МАТЕМАТИКА

К. Л. Глуско, С. С. Титов

О КВАДРАТИЧНЫХ РАСШИРЕНИЯХ БИНАРНЫХ ПОЛЕЙ

Статья посвящена расширению бинарных полей посредством операции симметричного квадратичного расширения, что тесно связано с информационными технологиями и микропроцессорной техникой. Последовательно вычислены многочлены квадратичных расширений. Рассмотрены примеры.

Ключевые слова: бинарное поле, симметричное квадратичное расширение, след, антислед.

Ch. Glusko, S. Titov

ON QUADRATIC EXTENSIONS OF BINARY FIELDS

This paper deals with the expansion of binary fields through the operation of the symmetric quadratic extension which is closely related to ITs and microprocessor technology. Polynomials of quadratic extensions have been computed and some examples are discussed.

Keywords: binary field, a quadratic extension of a symmetric, trace, antitrace.

Необходимым условием правильной работы системы является обеспечение безопасности и защиты каналов связи. Особое значение это имеет для транспортных систем, в том числе и железнодорожных, так как, в отличие от стационарных систем связи, специфика обмена информацией на транспорте состоит в невозможности препятствия физическому проникновению злоумышленника в канал связи. Важной задачей является удаленное управление транспортными средствами с защитой информации от несанкционированного доступа к управлению, примером такого управления служат замки автомобильной сигнализации, отслеживание положения локомотива, связь диспетчера с машинистом, оформление и проверка проездных документов [7, 12, 13].

При организации транспортного производства используется более двух десятков видов связи. Все шире внедряются беспроводные технологии, такие как GSM-R, TETRA, CDMA и др. При этом важно отметить, что именно беспроводные технологии наиболее уязвимы с точки зрения информационной безопасности. Перехват информации в беспроводных системах не требует физического контакта с линией связи, что существенно упрощает задачу несанкционированного доступа к информации [7, 8].

В устройствах связи ОАО «РЖД» предполагается применение системы GSM-R как основной системы технологической радиосвязи на участках высокоскоростного и скоростного движения, а также на основных транспортных магистралях. В системах GSM, GSM-R в качестве алгоритмов шифрования используются шифры семейства A5. Стандарт шифрования A5/1, используемый в GSM-R, можно считать примером кодирующего аппарата с обратной связью и без памяти, переход от GSM к GSM-R обусловлен выявленными уязвимостями [11].

Еще одним примером кодирующего аппарата является регистр сдвига с линейной связью (РСЛОС, *Linear feedback shift register*, *LFSR*). Он состоит из двух частей: собственно регистра сдвига и функции обратной связи. Регистр состоит из битов, его длина — количество этих битов. Новый крайний слева бит определяется функцией остальных битов. На выходе регистра оказывается один, обычно младший, значащий бит. Период регистра сдвига — длина получаемой последовательности до начала ее повторения.

На рисунке 1 представлен пример сдвигового регистра *LFSR PnP*. *Plug and Play* (*PnP*) — технология, предназначенная для быстрого определения и конфигурирования технических устройств.

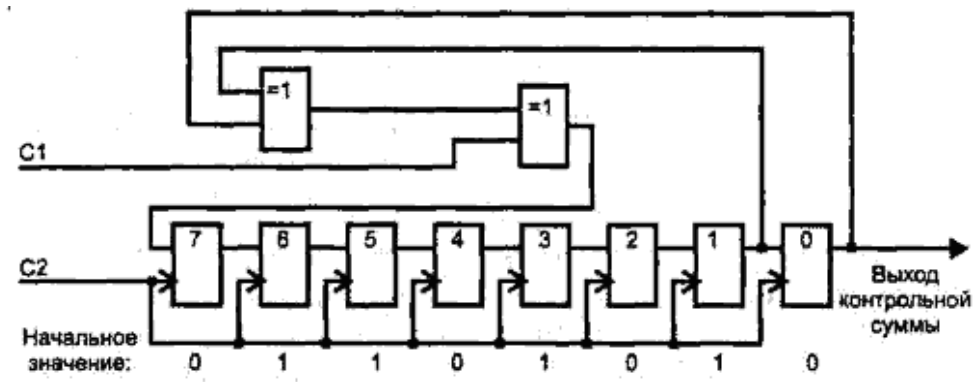

Рис. 1. Сдвиговый регистр *LFSR* карты *PnP*

Положение отводов определяется характеристическим многочленом регистра сдвига вида $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Схеме на рисунке 1 соответствует характеристический многочлен $x^8 + x + 1 = (x^2 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1)$, на $C1$ подается входная последовательность битов, вход $C2$ — тактовый. Период многочлена $f(x) = x^8 + x + 1$ будет равен 63: $\mathrm{ord}\, f(x) = 2^0$ НОК [3, с. 63] $= 1 \cdot 63 = 63$ [4].

