9. *Лушников А.А.* Некоторые новые аспекты теории коагуляции // Изв. АН СССР, Физ. атмосферы и океана. 1978. Т. 14. № 10. С. 1048-1055.

10.*Бурмистров А.В., Коротченко М.А.* Весовые алгоритмы метода Монте-Карло для оценки и параметрического анализа решения кинетического уравнения коагуляции // Сиб. журн. вычисл. математики. 2014. Т. 17. № 2. С. 125-138.

11.*Burger M., Caffarelli L., Markowich P., Wolfram M.T.* On a Boltzmann-type price formation model // Proc. R. Soc. A 2013. V. 469. No. 2157. 20130126.

Simulation of dynamics of multiparticle systems for kinetic model consideration

***Mariya Korotchenko**, PhD, Research Associate, Institute of Computational Mathematics and Mathematical Geophysics SB RAS*

***Aleksandr Burmistrov**, PhD, Research Associate, Institute of Computational Mathematics and Mathematical Geophysics SB RAS*

We consider four problems, three of which are not related to rarefied gas dynamics, but are described by the Boltzmann type equations. To solve these problems, we propose to use the integral equation of the second kind approach and the weight simulation of Markov chain, the latter is uniquely determined by the coefficients of the integral equations.

Keywords: Monte Carlo method, pair interactions, vehicular traffic flow, coagulation equation, price formation

УДК 512.554

О ГИПОТЕЗЕ ЛЕВОПРИМИТИВНОСТИ КОНЕЧНОГО ПОЛУПОЛЯ

***Ольга Вадимовна Кравцова**, к. ф.-м.н., доцент*
Тел. 8 902 925 08 40, E-mail: ol71@bk.ru
Сибирский федеральный университет
http://www.sfu-kras.ru

Изучаются алгебраические свойства полуполя порядка 64, представляющего один из двух известных контрпримеров к гипотезе Г. Вене о левопримитивности конечного полуполя. Описаны подполя, автоморфизмы, спектр, доказана однопорожденность мультипликативной лупы ненулевых элементов.

Ключевые слова: полуполе, спектр полуполя, левопримитивность, автоморфизм.

Работа выполнена при финансовой поддержке РФФИ, гранты 15-01-04897 А, 16-01-00707

О.В. Кравцова

Конечным полуполем W называется конечное неассоциативное кольцо с единицей e, такое, что множество ненулевых элементов $W^* = W \setminus \{0\}$ является лупой по умножению. Полуполе является векторным пространством над ассоциативно-коммутативным центром и имеет порядок p^n, где p – простое число. Описание строения мультипликативной лупы W^* произвольного конечного полуполя W является открытой проблемой. В частности, если W – конечное поле, то W^* – циклическая группа. В 1991 году Г. Вене предположил, что мультипликативная лупа всякого конечного полуполя является либо левопримитивной, либо правопримитивной [1].

Определение 1. Пусть W – конечное полуполе и $a \in W$. *Левоупорядоченные степени* элемента a определяются правилом:

$$a^{(0} = e, \quad \forall i \in \mathbb{N}\colon\ a^{(i+1} = aa^{(i}.$$

Правоупорядоченные степени определяются аналогично.

Определение 2. Конечное полуполе W называется *левопримитивным* (*правопримитивным*), если найдется такой элемент $a \in W$, что W^* совпадает с множеством всех левоупорядоченных (правоупорядоченных) степеней элемента a.

В 2004 году И. Руа показал [2], что полуполе Кнута порядка 32 не является ни лево- ни правопримитивным, опровергнув гипотезу Вене. Далее, в 2007 году И. Руа и И. Хентзел [3] построили второй контрпример – полуполе порядка 64, также не являющееся ни лево- ни правопримитивным. Кроме того, они привели примеры полуполей порядка 64, являющихся односторонне-примитивными, и доказали, что все полуполя порядка 81 являются и лево-, и правопримитивными.

