

In the case of the quasigroup $\mathbb{C}(\frac{1+i}{2})$ Theorem 8 proves some statements from [14] and [8].

Theorem 9. *If*

$$S_o(p, a, u, b), \qquad S_{o'}(p, a', u', b'), \tag{23}$$

$$Par(a', p, b, c), \qquad Par(a, p, b', c') \tag{24}$$

holds, then the rotation for a right angle about the point o maps $Par(p, b, c, a')$ onto $Par(a, p, b', c')$ and the rotation for a right angle about the point o' maps $Par(a, p, b', c')$ onto $Par(c, a', p, b)$ (Figure 7).

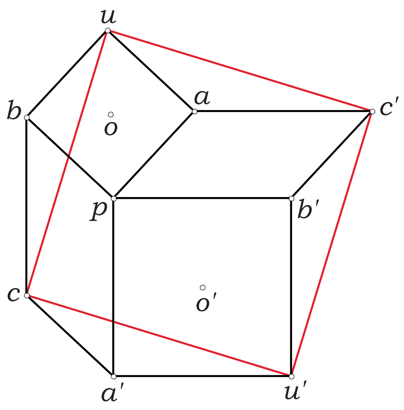


Figure 7.

Proof. Let the statements (23) hold and let c, c' be the points such that $cb' = o$, $c'b = o'$. The equalities

$$pa = o = cb', \quad pa' = o' = c'b$$

imply by (8) the equalities

$$ac = b'p = o', \quad a'c' = bp = o.$$

Now, the equalities

$$a'b' = p = pp,\ cb' = o = bp \ \text{resp.}\ ab = p = pp,\ c'b = o' = b'p$$

prove the statements (24). The last two statements of theorem are the consequences of the equalities
$pa{=}o$, $bp{=}o$, $cb'{=}o$, $a'c'{=}o$ resp. $ac{=}o'$, $pa'{=}o'$, $b'p{=}o'$, $c'b{=}o'$. □

In the case of the quasigroup $\mathbb{C}(\frac{1+i}{2})$ Theorem 9 proves some statements from [4]. The fact that the rotation for a right angle about the points o maps the segment (b, a') onto the segment (p, c') proves that the median from the vertex p of the triangle (p, b', a) is orthogonal to the side (b, a') of the triangle (p, b, a') and equal to the half of this side and a similar fact holds for the median from the vertex p of the triangle $(p,\ b,\ a')$ and the segment (b', a) (cf. [18]).

Theorem 10. *With the hypotheses of Theorem 9 it holds* $S(u, c, u', c')$ (*Figure* 7).

Proof. According to Corollary 2 we observe the implications

$$Par(b,p,a',c),\ u'p=a',\ pu=b\ \Rightarrow u'u=c,$$
$$Par(b',p,a,c'),\ up=a,\ pu'=b'\ \Rightarrow uu'=c',$$

and the equalities $u'u=c$, $uu'=c'$ imply $S(u,c,u',c')$. □

Theorem 11. *The statements* $S(b,c,a_1,a_2)$, $S(c,a,b_1,b_2)$, $S(a,b,c_1,c_2)$ *and the equalities* $a_o=c_1b_2$, $b_o=a_1c_2$, $c_o=b_1a_2$ *imply*

$$Par(c,a,b,a_o),\ Par(a,b,c,b_o),\ Par(b,c,a,c_o) \tag{25}$$

$b_o\bullet c_o=a,\ c_o\bullet a_o=b,\ a_o\bullet b_o=c_o$ (*Figure* 8).

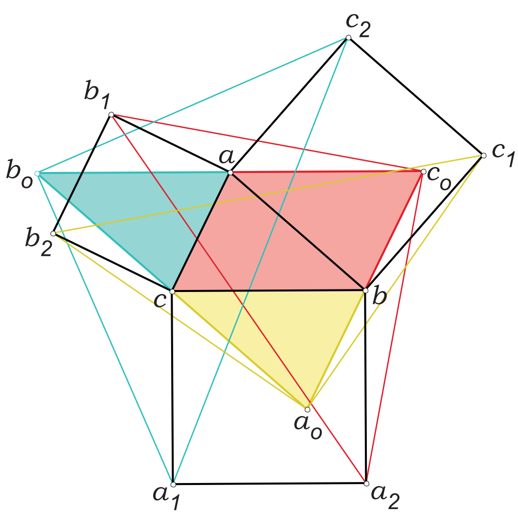


Figure 8.