Для оптимизации работы конечного автомата в качестве характеристического многочлена используют малочлены (идеальный случай — трехчлены), и лучше — примитивные (то есть максимального порядка).

Поэтому актуальной темой становится построение неприводимых многочленов в бинарных полях для реализации экономичных регистров сдвига с обратными связями, обладающими большими периодами работы в автономном режиме.

В связи с этим появляются следующие задачи для исследования:

1. Построение многочленов простой степени p.

2. Построение многочленов p^n, где $n = 2, 3, 4, \ldots$, построение гарантированно неприводимого многочлена данной большой степени.

3. Алгоритм построения неприводимых многочленов степени $n = pq$, где p и q — простые числа. Например, если x — корень уравнения $x^3 + x + 1$ ($p = 3$), а y — корень $y^5 + y^2 + 1$,

то для $n = 5 \cdot 3 = 15$, где $z = xy$, минимальный характеристический многочлен имеет вид $z^{15} + z^{12} + z^{10} + z^7 + z^6 + z^2 + 1$.

4. Анализ примитивности многочленов больших степеней.

Особенность вычислений в конечном поле состоит в необходимости выбора представления элементов — от него существенно зависит способ реализации, а значит, и сложность построения логических схем. Потенциально возможны разные представления, но практически используются в основном два, а именно представления в стандартных и нормальных базисах, а также производные от них. Наиболее широко используемым является представление в стандартном базисе — элементы поля в нем представляются многочленами, арифметические операции с которыми выполняются по модулю неприводимого многочлена, определяющего этот базис [9]. В работах [2, 3] рассмотрено построение нормальных базисов посредством расширения полей и применения их для решения квадратных уравнений в конечных полях [1, с. 11–15].

Рассмотрим идею расширения полей посредством операции *симметричного квадратичного расширения* (*СКР*):

$$\alpha = \beta + \beta^{-1}, \qquad (1)$$

где α является элементом поля F, β является элементом поля K, а поле K является расширением поля F [5, с. 10].

Актуальность тематики расширения бинарных полей тесно связана с изменением архитектуры в вычислительной технике: переход от битовой архитектуры к байтовой, от 32-разрядной к 64-х, а впоследствии к 1024-битовой.

Развитие в области информационных технологий увеличивает функционал видеокарт и эффективность работы. За счет распараллеливания операций обеспечивается мультибитовость. Поэтому гибкая аппаратная компоновка видеокарт благодаря рациональной организации отводов регистров сдвига может позволить реализовать широкий спектр возможностей, в том числе и взлом шифров.

GPU уже достигли той точки развития, когда многие приложения реального мира могут с легкостью выполняться на них, причем быстрее, чем на многоядерных системах. Будущие вычислительные архитектуры станут гибридными системами с графическими процессорами, состоящими из параллельных ядер и работающими в связке с многоядерными CPU.

Для более детального изучения свойств операции СКР рассмотрим функцию $x_n = h_n(x) = h(h(h\ldots(h(h(x)))))$, где $h(x) = (x + x^{-1})$ и число итераций $h(x)$ равно n. Последовательное применение операции СКР дает следующие значения x_n:

$$x_0 = x;$$

$$x_1 = \frac{(x+1)^2}{x} = \frac{x^2+1}{x} = x + x^{-1} = h_1(x);$$

$$x_2 = \frac{(x^2+x+1)^2}{x(x+1)^2};$$

$$x_3 = \frac{(x^4+x^3+x^2+x+1)^2}{x(x+1)^2(x^2+x+1)^2};$$

$$x_4 = \frac{(x^8+x^7+x^6+x^4+x^2+x+1)^2}{x(x+1)^2(x^2+x+1)^2(x^4+x^3+x^2+x+1)^2};$$

$$x_5 = \frac{(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+x^3+x^2+x+1)^2}{x(x+1)^2(x^2+x+1)^2(x^4+x^3+x^2+x+1)^2(x^8+x^7+x^6+x^4+x^2+x+1)^2};$$

$$x_6 = \frac{(x^{32}+x^{31}+x^{30}+x^{28}+x^{27}+x^{26}+x^{24}+x^{22}+x^{17}+x^{16}+x^{15}+x^{10}+x^8+x^6+x^5+x^4+x^2+x+1)^2}{x(x+1)^2(x^2+x+1)^2(x^4+x^3+x^2+x+1)^2(x^8+x^7+x^6+x^4+x^2+x+1)^2(x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}+x^8+x^5+x^4+x^3+x^2+x+1)^2}.$$