В работе [4] описано строение полуполя Кнута – Руа порядка 32: перечислены порядки элементов, подполя, указаны некоторые аномальные свойства изотопных полуполей. В настоящей работе автор исследует строение второго известного на текущий момент контрпримера к гипотезе Вене – полуполя Хентзела – Руа порядка 64.

Пусть W – 6-мерное линейное пространство над полем $\mathbb{Z}_2$,

$$W = \{x = (x_1, x_2, x_3, x_4, x_5, x_6) \mid x_i \in \mathbb{Z}_2, i = 1, \dots, 6\},$$

$A_1, A_2, \dots, A_6$ – матрицы в $GL_6(2)$: $A_1 = E$ – единичная матрица,

$$A_2 = \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&1&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&0&0&1\\ 1&0&0&1&1&0 \end{pmatrix}, A_3 = \begin{pmatrix} 0&0&1&0&0&0\\ 1&1&0&0&0&0\\ 0&1&1&0&0&0\\ 1&1&0&0&0&1\\ 0&0&0&1&1&0\\ 1&1&1&0&1&1 \end{pmatrix}, A_4 = \begin{pmatrix} 0&0&0&1&0&0\\ 0&1&0&0&1&0\\ 0&1&1&0&0&1\\ 0&1&1&0&1&1\\ 1&1&0&0&0&0\\ 1&0&0&0&0&1 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 0&0&0&0&1&0\\ 1&0&0&0&0&1\\ 1&0&0&1&1&0\\ 1&1&0&0&1&0\\ 0&0&1&1&0&1\\ 1&1&0&1&1&0 \end{pmatrix}, \quad A_6 = \begin{pmatrix} 0&0&0&0&0&1\\ 0&1&0&1&1&0\\ 0&1&0&0&1&1\\ 1&0&0&1&0&0\\ 0&1&0&1&0&0\\ 0&0&1&0&0&1 \end{pmatrix}.$$

Определим отображение θ из W в кольцо 6×6-матриц над $\mathbb{Z}_2$:

$$\theta(x) = x_1A_1 + x_2A_2 + x_3A_3 + x_4A_4 + x_5A_5 + x_6A_6, \quad x \in W.$$

Как показано в [3], $\det\theta(x) \neq 0$ для всех $x \neq 0$, поэтому θ – биекция из W в $GL_6(2) \cup \{0\}$. Умножение $*$ на W зададим правилом

$$x * y = x \cdot \theta(y) = x(y_1A_1 + y_2A_2 + y_3A_3 + y_4A_4 + y_5A_5 + y_6A_6).$$

Тогда $\langle W, +, * \rangle$ - полуполе порядка 64; назовем его полуполем Хентзела – Руа. Оно не является ни лево- ни правопримитивным [3]. Нейтральным по умножению является элемент $e = (1,0,0,0,0,0)$.

Лемма 1. *Полуполе Хентзела – Руа W порядка 64 содержит простое подполе $\{0, e\}$ порядка 2, единственное подполе F порядка 4 и пять подполей H_i, $i = 1, \ldots, 5$ порядка 8. Других подполей в W нет.*

Доказательство. Рассмотрим множество $F = \{0, e, a = (0,1,0,0,0,1), a + e\}$

и вычислим произведение

$$a * a = a \cdot \theta(a) = a(A_2 + A_6) = (1,1,0,0,0,1) = a + e;$$

отсюда $F \cong GF(4)$ – подполе порядка 4.

Рассмотрим $h_1 = (0,0,0,0,1,0)$ и вычислим h_1^2 и h_1^3:

$h_1^2 = h_1\theta(h_1) = h_1A_5 = (0,0,1,1,0,1)$, $h_1^{(3} = h_1^{3)} = (1,0,0,0,1,0) = e + h_1$.

