The structure of Hentzel–Rúa semifield of order 64

Kravtsova O.V.

Siberian Federal University

Novosibirsk, August 2016

Semifield, nuclei

A *semifield* is an algebraic structure $(W, +, \circ)$, satisfying the following axioms:
1) $(W, +)$ is abelian group;
2) $(W^*, \circ)$ is a loop;
3) $x \circ (y+z) = x \circ y + x \circ z$ and $(y+z) \circ x = y \circ x + z \circ x$ for all $x, y, z \in W$.
Right, middle and left nuclei of semifield W are the subsets

$$N_r = \{x \in W \mid (a \circ b) \circ x = a \circ (b \circ x)\ \forall a, b \in W\},$$
$$N_m = \{x \in W \mid (a \circ x) \circ b = a \circ (x \circ b)\ \forall a, b \in W\},$$
$$N_l = \{x \in W \mid (x \circ a) \circ b = x \circ (a \circ b)\ \forall a, b \in W\}.$$

The *nucleus* of semifield W is an intersection

$$N = N_l \cap N_m \cap N_r.$$

The *center* of semifield W is a set

$$Z = \{x \in N \mid x \circ a = a \circ x\ \forall a \in W\}.$$

The nuclei and the center of any finite semifield W are the subfields.

Spread set

Theorem

Any finite semifield is a linear space over N_l, N_m, N_r, N, Z.

Let W be n-dimensional linear space over $F \simeq \mathbb{Z}_p$ and θ be a bijective map from linear space W to ring $M(n, F)$ of all $(n \times n)$-matrices over F. The image $R = \theta(W)$ is called a **spread set**, if:
1) identity and zero matrices E and O are in R,
2) $R \setminus \{O\}$ is a subset of $GL(n, F)$,
3) R is closed under addition: $\theta(u + v) = \theta(u) + \theta(v)$ $(u, v \in W)$.

In this case we have a semifield $(W, +, \circ)$ with multiplication law

$$x \circ y := x \cdot \theta(y) \qquad (x = (x_1, x_2, ..., x_n),\ y \in W).$$

Degrees, orders, spectra

Let v be an element of multiplicative loop L. An arbitrary product of m multipliers is said to be m**-th degree of** v, if every multiplier coincides with v. If there exist some m-th degree of v which is equal to the identity, then minimal such integer $m \geq 1$ is said to be **the order of** v and denoted by $|v|$. The set of orders $|v|$ of all elements $v \in L$ is said to be **a spectrum of loop** L.
Using the formulas

$$v^{1)} = v = v^{(1}, \qquad v^{m)} = v^{m-1)} \cdot v, \qquad v^{(m} = v \cdot v^{(m-1},$$

we define the right-ordered and the left-ordered m-th degrees of v, respectively, $v^{m)}$ and $v^{(m}$. Analogously we define right order $|v|_r$ and left order $|v|_l$ of v and, also, **right and left spectra** of L.

Problems

For finite proper semifields and quasifields we investigate the following problems which were presented, in mainly, in 2013 at Mech.-Matem. Dept. of Moscow State Univ. (research seminar of chair of algebra) and in 2014[1].

(A) *Enumerate maximal subfields and their possible orders.*

(B) *Find the finite quasifields S with not-one-generated loop S^*.*
Hypotheses: *the loop of any finite semifield is one-generated.*

(C) *What loop spectra S^* of finite semifields and quasifields are possible?*

(D) *Find the automorphism group $Aut\, S$.*

---

[1] V.M. Levchuk, S.V. Panov, P.K. Shtukkert, The structure of finite quasifields and their projective translation planes, Proceed. XII Intern. Conf. on Algebra and Number Theory. Tula, 106–108 (2014).

Wene's conjecture

It was conjectured by Wene[2] that any finite semifield is right or left primitive, i.e. D^* is the set of right- or left-ordered degrees of an element in a semifield D. In 2004 I. Rúa[3] has provided a counter-example to Wene's conjecture by showing that Knuth's Binary semifield of order 32 is neither right nor left primitive. This is the unique semifield with this property, among all 2502 finite semifields of order 32.