Рассмотрим свойства этой функции, одним из которых является коммутативность:

$$h_n(h_m(x)) = h_m(h_n(x)).$$

Отсюда получаем следующее равенство для операции СКР:

$$h_n(x + x^{-1}) = x_n(x) + (x_n(x))^{-1}.$$

Так, на примере x_3:

$$h_2(x + x^{-1}) = \frac{(x^2 + x^{-2} + x + x^{-1} + 1)^2}{(x + x^{-1})(x^2 + x^{-2} + 1)} = \frac{x^{-4}(x^4 + x^3 + x^2 + x + 1)^2}{x^{-3}(x^2 + 1)(x^4 + x^2 + 1)} =$$

$$= \frac{x^{-4}(x^4 + x^3 + x^2 + x + 1)^2}{x^{-3}(x^2 + 1)(x^4 + x^2 + 1)} = \frac{(x^4 + x^3 + x^2 + x + 1)^2}{x(x+1)^2(x^2 + x + 1)^2} = x_3(x).$$

Можно заметить, что числитель дроби $x_3(x)$ — это квадрат ранее вычисленного с помощью операции СКР неприводимого многочлена $D_3(x) = x^4 + x^3 + x^2 + x + 1$, а знаменатель — произведение $x(D_1(x))^2(D_2(x))^2$.

Последовательно применяя операцию СКР, получим по индукции формулу для $x_n(x)$ в общем виде.

Утверждение. Для любого $n \geq 1$ имеем

$$x_n(x) = \frac{(D_n(x))^2}{x(D_1(x))^2(D_2(x))^2 \ldots (D_{n-1}(x))^2}, \qquad (4)$$

где $D_n(x) = \Delta D_{n-1}(x) = x^{2^{n-2}}(D_{n-1}(x + x^{-1}))$, $D_1(x) = x + 1$.

По очереди вычисляем значения $D_n(x)$:

$D_2(x) = x(x + 1) = x^2 + x + 1$;

$D_3(x) = x^2((x + x^{-1})^2 + (x + x^{-1}) + 1) = x^4 + x^3 + x^2 + x + 1$;

$D_4(x) = x^4((x + x^{-1})^4 + (x + x^{-1})^3 + (x + x^{-1})^2 + (x + x^{-1}) + 1) = x^8 + x^7 + x^6 + x^4 + x^2 + x + 1$;

$D_5(x) = x^8((x + x^{-1})^8 + (x + x^{-1})^7 + (x + x^{-1})^6 + (x + x^{-1})^4 + (x + x^{-1})^2 + (x + x^{-1}) + 1) = x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^5 + x^4 + x^3 + x^2 + x + 1$;

$D_6(x) = x^{16}((x + x^{-1})^{16} + (x + x^{-1})^{15} + (x + x^{-1})^{14} + (x + x^{-1})^{13} + (x + x^{-1})^{12} + (x + x^{-1})^{11} + (x + x^{-1})^8 + (x + x^{-1})^5 + (x + x^{-1})^4 + (x + x^{-1})^3 + (x + x^{-1})^2 + (x + x^{-1}) + 1 = x^{32} + x^{31} + x^{30} + x^{28} + x^{27} + x^{26} + x^{24} + x^{22} + x^{17} + x^{16} + x^{15} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^2 + x + 1$.

Отметим [2], что корни многочленов $D_n(x)$ задают нормальные базисы полей $GF(2^m)$ при $m = 2^k$.

Примеры, представленные выше, показали, что применение операции СКР порождает цикличность многочленов, так как $\deg D_n = 2^{n-1}$ [4]. Рассмотрим подробнее многочлены, отвечающие этому критерию.

После одноразового применения операции СКР результат при зацикливании Δf делится на f, это значит, что корень x многочлена f является и корнем Δf, поэтому операция СКР просто циклически сдвигает корни многочлена f, то есть корень x этого многочлена

преобразуется в корень x^N, где $N = 2^n$, $n = 1, 2, 3, \ldots$. Цикл графа такого многочлена равен 1, для примера: это многочлены степеней 3, 4, 5 (рис. 2).