Тогда h_1 – корень многочлена $x^3 + x + 1$, неприводимого над $\mathbb{Z}_2$, поэтому множество $H_1 = \{0, e, h_1, h_1^2, \ldots, h_1^6\}$ – подполе порядка 8 в W. Аналогично, имеем:

$h_2 = (0,0,0,1,0,1)$, $h_2^2 = (0,1,0,1,1,1)$, $h_2^{(3} = h_2^{3)} = (1,1,0,1,1,1) = e + h_2^2$,

$H_2 = \{0, e, h_2, h_2^2, \ldots, h_2^6\}$;

$h_3 = (0,0,0,1,1,1)$, $h_3^2 = (1,1,1,0,1,0)$, $h_3^{(3} = h_3^{3)} = (1,0,0,1,1,1) = e + h_3$,

$H_3 = \{0, e, h_3, h_3^2, \ldots, h_3^6\}$;

$h_4 = (0,0,1,0,0,0)$, $h_4^2 = (0,1,1,0,0,0)$, $h_4^{(3} = h_4^{3)} = (1,0,1,0,0,0) = e + h_4$,

$H_4 = \{0, e, h_4, h_4^2, \ldots, h_4^6\}$;

$h_5 = (0,0,1,0,1,0)$, $h_5^2 = (1,1,0,1,0,1)$, $h_5^{(3} = h_5^{3)} = (0,1,0,1,0,1) = e + h_5^2$,

$H_5 = \{0, e, h_5, h_5^2, \ldots, h_5^6\}$.

Поскольку элементы h_1, h_3, h_4 – корни многочлена $x^3 + x + 1$, h_2, h_5 – многочлена $x^3 + x^2 + 1$ (неприводимых над $\mathbb{Z}_2$), то H_1, H_2, H_3, H_4, H_5 являются подполями порядка 8 в полуполе W.

Рассмотрим множество $U = W \setminus (F \cup H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5)$. Для каждого элемента $x \in U$ левая и правая третьи степени не совпадают:

$$x^{(3} = x * (x * x) \neq (x * x) * x = x^{3)}.$$

Следовательно, полуполе W не содержит подполей, кроме простого подполя, F и H_i, $i = 1, \ldots, 5$.

Определение 3. *Левым порядком* элемента $a \in W$, $a \neq e$, назовем такое наименьшее натуральное число $m = |a|_l$, что $a^{(m} = e$. *Правый порядок* $|a|_r$ определим аналогично. *Порядком* $|a|$ назовем наименьший показатель степени элемента a, при некоторой расстановке скобок равной единичному элементу. Множество порядков (левых, правых) всех элементов лупы будем называть ее *спектром* (левым, правым).

Очевидно, что $|a| \leq |a|_l$ и $|a| \leq |a|_r$ для всех $a \neq e$. Введем обозначение для подмножеств элементов в W, имеющих определенный левый и правый порядок: пусть для $a, b, c \in \mathbb{N}$

$$K(a,b,c) = \{x \in W \mid |x|_l = a, |x|_r = b, |x| = c\}.$$

Тогда, очевидно,

$K(3,3,3) = \{x \in W \mid |x|_l = |x|_r = |x| = 3\} = \{a = (0,1,0,0,0,1), e + a = (1,1,0,0,0,1)\}$,

$F = K(3,3,3) \cup \{0, e\}$;

$K(7,7,7) = \{x \in W \mid |x|_l = |x|_r = |x| = 7\} = (H_1 \cup H_2 \cup H_3 \cup H_4 \cup H_5) \setminus \{0, e\}$,

$|K(7,7,7)| = 30$;

$K(7,7,7) \cup \{0, e\}$ – объединение всех подполей порядка 8. Далее,

$K(6,6,6) = \{x \in W \mid |x|_l = |x|_r = |x| = 6\} =$

$= \{a_1 = (0,0,0,1,0,0), a_2 = (0,0,1,1,1,0), a_3 = (0,1,0,0,1,1), a_4 = (0,1,1,0,1,1),$

$a_5 = (0,1,1,1,0,0), a_6 = (0,1,1,1,1,0), e + a_1, e + a_2, e + a_3, e + a_4, e + a_5, e + a_6\}$,

$|K(6,6,6)| = 12$;