Proof. We have the equalities $c_1a=b$, $ab_2=c$, $c_1b_2=a_o$ and according to Corollary 2 it follows $Par(c,a,b,a_o)$. Analogously we can prove other statements (25). From $Par(b_o,a,b,c)$ and $Par(b,c,a,c_o)$ by (P3) we obtain $Par(b_o,a,c_o,a)$, i.e., $b_o\bullet c_o=a$. □

References

[1] **P. Baptist**, *Die Entwicklung der neueren Dreiecksgeometrie*, Lehrbücher und Monographien Didaktik Math., Mannheim, 1992.

[2] **A. Barlotti**, *Intorno ad una generalizzazione un noto teorema relativo al triangolo*, Boll. Unione Mat. Ital., III Ser. **7** (1952), 182 – 185.

[3] **A. Barlotti**, *Una propietà degli n-agoni si ottengono transformando di una affinità un n-agono regolare*, Boll. Unione Mat. Ital., III Ser. **10** (1955), 96 – 98.

[4] **V. G. Boltjanskij**, *On a tesselation*, (Rssian), Mat. v škole, 1984, No. 1, 65 – 66.

[5] **H. Demir**, *Problem E* 2124, Amer. Math. Monthly **75** (1968), 899; **76** (1969), 938.

[6] **W. A. Dudek**, *Quadratical quasigroups*, Quasigroups and Related Systems **4** (1997), 9 – 13.

[7] **L. Gerber**, *Napoleon's theorem and the parallelogram inequality for affine-regular polygons*, Amer. Math. Monthly **87** (1980), 644 – 648.

[8] **M. Goljberg**, *Problems* 3275 *and* 3276, Mat. v škole (1989), No. 4, 109 – 110.

[9] **D. I. Han**, *On solving geometrical problems using vectors*, (Russian), Mat. v škole 1974, No. 1, 22 – 25.

[10] **M. Jeger**, *Komplexe Zahlen in der Elementargeometrie*, Elem. Math. **37** (1982), 136 – 147.

[11] **D. Kahle**, *Eine Bemerkung zum Satz von Napoleon–Barlotti für das Parallelogram*, Didaktik Math. **22** (1994), 217 – 218.

[12] **J. Kratz**, *Vom regulären Fünfeck zum Satz von Napoleon–Barlotti*, Didaktik Math. **20** (1992), 261 – 270.

[13] **V. Thébault**, *Problem* 169, Nat. Math. Mag. **12** (1937/38), 55.

[14] **V. Thébault**, *Quadrangle bordé de triangles isoscèles semblables*, Ann. Soc. Sci. Bruxelles **60** (1940/46), 64 – 70.

[15] **V. Volenec**, *Geometry of medial quasigroups*, Yugoslav Academy of Science and ART **421** (1986), 79 – 91.

[16] **V. Volenec**, *Quadratical groupoids*, Note di Mat. **13** (1993), 107 – 115.

[17] **V. Volenec**, *Squares in quadratical quasigroups*, Quasigroups and Related Systems **7** (2000), 37 – 44.

[18] **I. Warburton**, *Brides chair revisited again*, Math. Gaz. **80** (1996), 557 – 558.

Received July 29, 2010

V. Volenec
Department of Mathematics, University of Zagreb, Bijenička c. 30, 10 000 Zagreb, Croatia, *E-mail*: volenec@math.hr

R. Kolar–Šuper
Faculty of Teacher Education, University of Osijek, Lorenza Jägera 9, 31 000 Osijek, Croatia, *E-mail*: rkolar@ufos.hr