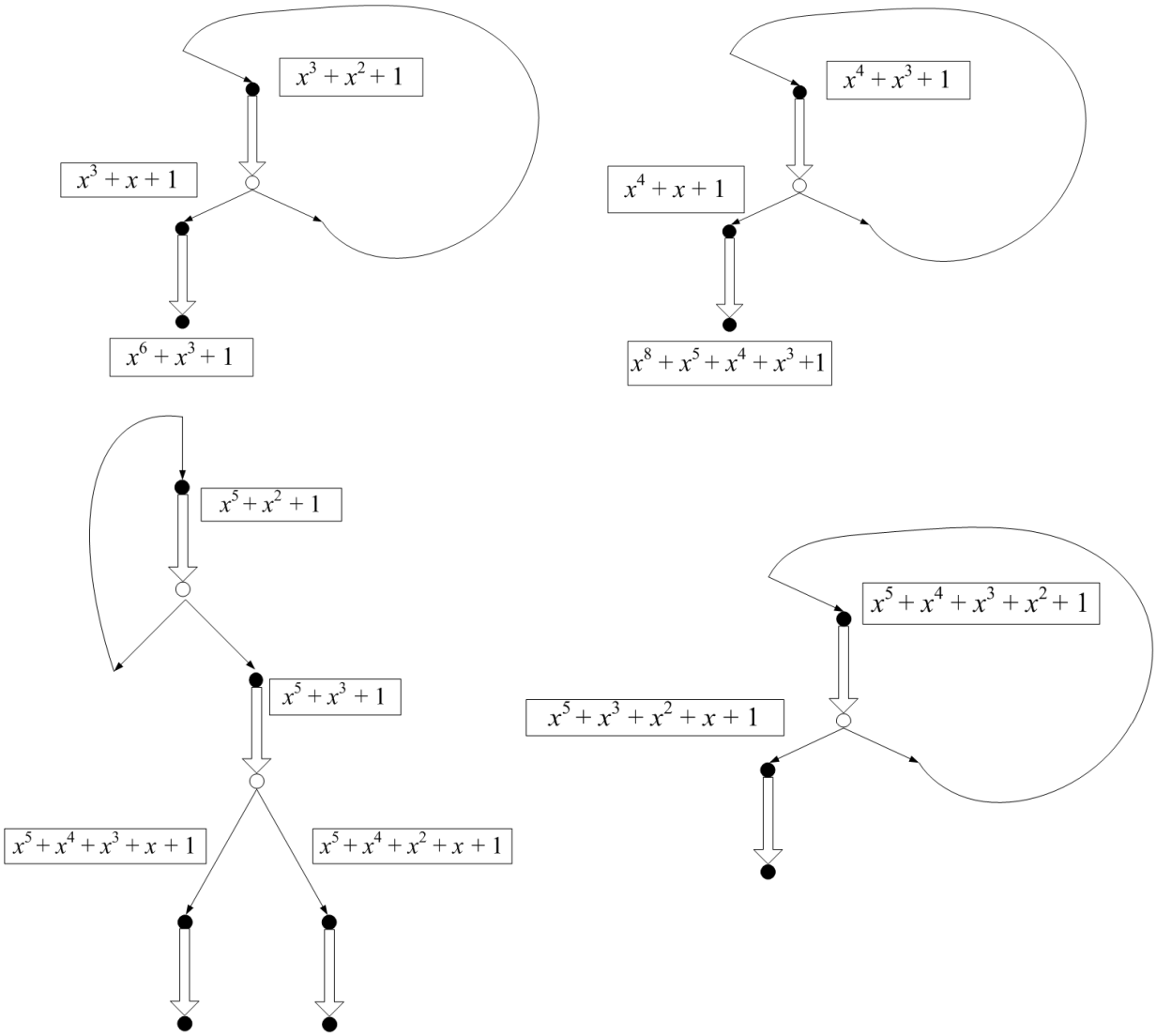

Рис. 2. Орграф неприводимых многочленов
третьей, четвертой и пятой степеней с циклом 1

Представление операции СКР для $h_1(x) = x + x^{-1}$ в виде $x + x^{-1} = x^N$ дает формулу

$$x^{N+1} + x^2 + 1 = 0. \qquad (5.1)$$

Последовательно вычислим многочлены квадратичного расширения в зависимости от значения n:

$n = 0 \quad N = 1$
$x + x^{-1} = x \qquad x^{-1} = 0 \qquad$ не существует
$n = 1 \quad N = 2$
$x + x^{-1} = x^2 \qquad x^3 + x^2 + 1 = 0 \qquad$ примитивный
$n = 2 \quad N = 4$
$x + x^{-1} = x^4 \qquad x^5 + x^2 + 1 = 0 \qquad$ примитивный

$n = 3 \quad N = 8$

$x + x^{-1} = x^8 \qquad x^9 + x^2 + 1 = (x^5 + x^4 + x^3 + x^2 + 1)(x^4 + x^3 + 1)$

$x^9 + x^2 + 1 \equiv 0 \pmod{x^5 + x^4 + x^3 + x^2 + 1}$

$x^9 + x^2 + 1 \equiv 0 \pmod{x^4 + x^3 + 1}$

$n = 4 \quad N = 16$

$x + x^{-1} = x^{16} \qquad x^{17} + x^2 + 1 = (x^3 + x^2 + 1)(x^{14} + x^{13} + x^{12} + x^{10} + x^7 + x^6 + x^5 + x^3 + 1)$,

причем оба многочлена примитивны.

$x^{17} + x^2 + 1 \equiv 0 \pmod{x^3 + x^2 + 1}$

$n = 5 \qquad N = 32$

$x + x^{-1} = x^{32} \qquad x^{33} + x^2 + 1 = 0$

$n = 6 \qquad N = 64$

$x + x^{-1} = x^{64} \qquad x^{65} + x^2 + 1 = 0$

$n = 7 \qquad N = 128$

$x + x^{-1} = x^{128} \qquad x^{129} + x^2 + 1 \equiv 0 \pmod{x^3 + x^2 + 1}$

$x^{129} + x^2 + 1 \equiv 0 \pmod{x^5 + x^2 + 1}$

$x^{129} + x^2 + 1 \equiv 0 \pmod{x^4 + x^3 + 1}$

Можно заметить, что многочлены степени p повторяются через p шагов, так как в поле $GF(2^p)$ $x^{(2^p)^2} = x^{(2^p)2^p} = x^{2^p} = x$; к примеру, в поле $GF(2^3)$ $x^{64} = (x^8)^8 = x^8 = x$.