$K(7,7,6) = \{x \in W \mid |x|_l = |x|_r = 7, |x| = 6\} =$

$= \{b_1 = (0,0,0,0,0,1), b_2 = (0,0,0,1,1,0), b_3 = (0,1,0,1,1,0), e + b_1, e + b_2, e + b_3\}$,

$|K(7,7,6)| = 6$;

$K(12,12,7) = \{x \in W \mid |x|_l = |x|_r = 12, |x| = 7\} =$

$= \{c_1 = (0,0,1,0,0,1), c_2 = (0,0,1,1,0,0), c_3 = (0,1,0,1,0,0), e + c_1, e + c_2, e + c_3\}$,

$|K(12,12,7)| = 6$;

$K(15,15,5) = \{x \in W \mid |x|_l = |x|_r = 15, |x| = 5\} =$

$= \{d_1 = (0,0,0,0,1,1), d_2 = (0,0,1,0,1,1), d_3 = (0,1,1,0,0,1), e + d_1, e + d_2, e + d_3\}$,

$|K(15,15,5)| = 6$.

Из этого перечисления следует

Лемма 2. *Спектр лупы W^* ненулевых элементов полуполя W Хентзела – Руа порядка 64 равен* $\{1,3,5,6,7\}$, *левый и правый спектры совпадают и равны* $\{1,3,6,7,12,15\}$.

Замечание 1. Для любого элемента $x \in W^*$ левый и правый порядки равны,

$$|x|_l = |x|_r,$$

для любого элемента $x \in W^* \setminus \{e\}$ (левый, правый) порядок элемента $e + x$ равен (левому, правому) порядку элемента x,

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

Лемма 3. Отображение $\varphi: x \to x^2$, $x \in W$, является биекцией на W, причем

$$\varphi\big(K(3,3,3)\big) = K(3,3,3), \ \ \varphi\big(K(7,7,7)\big) = K(7,7,7), \ \ \varphi\big(K(6,6,6)\big) = K(6,6,6),$$

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

Доказательство. Вычисляя для каждого $x \in W$ значение

$\varphi(x) = x * x = x\theta(x) = x(x_1A_1 + x_2A_2 + x_3A_3 + x_4A_4 + x_5A_5 + x_6A_6)$,

отмечаем, что $\{\varphi(x) \mid x \in W\} = W$. Укажем орбиты элементов W под действием φ. Для упрощения записи обозначим элемент $x = (x_1, x_2, x_3, x_4, x_5, x_6)$ числом

$$32x_1 + 16x_2 + 8x_3 + 4x_4 + 2x_5 + x_6,$$

тогда $(0,0,0,0,0,0) \leftrightarrow 0$, $e = (1,0,0,0,0,0) \leftrightarrow 32$,

$$K(3,3,3) = \{17,19\},\quad K(6,6,6) = \{4,14,19,27,28,30,36,46,51,59,60,62\},$$

$$K(7,6,6) = \{1,6,22,33,38,54\},\quad K(12,12,7) = \{9,12,20,40,44,52\},$$

$$K(15,15,5) = \{3,11,25,35,43,57\}.$$

Остальные элементы $K(7,7,7)$ и образуют 10 орбит длины 3:

$$(2,13,15),\quad (5,23,50),\quad (7,58,61),\quad (8,24,16),\quad (10,53,31),$$

$$(18,37,55),\quad (21,63,42),\quad (26,29,39),\quad (34,45,47),\quad (40,56,48).$$

Элементы каждой орбиты записаны в порядке $(x, \varphi(x), \varphi^2(x), \dots)$. Множество $K(6,6,6)$ является объединением двух орбит длины 6:

$$(4,27,46,36,59,14),\quad (19,62,28,51,30,60).$$

Множество $K(7,7,6) \cup K(12,12,7) \cup K(15,15,5)$ есть объединение трех 6-элементных орбит:

$$(1,9,57,33,41,25),\quad (3,38,52,35,6,20),\quad (11,54,12,43,22,44),$$

причем для каждого $x \in K(7,7,6)$

$$\varphi(x) \in K(12,12,7),\quad \varphi^2(x) \in K(15,15,5),\quad \varphi^3(x) \in K(7,7,6).$$

Отметим также, что φ не является автоморфизмом полуполя W, так как условия

$$\varphi(x + y) = \varphi(x) + \varphi(y),\quad \varphi(x * y) = \varphi(x) * \varphi(y)$$

выполняются не для всех элементов полуполя. Также заметим, что $|\varphi| = 6$.