Now the primitivity investigations are completed for semifields of orders up to 125. Only two semifields of even orders 32 and 64 are neither left nor right primitive. And the counter-examples for semifields of odd order are not known.

---

[2] G.P. Wene, On the multiplicative structure of finite division rings, Aequationes Math. **41** 791–803 (1991).

[3] I.F. Rua, Primitive and Non-Primitive Finite Semifields, Commun. Algebra. **22** 223–233 (2004).

Wene's conjecture

The investigations of primitivity are based on properties of spread set. It is known that for any finite semifield D with $Z(D) \simeq GF(q)$ and spread set Σ the characteristic polynomial for any matrix from $\Sigma \setminus \{\lambda I \mid \lambda \in GF(q)\}$ has no linear factors. Moreover, it was proved[4]:

Theorem

If D is a finite semifield of dimension d over its center $Z(D) = GF(q)$, then $w \in D$ is a left primitive element of D iff the characteristic polynomial of a linear map $L_w : D \to D$, given by $L_w(x) = wx$, is an irreducible primitive polynomial of degree d over $Z(D)$.

[4] I.R. Hentzel, I. F. Rua, Primitivity of Finite Semifields with 64 and 81 elements, International Journal of Algebra and Computation, **17** (7), 1411–1429 (2007).

Wene's conjecture

We also note some general results on primitivity.

Theorem

Let S be a semifield, n-dimensional over its center $GF(q)$.
(a) If $n = 3$, then S is left and right primitive[a].
(b) If n is prime and q is large enough, then S is left and right primitive[b]

---

[a] I.F. Rua, Primitive and Non-Primitive Finite Semifields, Commun. Algebra. **22** 223–233 (2004).

[b] R. Gow, J. Sheekey, On primitive elements in finite semifields, Finite Fields and Their Applications, **17**, 194–204 (2011).

Wene's conjecture

Cordero and Jha (2009-2010) demonstrate the existence at least one non-primitive quasifield for any order $p^{2n} > 16$ and give the geometrical condition for primitivity:

Lemma

A non-primitive quasifield of square order q^2 exists iff $q > 4$.

Lemma

For all sufficiently large primes p, the semifields coordinatizing a semifield plane Π of order p^5 are all primitive (right and left) if Π does not contain any proper subplane Π_0 of order $> p$.

Hentzel – Rúa semifield of order 64

In 2007 I. Rúa and I. Hentzel has provide[5] second counter-example to Wene's conjecture. This new finite semifield is the unique which is neither left nor right primitive among all finite semifields with 64 elements. These authors construct also 35 semifields of order 64 that not left but are right primitive.

[5] I.R. Hentzel, I. F. Rua, Primitivity of Finite Semifields with 64 and 81 elements, International Journal of Algebra and Computation, **17** (7), 1411–1429 (2007).

Hentzel – Rúa semifield of order 64

Let $\mathcal{H}$ be a 6-dimensional linear space over $\mathbb{Z}_2$,

$$\mathcal{H} = \{x = (x_1, \ldots, x_6) \mid x_i \in \mathbb{Z}_2,\ i = 1, \ldots, 6\},$$

$A_1,\ A_2, \ldots, A_6$ be the matrices in $GL_6(2)$, determined by Hentzel and Rúa. Define the map θ from $\mathcal{H}$ to the ring of (6×6)-matrices over $\mathbb{Z}_2$ by the rule:

$$\theta(x) = x_1 A_1 + \cdots + x_6 A_6, \quad x \in \mathcal{H};$$

θ is a bijection from $\mathcal{H}$ into $GL_6(2) \cup \{0\}$ and $R = \{\theta(x) \mid x \in \mathcal{H}\}$ is a spread set in $GL_6(2) \cup \{0\}$. Define the multiplication rule $*$ on $\mathcal{H}$ as

$$x * y = x \cdot \theta(y) = x \sum_{i=1}^{6} y_i A_i.$$

Then $\langle \mathcal{H}, +, * \rangle$ is a semifield of order 64, which is said to be the Hentzel–Rúa semifield. It is neither right nor left primitive. The vector

$$e = (1, 0, 0, 0, 0, 0)$$

is an identity under multiplication in $\mathcal{H}$.