После двукратного применения операции СКР для $x_2 = \dfrac{(x^2 + x + 1)^2}{x(x+1)^2} = x^N$, домножив обе части на $x^2(x + x^{-1})$, получаем следующую формулу:

$$x^{N+3} + x^{N+1} + x^4 + x^{-2} + 1 = 0. \tag{5.2}$$

Цикл графов таких многочленов будет равен 2, то есть после двух применений операции СКР корень x многочлена $\Delta^2 f$ будет корнем многочлена f, таким образом, они получаются друг из друга путем возведения в степень двойки. Все многочлены с циклом 1 удовлетворяют уравнению для циклов 2, 3 и т. д., так как накручивание цикла даст тот же результат, по аналогии многочлены с циклом 2 будут удовлетворять циклам 2^p. Примерами графов с циклом, равным 2, являются графы седьмой и девятой степеней (рис. 3).

Последовательно вычислим многочлены по данной формуле в зависимости от значения n:

$n = 0 \qquad N = 1$

$x^4 + x^2 + x^4 + x^2 + 1 = 0 \qquad 1 = 0 \qquad$ не существует

$n = 1 \qquad N = 2$

$x^5 + x^4 + x^3 + x^2 + 1 = 0 \qquad$ примитивный

$n = 2 \qquad N = 4$

$x^7 + x^5 + x^4 + x^2 + 1 = (x^3 + x^2 + 1)(x^4 + x^3 + 1)$

$n = 3 \qquad N = 8$

$x^{11} + x^9 + x^4 + x^2 + 1 = 0 \qquad$ примитивный

$n = 4 \qquad N = 16$

$x^{19} + x^{17} + x^4 + x^2 + 1 = (x^5 + x^2 + 1)(x^7 + x^5 + x^4 + x^3 + 1)(x^7 + x^3 + 1) = 0$

После трехкратного применения операции СКР для $x_3 = \dfrac{(x^4 + x^3 + x^2 + x + 1)^2}{x(x+1)^2(x^2 + x + 1)^2} = x^N$ итоговая формула выглядит следующим образом:

$$x^{N+7} + x^{N+1} + x^8 + x^6 + x^4 + x^2 + 1 = 0. \tag{5.3}$$

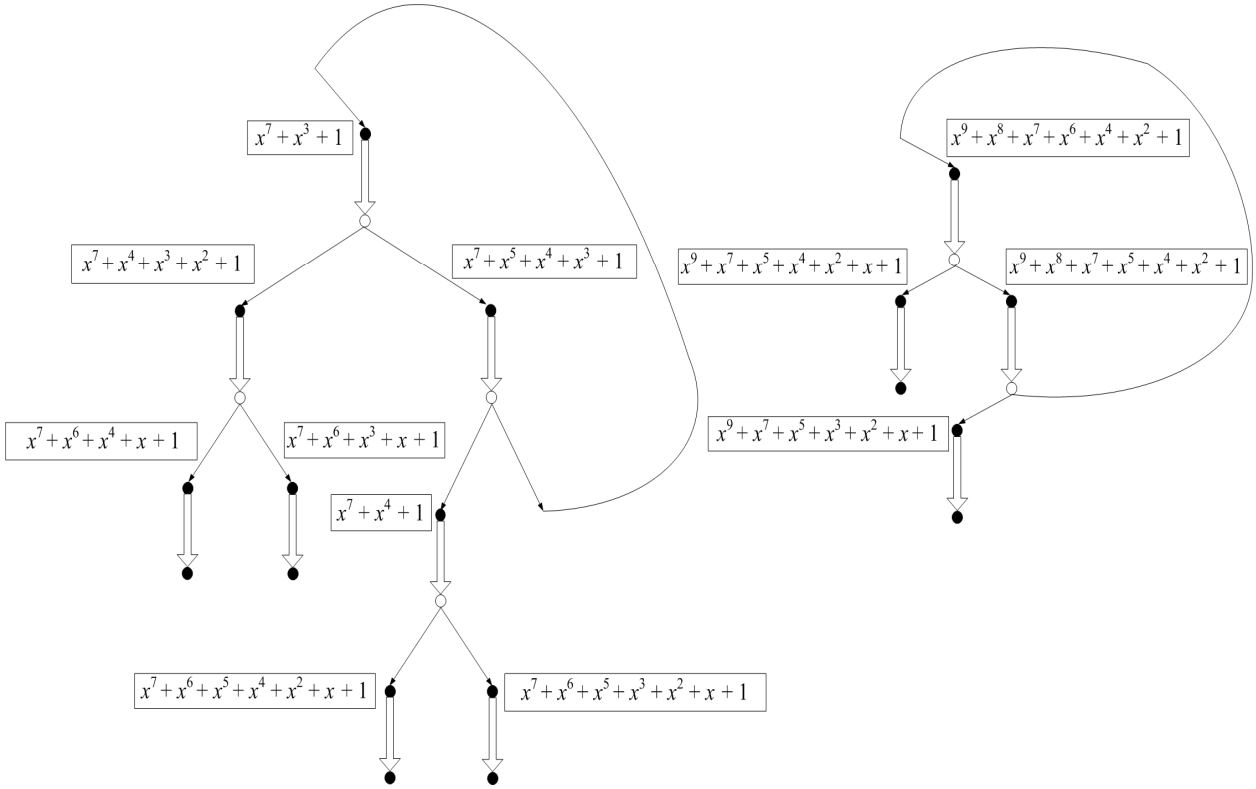

Рис. 3. Орграф неприводимых многочленов
седьмой и девятой степеней с циклом 2

Пример графа цикла 3 — многочлены шестой степени (рис. 4).

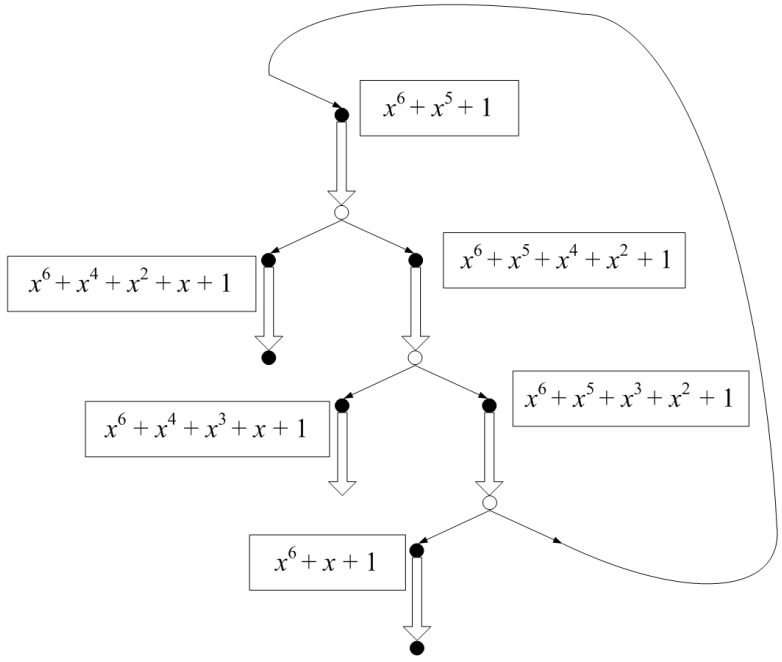

Рис. 4. Орграф неприводимых многочленов шестой степени с циклом 3

Последовательно вычислим многочлены по данной формуле в зависимости от значения n:

$n = 0 \quad N = 1$

$(x^8 + x^6 + 1) = (x^3 + x^2 + 1)^2 = 0$

$n = 1 \quad N = 2$

$x^9 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 = (x^4 + x^3 + 1)(x^5 + x^2 + 1) = 0$

$n = 2 \quad N = 4$

$x^{11} + x^8 + x^6 + x^5 + x^4 + x^2 + 1 = 0$ примитивный

$n = 3 \quad N = 8$

$x^{15} + x^{11} + x^8 + x^6 + x^4 + x^2 + 1 = (x^3 + x^2 + 1)(x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + + x^4 + x^3 + 1) = 0$

После четырех раз применения к исходному многочлену операции СКР для $x_4 = \dfrac{(x^8 + x^7 + x^6 + x^4 + x^2 + x + 1)^2}{x(x+1)^2(x^2 + x + 1)^2(x^4 + x^3 + x^2 + x + 1)^2} = x^N$ итоговая формула выглядит следующим образом:

$$x^{N+15} + x^{N+13} + x^{N+11} + x^{N+5} + x^{N+3} + x^{N+1} + x^{16} + x^{14} + x^{12} + x^8 + x^4 + x^2 + 1 = 0. \qquad (5.4)$$

Примеров графов многочленов цикла, равного 4, до десятой степени нет.

Последовательно вычислим многочлены по данной формуле в зависимости от значения n:

$n = 0 \quad N = 1 \qquad x^8 + x^6 + 1 = (x^4 + x^3 + 1)^2 = 0$

$n = 1 \quad N = 2 \qquad x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1 =$

$= (x^3 + x^2 + 1)(x^7 + x^5 + x^4 + x^3 + 1)(x^7 + x^3 + 1) = 0$

С помощью операции СКР можно осуществить перебор всех неприводимых многочленов, причем они разделятся на три группы в зависимости от значений следа $Tr(x)$ и антиследа $Tr(x^{-1})$ элемента x. Каждая из этих групп образует свой орграф, вид которых также зависит от значений следа и антиследа многочлена.