Лемма 4. Каждый элемент $x \in K(6,6,6) \cup K(7,7,6) \cup K(12,12,7) \cup K(15,15,5)$ порождает лупу W^*, причем для любого $n \geq 10$ все -е степени элемента x исчерпывают W^*.

Доказательство. Третья степень каждого элемента $x \in U$ определяется двумя способами:

$$x^{(3} = x * (x * x) \neq (x * x) * x = x^{3)}.$$

Вычисляя последовательно четвертые, пятые и следующие степени элемента x всеми возможными способами, получаем все элементы W^*. Для каждого x выберем наименьшее число $n = n(x)$ такое, что все -е степени элемента x образуют W^*, тогда

$$n(x) = 8 \quad \text{для} \quad x \in K(7,7,6),$$

$$n(x) = 9 \quad \text{для} \quad x \in K(6,6,6) \cup K(15,15,5),$$

$$n(x) = 10 \quad \text{для} \quad x \in K(12,12,7).$$

Лемма доказана.

Лемма 5. Группа автоморфизмов полуполя W имеет порядок 6 и изоморфна симметрической группе S_3.

Доказательство. Если τ – автоморфизм полуполя W, то для всех $x, y \in W$

$$\tau(x + y) = \tau(x) + \tau(y), \quad \tau(x * y) = \tau(x) * \tau(y).$$

Очевидно, τ является линейным преобразованием векторного пространства W и задается некоторой 6×6-матрицей T над $\mathbb{Z}_2$. Выберем базис W:

$$e_1 = (1,0,0,0,0,0) = e, \quad e_2 = (0,1,0,0,0,0), \quad e_3 = (0,0,1,0,0,0),$$

$$e_4 = (0,0,0,1,0,0), \quad e_5 = (0,0,0,0,1,0), \quad e_6 = (0,0,0,0,0,1)$$

и выясним, при каком условии верно

$$\tau(e_i * e_j) = \tau(e_i) * \tau(e_j), \quad i, j = 1,2, \dots, 6.$$

Так как $e_i * e_j = e_i\theta(e_j) = e_iA_j$, то $\tau(e_i * e_j) = e_iA_jT$; далее

$$\tau(e_i) * \tau(e_j) = e_iT\theta(e_jT) = e_iT\theta(t_{j1}, t_{j2}, \dots, t_{j6}) = e_iT\textstyle\sum_{k=1}^{6} t_{jk}A_k.$$

В силу произвольности $i = 1, \dots, 6$ получим условие

$$T\textstyle\sum_{k=1}^{6} t_{jk}A_k = A_jT, \quad j = 1, \dots, 6. \tag{1}$$

Для $j = 1$ имеем $t_{11} = 1$, $t_{12} = t_{13} = \dots = t_{16} = 0$. Каждая матрица $T \in GL_6(2)$, удовлетворяющая условию (1), задает автоморфизм полуполя W. Этому условию удовлетворяют ровно 6 матриц:

$$T_1 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&0&0&1&1&1\\ 1&1&1&0&1&0\\ 1&0&1&1&1&0\\ 0&0&1&1&1&1\\ 0&1&0&1&1&0 \end{pmatrix}, \; T_2 = \begin{pmatrix} 1&0&0&0&0&0\\ 1&1&0&1&1&1\\ 0&1&0&0&1&0\\ 1&1&1&0&1&1\\ 0&0&1&1&0&1\\ 1&0&0&1&1&0 \end{pmatrix}, \; T_3 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&0&0&1&1&1\\ 1&1&1&0&1&0\\ 1&1&0&0&1&1\\ 0&1&0&1&0&1\\ 1&1&0&1&1&0 \end{pmatrix},$$