Automorphism group, maximal subfields

Theorem

The automorphism group of Hentzel–Rúa semifield $\mathcal{H}$ is isomorphic to the symmetric group S_3 and hence has exactly three involution automorphisms.

Theorem

The semifield $\mathcal{H}$ contains exactly six maximal subfields:

5 subfields of order 8, three from them are stabilizators of different involution automorphisms;

the unique subfield of order 4, which is a stabilizator of automorphism of order 3.

Automorphism of order 2

Theorem

Let W be a semifield of order p^n which admits an automorphism τ of order 2. Then $n = 2m$ and W contains the sub-semifield of order $p^{n/2}$

$$\mathcal{F}(\tau) = \{x \in W \mid x^\tau = x\}.$$

Remark. As Hentzel–Rúa semifield $\mathcal{H}$ is of order 64, then sub-semifields which are the stabilizators of involutory automorphisms are all the sub-fileds of order 8.

Spectra

Let's denote the subsets of elements from $\mathcal{H}$:

$$K(m,n,k) = \{x \in \mathcal{H} \mid |x|_l = m,\ |x|_r = n,\ |x| = k\}, \quad m,n,k \in \mathbb{N}.$$

Then, evidently, $K(3,3,3) \cup \{0,e\}$ is a subfield of order 4, $K(7,7,7) \cup \{0,e\}$ is an union of all subfields of order 8. Moreover,

$$|K(6,6,6)| = 12,\ |K(7,7,6)| = 6,\ |K(12,12,7)| = 6,\ |K(15,15,5)| = 6.$$

The calculation of orders allows to

Lemma

The spectrum of the loop $\mathcal{H}^*$ *is* $\{1,3,5,6,7\}$, *the left and right spectra coincide with* $\{1,3,6,7,12,15\}$,

$$\mathcal{H}^* = K(1,1,1) \cup K(3,3,3) \cup K(7,7,7) \cup K(6,6,6) \cup \\ \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5).$$

Remarks on orders

Remark 1. For any $x \in \mathcal{H}^*$ its left order coincides with right order,

$$|x|_l = |x|_r;$$

for any $x \in \mathcal{H}^* \setminus \{e\}$ (left, right) order of element $x + e$ coincides with (left, right) order of x:

$$|x + e|_l = |x|_l, \quad |x + e|_r = |x|_r, \quad |x + e| = |x|.$$

Remark 2. For any $x \in \mathcal{H}^* \setminus \{e\}$

$$(|x|_l, |\mathcal{H}^*|) \neq 1, \quad (|x|_r, |\mathcal{H}^*|) \neq 1.$$

Remark 3. Let $x \in \mathcal{H}$ and for any $n \in \mathbb{N}$

$$x^{n)} = x^{(n}.$$

Then x belongs to the union of subfields $\{0, e\} \cup K(3, 3, 3) \cup K(7, 7, 7)$.

One-generability conjecture

Hentzel–Rúa semifield $\mathcal{H}$ is not primitive but the loop W^* is one-generated:

Lemma

Any element $x \in K(6,6,6) \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5)$ *generates the loop* $\mathcal{H}^*$*, and for any* $n \geq 10$ $\mathcal{H}^*$ *is a union of all* n*-th degrees of* x*.*

Lemma

For any $x \in \mathcal{H}$

$$x^{4)} = x^{(4}, \qquad x^{8)} = x^{(8}.$$

Lemma

Hentzel–Rúa semifield $\mathcal{H}$ *is not commutative and*

$$N_l = N_m = N_r = N = Z = \{0, e\} \simeq \mathbb{Z}_2.$$

Map $x \to x^2$

Lemma

The map $\varphi : x \to x^2$ *is a bijection on* $\mathcal{H}$, *and*

$$K(3,3,3) \xrightarrow{\varphi} K(3,3,3),$$
$$K(7,7,7) \xrightarrow{\varphi} K(7,7,7),$$
$$K(6,6,6) \xrightarrow{\varphi} K(6,6,6),$$
$$K(7,7,6) \xrightarrow{\varphi} K(12,12,7) \xrightarrow{\varphi} K(15,15,5) \xrightarrow{\varphi} K(7,7,6).$$

Primitivity and ciclycity

Definition

Finite semifield D, d-dimensional over its center $Z(D)$, is said to be:
1) **left-ciclyc** if there exists such an element $a \in D$ (**left-ciclyc** element) that

$$\{e,\ a,\ a^{(2}, \ldots, a^{(d-1}\}$$

is $Z(D)$-base of semifield D;
2) **left-primitive** if there exists such an element $a \in D$ (**left-primitive** element) that

$$D^* = \{e,\ a,\ a^{(2},\ a^{(3}, \ldots\},$$

where $a^{(2} = aa$, $a^{(3} = aa^{(2}$, ...