Если у многочлена l степени $n = 2^k$ корень x удовлетворяет условиям $Tr(x) = 1$, $Tr(x^{-1}) = 0$, то после применения операции СКР получим многочлен $2n$-й степени $t(X) = p(X)q(X)$, где $p(X)$ и $q(X)$ суть неприводимые многочлены степени n, один из которых аналогичен l, для его корня u справедливы равенства $Tr(u) = 1$, $Tr(u^{-1}) = 0$, а другой ему симметричен (взаимно возвратен), то есть для его корня v справедливы равенства $Tr(v) = 0$, $Tr(v^{-1}) = 1$, $v = u^{-1}$. Причем после прохождения определенного числа шагов — цикла (к примеру, для $n = 8$ цикл равен $n - 1 = 7$) получается исходный многочлен $l(x)$ n-й степени. Если же у многочлена n-й степени $Tr(x) = 0$, $Tr(x^{-1}) = 1$, то после применения операции СКР получится неприводимый многочлен степени $2n$. Такие многочлены со значениями $Tr(x) = Tr(x^{-1}) + 1$ образуют циклический орграф.

Орграфы многочленов различных степеней со значениями $Tr(x) = Tr(x^{-1}) + 1$ имеют циклический вид разной длины: длиной 1 для 3, 4, 5-й степеней, длиной 2 для 9-й степени, длиной 3 для 6-й степени, длиной 5 для 7-й степени, длиной 7 для 8-й степени, длиной 12 для 9-й степени, длиной 27 для 10-й степени. В свою очередь, графы многочленов со значениями $Tr(x) = Tr(x^{-1})$ зацикливаются у 5-й (цикл = 1), 7-й (цикл = 2), 9-й (цикл = 7) и 10-й (цикл = 5) степеней.

Анализируя представленные выше орграфы, можно сделать следующие выводы:

1. Коэффициент при элементе x определяет приводимость многочлена, полученного из данного с помощью операции СКР (если у многочлена $f(x)$ коэффициент при x равен 1, то $\Delta f(x)$ неприводимый многочлен, если равен 0 — $\Delta f(x)$ приводимый).

2. Взаимосвязь значений следа и антиследа многочлена определяет вид орграфа, который порождает данный многочлен.

Итак, посредством применения операции симметричного квадратичного расширения можно последовательно построить расширения полей, таким образом, облегчив задачу нахождения неприводимых многочленов (малочленов) больших степеней с заданными свойствами.

На основании рассмотренных примеров можно говорить об упорядочивании неприводимых многочленов в зависимости от их значений следа и антиследа и представлении этой зависимости в виде орграфов [4].

Идея расширения полей нашла свое практическое применение в информационных технологиях, где стремительно совершенствуются архитектура и конструкция вычислительной техники, а также при производстве микропроцессорных устройств, таких как конечные автоматы, работа которых зависит от запрограммированного характеристического многочлена. Такие автоматы нашли широкое применение при построении (организации) каналов связи в различных областях, в том числе на транспорте.

СПИСОК ЛИТЕРАТУРЫ

1. *Болотов А. А., Гашков С. Б., Фролов А. Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006. С. 76–81.

2. *Глуско К. Л., Титов С. С.* Нормальные базисы и дерево квадратичных расширений бинарных полей // Некоторые актуальные проблемы современной математики и математического образования: Материалы научной конференции «Герценовские чтения — 2012». СПб.: БАН, 2012. С. 221–226.

3. *Глуско К. Л., Титов С. С.* Решение квадратных уравнений в конечных полях характеристики два // Проблемы теоретической и прикладной математики: Труды 43-й Всероссийской молодежной конференции. Екатеринбург: УрО РАН, 2012. С. 23–25.

4. *Глуско К. Л., Титов С. С.* Специфика проблем связи и управления на транспорте // Инновационный транспорт. Екатеринбург: Изд-во УрГУПС. 2012. № 2 (3). С. 44–50.

5. *Демкина О. Е., Титов С. С., Торгашова А. В.* Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования // Молодые ученые — транспорту: Труды IV научно-технической конференции. Екатеринбург: Изд-во УрГУПС, 2003. С. 391–404.

6. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. С. 41–53.

7. *Паршин А. В.* Классический протокол пакетной коммутации: Монография. Екатеринбург: Изд-во УрГУПС, 2007. 242 с.

8. *Рожнев А. Ю.* Теория запретов многобитовых функций и ее применимость в системах связи на железнодорожном транспорте // Современные проблемы науки и образования. 2012. № 2; URL: www.science-education.ru/102-5849.

9. *Сергеев И. С.* О реализации некоторых операций в конечных полях схемами логарифмической глубины: Автореф. дис. … канд. физ.-мат. наук. М., 2007. 96 с.