$$T_4 = \begin{pmatrix} 1&0&0&0&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&1&1&1&0&0\\ 1&0&1&0&1&0\\ 1&0&0&0&0&1 \end{pmatrix}, \; T_5 = \begin{pmatrix} 1&0&0&0&0&0\\ 1&1&0&1&1&1\\ 0&1&0&0&1&0\\ 1&1&1&1&1&0\\ 1&1&1&1&1&1\\ 0&0&0&1&1&0 \end{pmatrix}, \; T_6 = E.$$

Так как $T_2 = T_1^2, T_1 = T_2^2, T_3^2 = T_4^2 = T_5^2 = E$, то

$$Aut\, W = \{T_1, T_2, T_3, T_4, T_5, T_6\} \cong S_3.$$

Лемма доказана.

Замечание 2. Обозначим $\mathcal{F}(\tau)$ множество элементов полуполя W, фиксируемых преобразованием τ. Непосредственными вычислениями выясняется, что

$$\mathcal{F}(T_1) = \mathcal{F}(T_2) = F,\ \ \mathcal{F}(T_3) = H_2,\ \ \mathcal{F}(T_4) = H_4,\ \ \mathcal{F}(T_5) = H_3.$$

Автор считает, что все перечисленные выше результаты (леммы 1–5) являются новыми. Ослабление ассоциативности умножения приводит к появлению свойств конечного полуполя, являющихся аномальными в сравнении со свойствами конечного поля. Отметим, что изученное полуполе Хентзела – Руа содержит пять различных подполей одного и того же порядка 4 (свойство, невозможное для поля $GF(64)$). Кроме того, порядок мультипликативной лупы ненулевых элементов не делится на порядки элементов 5 и 6, а также на правые (левые) порядки 6, 12 и 15. Однако даже не являющееся ни лево-, ни правопримитивным полуполе W удовлетворяет условию однопорожденности лупы W^*.

Литература

1. *Wene G.P.* On the multiplicative structure of finite division rings // Aequation Mathematicae. 1991. № 41. С. 222-233.

2. *Rúa I.F.* Primitive and non-primitive finite semifields // Commun. Algebra. 2004. Вып. 32. № 2. С. 793-803.

3. *Hentzel I.R., Rúa I.F.* Primitivity of finite semifields with 64 and 81 elements // Int. J. Algebra Comput. 2007. Вып. 17. № 7. С. 1411-1429.

4. *Левчук В.М., Штуккерт П.К.* Строение квазиполей малых четных порядков // Тр. ИММ УрО РА. 2015. Вып. 21. № 3. С. 197-212.

On right-primitivity conjecture for finite semifield

Olga Vadimovna Kravtsova, *PhD., Associate Professor, Siberian federal university*

The author consider the algebraic properties of the semifield of order 64 that is one of two known counter-examples to G. Wene conjecture of left-primitivity for any finite semifield. The subfileds, automorphisms and spectrum are described. It is proved that the multiplicative loop of non-zero elements of this semifield is singly-generated.

Keywords – semifield, spectrum of semifield, left-primitivity, automorphism.

УДК 539.37

МОДЕЛИРОВАНИЕ МЕДЛЕННОГО ДВИЖЕНИЯ СЫПУЧЕЙ СРЕДЫ В СХОДЯЩЕМСЯ КАНАЛЕ

Ольга Игоревна Кузоватова, *к ф.-м.н, доцент*
Тел.: 8 391 206 2116, e-mail: oik17@yandex.ru
Сибирский федереальный университет
http://www.sfu-kras.ru

Для исследования локализации деформаций при движении сыпучей среды под действием собственного веса в сходящемся канале используются вариационные принципы теории предельного равновесия, установленные в рамках специальной математической модели материала, по-разному сопротивляющегося растяжению и сжатию. Получена оценка для коэффициента запаса.