Any left-primitive semifield is also left-ciclyc[6]. Nevertheless, even two known exceptional semifields of orders 32 and 64 are ciclyc.

[6] I.R. Hentzel, I. F. Rua, Primitivity of Finite Semifields with 64 and 81 elements, International Journal of Algebra and Computation, **17** (7), 1411–1429 (2007).

Primitivity and ciclycity

Lemma

Any element $x \in K(7,7,6) \cup K(12,12,7)$ *is both left-ciclyc and right-ciclyc, i.e.*

$$\{e,\ x,\ x^2,\ x^{(3},\ x^{(4},\ x^{(5}\} \text{ and } \{e,\ x,\ x^2,\ x^{3)},\ x^{4)},\ x^{5)}\}$$

are the bases of linear space $\mathcal{H}$ *over* $\mathbb{Z}_2$.

Corollary

Hentzel–Rúa semifield $\mathcal{H}$ *is both left-ciclyc and right-ciclyc.*

Minimal polynomials

Let a be an element from $\mathcal{H}^*$ and $\theta(a)$ is a correspondent matrix from spread set,

$$x * a = x\theta(a) \quad (x \in \mathcal{H}).$$

We shall denote by $\mu_a(x)$ the **minimal polynomial of matrix** $\theta(a)$ (according the classical definition) and also introduce the minimal left and right polynomials of element a.

The polynomial

$$M_a^r(x) = c_m * x^{m)} + c_{m-1} * x^{m-1)} + \cdots + c_2 * x^2 + c_1 * x + c_0 * e$$

(where $c_m, \ldots, c_1, c_0 \in \mathbb{Z}_2$) is said to be **right minimal polynomial of element** $a \in \mathcal{H}^*$ if $m \in \mathbb{N}$ is minimal degree such that $M_a^r(a) = 0$. The left minimal polynomial $M_a^l(x)$ of element a we define analogously.

Minimal polynomials

Lemma

The element $a \in \mathcal{H}^*$ is left-ciclyc if and only if its left minimal polynomial $M_a^l(x)$ is of degree 6.

(Analogously for right-ciclyc element.)

Remark. In general, the left (right) minimal polynomial of element $a \in \mathcal{H}^*$ does not coincide with minimal polynomial $\mu_a(x)$ of the matrix $\theta(a)$.

The information on minimal polynomials is resumed in the table.

The minimal polynomials of element $a \in K$ and matrix $\theta(a)$

Subset K	$M_a^r(x)$	$\mu_a(x)$
$K(7,7,6)$	$x^{6)} + x^{5)} + x^{4)} + x^{3)} + x^2 + x + e$	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$K(12,12,7)$	$x^{6)} + x^{5)} + x^{3)} + x + e$	$x^6 + x^5 + x^3 + x + 1$
$K(15,15,5)$	$x^{4)} + x + e$	$x^6 + x^5 + x^4 + x^3 + 1 =$ $= (x^4 + x + 1)(x^2 + x + 1)$
$K(6,6,6)$	$x^{4)} + x^2 + e$	$x^6 + x^5 + x^3 + x + 1 =$ $= (x^4 + x^2 + 1)(x^2 + x + 1)$
$K(7,7,7)$	$x^{3)} + x + e$ or $x^{3)} + x^2 + e$	$x^6 + x^2 + 1 = (x^3 + x + 1)^2$ or $x^6 + x^4 + 1 = (x^3 + x^2 + 1)^2$
$K(3,3,3)$	$x^2 + x + e$	$x^2 + x + 1$

Thank you for your attention!