10. *Титов С. С., Торгашова А. В.* Генерация неприводимых многочленов, связанных степенной зависимостью корней // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. № 2 (22). Ч. 1. С. 310–318.

11. *Biryukov A., Shamir A., Wagner A.* Real Time Cryptanalysis of A5/1 on a PC. Fast Software Encryption Workshop. 2000. April 10–12. P. 1–18.

12. *Koblitz N.* Hyperelliptic cryptosystems // Journal of cryptology. 1989. N 1. P. 139–150.

13. *Koblitz N.* Algebraic aspects of Cryptography: Springer. 2004. 109 p.

14. *Menezes A. J., Vanstone S.* Elliptic Curve Cryptosystems and their implementation // Journal of Cryptology. 1993. N 6. P. 209–224.

15. *Rosing M.* Implementing Elliptic Curve Cryptography. Greenwich: Manning Publication, 1998. 338 p.

REFERENCES

1. *Bolotov A. A., Gashkov S. B., Frolov A. B.* Elementarnoe vvedenie v jellipticheskuju kriptografiju: Protokoly kriptografii na jellipticheskih krivyh. M.: KomKniga, 2006. S. 76–81.
2. *Glusko K. L., Titov S. S.* Normal'nye bazisy i derevo kvadratichnyh rasshirenij binarnyh polej // Nekotorye aktual'nye problemy sovremennoj matematiki i matematicheskogo obrazovanija: Materialy nauchnoj konferencii «Gercenovskie chtenija — 2012». SPb.: BAN, 2012. S. 221–226.
3. *Glusko K. L., Titov S. S.* Reshenie kvadratnyh uravnenij v konechnyh poljah harakteristiki dva // Problemy teoreticheskoj i prikladnoj matematiki: Trudy 43-j Vserossijskoj molodezhnoj konferencii. Ekaterinburg: UrO RAN, 2012. S. 23–25.
4. *Glusko K. L., Titov S. S.* Specifika problem svjazi i upravlenija na transporte // Innovacionnyj transport. Ekaterinburg: Izd-vo UrGUPS. 2012. № 2 (3). S. 44–50.
5. *Demkina O. E., Titov S. S., Torgashova A. V.* Rekurrentnoe vychislenie neprivodimyh mnogochlenov v zadachah dvoichnogo kodirovanija // Molodye uchenye — transportu: Trudy IV nauchno-tehnicheskoj konferencii. Ekaterinburg: Izd-vo UrGUPS, 2003. S. 391–404.
6. *Logachev O. A., Sal'nikov A. A., Jawenko V. V.* Bulevy funkcii v teorii kodirovanija i kriptologii. M.: MCNMO, 2004. S. 41–53.
7. *Parshin A. V.* Klassicheskij protokol paketnoj kommutacii: Monografija. Ekaterinburg: Izd-vo UrGUPS, 2007. 242 s.
8. *Rozhnev A. Ju.* Teorija zapretov mnogobitovyh funkcij i ee primenimost' v sistemah svjazi na zheleznodorozhnom transporte // Sovremennye problemy nauki i obrazovanija. 2012. № 2; URL: www.science-education.ru/102-5849.
9. *Sergeev I. S.* O realizacii nekotoryh operacij v konechnyh poljah shemami logarifmicheskoj glubiny: Avtoref. dis. … kand. fiz.-mat. nauk. M., 2007. 96 s.
10. *Titov S. S., Torgashova A. V.* Generacija neprivodimyh mnogochlenov, svjazannyh stepennoj zavisimost'ju kornej // Doklady Tomskogo gosudarstvennogo universiteta sistem upravlenija i radiojelektroniki. 2010. N 2 (22). Ch. 1. S. 310–318.
11. *Biryukov A., Shamir A., Wagner A.* Real Time Cryptanalysis of A5/1 on a PC. Fast Software Encryption Workshop. 2000. April 10–12. P. 1–18.
12. *Koblitz N.* Hyperelliptic cryptosystems // Journal of cryptology. 1989. N 1. P. 139–150.
13. *Koblitz N.* Algebraic aspects of Cryptography: Springer. 2004. 109 p.
14. *Menezes A. J., Vanstone S.* Elliptic Curve Cryptosystems and their implementation // Journal of Cryptology. 1993. N 6. P. 209–224.
15. *Rosing M.* Implementing Elliptic Curve Cryptography. Greenwich: Manning Publication, 1998. 338 p.

А. В. Коптев

МЕТОД ПОСТРОЕНИЯ РЕШЕНИЙ УРАВНЕНИЙ НАВЬЕ — СТОКСА

Рассматриваются уравнения Навье — Стокса для движения вязкой несжимаемой жидкости. Предлагается процедура аналитического построения решений на основе первого интеграла уравнений и уравнения Риккати в частных производных. Построены некоторые новые решения, представляющие практический интерес.

Ключевые слова: частная производная, дифференциальное уравнение, движение, жидкость, интеграл, вязкость, вихрь.